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:

- **Jak fungují antivirové programy?**
- **Norman Spam Control: bojovník se spamem**
- **Personální firewall z laboratoří AEC**

V rámci veletrhu informačních technologií Invex v Brně (viz foto) se počátkem října uskutečnil již pátý ročník konference Viry a antivirová ochrana. Na akci pořádané pod záštitou vydavatelství Vogel Burda Communications se prezentovali také odborníci z AEC.

AEC DATA SECURITY COMPANY

Jak fungují antivirové programy?

Antivirový program našel v počítači virus Iloveyou (Bugbear, Sircam apod. – jméno si doplňte dle vlastní libosti či zkušenosti). Jak to ale dokázal? Vždyť příslušný „nemocný“ soubor (e-mail, disketa apod.) vypadal zdravě!

Pomiňme nyní skutečnost, že právě nenápadnost počítačového viru je základní podmínkou jeho „přežití“ v reálném světě. Virus, který na sebe jakkoliv upozorňuje totiž přímo vyzývá uživatele, aby se s ním pustil do boje. A v takovém případě zpravidla vítězí právě uživatel. Podívejme se nyní na několik základních metod, jimiž antivirové programy škodlivé kódy detekují.

Základním způsobem odhalování virů je vyhledávání. Jeho princip by se dal přirovnat k hledání podle jakési kartotéky, ve které jsou všechny význačné znaky daného viru. Výhodou této metody je zpravidla naprosto minimální počet falešných poplachů, neboť je věnována velké pozornost úplnému vypsání informací o konkrétním viru. Dále je zde díky přesné znalosti podoby viru vysoká úspěšnost při léčení souborů. Nevýhod je ovšem více. Především si takovýto vyhledávací program těžko poradí i s nepatrně upraveným virem. Kontrola trvá dlouho, neboť je potřeba pohlížet na každý soubor jako na potencionálně nebezpečný a porovnávat jej se všemi údaji v databázi, které pro něj připadají v úvahu. V neposlední řadě nesmíme zapomenout, že si takovýto vyhledávací motor neporadí s neznámými viry.

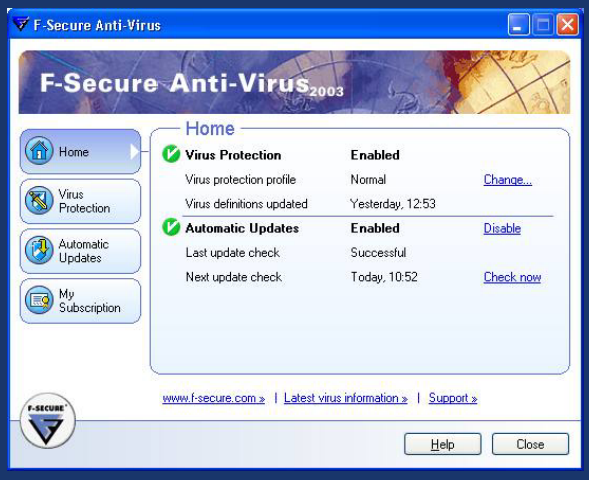
Další antivirovou metodou je skenování. U jejich zrodu stál geniálně jednoduchý nápad: Využít k pátrání po virech jen jejich některých typických znaků. Tedy ne jejich celou podobu, ale pouze jakýsi „otisk prstu“. Nevýhodou je poměrně složitější léčení, neboť skener zpravidla

neví, co všechno k viru patří a co už nikoliv.

Heuristická analýza je dalším krokem vpřed. Ve své podstatě je to rozbor kódu viru, přičemž dochází k vyhledávání postupů pro viry typických. Jinými slovy – antivirový program „nahlédne“ do zkoumaného programu a postupuje krok po kroku, jako by se snažil program spustit. Pokud by zde zjistil nějakou podezřelou instrukci či spíše soubor více podezřelých příznaků, varuje uživatele. Heuristická analýza je velmi náchylná k falešným poplachům (označení zdravého souboru za infikovaný), ale na druhé straně dokáže odhalit i „neznámé“ viry.

