Jak zabezpečit domácí počítač

ZÁSADY BEZPEČNÉHO PŘIPOJENÍ K INTERNETU

MARTIN IGNJATOVIĆ

Vposlední době se opět začínají rozmáhat kauzy okolo vysokých telefonních účtů, šíření nejrůznějších virů a zneužití dat. Tyto problémy se týkají většinou běžných domácích uživatelů připojených k internetu. Domácí uživatelé, kteří jsou připojeni nějakým způsobem k internetu, se stávají oběťmi podobných útoků stále častěji. My si nyní vyjmenujeme a popíšeme devět základních bodů, po jejichž splnění budete moci konstatovat, že váš počítač je bezpečný a před těmito a jinými útoky chráněný. Návod samozřejmě není univerzální a nikdy nebudeme moci říct, že pro zabezpečení počítače nemůžete udělat více. Tato osnova je pouze vodítkem, které by vám mělo pomoci v zabezpečení vašeho počítače. V celém článku bude řeč výhradně o systémech Windows, protože těch se podobné útoky týkají nejčastěji.

1. KROK – SOUČASNÝ STAV SYSTÉMU

Myslíte si, že váš *současný* systém je bezpečný? Odpověď na tuto otázku je klíčová v celém procesu zabezpečení. Nemá cenu aplikovat bezpečnostní opatření na systému, který může být ovládán někým jiným. Rovněž nemá cenu zabezpečovat systém, který může mít poškozené systémové soubory, v lepším případě virem, v horším nezvaným útočníkem. Jak tedy zjistíte, jestli je váš systém bezpečný? Pokud máte systém „čerstvě“ nainstalovaný a nebyl dosud připojen k síti, je pravděpodobné, že bude bezpečný. Ale pozor na to, kdo instalaci prováděl! Pokud systém instaloval někdo jiný než vy, zejména někdo, koho neznáte nebo komu nemůžete stoprocentně věřit, nemůžete svůj systém prohlásit za zcela bezpečný. To se týká zejména systémů koupených tzv. „z druhé ruky“.To však neznamená, že systém, který byl připojený k síti, nemůže být bezpečný. Záleží na tom, jaký software používáte, kde hoshánite, jak instalujete a na mnoha dalších faktorech. A nyní již přistupme k praktickým krokům. Pokud nemůžete o svém systému prohlásit, že je bezpečný a máte podezření, že by integrita systému mohla být nějakým způsobem porušena, zazálohujte si svá data a systém přeinstalujte. Vhodné je před instalací disk zformátovat a ne systém pouze takzvaně „přeplácnout“. Některé nástroje umí data z disku bezpečně odstranit. Jedním z nich je například nástroj Partion Magic. Budete muset odstranit vybranou partion, a poté ji znovu vytvořit. Ne každému se však chce disk formátovat a mnoho z vás bude mít jistě pocit, že jejich systém je bezpečný. Přistoupíme k jinému řešení, a tím je analýza systému. Více o analýze systému v kroku dvě.

2. KROK – ANALÝZA SOUČASNÉHO SYSTÉMU

Pokud jste se rozhodli, že nebudete disk formátovat a systém znovu instalovat, je pro vás určen druhý krok, kterým je analýza systému. Cílem této analýzy je zjistit podezřelé aktivity v systému, a případně zjistit jejich původ a zdroj. Prvním krokem bude antivirová kontrola. Tuto kontrolu lze provést antivirovým programem nainstalovaným na daném systému, ale musíte počítat s tím, že tato kontrola nemusí být stoprocentní, neboť mohou být infikovány soubory samotného antivirového programu. Nejjistější metodou je provést kontrolu z jiného média než z lokálního disku, například ze záchranné diskety, jejíž vytvoření umožňuje většina moderních antivirových programů, nebo připojením disku k jinému počítači. Ideální je vytvořit záchrannou disketu na systému, o kterém víte, že je čistý, a ne na podezřelém systému, kde přítomnost virové nákazy předpokládáte nebo nemůžete vyloučit. Ještě dejte pozor, aby vaše virové databáze byly aktuální.

