

AEC Magazín – Viry, antiviry a bezpečnost

Milí přátelé!

Vítáme Vás při četbě našeho informačního bulletinu, který má za cíl seznámit Vás s novinkami na poli virů, antivirů a bezpečnosti dat všeobecně.

Z dnešního obsahu vybíráme:

OHLÉDNUTÍ ZA KONFERENCÍ SECURITY 2000	1
PO „LÁSCE“ PŘIŠLA „NOVÁ LÁSKA“	3
TIMOFONICA – VIRUS, KTERÝ ÚTOČÍ NA MOBILNÍ TELEFONY	3
AVP UMÍ ČISTIT VBS	4
TRUSTCERT PŘÍCHÁZÍ SE SERVEROVÝMI CERTIFIKÁTY	4
O FIRMĚ AEC, SPOL. S R.O.	4

Příjemné počtení a co nejméně potíží s viry a zabezpečením dat přeje Vaše firma

AEC, spol. s r.o.

Ohlédnutí za konferencí Security 2000

V prvních dvou červnových dnech proběhla konference Security 2000, tedy akce, jejíž historie se začala odvíjet již v roce 1992. V minulých letech se sice tato významná akce jmenovala Virus a až letošní ročník nese název Security, ale vždy se jednalo o konferenci zaměřenou na problematiku virů, antivirů a ochranu dat.

Pro rok 2000 jsme jako organizátoři váhali, jak nazvat v pořadí již pátou konferenci „Virus“. Vzhledem k širšímu významu pojmu bezpečnost dat (security) a neustále rostoucí potřebě zajištění informací nejen před viry, ale především i před jejich zcizením, záměnou a zneužitím a prolínáním se obou „oborů“ se přikláníme pro rok 2000 k hlavnímu názvu „SECURITY 2000“. Objevilo se i několik názorů, že by bylo napříště vhodné se vrátit k dřívějšímu názvu, který by snad přilákal ještě více lidí i z řad „neodborníků“, ale vzhledem k rozsahu a zaměření konference i na jiné oblasti bezpečnosti dat, než jen na antivirovou ochranu i nadále zůstáváme u názvu Security. Jedinou otázkou do budoucnosti zůstává skutečnost, zda budou od příštího roku tyto konference, vzhledem k jejich úspěšnosti a myslíme i potřebnosti, pořádány, namísto jednou za dva roky, každý rok.

A jak proběhla konference Security 2000? Zájem odborné i neodborné veřejnosti byl, stejně jako v předchozích letech veliký. Letošní seminář navštívilo téměř čtyři sta zájemců o informace z oblasti virové a antivirové problematiky (starší i nové viry, antivirové programy a jejich nasazení v praxi apod.), ale také např. o problematiku elektronického podpisu a kryptografie.

Program byl, stejně jako v minulých letech, rozdělen do dvou dnů. První den byl více zaměřen na virovou a antivirovou problematiku, zatímco druhý den se zabýval spíše právními otázkami z oblasti ochrany dat, zákonem o elektronickém podpisu, kryptografií apod. Díky tomuto členění si mohli účastníci lépe vybrat a snadněji tak naplánovat svoji účast na konferenci. Například zájemce o informace výhradně z oblasti kryptografie nemusel absolvovat oba konferenční dny a stačilo mu přijet až na den druhý.

Akce se po všech stránkách vydařila a svědčí o tom nejen vynikající odborná úroveň všech přednášejících, ale i velký zájem posluchačů, nejen během přednášek (sál byl po celou dobu konference zaplněn), ale i během diskuse a několik dní po konferenci, kdy někteří přednášející odpovídali na otázky i prostřednictvím elektronické pošty.

Pokud byste se chtěli dozvědět o jednotlivých přednáškách trochu více, navštivte internetové stránky konference www.security2000.cz, na kterých najdete většinu anotací přednášek, včetně prezentací v PowerPointu. A jestliže jste se letošní konference nemohli z jakéhokoliv důvodu zúčastnit, přijměte pozvání alespoň na tu příští. Určitě nebudete litovat.



Mediálním partnerem konference se stalo vydavatelství Vogel Publishing. Na snímku ředitel divize Computer Media ing. Milan Loucký.



Chvilí před bojem jsou horší než boj samotný...



