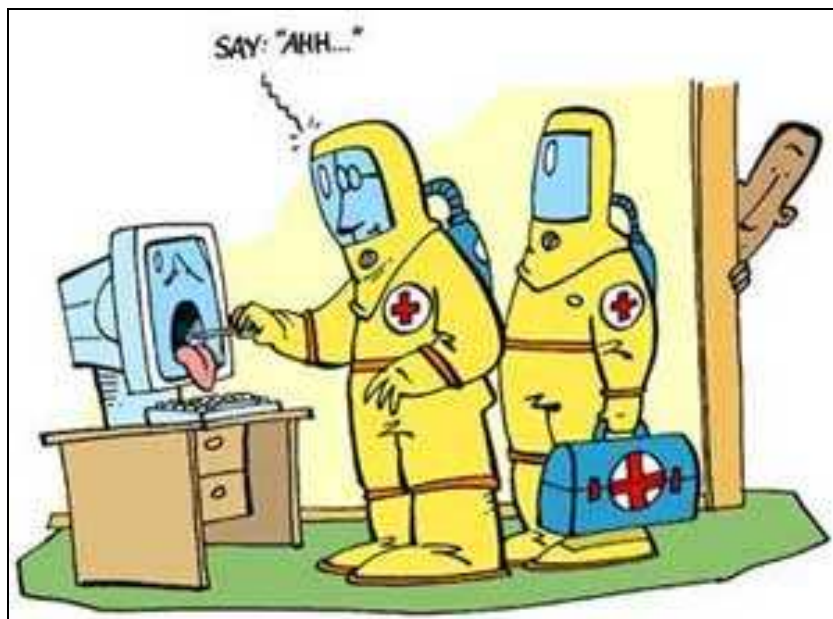


POČÍTAČOVÉ VIRY

ZÁSADY POČÍTAČOVÉ BEZPEČNOSTI

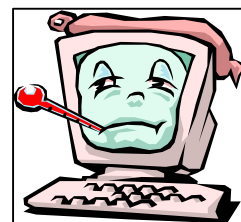


OBSAH

CO JSOU POČÍTAČOVÉ VIRY.....	3
VLASTNOSTI POČÍTAČOVÝCH VIRŮ	3
PODMÍNKY ŠÍŘENÍ VIRŮ A PREVENCE	4
ČLENĚNÍ VIRŮ Z HLEDISKA ŠKODLIVOSTI.....	4
ZÁKLADNÍ TYPY INFILTRACÍ.....	5
POČÍTAČOVÝ VIR	5
ČERV (WORM)	5
TROJSKÝ KŮŇ	5
ŽERTOVNÝ PROGRAM.....	7
HOAX.....	7
NEJBĚŽNĚJŠÍ TYPY POČ. VIRŮ.....	7
SOUBOROVÉ VIRY	7
BOOTOVÉ VIRY	8
MULTIPARTITNÍ VIRY	8
MAKROVIRY	8
ANTIVIROVÉ PROGRAMY.....	9
METODY PRÁCE ANTIVIROVÝCH PROGRAMŮ.....	10
ODSTRANĚNÍ VIRŮ	11
PRAVIDLA POČÍTAČ. BEZPEČNOSTI.....	12

CO JSOU POČÍTAČOVÉ VIRY

Počítačový virus je umělý útvar, záměrně vytvořený člověkem. Označení „virus“ zavedl do počítačové praxe poprvé ve své odborné přednášce v roce 1983 výzkumný pracovník Frederick Cohen. Jeho definice počítačového viru zní: *„Počítačový virus je počítačový program, který může infikovat jiný počítačový program takovým způsobem, že do něj nakopíruje své tělo, čímž se infikovaný program stává prostředkem pro další aktivaci viru.“*



První počítačový virus, který se dostal do oběhu, byl virus BRAIN (mozek) v roce 1987. Napadal boot sektory počítačových disket (tehdy 5 ¼“) a způsoboval, že počítač nebyl schopný disketu rozpoznat. Ve stejném roce se objevil také virus STONE (u nás nazývaný Kameňák), který modifikoval zápis v Master Boot Record a znemožňoval natahování systému z pevného disku.

Počítačové viry jsou většinou vytvářeny na nejnižší programátorské úrovni – tedy ve strojovém kódu, ale je možné je vytvářet i ve vyšších programovacích jazycích.

Počítačový virus je krátký spustitelný nebo interpretovatelný program, který je schopen sám sebe připojovat k jiným programům a dále se z nich (bez vědomí uživatele) šířit. Má tři části:

1. spouštěcí
2. vlastní funkční
3. reprodukční.