Pokud vše proběhne v pořádku a váš systém nejeví známky virové infekce, je třeba zjistit, jestli na systému neběží nějaký jiný škodlivý druh softwaru. Nejčastěji se jedná o trojské koně a backdoory. Tento software, pokud zrovna nelikviduje vaše data, může sloužit někomu cizímu k ovládnutí vašeho počítače. Veškerý software, který má být po startu systému funkční, se musí také po startu aktivovat. Co není spuštěno, nemůže naslouchat požadavkům a na tyto požadavky reagovat. Jak tedy zjistíme, který software je po startu počítače spouštěn? Nejdříve se podíváme na složku „Po spuštění“. U systémů Windows 2000 a XP si dejte záležet a prohledejte tuto složku u všech uživatelů. Pokud v této složce naleznete nějaký soubor (zástupce), o kterém nevíte, proč by tam měl být a název programu vám nic neříká, smažte nebo přesuňte tohoto zástupce na jiné místo, než je složka „Po spuštění“. Pokud by vám přestala fungovat nějaká aplikace, kterou využíváte, možná to bude způsobeno tímto zástupcem. Proto jej nakopírujte zpět. Dalším místem, jež umožňuje spouštění aplikací po startu systému, je systémový registr Windows. Zde prohledejte položky *HKLM\Software\Microsoft\Windows\CurrentVersion* a pak jednotlivé položky ve složkách *Run, RunServices*. Alternativně prohlédněte stejné položky i ve větvi HKCU. Pokud nic podezřelého neobjevíte, neznamená to ještě, že na vašem počítači nic škodlivého není. Existuje software, který umí modifikovat knihovny nebo spustitelné soubory jiných aplikací a spouštět se společně s nimi. Proto můžete spustit například svůj oblíbený webový prohlížeč a nevědomky tak aktivovat i program, jenž umožní někomu cizímu plně ovládnout váš systém. V takovém případě byste měli sáhnout po softwaru, který umí detekovat trojské koně a backdoory. Jedním z nejznámějších a nejúčinnějších je The Cleaner, který si můžete stáhnout ze stránek ***www.moosoft.com***. Tento software je poměrně spolehlivý, co se týká detekce trojských koní a dalšího škodlivého softwaru. Většinu známých programů podobného typu detekují i kvalitní antiviry, takže pokud provedete důkladnou prohlídku systému, neměly by uniknout vaší pozornosti. Existují však i programy, které tak známé nejsou a nechovají se standardně. S detekcí takových programů mohou mít některé antivirové programy problémy, a některé z nich je nemusí najít vůbec. V takovém případě existuje už jen jediná pomoc, a tou je sledování síťového provozu. To můžete realizovat pomocí nějaké speciálního softwaru, například pomocí snifferů, nebo můžete použít zcela prozaický firewall, který splní tutéž funkci a navíc ho k ochraně počítače využijete i jinak. K firewallu a jeho úloze při ochraně se ještě vrátíme, nyní se podíváme na to, jak nám firewall poslouží v případě, kdy chceme odhalit podezřelý síťový provoz z našeho počítače. Pokud to myslíte s bezpečností vážně, sáhněte po nějakém opravdu kvalitním firewallu, typu Kerio Personal Firewall. Tento produkt je jedním z nejlepších na trhu, a navíc je pro domácí použití zdarma. Stáhnout jej můžete ze stránek ***www.kerio.com***. Detailní popis činnosti tohoto firewallu najdete v některém z minulých čísel PC WORLDu, proto se všemi technickými detaily zabývat nebudeme a řekneme si jen rámcově, co je třeba sledovat.

Implicitně zakažte veškerý síťový provoz, přesněji řečeno nedefinujte žádná pravidla. Potom se pokuste připojit k síti. Firewall by vás poté měl upozornit, jestliže se nějaká aplikace pokouší navázat spojení. Rovněž vás upozorní, na jakou adresu a na který port. Ale pozor! Pokud nějaké aplikaci povolíte komunikovat neomezeně, ani nejlepší firewall vás neochrání. Jde-li vám tedy o absolutní bezpečnost a chcete mít jistotu, že váš systém používá originální, nenapadené aplikace, nové instalaci systému se stejně nevyhnete. Rovněž můžete použít program pro sledování síťového provozu, který bezpečně odhalí, jaké pakety do vašeho systému přicházejí a jaké odcházejí. Z jejich analýzy můžete lehce vyvodit, děje-li se na vašem počítači něco podezřelého. Ideálním nástrojem je například ethereal – pokud chcete využít standardní součásti Windows, můžete použít příkaz netstat, ale pozor, i tento nástroj může být pozměněn, aby zobrazoval jen to, co si útočník přeje.

