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:

- **Ohlédnutí za konferencí Security 2004**
- **Novinky mezi škodlivými kódy: NetSky.V**
- **Elektronická podatelna s atestem**
- **AEC míří do Polska**

V úterý 6. dubna se v prostorách hotelu Andel´s uskutečnila pod záštitou AEC a za mediálního partnerství vydavatelství Vogel Burda Communications tradiční konference Security 2004.

AEC DATA SECURITY COMPANY

Ohlédnutí za konferencí Security 2004

Každoročním vrcholem mezi akcemi věnovaným oblasti počítačové bezpečnosti je konference Security, kterou už mnoho let pořádá společnost AEC. Nejinak tomu bylo i letos – konference se uskutečnila v Praze v úterý 6. dubna.

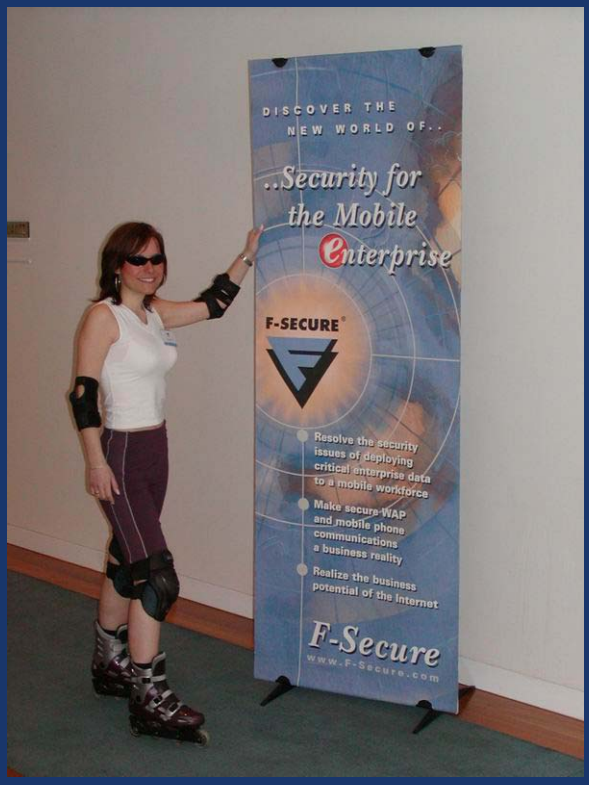
Staré dobré fotbalové pravidlo praví, že „trenér nemění osvědčenou sestavu“. A tak ani AEC nezasahovalo od posledního většího zemětřesení na přelomu tisíciletí (změna názvu konference z Virus na Security, zkrácení akce ze dvou na jeden a den a změna periodicity ze dvouleté na roční) do podoby konference. Ovšem nelze věčně spát na vavřínech, a tak návštěvníci mohli v roce 2004 jednu radikální změnu přece jen zregistrovat: po mnoha letech jsme opustili zaběhnuté konferenční prostory a poprvé zrealizovali akci v prostorách hotelu Andel´s. Nyní už můžeme konstatovati, že to byl krok správným směrem.

Letošní konferenci pomohla zajistit nejen pořadatelská společnost AEC, ale také mediální partner Vogel Burda Communications (Chip, Počítač pro každého, Level aj.). Záštitu nad akcí převzalo Ministerstvo informatiky, patronaci Tuesday Business Network a hlavním zahraničním partnerem se stala společnost F-Secure.

A co bylo na programu konference? Především vystoupení předních českých i zahraničních odborníků – na rozdíl od jiných podobných akcí přitom dostávají na Security výběr lidé takříkajíc z praxe. Jejich výklady tak nejsou suchopárnou teorií, ale seznámením se skutečnými problémy, s nimiž se administrátoři i uživatelé dnes a denně mohou setkat (a také setkávají).

Pokud bychom měli zmínit alespoň některá témata přednášek, pak jsou to:

- Viry a spam – bratři ve zbrani
- Firewally: bojovníci první linie
- Tajemství IDS/IPS
- Virová události za poslední rok v kostce
- Počítačová bezpečnost a reálný svět



A další a další a další. Kdo přišel, rozhodně nelitoval. A kdo nepřišel? Bude mít možnost svou chybu napravit v roce 2005. Velký zájem posluchačů je totiž už nyní zárukou, že konference Security bude uspořádaná i příští rok.

AEC
DATA SECURITY COMPANY

Novinky mezi škodlivými kódy: NetSky.V

NetSky.V, který se objevil v pozdních nočních hodinách 14. dubna 2004, se nešíří jako soubor přiložený k infikovanému e-mailu. Místo toho zneužívá dvojici bezpečnostních děr.

NetSky.V se šíří pomocí e-mailové zprávy v HTML formátu, která obsahuje odkaz na stránku umístěnou na již infikovaném počítači, ze kterého byl inkriminovaný e-mail odeslán. Pomocí bezpečnostní chyby známé jako „Microsoft Internet Explorer XML Page Object Type Validation Vulnerability (MS03-040)“ dochází v okamžiku, když uživatel na tento odkaz v e-mailu klikne, ke stažení speciálně vytvořené HTML stránky prostřednictvím portu 5557. Tato HTML stránka zneužívá další bezpečnostní díru „Internet Explorer Object Data Remote Execution (MS03-032)“, která dovolí stažení a spuštění spustitelného souboru červa ze stejného dříve infikovaného počítače (odkud došlo ke stažení HTML stránky). K tomuto červ zneužívá přímo FTP klienta (prostřednictvím portu 5556).

