Konference Security 2001

7. června 2001, Praha, Národní dům na Vinohradech

Program

8.00 - 9.00	Prezence	11.20 - 12.20	Bezpečnost na Internetu, rizika elektronického obchodu
9.00 - 9.10	Úvod	12.20 - 13.00	Přestávka - občerstvení
I. blok	**Bezpečnost dat**	13.00 - 13.20	Hardwarové autentizační prostředky
9.10 - 9.20	Elektronický podpis Zavádění elektronického podpisu do praxe	13.20 - 13.40	Možnosti zabezpečeného monitoringu a správy DMZ
9.20 - 9.30	Zákon o elektronickém podpisu z pohledu právníka. Implementace zákona v české legislativě, pozitiva a úskalí, návaznost na direktivy a zákonné a standardizační prostředky a aktivity EU	13.40 - 14.00	Bezpečnost v MS Windows 2000, PKI, kerberos, smart card
		II. blok	**Antivirová ochrana**
9.30 - 9.50	Zákon o ochraně utajovaných skutečností a ochraně osobních údajů	14.00 - 14.30	Celkový obraz virové a antivirové problematiky v roce 2000, výhledy na rok 2001
9.50 - 10.10	Zákon o elektronickém podpisu, akreditace CA, uplatnění certifikátů v praxi.	14.30 - 15.00	Jaké prostředí dnes tvoří živnou půdu pro viry, nové hrozby, modelové útoky
10.10 - 10.40	Přestávka - občerstvení	15.00 - 15.30	Moderní trendy aplikované v AV programech
10.40 - 11.00	Analýza rizik ve společnosti, lidský faktor	15.30 - 16.00	Přestávka - občerstvení
11.00 - 11.20	Vývoj kryptografických technologiíc, autorita časové značky, problematika odvolávání certifikátů	16.00 - 16.30	Postup při nasazování AV ochrany ve společnosti, projekty, pilotní instalace
			Diskuse a závěr
			Večerní raut

AEC DATA SECURITY COMPANY **Bulletin**

www.aec.cz, www.trustcert.cz **březen/2001**

SECURITY 2001

Praha 7. června

Úvod

Deset let. Přesně tak dlouho působí na českém počítačovém nebi hvězda jménem AEC. Na rozdíl od mnoha jiných hvězd se nestala kometou, která zazáří, aby vzápětí poté mohla nenávratně zmizet v hlubinách bezbřehého vesmíru. AEC se během uplynulých deseti let změnila ve hvězdnou stálici nejen na nebi českém, ale i světovém.

Ve srovnání s dobou existence vesmíru je deset let zanedbatelná doba - ale na druhé straně je to doba dostatečně dlouhá na založení a vytvoření úspěšné firmy působící v oblasti zabezpečení elektronických dat (počítačové viry, antivirová problematika, kryptologie, elektronický podpis, šifrování, bezpečná skartace dat apod.).

Protože již Lev Nikolajevič Tolstoj prohlásil, že „provaz je dobrý dlouhý a řeč krátká“, přeji Vám krásný (nejen) dnešní den a co nejméně bezpečnostních incidentů! AEC je pro Vás v dané oblasti tím nejlepším partnerem.

Tomáš Přibyl
tomas.pribyl@aec.cz

E-mailový červ Myba

Myba se šíří v exe souboru. Programový kód tohoto červu (speciální případ viru, který se šíří prostřednictvím elektronické pošty) byl napsán ve Visual Basicu a následně zkompilován do exe aplikace. Části kódu jsou přitom beze zbytku „opsané“ z nechvalně proslulého červu Iloveyou. Další rutiny jsou upravené jen lehce.

Myba se šíří e-mailovými zprávami s následující podobou:
Předmět: My baby pic !!!
Tělo: Its my animated baby picture !!
Příloha: Mybabypic.exe
Myba obsahuje velmi nebezpečnou rutinu, která může jednoduše zničit důležitá data na počítači. V závislosti na systémovém datu počítače na všech dostupných discích poruší soubory s koncovkou VBS, VBE, JS, JSE, CSS, WSH, SCT, HTA, PBL,CPP, PAS, C, H, JPG, JPEG, MP2 a MP3.

Pozor na "Naked Wife"!

Červ Naked je napsaný ve Visual Basicu 6 a světem se šíří jako příloha zpráv elektronické pošty v souboru NakedWife.exe, o velikosti 74 kB. Nebezpečný je především tím, že se snaží z adresáře Windows smazat soubory s příponami com, exe, dll, bmp, log a ini, což vede ke ztrátě operačního systému.

Po spuštění souboru NakedWife.exe se zobrazí animace podobná ShockWave Flash, obsahující menu. Položky menu jsou nefunkční s výjimkou Helpu, který zobrazí hlášení "You're are now FU.ED! (C) 2001 by BGK (Bill Gates Killer)".

Červ se vzápětí automaticky rozešle pomocí aplikace MS Outlook na všechny adresy ze seznamu adres. Šíří se přitom ve zprávě s následující podobou:

Předmět: Fw : Naked Wife
Tělo: > My wife never look like that! ;-)
Best Regards,
[Uživatel]
Příloha: NakedWife.exe
Kde volba [Uživatel] je jméno infikovaného uživatele.

Anna Kurnikovova do každého počítače

Z technologického hlediska nejde v případě počítačového červu „Kurnikovova“ (objevují se ovšem i označení jako Lee, Anna či Kalamar) o žádnou novinku. Byl vytvořen pomocí virového generátoru [K]Alamar's Vbs Worms Creator. To je program, který umožňuje vytvořit počítačový virus "na míru" - podle stanoveného zadání.

Jediným projevem tohoto škodlivého kódu je kromě masového šíření jen to, že se vždy 26. ledna pokusí přesměrovat startovací stránku internetovského prohlížeče na stránky jisté nizozemské webové prodejny.

Melissa se vrátila

Sedmnáctého ledna 2001 byl poprvé zaregistrován škodlivý kód Melissa.W, který se šíří pomocí elektronické pošty v souboru Anniv.doc. O dva dny později má její výskyt již podobu epidemie, která se šíří po celém světě - nevyhnula se přitom ani České republice. AEC zaznamenala desítky zpráv o napadení tímto kódem.

Melissa.W ve skutečnosti není revoluční novinkou. Skoro by se dalo říci, že ve srovnání s původní Melissou je téměř stejná - změnila se pouze jedna (ovšem poměrně podstatná) věc. Infikovaný soubor Anniv.doc je MS Wordem pro počítače Macintosh. A v tom je celý problém: Jednak si některé antivirové programy s tímto relativně novým formátem nedokáží poradit a jednak se jedná o první virus právě v tomto formátu. Soubor i virus jsou přitom plně funkční nejen pod Macintoshem, ale také pod windowsovými verzemi MS Office.

Hermes, virus s příchutí domoviny

Ano, je to tak. Opět se objevil počítačový virus, který se do světa šíří z krásné země v srdci Evropy, z České republiky. Jeho jméno je Hermes.

Jedná se o e-mailového červa napadajícího MS Outlook. Červ samotný je Win32 aplikace, velká cca 20 kilobajtů (protože je jeho tělo komprimováno; ve skutečnosti má zhruba trojnásobnou velikost). Hermes je napsaný v jazyce Visual Basic.

Červ využívá MAPI funkcí, získává kontakty z Address Book a posílá na ně e-mailové zprávy s předmětem "Re:", přičemž v těle zprávy není nic jiného než jméno odesílatele.

Autorizované středisko podpory NAI

Od doby ne tak dávné pyšní se naše firma novým titulem. Ano, stali jsme se autorizovaným střediskem podpory pro antivirové produkty firmy Network Associates. Tato informace byla zveřejněna nejen na našich webových stránkách (www.aec.cz), ale byla patřičně medializována i v průběhu nedávného setkání našich partnerů a novinářů na Prvním partnerském dni v Praze. Naši stávající i příští zákazníci se mohou na tuto novinku v seznamu poskytovaných služeb těšit v nabídkách.

Přívlastek "autorizované" přináší našemu centru podpory výjimečnost, kterou se v České republice pyšní právě, pouze a jedině AEC. Tuto výsadu získala firma AEC na základě přísných výběrových podmínek, které si společnost Network Associates stanovuje sama. Těší nás o to víc, že právě tento důkladný výběr a následná volba byly plně v režii NAI, a tím nejlepším byla pro oblast České republiky zvolena právě naše společnost.

Co předcházelo získání titulu a jaké vlastně byly podmínky, které jsme splňovali či později museli splnit?

Prvotním popudem k celému procesu bylo oslovení ze strany NAI na základě výběru. Naše společnost má na trhu antivirové ochrany a bezpečnostních produktů již dlouhou dobu své pevné místo. Právě v těchto dnech slavíme desáté výročí vzniku AEC. Přední pozici si AEC stále udržuje díky profesionálnímu týmu odborníků, kteří byli a jsou schopni vyvíjet a podporovat celé portfolio produktů této oblasti, ať se jedná o vývoj unikátního světově konkurence-schopného a přitom ryze českého bezpečnostního řešení s názvem IronWare Security Suite (nyní Norman Security Suite) nebo o podporu a poskytování služeb antivirových produktů, jako jsou programy firmy NAI (sekce McAfee), KAV/AVP (z dílny Kaspersky Lab), Norman, F-Secure (dříve DataFellows) a další. Služby týkající se technických a odborných znalostí jsou neustále na vysoké úrovni a odezva našich spokojených zákazníků i stále více zájemců o podporu pro tyto produkty svědčí o tom, že jdeme správnou cestou.

Cílem NAI je vybudovat jedno autorizované centrum v každém regionu. Pro AEC z toho plyne, že plní funkci ASC (Authorized Support Centre) v regionu České republiky. Smlouva o poskytování podpory pod hlavičkou ASC byla podepsána začátkem roku 2001 a následovala příprava na povinné autorizované školení vybraných specialistů, které čekala cesta za La Manche, na ostrov nyní tak těžce zkoušený v oblasti zemědělství.

Měla jsem to štěstí být jedním z oněch dvou techniků, kteří měli absolvovat ono školení a posléze také podat příslušné informace o jeho průběhu. Tady jsou: Relativně nedaleko od Londýna, (vzhledem k celkové délce cesty), asi hodinu jízdy autem leží město Aylesbury. Tady byste našli sídlo anglické pobočky společnosti Network Associates, které skrývá mimo jiné i technické týmy, pěkně systematicky rozdělené podle jednotlivých produktů, které NAI vyvíjí. Protože cílem našich snah bylo stát se autorizovanými pro podporu antivirových produktů, byli jsme přiděleni k odpovídající skupině odborníků, kteří se celé dva týdny prezentovali svými znalostmi a praktickými ukázkami toho, co se peče pod pokličkou antivirové produkce. Mám být konkrétní? Tak tedy absolvovali jsme školení na VirusScan, NetShield, GroupShield, WebShield, Management Edition Console, ePolicyOrchestrator, Eppliance aj. v aktuálních verzích. Kromě mluveného slova a bezděčného srovnávání bezpočtu dialektů používaných jednotlivými školiteli bylo možno srovnávat i úroveň a hloubku jejich zkušeností, pokud nám dovolili shlédnout víc než normálním smrtelníkům, a přitom posuzovat, jak jsme na tom se svými znalostmi. S pýchou můžeme tvrdit, že se nemáme za co stydět.

A tak po 14 dnech odjížděli z Anglie dva spokojení, vědomostmi a spoustou dalších informací naplnění, dokumentací a zavazadly obtěžkaní, ale hlavně - certifikovaní technici (i s barevnými certifikáty).

Je zde hlavně další podmínka, za které smíme používat titul ASC. Veškeré naše působení pod touto hlavičkou, zejména spokojenost našich zákazníků, úroveň naší podpory, rychlost a kvalita, což jsou nejdůležitější měřítka pro poskytování profesionálních služeb, jsou sledovány, posuzovány a průběžně vyhodnocovány již nejen námi samotnými, ale také ze strany NAI. Jsou to ale také některé výhody, které nám nyní umožňují poskytovat ještě lepší a profesionálnější služby. Zejména přednostní přístup k informacím, AVERT týmu a know-how, využití našich znalostí v marketingových a PR aktivitách, aktivní odkaz z webovských stránek NAI směřující na AEC pro zákazníky hledající lokální podporu pro svůj antivirový program v českém jazyce a samozřejmě také logo ASC. Ten odkaz najdete na následující adrese:
http://www.nai.com/international/easteurope/asp-content/support/asc-czech.asp.

To podstatné z celého povídání jsem si však nechala na konec. Totiž co z toho všeho plyne pro vás, naše zákazníky?

Hlavní výhodou pro naše zákazníky je podpora, poskytovaná v lokálním jazyku. Neocenitelnou předností je také okamžitá odezva, telefonická či elektronická, větší dostupnost případného osobního zásahu technika u zákazníka v případě havárie ve srovnání s vyhledáváním pomoci v zahraničí. Odbornost této pomoci, zaručuje samozřejmě především titul "certifikovaných" odborníků, kteří se problémům věnují a mají pro jejich řešení jak odborné znalosti, tak velké zkušenosti, zkrátka ví, jak na to. Ačkoliv je služba poskytování podpory naším autorizovaným střediskem podpory placená, zákazníkovi je k dispozici za zvýhodněných podmínek, přizpůsobených našemu trhu, tedy za odpovídající ceny. Zákazník, který si tuto formu podpory zaplatí a zvolí další možnosti jejího poskytování, získá tak jistotu, že najde pomoc podle své potřeby v pracovní době od 8:00 do 17:00 hod (nebo celých 24 hodin po 7 dní v týdnu) a kromě toho také přístup k informacím a znalostem, které jsou pro něj jinak nepřístupné.

To vše, o čem byla řeč v tomto článku, by mělo sloužit neustále se zvyšující úrovni služeb pro naše zákazníky, proto, aby se necítili opuštěni v situacích, kdy zlomyslný virus napadá jejich systém, kdy si neví rady s programem či nastavením, nebo kdy potřebují získat jistotu. Uděláme všechno pro to, aby tomu tak bylo, abychom si udrželi své postavení certifikovaných odborníků, abychom tu byli stále pro vás.

Olga Přikrylová

SECURITY 2001 - Bezpečně do nového milénia

Vážení přátelé,

dovolujeme si vás pozvat na již šestý ročník konference zaměřené na ochranu a bezpečnost dat stejně jako na antivirovou problematiku. Při loňském (pátém) ročníku akce Vás mohla překvapit změna názvu akce (dříve Virus, nyní vzhledem ke stále širšímu záběru bezpečnostní problematiky Security) - také nyní dochází k další radikální změně. Tou je periodicita konference - dosud se konala jen v letech sudých. Ovšem vzhledem k neutuchajícímu zájmu o počítačovou bezpečnost a otázky s ní související a také vzhledem k překotnému vývoji na poli IT security jsme se rozhodli konferenci pořádat každý rok. V souvislosti s tímto jsme obvyklou dvoudenní akci zredukovali do jednoho dne.

A tak se i letos setkáme na konferenci Security 2001, a to ve čtvrtek 7. června 2001. Konferenci pořádáme za mediální podpory vydavatelství Vogel Publishing (Chip, Počítač pro každého, IT Net, Level, Media Shop).

Těšíme se na setkání v červnu!

AEC, spol. s r.o., pořadatel konference Security 2001

Historie konference Security

Již od roku 1992 pořádá společnost AEC každé dva roky konference, věnované problematice počítačových virů, antivirové ochraně a souvisejícím otázkám.

V letech 1992, 94, 96 a 98 se konference konala pod názvem 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" jsme se v "magickém" roce 2000 rozhodli pro přece jen výstižnější název Security 2000.

Ať tak či onak, smysl a náplň konference zůstal stejný jako v předchozích letech - a nejinak tomu bude iv roce letošním. Jde nám především o to nabídnout co nejširšímu okruhu kompetentních pracovníků aktuální informace v oblasti ochrany dat.

Konference Security 2001 proběhne ve čtvrtek 7. června 2001 v Praze. Přednášet budou, jak se stalo zvykem, přední specialisté z oboru.

Jsme přesvědčeni, že stejně jako v předchozích ročnících konferencí se nám i letos podaří přivítat co nejvíc účastníků a že si z konference Security 2001 odnesete cenné a hlavně pro svou práci užitečné informace. Další a postupně stále více upřesňující informace týkající se příprav konference můžete sledovat v odborném tisku a na Internetu.

Na Prvním partnerském dni AEC se především odměňovalo

Jednou z prvních významných firemních akcí v roce 2001 byla nesporně událost, která se odehrála 1. února v Národním domě v Praze na Vinohradech. První partnerský den AEC, jak jsme událost nazvali, položil základ tradici setkávání našich specialistů s odborníky partnerských společností a troufám si říct, že nasadil vysokou laťku těm dalším.

Celý minulý rok jsme se postupně připravovali na skutečnost, že své partnery odměníme "podle zásluh" - čili podle dosaženého obratu z prodeje našich antivirových a šifrovacích produktů. Rozdat výhry, jakými bylo značkové horské kolo Superior, luxusní kožená galanterie, osmnáctiletá whisky Johnnie Walker, společenská hra elektronické šipky, archivní víno či sportovní doplňky Adidas, bylo velmi příjemné jak pro nás s kolegyní Andreou, tak i pro výherce. Dary, stříbrný celofán, stužky a celkové aranžmá vyvolávaly skoro vánoční pocit, a proto je škoda, že pár výherců bohužel podlehlo viru (chřipkovému), a tudíž se nemohli osobně dostavit pro výhru.

Měli jsme ovšem mnohem více důvodů k tomuto neformálnímu setkání specialistů IT security společnosti AEC a partnerů ze strany dodavatelů, distributorů a zástupců tisku.

Úvodní slovo patřilo paní ředitelce ing. Aleně Řezníčkové (mimochodem, také bojovala - statečně - s chřipkou). Přivítala zaplněný sál pozvaných hostů a představila jim společnost AEC, hovořila o budoucím trendu dalšího rozvoje a o nových službách.

První partnerský den AEC byl i příležitostí pro zástupce tisku, a ti ji využili pro představení svých vydavatelství a periodik zaměřených na informační technologie. Za PC World hovořil redaktor Patrik Malina a za vydavatelství Vogel Publishing pan Petr Moláček a paní Maria Dvořáková.

Těsně před vyhlášením přestávky pozvala Hana Stojanová všechny přítomné na divadelní představení do Divadla Bez zábradlí "Kdes to byl(a) v noci?", kterým jsme v březnu oslavili desetileté působení naší společnosti. A vzápětí je pozvala na "představení", které se konalo ve vedlejší místnosti - na raut. Ano, byla to nádherná část semináře, kterou si všichni dlouze vychutnávali. Barevně sladěná dekorace jídel byla velmi působivá a smysly zrakové, čichové, chuťové i hmatové byly neustále v pohotovosti a posléze velmi vyčerpané.

Paní Susanne Ullrich, která přijela s kolegy z německé pobočky Network Associates GmbH, to rozhodně neměla jednoduché, přesto dokázala znovu po této přestávce zaujmout přítomné hosty, když představovala Authorized Support Center Program (Program ASC). Naše společnost AEC jako jediná dosáhla právě toho, že může nabízet zákazníkům novou službu - Centrum autorizované servisní podpory produktů firmy NAI pro antivirovou ochranu v regionu České republiky. Informacemi o spolupráci a vlastní společnosti NAI doplnil svým vystoupením Wirk Roemmelt, který je regionálním manažerem NAI pro střední Evropu.

Služby AEC pohledem technického specialisty detailně vysvětlila Olga Přikrylová - tak, aby každý partner dokázal nabídnout k produktům i služby (ať už se jedná o běžnou podporu typu instalace, školení u zákazníka, hot-line a aktualizace nebo o speciální řešení, vypracování bezpečnostních projektů, rizikové analýzy, ASC službu, auditorské služby apod).

Neméně kompetentně ve své přednášce popsal Tomáš Vobruba kompletní portfolio produktů. Živým, ale velmi srozumitelným způsobem hovořil o vlastnostech těchto produktů. Dlouholeté zkušenosti z oboru při tom rozhodně nezapřel.

Následovala dvojice přednášek v mém podání. V případě první bylo téma široké - certifikační a registrační autorita, elektronický podpis, pocity smíšené, nohy dřevěné... Dotkla jsem se pojmů, které souvisejí s elektronickým podpisem, objasnila CA a RA, vysvětlila, jak fungují v praxi. Podruhé jsem se obrátila na posluchače, abych v další přednášce představila Partnerský program Lighthouse (maják jako symbol bezpečí - a o bezpečí nám stále jde) a ukázala speciální možnosti spolupráce s individuálními výhodami pro distributory.

Vysvobodila mne až Andrea Koláčková vyhlášením nové soutěže pro letošní rok 2001. A ceny? Posuďte sami: zájezd od CK Fischer dle vlastního výběru, poukázka na luxusní kožené zboží, značkové sportovní oblečení, hodinky a archivní alkohol.

A to je ta část programu, na kterou se nejvíce těším v příštím roce 2002!

Jitka Brandejsová

Ohlédnutí za dnem elektronického podpisu

Jak je patrno z odborných i méně odborných médií, i v naší malé středoevropské republice nabývá poslední dobou problematika elektronického podpisu na důležitosti. Přestože je tato oblast u nás zatím pouze v plenkách, je stoupající trend zájmu o tuto oblast (nejen v řadách odborníků, ale i v řadách běžných uživatelů) dosti patrný. Tomuto zájmu jistě napomohlo i nedávné přijetí příslušného zákona, který je jedním z prvních podobných zákonů na světě.

Vědoma si těchto faktů, uspořádala naše firma jednodenní seminář věnovaný právě tomuto tématu. I vzhledem k tomu, že měsíc březen je věnován Internetu, bylo načasování této akce vhodné. Seminář se uskutečnil v Praze ve stabilních přednáškových prostorách, které naše firma používá (budova Stimbuildingu, Vinohradská 184), pod záštitou počítačového magazínu PC WORLD. Semináře se zúčastnilo osm přednášejících a přes šedesát posluchačů.

Již v 9:00 hodin se začali scházet první zájemci chtiví informací o elektronickém podpise. S blížícím se časem zahájení semináře stoupala i nervozita v řadách našich odborníků, kteří dostali za úkol prezentovat jednotlivé příspěvky.

Seminář byl zahájen moderátorkou Helenou Ciprysovou přesně v 9:30. S úvodním příspěvkem na téma "Proč elektronický podpis" vystoupila Hana Stojanová. Ve své stručné a výstižné přednášce uvedla danou problematiku, objasnila některé základní pojmy a vysvětlila oblasti a důvody použití elektronického podpisu.

Na její příspěvek bezprostředně navázal Tomáš Přibyl s bližším popisem technologie elektronického podpisu. Provedl porovnání elektronického a klasického podpisu. Blíže si všiml rozdílů mezi pojmy "elektronický" a "digitální" podpis. Názorně popsal principy použití a ověření digitálního podpisu a uvedl některé možné oblasti jeho praktické aplikace.

Dalším zpestřením dopoledního programu byl příspěvek Evy Šebkové, která přítomným posluchačům objasnila problematiku vystavení a použití certifikátu. Maximálně srozumitelným

Chceš ten kousek vlevo nebo vpravo?
Hana Stojanová za asistence Davida Pavlíčka právě „útočí“ na narozeninový dort AEC.

způsobem vyložila pojmy, jako např. certifikát, třídy a druhy certifikátů, certifikační a registrační autorita.

Dopolední program ukončil Jiří Hudec, který ve svém vystoupení prostřednictvím názorných příkladů seznámil přítomné s praktickým použitím elektronického podpisu. Na vysoké odborné úrovni předvedl konfiguraci systému, generování klíčového páru u certifikační autority, použití elektronického podpisu v produktech Microsoft Outlook a Outlook Express. Závěrem popsal použití elektronického podpisu v Netscape Navigatoru a všiml si možností a výhod, které v této oblasti nabízí software Norman Security Suite, zvláště možnosti definice skupinových klíčů.

Po přestávce, která přítomným umožnila naplnit se

vedle užitečných informací také dobrým jídlem, nastoupil na odpočaté posluchače obchodní ředitel AEC Jan Novotný a seznámil je se Zákonem o elektronickém podpisu. V úvodu svého příspěvku přítomné přehlednou formou seznámil se základní terminologií zákona, s úřady a institucemi, na které se tento zákon vztahuje, a také se souvisejícími zákony a vyhláškami. Dále popsal historii a současný stav zákona a jeho prováděcích vyhlášek včetně návazných direktiv EU. Závěrem si všiml praktického využití elektronického podpisu z pohledu Zákona o elektronickém podpisu.

Po této smršti údajů následovala další přednáška Tomáše Přibyla, tentokrát na téma "Časové značky u elektronických podpisů". Ve svém zajímavém projevu seznámil přítomné s touto (u nás prozatím nepříliš známou) technologií, která slouží především jako „prostředek k důkazu existence v určitém časovém okamžiku", například právě u elektronických podpisů.

S bezesporu nejzajímavější přednáškou semináře vystoupil pan ing. Jaroslav Pinkava, CSc., který patří mezi největší odborníky na kryptografii a elektronický podpis u nás. Přítomné posluchače podrobně seznámil s historickým vývojem elektronického podpisu u nás a ve světě, s platnými a chystanými normami a směrnicemi EU a snahami o sjednocení a normalizaci v oblasti elektronického podpisu. Tuto přednášku lze nepochybně označit za pověstný "zlatý hřeb" programu.

Zajímavým bodem programu bylo vystoupení redaktora spolupracujícího počítačového magazínu PC WORLD Patrika Maliny. Ve svém příspěvku se podíval na problematiku elektronického podpisu očima běžného uživatele. Jeho postřehy byly určitě přínosné nejen pro přítomné posluchače, ale také pro naši firmu.

V posledním bodě programu vystoupil náš kolega z pražské pobočky David Pavlíček.

Ve svém příspěvku v podstatě shrnul celodenní seminář formou FAQ (často kladených dotazů) o elektronickém podpisu.

Seminář byl ukončen řízenou diskusí. Nejvíce dotazů směřovalo na pana Pinkavu, který na ně ochotně a zcela vyčerpávajícím způsobem odpovídal. Sladkou tečkou programu byl dort upečený u příležitosti desetiletého výročí, které naše firma v těchto dnech slaví.

Co říci závěrem?
Snad jen: kdo tam nebyl, chybil.

Petr Nádeníček

První partnerský den AEC

První partnerský den AEC

1. února 2001, Praha

Národní dům

na Vinohradech

Připravit setkání se nedá jen tak - s rukama v kapsách…

Funkce nástěnkáře na Prvním partnerském dni AEC se ochotně ujala Jitka Brandejsová.

Urobime prezenčku.

Na Prvním partnerském dni AEC se především odměňovalo - viz článek na straně 7.

Chip je prostě časopis k sežrání…

Den elektronického podpisu

Den elektronického podpisu

8. března 2001, Praha

Stmbuilding

Vinohradská 184

Dort vyrobený (a zneškodněný) při příležitosti Dne elektronického podpisu.

Při přednášení vyschne v krku. Hana Stojanová hovoří na téma „Proč elektronický podpis?“

Sál nabitý k prasknutí, spokojení účastníci.

Pan Patrik Malina z časopisu PC World, který byl mediálním partnerem akce.

Celý seminář bravurně moderovala Helena Ciprysová z pražské pobočky AEC.

Nové technologie, nová rozhraní?

Na tuto otázku se pokusím podat v několika příštích odstavcích odpověď.

Americká firma NAI, divize McAfee, vyvíjí antivirový software, držící se na absolutní špičce mezi antivirovými programy. Hlavní předností je kvalitní skenovací motor, který zajišťuje bezchybnou a velmi rychlou detekci virové infiltrace. Další velmi významnou vlastností je komplexnost řešení. V rámci softwarového balíku dostanete nejen "antivirák" pro stanice, servery, groupware a gateway, ale navíc budete mít přibalen software pro centrální správu toho všeho a další utility a programy automatizující rutinní záležitosti správy antivirového prostředí na síti.

Vlajkovou lodí McAfee je produkt VirusScan. Nyní je k dispozici ve verzi 4.5 pro nejrozšířenější operační systémy Windows - 9x, NT a 2000. Připravuje se nová verze 4.5.1, která bude také pro všechny známé windows operační systémy a bude navíc obsahovat podporu pro Windows ME. Momentálně (druhá dekáda 03/01) je ve verzi VS 4.5.1 Beta1. Uvolnění softwaru očekávejme ve druhém kvartále tohoto roku.

VirusScan 5.1 je antivirový systém určený pro domácí uživatele. Je funkčně totožný s verzí VS 4.0.3 pro Windows 9x, nicméně hlavní rozdíl je v uživatelském rozhraní a nemožnosti správy na dálku.

Novou verzí verzemi VirusScanu je VirusScan 6.0.0 Think Client, což je antivirový produkt určený pro operační systémy Win32. Jedná se pouze o On-Access skener, který lze spravovat pouze na dálku z nástroje ePolicy Orchestrator. Druhým produktem je VirusScan Wireless určený pro palmtopy s operačními systémy PalmOS a Windows CE. Je to jediný antivirový produkt tohoto typu na trhu.

Dalším programem z řady VirusScan, který je neustále vyvíjen a aktualizován, je Command Line Scanner pro DOS, který je ve verzi 4.1.4.0 a Command Line Scanner pro UNIX, implementovaný pro všechny verze tohoto systému - Linux, SUN Solaris, Free BSD, AIX, HPUX, SCO.

Systém pro počítače Mac - Virex je ve verzi 6.1 a VirusScan pro OS/2 je stále ve verzi 4.0.3.

Serverové systémy NetShield pro Windows a pro Novell Netware mají verzi 4.5. Pro verzi Novell Netware byl vydán aktuální engine 4.1.40.

