AEC
DATA SECURITY COMPANY

informační
bulletin

(Připravuje AEC Data Security Company – jakékoliv připomínky, náměty či dotazy posílejte na e-mailové adresy tomas.pribyl@aec.cz nebo petr.nadenicek@aec.cz)

Počítačové viry, antivirové technologie, elektronický podpis, šifrování dat – prostě ochrana datových informací vůbec.

Dnes přinášíme:

- **Novinky mezi počítačovými viry: Swen**
- **Světem se šíří nebezpečný virus!**
- **F-Secure Anti-Virus Client Security**
- **Disk Protection: šifrovaný virtuální disk**

Na přelomu září a října 2003 se v šesti městech České republiky uskutečnila AEC roadshow 2003 – série seminářů, jichž se zúčastnilo přes 300 posluchačů.

AEC
DATA SECURITY COMPANY

Novinky mezi počítačovými viry: Swen

V průběhu září zasáhla světové počítačové sítě další virová epidemie e-mailového červa Swen. Ten se umí šířit e-mailem, v lokální síti, prostřednictvím IRC a výměnné sítě KaZaa.

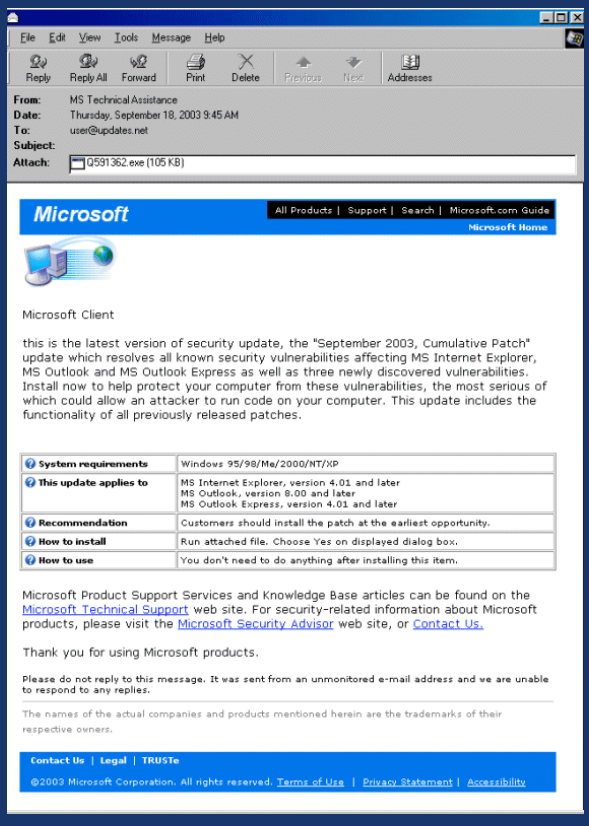
Při svém šíření e-mailem červ využívá metod sociálního inženýrství a dovedně se maskuje za bezpečnostní aktualizaci společnosti Microsoft. Zneužívá bezpečnostní chybu Internet Exploreru, díky níž se může spustit z infikovaného e-mailu automaticky (bez zásahu uživatele). Pokud se tak stane, má k dispozici řadu dialogových oken, které vypadají velmi věrohodně. Zajímavé je, že se do systému skrytě nainstaluje i tehdy, když uživatel instalaci domnělého bezpečnostního update ukončí hned na začátku. Do systému se fyzicky instaluje pod náhodným jménem jako EXE soubor do adresáře Windows. Kromě toho vytváří ještě soubor s příponou DAT, kam si ukládá seznam dostupných SMTP a NNTP serverů.

Svoje spouštění si na infikovaném systému zabezpečuje modifikací hned několika klíčů v systémových registrech, které zabezpečují spouštění souborů s příponou BAT, SCR, EXE, REG a PIF. Následně je tedy červ vždy spuštěn současně s některým z těchto souborů. Opravě klíčů do původního stavu se brání zablokováním editoru registrů.

E-mailové adresy pro další šíření čerpá ze souborů s příponami HTML, ASP, EML, DBX, WAB, a MBX, které následně pravidelně kontroluje. Infikovaný e-mail je skládán z více možných předem definovaných komponent. Vždy však vypadá velmi věrohodně.