Jiří Mrnušík (AEC) hovoří, Milan Loucký (Vogel Publishing) se modlí



Petr J. Drahovzal („Viry a právo“) zoufale studuje otázku v průběhu diskuse.



Ke slovu přišla i moderní technika.



Pavel Baudiš (Alwil) a Petr Odehnal (Grisoft) se krčí ve stínu AEC.

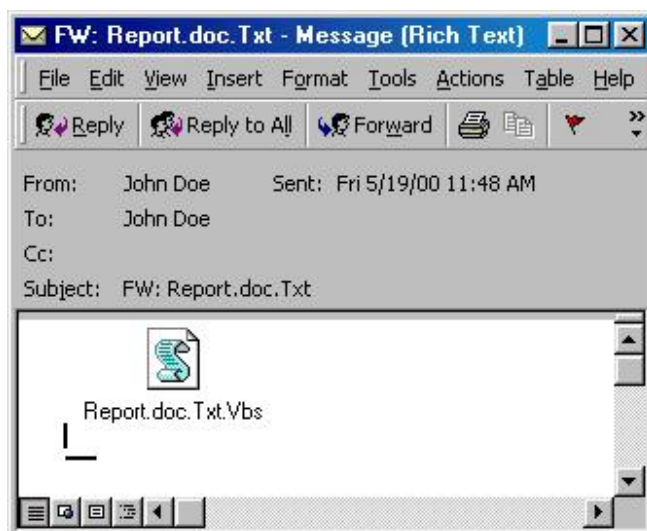
Po „Lásce“ přišla „Nová láska“

V polovině zaútočil na počítače nový e-mailový červ (speciální případ počítačového viru) NewLove. Napsaný byl podobně jako o dva týdny dříve kód Iloveyou.

Naštěstí se tentokrát nedočkal většího rozšíření, což bylo vzhledem k jeho nebezpečnosti jen dobře. NewLove je totiž schopen se šířit nejen pomocí elektronické pošty (e-mail), ale také ničí prakticky všechny soubory v napadeném počítači i na síťových discích. Jinými slovy: Stačí jeden napadený počítač (tedy jeden neukázněný uživatel, který spustí zavirovanou přílohu u e-mailové zprávy) v podnikové síti a dojde k nenávratnému zničení obrovského množství dat umístěných na síti a za určitých okolností také v počítačích ostatních uživatelů sítě. O tom se ostatně přesvědčili uživatelé jisté nejmenované kalifornské společnosti, kde virus „vyluxoval“ data z pěti tisíc počítačů.

Lidé pracující s počítači v ČR byli tentokrát velmi obezřetní. Několik kopií NewLove sice dorazilo prostřednictvím Internetu i k nám, ale drtivá většina uživatelů byla pod vlivem událostí z minulých týdnů pozorná. Antivirovým firmám bylo hlášeno několik spíše ojedinělých případů incidentů.

„Musíme pochválit jednak uživatele a jednak média,“ uvádí technický ředitel antivirové firmy AEC Pavel Mrnušík. „Uživatelé, neboť se ukázali a jsou opatrní při spouštění příloh u e-mailových zpráv. A média, neboť uživatele tentokrát zavčas upozornila na hrozící nebezpečí, čímž zabránila dalekosáhlým škodám.“



Timofonica – virus, který útočí na mobilní telefony

Dnes již málokdo pochybuje o tom, že se dříve nebo později objeví škodlivé programové kódy (viry), které zasáhnou mobilní telefony. Současné mobily sice v žádném případě nedávají virům šanci, ale s tím, jak se budou rozšiřovat jejich možnosti, bude škodlivým kódům vznikat živná půda.

Počátkem června 2000 spatřila světlo světa první vlašťovka z této kategorie: Počítačový virus, který majitele mobilních telefonů alespoň obtěžoval posíláním SMS zpráv. Pojmenovaný byl Timofonica – podle předmětu e-mailové zprávy, kterou se šířil a také podle telefonního operátora, jehož služby kritizoval.

Timofonica se do počítače dostane zprávou, která má jako předmět uvedeno právě jméno tohoto operátora, přičemž v jejím těle je španělsky psaný text hodnotící jeho služby a tržní chování. Na konci je připojený soubor TIMOFONICA.TXT.vbs. Poté, co se uživatel pokusí připojený soubor spustit, nastává víceméně klasická infekční rutina: Timofonica rozesílá své kopie na všechny adresy ze seznamu kontaktů MS Outlooku.

