informační bulletin

AEC DATA SECURITY COMPANY

(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:

- **Metodika zavádění elektronického podpisu**
- **Sasser: další síťové nadělení**
- **Kaspersky Anti-Virus 5.0**
- **Nové verze programů od AEC**
- **Vytvořte si počítačový virus!**

Pro zájemce o problematiku informační bezpečnosti pořádá společnost AEC nejrůznější semináře.

AEC DATA SECURITY COMPANY

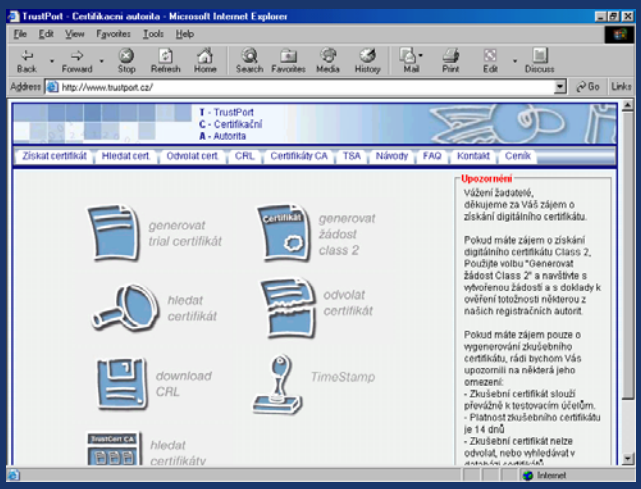
Metodika zavádění elektronického podpisu

Ve čtvrtek 29. dubna 2004 se v Praze v budově Stimbuildingu uskutečnil seminář Metodika zavádění elektronického podpisu.

Seminář byl určen zejména pro zástupce úřadů, organizací a dalších institucí. Bezplatného vstupu využilo více jak pět desítek informací chtivých účastníků, kteří se chtěli dozvědět něco nového o elektronickém podpisu a dalších souvisejících technologiích.

Dvě úvodní přednášky věnované teoretické stránce elektronického podpisu a jeho praktickému použití přednesl Tomáš Přibyl. Ve spontánní diskusi, která po jeho přednáškách následovala, zodpověděl ještě několik velmi zajímavých dotazů. Stěžejní přednášku dne věnovanou samotné metodice zavádění elektronického podpisu na našich úřadech přednesla Olga Přikrylová, která se ve společnosti AEC věnuje mimo jiné také problematice bezpečnostních politik a analýz a má řadu zkušeností z praxe.

Po dobrém obědě se chopil slova Vladimír Fux, který přítomné podrobně seznámil s komplexním řešením elektronické podatelny z vývojové dílny AEC – TrustPort® ePodatelnou. Protože je jedním z těch, kteří se na vývoji tohoto řešení bezprostředně podílejí, mohl účastníkům objasnit i řadu „tajemných“ zákoutí tohoto jedinečného systému, který v současnosti patří mezi nejlepší tuzemská řešení v této oblasti. V závěrečné diskusi ještě padlo několik zajímavých dotazů.



AEC
DATA SECURITY COMPANY

Sasser: další síťové nadělení

Počátkem května 2004 se objevila také nová rodinka internetových červů. Jmenují se Sasser a už se vyskytují ve třech variantách. Díky „dovednostem“, které ovládají, můžeme očekávat, že se budou šířit v podobné míře jako svého času jejich „legendární“ kolega Blaster.

Všechny tři varianty Sasser.A, B i C zneužívají ke svému šíření bezpečnostní chybu v LSASS.EXE, která byla zveřejněna Microsoftem v Security Bulletinu MS04-011 již někdy v polovině letošního dubna.