Šíření prostřednictvím lokální sítě probíhá podle zavedeného scénáře. Červ hledá dostupná sdílení a na vzdálené počítače se kopíruje do „StartUp“ adresáře, takže počítač je infikován po následném restartu. Stejně tak „klasickým“ způsobem probíhá i šíření po IRC a síti KaZaa. Modifikací SCRIPT.INI ovlivňuje instalaci mIRC klienta tak, že ten následně šíří soubor červa všem uživatelům v kanále, kde je aktuálně přihlášen. Vyhledává také adresář sdílený do sítě KaZaa a vytváří do něj množství svých kopií s „lákavými“ názvy.

Swen obsahuje i funkci, která v systému ukončuje procesy patřící některým bezpečnostním a antivirovým programům. Rozlišuje je podle definovaných textových řetězců.



AEC
DATA SECURITY COMPANY

Světem se šíří nebezpečný virus!

Čas od času přijde do většiny e-mailových schránek zpráva podobná té následující:

Pozor, světem se od včerejška šíří nebezpečný virus. Nikdo o něm nic neví, nikdo ho neumí léčit… **Následuje popis šílených a mimořádných vlastností tohoto škodlivého kódu zakončený výzvou:** ***Pošlete tuto zprávu co nejvíce lidem, raději desetkrát než ani jednou.***

Tento e-mail označujeme jako tzv. hoax. Tento anglický výraz by se dal česky přeložit jako „smyšlenka“ nebo „žert“. Jeho podstata je jednoduchá: Vystrašit uživatele počítače a přinutit jej, aby zprávu rozeslal co nejvíce lidem. Neznalý uživatel tak vlastně vykoná činnost, která jinak přísluší pouze virům – rozdistribuuje e-mail na všechny strany. To je přitom nejpodstatnější projev většiny škodlivých kódů šířených elektronickou poštou, neboť málokterý z nich vykonává nějakou destrukční či jinak obtěžující rutinu. Svým způsobem se jedná o jakýsi „manuální virus“.

Že vlastně nikomu neškodí a neubližuje? Ale omyl! E-mailové zprávy odesílané ve velkém množství zpomalují či dokonce blokují provoz poštovních serverů (např. největším důsledkem šíření kódu Melissa bylo právě „shazování“ přetížených systémů). Navíc (na rozdíl od klasické pošty, kde za její využití platí odesílatel) za elektronickou poštu platí i příjemce (telefonní poplatky, paušál za pevnou linku). V nespolední řadě lze hovořit o značné neúctě k adresátovi zpráv zasypáváním jej informacemi z oboru, kterému dotyčná osoba nerozumí (kdyby rozuměla, nikdy by podobnou zprávu nerozšiřovala).

Jak vlastně typický hoax vypadá? Nejčastěji se objevujícím znakem hoaxu jsou informace o počítačových virech odvolávající se na firmu nebo společnost, která je u řadových uživatelů známá a budí respekt. Hlavním znakem všech hoaxů je žádost (nebo prosba) o další rozesílání zprávy dál. Tato žádost je většinou v e-mailu několikrát zdůrazněna tak, aby v příjemci vyvolala pocit, že je skutečně nutné, aby o této informaci věděli naprosto všichni jeho známí.

Pomyslným vrcholem mezi hoaxy je zpráva označovaná jako SULFBNK.EXE. Ta uživatele varuje před virem, který v počítači sídlí ve výše uvedeném souboru. Připojuje návod na jeho nalezení a odstranění – protože je ovšem SULFBNK.EXE regulérní součástí operačního systému Windows, naleznete jej každém počítači. To ovšem většina uživatelů netuší, k smrti se vyděsí a soubor dle přiloženého návodu smaže, čímž si ovšem poškodí počítač (tady je člověk skutečně sám sobě škůdcem!). Na druhou stranu je ovšem zapotřebí podotknout, že dotyčný soubor není klíčovou součástí operačního systému, takže počítač s popsanou „úpravou“ funguje v drtivé většině bez potíží dál.

Před hoaxy přitom neexistuje žádná ochrana. Sami se sice bránit nemůžete, co ale můžete, je neposílat hoaxy dál. Odesílatele taktně upozorněte na to, že jím zaslaná zpráva se nezakládá na pravdě, vysvětlete mu, v čem spočívá podstata hoaxů, a požádejte ho, aby podobné informace dále nešířil.