Největší novinky se týkají prostředků pro ochranu groupware na platformách Microsoft Exchange. S nástupem nového aplikačního prostředí MS Exchange 2000 byl uvolněn produkt GroupShield 4.5 pro Exchange 2000. Exchange 2000 jako "novorozeně" má nějakou tu "dětskou nemoc" a proto se chystá SP1 pro Exchange 2000. Reakcí NAI na tuto skutečnost je vývoj service packu. Je postaven na SP1 pro Exchange 2000 a bude distribuován formou opravy. Dnes je ve verzi GSE 4.5.1 SP1 Beta1. Bude aplikovatelný na GSE 4.5 pro Exchange 2000, nicméně pro využití všech oprav a nových vlastností Exchange 2000 SP1 bude vyžadovat jeho instalaci. Pomocnou službou pro skenování SMTP na GSE pro Exchange 2000 je utilita SMTP Scan pro Exchange 2000.

Pro GroupShield 4.5 SP1 pro Exchange 5.5 byl uvolněn poslední hot fix 5. Spolu s ním je k dispozici Message Body Scan Utility, což je služba, provádějící skenování těla e-mailové zprávy na destruktivní kód, procházející Exchange serverem. Velké množství chyb v rozhraní VSAPI (Virus Scanning Application Programming Interface), implementovaného do Exchange serveru, způsobuje, že soubory ukládané ' v karanténě a virusová hlášení neobsahují informaci o odesílateli a příjemci e-mailové zprávy. Tuto velmi důležitou informaci uloží Resolve Names Utility, která je dodávána samostatně.Ke správné činnosti utility je nutné splnit základní požadavek - karanténu v databázi. Tento malý program je součástí instalace GSE 4.5 pro Exchange 2000.

GroupShield pro Lotus Notes je v současnosti k dispozici ve dvou verzích - GSD 5.0a for NT a GSD 5.0 for AIX.

WebShield for MS Proxy není dále vyvíjen, ale pouze podporován ve stávající verzi 4.0.3. Pro bezchybný provoz je nutné provádět aktualizace datových souborů a upgrade motor. Poslední verze 4.1.40 pro Intel je s tímto systémem kompatibilní.

WebShield SMTP je antivirový systém pro skenování

Novinky u MCAFEE

SMTP bran. Svým chováním je nejrychlejším antivirovým prostředkem tohoto druhu, jaký lze na trhu získat. Nyní je ve verzi WS SMTP 4.5 SP1. Chystá se nová verze - WS SMTP 4.5 MR1, která se očekává v druhém kvartálu letošního roku. Všude určeno pro operační systém Windows NT/2000.

Poslední verzí skenovacího motoru je Solomon 4.1.40, který je k dispozici pro veškerý software s výjimkou Virexu a VirusScanu pro OS/2. Aplikace SDATu provede upgrade všech zmíněných systémů na platformě Intel a kompatibilních systémech. Pro ostatní systémy je dodávána speciální oprava.

Správce velkých sítí bude jistě zajímat, co je nového v oblasti centrální správy. Byla uvolněna poslední verze oblíbeného správcovského nástroje Management Edition 2.5 Maintenance Release 1. Další vývoj byl zastaven, nicméně podpora produktu bude ještě nějakou dobu pokračovat.

Náhradou by se měl stát program ePolicy Orchestrator. Nynější verze 1.1 má být v brzké době nahrazena verzí 2.0 s podporou Windows 2000 a množstvím vylepšení a zjednodušení vzdálené správy a údržby systémů VirusScan, NetShield, GroupShield a WebShield. Správci, těšte se!

A co se připravuje dále? VirusScan 7.0, ePolicy Orchestrator 2.1 a mnoho a mnoho dalších novinek. Ale informace o těchto produktech si ponechme na příště.

Tomáš Kočnar
tomas.kocnar@aec.cz

Pro úplnost uvádím seznam softwarových balíků McAfee a jejich obsah včetně verzí:

Balík		Produkt	Platforma	Verze	Balík	
VirusScan Think Client Suite		VirusScan TC	Windows 9x, NT, 2000	6.0.0		
		ePolicy Orchestrator	Windows NT	1.1	Active Virus Scan Security Suite	Active Virus Defence Suite
Total Virus Defence Suite	VirusScan Security Suite	VirusScan	Windows 9x, NT, 2000 OS/2 DOS UNIX	4.5 4.0.3 4.1.14 4.1.12		
		NetShield	Windows NT/2000 Novell Netware	4.5 4.5		
		Management Edition	Windows NT	2.5 MR1		
	GroupShield Security Suite	GroupShield	Domino - NT Domino - AIX Exchange 5.5 Exchange 2000	5.0a 5.0 4.5 SP1 4.5		
		WebShield	Proxy SMTP	4.0.3 4.5 SP1		
		VirusScan Wireless	Windows CE PalmOS	2.0.0		
		Virex	MacOS	6.1		
		WebShield for Solaris	Solaris	4.1		

Kaspersky Lab v roce 2000 a 2001

V průběhu roku 2000 firma Kaspersky Lab dokázala, že je jednou z vedoucích firem na světovém trhu s antivirovými produkty. O tom svědčí například mnohá ocenění počítačových i internetových magazínů. Některé z nich dokonce ocenily Kaspersky Anti-Virus, dříve známý spíše pod zkratkou AVP (Antiviral Toolkit Pro), jako produkt roku 2000!

V průběhu "magického" roku 2000 firma ohlásila několik jedinečných softwarových produktů a již existující verze antiviru Kaspersky Anti-Virus (AVP) byly zdokonaleny a transformovány do nejnovější verze 3.5, která je vybavena novými možnostmi pro zabezpečení jak domácích počítačů, tak i firemních sítí. Podle slov Natalie Kasperské, CEO firmy Kaspersky Lab, byl loňský rok velmi důležitým milníkem ve vývoji společnosti.

Patnáctého května minulého roku se stala Kaspersky Lab jednou z prvních antivirových firem poskytujících každodenně aktualizované virové databáze. A to zdarma pro všechny uživatele! Nyní již není nutné několik dní čekat až budou hotovy nejnovější virové databáze - ty jsou nyní k dispozici ihned, jakmile je připravena odpovídající ochrana proti novému viru. Tímto způsobem je eliminováno na minimum to nejkritičtější období mezi detekcí viru a dodáním modulu k jeho odstranění. Přitom rychlost odezvy na nově objevené viry je jednou z klíčových priorit firmy. V říjnu loňského roku byla firma Kaspersky Lab, na základě výsledků testů organizace Secusys, oceněna jako vůbec nejrychlejší co se týká odezvy na nové viry. Ostatní konkurenti zůstali daleko za ní.

Poslední březnový den roku 2000 přišla firma Kaspersky Lab s produktem Kaspersky Anti-Virus (AVP) pro Firewall, založeným na velmi rozšířeném protokolu CVP (Content Vector Protocol). Tato antivirová ochrana je tak použitelná pro nejznámější firewally jako jsou například CheckPoint Firewall-1, Gauntlet Firewall, AltaVista Firewall, SecureIT Firewall, Guardian Firewall a další. Kaspersky Anti-Virus rozšiřuje jejich možnosti tím, že je doplňuje o modul pro virovou filtraci, který umožňuje v reálném čase virovou detekci a dezinfekci veškeré komunikace jdoucí přes firewall.

Jako odpověď na celosvětovou virovou epidemii typu Iloveyou ohlásila 7. května 2000 firma Kaspersky Lab nový modul Script Checker, chránící proti skriptovacím virům a to i těm dosud neznámým. Tím se stal Kaspersky Anti-Virus (AVP) zatím jediným antivirovým systémem schopným odolávat všem virovým nákazám typu Iloveyou. Script Checker byl do konce minulého roku zdarma distribuován jako doplněk softwaru Kaspersky Antivirus (AVP). Od verze 3.5 je však již implementován jako součást antivirového systému.

Kaspersky Lab rozšířila svoje portfolio i o antivirovou ochranu e-mailových serverů. Po produktu Kaspersky Anti-Virus (AVP) pro Microsoft Exchange Server tak následovaly verze pro Sendmail a později i pro Qmail. Jejich hlavní výhodou je možnost práce pod operačními systémy Linux, BSDi a FreeBSD. K těmto verzím jsou navíc k dispozici i zdrojové kódy, což umožňuje implementovat antivirová řešení i do některých dalších vyvíjených produktů.

A co se bude dít letos? Během roku 2001 má firma Kaspersky Lab v plánu další vylepšení a rozšíření existující produktové řady Kaspersky Anti-Virus a dále snahu o rozšíření svých aktivit i do jiných oblastí počítačové bezpečnosti. Do konce prvního čtvrtletí by měl být uveden Kaspersky Anti-Virus (AVP) pro servery Novell NetWare 5, jehož hlavní předností bude možnost instalace a správy antivirové ochrany prostřednictvím NDS (Novell Directory Services) za pomoci Console One.

Další očekávanou inovací by měl být antivirový filtrační systém veškerého provozu přes SMTP protokol. Data jdoucí touto cestou budou tak zkontrolována ještě před tím, než se dostanou na e-mailový server. Tento software bude možno provozovat na operačních systémech Linux, FreeBSD a BSDi. Během druhého čtvrtletí tohoto roku by pak taky měla být k dispozici verze antiviru pro e-mailové servery Lotus Notes/Domino, pro Linux a Windows NT.

Zhruba ve stejnou dobu by měla být hotova i WEB Management Console, která umožní vzdálenou správu antivirového systému běžícího pod operačními systémy Linux, FreeBSD a BSDi. Webová technologie umožní vývoj systému nezávislého na platformě pomocí internetového prohlížeče.

Také Network Control Centre dozná výrazných změn. Velmi brzy bude umožňovat centrální správu nejen pod systémem Windows, ale i pro platformy NetWare, Linux, FreeBSD a BSDi.

Ve třetím čtvrtletí tohoto roku bude představen Kaspersky Anti-Virus ve verzi pro PDA na bázi Palm OS a pro procesory SPARC s podporou operačního systému Solaris. A konečně v posledním čtvrtletí roku 2001 by měla být dokončena nová verze antivirového programu Kaspersky Anti-Virus 4.0. Tato verze bude založena na nejnovějších technologiích a její unikátní architektura umožní jednoduše celý systém přenést na libovolnou platformu což zahrnuje kromě obvyklých operačních systémů i mobilní telefony nebo kapesní počítače.

Nezbývá tedy než trpělivě čekat a těšit se na to, co nám v budoucnu softwarové dílny společnosti Kaspersky Lab nabídnou.

David Pavlíček

F-Secure Workstation Suite

V předchozích seriálech bulletinech se vždy někdo z nás zmínil o nějaké softwarové novince z dílen našich partnerů. Mou povinností je seznámit Vás s pokročilou technologií, kterou nám dnes nabízí společnost F-Secure.

Jak jistě víte, produkty této společnosti jsou v českých zemích velmi populární. Vzpomeňme si na první verze oblíbeného antivirového programu - kdysi (před lety) vše začalo F-Protem. Tenkrát to byl v podstatě DOSový antivirový program, ke kterému se přidala grafická nadstavba do systému Windows. Toto vše Vám AEC nabídlo již v roce 1993. Grafická nadstavba nepřinesla jenom hezké ikonky, ale i centrální správu, alerty, skenování v reálném čase a spoustu dalších více či méně důležitých funkcí.

Tehdy ještě tento program nepoužíval countersign technologii (to je technologie sdružování několika skenovacích prostředků dohromady), ale využíval pouze motor F-Prot z dílny Frisk Software (Island). Vymoženosti, které tenkrát tento program přinesl, byly natolik kvalitní, že se v podstatě nezměnily dodnes.

Jeho důstojným nástupcem, který zachoval vzhled F-Protu, se stal F-Secure Anti-Virus 4.x. Přestože program navenek vypadal stejně, celé jeho jádro bylo změněno. Přinesl další skenovací motor z dílny ruských autorů - AVP, uměl skenovat archívy… Na svou dobu obsahoval i další značné novinky a přinášel výhody a kvality poskytované dosavadním skenovacím motorem F-Prot. Zde již byla použita zmiňovaná CouterSign Technology. Tato verze je na našem trhu i přes různé modifikace již déle jak tři roky. Verze stále oplývá centrální správou (aktualizací, instalací, sběrem hlášení a virových incidentů) a umožňuje širší podporou distributorů. Má české národní prostředí, které nabídla právě naše společnost. Nicméně neumožňovala spoustu věcí, které si postupem času uživatelé začali žádat. Pro pořádek mohu zmínit alespoň několik z nich: správu ve velkých WAN sítích, modulárnost a třeba skenování na kontextové menu.

Proto po delší časové odmlce přišla firma F-Secure s produktem F-Secure Workstation Suite.

Jak je již patrno z anglického názvu, jedná se o balíček pro pracovní stanici, pro kterou je také určen. Oproti minulosti již neobsahuje pouze antivirový program (který je ovšem i nadále jeho hlavní součástí), ale i jiná bezpečnostní řešení, která se stávají poslední dobou velmi populární. Vyjmenujme například virtuální privátní sítě (F-Secure VPN+), osobní firewally (F-Secure Distributed Firewall) a šifrování dat (F-Secure FileCrypto).

Program také přinesl nový vzhled, který ještě více zjednodušuje práci s antivirovým programem, a zdá se, že úspěšně - uživatelé si na něj rychle zvykli.

To samozřejmě samo o sobě nestačí. Program musí být dobře spravovatelný nejenom uživatelem, který jej má na svém počítači nainstalovaný, ale také administrátorem. Ono dnes snad ani není myslitelné, aby se antivirový program nedal centrálně ovládat a spravovat. Je to jeden ze základních požadavků

stávajících i budoucích zákazníků, kteří mají o antivirová řešení zájem. Společnost F-Secure se rozhodla v tomto ohledu pro velmi razantní krok. Oddělila centrální správu od samotného antivirového programu a vytvořila sofistikovaný modulární systém centrální správy pro všechny produkty, které na trhu nabízí.

Centrální správa je rozdělena na dvě části: konzolu a server na straně administrátora, pojmenované samostatně jako F-Secure Policy Manager, a na jedinou část a hromadu modulů na straně uživatele. Tou jedinou částí je univerzální agent, který má na starosti komunikaci s administrátorem a serverem a moduly, které jsou na něj navázány. Co je vlastně míněno těmi moduly? Například antivirový program. V F-Secure Workstation Suite je totiž implementován nový F-Secure Anti-Virus ve verzi 5.x.

Bezpochyby jste si i všimli, že s novým označením vždy přišlo něco nového do antivirového programu. Nová verze přináší nový, v pořadí již třetí, skenovací motor ORION, který reaguje na novinky ve světě virů a antivirů. Specializuje se na heuristické vyhledávání souborových, čistě 32bitových virů, které se začínají dravě předvádět nebohým uživatelům výpočetní techniky.

Program umožňuje, díky použité technologii centrální správy, používání v již zavedených modelech podnikové správy (například pomocí software Microsoft SMS nebo HP OpenView). Samozřejmostí je použití bezpečnostních prvků jako je silná autentizace administrátora k systému a elektronicky podepisované příkazy administrátora jednotlivým skupinám klientů nebo samotným klientům. V novém produktu firma F-Secure také nezapomněla na domácí uživatele. Praxe totiž ukázala, že spousta uživatelů spoléhá na samotnou instalaci a již se o program nezajímají (natož o aktuální novinky ve světě virů). Předpokládají, že je program ochrání před viry stejně tak dobře i za půl roku! Jaká chyba! Antivirový program potřebuje aktuální databázi, podle které dané viry hledá. Proto je možné dostávat datové řetězce automaticky i s krátkými zprávami o novinkách v elektronickém světě virů.

A to je snad pro dnešek vše, přátelé. Snad ještě dlužno poznamenat, že tato F-Secure Workstation Suite se nachází na našem aktualizačním CD - a ti, kdož nemají F-Secure Anti-Virus koupen, si jej mohou zapůjčit po zavolání na naše obchodní oddělení.

Tomáš Vobruba

Pomóc, mám virus!

Řešíte právě problém se zavirovaným souborem/počítačem? Nebo jste již řešili, či jste alespoň připraveni jej do budoucna řešit? Dříve nebo později možná řešit budete. A my jsme tu pro vás! A abychom vám mohli pomoci, potřebujeme co nejpřesnější informace. Jaké? To závisí zejména na vás a tento článek vám usnadní jejich poskytnutí. Budeme uvažovat o dvou případech uživatelů (dále rozdělených viz body A a B).

Za A):

Předpokládejme, že jste (pokud možno spokojenými) zákazníky AEC, a že používáte některý antivirový produkt osvědčené firmy, jako jsou Network Associates, F-Secure, Norman, Kaspersky Lab…. V tom případě vás může (mile v prvním bodě, či poněkud nemile v bodech následujících) překvapit pouze několik situací:

- Antivirový program si s virem hravě poradil, odstranil jej a vše opět funguje, jak má.
- Antivirový program virus našel, ale nedokázal jej odstranit.
- Antivirový program žádný virus v počítači nenašel, tudíž neodstranil, přesto jste skálopevně přesvědčeni, že tam virus je a škodí.

Pomineme-li pak první bod, zbývají dva následující, u kterých zřejmě potřebujete podporu. Tu vám samozřejmě poskytnou odborníci z firmy AEC. Pokud tedy nechcete koktat do telefonu nebo zdlouhavě

doplňovat další informace do dalších e-mailů, máme pro vás jednoduchý návod složený z bodů, jež vám usnadní nahlášení vašich potíží jak telefonicky, tak např. elektronickou poštou. Jinými slovy: co vše byste si měli raději dopředu připravit, než kontaktujete naši firmu?

1. název vaší firmy (příp. číslo smlouvy mezi vámi a AEC);

2. vaše jméno s uvedením kontaktních údajů (č. telefonu, e-mail);

3. datum, případně i čas, ve kterém došlo k napadení virem;

4. verze instalovaného antivirového produktu

- najdete ji podle používaného antivirového programu nejčastěji např. v okně AV-programu v menu Help (Nápověda) a pod volbou About (O programu, Informace o programu ap.), nebo při spuštění skenovacího úkolu;

příklad informací o verzích VirusScanu viz obrázek.

5. verze skenovacích motorů (scan engine)

- najdete ji většinou tam, kde se rovněž nacházejí informace o verzi programu;

6. verze aktualizace (update)

- najdete ji většinou tam, kde se nacházejí informace o verzi programu;

7. instalovaný SW, platforma, na níž antivirový program běží, a jde-li o server/klient;

8. název nalezeného viru;

9. akce antivirového programu, případně výsledek akce použité v daném antivirovém programu;

10. typ souboru, u kterého k napadení došlo;

11. popis současného stavu - chování napadeného počítače;

12. ostatní související informace;

13. je-li to možné, zkomprimujte napadený soubor (programem WinZip) a pošlete jej elektronickou poštou (e-mail) na adresu support@aec.cz.

Za B):

Že nemáte žádný antivirový program? Tento stav by se dal nazvat hazardem nejen s vašimi daty, potažmo penězi, a bylo by záhodno jej ve vlastním zájmu co nejdříve změnit! Tato rada vám ale právě v čase, kdy řešíte virové napadení, nepomůže. V tom horším případě už to víte, nyní však potřebujete pomoc.

Kromě nabídky vhodného antivirového programu, navíc se všemi službami a podporou v rámci smlouvy, jsme samozřejmě schopni vám poskytnout také kvalitní technické služby k odstranění viru, případně odborné informace, jak správně postupovat. Ke kontaktu s našimi odborníky ať už telefonickou, elektronickou nebo písemnou formou využijte opět všechny relevantní body z vyjmenovaných bodů v odstavci A), které pomohou našim specialistům při stanovení postupu vedoucímu k odstranění virové infekce a jejích následků.

Neodpustíme si však jednu obecnou radu na závěr: Neváhejte s výběrem antivirového zabezpečení svého počítače/počítačů pro příště! Ušetříte (ztrátu dat, finance, čas, starosti, nervy…).

Olga Přikrylová

Amsterdam - seminář

Co:
Sales training fy Norman Data Defense
Kdy:
19. až 22. února 2001
Kde:
Hoofddorp, Amsterdam (Holandsko), Hotel de Beurs
Kdo:
R. Šimonová, J. Novotný

Oba snímky na této stránce názorně dokládají, že Holandsko je zemí sýrů a dřeváků.

Tolik z oficiální zprávy předané ředitelce společnosti ing. Aleně Řezníčkové. Ale o co vlastně šlo? Stejně jako většina dodavatelů společnosti AEC, tak i norská firma Norman Data Defense pořádá zhruba dvakrát za rok tréninkový seminář. Tyto semináře jsou u jednotlivých společností (dodavatelů) prakticky shodné, každý má za cíl naučit účastníky jak "lépe a radostněji" prodávat produkt právě té které společnosti. Proč tedy píši právě o tomto semináři? Nejen proto, že jsem se jej zúčastnil, ale především proto, že by byla škoda se s Vámi nepodělit o novinky a akce, které společnost Norman plánuje a chystá na rok 2001.

První a nejdůležitější staronovinkou je pokračující vývoj a vylepšování dlouho očekávané verze 5 produktu Norman Virus Control. Tento produkt by se měl letos objevit mimo jiné již na veletrhu informačních technologií CeBITu. Podle slov Arvida Gomeze z fy. Norman bude obsahovat nejen centrální instalaci a správu, ale vývojáři společnosti pracují také na inkrementálním upgrade a automatizaci aktualizací, které bude možné provádět zcela bez účasti uživatele.

Další část semináře se zabývala celkovou strategií firmy Norman a způsoby, jakými je možné produkty Norman Virus Control poskytovat. Za velmi perspektivní považuji vizi společnosti Norman vytvořit bezpečnostní řešení sloužící jak k ochraně dat (šifrováním), tak k antivirové ochraně. Prvním krokem k tomuto řešení je vytvoření konzoly společné jak pro Norman Virus Control verze 5, tak pro Norman Privacy a Norman Personal Firewall. Z ní bude možné tyto produkty nejen instalovat, ale i spravovat. O tom, jak probíhá a postupuje vývoj těchto produktů, se s Vámi samozřejmě při nejbližší příležitosti podělíme.

I když zde nemohu popsat vše, co bylo na semináři probíráno (inu, služební tajemství je služební tajemství), přesto musím konstatovat, že seminář nejen splnil svůj účel, ale protože zde bylo možné potkat velmi zajímavé a přátelské lidi, byl i vítaným zpestřením v práci.

Jan Novotný

Nemáme se za co stydět

Nedávno se na mě obrátil kolega z marketingového oddělení ing. Tomáš Přibyl s prosbou: "Napiš, prosím tě, nějaké zajímavé postřehy z konference Security 2000". Tato odborná oblast není právě mou doménou, a tak jsme se nakonec dohodli, že raději napíši článek z oblasti personalistiky a řízení lidských zdrojů v naší firmě, což je vzhledem k mému pracovnímu zařazení problematika, ke které mám rozhodně blíže.

Povolání personalisty vykonávám asi pět let a vždy v minulosti jsem se podivovala nad množstvím článků v různém tisku a odborných časopisech zabývajících se řízením lidí, tím jak je motivovat, jak si vybrat správné a kvalitní pracovníky, jak vytvářet a zdokonalovat firemní kulturu apod.

Zdálo se mi, že to není až tak těžké realizovat dobrou personální politiku. Teprve až s reálnou personální praxí jsem si čím dál více začala uvědomovat, proč mají některé firmy tak velké problémy ani ne tak se získáváním kvalitních pracovníků, jako spíše s jejich udržením.

To, co jsem dosud velmi krátce zmínila a nastínila, však není problém naší firmy, společnosti AEC. Celkové ovzduší ve firmě, postoj vedení společnosti k vlastní personální politice, jednotný směr a koncepce je dána především osobností majitele firmy pana Ing. Jiřího Mrnuštíka, který úzkostlivě dbá na to, aby pracovníci ve firmě cítili na jedné straně osobní zodpovědnost za své pracovní úkoly, ale na druhé straně se cítili svobodní, měli možnost se realizovat a byli za svou práci dostatečně oceněni.

Firma vynakládá nemalé úsilí a prostředky na soustavné vzdělávání a doškolování svých zaměstnanců ať už se to týká jazykové vybavenosti, odborného výcviku, nebo také nadstavbové vzdělávání, jako jsou například kurzy rétoriky, psychologie prodeje, marketingové semináře apod.

Dlouholetou a milou tradicí naší firmy jsou i takzvaná „výjezdní zasedání“. Na těchto firemních sportovních dnech konajících se mimo Brno (zpravidla třikrát do roka) se nejen hodnotí pracovní úspěchy, plánuje se strategie firmy, ale daří se i úspěšně stmelovat kolektiv formou outdoorových a psychologický her, které skvěle prohlubují a utužují vztahy mezi spolupracovníky.

Přesto, že je těžké vyhovět vždy všem, a i do mezilidských vztahů v naší společnosti se občas vloudí „chybičky“, máme vždy tendenci problémy řešit otevřeně a hned, což zpravidla v konečném důsledku vede k eliminaci většiny případných nedorozumění.

Nemalou zásluhu na budování vysoké úrovně firemní kultury má i skutečnost v podmínkách českého podnikání poměrně neobvyklá. Ve vedení společnosti stojí výhradně ženy. Brněnské centrále „vládne“ ing. Alena Řezníčková, ředitelka společnosti, pražské pobočce paní Renata Šimonová, pobočce bratislavské Alena Mračková a marketing drží pevně v rukou Hana Stojanová. Za zmínku určitě stojí i fakt, že téměř polovinu zaměstnanců tvoří ženy. Dnes tak často diskutovaný problém profesní diskriminace u nás skutečně neřešíme. Žádný totiž nemáme. A pokud se týká onoho staročeského: „Běda mužům, kterým žena vládne“, asi neobstojí, podíváme-li se na hospodářské výsledky naší společnosti a na její vysokou dynamiku vykazovanou za posledních několik let.

Miroslava Dohnalová

Součástí přípravy specialistů AEC je i výcvik pro přežití v exterémních podmínkách.

AEC
DATA SECURITY COMPANY

Bulletin

www.aec.cz, www.trustcert.cz červen/2001

Úvod

Milí přátelé!

Čtvrtrok se se čtvrtrokem sešel a opět držíte v rukách AEC aktualizační bulletin, vytvářený pro Vaši informovanost na poli antivirových technologií a počítačové bezpečnosti.

Kdepak, letošní jaro bylo v oblasti počítačové bezpečnosti vším možným, jen ne okurkovou sezónou. Musíme ovšem přiznat, že do jisté míry si za to můžeme sami, neboť množství námi připravovaných akcí roste řadou vpravdě geometrickou. Semináře Bezpečnost dat v Praze a Brně, divadelní představení uspořádané k desátému výročí založení AEC, akce související s veletrhem Idet, „naše“ konference Security 2001 (Praha) a Bezpečnosť dát (Bratislava), veleúspěšná Roadshow na Slovensku, několik dalších konferencí a seminářů, kam jsme „vyslali“ naše specialisty, návštěva CeBITu… A v celém tomto období zcela nerovnoměrně a nepravidelně ještě několik desítek více a několik set méně zajímavých počítačových virů… A veškeré toto snažení bylo korunováno pomyslnou „třešničkou na dortu“, bulletinem, který právě držíte v ruce.

Příjemné čteni!

Tomáš Přibyl
tomas.pribyl@aec.cz

Autoři kreseb na obálce: (zleva)
Vendula Radová (Stod), Miroslav Švec (Horné Rakovce),
Jan Putiš (Stod), Marie Řádková (Brno), Miloš Kostka (Kladno)

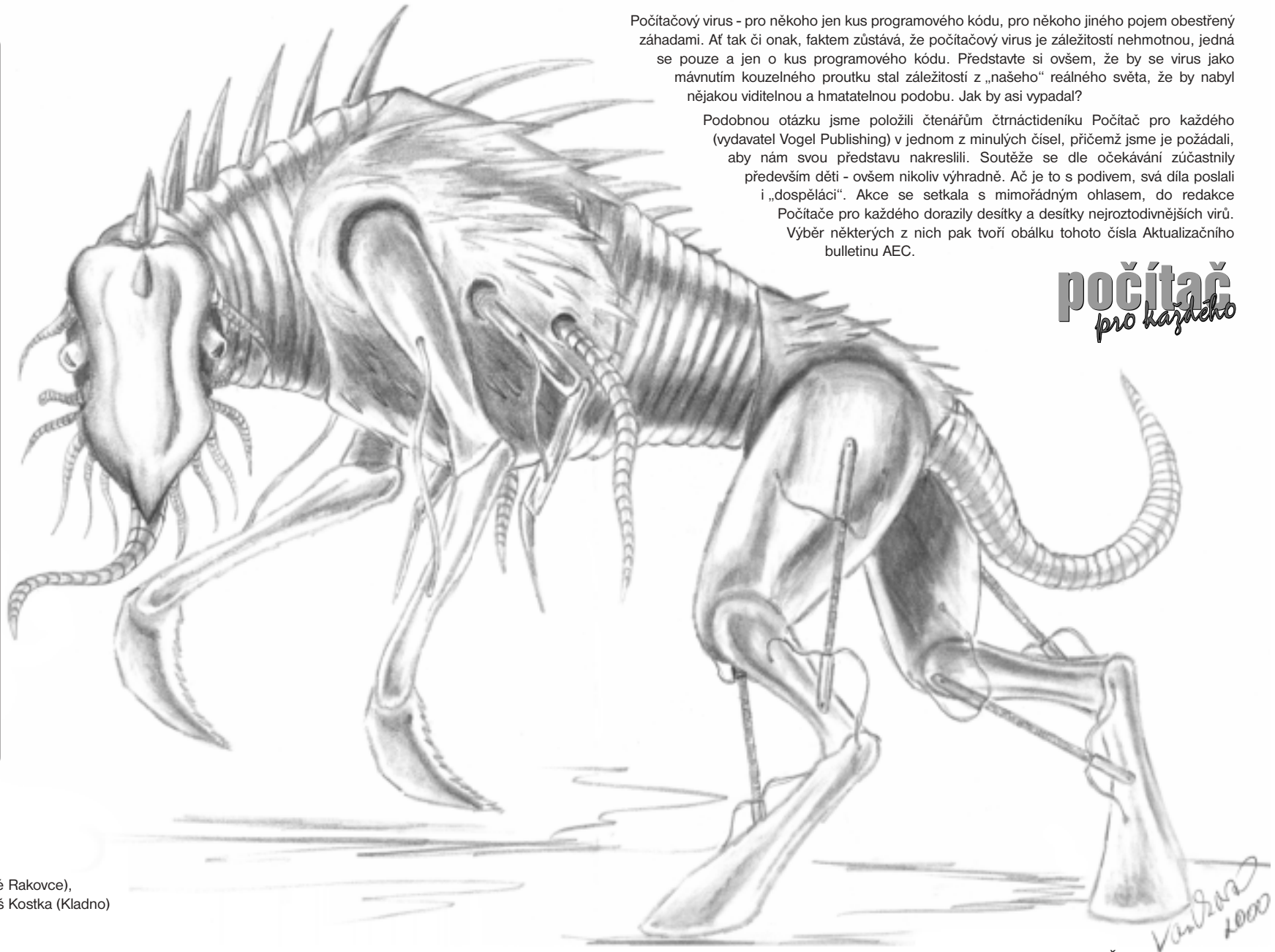
Foto na obálce: David Mráz a Jan Kroupa

Jak vypadá počítačový virus?

