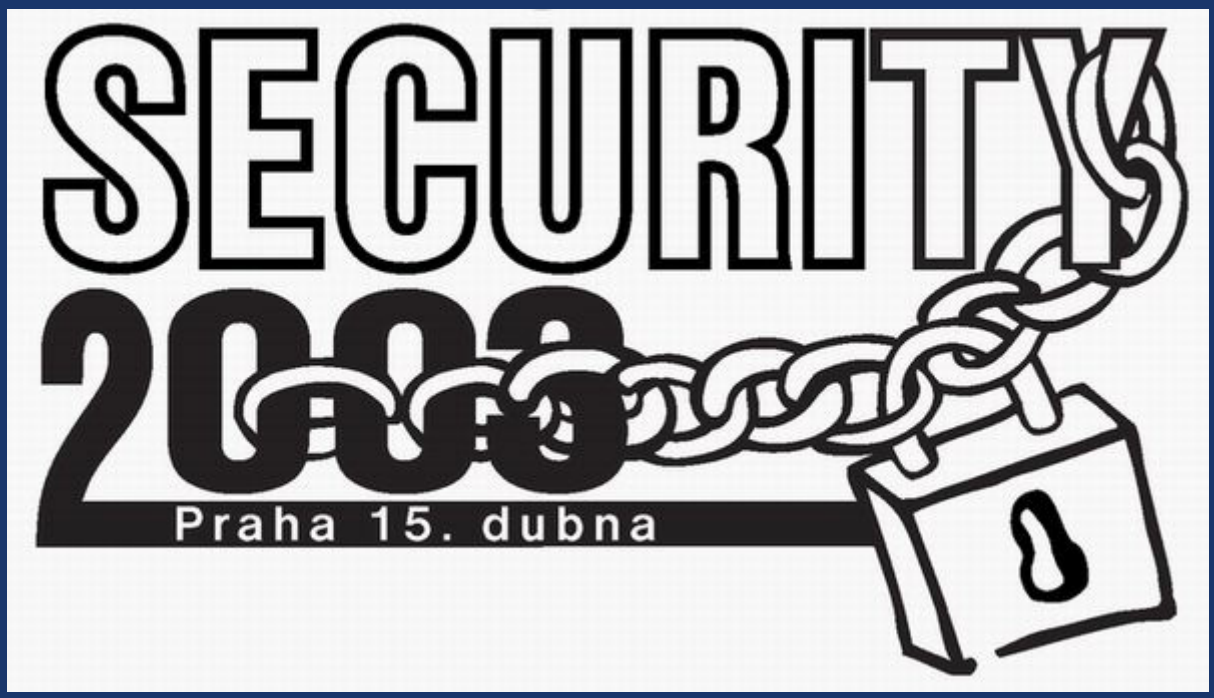
AEC
DATA SECURITY COMPANY

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:



Konference Security 2003

Stejně jako v minulých letech se i letos stane pražský Národní dům na Vinohradech na jeden den hostitelem příznivců bezpečnosti informačních a komunikačních technologií.

Pořádající společnost AEC Data Security Company společně s mediálním partnerem Vogel Burda Communications srdečně zve všechny zájemce o aktuální informace ze světa antivirové ochrany a informační bezpečnosti na konferenci Security 2003, která se bude konat v úterý 15. dubna 2003 již tradičně v reprezentativních prostorách Národního domu na Vinohradech v Praze. Záštitu nad letošním ročníkem konference převzalo Ministerstvo vnitra České republiky.

Stejně jako každý rok je program rozdělen do několika bloků. První bude věnován obecným i praktickým otázkám informační bezpečnosti jako takové. V jeho rámci se budeme moci seznámit např. s problematikou kyberterorismu, detekcí narušení (IDS), bezpečnostní politikou společnosti nebo třeba s bezpečnostními aspekty webových služeb a internetového bankovnictví. Zajímavým bodem programu jistě bude přednáška zabývající se certifikační autoritou ve spojení s praktickou aplikací časových značek.

Druhý programový blok je do značné míry novinkou. Je jím vystoupení zástupců zahraničních společností, které se na pořádání konference taktéž podílí. Účastníci Security 2003 si budou moci vyslechnout dvě přednášky na téma antivirové problematiky. První přednese „antivirový specialista“ finské společnosti F-Secure Corporation - Mikko Hypponen a druhou zástupce maďarské společnosti Virus Buster – Tibor Bial.