Označení počítačových virů není standardizováno, nejčastěji se označují:

- **číslem** - toto číslo udává počet bytů, o které se prodlouží hostitelský soubor po napadení virem,
- **názvem místa prvního výskytu** (Barcelona, Jerusalem...)
- **charakteristickým řetězcem znaků**, který se vyskytuje v těle viru (Slowakia Happy),
- **charakteristikou činnosti viru** - Killer.

VLASTNOSTI POČÍTAČOVÝCH VIRŮ

1. Schopnost množit se - nekontrolovaně se připojuje k jiným, tzv. hostitelským programům (souborové viry), nebo se zapisuje do systémových oblastí disků (bootové viry).
2. Schopnost vykonávat další činnost.

PODMÍNKY ŠÍŘENÍ VIRŮ A PREVENCE

1. **Vhodné prostředí** (počítač se známým operačním systémem).
2. **Objekty, které dokáže napadnout:**
 - a. **Spustitelné soubory** – běhu schopné programy – jeden z nejčastějších případů šíření virů. Vir se při odstartování nakaženého programu nahraje do operační paměti a poté provádí svou nekalou činnost. Nákazy hrozí u souborů s koncovkou EXE, COM, SYS. *Nikdy nespouštíme program, o kterém nevíme, co je zač a z jakého zdroje pochází. Pokud je program součástí ověřeného CD ze seriózní firmy, nemusíme se obávat. Jiné nosiče před použitím prověříme antivirovou kontrolou. Vůbec nespouštíme programy stažené z různých pochybných serverů z internetu.*
 - b. **Systémové oblasti paměťových médií** – disků – cílem viru je v tomto případě boot sektor nebo partition tabulka disku. Jedná se o oblasti, do kterých uživatel nemá za normálních okolností přístup a které slouží pouze operačnímu systému. *Nikdy nebootujeme – nezavádíme do počítače operační systém z nám neznámé diskety. Právě tímto způsobem se tyto viry šíří. Tento typ virů byl velmi populární v době, kdy nejrozšířenějším operačním systémem byl MS DOS.*
 - c. **Dokumenty obsahující makra** – vir se uloží přímo do dokumentu, který může obsahovat makra (Word, Excel). Pokud pak takovýto nakažený soubor otevřeme, spustí se i vir. *V programech, které používáme pro editaci textů a tabulek zakážeme automatické spouštění maker. V takovémto případě se nás program při otvírání nakaženého souboru zeptá, jestli chceme tento soubor otevřít i přesto, že obsahuje makra. Už v této fázi by nám to mělo být podezřelé a raději bychom soubor neměli otevírat.*
 - d. **Elektronická pošta (e-mail)** – velmi moderní a v poslední době častý případ virových invazí. Vir je přenášen jako samospustitelná příloha e-mailu, takže jakmile nám dojde nová zpráva, stačí ji otevřít a vir se aktivuje. Viry tohoto typu jsou o to zákeřnější, že často přicházejí pod zajímavým názvem (předmětem) ze zajímavé adresy. *Obranou je pouze stála a velká opatrnost. V žádném případě neotvíráme e-maily, které obsahují přílohu a které přicházejí z nám neznámé adresy. Tyto e-maily hned mažeme, nejenom vyhazujeme do koše. Rovněž neotvíráme e-maily, které sice přišli ze známé adresy, ale obsahují podezřelé přípony.*

ČLENĚNÍ VIRŮ Z HLEDISKA ŠKODLIVOSTI

1. **Měkké - neškodné viry.** Říkáme jim také „neškodné“ nebo „málo škodlivé“. Za určitých okolností vypisují na monitor různá hlášení, žertovné nebo propagandistické nápisy, projevují se akusticky nebo vizuálně, žádají vykonání určitých činností apod. Uživatelé zásadně neškodí, zabírají pouze místo na disku a v operační paměti.
2. **Středně škodlivé - nebezpečné viry.** Uživatelé škodí, ale ne zásadním způsobem (např. provedou restart počítače, zaměňují písmena psaná z klávesnice, způsobují zahlcení místa na disku, zahlcení průchodnosti internetových serverů apod.), zdržují uživatele v práci, ale data se neztrácejí.

3. **Tvrdé (agresivní) - nejnebezpečnější viry.** Dochází ke ztrátě dat - způsobují mazání, přepis a likvidaci dat na pevných discích nebo disketách (vymaže se část souboru, celý soubor, celý adresář, celý disk apod.).

Někdy dělíme viry podle jejich účinků také na:

1. **Obtěžující**
2. **Destrukční**

ZÁKLADNÍ TYPY INFILTRACÍ

POČÍTAČOVÝ VIR

Počítačový vir je jeden druh tzv. škodlivých programů. Je to program, který se bez vědomí uživatele počítače samovolně šíří tak, že se připojuje, přepisuje nebo jinak modifikuje ostatní programy (pokud potom napadený program otevřeme, začne nejprve pracovat právě tento vir), dokumenty nebo systémové oblasti pevného disku a disket s cílem vlastní reprodukce. Kromě samotné reprodukce může přitom kód viru vykonávat různé grafické, zvukové a textové efekty, ale i destruktivní činnost – mazání, kódování a jiné modifikace v uživatelském počítači.