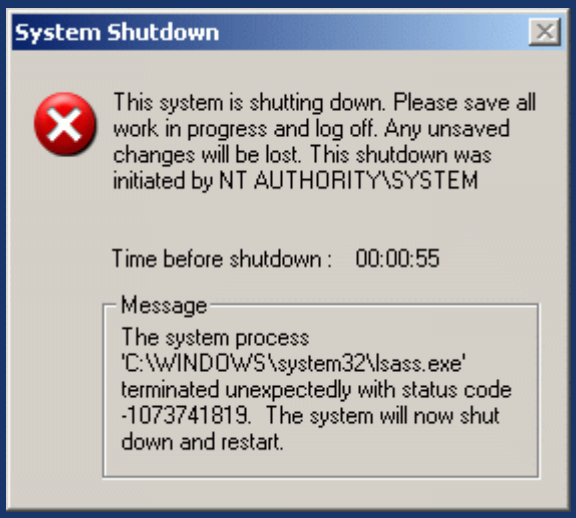
Sasser pracuje tak, že z infikovaného počítače otevírá různý počet spojení nebo na něm spouští různý počet procesů, s jejichž pomocí se snaží nalézt další infikovatelný počítač. Cílovým portem je port 445.

- **Sasser.A – 128 spojení (threads);**
- **Sasser.B – 128 procesů;**
- **Sasser.C – 1024 procesů.**

Rutina pro generování IP adres je nastavena tak, že červ vždy určitou část pokusů směřuje do lokální sítě daného infikovaného počítače, část do okolních sítí a část IP adres generuje zcela náhodně.

Pokud červ najde infikovatelný počítač se systémem Windows 2000 nebo XP způsobí na něm pomocí uvedené bezpečnostní díry „buffer overflow“ v procesu LSASS.EXE. Potom na vzdáleném počítači dokáže na dálku ovládnout na TCP portu 9996 příkazovou řádku, vytvořit skript cmd.ftp a spustit jej. Tento skript přinutí vzdálený počítač ke stažení samotného souboru červa prostřednictvím FTP protokolu na TCP portu 5554 z prvotně infikované stanice a jeho spuštění.

Vedlejším efektem činnosti červa Sasser je porucha činnosti LSASS.EXE, která vede k vynucenému restartu systému. Ten je provázen zobrazením následujícího dialogu:



Jako prevenci proti infekci použijte záplatu, kterou najdete na:
http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

AEC
DATA SECURITY COMPANY

Kaspersky Anti-Virus 5.0

Společnost Kaspersky Labs představila další generaci svých antivirových programů pro operační systémy Windows. Kaspersky Anti-Virus 5.0 se vyznačuje především řadou nových funkcí , novým grafickým rozhraním a vysokou úrovní ochrany proti virům, jak je již u programů z produkce tohoto výrobce zvykem. S novými verzemi svých produktů chce Kaspersky Labs dále upevnit svoje postavení na světových trzích.

Jedním z nejkomplikovanějších problémů dnešních antivirových programů je především znatelné snížení výkonu počítače při kontrole velkých objemů dat na pozadí. Pátá generace produktů Kaspersky Labs tento problém elegantně řeší. Díky integraci unikátních technologií pro zpracování souborů iChecker, iStream a iCache pracují nyní programy Kaspersky Anti-Virus v průměru třikrát rychleji a vyžadují polovinu operační paměti systému než dříve. A to všechno při dalším zvýšení úrovně ochrany a přidání řady nových funkcí. Tento obrovský nárůst rychlosti je umožněn díky využití inteligentního skenovacího motoru a jeho provázáním s Windows cache managerem. Kaspersky Anti-Virus tímto způsobem zabraňuje zbytečnému vícenásobnému skenování souborů, které již byly jednou úspěšně zkontrolovány a shledány „čisté“.

Kaspersky Anti-Virus je efektivní odpovědí na narůstající hrozby virových infekcí přicházejících ve většině případů prostřednictvím e-mailu. Nová verze obsahuje mimo jiné také univerzální modul MailChecker Traffic Monitor, který má stěžejní úlohu v zajištění ochrany a kompatibility při skenování pošty. Díky němu také nemusí uživatel ztrácet čas při složité integraci antivirového programu do svého e-mailového klienta. MailChecker Traffic Monitor se hned po instalaci vloží mezi e-mailový server a klientský program na stanici uživatele a automaticky kontroluje veškerou příchozí i odchozí komunikaci. Tím je zajištěna bezproblémová kompatibilita se všemi e-mailovými programy, které využívají protokoly SMTP a POP3.

