

# OCHRANA DAT, POČÍTAČOVÁ BEZPEČNOST, POČÍTAČOVÉ VIRY



# OBSAH

- VÝZNAM OCHRANY DAT
- ZÁKLADNÍ TYPY INFILTRACÍ
- POČÍTAČOVÉ VIRY
- ANTIVIROVÉ PROGRAMY
- SPAM
- PŘEHLED PRAVIDEL BEZPEČNOSTI

# VÝZNAM OCHRANY DAT



# VÝZNAM OCHRANY DAT

- **V SOUČASNÉ DOBĚ MÁ MNOHO JEDNOTLIVCŮ A HLAVNĚ FIREM VĚTŠINU SVÝCH DAT ULOŽENÝCH VE FORMĚ POČÍTAČOVÝCH SOUBORŮ A VĚTŠINA Z NICH JE JEŠTĚ PŘIPOJENA K PONĚKUD NEBEZPEČNÉMU INTERNETU. PROTO JE PROBLEMATIKA OCHRANY DAT TAK DŮLEŽITÁ A ZÁVAŽNÁ A MŮŽEME JI PODLE MOŽNÉHO OHROŽENÍ ZHRUBA ROZDĚLIT DO DVOU OBLASTÍ:**

# VÝZNAM OCHRANY DAT

- **ZNEUŽITÍ DAT CIZÍ OSOBOU – MŮŽEME MU ZABRÁNIT ZABEZPEČENÍM POČÍTAČE A DAT.**
- **ZTRÁTA DAT (TECHNICKÝM SELHÁNÍM POČÍTAČE, PŮSOBENÍM POČÍTAČOVÝCH VIRŮ, CHYBOU OBSLUHY APOD.). TADY JE ZÁKLADNÍ OCHRANOU ZÁLOHOVÁNÍ DAT.**

# VÝZNAM OCHRANY DAT

## ZABEZPEČENÍ PC A DAT PŘED ZNEUŽITÍM

- MÍSTNOST S POČÍTAČEM CHRÁNIT PŘED VNIKNUTÍM NEPOVOLANÉ OSOBY  
BEZPEČNOSTNÍMI PRVKY – KVALITNÍ DVEŘE, ZÁMKY, FÓLIE, MŘÍŽE NA OKNA. TENTO ZPŮSOB JE JEDNODUCHÝ ALE ÚČINNÝ A BEZPEČNÝ. MÉNĚ BEZPEČNOU VARIANTOU JE UZAMČENÍ POČÍTAČE VE STOLE.

# VÝZNAM OCHRANY DAT

## ZABEZPEČENÍ PC A DAT PŘED ZNEUŽITÍM

- **VÁZAT SPUŠTĚNÍ POČÍTAČE (START OPERAČNÍHO SYSTÉMU) NA HESLO. JE TO POMĚRNĚ ÚČINNÁ OCHRANA, HESLO SE VŠAK DÁ UHODNOUT NEBO ODPOZOROVAT PŘI ZADÁVÁNÍ. HESLO NÁS NEOCHRÁNÍ NAPŘ. PŘED KRÁDEŽÍ CELÉHO POČÍTAČE – HESLO LZE VYMAZAT A K DATŮM SE DOSTAT.**

# VÝZNAM OCHRANY DAT

## ZABEZPEČENÍ PC A DAT PŘED ZNEUŽITÍM

- **POUŽÍT K POČÍTAČI SPECIÁLNÍ PŘÍDAVNÉ ZAŘÍZENÍ, DO KTERÉHO JE PRO SPUŠTĚNÍ SYSTÉMU NUTNÉ VLOŽIT IDENTIFIKAČNÍ KARTU. ODPADÁ NUTNOST PAMATOVAT SI HESLO. JE TO VELMI DOBRÉ ZABEZPEČENÍ POČÍTAČE. JEŠTĚ MODERNĚJŠÍ JE POUŽITÍ OTISKŮ PRSTŮ.**

# VÝZNAM OCHRANY DAT

## ZABEZPEČENÍ PC A DAT PŘED ZNEUŽITÍM

- MŮŽE SE STÁT, I ŽE PŘES VÝŠE UVEDENA OPATŘENÍ SE NĚKDO K NAŠEMU POČÍTAČI DOSTANE, NEBO HO ODCIZÍ. DÁ SE I V TĚCHTO PŘÍPADECH ZABRÁNIT ZNEUŽITÍ DAT?

# VÝZNAM OCHRANY DAT

## ZABEZPEČENÍ DŮVĚRNOSTI DAT

- **OPERAČNÍ SYSTÉMY PŘI STARTU POČÍTAČE VYŽADUJÍ ZADÁNÍ JMÉNA UŽIVATELE A HESLO, BEZ KTERÉHO NEPOVOLÍ PRÁCI. NEJLEPŠÍ SYSTÉMY DATA PŘI UKLÁDÁNÍ NA DISK ŠIFRUJÍ. PŘI PRÁCI V SÍTI KLIENT-SERVER JSOU DATA POUZE NA DISKU SERVERU, OCHRANA DAT NA JEDNOTLIVÝCH STANICÍCH SE NEMUŠÍ ŘEŠIT, JE POTŘEBNÉ DŮSLEDNĚ ZABEZPEČIT PŘÍSTUP K SERVERU.**

# VÝZNAM OCHRANY DAT

## ZABEZPEČENÍ DŮVĚRNOSTI DAT

- **SOFTWAREOVÁ OCHRANA POČÍTAČE.** EXISTUJÍ SPECIÁLNÍ PROGRAMY, KTERÉ SE STÁVAJÍ SOUČÁSTÍ OPERAČNÍHO SYSTÉMU A ŠIFRUJÍ VEŠKERÉ ZÁPISY NA DISK A ČTENÍ Z NĚHO DEŠIFRUJÍ. OPRÁVNĚNÝ UŽIVATEL SE OPĚT MUSÍ PROKÁZAT HESLEM, BEZ KTERÉHO OBSAH DISKU NELZE ČÍST. HESLO (KÓD NA DEŠIFROVÁNÍ) MŮŽE BÝT ULOŽENO NA EXTERNÍM ZARÍZENÍ - TOKENU (NAPŘ. USB DISK) A V TOMTO PŘÍPADĚ MŮŽE BÝT I DOST DLOUHÉ (NAPŘ. 128 ZNAKŮ).

# VÝZNAM OCHRANY DAT

## ZABEZPEČENÍ DŮVĚRNOSTI DAT

- **HARDWAROVÁ OCHRANA POČÍTAČE. PATŘÍ SEM BEZPEČNOSTNÍ KARTY DO POČÍTAČE, KTERÉ JSOU VELMI SPOLEHLIVÉ. BEZ ZNALOSTI HESLA SE S POČÍTAČEM NEDÁ PRACOVAT A JEHO OBSAH JE POUZE ZMĚTÍ NUL A JEDNIČEK.**

# VÝZNAM OCHRANY DAT

## ZÁLOHOVÁNÍ DAT

- PORUCHA POČÍTAČE, CHYBA OBSLUHY NEBO INFEKCE POČÍTAČOVÝMI VIRY MAJÍ STEJNÉ ÚČINKY – POŠKOZENÍ NEBO ÚPLNÉ ZNIČENÍ DAT ULOŽENÝCH NA PEVNÉM DISKU. PROTOŽE MAJÍ SPOLEČNÝ ÚČINEK, MAJÍ I SPOLEČNÝ ZÁKLADNÍ ZPŮSOB OCHRANY – ZÁLOHOVÁNÍ DAT.