Počítačový virus - pro někoho jen kus programového kódu, pro někoho jiného pojem obestřený záhadami. Ať tak či onak, faktem zůstává, že počítačový virus je záležitostí nehmotnou, jedná se pouze a jen o kus programového kódu. Představte si ovšem, že by se virus jako mávnutím kouzelného proutku stal záležitostí z „našeho“ reálného světa, že by nabyl nějakou viditelnou a hmatatelnou podobu. Jak by asi vypadal?

Podobnou otázku jsme položili čtenářům čtrnáctideniku Počítač pro každého (vydavatel Vogel Publishing) v jednom z minulých čísel, přičemž jsme je požádali, aby nám svou představu nakreslili. Soutěže se dle očekávání zúčastnily především děti - ovšem nikoliv výhradně. Ač je to s podivem, svá díla poslali i „dospěláci“. Akce se setkala s mimořádným ohlasem, do redakce Počítače pro každého dorazily desítky a desítky nejroztodivnějších virů. Výběr některých z nich pak tvoří obálku tohoto čísla Aktualizačního bulletinu AEC.

počítač pro každého



Vaňková Šárka, Chomutov

Bezpečnost elektronického podpisu: Bouře ve sklenici vody

Začalo to stručným oznámením, pak následovala tisková konference a velké diskuse v tisku často přecházející až téměř do podněcování hysterie okolo základů elektronického podpisu („Elektronický podpis není bezpečný“, „Konec elektronického podpisu v Čechách“ apod.).

Co se tedy za tím vším skutečně skrývá? Nejprve - útok, který pánové Rosa a Klíma popsali, je skutečně reálný a opodstatněný. Týká se způsobu práce se soukromým klíčem v PGP, přesněji postupů jakým je tento klíč uchováván. Existující implementace vychází z doporučení rfc2440, OpenPGP Message Format. Autoři ukázali, že doporučení daná touto normou nejsou z hlediska kryptografické ochrany soukromého klíče dostatečná. Co víc, ukázali, že existující implementace PGP (včetně posledních verzí) nejsou vůči jimi popsaným útokům odolné. Toto se týká podpisů, které jsou v PGP vytvářeny algoritmem DSA. Algoritmus RSA je naštěstí v PGP ošetřen ještě dodatečnou kontrolou integrity datového souboru, ve kterém leží zašifrovaný soukromý klíč a popsaný útok není dle autorů tedy přímo aplikovatelný.

Pro úspěšnost útoku je třeba zabezpečit, aby útočník měl buď přístup k počítači napadeného uživatele, nebo se k němu mohl dostat přes síť, resp. měl přístup k nějakému počítači, ve kterém se vyskytuje exportovaný zašifrovaný soukromý klíč uživatele (ve formátu OpenPGP).

Vůči PGP je to poměrně nepříjemný úder. Analytikové se shodují, že bude třeba připravit příslušné úpravy všech verzí, kterých se to týká. Logicky se objevují doporučení nevytvářet ukvapená řešení, ale provést hlubokou analýzu protokolu a vytvořit nový (snazší) přístup k formátům, ve kterých jsou soukromé klíče v PGP ukládány spolu s využitím dalších kontrol integrity příslušného souboru dat.

Přes svou rozšířenost je PGP označováno jako proprietární řešení. Je to z celé řady důvodů. Některé okruhy otázek jsou totiž v těchto produktech řešeny postupy, které platí výlučně pro software PGP (namátkou PGP/MIME, koncepce důvěry, zmíněné formáty atd.). Nemají však pravdu ti, kteří hovoří o tom, že PGP není systém, kterého by se týkal zákon o elektronickém podpisu. Je to jeden z mnoha možných způsobů, kterým lze k využívání elektronického podpisu dospět a např. při existenci odpovídající smlouvy zúčastněných stran má takovýto podpis i všechny náležitosti z hlediska zákonných dopadů.

Na druhou stranu je nutné říci, že profesionální řešení, která jsou připravována pro řešení elektronického podpisu (ve světě ale i u nás) vychází v daném ohledu z jiných principů a doporučení. Takováto řešení jsou připravována pro využití i v ČR (ať už ve státní či soukromé sféře).

Není tedy naprosto žádný důvod propadat jakékoliv panice.

Rozšiřujeme nabídku: Panda Software

Nedávno jsme na základě požadavků našich zákazníků rozšířili naši nabídku o antivirový software od dalšího dodavatele **Panda Software** ze Španělska, který se již od svého založení v roce 1990 zabývá výzkumem a vývojem antivirových řešení pro všechny typy uživatelů. V současné době používá antivirové produkty této společnosti více než dva milióny uživatelů v 35 zemích.

Software Panda je vhodný i pro sítě, jejichž součástí jsou méně výkonné počítače nebo stanice se staršími operačními systémy - funguje např. i pro Win 3.x nebo OS/2, což potvrzuje i certifikát kvality, který byl firmě Panda Software udělen asociací International Computer Security Association (ICSA) a společností Checkmark (West Coast Labs) za široký rozsah podporovaných platforem. Další z řady ocenění získal letos v dubnu software **Panda Antivirus Platinum** (verze 6.23.00), a to 100 % Award od časopisu Virus Bulletin pro Windows 2000.
Vzhledem k propracované centrální správě produktů společnosti Panda je lze aplikovat i v rozsáhlejších sítích.
Aktualizace databází virů probíhá denně. Informace o nových virech lze získat z bulletinu Oxygen3 24h-365d, který společnost Panda Software na vyžádání zasílá e-mailem a poskytuje tak minimálně jednou denně nejnovější informace nejen o svých produktech, ale též o antivirovém a bezpečnostním softwaru obecně.

Nabídka společnosti Panda Software je poměrně široká a zahrnuje nejen řešení pro domácí uživatele, ale i software pro střední a velké podnikové sítě. Pro Vaši informaci uvádíme stručný **přehled produktů** společnosti Panda Software:

1) pro domácí uživatele:
- Home Edition - pro začínající uživatele, v nejbližší době bude nahrazen novým produktem Panda Antivirus Titanium;
- Panda Antivirus Platinum - pro pokročilejší uživatele.

2) pro podnikové sítě:
- Panda Antivirus Platinum - poskytuje ochranu pracovních stanic;
- Panda Antivirus for Servers and Desktops - zajišťuje ochranu stanic a souborových serverů (NT a Novell);
- Panda Global Virus Insurance - zahrnuje moduly na ochranu pracovních stanic, souborových a poštovních serverů i firewallu;
- Panda Antivirus for Firewalls - funguje na jakémkoli firewallu plně kompatibilním s CVP protokolem nezávisle na operačním systému;
- Panda Antivirus for Microsoft Proxy Server;
- Panda Antivirus for Notes / Domino Server;
- Panda Antivirus for Exchange Server;
- Panda Invent - nástroj ke správě inventáře, a to nejen hardwaru, telefonů, faxů, CD, disket, ale i softwaru v síti.

Ceny licencí jsou určeny na jeden, dva či tři roky nebo na dobu neurčitou, sleva za obnoveni licence činí 30 procent z aktuální ceny na dobu, na kterou byla zakoupena původní licence. Pro školství poskytujeme u objednávek nad 10 licencí slevu 50 procent.

Andrea Koláčková
andrea.kolackova@aec.cz

V rámci uvedení nového produktu na trh se firma AEC stala sponzorem pandy v pražské ZOO.

CeBIT na vlastní kůži

Jednou za rok se celý počítačový svět zblázní a rozhodne se dát si sraz v německém Hannoveru. Letošní „hannoverské šílení“ proběhlo ve dnech 21. až 28. března 2001 pod již ustáleným názvem CeBIT.

Stejně jako v jiných letech se bylo věru nač dívat. Pozornost nepoutaly ani tak informační technologie „denní potřeby“ (i když ani ty si v žádném případě nemohly na nedostatek pozornosti stěžovat - o tom ostatně svědčí věčně obležené stánky výrobců mobilních telefonů), ale především zařízení bližší či vzdálenější budoucnosti. Je sice pravdou, že mnoho z nich nikdy neopustí rýsovací prkna konstruktérů, ale stejně tak se mnoho z nich stane běžnou součástí každodenního života jakou jsou nyní třeba náramkové hodinky nebo teplá voda.

Návštěvníci zůstávali před jednotlivými exponáty stát v němém úžasu. Ostatně - zajímavá je třeba taková krabička velikosti mobilního telefonu, která je vybavena digitální kamerou pro videotelefonování nebo pořizování elektronických snímků. A když tuto „krabičku“ prostě „rozcvaknete“, objeví se vám jednak barevný displej a jednak klávesnice. Celé toto zařízení je pak schopné být non-stop připojené k Internetu a má stejné schopnosti jako většina běžných PC. Jedinou nepříjemnou vlastností je velikost klávesnice - ta totiž plnohodnotnou práci ještě neumožňuje (byť k poslání SMS, vyřízení e-mailu nebo brouzdání po Internetu plně postačuje). Ale žádný problém - výrobci přišli i se skládací klávesnicí, která má ve složeném stavu velikost většího balíčku od karet či pánské peněženky. Tuto stačí rozložit - a z kapsy vytáhnout zařízení, které v sobě spojuje výhody mobilního telefonu, osobního počítače a připojení k Internetu.

Výše uvedený příklad jen potvrzuje nastoupený trend posunu od jednoúčelových k multifunkčním zařízením. Notebook už není jen notebookem, ale díky čím dál většímu množství přídavných zařízení (digitální kamera se pomalu, leč jistě stává standardem) je nepostradatelným pomocníkem. Mikročip vestavěný třeba v kuchyňských spotřebičích dnes překvapí asi málokoho a díky moderním technologiím je tak možné např. pomocí Internetu kontrolovat z dovolené na druhém konci světa stav potravin v domácí chladničce…

Podtrženo, sečteno: Letošní CeBIT potvrdil svou pověst jedné z nejvýznamnějších akcí svého druhu na světě. Bylo nač se koukat a bylo o čem přemýšlet.

A propo, CeBIT 2002 se koná od 13. do 20. března 2002.

Tomáš Přibyl
tomas.pribyl@aec.cz

Roadshow 2001 - aneb cesta do Košic a zpět

Stejně jako minulý rok, tak i letos, vyrazili vybraní odborníci na problematiku antivirů a bezpečnosti dat na přednáškové turné po některých slovenských městech. Měl jsem to štěstí, že jsem mezi ně tento rok patřil i já. Mimo mojí maličkosti se na dlouhou cestu vypravil i kolega z brněnské centrály Tomáš Přibyl a také dvojice zástupců slovenské pobočky: ředitelka Alena Řezníčková a technik Ján Šimko.

V tomto složení jsme šířili osvětu postupně ve třech malebných slovenských městech: Žilině, Banské Bystrici a Košicích, a to od 15. do 17. května 2001.

Již samotná cesta do prvního působiště (Žiliny) byla nadmíru zajímavá. Z rozličných důvodů jsme z Brna vyrazili poměrně pozdě k večeru dne 14. května. Tomáš Přibyl navíc ten den asi nějakým zvláštním osobním kouzlem přitahoval pozornost příslušníků policie. Celkem nás, ještě na českém území, zastavili dvakrát. Naštěstí asi bylo zrovna po výplatě a naši uniformovaní spoluobčané neměli potřebu vybírat peníze. A důvod by se při momentálním Tomášově jízdním stylu určitě našel… Celnicemi jsme projeli již bez sebemenších problémů a v pořádku dorazili do žilinského hotelu Slovakia. Úroveň hotelu sice nebyla zrovna stoprocentní, ale únava nad námi brzy zvítězila a usnuli jsme spánkem spravedlivých.

Hned druhý den brzy ráno jsme se (samozřejmě po nezbytné snídani) vrhli na přípravu přednáškových prostor a materiálů pro očekávané návštěvníky. Netrvalo dlouho a sál se začal plnit lidmi. Obsazení sálu sice nebylo nijak oslnivé, ale na „rozjezd“ byla účast bezmála dvaceti posluchačů poměrně příjemná.

Tak jako následující dva dny vyslechli přítomní pět přednášek. V první je Tomáš Přibyl seznámil s nebezpečím, jaké představují počítačové viry. Vesměs zneklidněné posluchače poté ukonejšil Jano Šimko, který jim předvedl možnosti antivirové ochrany v praxi. Po přestávce s nezbytným občerstvením v podobě kávy a chlebíčků jsem nastoupil já a ve své přednášce vysvětlil, jak to vlastně bylo s prolomením formátu OpenPGP. Poslední dva příspěvky patřily také do oblasti bezpečnosti dat. Tomáš Přibyl promluvil na téma Rizika kybernetického prostoru a Ján Šimko popsal konkrétní bezpečností řešení Norman Security Suite. Vyčerpaní přednášející se poté rozloučili se spokojenými posluchači, posbírali si svých „pět švestek“ a vyrazili do dalšího města.

Cesta do Banské Bystrice byla poměrně příjemná. Silnice se kroutila horskými údolími a byla lemována nádhernou přírodou. Té jsem se ale bohužel nemohl dost věnovat, protože jsem měl na úzkých silnicích doslova „plné ruce“ volantu. Do banskobystrického hotelu Lux jsme dorazili v pořádku a bez nehody. Nastávající večer byl vyplněn návštěvou vybraných restauračních zařízení spojenou s prohlídkou středu města. Nicméně únava se brzy projevila a my byli nuceni ulehnout. Další den nastal opět již známý kolotoč přednášek. Účast v Banské Bystrici byla daleko největší ze všech tří uvedených měst. Již dokonale rozmluvené přednášející sledovalo více jak čtyřicet posluchačů. Nejvíce zaujalo téma elektronického podpisu, na něž se rozproudila dlouhá diskuse. Po skončení naší „produkce“ jsme, ještě před odjezdem do Košic, navštívili okolí památníku SNP.

Cesta do Košic byla sice nepoměrně delší, než předchozí den z Žiliny do Banské Bystrice, ale scenérie Spišského hradu a Liptovskej Mary byla dostatečnou „náplastí“ na unavené tělo. Ubytování v košickém hotelu Slovan bylo nadmíru příjemné, stejně jako prohlídka nočního města, ale nastřádaná únava nakonec opět zvítězila a zahnala nás do hotelového pokoje a posléze i do postele. Následující den se již od rána nesl v duchu dalších přednášek, tentokrát pro asi dvacet pozorných posluchačů, kteří nešetřili zvědavými otázkami.

Ihned po ukončení semináře jsme se srdečně rozloučili s našimi bratislavskými přáteli a vyrazili na zpáteční cestu do Brna. Košice opravdu nejsou „za humny“, takže nám zpáteční cesta zabrala bezmála sedm hodin svižné jízdy po slovenských silnicích střídavé kvality a šířky. Cesta probíhala bez větších komplikací, takže v pozdních večerních hodinách 17. května jsme již byli zpátky v Brně. Byli jsme unavení, ale šťastní, že jsme doma, a že se Roadshow tento rok opravdu povedla.

Petr Nádeníček
petr.nadenicek@aec.cz

Finanční ztráty způsobené útoky z Internetu se zvyšují

Jak vyplývá z každoroční zprávy Computer Security Institute (CSI), která byla nedávno zveřejněna, ztráty způsobené útoky prostřednictvím Internetu rok od roku stoupají. S vývojem informační společnosti se bohužel překotným tempem vyvíjí i počítačová kriminalita. To je bezesporu argument pro další posilování bezpečnostních a antivirových prvků ochrany dat.

CSI byla založena v roce 1974 v San Franciscu a sdružuje několik tisíc členů z oblasti informační bezpečnosti. Poskytuje různé služby a vzdělávací programy s cílem zvýšit informační bezpečnost ve firemních a vládních sítích.

Zpráva pod názvem „Computer Crime and Security Survey“ byla vypracována za účasti FBI (specializované oddělení pro počítačové útoky se sídlem v San Franciscu). Podkladem byly odpovědi 538 počítačových odborníků z praxe, kteří působí v různých společnostech, vládních agenturách, finančních institucích, universitách apod.

Z provedeného výzkumu vyplývá několik hlavních závěrů, které mohou vzbuzovat neklid v myslích bezpečnostních manažerů většiny firem. Zejména jsou to následující skutečnosti:

• 84 procent respondentů (zejména velké společnosti a vládní agentury) zaznamenalo porušení počítačové bezpečnosti minimálně dvanáctkrát do měsíce.

• Pouze 64 procent však přiznalo, že jim tyto útoky způsobily finanční ztráty, přičemž jen část z nich byla schopna nebo ochotna je vyjádřit v absolutních hodnotách.

• Ztráty způsobené útoky na firemní a vládní informační systémy narostly o 42 procent v porovnání s rokem předchozím.

• Celkově vyjádřeno v absolutních hodnotách škody činily 378 milionu dolarů (podle předchozí zprávy to bylo „pouze“ 265 milionu dolarů).

• Alarmující skutečností je, že 70 procent respondentů uvedlo internetové připojení jako nejčastější zdroj útoků. V porovnání s předchozím hodnocením, kdy Internet figuroval „pouze“ u 59 procent útoků, je nárůst dosti významný. Co do četnosti následují útoky zevnitř systémů, které přiznalo 31 procent dotazovaných. Minimum těchto incidentů (36 procent) vyústilo v soudní dohru.

• Účastníci výzkumu uvedli široké spektrum útoků na své systémy. Například jen počítačové viry byly detekovány v sítích 94 procent respondentů (oproti 85 procentům v předchozím výzkumu).

• V oblasti elektronického obchodu přes Internet, která byla také součástí výzkumu, uvedlo 23 procent respondentů, že do jejich systémů bylo neoprávněně vstoupeno. Zvláště alarmující skutečností však je, že kromě vandalismu a podobných aktivit 13 procent z těchto proniknutí vyústilo v krádeže informací a 8 procent přímo ve finanční zpronevěru.

Nejdůležitějším závěr zprávy však je, že „násilnost“ a počet případů proniknutí do počítačových systémů rok od roku výrazně narůstá. Je to velice cenná a alarmující zpráva pro manažery pověřené správou informačních systémů firem, kteří by si měli být vědomi své zodpovědnosti, a zajistit svoji síť vhodnými prostředky dříve, než dojde k jakékoliv nemilé události. Potom již bude pozdě „plakat nad rozlitým mlékem“. Vhodné prostředky pro zabezpečení informačních systémů jsou běžně dostupné a řadu z nich nabízí i naše firma.

Petr Nádeníček
petr.nadenicek@aec.cz

Kdes to byl(a) v noci ? *Divadlo Bez zábradlí*

Dne 15. března 2001 se k desátému výročí založení společnosti AEC v prostorách Divadla Bez zábradlí v pražském paláci Adria uskutečnilo představení komedie Alana Ayckbourna v režii Jiřího Menzla nazvané „Kdes to byl(a) v noci ?“. V hlavních rolích této mimořádně úspěšné komedie vystoupili paní Veronika Freimanová, Ljuba Krbová, pan Rudolf Hrušínský, pan Zdeněk Žák a také mnozí další. Představení, následného cocktailu a tomboly, losované představitelem hlavní role panem Zdeňkem Žákem se zúčastnilo přes 300 hostů a přiznám se, že jsme litovali, že divadlo má omezenou kapacitu. Slavnostní večer zahájila a hosty přivítala ředitelka společnosti AEC paní Alena Řezníčková.

Ano, právě deset let bylo antivirové a bezpečnostní firmě AEC. Od roku 1991 za námi zůstaly tisíce spokojených uživatelů a tisíce nespokojených počítačových virů. Cesta, kterou jsme za tu dobu urazili, byla dlouhá, Z lokálního distributora antivirových programů jsme se vyšplhali na samotný vrchol pomyslného Olympu, když jsem dokázali vyvinout bezpečnostní a šifrovací program světových parametrů IronWare Security Suite (nyní Norman Security Suite).

Pomáháme také elektronickému podpisu opustit dětské plenky v českých a moravských luzích a hájích. Bojujeme nejen proti počítačovým virům, ale také proti hackerům ve všech možných podobách. A máme úspěchy. Ano, je to tak: deset z deseti hackerů nedoporučuje bezpečnostní programy a služby poskytované AEC.

Zkrátka není toho málo, co jsme za deset let dokázali. Stejně tak toho není málo, co máme ještě na seznamu „Zbývá vykonat“.

Konference Bezpečnost dat *Hotel Holiday Inn, Bratislava*

V kongresové hale bratislavského hotelu Holiday Inn se 4. dubna letošního roku uskutečnil druhý ročník konference Bezpečnost dát. Na přípravě akce spojili síly AEC SK, SASIB a v roli mediálního partnera PC Revue. Program konference byl rozdělen na tři části, prvním tématem byla bezpečnost v počítačových sítích, druhým bezpečnost ve světě elektronického obchodu a třetím (posledním) tématem pak antivirová ochrana. Konference se zúčastnilo 150 návštěvníků z celého Slovenska. V průběhu závěrečného rautu předala společnost AEC SK dar dětem ze Základní internátní školy pro slabozraké a nevidomé v Bratislavě - Karlovej Vsi.

Stránku připravila Hana Stojanová
hana.stojanova@aec.cz

Kde jsi byl(a) v noci?

15. března 2001,

Praha

Divadlo Bez zábradlí

Výborné představení končí, nekonečná děkovačka začíná.

Po celý večer bylo o dobré pití a zábavu postaráno.

Každý účastník dostal los, někteří účastníci byli vylosováni.

Ředitelka AEC Alena Řezníčková byla za zásluhy o budování firmy oceněna.

Konec dobrý, všechno dobré.

Bezpečnosť dát 2001

3.dubna 2001,

Bratislava

Hotel Holiday Inn

T minus deset minut a odpočítáváme…

Čas nula, startujeme!

Nacpaný konferenční sál bratislavského hotelu.

Raut po skončení konference ozdobil kulturní program.

Takhle nějak to bylo, jedlo se, zpívalo, pilo.

Elektronický obchod á la AEC

Pokud patříte k těm, kteří se při pouhém pomyšlení či dokonce vyslovení sloviček „elektronický obchod“ začínají obsypávat pupínky, pokouší se o ně mrákoty a po očku se rozhlížíte po nejbližším stromě s vhodnou větví, nebojte se. Elektronický obchod AEC Vás zbaví pupínků, vyléčí z mrákot a odstraní nutkání hledat si vhodnou větev.

V e-shopu AEC není elektronické obchodování obestřeno žádnou neprůhlednou zástěnou. Vše je zcela transparentní a jednoduché, neb staré pořekadlo praví, že „v jednoduchosti je síla“. Ostatně - pojďte s námi na krátkou exkurzi do elektronického obchodu AEC.

Pokud vstoupíte na stránky shop.aec.cz, může nastat jedna ze tří možností:

1) jste tu poprvé, a tudíž ještě nejste registrován;
2) nejste tu poprvé, ale ještě jste se neregistroval;
3) nejste tu poprvé a již jste registrovaný v systému.

Z hlediska celého systému jsou přitom varianty 1) a 2) rovnocenné, protože vstupující do systému je v obou případech dosud nezaregistrovaný.

V této fázi nakupování prostřednictvím stránky shop.aec.cz ale ještě na registraci či neregistraci vstupujícího uživatele nezáleží, ta je podstatná pro běh událostí až dále.

Podobně jako v reálném světě máte i v elektronickém obchodě k dispozici „nákupní košík“, do nějž ukládáte „zboží“, které si při procházení „obchodu“ vyberete. Jak vidno, terminologie i principy reálného světa zůstaly zachovány i v kybernetickém prostoru, není tedy nutné obávat se něčeho neznámého. Jediný rozdíl mezi reálným a elektronickým obchodem je v tom, že na reálné zboží, reálný košík či reálnou prodavačku si můžete „sáhnout“.

V elektronickém obchodě procházíte mezi „regály“ (tedy pohybujete se po webovských stránkách, na nichž je nabízeno jednotlivé zboží či služby) a co se vám líbí, „ukládáte“ do svého osobního „košíku“. Přitom máte možnost do košíku zboží nejen vkládat, ale i z něj odebírat. Stejně jako v reálném světě, když se o dva regály dál rozhodnete pro vhodnější či zajímavější zboží - vložení zboží do košíku neznamená závazek jeho zaplacení!

V okamžiku, kdy se nakupující rozhodne dále v plnění košíku nepokračovat a hodlá zboží či službu získat, začíná být důležitá informace zmíněná na úvod tohoto textu - tedy zdali je registrovaný (tedy známý) či neregistrovaný (tedy neznámý). V případě, že jde o uživatele již registrovaného, nevzniká žádná další zbytečná prodleva - je zobrazena kompletní objednávka včetně plátce. Je zde i možnost poslat vybrané zboží na jinou adresu než je adresa plátce - velmi praktické například v případě dárků! Pak už následuje jen zašifrování objednávky a její odeslání prodejci.

Pokud ale systém zjistí, že uživatel pokoušející se o nákup není zaregistrovaný, je nutné před tuto finální fázi vložit ještě registraci zákazníka bezprostředně spojenou se zašifrováním a uložením těchto informací pro pozdější potřebu. Zdůrazňujeme, že uložení těchto dat je provedeno v šifrované (a tudíž bezpečné) podobě, takže nějaká „causa pojišťovna“ absolutně nehrozí. Poslední fáze je stejná jako v předchozím případě, neboť z neregistrovaného zákazníka se jakoby mávnutím kouzelného proutku stal zákazník registrovaný se všemi výhodami z toho plynoucími.

Nejčastější nejasnosti týkající se elektronického obchodování jsou zaměřeny na otázku bezpečnosti. Je to celkem pochopitelné - v reálném světě existují fyzické peníze a občanské průkazy, tedy věci, na které si lze reálně „sáhnout“ a které lze „nedat z ruky“. V kybernetickém prostoru je to kapku jiné - jsou zda jak peníze, tak identita, ale v trochu jiné podobě. Ostatně, také v bance na vašem kontě neleží balíček stokorun či tisícikorun, ale pouze jakési imaginární číslo - které ovšem v případě potřeby (a solventnosti banky) lze vmžiku proměnit na hotové „fyzické“ peníze.

Ale zpět k zabezpečení elektronického obchodu. Veškerá komunikace probíhá zabezpečená pomocí protokolu HTTPS. Autentizace se pak děje pomocí přihlašovacího jména a hesla (nebo certifikátu), které jsou jedinečné - jedná se o jakousi obdobu prokázání totožnosti a jejího potvrzení podpisovým vzorem v „kamenné“ bance. Samozřejmě, v reálném světě může někdo Váš podpis napodobit - kybernetickém prostoru to absolutně nehrozí. Heslo buď je platné nebo není. Tečka. Samozřejmě, že může dojít k jeho prozrazení (např. je příliš jednoduché nebo si jej uživatel přilepí na kus papíru na klávesnici zespod), ale to už je vina nesprávného chování uživatele (stejně jako třeba zapomenutý občanský průkaz v dopravním prostředku).

Ovšem elektronický svět má jednu velkou výhodu - zatímco v reálném můžete s občanským průkazem dělat prakticky cokoliv, heslo v kybernetickém prostoru má velmi malé uplatnění. navíc ho můžete dle libosti měnit.

Stále ještě se vám zdá elektronické obchodování složité?

Autentizace spojení prostřednictvím webu

Mnohé organizace a firmy, jež chtějí nebo potřebují komunikovat jak v rámci lokální sítě, tak i mimo ni pomocí Internetu, stojí dnes před problémem, jak tuto komunikaci zabezpečit. Zabezpečení je nutné z toho důvodu, aby se nepovolaná osoba nedostala do systému a k datům. Cílem je také zabezpečit, aby takový útočník nebyl schopen odchytit přístupové jméno a heslo přihlašovaného oprávněného uživatele, a nemohl pak jeho prostřednictvím přistupovat k chráněným a citlivým údajům v systému, v aplikacích, či na webových serverech a stránkách.

Bezpečnost informačních systémů má pro tyto potřeby v záloze termín „autentizace“. Autentizace slouží k ověření identity přihlašovaného uživatele a jeho oprávněnosti přistupovat k informacím prostřednictvím zabezpečeného spojení mezi ním a zdrojem těchto informací. Procesem autentizace prochází přihlašovaný uživatel dříve, než je mu umožněn přístup na základě příslušných přístupových práv. Teprve po autentizaci - identifikaci oprávněného uživatele je přístup povolen v odpovídajícím rozsahu.

Pro stále žádanější potřeby autentizace přichází společnost AEC se softwarovým produktem, který splňuje podmínky bezpečného ověřování a umožnění přístupu uživatelům „zvenčí“, převážně prostřednictvím internetu. Užitečnost a potřebnost takového zabezpečení ocení zejména firmy, které využívají vzdáleného přístupu k datům pro svá odloučená pracoviště a pobočky, pro mobilní pracovníky a zaměstnance na cestách, pro přístup a správu systému z domova atd.

Autentizační modul firmy AEC poskytuje tyto výhody:

• Program je vyvíjen jak pro spolupráci a využití s dalšími stavebnicovými moduly (propojení na účetní systém, databáze, elektronický obchod, další komponenty), tak i samostatně.

• Autentizace je v tomto samostatném modulu možná prostřednictvím hned několika způsobů:
- pomocí digitálních certifikátů;
- pomocí přihlašovacího jména a hesla;
- využitím autentizačních předmětů, jako jsou např. čtečky karet.

