Západočeská univerzita v Plzni

Fakulta pedagogická

Diplomová práce

PROBLEMATIKA OCHRANY A BEZPEČNOSTI DAT NA STANICÍCH S OS MS WINDOWS PROVOZOVANÝCH VE ŠKOLNÍM PROSTŘEDÍ

Jakub Kubát

Plzeň 2012

Prohlašuji, že jsem práci vypracoval(a) samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni, 15.06.2012

……

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta pedagogická
Akademický rok: **2009/2010**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jakub KUBÁT, DiS.**
Studijní program:	**N7503 Učitelství pro základní školy**
Studijní obory:	**Učitelství informatiky pro 2. st. ZŠ** **Učitelství technické výchovy pro 2. st. ZŠ**
Název tématu:	**Problematika ochrany a bezpečnosti dat na stanicích s OS MS Windows provozovaných ve školním prostředí**
Zadávající katedra:	**Katedra výpočetní a didaktické techniky**

Zásady pro vypracování:

1. Popište základní principy, zásady, mechanismy ochrany dat s ohledem na specifika školního prostředí.
2. Zaměřte se na bezpečnost a ochranné mechanismy na stanicích s OS MS Windows.
3. Analyzujte základní problémy a mechanismy nežádoucích vlivů, navrhněte možnosti jejich řešení.
4. Analyzujte problematiku šifrovaných připojení, identifikaci a certifikáty serverů a osob. Realizujte a demonstrujte na konkrétních příkladech.
5. Analyzujte problematiku elektronického podpisu. Realizujte a demonstrujte konkrétním příkladem ve zvoleném poštovním prostředí.

Rozsah grafických prací:

Rozsah pracovní zprávy: **40 - 100 stran + CD**

Forma zpracování diplomové práce: **tištěná**

Seznam odborné literatury:

1. **Certifikáty, elektronický podpis [online]. 2010 [cit. 2010-01-04]. Dostupný z WWW: ⟨http://support.zcu.cz/⟩.**
2. **Manuály OS Microsoft Windows**
3. **OS Microsoft Windows [online]. 2010 [cit. 2010-01-04]. Dostupný z WWW: ⟨http://support.microsoft.com/⟩.**
4. **Endorf, C. Hacking - detekce a prevence počítačového útoku. Praha : Grada, 2005. 200 s. ISBN 80-247-1035-8.**
5. **Doseděl, T. Počítačová bezpečnost a ochrana dat. Brno : Computer Press, 2004. 230 s. ISBN 80-251-0106-1.**
6. **Eisenkolb, K. Bezpečnost Windows 2000/XP. Praha : Computer Press, 2003. 290 s. ISBN 80-7226-789-2.**

Vedoucí diplomové práce: **Dr. Ing. Jiří Toman**
Katedra výpočetní a didaktické techniky

Datum zadání diplomové práce: **4. ledna 2010**

Termín odevzdání diplomové práce: **15. března 2011**

v.z. J. Coufalová

Doc. PaedDr. Jana Coufalová, CSc.
děkanka

L.S.

Doc. Ing. Václav Vrbík, CSc.
vedoucí katedry

V Plzni dne 18. ledna 2010

OBSAH

1 ÚVOD

Počítače jsou v dnešní době neodmyslitelnou součástí našeho života. Používají se ve firmách, státním a veřejném sektoru, ale i v domácnostech. Je proto zcela logické, že se v rámci vyučovacího procesu používají i na školách. Již od dob, kdy se počítače začaly masivněji používat v komerční sféře, vznikly nároky na ochranu a bezpečnost dat. S příchodem počítačových sítí, hlavně pak sítě Internet, se nároky na bezpečnost a ochranu dat mnohonásobně zvýšily. V tuto chvíli již bylo nutné řešit ochranu a bezpečnost dat nejen v rámci lokálních stanic, ale i v rámci celých počítačových sítí. K základním ochranným prostředkům, jako byla například autentizace uživatele a zabezpečení dat na lokálních stanicích, přibyla řada dalších. Jednalo se především o mechanismy zabraňující poškození, smazání a únikům dat v počítačových sítích. Nutné bylo také sáhnout k řešení, které by vhodným způsobem zajišťovalo ověření identit osob a počítačů při síťové komunikaci.

Nutnost použití řady těchto bezpečnostních prostředků se nevyhnula ani školám. V rámci zajištění ochrany a bezpečnosti dat učitelů a žáků bylo nutné začít řešit správu těchto účtů centralizovaným způsobem. Často se tak na základních školách začaly používat doménové servery, pomocí kterých se nastavila bezpečnostní politika efektivním způsobem.

Cílem této práce je poskytnout komplexní pohled na aktuálně používané bezpečnostní mechanismy na stanicích s operačními systémy rodiny Microsoft Windows, které jsou provozovány ve školním prostředí. Velký důraz je kladen na uvedení praktických příkladů, které lépe demonstrují nastavení ochranných prostředků. Praktické příklady jsou doplněny metodickými obrázky. Pokud není v textu práce uvedeno jinak, jsou postupy nastavení ochranných prostředků popsány v operačním systému Microsoft Windows 7.

2 ZABEZPEČENÍ STANIC S OS MICROSOFT WINDOWS

V této kapitole shrneme celou řadu bezpečnostních prvků v operačních systémech rodiny Microsoft Windows. Jedná se o základní bezpečnostní prvky, které je potřeba používat na všech počítačových stanicích, včetně stanic provozovaných ve školním prostředí.

2.1 BRÁNA FIREWALL

Jedním ze základních bezpečnostních prvků je brána Firewall. Pro prvotní pochopení funkce brány Firewall uveďme jednoduchý příklad. Bránu firewall si můžeme představit jako vratného, který hlídá provoz u brány určité společnosti. Ten, kdo chce projet dál, se musí legitimovat (ověření totožnosti) a také musí vrátnému sdělit, za kým jede (cíl cesty). Vrátný má pak většinou dvě možnosti, buď dotyčného pustí, nebo ho pošle pryč. Samozřejmě, vrátný takto nepostupuje pokaždé. Pokud se jedná o osobu, která do společnosti jezdí často, vrátný si ji zapamatuje a nemusí ji pokaždé legitimovat. Do společnosti ji samozřejmě pustí. Opusťme tento jednoduchý příklad a řekněme si, jak je to s bránou firewall u osobních počítačů.

Brána firewall je software[1] či hardware[2], který vhodným způsobem propouští informace a hlídá komunikaci mezi počítači, které se nachází v počítačové síti. Počítače se mohou nacházet ve stejné, nebo naopak i v různých počítačových sítích. Právě přes místní síť nebo Internet[3] často dochází k útokům Hackerů, či k napadení Vašeho počítače škodlivým softwarem (červy, trojskými koni). Dalším úkolem brány Firewall může být i kontrola, zda Váš počítač tento škodlivý software neodesílá ven do sítě.

Činnost a princip funkce firewallů se liší podle toho, na jaké úrovni sedmivrstvého modelu ISO / OSI[4] pracují. Podle toho můžeme firewally rozdělit do dvou základních skupin.

2.1.1 FIREWALLY PRACUJÍCÍ NA ÚROVNI SÍŤOVÉ A TRANSPORTNÍ VRSTVY

Na úrovni síťové a transportní vrstvy jsou data (informace) přenášena v samostatných blocích, které se nazývají pakety. Firewally pracující na této úrovni jsou proto nejčastěji nazývány "Paketové filtry". Paket se skládá ze dvou hlavních částí:

[1] **Software je** programové vybavení počítače. Můžeme říct, že software jako takový nelze uchopit do ruky. Mezi zástupce můžeme zařadit například operační systém, ovladače zařízení, atd.
[2] **Hardware** je technické (fyzické) vybavení počítače. Tato zařízení lze uchopit do ruky. Může se jednat například o monitor, pevné disky, klávesnici, atd.
[3] **Internet** je celosvětová počítačová síť, která se skládá z velkého množství menších, vzájemně propojených sítí.
[4] **Model ISO/OSI** je referenční komunikační model, který rozděluje síťovou komunikaci do jednotlivých úrovní (vrstev).

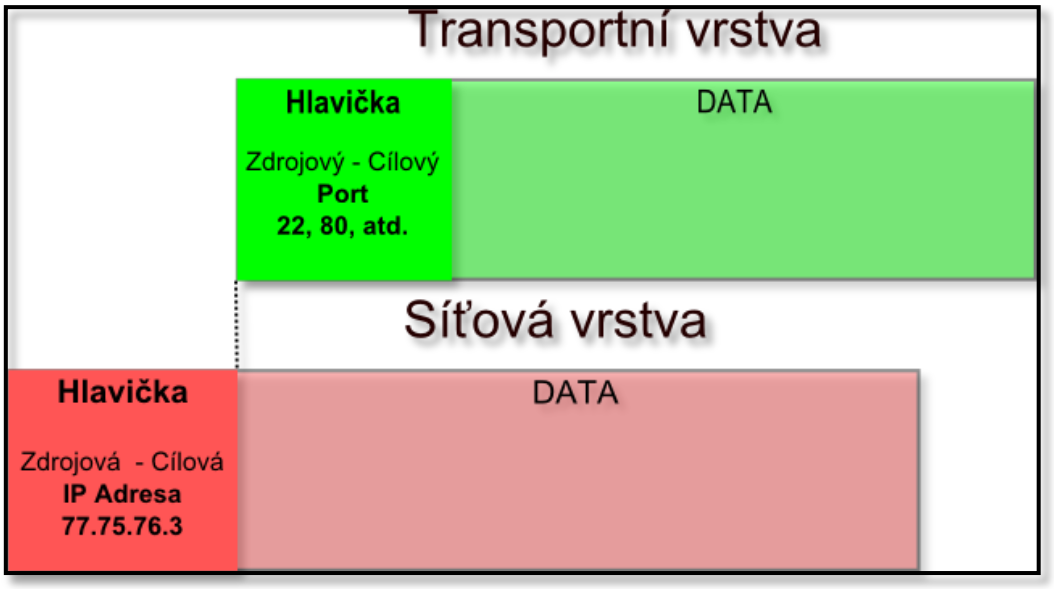
a) **Řídících dat** - Nesou informace o směrování paketu, například zdrojovou a cílovou adresu. Nacházejí se nejčastěji v hlavičce paketu nebo na jeho konci.

b) **Uživatelských dat** - Část konkrétních informací. Nacházejí se mezi hlavičkou a koncem paketu.

Úkolem paketového filtru je prozkoumat hlavičku paketu, zjistit adresu příjemce a odesilatele a podle toho se rozhodnout, zda daný paket dál propustit, nebo ho odmítnout (zahodit, odfiltrovat). Nutno zmínit, že adresa příjemce a odesilatele a také její tvar je dán určitými pravidly, která stanovuje sada komunikačních protokolů. V počítačových sítích je to pak nejběžněji sada protokolů TCP/IP, které určují jakým způsobem a podle jakých pravidel má komunikace mezi počítači probíhat. Zkoumaná adresa v hlavičkách paketů, se kterou pracují "paketové filtry", se pak nazývá IP adresa.

Podle toho, co jsme si řekli v předchozím odstavci, dokážou "paketové filtry" na úrovni **síťové vrstvy** zakázat nebo povolit veškerou komunikaci od určitého vnějšího, popřípadě vnitřního uzlu sítě (počítače - serveru). Co když ale potřebujeme přenést mezi uzly sítě pouze konkrétní druh informací, například zprávy elektronické pošty. V tomto případě musí "paketové filtry" pracovat nejen na úrovni síťové vrstvy, ale také na úrovni **vrstvy transportní** modelu ISO/OSI. Na této úrovni mohou totiž z daného paketu zjistit číslo portu, podle kterého poznají, o jaký typ informace se jedná. Například zprávy elektronické pošty jsou odesílány na port 25 a přenos souborů protokolem FTP[5] probíhá na portu 20. Následující obrázek ukazuje, jaké informace obsahuje paket ve dvou výše zmiňovaných vrstvách protokolu ISO/OSI.

[5] **FTP** je protokol určený pro přenos souborů v počítačové síti.



Obrázek 1, Vrstvy 1

2.1.2 FIREWALLY PRACUJÍCÍ NA ÚROVNI APLIKAČNÍ VRSTVY

Firewally pracující na transportní a síťové vrstvě jsou omezeny tím, že nemohou z přicházejících dat získat podrobnější informace. Zjistí pouze cílovou a zdrojovou IP adresu, popřípadě čísla portů, na která data přistupují. Nedokážou ale zjistit, o jaký formát dat se jedná a tím pádem neznají ani jeho obsah. Díky tomuto omezení nedokážou tyto firewally zachytit některé druhy útoků a tím pádem do jisté míry vystaví Vaše informace nebezpečí. Tento problém řeší firewally pracující na aplikační vrstvě - nejčastěji se označují názvem "Aplikační brány". Aplikační brány zkoumají přicházející data podrobněji, zjišťují konkrétní typ protokolu a dokážou jednotlivé druhy dat lépe analyzovat a odlišit. Můžeme si představit, že takových bran je více, přičemž každá je specializovaná pro konkrétní typ dat. Některá na poštovní zprávy, některá například na hrozby přicházející přes nezabezpečené protokoly http. Každá je specializovaná pro danou oblast a může tak lépe vyhodnotit, zda mohou být příchozí data škodlivá a podle toho zablokovat jejich postup dále. Jak vypadá paket na úrovni aplikační vrstvy, znázorňuje následující obrázek.

Obrázek 2, Vrstvy 2

2.1.3 FIREWALLY V OPERAČNÍCH SYSTÉMECH MS WINDOWS

Na počítačích s operačními systémy společnosti Microsoft jsou ve většině případů použity firewally nesoucí označení "stavové brány". To že jsou firewally stavové znamená, že ukládají informace o povolených spojeních. Pokud bylo někdy v minulosti spojení přijato, je toto konkrétní spojení zaznamenáno do databáze. Pokaždé, kdy přijde požadavek na identické spojení, firewall toto spojení již znovu nezkoumá a podle existujícího záznamu v databázi ho přijme. Tento typ firewallů je například součástí operačních systémů Microsoft Windows XP, Windows Vista, Windows 7 a dalších.

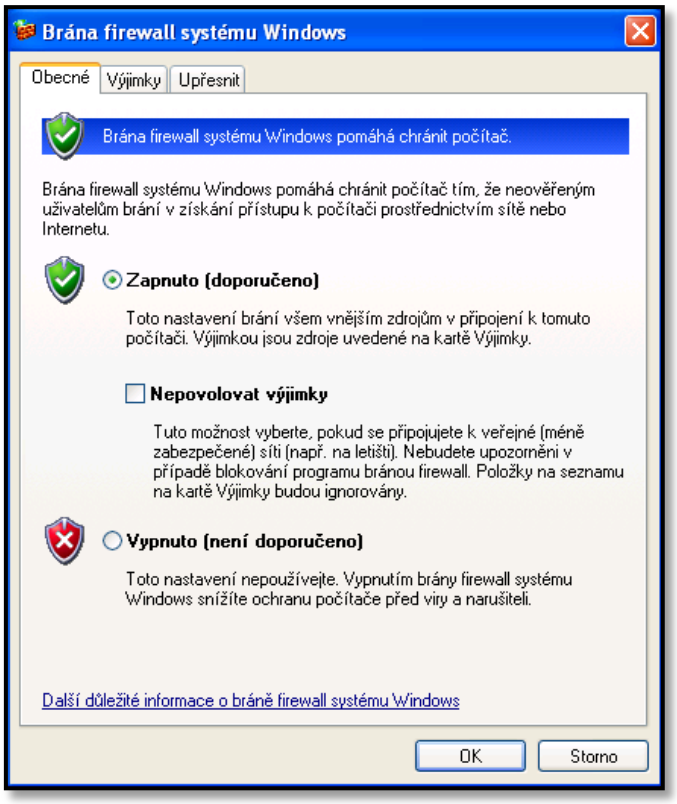
V dnešní době samozřejmě existuje mnoho firem, které vyvíjejí své vlastní firewally, nebo dokonce komplexní řešení pro zabezpečení počítače obsahující v jednom softwaru jak bránu firewall, antivirový program, tak třeba i antispyware[6].

My si v této kapitole ukážeme, kde v operačních systémech Windows najdeme bránu Firewall a popíšeme také její nastavení.

2.1.3.1 WINDOWS XP

To, zda je brána firewall aktivní, zjistíme jednoduchým způsobem. Stiskneme tlačítka **Start -> Nastavení -> Ovládací panely -> Brána Firewall systému Windows**. Zobrazí se nám nové okno "Brána Firewall systému Windows". Pro lepší představu se můžete podívat na obrázek č. 3. Implicitně je brána nastavena jako zapnutá. Pokud v systému Windows používáte bránu Firewall od jiného výrobce, doporučuje se, abyste Bránu firewall systému Windows vypnuli. Vypnutí provedete zaškrtnutím volby **Vypnuto.**

[6] **Antispyware je** program pro odstranění škodlivého softwaru - Spywaru. Spyware je nežádoucí software, který samovolně rozesílá data z Vašeho počítače.



Obrázek 3, Základní nastavení Windows Firewall

Pro další popis budeme brát v úvahu skutečnost, že používáte bránu Firewall systému Windows. Pokud je brána zapnuta, automaticky blokuje všechnu nevyžádanou příchozí komunikaci. Pokud bude chtít některý z nových programů komunikovat po síti, objeví se v systému Windows okno "**Výstraha zabezpečení systému Windows**". V tomto okně budete informováni, který z programů se snaží se sítí komunikovat. Budeme mít tři možnosti, jak tuto skutečnost vyřešit.

a) **Odblokovat** - Bude vytvořena výjimka, která povolí programu kdykoli komunikovat s vnější sítí. Výjimku najdete na kartě "Výjimky" a bude povolena. Kdykoli bude chtít tento program komunikovat po síti, okno "Výstraha zabezpečení systému Windows" se Vám již nezobrazí.

b) **Blokovat -** Bude vytvořena výjimka, ale nebude aktivní. Tento program nebude schopen komunikovat v síti a přijímat tak data. Okno "Výstraha zabezpečení systému Windows" se Vám již nezobrazí.

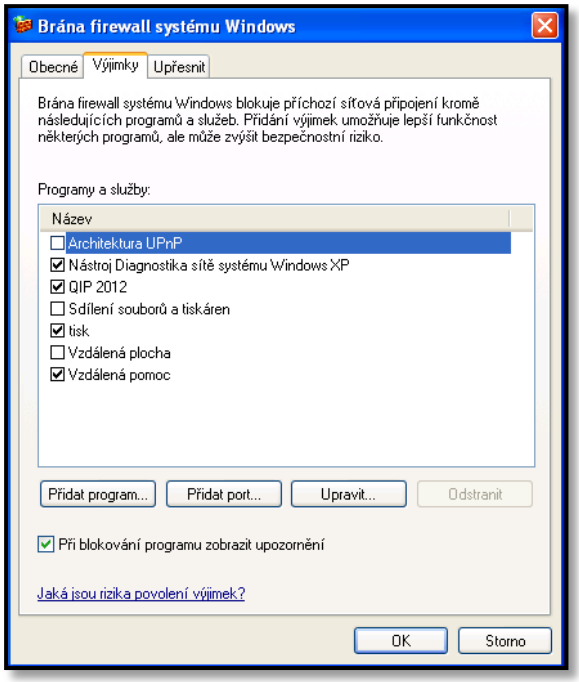
c) **Odložit dotaz na později** - Výjimka nebude vytvořena, program nebude moci komunikovat po síti. Pokaždé, kdy bude chtít program opět navázat spojení po síti, objeví se znovu okno "**Výstraha zabezpečení systému Windows**".

Programy, které nebudou uvedeny v seznamu výjimek, nebudou moci komunikovat po síti. V odborné terminologii to znamená, že programy, které se pokusí naslouchat přenosu na portu TCP nebo UDP, nebudou schopny přijímat data po síti. Může však nastat situace, kdy jste na předchozí výzvu **"Výstraha zabezpečení systému Windows"** nereagovali a potřebujete program přidat do výjimek ručním způsobem. V tomto okamžiku máme dvě možnosti, jak to udělat.

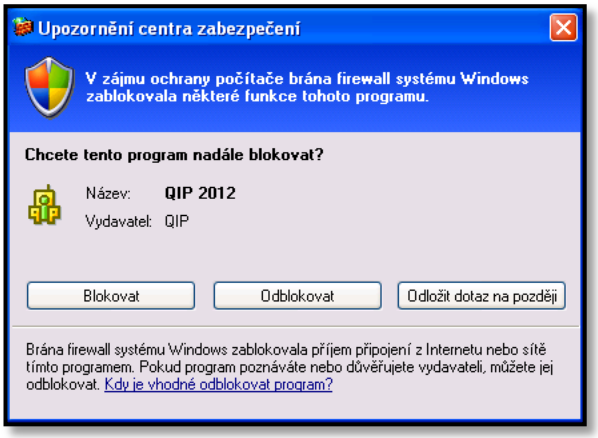
a) Konkrétní program přidáme do seznamu výjimek.

b) Najdeme konkrétní port, který daný program používá a přidáme ho do seznamu výjimek.

Pokud se na kartu výjimek přepneme, zobrazí se nám okno, kde můžeme přidat konkrétní program, nebo konkrétní číslo portu. Program vybereme tak, že stiskneme volbu **Přidat program** a vybereme ho z nabídky. Můžeme ho také najít pomocí tlačítka **Procházet**. Na následujících obrázcích je vidět karta "Výjimky" a karta "Upozornění centra zabezpečení".



Obrázek 4, Výjimky firewall



Obrázek 5, Výstraha centra zabezpečení

Některé programy mají již implicitně výjimky vytvořeny po nainstalování systému Windows. V následující tabulce uvedeme některé z nich a popíšeme jejich funkci.

Výjimka	Popis
Vzdálená plocha	Otevře port TCP 3389. Váš počítač může být vzdáleně ovládán pomocí funkce "Připojení ke vzdálené ploše".
Sdílení souborů a tiskáren	Otevře porty TCP 139 a 445 a porty UDP 137 a 138. Umožňuje sdílet soubory, složky a tiskárny v rámci sítě.
Architektura UPnP	Otevře port TCP 2869 a port UDP 1900. Umožňuje podporovat technologii UPnP (Universal Plug and Play).

Tabulka 1, Výjimky firewall

2.1.3.2 WINDOWS 7

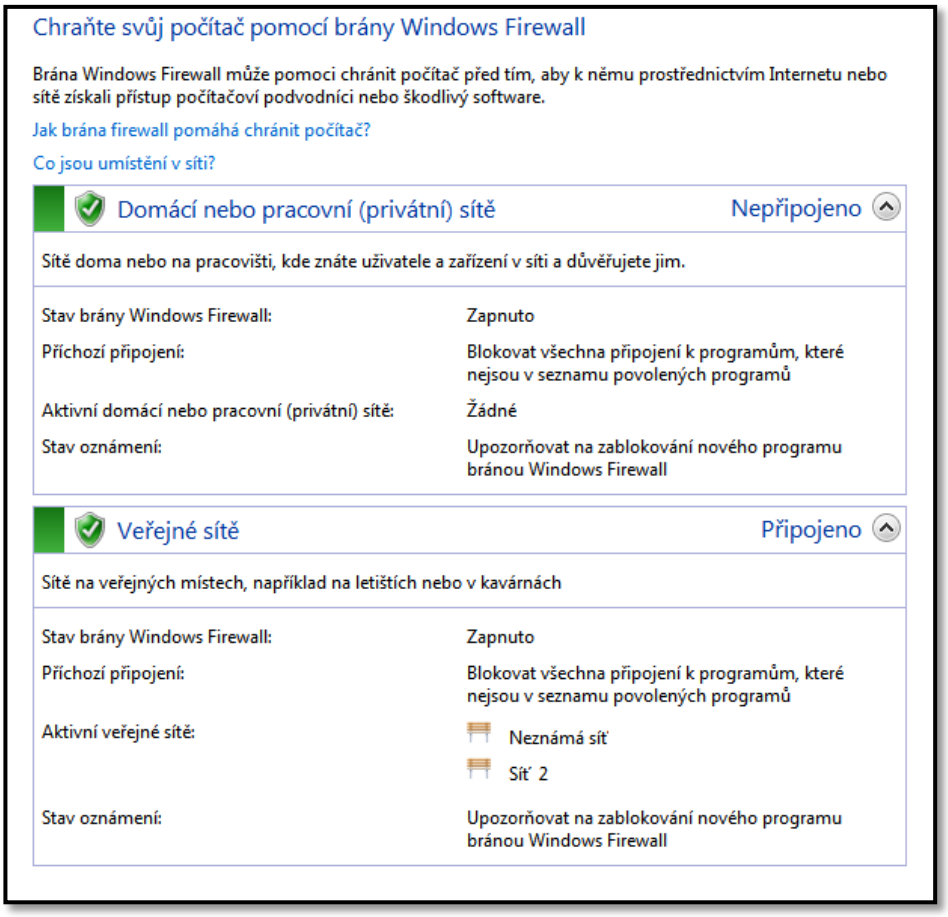
Systém Windows 7 v sobě samozřejmě také integruje bránu Firewall. Jedná se však o firewall s pokročilým zabezpečením oproti firewallu v systémech Windows XP (SP2 a vyšší). Obsahuje modul "Snap-in Windows Firewall with Advanced Security", pomocí kterého dosáhneme lepšího zabezpečení počítače v síti. Užitečnou vlastností je přítomnost několika profilů brány firewall. Tyto profily se dají použít v různých situacích, na různých místech, kde se snažíme připojit do sítě. Každý profil obsahuje souhrn konkrétních pravidel zabezpečení, která jsou aktivní, v závislosti na místě připojení počítače do sítě. Firewall s pokročilým zabezpečením obsahuje tři profily.

a) **Doména**[7] - Používá se pro připojení do sítě, kde se nachází doménový server[8].
b) **Privátní -** Používá se k připojení do privátní sítě. Privátní síť není přímo připojena k Internetu. Pro připojení k Internetu je tato síť zajištěna bezpečnostním zařízením (routerem, překladačem síťových adres, atd.). Pravidla privátního profilu jsou více omezující, než jsou pravidla profilu domény.
c) **Veřejný** - Používá se, pokud počítač připojujete do neznámé veřejné sítě, například v kavárně, u benzínové pumpy, atd. Tento profil obsahuje nejvyšší stupeň zabezpečení. Pokud bude počítač připojen do veřejné sítě, budou všechny přenosy dat do nebo z této sítě filtrovány podle pravidel veřejného profilu.

Firewall s pokročilým zabezpečením dokáže pracovat s protokolem IPSec a filtrovat tak i zabezpečená data. Data bývají zabezpečena šifrováním[9], přičemž šifrován bývá každý paket.

[7] **Doména** je skupina počítačů, které mohou být společně ovládány a spravovány centralizovaným způsobem pomocí řadiče domény - softwarem MS Windows Server.
[8] **Doménový server**, nebo též řadič domény, je počítač, používaný pro správu domény.
[9] **Šifrování** je proces, při kterém jsou informace z čitelné podoby převedeny do podoby nečitelné. Převedení se realizuje aplikací speciální matematické funkce.

A nyní si již řekneme, jak zjistit, zda je Firewall aktivní, či nikoli. Stiskněte tlačítka **Start -> Ovládací panely -> Brána Windows Firewall**. Otevře se Vám okno hlavního ovládacího panelu brány firewall. Jelikož může počítač obsahovat více síťových adaptérů a každý může být připojen do jiné, jinak zabezpečené sítě, vidíme zde více síťových profilů. U každého profilu je pak zmínka, zda je aktivní, či nikoli. Jednotlivé profily a připojené sítě jsou vidět na následujícím obrázku.



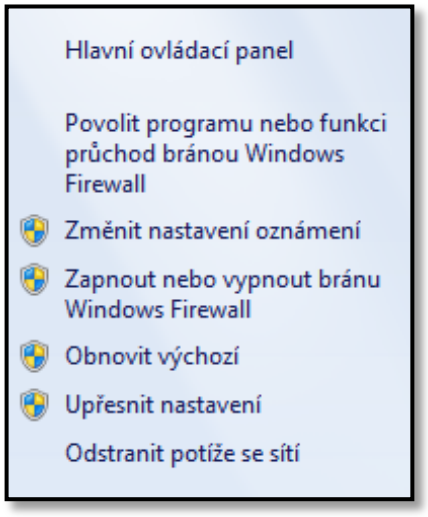
Obrázek 6, Firewall Windows 7

Z obrázku je dobře patrné, že se v počítači nacházejí pouze dva profily (privátní a veřejný). Privátní profil je aktivní, ale nespadají do něj žádná konkrétní připojení (nejsou připojeny žádné síťové adaptéry). Veřejný profil je také aktivní a jak je vidět z obrázku, určuje pravidla dvěma připojeným sítím (Neznámá síť a Síť 2).

Princip funkce firewallu je podobný, jako tomu bylo u firewallu ve Windows XP. Pokud přijde přes konkrétní síť (spadající do konkrétního profilu, například "Síť 2") požadavek na komunikaci s určitým programem, objeví se Vám okno centra zabezpečení, které Vás informuje, jaký program se snaží přes tuto síť komunikovat. Vy se můžete

rozhodnout, zda mu chcete udělit výjimku a povolit přístup. Navíc můžete také definovat, pro jaké profily chcete výjimku přidat. Pokud výjimku udělíte, program bude komunikovat s okolním prostředím (vnější sítí). Pokud výjimku neudělíte, komunikace bude zakázána.

Pokud máte otevřené okno s jednotlivými profily brány, podívejte se na levý panel. Najdete zde rozšířená nastavení brány Firewall (obrázek č. 7). Popišme si základní volby, které na tomto panelu nalezneme.

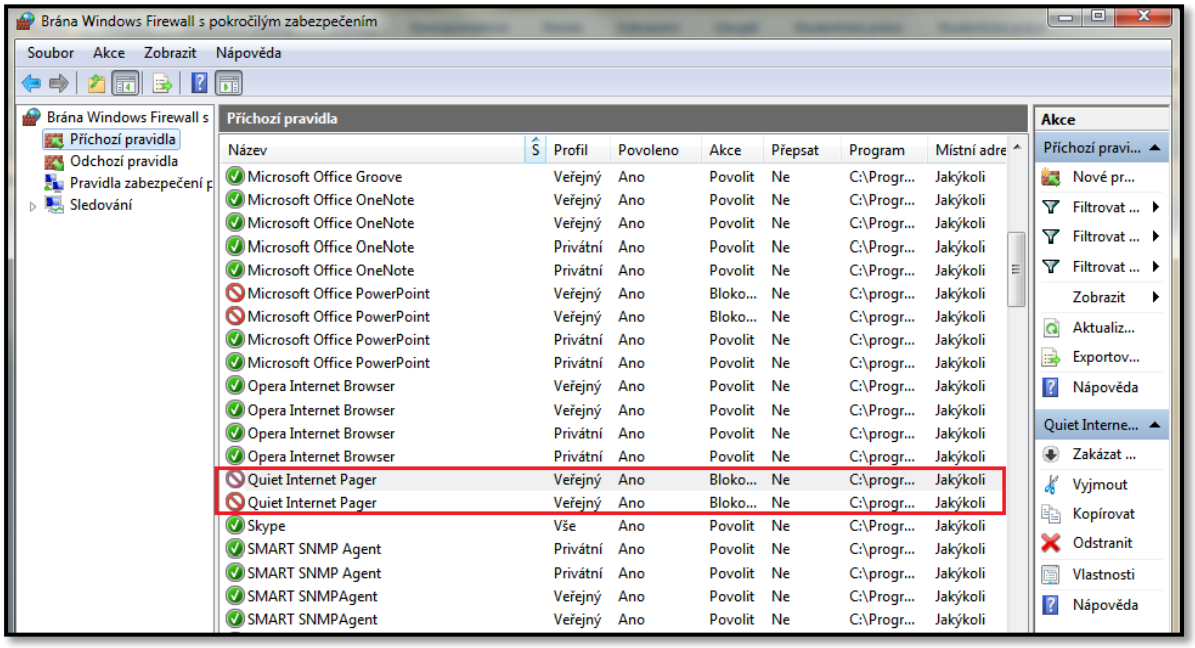


Obrázek 7, Základní nastavení firewall Windows 7

- **Povolit programu nebo funkci průchod bránou Windows Firewall** - V jednoduché a přehledné tabulce můžete definovat, který z nainstalovaných programů bude moci komunikovat s vnější sítí. Komunikaci můžete definovat pro více profilů.
- **Změnit nastavení oznámení**, **Zapnutí nebo vypnutí brány Windows Firewall** – Informace o zapnutí či vypnutí firewallu a jeho jednotlivých profilů.
- **Obnovit výchozí** - Vrátí původní nastavení brány firewall. Zruší výjimky všech programů. Některé programy pak nemusí být plně funkční.
- **Upřesnit nastavení -** Podrobný modul, ve kterém najdete všechny zaznamenané výjimky, včetně jejich podrobného popisu. Výjimky můžeme samozřejmě editovat a odstraňovat.

Ukažme si nyní, jak vyřešit jeden konkrétní problém. Chtěli jste si psát zprávy se svým známým přes program QIP (program pro online chatování). Program jste spustili, ale omylem jste v okně centra zabezpečení nevytvořili pro tento program výjimku. Firewall v tomto případě neumožní programu QIP odesílat a přijímat data. Využijeme tedy jedné z voleb uvedené výše. Bude to volba **Upřesnit nastavení**. Po stisknutí volby se nám otevře nové okno s podrobným modulem "**Brána Windows Firewall s pokročilým nastavením"**. V levé části vybereme položku **Příchozí pravidla**. V seznamu najdeme daný program, v našem případě je to "Quiet Internet Pager - QIP". Podle červené přeškrtnuté ikony vidíme, že je komunikace blokována. Dvojklikem výjimku otevřeme a v bloku **Akce** vybereme možnost **Povolit**

připojení. Změnu výjimky potvrdíme tlačítkem **ok**. Výjimka pro program QIP je vidět na následujícím obrázku.



Název	Profil	Povoleno	Akce	Přepsat	Program	Místní adre
Microsoft Office Groove	Veřejný	Ano	Povolit	Ne	C:\Progr...	Jakýkoli
Microsoft Office OneNote	Veřejný	Ano	Povolit	Ne	C:\Progr...	Jakýkoli
Microsoft Office OneNote	Veřejný	Ano	Povolit	Ne	C:\Progr...	Jakýkoli
Microsoft Office OneNote	Privátní	Ano	Povolit	Ne	C:\Progr...	Jakýkoli
Microsoft Office OneNote	Privátní	Ano	Povolit	Ne	C:\Progr...	Jakýkoli
Microsoft Office PowerPoint	Veřejný	Ano	Bloko...	Ne	C:\progr...	Jakýkoli
Microsoft Office PowerPoint	Veřejný	Ano	Bloko...	Ne	C:\progr...	Jakýkoli
Microsoft Office PowerPoint	Privátní	Ano	Povolit	Ne	C:\progr...	Jakýkoli
Microsoft Office PowerPoint	Privátní	Ano	Povolit	Ne	C:\progr...	Jakýkoli
Opera Internet Browser	Veřejný	Ano	Povolit	Ne	C:\Progr...	Jakýkoli
Opera Internet Browser	Veřejný	Ano	Povolit	Ne	C:\Progr...	Jakýkoli
Opera Internet Browser	Privátní	Ano	Povolit	Ne	C:\progr...	Jakýkoli
Opera Internet Browser	Privátní	Ano	Povolit	Ne	C:\progr...	Jakýkoli
Quiet Internet Pager	Veřejný	Ano	Bloko...	Ne	C:\progr...	Jakýkoli
Quiet Internet Pager	Veřejný	Ano	Bloko...	Ne	C:\progr...	Jakýkoli
Skype	Vše	Ano	Povolit	Ne	C:\Progr...	Jakýkoli
SMART SNMP Agent	Privátní	Ano	Povolit	Ne	C:\progr...	Jakýkoli
SMART SNMP Agent	Privátní	Ano	Povolit	Ne	C:\progr...	Jakýkoli
SMART SNMPAgent	Veřejný	Ano	Povolit	Ne	C:\Progr...	Jakýkoli
SMART SNMPAgent	Veřejný	Ano	Povolit	Ne	C:\Progr...	Jakýkoli

Obrázek 8, Brána firewall s pokročilým nastavením - Windows 7

Jak je vidět z předchozího obrázku, v okně pokročilého nastavení brány firewall se můžeme v levém panelu přepínat mezi příchozími a odchozími pravidly (výjimkami). U každé výjimky je vždy uvedena celá řada doplňujících informací. Uveďme některé z nich.

- **Profil** - Položka udává, pro jaký profil je výjimka vydána.
- **Název a program** - Název programu a jeho umístění na pevném disku.
- **Akce** - Popisuje, zda je výjimka povolena nebo zakázána.
- **Protokol** - Popisuje, pro jaký komunikační protokol je výjimka vydána.
- **Port** - Můžeme definovat určité číslo portu, přes který program komunikuje. Automaticky však bývají povoleny pro daný program všechny porty, které používá.

V pravé části okna pak můžeme přidávat nové výjimky, nebo filtrovat již existující výjimky podle určitých kritérií. Další příklad týkající se konkrétního nastavení brány firewall bude uveden v závěru kapitoly "Nežádoucí vlivy a jejich možná řešení", kde budeme upravovat vlastnosti pravidla pro přístup k počítači přes vzdálenou plochu.