# VÝZNAM OCHRANY DAT

## ZÁLOHOVÁNÍ DAT

- **ZÁLOHOVÁNÍ (ARCHIVACE) DAT JE JEJICH ZKOPÍROVÁNÍ Z PEVNÉHO DISKU NA JINÉ ZÁZNAMOVÉ MÉDIUM. NEJČASTĚJI TO MŮŽE BÝT:**

# VÝZNAM OCHRANY DAT

## ZÁLOHOVÁNÍ DAT

- **PEVNÝ DISK POČÍTAČE: VYTVÁŘÍME PROSTÉ NEBO KOMPRIMOVANÉ (ZIP) KOPIE DŮLEŽITÝCH SLOŽEK. KOMPRIMOVANÁ ZÁLOHA JE VÝHODNĚJŠÍ – JE ODDĚLENA FORMÁTEM A ŠETŘÍ MÍSTO NA DISKU. ZÁLOHA NA STEJNÉM DISKU, KDE JSOU I CHRÁNĚNÁ DATA CHRÁNÍ PŘED VLASTNÍ CHYBOU UŽIVATELE (SMAZÁNÍ) ALE NECHRÁNÍ PŘED ZNIČENÍM DAT NA CELÉM DISKU.**

# VÝZNAM OCHRANY DAT

## ZÁLOHOVÁNÍ DAT

- **ZAPISOVATELNÉ CD (700 MB) A DVD DISKY (4,7 – 17 GB). PŘI POUŽITÍ JEDNORÁZOVÝCH ZAPISOVATELNÝCH MÉDIÍ JDE O DLOUHODOBOU ZÁLOHU A TENTO ZPŮSOB POUŽÍVÁME NAPŘ. PO DOKONČENÍ ZAKÁZKY APOD. CD DISKY JSOU POVAŽOVÁNY ZA VÝRAZNĚ TRVANLIVĚJŠÍ.**



# VÝZNAM OCHRANY DAT

## ZÁLOHOVÁNÍ DAT

- **USB DISKY (128 MB – NĚKOLIK GB). ZÁLOHA SE PROVEDE VELICE RYCHLE, JE TO ZPŮSOB VHODNÝ PRO OKAMŽITÉ ZÁLOHOVÁNÍ JEŠTĚ PŘED UZAVŘENÍM PRÁCE.**
- **SERVERY SÍTÍ ZÁLOHUJÍ SVŮJ OBSAH VĚTŠINOU NA PÁSKY S KAPACITOU AŽ STOVEK GB.**



# VÝZNAM OCHRANY DAT

## ZÁLOHOVÁNÍ DAT

- **EXTERNÍ PEVNÉ DISKY – PŘIPOJUJÍ SE PŘES USB ROZHRANÍ A JSOU TO BĚŽNÉ, KAPACITNĚ VĚTŠINOU MENŠÍ DISKY, DOPLNĚNÉ O ŘÍDÍCÍ ELEKTRONIKU. JSOU VHODNÉ PRO ZÁLOHOVÁNÍ CELÝCH DISKŮ NEBO DISKOVÝCH ODDÍLŮ. ZÁLOZE SE V TOMTO PŘÍPADĚ ŘÍKÁ OBRAZ (IMAGE) DISKU.**



# VÝZNAM OCHRANY DAT

## ZÁLOHOVÁNÍ DAT

- **KLASICKÉ 3,5" DISKETY JSOU PRO SVOJI MALOU KAPACITU A NÍZKOU TRVANLIVOST ZÁZNAMU PRO ZÁLOHOVÁNÍ DAT ZCELA NEVHODNÉ A POUŽÍVÁME JE POUZE V PŘÍPADĚ NOUZE.**

# VÝZNAM OCHRANY DAT

## ZÁLOHOVÁNÍ DAT - PRAVIDLA

- **ZÁLOHOVÁNÍ PROVÁDÍME ČASTO, PRAVIDELNĚ, PEČLIVĚ A NA KVALITNÍ ZÁZNAMOVÁ MÉDIA.**
- **ČASTO. PŘI PORUŠE POČÍTAČE JE NOVÁ PRÁCE OD ARCHIVACE DO PORUCHY ZTRACENA. PROTO SE DOPORUČUJE PROVÁDĚT ARCHIVACI DŮLEŽITÝCH DAT KAŽDÝ DEN NEBO ALESPON POKAŽDÉ, KDY BYLO ZAZNAMENÁNO VELKÉ MNOŽSTVÍ DAT.**

# VÝZNAM OCHRANY DAT

## ZÁLOHOVÁNÍ DAT - PRAVIDLA

- **PRAVIDELNĚ. CO SE NEDĚLÁ PRAVIDELNĚ, ZPRAVIDLA SE NA TO ZAPOMENE.**
- **PEČLIVĚ. VŽDY JE POTŘEBNÉ ZÁLOHOVAT NOVÁ DATA A VEŠKEROU HOTOVOU PRÁCI, POMÁHAJÍ S TÍM I SPECIALIZOVANÉ PROGRAMY, KTERÉ UMÍ KROMĚ DOKUMENTŮ ZÁLOHOVAT I E-MAILOVÉ ZPRÁVY, ADRESÁŘ, OBLÍBENÉ POLOŽKY, NASTAVENÍ SYSTÉMU APOD.**

# VÝZNAM OCHRANY DAT

## ZÁLOHOVÁNÍ DAT - PRAVIDLA

- **KVALITNÍ ZÁZNAMOVÁ MÉDIA.**  
ZNAČKOVÍ VÝROBCI UVÁDĚJÍ STUDIE TRVANLIVOSTI DAT A POSKYTUJÍ VYŠŠÍ ZÁRUKU OBNOVENÍ DAT NEŽ NEZNAČKOVÁ MÉDIA.

# VÝZNAM OCHRANY DAT

## MOŽNÉ ZPŮSOBY ZNIČENÍ DAT

- **TECHNICKÁ PORUCHA PEVNÉHO DISKU. JE POMĚRNĚ NEPRAVDĚPODOBŇÁ. MODERNÍ DISKY JSOU VELMI SPOLEHLIVÉ, ALE MŮŽE K NÍ DOJÍT. ČASTĚJŠÍ NEŽ SAMOVOLNÁ PORUCHA JE ZNIČENÍ DISKU PŘEPĚTÍM.**

# VÝZNAM OCHRANY DAT

## MOŽNÉ ZPŮSOBY ZNIČENÍ DAT

- **PORUŠENÍ DAT NA DISKU VÝPADKEM NAPÁJENÍ POČÍTAČE. K PORUŠENÍ DAT DOCHÁZÍ POUZE V PŘÍPADĚ, KDY V MOMENTĚ VÝPADKU PROUDU POČÍTAČ ZAPISUJE NA DISK. TEHDY MŮŽE DOJÍT K PORUŠENÍ STRUKTURY DATOVÝCH SOUBORŮ A NUTNOSTI JEJICH OBNOVY Z ARCHIVU.**

# VÝZNAM OCHRANY DAT

## MOŽNÉ ZPŮSOBY ZNIČENÍ DAT

- VÝPADKŮM NAPÁJENÍ A PŘEPĚTÍ MŮŽEME PŘEDEJÍT POUŽÍVÁNÍM UPS – ZDROJE NEPŘETRŽITÉHO NAPÁJENÍ (ZÁLOŽNÍ ZDROJ). TENTO PŘÍSTROJ SE ZAPOJÍ MEZI ZÁSUVKU 230 V A NAPÁJECÍ KABEL POČÍTAČE. PŘI VÝPADKU SÍTĚ 230 V ZAČNE UPS NAPÁJET POČÍTAČ ZE SVÉ BATERIE A UPOZORNÍ NA TO ZVUKOVÝM SIGNÁLEM. BĚŽNÉ UPS MOHOU NAPÁJET POČÍTAČ I 15 MINUT, COŽ STAČÍ NA ULOŽENÍ DAT, UKONČENÍ PRÁCE PROGRAMŮ A VYPNUTÍ POČÍTAČE.

# VÝZNAM OCHRANY DAT

## MOŽNÉ ZPŮSOBY ZNIČENÍ DAT

- **SMAZÁNÍ DŮLEŽITÝCH DAT CHYBOU (OMYLEM) UŽIVATELE. POKUD JSOU DATA VYHOZENA DO KOŠE OPERAČNÍHO SYSTÉMU, LZE JE ODTUD BEZ PROBLÉMU OBNOVIT. POKUD JE KOŠ VYSYPÁN, JDE O HORŠÍ PŘÍPAD, ALE JEŠTĚ TU JE ŠANCE NA OBNOVU DAT, POKUD SI TO UVĚDOMÍME HNED. JE POTŘEBA IHNEK UKONČIT PRÁCI NA POČÍTAČI A POŽÁDAT NĚKOHO KOMPETENTNÍHO O POMOC. PŘI VYSYPÁNÍ KOŠE TOTIŽ SYSTÉM SOUBORY FYZICKY NEMAŽE, POUZE OZNAČÍ MÍSTO, KDE BYLY, JAKO VOLNÉ. KDYBYCHOM PO VYMAZÁNÍ NĚCO NA DISK ULOŽILI, MOHLO BY SE TO ULOŽIT PŘÁVĚ DO TOHOTO UVOLNĚNÉHO MÍSTA.**

# VÝZNAM OCHRANY DAT

## MOŽNÉ ZPŮSOBY ZNIČENÍ DAT

- **SMAZÁNÍ NEBO PORUŠENÍ DAT NA DISKU PŮSOBENÍM POČÍTAČOVÉHO VIRU. PROBLEMATIKA POČÍTAČOVÝCH VIRŮ JE PODROBNĚ ROZEBRÁNA V SAMOSTATNÉ KAPITOLE.**