Počet útoků škodlivých kódů, které jsou komprimovány nebo se „schovávají“ v archivních souborech či využívají některý jiný způsob komprese svého kódu rok od roku narůstá. Nejúčinnější obranou proti nim je využít účinné dekomprimační technologie, které umožňují zjistit pravý obsah podezřelého souboru. Kaspersky Anti-Virus 5.0 se dokáže vypořádat nejen s komprimovanými soubory, ale také s nejpoužívanějšími formáty souborů archivních, jako je ZIP, ARJ, RAR nebo CAB. Spolehlivě odstraní infekci bez nutnosti manuálního zásahu uživatele do archivu.

AEC
DATA SECURITY COMPANY

Nové verze programů od AEC

Pomyslné brány vývojových laboratoří společnosti AEC opustily nové verze bezpečnostních řešení TrustPort® Disk Protection a TrustPort® DataShredder. Uživatelé v nich najdou řadu novinek a vylepšení.

TrustPort® Disk Protection představuje software pro maximálně transparentní on-line šifrování dat na speciálním virtuálním disku. Nová verze přináší řadu zajímavých novinek, které jistě uživatelé přivítají.

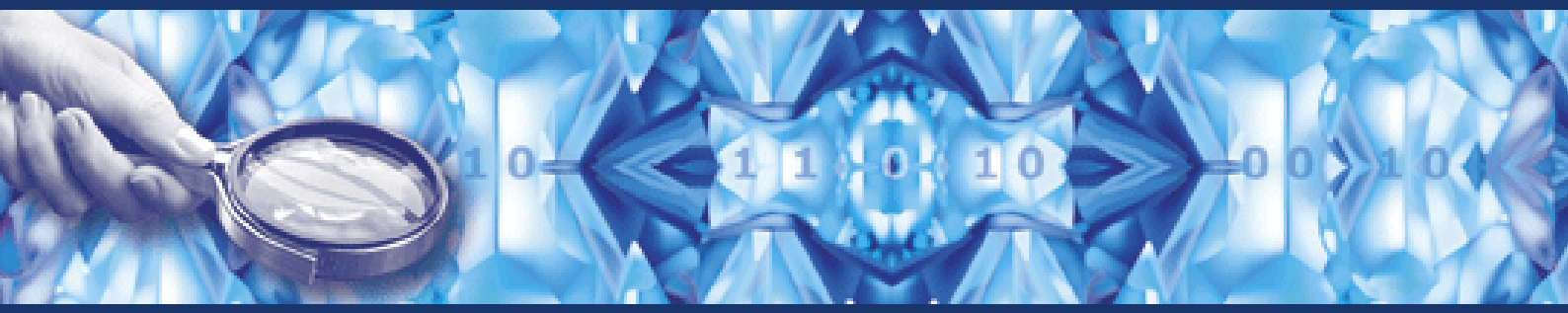
Jednou ze stěžejních novinek je, že TrustPort® Disk Protection ve verzi 3.5 je jednotné rozhranní pro konfiguraci produktu, které je společné s aplikací TrustPort® DataShredder. Na jednom místě tak uživatel najde nejen samotné nastavení, ale také např. správu licenčních klíčů. Přibyly také různé speciální funkce, jako je např. „Hotkey" pro rychlé a bezpečné odpojení všech diskových obrazů stisknutím definované klávesy nebo přehledná historie připojených virtuálních disků. Přímo v panelu Windows pro snadné spouštění nyní uživatel najde seznam aktuálně připojených šifrovaných disků a může je zde také interaktivně odpojovat. Program může být nyní instalován i na operační systémy Windows NT 4.0 (SP6).

