AEC
DATA SECURITY COMPANY

# Bulletin

www.aec.cz, www.trustcert.cz

březen/2002

## OPRAVDU BOHATÁ VELIKONOČNÍ NADÍLKA

# Úvod

Milí přátelé!

Jak jste si už možná všimli (nebo v příštích nejbližších okamžicích všimnete) tento bulletin „přibral“ čtyřstránkovou přílohu, která má jednu zvláštnost - je v anglickém jazyce. Její vznik sleduje několik cílů - jednak zvýšit znalosti anglického jazyka v oblasti počítačové bezpečnosti a jednak vám předat některé informace přímo od našich zahraničních partnerů „v původním znění, bez titulků“ (tedy v podobě nezkreslené překladem).

Věříme, že tento počin zvýší atraktivitu, užitnou hodnotu i zajímavost bulletinu AEC.

Tomáš Přibyl
tomas.pribyl@aec.cz

**Obsah:**




©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 opět na CeBITu!

**Stejně jako v předchozích letech, s výjimkou loňského roku, nebudeme ani letos chybět na mezinárodních veletrzích a výstavách. Po roční pauze, vzniklé prodejem produktu IronWare® Security Suite spolu s částí vývojového oddělení norské firmě Norman ASA, se společnost AEC představila na mezinárodním veletrhu informačních technologiích CeBIT.**


CeBIT 2002 se konal v termínu od 13. do 20. března v německém Hannoveru pod heslem „Get the spirit of tomorrow“. Vystavní expozici AEC bylo možné nalézti v hale číslo 17, která byla celá věnovaná bezpečnosti, na stánku 25A.

Vývojové oddělení AEC zde představilo na dvou předváděcích stanovištích nová bezpečnostní řešení, mezi které náleží (podobnější informace - viz str. 16 a 17):

**TrustPort CA** - produkt věnovaný outsourcingu certifikační autority.

**TrustPort Encryption** - software pro off-line šifrování a dešifrování souborů a adresářů na EPOC a PC.

**TrustMail** - aplikace zajišťující bezpečnost elektronické pošty, na bázi šifrování a elektronického podpisu.

**DataShredder**
- „skartovačka“, která zajišťuje neobnovitelné a bezpečné smazání souborů, archivů nebo pevného disku.

Návštěvníci expozice měli k dispozici kromě výše uvedených dvou předváděcích míst také informační stanoviště a prostory k jednáním. Zajímavostí připravenou pro uvedení nových bezpečnostních řešení na trh byly přitažlivé zaváděcí ceny.

Rádi jsme se s Vámi na CeBITu setkali! A v případě, že jste neměli možnost CeBIT navštívit, rádi se s Vámi setkáme při osobním jednání, nebo zašleme informační materiály.



# Znalosti a vzdělávání

Odborné znalosti velmi rychle zastarávají. Obecně v intervalu tří let, v informačních technologiích daleko dříve, někdy už v intervalu jednoho roku.

A paradoxně k tomu jsou základním zdrojem růstu společnosti a budou čím dál více. Jsou a budou firemním know-how, a tak je vzdělávání po celou dobu profesní kariéry nutností. Nesděluji tímto žádnou novinku a také většina společností podle toho jedná. Investuje do vzdělávání svých zaměstnanců. I přesto, že to může pro ni být ekonomicky náročné, a i přesto, že migrace pracovníků, a to zejména v IT je vysoká. Obojí je práce personalisty a managementu ve společnosti a je nutné zajistit toto vzdělávání zaměstnanců především efektivně.

Takové efektivní vzdělávání právě pro naše klienty připravujeme v oblasti bezpečnosti informačních technologií.

## Jaké jsou možnosti vzdělávání?

Vzdělávání je obvykle realizováno formou pravidelného prezenčního studia nebo jako distanční vzdělávání. Prezenční studium přenecháme vzdělávacím subjektům, kterými jsou například školy, a budeme se zde věnovat distančnímu studiu dospělých. Studující může přijímat informace ze zdroje pasivně, dnes tak činí nejraději z Internetu, nebo aktivně, kdy je vytvořen komunikační kanál mezi studujícím a tutorem, eventuelně mezi účastníky studijní skupiny, třeba v on-line diskusní skupině.

U aktivního distančního vzdělávání se nabízí několik typů: řízené samostudium, interaktivní programy na různých nosičích ( magnetofonové, magnetoskopické záznamy, diskety či CD, rozhlasové a televizní programy, telefonické, e-mailové vzdělávací programy, video konference), kvalifikační a rekvalifikační kurzy, e-learning.

Tady si dovolím učinit malou vsuvku k pasivnímu vzdělávání a připojuji vtip, který vyjadřuje charakteristiku naší české povahy v kladném slova smyslu:

„Byl proveden průzkum, za jak dlouho se Čech, Angličan a Američan naučí japonsky. Angličani jsou zaskočeni, nicméně prohlásí, že japonština je opravdu těžký jazyk a že potřebují minimálně dva roky. Američani sice kroutí hlavou, ale nakonec řeknou, že tak nejméně rok by potřebovali. Čech s trochu zarudlýma očima se ptá: Prosím vás, a jsou na to skripta? Anglická určitě, dostane se mu odpovědi. A Čech tedy po zaváhání odpoví: No, a stačilo by to pozítří?“

Jak je vidět, hlavičky nás Čechů jsou schopné se vzdělávat a hladové po informacích, a to je velmi příznivé jak pro zaměstnavatele, tak pro vzdělávající společnosti - pro nás.

## Vzdělávací projekt AEC

AEC zřizuje v tomto roce centrum vzdělávání zaměřené na bezpečnost IT. Zaměříme se na poslední dva typy aktivního distančního vzdělávání - kvalifikační a rekvalifikační kurzy, e-learning.