2.2 ANTIVIROVÁ OCHRANA

V předchozí kapitole jsme si popsali, jak funguje brána firewall. Nyní si řekneme, jak funguje antivirová ochrana, jejíž funkce bývá často zaměňována právě s funkcí brány firewall. Z předcházející kapitoly víme, že firewall zkoumá a filtruje komunikaci počítačů, které jsou zapojeny do sítě. Komunikaci buď zamítne, nebo povolí. Tím ochraňuje počítače před škodlivým softwarem, který se šíří přes síť. Můžeme také říct, že firewall hlídá počítač, aby do něj přes síťové rozhraní nepronikl škodlivý software. Do škodlivého softwaru můžeme zařadit například počítačové viry, trojské koně a další.

Počítačový vir je nežádoucí program či kód, který se sám od sebe šíří a napadá jednotlivé soubory, především pak soubory spustitelné (programy). **Trojského koně** můžeme chápat jako jeden z druhů počítačového viru. Je to program, který se na první pohled tváří neškodně, může se tvářit například jako spořič obrazovky nebo jako hra. Tento zdánlivě neškodný program může například mazat soubory na pevném disku, sledovat jaké klávesy mačkáte (sledování hesel), nebo vpouštět do počítače další škodlivý software.

Antivirový program pak zkoumá obsah souborů přímo v počítači. Prohledává je a testuje, zda v sobě neobsahují nějaký známý vir. Úkolem antiviru je daný vir identifikovat a vhodným způsobem ho odstranit. Existuje celá řada dělení antivirových programů. Uveďme například dělení antivirů podle jejich složitosti od nejjednodušších po nejsložitější.

a) **Jednoúčelové antiviry** – Programy, které slouží k odhalení a odstranění jednoho konkrétního viru, popřípadě skupiny. V žádném případě neslouží jako plnohodnotná antivirová ochrana. Tento typ antivirů se používá v případech, kdy víte, jaký vir napadl Váš počítač. Tyto antiviry jsou většinou k dispozici zdarma a používají se na odstraňování sezónních virů (virů rozšířených v dané době).
b) **On - demand skenery** – Programy, které neběží přímo pod operačním systémem Windows, ale bývají například spuštěny v příkazovém řádku (prompt). Používají se především tehdy, pokud již není operační systém schopen normálně fungovat a přesto jej potřebujete dezinfikovat.
c) **Antivirové systémy** – V dnešní době nejpoužívanější podoba antivirových programů. Antivirové systémy dokážou efektivně vyhledávat viry v programech, zkoumají většinu nejpoužívanějších vstupních / výstupních míst v počítači, přes která může

dojít k infekci. Mezi tato místa patří například elektronická pošta, přes kterou dochází k infekci trojskými koni. Většina moderních antivirových systémů v sobě obsahuje také bránu firewall. Do zástupců této kategorie pak můžeme zařadit: NOD32, Avast!, AVG, Kaspersky Antivirus, Symantec endpoint protection.

V předchozích odstavcích jsme si uvedli jednoduché dělení antivirů. Nyní si řekneme, jak dokážou nejčastěji antiviry nejčastěji odhalit vir v počítači. Metod, pomocí kterých antiviry zjišťují přítomnost virů, je více. Uveďme ty nejčastější.

a) **Metoda virových slovníků a databází** – Při prohledávání souborů antivirový program zjišťuje, zda se nějaká část souboru neshoduje s některým známým virem. Velice důležitou podmínkou, aby byl vir nalezen, je aktuální (aktualizovaná) virová databáze antivirového programu. Pokud by virová databáze nebyla aktualizovaná, je to skoro stejné, jako by antivirový program nebyl v počítači vůbec nainstalován. Pokud je vir úspěšně odhalen, máme více možností, co s infikovaným souborem udělat.

   i. Vyléčení souboru – Vir je odstraněn ze souboru a původní soubor je zachován. Tuto možnost však nelze z technických důvodů použít v každém případě.

   ii. Umístění souboru do karantény – Celý soubor se umístí do karantény a systém s ním již nepracuje. Vir se poté nemůže šířit.

   iii. Smazání souboru i s virem – Zneškodní se jak vir, tak soubor. Tuto volbu není vhodné používat u systémových souborů.

Metoda slovníků a databází však nemusí odhalit všechny typy virů. Některé viry, označované jako "polymorfní a metamorfní" se dokážou maskovat. Dokážou měnit svůj vlastní kód, například pomocí šifrování, a znemožnit vlastní odhalení.

b) **Heuristická analýza –** Jak již bylo zmíněno, ne každý vir je hned rozpoznán, například pokud se jedná o polymorfní viry. Princip heuristické analýzy vychází ze spuštění souboru v tzv. virtuálním (odděleném) prostředí od operačního systému. Antivir v tomto prostředí zkoumá chování spuštěného programu a porovnává ho s typickým chováním viru, jako je replikace, přepisování souborů a další. Pokud spuštěný program vykazuje některé z příznaků podezřelého chování, uživatel je upozorněn, že

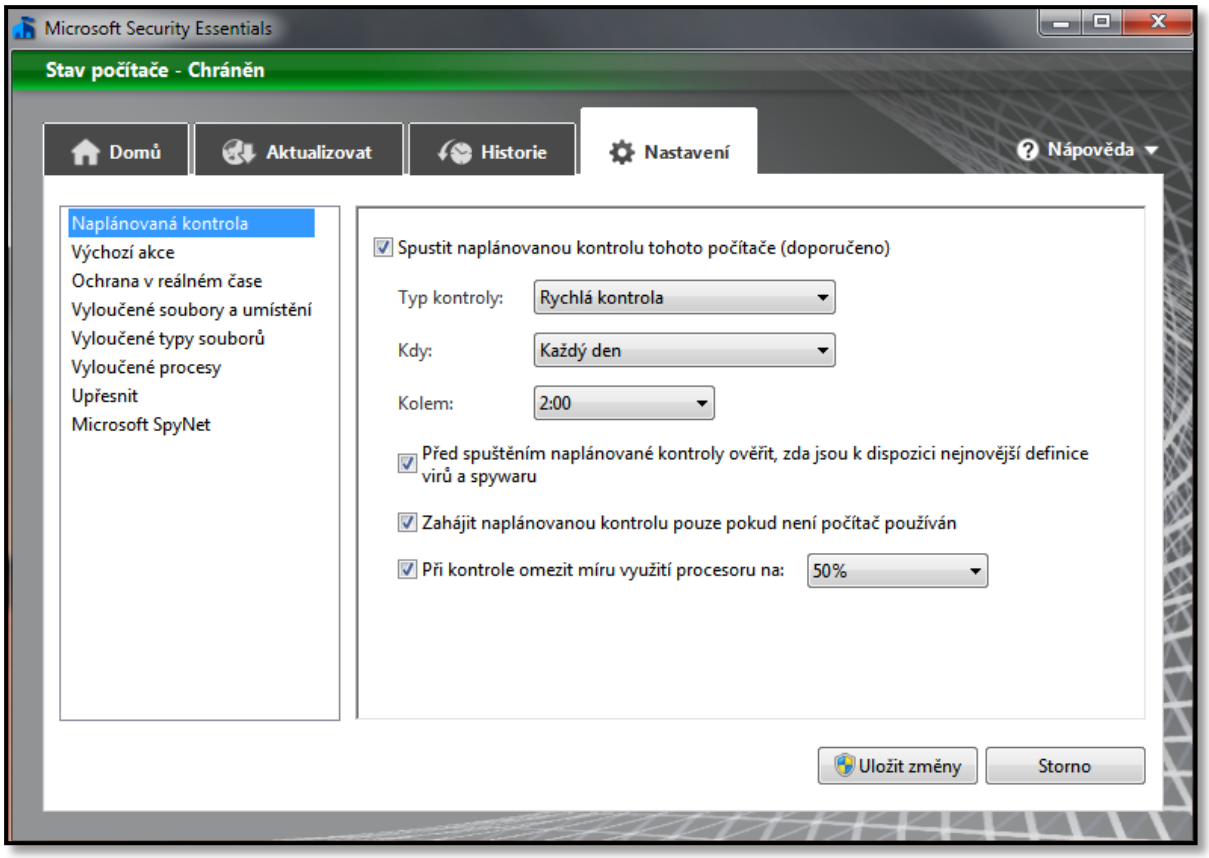
program může obsahovat vir. Heuristická analýza také dokáže dekompilovat[10] program na úroveň zdrojového kódu a poté porovnávat, zda se zdrojový kód nepodobá některému z virů uložených v databázi. Nevýhodou heuristické analýzy je nadbytek falešně zjištěných virů. Některá podezřelá chování programů mohou být totiž záměrná a bezpečná, přitom je antivir s heuristickou analýzou může vyhodnotit jako vir.

Většina moderních antivirových programů používá pro nalezení viru více druhů metod. Často bývá také používána metoda "**Sledování v reálném čase**", která běží skrytě na pozadí a obyčejný uživatel o její činnosti vůbec neví. Pokud je tato metoda aktivní, antivir zkoumá zvýšenou aktivitu programů v počítači, zaměřuje se například na komunikaci přes elektronickou poštu. Dále také zkoumá obsah nově stažených souborů a monitoruje obsah aktuálně navštívených internetových stránek.

Pokud bychom měli shrnout, jakých bezpečnostních zásad se držet, abychom uchránili počítač před škodlivým softwarem, byl by to určitě nainstalovaný a hlavně aktualizovaný antivirový program. V určitých časových intervalech (minimálně 1x za měsíc) spustit antivirovou kontrolu celého počítače. Zbytečně neotvírat spustitelné soubory, které jsme si nevyžádali nebo ty, které mají podezřelý název.

Abychom ale nemluvili pouze v teoretické rovině, ukažme si, co vše můžeme u antivirového programu nastavit. Antivirových programů je celá řada, pro ukázku jsem zvolil program "Microsoft Security Essentials", který si můžete stáhnout zdarma na stránkách společnosti Microsoft. Jedinou podmínkou je mít nainstalovanou legální verzi operačního systému. Nabídku nastavení programu "Microsoft Security Essentials" můžete vidět na obrázku č. 9.

[10] Dekompilace je převedení spustitelné verze programu do jeho zdrojového kódu. Zdrojový kód je text psaný jedním z programovacích jazyků.



Obrázek 9, Nastavení Microsoft Security Essentials

- **Naplánovaná kontrola** - V této záložce si můžete nastavit, kdy se má automaticky provádět kontrola Vašeho počítače. Můžete vybírat mezi rychlou a kompletní kontrolou. Rychlá kontrola prohledává pouze umístění, ve kterých by se viry mohly ukrývat nejčastěji. Úplná kontrola pak prohledá všechna umístění, je ale pomalejší.
- **Výchozí akce** - Pokud nalezne antivir nějakou hrozbu (vir), podle vlastního uvážení jí přiřadí určitý stupeň výstrahy (nízká, vysoká, střední). Pro každý tento stupeň si můžete nastavit, jak se má s danou hrozbou (virem) naložit (odebrat, vložit do karantény, povolit).
- **Ochrana v reálném čase** - Pokud chcete, aby antivir prohledával Váš počítač neustále, aniž byste o tom věděli, zapnutí provedete v této záložce. Můžete zde také nastavit, zda se mají automaticky prohledávat i stahované soubory nebo zda se má sledovat samovolné spuštění programů.
- **Vyloučené soubory, typy souborů, procesy a umístění** - V této záložce můžete definovat, které typy souborů a složek **nebude** antivirový program prohledávat.

- **Upřesnit** - Záložka, která obsahuje další nastavení. Najdete v ní možnosti prohledávání archivů (zip, cab, atd.), vytvoření bodu obnovení systému, odebírání souborů z karantény a další. Bod obnovení je dobré vytvořit před kontrolou, která by mohla z různých důvodů změnit nastavení systémových souborů a tím poškodit funkci systému. Pomocí bodu obnovení může vrátit nastavení systémových souborů do podoby, ve které byly, když byl bod obnovení vytvořen. Bod obnovení bude podrobně popsán v kapitole "Obnovení systému".

Většina konkurenčních antivirových programů nabízí obdobné funkce jako program "Microsoft Security Essentials".

Řada výrobců antivirových programů zakládá tzv. internetové komunity, kde jsou sbírány informace o internetových hrozbách. Každý z uživatelů antivirového programu si může vybrat, zda bude do této komunity přispívat informacemi ze své databáze. V antivirovém programu Microsoft Security Essentials patří této problematice záložka "**Microsoft Spy Net**".

2.3 AKTUALIZACE SYSTÉMU

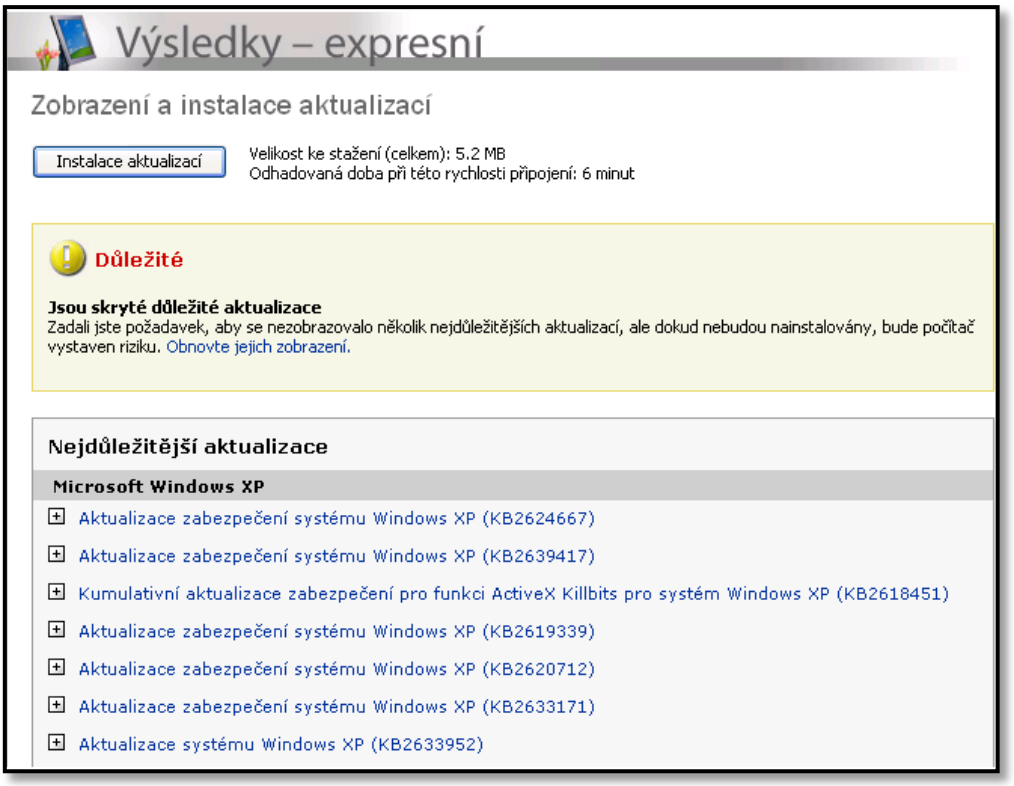
2.3.1 PRINCIP FUNKCE

Dalším, poměrně důležitým bezpečnostním prvkem jsou aktualizace systému. Jedním z jejich hlavních úkolů je opravit bezpečností chyby (nedostatky) v operačním systému a minimalizovat tak možné škody, které by mohl způsobit nežádoucí software (například počítačové viry), případně počítačový hacker (útočník). Automatické aktualizace mohou navíc také obsahovat nové ovladače. Většina operačních systémů rodiny Windows má slabá místa, přes která se snaží útočník či program poškodit Váš počítač. Aktualizace systému, které je nejlépe stáhnout hned po jejich vydání, ošetřují tato slabá místa a jsou tak velice dobrou prevencí při ochraně Vašeho počítače. Aktualizace bývají často vydávány bohužel až po prvních útocích hackerů na slabá místa operačního systému. Často se stává, že až hackeři svými činy upozorní společnost Microsoft, že jejich operační systémy disponují slabými místy. Microsoft pak musí urychleně vydat záchranné balíčky, často nazývané jako "záplaty" a umístit je někam, kde budou pro všechny uživatele operačních systémů dobře dostupné. I přesto, že jsou aktualizace vydávány se zpožděním, platí jedno základní pravidlo. **Čím dříve si aktualizaci s konkrétní záplatou stáhnete, tím menší je pravděpodobnost, že útočník stihne Váš počítač napadnout.**

Aby byly aktualizace dobře dostupné, umísťuje je společnost Microsoft na síť Internet. Uživatelé si je pak mohou stáhnout prostřednictvím služby "Windows Update". V novějších verzích operačních systémů společnosti Microsoft (od verze Windows Vista) je "Windows Update" součástí operačního systému. Není to již jen služba, ale program, který najdete v nabídce **Start**, pod skupinou **Všechny programy**. Princip funkce je velice jednoduchý. Pokud službu nebo program Windows Update spustíte, zkontroluje stav Vašeho operačního systému (nainstalované programy a aktualizace). Na základě této kontroly Vám doporučí, jaké aktualizace byste si měli stáhnout a nainstalovat. Doporučené aktualizace potvrdíte a instalace již probíhá automaticky. Dostupné aktualizace ale nemusíte zjišťovat pokaždé tímto způsobem. V ovládacích panelech můžete nastavit, aby byly aktualizace stahovány a instalovány automaticky. Windows Update může být často zaměňován se službou Microsoft Update, avšak jejich funkce není úplně stejná. Microsoft Update vyhledává aktualizace nejen pro samotný operační systém, ale také pro další software společnosti Microsoft nainstalovaný ve Vašem počítači. V operačních systémech Windows XP a starších bylo nutné spouštět službu přes Internetový prohlížeč Internet Explorer podporující prvek ActiveX. Pod jiným prohlížečem nešla tato služba spustit.

2.3.2 WINDOWS UPDATE V OPERAČNÍCH SYSTÉMECH WINDOWS

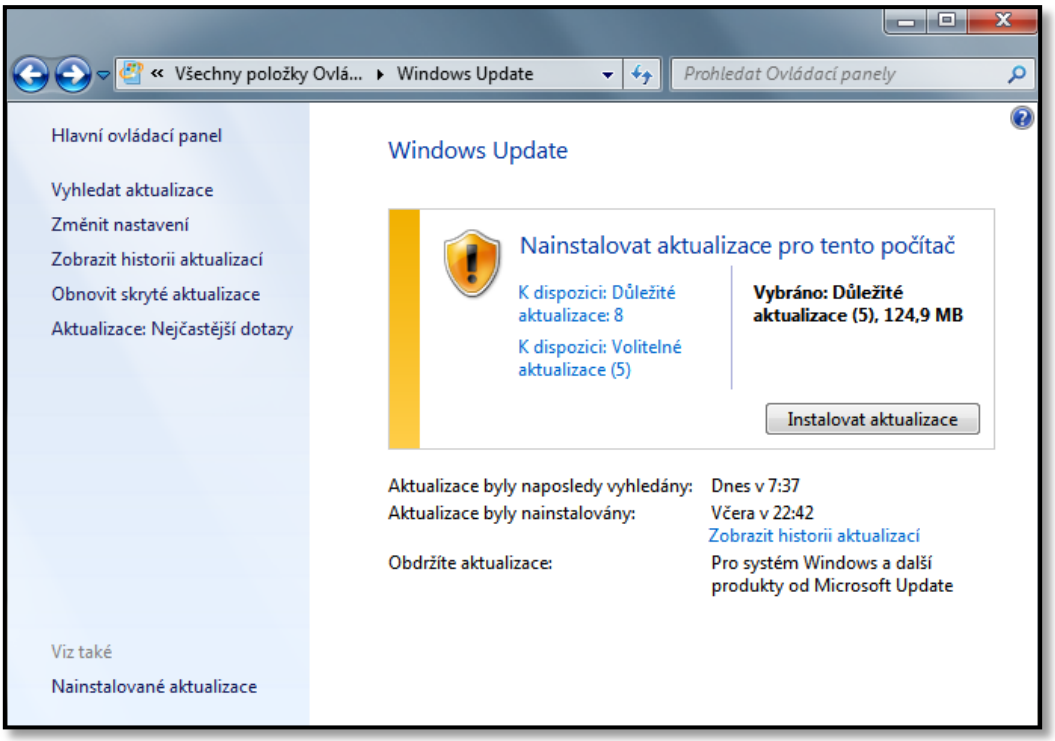
Ještě než se podíváme, jak spustit Windows Update v systémech Windows XP a Windows 7, je důležité zmínit jednu velmi podstatnou skutečnost. Pokaždé, budete-li chtít poprvé aktualizovat Váš operační systém, budete nuceni si spolu s aktualizacemi stáhnout i nástroj na ověření platnosti Vašeho operačního systému. Nástroj WGAN (Windows Genuine Advantage Notifications) bývá automaticky stažen s ostatními aktualizacemi a pokud nemáte legální verzi operačního systému, může Vám značným způsobem znepříjemňovat práci (změna pozadí plochy na černou, informace o používání nelegálního softwaru). Jak již bylo řečeno v předchozích odstavcích, v systémech Windows XP se dají aktualizace stahovat a instalovat dvěma způsoby. Ruční způsob spočívá v otevření programu Internet Explorer a stisknutí příkazu "Windows Update". Automatické stahování a instalování nastavíte stisknutím tlačítek **Start -> Nastavení -> Ovládací Panely -> Automatické aktualizace**. Na následujícím obrázku vidíte ručně vyhledané aktualizace v systému Windows XP.



Obrázek 10, Nalezené aktualizace Windows XP

Pokud chcete, aby se aktualizace stahovaly a instalovaly zcela automaticky, nastavení provedete v **Ovládacích panelech**, kde najdete položku **Automatické aktualizace**. Otevře se Vám okno, kde můžete nastavit, zda se mají aktualizace pouze stahovat, k jejich instalaci pak budete vyzváni, nebo zda se mají stahovat a instalovat automaticky. Naleznete zde i další možnosti nastavení, jako například aktualizace vůbec nevyhledávat. Toto nastavení se ovšem nedoporučuje, protože může ohrozit Váš počítač.

V operačních systémech Windows 7 již nepřistupujete ke službě Windows Update pomocí webového prohlížeče, ale veškeré nastavení automatických aktualizací je integrováno přímo v operačním systému. Pokud chcete zjistit, jaké je nastavení automatických aktualizací, stiskněte posloupnost příkazů **Start -> Ovládací panely -> Windows Update**. Otevře se Vám nové okno, ve kterém najdete veškerá nastavení týkající se automatických aktualizací - viz následující obrázek.



Obrázek 11, Nalezené aktualizace Windows7

- **Vyhledat aktualizace** - Vyhledají se důležité aktualizace potřebné pro Váš operační systém. Po vyhledání jsou nabídnuty také volitelné aktualizace. Volitelné aktualizace obsahují často nejnovější ovladače dalších komponent (grafická karta, zvuková karta, atd.) pracujících s operačním systémem.
- **Změnit nastavení** - Karta, kde nastavíte, kdy se mají aktualizace stahovat a instalovat. Dá se zde také nastavit, zda se mají aktualizace instalovat automaticky, nebo ručně.
- **Zobrazit historii aktualizací** - Zobrazí se tabulka historie aktualizací, ve které je vidět, kdy byla jaká aktualizace nainstalována.
- **Obnovit skryté aktualizace** - Pokud některou z aktualizací nenainstalujete (odškrtnete ji v seznamu vyhledaných aktualizací připravených k instalaci), automaticky se tato aktualizace již nestahuje a přesune se do skupiny skrytých aktualizací. Pokud ji přesto časem chcete nainstalovat, najdete jí v této záložce. Kliknutím ji opět přidáte do skupiny důležitých aktualizací. Aktualizace se vyhledá a můžete ji nainstalovat.
- **Aktualizace: Nejčastější dotazy** - Spustí se nápověda systému Windows, kde se dozvíte odpovědi na nejčastější dotazy ohledně automatických aktualizací.

2.4 OBNOVENÍ SYSTÉMU

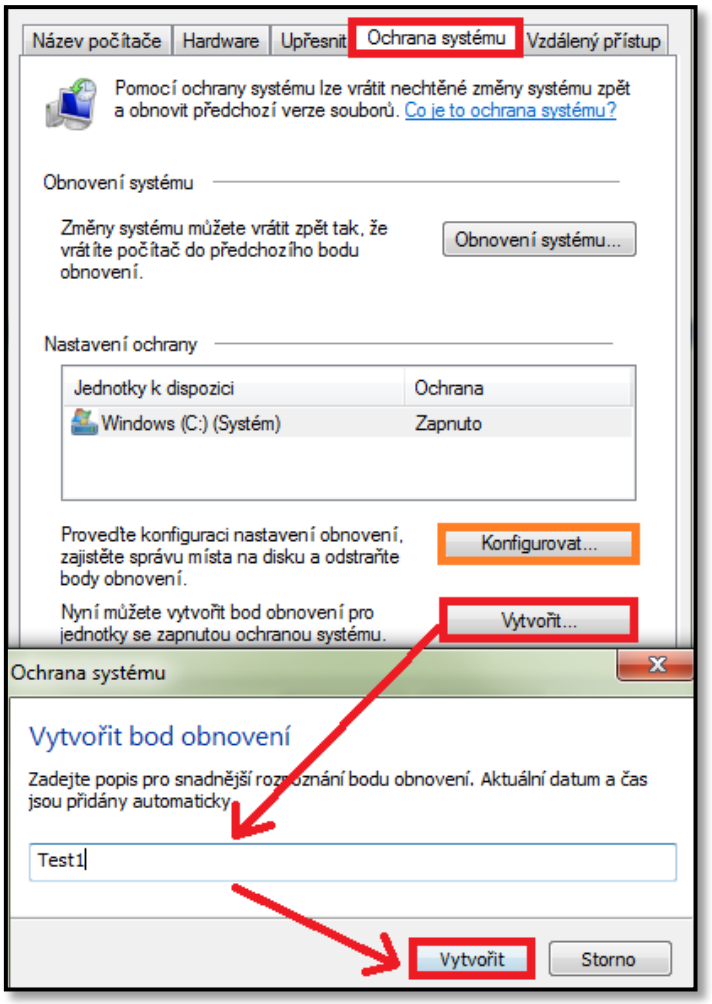
Můžeme se setkat se situací, kdy po nainstalování aktualizace, nových ovladačů, nebo při jiných větších zásazích do systému přestane operační systém korektně fungovat. V tomto případě můžeme použít funkci **Obnovení systému,** která dokáže vrátit veškerá systémová nastavení do doby před zásahem do systému. Před každou větší změnou v systému (instalace aktualizace, instalace programu, atd.) vytváří systém automaticky tzv. "bod obnovení", do kterého ukládá aktuální stav systému (nainstalované programy, stav registrů a další). Body obnovení neobsahují informace o osobních souborech a složkách[11] (fotografie, dokumenty, emailové zprávy a další). Pokud by došlo ke smazání osobních souborů a složek, nebude možné je pomocí bodu obnovení systému získat zpět. Bod obnovení systému je také možné vytvořit v libovolný časový okamžik ručně.

Obdobou bodu obnovení je tzv. **Bitová kopie systému**, ta však na rozdíl od bodu obnovení obsahuje přesnou podobu (identickou kopii) systémového disku včetně všech dat (složek a souborů).

2.4.1 VYTVOŘENÍ BODU OBNOVENÍ

Stiskneme tlačítka **Start -> Ovládací panely -> Systém**. Na levém panelu vybereme kartu **Ochrana systému**. Nacházíme se v sekci **Obnovení systému,** stiskneme příkaz **Vytvořit**. V novém okně zapíšeme název nového bodu obnovení. Postup zobrazuje obrázek č. 12.

[11] **Osobní soubory a složky** jsou implicitně uloženy na systémovém disku pod složkou Users. Každý z uživatelů, který má na počítači zřízen účet, má ve složce Users i svojí osobní složku. Ke své osobní složce má přístup pouze on.

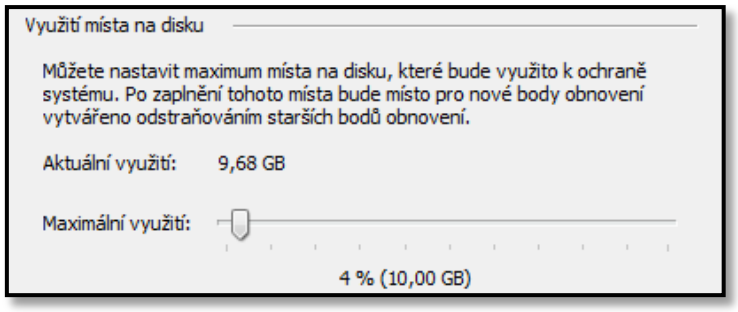


Obrázek 12, Vytvoření bodu obnovení

Na obrázku č. 12 také najdete tlačítko **konfigurovat**. Pokud tlačítko stiskneme, otevře se nám nové podokno, kde můžeme upravit vlastnosti týkající se obnovení systému. Najdeme zde tyto možnosti:

- **Obnovit nastavení systému a předchozí verze souborů** – Součástí nových bodů obnovení bude jak stav systému, tak změněné soubory.
- **Obnovit pouze předchozí verze souborů** – Součástí nových bodů obnovení budou pouze změněné systémové soubory.
- **Vypnout ochranu systému** – Žádné nové body obnovení nebudou automaticky vytvářeny.
- **Odstranit** – Odstraní se všechny body obnovení uložené v systému. Budou odstraněny i všechny verze změněných souborů.

- **Využití místa na disku** – Můžete měnit maximální velikost místa na pevném disku, kterou mohou body obnovení zabírat.

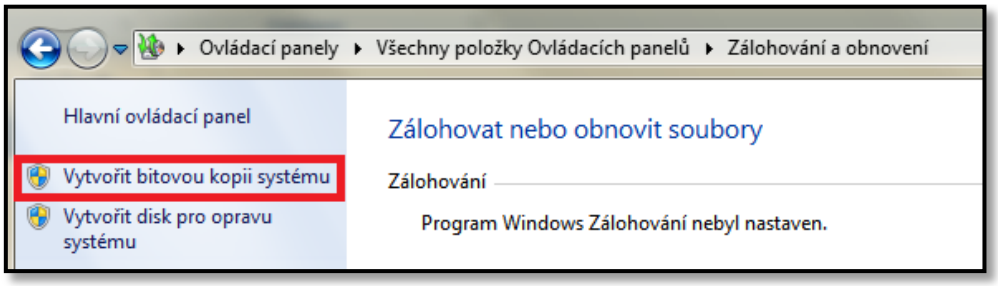


Obrázek 13, Velikost místa pro body obnovení systému

2.4.2 VYTVOŘENÍ BITOVÉ KOPIE SYSTÉMU

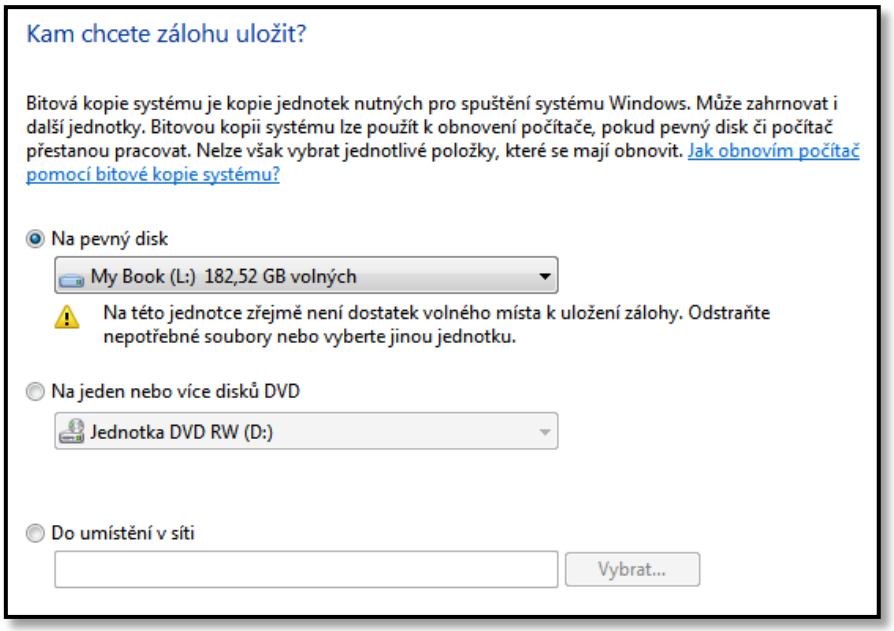
Bitová kopie systému obsahuje veškerá data z disku, ze kterého je vytvořena. Oproti bodu obnovení systému se tedy liší tím, že jsou obnovovány i osobní soubory a složky. Bitová kopie je vlastně přesná kopie pevného disku. Výhodou tohoto typu obnovení je, že se dá použít i v případě, kdy přestane fungovat pevný disk, popřípadě jiná část počítače.

Bitovou kopii vytvoříte stisknutím příkazů **Start -> Ovládací panely -> Zálohování a obnovení**. V levém panelu vyberete položku **Vytvořit bitovou kopii systému**.



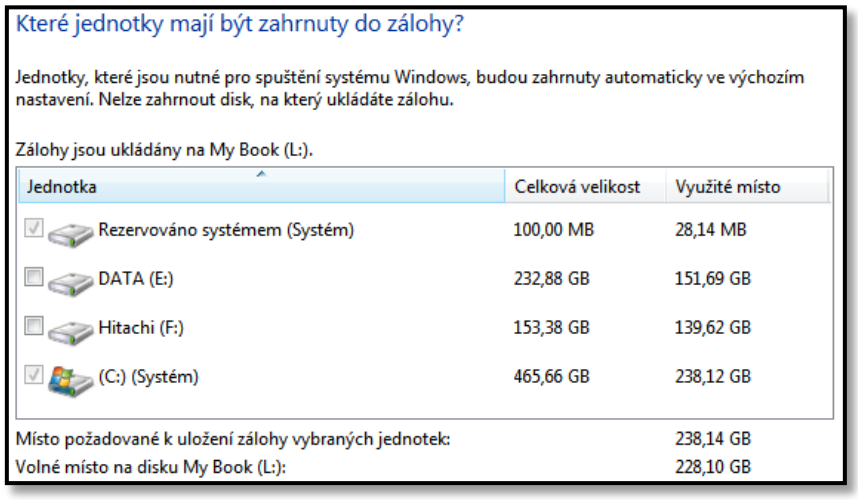
Obrázek 14, Vytvoření bitové kopie systému

Jelikož má celý systémový disk často poměrně velkou kapacitu, můžete si vybrat, kam kopii uložíte. K dispozici máme úložiště - viz následující obrázek.



Obrázek 15, Uložení zálohy bitové kopie systému

Po vybrání úložiště, kam bude uložena bitová kopie, přejdeme k dalšímu kroku. Nyní si můžete vybrat ještě další pevné disky, jejichž data budou také součástí nové bitové kopie. Tuto volbu však osobně nedoporučuji a to z důvodu příliš vysokých nároků na kapacitu záložních médií.



Obrázek 16, Jednotky zahrnuté do zálohy bitové kopie systému

Nyní již stačí stisknout tlačítko **Spustit zálohování**. Mějte na paměti, že doba potřebná pro provedení zálohy bitové kopie je přímo úměrná velikosti zálohovaných dat.

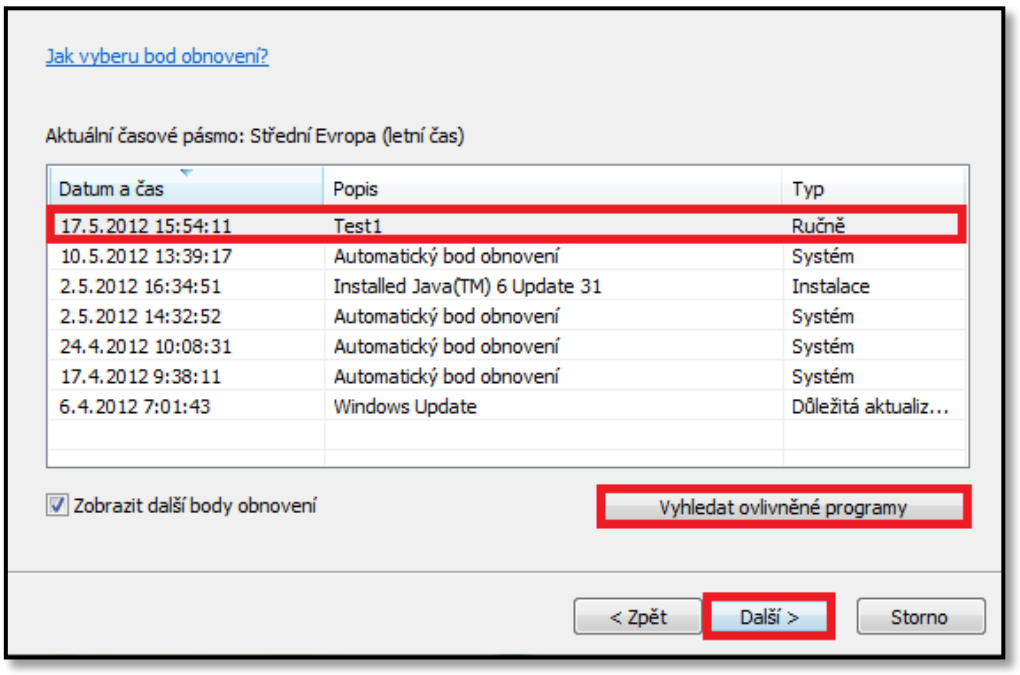
2.4.3 VRÁCENÍ SYSTÉMU DO PŘEDCHOZÍHO STAVU

Systém lze vrátit do předchozího stavu, nachází-li se v různých stavech, zmiňme například stavy kdy:

- Systém lze spustit ve standardním režimu.
- Systém lze spustit pouze v nouzovém režimu.
- Systém nelze spustit.