• Pro ověřování identity uživatelů je v modulu implementována možnost využít stále populárnější technologie klientských digitálních certifikátů. Princip spočívá v kontrole certifikační autority, jež vydala certifikát klienta. Pokud je certifikát podepsán autoritou přítomnou na straně serveru v podobě jejího certifikátu a certifikát má platný atribut času, je tento certifikát akceptován pro navázání spojení klient - server.

• Způsob zabezpečení přenášených dat včetně jména a hesla tkví v šifrovacím mechanismu, jenž umožňuje bezpečný průchod těchto údajů a ověření, že přihlašovaný uživatel je uveden v zašifrované databázi oprávněných uživatelů. Pro šifrování je možné volitelně využít externího propojení s šifrovacími technologiemi
- Norman;
- PGP;
- Microsoft.

• Program vytváří zabezpečený HTTPS tunel pro přenos dat mezi klientem a serverem bez rizika jejich odchycení v otevřené podobě a následného zneužití.

• Výhodou řešení AEC je zajištění řízeného přístupu v prostředí webu i do intranetu bez vazby na účty operačního systému, a to bez omezení co do počtu licencí systému.

Funkce programu jsou maximálně přizpůsobovány volbám uživatelů a jsou budovány pro téměř univerzální využití. Vycházejí z potřeb zákazníků, myslí na jejich nejčastější požadavky, sledují nejnovější trendy a jsou využitelné v běžném prostředí současných systémů.

Produkt firmy AEC je vyvíjen jako samostatný modul aplikovatelný v prostředí klient/server na těchto platformách:

• klient - www prohlížeč pro Windows 95, 98, NT;
• server - Windows 2000 server.

Olga Přikrylová
olga.prikrylova@aec.cz

Vyzkoušejte NORMAN VIRUS CONTROL

vyzkoušeli ho i ve společnosti Virus Bulletin Ltd. a podívejte se na výsledky

Norman získal Virus Bulletin 100%

Světově uznávaný časopis Virus Bulletin testuje a hodnotí všechny známé antivirové produkty od roku 1998. V současné době se testy uskutečňují každé dva měsíce. Testování a následné ocenění je považováno za vysoké uznání technických vlastností antivirového produktu.

Nejnovější testy Virus Bulletinu byly první důležitou zkouškou nové technologie Norman Virus Control v5 uvedené na trh nedávno a právě tato nová generace produktu způsobila, že v únorovém testu 2001 obstál se cti.

(Více informací najdete na
http://www.virusbtn.com/100/ .)

Tuto verzi máme exkluzivně k dispozici a vy ji můžete zdarma zkoušet.
Naše technické oddělení vždy provádí testy nové verze před uvedením na českém trhu, a od poloviny března si můžete o tuto verzi požádat. Současně u nás probíhá překlad do češtiny. Na vyžádání obdržíte informační materiály k produktu Norman Virus Control v tištěné nebo elektronické podobě.
Přestože testy na viry jsou jedním z ocenění produktu, tento produkt je navíc velmi svižný, spolehlivý, jednoduchý na používání a nenáročný na HW prostředky. Kromě uživatelsky příjemnějšího, intuitivnějšího a atraktivnějšího grafického interface, nabízí verze 5 lepší funkčnost, která upevňuje pozici tohoto produktu mezi produkty bojujícími proti útokům škodlivých programů.

Norman Virus Control 5

- zjednodušuje život administrátorům jednodušší instalací, updaty, konfigurací, správou.
- zaměřuje se na správu softwaru a snížení nákladů majitelů společností, protože jednodušší instalace a správa výrazně šetří čas administrátorů, skenování probíhá transparentně a nezatěžuje uživatele, jsou poskytovány automatické aktualizace přes Internet.

Jednodu instalace

Instalace na jednotlivé stanice je velmi jednoduchá. Instalujete NVC na vybraném počítači (administrátora), zvolíte nastavení konfigurace a určíte stanice, na nichž má být NVC instalován. Zbývající část instalace proběhne automaticky. NVC bude během několika minut instalován na zvolených počítačích.

JednoduchÆ správa

Správa tohoto softwaru je také velmi jednoduchá. Instalace, údržba a konfigurace jsou v NVC centralizovány. Administrátor může z jednoho jediného místa spravovat stanice podle typu sítě buď jako skupinu nebo jako samostatné jednotky. Sami rozhodujete o tom, které moduly instalujete nebo odinstalujete a určíte, jaká oprávnění přidělíte koncovým uživatelům. Případné změny jsou účinné po několika minutách. Systém hlášení lze konfigurovat mnoha způsoby (hlášení varovných zpráv o napadení viry, zápisy o různých jiných událostech do souboru nebo na konzolu …). Zaměstnanci IT tak ušetří spoustu času a mohou jej věnovat dalším potřebám systému IT společnosti

Transparentnost

Většina uživatelů si nepřeje být aktivně zatěžována kontrolou virů. Uživatelé v rozsáhlých sítích nepotřebují ani vědět, že mají na svých počítačích instalovaný antivirový program. Neustálá přítomnost antivirového programu působí velmi rušivě. Verze 5 softwaru NVC zajišťuje nerušenou práci těmto uživatelům. V tomto případě je vše řízeno a spravováno z jednoho počítače.

Aktualizace přes Internet

Pomocí Norman Internet Update (NIU) lze nyní aktualizovat celý produkt přes Internet. V současné době existuje přibližně 50 000 různých známých virů. Stále se však objevují nové viry a NVC je průběžně aktualizován, aby byla neustále poskytována ochrana před možným ohrožením. Můžete nakonfigurovat NIU tak, abyste prověřili aktualizované programové moduly a databáze virů v pravidelných intervalech. Administrátoři mohou konfigurovat NVC tak, aby tento software stahoval a distribuoval aktualizace na veškeré pracovní stanice i servery, včetně počítačů zaměstnanců, kteří pracují doma.

Jitka Brandejsová
jitka.brandejsova@aec.cz

Nová produktová řada od Kaspersky Lab

Společnost Kaspersky Lab (světový producent antivirových a bezpečnostních programů) nedávno představila inovovanou řadu svého pilotního produktu - Kaspersky™ Anti-Virus. Nová řada produktů v sobě odráží marketingovou strategii firmy spočívající v širší orientaci na potřeby koncového zákazníka.

Podle nové produktové řady jsou nyní všechny programy od Kaspersky Lab rozděleny do tří základních kategorií:
- domácí uživatelé;
- malé a střední podnikové sítě;
- rozsáhlé podnikové sítě velkých firem.

V kategorii domácích uživatelů Kaspersky Lab nabízí:

• **Kaspersky AV Lite:** „odlehčená“ verze známého programu AVP s novým rozhraním speciálně upraveným pro začínající uživatele.

• **Kaspersky AV Personal:** balík pro komplexní antivirovou ochranu určený pro zkušené uživatele včetně ochrany e-mailu.

• **Kaspersky AV Personal Pro:** nejobsáhlejší balík v této kategorii, který obsahuje antivirový skener, monitor, e-mailový filtr, prostředky pro kontrolu skriptů a integrity systému, nástroj pro blokování činnosti podezřelých programů a v neposlední řadě uživatelskou konzoli.

Kaspersky AV Personal a **Personal Pro** obsahují jako jedny z mála antivirových programů modul pro detekování a odstranění virů v e-mailové databázi programu Outlook Express. Oba tyto balíky programů jsou již nyní k dispozici. Kaspersky AV Lite je možné koupit pouze v Kasperskeho on-line obchodu, formou OEM nebo v rámci speciálních akcí.

Pro potřeby malých a středních firem Kaspersky Lab nabízí balík **Kaspersky Business Optimal**, který obsahuje jak antivirovou ochranu pro stanice (Windows 95/98/ME, Windows 2000/NT, Linux, OS/2, MS Office 2000 a DOS), tak i pro servery (Windows 2000/NT Server, Linux, Novell NetWare, FreeBSD a BSDi) a e-mailové brány (MS Exchange Server, Lotus Notes/Domino, Sendmail, Qmail a Postfix). Tento balík je také vybaven nástroji pro komplexní centralizovanou síťovou správu antivirové ochrany.

Obsah balíku (jednotlivé jeho komponenty) Kaspersky Business Optimal lze upravit podle individuálních požadavků, což umožňuje určit cenu na úrovni zákazníkových potřeb a možností.

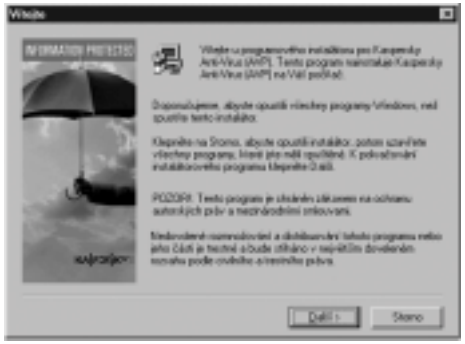
Pro velké firmy s rozsáhlými podnikovými sítěmi nabízí Kaspersky Lab balík **Kaspersky Corporate Suite**. Mimo podpory všech běžných operačních systémů a aplikací pro stanice, servery a e-mailové brány Kaspersky Corporate Suite poskytuje komplexní centralizovanou kontrolu síťového provozu (jak směrem dovnitř lokální sítě, tak i ven) prostřednictvím CVP kompatibilních firewallů. Balík také obsahuje program **Kaspersky WEB Inspector**, který chrání firemní webové stránky proti neautorizovaným změnám a v poslední době před stále častějšími útoky hackerů. V průběhu tohoto roku má být do popisovaného balíku zařazen i distribuovaný softwarový firewall.

V případě přání zákazníka může být balík Kaspersky Corporate Suite doplněn řadou dalších poskytovaných služeb, které mu pomohou v budování plně zajištěné sítě s komplexním bezpečnostním řešením.

Všechny ostatní dříve běžné služby zákazníkům, včetně denních updatů po Internetu, zůstávají zachovány.

AEC, spol. s r.o. **(www.aec.cz)** je distributorem antivirových produktů společnosti Kaspersky Lab a poskytovatelem služeb v oblasti antivirové ochrany a bezpečnosti dat.

Erik Borecký
erik.borecky@aec.cz



Průvodce světem VPN

V poslední době se často objevují tato tři magická písmena v souvislosti s bezpečností dat. Co ale ve skutečnosti VPN je a jak pracuje? Na tuto otázku se Vám pokusím dát odpověď v následujícím článku.

VPN je soubor metod a služeb, které umožňují chráněnou komunikaci v otevřené síti. VPN šifruje IP datagramy, používá silnou autentizaci, před povolením komunikace sleduje integritu dat pro zajištění, že doručené pakety došly nezměněny. VPN se používá pro zajištění zabezpečené komunikace mezi počítačovými sítěmi. Konkrétně je VPN využíváno mezi sítěmi velkých firem, geograficky vzdálených, které potřebují zabezpečit chráněnou komunikaci mezi sebou a svými partnery. Tradičně jsou pro tento účel vyžívány WAN - X.25. Dnes je k dispozici Internet a patří k relativně nejlevnějším řešením pro realizaci komunikace mezi sítěmi. Většina uživatelů, pokud bude potřebovat vyžít VPN, nebude chtít, aby VPN zasahovala do jejich rutinních záležitostí, tzn. chtějí, aby celá záležitost probíhala transparentně. Aplikace musí být schopny běžet, bez jakýchkoliv znalostí VPN služeb, které pracují na nižších vrstvách. Transparentnost je velmi důležitým prvkem VPN.

VPN provádí všechny své služby, autentizace, šifrování, kontrola integrity, na síťové vrstvě referenčního OSI modelu. Aplikace provádí tyto činnosti na vrstvách vyšších. Přesunem těchto služeb na síťovou vrstvu je umožněno systému poskytnutí původních služeb pro všechny aplikace, přičemž tyto aplikace nemusí mít žádné znalosti zabezpečení.

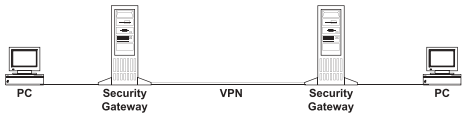
Tunneling je základní vlastností všech implementací VPN. Jsou definovány dvě základní třídy tunelů:

End - to - End Tunneling

Tunel mezi vzdáleným počítačem a serverem, ke kterému je připojen uživatel. V tomto scénáři musí obě koncové stanice držet nastavení VPN tunelu, provádí šifrování a dešifrování dat, přenášených mezi těmito body.

Node - to - Node Tunneling

Druhým typem tunelů je node - to - node, kde tunel končí na okraji sítě. Tento typ je používán pro propojování dvou LAN geograficky vzdálených. V této konfiguraci je veškerý provoz na LAN nezměněn. Komunikace prochází skrz VPN security gateway na hranici sítě, kde jsou přenášená data zašifrována a odeslána do druhé sítě. Na hranici druhé sítě jsou data dešifrována a po LAN dále přenášena v originálním formátu.



IP Security (IPSec)

IPSec je soubor protokolů, vytvořených pro chráněnou IP komunikaci přes Internet. Je vyvíjen IETF (Internet Engineering Task Force) IP Security Working Group a od roku 1995 je specifikován v Internet Draft documents (IDs) a RFC. Cílem skupiny je definování protokolů, které poskytují ochranné prvky, které chybí v IPv4. IPSec kombinuje několik různých bezpečnostních technologií k poskytnutí utajení, integrity a autenticity.

IPSec specifikuje 2 typy záhlaví které jsou připojeny k IP-datagramu. Poskytují bezpečnostní služby v IPv4 a Pv6.

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

Autentication Header (AH)

Hlavní výhodou AH je poskytnutí potvrzení původu dat v IP-datagramu. Toto je provedeno pomocí kryptografické autentizační funkce pro IP-datagram s použitím autentizačního klíče. Příjemce zkontroluje správnost autentizovaných dat při přijetí. Určité položky, které musí být měněny během přenosu (např. počet hopů), jsou vyjmuty z autentizačního výpočtu. AH protokol je navržen tak, aby byl schopen pracovat s jakýmkoliv autentizačním algoritmem. Dva algoritmy jsou povinné pro IPSec - SHA1, MD5. AH dále poskytuje zajištění integrity a zabezpečení odpovědi. AH neposkytuje utajení IP-datagramů.

Encapsulating Security Payload (ESP)

ESP protokol poskytuje bezpečnostní službu pro IP-datagramy, nejdůležitější utajení, které neposkytuje AH. ESP volitelně také poskytuje služby poskytované AH , jmenovitě původ dat, kontrola integrity a ochranu odpovědí.

Utajení je dosaženo zabalením buď celých IP-datagramů, nebo zabalením pouze protokolů vyšších vrstev (TCP, UDP) do ESP, zašifrování ESP obsahu a přidáním nového IP-záhlaví k tomuto zašifrovanému paketu.

Pokud je zapouzdřen IP-datagram, můžeme pracovat v módu tunnel. Protože toto ukrývá zdrojovou a cílovou IP-adresu, může se dosáhnout nejen utajení dat v transport módu, ale také utajení komunikačního proudu. Utajení je dosaženo zapouzdřením dat do zašifrovaného ESP paketu. ESP může být využito jak v transportním, tak v tunneling módu.

Operační módy

V předchozím textu je zmíněno, že oba typy protokolů lze využít ve dvou režimech - trans-portním a tunneling. Rozdíl mezi nimi je následující: Tunneling mode nechává originální IP-datagramy a balí je do nových paketů s novým záhlavím. Transport mode přidá nové AH/ESP záhlaví mezi originální záhlaví a data. Obecně, tunel mode zapouzdří IP vrstvu paketu, transport zapouzdří pouze vyšší protokolovou vrstvu - TCP a UDP datagram.

Authenticated data	Encrypted Data

Barevné rozlišení

IP Header	AH	IP Peyload

AH Transport Mode

Veškeré vstupující datagramy, jsou autentizovány autentizačním mechanismem, vytvořeným podle odpovídajícího SA. Datagram je odesílán jako plain text.

New IP Header	AH	Old IP Header	IP Peyload

AH Tunnel Mode

V tunneling módu je IP-datagram je předřazen novým IP-záhlavím. Dále je datagram autentizován AH protokolem, autentizace se zapíše mezi nové a staré záhlaví datagramu. Datagram je stále odesílán jako plain text. Rozdíl je, že nové IP-záhlaví má pouze směrovací informace k jednotce na konec tunelu. Cílová směrovací informace je uložena v původním IP-záhlaví.

IP Header	ESP Header	IP Payload	ESP Footer	ESP Authenticated Data

ESP TransportMode

Utajení je dosaženo zapouzdřením dat do šifrovaného ESP datagramu. V transportním módu jsou zašifrovány pouze protokoly vyšší vrstvy (TCP, UDP). Originální IP obsah je autentizován a zašifrován, ale bez původního IP-záhlaví. Z tohoto důvodu zdrojové a cílové směrovací informace jsou čitelné po celou dobu přenosu.

New IP Header	ESP Header	IP Header	IP Payload	ESP Footer	ESP Authetication Data

ESP Tunnel Mode

V módu tunnel je celý IP-datagram zapouzdřen do ESP. Protože toto skrývá zdrojové a cílové směrovací informace, bylo dosaženo kromě utajení dat také utajení přenosu. ESP tunnel skryl adresní informace, omezující se pouze na části pro doručení datagramu.

Jak jsem dříve zmínil, je možné použít oba protokoly AH i ESP. Vyplývající formát paketu závisí na módu pro AH a ESP. V případě, kde je ESP použito v tunnel módu a AH v trans-port módu, je výsledný datagram následující:

New IP Header	AH	ESP Header	IP Header	IP Payload	ESP Footer	ESP Authetication Data

AH Transport Mode, ESP Tunnel Mode

Originální IP datagram je zapouzdřen do ESP a vygenerován nové IP-záhlaví. Potom je aplikováno AH, mezi novým IP-záhlavím a ESP paketem. Nakonec je potřeba vzít v úvahu kdy použít tunnel mód a kdy použít transport mód. Transport mód se normálně používá mezi dvěma komunikačními body, Tunnel mód je využíván v komunikaci mezi sítěmi. Takhle je možné pro dva počítače mít nastaven transport mód položený v chráněném tunelu mezi dvěma bezpečnostními branami.

Tomáš Kočnar
tomas.kocnar@aec.cz

Elektronický bulletin

Milí přátelé!
Vítáme Vás při četbě našeho informačního bulletinu, který má za cíl seznámit Vás s novinkami na poli bezpečnosti informačních systémů.
AEC, Data Security Company

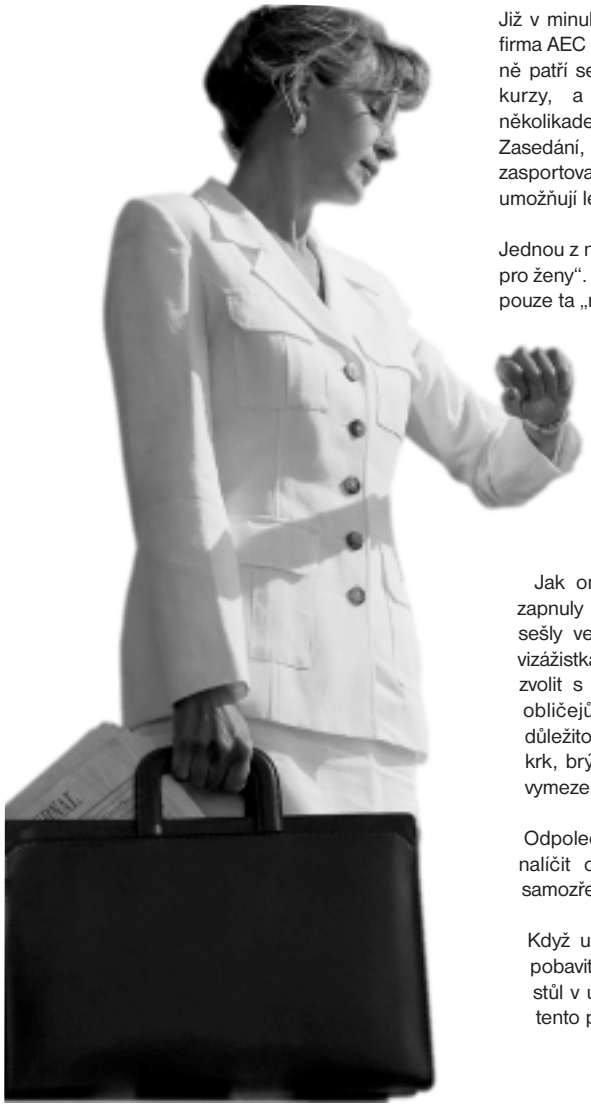
Těmito víceméně formálními řádky začíná každé vydání našeho elektronického bulletinu, které pro vás více či méně pravidelně s dvoutýdenní periodicitou připravuje kolektiv odborníků z firmy AEC. Elektronický bulletin je v současné době záležitostí vpravdě tuctovou, přesto je ten „náš“ v něčem jiný než ostatní.
Stará známá pravda praví, že „s nepřítelem, kterého známe, se bojuje lépe, než s nepřítelem neznámým“. V oblasti informačních technologií to platí dvojnásob, v případě boje proti počítačovým virům pak ještě výrazněji. Každá včas získaná informace má cenu zlata - je možné se lépe připravit, uživatele varovat. (V každém případě je jednodušší člověku vysvětlit, že nemá spouštět přílohu VIRUS.EXE než že má být opatrný v případě jakékoliv přílohy.)

A právě především novinkám v oblasti počítačových virů a antivirových technologií stejně jako bezpečnosti dat vůbec, je věnovaný elektronický bulletin připravovaný společností AEC.

Možná namítnete: Proč nějaký bulletin, když je možné všechny tyto informace a mnohdy i nepoměrně podrobněji získat třebas z webovských stránek? Ano, to je pravda. Ale kdo z nás má chuť stále „projíždět“ donekonečna webovské stránky antivirových firem, zdali se právě teď neobjevilo něco „ošklivého“. Ty nejdůležitější a nepotřebnější informace pro Vás v případě bulletinu připraví fundovaní odborníci, v případě nějaké skutečně nebezpečné a rychlé virové nákazy (např. causa Iloveyou) jsou navíc rozesílána mimořádná varování.

Podtrženo, sečteno - elektronický bulletin připravovaný AEC je velmi silnou zbraní v boji proti počítačovým virům a dalším nepravostem, které mohou Váš počítač (resp. počítače) ohrožovat.

A na závěr ještě dlužíme informaci, kde a jak se k odběru elektronického bulletinu přihlásit. Tak tedy: Stačí navštívit stránky **www.aec.cz**, kde na levé straně pod nabídkovým menu naleznete okénko. Do něj vložíte svůj e-mail, stisknete „Přihlásit se“ a můžete se těšit na informace přicházející v elektronických bulletinech AEC.



Již v minulém čísle našeho bulletinu jste se mohli dočíst, že firma AEC pořádá nejrůznější akce pro své zaměstnance. Mezi ně patří semináře a školení pro zvýšení odbornosti, jazykové kurzy, a hlavě - mezi zaměstnanci nejoblíbenější - několikadenní výjezdní zasedání po celé České republice. Zasedání, při nichž se můžeme oddat rekreaci a relaxaci, zasportovat si, pobavit se. Pobyty mimo firmu nám také umožňují lépe se poznat a stmelit kolektiv.

Jednou z nedávných akcí pořádanou naší firmou byl i tzv. „Den pro ženy“. Sám název již napovídá, že tohoto dne se zúčastnila pouze ta „něžnější“ polovička naší firmy - tedy ženy. O co šlo?

Všechny ženy i dívky - na věku nezáleží - se chtějí líbit svým blízkým, chtějí pozitivně působit na své okolí, své známé i své obchodní partnery. A právě ve „Dni pro ženy“ jsme se mohly dozvědět o nejnovějších trendech v líčení a účesové tvorbě, o tom, co se právě nosí, jak si udržet dobrou kondičku, no zkrátka - co dělat, abychom byly IN.

Jak onen den probíhal? Ráno, namísto toho abychom zapnuly počítače a vrhly se do plnění svých úkolů, jsme se sešly ve školící místnosti naší firmy. Zde na nás čekala vizážistka, od které jsme se dozvěděly, jaké střihy oblečení zvolit s ohledem na naši postavu, jaké rozlišujeme tvary obličejů a které účesy jsou k nim vhodné. Podtrhla důležitost výběru doplňků - jako jsou náušnice, ozdoby na krk, brýle, šátky apod. Ani jsme se nenadály a dopoledne vymezené k její přednášce bylo pryč.

Odpoledne jsme všechny mohly využít příležitosti, nechat se nalíčit od profesionální kosmetičky. Žádná z nás si ji samozřejmě nenechala ujít.

Když už jsme byly takto upravené, byl by hřích nejít se pobavit někam do společnosti. Proto jsme si zarezervovaly stůl v útulné, stylové restauraci v centru Brna a zakončily tento příjemný, nepracovní den výbornou večeří.

Eva Šebková
eva.sebkova@aec.cz

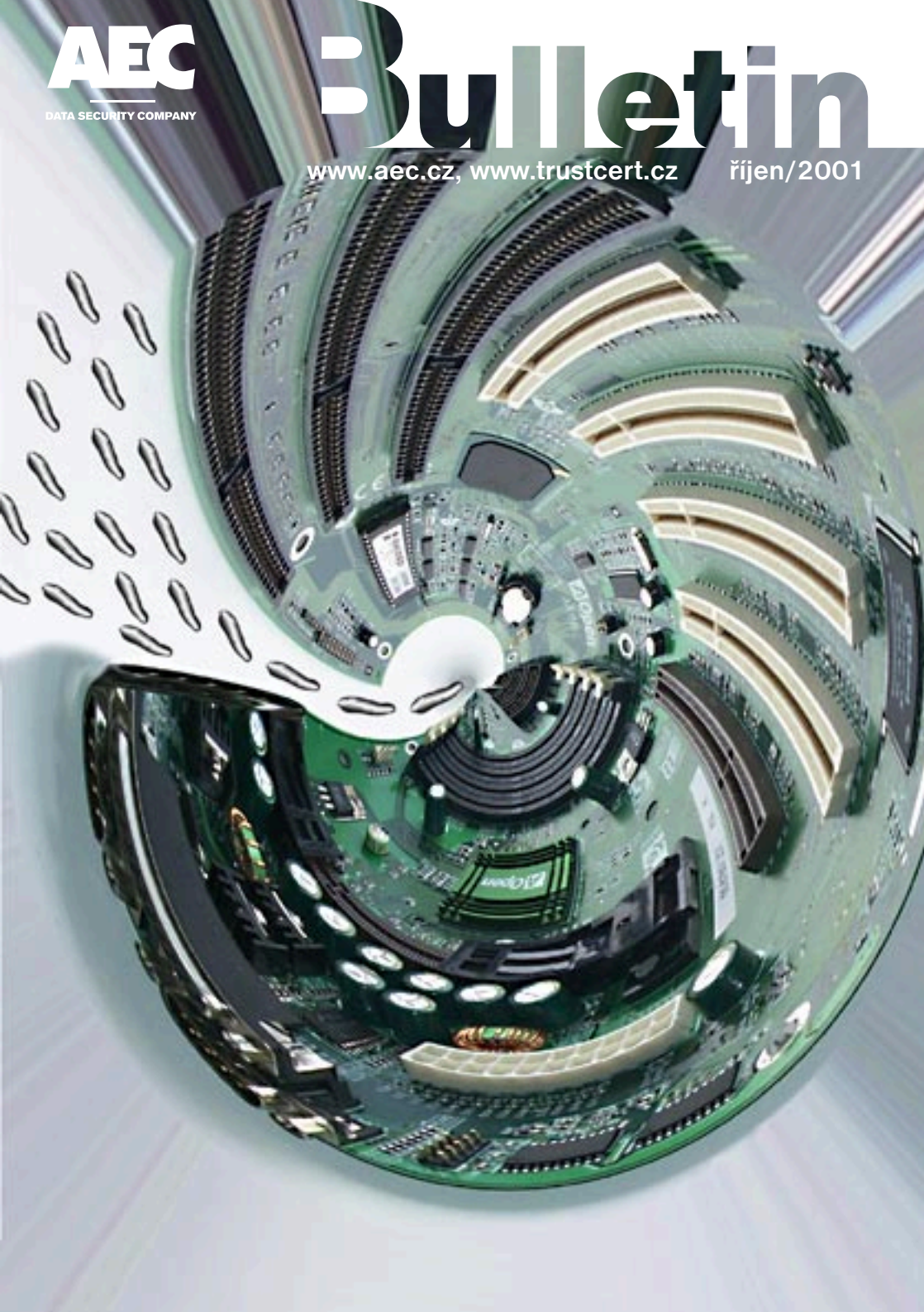
©Vydává AEC, spol. s r.o., Bayerova 799/30, 602 00 BRNO, tel.: (05) 4123 5466-7, fax: (05) 4123 5038, www.aec.cz, www.trustcert.cz

AEC

DATA SECURITY COMPANY

Bulletin

www.aec.cz, www.trustcert.cz říjen/2001



Úvod

Milí přátelé!

Právě držíte v rukou podzimní číslo našeho AEC informačního bulletinu. Co nás dnes čeká na jeho stránkách? Informace o akcích, kterých jsme se zúčastnili či které jsme pořádali. Ohlédnutí za konferencí Security 2001. Informace o našem působení v rámci veletrhu informačních technologií Invex. Popisy počítačových virů a dalších škodlivých kódů z poslední doby. Základní seznámení s oblíbeným bezpečnostním software PGP. A mnoho dalšího - věříme, že zajímavého - čtení. Přejeme příjemné počtení a neméně příjemný podzim!

Tomáš Přibyl
tomas.pribyl@aec.cz

Ve stínu teroru: Vote

Jako sup parazitující na neštěstí druhých se chová nově objevený e-mailový červ Vote. Jedná se o přímo ukázkový případ sociálního inženýrství, když se snaží nabádat uživatele počítače k otevření přílohy výzvou, aby po nedávných tragických událostech ve Spojených státech hlasovali pro mír…

Vote se šíří ve zprávě elektronické pošty s následujícími parametry:

Předmět: Fwd:Peace BeTweeN AmeriCa And IsLaM !

