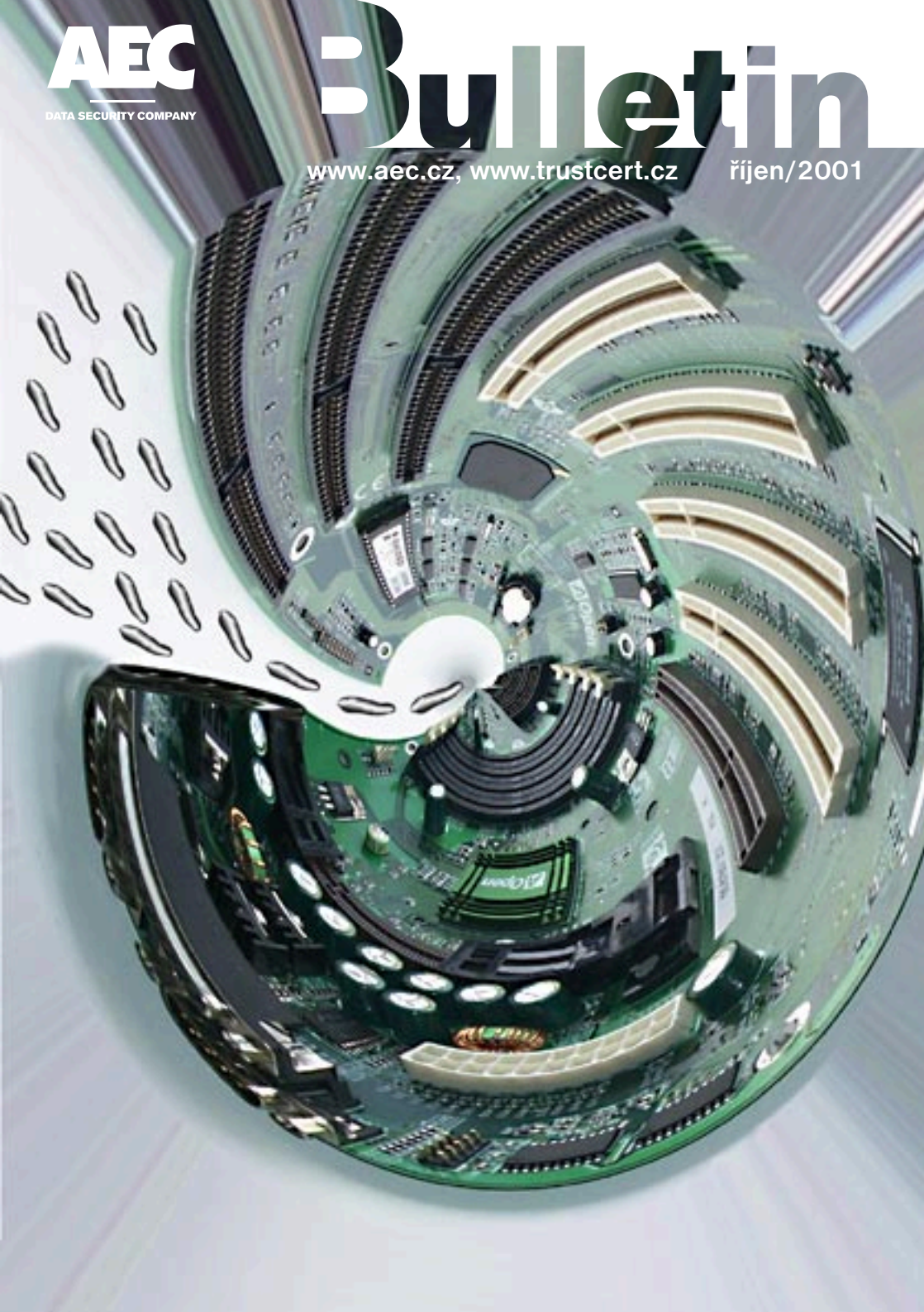
AEC

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**

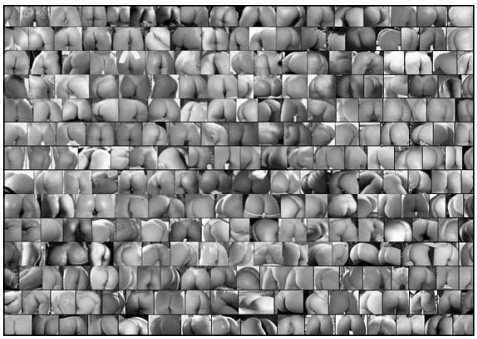
Spuštěn bez kliknutí: Cuerpo

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

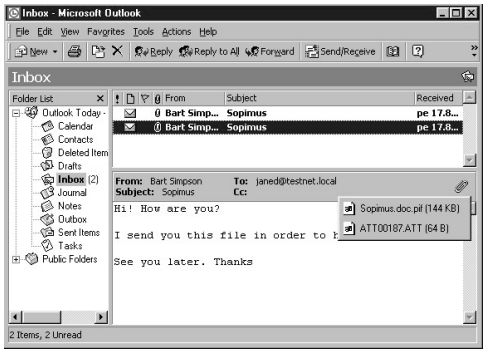


software potom umožňuje tyto dokumenty otevírat a ty mohou obsahovat virus. Peachy ke svému šíření potřebuje „plnou verzi“ programu Adobe Acrobat (pouhé čtení pomocí Adobe Acrobat Readeru jej aktivovat nedokáže).

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

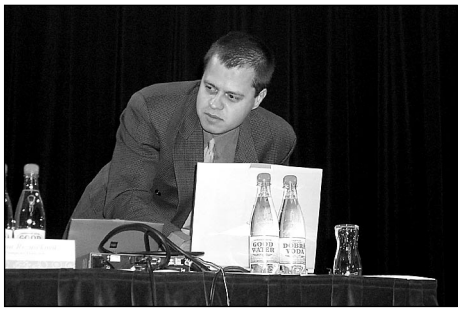
IT-NET