Každopádně ale: Nakupujte u odborníků! I nejrůznější zaručené zprávy o nepředstavitelně nebezpečných virech…

AEC

DATA SECURITY COMPANY

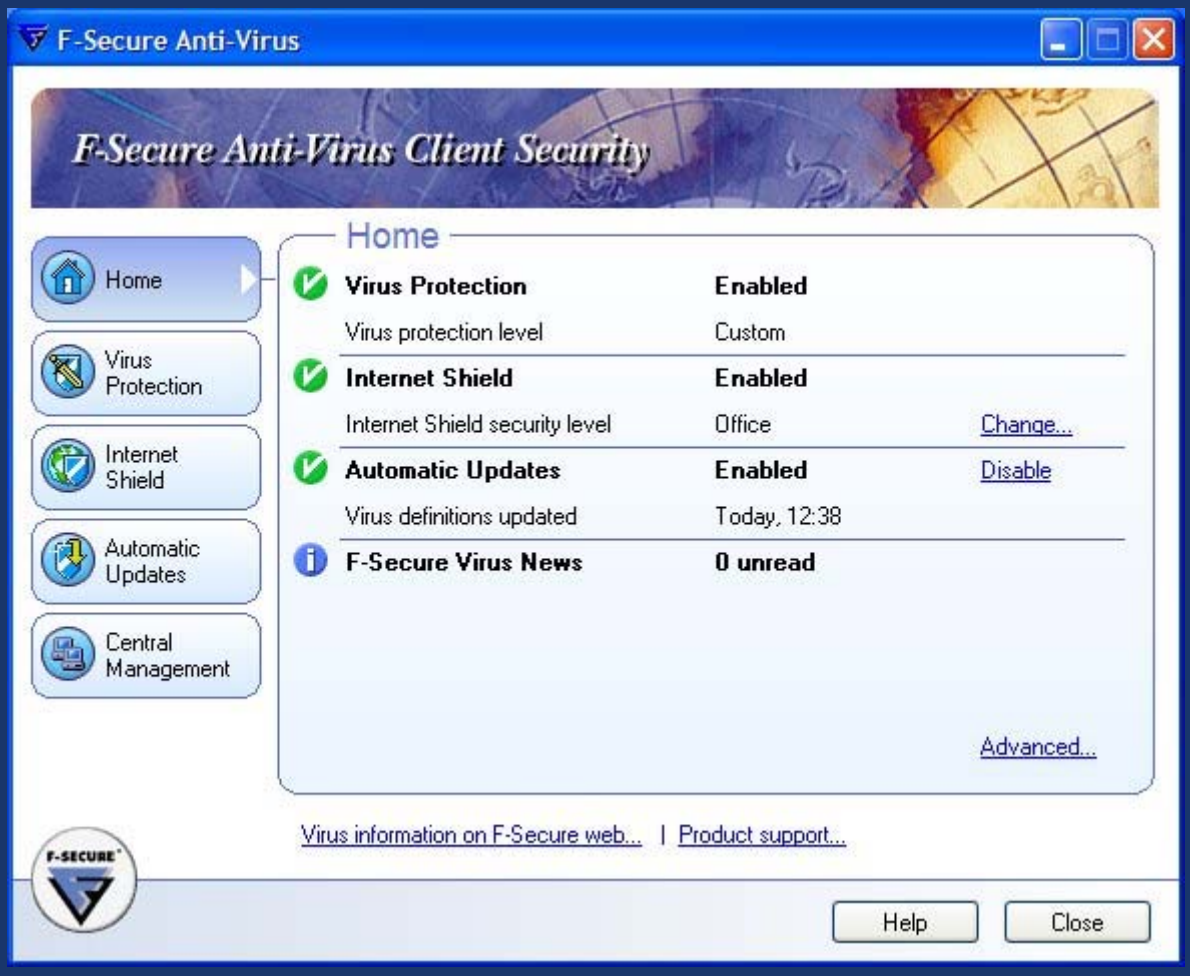
F-Secure Anti-Virus Client Security

Finská společnost F-Secure, jeden k klíčových dodavatelů AEC, oficiálně uvedla na trh nový produktový balík F-Secure Anti-Virus Client Security.

Různých škodlivých kódů je stále dost a dost. Zvláště v oblasti různých internetových červů je v posledních dnech a týdnech velmi živo. Proto je více než kdy jindy třeba, se odpovídajícím způsobem chránit. S novými i stávajícími antivirovými a bezpečnostními produkty F-Secure to jde opravdu velice snadno a efektivně.