2.4.3.1 SYSTÉM LZE SPUSTIT VE STANDARDNÍM REŽIMU

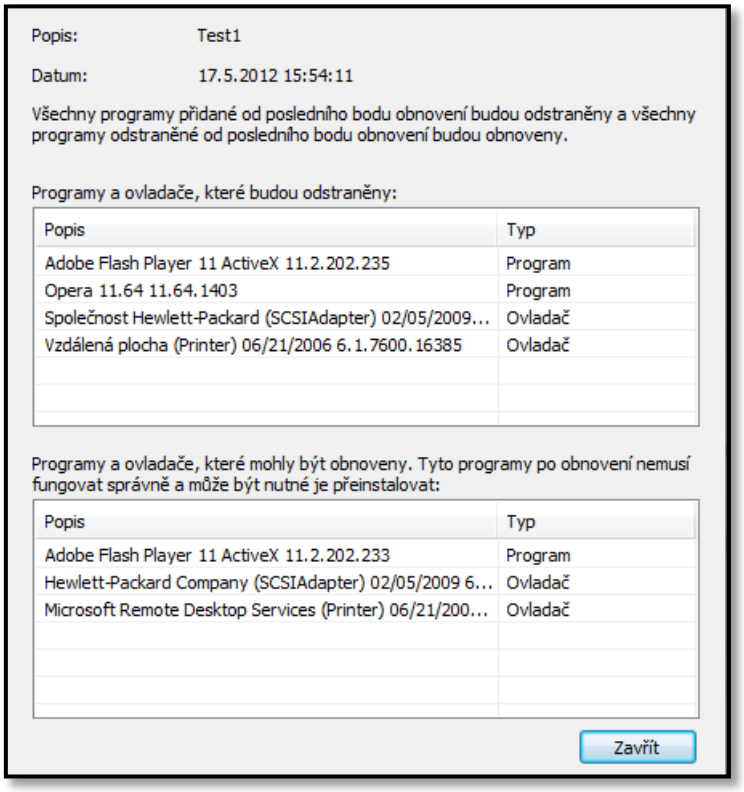
Podíváme-li se zpět na obrázek č. 12, v horní části vidíme tlačítko **Obnovení systému.** Stisknutím tohoto tlačítka zobrazíme nabídku již vytvořených bodů obnovení. U každého bodu obnovení také vidíme, jakým způsoben byl vytvořen (ručně, automaticky), popřípadě, zda byl vytvořen před nějakou důležitou instalací softwaru. Body obnovení také obsahují informace o ovlivněných programech, respektive o programech, které byly instalovány až po vytvoření bodu obnovení, nebo o těch, které již v současnosti součástí systému nejsou.



Obrázek 17, Výběr bodu pro obnovení systému

V předchozí podkapitole jsme vytvářeli nový bod obnovení ručně, pojmenovali jsme ho "Test1". V nabídce bodů obnovení se nachází jako první - viz obrázek č. 17. Dvojitým kliknutím, popřípadě stisknutím tlačítka **Vyhledat ovlivněné programy** zobrazíme tabulku programů, které byly nainstalovány až po vytvoření tohoto bodu obnovení, nebo těch, které

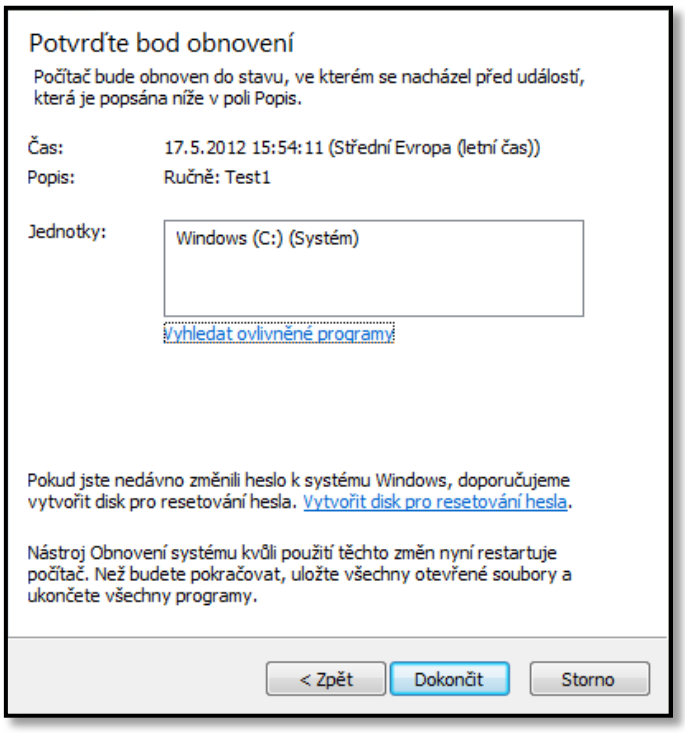
už součástí systému nejsou. Na obrázku č. 18 se můžeme podívat o jaké programy, případně ovladače se jedná.



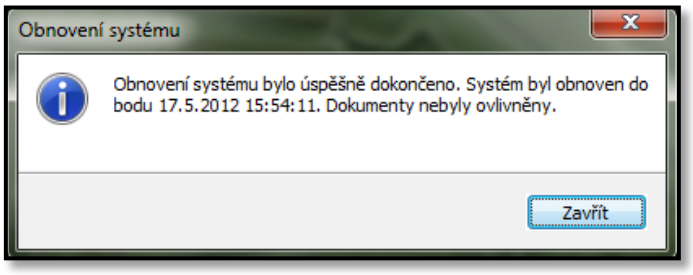
Obrázek 18, Bod obnovení systému - ovlivněné programy

Podívejme se zpět na obrázek č. 17. Stiskneme-li tlačítko **další,** dostaneme se do situace, ve které potvrdíme, že chceme systém doopravdy vrátit do předchozího stavu.

Stisknutím tlačítka **dokončit** (obrázek č. 19) bude zahájen proces obnovování. Při tomto procesu se nesmí s počítačem provádět žádné akce (restartování, spouštění programů, atd.). Restart počítače se následně provede automaticky. Po úspěšném vrácení systému do předchozího stavu budete informováni (obrázek č. 20).



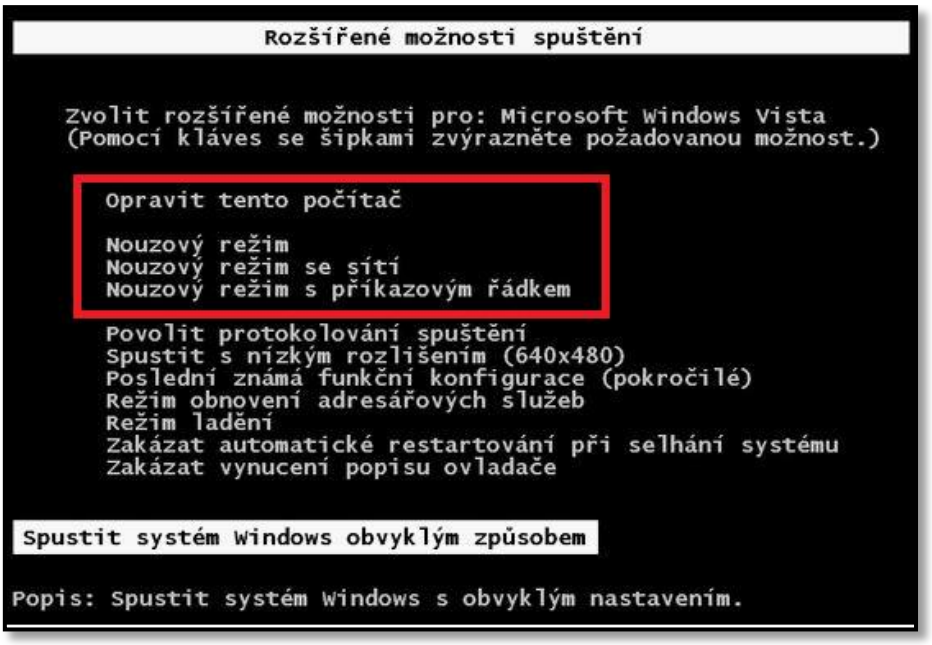
Obrázek 19, Potvrzení vybraného bodu obnovení



Obrázek 20, Dokončení obnovy systému

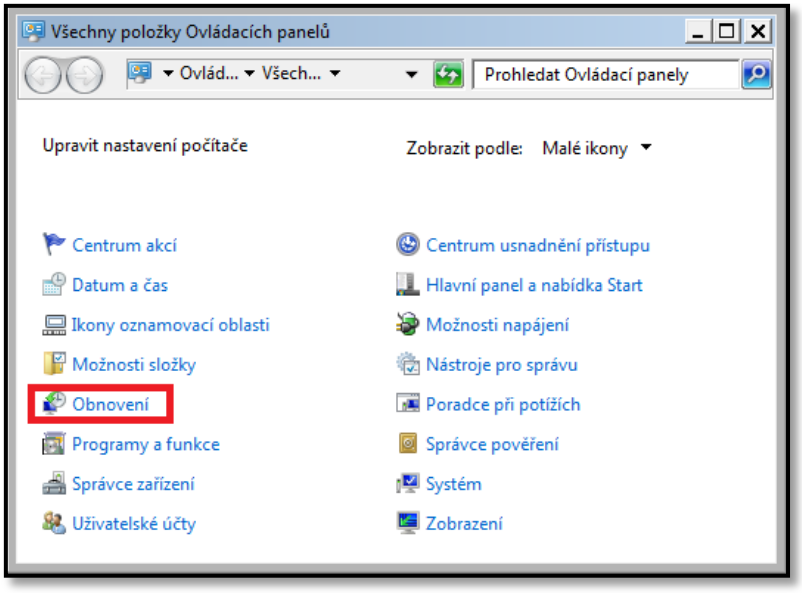
2.4.3.2 SYSTÉM NASTARTUJE POUZE V NOUZOVÉM REŽIMU

Systém nastartuje do nouzového režimu automaticky, pokud v něm nastal problém, bránící v jeho standardním spuštění. Může se jednat o špatně nainstalované ovladače, popřípadě stav vyvolaný škodlivým softwarem. Pokud byste chtěli vyvolat nabídku rozšířených možností spuštění a přepnout se do nouzového režimu ručně, stiskněte při startování (bootu) systému **klávesu F8**. Na následujícím obrázku můžete vidět rozšířené možnosti spuštění systému Windows.



Obrázek 21, Rozšířené možnosti spuštění

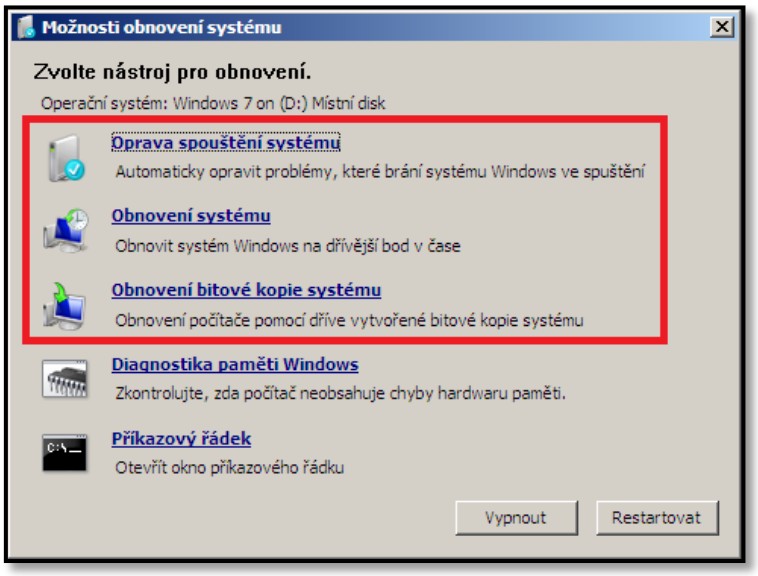
Po stisknutí volby **Nouzový režim** naběhne systém do stavu nouze, kde budou omezeny jeho některé funkce. Systém bude například odpojen od sítě, nebudou instalovány některé ovladače, což ovlivní velikost rozlišení obrazu a barevnou hloubku. Obnovení systému opět spustíte stisknutím příkazů **Start -> Ovládací panely -> Obnovení**. Postup obnovení předchozí verze systému je identický jako v případě, kdybyste obnovovali systém při plné funkcionalitě – viz postup v kapitole "Systém naběhne v pořádku". Na následujícím obrázku si můžete prohlédnout ztenčenou nabídku ovládacích panelů, pokud je systém spuštěn ve stavu nouze.



Obrázek 22, Nabídka "Ovládacích panely" v nouzovém režimu

2.4.3.3 SYSTÉM NELZE SPUSTIT

Pokud nelze systém spustit žádným způsobem, je možné využít nástroje **Opravit tento počítač**, který je součástí nabídky **Rozšířené možnosti spuštění**. Nabídku aktivujete stisknutím klávesy **F8** při startu (bootu) systému. Z nabídky pak vyberete právě možnost **Opravit tento počítač.** Začne se spouštět nástroj pro obnovení systému. Po krátké době budete vyzváni k přihlášení. **Je nutné se přihlásit jako lokální uživatel s právy administrátora, popřípadě jako administrátor.** Nyní se Vám zobrazí nabídka, ve které si vyberete způsob opravy systému.



Obrázek 23, Možnosti obnovení systému

- **Oprava spouštění systému** – Nástroj, který se snaží opravit **aktuální verzi** systému v počítači. Nejčastěji se tento nástroj pokouší o opravy:
  - MBR[12], tabulky oddílů, systémových registrů.
- **Obnovení systému** – Nástroj, pomocí kterého vrátíte systém do **předchozího** funkčního **stavu**. Principielně se jedná se o stejný způsob obnovy jako ten uvedený v předchozích odstavcích.
- **Obnovení bitové kopie systému** – Nástroj, který vrací systém do předchozího funkčního stavu **včetně obsahu dat na disku**. Bitovou kopii systému jsme vytvářeli na začátku této podkapitoly. Po stisknutí této volby bude zahájeno prohledávání bitové kopie systému na místním počítači. Bitovou kopii lze načíst také z disků DVD.

[12] **MBR**, neboli Master Boot Record, je část pevného disku (prvních 512 bytů), kde je umístěn zavaděč systému. Dále se zde nachází také tabulka oddílů pevného disku.

2.5 SDÍLENÍ A ZABEZPEČENÍ SOUBORŮ A SLOŽEK

V této kapitole si popíšeme základní principy sdílení a zabezpečení souborů a složek. Důležité je zmínit, že **sdílení (share) a zabezpečení jsou v systémech s OS Microsoft Windows dva odlišné mechanismy**, které se však při přístupech k datům do velké míry prolínají. **Zabezpečení se týká jak souborů, tak složek. Sdílení lze aplikovat pouze na složky.**

2.5.1 ROZDÍL MEZI SDÍLENÍM A ZABEZPEČENÍM

Pokud byste chtěli zpřístupnit Vaše soubory, popřípadě složky tak, aby byly **přístupné v síti, musíte je sdílet**. Pokud složku sdílíme, můžeme říct, že jsme ji vystavili v síti pod určitým názvem. V rámci větších sítí se pak takové složky často nachází na doménovém serveru. Oproti tomu **zabezpečení souborů a složek opravňuje k přístupu v rámci lokálních stanic** za předpokladu, že používáte souborový systém NTFS[13]. **Zabezpečení je tedy vlastností souborového systému NTFS**. Pro vysvětlení rozdílu mezi sdílením a zabezpečením uveďme jednoduchý příklad.

Mějme uživatele, který chce přistupovat ke složce na serveru z lokálního počítače připojeného v místní síti. V rámci **sdílení nebylo na serveru uživateli poskytnuto žádné právo**. V rámci zabezpečení souborového systému má však na serveru, kde se tato složka nachází, povolena všechna přístupová práva. Z tohoto příkladu můžeme vyvodit následující závěry:

- Pokud bude uživatel přihlášen na počítači v síti, složka pro něj bude **nedostupná**.
- Pokud se uživatel přihlásí na serveru, bude mít ke složce všechna práva.

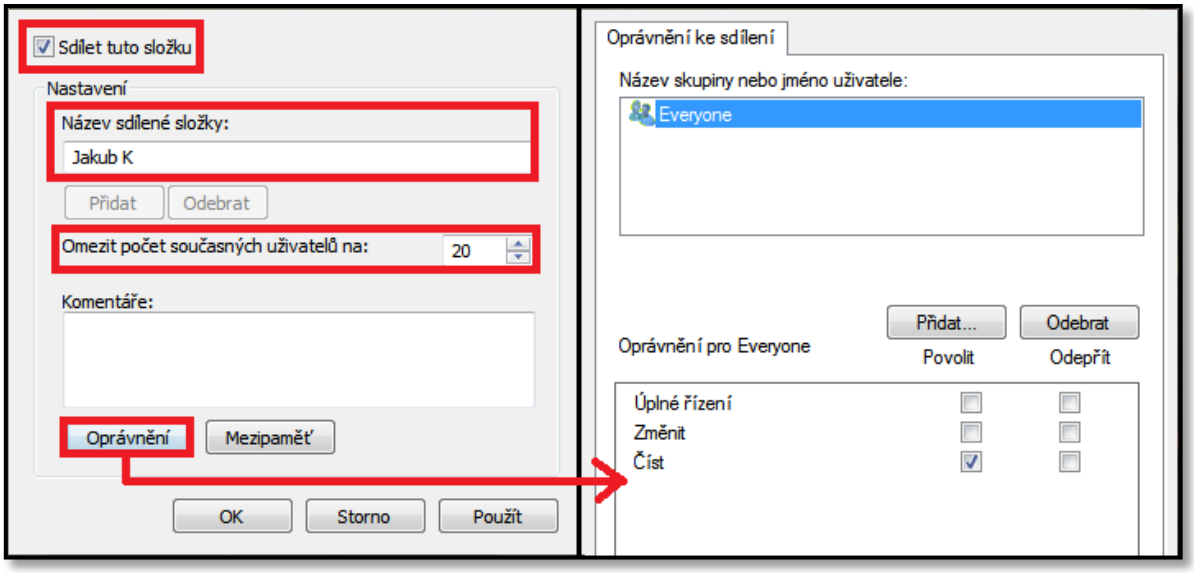
V praxi bývá používána kombinace sdílení a zabezpečení. Sdílením povolíte síťový přístup ke složkám tzv. "hrubým způsobem". Jemnější doladění přístupu pak upřesníte pomocí zabezpečení, kde definujete jednotlivá práva pro uživatele, popřípadě skupiny.

2.5.2 SDÍLENÍ SLOŽEK V SÍTI

Pokud chceme sdílet složku v rámci sítě, stiskněme na ní **pravé tlačítko** myši a vyberme položku **Vlastnosti**. V novém okně poté vybereme kartu **Sdílení**. Sdílení lze nastavit stisknutím tlačítek **Sdílení,** popřípadě **Rozšířené možnosti sdílení**. My stiskneme tlačítko **Rozšířené možnosti sdílení**. Zobrazí se nám nové okno, kde musíme zaškrtnout

[13] **NTFS** je souborový systém společnosti Microsoft, který poskytuje pokročilé možnosti zabezpečení a ochrany dat. Dnes již značně nahradil dřívější souborový systém FAT / FAT32.

možnost **Sdílet tuto složku**. Všimněte si, že pro uživatele, který ke složce přistupuje přes síť, může mít složka odlišný název, než jaký má na lokální stanici, či serveru. Dále můžeme také omezit počet současně připojených uživatelů.



Obrázek 24, Sdílení složky

Z obrázku č. 24 je patrné, že složka je přístupna v síti každému uživateli. Do skupiny Everyone spadá každý uživatel, který se v síti přihlásí. Nyní již k jednotlivým právům, která lze pro sdílení nastavit. U popisovaných práv budeme vycházet z publikace "Bezpečnost Windows 2000/XP" od Kerstin Eisenkolb.

- **Úplné řízení** (Full Control) - Právo, které by mělo být přiřazeno administrátorům, případně skupině Administrators. Uživatel může číst, zapisovat, spouštět, prohlížet, měnit obsah a mazat obsah složky. Může také přidělovat práva.
- **Změnit** (Change)- Uživatel může číst, zapisovat, spouštět, prohlížet a mazat. Nemůže přidělovat práva.
- **Číst** (Read) - Nejnižší právo uživatele. Uživatel dokáže číst soubory ve složce a procházet její obsah. Není schopen do složky cokoli zapisovat.

Všechna tato práva lze buď přidělit, nebo odepřít.

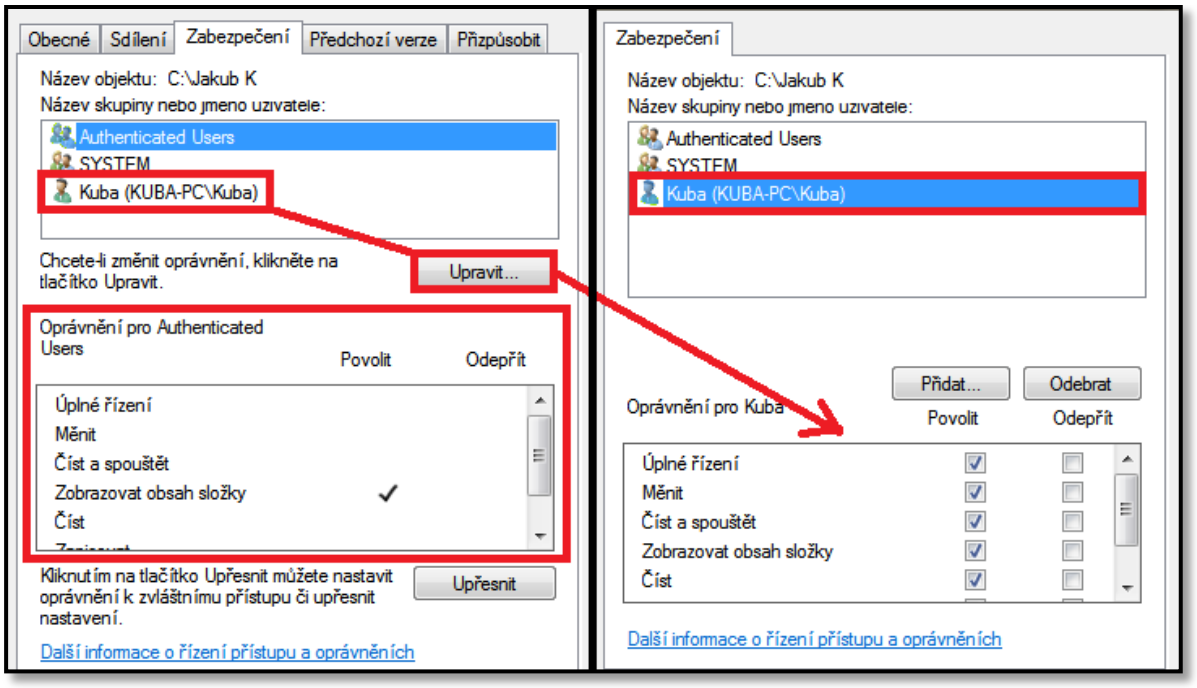
V praxi se řeší přístup ke sdíleným složkám v síti nejčastěji dvěma způsoby:

a) Nástrojem sdílení se povolí maximální přístupová práva pro skupinu "Everyone", například úplné řízení. Přístup uživatelů se dále omezí pomocí zabezpečení souborového systému.

b) Pokud to vyžaduje politika společnosti, je nutné odstranit skupinu "Everyone" a nahradit ji skupinou "Authenticated users". Do skupiny "Authenticated users" patří všichni uživatelé, kteří jsou ověřeni proti účtům na doménovém serveru. Sdílení a zabezpečení se pak nastaví obdobně jako v předchozím bodu.

2.5.3 ZABEZPEČENÍ V SOUBOROVÉM SYSTÉMU

Pokud chceme složku, případně soubor zpřístupnit uživatelům v rámci zabezpečení souborového systému, stiskneme na složce **pravé tlačítko** myši a vybereme příkaz **Vlastnosti**. V novém okně poté vybereme kartu **Zabezpečení**. Otevře se nám základní tabulka zabezpečení, kde vidíme uživatele a skupiny disponující různými právy k této složce. Pro lepší názornost se můžeme podívat na obrázek č. 25.



Obrázek 25, Zabezpečení složky v souborovém systému

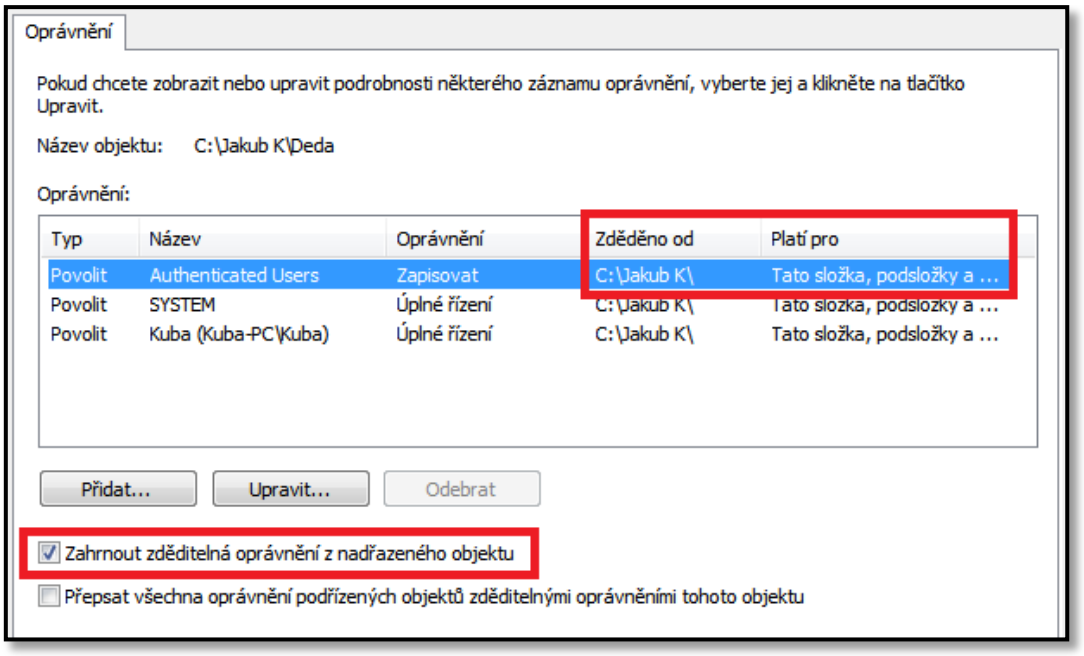
Na obrázku č. 25 je vidět, že ke složce mají přístup skupiny uživatelů "Authenticated users", kteří mají ovšem nastaveno pouze právo "Zobrazovat obsah složky", dále pak skupina "SYSTEM" a uživatel "Kuba". Uživatel "Kuba" má pak ke složce úplný přístup. Pokud je zabezpečení nastaveno tímto způsobem, znamená to, že:

- Uživatel Kuba může do složky zapisovat, může složku procházet, číst a spouštět soubory, může také přidělovat práva.
- Ostatní uživatelé (kromě administrátora), kteří se přihlásí k lokální stanici, popřípadě doméně, můžou složku pouze procházet.

Pokud bychom chtěli práva pro jednotlivé skupiny a uživatele změnit, stiskneme tlačítko **Upravit**. Nyní můžeme pro každou skupinu či uživatele měnit jednotlivá práva. Na obrázku č. 25 pak můžeme jednoduše odebrat některá práva uživateli "Kuba". V následujících bodech si popíšeme základní práva ke složkám. Tato základní práva, která jsou vidět také na obrázku č. 25, se skládají z dalších, ještě "jemnějších" práv. Pro jejich výčet a následnou úpravu bychom museli stisknout tlačítko **Upřesnit**. **Základní práva ke složkám jsou**:

- **Úplné řízení** (Full Control) - Uživatel může číst, zapisovat, spouštět, prohlížet, měnit a mazat obsah složky a souborů. Může také přidělovat práva.
- **Měnit** (Modify) - Uživatel může číst, zapisovat, spouštět, prohlížet a mazat soubory a složky. Nemůže přidělovat práva.
- **Číst a spouštět** (Read & Execute) - Uživatel může číst obsah složek a souborů. Může procházet složky a spouštět soubory.
- **Zobrazovat obsah složky** (List Folder contents) - Uživatel může zobrazit obsah složky. Pozor platí pouze pro složky.
- **Číst** (Read) - Uživatel může zobrazit obsah složek a prohlížet soubory.
- **Zapisovat** (Write) - Uživatel může zapisovat do složky, vytvářet soubory.
- **Oprávnění ke zvláštnímu přístupu** (Special permissions) - Speciální nastavení, kde se nastavují "jemná práva".

Důležité je zmínit ještě jednu podstatnou skutečnost, a to je **dědění práv**. Pokud pro složku nastavíte určité skupině například právo "Zapisovat", právo se automaticky zkopíruje na všechny podsložky a soubory. Pokud chcete dědičnou linii v některé z podsložek přerušit, musíte upravit zabezpečení dané podsložky. Stiskneme tlačítko **Upřesnit** - viz obrázek č. 25 a dostaneme se do pokročilého nastavení zabezpečení složky. Zde pro konkrétní skupinu uživatelů odškrtneme volbu **Zahrnout zděditelná oprávnění z nadřazeného objektu.** Pro lepší názornost se podívejte na obrázek č. 26.



Obrázek 26, Dědění oprávnění z nadřazeného objektu

Jak jste si jistě všimli, zabezpečení a sdílení se vždy týká uživatele, popřípadě skupiny uživatelů. Na lokálních stanicích vytváří uživatele administrátor a to stisknutím **pravého tlačítka myši** a výběru položky **Spravovat** na ikoně **Tento počítač.** Administrátor pak uživatele založí a může mu udělit členství v některé z předem definovaných skupin (skupiny už mají implicitně nastavena různá práva pro spuštění programů). Sdílení a zabezpečení složek pak bývá řešeno způsoby popsanými v této kapitole.

Konkrétní založení uživatele a jeho přiřazení do skupiny bude popsáno v následující kapitole "Bezpečnost a ochrana dat na počítačových stanicích ve školním prostředí", kde budeme uživatele zakládat přímo do domény v adresářové struktuře Active Directory. Způsob centralizované správy pomocí doménových serverů bývá charakteristický pro správu uživatelských účtů ve školním prostředí.

3 BEZPEČNOST A OCHRANA DAT NA POČÍTAČOVÝCH STANICÍCH VE ŠKOLNÍM PROSTŘEDÍ

Ve školním prostředí je potřeba vhodným, někdy velmi specifickým způsobem zabezpečit přístup k jednotlivým složkám a souborům. Často je nutné rozlišit práva jednotlivých žáků, učitelů a také administrátorů. Veškerá tato koncepce vychází z přidělování práv jednotlivým uživatelům a skupinám. Právě členstvím ve skupinách se dá vhodným způsobem ošetřit přístup do systémových složek, popřípadě omezit schopnost instalace programů uživatelům (většinou žákům), kteří by pro takovou operaci neměli mít oprávnění. Pro takovou správu uživatelských účtů může být použito komplexní řešení v podobě serverové správy s adresářovou službou Active directory, kde jsou všichni uživatelé členy jedné domény.

Hlavní část této kapitoly je věnována modelovým příkladům, ve kterých si popíšeme, jakým způsobem spravovat uživatele v doméně. Modelové příklady budou popsány z prostředí doménového serveru a lokálních stanic připojených do domény. Pro operační systém serveru bude použit Microsoft Windows Server 2008 (anglická jazyková verze) a pro lokální stanice operační systém Microsoft Windows 7 (česká jazyková verze).

V závěru této kapitoly uvedeme, jakým způsobem je řešena bezpečnost a správa počítačových stanic na základních školách v Plzni.

3.1 UŽIVATELSKÉ ÚČTY A SKUPINY UŽIVATELŮ NA DOMÉNOVÉM SERVERU

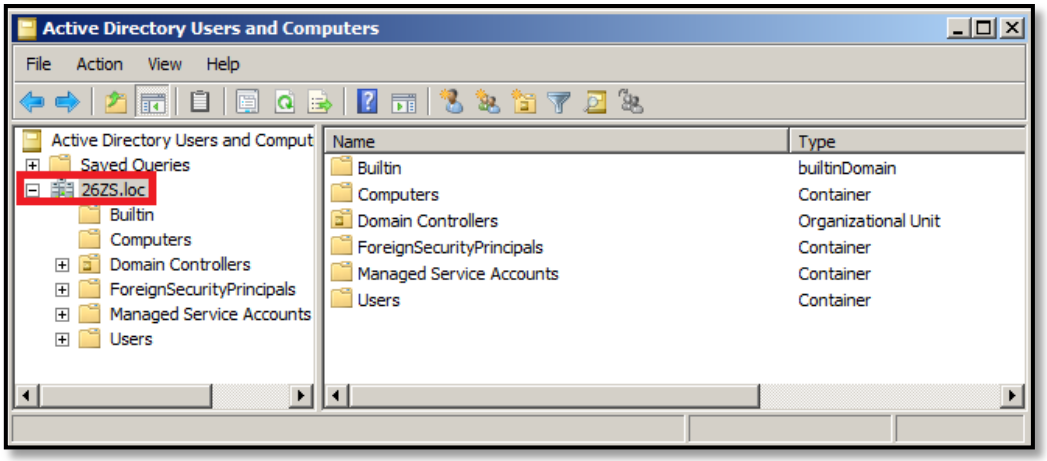
Na úvod kapitoly je dobré zmínit, že v rámci doménového serveru budeme mluvit o dvou různých typech skupin.

- **Předdefinované systémové skupiny** – Skupiny, které jsou serverem vytvořeny automaticky. V závislosti na tom, které skupiny jste členem, liší se vaše oprávnění k administraci lokální stanice a instalování programů.
- **Nově zakládané skupiny** – Jsou vytvářeny především k odlišení oprávnění při přístupu ke sdíleným položkám v síti.

3.1.1 VYTVOŘENÍ UŽIVATELE

Na serveru se přihlásíme jako administrátor a stiskneme položky **Start -> Administrative Tools -> Active Directory Users and Computers.** Otevře se nám

správa skupin a uživatelů v adresářové struktuře Active Directory v dané doméně. Pro náš modelový příklad jsme vytvořili doménu s názvem 26.ZS a veškeré účty budeme dále vytvářet v rámci této domény. Podívejte se na obrázek č. 27.

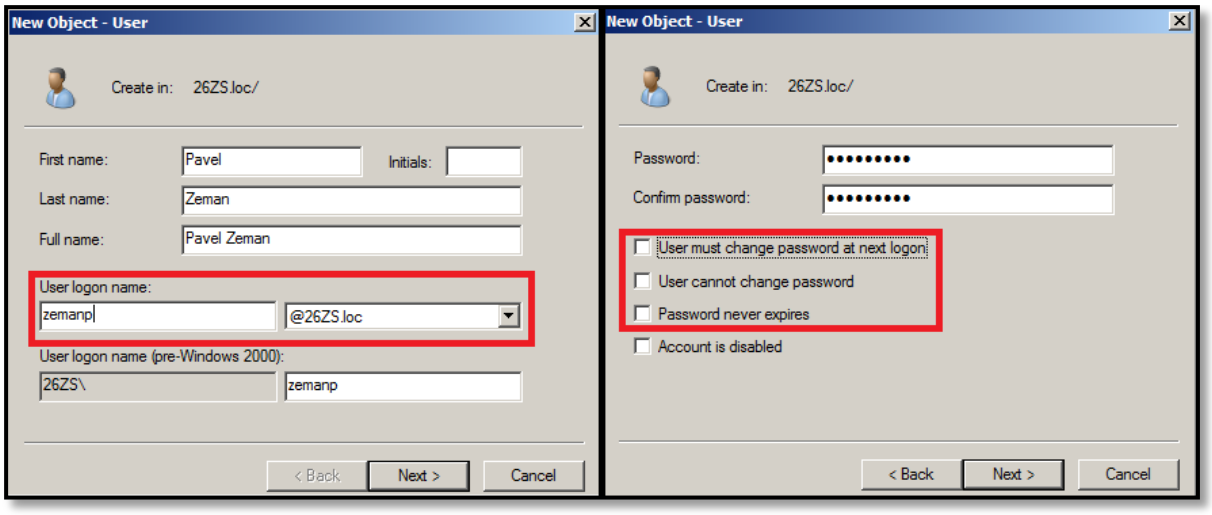


Obrázek 27, Doména 26ZS v adresářové struktuře Active Directory

Na obrázku vidíme složky, které obsahují různé doménové objekty. My popíšeme ty, které nás zajímají nejvíce. Jsou to:

- **Builtin** – Složka obsahující předdefinované systémové skupiny s různými právy. Tyto skupiny jsou vytvářeny serverem automaticky.
- **Computers** – Složka obsahující seznam počítačů v doméně.
- **Users** – Složka obsahující jak předdefinované systémové skupiny serveru, tak nově vytvořené skupiny a uživatele.