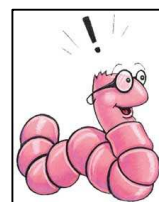
S výjimkou možnosti vymazání Flash BIOS paměti v současnosti nejsou známy viry poškozující hardware počítače.

Některé viry podobně jako dále zmíněné trójské koně narušují bezpečnost počítače a údajů na pevném disku zasíláním tajných šifrovacích klíčů, odchycených hesel a e-mailových adres atd. různými komunikačními kanály mimo napadený počítač (např. autorovi viru). Také na pohled neškodné viry mohou způsobit svou přítomností problémy v souvislosti se spotřebou části operační paměti, výpočetní kapacity procesoru, ale hlavně vznikem různých typů interferencí s jinými programy a samotným operačním systémem.

ČERV (WORM)

Červ žádné soubory nenapadá. Při šíření sám sebe odešle prostřednictvím počítačové sítě jako přílohu e-mailu nebo jiným pokoutným způsobem. Parazituje v jednom exempláři (v jedné kompletní sadě souborů) na hostitelském počítači, přičemž používá jeho komunikační propojení s dalšími počítači pro svoje šíření.

Klasický červ se tedy nepřipojuje k žádnému hostitelskému souboru, ani se na lokálním disku nešíří.



TROJSKÝ KŮŇ

Trojský kůň je program, který navenek navozuje dojem užitečnosti (např. přehrává hudbu, zobrazuje předpověď počasí), ale přitom v pozadí dělá ještě i něco nekalého - maže soubory, formátuje pevný disk, skrytou komunikací přes Internet narušuje soukromí uživatele počítače - zaznamenává hesla, která vkládáme do různých formulářů, pozoruje, jaké stránky na Internetu otvíráme, umožňuje úplné dálkové ovládnutí počítače apod.

Trojský kůň je buď naprogramovaný jako původní aplikace, nebo je vytvořený z už existujícího programu jeho spojením s destrukčním kódem, který se vykonává před samotným programem. Od počítačového viru nebo červa se trojský kůň odlišuje tím, že se dál nereprodukuje.



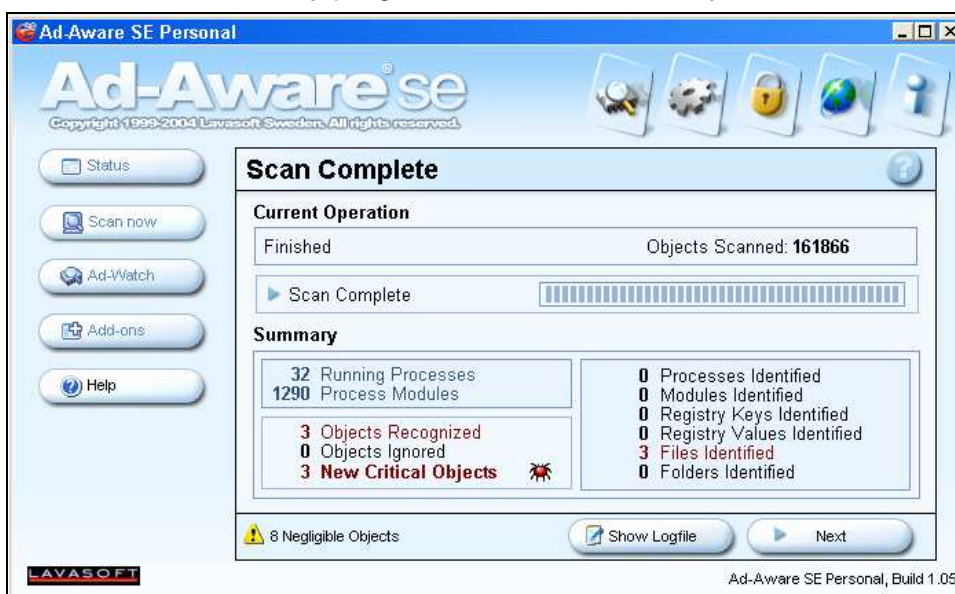
Trojské koně můžeme dále dělit na dvě skupiny:

Spyware – shromažďuje nejrůznější informace a odesílá je bez vědomí uživatele počítače někomu jinému. Nezáleží na tom, jaké informace sbírá (seznam zadávaných hesel, seznam skladeb přehrávaných na počítači ...).