Výše uvedené kroky by měly odhalit veškeré podezřelé aktivity ve vašem systému. Pokud jste se rozhodli systém nově nainstalovat, můžete prohlásit, že váš systém je bezpečný. Tím končí i úvodní fáze kontroly systému. Nyní se tedy podíváme na další kroky, pomocí kterých bezpečnost vašeho systému zvýšíte.

3. KROK – SOFTWARE

Každý jistě uzná, že systém bez programového vybavení je jen hromadou zbytečných součástek. Bez programového vybavení by nemělo cenu počítač mít (pomineme lidi, kteří počítače sestavují, rozebírají, montují). Právě software je potenciální branou průniků do vašeho systému. Výběr softwaru je jedním z nejdůležitějších kroků k dosažení bezpečnosti vašeho systému. Ne všechny programy jsou tak poctivé, jak se tváří, a ne všechny dělají to, co očekáváte. Nejlepším příkladem je takzvaný spyware, který často z vašeho počítače odesílá citlivé informace, například o tom, jaký software máte nainstalovaný, případně to, jaké webové stránky navštěvujete. Obrana proti tomu druhu softwaru není snadná, ale naštěstí máme po ruce nástroj, který umí spyware odhalit a odstranit. Tímto nástrojem je Ad-aware, jejž můžete získat na stránkách ***www.lavasoft.de***. Dalším důležitým krokem je samozřejmě antivirová kontrola softwaru, případně kontrola přítomnosti trojských koňů. Touto kontrolou by měl projít veškerý software, který se snažíte na svůj systém instalovat. V posledním stadiu by vás měl ochránit ještě firewall, jenž odhalí všechny aplikace, které se snaží komunikovat přes síť. Těmto výstrahám věnujte zvýšenou pozornost!

Dalším případem je software, který ke svému fungování síť vyžaduje a využívá. Nemusí však jít jen o škodlivý software. Můžete mít na svém počítači například nainstalován webový server Apache a databázi MySQL, kde si testujete vlastní skripty v PHP. Nebo může jít o webový server IIS, který používáte k testování stránek ASP. Příkladů může být více. Tyto aplikace je však také třeba chránit. I když nejsou primárně určeny k zneužívání dat a k oklamání uživatele, jsou potenciální dírou do vašeho systému. Tyto aplikace jsou navíc velmi dobře identifikovatelné, a pokud nejsou aktuální, jsou i poměrně dobře zneužitelné. Nejlepší obranou je tedy tyto služby v průběhu připojení k internetu vypnout, zejména jste-li připojeni přes dial-up. Jste-li připojeni k síti stále, nemá cenu tyto služby vypínat, pokud je ke své práci chcete nebo potřebujete. Musíte se podívat po jiné ochraně. Jako první se nabízí konfigurační soubory těchto aplikací. Zde můžete určit, odkud lze ke službám přistupovat. Pokud aplikace tuto možnost nenabízí, musíme ji blokovat na firewallu. Firewall je rovněž nejjistějším řešením, protože útočníka k samé aplikaci vůbec nepustí, kdežto samotná aplikace umožní připojení a poté, na základě konfigurace, rozhoduje o tom, zda umožní další činnost či ne. To může být nebezpečné v případě, že je v aplikaci bezpečnostní chyba. Takto může být tato chyba zneužita. Aktualizace je tématem sedmého kroku.

4. KROK – ANTIVIROVÝ PROGRAM

Výběr a instalace správného antivirového programu jsou ve světě operačních systémů Win-

dows opravdu klíčové a zásadní při ochraně počítače. Šetřit na antiviru se skutečně nevyplatí. Investice do antivirového programu se vám bohatě vrátí. Není snadné říct, který antivirový program je nejlepší a nejvhodnější. Existuje však několik renomovaných antivirových programů, jež lze považovat za spolehlivé. Jde například o produkty AVP, AVG, Panda, Norton AV. Výběr záleží na vás a vašich finančních možnostech. Zde je několik obecných vlastností, které by měl kvalitní antivirový program splňovat:

- Pravidelné aktualizace – klíčová vlastnost, čím častější aktualizace, tím lépe
- Kvalitní virová databáze – program, který nedokáže odhalit virus, není k ničemu
- Kvalitní heuristická analýza – program by neměl odhalovat jen známé viry, ale měl by umět hledat i jejich příznaky.