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

počítač pro každého

prestižní magazín počítačových her
LEVEL

SECURITY 2001
Praha 7. června

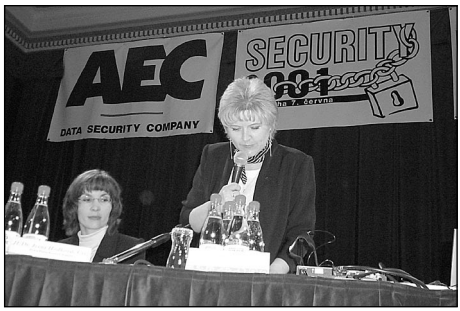


Poslední přípravy a začínáme!

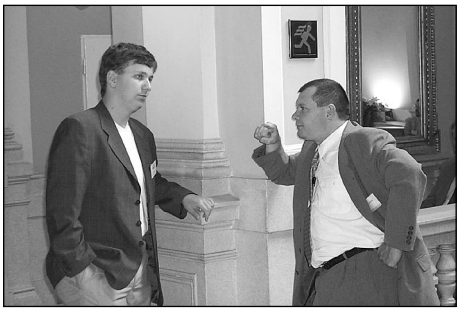
Zvládnout nápor stovek návštěvníků je úkol obtížný, nikoliv však nemožný.

Naplněný sál Národního domu na Vinohradech.

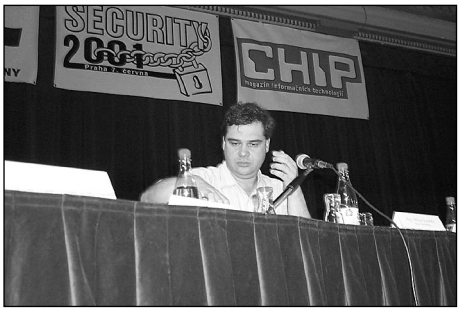
Účastníci odbaveni, začínáme!



Hovoří Ing. Alena Řezníčková z pořádající společnosti AEC.

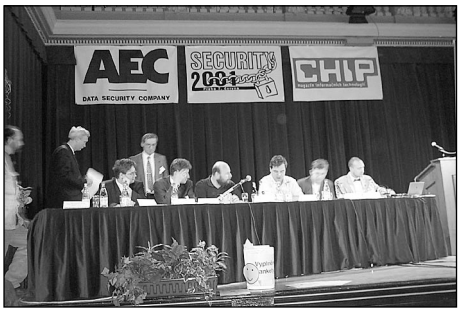


Igor Hák (**www.viry.cz**) a Jan Džubák (**www.hoax.cz**).