F-Secure Anti-Virus Client Security je odpovědí na hrozby, které přicházejí s komplexními internetovými červy. Jejich šíření se neustále zrychluje, zneužívají nové a stále netradičnější cesty (např. P2P sítě) a většinou si s sebou nesou další nebezpečný náklad v podobě trojských koňů, zadních vrátek, zákeřných virů apod. S těmito hrozbami si už někdy neumí poradit ani sebelepší antivirový program. Zde již potřebujeme počítač chránit také pomocí personálního firewallu a systému prevence průniků (IDS). Neméně důležitá je také spolehlivá aktualizace skenovacích motorů a včasné doručení nových důležitých informací koncovému uživateli.

Toto všechno F-Secure Anti-Virus Client Security přináší. Obsahuje robustní antivirové řešení F-Secure Anti-Virus, spolehlivý integrovaný personální firewall, systém prevence průniků IDS, jednoduché a přehledné uživatelské rozhranní, nástroje pro kontrolu e-mailové komunikace a integrovaný informační systém F-Secure Radar, který uživatele včas varuje před novými škodlivými kódy a možnými bezpečnostními incidenty. Řešení lze centrálně spravovat pomocí nástroje F-Secure Policy Manager a je tedy vhodné i pro větší firemní sítě.



TrustPort Disk Protection: šifrovaný virtuální disk

Můžete se snažit sebevíc, ale uhlídat počítačová data je mnohdy úkolem vpravdě nadlidským. Nebezpečí na ně číhají na všech stranách – přicházejí v podobě škodlivých kódů, hackerů, zvědavců z blízkého okolí apod.

Proto je elektronická data (zvláště ta citlivá – smlouvy, objednávky, databáze, soukromé údaje…) zapotřebí chránit. Jak to ale udělat dostatečně kvalitně – a přitom pro uživatele jednoduše? Jak zajistit data tak, aby k nim neměly přístup neoprávněné osoby a naopak co nejméně omezovat osobu oprávněnou?

Představte si, že na pevném disku počítače vznikne bezpečný „šuplík“, do něhož budete moci dle libosti data odkládat a zase se k nim vracet. Onen „šuplík“ je zamykatelný a klíčem k němu je heslo, které zná pouze oprávněná osoba. Přitom velikost tohoto „šuplíku“ si určuje uživatel sám v závislosti na tom, jak velký objem dat se chystá chránit.

Takovýto „šuplík“ do počítače se jmenuje TrustPort Disk Protection.

Princip fungování aplikace TrustPort Disk Protection je takový, že na příslušném počítači vytvoří novou virtuální diskovou jednotku. Práce s tímto virtuálním diskem je pak zcela shodná jako zacházení s kterýmkoliv jiným diskem na počítači. Veškerá data na tento virtuální disk ukládaná jsou při zápisu on-line zašifrovaná. Při čtení nebo kopírování z disku jsou opět on-line rozšifrovaná. On-line šifrování a dešifrování probíhá na pozadí bez účasti uživatele. (O data nepřicházíte ani při pádu operačního systému nebo při nečekaném výpadku elektrické energie: diskový obraz je totiž neustále šifrovaný.)

Pro vytvoření virtuálního disku pomocí programu TrustPort Disk Protection je na logickém disku (pevný disk, disketa, USB úložiště…) zapotřebí prostor o požadované velikosti. Na logický disk se vytvoří obraz (image) virtuálního disku, který se z pohledu uživatele chová jako „normální“ soubor. Díky této vlastnosti lze snadno archivovat a přenášet obrazy virtuálních disků v zašifrované podobě.

Heslo samo o sobě slouží pouze pro rozšifrování uživatelského záznamu, který s sebou nese atributy přístupu daného uživatele k virtuální jednotce. Uživatel, který obraz disku vytvářel, je zároveň i administrátorem a může vytvářet i další uživatele, kteří budou mít možnost připojit tento obraz jako diskovou jednotku. Administrátor určuje práva zápisu/čtení na tento virtuální disk.

Častým problémem bývá potřeba zvětšení místa ve virtuálním disku. TrustPort Disk Protection umožňuje v určitém rozmezí zvětšit tento diskový prostor. Velikost „rezervy“ je určována podle požadované velikosti virtuálního disku.

AEC
DATA SECURITY COMPANY