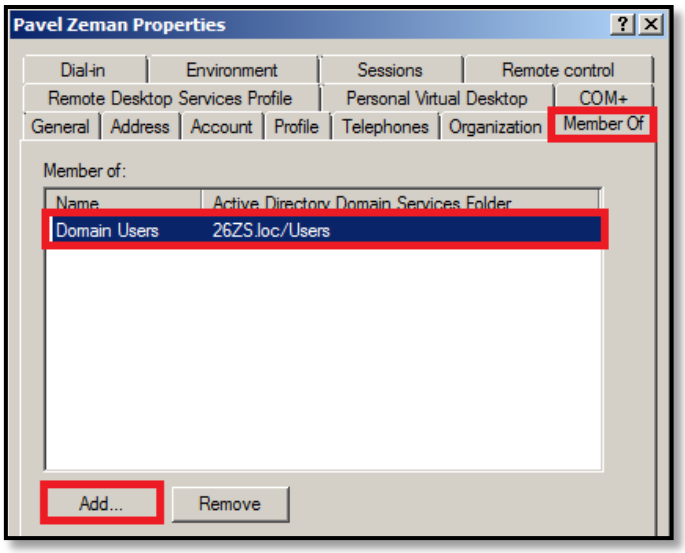
Nového uživatele vytvoříme stisknutím **pravého tlačítka myši** na složce **Users**, z nabídky vybereme položku **New -> User.** V novém okně definujeme název uživatele a jeho přihlašovací jméno (User logon name). V příštím kroku definujeme další vlastnosti a zásady uživatelského konta. Podívejte se na obrázek č. 28.



Obrázek 28, Založení nového uživatele v doméně

Nejdůležitější volbou je **heslo** uživatele, které při vytváření účtu zapisuje sám administrátor. Často je z bezpečnostních důvodů požadováno, aby si uživatel své heslo co nejdříve změnil, proto je zde možnost **User must change password at next logon** (při příštím přihlášení musí uživatel změnit své heslo). Mezi další nastavení patří volby **User cannot change password** (uživatel nemůže měnit heslo) a **Password never expires** (heslo nikdy nevyprší). Vytvoření uživatele dokončíme stisknutím tlačítka **Finish**. Uživatele najdeme pod složkou users. Pokud chceme zjistit další vlastnosti uživatele, stiskneme na jeho názvu pravé tlačítko myši a vybereme položku **Proporties**.

Každý nově vytvořený uživatel je automaticky členem skupiny **Domain Users**. Skupina Domain Users je pak členem předdefinované systémové skupiny **Users**.



Obrázek 29, Vlastnosti uživatelského účtu v doméně

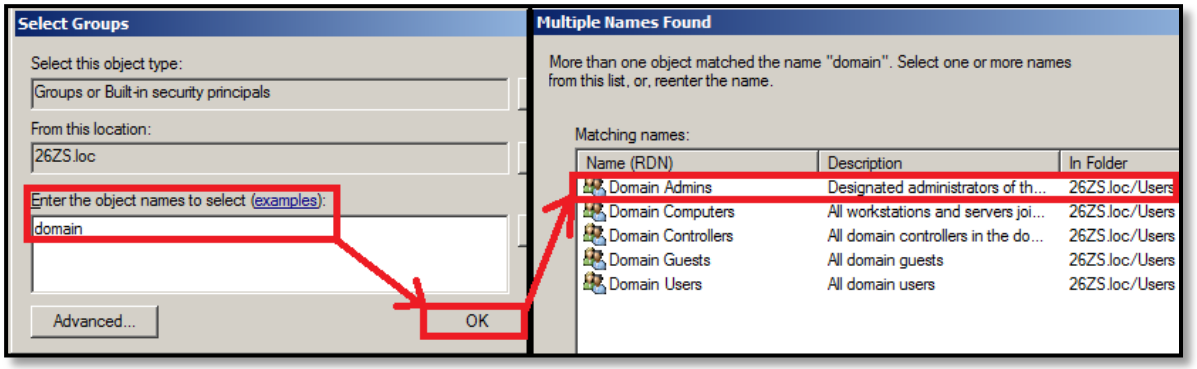
Jelikož v adresářové struktuře Active Directory funguje **dědění práv** z vyšších objektů na nižší, všichni nově vytvoření uživatelé mají oprávnění jako systémová skupina Users. Členství uživatele ve skupině Users je ideální pro profily **žáků**, jelikož uživatelé skupiny **Users**:

- Mohou spouštět nainstalované programy.
- Nemohou samovolně instalovat programy, zasahovat do systémových složek a jakkoli spravovat počítač v doméně.

Pokud byste zakládali nového uživatele a potřebovali byste mu přidělit vyšší práva (jednalo by se například o učitele informatiky), musíte ho zařadit do skupiny **Domain Admins**. Tato skupina disponuje administrátorskými právy a její členové:

- Mohou plně spravovat počítač v doméně včetně instalace programů.

Zařazení uživatele do skupiny provedete tak, že si zobrazíte jeho vlastnosti, otevřete si kartu **Member Of** (je členem) a stisknete tlačítko **Add**. Pro lepší představu se můžete podívat na obrázek č. 29. Do textového pole napíšeme začátek názvu skupiny a stiskneme tlačítko **Ok**. V tomto okamžiku se nám automaticky nabídne tabulka skupin a uživatelů obsahující zadaný textový řetězec. Správnou skupinu poté označíme a stiskneme tlačítko **Ok.** Podívejte se na obrázek č. 30.



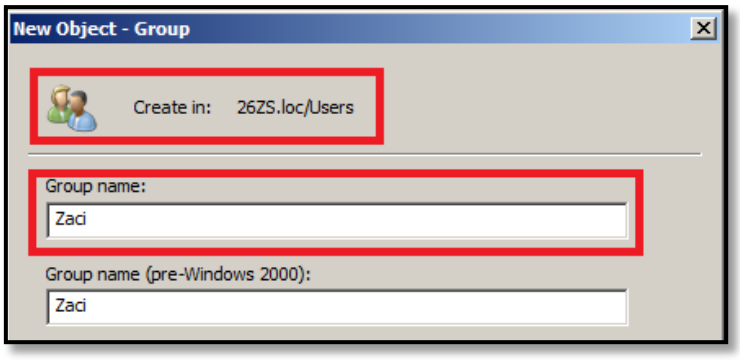
Obrázek 30, Členství ve skupině Domain Admins

V této kapitole jsme si vyzkoušeli vytvořit uživatele v doméně a přiřadit mu členství v systémových skupinách. Ne vždy si ale vystačíme pouze s předem definovanými systémovými skupinami, které nás opravňují k instalaci programů a přístupu k systémovým složkám. Často potřebujeme vytvořit skupiny, pro které bychom společně definovali přístup ke sdíleným složkám na serveru. Ve školní praxi se může jednat o skupiny učitelů, žáků, popřípadě administrátorů, kdy každý má ke stejné sdílené složce jiná práva. V podkapitole

"Vytvoření skupiny" si jednoduchým způsobem vytvoříme novou skupinu, které pak v kapitole "Sdílení a zabezpečení dat" nastavíme přístup ke sdílené serverové složce.

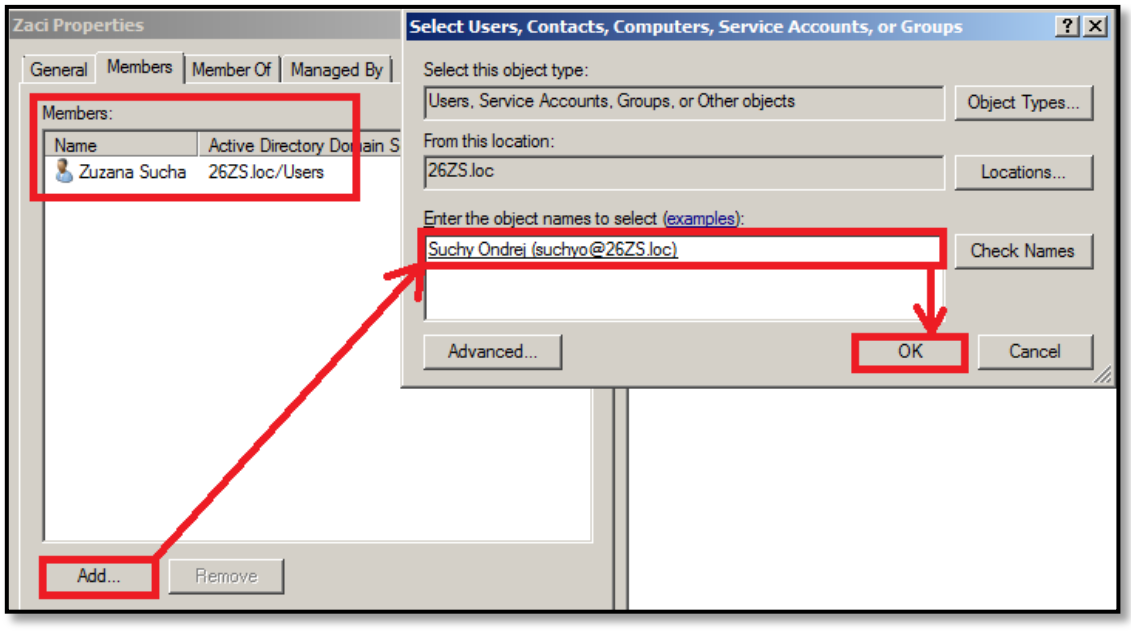
3.1.2 VYTVOŘENÍ SKUPINY

Na serveru jsme opět přihlášeni jako administrátor a stiskneme položky **Start -> Administrative Tools -> Active Directory Users and Computers.** Novou skupinu vytvoříme stisknutím pravého tlačítka myši na složce **Users**, z nabídky vybereme položku **New -> Group**.



Obrázek 31, Vytvoření nové skupiny v doméně

Z obrázku č. 31 je patrné, že vytvoříme novou skupinu "Zaci". Této skupině pak přiřadíme její členy. Přiřazovat budeme již vytvořené uživatele. Otevřeme vlastnosti vytvořené skupiny "Zaci" a přepneme se na kartu **Members** (členové). Po stisknutí tlačítka **Add** vyhledáme uživatele a stisknutím tlačítka **Ok** ho zařadíme do skupiny. Podívejte se na obrázek č. 32.



Obrázek 32, Zařazení uživatele do skupiny

V levé části obrázku č. 32 také vidíme, že členem skupiny "Zaci" je již uživatel Zuzana Sucha. Do skupiny můžeme přidat libovolné množství uživatelů. **Výhodou skupin je to, že oprávnění přístupu ke sdíleným složkám stačí nastavit pro skupinu. V rámci dědičnosti pak mají stejná práva i všichni její členové**.

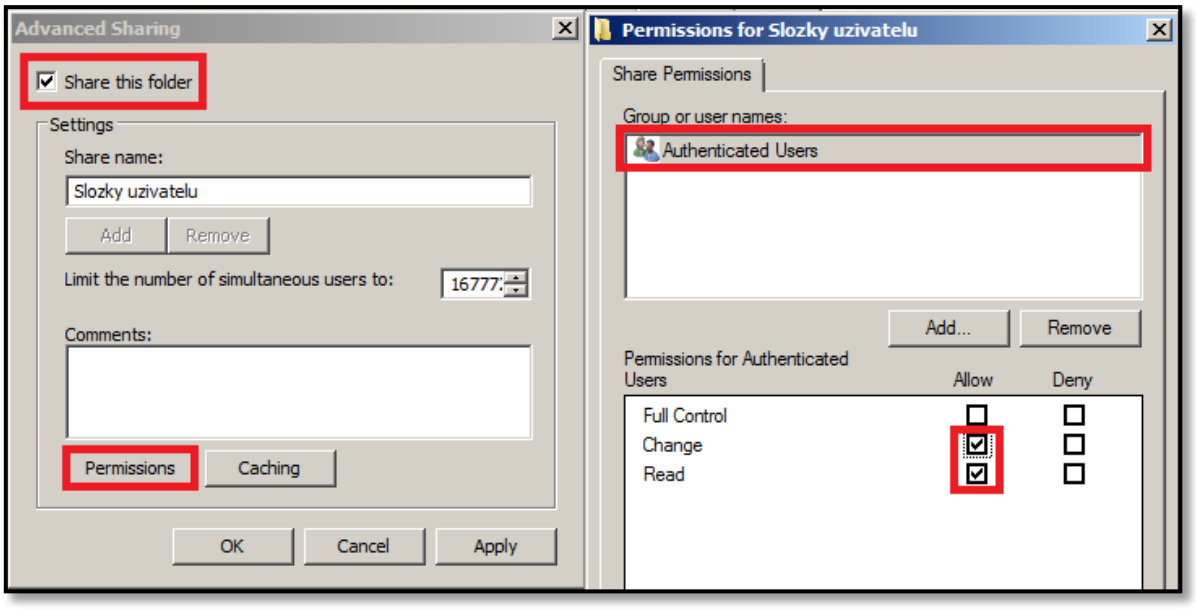
Obdobným způsobem bychom pro školní prostředí mohli vytvořit i skupiny "Ucitele" a "Administratori".

3.2 SDÍLENÍ A ZABEZPEČENÍ DAT NA DOMÉNOVÉM SERVERU

Jsme v situaci, kdy máme vytvořené uživatele a skupiny a chceme jim poskytnout složku, do které by mohli ukládat své vlastní dokumenty a soubory. Taková složka se bude fyzicky nacházet na doménovém serveru a přístup k ní bude řízen pravidly pro sdílení a zabezpečení. Obecné principy sdílení a zabezpečení složek jsme probrali v kapitole "Sdílení a zabezpečení souborů a složek", nyní již tedy ke konkrétním příkladům.

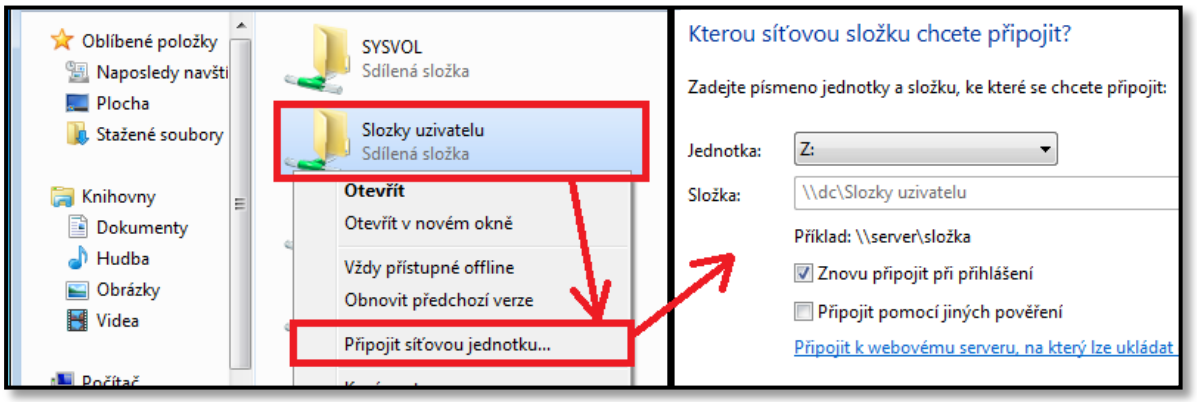
3.2.1 ZPŘÍSTUPNĚNÍ A SDÍLENÍ SLOŽKY NA SERVERU

Pro naši práci jsme vytvořili složku s názvem "slozky uzivatelu", kterou budeme sdílet. Tato složka obsahuje ještě další podsložky "Zaci" a "Ucitele". Sdílení provedeme stisknutím **pravého tlačítka** myši na složce a vybereme možnost **Properties** (vlastnosti). V kartě **Sharing** (sdílení) stiskneme tlačítko **Advanced Sharing** (rozšířené možnosti sdílení). Zaškrtnutím políčka **Share** složku nasdílíme. Nyní upravíme oprávnění ke sdílení této složky. Skupinu "Everyone" nahradíme skupinou "Authenticated Users". Skupině udělíme právo **Change** (měnit) a **Read** (číst). Pro lepší představu se můžete podívat na následující obrázek.



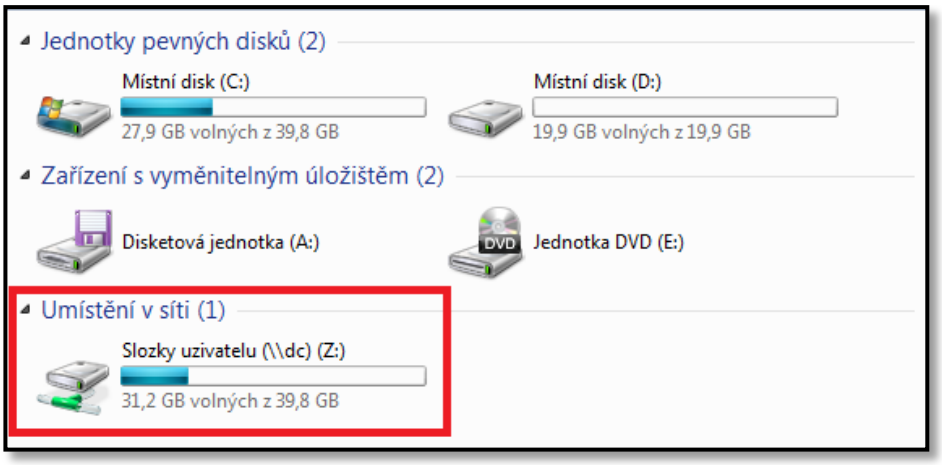
Obrázek 33, Sdílení složky v doméně

V tomto okamžiku je složka "Slozky uzivatelu" včetně podsložek přístupna v síti každému uživateli, který má v doméně vytvořen účet. Pro lepší přehlednost je možné na **lokální stanici** připojit sdílenou složku **jako novou síťovou jednotku**. V průzkumníku Windows se pak bude zobrazovat jako samostatná jednotka. Připojení provedete vybráním sdílené položky, stisknutím **pravého tlačítka** myši a vybráním možnosti **Připojit síťovou jednotku**. **Operaci provádíme na lokální stanici**.



Obrázek 34, Připojení síťové jednotky na lokální stanici

Novou síťovou jednotku můžeme nyní vidět jako součást lokální stanice. Podívejte se na následující obrázek.



Obrázek 35, Síťová jednotka na lokální stanici

V tomto okamžiku je sdílená složka přístupna všem uživatelům, kteří mají v doméně založen účet. Uživatelé disponují právy číst a měnit. **Jemnější práva přístupu k této složce nastavíme pomocí zabezpečení souborového systému, kde budeme definovat práva jednotlivým skupinám ("Zaci", "Ucitele", popřípadě "Administratori")**.

3.2.2 NASTAVENÍ ZABEZPEČENÍ SLOŽKY NA SERVERU

Nyní nastavíme pro složky "Slozky uzivatelu", "Zaci" a "Ucitele", práva tak, že:

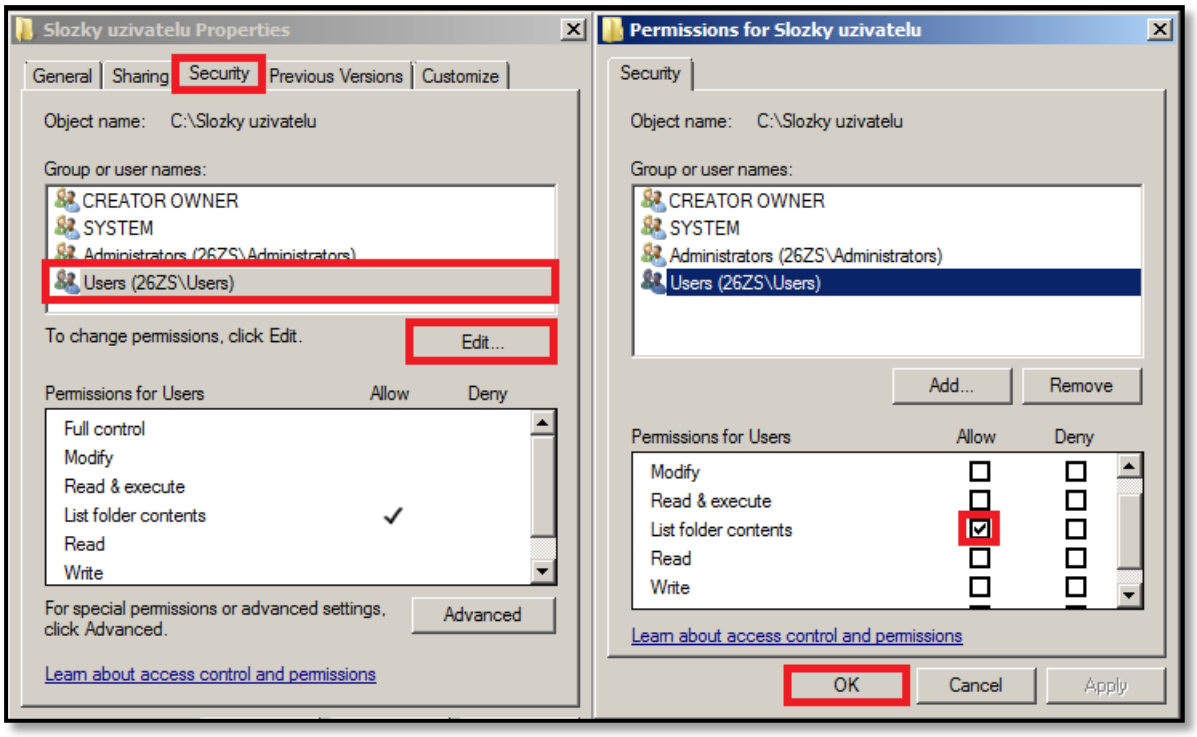
a) Všichni administrátoři budou moci procházet, vytvářet, mazat a číst všechny soubory a složky.

b) Všichni uživatelé budou mít přístupnou složku "Slozky uzivatelu" pro čtení. Podsložky "Zaci" a "Ucitele" už ale všem uživatelům přístupny nebudou.

c) Možnost vytvářet, mazat a číst složky a soubory budou mít ve složce "Zaci" administrátoři a žáci.

d) Možnost vytvářet, mazat a číst složky a soubory budou mít ve složce "Ucitele" administrátoři a učitelé.

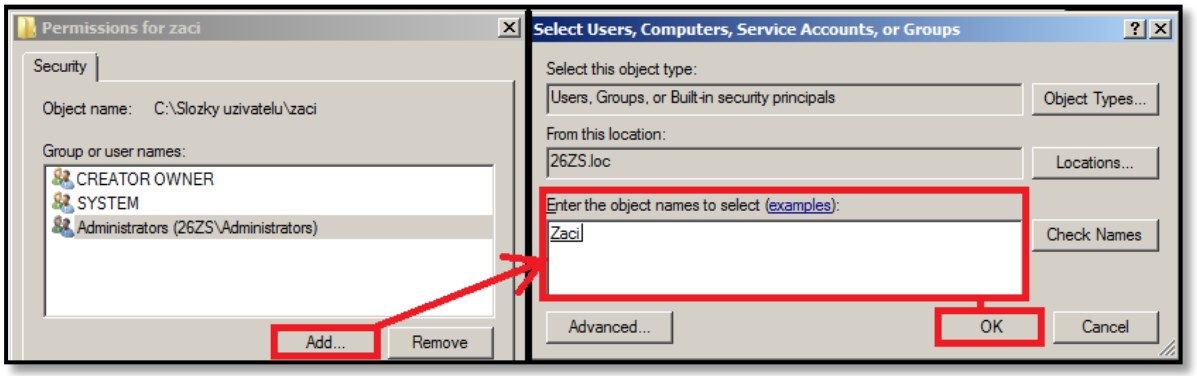
1. Pro složku "Slozky uzivatelu" upravíme práva tak, aby byla složka přístupná všem uživatelům, ale pouze pro čtení. Na složce stiskneme pravé tlačítko myši a vybereme položku **Properties** (vlastnosti). Na kartě **Security** (zabezpečení) upravíme práva skupiny Users (všichni uživatelé) tak, aby bylo povoleno pouze právo **List folder contents (číst obsah složky).** Můžete se podívat na následující obrázek.



Obrázek 36, Zabezpečení složek na doménovém serveru 1

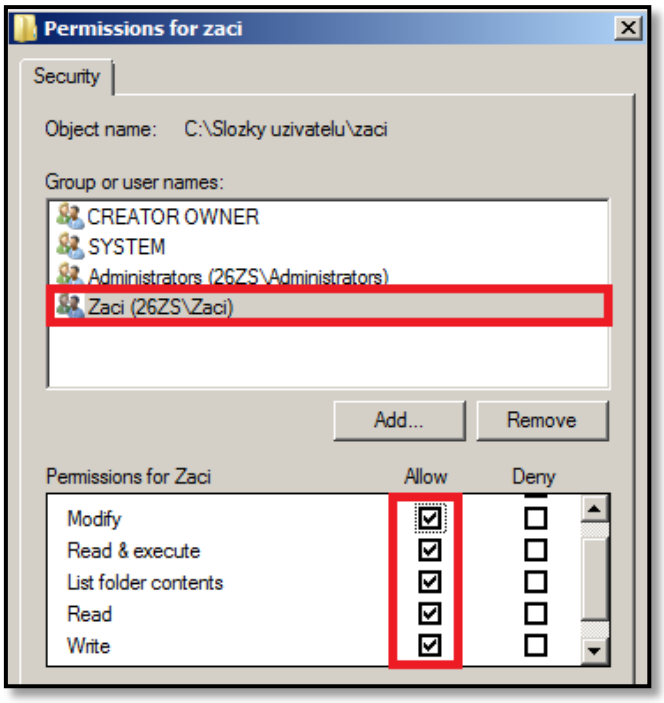
U podsložek "Zaci" a "Ucitele" skupinu "Users" odstraníme. Zde budeme definovat nová práva skupinám "Zaci" a "Ucitele".

2. Aby byla složka "Zaci" přístupná všem žákům, nastavíme práva pro skupinu "Zaci". Klikneme pravým tlačítkem na složku, opět zvolíme možnost **Properties** a na kartě **Security** přidáme skupinu "Zaci". Pro lepší názornost se můžete podívat na obrázek č. 37.



Obrázek 37, Zabezpečení složek na doménovém serveru 2

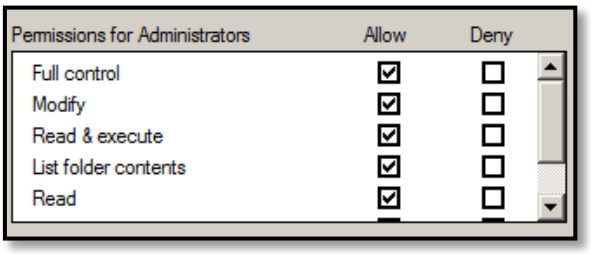
Skupině "Zaci" přidáme práva pro čtení, zápis a procházení složek. Podívejte se na obrázek č. 38.



Obrázek 38, Zabezpečení složek na doménovém serveru 3

3. Analogickým způsobem nastavíme práva pro složku "Ucitele". Jediný rozdíl bude v tom, že místo skupiny "Zaci" bychom přidáme skupinu "Ucitele" a té pak nastavíme práva.

4. Co se týká práv administrátorů, ty mají v našem příkladě ke složce "Uzivatelske slozky" a jejím podsložkám nastavena automaticky nejvyšší práva. To znamená, že bude-li některý z uživatelů členem skupiny "Administrators", bude disponovat právy: udělovat oprávnění, měnit, číst, a další. Můžete se podívat na obrázek č. 39.



Obrázek 39, Zabezpečení složek na doménovém serveru 4

Tímto způsobem jsme tedy zajistili různá přístupová oprávnění ke složkám pro různé skupiny uživatelů podle zadání na začátku této kapitoly.

3.3 BEZPEČNOST A OCHRANA DAT NA ZÁKLADNÍCH ŠKOLÁCH V PLZNI

Pro základní školy zřízené městem Plzní zajišťuje veškerou správu informačních technologií příspěvková organizace SIT (Správa informačních technologií města Plzně). Počítače (včetně softwaru) a všechny síťové prvky jsou majetkem této příspěvkové

organizace. Od toho se odvíjí i celá IT koncepce včetně práv jednotlivých uživatelů (žáků a učitelů). Na základě komunikace s panem Mgr. Miroslavem Nozarem ze SIT Plzeň jsem získal tyto informace o bezpečnostní politice a IT koncepci na základních školách v Plzni:

- Všechny počítače na ZŠ, účty žáků a učitelů jsou součástí jedné domény.
- Uživatelé se přihlašují k doménovým serverům. Doménové servery jsou umístěny v serverovnách SIT.
- Na serverech běží operační systém Microsoft Windows Server 2008 R2.
- Většina aplikací na ZŠ je spouštěna vzdáleně (ze sítě). Nachází se na serveru.
- Přístupová práva ke složkám jsou řešena na úrovni souborového systému NTFS, kde se nastavují oprávnění pro konkrétní osoby nebo skupiny.
- Data na počítačových stanicích jsou každou noc zálohována na pásky a na požadavek uživatele je možné je obnovit.
- Pro sledování činnosti žáků jsou v PC učebnách nainstalovány monitorovací aplikace Desktop klient, případně Master Eye nebo Smart Sync.
- Žáci mohou spouštět nainstalované programy, ukládat si soubory do vlastních uživatelských složek. Žáci samozřejmě nemůžou žádným způsobem administrovat počítač.
- IT Metodici (zvolení uživatelé na ZŠ) mohou zakládat nové účty a provádět jejich editaci (měnit hesla, odemykat účty apod.)
- Klasifikace žáků je zaznamenávána do aplikace "Škola OnLine". Rodiče mohou pohodlně sledovat klasifikaci přes webový portál "Škola OnLine".
- V budoucnu bude zakládání účtů fungovat tak, že škola bude zakládat žáka pouze do aplikace Škola OnLine a doménový účet bude založen automaticky.

4 NEŽÁDOUCÍ VLIVY A JEJICH MOŽNÁ ŘEŠENÍ

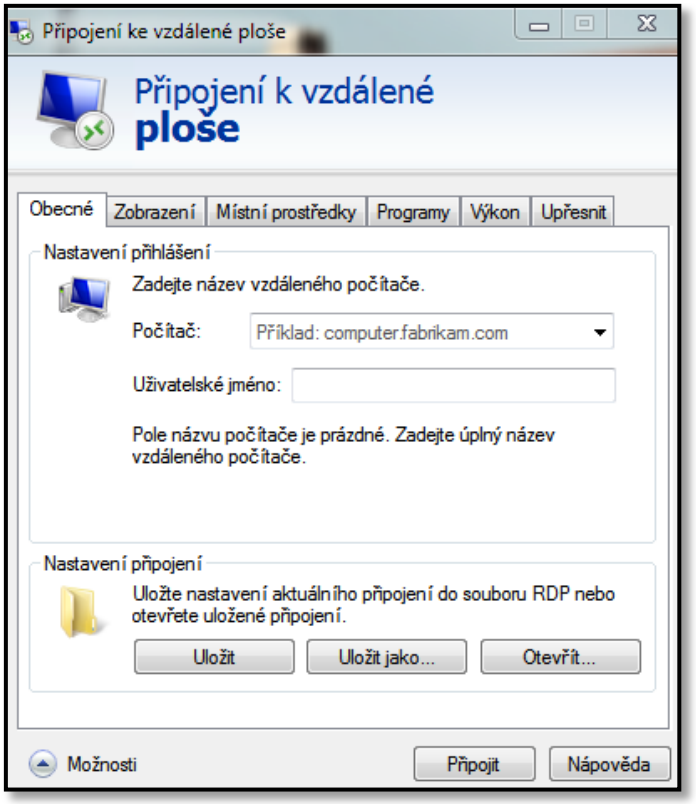
Dalším bezpečnostním problémem může být nežádoucí šíření škodlivého softwaru (Malwaru) označovaného jako "červ" anglicky "worm". V této kapitole se zaměříme na šíření počítačového červa "Morto", který přibližně před rokem zaútočil i na servery nacházející se na ZČU v Plzni.

4.1 WORM "MORTO" A JEHO ŠÍŘENÍ PŘES REMOTE DESKTOP PROTOKOL

Přibližně koncem léta 2011 se začíná v síti Internet silně rozšiřovat nebezpečný Malware, pojmenovaný jako worm (červ) "Morto". Tento červ napadá počítače a servery s operačními systémy Windows přes protokol RDP (Remote Desktop protokol).

4.1.1 ŠÍŘENÍ A CHOVÁNÍ

Jak již bylo zmíněno v předchozím odstavci, "Morto" se šíří přes RDP, který je v operačních systémech Windows používán při přístupu k počítači pomocí vzdálené plochy. Často tak může způsobit velkou řadu problémů ve školních prostředích, kde se přes vzdálenou plochu připojujeme do virtuálních učeben. Každý z operačních systémů Microsoft (od verze Windows XP) obsahuje službu "Remote desktop Connection", která slouží k připojení počítače přes vzdálenou plochu.



Obrázek 40, Připojení ke vzdálené ploše

Poměrně velkým problémem je rychlost a systém šíření tohoto červa. Morto prohledává všechny dostupné počítače v místních sítích a zkoumá, zda mají povolenu komunikaci na portu 3389 (vzdálené přihlášení). Tím, jak port testuje, značně zvyšuje traffic (požadavky na port), což může vést k nadbytečnému zatížení sítě. Z výzkumu na ZČU v Plzni bylo zjištěno, že příchozí traffic na port 3389 byl ve většině případů veden z počítačů mimo univerzitní síť, z čehož vyplývá, že se tento červ pokouší šířit nejen mezi místními sítěmi.

Princip infikace:

a) Z infikovaného počítače se zkouší připojit na IP adresy ze stejné podsítě, v níž se tento počítač nachází, a to pomocí protokolu RDP (TCP port 3389).

b) Pokud je na cílovém počítači tento protokol povolen (je zde povoleno vzdálené přihlášení), zkouší pro přihlášení vybraná jména a hesla.

c) Pokud je úspěšný (na cílovém počítači jsou slabá hesla), nainstaluje se na cílový počítač spuštěním DLL knihovny. K tomu využije vlastnosti vzdálené plochy, která spočívá ve zpřístupnění lokálních disků (jsou dostupné jako \\tsclient\X).

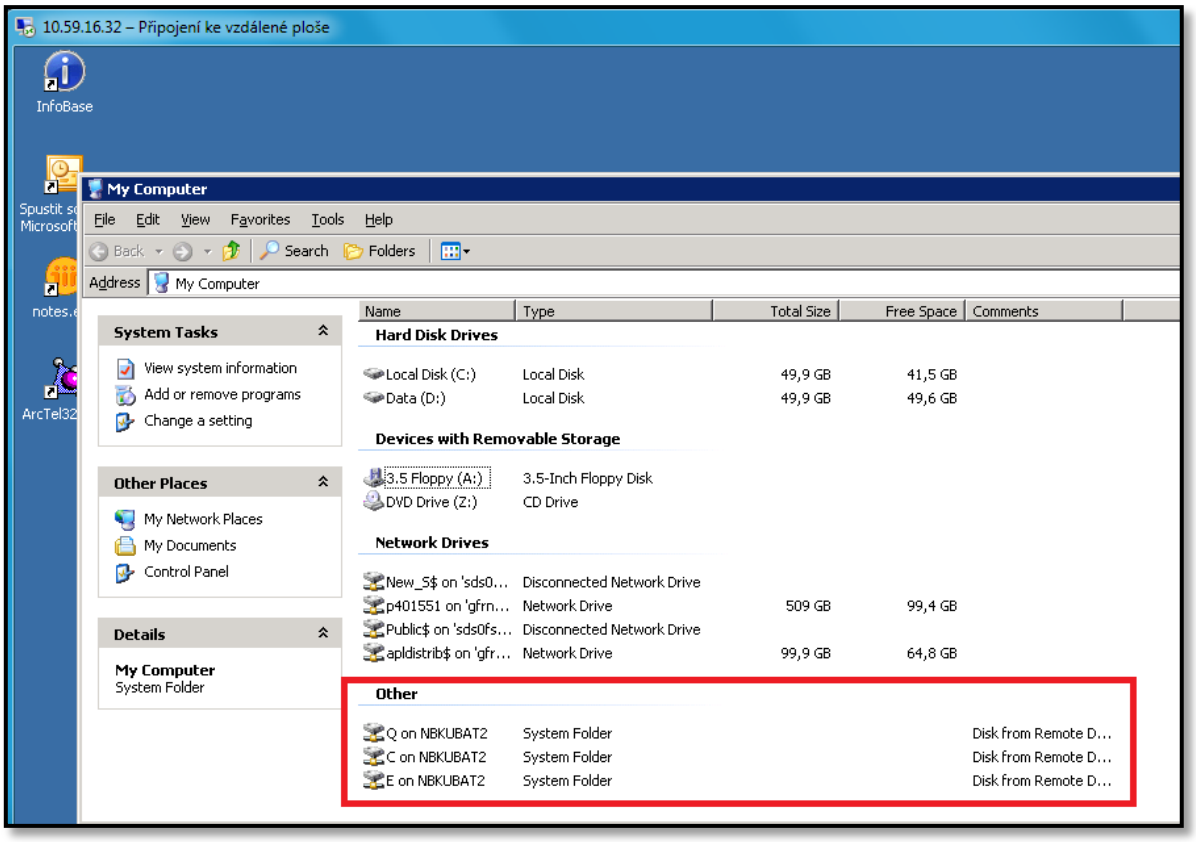
Dle informací ze serveru *"Microsoft Malware Protection Center"* patří mezi často používané přihlašovací údaje:

- Jména:
    - server, test, user, admin, admin2, actuser, owner, root, david, console, sys, user1, user2, atd.
- Hesla:
    - 111, 1234, 111111, 123123, 666666, 888888, 1234567, 12345678, admin123, atd.