Připravovaná nabídka vzdělávacích programů zahrnuje komplexní nabídku informační bezpečnosti od virové a antivirové problematiky, přes kryptologii a kryptografii, elektronický podpis a certifikační autoritu, legislativní rámec problematiky, normy a standardy, právnický pohled na bezpečnost, využití v e-komerci, zabezpečení LAN a WAN a mnoho dalších témat. Je určena začátečníkům, pokročilým nebo kombinuje teoretické lekce s praktickým trainingem. Oslovuje uživatele, administrátory IT, manažery.

Naše první kroky v tomto projektu „vedly“ na Ministerstvo školství, mládeže a tělovýchovy, které jsme požádali o akreditaci na rekvalifikační kurz Bezpečnostní manažer v IT. Tuto akreditaci jsme získali 17. prosince 2001 a absolventi kurzů mohou od nás odcházet s kvalifikací manažera bezpečnosti IT s certifikátem s akreditací MŠMT.

## Co nás k tomu vede?

Průzkum trhu ukázal, že je odzvoněno kurzům nabízejícím základní dovednosti v oblasti obsluhy PC. Poptávka klesá proto, že za posledních deset let se informační technologie rozšířily téměř na všechna pracoviště a do mnohých domácností, je tedy se koho zeptat na radu nebo požádat o pomoc. Navíc do pracovního procesu přichází mladá generace, která si s sebou nese tyto znalosti už ze škol. Naproti tomu roste poptávka po specializovaných kurzech, protože není v silách jedince proniknout opravdu do hloubky problému jen samostudiem. My máme již zavedené tradiční cykly seminářů a školení, a poptávka po nich je ze strany našich zákazníků stále větší. Zřízení centra vzdělávání AEC je tedy logickým vyústěním poskytování ucelených služeb našim klientům.

„Vždy můžete znát víc než ti druzí!“

Jitka Brandejsová

## Konference SECURITY 2002

Ani jsme se nenadáli, rok se s rokem sešel - a máme tu další konferenci věnovanou problematice počítačových virů a bezpečnosti dat vůbec, Security 2002. Proto si nezapomeňte do svých diářů poznačit datum **6. června (čtvrtek)**, kdy se tato již tradiční akce (víte, že její první ročník pod názvem Virus 1992 proběhl právě před deseti lety?) uskuteční na neméně tradičním místě - v Národním domě na Vinohradech.

Co vám můžeme slíbit? Totéž, co v letech minulých a opět něco navíc. Spoustu zajímavých a aktuálních přednášek (vzhledem k tomu, nemáme všechny definitivně potvrzené, zatím není jejich seznam veřejný) od IT security specialistů z českých i zahraničních firem. Oficiální i neoficiální diskuse a setkání. Raut pro všechny účastníky. A to vše pod záštitou odborného garanta (AEC Data Security Company) a mediálního partnera, kterým je Vogel Publishing (Chip, Počítač pro každého, Level, Media shop, IT Net).

Pro bližší informace sledujte **www.aec.cz**, event. pište na e-mailovou adresu **seminar@aec.cz**

## Ples Domova sv. Markéty

Letošní plesová sezóna je pomalu za námi. Pomalu přichází jaro a první vydatnější sluneční paprsky, které nás hřejí na těle. My ale máme i další důvod k zahřátí - tentokrát na duši. Osmého února 2002 se totiž uskutečnil ples Domova sv. Markéty v Brně (zařízení poskytující azyl matkám s dětmi, které se ocitly v tísni), do jehož přípravy se pověstnou „troškou do mlýna“ zapojilo i AEC. Ta příslovečná „troška“ (nezapomínejte ale, že „nemusí pršet, stačí, když kape") měla podobu cen věnovaných do tomboly. Jsme rádi, že se v dnešní hektické době najdou lidé, kteří se dokáží zastavit a věnovat druhým. A že k nim (alespoň doufáme) patříme.


PODĚKOVÁNÍ

Ing. Klára Vlachová
ředitelka Domova

V Brně dne 20.2. 2002



# Setkání s partnery AEC - narodila se nová tradice

AEC má jedenáctiletou tradici svého trvání, má přibližně desetiletou tradici setkávání se se svými zákazníky a teď má AEC také dvouletou tradici setkávání se s partnerskými společnostmi.

Tradice je slovo, které pro mnohé má více či méně „familierní“ nádech a často se jako tradice vybaví lidové kroje, velikonoční zvyky nebo oslava Nového roku. Partnerský den sice nemá se žádným z těchto zvyků nic společného, protože my se nepřevlékáme do krojů, nevyplácíme pomlázkou a neholdujeme alkoholu, ale zažíváme podobný příjemný pocit z nadcházejícího setkání a těšíme se, že se nám podaří navodit neméně slavnostní pocit u našich partnerů. Nejde jen o prezentaci AEC, o předvedení novinek a vysvětlení strategických záměrů, ale jde, a to hlavně, o osobní setkání a poznání se mimo každodenní pracovní shon. Protože dnešní e-mailová komunikace navzdory tomu, že nám přináší mnoho dobrého, způsobuje anonymnost mezi komunikujícími stranami, a tak je Partnerský den jedním z prostředků, který toto napravuje.

Tradičně nás touto akcí také doprovází mediální partner PC World.

Druhý partnerský den měl s Prvním mnoho společného: konal se ve stejném kalendářním měsíci - v únoru, konal se ve stejných prostorách Národního domu na Vinohradech, a byl určen k neformálnímu setkání s partnery stejně jako předchozí rok. Zkušenosti z Prvního partnerského dne nám vnukly mnoho nových myšlenek pro jeho zpestření a zlepšení. A tak se Druhý partnerský den od prvního odlišoval například programem.