Další kroky jsou již v režii uživatele. K čemu vám bude antivirový program, který není aktualizován? Rovněž nemá smysl mít antivirový program, jenž neprovádí rezidentní kontrolu všech souborů, nebo který nemá tuto kontrolu aktivovanou. Dalším důležitou vlastností je schopnost kontroly příchozí pošty. Právě elektronickou poštou se šíří nejvíce virů a jiné elektronické havěti, a proto je kontrola pošty velmi důležitou. Kvalitní antivir by měl být schopen kontrolovat i obsah webových stránek, které si prohlížíte. Pravidelné kontroly systému jsou rovněž namístě. Měli byste mít naplánovanou určitou strategii, kterou se budete řídit. Měly by v ní být zahrnuty pravidelné aktualizace, kontroly systému a sledování novinek v oblasti virů. Pokud budete mít toto řádně naplánováno a plánu se budete držet, jste před viry celkem v bezpečí. Pokud máte dostatečně výkonný počítač, můžete uvažovat i o nasazení dvou antivirových programů. Ale musíte mít na zřeteli své možnosti a potřeby, abyste se ve výsledku nedostali do situace, které se říká „hodně peněz za málo muziky“. Ve většině případů vám bude jeden kvalitní antivirový program stačit bohatě.

5. KROK – FIREWALL

Instalace firewallu je v dnešní době takřka nutností. Pokud jste připojeni k internetu pomocí vytáčeného připojení (dial-up), není pro vás situace tak nebezpečná, jako pro uživatele, kteří jsou připojeni stále, ale stejně se musíte mít na pozoru. Chráníte svůj systém nejen před útočníky zvenku, ale také chráníte data a aplikace na svém systému tak, aby se chovaly jak mají a data zůstala tam, kde mají být. Ideálním pomocníkem je v takovém případě firewall. Ten ochrání váš systém nejen před útočníky zvenku, ale i před škodlivým softwarem ve vašem počítači. Když nějaký škodlivý software není odhalen antivirem ani jinými programy pro kontrolu nebezpečného softwaru, stává se firewall poslední instancí. Firewally obecně, zejména nástrojem Kerio Personal Firewall, jsme se zabývali v minulých číslech PC WORLDu, proto zde opět nebudeme vyjmenovávat všechny „triky“ a možnosti nastavení jednotlivých produktů, ale zopakujeme si obecné zásady.

Z praxe se ukazuje, že nejlepší metodou je zakázat veškeré služby a poté povolit jen ty, které chceme nebo potřebujeme. Tato taktika je lepší než zakázat aplikace, jež nechceme, a povolit vše ostatní. Je to z jednoho prostého důvodu a sice, že dopředu nemůžeme identifikovat aplikaci, kterou chceme zakázat, zejména pokud o ní předem nevíme. Dalším důležitým pravidlem je dobře si promyslet, než nějakou aplikaci povolíme. Jakmile nějaká aplikace dostane možnost komunikovat po síti (v případě, kdy ji přesně neurčíme, s kterou vzdálenou adresou), nemáme v podstatě žádnou možnost ovlivnit jaká data aplikace posílá.

6. KROK – PŘIPOJENÍ

V poslední době se, po delší odmlce, opět rozhořela kauza přepojování telefonních linek a aféry týkající se vysokých telefonních účtů. Ochrana proti těmto druhům útoků je však poměrně snadná a vybaveni znalostmi se jim můžeme lehce bránit. Celý princip spočívá v kousku programového kódu, který po svém spuštění odpojí modemové připojení, vypne interní ozvučení modemu a připojí se k číslu, o kterém nemáme ani ponětí. Cena takovéhoto hovoru se pak pohybuje v řádu desítek korun za minutu. Lze si lehce představit, jak bude vypadat telefonní účet po několika hodinách připojení. Jak se však tento druh programového kódu, jenž toto činí, může dostat do vašeho systému? Způsobů je několik, nejčastější jsou tři.

První a nejrozšířenější způsob využívá webových stránek. Aplikace způsobující přepojení je na stránku umístěna jako applet, a po její aktivaci v prohlížeči je uživatel zpravidla vyzván, aby potvrdil aktivaci a instalaci appletu. Většina uživatelů tuto nabídku odmítne, jsou však i tací, kteří bezhlavě kliknou na OK a neštěstí je na světě. Někdy se ani tato výzva nezobrazí. To může být způsobeno nastavením prohlížeče (přesněji IE). Proto si v nastavení Internet Exploreru aktivujte vysoký stupeň ochrany a dobře zkontrolujte, zdali máte zakázáno stahování appletů, zejména těch nepodepsaných. Rovněž může být k instalaci využito konkrétní bezpečnostní chyby.