Závěrečný přednáškový blok bude tradičně patřit počítačovým virům a ochraně proti nim. Vystoupí přední odborníci na tuto problematiku z tuzemska a blízkého zahraničí. Pravidelnému návštěvníkovi odborných konferencí jistě stačí uvést jména jako Petr Odehnal, Pavel Baudiš nebo Tomáš Vobruba, která jsou dostatečnou zárukou zajímavých prezentací. Zvláštní pozornost posluchačů si jistě zaslouží přednáška Miroslava Trnky zabývající se počítačovým virem jako formou umělého života.

Poplatek za účast na konferenci pro jednu osobu je 3150 Kč (včetně 5 % DPH). V ceně je zahrnuto vstupné, informační materiály a občerstvení. Pro zákazníky AEC, členy AFOI, MAPM, AFCEA a předplatitele některého z titulů Vogel Burda Communications je cena 2415 Kč (včetně 5 % DPH) .

Další podrobnosti najdete na www.security2003.cz. Svoji účast můžete přihlásit pomocí on-line formuláře, který najdete na adrese https://www.aec.cz/forms/formsecurity.asp. V případě jakýchkoliv dotazů jsme vám k dispozici na e-mailové adrese konference@aec.cz nebo na telefonním čísle +420 541 235 466.

AEC

DATA SECURITY COMPANY

SQL servery pod palbou: Slammer

Internetový červ Slammer (známý také jako Helkern či Sapphire) se začal šířit v sobotu 25. ledna 2003. Na mušku si vzal servery s instalovanou databází Microsoft SQL. K napadení serveru využil bezpečnostní chybu, která byla známa již od poloviny minulého roku. Stejnou dobu byla k dispozici i záplata, která ji eliminuje. Opět se tak bohužel projevila smutná pravda o „důsledném“ záplatování bezpečnostních děr.

I když červ napadá pouze servery, pocítili jeho existenci i běžní uživatelé. V době jeho největšího rozšíření (určitě ne náhodou naplánovaného na víkend) totiž docházelo k zahlcení infrastruktury internetu do té míry, že docházelo ke zpomalení přenosu paketů a znepřístupnění řady serverů. Podle dostupných zpráv bylo dokonce jistou dobu znepřístupněno celkem pět ze třinácti kořenových DNS serverů. Epidemii červa Slammer tak lze zařadit mezi množící se útoky na internet jako takový.

Slammer infikuje pouze servery, na kterých běží nezáplatovaný Microsoft SQL Server. Šíří se prostřednictvím UDP portu 1434. Server napadá pomocí bezpečnostní díry, která spočívá v „buffer overflow“ (přetečení zásobníku). Nezapisuje se do žádného souboru na pevný disk, ale přežívá pouze v paměti serveru. K jeho odstranění proto stačí jednoduše provést restart napadeného počítače. Pokud ale nedojde k následnému ošetření pomocí Servis Pack 2 nebo 3 pro MS SQL Server, je velmi pravděpodobné, že k infikování dojde znovu...

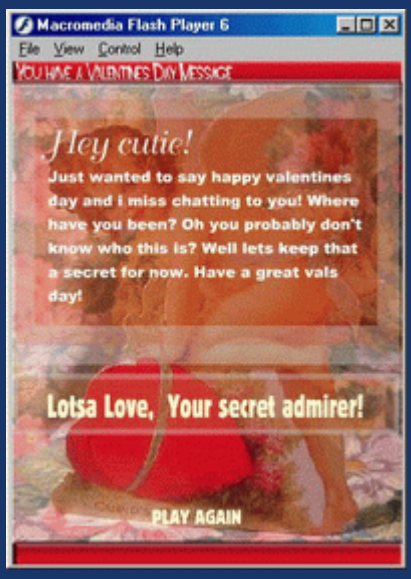
Dalším velice zajímavým aspektem Slammeru je jeho opravdu extrémně malá velikost. Veškerý kód červa dokázal neznámý programátor „nacpat“ do pouhých 376 bytů. Pro uživatele postižených databázových serverů je velikým štěstím, že do něj nepřidal také nějakou tu destrukční rutinu. Podle slov antivirového odborníka finské společnosti F-Secure Mikko Hypponena jsme se doposud v praxi nesetkali s tak malým červem, který by vykazoval takovou rychlost šíření a dokázal způsobit takové škody. Na druhé straně se ale Slammer šířil s takovou vervou a agresivitou, že zpomalil i šíření sebe sama.