Okno programu Microsoft AntiSpyware Beta1

Adware je program, který během své běžné činnosti zobrazuje reklamu (běžné reklamní proužky - bannery – známe i z internetových stránek) nebo vyskakující reklamní okna. Škodlivý program může ale nemusí být zároveň Adware i Spyware.



Okno programu Ad-Aware s indikací nalezených kritických objektů adware

ŽERTOVNÝ PROGRAM

Jsou to neškodné programy (joke), které simulují chybové stavy operačního systému, nebo také nějaký druh destrukční činnosti (mazání dat, formátování disku) a jsou určeny k pobavení ve formě kanadského žertíku. Kromě vystrašení uživatele nezpůsobuje žádné škody.

HOAX

Jsou to E-mailové zprávy obsahující falešné upozornění na nebezpečí nakažení se nějakým novým virem případně jinou na pohled důležitou (zajímavou, užitečnou) zprávu, kterou uživatelé vlastnoručně rozšiřují dále mezi svými kontakty a způsobují tak lavinovité šíření zprávy po síti. Následkem je zbytečné dezinformování masy lidí a zahlcování sítě.



NEJBĚŽNĚJŠÍ TYPY POČ. VIRŮ

Podle toho, jakým způsobem viry pracují a jak se projevují, je můžeme rozčlenit na **souborové viry**, **bootviry**, **multipartitní viry** a na **makroviry**.

SOUBOROVÉ VIRY

Souborové viry napadají pouze soubory (programy a dokumenty). Projevují se nejrozmanitějším způsobem a podle svých projevů se dále dělí na:

1. **Přepisující viry** - přepíší část těla své oběti – napadeného souboru-programu vlastním kódem. Takto napadené soubory jsou nenávratně zničeny a nejsou schopny žádné jiné činnosti kromě šíření viru. Tyto viry jsou velmi nápadné a nemají velkou šanci šířit se.
2. **Link viry** – přilepí (přilinkují) se k napadenému souboru, což umožňuje chod hostitelského programu a zároveň i činnost viru.
3. **Doprovodné viry** – nezapisují svůj kód přímo do napadeného souboru, ale vytvářejí kopii - stínový soubor stejného jména s příponou **.com**. Využívají vlastnost operačního systému MS DOS, který dává při spouštění programů přednost souborům typu **.com**.
4. **Viry přímé akce** – poté, co se takovýto vir dostane se svým hostitelem do operační paměti počítače, provede jednou destrukční činnost a tím skončí. např., smaže celý disk a tím vlastně zničí i sám sebe.
5. **Rezidentní viry** – po načtení do operační paměti se tam drží i poté, co práce hostitelského programu skončila, až do vypnutí počítače. Sledují, se kterými soubory uživatel pracuje a útočí na ně.
6. **Stealth viry** – dostanou-li se do operační paměti, dovedou převzít kontrolu nad některými funkcemi operačního systému. Při pokusu o čtení napadeného souboru nebo při kontrole zavirovaného souboru antivirovým programem vracejí stav před infekcí. Pro antivirové programy bez anti-stealth techniky jsou jakoby „neviditelné“.

7. **Zakódované viry** – jsou zakódované určitým proměnlivým algoritmem, takže jejich tělo je pokaždé jiné. Stejná je pouze dekodovací instrukce.
8. **Polymorfní viry** – pro každý napadený soubor se kódují jiným způsobem a vytváří i jinou dekodovací funkci. V napadených souborech nelze najít žádné sekvence stejného kódu.
9. **Fast infektory** – rezidentní viry, které se šíří velice rychle, protože napadají soubory nejenom při jejich spuštění, ale téměř při každé manipulaci s nimi. Rychlost šíření může ale znamenat i vysokou pravděpodobnost, že tyto viry na sebe rychle upozorní.
10. **Slow infektory** – šíří se velice pomalu a obezřetně, např. napadá pouze soubory, které jsou na disku nově vytvářeny (např. kopírováním).

BOOTOVÉ VIRY

Už podle názvu je jasné, že jsou to viry, které mají spojitost se zaváděním operačního systému (bootováním). Vir napadne boot sektor nebo partition tabulku pevného disku nebo diskety. Při startu počítače a zavádění operačního systému do operační paměti je potom pohodlně aktivován a převezme kontrolu nad nejnižšími diskovými funkcemi systému.

Tyto viry se šíří prostřednictvím boot sektoru disket. Aby byl počítač takovými virem napaden, musí se z nakažené diskety naboootovat (např. necháme v disketové mechanice nakaženou disketu a spustíme počítač).

Během své činnosti při práci procesoru s nenakaženým diskem, disketou napadají jeho boot sektor. Tyto viry mohou být rezidentní i přímé akce.