# VÝZNAM OCHRANY DAT

## NEBEZPEČÍ Z INTERNETU

- **OVLÁDNUTÍ POČÍTAČE. PROGRAM TYPU BACKDOOR (ZADNÍ VRÁTKA) OTEVŘE NĚKTERÉ PORTY POČÍTAČE A NASLOUCHÁ NA NICH POVELŮM ZVENČÍ. PODOBNĚ PRACUJE PROGRAM TYPU TROJSKÝ KŮŇ, KTERÝ KROMĚ SVÉ ZJEVNÉ ČINNOSTI VYKONÁVÁ JEŠTĚ NIKDE NEUVEDENÉ ČINNOSTI BEZ SOUHLASU UŽIVATELE. UMOŽNÍ TAK ÚTOČNÍKOVI PŘÍSTUP DO POČÍTAČE A PRÁCI S NÍM.**

# VÝZNAM OCHRANY DAT

## NEBEZPEČÍ Z INTERNETU

- **ODCIZENÍ OBSAHU POČÍTAČE. VZDÁLENÝ ÚTOČNÍK MŮŽE DÍKY ZÍSKANÉMU PŘÍSTUPU KOPÍROVAT SOUBORY Z NAPADENÉHO POČÍTAČE, NEBO POUŽÍT PROGRAM KEYLOGGER KE SLEDOVÁNÍ STISKNUTÝCH KLÁVES (NAPŘ. PŘI VYPLŇOVÁNÍ POLÍČEK VE FORMULÁŘÍCH), NEBO DATAMINDER – PROGRAM, KTERÝ SHROMAŽDUJE DATA O ČINNOSTI POČÍTAČE.**

# VÝZNAM OCHRANY DAT

## NEBEZPEČÍ Z INTERNETU

- **VYUŽITÍ POČÍTAČE PRO NELEGÁLNÍ ČINNOST. MNOHO ZÁSAHŮ POLICIE PROTI ROZESÍLATELŮM SPAMU NEBO PROTI SERVERŮM S NELEGÁLNÍM OBSAHEM SKONČÍ U NIC NETUŠÍCÍHO UŽIVATELE POČÍTAČE, KTERÝ O JEHO NELEGÁLNÍ FUNKCI NEMĚL ANI ZDÁNÍ. VZDÁLENÝ ÚTOČNÍK PŘEMĚNIL NEZABEZPEČENÝ POČÍTAČ NA SERVER ROZESÍLAJÍCÍ SPAM NEBO POSKYTUJÍCÍ ZMÍNĚNÉ STRÁNKY.**

# VÝZNAM OCHRANY DAT

## NEBEZPEČÍ Z INTERNETU

- **UKRADENÍ (ZNEUŽITÍ) IDENTITY.** TYPICKÝM PŘÍKLADEM JE TZV. PHISHING. ÚTOČNÍK ROZEŠLE PODVODNÉ E-MAILY NAPODOBUJÍCÍ NAPŘ. STYL ZNÁMÉ BANKY A VYZÝVAJÍCÍ ADRESÁTA Z NEJ-RŮZNĚJŠÍCH DŮVODŮ KE KONTROLE ÚČTU. PO KLEPNUTÍ NA ODKAZ SE ZOBRAZÍ STRÁNKY PODOBNÉ ORIGINÁLNÍ WEB BANCE. PO ZADÁNÍ PŘIHLAŠOVACÍHO JMÉNA A HESLA (ČÍSLO PĚTEBNÍ KARTY) SE VYKONÁ ZDANLIVĚ SLIBOVANÁ AKCE, VE SKUTEČNOSTI JSOU VŠAK TATO DATA ODESLÁNA ÚTOČNÍKOVI.

# VÝZNAM OCHRANY DAT

## NEBEZPEČÍ Z INTERNETU

- INTERNET NEMÁ ŽÁDNOU CENTRÁLU, ŽÁDNÉHO SPRÁVCE, ZA JEHO OBSAH JAKO CELEK NIKDO NEODPOVÍDÁ. JE VŽDY NA UŽIVATELI, ABY POSOUDIL INFORMAČNÍ HODNOTU PŘEDKLÁDANÝCH INFORMACÍ A ROZLIŠIL PRAVDIVÉ, NEPŘESNÉ, NEÚPLNÉ, ZAVÁDĚJÍCÍ A ÚMYSLNĚ NEPRAVDIVÉ INFORMACE.

# VÝZNAM OCHRANY DAT

## NEBEZPEČÍ Z INTERNETU

- DALŠÍ KOMPLIKACÍ JE OBTÍŽNOST APLIKACE ZÁKONŮ NA PODNIKÁNÍ NEBO ZLOČINNOU ČINNOST POMOCÍ INTERNETU. V BĚŽNÉM PRÁVNÍM ŘÁDU PLATÍ, ŽE K POSOUZENÍ TRESTNOSTI SE POUŽÍVAJÍ ZÁKONY ZEMĚ, VE KTERÉ KE ZLOČINU DOŠLO. JAK ALE POSOUDIT ZLOČINY, KTERÉ POSTIHLY OBČANY NAŠÍ ZEMĚ PROVEDENÉ OBČANY JINÉ ZEMĚ S VYUŽITÍM POČÍTAČŮ (DOMÉN, ADRES) REGISTROVANÝCH VE TŘETÍ ZEMI?

# VÝZNAM OCHRANY DAT

## NEBEZPEČÍ Z INTERNETU

- **PROSAZUJE SE NÁZOR, ŽE ZA OBSAH STRÁNEK ODPOVÍDÁ JEJICH AUTOR A NIKOLIV POSKYTOVATEL PŘIPOJENÍ A DATOVÉHO PROSTORU, KTERÝ O NELEGÁLNÍM OBSAHU NEMUSÍ VĚDĚT. OVŠEM POKUD JE POSKYTOVATEL NA NELEGÁLNÍ OBSAH STRÁNEK UPOZORNĚN, JE POVINEN JI ODSTRANIT.**



# VÝZNAM OCHRANY DAT

## NEBEZPEČÍ Z INTERNETU – PODVODNÉ SOCIOTECHNIKY

- **NAPROSTÁ VĚTŠINA VÝŠE UVEDENÝCH NEBEZPEČNÝCH KÓDŮ VYŽADUJE SOUČINNOST UŽIVATELE NAPADENÉHO POČÍTAČE, ZBYTEK JE NEOPATRNOT NEBO NEDBALOST – NAINSTALUJEME SI ZÁVADNÉ PROGRAMY, ZADÁME SVÁ PŘIHLAŠOVACÍ JMÉNA A HESLA DO PODVODNÝCH FORMULÁŘŮ APOD. ÚTOKY TOHOTO TYPU SE NAZÝVAJÍ SOCIOTECHNICKÉ ÚTOKY.**

# VÝZNAM OCHRANY DAT

## NEBEZPEČÍ Z INTERNETU – PODVODNÉ SOCIOTECHNIKY

- ODBORNÍCI ČASTO KONSTATUJÍ, ŽE „NEJVĚTŠÍ BEZPEČNOSTNÍ PROBLÉM JE MEZI ŽIDLÍ A KLÁVESNICÍ“, TEDY V ČLOVĚKU, KTERÝ POČÍTAČ OBSLUHUJE. ÚTOKY VEDENÉ TÍMTO ZPŮSOBEM VYCHÁZEJÍ ZE ZNALOSTI PSYCHOLOGIE ČLOVĚKA, A NEZNALÝ ČLOVĚK JIM MŮŽE SNADNO PODLEHNOUT BEZ OHLEDU NA SVOJE VZDĚLÁNÍ.

# VÝZNAM OCHRANY DAT

## NEBEZPEČÍ Z INTERNETU – PODVODNÉ SOCIOTECHNIKY

- ZÁKLADNÍ OBRANOU PROTI TĚMTO TECHNIKÁM JE VĚDĚT O JEJICH EXISTENCI A UVĚDOMOVAT SI SKUTEČNOST, ŽE INTERNET JE POTENCIÁLNĚ NEBEZPEČNÉ PROSTŘEDÍ, KTERÉ MŮŽE PŘIVÉST ÚTOČNÍKA KDYKOLIV A KDEKOLIV. NENÍ TŘEBA BÝT CHOROBNĚ PODEZÍRAVÝ, ALE NEBEZPEČÍ REÁLNĚ EXISTUJE A JE TŘEBA O NĚM VĚDĚT.