Zpráva: Hi <Jméno> iS iT A waR Against AmeriCa Or IsLaM !? Let's Vote To Live in Peace!

Příloha: WTC.exe

Vote v počítači vytváří dvojici nových souborů. První z nich se jmenuje MixDaLaL.VBS, přičemž červ jej vytváří ve složce Windows a spouští okamžitě. Je to skript, který vyhledává všechny soubory s příponou HTM a HTML na lokálních discích a přepisuje je krátkým textem:

AmeRiCa …Few Days WiLL Show You What We Can Do !!! It's Our Turn >>> ZaCkEr is So Sorry For You .

Druhý soubor je vytvořen v systémovém adresáři Windows pod jménem ZaCker.VBS a zapíše se do registrů do auto-run sekce. To znamená, že soubor je automaticky vykonán při následujícím (re)startu Windows. Po spuštění se pokouší smazat všechny soubory v adresáři Windows a přepíše AUTOEXEC.BAT příkazem likvidujícím data na disku C:.

Poté zobrazí zprávu:

I promiss We WiLL Rule The World Again…By The Way,You Are Captured By ZaCker !!!

Družicový snímek na Pentagon poškozený útokem teroristů.

Invex 2001

Pravidelně vždy v podzimním čísle našeho bulletinu jsme Vás rok co rok zvali na veletrh informačních technologií Invex na náš státek. Letos jsme se ovšem rozhodli tuto „tradici“ pozměnit. Bez dlouhých okolků proradím, že tentokrát se Invexu coby vystavovatelé neúčastníme, takže náš stánek budete hledat marně.

Již několik let byly na všech předinvexovských poradách na pořadu dne otázky „má smysl na tuto akci jít?“ Nehledě na diskutabilní návratnost této investice je pro firmu personálně velmi náročné zajistit odborné obsazení veletrhu a současně udržet provoz technické podpory našich klientů. Nakonec jsme usoudili, že nejlepším (a asi jediným) způsobem, jak zjistit, zdali Invex má smysl či nikoliv, je změnit formu naší účasti. A tak jsme se rozhodli tento „pokus“ udělat letos.

To ale neznamená, že bychom na Invexu nebyli - budeme se o to více podílet na několika akcích, které jej doprovázejí - viz níže.

Nepřítomnost našeho stánku na Invexu neznamená, že bychom neměli co vystavovat - ostatně už teď žijeme přípravami na CeBIT, který bude příští rok v březnu.

Takže přestože náš stánek na letošním Invexu navštívit nemůžete, nás najdete určitě. Na shledanou na Invexu!

Alena Řezníčková

Akce, na kterých se AEC v rámci Invexu podílí:

E-Zona

Pondělí, úterý, středa - vždy od 11:00 do 11:30 hodin.
Elektronický podpis - sliby, mýty, realita (přednáší Jan Novotný)
Bezpečí a bezpečnost v elektronickém obchodě (Olga Přikrylová)
Desatero počítačové bezpečnosti (Tomáš Přibyl)

Konference o počítačových virech a antivirových programech

pořádaná pod záštitou vydavatelství Vogel Publishing
ve čtvrtek 18. října 2001 ve výškové budově u hlavní brány BVV.
Vstup zdarma!
Počítačové viry v roce 2001 (přednáší Tomáš Přibyl)
Řešení virových incidentů ve velkých společnostech (Tomáš Vobruba)

Informační bezpečnost - konference pořádaná pod záštitou AFCEA.

Normy digitálních podpisů (ISO/IEC) - přednáší Jaroslav Pinkava.
Termín konání: 15. října 2001, 15:30 až 16:00 hod.
Místem konání je pavilon G2 na Invexu.

Pro bližší informace sledujte **www.aec.cz**
Samozřejmě, že jste zváni také do sídla naší firmy v Brně (Bayerova 799/30).

SETKÁNÍ NA WORKSHOPU 11. ZÁŘÍ 2001

Několikrát do roka se setkáváme se zástupci společností, se nimiž spolupracujeme, abychom prodiskutovali různé otázky z oblasti informačních technologií, především otázky bezpečnosti dat a komunikace. Tentokrát jsme tedy pozvali naše obchodní partnery na wokshop Bezpečnost dat 11. září 2001 do prostor budovy Stimbuildingu v Praze. S mnohými spolupracujeme léta, některé poznáme právě až při příležitosti, jakou byla například tato. S obchodními partnery si v průběhu roku často píšeme nebo voláme, ale díky podobným seminářům bouráme onu anonymitu elektronického mailování a telefonického hovoru a potkáváme se i osobně.

Ani tento workshop nebyl výjimkou z řady předchozích seminářů a nabídl mnoho informací o bezpečnostních produktech a službách AEC, představil nová řešení a nové pohledy na všeobecné trendy.

Snad nejvýstižněji hovořily titulky v programu workshopu, které doslova zněly: „Dějství první: Trocha teorie nikoho nezabije“ a „Dějství druhé: Praxe nad zlato“. První přednášky obsahovaly mnoho teorie o světě bezpečných dat a bezpečné elektronické komunikaci, o šifrování i autentizaci a souvisejících technologiích, o bezpečnosti v elektronickém obchodování. Druhá část byla věnována podrobným praktickým ukázkám produktů, zejména pro šifrování a elektronický podpis.

Software Norman Security Suite, který byl představen na workshopu, určený k šifrování dat a elektronickému podepisování, byl vyvinut naší společností AEC. Druhým představeným byl PGP (Pretty Good Privacy), jehož autorem je Philip R. Zimmermann (Více viz článek na stranách 16-18). Oba umožňují velkou komfortnost, oba nabízejí širokou funkčnost uživateli a o obou si účastníci měli možnost díky podrobnému výkladu a početným praktickým ukázkám udělat relevantní obrázek a srovnání.

„…nová řešení na trhu a nový vývoj v AEC, rozšíření obchodních příležitostí a …“, slibovala pozvánka a ve skutečnosti šlo o představení dokonce čtyř produktů: elektronického obchodu a autentizačního modulu, antivirového řešení společnosti Panda Software a společnosti Sybari.

Naše společnost vyvíjí nové aplikace zaměřené na e-byznys a další webové aplikace, jejichž charakteristickými znaky je právě kvalita zabezpečení a spolehlivost autentizace.

Na druhou stranu jsme společností, která kdysi vznikla jako antivirová firma a jako taková stále poskytuje rozsáhlé služby a širokou nabídku antivirových produktů. Poskytnout nejvhodnější antivirové řešení a tedy nebýt závislý na jednom dodavateli je i důvodem, proč jsme letos rozšířili nabídku o produkty společnosti Panda Software a Sybari.

Poptávka po vypracování analýzy rizik či bezpečnostní politiky ze strany obchodních partnerů i zákazníků je natolik častá, že jsme se rozhodli toto téma nabídnout na workshopu také. Koncepční a systematický přístup v této problematice a praktický způsob provedení je velkou neznámou, a díky preciznímu vysvětlení těchto otázek patřila přednáška mezi nejúspěšnější.

„…přednášející mají velmi dobré znalosti…“, takto pochvalně ohodnotil jeden ze zúčastněných úroveň přednášejících a těm patří velký dík, protože si své přednášky připravili nadmíru kvalitně a poutavě. Na workshopu vystoupili s příspěvky jak kolegové z Brna tak z Prahy, jak IT konzultanti a obchodníci, tak techničtí specialisté - Olga Přikrylová, Helena Ciprysová, David Pavlíček, Petr Nádeníček, Tomáš Přibyl a já.

Kladná hodnocení workshopu převážila a hřála nás na srdci, tak za všechny například tohle: „…kvalitně připraveno, jako vždy u AEC…“.

Zase někdy příště!
Jitka Brandejsová

AEC Data Security Day - 9. až 11. října 2001

Společnost AEC - navazuje na úspěch své jarní akce Roadshow po slovenských městech pořádáním další série odborných přednášek z oblasti antivirové ochrany a bezpečnosti dat, tentokrát pod názvem AEC Data Security Day.

Se vzrůstajícím podílem dat a především dokumentů v elektronické podobě neustále stoupá i význam jejich zabezpečení. Tento trend není rozhodně krátkodobým jevem, ale trvá již několik let. S problematikou bezpečnosti dat úzce souvisí také otázka realizace účinné antivirové ochrany, která stále častěji palčivě doléhá především na firmy, jejichž zaměstnanci komunikují prostřednictvím e-mailu.

Semináře se stejně jako na jaře uskuteční ve třech vybraných slovenským městech. Vedle aktuálních témat z oblasti počítačové bezpečnosti se budeme v přednáškách věnovat také stěžejním antivirovým produktům z portfolia AEC. Přednášet budou odborníci AEC z České i Slovenské republiky. Mediálním partnerem akce je známý počítačový měsíčník PC WORLD.

Nedílnou součástí AEC Data Security Day bude možnost navázání spolupráce dalším firmám z oboru informačních technologií, pro které máme v rámci této akce připravenu zajímavou nabídku. Všichni dealeři našich produktů, kteří se AEC Data Security Day zúčastní, obdrží o sto procent vyšší rabat při prodeji produktů F-Secure.

Na závěr každého dne proběhne slosování účastníků o věcné ceny, mezi nimiž je mimo jiné také například padesáti-procentní sleva na F-Secure Antivirus a řada dalších cen.

Termíny konání:

9. října (úterý)
Bratislava - hotel Danobe

10. října (středa)
Komárno - hotel

11. října (čtvrtek)
Banská Bystrica - hotel Lux

Průběh:

9:30 hodin	prezence
10:00 hodin	zahájení přednášek
12:00 - 12:30	přestávka spojená s občerstvením
14:00 hodin	ukončení přednášek

Témata přednášek:

Alena Mračková Úvod, představení firmy AEC

Jano Šimko
AV program F-Secure - bezpečnostní politika bez kompromisů

Kaspersky Anti-Virus - kvalitní a osvědčený strážce Vašich dat

Petr Nádeníček
McAfee VirusScan - pro stanice i sítě Norman Virus Control - jednoduchý a účinný

Účast na semináři je bezplatná. Přihlášení je možné vyplněním a odesláním návratky na adresu naší bratislavské kanceláře nebo prostřednictvím formuláře na webových stránkách **www.aec.sk**

Neváhejte a přijďte se na nás podívat! Určitě nebudete litovat a nabyté znalosti pro Vás budou jistě přínosem.

Alena Mračková
AEC Bratislava

Novinky mezi počítačovými viry

Podle statistik antivirových firem se každý měsíc objeví pět až osm set nových škodlivých kódů. Jen málo z nich ovšem představuje pro uživatele počítačů skutečné nebezpečí. Na následujících řádcích se lze seznámit s tím nejzajímavějším, co se na poli škodlivých kódů za poslední měsíce objevilo - jedná se jen o stručné popisy, podrobnější najdete na **www.aec.cz**

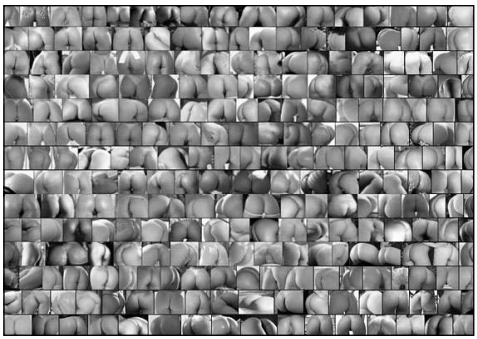
Spuštěn bez kliknutí: Cuerpo

Hlavní vlastností tohoto kódu je, že ke spuštění ani není třeba kliknout na „nakaženou“ přílohu e-mailu, ale úplně stačí, pokud zprávu jednoduše otevřete. Zpráva je vždy ve formátu HTML. Nebezpečný skript může být také obsažen v přiloženém souboru s koncovkou VBS.

Není také bez zajímavosti, že červ nespoléhá pouze na jedinou šířící rutinu. Mimo používání poštovního klienta MS Outlook, také sbírá e-mailové adresy z databázových souborů různých typů, ukládá je do souboru a odesílá na webovskou stránku autora viru. Tam byly došlé e-mailové adresy zpracovány tak, že na ně byl odeslán infikovaný e-mail - v HTML formátu. Několik hodin po objevení viru však byl tento způsob šíření díky zablokování zmíněné stránky znemožněn.

Pozor na broskve: Peachy

Škodlivý kód Peachy využívá možnosti zahrnout do PDF souboru dokumenty jiného typu. Adobe Acrobat

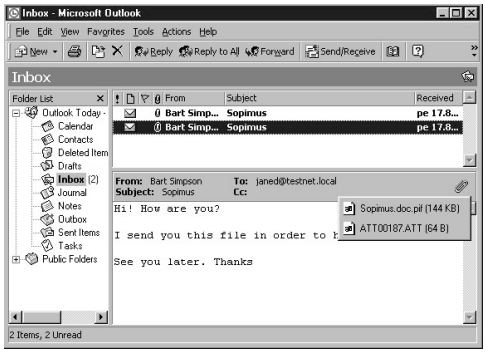


software potom umožňuje tyto dokumenty otevírat a ty mohou obsahovat virus. Peachy ke svému šíření potřebuje „plnou verzi“ programu Adobe Acrobat (pouhé čtení pomocí Adobe Acrobat Readeru jej aktivovat nedokáže).

Peachy se šíří pomocí infikovaného e-mailu s přílohou. Otevřením PDF souboru se zobrazí následující vzkaz:
„You have one minute to find the peach!“.
Dále se zobrazí obrázek obnažených dámských pozadí (viz ilustrace) a ikona s popisem:
„Double click the icon to show the solution.“
Ta je však dostupná pouze uživatelům „plné verze“ Adobe Acrobat. Uživatelé Acrobat Readeru na ni „kliknout“ nemohou. Kliknutím na uvedenou ikonu se aktivuje samotný škodlivý kód.

Hit letošního léta: Sircam

Kromě Windows Address Book může W32/SirCam najít e-mailové adresy také v uložených webových stránkách (Internet cached files). Pokud je virus spuštěn, nakopíruje se do C:\RECYCLED pod jménem SirC32.exe s atributem „skrytý“.



Hlavní nebezpečí tohoto viru spočívá v tom, že „Odpadkový koš“ je často vyjmut ze seznamu skenovaných oblastí.

Virus se také pod názvem SCam32.exe kopíruje do adresáře WINDOWS\SYSTEM a vytváří klíč v registrech, který zajišťuje jeho automatické spuštění. Posledním místem, kam se virus kopíruje, je adresář WINDOWS\TEMP.

Do souboru SCD.DLL uloženém v adresáři WINDOWS\SYSTEM si vytváří seznam souborů s koncovkami: .GIF, .JPG, .JPEG, .MPEG, .MOV, .MPG, .PDF, .PIF, .PNG, .PS, a .ZIP, které jsou uloženy ve složce dokumentů. Do souboru SCD1.DLL uloženého ve stejném adresáři si podobným způsobem ukládá e-mailové adresy získané z Windows Address Book a z „temporary Internet cached pages".

Červ se odesílá pomocí e-mailu (s náhodně generovaným předmětem a textem), ke kterému připojuje jeden ze souborů uvedených v SCD.DLL. Finální soubor používá zdvojenou příponu: .BAT, .COM, .EXE, nebo .LNK (např. DOC.EXE apod.). Z počítače tak mohou mnohdy odejít i citlivé dokumenty.

Podle některých zdrojů může v jednom z dvaceti případů na počítačích s datem v evropském formátu den/měsíc/rok 16. října dojít ke smazání obsahu pevného disku.

Tisíce napadených serverů: CodeRed

Internetový červ CodeRed putuje Internetem, hledá IIS servery s neopravenou .ida chybou a útočí na doménu www.whitehouse.gov.

Zamýšlený útok probíhá tak, že je ve stanovený čas z každého napadeného serveru zasíláno na doménu whitehouse.gov přibližně 400 MB požadavků za hodinu. Díky pečlivé přípravě na odražení tohoto útoku a chybě v návrhu červa se však tento útok nezdařil. Došlo k přemístění whitehouse.gov na jinou IP adresu, a protože červ nedokázal navázat spojení na aktuální IP adresu, neuspěl.

Pokračování „rudého kódu": CodeBlue

Zatímco CodeRed se ve své původní verzi snažil útočit na webové stránky Bílého domu, CodeBlue se snaží z infikovaných počítačů obdobným způsobem útočit na doménu na adrese http://www.nsfocus.com, která patří čínské firmě Nsfocus Information Technology Co.,Ltd. Ta se zabývá datovou a informační bezpečností.

CodeBlue napadá počítače s operačním systémem Windows 2000/NT s instalovaným IIS serverem, k čemuž využívá jejich známé bezpečnostní slabiny. Pokud jsou na napadaném systému aplikovány všechny potřebné záplaty, má červ smůlu.

Poměrně zajímavá je šířící rutina, kterou CodeBlue používá. Červ generuje celkem stovku náhodných IP adres, z nichž se polovina nachází ve stejné síti (první polovina IP adresy je stejná) jako napadený počítač a druhá polovina je generována zcela náhodně.

Hrozba jménem Nimda

Nimda je komplexní Win32 virus. Ve svém repertoáru má celou řadu způsobů šíření: infikovaným e-mailem, po sdílení v lokální síti a prostřednictvím WWW stránek. V poštovních klientech MS Outlook a Outlook Express může při absenci příslušné bezpečnostní záplaty dojít k nepozorovanému spuštění přílohy již při pouhém čtení nebo zobrazení náhledu.

Infikovaný e-mail je ve formátu HTML, má různý text předmětu. Jinak je až na spustitelnou přílohu (většinou je to soubor README.EXE s ikonou HTML souboru) prázdný. V nebezpečí jsou uživatelé systémů Windows 95, Windows 98, Windows Me, Windows NT 4 a Windows 2000.

Nimda je první červ, který dokáže modifikovat webové stránky. Provádí to tak, že k dokumentům typu .ASP, .HTM, a .HTML a také k souborům se jmény INDEX, MAIN a DEFAULT připojuje javascript. Ten obsahuje instrukce k otevření nového okna prohlížeče obsahujícího nakažený e-mail (uživateli je poslán soubor s červem - README.EML). Pokud je tato stránka uživateli zobrazena (ať již lokálně nebo vzdáleně) je počítač, ze kterého tak činí, nakažen.

K vyhledávání zranitelných serverů využívá na rozdíl od svého předchůdce CodeRed "obyčejné" uživatelské stanice, což mu dovoluje snadněji proniknout například také na intranetové webové stránky skryté za firewallem. Na servery proniká pomocí další známé bezpečnostní slabiny, která umožňuje spustit aplikaci na vzdáleném stroji.

Tomáš Přibyl

Taková byla konference Security 2001...

Nikoliv dvoudenní, ale jednodenní.

Nikoliv každé dva roky, ale každý rok.

Taková je stručná charakteristika dvou zásadních změn, které potkaly konferenci Security v letošním roce. Stejně jako v letech předchozích se uskutečnila v reprezentativních prostorách Národního domu v Praze na Vinohradech. Konference byla již tradičně věnovaná problematice počítačových virů a ochraně před nimi, dále problematice elektronického podpisu, šifrování a ochraně dat vůbec. Pořadatelem celé akce byla již tradičně společnost AEC ve spolupráci s mediálním partnerem Vogel Publishing (Chip, Level, Počítač pro každého, IT Net, Media shop…).

Historie akce Security se začala psát již v roce 1992, kdy začala AEC každé dva roky pořádat konference, věnované problematice počítačových virů, antivirové ochraně a souvisejícím otázkám. V letech 1992, 94, 96 a 98 se přitom konference konala pod názvem Virus. Ovšem 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“ jsme se již v roce 2000 rozhodli pro přece jen výstižnější název Security.

Ať tak či onak, smysl a náplň konference zůstal stejný jako v předchozích letech - a nejinak tomu bylo i v roce letošním, kdy se o její zahájení postaral pan JUDr. Luděk Rataj, předseda Asociace pro ochranu informací (AFOI).

Celá konference byla rozdělena do dvou tématických bloků. První blok byl věnován problematice bezpečnosti dat a zejména elektronickému podpisu. V první přednášce se paní JUDr. Iveta Hodková, CSc. ze společnosti PriceWaterhouseCoopers podívala na Zákon o elektronickém podpisu z pohledu právníka a široce z tohoto úhlu pohledu rozebrala vznikající problémy a návaznosti. Bezpečností jednotlivých druhů elektronického podpisu a možnostem jejich zneužití se ve svém příspěvku věnoval Mgr. Pavel Vondruška z Úřadu na ochranu osobních údajů.

Po první krátké přestávce informoval Ing. Jiří Mrnuštík (z pořádající společnosti AEC) posluchače o aktuálním stavu Zákona o elektronickém podpisu viděného zejména z pohledu poskytovatele certifikačních služeb. V další přednášce Olga Přikrylová (taktéž z AEC) opustila úzce vyhraněnou oblast problematiky elektronického podpisu a zaměřila se na analýzu rizik ve společnosti s ohledem na lidský faktor. Přínosem její přednášky je právě ono potřebné uvědomění si role lidského činitele, který je v oblasti bezpečnosti do značné míry limitující a přesto tak často přehlížený. Další presentací patřící spíše do oblasti praxe byl příspěvek Ing. Jaroslava Pinkavy, předního odborníka na kryptografii u nás, který popsal poslední vývoj v kryptografických technologiích a povšiml si hlavně problematiky autority časové značky a odvolávání certifikátů.

Další dva přednášející na konferenci přijeli z akademické půdy. Prvním byl Doc. Ing. Jan Staudek, CSc., proděkan Fakulty informatiky Masarykovy univerzity Brno. Široce rozvedl problematiku času a důvěryhodnosti digitálních dokumentů v něm. Věnoval se tedy problému časové autentizace digitálních dokumentů a mimo jiné popsal také problematiku časového razítka elektronického podpisu a bezpečného protokolu jeho používání. Druhým zástupcem brněnské akademické půdy byl Dr. Ing. Petr Hanáček z Ústavu informatiky a výpočetní techniky Fakulty elektrotechniky a informatiky VUT Brno, který zvážil jednotlivá rizika elektronického obchodu s důrazem na elektronické platební systémy.

Následovala další, přestávka, po níž RNDr. Ivan Svoboda, CSc. ze společnosti T-soft předvedl a zhodnotil možnosti jednotlivých používaných hardwarových autentizačních prostředků a čipových karet. V poslední přednášce prvního bloku vystoupil Ing. Martin Havlíček ze společnosti Hewlett Packard. Povšimnul si aplikace jako kritického místa z hlediska bezpečnosti dat a předvedl některé možnosti jejího zabezpečení.

Druhý blok přednášek byl věnován problematice antivirové ochrany. Na konferenci se sešli opravdu přední odborníci na antivirovou ochranu jak z domova, tak i z blízkého zahraničí. Jednalo se o zástupce ze všech nejdůležitějších antivirových firem (AEC, Alwil, Grisoft, Eset…).

Blok zahájil svojí přednáškou Ing. Miroslav Trnka ze slovenské antivirové firmy Eset. Dopodrobna rozebral

problematiku heuristické analýzy a seznámil přítomné s jejím současným stavem i minulým vývojem. Pavel Baudiš, zástupce antivirových odborníků ze společnosti Alwil, nastínil celkový obraz virové a antivirové problematiky v minulém roce včetně výhledu do blízké budoucnosti. Bezesporu nejmladším přednášejícím na konferenci byl Igor Hák, tvůrce stránek **www.viry.cz**, který hovořil o Windows jako o živné půdě pro počítačové viry. Absolutně nenapodobitelným způsobem přednášel Petr Odehnal z brněnské firmy Grisoft Software o současných trendech aplikovaných v antivirových programech. Svým zajímavým způsobem projevu jistě upoutal většinu přítomných v sále.

Po poslední přestávce, opět spojené s nezbytným občerstvením, vystoupil Tomáš Vobruba, jeden z nejzkušenějších techniků společnosti AEC, a názorně pohovořil o nasazování antivirové ochrany ve firmě a možnostech jejího použití. V poslední přednášce se zajímavým názvem „To nejhorší nakonec“ vystoupil Ing. Milan Loucký (Vogel Publishing) a vytrvalé posluchače seznámil se svým pohledem na to, kde lze získávat spolehlivé informace o počítačových virech a jak se v této oblasti angažují naše média.

Na závěr konference byla zařazena diskuse, ve které mohli přítomní posluchači klást otázky jednotlivým přednášejícím. Po jejím skončení následoval večerní koktejl v přilehlých prostorech Národního domu s kulturním programem, o který se postarali žáci Konzervatoře a ladičské školy Jana Deyla. U dobrého jídla a pití měli posluchači i přednášející možnost prodiskutovat svoje dojmy z konference i jednotlivých přednášek. Společnost AEC jako hlavní pořadatel konference Security 2001 doufá, že většina účastníků byla s jejím programem spokojena a těší se, že se s nimi setká i příští rok na Security 2002 nebo na některé z dalších akcí.

Tomáš Přibyl

Mediální partner Security 2001:

Vydavatelství Vogel Publishing

Vydavatelství Vogel Publishing s. r. o. je v současné době největším vydavatelstvím na trhu s odbornými časopisy, mezi kterými má zhruba 58% podíl. Portfolio společnosti tvoří odborné časopisy pro specialisty - Chip, IT-NET a řada speciálů. Na volný čas je zaměřen časopis Level, který se zabývá problematikou her, a pro začínající uživatele je určen časopis Počítač pro každého. Tištěné tituly doplňuje inzertní příloha MEDIAshop, která je vkládána do všech časopisů našeho vydavatelství. Společnost Vogel Publishing se ale věnuje i vzdělávání uživatelů výpočetní techniky svým projektem CHIP Akademie. Vogel Publishing se aktivně účastní i přednáškové činnosti (konference Security, pětidenní přednáškový maraton s názvem E-Zona apod.).

VOGEL PUBLISHING s. r. o.

CHIP magazín informačních technologií

VOGEL online

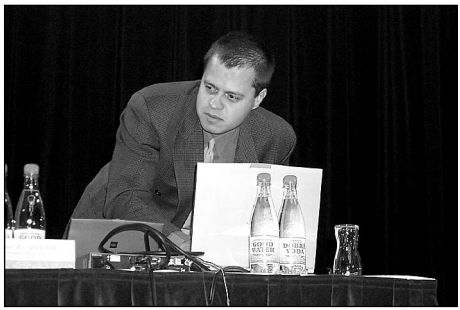
IT-NET

Katalog vydavatelství Vogel Publishing, s. r. o.
MEDIA shop
VOGEL

počítač pro každého

prestižní magazín počítačových her
LEVEL

SECURITY 2001
Praha 7. června

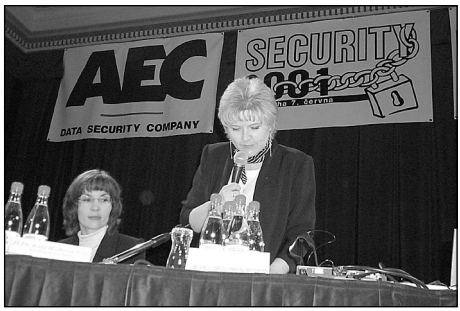


Poslední přípravy a začínáme!

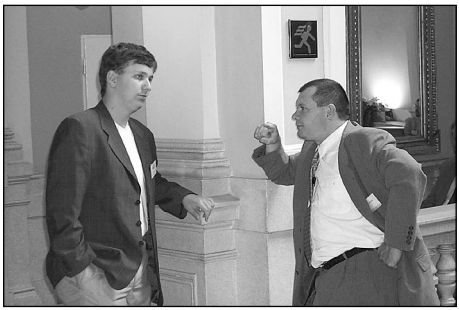
Zvládnout nápor stovek návštěvníků je úkol obtížný, nikoliv však nemožný.

Naplněný sál Národního domu na Vinohradech.

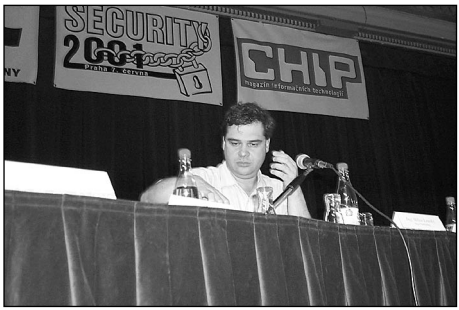
Účastníci odbaveni, začínáme!



Hovoří Ing. Alena Řezníčková z pořádající společnosti AEC.

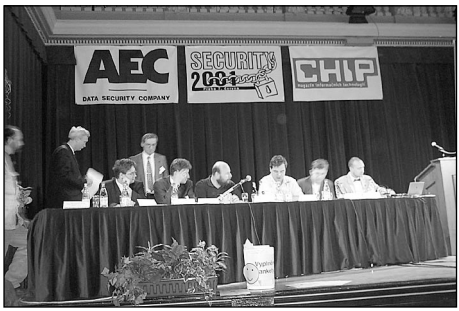


Igor Hák (**www.viry.cz**) a Jan Džubák (**www.hoax.cz**).



Milan Loucký, zástupce mediálního partnera konference - vydavatelství Vogel Publishing.

Tomáš Vobruba a jeho aktivní antivirová ochrana.



Po celodenním maratonu zůstal přednášejícím a posluchačům elán i na diskusi.

Společenskému rautu předcházelo předání bezpečnostního software konzervatoři Jana Deyla.

Takhle nějak to bylo…

Třetí partnerská konference Kaspersky Lab, Kypr

Konference partnerů společnosti Kaspersky Lab se stala již tradicí, ovšem po Moskvě a Petrohradu jsme tentokrát byli mile překvapeni místem konání konference - město Limassol se nachází na jihovýchodním pobřeží ostrova Kypr. Oč zajímavějšími městy jsou Moskva i Petrohrad (a jistě stojí zato je spatřit, což se mi bohužel zatím nepoštěstilo), o to exotičtější se jevil Kypr už ve chvíli příprav. Považuji za rozumné zjistit si alespoň základní data o zemi, kam se chystám jet, takže jsem zjistila své zeměpisné i geopolitické mezery ve vzdělání. Víte například, že tento ostrov je již od roku 1974 rozdělen na dvě části, z nichž ta severní je obsazena Tureckou armádou?