Nejprve jsme se přivítali s mnoha známými i novými tvářemi. Tomáš Přibyl zahájil a uvítal všechny přítomné úvodním slovem. Své „ovečky“ pozdravila také Jitka Brandejsová, která se společně s dalšími kolegyněmi Andreou Koláčkovou a Helenou Ciprysovou partnerům věnuje celoročně. Ve své prezentaci zhodnotila rok 2001 a přednesla možnosti partnerské spolupráce, nabídla mimo jiné využití diferencovaných partnerských programů. Tím byla linie roku 2002 týkající se společné práce řečena a už následovaly konkrétní produktové prezentace. Zbrusu nové produkty a projekt Elektronické podatelny představil Jaromír Klimek. S projektem vzdělávacího střediska a rekvalifikačních kurzů předstoupila Jitka Brandejsová.

Poutavou přednášku o antivirovém produktu F-Secure Anti-Virus měl kolega Tomáš Vobruba, o němž žádný z účastníků nepochyboval, že je mu jeho práce koníčkem. Jeho hodinová přednáška byla nabita informacemi a vyvolávala neformální komunikaci s nadšenci z řad posluchačů. Bylo proto nadlidským úsilím uzavřít dopolední část a věnovat se obědové přestávce ve formě rautu. Není možné v tomto místě přejít okamžitě k odpolednímu programu Partnerského dne a vynechat tuto část. A tak se chvíli rozplývejte nad jídlem s námi: v teplé kuchyni se kuřecí kapsa na talířích střídala s hovězím gulášem a americké brambory s bramboráčky. Prostory dekorovaly mísy vybraných lahůdkových salámů a voňavých sýrů, milovníci sladkého mohli okusit minivětrníky (setkali jsme se tu s označením „ventilátorky") a další z bohatého výběru zákusků. Ani dietáři nemuseli stát zkroušeně opodál, ale mohli se věnovat salátům, čerstvé zelenině či ovoci.

A bezprostředně poté už syté účastníky lákala v další prezentaci Hana Stojanová na neméně zajímavé jak vzdělávací tak společenské události připravované v roce 2002 a ujistila partnery o marketingové podpoře pro jejich, resp. naše společné zákazníky, nabídla jim různé formy podpory prodeje.

Vydavatelství PC Worldu IDG představil pan Patrik Malina a přednáškou o možných virových nebezpečích v tomto roce „Viry roku 2002“ charakteristicky uzavřel Tomáš Přibyl.

Celý den vyvrcholil slavnostním předáváním cen, a na tuto část jsme se opravdu těšili. Odměnit nejlepšího prodejce zájezdem dle vlastního výběru v hodnotě dvaceti tisíc korun, koženými či sportovními výrobky také dle vlastního výběru, značkovými hodinkami anebo značkovým alkoholem bylo příjemnou tečkou za letošním setkání partnerů. Zasloužili si to. Těch, co nevyhráli, nám bylo líto, a tak každý ze zúčastněných obdržel kromě materiálů, časopisu, CD i keramický hrnek s logem AEC.

Vše příjemné jednou skončí a tak skončil 14. února 2002 i Druhý partnerský den AEC. Těšme se tedy na Třetí!

Jitka Brandejsová

# Semináře v Uherském Hradišti a Slavičíně


Na „Dni elektronického podpisu“ postupně zazněly následující přednášky:

- **Proč elektronický podpis?**
- **Technologie elektronického podpisu**
- **Certifikáty a certifikační autority**
- **Elektronický podpis v praxi**
- **Zákon o elektronickém podpisu**
- **Časové značky u elektronických podpisů**

Přesně před rokem - v březnu 2001 - jsme v reakci na vlnu zájmu o problematiku elektronického podpisu uspořádali ve spolupráci s redakcí měsíčníku PC World akci nazvanou „Den elektronického podpisu“.

Jednodenní seminář určený pro nejširší veřejnost byl zaměřený na seznámení se s celou problematikou elektronického podpisu. Od úvodního zodpovězení otázky „proč vůbec potřebujeme elektronický podpis“ přes vysvětlení jeho technologie a standardů přes problematiku certifikátů až po legislativní „podhoubí“ v České republice.

V průběhu března 2002 jsme pro velký zájem našich partnerů celý seminář zopakovali - v Uherském Hradišti a ve Slavičíně. Stejně jako před rokem přednášeli specialisté z AEC, stejně jako před rokem byl mediálním partnerem měsíčník PC World - a stejně jako před rokem se akce setkala s nemalým zájmem posluchačů (alespoň v Uherském Hradišti - seminář ve Slavičíně je v době uzávěrky teprve před námi).

O tom, že problematika elektronického podpisu je stále zajímavá, svědčilo i velké množství dotazů nejen v průběhu závěrečné diskuse, ale vlastně po každé přednášce i při neoficiálních setkáních v průběhu celého dne.

### UHERSKÉ HRADIŠTĚ, 7. března 2002

Seminář s názvem „Den elektronického podpisu“ uspořádala Okresní hospodářská komora v Uherském Hradišti ve spolupráci se společnostmi AEC Brno a CAMO Slavičín dne 7. března 2002. Seminář se uskutečnil v hotelu Grand v Uherském Hradišti. Bližší informace najdete na www.uh.cz/ohk

### SLAVIČÍN
### 28. března 2002

Seminář s názvem „Den elektronického podpisu“ pořádá město Slavičín ve spolupráci se společnostmi AEC Brno, CAMO Slavičín a Vojenským technickým ústavem výzbroje a munice ve Slavičíně dne 28. března 2002. Bližší informace najdete na www.mesto-slavicin.cz

# AEC slavilo jedenáct let své existence

Dne 8. února 2002 se u příležitosti jedenáctého výročí založení společnosti AEC uskutečnil, stejně jako v minulém roce, společenský večer, tentokrát spojený s inscenací autora Francise Vebera nazvanou Blbec k večeři.

První pozvaní návštěvníci se v Divadle Bez zábradlí začali objevovat chvíli před půl sedmou večer. Hned u vchodu jim kolegyně z obchodního a marketingového oddělení, které pro dnešní večer zastávaly úlohu hostesek, předaly originální perníkový los do tomboly v podobě počítačové diskety. Po nezbytném odevzdání svrchního ošacení v šatně divadla si hosté mohli ve zbytku času vychutnat přípitek na uvítanou.