Trojský kůň ve službách reklamy: AdwareDropper

Už se vám někdy stalo, že jste dostali e-mailem valentýnku nebo přáníčko k nějakému jinému svátku? Pokud ano, dejte si pozor! S přáníčkem se totiž může do vašeho počítače dostat i něco jiného, co se vám nemusí zrovna líbit. Může to být nevyžádaná reklama nebo třeba virus.

U příležitostí různých svátků se vždy setkáváme s větším či menším množstvím škodlivých kódů, které se jimi inspirují a snaží se je zneužít pomocí metod sociálního inženýrství. Typickým příkladem je i trojský kůň označovaný jako AdwareDropper.

Uvedený trojský kůň byl rozeslán 12. února 2003. E-mail se „tváří“ jako typická elektronická pohlednice zaslaná od „tajného ctitele(ky)“ a obsahuje odkaz, na kterém si ji můžete prohlédnout.



Ve skutečnosti je směřován na soubor CARD.EXE. Ten sice pohlednici vyrobenou ve flashi zobrazí, ale současně také nainstaluje do počítače tři další DLL soubory, které jsou vlastně přídavnými objekty do Internet Exploreru a slouží k monitorování uživatele a zobrazování reklamy.

Protože uživatel není na instalaci těchto souborů nijak upozorněn (např. v licenčním ujednání apod.), lze tento program s určitostí označit za škodlivý kód.

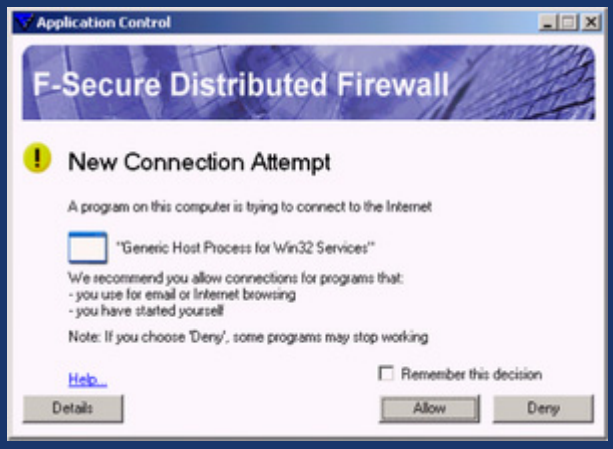
Máte už svůj personální firewall?

Z hlediska dostatečného zabezpečení počítačů připojených k internetu není pochyb, že potřeba personálních firewallů v posledních několika letech stoupá. Důvodů je spousta. V první řadě jsou to stále sofistikovanější počítačové viry a internetoví červi. Významnou oblastí pro aplikaci personálních firewallů jsou tzv. mobilní kanceláře, kdy přenosný počítač putuje spolu se svým uživatelem a je připojován do internetu na různých místech s určitým stupněm ne-bezpečnosti. Typickým příkladem mohou být např. veřejné bezdrátové sítě apod.

Neznalého uživatele je ale třeba upozornit na některé specifické vlastnosti personálních firewallů, kterými se liší od svých velkých příbuzných - podnikových firewallů nasazovaných na internetových bránách. Personální firewall je program, který je určen pro instalaci na koncovou stanici, a až na jisté výjimky jej nelze použít k ochraně více počítačů. Většinou pracuje na principu tzv. paketového filtru, což znamená, že jeho primární funkcí je kontrola obsahu jednotlivých příchozích a odchozích IP datagramů a jejich zpracování podle stanovených pravidel (odkud a kam je paket určen, jaký se používá protokol a port).

Finská společnost F-Secure Corporation, jeden z předních světových výrobců antivirového a bezpečnostního softwaru, uvedla nedávno na trh novou verzi svého personálního firewallu, který se může pochlubit mnoha užitečnými funkcemi a špičkovými parametry.

Základním prvkem F-Secure Distributed Firewallu 5.50 je výkonný paketový filtr, který je dokonale přizpůsoben prostředí pracovní stanice. Pravidla nastavená pro tento filtr jsou uplatňována jak na příchozí, tak i odchozí komunikaci. F-Secure šel však ještě mnohem dál a do svého řešení zabudoval také účinné nástroje pro přímou kontrolu jednotlivých aplikací, která slouží hlavně k ochraně proti škodlivých programům pokoušejících se o komunikaci do internetu bez vědomí uživatele. V případě sdíleného internetového připojení lze distribuovaný firewall použít také jako náhradu plnohodnotného firewallu.