Vlastně jsem se dost těšila, a tak jsem pročetla vše, co se mi během těch pár dnů příprav podařilo sehnat. Těšila jsem se, že bude čas na nějaký výlet do vnitrozemí ostrova a za památkami, pozůstalými po bohaté a pohnuté minulosti ostrova.
Jistě ale znáte ty služební cesty, kdy Vám známí závidí, kam všude se podíváte po světě a po návratu očekávají dlouhé vyprávění. No a Vy rozhodně můžete podat vyčerpávající popis letiště, hotelového pokoje (a často i blízkého okolí hotelu) a samozřejmě také silnice vedoucí od letiště k hotelu.

Jedinou nadějí pro dychtivého návštěvníka pak jsou podmínky leteckých společností, protože ceny letenek jsou podstatně mírnější při cestě, která zahrnuje víkendovou noc. Takže po skončení jednacích dnů došlo i na výlet, i když jsme samozřejmě viděli jen malou část tohoto krásného ostrova, v červnu již značně vyprahlého, a přesto rozkvetlého oleandry všech barev všude kolem dálnice i městských silnic. Ostrova, u jehož břehů se z mořské pěny zrodila Afrodíté a který se kvůli své

strategické poloze postupně stal cílem starých Řeků i Římanů, byzantských vládců i Benátčanů, a dlouhou dobu byl britskou kolonií.

Všechny historické éry zanechaly na Kypru své stopy a například na britský vliv narazíte okamžitě po vystoupení z letadla, kdy se musíte vyzpovídat imigračnímu úředníkovi a hned vzápětí jste nuceni nasednout do auta, které má volant na úplně špatné straně a musíte jet po neméně špatné straně silnice.

Podstatnou část našeho pobytu jsme samozřejmě strávili v klimatizovaných konferenčních prostorách hotelu v technické a obchodní sekci konference. Bylo nutné seznámit se s novými strategickými plány společnosti Kaspersky Lab, která dnes čítá zhruba 70 zaměstnanců a podporuje 170 svých distributorů (z toho 108 mimo území Ruska). Jen na tuto konferenci přijeli partneři z Austrálie, Brazílie, Číny, ČR, Dánska, Francie, Německa, Řecka, Maďarska, Itálie, Malajsie, Polska, Rumunska, Singapuru, Španělska, Švédska, Holandska, Turecka a USA.

Součástí programu bylo také představení nových lidí ve společnosti včetně jejich rozčlenění do zcela nově založených divizí. Pro nás jako partnery je samozřejmě velmi důležité znát osobně ty, s nimiž poté komunikujeme telefonicky a e-mailem. To se pak samozřejmě odráží také v rychlosti řešení problémů klientů, a to obchodního i technického charakteru, zkrácení délky odezvy.

Obchodníci byli seznámeni s novou politikou prodeje, s novými produktovými balíky a plánovanými aktivitami v oblasti prodeje programů přes Internet. Poněkud vzrušená debata se rozproudila kolem nově navržené grafiky a nových názvů programů. Z hlediska prodejců je samozřejmě velkou komplikací jakákoliv změna ve chvíli, kdy je trh už zvyklý na známé jméno programu. Také změna grafického ztvárnění může v první fázi přinést spíše negativní výsledky. Ovšem organizační změny ve společnostech a nová marketingová oddělení vždy přinášejí i změny takového charakteru, protože chtějí svou práci dělat nově a po svém a jsou o své pravdě přesvědčeni. Navíc neexistují dostatečně měřitelná srovnání podobných marketingových rozhodnutí, protože nikdy není možné porovnat výsledek s tou druhou variantou, která se neuskutečnila. Ať je však vnější působení produktů jakékoliv, nejdůležitější je funkčnost a výsledky software, a ty jsou stále na vysoké úrovni a dosahují ve světě vysokých ocenění.

Techniky samozřejmě zajímaly především plány vývoje, jejichž cílem je vytvoření komplexního bezpečnostního řešení, které kromě antivirové ochrany nabídne svým uživatelům například také personální firewall.

Neméně zajímavé novinky jsme se dozvěděli v souvislosti s nově zaváděným partnerským programem. Pro zákazníky by měl být prospěšný program certifikací partnerů, což by mělo přinést ještě vyšší úroveň technické podpory ze strany lokálních dodavatelů řešení. Zákazník tak navíc získá možnost vybrat si dodavatele podle rozsahu poskytovaných služeb.

Snad nejzajímavější však byly informace získané z různých průzkumů, na jejichž základě je možné do jisté míry plánovat zaměření vývoje a očekávání, které typy produktů se dostanou do popředí poptávky v následujícím období. Antivirové programy jsou v době stále rozsáhlejších virových epidemií naprostou nezbytností a rychlost reakce na nové viry je odrazem kvalitního týmu dodavatele. Stále se navíc zvyšuje počet uživatelů PC po celém světě, což vyžaduje vysoký komfort a snadné používání jakékoliv aplikace. Dalším parametrem pro vývoj řešení je obrovská popularita a rozvoj mobilních zařízení, která obsahují nebo přenášejí citlivé informace a vyžadují kvalitní ochranu. Zde přichází vedle antivirového zabezpečení nutnost zajištění ochrany dat šifrováním.

Všechny nashromážděné informace jsme samozřejmě dlouze diskutovali i při společných neformálních setkáních, protože pořadatelé konference se postarali také o bohatou kulturní náplň. Takže jsme mohli ocenit například hudební nadání Natalji Kasperské, ředitelky společnosti Kaspersky Lab.

Celková atmosféra byla velmi příjemná a všichni účastníci vypadali spokojeně. Jediná otázka však zůstala nezodpovězena: kde příště?

Alena Řezníčková

Když se řekne „Aktualizace“...

Antivirový motor, anglicky „Engine“ je jádrem každého antivirového produktu. Bez motoru, nebo jak se také někdy říká (jazykozpytci prominou), bez enginu, není možné detekovat žádný počítačový virus. Proč je tak důležitý?

Každý antivirový program má nějakou historii, byl nějakým způsobem vytvořen a neustále se vyvíjí, vylepšuje, obohacuje o nové prvky a možnosti. Nová verze programu obvykle obsahuje nová vylepšení, novou funkčnost a nový rozsah možností. Je to program, jako každý jiný a protože prochází vývojem, přicházejí stále nové a nové verze, které se liší většinou číselným označením. Antivirový program je, jak jeho název napovídá, primárně určen k odhalování neboli detekci počítačových virů. Samotná detekce však samozřejmě nestačí, antivirový program musí (nebo měl by, budeme-li shovívavější) umět virus zneškodnit, odstranit, zničit … Také by měl pamatovat na všechny možnosti, jak se počítačový virus může do systému dostat a měl by tedy být aplikovatelný na všech těchto definovaných vstupních místech pravděpodobné infekce. A co by měl umět víc? No přece hlídat pokud možno všechno, vždy a všude tak, aby s ním měl uživatel - (správce počítačové sítě) co nejméně práce a starostí. Mluvíme o centrální správě, která umožňuje jak instalaci antivirového programu na dálku, tak jeho konfiguraci (taky na dálku) a zejména pak aktualizaci (jak jinak než na dálku).

Aktualizace je pojem, který má u antivirových programů poněkud jiný, i když velmi podobný význam. Pod pojmem „aktuální antivirový program“ je možné si představit nejnovější verzi programu. Něco tomu ale chybí. A to něco je právě ona podstatná, a nebála bych se použít výrazu životně důležitá, část programu, která jej činí funkčním a účinným v boji proti virům (počítačovým, pochopitelně). Aktualizace se u tohoto speciálního software dělí na dvě části. Jednou z nich je takzvaný update, druhou pak upgrade.

Update znamená aktualizaci datových řetězců. Co to jsou datové řetězce? Antivirový program používá při své práci seznam dosud známých virů, který obsahuje typické části virového kódu a podle nich rozpoznává pojmenované počítačové viry nejrůznějších typů, od boot-sektorových virů, souborových virů, makrovirů až po velmi čilé a stále častější internetové červy a škodlivé Java aplety nebo tzv. Aktive-X objekty. Tento seznam umožňuje antivirovým motorům - skenovacím mechanismům identifikovat počítačový virus a jeho název. Podle odhadů tvůrců antivirových programů týdně spatří světlo světa na desítky i stovky virů, z nichž některé mohou být úplně nové, jiné vznikají mutací a různými modifikacemi již existujících virů. Takové množství varuje už svými počty před rizikem u nás poměrně častým - ponechání počítače i celé sítě bez ochrany (v tomto případě antivirové). Všechny nové, upravené či nově zmutované viry jsou pod známými jmény uvedeny v seznamu definic - v datových řetězcích. A jak tyto řetězce (signatury či definice, chcete-li) dostat do našeho chráněného počítače? Aktualizací, resp. pomocí update. To ale zdaleka není všechno.

Co ony důležité motory (engine), duše antivirového programu? Některé antivirové programy používají jeden typ motoru, jiné dokážou kombinovat výhody a přednosti několika motorů. Mezi nejznámějšími příklady bych uvedla antivirové programy firmy Network Associates Inc. s motorem, jenž používá jazyk Virtran, unikátní svou schopností detekovat viry, a který vytvořil známý antivirový specialista Dr. Alan Solomon. Dalším příkladem budiž antivirový program společnosti F-Secure Corp. s motory F-PROT (z původního názvu antivirového programu), AVP (z antivirového programu firmy Kaspersky) a Orion. Pro motory je vyhrazen druhý z pojmů, jež jsou součástí aktualizace, upgrade. Často se pojem upgrade zaměňuje s běžně používaným významem přechodu z nižší verze software na vyšší. U antivirového programu je to něco obdobného, máme však na mysli upgrade skenovacího motoru - onoho enginu, zmíněného na začátku tohoto článku, bez jehož existence by antivirus nedokázal škodlivý virus v systému odhalit. Motory obsahují způsob detekce viru a jeho odstranění. Je to souhrn metod skenování, které testují soubory v systému nebo v elektronické poště, a odhalují programové kódy, jež s legální činností programů nemají nic společného. S vývojem nových technologií, nových aplikačních platforem souvisí vývoj nových typů virů, a ten se zase odráží ve vývoji skenovacích technologií, pokrývajících nová nebezpečí. Četnost nově vznikajících technologií není taková, jako u datových řetězců, nicméně přibližná lhůta pro upgrade bývá asi tak jednou za čtvrt roku, případně častěji, pokud se v počítačovém světě objeví virus, jenž si upgrade vyžádá.

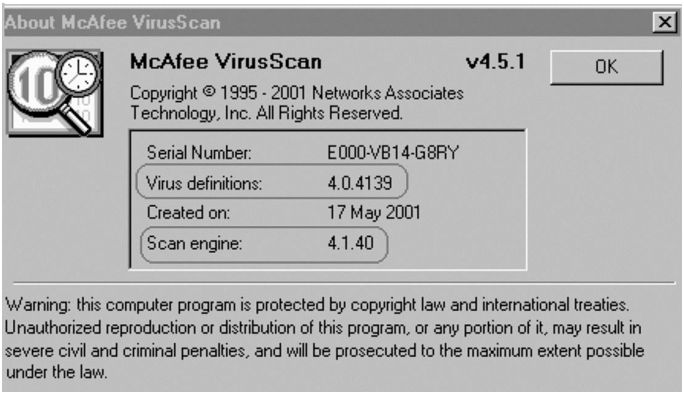
Ideálním stavem je po výšeu vedených informacích stav, kdy vlastníte nejnovější verzi antivirového programu s poslední aktualizací - a to jak update, tak upgrade. Pro přenos aktualizací na daný počítačový systém ze zdroje na Internetu je snad nejčastěji využíván protokol FTP, ať už prostřednictvím anonymního přihlašovaného uživatele (pokud to FTP server umožňuje), nebo na základě přihlašovacích údajů. Špičkoví výrobci antivirových produktů nabízejí ve svých programech funkce pro aktualizaci jednak manuálně - ručním způsobem (prostřednictvím http, nebo ftp spojení, downloadu aktualizačních souborů podle potřeby uživatele - správce sítě a vlastního procesu aktualizace datových řetězců antivirového programu), nebo automaticky, a to včetně spojení se zdrojem a stažení aktualizačních souborů z internetových stránek na distribuční počítač, ze kterého je možno dále aktualizace distribuovat na všechny ostatní stanice v síti, jež se k distribučnímu počítači obracejí se svými požadavky na aktualizace. Může se tak dít např. na základě naplánované úlohy, která podle potřeby uskuteční spojení se zdrojem aktualizací na internetu v plánovaném čase, a pokud existuje novější verze aktualizačních souborů, stáhne ji program na určené úložiště, automaticky zaktualizuje produkt a poskytuje nebo rozešle tuto aktualizaci i v rámci spravované sítě dalším počítačům v době k tomu určené, nebo např. po přihlášení stanice k síti. Je nanejvýš pochopitelné, že s množstvím nových virů roste i velikost virových definicí, jež je nutné dostat na cílový počítač. Mnohé antivirové produkty rozeznávají kromě aktualizačních souborů obsahujících všechny definice ještě tzv. inkrementální aktualizace, které se liší zejména podstatným rozdílem ve velikosti, a dále obsahem, který pouze doplňuje stávající řetězce z poslední aktualizace o nové. Takový způsob aktualizace je mnohem rychlejší a šetří čas i peněženku uživatelů antivirových produktů.

Nejnovějším trendem jsou nástroje antivirových firem, které tuto aktualizační činnost dovádějí téměř k dokonalosti. Aktualizace se pak uskutečňuje ne na popud žadatele, ale opačným směrem - rozesíláním souborů ze zdroje k cíli (žadateli), kdy inicializace vychází od příslušného výrobce antivirového programu, není tudíž třeba myslet na aktualizační úlohy a třeba opakovaně (byť i automaticky) testovat, zda se ve zdroji nachází nový update či upgrade. Zdroj sám distribuuje aktualizační soubory k cíli v okamžiku, kdy jsou nové aktualizace uvolněny. A probíhá-li takováto distribuce zabezpečenou formou, např. využitím certifikátů, které poskytují možnost ověřit si podpis u stahovaných dat a znemožní nežádoucí download podstrčených souborů z jiného pochybného zdroje, pak se může každý počítačový systém cítit před počítačovými viry již opravdu bezpečně.

Při vší automatizaci a četnosti aktualizací je však stále třeba mít na zřeteli, že tvůrci virů budou vždy o krůček dál, než jejich pronásledovatelé.

Jedná se o nekonečný proces v honbě na nepřítele, který nikdy nespí.

Olga Přikrylová

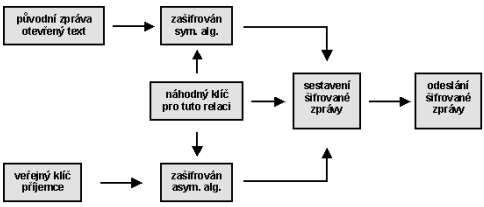


Představení programu PGP

PGP se za deset let své existence bezesporu stal v oblasti bezpečnosti dat a komunikace významným pojmem. Zkratka PGP pochází z anglického Pretty Good Privacy, což v češtině znamená „docela dobré soukromí“. V podstatě je to kryptografický balík programů, který obsahuje funkce především pro šifrování zpráv a souborů, ale také pro vytváření a ověřování digitálních podpisů. Jeho autorem je Američan Philip R. Zimmermann, který první verzi tohoto programu zveřejnil v červnu roku 1991. Od svých počátků bylo (a stále je) PGP šířeno jako tzv. „free software“. Postupem času se stal formát OpenPGP široce používaným řadou volných (freewarových) i komerčních programů (seznam můžete najít na **www.pgpi.org**).

Dnes patří program PGP bezesporu mezi jedny z nejrozšířenějších prostředků pro šifrování elektronické pošty a pro ověřování pravosti digitálních podpisů. PGP pracuje s šifrovacími algoritmy CAST, AES, TripleDES, IDEA, Twofish a lze tedy říci, že patří mezi kryptograficky silné prostředky. Nemalou výhodou je i jeho dostupnost pro většinu platforem.

PGP se (stejně jako většina obdobných programů) navenek „tváří“ jako systém používající asymetrické šifrování s veřejným a soukromým klíčem. Každý uživatel PGP si generuje jeden nebo více párů soukromého (tajného) a veřejného klíče. Veřejné klíče jsou pak zveřejňovány a předávány ostatním uživatelům, se kterými daná osoba komunikuje. Ve skutečnosti je však při každém šifrování pomocí PGP generován vždy nový náhodný symetrický klíč, kterým jsou e-mailová zpráva (soubor) zašifrována symetrickou šifrou. Tento symetrický klíč je poté zašifrován pomocí asymetrické šifry (veřejným klíčem příjemce) a připojen k zašifrovaným datům. Příjemce zašifrované zprávy dešifruje pomocí svého soukromého asymetrického klíče náhodný symetrický klíč, jímž následně dešifruje zprávu. Tato metoda je použita z důvodu značného rozdílu mezi šifrováním pomocí asymetrických a symetrických algoritmů. Pokud by byla všechna data šifrována pouze pomocí asymetrického algoritmu, zabralo by to v porovnání se symetrickým algoritmem nepoměrně delší dobu.



Kromě šifrování umožňuje PGP také pracovat s digitálními podpisy (signaturami). Ty příjemci umožňují se ujistit o integritě a autenticitě přijatých dokumentů (souborů).

Správa šifrovacích klíčů vypadá u programů z rodiny PGP následovně. Veřejné a soukromé klíče bývají obvykle uchovávány v tzv. svazcích klíčů. Veřejné klíče jsou uloženy v souboru, který je průběžně doplňován. Svazek soukromých klíčů je uchováván v souboru, který je obvykle neměnný a je udržován v zašifrovaném tvaru. Přístup do tohoto souboru je jištěn pomocí hesla (passphrase), kterou je zašifrován. Tato fráze nemá nic společného s klíčem, může být libovolně dlouhá a má být volena tak, aby si ji uživatel snadno zapamatoval a nebylo možné ji uhádnout (třeba i několik vět i s pravopisnými chybami - záleží na stupni vaší paranoie).

Systém PGP nabízí uživateli následující možnosti, jak publikovat svůj veřejný klíč.

- Zveřejnit klíč na veřejném serveru k tomuto účelu určenému.
- Poslat veřejný klíč e-mailem.
- Uložit ho do souboru, a ten distribuovat dle uvážení přímo konkrétním osobám.

V polovině devadesátých let se PGP chopila firma PGP Security (divize společnosti Network Associates) a uvedla jej jako komerční produkt. V této firmě donedávna působil i „otec“ programu PGP Philip R. Zimmermann.

V současné době existuje PGP (od NAI) ve verzi 7.0.4. Právě tuto verzi si ve zkratce představíme.

Instalace tohoto programu je standardní a běžný uživatel počítače by s ní neměl mít žádné vážnější problémy. Po instalaci je vyžadováno restartování systému.

PGP

PGP Desktop Security disponuje následujícími schopnostmi:

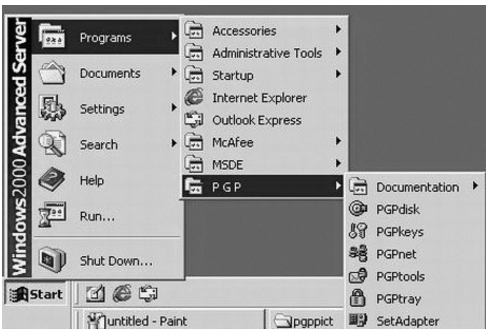
- šifrování (e-mailu, souboru na disku)
- ICQ komunikace
- elektronický podpis (e-mailu, souboru)
- bezpečné mazání souboru
- vytváření „samodešifrovacích“ souborů
- správa soukromých a veřejných klíčů
- klient VPN (Virtual Privat Network)
- personální firewall a IDS (Intrusion Detection Systém = detekce nepovolených průniků do systému)

Jednotlivé moduly PGP Desktop Security:

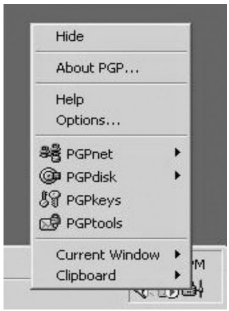
- PGPmail and PGPfile Encryption
- PGPdisk Encryption
- PGPfire (Personal Firewall Protection and Intrusion Detection System)
- PGPnet VPN Client
- PGP Desktop Manageability Tools (PGPadmin, PGP Certificate server)

K jednotlivým funkcím programu PGP se uživatel dostanete třemi způsoby:

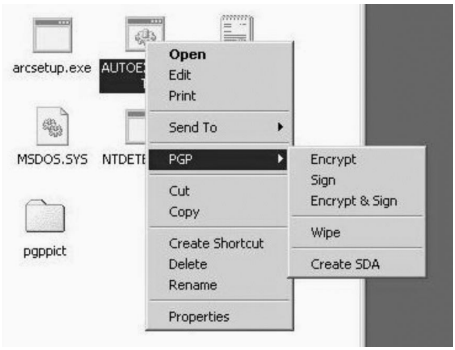
1) prostřednictvím nabídky „Start“



2) pomocí ikony v systémové liště („System Tray“)



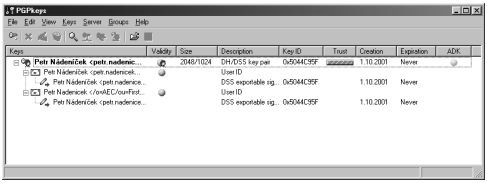
3) pomocí kontextového menu (při kliknutí pravým tlačítkem myši na soubor)



Základní funkce, jako vytváření/ověřování podpisu, bezpečné mazání (wipe) nebo správu klíčů, lze také používat prostřednictvím „PGP Tools“, které lze vyvolat pomocí ikony v „System Tray“.

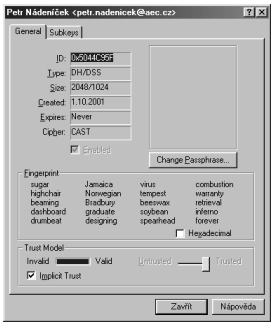
Nejdůležitější součástí PGP je bezesporu správa klíčů a jejich certifikátů - "PGP Keys". V PGP 7.03 lze používat certifikáty jak ve formátu PGP, tak i ve formátu X.509.

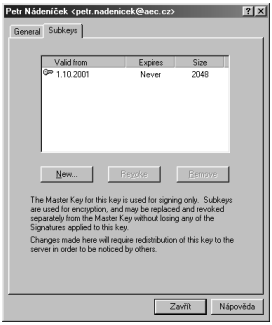
Vytváření nových klíčových párů je možno pomocí speciálního průvodce (wizardu), který uživatele bezpečně provede všemi úskalími. Po uživateli jsou



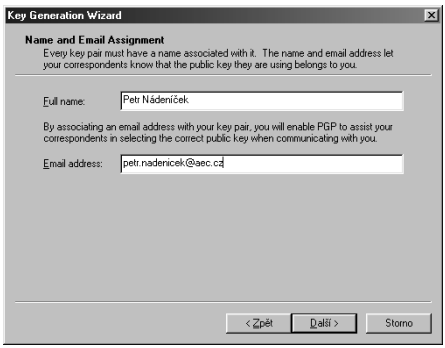
postupně vyžadovány následující údaje: jméno, e-mailová adresa a vstupní fráze. Klíče (certifikáty) jsou spravovány pomocí „PGP Keys“.

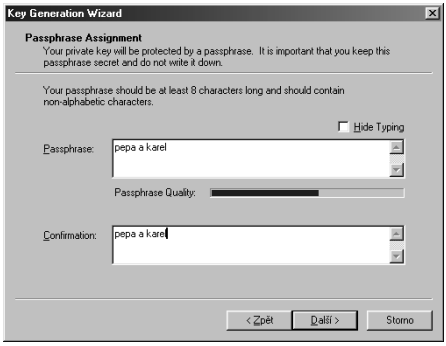
Pokud jste novým uživatelem PGP (tzn. bez vytvořených klíčů), bude po instalaci spuš-těn pomocník pro jejich generování. V opačném případě, či je-li třeba provést nějaké úpravy, je pomocník dostupný z programu PGP keys (Generate New Keypair). Při generování nového klíčového páru budete dotázáni na jméno a e-mailovou adresu. Bude také třeba zadat





frází (Passphrase), která slouží k ochraně soukromého klíče. Tuto frázi si musíte zapamatovat





a v žádném případě ji nesmíte prozradit. Pokud dojde k odcizení souboru se soukromým klíčem, je útočníkovi bez této tajné fráze k ničemu.

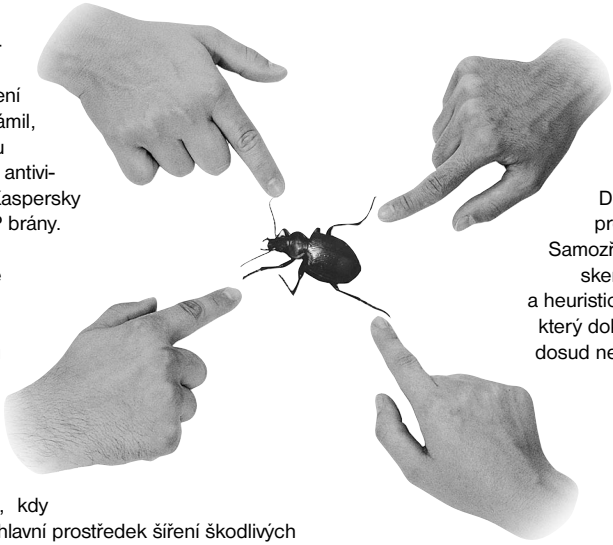
Při zadávání fráze je indikována kvalita hesla (Passphrase Quality), která odráží její složitost. Zkušení uživatelé mohou nastavit typ klíče, jeho délku a dobu platnosti a použitý algoritmus.

Program PGP také umožňuje vytvořit speciální šifrovaný disk. Ve skutečnosti se jedná o šifrovaný soubor, do kterého se data ukládají, ale uživateli se jeví jako plnohodnotný systémový disk.

Systém PGP z produkce firmy PGP Security (Network Associates) má ve skutečnosti mnoho dalších možností, které nelze na několika stranách představit. Vůbec jsme zde například nezmínili službu VPN nebo Personal Firewall a IDS. Pokud hledáte více informací, určitě je najdete např. na **www.pgp.com** nebo v češtině na **www.pgp.cz**.

Petr Nádeníček

Kaspersky uvádí: Antivirová ochrana pro SMTP!



Kaspersky Lab, mezinárodní producent software z oblasti zabezpečení a ochrany dat, oznámil, že zveřejňuje novou testovací beta verzi antivirového programu Kaspersky AntiVirus pro SMTP brány. Tento nový produkt uživatelům dovoluje implementovat centralizovanou antivirovou ochranu e-mailové komunikace nezávislou na typu použitého serveru.

V současné době, kdy e-mail představuje hlavní prostředek šíření škodlivých kódů (asi osmdesát procent z celkového počtu virových incidentů), je nasazení účinného a spolehlivého skenování příchozí a odchozí pošty více než potřebné. Vzhledem k možným následkům zavlečení virové infekce do lokální sítě se to jistě vyplatí i po finanční stránce.

Každý, kdo se kdy třeba jen okrajově zajímal o problematiku sítí a komunikace v nich, ví, že většina lokálních firemních sítí představuje naprosté unikáty - co do použitého hardwaru i softwaru. V některých případech si síť dokonce žije jakýmsi „vlastním životem“ nezávisle na vůli administrátora. Aby to všechno bylo ještě složitější, existuje také například množství typů e-mailových serverů, pro které musí existovat také příslušná antivirová ochrana. Jedním z možných řešení je zařadit filtr, který bude elektronickou poštu prověřovat přímo na úrovni SMTP protokolu nezávisle na typu konkrétního e-mailového serveru.

Kaspersky AntiVirus pro SMTP brány je software, který dokáže odhalit přítomnost virů ve veškerém příchozím i odchozím SMTP provozu. Tento systém je zařazen mezi vnější prostředí a vlastní e-mailový server, kde umí nejen odhalovat škodlivé kódy a čistit přenášené soubory, ale dokáže také zabránit případným DoS útokům vedeným prostřednictvím SMTP. Samozřejmostí je spolehlivé skenování příloh e-mailů a heuristický skenovací motor, který dokáže odhalit i většinu dosud neznámých škodlivých kódů. Management konzole založená na web technologii umožňuje vzdáleně spravovat jednotlivé moduly, automaticky updatovat a generovat statistické reporty.

V závislosti na přednastavené konfiguraci software umožňuje nakažený e-mail zablokovat, smazat nebo ignorovat. V každém případě však o incidentu informuje nejen administrátora, ale také příjemce a odesílatele.

Současnou verzi Kaspersky AntiVirus lze použít pro SMTP brány provozované pod operačním systémem Linux. Následující verze budou podporovat také například FreeBSD, OpenBSD a Solaris (Intel/Sparc). Kaspersky Lab také do budoucna plánuje rozšířit kontrolu na úrovni SMTP protokolu o další služby, jako jsou například systémy pro zálohování, ochrana před nevyžádanou poštou nebo šifrování.

Plná verze popisovaného produktu by měla být podle informací Kaspersky Lab dostupná do konce tohoto roku.

Jaromir Klimek

Norman Shredder

bezpečná skartace elektronických dat

Nepotřebné papírové dokumenty skartujeme, elektronické mažeme. **Ale pozor!** Smazané elektronické dokumenty lze velmi snadno obnovit! Bezpečné a nevratné skartování elektronických dat řeší program **Norman Shredder**.

Shredder - navěky smazáno

AEC
DATA SECURITY COMPANY

AEC, spol. s r.o. - Brno: Bayerova 799/30 602 00 Brno, tel.: 05/4123 5466 - 7 fax: 05/4123 5038, e-mail: info@aec.cz

AEC, spol. s r.o. - Praha: Vinohradská 184 130 52 Praha 3, tel.: 02/6731 1402, fax: 02/6731 4326, e-mail: praha@aec.cz

AEC
DATA SECURITY COMPANY

Bulletin

www.aec.cz, www.trustcert.cz

prosinec/2001

AEC DATA SECURITY COMPANY

Vám přeje hodně úspěchů v novém roce

pour felicitae

ifpo ucerleait

200

Úvod

Milí přátelé!