# VÝZNAM OCHRANY DAT

## NEBEZPEČÍ Z INTERNETU – PODVODNÉ SOCIOTECHNIKY

- **ÚTOČNÍCI NEJČASTĚJI POUŽÍVAJÍ TYTO SOCIOTECHNICKÉ METODY:**
  - **NABÍZEJÍ ZDARMA EROTICKÝ, PORNOGRAFICKÝ NEBO TAJNÝ OBSAH (FOTOGRAFIE CELEBRIT, ...).**
  - **NABÍZEJÍ VELKÝ FINANČNÍ ZISK PŘI MINIMÁLNÍM ÚSILÍ.**
  - **HRAJÍ NA CITY ADRESÁTA (ZÁCHRANA NEMOCNÉHO ČLOVĚKA, ...).**

# VÝZNAM OCHRANY DAT

## NEBEZPEČÍ Z INTERNETU – PODVODNÉ SOCIOTECHNIKY

- **ÚTOČNÍCI NEJČASTĚJI POUŽÍVAJÍ TYTO SOCIOTECHNICKÉ METODY:**
  - **VZBUZUJÍ STRACH („POKUD OKAMŽITĚ NEUČINÍTE OPATŘENÍ ... MŮŽE DOJÍT K VÁŽNÝM DŮSLEDKŮM“ – NAPŘ. KONTROLU SVÉHO BANKOVNÍHO ÚČTU).**
  - **NUTÍ JEDNAT OKAMŽITĚ NEDÁVAJÍ ČAS NA ROZMYŠLENOU („POKUD OKAMŽITĚ NENAINSTALUJETE TENTO PROGRAM, OBSAH DISKU POČÍTAČE BUDE VYMAZÁN...“).**

# VÝZNAM OCHRANY DAT

## NEBEZPEČÍ Z INTERNETU – PODVODNÉ SOCIOTECHNIKY

- **ÚTOČNÍCI NEJČASTĚJI POUŽÍVAJÍ TYTO SOCIOTECHNICKÉ METODY:**
  - **TVÁŘÍ SE DŮVĚRNĚ („PŘÍTEL TI VĚNOVAL PÍSEŇ, KLIKNI SEM A POSLECHNI SI JI...“).**
  - **MNOHÉ DALŠÍ METODY, KTERÉ VĚTŠINOU KOMBINUJÍ TY VÝŠE UVEDENÉ.**



# VÝZNAM OCHRANY DAT

**BEZPEČNOST POČÍTAČE TEDY SPOČÍVÁ V TECHNICKÝCH A OGRANIZAČNÍCH OPATŘENÍCH:**

- **ZÁKLADEM TECHNICKÝCH OPATŘENÍ JE UDRŽOVÁNÍ OPERAČNÍHO SYSTÉMU V AKTUÁLNÍM STAVU OKAMŽITOU (NEJLÉPE AUTOMATICKOU) INSTALACÍ BEZPEČNOSTNÍCH ZÁPLAT, ZAPNUTÝ A SPRÁVNĚ NASTAVENÝ FIREWALL A FUNKČNÍ A NEJLÉPE KAŽDÝ DEN AKTU-ALIZOVANÝ ANTIVIROVÝ PROGRAM.**

# VÝZNAM OCHRANY DAT

**BEZPEČNOST POČÍTAČE TEDY SPOČÍVÁ V TECHNICKÝCH A ORGANIZAČNÍCH OPATŘENÍCH:**

- **ORGANIZAČNÍ OPATŘENÍ STOJÍ NA ZNALOSTECH BEZPEČNOSTNÍCH HROZEB A NA OPATRNOSTI. VE FIRMÁCH A JINÝCH INSTITUCÍCH JSOU URČENA PŘÍSTUPOVÁ PRÁVA UŽIVATELŮ A STANOVENY SMĚRNICE, KTERÝMI SE MUSÍ ŘÍDIT – KOMU MOHOU A NEMOHOU POSKYTOVAT INFORMACE A JAKÉ, JAK SE NAKLÁDÁ S PÍSEMNOSTMI (VČETNĚ ZPŮSOBU SKARTOVÁNÍ).**

# VÝZNAM OCHRANY DAT

**BEZPEČNOST POČÍTAČE TEDY SPOČÍVÁ V  
TECHNICKÝCH A OGRANIZAČNÍCH  
OPATŘENÍCH:**

- **ORGANIZAČNÍ OPATŘENÍ -  
BEZPEČNOSTNÍM OPATŘENÍM JE I  
POUŽÍVÁNÍ JINÉHO NEŽ  
DOMINANTNÍHO SOFTWARE, ÚTOKY  
JSOU TOTIŽ VĚTŠINOU VEDENY PROTI  
NEJROZŠÍŘENĚJŠÍM APLIKACÍM.**

# VÝZNAM OCHRANY DAT

## BEZPEČNÁ KOMUNIKACE PO INTERNETU

- INTERNET JE NESMÍRNĚ VÝKONNÉ, ALE POTENCIÁLNĚ NEBEZPEČNÉ PROSTŘEDÍ PRO PŘENOS ZPRÁV. PŮVODNÍ PROTOKOL TCP/IP NEOBSAHOVAL ŽÁDNÉ BEZPEČNOSTNÍ PRVKY. PRIORITOU BYLO DORUČENÍ PAKETU DAT JAKÝMKOLIV ZPŮSOBEM K CÍLOVÉMU POČÍTAČI. BRZY SE PROJEVILA NUTNOST ŘEŠIT BEZPEČNOST PŘENOSU DAT NAD ÚROVNÍ TOHOTO PROTOKOLU, ABY BYL BEZPEČNÝ NEJENOM SAMOTNÝ POČÍTAČ, ALE I PŘENOS DAT.

# VÝZNAM OCHRANY DAT

## BEZPEČNÁ KOMUNIKACE PO INTERNETU

- **KLASICKÝ PŘENOS DAT PŘES INTERNET JE LEHCE ODPOSLOUCHATELNÝ, NEMŮŽEME MÍT JISTOTU, ŽE DATA DOŠLA V POŘÁDKU, ŽE JE NIKDO NEČETL A JISTÉ NENÍ ANI TO, ŽE KOMUNIKUJETE S TÍM, KOMU BYLA DATA URČENA. PROTO BYLY VYVINUTY RŮZNÉ BEZPEČNOSTNÍ PRVKY, KTERÉ SE ZAMĚŘUJÍ NA TYTO OBLASTI:**

# VÝZNAM OCHRANY DAT

## BEZPEČNÁ KOMUNIKACE PO INTERNETU

- **INTEGRITA DAT. ZARUČUJE, ŽE SE DATA BĚHEM PŘENOSU NEZMĚNILA.**
- **DŮVĚRNOST DAT. POŽADUJE, ABY K DATŮM MĚLI PŘÍSTUP POUZE UŽIVATELÉ, KTEŘÍ K TOMU MAJÍ OPRÁVNĚNÍ (AUTORIZACI).**

# VÝZNAM OCHRANY DAT

## BEZPEČNÁ KOMUNIKACE PO INTERNETU

- **AUTENTICITA. ZARUČUJE IDENTIFIKACI KOMUNIKUJÍCÍCH A DÁVÁ JISTOTU, ŽE KOMUNIKUJÍCÍ STRANY JSOU TY, ZA KTERÉ SE VYDÁVAJÍ.**
- **DATOVÁNÍ A ČASOVÁNÍ. UMOŽŇUJE URČIT PŘESNÝ OKAMŽIK VZNIKU NEBO DORUČENÍ ZPRÁVY.**

# VÝZNAM OCHRANY DAT

## BEZPEČNÁ KOMUNIKACE PO INTERNETU

- NEJČASTĚJŠÍM PROSTŘEDKEM BEZPEČNÉ WEBOVÉ KOMUNIKACE JE ZABEZPEČENÉ SPOJENÍ POMOCÍ PROTOKOLU HTTPS (S JAKO SECURITY). TO UMOŽŇUJE ŠIFROVANOU KOMUNIKACI MEZI WEBOVÝM SERVEREM A PROHLÍŽEČEM.

# VÝZNAM OCHRANY DAT

## BEZPEČNÁ KOMUNIKACE PO INTERNETU

- V SOUČASNOSTI POUŽÍVANÉ 128BITOVÉ ŠIFROVÁNÍ SSL (SECURE SOCKETS LAYER) POSKYTUJE VYSOKOU ÚROVEŇ ZABEZPEČENÍ. PROHLÍŽEČ WEBU VŽDY UKAZUJE POUŽITÍ BEZPEČNÉ KOMUNIKACE – IKONOU ZÁMEČKU, ZMĚNOU BARVY POLÍČKA ADRESA. PROTOKOL HTTPS POUŽÍVÁ PRINCIP KOMBINACE ASYMETRICKÉ A SYMETRICKÉ KRYPTOGRAFIE.