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.

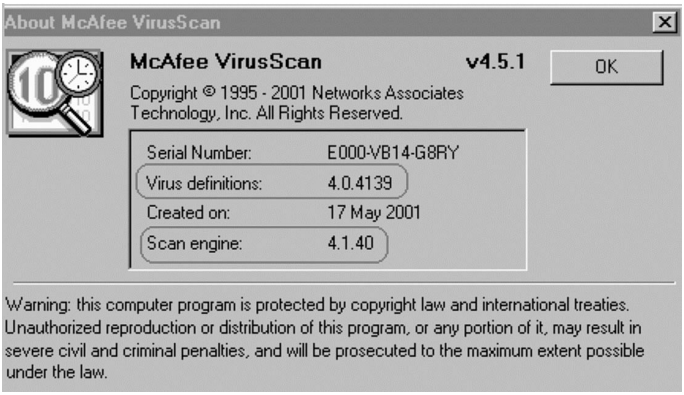
Ideálním stavem je po výšeu vedených informacích stav, kdy vlastníte nejnovější verzi antivirového programu s poslední aktualizací - a to jak update, tak upgrade. Pro přenos aktualizací na daný počítačový systém ze zdroje na Internetu je snad nejčastěji využíván protokol FTP, ať už prostřednictvím anonymního 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

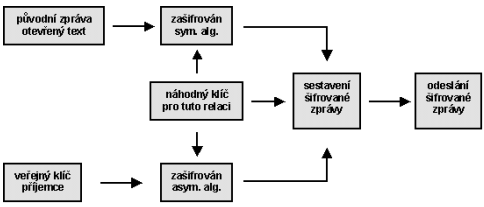


Představení programu PGP

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:

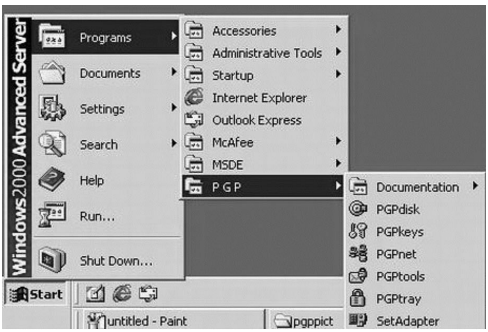
- šifrování (e-mailu, souboru na disku)
- ICQ komunikace
- elektronický podpis (e-mailu, souboru)
- bezpečné mazání souboru
- vytváření „samodešifrovacích“ souborů
- správa soukromých a veřejných klíčů
- klient VPN (Virtual Privat Network)
- personální firewall a IDS (Intrusion Detection Systém = detekce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

Jednotlivé moduly PGP Desktop Security:

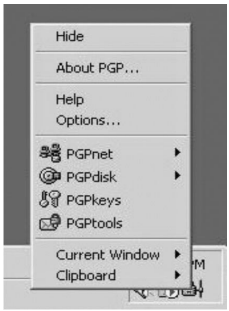
- PGPmail and PGPfile Encryption
- PGPdisk Encryption
- PGPfire (Personal Firewall Protection and Intrusion Detection System)
- PGPnet VPN Client
- PGP Desktop Manageability Tools (PGPadmin, PGP Certificate server)

K jednotlivým funkcím programu PGP se uživatel dostanete třemi způsoby:

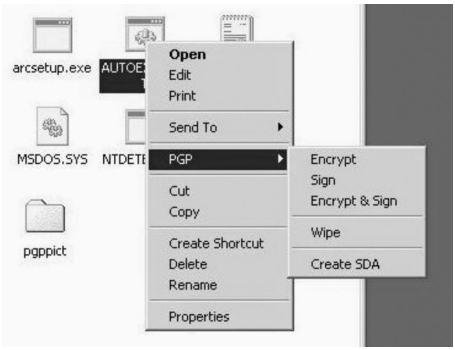
1) prostřednictvím nabídky „Start“



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



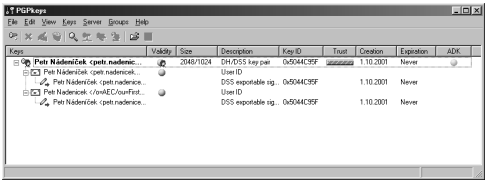
3) pomocí kontextového menu (při kliknutí pravým tlačítkem myši na soubor)



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“.