Přesně úderem sedmé hodiny večerní zahájila paní ředitelka AEC Ing. Alena Řezníčková svým úvodním projevem oficiální část večera. Přivítala všechny přítomné hosty i zaměstnance společnosti a v krátkosti shrnula základní vize a filozofii společnosti AEC. Pak již nic nebránilo tomu, aby začalo samotné představení. V hlavní roli se představil herec Václav Vydra, který po celou dobu na jevišti přímo exceloval. Jeho shrbená postava postižená houserem byla více než věrohodná. Neméně humornou podívanou divákům připravili i další představitelé, mezi nimiž byli Jiří Menzel, Rudolf Hrušínský a Naďa Urbánková. Hra pojednávala především o tématech mezilidských vztahů a lidské blbosti, která se ve hře stává zdrojem mnohých nedorozumnění a dlouhé řady překvapivých zápletek. Podle častých výbuchů smíchu v hledišti se dalo soudit, že se představení divákům velmi líbilo.

Po skončení představení následoval další zajímavý bod programu - losování tomboly. Ceny tvořilo několik obřích lahví kvalitního perlivého vína domácí provenience, o které zvláště někteří hosté jevili nebývalý a očividný zájem. Vyhrát však mohli jen někteří. Pro ty, kteří nevyhráli, mohlo být náplastí následné bohaté pohoštění, které se podávalo přímo v přilehlých prostorách divadla. Kdo ochutnal uzenou šunku nebo výborné moravské víno, jistě mi dá za pravdu! Atmosféra závěrečného rautu je také jistě dobře patrna z některých fotografií.

Jak šel čas, hosté postupně vyklízeli stoly s pohoštěním a posléze i prostory divadla. To, že vyklízení nebylo až tak rychlé svědčilo o tom, že akce byla úspěšná a hostům se, i dle jejich vlastních slov, nesmírné líbila. A co říci na závěr? Snad jen to, že příště budeme muset akci uspořádat ve větším divadle…

Petr Nádeníček

# Předvánoční setkání a nadílka

Co si představíte pod pojemem Mikuláš? Někdo staré české jméno, dnes již používané jen výjimečně. Někdo zážitek z dětství, kdy se schovával za rodiče před strašlivě vypadajícím čertem. A někdo vhodný důvod k oslavě.

Zákazníci, partneři a spřátelené duše nakloněné společnosti AEC si od 4. prosince loňského roku představí pravé Peklo.

Tuto velmi příjemnou, útulnou restauraci s veskrze mikulášským názvem Peklo jsme objevili v areálu Strahovského kláštera v Praze, hluboko pod zemí v prostorách starobylých vinných sklepů. Už jen to jméno! Dva diametrálně odlišné světy, klášter versus peklo. To jsme přece nemohli přejít bez povšimnutí!

A tak se zrodila myšlenka uspořádat namísto obligátních firemních vánočních večírků v posledním pracovním týdnu, kdy většina z přítomných už je duchem u své rodiny a vanočních svátků, večírek v prvním adventním týdnu, jako morální vzpruhu do vánočního maratonu, jako poděkování za přízeň v právě končícím roce a konečně jako možnost se společně sejít a strávit příjemný večer nad sklenkou ušlechtilého moku.

Podařilo se! I přes mimořádně studené a deštivé počasí se sešlo více než osmdesát hostů, doprovázených partnerkami i partnery. Po kratičkém a neformálním uvítání ředitelky společnosti Ing. Aleny Řezníčkové se hosté odebrali dílem k rautovým stolům a dílem na taneční parket. I přes počáteční ostych se cimbálové hudbě, importované z jižní Moravy, podařilo navodit uvolněnou atmosféru. Lidovým písničkám hraným na přání hostů se odolávalo opravdu obtížně a pak, ne nadarmo se říká, že „každý správný Pražák je vlastně původem z Moravy“. Nedovolím si jmenovat, ale přiznávám, že nekteří z přítomných pánů ředitelů a manažerů by se se ctí mohli vydat na dráhu profesionálních tanečníků nebo zpěváků.

Po přestávce, ve které se podávala večeře formou teplých i studených švédských stolů byla losována tombola z vizitek odevzdaných hosty na počátku večera. Vylosovaní šťastlivci si odnášeli ceny tekuté, poživatelné, a protože byl Mikuláš, také hořlavé - tzn. kvalitní alkohol, čokoládové mikuláše, čerty a anděly a dřevěné uhlí. I když tombola byla bohatá, nemohlo se dostat se na všechny, a odcházet z mikulášského večírku bez nadílky, to by nebylo to pravé. Proto dostali všichni přítomní hosté ještě dárek na odchodnou - a jak jinak než tekutý. Večírek končil za všeobecné spokojenosti hluboko po půlnoci, dokonce došlo i na děkovné dopisy.

Přiznám se, že mne to nesmírně těší.

Věřím totiž, že na rozdíl od typizovaných marketingových kampaní, pomáhají tato osobní setkání pochopit, že na obou stranách pomyslné „obchodní“ barikády stojí živí lidé. Lidé se svými pozitivy i negativními stránkami, lidé, kteří mohou nalézt společnou řeč a vzájemně si porozumět. A zdaleka ne jen v data security.

Hana Stojanová

# Mikulášská besídka Strahovský klášter 4. prosince 2001

Tajuplný strahovský klášter Vás vítá…

Odevzdejte navštívenku, bude se losovat…

Losujeme!


Hrajeme k tanci i k poslechu.

Předvánoční shon si na besídku cestu nenašel.

## Cross-Site Scripting vulnerabilities: what they are and how to prevent them

***„Whenever, therefore, people are deceived... it is clear that the error has slid into their minds through the medium of certain resemblances to that truth."***

Socrates (469-399 B.C.); Greek philosopher.