# VÝZNAM OCHRANY DAT

## PROBLEMATIKA HESEL

- **SILNÉ HESLO OBSAHUJE MINIMÁLNĚ 6 ZNAKŮ, NEMÁ DÁVAT ŽÁDNÝ SMYSL V ŽÁDNÉM BĚŽNÉM JAZYKU, OBSAHUJE VELKÁ I MALÁ PÍSMENA I ČÍSLICE A NEJLÉPE I DALŠÍ ZNAKY. VYTVOŘÍME HO NAPŘ. TAK, ŽE SI PRO SEBE ŘEKNEME DOBŘE ZAPAMATOVATELNOU FRÁZI, NEBO VĚTU A Z PRVNÍCH PÍSMEN JEDNOTLIVÝCH SLOV SESTAVÍME HESLO.**

# VÝZNAM OCHRANY DAT

## PROBLEMATIKA HESEL

- HESLO BY NEMĚLO OBSAHOVAT PÍSMENA S DIAKRITIKOU A MEZERY. NAPŘ. MŮJ NEOBLÍBENĚJŠÍ HEREC JE DUSTIN HOFFMANN, KTERÉMU JE 65 LET – HESLO BUDE **mnhjDHkj65l**.

# VÝZNAM OCHRANY DAT

## PROBLEMATIKA HESEL

- **HESLO MŮŽE BÝT ODCIZENO:**
  - **SOCIOTECHNICKÝMI PROSTŘEDKY –**  
**PODVODEM ZJIŠTĚNO OD UŽIVATELE,**
  - **VYUŽITÍM NEOPATRNOTI UŽIVATELE**  
**(NALEZENÍ HESLA NAPSANÉHO NA**  
**PŘÍSTUPNÉM MÍSTĚ),**
  - **POMOCÍ KEYLOGGERU (PROGRAM NA**  
**SLEDOVÁNÍ STISKNUTÝCH KLÁVES).**

# VÝZNAM OCHRANY DAT

## PROBLEMATIKA HESEL

- **K INFORMACÍM ZABEZPEČENÝM HESLEM SE ÚTOČNÍCI POKOUŠEJÍ DOSTAT I POMOCÍ KLASICKÝCH PROGRAMOVÝCH PROSTŘEDKŮ:**
  - **HRUBOU SILOU**
  - **SLOVNÍKOVÝ ÚTOK**
  - **STEJNÁ HESLA**

# ZÁKLADNÍ TYPY INFILTRACÍ



# ZÁKLADNÍ TYPY INFILTRACÍ

- POČÍTAČOVÝ VIR
- ČERV (WORM)
- TROJSKÝ KŮŇ
- ŽERTOVNÝ PROGRAM
- HOAX

# 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.**

# POČÍTAČOVÝ VIR

- KROMĚ SAMOTNÉ REPRODUKCE MŮŽE PŘITOM KÓD VIRU VYKONÁVAT RŮZNÉ GRAFICKÉ, ZVUKOVÉ A TEXTOVÉ EFEKTY, ALE I DESTRUKČNÍ ČINNOST – MAZÁNÍ, KÓDOVÁNÍ A JINÉ MODIFIKACE V UŽIVATELSKÉM POČÍTAČI.



# POČÍTAČOVÝ VIR

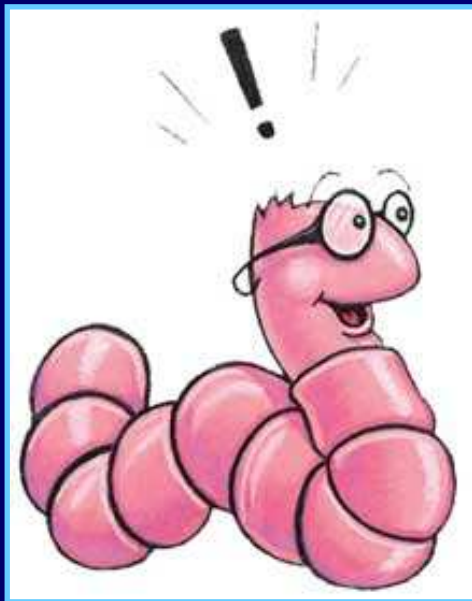
- S VÝJIMKOU MOŽNOSTI VYMAZÁNÍ FLASH BIOS PAMĚTI V SOUČASNOSTI NEJSOU ZNÁMY VIRY POŠKOZUJÍCÍ HARDWARE POČÍTAČE.
- NĚKTERÉ VIRY PODOBNĚ JAKO DÁLE ZMÍ-  
NĚNÉ TROJSKÉ KONĚ NARUŠUJÍ BEZPEČ-  
NOST POČÍTAČE A ÚDAJŮ NA PEVNÉM  
DISKU ZASÍLÁNÍM TAJNÝCH ŠIFROVA-  
CÍCH KLÍČŮ, ODCHYCENÝCH HESEL A E-  
MAILOVÝCH ADRES ATD. RŮZNÝMI KOMU-  
NIKAČNÍMI KANÁLY MIMO NAPADENÝ  
POČÍTAČ (NAPŘ. AUTOROVÍ VIRU).

# 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.

# ČERV (WORM)

- **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**



# TROJSKÝ KŮŇ

- **TROJSKÝ KŮŇ NAPŘ. 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

- **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.**

# TROJSKÝ KŮŇ

- **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 ...).**

# TROJSKÝ KŮŇ



# TROJSKÝ KŮŇ

- **TROJSKÉ KONĚ MŮŽEME DÁLE DĚLIT NA DVĚ SKUPINY:**
  - **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.**

# TROJSKÝ KŮŇ

The screenshot shows the Ad-Aware SE Personal interface. The main window title is "Ad-Aware SE Personal". The software logo "Ad-Aware se" is prominently displayed, with the copyright notice "Copyright 1999-2004 Lavasoft Sweden. All rights reserved." below it. On the left side, there is a vertical menu with buttons for "Status", "Scan now", "Ad-Watch", "Add-ons", and "Help". The main content area is titled "Scan Complete" and contains the following information:

- Current Operation:** Finished. Objects Scanned: **161866**.
- Summary:**
  - 32 Running Processes
  - 1290 Process Modules
  - 3 Objects Recognized
  - 0 Objects Ignored
  - 3 **New Critical Objects** (indicated by a red bug icon)
  - 0 Processes Identified
  - 0 Modules Identified
  - 0 Registry Keys Identified
  - 0 Registry Values Identified
  - 3 Files Identified
  - 0 Folders Identified
- 8 Negligible Objects (indicated by a yellow warning icon)

At the bottom of the main content area, there are buttons for "Show Logfile" and "Next". The Lavasoft logo is in the bottom left corner, and the version information "Ad-Aware SE Personal, Build 1.05" is in the bottom right corner.

# ŽERTOVNÝ PROGRAM

- JSOU TO NEŠKODNÉ PROGRAMY (JOKES), 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.

# HOAX



# POČÍTAČOVÉ VIRY



# CO JSOU POČÍTAČOVÉ VIRY

- POČÍTAČOVÝ VIRUS JE UMĚLÝ ÚTVAR, ZÁMĚRNĚ VYTVOŘENÝ ČLOVĚKEM.



# CO JSOU POČÍTAČOVÉ VIRY

- **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.“**

# CO JSOU POČÍTAČOVÉ VIRY

- **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:**
  - **SPOUŠTĚCÍ**
  - **VLASTNÍ FUNKČNÍ**
  - **REPRODUKČNÍ.**

# CO JSOU POČÍTAČOVÉ VIRY

- **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

- **SCHOPNOST MNOŽIT SE - NEKONTROLOVANĚ SE PŘIPOJUJE K JINÝM, TZV. HOSTITELSKÝM PROGRAMŮM (SOUBOROVÉ VIRY), NEBO SE ZAPISUJE DO SYSTÉMOVÝCH OBLASTÍ DISKŮ (BOOTOVÉ VIRY).**
- **SCHOPNOST VYKONÁVAT DALŠÍ ČINNOST.**

# PODMÍNKY ŠÍŘENÍ POČÍTAČOVÝCH VIRŮ

- **VHODNÉ PROSTŘEDÍ (POČÍTAČ SE ZNÁMÝM OPERAČNÍM SYSTÉMEM).**
- **OBJEKTY, KTERÉ DOKÁŽE NAPADNOUT**
  - **SPUSTITELNÉ SOUBORY**
  - **SYSTÉMOVÉ OBLASTI PAMĚŤOVÝCH DISKŮ**
  - **DOKUMENTY OBSAHUJÍCÍ MAKRA**
  - **ELEKTRONICKÁ POŠTA**

# ČLENĚNÍ VIRŮ PODLE ŠKODLIVOSTI

- **MĚKKÉ - NEŠKODNÉ VIRY. ŘÍKÁME JIM „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. UŽIVATELI ZÁSADNĚ NEŠKODÍ, ZABÍRAJÍ POUZE MÍSTO NA DISKU A V OPERAČNÍ PAMĚTI.