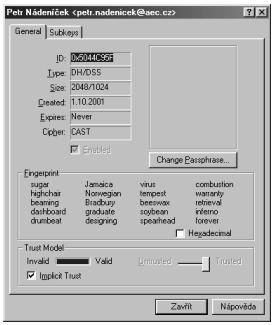
Nejdůležitější součástí PGP je bezesporu správa klíčů a jejich certifikátů - "PGP Keys". V PGP 7.03 lze používat certifikáty jak ve formátu PGP, tak i ve formátu X.509.

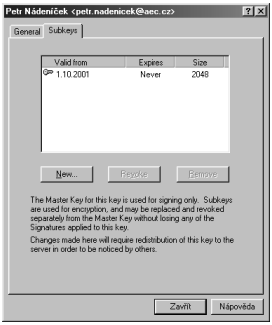
Vytváření nových klíčových párů je možno pomocí speciálního průvodce (wizardu), který uživatele bezpečně provede všemi úskalími. Po uživateli jsou



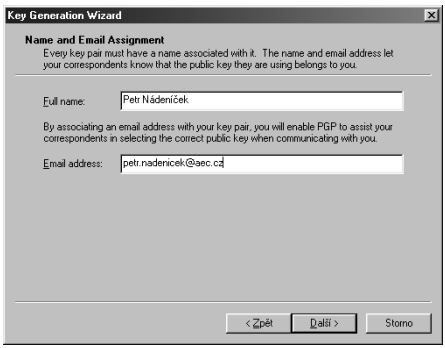
postupně vyžadovány následující údaje: jméno, e-mailová adresa a vstupní fráze. Klíče (certifikáty) jsou spravovány pomocí „PGP Keys“.

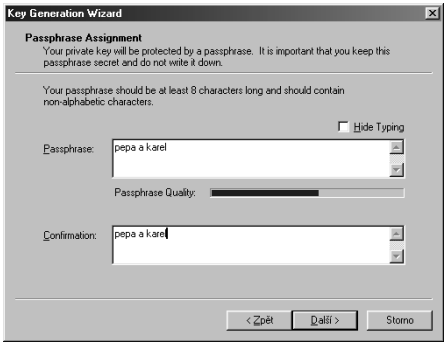
Pokud jste novým uživatelem PGP (tzn. bez vytvořených klíčů), bude po instalaci spuš-těn pomocník pro jejich generování. V opačném případě, či je-li třeba provést nějaké úpravy, je pomocník dostupný z programu PGP keys (Generate New Keypair). Při generování nového klíčového páru budete dotázáni na jméno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

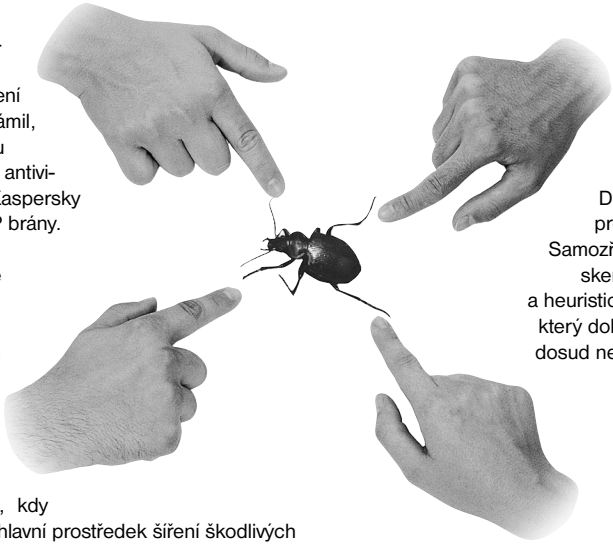
Při zadávání fráze je indikována kvalita hesla (Passphrase Quality), která odráží její složitost. Zkušení uživatelé mohou nastavit typ klíče, jeho délku a dobu platnosti a použitý algoritmus.

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