Za každou odeslanou zprávou s infikovanou kopií vygeneruje jedno náhodné číslo a odešle zprávu na e-mailovou adresu (náhodné číslo)@correo.movistar.net. Zpráva má předmět "TIMOFONICA" a text „informa que: Telefónica te está engañando.“ Adresa correo.movistar.net je přitom SMS bránou, která distribuuje uživatelům mobilních telefonů e-mailové zprávy. A tak dochází k tomu, že Timofonica spamuje (tedy obtěžuje nevyžádanou poštou) uživatele mobilních telefonů.

AVP umí čistit VBS

S obrovským rozmachem počítačových virů psaných v jazyce VBS (Visual Basic Script), jakými se stal např. Iloveyou, NewLove či několik desítek jejich variant, je zapotřebí disponovat také dostatečně kvalitní antivirovou ochranou, která si s nimi poradí. Přední světový antivirový program AVP (výrobce Kaspersky Lab) je nyní k dispozici i ve verzi Script Checker. Jedná se o heuristický kontrolní program, který je schopen odhalit známé i neznámé škodlivé kódy ve VBS a dalších skriptovacích jazycích. Neváže se přitom k žádnému konkrétnímu programu z produktové řady AVP, Script Checker je jakýmsi filtrem mezi aplikacemi a „motorem“, který zajišťuje vykonání skriptů (např. Windows Script Host). Navíc je k dispozici ZDARMA.

Trustcert přichází se serverovými certifikáty

Certifikační autorita AEC, spol. s r.o. nacházející se na webovské adrese **www.trustcert.cz** začala nabízet vydání ověřených certifikátů různých úrovní také pro servery (především pro Linux, Lotus Notes či IIS - Internet Information Server).

Jak uvádí jednatel společnosti AEC ing. Jiří Mrnušík: „Jedná se o významný krok vpřed v oblasti bezpečnosti na Internetu. Serverový certifikát je určen pro autentizaci serveru a pro zajištění bezpečné komunikace mezi ním a uživateli. Ti pak získávají jistotu, že server je skutečně tím zařízením, za které se vydává. To je mimořádně důležité zejména v okamžiku, kdy stahujeme soubory a potřebujeme mít stoprocentní jistotu ohledně jejich původu – třeba v případě aktualizací antivirových programů. Certifikace je samozřejmě možná obousměrně, takže server si může ověřit autenticitu uživatele a na základě předchozích informací mu umožní přístup k předplaceným službám či informacím.“

Všem zájemcům umožňuje certifikační autorita Trustcert ZDARMA generovat certifikáty DEMO pro výše uvedené servery.

O firmě AEC, spol. s r.o.

AEC, spol. s r.o. je jedním z předních poskytovatelů a výrobců software pro komplexní zabezpečení osobních počítačů jak z hlediska utajení informací, tak antivirové ochrany. Za své produkty obdržela několik prestižních ocenění a také certifikací ISO 9001 a TickIT. Společnost

byla založena v roce 1991. Jedná se o ryze českou firmu bez účasti zahraničního kapitálu. V současnosti disponuje prodejní sítí, pokrývající ČR i SR s kanceláři v Praze, Brně a Bratislavě. Důkazem toho, že Slovensko není jediným zahraničím, ve kterém AEC, spol. s r.o. působí, je distribuční síť v Belgii, Holandsku, Kanadě, Lucembursku, Maďarsku, Německu a v dalších zemích.

Kontakty:

Autorem „AEC Magazínu“ je Tomáš Příbyl: tomas.pribyl@aec.cz

AEC, spol. s r.o.

Bayerova 30, 602 00 Brno
Tel.: 05 / 4123 5466-7
Fax: 05 / 4123 5038
e-mail: info@aec.cz

AEC, spol. s r.o.

Vinohradská 184, 130 52 PRAHA 3
Tel./fax: 02 / 6731 4326 nebo 1402
e-mail: paha@aec.cz

AEC Bratislava, spol. s r. o.

POB 79, Pribinova 25, 810 11
BRATISLAVA, SK
Tel.: +421 (0)7 50633 027
Fax: +421 (0)7 50633 029
e-mail: bratislava@aec.sk