# ČLENĚNÍ VIRŮ PODLE ŠKODLIVOSTI

- **STŘEDNĚ ŠKODLIVÉ - NEBEZPEČNÉ VIRY. UŽIVATELI 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.**

# ČLENĚNÍ VIRŮ PODLE ŠKODLIVOSTI

- **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.).**

# ČLENĚNÍ VIRŮ PODLE ŠKODLIVOSTI

- NĚKDY DĚLÍME VIRY PODLE JEJICH ÚČINKŮ TAKÉ NA:
  - **OBTĚŽUJÍCÍ**
  - **DESTRUKČNÍ**

# NEJBĚŽNĚJŠÍ TYPY POČÍTAČOVÝCH VIRŮ

- **PODLE TOHO, JAKÝM ZPŮSOBEM VIRY PRACUJÍ A JAK SE PROJEVUJÍ, JE MŮŽEME ROZČLENIT NA**
  - **SOUBOROVÉ VIRY**
  - **BOOTVIRY**
  - **MULTIPARTITNÍ VIRY**
  - **MAKROVIRY.**

# **SOUBOROVÉ VIRY**

- **SOUBOROVÉ VIRY NAPADAJÍ POUZE SOUBORY (PROGRAMY A DOKUMENTY). PROJEVUJÍ SE NEJROZMANITĚJŠÍM ZPŮSOBEM A PODLE SVÝCH PROJEVŮ SE DÁLE DĚLÍ NA:**

# SOUBOROVÉ VIRY

- **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.**

# SOUBOROVÉ VIRY

- **LINK VIRY – PŘILEPÍ (PŘILINKUJÍ) SE K NAPADENÉMU SOUBORU, COŽ UMOŽŇUJE CHOD HOSTITELSKÉHO PROGRAMU A ZÁROVEŇ I ČINNOST VIRU.**

# SOUBOROVÉ VIRY

- **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.**

# SOUBOROVÉ VIRY

- **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.**

# SOUBOROVÉ VIRY

- **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.**

# SOUBOROVÉ VIRY

- **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 INFEKČÍ. PRO ANTIVIROVÉ PROGRAMY BEZ ANTI-STEALTH TECHNIKY JSOU JAKOBY „NEVIDITELNÉ“.

# SOUBOROVÉ VIRY

- **ZAKÓDOVANÉ VIRY – JSOU ZAKÓDOVANÉ URČITÝM PROMĚNLIVÝM ALGORITMEM, TAKŽE JEJICH TĚLO JE POKAŽDÉ JINÉ. STEJNÁ JE POUZE DEKÓDOVACÍ INSTRUKCE.**

# SOUBOROVÉ VIRY

- **POLYMORFNÍ VIRY – PRO KAŽDÝ NAPADENÝ SOUBOR SE KÓDUJÍ JINÝM ZPŮSOBEM A VYTVÁŘÍ I JINOU DEKÓDOVACÍ FUNKCI. V NAPADENÝCH SOUBORECH NELZE NAJÍT ŽÁDNÉ SEKVENCE STEJNÉHO KÓDU.**

# SOUBOROVÉ VIRY

- **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.**

# SOUBOROVÉ VIRY

- **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.

# BOOTOVÉ VIRY

- **TYTO VIRY SE ŠÍŘÍ PROSTŘEDNICTVÍM BOOT SEKTORU DISKET. ABY BYL POČÍTAČ TAKOVÝMTO VIREM NAPADEN, MUSÍ SE Z NAKAŽENÉ DISKETY NABOOTOVAT (NAPŘ. NECHÁME V DISKETOVÉ MECHANICE NAKAŽENOU DISKETU A SPUSTÍME POČÍTAČ).**

# BOOTOVÉ VIRY

- **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 NABOOTOVAT 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

- **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.**

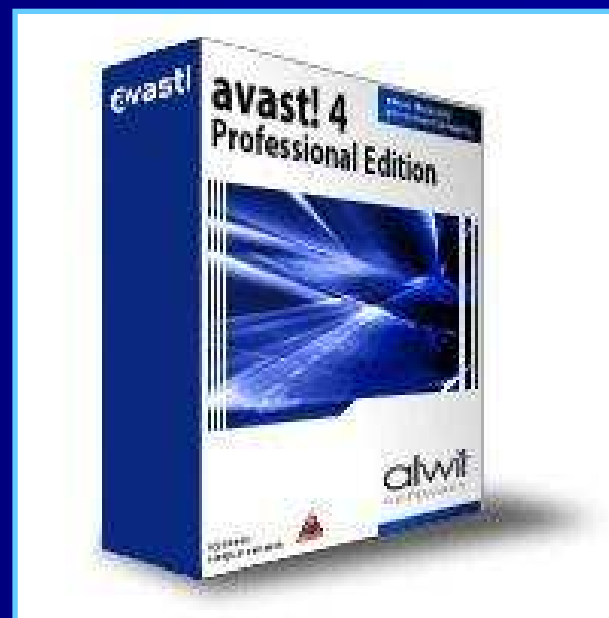
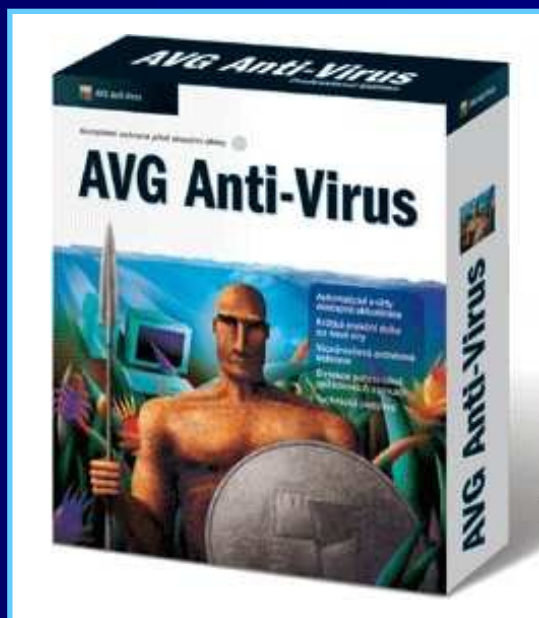
# MAKROVIRY

- **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.**

# MAKROVIRY

- **NEBEZPEČÍ MAKROVIRU SPOČÍVÁ V TOM, ŽE OVLÁDNE PROGRAM I JEHO ŠABLONY. POTÉ PŘI URČITÉ OPERACI (NAPŘ. ULOŽENÍ DOKUMENTU) BUDE SPUŠTĚNO MAKRO S DESTRUKČNÍMI ÚČINKY.**
- **ZATÍMCO S PŘÍCHODEM OPERAČNÍHO SYSTÉMU WINDOWS UBÝVÁ REZIDENTNÍCH A SOUBOROVÝCH VIRŮ, MAKROVIRY PŘEDSTAVUJÍ NASTÁVAJÍCÍ HROZBU.**

# ANTIVIROVÉ PROGRAMY



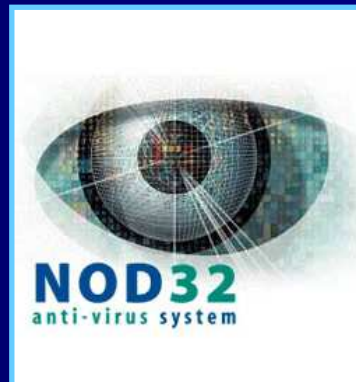
# ANTIVIROVÉ PROGRAMY

- **PROTI VIRŮM SE MUSÍME CHRÁNIT. V DNEŠNÍ DOBĚ SI UŽ ŽÁDNÝ UŽIVATEL, KTERÝ ALESPON ČÁSTEČNĚ DATOVĚ KOMUNIKUJE SE SVÝM OKOLÍM, NEMŮŽE BÝT JISTÝ.**
- **KROMĚ OPATRNOSTI JSOU SILNÝM PROSTŘEDKEM PROTI VIRŮM ANTIIVIROVÉ PROGRAMY. DOKÁŽÍ NEJEN VIR NAJÍT, ALE VĚTŠINOU I NAKAŽENÝ SOUBOR „VYLÉČIT“ TAK, ŽE PO ZÁSAHU ANTIIVIROVÉHO PROGRAMU FUNGUJE SPRÁVNĚ A NEMUSÍ BÝT SMAZÁN.**

# ANTIVIROVÉ PROGRAMY

- **EXISTUJÍ ANTIIVIROVÉ PROGRAMY JEDNOÚČELOVÉ, ZAMĚŘENÉ NA JEDEN TYP VIRU A PROGRAMY KOMPLEXNÍ - SCHOPNÉ VYHLEDAT ŠIROKÉ SPEKTRUM DOPOSUD ZNÁMÝCH VIRŮ.**
- **NA SOFTWAREM PŮSOBÍ POMĚRNĚ VELKÉ MNOŽSTVÍ ANTIIVIROVÝCH PROGRAMŮ. V ČESKÉ REPUBLICCE SE K NEJZNÁMĚJŠÍM ŘADÍ PROGRAMY AVG, AVAST, NOD32, Kaspersky Antivirus, Norton Antivirus NEBO F-SECUE.**

# ANTIVIROVÉ PROGRAMY



avast! antivirus Novinka v4.6!