Řada nových nástrojů a funkcí v nové verzi najde svoje uplatnění v lokálních sítích firem. Uživatelé již nejsou omezeni pouze prostorem svého počítače. Šifrované virtuální disky nyní mohou být umístěny přímo v lokální síti na podnikových serverech. Zde uložené soubory mohou být sdíleny v jednom okamžiku více uživateli (pouze pro čtení). Administrátoři, kteří tyto sítě spravují, jistě uvítají podporu tzv. „tiché instalace", kdy není vyžadován od uživatele žádný zásah. V nové verzi programu byly také podstatně rozšířeny možnosti parametrů při použití programu z příkazové řádky.

TrustPort® Disk Protection 3.0 je atestován dle standardů ISVS pro použití v informačních systémech státní správy.

Také v nové verzi 2.5 programu TrustPort® DataShredder uživatelé naleznou některé významné změny. Aplikace (včetně správy licenčních klíčů) byla taktéž převedena pod jednotné konfigurační rozhranní a byla přidána možnost spouštění programu přímo z panelu pro snadné spouštění. Skartovací jádro bylo optimalizováno, přičemž skartovací funkce byly rozšířeny např. o možnost skartace historie adres zadaných do Internet Exploreru. Administrátoři jistě uvítají možnost ovládat program přímo z příkazové řádky, včetně použití parametrů.

AEC
DATA SECURITY COMPANY



Vytvořte si počítačový virus!

Pokud teď čekáte návod na to, jak vytvořit ten zaručeně nejúspěšnější počítačový virus všech dob, pak asi budete zklamáni. Řeč totiž nebude o programování škodlivých kódů, ale o nástrojích, které se k jejich vytvoření používají. O tzv. virových generátorech.

Dávno pryč je doba, kdy naprogramování počítačového viru vyžadovalo kdovíjak hluboké znalosti programování a další dovednosti. Dnes se může „autorem“ viru stát prakticky kdokoliv. Stačí se z Internetu stáhnout speciální program, který virus na základě předdefinovaných údajů vytvoří.

„Normální lidé“ se přitom nemusejí obávat. Žádná volba „Vytvořit nebezpečný virus šílených destrukčních schopností“ v žádném generátoru není a ani být nemůže. Jedná se totiž o pouhý počítačový program, který dělá to, co mu jeho tvůrci dají do vínku. A tak máte možnost vybrat si sice z mnoha, leč přesně předdefinovaných vlastností. Pod jakým názvem se bude virus šířit? Bude polymorfní? V jakém operačním systému se bude šířit? Jak a kdy se bude projevovat?

Generátor virů je vlastně podobným programem jako třeba grafický či textový editor: Nabídne mnoho variant a uživateli možnost seberealizace, ale jen v přesně daných mantinelech. Což ale neznamená, že v grafickém či textovém editoru nemohou vzniknout zajímavé věci – tento je ale vždy pouze prostředkem, nikoliv cílem.

Generátory virů tak jsou zajímavou součástí počítačového světa, ale nějaké obrovské ohrožení nepředstavují. Jak uvádí Eugen Kaspersky z antivirové firmy Kaspersky Lab: „Jednou se mi do ruky dostal balíček celkem patnácti tisíc virů. Všechny byly vytvořeny jedním člověkem za pár hodin.“ Vzhledem k tomu, že tyto každý z těchto virů byl sestaven podobným způsobem, měly přes svou na první pohled patrnou rozdílnost (různá jména, projevy apod.) mnoho společných znaků. “Vytvořit detekční mechanismus na chytání a léčení těchto patnácti tisíc virů mi zabralo pár minut,” vysvětluje Kaspersky a ještě dodává: „Přitom tento mechanismus je schopen odhalovat všechny viry vytvořené dotyčným generátorem. Takže sebelépe vymyšlený virus vytvořený pomocí tohoto nástroje má stejně nulovou šanci uspět jako ten nejjednodušší.“

Je zajímavé, že slavný škodlivý kód Anna Kurnikovova byl také vytvořen pomocí generátoru virů VBSWG (Visual Basic Script Worm Generator). Jeho značné rozšíření je přitom dáváno do souvislosti s neopatrností uživatelů, neboť většina antivirových programů si s ním byla při správném používání a aktualizaci schopna poradit ještě dříve než vznikl.

AEC
DATA SECURITY COMPANY