4.1.2 ZJIŠTĚNÍ A ODSTRANĚNÍ

Pokud se worm "Morto" připojí ke vzdálenému počítači, má přístup ke všem službám, jako běžně přihlášený uživatel. Zároveň jsou mu přístupny **klientské disky C** a **D** přes službu tsclient.

Podívejte se na následující obrázek. Jedná se o přihlášení k serveru Windows 2003 přes vzdálenou plochu (RDP). V červeném rámečku jsou vidět pevné disky na klientském počítači. Právě z těchto disků se dokáže worm "Morto" jednoduše zkopírovat.



Obrázek 41, Připojení ke vzdálené ploše Windows Server 2003

"Morto" vytvoří dočasnou **diskovou jednotku A na klientském počítači** odkud se pomocí knihovny a.dll rozšíří na server. Dle informací ze serveru *"Microsoft Malware Protection Center"* se na systémových discích objeví celá řada nových souborů, podle kterých lze rozpoznat jeho přítomnost. Jedná se o tyto soubory:

- *%Windows%\clb.dll*
- *%Windows%\clb.dll.bak*
- *%windows%\temp\ntshrui.dll*
- *<systemfolder>\sens32.dll*
- c:\windows\offline web pages\cache.txt

Dochází také k úpravě některých registrů, zmiňme například změny u:

- HKLM\SYSTEM\WpaSets, kde "Morto nastavuje hodnoty":
  - value: *it*Sets
  - value: *id*Sets
  - value: *sn*Sets
  - value: ieSets
  - value: *md*Sets
  - value: *sr*

"Morto" je poměrně špatně detekován antivirovými programy. V době před psaním této práce ho nejlépe identifikoval a odstranil antivir společnosti Symantec. Pokud dojde k infekci, nebo máte podezření, že byl Váš počítač infikován a červa "Morto" se Vám běžným antivirovým programem nepodařilo odstranit, existují speciální nástroje na jeho odstranění.

Symantec

- Norton Power Eraser (NPE).

(http://security.symantec.com/nbrt/npe.aspx?lcid=1033)

Pokud by se nepodařilo nežádoucí software odstranit tímto programem, zvolte následující software, který se spouští při startu počítače na spustitelném médiu.

- Norton Bootable Recovery Tools.

(http://security.symantec.com/nbrt/nbrt.aspx?lcid=1033)

Microsoft

- Microsoft Security Essentials.

(http://windows.microsoft.com/cs-CZ/windows/products/security-essentials)

- Microsoft Safety Scanner (časově omezený program sloužící výhradně pro jednorázové vyhledání a odstranění škodlivého softwaru).

(http://www.microsoft.com/security/scanner/cs-cz/default.aspx)

4.1.3 ELIMINACE NEŽÁDOUCÍCH VLIVŮ

Nejdříve si shrneme základní bezpečnostní zásady, kterých se držet, aby k infekci červem Morto nedošlo. Tyto zásady samozřejmě platí i pro jiný škodlivý software. Následně

se pokusíme navrhnout řešení, které by eliminovalo nadměrný počet přístupu k počítačům, které mají povoleno vzdálené přihlášení (povolen protokol RDP).

4.1.3.1 BEZPEČNOSTNÍ ZÁSADY

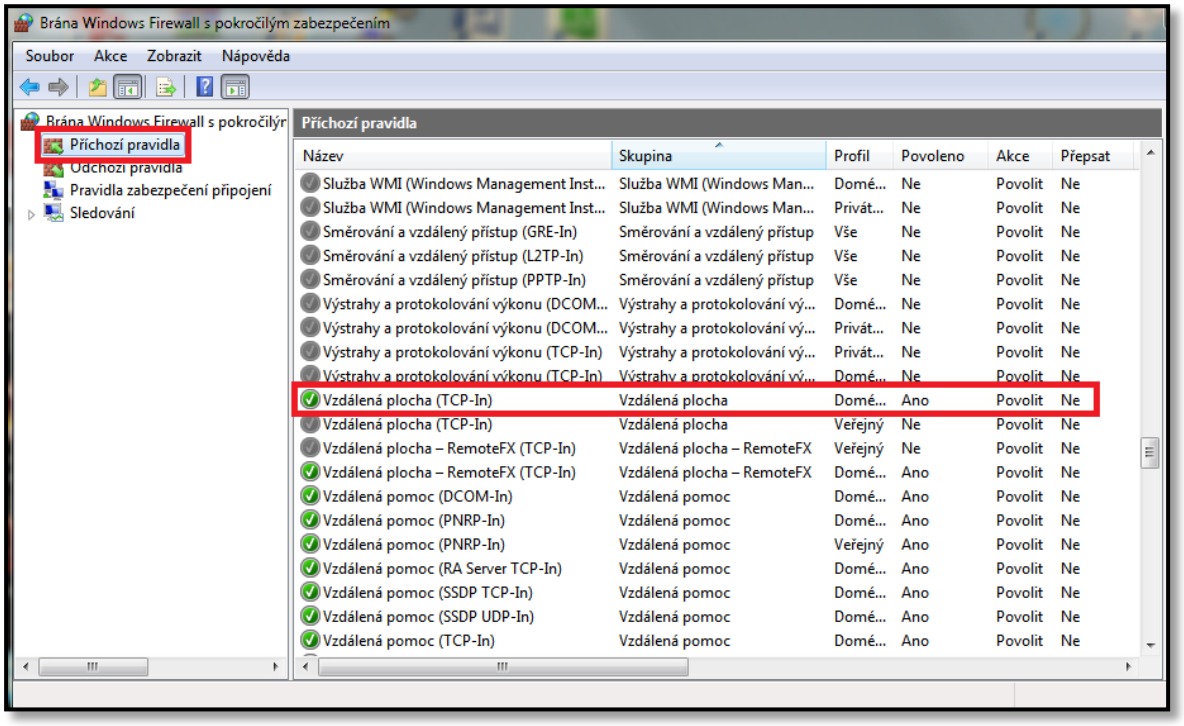
- Mít zapnutou bránu firewall a pro příchozí komunikaci mít povolené jen nezbytně nutné služby.
- Mít aktualizovanou virovou databázi a spuštěný antivirový program.
- Dodržovat správnou politiku hesel. Pro přihlašování volit silná hesla (kombinace písmen a číslic, minimální délka 8 znaků). Pokud se přihlašujete ke vzdálené ploše v doméně, volte silná doménová hesla.
- Zajistit, aby programy a uživatelé měli ta nejnižší práva potřebná pro danou činnost. Běžní uživatelé by neměli mít administrátorská práva, neměli by být schopni sami instalovat aplikace.
- Vypnout autoplay (spuštění programu po vložení média)
- **Nepoužívat sdílení souborů, je-li to možné. Uživatel s povoleným přístupem k adresáři do něj může omylem uložit škodlivý software. Tento software se pak může jednoduše rozšířit ke všem uživatelům, kteří mají tento adresář přístupný v síti.**

4.1.3.2 ELIMINACE NADMĚRNÝCH PŘÍSTUPŮ

Jak se ale zachovat v případě, kdy na daném počítači (serveru) chcete mít protokol RDP povolen, protože slouží například k výukovým účelům a pravidelně k němu přistupují žáci? Řešení nemusí být úplně složité, avšak může být z části lehce omezující. Doporučuji na firewallu počítače, či serveru pevně nastavit, z jakých IP adres je možné k danému výukovému počítači (serveru) přihlásit. Výhodou tohoto řešení je, že požadavky z okolních sítí budou jednoduše odmítány a nikdo mimo vybrané IP adresy se k počítači přes vzdálenou plochu nepřihlásí. Toto řešení je vhodné především v těch případech, pokud se žáci hlásí z nějaké počítačové učebny, kde přesně známe IP adresy počítačů. Nevýhodou může být situace, pokud by se chtěl žák, či jiný uživatel přihlásit z cizího počítače - mimo učebnu a tato IP adresa by ve firewallu nebyla uvedena. Nyní si ukážeme, jak nastavit firewall, aby přes vzdálenou plochu mohli k počítači přistupovat jen vybrané IP adresy.

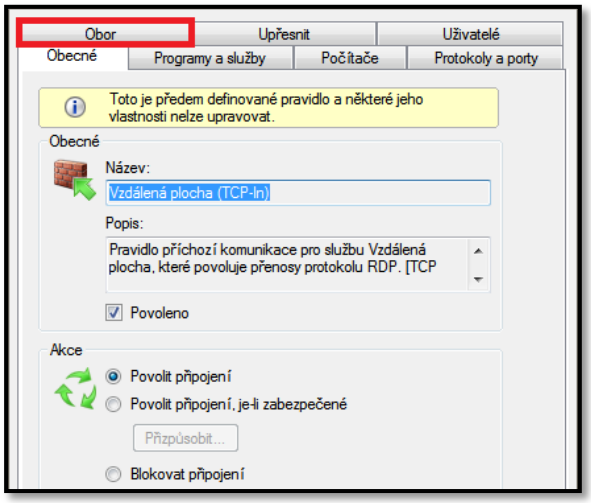
a) Otevřeme si bránu Windows Firewall s pokročilým nastavením. Tato brána je součástí operačních systémů Windows 7 a také Windows Server 2003, Windows Server 2008.

b) Najdeme si kategorii **příchozí** pravidla, ve které se nachází také **vzdálená plocha (TCP-In)**. Na obrázku je vidět, že v tomto případě je vzdálená plocha pro doménový profil povolena.

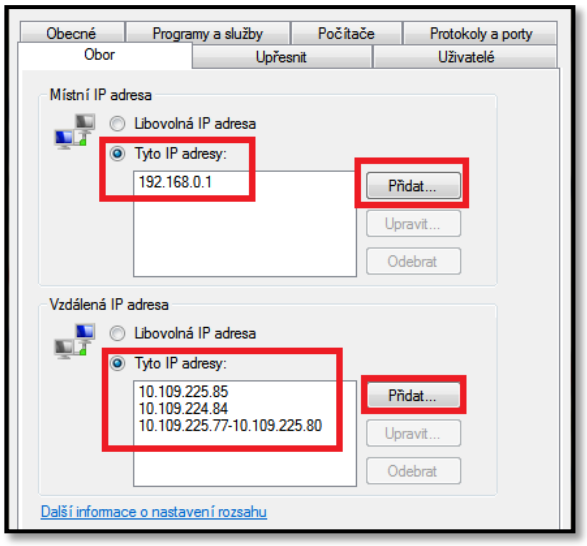


Obrázek 42, Pravidla pro vzdálenou plocha ve Windows Firewall

c) Pokud bychom chtěli, aby k tomuto počítači mohli přistupovat pouze konkrétní IP adresy (konkrétní počítače), pravidlo vzdálené plochy otevřeme. Zobrazí se nám karta pravidla, kde si v horní části vybereme kartu "obor". Podívejte se na následující obrázky.



Obrázek 43, Konfigurace pravidla vzdálené plochy 1



Obrázek 44, Konfigurace pravidla vzdálené plochy 2

d) Na kartě "obor" se nastavují 2 druhy IP adres. **Místní adresa** a **vzdálená IP adresa.** Místní adresa označuje jeden z Vašich síťových adaptérů (v místním PC). Vzdálená adresa označuje vzdálený síťový adaptér (počítače v síti). Pokud byste měli v místním počítači, či serveru více síťových adaptérů, můžete pomocí místní adresy definovat, přes který z těchto místních síťových adaptérů bude přihlášení k Vašemu PC přes vzdálenou plochu povoleno. V části vzdálené IP adresy definujete, které vzdálené počítače budou moci k Vašemu PC přistupovat.

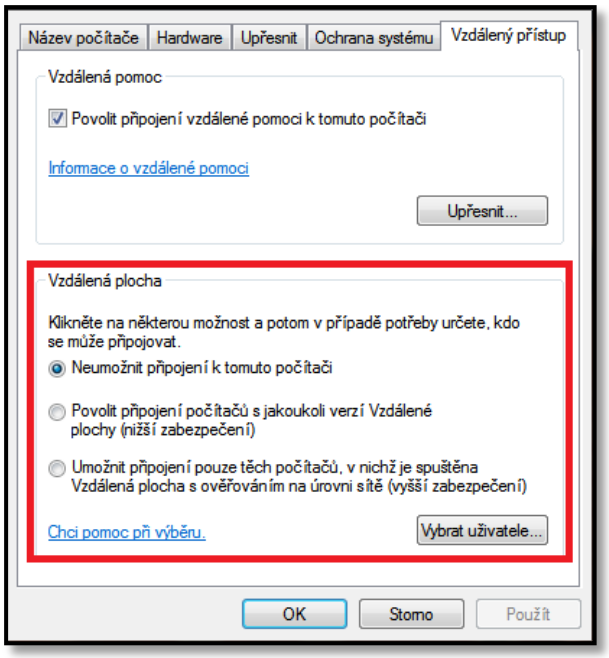
e) Pokud se podíváme na předchozí obrázek, můžeme z něj vyčíst, že veškeré přístupy k tomuto počítači přes vzdálenou plochu jsou povoleny jen přes místní síťový adaptér s IP adresou **192.168.0.1**. Pokud by se v počítači nacházely další síťové adaptéry, pak se přes ně k tomuto počítači pomocí vzdálené plochy nikdo nepřipojí. Z obrázku je také vidět, že se k počítači mohou přes vzdálenou plochu přihlásit tyto počítače, respektive tyto IP adresy:

i. 10.109.225.85

ii. 10.109.225.84

iii. 10.109.225.77, 10.109.225.78, 10.109.225.79, 10.109.225.80

Pokud byste chtěli přístup k Vašemu počítači přes vzdálenou plochu vypnout, můžete to udělat více způsoby.



Obrázek 45, Konfigurace pravidla vzdálené plochy 3

První možností je zakázat vzdálenou plochu přímo v systému. V nabídce **Start** vyberte **Ovládací panely** a následně možnost **Systém**. Otevře se Vám nové okno, kde vyberete záložku **Vzdálený přístup**. Můžete se podívat na obrázek vlevo.

Další možností je najít si v příchozích pravidlech konkrétní pravidlo (výjimku) pro vzdálenou plochu (výběr výjimky jsme popisovali na obrázku č. 42) a v okně **obecné** výjimku zakázat.

V předchozích řádcích jsme si popsali postup, jak eliminovat nadměrné přístupy ošetřením pravidel v bráně firewall. Další možností je definovat pravidla pro přístupy k počítačům v síti přímo na aktivních prvcích (switch[14], router[15]). Podmínkou je, abychom v sítí měli tzv. "chytré" switche či routery. Pod pojmem "chytré" si můžeme představit zařízení, které můžeme efektivně spravovat pomocí speciálního softwaru. "Chytrý" switch dokáže rozpoznat příchozí komunikaci na základě vlastností protokolu IP (například hlavičky datagramu). Díky této vlastnosti dokáže efektivně rozhodnout, co s informací (daty) udělá - jakému zařízení či síťovému prvku je předá. V praxi jsou tyto switche označovány jako L3, či L4 switch.

Administrátor může pomocí speciálního softwaru nastavit router, či "chytrý" switch tak, že povolí přístup na určitých portech (3389 - protokol RDP) pouze některým IP adresám. Pokud tedy zachytí požadavek pro přístup ke vzdálené ploše z některé IP adresy, pro kterou nemá přístup protokolem RDP povolen, požadavek odmítne (zahodí).

[14] **Switch** je aktivní prvek sítě, který spojuje počítače v síti. Počítače se připojují síťovými kabely do portů switche. Portů bývá nejčastěji 8, 16, 24, 48.
[15] **Router j**e aktivní prvek, který směruje - předává informace (data) v síti k jejich cíli. V češtině bývá označován jako směrovač.

5 ŠIFROVANÁ PŘIPOJENÍ A IDENTIFIKACE OSOB A SERVERŮ

Cílem této kapitoly bude přiblížit Vám problematiku šifrovaných připojení a prokázání identity pomocí certifikátů, respektive pomocí elektronických podpisů, v praxi. Začátek kapitoly bude věnován základním termínům v oblasti šifrování a principu podepisování. Uvedení teoretické části je nutné pro pochopení praktických příkladů v druhé části kapitoly.

5.1 ŠIFROVÁNÍ A ELEKTRONICKÝ PODPIS

5.1.1 ŠIFROVÁNÍ

Existuje celá řada pojmů, která je s šifrováním úzce spojena, zmiňme tedy alespoň ty nejpodstatnější. Můžeme využít knihy *"Bezpečnost v Unixu a Internetu v praxi" autorů Garfinkela a Spafforda, kde jsou základní pojmy v oblasti šifrování definovány takto:*

- **Šifrování** je proces, při kterém se zpráva (nešifrovaný text) převede na jinou zprávu (šifrovaný text) pomocí matematické funkce a speciálního šifrovacího hesla, kterému se říká klíč.
- **Dešifrování** je opačný proces. Zašifrovaný text se pomocí matematické funkce a klíče převede zpět na text nešifrovaný.
- **Šifrovací algoritmus** je funkce, nejčastěji sestavená na matematickém základě, pomocí které se provádí samotné šifrování a dešifrování dat.
- **Šifrovací klíč** udává šifrovacímu algoritmu, jak má data šifrovat nebo dešifrovat. Klíče se velice podobají počítačovým heslům. Pokud informaci zašifrujete, musíte k jejímu dešifrování použít správný klíč.
- **Délka klíče – hesla**, i klíče mají nějakou předem určenou délku. Delší klíče jsou bezpečnější než klíče kratší. Různé šifrovací systémy umožňují použití klíčů o různých délkách, některé pak i použití klíčů s proměnnou délkou.

Pokud tedy někomu chcete poslat zprávu (například elektronickou poštou) a nechcete, aby neoprávněná osoba přečetla její obsah, je potřeba zprávu šifrovat. Z definic popsaných výše je jasné, že pro zašifrování je potřeba klíč, který změní zprávu čitelnou (nešifrovanou) na zprávu nečitelnou (zašifrovanou).

Zpráva putuje od odesilatele k příjemci přenosovým kanálem, v dnešní době nejčastěji sítí Internet. Příjemce samozřejmě potřebuje "něco", aby mohl zprávu dešifrovat a přečíst její obsah. To "něco" není nic jiného než klíč. A právě na základě toho, zda nám pro šifrování a dešifrování postačí jeden klíč, rozdělujeme šifrovací systémy na dvě základní skupiny.

5.1.1.1 SYMETRICKÝ ŠIFROVACÍ SYSTÉM

Symetrický šifrovací systém používá pro šifrování a dešifrování zprávy, či dat pouze **jediný, stejný klíč.** To znamená, že zprávu, kterou odesilatel zašifruje svým klíčem, příjemce dešifruje pouze tím stejným klíčem. Výhodou tohoto šifrování je jeho rychlost, matematické výpočty jsou mnohonásobně rychlejší, než je tomu u **asymetrického šifrování**, které zmíníme v další podkapitole. Nevýhodou je nutnost předání jediného klíče příjemci. Pokud není způsob předání zabezpečen, hrozí odposlechnutí klíče a prozrazení obsahu zprávy. V praxi se můžeme se symetrickým šifrováním setkat například při šifrování dokumentů v programu Microsoft Word[16]. Velmi často je pak také používáno v kombinaci s asymetrickým šifrováním, například při zabezpečené komunikaci s webovými servery. Zabezpečené komunikaci se budeme věnovat v konkrétních příkladech na konci této kapitoly. Je nutné si však uvědomit, že použití symetrického šifrování vyžaduje předchozí výměnu šifrovacího klíče jiným bezpečným způsobem, a to například pomocí **asymetrického šifrování**.

5.1.1.2 ASYMETRICKÝ ŠIFROVACÍ SYSTÉM

Jak jistě tušíte, v asymetrickém šifrovacím systému se nesetkáme pouze s jedním klíčem, ale s takzvaným "klíčovým párem", který tvoří **klíč soukromý** a **klíč veřejný**. Jeden klíčový pár pak náleží vždy jedné konkrétní osobě, popřípadě serveru. Pro tento klíčový pár platí tato pravidla:

- **Zašifrovat data lze vždy jedním klíčem, dešifrovat pak pouze druhým.**
- **Z jednoho klíče nelze odvodit klíč druhý.**
- **Soukromý klíč zůstává vždy u jeho vlastníka, nikdy nesmí být zveřejněn.**
- **Veřejný klíč by měl být dostupný všem, kteří chtějí s dotyčnou osobou komunikovat.**

[16] **MS Word** je textový editor od společnosti Microsoft vhodný pro tvorbu a editaci dokumentů.

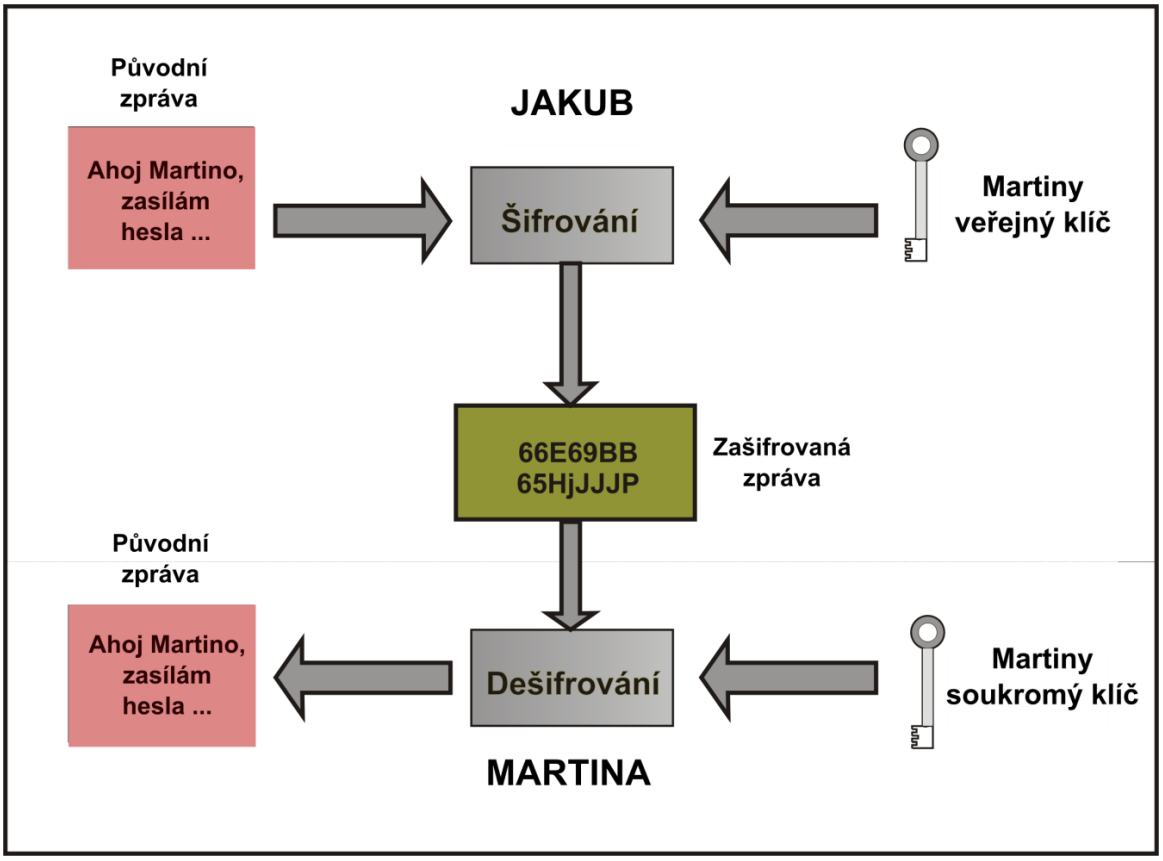
Princip asymetrického šifrování si můžeme popsat na jednoduchém příkladu.

a) Jakub chce zašifrovat dokument a poslat ho Martině. Přitom si chce být jist, že obsah dokumentu si přečte pouze Martina.

b) Jelikož Jakub ví, komu dokument posílá, najde si veřejný klíč Martiny (měl by být dostupný každému, kdo by chtěl Martině posílat zabezpečené zprávy) a zašifruje jím dokument.

c) Zašifrovaný dokument pošle nezabezpečeným kanálem Martině. V tuto chvíli je dokument nečitelný pro okolí.

d) Martina dokument obdrží, a jelikož pouze ona je vlastníkem soukromého klíče, dokument dešifruje a získá tak obsah Jakubovy zprávy.



Obrázek 46, Asymetrické šifrování

Mezi dnes nejpoužívanější asymetrické šifrovací algoritmy se řadí algoritmus RSA. **Používá se například pro šifrování symetrického klíče**, kterým bývá zašifrována celá zpráva. Asymetricky zašifrovaný symetrický klíč, jehož velikost je oproti původnímu dokumentu daleko menší, je díky technologii asymetrické kryptografie bezpečně chráněn při cestě komunikačním kanálem k příjemci dokumentu. Další oblastí, ve které se můžeme

s asymetrickým algoritmem RSA setkat, je digitální podepisování dokumentů (elektronický podpis), či ověření identity serverových služeb. Nyní si pojďme říci, jaký je základní rozdíl mezi šifrováním a podepisováním dokumentů.

5.1.2 ELEKTRONICKÝ PODPIS

Elektronický podpis je obdobou podpisu, kterým podepíšeme papírový dokument. Podepisujeme jím data v elektronické podobě. Elektronický podpis zaručuje:

- Identifikaci původce dokumentu.
- Integritu, celistvost původního dokumentu.
- Odesílatel je svázán s vytvořeným dokumentem a nemůže popřít, že jej vytvořil.

Při elektronickém podepisování dokumentů se opět využívá asymetrického šifrování RSA. Ovšem oproti šifrování se dokument podepisuje soukromým klíčem odesílatele a příjemce podpis ověří pomocí veřejného klíče odesílatele. Můžeme tedy říct, že podepisování je vlastně šifrování soukromým klíčem odesílatele.

Ve skutečnosti se ale nepodepisuje celá zpráva, ale jen její část a to tzv. **HASH (otisk)**. **HASH** je jednoznačný, relativně krátký řetězec, který vznikl z původní zprávy aplikováním jednosměrné transformace (Hashovací funkce). Velice důležitou vlastností HASHE je, že z něj **nelze zpětně získat původní dokument**. Mezi nejčastěji používané hashovací funkce můžeme zařadit funkce MD5 a SHA2.

Princip podepisování můžeme opět popsat na jednoduchém příkladu.

a) Jakub chce Martině poslat dokument a připojit k němu svůj elektronický podpis, aby bylo jasné, že dokument vytvořil doopravdy on.

b) Z dokumentu se pomocí matematické funkce vytvoří HASH (otisk), ten je daleko menší než původní dokument.

c) Hash (otisk) se zašifruje soukromým klíčem odesilatele, **výsledkem šifrování** je tzv. **elektronický podpis**.

d) Elektronický podpis je poslán spolu s dokumentem příjemci, v našem případě Martině.

e) Martina vypočítá z dokumentu stejnou matematickou funkcí HASH (otisk). Veřejným klíčem odesílatele pak dešifruje elektronický podpis, který vytvořil Jakub.

f) Původní HASH (otisk), který byl vytvořen na straně odesílatele - Jakuba, se porovná s HASHEM (otiskem) vytvořeným příjemcem - Martinou. Pokud jsou tyto hodnoty stejné, jedná se o originální a platný elektronický podpis.

Po přečtení principu elektronického podepisování dokumentů jste si určitě položili jednu zásadní otázku, jak ale ověříme, že veřejný klíč, kterým ověřujeme identitu podepsané osoby, patří právě jí? Ověření identit osob a serverů se provádí pomocí jejich certifikátů.

5.2 CERTIFIKÁTY, CERTIFIKAČNÍ AUTORITY A IDENTIFIKACE SUBJEKTŮ

5.2.1 CERTIFIKÁTY A JEJICH VÝZNAM

Certifikát je dokument, který zaručuje identitu podepsané osoby. Při tomto tvrzení je jasné, že certifikáty musí vydávat nějaké důvěryhodné třetí strany. Je tomu doopravdy tak, certifikáty vydávají **Certifikační autority,** přičemž každý certifikát, který vydají, samy podepisují svým elektronickým podpisem. Součástí certifikátu tedy bývá řada údajů jako:

- Jméno osoby, které byl certifikát vydán.
- Veřejný klíč osoby, datum platnosti certifikátu.
- Název vydavatele certifikátu, elektronický podpis vydavatele.

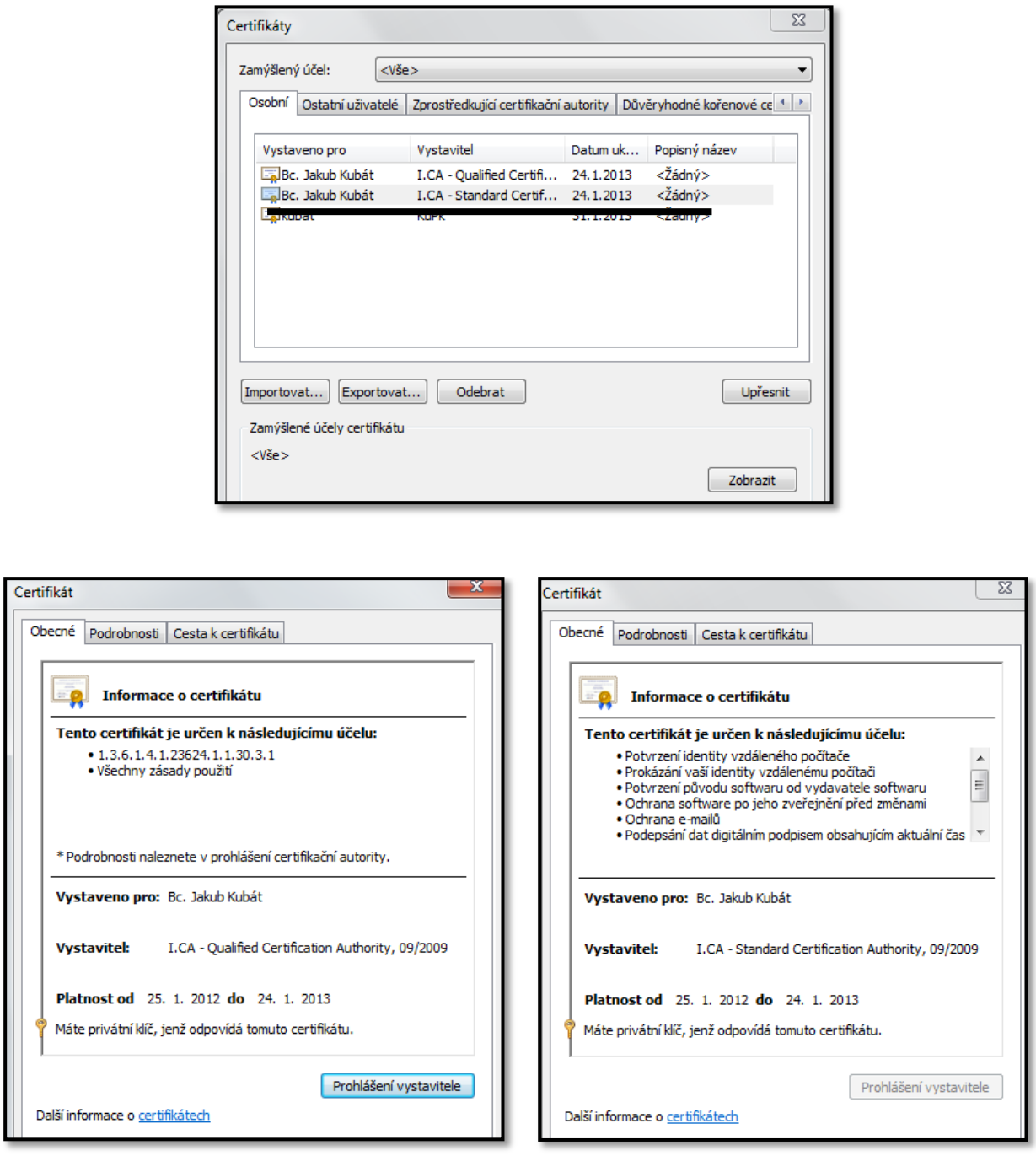
Existují různá dělení certifikátů, my se na dělení certifikátů podíváme ze dvou různých úhlů pohledu. V prvním případě můžeme vzít jako kritérium to, zda byl certifikát vydán fyzické, či právnické osobě. Podle toho rozdělujeme certifikáty na:

- **Osobní certifikáty** - Vydávány pouze fyzickým osobám.
- **Systémové certifikáty** - Vydávány fyzickým ale i právnickým osobám. Mohou být používány také pro identifikaci serverů či pro šifrovanou komunikaci.

V druhém případě můžeme certifikáty dělit podle toho, co všechno smí dle zákona obsahovat a k čemu se smí podle zákona používat. Rozdělujeme je na:

- **Komerční certifikáty** - Slouží k šifrování, přihlašování a prokázání identity při přístupu k serveru. Používají se například při přihlašování do internetového bankovnictví.
- **Kvalifikované certifikáty** - Slouží k podepisování a k ověřování podpisů. Používají se například při podepisování dokumentů.

Na následujícím obrázku můžete vidět kvalifikovaný a komerční certifikát vydaný 1. Certifikační autoritou (ICA). Certifikáty jsou uloženy v centrálním úložišti Windows.



Obrázek 47, Kvalifikovaný a komerční certifikát ve Windows

Rozdíl mezi komerčním a kvalifikovaným certifikátem je také ten, že pokud chcete komunikovat s orgány veřejné moci, musíte svoji identitu prokázat pomocí kvalifikovaného certifikátu. A nyní se již pojďme podívat na konkrétní postup, jak si vytvořit vlastní

kvalifikovaný či komerční certifikát, abyste byli schopni při elektronické komunikaci jasně prokázat svojí identitu[17].

5.2.2 VYDÁNÍ CERTIFIKÁTŮ ANEB PRVNÍ KROK PRO PROKÁZÁNÍ IDENTITY

1. Prvním krokem pro vydání certifikátu je podání žádosti o certifikát. Žádost podáte u jedné ze tří akreditovaných certifikačních autorit v České Republice. To, že byla certifikační autorita akreditována, znamená, že splňuje předepsané podmínky a může vydávat kvalifikované certifikáty pro potřeby komunikace s orgány veřejné moci.

    - ICA (První certifikační autorita, http://www.ica.cz)
    - PostSignum (Certifikační autorita České pošty, http://www.postsignum.cz/)
    - eIdentity (http://www.eidentity.cz)

    My si pro náš příklad zvolíme "První certifikační autoritu".

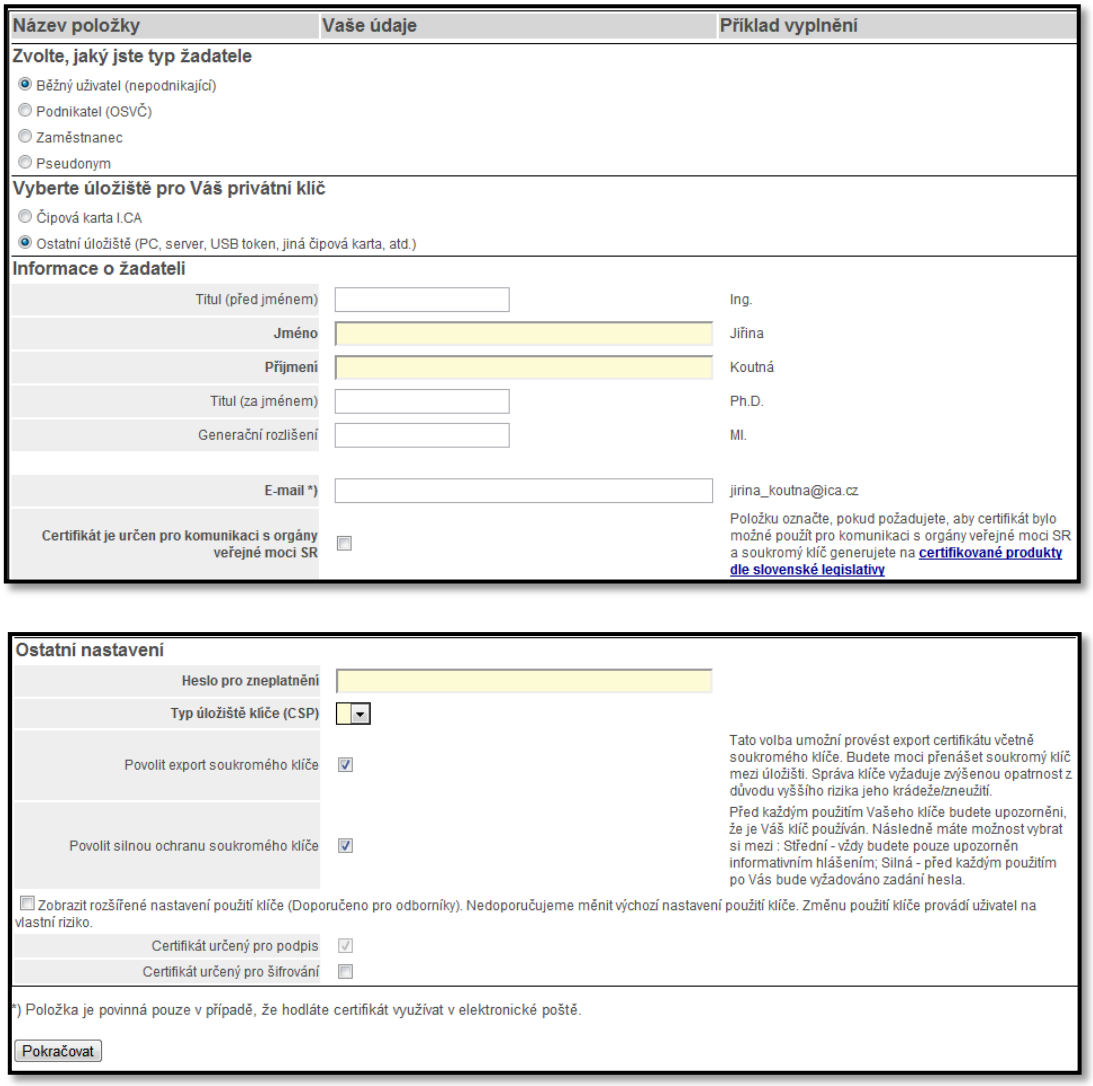
2. Po navštívení internetových stránek ICA vybereme položku "Komerční a kvalifikované certifikáty".