# ANTIVIROVÉ PROGRAMY

**AVG 7.0 Multilicense - Základní rozhraní**

Program Testy Výsledky Servis Informace

**AVG Anti-Virus**

- Pokročilé rozhraní
- Control Center
- Virový trezor
- Výsledky testů
- Informace o verzi
- Provést aktualizaci
- Ukončit program

**Otestovat počítač**

Kompletní test kontroluje všechny pevné disky vašeho počítače. Při nalezení viru jej systém AVG odstraní nebo vám poskytne instrukce pro jeho odstranění.

**Otestovat vybrané oblasti**

Test vybraných oblastí kontroluje vybrané složky, diskety, CD, optické disky, hard disky nebo jiné cíle, které lze před jeho spuštěním zvolit. Postup při odstraňování virové nákazy a případném léčení je shodný jako v ...

**Provést aktualizaci**

Spustí se aktualizace systému AVG.

Nápověda - F1 7.0.338 | 267.10.2/65 | 7.8.2005 9:45:00

# ANTIVIROVÉ PROGRAMY

- **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.**

# ANTIVIROVÉ PROGRAMY

- UŽ ZE SAMOTNÉHO PRINCIPU POTOM VYPLÝVÁ, ŽE ŽÁDNÝ ANTIKVIROVÝ PROGRAM NA SVĚTĚ NEMŮŽE POČÍTAČ OCHRÁNIT PROTI VIRŮM, KTERÉ VZNIKLY PRÁVĚ TEĎ. VIRY JSOU TEDY VŽDY O KROK VPŘED.

# **METODY PRÁCE ANTIVIROVÝCH PROGRAMŮ**

- **METODA VYHLEDÁVÁNÍ CHARAKTERISTICKÝCH ŘETĚZCŮ ZNAKŮ (VYHLEDÁVACÍ SEKVENCE)**
- **JE TO NEJBĚŽNĚJŠÍ A NEJRYCHLEJŠÍ METODA PRO JEDNORÁZOVOU KONTROLU. VĚTŠINA VIRŮ MÁ VE SVÉM TĚLE URČITOU SPECIFICKOU SEKVENCÍ – POSLOUPNOST ZNAKŮ, PODLE KTERÉ LZE VIR JEDNOZNAČNĚ URČIT (NAPŘ. A1 00 10 B5 C2 00). ANTI-VIROVÝ PROGRAM PROHLEDÁVÁ CELÝ DISK A SOUBORY, VE KTERÝCH NAJDE TAKOVOUTO SEKVENCÍ 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.**

# METODY PRÁCE ANTIVIROVÝCH PROGRAMŮ

- **SROVNÁVACÍ METODA (KONTROLA INTEGRITY) - PŘI PRVNÍM SPUŠTĚNÍ TENTO ANTI VIROVÝ 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 SYSTÉMU.**

# METODY PRÁCE ANTIVIROVÝCH PROGRAMŮ

- **HEURISTICKÁ METODA - KAŽDÝ ROK VZNIKAJÍ NA SVĚTĚ STOVKY NOVÝCH VIRŮ. OD VZNIKU VIRU PO VYDÁNÍ AKTUÁLNÍHO ANTIKVIROVÉHO PROGRAMU UBĚHNE POMĚRNĚ DLOUHÁ DOBA – VIR SE MUSÍ ROZŠÍŘIT, TVŮRCI ANTIKVIROVÉHO PROGRAMU HO MUSÍ ANALYZOVAT A ZAČLENIT DO NOVÉ VERZE PROGRAMU, TA MUSÍ BÝT VYROBENA, DISTRIBUTOVANÁ K ZÁKAZNÍKŮM, ZÁKAZ-NÍCI SI JI MUSÍ NAINSTALOVAT A POUŽÍT.**

# METODY PRÁCE ANTIVIROVÝCH PROGRAMŮ

- **HEURISTICKÁ METODA - PROTO ANTI-  
ROVÉ 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 ANTI-ROVÝ PROGRAM DOBŘE  
NAPSÁN, DOKÁŽE NAJÍT AŽ 70% NOVÝCH  
VIRŮ.**

# METODY PRÁCE ANTIVIROVÝCH PROGRAMŮ

- **METODA NÁVNADY - ANTIIVIROVÝ PROGRAM VYKONÁVÁ RŮZNÉ OPERACE S POKUSNÝMI SOUBORY TYPU .COM A .EXE, JEJICHŽ OBSAH JE ZNÁM. PO VYKONANÍ TĚCHTO OPERACÍ SROVNÁVÁ OBSAH POKUSNÝCH SOUBORŮ PŘED A PO OPERACI. ODHALUJE NAPŘ. REZIDENTNÍ SOUBOROVÉ VIRY.**

# METODY PRÁCE ANTIVIROVÝCH PROGRAMŮ

- **REZIDENTNÍ HLÍDAČ - JE TO ČÁST ANTIKVIROVÉHO 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 VŠÍMAT CHOVÁNÍ POČÍTAČE, PROTOŽE NĚKTERÉ VIRY SE PROJEVUJÍ SPECIFICKÝM CHOVÁNÍM, NAPŘ.:**
  - **NÁHLÉ ZPOMALENÍ PRÁCE POČÍTAČE**
  - **NEOČEKÁVANÉ ROZSVĚCOVÁNÍ KONTROLEK DISKOVÝCH MECHANIK**

# ODSTRANĚNÍ VIRŮ

- NÁRŮST DÉLKY SOUBORŮ
- ZMĚNA ČASU A DATA POSLEDNÍHO ZÁPISU
- MIZENÍ SOUBORŮ
- VIZUÁLNÍ A AKUSTICKÉ SIGNÁLY
- BĚŽNĚ POUŽÍVANÉ PROGRAMY HLÁSÍ CHYBY....

# ODSTRANĚNÍ VIRŮ

- **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.**

# ODSTRANĚNÍ VIRŮ

- **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.**

# ODSTRANĚNÍ VIRŮ

- **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.**

# SPAM



# SPAM

- **VÝRAZEM SPAM OZNAČUJEME NEVYŽÁDANÉ HROMADNĚ ROZESÍLANÉ ZPRÁVY. PROBLEMATIKA SPAMU JE DNES VELMI ZÁVAŽNÁ. BĚŽNÝ UŽIVATEL E-MAILU DENNĚ OBDRŽÍ DESÍTKY NEVYŽÁDANÝCH ZPRÁV, KTERÉ MUSÍ MAZAT, KTERÉ ZBYTEČNĚ PLNÍ JEHO SCHRÁNKU, JEJICHŽ PŘÍJEM PŘI VYTÁČENÉM PŘIPOJENÍ PLATÍ A KTERÉ ČASTO OBSAHUJÍ PODVODNÉ NABÍDKY.**

# SPAM

- **MŮŽE SE STÁT, ŽE SI UŽIVATEL SE SPAMEM VYMAŽE I JINOU DŮLEŽITOU ZPRÁVU NEBO ŽE TAKOVOU ZPRÁVU NEPŘEPUSTÍ ANTISPAMOVÝ FILTR.**
- **ROZESÍLÁNÍ SPAMU JE POVAŽOVÁNO ZA NEETICKÉ A DNES JE POSTIŽITELNÉ I PODLE ZÁKONA.**
- **MUSÍME BÝT OPATRNÍ PŘI REGISTRACI A UVÁDĚNÍ SVÉ E-MAILOVÉ ADRESY NA RŮZNÝCH SERVERECH S NABÍDKAMI SLUŽEB.**

# SPAM

## DŮVODY A ZPŮSOBY ŠÍŘENÍ SPAMU

- SPAM JE PRO SVÉ ŠÍŘITELÉ VÝNOSNÝ, JINAK BY NEEXISTOVAL. FIRMY VYUŽÍVAJÍCÍ SPAM TÍMTO ZPŮSOBEM VNUCUJÍ OBROVSKÉMU MNOŽSTVÍ LIDÍ SVÉ ČASTO NEKVALITNÍ NEBO NELEGÁLNÍ ZBOŽÍ, A TO ZA MINIMÁLNÍ NÁKLADY.



# SPAM

## DŮVODY A ZPŮSOBY ŠÍŘENÍ SPAMU

- ROZESÍLÁNÍ SPAMU TÉMĚŘ NIC NESTOJÍ – VYUŽÍVÁ VOLNĚ DOSTUPNÉ POŠTOVNÍ SERVERY A JE ZCELA OBVYKLÉ, ŽE JE SPAM ROZESÍLÁN Z NAKAŽENÝCH POČÍTAČŮ LIDÍ, KTEŘÍ O TOM VŮBEC NEVĚDÍ.