Nedávno jsem četl knihu od Andrew Chaikina „A man on the Moon“ (Člověk na Měsíci), kde byla následující věta:

On the night of July 20, 1969, our world changed forever when two Americans, Neil Armstrong and Buzz Aldrin, walked on the Moon.

V noci z 20. července 1969 se náš svět navždy změnil poté, co se dva Američané, Neil Armstrong a Buzz Aldrin, prošli po Měsíci.

Na tuto větu jsem si vzpomněl letos 11. září. A myslím, že nikomu nemusím říkat, proč. Náš svět se navždy změnil. A „odraz“ tohoto „nového“ světa nás teď provází a bude provázet doslova na každém kroku.

Náš svět už nikdy nebude stejný, ale to také neznamená, že zákonitě musí být horší.

Přejeme všem lidem (nejen „dobré vůle“, jak se někdy s oblibou říká) co nejvíce úspěchů a radosti v nadcházejícím roce 2002.

Tomáš Přibyl, tomas.pribyl@aec.cz

Data do diáře: konference a akce AEC v roce 2002

Přelom roku je dobou vánočních svátků, bujarých oslav Silvestra - a také časem odkládání starých diářů a zakládání nových. Zatímco mnoho akcí je „divokých“ a termín jejich konání se často mění (o mnoha událostech se beztak člověk dozvídá až v průběhu roku), jsou zde i různé „trvalky“ - události, o kterých bezpečně víme dlouhé měsíce (a někdy i roky) dopředu. Seznam několika takovýchto akcí „z dílny“ AEC v roce 2002 přinášíme na následujících řádcích.

Semináře Bezpečnost dat

Už pátým rokem přichází společnost AEC s řadou seminářů Bezpečnost dat, které mají za cíl v pravidelných tříměsíčních intervalech seznamovat laickou i odbornou veřejnost s problematikou počítačové bezpečnosti a posledním vývojem na tomto poli. K tradičním místům konání v Praze a Brně se od roku 2002 přidává také Ostrava a slovenská Bratislava.

Každý seminář z cyklu Bezpečnost dat se skládá zpravidla ze šesti přednášek týkajících se problematiky antivirové ochrany, elektronického podpisu, modelových příkladů, tipů a triků, právních otázek, šifrování, ochrany dat a dalších otázek souvisejících s bezpečností dat a informací.

Začátek seminářů je vždy v 9:30 hod.

Mediálními partnery jsou redakce počítačových měsíčníků PC World a IT System.

Cena za celý cyklus čtyř seminářů je 8200 Kč (vč. DPH) v České republice a 8400 Sk (vč. DPH) ve Slovenské republice.

Praha Místo konání: Budova Stimbuilding, Vinohradská 184 (stanice metra Želivského).
První seminář - pátek 25. ledna.
Druhý seminář - pátek 17. května.
Třetí seminář - pátek 13. září.
Čtvrtý seminář - pátek 15. listopadu.

Brno Místo konání: Síň vědecké rady v prostorách Vojenské akademie Brno (Kounicova 65).
První seminář - pátek 1. února.
Druhý seminář - pátek 24. května.
Třetí seminář - pátek 20. září.
Čtvrtý seminář - pátek 22. listopadu.

Ostrava Místo konání: Hotel Imperial (Tyršova 6).
První seminář - čtvrtek 24. ledna.
Druhý seminář - čtvrtek 16. května.
Třetí seminář - čtvrtek 12. září.
Čtvrtý seminář - čtvrtek 14. listopadu.

Bratislava Místo konání: Hotel Danube Bratislava (Rybné námestie 1), sál Diamant.
První seminář - čtvrtek 21. února.
Druhý seminář - čtvrtek 23. května.
Třetí seminář - čtvrtek 19. září.
Čtvrtý seminář - čtvrtek 21. listopadu.

Partnerský den AEC

Čtrnáctého února 2002 se uskuteční tradiční každoroční setkání představitelů AEC s partnery, distributory a dealery za účelem rekapitulace roku loňského a společné koordinace sil do sezóny nadcházející. Na programu dne jsou jednak odborné přednášky, dále seznámení s plány do budoucna a především vyhodnocení dealerské soutěže za rok 2001.

Partnerský den se koná v Národním domě na Vinohradech, začátek akce je v 9:00 hodin. Možnost přihlášení bude včas uvedena na webovských stránkách **www.aec.cz**

Konference Security 2002 (Praha)

Konference Security si v roce 2002 připomene deset let od okamžiku, kdy se konala poprvé - ještě pod názvem Virus 1992 v Olomouci. Od té doby prošla několika zásadními změnami - přesně tak, jak se měnil vývoj na poli informačních technologií a v otázce jejich bezpečnosti i zabezpečení. A tak se konference v současné době pyšní názvem Security (viry jsou jednou, ale nikoliv jedinou hrozbou života v kybernetickém prostoru). Namísto původního dvouletého intervalu mezi jednotlivými akcemi si překotné změny v IT vyžádaly pořádání konference každý rok - ovšem s tím, že nejde o dvoudenní, ale jen jednodenní akci.

V roce 2002 se tak konference Security uskuteční ve čtvrtek 6. června v Národním domě na Vinohradech.

Cena konference je pro jednu osobu 2200 Kč. Pro registrované uživatele produktů AEC a předplatitele kteréhokoliv časopisu z nabídky vydavatelství Vogel Publishing, spol. s r.o. činí 1700 Kč (bez DPH). Cena obsahuje vstupné, informační materiály a občerstvení.

Mediálním partnerem konference je vydavatelství Vogel Publishing (Chip, Počítač pro každého, IT Net, Media Shop, Level).

Konference Bezpečnosť dát (Bratislava)

Byť s poněkud kratší tradicí, také ve Slovenské republice je pořádána pod záštitou AEC celostátní konference věnovaná problematice ochrany dat a jejich zabezpečení. Podobně jako v minulých letech se bude konat 17. dubna 2002 v Bratislavě pod názvem Bezpečnosť dát. Přednášet na aktuální témata z oblasti bezpečnosti IT budou (jak se stalo dobrým zvykem) přední specialisté z České i Slovenské republiky.

Workshop pro dealery

Další z akcí, které AEC pravidelně pořádá pro své dealery a distributory. Cílem workshopu ovšem není prezentovat výhradně firmu AEC, ale především zvyšovat znalostní a vědomostní základnu našich partnerů tak, aby byli schopni svým zákazníkům poskytovat v odpovídající kvalitě a rozsahu všechny služby. Samozřejmě, že jsou otázky, které musí řešit přímo specialisté na dané produkty či oblasti - na druhé straně se ovšem drtivá většina dotazů a problémů opakuje. Workshopem se tak zvyšuje úroveň znalostí našich dealerů i komfort pro jejich zákazníky. Akce se bude konat v průběhu měsíce září 2002, bližší podrobnosti budou včas zveřejněny na **www.aec.cz**

Roadshow Slovensko 2002

Také další z připravovaných akcí navazuje na úspěchy z let minulých. Ve dnech 28. až 30. května 2002 se uskuteční Roadshow po slovenských městech, kdy specialisté z AEC vyrazí „do terénu". Postupně navštíví tři významná města ve Slovenské republice, kde se budou věnovat přednáškám z oblasti bezpečnosti IT a představování nových produktů.

Akce se bude konat od 28. do 30. května 2002 - její přesný program bude upřesněn dodatečně na **www.aec.sk**

AEC roadshow 2002

Uspořádat přednášky o počítačové bezpečnosti také mimo oblasti tradičních konferencí a seminářů je cílem této akce, se kterou společnost AEC začala před několika lety ve Slovenské republice - a v roce 2001 ji s velkým posluchačským ohlasem uskutečnila také v devíti českých a moravských městech.

AEC roadshow 2002 se bude konat na podzim 2002.

Pro bližší informace si můžete napsat na seminar@aec.cz nebo sledujte web **www.aec.cz** (resp. **www.aec.sk**).

Pro získávání aktuálních informací je možné se také zdarma přihlásit k odběru elektronického bulletinu AEC na **www.aec.cz**

PS Ač velice neradi, vyhrazujeme se právo změny - termínu, místa konání akce apod. (Kdo nikdy nic podobného nedělal, nedovede si představit, jak neřešitelným problémem může být rezervace přednáškového sálu rok dopředu…)

Počítačové viry v roce 2002

V roce 2000 jsme do říjnového čísla známého počítačového měsíčníku PC World připravili společně s jeho redakcí 64stránkovou brožurku „Svět elektronického podpisu“. Ani ve snu nás tehdy nenapadlo, jak velký ohlas (veskrze pozitivní) bude mít a jak velkého ocenění se na mnoha frontách dočká.

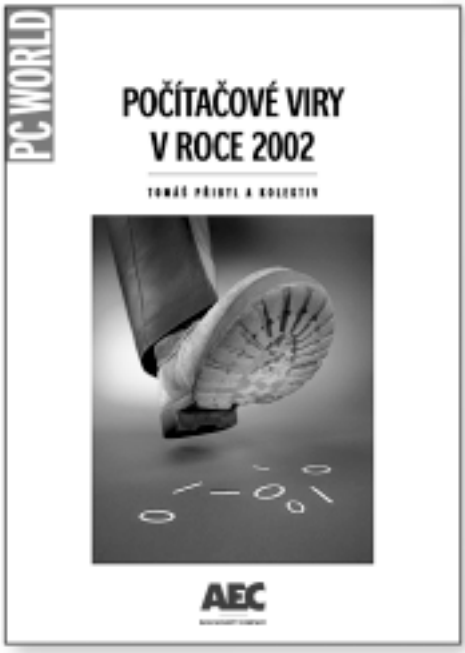
Nyní vrcholí další podobný projekt - opět ve spolupráci AEC a měsíčníku PC World (ani fotbalový trenér po úspěšném zápase nemění osvědčenou sestavu). A tak v lednovém čísle roku 2002 tohoto časopisu (vychází ovšem ještě před vánočními svátky 2001) najdou čtenáři brožurku „Počítačové viry v roce 2002“.

Její název by mohl svádět k domněnce, že bude pojednávat pouze o úzké oblasti škodlivých kódů, ale není tomu tak. Název „Počítačové viry v roce 2002“ byl zvolen proto, že jde o první z řady několika brožurek, které by se měly začít více či méně pravidelně (zhruba v jednoletých intervalech) objevovat jako příloha časopisu PC World. Postupně tak s jejich pomocí bude zmapována celá oblast počítačových virů a informacíchtivý čtenář si může vytvořit celou a úplnou knihovničku.

Brožura „Počítačové viry v roce 2002“ obsahuje následující kapitoly:

- Úvod
- Počítačový virus
- Úspěšný počítačový virus
- Projevy počítačových virů
- Jak vypadá počítačový virus
- Generátory počítačových virů
- Historie počítačových virů
- Počítačové viry v roce 2001 (Kurnikovová, Naked Wife, Magistr, Matcher, Myba, HappyTome, Peach, Sircam, CodeRed, Vote, Nimda, Anthrax, Aliz)
- Varování před virem, který neexistuje
- Mýty o počítačových virech
- Quo vadis, počítačové viry?
- Desatero antivirové ochrany
- Vizitky antivirových programů (Kaspersky Anti-Virus, F-Secure AntiVirus, Virus Scan Security Suite, Panda Antivirus, Sybari Antigen)

Projev počítačového viru Magistr - „uhýbání“ ikonek.



BadTrans - tvrdý úder po půl roce

BadTrans.B je nová verze červa BadTrans, který se poprvé objevil v dubnu 2001. Největší novinkou oproti původní variantě je využití bezpečnostní chyby v Internet Exploreru a MIME hlavičce e-mailu, které umožňuje spuštění červa již při pouhém otevření zprávy.

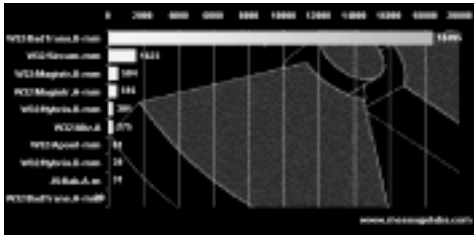
To, že je váš systém infikován virem BadTrans.B, poznáte bezpečně podle toho, že při pokusu o napsání velkého písmena s háčkem napíšete pouze dva háčky „ˇˇ“. Tento projev je způsoben programem pro snímání stisknutých kláves, který je taktéž součástí červa.

Badtrans.B se šíří v systémech Windows pomocí infikované přílohy e-mailu. Červ sám o sobě je Win32 aplikace (PE EXE soubor) o velikosti 29 kB (60 kB v dekomprimované podobě). Skládá se ze dvou hlavních částí: e-mailového červa a trojského koně. Červ zajišťuje rozesílání infikovaných e-mailů a trojský kůň odesílá z infikovaného počítače citlivé informace (user´s info, RAS data, cached passwords, keyboard log) na určitou e-mailovou adresu. Obsahuje také „keylogger“ - program pro snímání stisknutých kláves (Win32 DLL soubor).

Pokud je infikovaná příloha e-mailu spuštěna (ať již „manuálně“ - poklikáním, nebo „automaticky“- pomocí i-frame triku), převezme řízení nejprve e-mailový červ, nainstaluje svoje komponenty do systému a zapíše je v registrech.

Jméno souboru trojského koně a jeho cílový adresář se mohou změnit. Tyto údaje jsou uloženy v kódované podobě a kdokoliv je může nastavit dle své libosti předtím, než soubor odešle na cílový počítač nebo než jej třeba umístí na webovou stránku. Mezi další volitelná nastavení může patřit i smazání původního infikovaného souboru (po úspěšném nainstalování červa do systému) nebo nastavení velikosti souboru se záznamem stisknutých kláves.

K odesílání infikovaných e-mailů červ používá SMTP server. E-mailové adresy dalších potencionálních obětí získává dvěma způsoby:
1.) Vyhledává *.HTM, *.HTML a *.ASP soubory, z nichž extrahuje e-mailové adresy.



BadTrans se stal pomyslným „králem“ mezi škodlivými kódy (graf ze 30. listopadu 2001).

2.) Používá MAPI funkce ke čtení příchozích e-mailů, bere si adresy jejich odesílatelů a „odpovídá“ na ně.

Infikovaný e-mail je v HTML formátu a používá tzv. „i-frame“ bezpečnostní díru ke spuštění červa v přiloženém souboru.

Zpráva vypadá takto:

Od: e-mailová adresa konkrétního uživatele (oběti) nebo smyšlená adresa (jejich seznam škodlivý kód „vláčí“ s sebou).
Předmět: prázdný nebo „Re:“, nebo „Re:“ + původní předmět zprávy (z došlé pošty), na kterou červ odpovídá.
Text: žádný.
Příloha: náhodně zvolené jméno z předdefinovaného seznamu se „zdvojenou příponou“.

Červ se neodesílá na jednu e-mailovou adresu vícekrát. K tomuto účelu si vytváří v systémovém adresáři Windows soubor PROTOCOL.DLL, kam si ukládá odeslané e-mailové adresy a kde kontroluje zda se již na konkrétní adresu neodeslal dříve.

Badtrans.B se ukládá do systémového adresáře Windows jako soubor KERNEL32.EXE a zapisuje pro něj klíč v registrech. Dále spouští program pro snímání stisknutých kláves (keyboard hooker) KDLL.DLL a „ukradené“ informace odesílá na e-mailovou adresu na Hotmailu. Soubor se záznamem stisknutých kláves je uložena v systémovém adresáři Windows v souboru CP_25389.NLS. Červ také vypouští trojského koně KDLL.DLL (detekován např. jako PSW.Hooker), který je uzpůsoben pro krádež a odeslání hesel z infikovaného počítače.

Audit akreditovaných certifikačních autorit aneb workshop e-commerce

Poslední srpnový den roku 2001 se uskutečnil pro zákazníky, spolupracovníky a spřátelené duše společnosti AEC odborný seminář s názvem „Audit akreditovaných certifikačních autorit“. V devět hodin dopoledne se v zasedací místnosti firmy AEC v Brně shromáždilo přes třicet hostů, kteří se po registraci odebrali do areálu střelnice AWIW. Zde se od desáté hodiny konal v salonku seminář.

Pod názvem „Audit akreditovaných certifikačních autorit“ se skrývaly celkem čtyři odborné přednášky:

- Elektronický podpis a certifikační autorita (Ing. Jiří Mrnuštík, AEC, spol. s r.o.).
- Filozofie auditu certifikačních autorit (Ing. Jaroslav Pinkava, CSc., AEC, spol. s r.o.).
- Elektronický podpis a odpovědnost certifikační autority, podepisující osoby a třetích osob za způsobenou škodu (JUDr. Iveta Hodková z PriceWaterhouseCoopers).
- Certifikační autorita a prováděcí dokumentace s ní související (Petr J.Drahovzal, Norman Data Defense).

Po přednesení příspěvků se rozvinula bouřlivá diskuse trvající více než hodinu, svědčící o mimořádné zájmu posluchačů o tuto problematiku, a také o jejich ochotě zapojit se svými názory do debaty. Diskuzi ukončila nutnost dodržel čas rezervace salonku v blízké restauraci Valoria, kam se všichni přesunuli na oběd.

Po obědě navazoval program sportovním odpolednem, a to střeleckou soutěží, ve které měli

hosté semináře možnost vyzkoušet různé druhy zbraní i terčů, a to jak dlouhé kulové zbraně, tak i pistole a revolvery různých ráží. Střídali jsme se ve skupinách po čtyřech, podle počtu střeleckých boxů a zatímco čtveřice střílely, ostatní hosté pokračovali v rozvíjení dopolední diskuze na téma „Auditu akreditovaných certifikačních autorit“. Nutno poznamenat, že střeleb se zúčastnili i přítomné dámy - a vedly si velmi dobře. Ve večerních hodinách byli vyhlášeni a obdarováni vítězové jednotlivých disciplín.

Protože vítězství je nutné pořádně oslavit, celá společnost pokračovala do areálu „Staré pošty“ v Rousínově u Brna. V tomto historickém objektu původní přepřahací stanice koňské pošty, ve které v noci před bitvou u Slavkova přespal francouzský císař Napoleon Bonaparte, byla pro hosty připravena prohlídka prostor s výkladem a ochutnávka moravských vín v původním vinném sklepě spolu s večeří. Když jsme se v pozních nočních hodinách v dobré náladě rozcházeli, mnozí hosté se s díky ptali, zda budeme podobnou akci opakovat. Na podobné otázky exustuje jen jediná odpověď. Rozhodně ano!

Hana Stojanová, hana.stojanova@aec.cz

V roce 2002 opět na CeBITu

Zahraniční veletrhy informačních technologií, jakými jsou například mnichovský Systems, hannoverský CeBIT nebo londýnský Infosec jsou na rozdíl od našeho českého Invexu (a dovolím si s kapkou patriotismu říci - bohužel) rok od roku zajimavější a přitažlivější. Nejen pro vystavovatele, ale hlavně pro ty, o které jde především - pro zákazníky.

Málokterá firma si může dovolit vystavovat na každém realizovaném veletrhu, a ani naše společnost AEC není v tomto ohledu výjimkou. Právě proto jsme pečlivě zvažovali, kam namířit své aktivity, kde vlastně vystavovat, aby byl přínos co největší… Celé pomyslné klání „vyhrál" CeBIT.

Je nám potěšením oznámit, že od 13. do 20. března 2002 vystavujeme nové produkty vývojového oddělení firmy AEC v německém Hannoveru na veletrhu CeBIT v hale 17, stánek A 25.

Proč právě CeBIT?

Protože za něj hovoří čísla: V roce 2001 jej navštívilo 830 tisíc návštěvníků, z toho 160 tisíc ze zahraničí. K vidění byly expozice 8100 vystavovatelů ze šedesáti zemí světa. A co je nejdůležitější, 82 procent návštěvníků se rozhodlo pro investici do IT. Dalších čtyřicet milionů navštívilo webovské stránky CeBitu - to už přece stojí za to! (Zdroj statistických údajů: Messe Hannover.)

Pro rok 2002 jsou na CeBITu připravena tato témata:

- Informační technologie
- Telekomunikace a sítě
- Řešení IT Engineering
- Software, internetová řešení a služby
- Bezpečnost IT a technologie čipových karet
- Bankovní technologie
- Výzkum a technologie
- Automatic Data Capture, Vision systems & Voice Processing

AEC se představí novými produkty a službami na poli internetových aplikací, technologie čipových karet na bázi PKI a novými šifrovacími produkty.

Takže: na shledanou na CeBITu!

Hana Stojanová
hana.stojanova@aec.cz

Slovensko ve znamení počítačové bezpečnosti

Po úspěšné jarní roadshow, kdy zástupci české i slovenské části společnosti AEC postupně navštívili Žilinu, Banskou Bystrici a Košice, jsme se opět vydali na cestu po krásných slovenských městech s cílem šířit osvětu o bezpečnosti dat a antivirové ochraně. Původní záměr jsme nakonec museli lehce poopravit a podzimní akce pod názvem AEC Data Security Day (AEC DSD) se tak uskutečnila „pouze" v Bratislavě a v Banské Bystrici - „vyšší moc" nám zabránila vystoupit s přednáškami také v Komárně, jak bylo původně zamýšleno. Každopádně je možné bez váhání akci označit za úspěšnou.

První AEC DSD svého druhu na Slovensku se tedy uskutečnil devátého října 2001 v salónku Diamant v bratislavském hotelu Danube. Všechno začalo přesně úderem desáté hodiny. Postupně se před přítomnými posluchači vystřídali přednášející z bratislavské i brněnské AEC. Tomáš Přibyl vystoupil s přednáškou na téma historie virů, Petr Nádeníček představil produkty společnosti McAfee a Ján Šimko poutavě hovořil nejprve o produktech společnosti F-Secure a posléze též o nástrojích společnosti Kaspersky Lab.

V závěru akce proběhla diskuse, v níž padlo nemálo zajímavých a věcných dotazů na všechny přednášející. Jedním z vrcholů programu bylo také slosování přítomných, kteří si na památku odnesli nejen několik upomínkových předmětů, ale jeden z nich také padesátiprocentní slevu na F-Secure Anti Virus.

V Banské Bystrici se o dva dny později sešlo na AEC DSD opět takřka třicet posluchačů. Navštívil nás také známý slovenský tvůrce webových stránek s antivirovou tématikou (www.virusy.sk) Martin Lepiš a řada informatiků a administrátorů z blízkých i vzdálenějších průmyslových podniků a dalších organizací.

Scénář celé akce probíhal velmi podobně jako v Bratislavě - přednášky, dotazy, slosování šťastných výherců.

Soudě podle ohlasů, které celá akce vzbudila, se naše snaha zrealizovat další osvětový seminář podařila. Těšíme se na další akce na Slovensku, jako jsou například jarní roadshow v roce 2002, bratislavskou konferenci Bezpečnosť dát nebo třeba právě zopakování AEC Data Security Day.

Petr Nádeníček
petr.nadenicek@aec.cz

Roadshow aneb bezpečnost na cestách

Ve třech týdnech od třicátého října do patnáctého listopadu 2001 pořádala společnost AEC - Data Security Company přednáškovou túru po vybraných městech naší krásné a rozlehlé země české. Postupně jsme navštívili Olomouc, Ostravu, Hradec Králové, Liberec, Ústí nad Labem, Karlovy Vary, Zlín, České Budějovice a Plzeň. Ve všech uvedených městech byly přednášky o antivirové ochraně, elektronickém podpisu a bezpečnosti dat středem pozornosti zaujatých posluchačů, kteří byli vděčni za mnohdy zcela nové informace. Nás - přednášející - zase na druhé straně těšilo mít možnost poskytovat informace lidem, kteří o ně mají očividný zájem.

Vysoká účast na přednáškách je jedním z mnoha důkazů toho, že problematika bezpečnosti dat, elektronického podpisu a antivirové ochrany je čím dál častěji chápána jako jedna z klíčových oblastí informačních technologií. A není se čemu divit. Počítače v rozličných podobách a formách pronikají do všech oblastí lidského života a s tím, jak jim svěřujeme stále více osobních a jiných citlivých údajů, se stávají aktuální také otázky počítačové bezpečnosti. Také elektronický podpis se (sice pomalu, ale jistě) stává životní realitou všedního dne. Není tedy nic zarážejícího na tom, že naše semináře navštívily téměř tři stovky posluchačů.

Všechny semináře probíhaly v podobném duchu a s podobným sledem přednášek. Po nezbytném úvodu a přivítání byli přítomní posluchači v přednášce na téma „Seznamte se: Počítačové viry“ uvedeni do různorodého světa nebezpečných škodlivých kódů, s jejich projevy, stručnou historií a základními zásadami boje proti nim. Poté, co se posluchači dozvěděli, co jim bezprostředně hrozí, následovala další ze stěžejních přednášek semináře, která pojednávala o produktech finské společnosti F-Secure, zvláště o programu F-Secure Anti-Virus, ale také o dalších produktech, jako je File-Crypto nebo VPN+. Po této zpravidla poměrně dlouhé přednášce většinou následovala přestávka spojená s nezbytným občerstvením.

Druhá část programu byla věnována širší problematice bezpečnosti dat a elektronickému podpisu. Byla zahájena krátkou úvodní přednáškou o elektronickém podpisu, ve které byli posluchači seznámeni se základními principy šifrování a elektronického podepisování. Vysvětleny byly také některé základní pojmy, jako je certifikát nebo certifikační autorita a jaké jsou jejich role v procesu elektronického podepisování. Následovala přednáška, která ve stručnosti seznamovala posluchače s riziky existujícími v kybernetickém světě. Dozvěděli se, kdo jsou to hackeři, co mohou provést a jak se proti nim bránit. Závěrečná přednáška pak ve stručnosti shrnula portfolio bezpečnostních produktů a služeb, které naše firma nabízí.

Důkazem toho, že probíraná problematika měla u přítomných posluchačů značný ohlas, byly i poměrně četné dotazy z pléna, které padaly jak v průběhu jednotlivých přednášek, tak i v závěrečné diskuzi. Značnému ohlasu se těšila hlavně problematika elektronického podpisu a elektronických podatelen, která je v současné době z mnoha důvodů populární.

Závěrem tedy můžeme konstatovat, že AEC roadshow 2001, patřící již nyní bohužel minulosti, splnila svůj účel, kterým bylo především šíření osvěty a informací i mimo hlavní místa konání většiny akcí (jako jsou Praha, Brno nebo Bratislava). Vše nasvědčuje tomu, že se zrodila úspěšná akce, neboť už se pomalu rozjíždí soukolí příprav akce „AEC roadshow 2002“.

Petr Nádeníček, petr.nadenicek@aec.cz

AEC
Data Security Day

9. a 11. října 2001
Slovenská republika

Vzpomínka na jarní roadshow - Košice.

Přednáším, přednášíš, přednášíme…

Banská Bystrica - tradiční zastávka na našich slovenských „výletech".

Vylosovaní výherci se těšili na získané ceny.

K boji s počítačovými viry vždy připraveni!

AEC roadshow 2001

30. října
až
15. listopadu 2001

Olomouc - velká roadshow začíná!

Na roadshow je cesta dlouhá…

V Hradci Králové nás navštívil i Igor Hák (www.viry.cz).

Olga Přikrylová byla na roadshow skutečně "na roztrhání".

Tomáš Vobruba zaujal posluchače ve Zlíně.

Nebezpečí kybernetického prostoru jsou před námi

V několika minulých letech jsme se měli možnost setkat se s celou řadou prvků počítačové kriminality od jednoduchých hackerských průniků až po masivní virové útoky. Některé sofistikované útoky a průnikové aktivity je možné připsat skupinám kriminálních živlů, operujících v elektronickém prostoru, nebo také (a to bez nadsázky) například pokusům cizí moci o test zabezpečeních některých důležitých informací.

Průniky do webovských stránek státních úřadů, jako je ministerstvo obrany nebo změny web stránek velkých bankovních domů neposilují důvěru obyvatelstva v informace poskytované státními institucemi v rámci tzv. státního informačního systému. Útoky na e-commerce servery zase nevyvolávají velké nadšení u lidí, kteří by chtěli na Internetu obchodovat a například platit elektronicky pomocí kreditních karet či jiným elektronickým mechanismem.

Útoky, které mají za výsledek ukradení čísel kreditních karet nebo ztrátu citlivých vládních či bankovních informací mohou být nebezpečím pro národní bezpečnost a současně zcela jednoznačně podkopávají důvěru v e-commerce. Útoky, které jsou vedeny za účelem poškodit a zneprovoznit servery a služby v Internetu, jako například e-commerce, nebo informační či vyhledávací servery, mohou mít významné následky nejen pro firmu, která se stala obětí, ale pro hospodářství jako celek.

Nebezpečí útoků zevnitř

Nespokojený zaměstnanec je hlavním a základním zdrojem počítačové kriminality. Nepotřebuje mít vysoké znalosti o technikách průniků a IT bezpečnosti, protože má hluboké znalosti o informačním systému oběti, což mu umožňuje neomezený přístup, a tak může jak zničit, tak zcizit data. Například jenom v roce 1999 Computer Security Institute/FBI zjistil, že 55 procent dotázaných nebo vyšetřovaných firem připustilo napadení systému zevnitř.

Jeden z takových pěkných příkladů je případ paní Shakuntla Devi Singla, která zneužila informace o informačním systému a znalost hesel spolupracovníků a smazala data z personálního systému americké pobřežní hlídky. 115 zaměstnanců této agentury obnovovalo databáze více jak 1800 hodin. Paní Singla byla odsouzena k pěti měsíců vězení, pěti měsícům domácího vězení a k pokutě 35000 USD.

V lednu a únoru 1999 se stal terčem útoku počítačový systém National Library of Medicine, na který spoléhají statisíce doktorů z USA i z jiných zemí. Jsou zde informace o nemocech, léčivech, léčebných postupech apod.

V průběhu útoku bylo použito heslo administrátora systému a byly nahrány stovky souborů obsahující velmi citlivá lékařská varování a informace a navíc programové soubory, které řídily funkčnost celého systému.