MULTIPARTITNÍ VIRY

Bootové viry se aktivují při startu počítače a zavádění operačního systému do operační paměti, ale aby se počítač infikoval, musí se naboootovat z nakažené diskety, což jejich šíření omezuje. Souborové viry se šíří prostřednictvím nakažených souborů, což je pro jejich šíření výhodné, ale potřebují být aktivovány spuštěním či otevřením nakaženého souboru.

Multipartitní viry využívají kombinaci a výhody obou těchto druhů – infikují partition tabulku i soubory. Po ukončení zavedení operačního systému po zapnutí počítače přebírají kontrolu nad vyššími funkcemi služeb MS DOS.

MAKROVIRY

Makroviry se objevily až s příchodem makrojazyků hlavně v textových editorech a tabulkových kalkulátorech. Jejich zákeřnost spočívá v tom, že vir je přenášen a uložen v dokumentech - tedy objektech, které uživatelé nejvíce sdílejí.

Nebezpečí makroviru spočívá v tom, že ovládne program i jeho šablony. Poté při určité operaci (např. uložení dokumentu) bude spuštěno makro s destruktivními účinky.

Zatímco s příchodem operačního systému Windows ubývá rezidentních a souborových virů, makroviry představují nastávající hrozbu.

ANTIVIROVÉ PROGRAMY

Proti virům se musíme chránit. V dnešní době si už žádný uživatel, který alespoň částečně datově komunikuje se svým okolím, nemůže být jistý. Kromě opatrnosti jsou silným prostředkem proti virům antivirové programy. Dokáží nejen vir najít, ale většinou i nakažený soubor „vyléčit“ tak, že po zásahu antivirového programu funguje správně a nemusí být smazán.

Existují antivirové programy jednoúčelové, zaměřené na jeden typ viru a programy komplexní - schopné vyhledat široké spektrum doposud známých virů.

Na softwarovém poli působí poměrně velké množství antivirových programů. V České republice se k neznámějším řadí programy AVG, AVP, AVAST nebo F-Prot.



Antivirovou kontrolu by měl uživatel provádět v pravidelných intervalech a nesmírně důležitá je i aktualizace databáze virů. Tato akce způsobí, že antivirový program bude účinný i proti novým virům, které byly odhaleny do data poslední aktualizace. Většina firem poskytujících antivirové programy vydává denní aktualizace, tj. každý den lék na nové viry.

Už ze samotného principu potom vyplývá, že žádný antivirový program na světě nemůže počítač ochránit proti virům, které vznikly právě teď. Viry jsou tedy vždy o krok vpřed.



Hlavní obrazovka programu AVG

METODY PRÁCE ANTIVIROVÝCH PROGRAMŮ

Antivirové programy ve své činnosti využívají např. tyto metody:

METODA VYHLEDÁVÁNÍ CHARAKTERISTICKÝCH ŘETĚZCŮ ZNAKŮ (VYHLEDÁVACÍ SEKVENCE)

Je to nejběžnější a nejrychlejší metoda pro jednorázovou kontrolu. Většina virů má ve svém těle určitou specifickou sekvenci – posloupnost znaků, podle které lze vir jednoznačně určit (např. A1 00 10 B5 C2 00). Antivirový program prohledává celý disk a soubory, ve kterých najde takovouto sekvenci označí za napadené. Je nutná znalost charakteristických řetězců znaků obsažených v těle viru. Velmi obtížné až nemožné je touto metodou hledat polymorfní viry, které mění svůj vlastní kód. Je to metoda pro odhalování už známých virů.

SROVNÁVACÍ METODA (KONTROLA INTEGRITY)

Při prvním spuštění tento antivirový program vytvoří databázi informací o systému, adresářích a systémových oblastech na disku, při dalším spuštění srovnává aktuální stav s předchozím a na základě změn detekuje přítomnost viru. Tato metoda je velmi spolehlivá, ale neumí zjistit konkrétní vir, pouze signalizuje změnu v systému.

HEURISTICKÁ METODA

Každý rok vznikají na světě stovky nových virů.. Od vzniku viru po vydání aktuálního antivirového programu uběhne poměrně dlouhá doba – vir se musí rozšířit, tvůrci antivirového programu ho musí analyzovat a začlenit do nové verze programu, ta musí být vyrobena, distribuovaná k zákazníkům, zákazníci si ji musí nainstalovat a použít. Proto antivirové programy disponují i funkcí tzv. heuristické analýzy. Analyzují texty programových souborů a hledají v nich případný výskyt instrukcí charakteristických pro viry. Sledují, co sledovaný program s počítačem provádí a na základě zjištění vyhodnotí, jestli je to v pořádku, či nikoliv. Pokud je takovýto antivirový program dobře napsán, dokáže najít až 70% nových virů.

METODA NÁVNADY

Antivirový program vykonává různé operace s pokusnými soubory typu .com a .exe, jejichž obsah je znám. Po vykonání těchto operací srovnává obsah pokusných souborů před a po operaci. Odhaluje např. rezidentní souborové viry.