Obrázek 48, Internetové stránky 1. Certifikační autority

[17] Existují i jiné způsoby vydání certifikátu elektronického podpisu než ten uvedený dále v této kapitole. Jedná se většinou o certifikáty, kdy potřebujeme ověřit jejich pravost pouze v rámci uzavřené společnosti. V tomto případě není potřeba, aby certifikát vydávali akreditované certifikační autority. Certifikát si může vydat sama společnost pro své soukromé účely (například ověření identity při přihlášení k místní síti).

Ještě než přistoupíme k tvorbě žádosti, je nutné zmínit jednu zásadní skutečnost. Certifikát můžete mít nejen ve Vašem počítači, ale také například na nějakém přenosném zařízení, například čipové kartě. Pokud ale budete chtít používat certifikát ve Vašem PC, například pro následné podepisování emailových zpráv, je nutné, opakuji, je nutné **vytvářet žádost na tom počítači, kde chcete v budoucnu elektronický podpis používat**. Při tvorbě žádosti jsou totiž některé její údaje ukládány do registrů operačního systému.

3. Po stisknutí volby **vytvořit žádost** proběhne test připravenosti Vašeho PC. Pokud jsou výsledky testu v pořádku, stisknete tlačítko **zahájit tvorbu žádosti o certifikát**. Objeví se Vám tabulka, kde vyplníte Vaše osobní údaje a typ úložiště Vašeho budoucího certifikátu.



Obrázek 49, Žádost o certifikát

4. Po vyplnění všech položek, stisknete tlačítko "pokračovat". Žádost budete moci uložit na pevný disk Vašeho PC.

5. Soubor žádosti nesoucí název "certQC.req" uložíte na disk. Nyní je potřeba osobně navštívit operátorské centrum Certifikační autority, kde Vám bude vydán Váš certifikát, který si následně importujete do Vašeho počítače. Při návštěvě certifikační autority budete potřebovat:
    - Hlavní průkaz totožnosti (Občanský průkaz, pas).
    - Druhý průkaz totožnosti (Řidičský průkaz, kartička pojištěnce, nebo jiný doklad, kde bude Vaše fotografie a iniciály).
    - Žádost o certifikát, kterou jsme si před chvílí vytvořili.

6. Při návštěvě operátorského centra certifikační autority budete vyzváni k prokázání totožnosti a následně budou okopírovány Vaše osobní doklady. Operátor Vám vystaví certifikát, ten Vám přijde na Vaši emailovou adresu uvedenou v žádosti. Samozřejmostí při vydání certifikátu je také smlouva o certifikátu, ve které jsou uvedeny Vaše údaje a údaje o certifikátu (jeho platnost, sériové číslo, atd.). Platnost komerčních a kvalifikovaných certifikátů je 1 rok.

V mezidobí mezi vytvořením žádosti o certifikát a importem certifikátu je zakázáno jakýmkoli způsobem měnit heslo v operačním systému. Pokud by se tak stalo, následný import certifikátu by nebyl úspěšný.

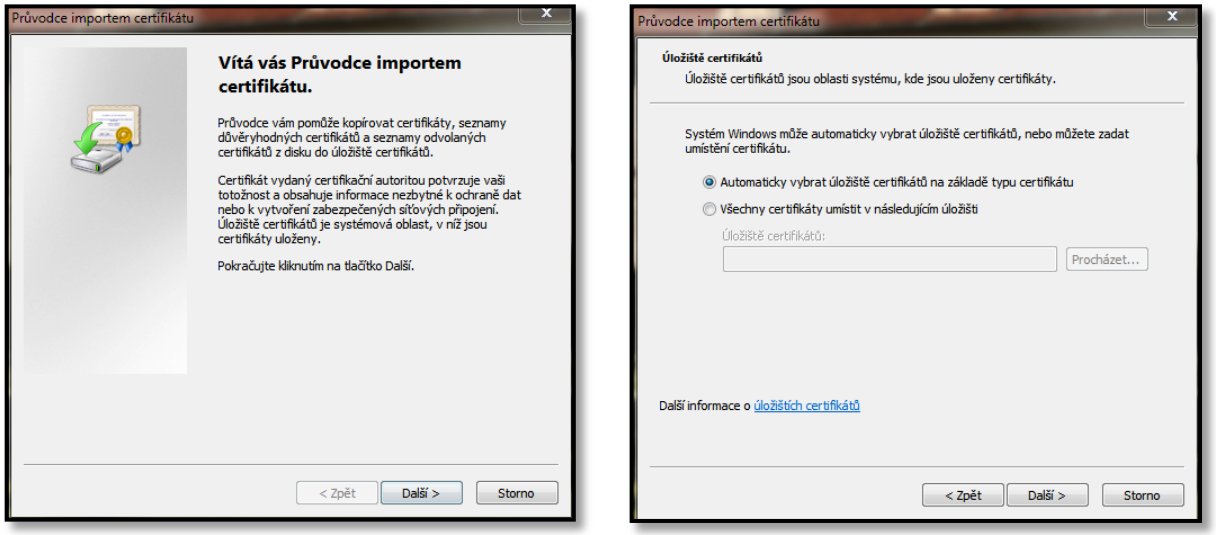
5.2.3 IMPORT CERTIFIKÁTU

V předchozí kapitole jsme si ukázali, jak certifikát získat. Abychom ale byli schopni prokazovat svoji identitu, je potřeba certifikát vhodným způsobem importovat do operačního systému. Nyní již k samotnému postupu importu.

1. Otevřeme si složku, kam jsme si uložili náš certifikát vydaný certifikační autoritou. Soubor s certifikátem má příponu "der". Stiskneme pravé tlačítko myši a vybereme položku **nainstalovat certifikát**.

2. Spustí se průvodce importem certifikátu, který na základě typu certifikátu automaticky vybere vhodné úložiště, kam se certifikát importuje. Osobní certifikáty se importují do úložiště systému Windows, které je společné pro všechny aplikace společnosti

Microsoft (Explorer, Word, Outlook, atd.). Úložiště Windows je zobrazeno na obrázku č. 47.



Obrázek 50, Import certifikátu

3. Pokud import proběhne v pořádku, budeme o tom informováni. Pro jistotu se můžeme ještě podívat do úložiště certifikátů Windows, kde by v záložce "osobní" měli být výše uvedené certifikáty - viz obrázek č. 47.

Na předchozích stránkách jsme si popsali postup, pomocí kterého si vytvoříte vlastní certifikát, abyste mohli dotyčnému, se kterým budete komunikovat, prokázat svoji identitu. Určitě Vás ale napadne zásadní myšlenka. Můžu považovat osobu nebo server, se kterými komunikuji, za důvěryhodné? Respektive jsou jejich certifikáty důvěryhodné? Zaručil se někdo za pravost těchto subjektů? Veškerá tato problematika je řešena pomocí "Důvěryhodných kořenových certifikátů certifikačních autorit".

5.2.4 PROBLEMATIKA OVĚŘENÍ SUBJEKTU

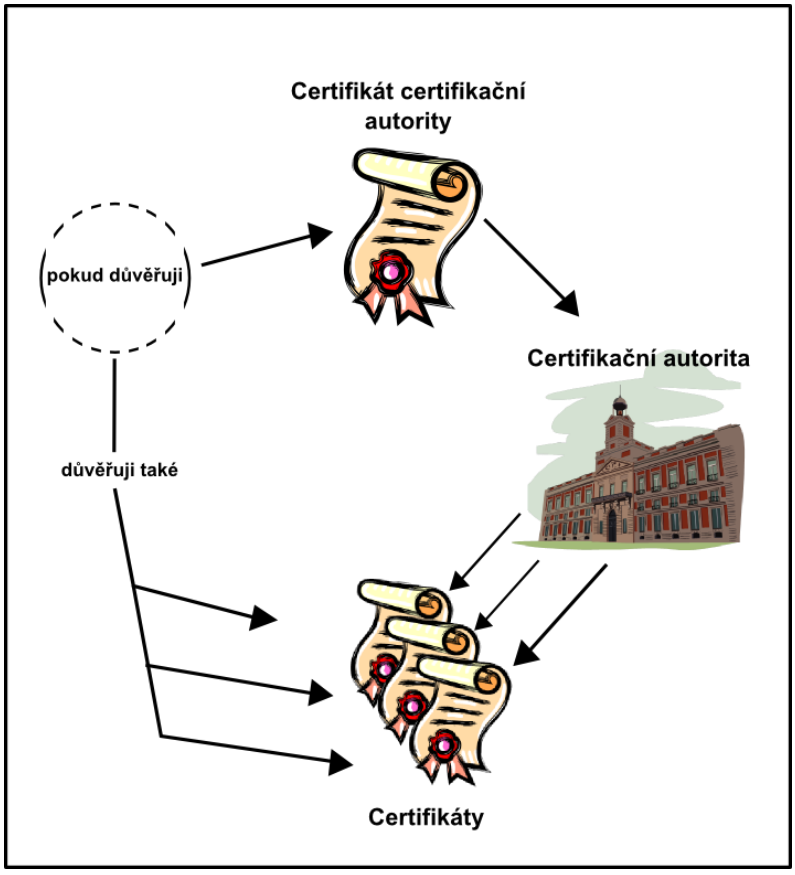
Z předchozí kapitoly je tedy jasné, že pokud chceme ověřit identitu osoby, či serveru, se kterými komunikujeme, je potřeba mít jejich certifikát v úložišti certifikátů. Existují dva základní způsoby, jak certifikát získat, nebo spíše, jak ověřit identitu.

- Osobu důvěrně známe, požádáme ji, aby exportovala svůj certifikát, a ten nám poslala. My si ho následně importujete do úložiště certifikátů.
- Osobu důvěrně neznáme. Její certifikát je posílán automaticky spolu se zprávou. Jelikož každý certifikát je někým vydáván (certifikační autoritou). V rámci tzv.

"stromu delegace důvěry" pak stačí důvěřovat kořenovému certifikátu certifikační autority, který je nutné mít uložen v úložišti certifikátů.

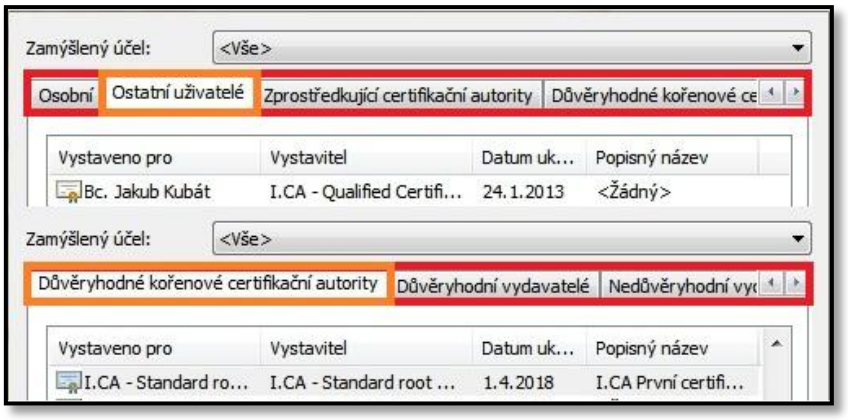
5.2.4.1 STROM DELEGACE DŮVĚRY A DĚLENÍ CERTIFIKÁTŮ V CENTRÁLNÍM ÚLOŽIŠTI WINDOWS

Představte si, že Vám přijde dokument nebo email podepsaný jistou osobou. S dokumentem bývá zasílán také certifikát této osoby. Dotyčného osobně neznáte, avšak potřebujete si být jisti, že certifikát byl vydán doopravdy té osobě, která je na něm uvedena. Základní filosofie vychází z toho, že certifikát byl vydán jistou certifikační autoritou a v rámci stromu hierarchie důvěry stačí důvěřovat pouze této certifikační autoritě, respektive jejímu certifikátu. Můžeme tedy říct, že **pokud důvěřujeme jisté certifikační autoritě, důvěřujeme všem certifikátům, které tato certifikační autorita vydala**.



Obrázek 51, Strom delegace důvěry

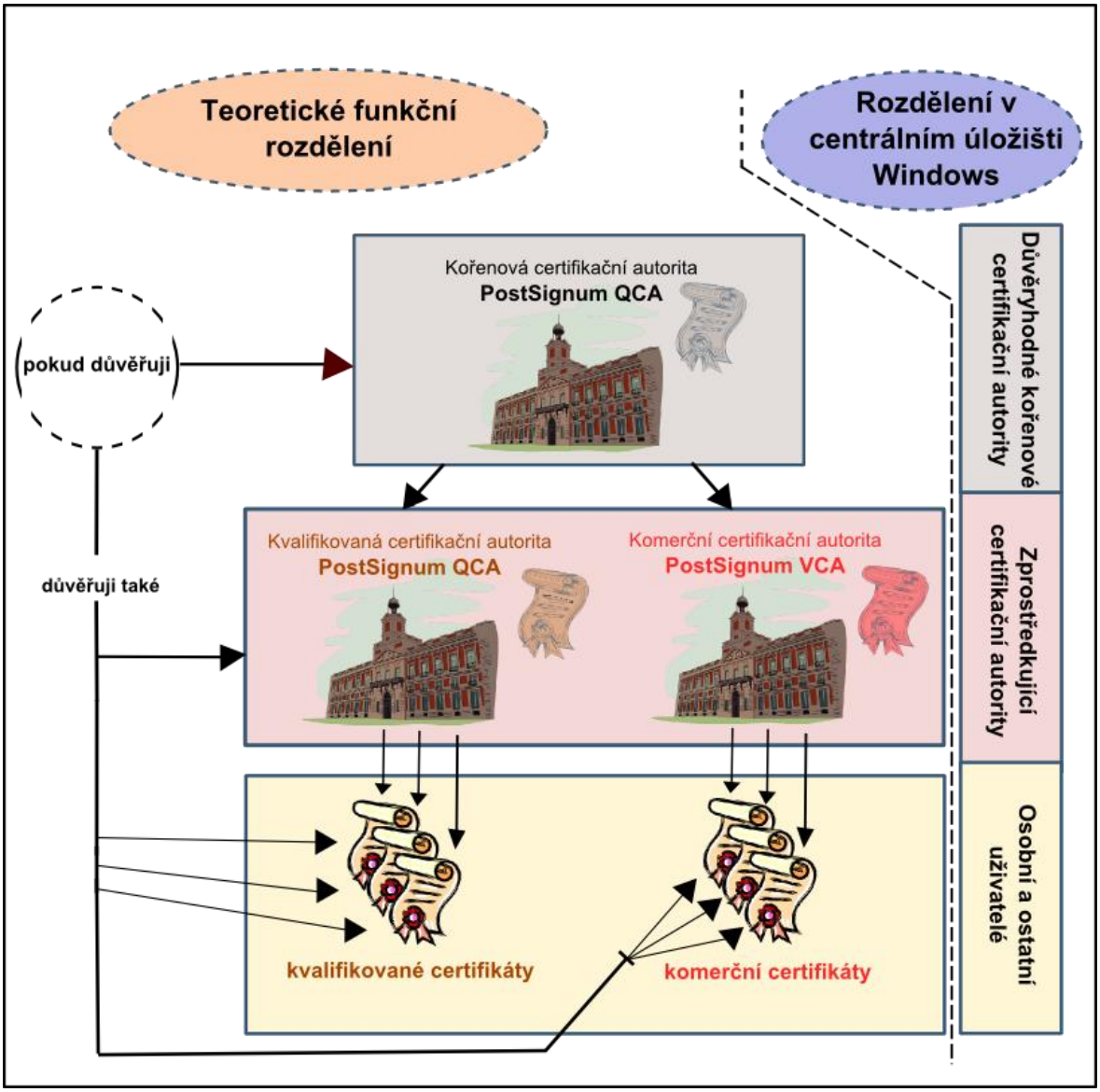
Na úplném počátku stromu důvěry je tzv. kořenový certifikát, který náleží kořenové certifikační autoritě. Pojďme se nyní podívat do úložiště certifikátů systému Windows a projděme si jeho jednotlivé části. Podívejte se na následující obrázek.



Obrázek 52, Centrální úložiště certifikátů Windows

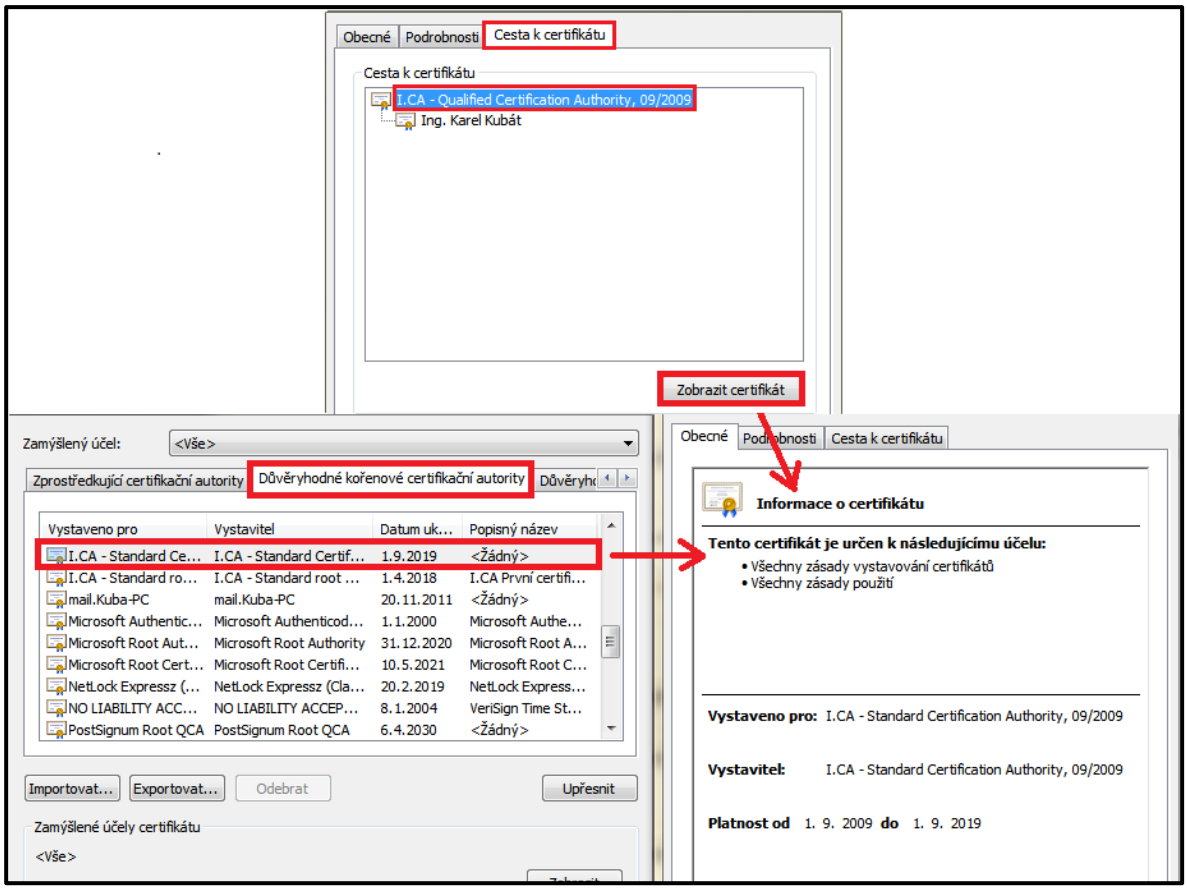
- **Osobní** - Zde jsou uloženy osobní certifikáty aktuálního uživatele. Do této složky bývají umísťovány certifikáty, jejichž součástí je také soukromý klíč, který je uložen v systému.
- **Ostatní uživatelé** - Osobní certifikáty dalších uživatelů. V systému nejsou uloženy soukromé klíče odpovídající těmto certifikátům. Můžeme říct, že se jedná o certifikáty, které jste například obdrželi od uživatele, který Vám poslal podepsaný dokument.
- **Zprostředkující certifikační autority** - Stromová hierarchie důvěry nemusí obsahovat pouze jednu certifikační autoritu, ale může jich být více. Například kořenová certifikační autorita PostSignum Root QCA má pod sebou ještě další dvě certifikační autority - PostSignum QCA a PostSignum VCA. A právě tyto dvě certifikační autority jsou poté zařazeny ve složce "Zprostředkující certifikační autority".
- **Důvěryhodné kořenové certifikační autority** - Zde jsou uloženy kořenové certifikáty důvěryhodných certifikačních autorit. Jedná se o tzv. self-signed certifikáty, neboli o certifikáty opatřené vlastním podpisem (podepíše si je sama kořenová certifikační autorita).
- **Nedůvěryhodní vydavatelé** - V této složce se nachází certifikáty, ke kterým nemáte důvěru.

Na následujícím obrázku můžete vidět stromovou hierarchii certifikačních autorit PostSignum s doplněním informací, kde příslušné certifikáty najdete v centrálním úložišti certifikátů Windows.



Obrázek 53, Stromová hierarchie důvěry

Jako další konkrétní důkaz stromové hierarchie můžeme zmínit osobní certifikát Ing. Karla Kubáta, který najdeme ve složce ostatní certifikáty (je určen pro ověření platnosti elektronického podpisu). Pokud si zobrazíme podrobnosti certifikátu, respektive cestu k certifikátu, jasně vidíme, že certifikát vydala 1. certifikační autorita. Jelikož kořenový certifikát 1. certifikační autority máme zařazen ve skupině "důvěryhodné certifikační autority" je identita tohoto osobního certifikátu bez problémů prokázána.



Obrázek 54, Důkaz stromové hierarchie důvěry ve Windows

Certifikáty některých certifikačních autorit jsou implicitně součástí systému Windows. Často dochází k automatické aktualizaci kořenových certifikátů certifikačních autorit, aniž byste o tom věděli. To do značné míry zjednodušuje proces ověřování identity. Systém si automaticky stahuje kořenové certifikáty a dokáže tak následně ověřit platnost všech podřízených osobních certifikátů, které certifikační autorita vydala.

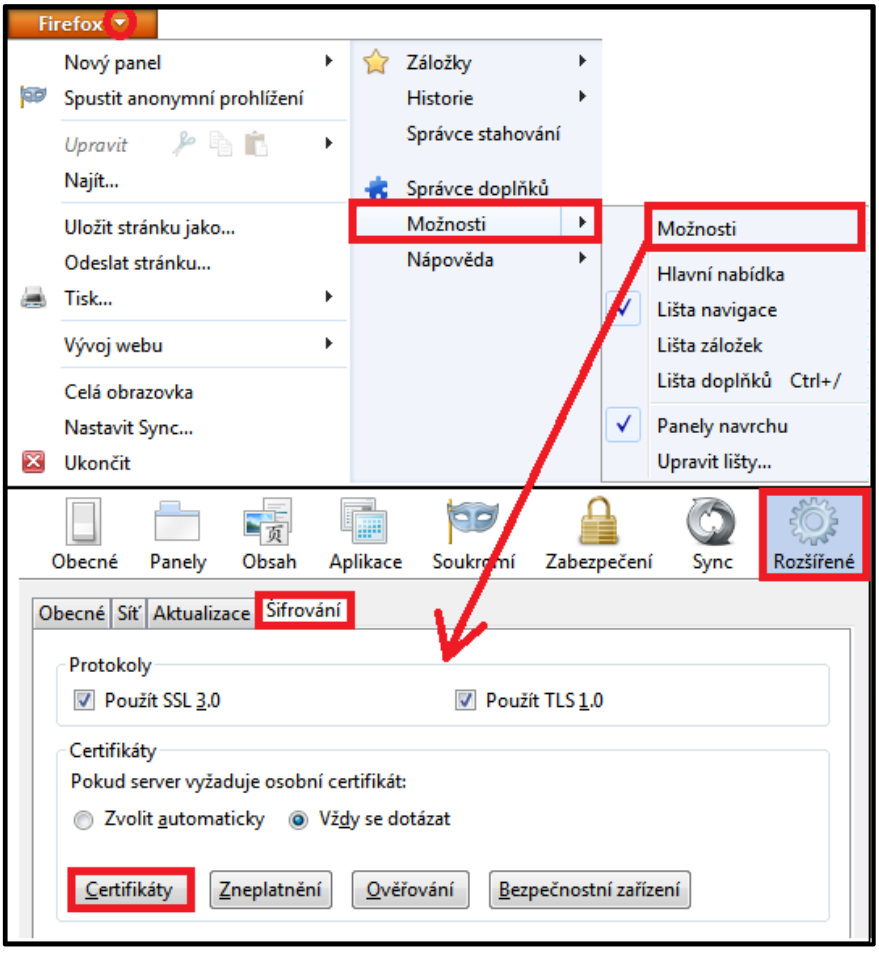
5.2.4.2 DALŠÍ ÚLOŽIŠTĚ CERTIFIKÁTŮ

Je třeba zmínit ještě jednu zásadní skutečnost. Některé aplikace, jako je například prohlížeč **Firefox, nevyužívají pro ověření identity centrální úložiště Windows**, ale certifikáty hledají ve svém vlastním úložišti. Podobně je tomu také například u aplikace **Acrobat Reader**, která má také svoje vlastní úložiště certifikátů.

Název úložiště		Programy využívající toto úložiště
Centrální úložiště Windows	Microsoft Windows	Internet Explorer, Google Chrome, MS Outlook, MS Word
Úložiště certifikátů prohlížeče Firefox		Mozzila Firefox
Úložiště certifikátů programu Adobe Reader	PDF Adobe	Adobe Reader

Tabulka 2, Úložiště certifikátů

Na dalším obrázku se můžeme podívat, jakým způsobem zobrazíte úložiště certifikátů prohlížeče Firefox.

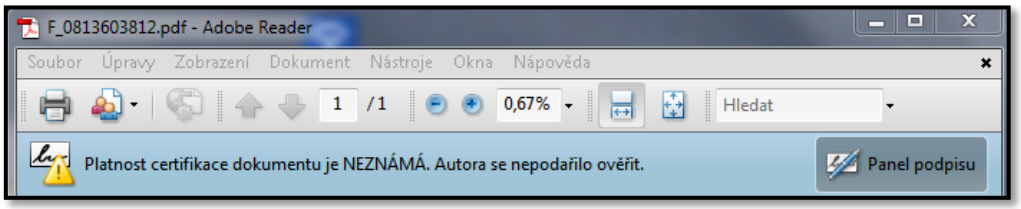


Obrázek 55, úložiště certifikátů Firefox

5.2.4.3 INTEGRACE APLIKACE ADOBE ACROBAT READER S ÚLOŽIŠTĚM WINDOWS

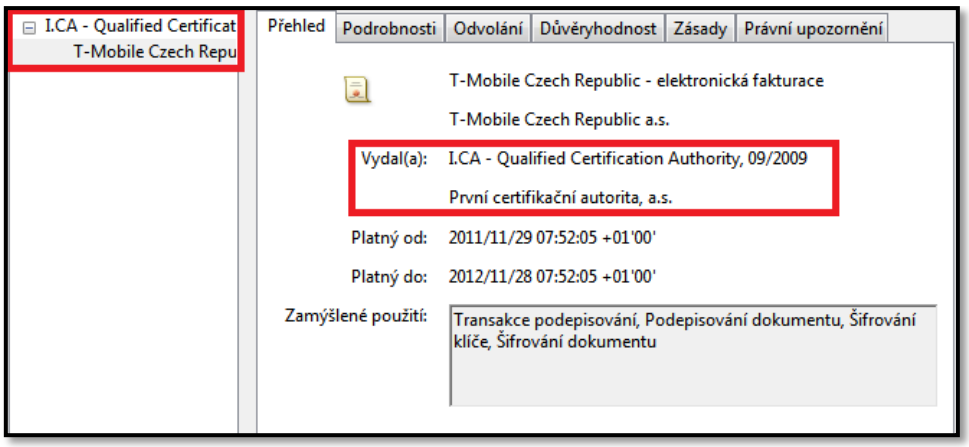
Na následujícím krátkém příkladu si ukážeme, jak umožnit, aby aplikace Adobe Reader při otevření dokumentů prohledávala centrální úložiště Windows a vy jste nemuseli jeden certifikát složitě importovat do více úložišť.

Určitě jste v aplikaci Adobe Reader někdy otevřeli podepsaný dokument a v jeho horní části se objevil nápis "Platnost certifikace dokumentu je NEZNÁMÁ. Autora se nepodařilo ověřit". Je to tím, že příslušný certifikát důvěryhodné certifikační autority nemáte uložen přímo v úložišti této aplikace.



Obrázek 56, Neúspěšné ověření podpisu Adobe Acrobat

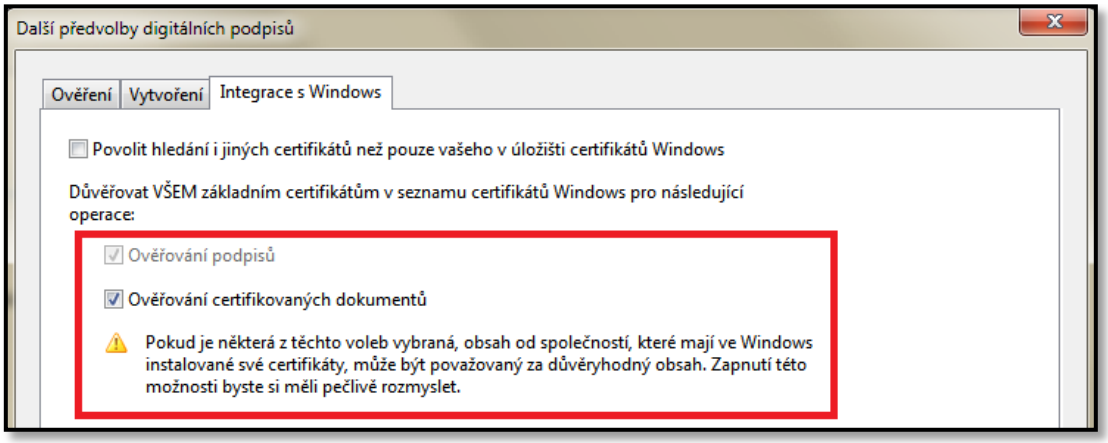
Pokud stiskneme položku **Panel podpisu** a dále vybereme možnost "Podrobnosti certifikátu", vidíme celou certifikační cestu. V našem případě je podepisovaný subjekt "T-Mobile Czech Republic" a jeho vydavatel je "1. Certifikační autorita - I.CA". My přitom máme certifikát 1. certifikační autority uložen mezi důvěryhodnými certifikáty v centrálním úložišti Windows.



Obrázek 57, Cesta k certifikátu Adobe Acrobat

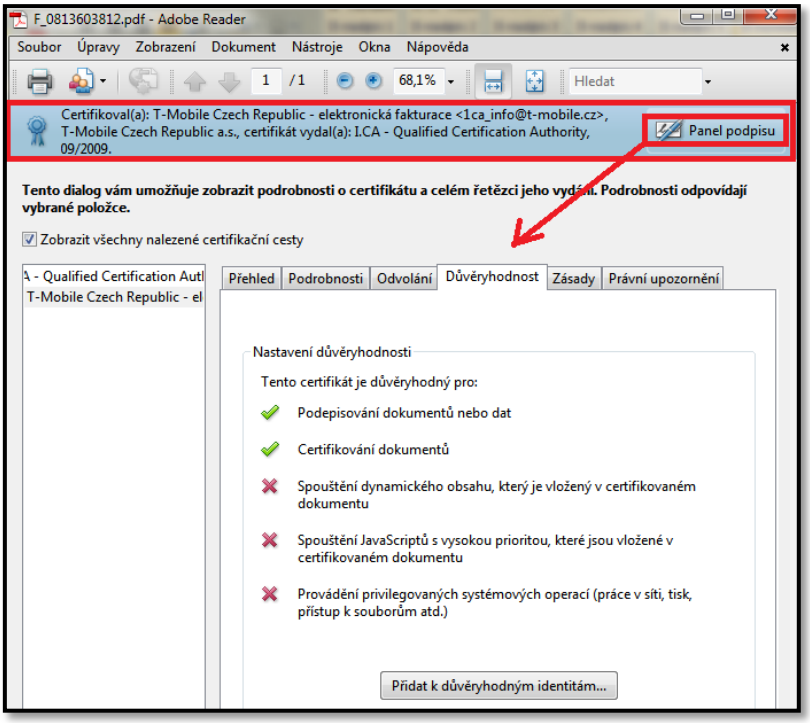
Než abychom složitě každý kořenový certifikát přidávali mezi důvěryhodné v úložišti aplikace Acrobat Reader, zvolíme jinou cestu a to "Integraci s úložištěm certifikátů Windows". V hlavním menu stiskneme příkaz **Úpravy** a vybereme možnost **Předvolby**. Následně vybereme položku **Zabezpečení** a v pravé části okna stiskneme možnost

Další předvolby. Otevře se nám nové okno s názvem "Další předvolby digitálních podpisů", kde třetí karta nese název "Integrace s Windows", a právě tato karta nás zajímá.



Obrázek 58, Integrace s úložištěm Windows

Zaškrtnutím položek **Ověřování podpisů** a následně **Ověřování certifikovaných dokumentů** bude pro ověření certifikátů prohledáváno centrální úložiště Windows. Když znovu otevřete podepsaný PDF dokument, prokázání identity autora podepsaného dokumentu bude již v pořádku. Pokud stisknete položku "Panel podpisu", můžete se podívat na další podrobnosti certifikátu, jako je například "Důvěryhodnost".



Obrázek 59, Korektní ověření podpisu Adobe Acrobat

5.3 ZABEZPEČENÁ PŘIPOJENÍ

5.3.1 PROKÁZÁNÍ VLASTNÍ IDENTITY PŘI KOMUNIKACI SE VZDÁLENÝM SERVEREM

Certifikáty se také dají využívat při ověření identity uživatele, který se přihlašuje k nějaké webové službě běžící na vzdáleném serveru. Základní princip při ověřování identity uživatele vůči vzdálenému serveru popíšeme v několika bodech:

1. Při komunikaci se serverem nejprve pošle server klientovi libovolná data, která klient zašifruje svým soukromým klíčem.
2. Tato data jsou spolu s klientským certifikátem odeslána zpět serveru.
3. Server pomocí veřejného klíče umístěného na klientském certifikátu přijatá data dešifruje.
4. Pokud se přijatá dešifrovaná data shodují s daty odeslanými v kroku č. 1, je ověření identity považováno za úspěšné.

V praxi je potřebné před prvním použitím ještě zaregistrovat Váš certifikát na konkrétním vzdáleném serveru. Do dané webové služby (například internetové bankovnictví) se většinou přihlašujete konkrétním uživatelským jménem a heslem. Při přihlašování do stejné služby pomocí certifikátu, ale nemusí být jméno vlastníka certifikátu shodné s uživatelským jménem, kterým se do služby přihlašujete. V tomto případě by nedošlo k provázání již konkrétního existujícího účtu s daným certifikátem. **Proto je nutné certifikát zaregistrovat, a to v době, kdy jste k dané službě přihlášeni pod Vaším uživatelským jménem a heslem**. Je nutné zmínit ještě jednu velice důležitou skutečnost - **pro přihlášení k webové službě pomocí certifikátu se nesmí používat kvalifikované certifikáty, ale pouze certifikáty komerční**. Důvod je ryze praktický. Budeme-li vycházet z teorie elektronického podpisu a šifrování, je jasné, že podle bodu 1 uvedeného na začátku této kapitoly šifruje klient svým soukromým klíčem náhodná data, která mu server posílá. Pokud by je šifroval soukromým klíčem umístěným na kvalifikovaném certifikátu, v podstatě by se podepisoval pod jejich platnost. Server by mohl uživateli poslat jakákoli zavádějící data, která by klient podepsal.

Přihlášení pomocí komerčního certifikátu si ukážeme na následujícím příkladu, kde se budeme přihlašovat ke službě "mojeID".

5.3.1.1 PŘIHLÁŠENÍ KE SLUŽBĚ MOJEID

Pomocí služby mojeID se můžete pohodlně přihlašovat k různým webovým službám. Výhodou je, že si nemusíte pro každou webovou službu pamatovat různé přihlašovací údaje a hesla. Služba mojeID je v podstatě důvěryhodný prostředník, který při přístupu k různým webovým službám prokáže Vaši identitu. Pomocí služby "mojeID" se můžete přihlašovat například k serverům:

- Volný, Seznam, Lupa, Živě, Tiscali, Titulky a mnoho dalším.