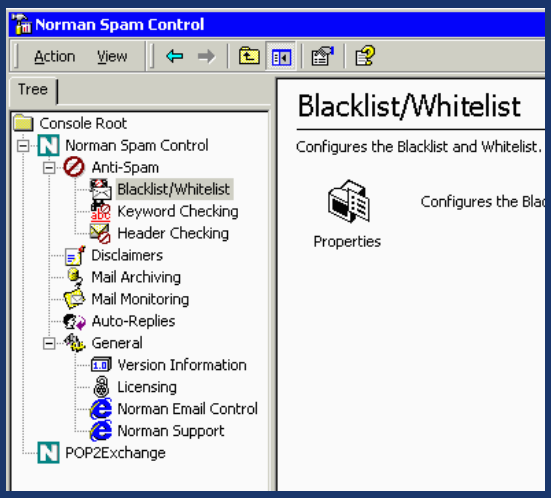
Kontrola integrity je další metodou antivirové ochrany. Její podstatou je porovnání aktuálních informací o stavu programů (např. Check Redundancy Code – CRC) či oblastí disku s databází, která vznikla v době jejich příchodu do systému či instalace. Filozofie kontroly integrity vychází ze zcela jednoduché úvahy: Pokud se do systému dostane virus a začne tam „pracovat“ musí se to nějak projevit. Nevýhodou této metody je především skutečností, že kontrola integrity nehledá vlastní viry, ale jejich PROJEVY.

Různé antivirové programy přitom mohou používat i další doplňkové metody pátrání po škodlivých kódech, ale tyto bývají zpravidla jen větší či menší modifikací způsobů vyhledávání výše uvedených.



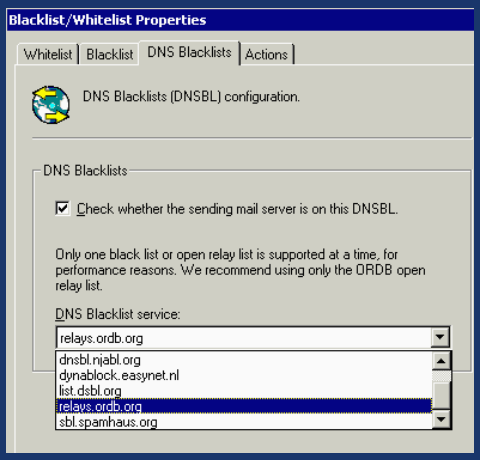
Norman Spam Control: bojovník se spamem

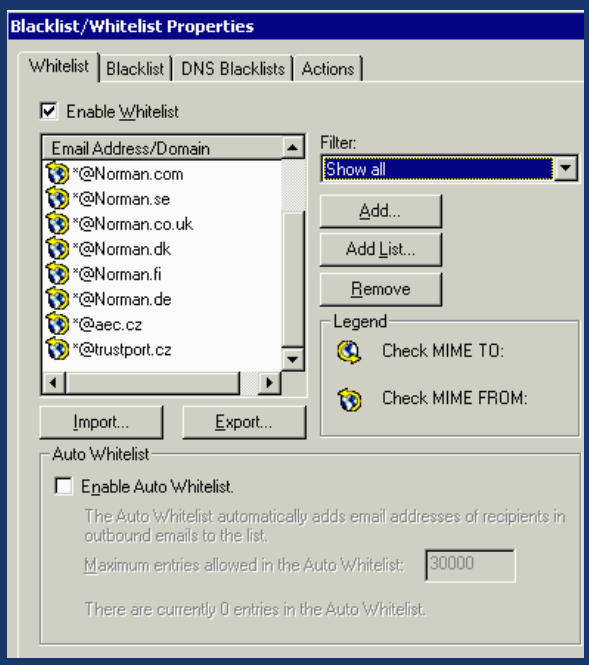
Díky stále dokonalejším technologiím a trikům používaným spammery se v posledních měsících stává spam obrovským problémem, který si vyžaduje systémové řešení. Je zřejmé, že ve firemním prostředí je optimálním anti-spamovým nástrojem ochrana přímo na úrovni vstupní brány.



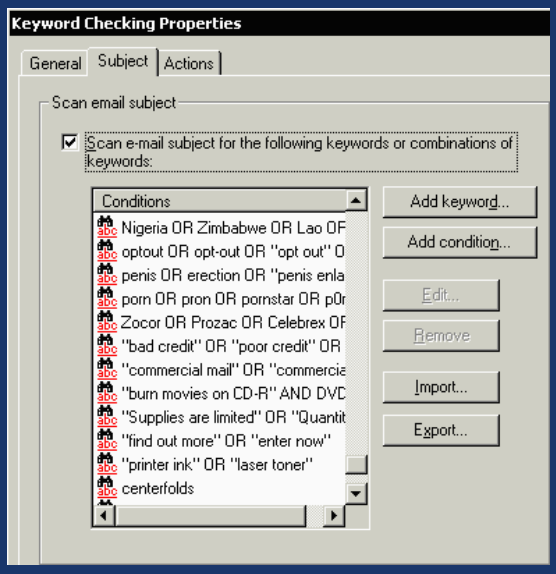
Možná řešení jsou v zásadě dvě:

- **Instalace antispamu přímo na e-mailový server.**
- **Instalace antispamu na předřazený dedikovaný server.**





Antispamový produkt Norman Spam Control (NSC) je přitom možné použít v obou výše zmíněných řešeních. NSC umožňuje efektivní filtrování spamu a také zálohovaní veškeré došlé/odešlé pošty. NSC je možno nainstalovat přímo na Exchange Server 2000/2003 nebo na předřazený stroj s Windows 2000/2003 + MS IIS 5 SMTP service.