F-Secure Distributed Firewallu 5.50 je kompletně integrován do prostředí centrální správy FSecure Policy Manageru, která je k dispozici zcela zdarma. Administrátor může distribuovaný firewall vzdáleně instalovat, modifikovat jeho nastavení a provádět další zásahy v souladu se stanovenou bezpečnostní politikou.

Uživatel má k dispozici čtyři přednastavené profily. Kromě toho může definovat vlastní pravidla pro další aplikace, jako jsou třeba hry po síti, které nejsou ve standardních filtrech zařazeny. Pravidla pro aplikace mohou být vkládána manuálně nebo automaticky na výzvu aplikačního filtru při prvním pokusu o komunikaci. Firewall také dokáže odhalit případnou modifikaci aplikace.

Ve srovnání s konkurenčními produkty disponuje F-Secure nadmíru propracovaným systémem „logování“. Uživatel má k dispozici hned tři typy záznamů: Action log, Packet log a Alert log. Další velmi užitečnou pomůckou je integrovaný paketový sniffer, s jehož pomocí můžete detailně analyzovat síťový provoz. Aktuální stav firewallu je signalizován ikonou v systémové liště.

Podrobnější popis řešení najdete na www.aec.cz, kde si můžete stáhnout i jeho trial verzi.

Kurzy a semináře AEC v březnu 2003

V průběhu měsíce března 2003 pořádá Centrum vzdělávání AEC následující kurzy:

- **CO JE TO VIRUS, JAKÉ JSOU DRUHY VIRŮ, PREVENCE VIROVÉHO NEBEZPEČÍ, ANTIVIROVÝ SOFTWARE A CENTRÁLNÍ SPRÁVA (3.dubna 2003, Praha; 10.dubna 2003, Ostrava) – Destruktivní působnost virů a jejich rychlý vývoj nutí uživatele počítačů, aby se informovali, jak se jim bránit. V tomto kurzu získáte přehled o typech virů, jejich chování, vlastnostech. Seznámíte se s polymorfními viry, makroviry, s virovými toolkity a s možnostmi ochrany dat před virovou infiltrací, jako jsou např. kontrola přístupu, šifrování, autentizace, ale zejména s antivirovými programy. Účastníci kurzu poznají principy AV programů, funkce a význam jejich centrální správy.**

- **INFRASTRUKTURA PRO SPRÁVU VEŘEJNÝCH KLÍČŮ (PKI), SOFTWAROVÁ KRYPTOGRAFICKÁ OCHRANA (8.dubna 2003, Praha) - Nejcennějším aktivem pro každou firmu jsou její data, informace nashromážděné jejími manažery a zaměstnanci, plány a strategie, průzkumy a rozpočty. O tato data je třeba se odpovídajícím způsobem „starat " - chránit je před zničením, ztrátou či prozrazením. Přitom skutečně spolehlivou metodou ochrany dat je jejich šifrování. A jednou z možností, jak se o šifrování dat postarat, je využít infrastrukturu PKI. Jedná se o zkratku z anglického *„Public Key Infrastructure"* - volně přeloženo to znamená „správa veřejných klíčů". Systém založený na PKI si můžeme zjednodušeně představit jako databázi veřejných klíčů vybavenou řadou nástrojů pro jejich správu a používání. V přednášce budou představeny základní používané technologie a řešení. Seznámíme vás i s vybranými bezpečnostními požadavky na kryptografické moduly.**

Bližší informace ke kurzům Centra vzdělávání AEC naleznete na http://vzdelavani.aec.cz, dotazy lze směrovat na e-mailovou adresu kurzy@aec.cz

Telegrafické informace

AEC na Infosecurity Europe 2003
AEC Data Security Company se v letošním roce účastní výstavy InfoSecurity, která se koná od 29. dubna do 1. května v londýnské Grand Hall Olympia. Naši expozici najdete na stánku číslo 184. AEC bude na svém stánku hostit svého partnera – italskou společnost Eutron.

Antivirové programy z nabídky AEC s VB 100 %
V únorovém čísle magazínu Virus Bulletin byl zveřejněn další z pravidelných testů antivirových programů. V konkurenci pětadvaceti antivirových programů od různých výrobců testovaných na platformě Windows NT získaly ocenění Virus Bulletin 100 % i programy F-Secure Anti-Virus, Kaspersky Anti-Virus, McAfee VirusScan, Norman Virus Control a NOD32, které najdete i v nabídce AEC. Známka VB 100 % je udělována pouze programům, které prokáží výborné schopnosti detekce škodlivých kódů vyskytujících se „In the Wild".

AEC
DATA SECURITY
COMPANY