# SPAM

## DŮVODY A ZPŮSOBY ŠÍŘENÍ SPAMU

- **ŠIŘITELÉ SPAMU (SPAMEŘI) ZÍSKÁVAJÍ ADRESY PRO ZASÍLÁNÍ ZPRÁV MNOHA ZPŮSOBY:**
  - **POMOCÍ SPECIALIZOVANÝCH PROGRAMŮ (ROBOTŮ PODOBNÝCH INDEXAČNÍM PROGRAMŮM VYHLEDÁVACÍCH SERVERŮ) PROCHÁZEJÍ WEBOVÉ STRÁNKY, DISKUSNÍ FÓRA A KONFERENCE A SBÍRAJÍ Z NICH ADRESY.**

# SPAM

## DŮVODY A ZPŮSOBY ŠÍŘENÍ SPAMU

- **ŠIŘITELÉ SPAMU (SPAMEŘI) ZÍSKÁVAJÍ ADRESY PRO ZASÍLÁNÍ ZPRÁV MNOHA ZPŮSOBY:**
  - **VYUŽÍVAJÍ VIRY, KTERÉ ODEŠLOU CELÝ ADRESÁŘ POŠTOVNÍHO PROGRAMU NA URČITOU ADRESU.**
  - **KUPUJÍ DATABÁZE ADRES OD JINÝCH SPAMERŮ.**
  - **GENERUJÍ NÁHODNÉ ADRESY PODLE SEZNAMŮ JMEN A ROZŠÍŘENÝCH POŠTOVNÍCH SERVERŮ.**

# SPAM

## OCHRANA PROTI SPAMU

- **BRÁNIT SE PROTI PŘÍJMU NEVYŽÁDANÉ POŠTY LZE RŮZNÝMI ZPŮSOBY, ŽÁDNÝ Z NICH VŠAK NENÍ STOPROCENTNĚ ÚČINNÝ.**
- **JE POTŘEBNÉ BÝT OPATRNÝ PŘI ZADÁVÁNÍ SVÉ E-MAILOVÉ ADRESY NA RŮZNÝCH WEBOVÝCH SERVERECH. JE VHODNÉ MÍT DVĚ ADRESY – JEDNU PRO SOUKROMÉ ÚČELY A JEDNU PRO RŮZNÉ REGISTRACE.**

# SPAM

## OCHRANA PROTI SPAMU

- **NA SPAM NEODPOVÍDÁME ANI NEVYUŽÍVÁME NĚKDY NABÍDNUTOU MOŽNOST SE Z DATABÁZE PRO ZASÍLÁNÍ ODHLÁSIT – NEMŮŽEME SE ODHLÁSIT ODNĚKUD, KDE JSME SE NIKDY NEPŘIHLÁSILI.**
- **VĚTŠINA SPAMU JE ZATÍM V ANGLIČTINĚ, TAKŽE JE PODEZŘELÁ ZPRÁVA PATRNÁ NA PRVNÍ POHLED A JEJÍ ODHALENÍ A MAZÁNÍ JE RYCHLÉ.**

# SPAM

## OCHRANA PROTI SPAMU

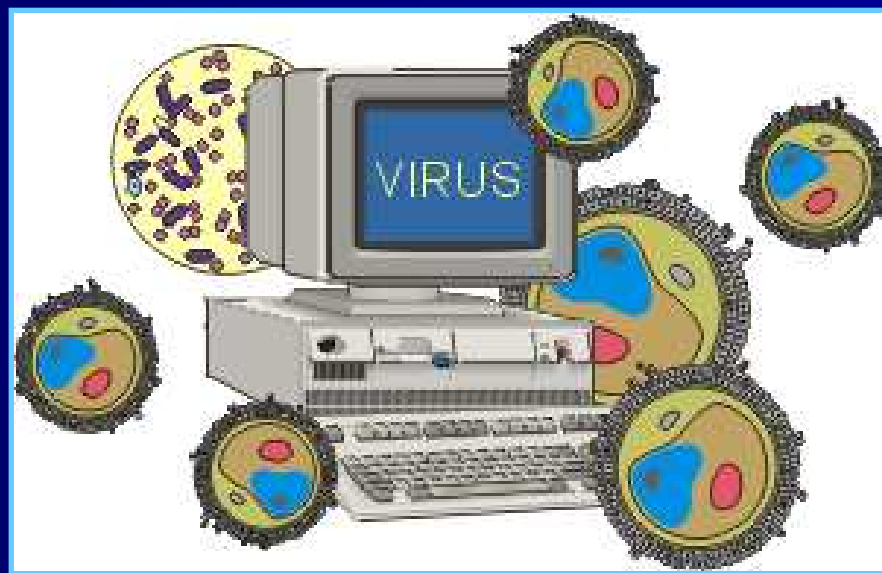
- **POŠTOVNÍ PROGRAM MŮŽEME DOPLNIT O ANTISPAMOVÝ FILTR. SLEDUJE V TEXTECH ZPRÁV VÝSKYT SLOV INDIKUJÍCÍCH SPAM (SEX, PORNO, ATD.) A PŘESUNUJE TAKOVÉ ZPRÁVY DO ZVLÁŠTNÍ SLOŽKY. UMÍ SE I UČIT – SLEDUJE, JAKÉ ZPRÁVY SAMI OZNAČÍME ZA SPAM, A PODOBNÉ ZPRÁVY PAK PŘESUNUJE AUTOMATICKY. JE VŠAK NUTNÉ OBČAS SLOŽKU SE SPAMEM PROHLÉDNOUT, JESTLI TAM NEJSOU OMYLEM I DŮLEŽITÉ ZPRÁVY.**

# SPAM

## OCHRANA PROTI SPAMU

- **VYSPĚLÉ ZEMĚ PŘIJÍMAJÍ ZÁKONY, UMOŽŇUJÍCÍ POSTIH NEVYŽÁDANÝCH REKLAMNÍCH SDĚLENÍ. SPAMĚŘI VŠAK ČASTO VYUŽÍVAJÍ SERVERY ZE ZEMÍ, KDE PODOBNÁ LEGISLATIVA NEPLATÍ.**
- **ZÁVAŽNOST SPAMU SI UVĚDOMUJÍ I FIRMY, KTERÉ URČUJÍ VÝVOJ VÝPOČETNÍ TECHNIKY. NAVRHUJÍ ŘEŠENÍ ZALOŽENÁ NA ZABUDOVÁNÍ TECHNOLOGIE OVĚŘENÍ ODESÍLATELE DO POŠTOVNÍHO SYSTÉMU.**

# PŘEHLED PRAVIDEL POČÍTAČOVÉ BEZPEČNOSTI



# PRAVIDLA POČÍTAČOVÉ BEZPEČNOSTI

- **VŠECHNO DŮLEŽITÉ SI ZAHESLUJEME.**
- **S HESLY ZACHÁZÍME OPATRNĚ,  
NECHÁVÁME SI JE PRO SEBE A ČAS OD  
ČASU JE ZMĚNÍME.**
- **Z INTERNETU NEOTVÍRÁME NIC, O ČEM SI  
NEJSME JISTI, ŽE JE TO BEZPEČNÉ.**
- **E-MAILY POUŽÍVÁME BEZPEČNĚ.**
- **CHRÁNÍME SE PŘED VIRY.**
- **VYŽEŇME Z POČÍTAČE ŠPIÓNY.**

# PRAVIDLA POČÍTAČOVÉ BEZPEČNOSTI

- PRAVIDELNĚ ZÁPLATUJEME OPERAČNÍ SYSTÉM.
- POZNEJME POČÍTAČOVÉ KRIMINÁLNÍKY.
- DŮLEŽITÉ VĚCI SI ZÁLOHUJEME.
- CHRAŇME DATA.
- SCHOVEJME SE ZA FIREWALLEM.
- DOMLUVME SE SE SOUSEDY.
- PŘÍSTUPOVÁ PRÁVA CHRÁNÍ NAŠE SOUBORY PŘED OSTATNÍMI UŽIVATELI.

# PRAVIDLA POČÍTAČOVÉ BEZPEČNOSTI

- **TAJNÁ DATA ŠIFRUJEME.**
- **NIKOMU NEMŮŽEME ÚPLNĚ VĚŘIT.**
- **ODLIŠUJME ZABEZPEČENÉ WEBY.**
- **VÍME, S KÝM SE BAVÍME?**
- **STÁLE JSME POD KONTROLOU.**
- **NEPROPADEJME PANICE.**
- **VYTVOŘME SI ZARUČENĚ ČISTOU  
BOOTOVACÍ DISKETU A PEČLIVĚ JI  
ULOŽME NA BEZPEČNÉ MÍSTO.**