Personální firewall z laboratoří AEC

Pokud si položíme otázku, zda personální firewall potřebujeme ke svému „kybernetickému životu“ a zamyslíme se nad ní v kontextu s každodenní praxí, bude odpověď zcela jistě znít „Ano!“. Odborníci z oblasti zabezpečení informačních technologií si dnes již počítač připojený ke světové síti internet bez tohoto základního bezpečnostního nástroje nedokáží představit. Personální firewall významně posiluje robustnost operačního systému, na jehož bezchybnost nemůžeme bezvýhradně spoléhat.

Prvním z mnoha důvodů, které nás nutí zabezpečovat počítače personálními firewally, je výskyt stále sofistikovanějších internetových červů a dalších škodlivých kódů. Zatímco v minulosti jsme se museli vypořádat pouze s poměrně primitivními e-mailovými červy, dnes stojíme tváří v tvář nebezpečí daleko zákeřnějšímu nepříteli.

Dnešní „kybernetická havěť“ se nespoléhá na e-mailové zprávy a šíří se přímo po síti, většinou prostřednictvím známých bezpečnostních děr v jednotlivých aplikacích nebo systémech. Pokud je bezpečnost počítače zajištěna personálním firewallem, není nic jednoduššího, než komunikaci na příslušných portech, které konkrétní červ využívá, zakázat a máme po problému.

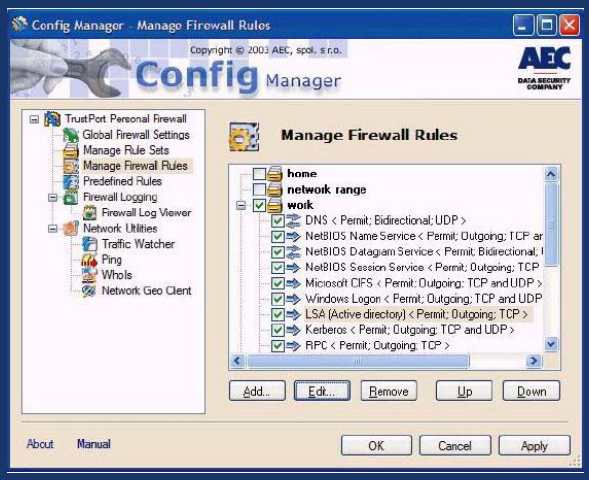
Personální firewall nachází svoje uplatnění i mimo oblast domácích počítačů. Typickým příkladem jsou notebooky, které „cestují“ mimo firemní síť, kde se připojují k internetu prostřednictví nedůvěryhodných sítí. Mohou se tak lehce stát nejen bacilonosičem ve vlastní podnikové síti, ale i zdrojem případných úniků citlivých obchodních tajemství. Svoje opodstatnění má i nasazení personálních firewallů na jednotlivé počítače pevně umístěné uvnitř lokální sítě.

Vzhledem k vnějšímu okolí jsou sice chráněny „velkým“ podnikovým firewallem, ale stačí, aby si některý z pracovníků firmy zahrál na hackera a veškerá bezpečnostní opatření přicházejí vniveč. Proto je rozumné zajistit klíčové počítače personálním firewallem, který případný pokus o průnik z bezprostředního okolí hravě odhalí a zneškodní.

Mezi moderní řešení, která pomáhají uživatelům chránit svoje „kybernetické soukromí“, patří i TrustPort® Personal Firewall vyvinutý ve společnosti AEC. Je vhodný jak pro pokročilejší uživatele, kteří disponují základním povědomím o síťových protokolech a službách, tak i pro ty, kterým vyhovuje aplikace předpřipravených sad pravidel navržených a odladěných pro provoz běžných internetových aplikací přímo výrobcem.

TrustPort® Personal Firewall vytváří na chráněném počítači bránu, kterou procházejí všechna síťová připojení. Brána umožňuje pomocí sady pravidel povolit nebo zakázat komunikaci počítače s okolní sítí. Sadu pravidel může uživatel nastavit pro všechny komunikační adaptéry současně (které jsou reprezentovány svými IP adresami) nebo pro konkrétní adresu či rozsah adres. Každá konkrétní IP adresa hostitelského počítače tedy má definovánu svoji sadu pravidel, která řídí vlastní tok dat přes bránu firewallu.

TrustPort® Personal Firewall je určen pro operační systémy Windows 2000 a Windows XP.



AEC
DATA SECURITY COMPANY