Madrid, March 8 2002 - The Computer Emergency Response Team Coordination Center -CERT/CC-) has published an interesting article(*) explaining Cross-Site Scripting vulnerabilities, and offering practical advice on how to deal with them.

Cross-Site Scripting (CSS) vulnerabilities center on the possibility for an attacker to make a legitimate web server send a page with harmful code in response to a request. So for example, when a user clicks on a link that points at a bank's web page, they could receive a false web page prepared by the attacker to resend any information entered (passwords, credit card details etc.). In this way, the user might enter any amount of confidential data, completely unaware that they are in fact sending this information to an intruder.

One of the most frequently used techniques consists of constructing links with script 'injected'. Along the lines of the example above, when the user clicks on the link, they would in fact be sending the injected code to their bank along with the request.

One of the preventive measures that can be taken is to always go directly to sites in which you may enter sensitive information, not via links from potentially untrustworthy sites or from HTML e-mails.

Webmasters can also contribute by ensuring that none of their web pages reply to requests that have not been validated. More sophisticated measures include the use of „signed scripting", which would prevent any code that was not digitally signed from being executed.

(*) The CERT/CC article is available at: http://www.cert.org/archive/pdf/cross_site_scripting.pdf.

## Seventh ICSA Labs report on virus incidents

***„Learn as though you would never be able to master it; hold it as though you would be in fear of losing it."***

Confucious (551-479 BC); Chinese philosopher.

Madrid, March 6 2002 - According to a survey released by ICSA Labs, around 1.2 million virus incidents affected the 300 American companies taking part during the 20 month period in which the survey was carried out.

The survey, also reported by CNN indicates that since ICSA Labs began compiling the data in 1996 there has been a monthly rise of some 20 infected machines per thousand.

Along with the fact that e-mail is still the principal means of virus propagation, the ISCA study also highlights the increasing risk factors inherent in new technologies. On example given is Nimda, which uses four different methods to infect computers with Windows 95, 98, Me and 2000, as well as Windows 2000 servers. This worm spreads by sending e-mails with infected attached files and then scanning for and infecting vulnerable web servers.

During the survey ICSA Labs reported that 28 percent of companies were hit by a virus 'disaster' -affecting 25 or more servers or PCs-. This figure has dropped with respect to the previous survey which recorded a figure of 51 percent.

The seventh annual ICSA Labs report also mentions that companies are beginning to take protection more seriously. The survey found that now 84 percent of participating companies had protected e-mail servers, 51 percent had protection for firewalls and 45 percent had antivirus protection in proxy servers. These figures contrast sharply with those of the previous survey, in which respondents had little or no protection for network services such as firewalls, etc.

The ICSA Labs was carried out between January 2000 and August 2001, with a sample group of 300 organizations. The report was sponsored by Panda Software.

# Norman Virus Control to cover MS Exchange 2000

The data security company Norman ASA have today announced the availability of Norman Virus Control version 5 for MS Exchange 2000.

Today most computer viruses spread through e-mails. Such viruses should already be detected and removed on the e-mail server to prevent that misuse leads to virus infections. The receiver of the virus might have forgotten to update the antivirus software and even turned off the antivirus product. It is therefore essential to have updated antivirus software on a central server in the network.

## Norman Virus Control for MS Exchange 2000

Norman Virus Control for Exchange 2000 uses an AVAPI 2.0 plug-in which connects to the Exchange Information Store on the server for access to emails and attachments. NVC for Exchange 2000 becomes an integrated part of Exchange itself.

## On-access scanning

All incoming and outgoing emails are scanned on access in both private and public information stores. Access is only granted to virus-free items or when a present virus has been removed. Each element of the email is scanned separately on-access. I.e. the attachment and the mail body are scanned individually. Access to an email is only granted if all elements are virus free.

## Updating virus definition files and scanner engine

Norman Internet Update (NIU) can be configured to automatically check the availability of new definition files dynamically and without any user interaction at any interval that you choose. Thus NVC for Exchange 2000 is automatically kept up-to-date offering customers the best levels of protection at all times.

-The rapid growth in malware infections through email has meant that scanning on the email server is therefore crucial.“ States Bjorn A. Windfeldt, VP Marketing, Norman ASA. „This solution integrates with Microsoft Exchange 2000 to ensure that all traffic passing through the Exchange 2000 server is scanned for malicious code.

# Norman Virus Control to cover Lotus Domino

The data security company Norman ASA have today announced the availability of Norman Virus Control version 5 for Lotus Domino.

Most companies are connected to the Internet, and email is a common communication method. However, email has also been the most common way for spreading malicious programs (viruses, worms etc.). The need for scanning for malware on the email server is therefore crucial. Norman Virus Control v5 (NVC v5) for Lotus Domino is a virus scanner that integrates with Lotus Domino to ensure that everything that passes through the Domino server is checked for viruses, trojans, and other malicious code

## Scanning

All incoming and outgoing e-mails are scanned on access. Documents that contain file attachments will be scanned for possible infections. Access is only granted to virus-free items or when a present virus has been removed. Infected documents can be cleaned, stopped, stopped if not cleaned, or logged only, all depending on user settings. NVC v5 for Lotus Domino protects the 3 main entree points for viruses on this platform using real-time scanning;

- E-mail attachments
- Database replication
- Database access

Updating virus definition files and scanner engine through Norman Internet Update

Updated virus definition files, scanner engine, or NVC v5 modules are available for download by Norman Internet Update.You can configure NVC v5 to look for updates automatically and by doing this, NVC v5 for Lotus Domino updates itself dynamically and without any user interaction.

# F-Secure Anti-Virus Technology To Be Integrated With CyberGuard Firewall/VPN Appliances

**Combined Gateway Solutions Protect Users From Increasing Number of Internet-borne Threats**

## Helsinki, Finland - January 29, 2002

F-Secure (HEX: FSC), a leading provider of centrally managed security for today's mobile, wireless enterprise, and CyberGuard (OTC: CYBG), a leading vendor of enterprise and electronic commerce security solutions to Fortune 1000 companies and governments worldwide, today announced that the F-Secure's anti-virus technology will be integrated with CyberGuard's family of firewall/VPN appliances.