Útok byl skutečným a vážným ohrožením veřejné bezpečnosti a zapříčinil finanční ztrátu větší jak 25 tisíc USD. Vyšetřování FBI identifikovalo jako útočníka Montgomery Johns Graye, III, který byl dřívějším zaměstnancem a programátorem National Library of Medicine a jehož přístup do databází a do informačního systémy byl zrušen. Gray mohl přistoupit do systému pomocí zadních dvířek, které si vytvořil v programovém kódu. Za útok na veřejnou bezpečnost byl Gray uvězněn FBI na několik dnů a jeho počítač byl po dobu šetření zabaven. Vyšetřování prokázalo jeho vinu a byl nakonec odsouzen

Hackeři

Hackeři jsou všeobecnou hrozbou. Čas od času se vloupají do počítačové sítě pouze pro radost, nebo proto, aby si zvýšili prestiž v hackerské komunitě. Častěji však se hackerské útoky dějí pro finanční profit útočníka. Dříve vzdálené hackerské útoky vyžadovaly velké znalosti o sítích, protokolech a programování. Dnes je možné v Internetu najít množství skriptů a programů které je pak možné vypustit proti informačnímu systému oběti. Podobné útočné programy jsou stále snadněji použitelné a jak se všeobecně zvyšuje snadnost použití software, tak roste i jednoduchost obsluhy těchto nástrojů. Hackeři také mohou být, ať již vědomě či nevědomě, použiti k jiným, mnohem nebezpečnějším útokům, které se maskují za jejich aktivitami.

Hactivism - hackerský aktivismu

Je naprosto nový typ aktivit, které se začínají objevovat v posledních měsících. Jde o politicky motivované útoky na veřejně přístupné webovské stránky nebo mailové servery. Takovéto skupiny přetěžují e-mailové servery a hackují webové stránky, aby mohly posílat politické zprávy a prohlášení. Jedna taková skupina se nazývá „Electronic Disturbance Theater“ a propaguje

civilní neposlušnost on-line (pro podpoření jejího politického programu ve vztahu k Zapatistickému hnutí v Mexiku a k dalším cílům). Uveďme jen několik dalších příkladů.

Například během války v Jugoslávii hackeři sympatizující se Srby elektronicky napadli NATO web servery. Rusové a ostatní, kteří sympatizovali se Srby atakovali web servery v zemích NATO za použití infikovaných e-mailů a hackerských útoků.

Přívrženci Kevina Mitnicka napadli web stránku Senátu USA a poškodili ji v průběhu procesu s ním. Mitnick byl nakonec odsouzen k 46 měsícům ve federálním vězení a k úhradě škod. Byl propuštěn v lednu 2000 po vykonání trestu s odečtením doby ve vyšetřovací vazbě.

Internet umožňuje nové formy politického shromažďování a výměny informací. To může mít samozřejmě jak pozitivní, tak i negativní důsledky podle toho, kterým lidem se tento nástroj dostane do ruky.

Pisatelé virů

Viry se stávají vážným nebezpečím pro počítače, sítě a informační systémy globálně a nebezpečí se stále zvyšuje.

Virus Melissa je dobrým příkladem s úspěšným vyšetřovatelským koncem. NIPC (National Infrastructure Protection Center) fungoval jako centrální kontaktní bod pro polní kanceláře, které vedly vyšetřování. Na základě tipu z America Online, který byl zaslán New Jersey State Police následovalo vyšetřování vedené ve FBI Newark Field Office, které vedlo 1. dubna 1999 k zatčení Davida L. Smithe. Byl shledán vinným a bylo mu prokázáno poškození jednoho miliónu počítačů a způsobená škoda 80 milionů USD.

Kriminální skupiny

Kriminální skupiny jsou velkým nebezpečím pro celý kybernetický prostor, protože jejich aktivity se blíží a nebo jsou zařaditelné do skupiny organizovaného zločinu. Jejich útoky na informační systémy jsou skupinové a jsou vedeny s cílem finančního zisku. Jedna ze známých skupin byla mezinárodní skupina „Phonemasters“, která pronikla do počítačů MCI, Sprint, AT&T, Equifax, a také do FBI National Crime Information Center.

Na základě soudního příkazu k elektronickému sledování byly monitorovány aktivity modemu podezřelého Calvina Cantrella. Calvin stahoval stovky čísel telefonních karet, která prodal do Kanady, odkud byla předána do Ohia. Cantrell byl odsouzen na dva roky a jeho společnice Cory Lindsay na čtrnáct měsíců. Tato skupina pracovala metodou sociálního inženýrství, a tak pod záminkou falešný důvodů a na základě starých informací získávala od obětí přístupové kódy.

Kyberterorismus

Teroristé jsou známí tím, že používají informační technologie a Internet pro formulování svých plánů, zajišťování peněz, šíření propagandy a pro bezpečnou komunikaci. Například usvědčený terorista Ramzi Yousef, který byl organizátorem bombového útoku na World Trade Center v první polovině devadesátých let, přechovával plány na zničení US Airlines v šifrovaných souborech na svém laptopu. Některé skupiny používají kybernetické útoky, aby poškodili informační systémy jejich protivníků. Například skupina, která se nazývá „Internet Black Tigers“ provedla úspěšný útok s následným vyřazením z provozu serveru ambasády Srí Lanky.

Informační válka

Jedno z největších nebezpečí pro národní bezpečnost a pro bezpečnost ve světě vůbec je informační válka zaměřená cizí mocností proti důležitým bodům insfrastruktury. Tam, kde státy a nebo militantní skupiny nemohou obstát v konfliktu tváří v tvář (klasický konflikt), mohou však uspět při vedení kybernetické informační války. Nejvíce zranitelné jsou samozřejmě nejsilnější a nejvyspělejší státy s rozvinutou infrastrukturou, která je stále závislejší na elektronice a informačních systémech.

Počítačová kriminalita je jeden z nejdynamičtěji se rozvíjejících problémů, kterému tváří v tvář stojí vyšetřovací a bezpečnostní služby celého osvěta. Jenom si pomysleme kolik počítačů vlastníme a kolik různých operačních systémů a softwarových balíků se objevilo v několika posledních letech. Problémy v budoucnosti z tohoto množství můžeme jen stěží odhadovat. Bezpečnost státních informačních systémů a jejich veřejná dostupnost bude záležet na znalostech a možnostech státních úředníků a také na znalostech uživatelů počítačů.

Tomáš Přibyl, tomas.pribyl@aec.cz

AEC představuje nový produkt

Dobrý den přátelé,
vzhledem k tomu, že se našim zákazníkům snažíme poskytovat komplexní řešení bezpečnosti dat a navíc tato řešení „šít“ zákazníkům na míru, rozhodli jsme se přibrat do naší nabídky antivirového software nový produkt.

Jedná se o produkt s krásným jménem Antigen, který pochází s dílny celosvětové společnosti Sybari. Tato společnost disponuje pobočkami v Dubaii, Singapuru, Sydney, Filipínách, Sao Paulu, Madridu, Paříži, Frankfurtu, Římě i Londýně, přičemž jejím sídlem je New York.

Produkt Antigen je řešení pro groupware prostředí, tedy o antivirový program na ochranu Exchange a Lotus Domino serveru. Teď se zkusíme podívat, jaké možnosti a vlastnosti produkt Antigen nabízí, co umí a s čím může pomoci.

Antigen 6.0 pro Lotus Domino

je produkt vytvořený s ohledem na nutnost neustálé ochrany prostředí, tedy pro provoz 24 x 7. Díky tomu není server nikdy bez aktivní antivirové ochrany, a to ani při aktualizacích a upgradech. Je kompatibilní s Lotus Notes a Domino Server verzí 4.5x a 5x.

Sybari Antigen 6.0 pro Lotus Domino nabízí mimo vlastností dnes už standardních u každého antivirového programu také

- detekci a možnost úplného mazání e-mailových červů,
- podporu skenovacích motorů třetích stran (Norman Data Defense, McAfee, Sophos, Computer Associates),
- ochranu Domino Net Store,
- podporu skenování souborů ve formátu Macintosh,
- podporu skenování digitálně podepsaných zpráv,
- skenování a čištění víceúrovňových zipovaných příloh a jiných cyklických příloh,
- Content Management s nastavitelnými filtry,
- iNotes Web Access Protection.

Celý produkt je možné velmi snadno vzdáleně instalovat a spravovat, přičemž aktualizace virových řetězců mohou probíhat zcela automaticky, bez jakéhokoliv zásahu uživatele. Za zmínku stojí také propracovaný reporting virových incidentů, přičemž reporty a z nich vycházející statistiky jsou dostupné přes povelové rozhraní Domino serveru.

Antigen pro Lotus Domino nabízí skenování procesů čtení a zápisů v reálném čase a kontrolu SMTP zpráv, Native Notes Mail. Toto skenování probíhá „za letu“ (on the fly). Mezi další schopnosti patří také manuální skenování mailboxů a databází.

Detekční schopnosti antivirového programu umožňují přeskočení, vyčištění, přesunutí nebo vymazání e-mailové zprávy či přesunutí příloh do karantény (před vyčištěním nebo smazáním). Navíc jsou podpořeny filtrováním e-mailů, resp. souborů (dle typu, velikosti, jména a adresy).

Tyto e-maily je pak podle nastavení možné přesouvat, mazat, kopírovat nebo rovněž „uložit do karantény“. Filtrace e-mailových zpráv je vhodná zejména pro období od objevení nového viru po vydání nových virových signatur.

Komponenty Antigenu pro Lotus Domino jsou následující:

- Antigen Nshield - zajišťuje ochranu všech databází v reálném čase.
- Antigen Nwall - zajišťuje ochranu procházejících zpráv a příchozích i odchozích dokumentů reálném čase.
- Antigen Nscan - umožňuje skenování všech individuálních databází a uživatelských schránek, a to buď časově plánované nebo manuální.

Antigen pro Microsoft Exchange

je antivirové řešení pro Microsoft Exchange 2000 a Exchange 5.x, ve kterém je možné (tak jako i v Antigenu pro Lotus Dominu) využít až pěti na sobě nezávislých skenovacích motorů.

Mimo obousměrného skenování všech příchozích a odchozích SMTP zpráv v reálném čase a zpráv zaslaných přes Outlook Web Access nabízí také skenování zpráv v osobních i veřejných složkách a jejich databázích. Tuto kontrolu lze buď spouštět časově plánovanou nebo manuální. Samozřejmostí je skenování digitálně podepsaných zpráv a vícenásobných komprimovaných souborů (ZIPů). Nastavení antivirového programu umožňuje napadenou přílohu e-mailu vyčistit, smazat, přeskočit nebo přesunout do karantény.

Sybari

Instalace a správa antivirového programu probíhá vzdáleně, s možností automatické aktualizace virových signatur. Všechny informace o virových incidentech jsou ve formě reportů a logů přístupných na obrazovce, v souboru nebo v logu událostí NT.

Sybari Antigen pro Microsoft Exchange je spouštěn jako NT služba a plně podporuje clusterová řešení Active/Active.

Produkt se skládá ze tří základních částí:

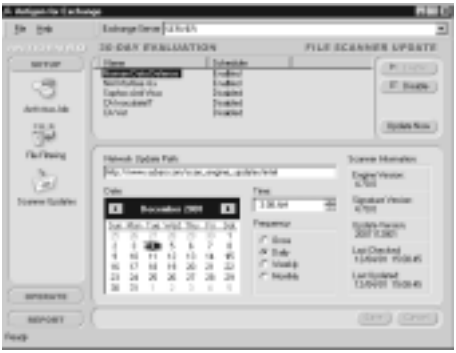
- Antigen Realtime Job - tato část slouží pro skenování probíhající v reálném čase, kdy zprávy jsou skenovány „za letu“ (on the fly). Tato část skenuje Storage Groups a databáze.
- Antigen SMTP/IMS Job - slouží pro ochranu příchozích a odchozích zpráv v reálném čase.
- Antigen Manual Scan Job - slouží pro skenování časově plánované nebo spouštěné manuálně.

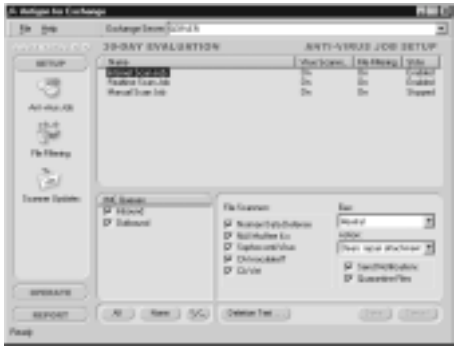
Oba tyto produkty jsou, jako ostatně všechny z nabídky AEC, dodávány spolu s technickou podporou, možností instalace, vyškolením obsluhy, auditů správného nasazení apod. Díky tomu, že tento produkt přesně zapadá do nabídky AEC, jsme schopni našim zákazníkům nabídnout nejen jedno antivirové řešení bezpečnosti, ale celou škálu možných řešení z nich podle Vašich požadavků sestavíme to nejoptimálnější.

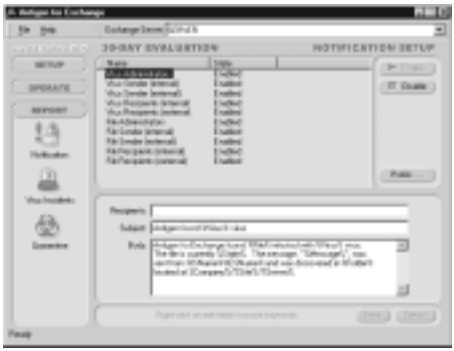
Teď už je jen na uživateli, aby specifikoval svoje potřeby v oblasti ochrany dat a tyto nám sdělil. Takže neváhejte a piště, telefonujte, faxujte a mailujte…

… a samozřejmě se mějte dobře.

Jan Novotný, jan.novotny@aec.cz







Projekt elektronické podatelny

Elektronický podpis je technologie, která má (mimo jiné) úřadům a občanům pomoci urychlit, usnadnit a vůbec zjednodušit vzájemnou komunikaci. Jedním z největších problémů při zavádění elektronického podpisu do života je absence vhodných aplikací, které by bylo možné nasadit v praxi. Jedním z mála produktů na trhu, které celý problém řeší, je projekt Podatelna, který spatřil světlo světa ve vývojových laboratořích firmy AEC.

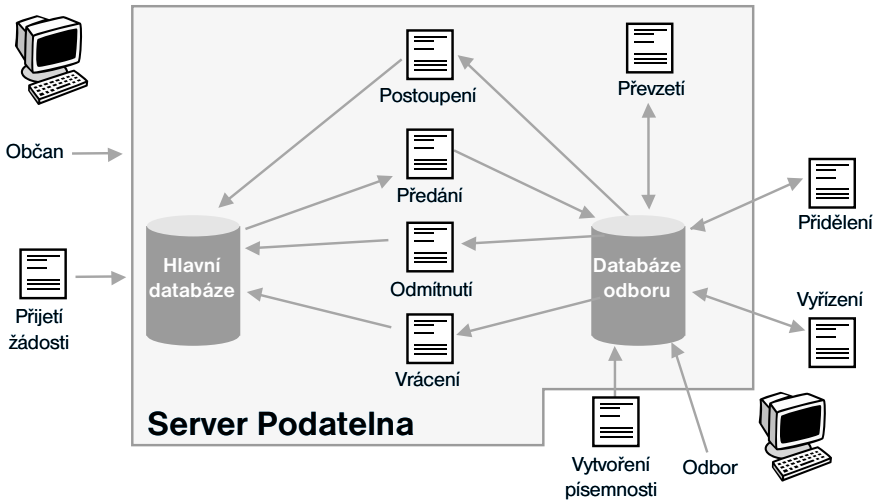
Jedná se o databázový systém, který umožňuje jednoduchou formou realizovat tzv. elektronické podatelny ve smyslu nařízení vlády ze dne 25. července 2001, kterým se provádí zákon o elektronickém podpisu. Řešení vychází z elektronické spisové služby, kterou doplňuje o možnost vytváření a ověřování elektronického podpisu.

Použité technologie v projektu elektronické podatelny

Celý systém je postaven na platformě Windows - na jedné straně web server MS IIS s databázovým systémem MySQL (případně jiný typ databáze) a na straně klienta web prohlížeč, nejlépe MS Internet Explorer. Řešení je možné realizovat buď formou služby jako pronajatá podatelna na připravovaném portálu **e-kiosek.cz**, nebo jako vlastní řešení v místě zákazníka. Vytváření a ověřování elektronického podpisu probíhá v Open SSL knihovně a za pomoci nástrojů pro ověřování kořenových certifikátů podepisujících

Jak funguje projekt elektronická podatelna?

Občan zasílající podání se připojí prostřednictvím svého prohlížečem k web serveru Podatelna. Díky svému osobnímu certifikátu (který má uložený v HW prostředku nebo importovaný v prohlížeči) je na web serveru autentizován. Tedy je ověřena jeho totožnost na základě osobního certifikátu. Občanovi je nabídnut výběr odboru, na který chce podání zaslat, a následně i formulář k vyplnění včetně elektronického podepsání. Formulář je uložen do databáze a přiřazen určenému pracovníkovi ke zpracování. Občan obdrží automaticky potvrzení přijetí žádosti formou zprávy s jednacím číslem. K evidenci o aktuálním místě uložení písemností a jejích stavů se využívá systému spisových „knih“ (centrální podací kniha - podatelna, místní spisová kniha - podací kniha odboru) představovaných databázemi MySQL. Veškeré činnosti jsou logovány pro případ pozdější kontroly.



Procesní diagram

Odpovědný pracovník odboru přistoupí ke svým agendám podobně jako uživatel pomocí web prohlížeče. Po autentizaci na stránce „Podatelna“ obdrží přehlednou formou ke zpracování všechna podání. Ta jsou zobrazena včetně datových údajů, odpovědných osob, podacích čísel, subjektu a odesílatele.

Odpovědný pracovník rozhodne o převzetí písemnosti nebo vrácení na podatelnu. Vrácená písemnost může být zaslána k vyřízení jinému odboru. Přijatou písemnost lze přidělit pracovníkovi pověřenému jejím vyřízením. Pověřený pracovník může postoupit zpracovávaný spis k vyjádření jinému odboru.

Od okamžiku zaevidování písemnosti až do jejího vyřízení se veškeré operace zaznamenávají do protokolu (druh operace, osoba, datum a čas, případně doplňující poznámka).

Bezpečnost projektu elektronické podatelny

Systém Podatelna je realizován s maximálním důrazem na bezpečnost a důvěryhodnost přenášených dat. Základními rysy jsou autentizace, vytváření šifrovaného kanálu při přenosu dat, využívání digitálních certifikátů pro ověření totožnosti korespondujících stran a k elektronickému podepisování dokumentů.

Doplňkem k řešení může být zřízení registračního místa, tzv. registrační autorita příslušná k certifikační autoritě (poskytovatel certifikačních služeb), jejíž náplní je přijímat žádosti o vydání certifikátů.

HOAX - otázky a odpovědi

Hoax je zpráva, šířená zpravidla e-mailem, která se snaží přesvědčit příjemce, aby jí poslal dalším známým a přátelům. (Nejčastěji se jedná o varování přes supernebezpečnými počítačovými viry, které ovšem neexistují - což ale uživatel netuší.) Vzhledem k rychlosti e-mailové komunikace a neznalosti uživatelů počítačů se dokáže podobná zpráva během několika dní velice rychle rozšířit.

Může být hoax nebezpečný?

Nemůže, jediným vážnějším důsledkem hoaxů je přetěžování poštovních serverů a linek naprosto zbytečnou a nesmyslnou poštou, kterou posílají naivní uživatelé, jež uposlechli příkazu a poslali zprávu dál. Pokud dostane jeden příjemce stejnou zprávu od více odesílatelů, musí jí také několikrát stahovat, což se, v případě dial-up připojení, může negativně promítnout na výši jeho telefonního účtu.

Jak lze hoax poznat?

Nejčastěji se objevujícím znakem hoaxu jsou informace o počítačových virech odvolávající se na firmu nebo společnost, která je u řadových uživatelů známá a budí respekt. Hlavním znakem všech hoaxů je žádost (nebo prosba) o další rozesílání zprávy dál. Tato žádost je většinou v e-mailu několikrát zdůrazněna tak, aby v příjemci vyvolala pocit, že je skutečně nutné, aby o této informaci věděli naprosto všichni jeho známí.

Jak se bránit?

Sami se příliš bránit nemůžete, co ale můžete, je neposílat hoaxy dál. Odesílatele taktně upozorněte na to, že jím zaslaná zpráva se nezakládá na pravdě, vysvětlete mu v čem spočívá podstata hoaxů, a požádejte ho, aby podobné informace dále nešířil.

Kde lze najít další informace o hoaxech?

Nejlépe na webových stránkách velkých antivirových firem.

- informace v češtině - www.hoax.cz
- McAfee - vil.mcafee.com/hoax.asp
- AVP - www.avp.ch/avpve/other/hoax.stm
- F-Secure - www.f-secure.com/news/hoax/
- Computer Virus Myths - www.vmyths.com/

McAfee VirusScan 6.0 - antivirový desktopový program určený pro domácí použití

V současné době je známo okolo šedesáti tisíc počítačových virů! A jako by to nebylo málo, toto číslo se denně zvyšuje. Jejich dosah je přitom děsivý. Během chvíle se může jednoduchý virus rozšířit na milióny počítačů po celém světě a způsobit tak miliardové škody. Stále častěji se také dočítáme o hackerských průnicích do systému počítačů. Mohl by však přijít den, kdy o těchto průnicích nebudeme jen číst, ale staneme se jejich obětí. Proto, aby se tak nestalo, neměli bychom nechávat žádný počítač bez antivirové ochrany a osobního firewallu.

Firma McAfee nedávno představila svůj nový produkt, který má integrovanou jak antivirovou ochranu tak personální firewall v jednom balíku. Nese název VirusScan 6.0 a je určen pro kategorii domácích uživatelů. Mnohým uživatelům je známá verze 5.0. VirusScan 6.0 však přichází s mnohými vylepšeními a novinkami.

McAfee - VirusScan 6.0

- detekuje a odstraňuje všechny známé škodlivé kódy jako jsou polymorfní viry, stealth viry, makroviry, trojské koně apod.;
- poskytuje kompletní ochranu počítače před neoprávněným přístupem - znemožňuje hackerům přístup do Vašeho PC;
- obsáhlá a souhrnná internetová filtrace - zabraňuje všem internetovým a e-mailovám hrozbám;
- detekuje destruktivní ActiveX a Java Applety;
- chrání PC během synchronizace s PDA (For Palm OS, Win CE, Pocket PC, Symbian Epoc);
- obsahuje integrovaný personální firewall;
- bezpečná skartace dat (pouze ve verzi VirusScan Professional 6.0).

McAfee VirusScan technologie detekuje a odstraňuje všechny typy známých virů ze všech zdrojů - e-mailových zpráv i připojených příloh, internetových downloadů, sdílených disků, CD-ROMů. Ne, každý si uvědomuje, že každé připojení PDA k počítači a synchronizace dat, skýtá stejné nebezpečí jaké na nás číhá při kopírování dat z jakékoliv jiné mechaniky vložené do našeho počítače (disketa, CD-ROM). VirusScan 6.0 nabízí spolehlivou ochranu při synchronizaci počítače s PDA.

McAfee VirusScan rovněž detekuje destruktivní ActiveX a Java Applety, které jsou často stahovány do počítače, zatímco si bezstarostně brouzdáte po Internetu.

VirusScan 6.0 je jedním z prvních antivirových programů které přicházejí s integrovaným personálním firewallem a je schopný zablokovat hackerům přístup do systému. Nezáleží na tom, zda máte dial-up (vytáčenou linku) nebo pevné připojení. Firewall postaví kolem počítače ochrannou bariéru.

Systémové požadavky:

Pentium 100MHz nebo vyšší procesor.
32 MB RAM
Prostor na disku: 33 MB.
CD mechanika pro instalaci programu.
Doporučujeme přístup na Internet pro updaty produktu.

Kromě VirusScanu 6.0 je v naší nabídce i program VirusScan Professional 6.0. Sám název napovídá, že se jedná o rozšířenou verzi VirusScanu 6.0. Do „Professional“ verze je přidán i modul na bezpečnou skartaci dat.

Systémové požadavky jsou stejné jako u výše popsaného produktu. Potřebujete pouze větší prostor na disku - 40 MB.

Podporované platformy u obou programů:
Microsoft Windows 95b, 98, ME, NT 4, 2000, XP Home Edition a XP Professional.

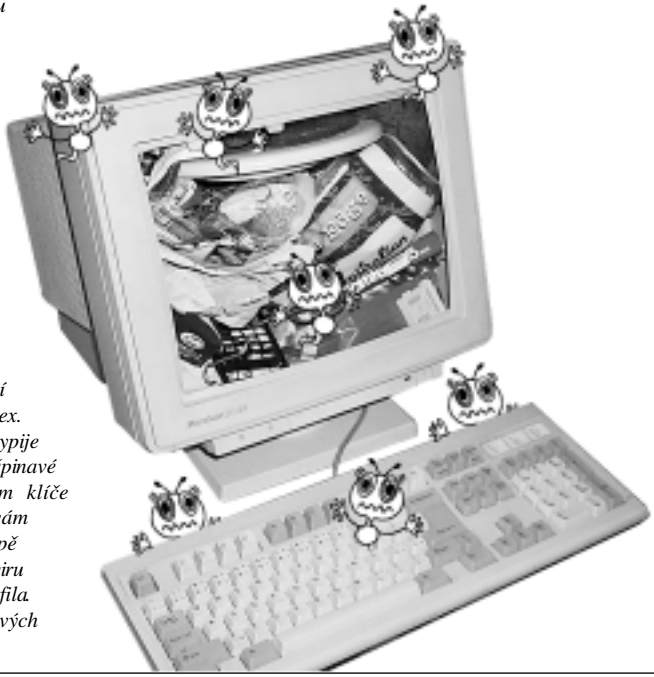
V případě jakýchkoli dotazů či zájmu o uvedené produkty kontaktujte naše obchodní či technické oddělení

Eva Šebková
eva.sebkova@aec.cz

Pozor, šíří se nebezpečný virus, který nikdo nedokáže detekovat!

Protože se blíží konec roku a čas vánočního i novoročního veselí, opustíme na následujících řádcích „vážný“ tón a podíváme se na oblast zvěstí o nejnebezpečnějších a nedetekovatelných počítačových virech (tzv. hoaxy) trochu méně vážně. Nebo snad ne?

Po Internetu se začíná šířit zatím nejnebezpečnější virus! Do počítače proniká protokolem ICMP a DNS dotazy, takže je prakticky nezjistitelný a firewally jej nezadrží. Pokud dostanete e-mail se slovem Badtimes v předmětu, okamžitě ho smažte bez čtení! Jde o doposud vůbec ten nejnebezpečnější virus!!! Po průniku do počítače nejprve rozbliká obrazovku na takovém kmitočtu, že kdo se na ni podívá, je do dvou až tří sekund zhypnotizován a upadne na své židli do alfa-spánku. Poté virus roztočí pevný disk na tak vysoké obrátky, že plotny disku prorazí kryt disku i počítače a uříznou spícímu uživateli hlavu. Při tom dojde samozřejmě také ke ztrátě všech dat z této i z disku. Nejen to, on zničí i všechny diskety položené poblíž počítače. Přenastaví váš termostat v ledničce, takže vám roztaje zmrzlina a srazí se mléko. Demagnetizuje vám proužky na platebních kartách, zruší předvolby na videu a pomocí prostorového harmonického pole poškrábe všechna CD, která si budete chtít přehrát. Vaší dívce změní telefonní číslo. Do akvária vám naleje Fridex. Před příchodem návštěvy vám vypije všechno pivo a na stole nechá špinavé fusekle. Až zaspíte, schová vám klíče od auta a přeprogramuje vám autorádio tak, že v dopravní zácpě uslyšíte jenom šum. Vinou tohoto viru se zamilujete do zatvrzelého pedofila. V noci se vám bude zdát o cirkusových trpajzlících. Až vám vaše dívka zahne v hotelu, účet se připíše do vyúčtování vaší karty. Virus pošle tchýni pozvání na týdenní návštěvu. A oznámí vaší bývalé dívce vaše nové telefonní číslo. Svede vám babičku, bez ohledu na to, jestli je mrtvá. Taková je síla nového viru, že sahá až za hrob, aby se dotkl toho, co je nám nejdražší. Onemocníte tou nemocí, která napadá kaštany. Je zákeřná a vynalézavá. Je nebezpečná a strašná. A to jsem se zmínil jen o části toho, co umí! Obavy jsou velmi, velmi na místě. Horší virus neexistuje! Okamžitě po obdržení tohoto dopisu jej rozešlete na všechny adresy, které znáte; na každou z nich sedmkrát až třiadvacetkrát, protože virus číhá na routerech a tyto dopisy žere. Ihned po rozeslání vytrhněte počítač ze zásuvky a co nejrychleji utíkejte na nejbližší kopec, kde vyčkejte na další informace...



Dejte přednost jistotě!

AEC - společnost s desetiletou tradicí v oblasti software a služeb pro komplexní zabezpečení a ochranu dat.

- bezpečnostní analýzy
- studie a projekty
- komplexní návrhy řešení včetně jejich realizace
- konzultace
- audit bezpečnostních řešení
- odborná školení a semináře
- certifikační autorita „na klíč“

AEC

DATA SECURITY COMPANY

BRNO: AEC, spol. s r.o., Bayerova 799/30, 602 00 Brno, tel.: 05/4123 5466-7
fax: 05/4123 5038, e-mail: info@aec.cz, www.aec.cz

PRAHA: AEC, spol. s r.o., Vinohradská 184, 130 52 Praha 3
tel./fax: 02/6731 4326, 6731 1402, e-mail: praha@aec.cz, www.aec.cz

Bratislava: AEC Bratislava, s.r.o.
Pribinova 25, P.O.Box 79, 810 11 Bratislava, Slovenská republika
tel: + 421 2 50633 027, fax: + 421 2 50633 029, e-mail: bratislava@aec.sk