REZIDENTNÍ HLÍDAČ

Je to část antivirového programu, která se zavádí do operační paměti po startu počítače a potom kontroluje všechny nebo vybrané typy souborů a e-maily. Pokud narazí při otvírání na vir, informuje o tom uživatele dřív, než se soubor spustí. Rychlost práce je vysoká a je prakticky nemožné, aby do počítače pronikl známý vir.

ODSTRANĚNÍ VIRŮ

Aby byl virus co nejdříve odhalen a udělal co nejméně škody, je nutná pravidelná antivirová kontrola disku. Musíme si všimnout chování počítače, protože některé viry se projevují specifickým chováním, např.:

- náhlé zpomalení práce počítače
- neočekávané rozsvěcování kontrolky diskových mechanik
- neobvyklá chybová hlášení
- nárůst délky souborů
- změna času a data posledního zápisu
- mizení souborů
- vizuální a akustické signály
- běžně používané programy hlásí chyby,

Při odstraňování odhaleného viru musíme dodržovat tyto zásady :

- zachovat chladnou hlavu a postupovat promyšleně,
- má-li být virus odstraněn, nesmí být aktivní v operační paměti, proto je potřebné zavést systém (nastartovat počítač) z bezpečné záložní diskety poslední záchrany.

ODSTRAŇOVÁNÍ BOOTOVÝCH VIRŮ

Je-li virus v boot sektoru, je možné ho odstranit novým zapsáním operačního systému na disk, nebo příkazem SYS C:. Je-li bootový virus na disketě, nahrajeme všechny soubory na disk, disketu naformátujeme a vrátíme soubory zpět. Příkazy SYS a FORMAT vytvářejí nový boot sektor. Můžeme použít i vhodný antivirový program.

ODSTRAŇOVÁNÍ SOUBOROVÝCH VIRŮ

Nejjednodušší je nakažené soubory vymazat a nainstalovat je znova ze záložních kopií. Jde-li o cenné soubory, u kterých nemáme pořízenou záložní kopii, můžeme se pokusit o léčbu antivirovým programem.

PRAVIDLA POČÍTAČ. BEZPEČNOSTI

1. Všechno důležité si zaheslujeme.

Přístup k počítači a ke všem důležitým informacím, které jsou v něm uloženy, by měl být chráněn heslem.

- Heslo plní stejnou funkci jako v běžném světě klíč.
- Každý počítač by měl po spuštění od uživatele požadovat heslo.
- Další hesla by měla chránit přístup k nastavení systému a k důležitým souborům.



2. S hesly zacházíme opatrně, necháváme si je pro sebe a čas od času je změníme.

- Heslo by nemělo být snadno odhadnutelné – nevolíme nic co má souvislost s našim životem - žádná jména, telefonní čísla, data narození svých blízkých. Neodhadnutelné heslo se však hůře pamatuje.
- Za rozumnou minimální délku pro běžná hesla se považuje osm až deset znaků.
- Ideální heslo by mělo kromě písmen obsahovat alespoň jednu číslici nebo jiný neobvyklý znak. Vyhýbáme se české diakritice i písmenům Z a Y (kvůli rozložení na některých klávesnicích).
- Heslo nikdy nikomu nesdělujeme, ani si ho nikam nepíšeme.
- Hesla v určitých časových intervalech měníme (nejčastěji hesla přenášená po síti, např. k mailové schránce, nejméně hesla k jednotlivým chráněným souborům).

3. Z internetu neotvíráme nic, o čem si nejsme jisti, že je to bezpečné.

- Na Internetu se vyskytuje spousta škodlivých programů, většinou na pornografických a hackerských stránkách.
- Správně nastavený počítač se nejprve zeptá, zda může potenciálně nebezpečný program otevřít (např. v programu Internet Explorer nastavíme v dialogovém panelu MOŽNOSTI INTERNETU na záložce ZABEZPEČENÍ střední nebo vysokou úroveň ochrany). Proti škodlivým programům slouží také antivirové programy a osobní firewall.
- Pokud přesně nevíme, co děláme, spuštění neznámého programu nepovolíme.

4. E-maily používáme bezpečně – než otevřeme podezřelou přílohu nebo zareagujeme na podezřelý e-mail, poradíme se s někým zkušenějším.

- Často jsou odesílatelem e-mailů s nebezpečnou přílohou viry nebo červy.
- V mailové poště rozhodně neotvíráme přílohy (ani obrázky a videa), jejichž původem si nejsme jisti.
- Nevyžádanou reklamní poštu (spam) hned mažeme.
- Rozesíláním řetězových dopisů, slibujících lásku či bohatství, žádajících pomoc pro trpícího chlapečka z druhého konce světa nebo varujících před novým virem riskujeme ztrátu dobrého jména. Těmto zprávám říkáme HOAX (kachna, fáma, poplašná zpráva).
- Hoaxům se v Čechách věnuje server www.hoax.cz.