Products developed under the new partnership will provide networks with unparalleled protection, at the gateway or intended point of entrance, against viruses, worms, Trojans, and other forms of threat that attack enterprises.

By incorporating F-Secure's Anti-Virus for Firewalls technology into its CVP-compliant solution, CyberGuard is developing what is believed to be the only integrated anti-virus bundle that is sold, certified and supported by one vendor and that incorporates both gateway and firewall protections. The content vectoring protocol (CVP) is a mechanism for integrating anti-virus gateway solutions with firewalls.

"We were looking for an anti-virus solution that was proven, and with off-the-shelf interoperability with CyberGuard's own technology. Equally important, we required a partner with a reputation for excellent support," said Pat Wheeler, vice president of business development at CyberGuard. „F-Secure's technology stands above all the others, and combined with its frequent anti-virus signature updates, the decision was an easy one. We are pleased to be bringing this gateway solution to our customers."

Increased Internet connectivity has enabled viruses and other malicious code to spread faster than ever before, causing a huge amount of damages and untold costs. „In addition to protecting individual end devices using local anti-virus products, many problems may be avoided if the threats are removed already at the gateway level. This gateway protection is core to our strategy, and personifies CyberGuard's leading-edge solutions," said Ilkka Starck, Executive Vice President of North American operations for F-Secure. „We are delighted to be partnering with CyberGuard, it's a win-win for our companies and our customers."

F-Secure estimates that 90 percent of computer viruses arrive via email. Additionally, new kinds of complex and destructive viruses, worms and Trojans spread through Web surfing and file downloading. If a virus enters the corporate network, fighting against it can be very costly, difficult and time consuming. Virus infections often cause big financial losses because of network disruptions, decreased productivity, corrupted data and leaks of confidential information. Also, companies' reputations can be in danger if they spread viruses to business associates.

To minimize the costs and damages stemming from virus infections, scanning should ideally be performed at the perimeter of the corporate network. F-Secure Anti-Virus for Firewalls is a gateway level solution ensuring that viruses, worms and Trojans hidden in Web and file transfers and email attachments do not access or leave the corporate network. If a virus is found while employees transfer and receive files, use email, or even browse the Web, the files can be automatically disinfected before they are allowed to traverse through the firewall.

CyberGuard's firewall/VPN appliances incorporate multilevel security (MLS). MLS treats each layer of the secure operating system discretely, maintaining complete separation of network traffic from system components. This design removes access to the operating system from would-be hackers, creating a virtually impenetrable firewall environment. In December 2000, CyberGuard's appliances became the world's first to earn the Common Criteria Evaluation Assurance Level 4 certification, a rigorous security standard that is recognized by 15 countries around the world.

## About CyberGuard Corporation

CyberGuard Corporation, the technology leader in network security, provides enterprise and electronic commerce security solutions to Fortune 1000 companies and governments worldwide. CyberGuard's high-security, high-performance integrated firewall and VPN appliance products and services protect the integrity of data and applications

from unauthorized access. CyberGuard's appliances are the world's first to receive the rigorous information technology security certification Common Criteria EAL4, plus the first to enroll in Common Criteria evaluation assurance maintenance. The company has world headquarters in Ft. Lauderdale, Florida, regional offices in Europe and Asia, and a worldwide reseller network. More information on CyberGuard Corporation can be found at www.cyberguard.com.

### About F-Secure

F-Secure Corporation is a leading developer of centrally managed security solutions for the mobile enterprise. The company's award-winning, integrated anti-virus, file encryption and network security solutions for handhelds, laptops, desktops, servers, mail servers and firewalls provide centralized policy based management of widely dispersed user communities. Founded in 1988, F-Secure is listed on the Helsinki Stock Exchange [HEX: FSC]. Corporate headquarters is in Helsinki, Finland with North American main office in San Jose, California. The company maintains offices in Germany, Japan, Sweden and the United Kingdom, and is supported by a network of VARs and Distributors in over 90 countries around the globe.

KASPERSKY ANTI-VIRUS

## Our partners - Kaspersky

# Description of Myparty e-mail worm

**This is the worm virus spreading via the Internet being attached to infected emails. The worm itself is a Windows PE EXE file about 30Kb of length (compressed by UPX, 76K decompressed), written in Microsoft Visual C++.**

**The infected messages have:**

Subject: new photos from my party!
Body:
Hello!
My party… It was absolutely amazing!

I have attached my web page with new photos!

If you can please make color prints of my photos. Thanks!

Attach: www.myparty.yahoo.com

The worm activates from infected email only in case a user clicks on attached

file. The worm then installs itself to the system and runs spreading routine.

### Installing

While installing the worm copies itself to:
c:\regctrl.exe
- under WinNT/2K/XP

c:\recycled\regctrl.exe
- under Win9x/ME

and spawns this copy. In case the worm file name is not „.com“ (as in attach) but „.exe“ (the worm is renamed) it also opens the Web page „http://www.disney.com".

The original file (as it was run from infected email) is moved to Recylced or Recycler directory with one of names:

C:\RECYCLER\F-%1-%2-%3

C:\RECYCLED\F-%1-%2-%3

where %1, %2, %3 are random selected numbers, for example:

F-12158-19044-21300

F-27729-23255-31008

While installing the worm checks the keyboard layouot set, and in case there is Russian keyboard support the worm copies itself to Recycled/Recycler in the same way and exits. The same on any date except 25-29 January 2002.

As a result, the worm works only from 25 till 29 Jan 2002 and only on machines without Russian keyboard support.

### Spreading

To send infected messages the worm uses direct SMTP connection to email server. To get victim email addresses the worm scans WAB files (Windows Address Book) and *.DBX files (Outlook Express).