Dalším způsobem, jak dostat tento škodlivý software do systému, je elektronická pošta. Tento způsob využívá buď konkrétní bezpečnostní chyby e-mailového klienta, nebo spoléhá na naivnost uživatelů, slepě klikajících na jakékoliv tlačítko OK, které je k dispozici.

Třetí a nejméně rozšířený způsob je aktivace tohoto softwaru pomocí nějaké jiné aplikace, podobně jako u trojských koní nebo backdoorů.

Jak se tedy bránit? Jedním ze základních a nejdůležitějších ochranných prostředků je obezřetnost a opatrnost. Tato opatrnost souvisí zejména s chováním na internetu a dodržováním elementárních bezpečnostních zásad. Více o těchto zásadách a chování v síti si povíme v osmém kroku. Dalším ochranným prostředkem je výběr prohlížeče a jeho pravidelná aktualizace, stejně jako e-mailového klienta. Tyto dvě aplikace jsou klíčové, co se týče průniků škodlivého softwaru do vašeho systému. Pokud se však nechcete spoléhat jen na „aktuální“ bezpečnost svého prohlížeče, máte ještě jednu možnost. Tou je instalace programu na ochranu telefonního připojení. Tento program hlídá vaše telefonické připojení, a pokud dojde k nějakému pokusu o vytočení jiného čísla, než které povolíte, program vás na to upozorní a navíc připojení neumožní. Programů na hlídání připojení je několik, my si představíme OptimAccess Dial, jejž můžete získat na adrese ***www.optimaccess.cz***. Program je k dispozici zdarma, ovládání je snadné (kompletně v češtině) a jeho instalace se vám určitě vyplatí. Nikdo vám totiž nemůže zaručit, že ve vašem oblíbeném prohlížeči nebude objevena bezpečnostní chyba.

7. KROK – AKTUALIZACE SOFTWARU

Aktualizace softwaru je poměrně obecně známá a je v povědomí uživatelů, že by se měla provádět. Bohužel od teorie k praxi bývá často velmi dlouhá cesta. Aktualizace softwaru je ve většině organizací a také u většiny uživatelů spíše sporadická než pravidelná. Co je tedy vlastně potřeba aktualizovat a jak často? Nejdůležitější součástí každého osobního počítače je operační systém. Není tedy od věci, začít u něj. Jak již bylo v úvodu řečeno, je tento článek určen uživatelům operačních systémů Windows. Aktualizace pro tento systém naleznete na stránkách ***www.microsoft.com***. Zde zvolte položku *Windows update*. Bude detekována verze vašeho operačního systému a po analýze systému vám budou nabídnuty příslušné opravy pro váš systém. Pokud jste váš systém ještě neaktualizovali, bude seznam velmi dlouhý, zejména u operačních systémů Windows 2000 a XP, kde jsou záplaty distribuovány formou service packů, jejichž velikost je okolo stovky MB. Tyto service packy naštěstí naleznete na CD příloze časopisu PC WORLD a nemusíte stahovat ohromné množství dat, zejména pokud jste připojeni přes modem. Nedílnou součástí systémů Windows je i webový prohlížeč Internet Explorer a e-mailový klient Outlook Express. Do těchto míst by měla směřovat další vaše aktualizace. Je to proto, že tyto dvě aplikace jsou nejčastější branou útoků na váš systém. Většina lidí používajících operační systémy Windows používá i další nástroj Microsoftu, a tím je Microsoft Office. Jelikož je MS Office aplikace přímo svázaná s operačním systémem Windows, je její aktualizace rovněž důležitá, stejně jako aktualizace všech produktů od Microsoftu. Aktualizovat však není třeba jen aplikace od Microsoftu, ale všechny aplikace, které mohou být branou do vašeho systému. Pokud tedy například provozujete webový server Apache či MySQL, je jeho aktualizace rovněž důležitá, stejně jako například aktualizace firewallu. Informace o aktualizacích naleznete na stránkách výrobce aplikace. Na některých se dokonce můžete zaregistrovat a být informování o novinkách e-mailem pravidelně.