5. **Chráníme se před viry** – nainstalujeme si do počítače antivirový program, pravidelně ho aktualizujeme a používáme.
 - Škodlivé programy dělíme na viry, červy a trojské koně.
 - Škodlivý program můžeme do svého počítače dostat např. v nějakém souboru nakopírovaném z diskety, CD-ROMu apod., elektronickou poštou otevřením zavírované přílohy.
 - Pravidelně aktualizovaný antivirový program si s viry poradí.
6. **Vyžeňme z počítače špióny** – jsou to většinou programy zobrazující reklamu (Adware, Spyware) a většinou nejsou nebezpečné, jen nás obtěžují.
 - Přítomnost adware v počítači poznáme podle toho, že se nám zobrazují podezřelé reklamy.
 - Programy Adware odstraníme spuštěním programu pro tuto činnost – např. Lavasoft Adware.
 - Preventivně neotvíráme podezřelé programy z internetu a používáme dobrý antivirový program.
7. **Pravidelně záplatujeme operační systém** – odstraňujeme z operačního systému díry, které by jinak mohli zneužít např. tvůrci virů.
 - V operačním systému se objevují chyby, které mohou být zneužívány např. k šíření virů.
 - Výrobce operačního systému zveřejňuje na své internetové stránce tzv. záplaty, jejichž instalací můžeme chyby odstranit.
 - V počítači si můžeme nastavit automatické stahování aktualizací souborů (START-NASTAVENÍ-OVLÁDACÍ PANELY-SYSTÉM-AUTOMATICKÉ AKTUALIZACE).
 - Nezáplatovaný systém snadněji podlehne útokům virů, červů či hackerů.
8. **Poznejme počítačové kriminálníky** – pravidelné záplatování nás ochrání před všemi útoky hackerů.
 - Hackeři se snaží napadnout cizí počítače.
 - Crackeri se zabývají prolamováním ochrany proti kopírování.
 - Útoky na náš počítač mohou mít formu odposlechu, změny dat, získání kontroly nad počítačem nebo útoku na dostupnost (zahlcení dotazy).
 - Proti útokům nás chrání pravidelné záplatování a osobní firewall.
9. **Důležité věci si zálohujeme** – zálohování slouží jako ochrana před úmyslným či neúmyslným smazáním důležitých dat.
 - Datům v počítači hrozí kromě útoků hackerů a virů také přírodní katastrofy, smazání uživatelem a zničení vadou počítačových komponent.
 - Jako ochrana proti těmto nepříjemnostem slouží vytváření záložních kopií především důležitých vlastnoručně vytvořených souborů - dokumentů.
 - K běžnému zálohování se v současnosti nejlépe hodí vypalování souborů na prepisovatelné cédéčko.
10. **Chraňme data** – počítačům a paměťovým médiím s uloženými daty hrozí fyzické zničení („vyšší moc“ – požár, povodeň, zemětřesení, nebo následek nechtěné či cílené činnosti) nebo krádež.
 - Pro ochranu proti těmto nebezpečím stačí dodržovat jednoduchá organizační pravidla.
 - Kromě zámků na dveřích hlídáme, kdo má k počítači a nosičům dat přístup.
 - Stoprocentně účinná ochrana je pro běžné situace příliš drahá, a tudíž zbytečná.