The worm also sends one email (without attach) to „napster@gala.net".

### Backdoor

Under WinNT/2000/… the worm also creates a new file in user's auto-run directory:

%Userprofile%\Start Menu\Programs\Startup\msstask.exe

and writes a backdoor program to there. This backdoor is being run by a data

that is stored in a file at the Web site „http://209.151.250.170".

### Known variants

**Myparty.b**

This one is slightly modified 'a' version. The differences are:
The attached file name is „myparty.photos.yahoo.com".

# „Blbec k večeři“ Divadlo Bez zábradlí 8. února 2002

Účinkující se pomalu scházejí.

Začínáme…

…a končíme. (Mezi těmito úkony byly samozřejmě dvě hodiny výborné zábavy.)

Po představení proběhlo losování výherců.

Ostatní se alespoň trochu občerstvili.

# DataShredder (DiscShredder)

Pro běžné uživatele počítačů je to problém mnohdy nepochopitelný. Ale je to skutečně tak: smazání dat na pevném disku počítače není tak jednoduchou záležitostí, jak by se na první pohled mohlo zdát.

Princip mazání dat na pevných discích počítačů je totiž poměrně triviální, neboť ve skutečnosti nedochází k fyzickému mazání celého souboru, ale pouze prvního znaku jeho jména. Smazaný soubor tak na disku stále fyzicky existuje a jeho obnovení je otázkou obnovení smazaného znaku jeho jména a vytvoření odkazu na tento soubor. Pro uživatele je sice „neviditelný“, ale jeho obnova není vůbec obtížná. „Smazaný“ soubor totiž na disku dále existuje až do svého náhodného přepsání jinými daty.

Právě neobnovitelné likvidaci dat na pevných discích počítače se věnuje produkt DataShredder. Princip jeho fungování je poměrně jednoduchý - vybraná data nebo oblasti na disku přepíše předdefinovaným řetězcem. Po několikanásobném přepsání se obnova původních informací stává zhola nemožnou.

DataShredder může mazat:

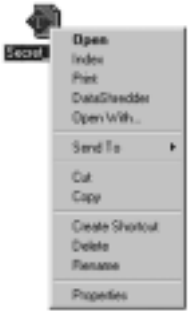
- soubory,
- složky,
- obsah odpadkového koše,
- Temporary Internet Files,
- dočasné (temp) soubory,
- cookies,
- volné místo na disku aj.

Možnost výběru bezpečného mazání dat je hned ze tří předdefinovaných metod:

- Metoda rychlá (quick). Vybraná data (oblasti) jsou přepsány náhodnými daty jen jednou. Rychlá a pro běžné použití dostačující.
- Metoda DoD. Tato metoda splňuje standardy pro likvidaci elektronických dat publikovaných americkou NSA (National Security Agency). Cílové místo je přepsáno celkem sedmkrát - metoda je pomalejší, leč výrazně bezpečnější.
- Metoda Petra Gutmanna. Při jejím zvolení dochází k 35násobnému přepsání vybraných dat - velmi pomalá, ale absolutně bezpečná metoda.

Speciální aplikací je pak DiscShredder - bootovací disketa, která slouží ke kompletnímu mazání celých počítačových disků. Její použití je vodné při vyřazování hardware nebo při potřebě odstraňování dat z celých médií.






**DataShredder v kontextovém menu.**

## TrustMail


Jedná se o aplikaci, která off-line šifruje a dešifruje data, např. přílohy e-mailových zpráv. Stejně tak je určena k vytváření a ověřování elektronického podpisu. Program může být použit s jakýmkoliv poštovním klientem, neboť se jedná o samostatnou aplikaci.

Důležitou vlastností je též „multisigning" - možnost podepsání jednoho datového souboru více osobami.

**Podporované standardy**
Formát dat: PKCS7
Certifikáty: PEM, P7C
Klíče: P12

Je důležité, aby při komunikaci byl na obou stranách (jak u odesílatele, tak u příjemce) software podporující tyto standardy.

**Podporované algoritmy**

Asymetrické: RSA 1024 -4096, DSA 1024, ECC 192-256,

Symetrické: CAST 128, RC2 128 bits, BlowFish, DES, 3DES

HASH funkce: SHA1, MD5, RIPEMD 160


## TrustPort Encryption


Z bezpečnostního hlediska jsou handheldy ve stejné kategorii jako přenosné počítače - tedy velmi náchylné k odcizení nebo ztrátě. Vzhledem k tomu, že tak hrozí možnost přístupu k informacím nepovolaným osobám, je zapotřebí data chránit. Právě tento problém ošetřuje aplikace TrustPort Encryption.

Nutnost ochrany dat se ovšem netýká pouze možnosti odcizení či ztráty zařízení. Ne všechna data jsou veřejná a je zapotřebí je chránit též před nepovolanými osobami - to platí třeba při sdílení handheldu více uživateli nebo při jeho připojení do počítačové sítě.

TrustPort Encryption je unikátní zařízení sloužící k šifrování souborů, které využívá silné šifrovací/dešifrovací algoritmy. Zašifrovaná data lze v případě potřeby odšifrovat (samozřejmě při znalosti příslušného hesla) i na zařízení, které není vybaveno dešifrovacím programem - TrustPort Encryption totiž umožňuje vytvářet spustitelné soubory s vestavěnou dešifrovací funkcí.

Jako šifrovací algoritmus je použit CAST s délkou klíče 128 bitů. Vybrané soubory/adresáře mohou být zašifrovány do souboru s extenzí *.cph, který lze přenést na zařízení PDA (např. Nokia 9210). Zašifrovaný soubor je přitom kompatibilní nejen s PDA, ale také s PC.

# Zpráva o stavu škodlivých kódů

Lepší už to nebude. Bez jakékoliv nadsázky lze tímto mírně „optimistickým“ prohlášením hodnotit současný stav vývoje v oblasti počítačových virů. Přestože už několikrát v relativně krátké historii informačních technologií různí analytici prorokovali zánik těchto nežádoucích kusů programových kódů, opak je pravdou. Viry jsou stále tu - a daří se jim lépe než kdy dříve.