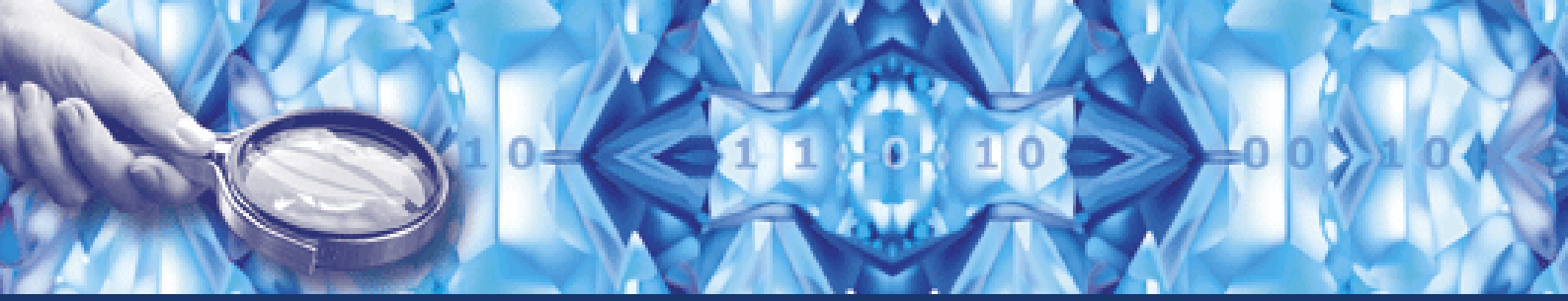
Podrobné informace o uvedených bezpečnostních dírách najdete přímo na stránkách Microsoftu:
http://www.microsoft.com/technet/security/bulletin/ms03-032.mspx
http://www.microsoft.com/technet/security/bulletin/ms03-040.mspx

Programový kód verze „V“ je velmi podobný verzi předchozí. Některé jeho části jsou šifrovány. Na infikovaný počítač se červ kopíruje jako soubor EastAV.exe do systémového adresáře Windows. Svoje spuštění při každém startu operačního systému si zajišťuje pomocí klíče v systémovém registru.

E-mailové adresy pro svoje další šíření NetSky.V získává podobně jako předchozí verze extrahováním z určitých typů souborů nalezených na lokálních discích. „Infikovaná“ zpráva (resp. zpráva s odkazem vedoucím k infekci) může mít několik různých podob.

Červ je naprogramován tak, aby v období od 22. do 29. dubna prováděl DoS (Denial of Service) útok na vybrané webové servery.

AEC
DATA SECURITY COMPANY



Elektronická podatelna s atestem

Řešení elektronické podatelny, které vzniklo ve společnosti AEC a bylo prezentováno na konferenci ISSS 2004, získalo atestaci na shodu se standardy ISVS.

Atest číslo 04-20040112, který vydalo atestační středisko společnosti BDO IT, a.s. v Praze dne 22. března 2004, vyjadřuje shodu řešení TrustPort® ePodatelna s následujícími standardy ISVS:

- ***Standard ISVS pro náležitosti procesu a metodiky atestace jakosti produktů 007/01.02.***
- ***Standard ISVS pro náležitosti životního cyklu informačního systému 005/02.01.***
- ***Standard ISVS pro provoz elektronických podatelen ve vztahu k používání zaručeného elektronického podpisu 016/01.01.***

TrustPort® ePodatelna představuje kompletní webové řešení elektronické podatelny. Zpracovává podání v elektronické podobě a předává je úředníkům příslušného úřadu či instituce. Formuláře pro jednotlivá podání jsou zobrazovány a vyplňovány uživatelem na zabezpečených www stránkách. Samotné vytvoření elektronického podpisu probíhá v e-mailovém programu na počítači uživatele. Ten si tedy vystačí pouze s běžným webovým prohlížečem s podporou SSL a poštovním klientem s podporou S/MIME, což jsou naprosto standardní nástroje. Pro úředníka elektronické podatelny je k dispozici vnitřní rozhranní, které slouží předání podání příslušnému odboru úřadu.

AEC míří do Polska

Jedním z úspěchů dosažených společností AEC na letošním veletrhu CeBIT je podpis distribuční smlouvy s polskou společností DAGMA (www.dagma.pl). Díky ní si budou programy z řady TrustPort® lehce dostupné i pro polské zákazníky.

Na základě uvedené smlouvy s firmou DAGMA byl program TrustPort® eSign kompletně lokalizován do polského jazyka a má tak k našim polským zákazníkům daleko blíže, než ostatní konkurenční produkty.

TrustPort® eSign je aplikace sloužící k zabezpečení elektronické komunikace. Je založená především na asymetrickém šifrování a technologii elektronického podpisu. S jeho pomocí může uživatel jednoduše šifrovat/dešifrovat soubory a vytvářet/ověřovat jejich elektronický podpis. Unikátní je i podpora časových razítek, která jsou k elektronickému podpisu vytvářena. Program obsahuje také nástroje ke kompletní správě privátních klíčů, certifikátů, CRL atd.

Společnost DAGMA Sp. z o.o. působí v polských Katovicích již od roku 1987. Kromě jiného se zabývá také např. antivirovou ochranou, bezpečností sítí, firewally apod. Je držitelem certifikátu ISO 9001:2000.

AEC
DATA SECURITY
COMPANY