Ke službě "mojeID" se můžete přihlašovat také pomocí certifikátu. Z toho vyplývá, že certifikát můžete používat také pro přihlašování k výše uvedeným serverům. Tento fakt vychází ze skutečnosti, že Vaši identitu ověřujete pouze proti službě "mojeID" a ta, pokud identifikace proběhla v pořádku, potvrdí přihlášení cílovému serveru. Právě přihlášení pomocí certifikátu si zanedlouho ukážeme. Nejprve je ale nutné vytvořit si na serveru "mojeID" nový účet a následně v něm zaregistrovat Váš certifikát. Samotný postup registrace v této práci nebudeme detailně popisovat, jen zmiňme, že registrace není anonymní a služba "mojeID" pracuje s ověřenými údaji. Pro plnou funkčnost Vašeho konta je potřeba v rámci registračního formuláře vyplnit jedinečné kódy, které jsou zaslány na:

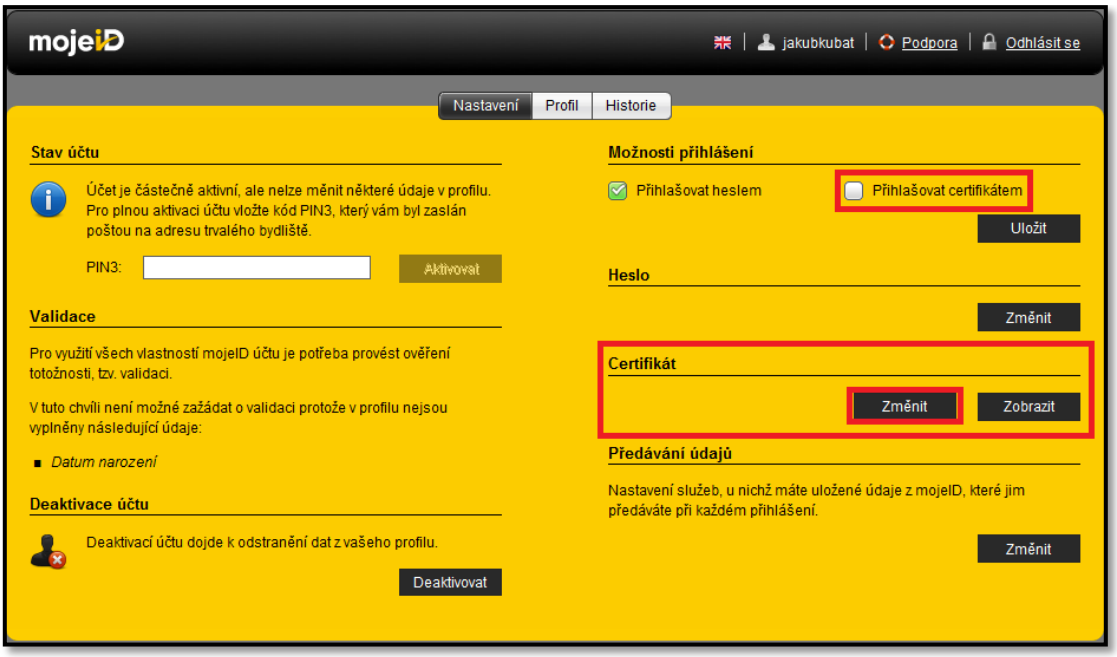
- Uvedenou emailovou adresu.
- Uvedené telefonní číslo.
- Uvedenou adresu a to formou dopisu.

Až po zapsání **všech** těchto jedinečných kódů do registračního formuláře je Váš účet plně aktivní[18].

Registrace certifikátu

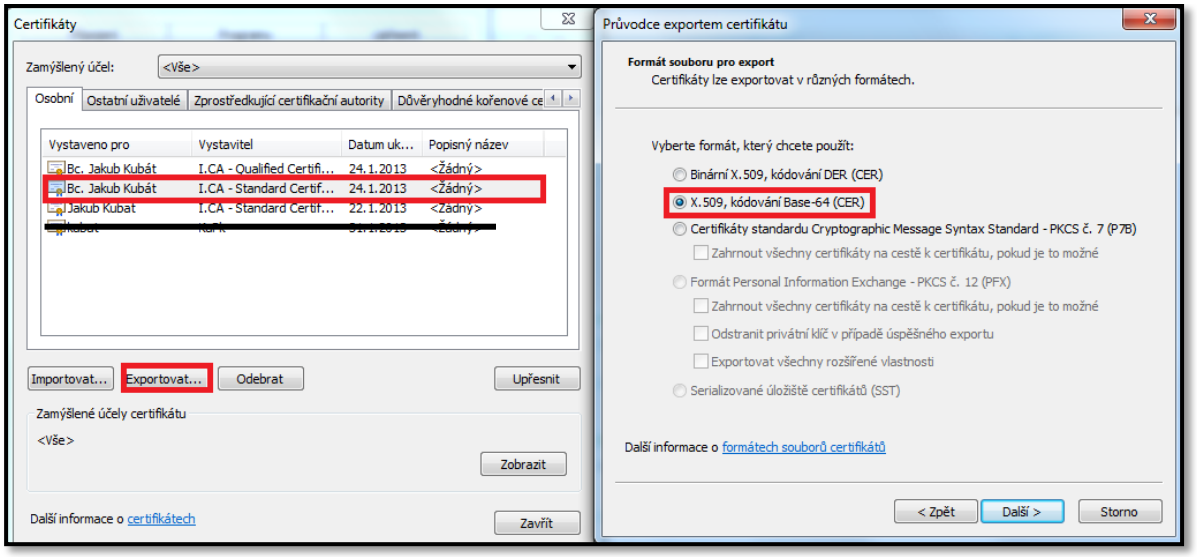
Budeme předpokládat, že jste si již založili účet a nyní chcete registrovat Váš uživatelský certifikát. Po přihlášení uživatelským jménem a heslem do služby "mojeID" na stránkách http://www.mojeid.cz, zvolíme sekci **Nastavení** a v části **Certifikát** stiskneme tlačítko **Změnit**, následně uživatelský certifikát zaregistrujeme. Nesmíme také zapomenout zaškrtnout možnost **přihlašovat certifikátem**. Podívejte se na obrázek č. 60.

[18] Pro částečné zprovoznění Vašeho účtu stačí v rámci prvotní registrace vyplnit pouze kódy zaslané na mobilní telefon a email.



Obrázek 60, Registrace certifikátu mojeID

Jen připomeňme, že pro ověření identity je potřeba používat **komerční certifikát**. Při registraci certifikátu je nutné mít certifikát exportovaný ve formátu "PEM". Jedná se o formát standardu "X.509" s kódováním "Base-64". Tyto certifikáty mají nejčastěji příponu "cer". Export ze systémového úložiště Windows do tohoto formátu můžete vidět na následujícím obrázku.

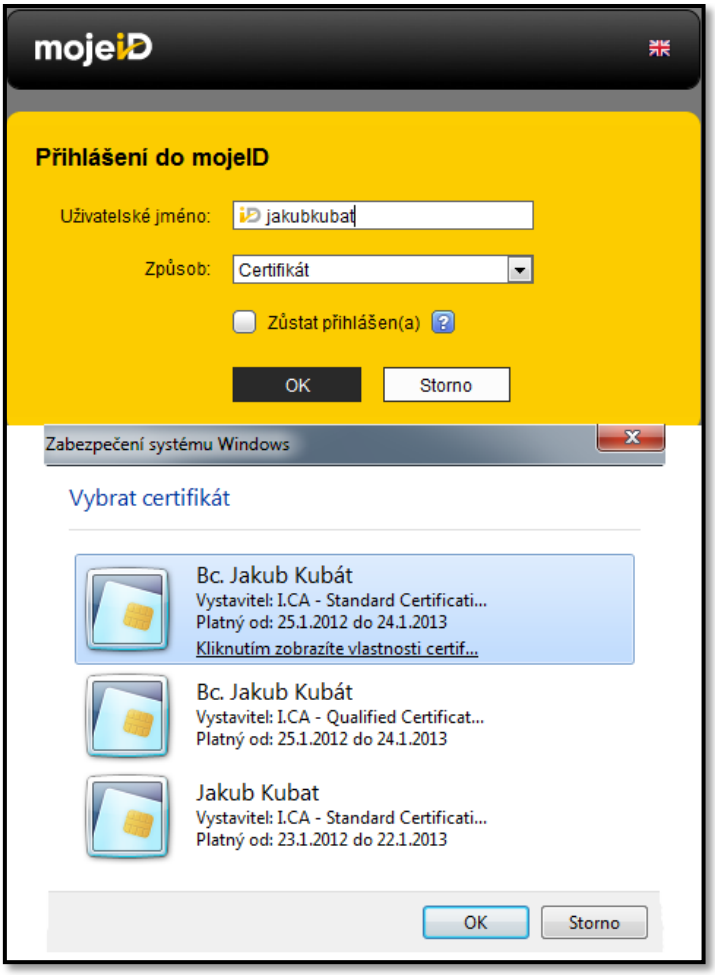


Obrázek 61, Export certifikátu ve formátu PEM

Přihlášení pomocí certifikátu

Přihlášení k webovým stránkám služby "mojeID" pomocí certifikátu je velice jednoduché. V přihlašovacím okně stačí zadat Vaše uživatelské jméno a jako způsob

přihlašování vybrat možnost "Certifikát". Následně se Vám zobrazí seznam osobních certifikátů, ze kterých je potřeba vybrat ten správný (výše registrovaný na webových stránkách www.mojeid.cz).



Obrázek 62, Přihlášení k serveru mojeID

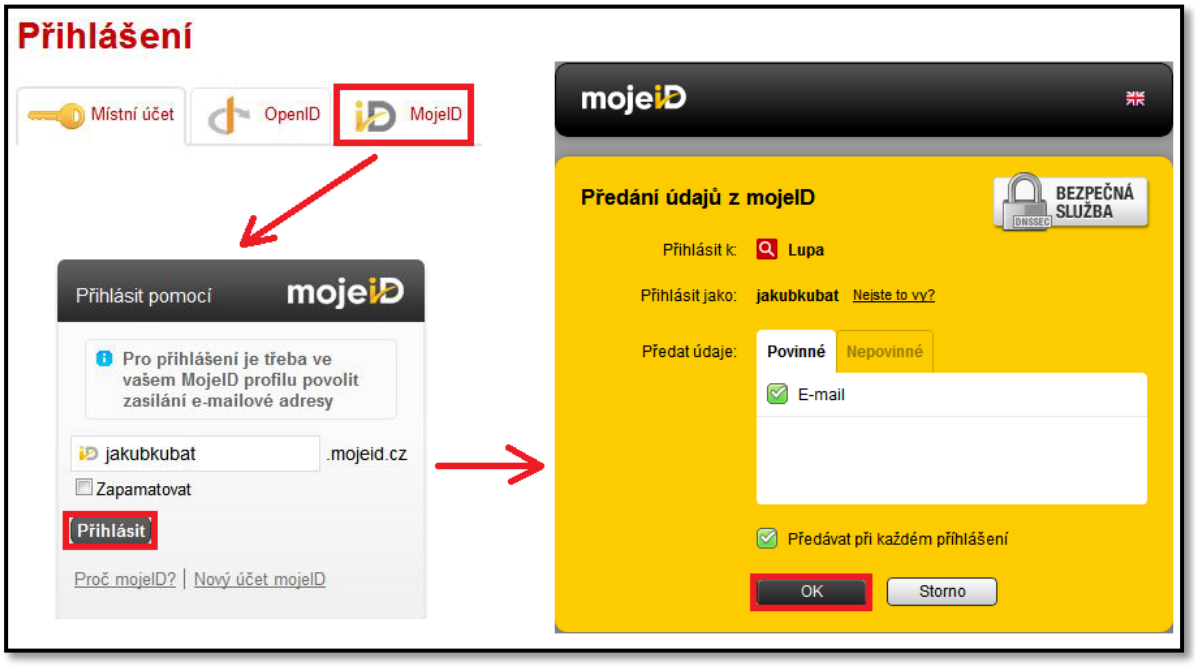
5.3.1.2 PŘÍSTUP K OSTATNÍM SERVERŮM, KTERÉ PODPORUJÍ PŘIHLÁŠENÍ PŘES "MOJEID"

Obdobným způsobem můžete přistupovat i k dalším serverům, které podporují přihlášení přes službu "mojeID". Přístup ke konkrétnímu serveru se nepatrně liší v závislosti na tom, zda již máte na tomto serveru založen účet.

Mám založen místní účet.

Ke konkrétnímu účtu (například k serveru "Lupa") se přihlásíte přes službu "mojeID" a vyberete Váš certifikát. V tuto chvíli dojde k předání několika Vašich údajů ze serveru "mojeID" cílovému serveru, ke kterému se hlásíte. Předání údajů je potřebné k tomu, aby Vás cílový server automaticky přihlásil. Po přihlášení certifikátem po Vás budou požadovány přihlašovací údaje k Vašemu místnímu účtu. V tomto kroku dojde ke spárování účtu

"mojeID" s Vaším místním účtem. Při dalších přihlášeních se již stačí přihlašovat pouze přes "mojeID" a přihlášení k cílovému serveru se provede automaticky. Postup přihlášení k serveru "Lupa" ukazuje následující obrázek. Nacházíme se na stránkách http://www.lupa.cz/.

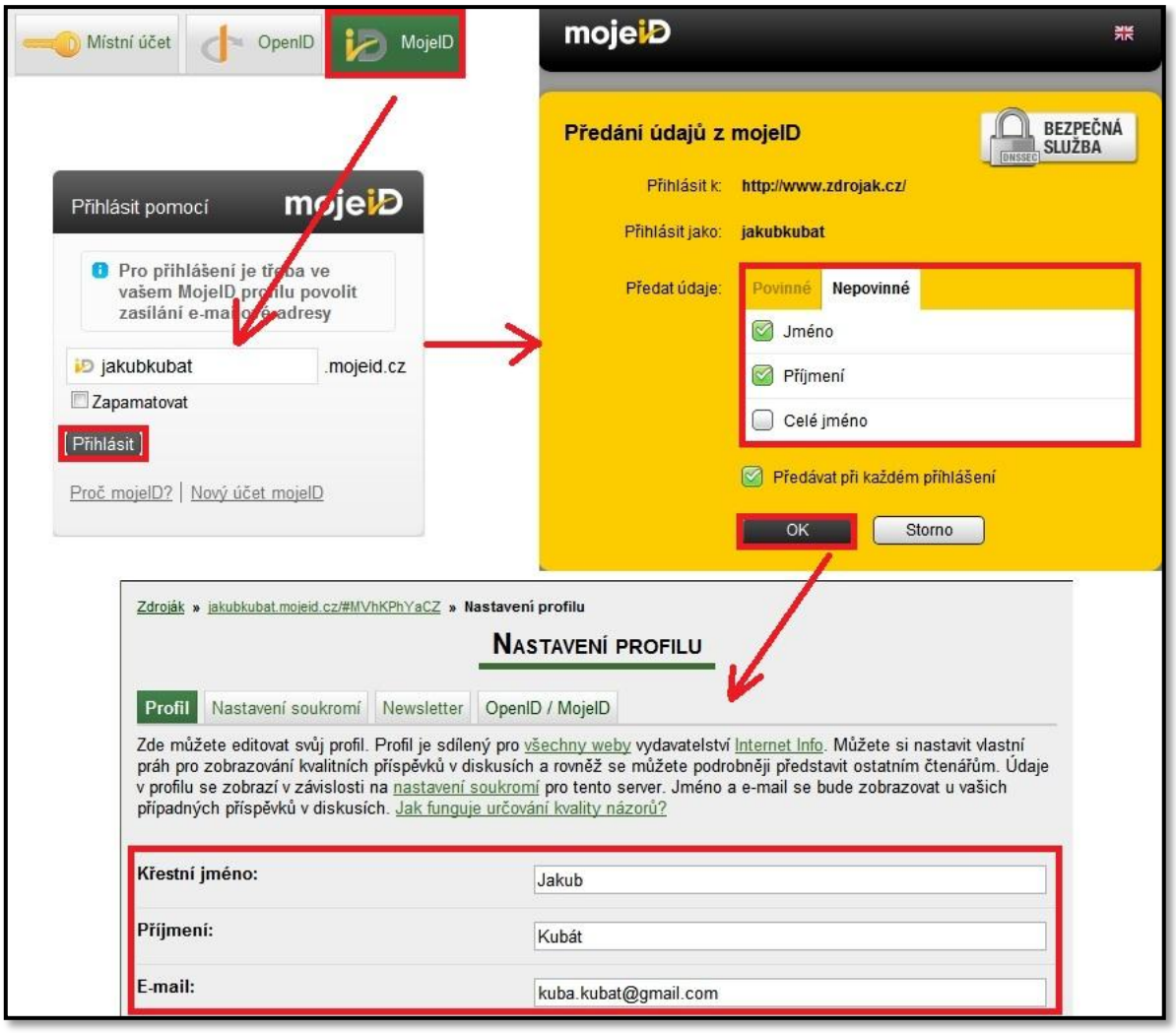


Obrázek 63, Přihlášení k serveru Lupa

Předání údajů můžete samozřejmě modifikovat. Důležité je především předání povinných údajů. V záložce nepovinné údaje můžete některé z údajů odškrtnout.

Nemám založen místní účet.

Postup je v počáteční fázi obdobný, jako kdybyste místní účet založený měli. U konkrétního serveru (v našem případě server "Zdrojak") vyberete možnost přihlásit se přes službu "mojeID". Proběhne celý proces včetně předání Vašich údajů. Jelikož bude ve většině případů (u většiny serverů) vytvořen automaticky nový místní účet, můžete při předání údajů vybrat i některé nepovinné údaje, které budou automaticky do tohoto místního účtu přeneseny. Poté můžete provést editaci Vašeho místního účtu a doplnit další údaje. Pro lepší představu se můžete podívat na následující obrázek.



Obrázek 64, Přihlášení k serveru Zdrojak

5.3.2 PROKÁZÁNÍ IDENTITY VZDÁLENÉHO SERVERU A ŠIFROVANÁ KOMUNIKACE POMOCÍ SSL/TLS

5.3.2.1 PRINCIP FUNKCE

V dnešní době, kdy často vyplňujete Vaše osobní údaje a hesla do formulářů na různých internetových stránkách, je potřeba zaručit pravost těchto stránek a také bezpečnost přenášených údajů. To obojí můžeme zajistit použitím protokolu **SSL,** popřípadě jeho následovníkem **TLS.** Protokoly SSL a TLS jsou umístěny v rámci modelu ISO/OSI mezi transportní a aplikační vrstvu síťového modelu TCP/IP. V praxi se jedná o komunikaci mezi klientem a serverem, kdy je před vyplněním důležitých údajů navázána zabezpečená komunikace, kterou můžeme také označit jako **SSL/TLS komunikaci**. Mezi nejnovější verzí protokolu SSL 3.0 a zatím nejpoužívanější verzí protokolu TLS 1.0 jsou jen minimální funkční rozdíly, proto budeme v této práci zabezpečenou komunikaci pro zjednodušení označovat pouze jako "SSL komunikaci". SSL komunikace se dá využívat v různých aplikačních

protokolech (například FTP), my se však v této práci budeme zabývat SSL komunikací probíhající v internetovém prostředí (protokol https).

Pomocí SSL komunikace můžeme zajistit:

- **Autentizaci[19] serveru vůči klientovi**. Jinak řečeno "jistotu", že klient doopravdy komunikuje se serverem, se kterým si myslí, že komunikuje.
- **Šifrovaní komunikace mezi serverem a klientem**. "Jistotu", že přenášená data, nebudou zneužita, jelikož budou pro útočníka nečitelná.
- *Autentizaci klienta vůči serveru. Server má "jistotu", že komunikuje s tím klientem, se kterým si myslí, že komunikuje.*

Nejčastěji jsou však pomocí SSL komunikace zajišťovány pouze první dva body a to **autentizace serveru vůči klientovi** a **šifrovaná komunikace.** Klient vůči serveru se většinou autentizuje jiným způsobem než přímo pomocí SSL komunikace - například svým klientským certifikátem nebo uživatelským jménem a heslem při přístupu ke konkrétní internetové službě. Tento postup jsme si popisovali v předchozí části práce. **Je ovšem poměrně důležité, aby autentizace klienta vůči serveru proběhla až po úspěšném navázání bezpečné SSL komunikace, aby nemohlo dojít k potenciálnímu odposlechnutí uživatelského jména a hesla.**

Popišme si nyní v několika bodech, jakým způsobem vlastně vzniká zabezpečená SSL komunikace (v angličtině označováno jako "SSL handshake").

1. Klient pošle serveru požadavek na SSL spojení, spolu s požadavkem posílá doplňující informace, například jaké šifrování bude při komunikaci použito.
2. Server pošle klientovi odpověď, jejíž součástí je serverový certifikát. Klient si ověří platnost serverového certifikátu. Součástí tohoto certifikátu je také veřejný klíč.
3. Na základě dosud známých informací vygeneruje klient základ symetrického šifrovacího klíče, kterým bude šifrována následná komunikace. Tento klíč zašifruje veřejným klíčem serveru a odešle mu ho.

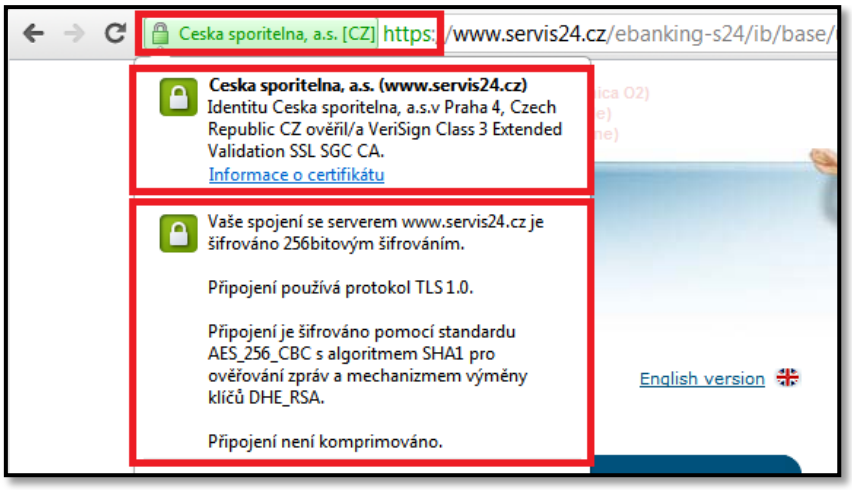
[19] **Autentizace** je proces ověření identity subjektu (uživatele, serveru)

4. Server obdrží tajnou informaci od klienta (zašifrovaný základ klíče). Informaci dešifruje svým soukromým klíčem. Nyní má k dispozici základ symetrického klíče, kterým bude šifrována následná komunikace.
5. Ze základu symetrického klíče, který mají k dispozici jak klient, tak server, je vygenerován hlavní symetrický šifrovací klíč.
6. Klient a server si vzájemně potvrdí, že následná komunikace bude probíhat šifrovaně. Pro šifrování a dešifrování je použit hlavní symetrický šifrovací klíč, který je shodný pro obě dvě strany.

Pro zabezpečenou komunikaci pomocí SSL bývají použity nejrůznější kryptografické mechanismy. V dnešní době bývají často používány například tyto:

- Pro generování asymetrických klíčů (prokázání identit serveru vůči klientovi): **RSA, Diffie-Helmann, DSA**.
- Pro generování symetrického klíče (šifrovaná komunikace mezi klientem a serverem): **DES, 3DES, RC4, AES.**

V předchozích řádcích jsme si řekli něco z teorie zabezpečené komunikace pomocí protokolu SSL, popřípadě TLS. Jak ale jednoduše v internetovém prohlížeči poznat, že je tato zabezpečená komunikace navázána? Je to jednoduché. Internetový prohlížeč musí obsahovat v adrese internetové stránky (URL) protokol "**https**", nikoli "http". Právě protokol HTTPS umožňuje používat zabezpečenou komunikaci pomocí protokolů SSL, případně TLS. Jednotlivé internetové prohlížeče pak poskytují ještě další doplňkové informace o zabezpečeném připojení. V prohlížeči Google Chrome je při zabezpečeném připojení zobrazen u hlavičky URL adresy zámek. Pokud na zámek kliknete levým tlačítkem myši, zobrazí se Vám doplňkové informace o používaných certifikátech a kryptografických algoritmech. Pro lepší představu se můžete podívat na obrázek č. 65.



Obrázek 65, Zabezpečený SSL přístup na stránkách České spořitelny

5.3.2.2 BEZPEČNOSTNÍ RIZIKA A JEJICH ŘEŠENÍ

Při popisu poměrně zásadního bezpečnostního rizika spojeného s implementací protokolů TLS a SSL budeme vycházet ze článku *Petra Krčmáře uvedeného na serveru "Root.cz".*

Dvojice bezpečnostních analytiků Thai Duong a Julian Rizzo předvedla útok na protokoly TLS a SSL. Úspěšný útok, který vedl k odposlechu a prolomení šifrované komunikace, tak upozornil na zranitelnost některých (v dnešní době nejvíce používaných) implementací protokolů TLS a SSL.

Útok nazvaný "BEAST" (Browser Exploit Against SSL/TLS) lze použít na dnes nejvíce používané verze protokolů SSL a TLS, konkrétně pak verze TLS 1.0, SSL 3.0. Výjimku tvoří ta verze protokolů TLS 1.0 a SSL 3.0, kde je pro šifrování dat použita symetrická proudová šifra RC4 namísto symetrické blokové šifry AES. Novější verze TLS 1.1 a 1.2 jsou proti útoku odolné v každém případě. Řešení tohoto problému by se tedy mohlo zdát poměrně jednoduché - používat novější verzi těchto protokolů. Zásadní problém ovšem tkví v tom, že poměrně značná část internetových prohlížečů tyto novější verze protokolů nepodporuje. Problém může být také na straně serveru, ani ten nemusí novější verze protokolů podporovat. Útok, který představila dvojice bezpečnostních analytiků, spočívá v instalaci jednoduchého Javascriptu[20], který si uživatel nevědomě stáhne do svého počítače. Javascript může být součástí obsahu navštívené stránky. Tento jednoduchý program upraví způsob šifrování **symetrické blokové šifry AES**, pomocí které jsou šifrovány jednotlivé komunikační

[20] **Javascript** je počítačový program vytvořený stejnojmenným objektově orientovaným programovacím jazykem.

bloky a donutí šifrovací mechanismus, aby používal slabé šifrovací klíče (lehce odvoditelné). Útočník může tudíž komunikaci lépe prolomit. Útěchou snad může být fakt, že k prolomení nedojde v reálném čase. Při dnešních početních výkonech trvá dešifrování informace o velikosti 1 byte přibližně 2 sekundy. Celé sezení by tedy mohlo být prolomeno cca. za 10 minut. Otázkou je, za jak dlouho budou moci potenciální útočníci prolomit spojení v reálném čase při vzrůstajících početních výkonech.

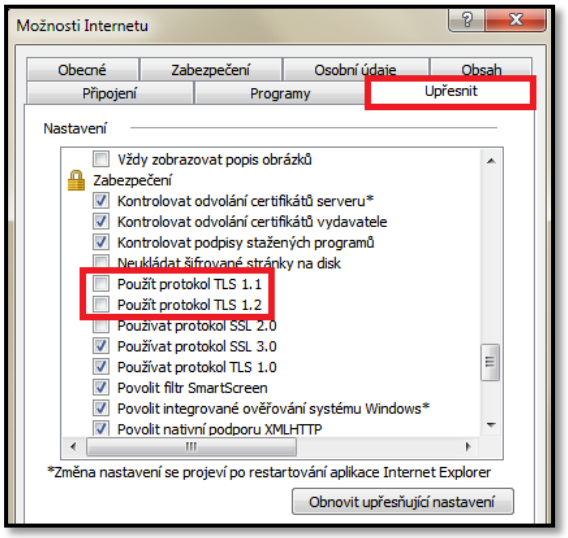
Jak se ale možnému napadení zcela vyhnout, je poměrně složité. Pokud bychom se zaměřili na různé Internetové prohlížeče je potřeba říct, že některé z nich novější verzi protokolu podporují, ale implicitně protokol povolený nemají. Jedná se například o prohlížeč Internet Explorer a Opera. Popišme si, jak v těchto prohlížečích protokol TLS 1.2 povolit.

Internet Explorer

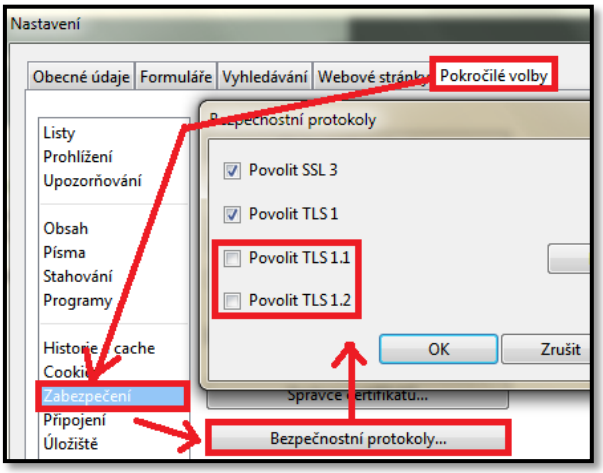
Stiskneme příkaz **Nástroje** a vybereme položku **Možnosti Internetu**. Vybereme kartu **Upřesnit**. Ve spodní části se nachází sekce **zabezpečení**, kde lze nastavit, jaké protokoly mohou být pro zabezpečenou komunikaci použity. Najdeme zde i protokol TLS 1.2.

Opera

Stiskneme tlačítko **Opera** a vybereme možnost **Nastavení**. V kartě **Pokročilé volby** vybereme sekci **Zabezpečení** a stiskneme tlačítko **Bezpečnostní protokoly.**

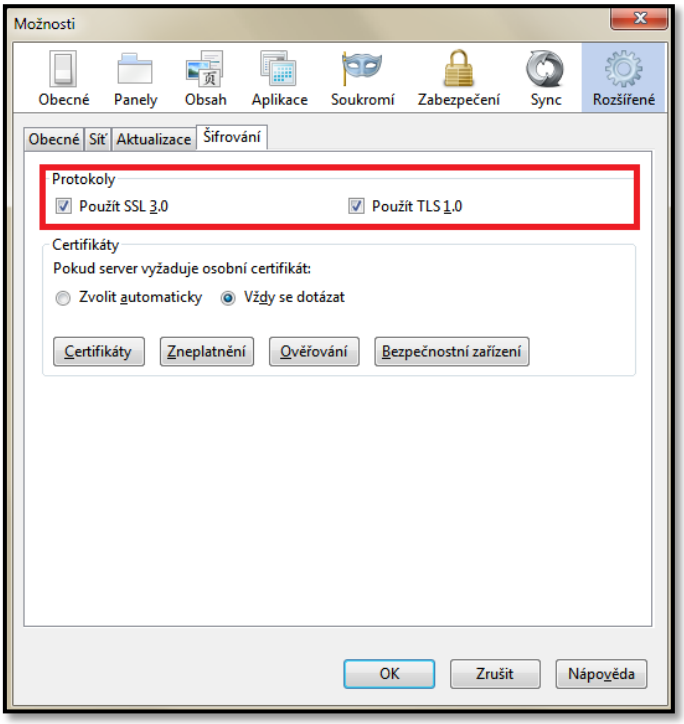


Obrázek 66, TLS a SSL protokoly v aplikaci Internet Explorer



Obrázek 67, TLS a SSL protokoly v aplikaci Opera

Existují také prohlížeče, jako je například Mozzila Firefox, které novější verze protokolů TLS nepodporují vůbec. V prohlížeči Mozzila Firefox máme na výběr pouze používání protokolů SSL 3.0 a TLS 1.0. Nastavení protokolů TLS a SSL najdeme pod tlačítkem **Firefox**, kde vybereme položku **Možnosti**. V otevřeném okně pak vybereme sekci **Rozšířené** a kartu **Šifrování**.



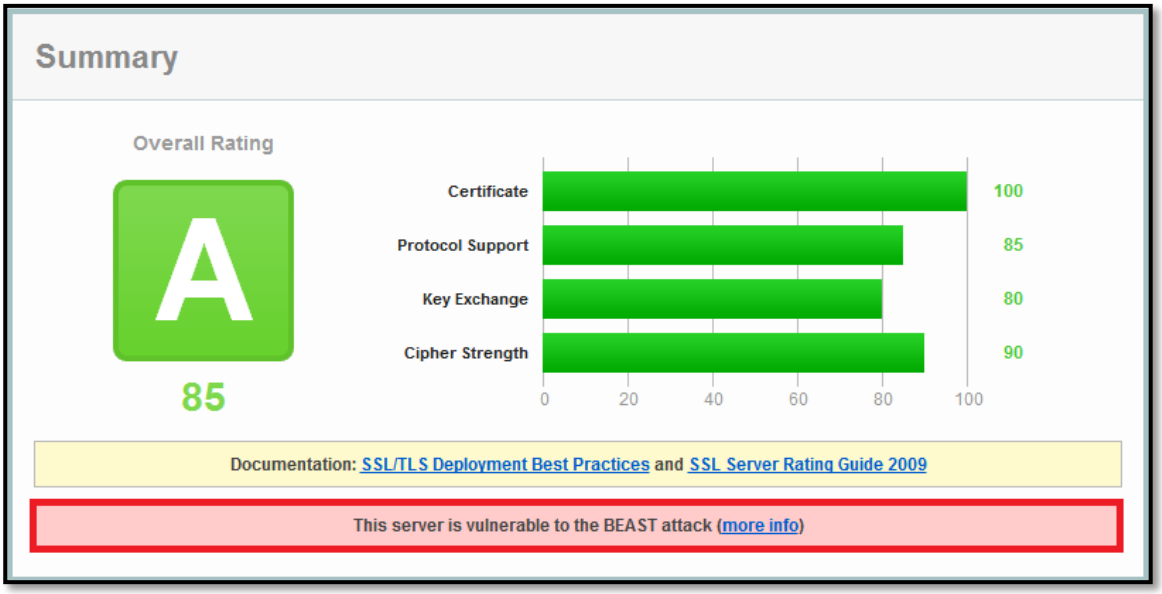
Obrázek 68, TLS a SSL protokoly v aplikaci Mozzila Firefox

Řekněme, že zvolíte ten internetový prohlížeč, který podporuje nové verze protokolů TLS, a povolíte je. V tomto okamžiku nemusíte mít ale ještě zdaleka vyhráno. Důležité totiž je, aby nové protokoly podporoval i server, na který se přihlašujete. To je ovšem v dnešní době poměrně značný problém. Celá řada serverů, ke kterým se přihlašujete a zadáváte zde citlivé údaje (například servery internetového bankovnictví, či servery ZČU), podporují pouze starší verze protokolů TLS/SSL. Relativně dobrou zprávou může být skutečnost, že i přes to, že nejsou na straně některých serverů podporovány nové verze protokolů TLS, může být komunikace vůči útoku "BEAST" odolná. Východiskem je totiž již výše zmiňované použití proudové šifry RC4 pro šifrování dat. Bohužel, alespoň v polovině případů je jako součást protokolu TLS, či SSL použita šifra AES, která vůči útoku BEAST odolná není. Pokud byste chtěli zkontrolovat, zda je server, na který se hlásíte, rezistentní vůči výše popisovanému útoku "BEAST", můžete to ověřit na stránkách společnosti "SSL Labs" (https://www.ssllabs.com/). Test, který najdete ve spodní části stránky, zjišťuje, jaké

kryptografické mechanismy včetně protokolů TLS/SSL jsou použity na vybraném internetovém serveru a zda jsou odolné vůči potencionálnímu útoku BEAST.

Obrázek 69, Test SSL

Nyní si pojďme ukázat výsledky testu internetového bankovnictví České spořitelny (https://www.servis24.cz). Test spustíte kliknutím na tlačítko "Submit", které je vidět na předchozím obrázku.