11. **Schovejme se za firewallem** – firewall ochrání náš počítač před útoky z internetu.
 - Firewall je počítač s nainstalovaným programem, který je zapojený někde mezi vnitřní firemní sítí a vnějším světem – internetem. Hlídá komunikaci z Internetu do firemní stě.
 - Pro ochranu jednotlivých počítačů slouží tzv. osobní firewall, nainstalovaný přímo v uživatelském počítači. Po celou dobu zapnutí počítače běží tento program v pozadí naší práce a hlídá, co se děje. Někdy bývá propojen s antivirovým programem.
 - Na začátku všechnu podezřelou komunikaci svého počítače zakážeme, teprve pokud přestanou fungovat některé programy, tak ji povolíme.
12. **Domluvme se se sousedy** – jestliže jeden počítač používá více uživatelů, zvolme si vůdce – správce a stanovme pravidla, protože jinak pořádek v počítači neudržíme.
 - Na počítači, který sdílí více osob, by měl pořádek udržovat jeden - správce.
 - Každý uživatel by měl mít vlastní uživatelský účet a domovský adresář.
 - Všechny změny nastavení a instalaci nových programů zajišťuje pouze správce.
13. **Přístupová práva chrání naše soubory před ostatními uživateli.**
 - Přístupová práva stanovují, co může uživatel s jednotlivými soubory dělat. Můžeme nastavit:
 - právo ke čtení
 - právo k zápisu
 - právo k mazání
 - právo ke spuštění programů
 - správcovské právo.
 - S pomocí přístupových práv můžeme dosáhnout toho, že se ostatní nedostanou k našim dokumentům.
 - Správně nastavena přístupová práva usnadňují používání jednoho počítače více lidmi.
14. **Tajná data šifrujeme** – šifrování ochrání data tak, že je nepřečte ani člověk, který nám např. ukradne počítač a prolomí heslo.
 - Z hlediska důvěrnosti dělíme data na:
 - **Veřejná data**, ke kterým se může dostat kdokoliv (většina programů, hudba, filmy, soubory stáhnuté z Internetu ...)
 - **Citlivá data**, ke kterým by se neměl dostat každý (údaje o členech domácnosti, rodinné fotografie ..). Pro tento účel chráníme počítač heslem.
 - **Důvěrná data**, která skrýváme i před ostatními lidmi, kteří mají přístup k našemu počítači. Ukládáme je do soukromého adresáře, ke kterému systém přístupových práv nikoho kromě nás nepustí.
 - **Tajná data** by neměl přečíst ani ten, kdo nám ukradne počítač, uhodne heslo a dostane se do soukromého adresáře (např. obchodní informace). Taková data šifrujeme.
 - Důvěrná data je vhodné šifrovat, používají se k tomu šifrovací programy a šifrovací klíč.
 - Pokud někomu posíláme zašifrovaný soubor, sdělíme mu šifrovací klíč jinou formou (např. telefonem).
 - Na Internetu najdeme řadu šifrovacích programů různého druhu. Asi nejznámější je program PGP, který najdeme na www.pgp.cz.

15. **Nikomu nemůžeme úplně věřit** – své heslo nikdy nikomu nesvěřujeme.
 - Neexistuje žádný důvod, proč by měl správce znát naše heslo.
 - Pokud někdo – kolega – potřebuje soubor z našeho počítače, může mu ho dát správce.
 - Hesla volíme rozumně a pečlivě je utajujeme.
16. **Odlišujeme zabezpečené weby** – heslo zadáváme pokud možno pouze do zabezpečených internetových stránek.
 - Nezabezpečené www stránky přenášejí po Internetu heslo v nezašifrované podobě, takže není těžké je odposlechnout.
 - Zabezpečení stránky heslo před odesláním zašifruje. Poznáme to podle symbolu malého zámečku.
 - Před zadáním hesla vždy zkontrolujeme adresu uvedenou v adresovém řádku.
 - Na obranu před nebezpečím podloudného získání hesla byl vyvinut SSL protokol. WWW stránky chráněné tímto protokolem mají v adrese místo http text https a ve stavovém řádku mají symbol zamčeného zámku.
17. **Víme, s kým se bavíme?** Pamatujme na to, že obsah e-mailu nemusel vytvořit člověk, který je pod ním podepsaný.
 - Není těžké podvrhnout adresu odesílatele nebo odeslat e-mail pod jeho jménem.
 - Pokud se nám obsah nějakého e-mailu nezdá, ověříme si ho jinou cestou přímo u podepsaného odesílatele.
 - Chceme-li mít stoprocentní jistotu, že nikdo nezneužije naši e-mailovou adresu, používáme u své pošty elektronický podpis.
18. **Stále jsme pod kontrolou** – naše práce s počítačem je neustále kontrolována.
 - Všechny důležité akce, které na počítači provedeme, se někde archivují.
 - Správce sítě dokáže dohledat, kdy jsme co provedli.
 - Pokud se chováme podle pravidel a hlídáme si svůj uživatelský účet, nic nám nehrozí.
19. **Nepropadejme panice** – pokud se počítač chová divně, zkusme pár věcí a potom volejme o pomoc.
 - Když se počítač začne chovat divně, zkusme spustit antivirový program, nic tím nepokazíme.
 - Pokud antivirový program nepomůže, zeptáme se kolegů, jestli na tom nejsou stejně.
 - Potom zkusíme pár jednoduchých kroků a požádáme o pomoc správce.
 - Co můžeme udělat sami:
 - Odstranit virus či spyware
 - Záplatovat počítač
 - Promluvit si s ostatními
 - Zkusit změnit heslo
 - Oinstalovat program.
20. **Vytvořme si zaručeně čistou bootovací disketu a pečlivě ji uložíme na bezpečné místo.**
 - Může nastat případ, že na počítači, který byl napaden virem, nelze spustit operační systém. Pomocí této diskety lze napadený počítač spustit a infikované soubory vyléčit či smazat.
 - Disketa obsahuje operační systém a podle možnosti také antivirový program.