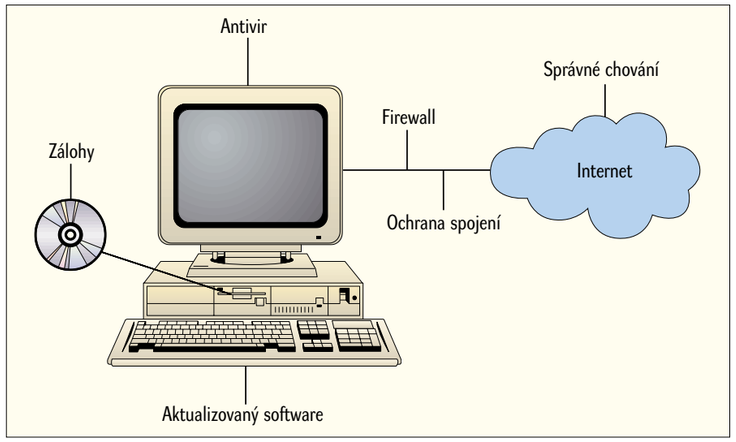
8. KROK – CHOVÁNÍ NA SÍTI

Pokud jste se drželi předchozích rad a doporučení, instalovali bezpečnostní software, provedli všechny testy a instalovali aktualizace, můžete prohlásit, že váš počítač je relativně bezpečný. Bezpečnost však není jen dílem okamžiku, měl by to být trvalý stav. Jak tento stav udržet, si řekneme v několika následujících řádcích.

Prvním a nejdůležitějším faktorem je vaše chování a zacházení se systémem. K čemu vám budou pravidelné aktualizace a instalace oprav, když pak bezhlavě stahujete kdejakou utilitku a navštěvujete stránky, jejichž obsah je mírně řečeno pochybný? Rovněž nemá cenu uvažovat o nějaké bezpečnosti, pokud bezhlavě uvádíte svoji e-mailovou adresu kde vás napadne, a stáváte se tak, mnohdy nevědomky, členem databáze příjemců různých virů. Základních zásad, jak se chovat na síti, je mnoho, zde je přehled těch nejdůležitějších:

- Stahujte a instalujte jen to, co opravdu potřebujete
- Svoji e-mailovou adresu poskytujte jen tam, kde nehrozí její zneužití
- Vyvarujte se poskytování důvěrných osobních informací
- Navštěvujte jen stránky, které jsou dle vašeho názoru seriózní
- Neklikejte bezhlavě na jakékoliv výzvy vašeho prohlížeče či e-mailového klienta
- Neinstalujte jakékoliv applety a plug-iny, které nutně nepotřebujete nebo o kterých nevíte, jakou mají funkci

Tyto základní zásady si můžete libovolně rozšířit o další, které se vám zdají rozumné a užitečné.



9. KROK – ZÁLOHOVÁNÍ

I když budete dodržovat všechny zásady vyjmenované v předchozích krocích, nikdo vám nezaručí, že se objeví bezpečnostní chyba a váš systém nebude napaden do doby, než stáhnete příslušnou opravu či novou virovou databázi. V takovém případě je důležité mít aktuální zálohy, aby váš systém mohl být zálohován. Co tedy zálohovat? Výběr může být různý. Zde je několik základních položek, které by měl zálohovat každý, a slouží jen jako jakési vodítko:

- Složka Dokumenty
- Plocha
- Nabídka Start
- Registr systému
- Konfigurace telefonického připojení
- Další vámi vytvořené složky a soubory
- Instalační soubory softwaru, který jste stáhli
- Konfigurační soubory důležitých aplikací.

Mělo by platit, že budete zálohovat vše, co jste sami vytvořili. Nemá cenu zálohovat binární soubory jednotlivých aplikací, ty mohou být obnoveny z instalačního CD. Další otázkou je, jak často a kam zálohovat. Většina domácích uživatelů nebude mít potřebu zálohovat příliš často, jednou týdně postačí. Pokud na svém počítači pracujete denně a vytvoříte velké množství dat, je namístě zamyslet se nad denním zálohováním. Pokud naopak data vytváříte jen sporadicky, postačí vám měsíční zálohy. Zálohovací médium může být různé, ale neměl by to být lokální disk. Ideálním zálohovacím médiem pro domácí použití je vypalovačka, případně zip mechanika. Pokud máte nějaký externí disk, můžete přemýšlet i o něm.

Nápady, dotazy, návrhy témat, jež vás zajímají, a připomínky zasílejte na adresu igm@centrum.cz. Na vaše dotazy k této problematice se pokusíme najít odpovědi. 3 0229/FEL ❑