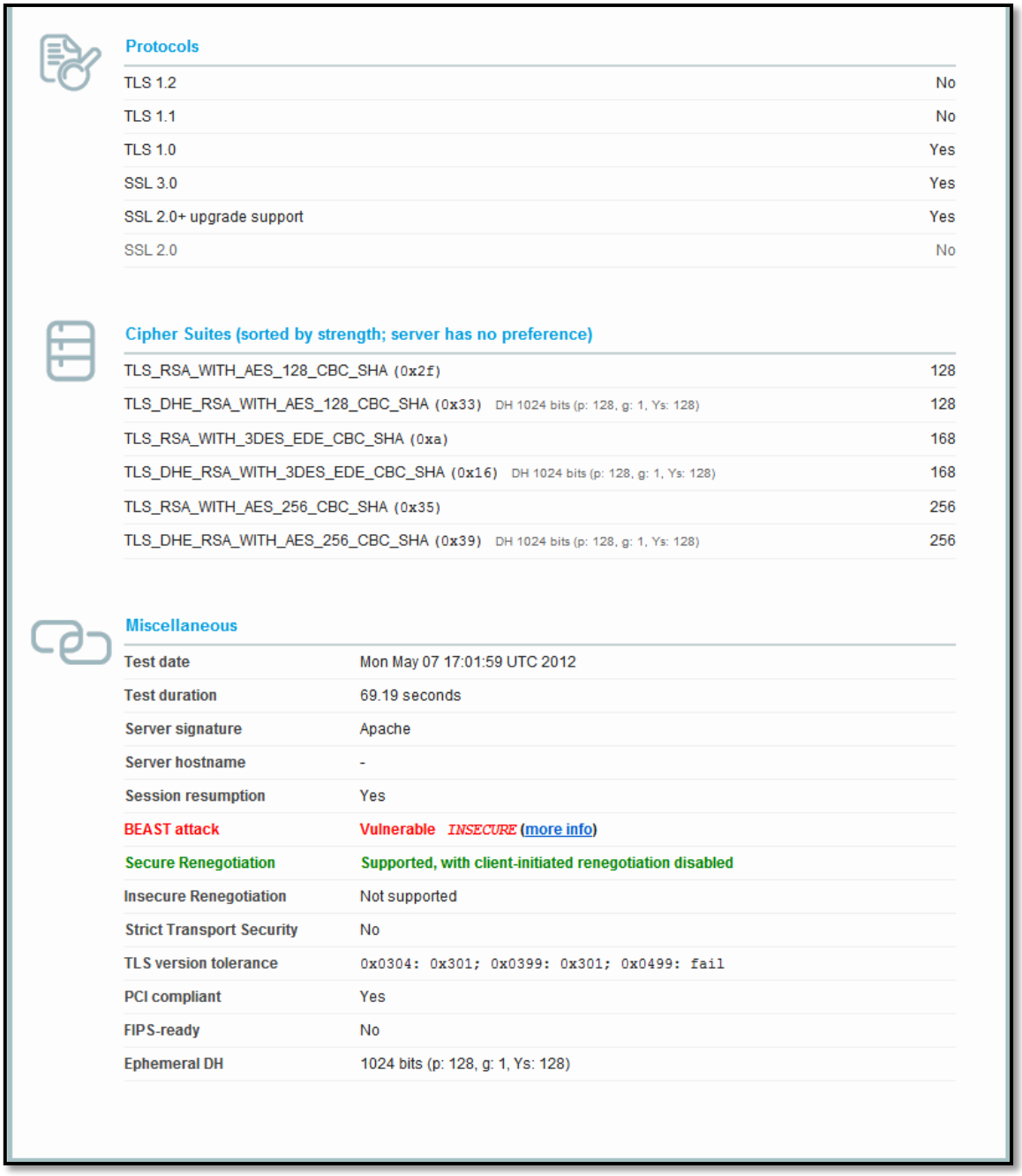
Obrázek 70, Výsledky SSL testu webového serveru, část 1

Ze základních výsledků je vidět bodové ohodnocení jednotlivých kategorií, kdy 100 bodů je maximální možný dosažený počet:

- Certificate - Důvěryhodnost použitých serverových certifikátů.
- Protocol Support - Podporované verze protokolů TLS a SSL.
- Key Exchange - Bezpečnostní úroveň (síla) použitých asymetrických kryptografických metod pro výměnu klíčů.

- Cipher Strenght - Délka symetrických a asymetrických klíčů použitých pro celkový zabezpečený přenos informací.

Pokud se podíváme na spodní část obrázku, je vidět, že tento server může být ohrožen útokem "BEAST". Útok je možné provést, jelikož server nepodporuje novější verze protokolů TLS.



Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3.0	Yes
SSL 2.0+ upgrade support	Yes
SSL 2.0	No

Cipher Suites (sorted by strength; server has no preference)

TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys: 128)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	168
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits (p: 128, g: 1, Ys: 128)	168
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits (p: 128, g: 1, Ys: 128)	256

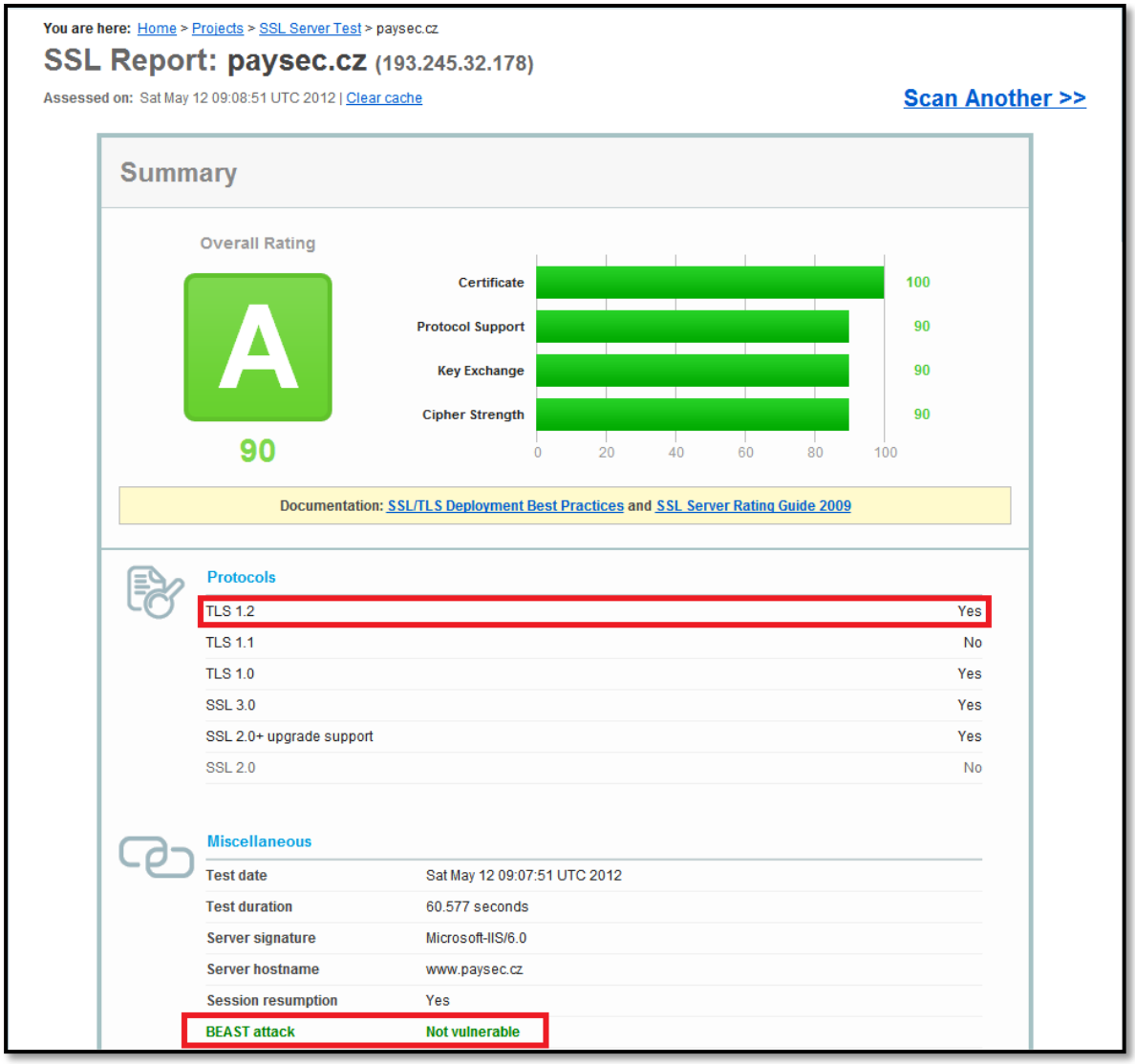
Miscellaneous

Test date	Mon May 07 17:01:59 UTC 2012
Test duration	69.19 seconds
Server signature	Apache
Server hostname	-
Session resumption	Yes
BEAST attack	Vulnerable *INSECURE* (more info)
Secure Renegotiation	Supported, with client-initiated renegotiation disabled
Insecure Renegotiation	Not supported
Strict Transport Security	No
TLS version tolerance	0x0304: 0x301; 0x0399: 0x301; 0x0499: fail
PCI compliant	Yes
FIPS-ready	No
Ephemeral DH	1024 bits (p: 128, g: 1, Ys: 128)

Obrázek 71, Výsledky SSL testu webového serveru, část 2

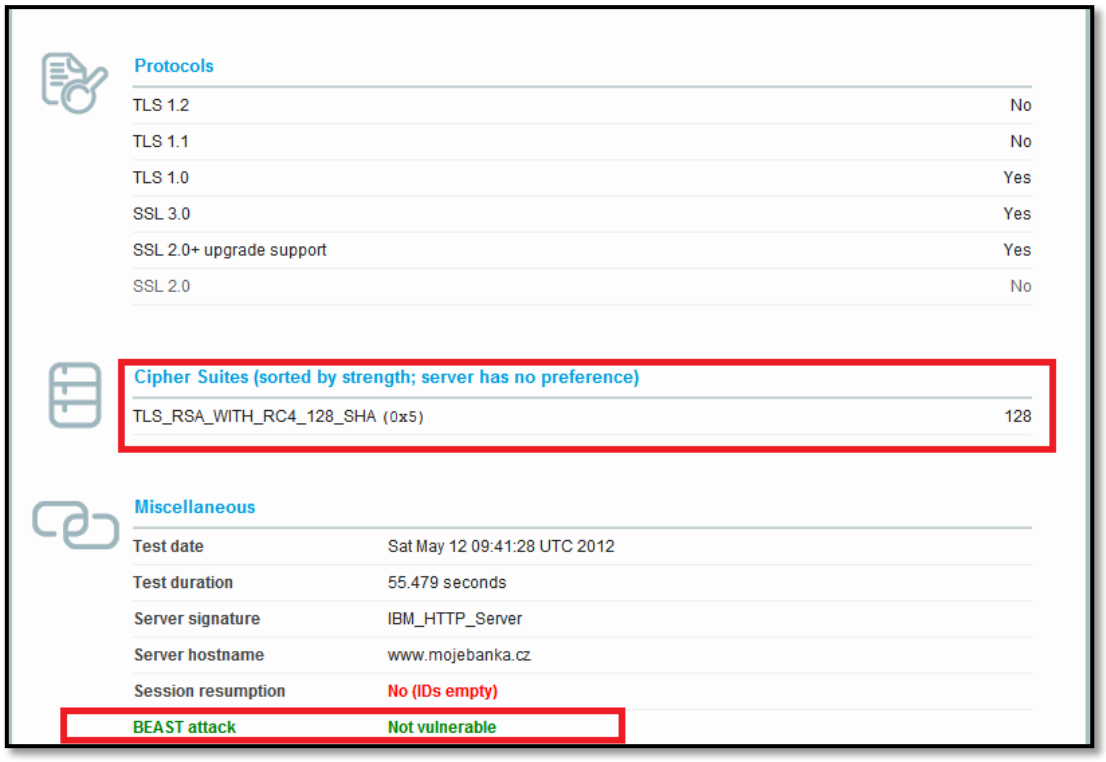
Obdobným způsobem je možné otestovat jakýkoli jiný webový server. Abychom dokázali, že v dnešní době existují i servery, které podporují novější verze protokolů TLS,

vybrali jsme si server "PaySec" (https://www.paysec.cz) patřící Československé obchodní bance. Obdobných výsledků dosáhly také například stránky internetového bankovnictví Československé obchodní banky.



Obrázek 72, Výsledky SSL testu serveru Paysec

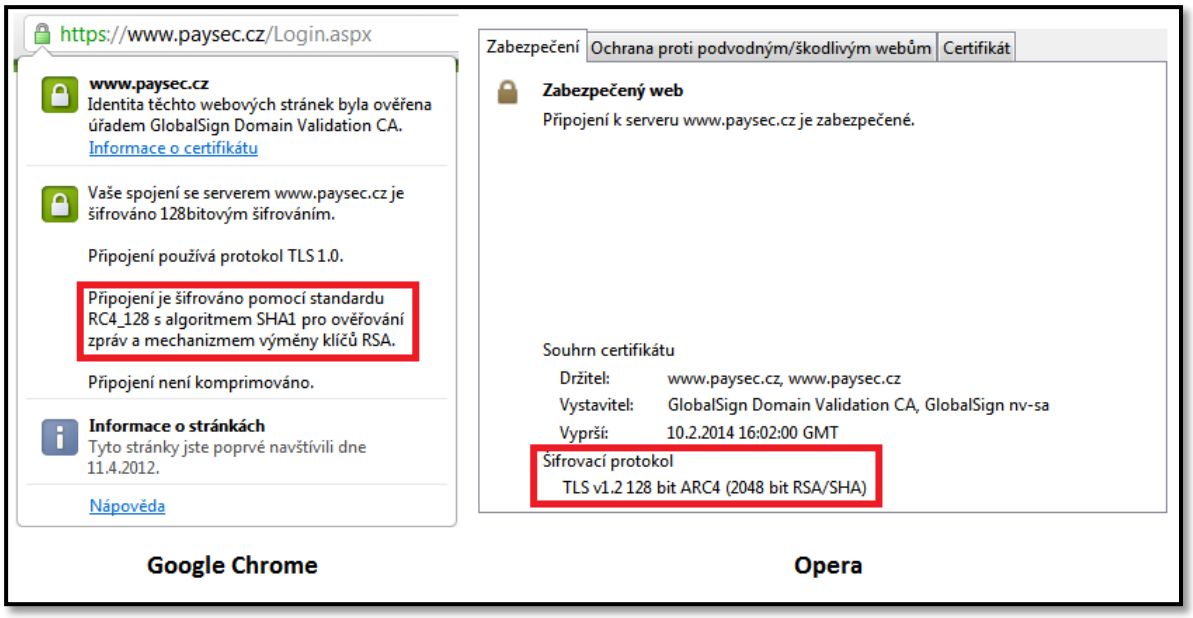
Poslední obrázek v této podkapitole je věnován SSL testu webového serveru, kde jsou použity starší verze protokolů TLS a SSL. Pro šifrování dat je ale použita proudová šifra RC4, tudíž potencionální útok BEAST zde nehrozí.



Obrázek 73, Výsledky SSL testu při použití proudové šifry RC4

Shrňme si tedy zásady, kterých se držet, chceme-li se možnému útoku BEAST vyhnout:

- Při přístupu k webovému serveru kontrolovat použití protokolu https.
- Pokud to Váš prohlížeč podporuje, povolte v něm novější verze protokolů TLS. Pokud Váš prohlížeč nové verze protokolů nepodporuje, stáhněte si ten, který ano (například Internet Explorer, Opera).
- Po povolení TLS protokolů ve Vašem prohlížeči můžete otestovat i server, na který přistupujete. Test můžete provést na stránkách: https://www.ssllabs.com. Protokoly TLS / SSL použité cílovým serverem bohužel ovlivnit nemůžete. Alespoň ale zjistíte, zda by mohlo k potencionálnímu útoku BEAST dojít.
- Při navázané zabezpečené komunikaci zkontrolovat detailní údaje o spojení. Až po ověření, že je spojení bezpečné, vyplnit přihlašovací údaje. Následující obrázek ukazuje příklad bezpečného připojení mezi prohlížeči Google Chrome, Opera a serverem Paysec. V případě prohlížeče Google Chrome sice není použit protokol TLS 1.2, ale pro šifrování dat je použita 128 bitová proudová šifra RC4, která je vůči potencionálnímu útoku BEAST rezistentní.



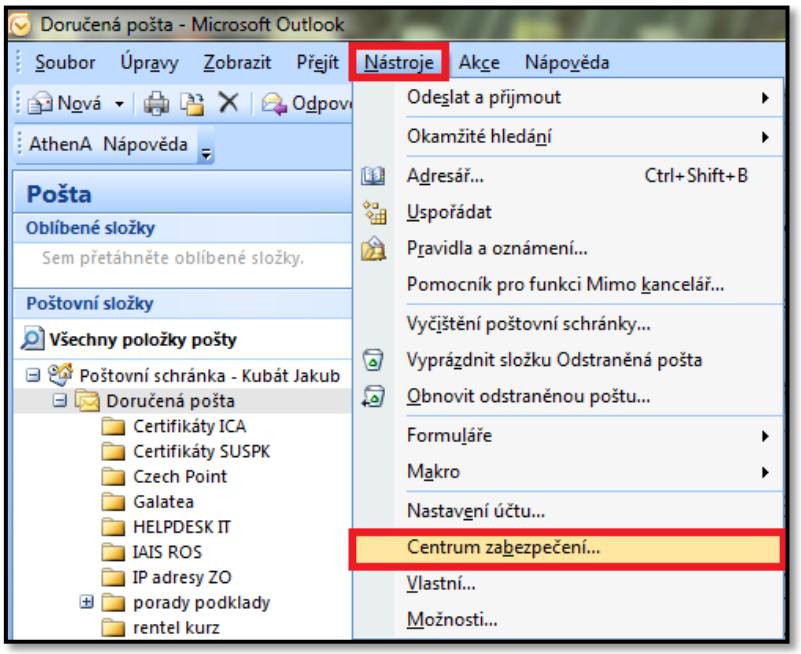
Obrázek 74, Připojení rezistentní vůči útoku BEAST

6 POUŽITÍ ELEKTRONICKÉHO PODPISU V APLIKACI MS OUTLOOK 2007

V předchozí poměrně rozsáhlé kapitole jsme si popsali principy týkající se vydávání certifikátů, ověřování identit subjektů, šifrovaných připojení, ale neukázali jsme si, jak a kde konkrétně elektronický podpis použít. Použití elektronického podpisu není vázáno jen vydáním certifikátu a jeho následným importem do operačního systému, i když to je samozřejmě nutnou podmínkou. Nutné je totiž použít program, který technologii elektronického podpisu podporuje a umí ji využít. Ve své práci jsem pro demonstraci použití elektronického podpisu vybral poštovního klienta společnosti Microsoft, Outlook 2007. Obdobným způsobem lze pracovat s elektronickým podpisem i ve starších verzích aplikace Outlook (2000, XP, 2003).

6.1 VÝBĚR CERTIFIKÁTU PRO ELEKTRONICKÝ PODPIS

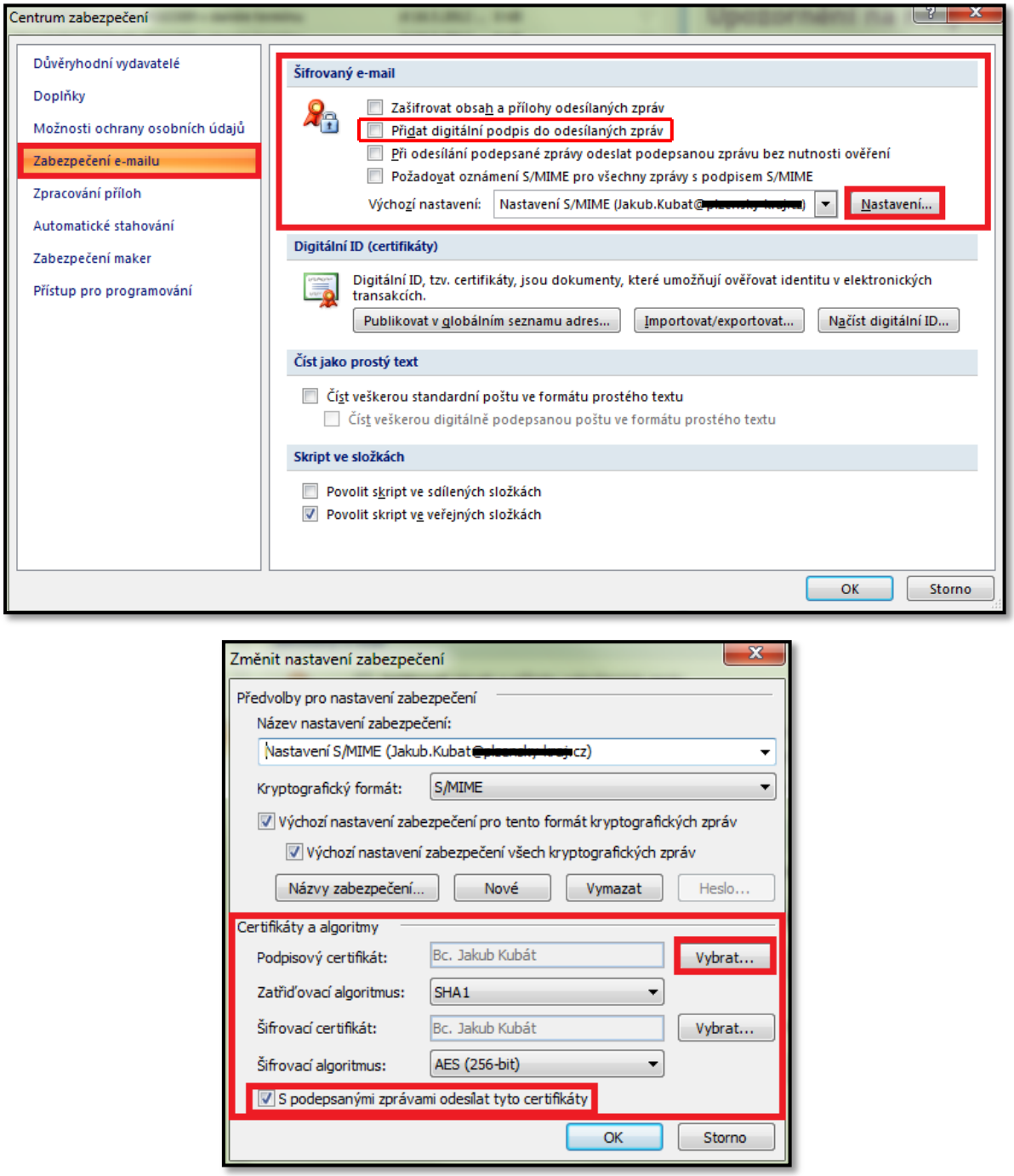
Nyní se pojďme podívat, kde konkrétně vybrat v aplikaci MS Outlook 2007 kvalifikovaný certifikát, abychom byli schopni přidávat ke zprávám elektronický podpis. V základní nabídce stiskneme příkaz **Nástroje** a vybereme položku **Centrum zabezpečení**. Pro lepší představu se můžete podívat na následující obrázek.



Obrázek 75, MS Outlook 2007, výběr certifikátu 1

Otevře se nám nové okno **Centra zabezpečení**, kde v levé části vybereme položku **Zabezpečení emailu**. Celá horní část pravého okna se týká elektronického podepisování

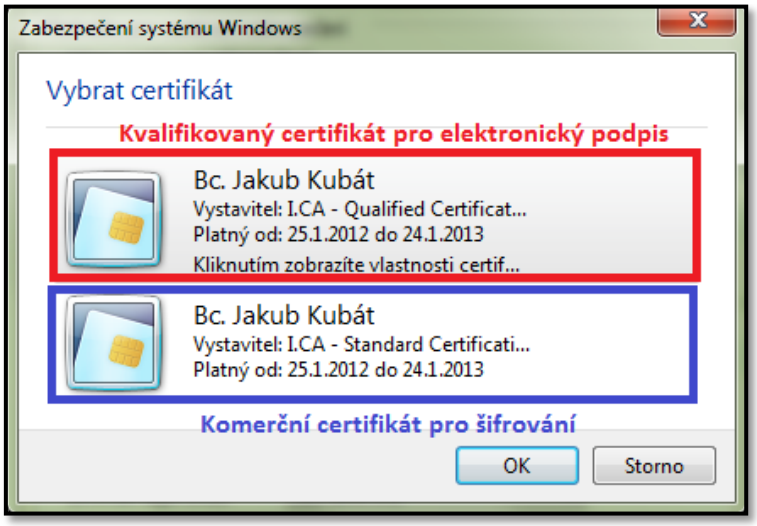
a nastavení certifikátu pro elektronický podpis. V sekci **Šifrovaný e-mail** stiskneme položku **Nastavení**.



Obrázek 76, MS Outlook 2007, výběr certifikátu 2

Ve spodní části okna můžeme vybrat certifikát pro digitální podpis a certifikát pro šifrování. Podmínkou je, aby se certifikáty nacházely v centrálním úložišti Windows. Import certifikátu do centrálního úložiště Windows jsme popisovali v kapitole **Certifikáty, certifikační autority a identifikace subjektů**. Stejně tak jsme v této kapitole zmínili důvody, proč se k šifrování nesmí používat kvalifikovaný certifikát. Nyní se ale vraťme

k výběru podpisového certifikátu. Stisknutím tlačítka **Vybrat** v kategorii "Podpisový certifikát" se nám otevře nabídka s certifikáty uloženými v centrálním úložišti Windows. Z nabídky vybereme kvalifikovaný certifikát. Obdobným způsobem bychom vybrali i komerční certifikát pro šifrování.



Obrázek 77, MS Outlook 2007, výběr certifikátu 3

Na obrázku č. 76 jsme měli zaškrtnutou volbu "S podepsanými zprávami odesílat tyto certifikáty". Jedná se o velmi užitečnou funkcionalitu. Pokud budete posílat elektronicky podepsanou zprávu, příjemce musí nějakým způsobem ověřit Vaši identitu. V tomto případě mu bude se zprávou automaticky odeslán i Váš certifikát (na odeslaném certifikátu se samozřejmě nachází pouze Váš veřejný klíč). Příjemce může poté jednoduše ověřit, že zprávu jste podepsali doopravdy vy (zpráva je dešifrována Vaším veřejným klíčem umístěným na certifikátu). Samotná důvěryhodnost podepsané osoby je řešena pomocí stromové delegace důvěry popisované v dřívějších kapitolách. Pokud nedojde k automatickému odeslání certifikátu příjemci, je nutné, aby ho příjemce získal jiným způsobem, například importem z přenosového média.

6.2 PŘIPOJENÍ ELEKTRONICKÉHO PODPISU DO EMAILOVÝCH ZPRÁV

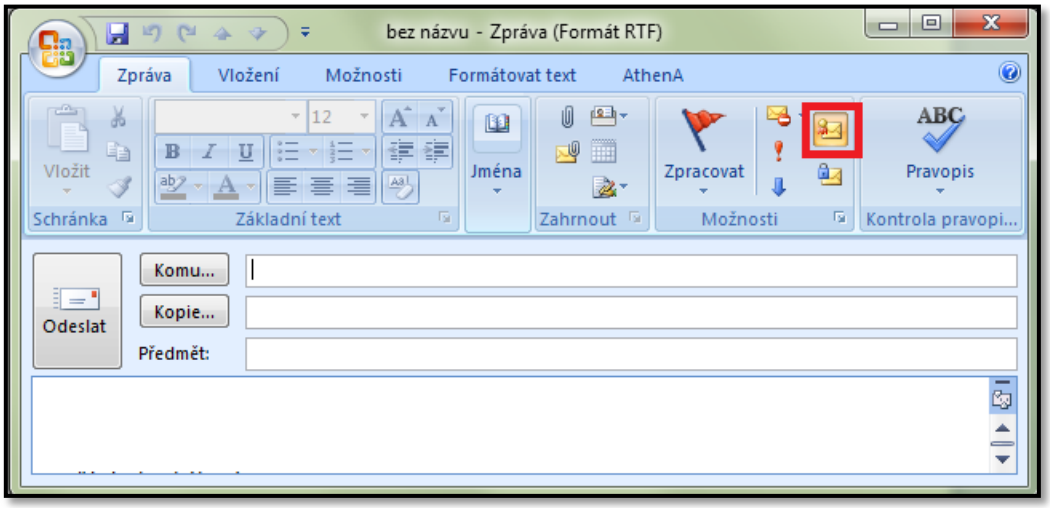
Samotné připojení elektronického podpisu ke zprávě může probíhat dvěma způsoby.

a) Elektronický podpis bude automaticky připojen ke všem odesílaným zprávám.

b) Elektronický podpis budeme připojovat manuálně ke každé zprávě zvlášť.

Pokud chcete, aby byl elektronický podpis připojen ke každé nové zprávě, stačí zaškrtnout volbu "Přidat digitální podpis do odesílaných zpráv". Tato volba se nachází

v **Centru zabezpečení**, v části **Šifrovaný e-mail**. Můžete ji také vidět v horní části obrázku č. 76. Nyní stačí vytvořit novou zprávu, v základní nabídce vyberete příkaz **Nový** a možnost **Poštovní zpráva**. Podbarvená ikona v okně zprávy symbolizuje připojení elektronického podpisu.



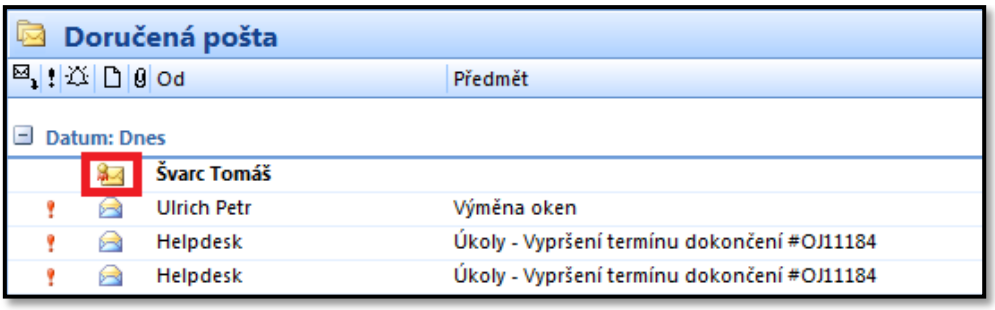
Obrázek 78, Připojení elektronického podpisu ke zprávě

Pokud chcete elektronický podpis připojit jen k některým zprávám, nezaškrtávejte v **Centru zabezpečení** možnost "Přidat digitální podpis do odesílaných zpráv". V tomto případě není ikona elektronického podpisu u všech nově vytvářených zpráv podbarvena (není aktivní). Elektronický podpis ke zprávě připojíte jejím stisknutím. Tato varianta se hodí v případě, pokud chcete elektronicky podepisovat jen některé zprávy.

Pokud byste neměli vybraný certifikát pro elektronický podpis (viz kapitola "Výběr certifikátu pro elektronický podpis"), ikona elektronického podpisu se Vám v okně zprávy nezobrazí.

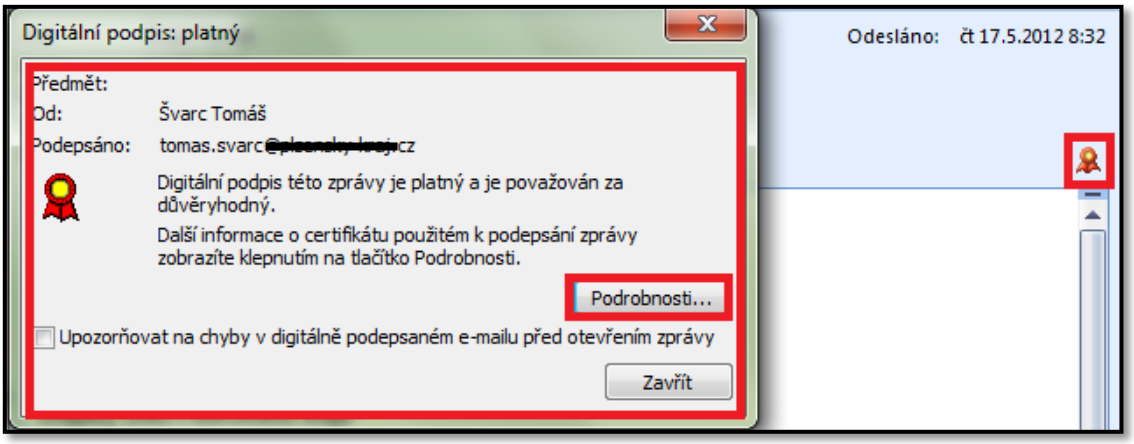
6.3 OVĚŘENÍ PODEPSANÉ OSOBY

Přijatou elektronicky podepsanou zprávu poznáte poměrně jednoduchým způsobem, v její hlavičce se nachází ikona symbolizující elektronický podpis.



Obrázek 79, Ověření elektronicky podepsané zprávy 1

Pokud zprávu otevřeme a v její pravé části klikneme na ikonu elektronického podpisu, zobrazí se nám další podrobnosti. V podrobnostech je uvedena podepsaná osoba včetně informace o důvěryhodnosti jejího podpisu. Důvěryhodnost podpisu je založena na důvěryhodnosti certifikátu osoby a stromu delegace důvěry (popisovali jsme v předcházejících částech práce).



Obrázek 80, Ověření elektronicky podepsané zprávy 2

7 ZÁVĚR

Práce představila různé prostředky, které se používají k zajištění bezpečnosti a ochrany dat na stanicích s operačními systémy Microsoft Windows provozovaných ve školním prostředí. Jejich teoretické funkční principy byly doplněny konkrétními praktickými příklady. Od obecných bezpečnostních prvků jako je například Antivir, Firewall a aktualizace systému práce směřovala ke specifickým nastavením bezpečnostních mechanismů typických pro školní prostředí, jako je například centralizovaný způsob sdílení a zabezpečení souborů. Prostřední část práce obsahovala praktické ukázky eliminace šíření škodlivého softwaru, konkrétně počítačového červa.

Práce se dále věnovala problematice ověření identity osob a serverů, kde tuto problematiku nejdříve rozebrala v teoretické rovině, upozornila na možná bezpečnostní rizika a praktickými příklady naznačila jejich možná řešení. V této části byly podrobně rozebrány termíny z oblasti elektronického podpisu a šifrování dat, které byly následně ilustrovány na použití elektronického podpisu v poštovním prostředí MS Outlook 2007.

Diplomová práce byla záměrně doplněna řadou praktických příkladů, které si kladly za cíl dosáhnout lepšího pochopení jednotlivých bezpečnostních mechanismů.

Bezpečnostních rizik spojených s poškozením, ztrátou či zneužitím dat je v dnešní době obrovské množství. Z toho vyplývá nejen nutnost zvýšené obezřetnosti uživatelů, kteří by měli dodržovat řadu bezpečnostních zásad a konfiguračních postupů zmíněných v této práci, ale také nutnost používání nejnovějších programů, které svojí přítomností chrání data v počítači.

8 SEZNAM OBRÁZKŮ

9 SEZNAM TABULEK

10 SEZNAM LITERATURY

CZ.NIC. Bezpečné a pohodlné přihlašování k webovým službám. *mojeID* [online]. 2012. [cit. 2012-05-06]. Dostupné z: <http://www.mojeid.cz/>

DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1

EISENKOLB, K. - GÖKHAN, M. - WEICKARDT, H. *Bezpečnost Windows 2000/XP.* Praha: Computer Press, 2003. 501 s. ISBN: 80-7226-789-2.

ENDORF, C. *Hacking - detekce a prevence počítačového útoku.* Praha: Grada, 2005. 200 s. ISBN: 80-247-1035-8.

GARFINKEL, S. – SPAFFORD, G. *Bezpečnost v Unixu a internetu v praxi*. Praha: Computer Press, 1998. 948 s. ISBN: 80-7226-082-0.

HÁK, P. Moderní počítačové viry. *Viry.cz* [online]. 2005. [cit. 2012-02-02]. Dostupné z: <http://viry.cz/download/kniha.pdf >

KRČMÁŘ, P. SSL v ohrožení: Komunikaci je možné dešifrovat. *Root.cz* [online]. 2011. [cit. 2012-02-05]. Dostupné z: <http://www.root.cz/clanky/ssl-v-ohrozeni-komunikaci-je-mozne-desifrovat/>

MALINA, P. *Microsoft Windows Server 2003 Hotová řešení*. Brno: Computer Press, 2006. 358 s. ISBN: 80-251-1096-6.

MICROSOFT. Pomoc a podpora Microsoft [online]. 2012. [cit. 2012-04-15]. Dostupné z: <http://support.microsoft.com/>.

MICROSOFT. Microsoft TechNet [online]. 2012. [cit. 2012-05-02]. Dostupné z: <http://technet.microsoft.com/cs-cz/ >

MICROSOFT CORPORATION. Worm:Win32/Morto.A. *Malware Protection Centre* [online]. 2011. [cit. 2012-02-14]. Dostupné z: < http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Worm%3AWin32%2FMorto.A >

PETERKA, J. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. 430 s. ISBN: 978-80-904248-3-8

PETERKA, J. Jak fungují firewally? *eArchiv.cz* [online]. 2011. [cit. 2012-02-10]. Dostupné z: WWW: <http://www.earchiv.cz/b03/b0800001.php3>

PETERKA, J. Princip firewallů. *eArchiv.cz* [online]. 2011. [cit. 2012-02-10]. Dostupné z: <http://www.earchiv.cz/b01/b0100020.php3>

PRVNÍ CERTIFIKAČNÍ AUTORITA. Komerční a kvalifikované certifikáty. [online]. 2012. [cit. 2012-03-25]. Dostupné z: <http://www.ica.cz/Certifikaty>

QUALYS, INC. How well do you know SSL? *Qualys SSL Labs* [online]. 2012. [cit. 2012-05-04]. Dostupné z: <https://www.ssllabs.com/index.html>

ZÁPADOČESKÁ UNIVERZITA. Ověření komunikujícího protějšku certifikáty. *support.zcu.cz- server uživatelské podpory* [online]. 2008. [cit. 2012-06-02]. Dostupné z: <http://support.zcu.cz/index.php/Ov%C4%9B%C5%99en%C3%AD_komunikuj%C3%ADc%C3%ADho_prot%C4%9Bj%C5%A1ku_certifik%C3%A1ty>

11 RESUMÉ

The diploma work introduces many means used for security and data protection of stations with Microsoft Windows operating systems at schools. Their theoretical functional principles were supplemented with particular examples. The work analyzes general security elements such as Antivirus, Firewall and system update, as well as specific security settings. Those security mechanisms are typical for school environment such as centralized way of sharing and securing data files.

The work pays attention to identity and server identification issues. Those issues were analyzed on the theoretical basis. Furthermore, it points out the possible security risks and uses the practical examples to show their feasible solutions.

Nowadays we have to face a huge amount of security risks leading to damage, loss or data abuse. That demonstrates the users' need of increased vigilance along with complying with certain precautions and configuration processes. Using the latest programs to protect data files in PC is, as stated in the work, equally important.