Odborníci na počítačovou bezpečnost se shodují, že co do rozmanitosti a počtu útoků škodlivých kódů byl právě uplynulý rok 2001 mimořádný. Prakticky nikdo přitom neočekává změnu nastoupeného trendu v roce 2002. A pokud snad ano, tak k horšímu.

Důvodů masového šíření škodlivých kódů (především pak počítačových virů) je několik. Uživatelské prostředí v informačních technologiích se výrazně unifikovalo, což znamená „bourání bariér“ pro vstup nežádoucího softwaru do počítače. Zároveň se také dramaticky rozšiřuje využití výpočetní techniky, přičemž nejvíce samozřejmě přibývá tzv. běžných uživatelů. Po takovýchto lidech samozřejmě nikdo nemůže chtít hlubší znalosti operačních systémů a používaných aplikací - pro ně je počítač pouhým pracovním nástrojem (i když trocha opatrnosti a dodržování bezpečnostních pravidel neuškodí nikomu).

V případě rozboru značného rozšíření počítačových virů se musíme podívat také na „druhou stranu barikády“ - na pisatele škodlivých kódů. Dávno pryč je doba, kdy výroba počítačového viru vyžadovala hluboké znalosti programování, síťové problematiky a dalších oblastí. Dnes není problém stáhnout si z webu utilitu na vytvoření počítačového viru dle zadaných parametrů (tzv. virové generátory) či jednoduše doplnit chybějící znalosti na různých „studijních“ stránkách na Internetu.

Takovéto masově vytvářené kódy samozřejmě nejsou nikterak mimořádně nebezpečné či nesnadno detekovatelné, ale objevuje se jich obrovské množství (dle statistik antivirových firem je to už kolem osmi set škodlivých kódů měsíčně).

V neposlední řadě „pachatelům“ virů nahrává i nedostatečné právní prostředí a jejich praktická beztrestnost. Ruku v ruce s tímto faktorem jde i Internet coby médium neznající hranic, což samozřejmě jakékoliv postihy nesmírně ztěžuje.

Počítačové viry, které se objevily v roce 2001, také v množství větším než obvyklém využívaly nejrůznějších bezpečnostních chyb a nedostatků (především aplikací MS Outlook a Internet Explorer). Pro průnik do počítače (resp. vykonání nežádoucí rutiny) přitom bylo v drtivé většině případů použito známých a zveřejněných bezpečnostních děr, na něž už byly k dispozici „záplaty“ (patche). Je to celkem logické - nač by se hackeři trápili s hledáním nových nedostatků, když těch známých je doslova nepřeberné množství a (ruku na srdce) málokterý uživatel/administrátor věnuje svůj čas a energii jejich odstraňování.

Do podobné kategorie patřil i škodlivý kód CodeRed, který se začal šířit v polovině července 2001 a postupně samočinně napadl statisíce serverů na celém světě. Jedná se o internetového červa, který se šíří mezi servery Windows 2000 s IIS (Internet Information Services) a MS Index Server 2.0 nebo Windows 2000 Indexing Services. Využíval přitom bezpečnostní chybu „Unchecked Buffer in Index Server ISAPI Extension", která byla detailně popsána v Microsoft Security Bulletin MS01-033 vydaném 18. června 2001. („Záplatu“ na tuto chybu lze stáhnout z p://www.microsoft.com/technet/security/bulletin/MS01-033.asp.)

Fungování červa CodeRed je následující: Vyhledává počítačové severy a mezi 20. a 27. každého měsíce se pokouší z napadených serverů „útočit“ na webovskou stránku www.whitehouse.gov (oficiální doména americké vlády - pozor, nezaměňovat s doménou www.whitehouse.com, což je pornografická stránka!). A vždy od 1. do 19. každého měsíce se snaží rozšířit na co nejvíce serverů. Z každého napadeného stroje se přitom pokouší náhodně nainstalovat na 99 dalších - vzhledem k tomu, že „opravování“ bezpečnostních děr se příliš část nepraktikuje, má CodeRed velkou pravděpodobnost, že se mu na těchto serverech podaří uchytit. A z každého nově napadeného se rozšíří na 99 dalších atd. Jde tedy o jakýsi princip „letadla“.

A ještě pár slov k provedení „útoku“. Ten je veden metodou DDoS (Distributed Denial of Service). Její podstata spočívá v tom, že na jeden určený server (v daném případě internetový server vlády USA) je v jednom okamžiku vysláno takové množství nejrůznějších žádostí, že je není možné zvládnout. Server je pak přetížený a kolabuje. Metoda DDoS se vyznačuje tím, že útok je veden z velkého množství počítačů. (Vzhledem k tomu, že každá internetová

adresa má svou unikátní IP adresu, stačilo správcům www.whitehouse.org tuto hodnotu změnit a jejich server je v bezpečí před účinky kódu CodeRed. Ten se nyní pokouší „útočit" na neexistující adresu.)

V době, kdy se CodeRed objevil (a veleúspěšně šířil - na celém světě napadl skoro půl miliónu serverů), probíhala každoroční okurková sezóna, takže se jej ihned chopili senzacechtiví novináři. Ti celou „causu CodeRed" nafoukli do olbřímích rozměrů a varovali všechny uživatele před hrůzostrašnými účinky neméně hrůzostrašného viru. Základní fakt, že CodeRed hrozí výhradně serverům a nikoliv „běžným" uživatelům přitom taktně média pomlčela.

Toto je ostatně častý problém - na první pohled „atraktivním" škodlivým kódům věnují média značnou pozornost, zatímco skutečně nebezpečné kódy povětšinou ignorují. A tak se na podzim 2001 dostalo mimořádné publicity e-mailovému červu Anthrax - právě pro svůj zajímavý (a aktuální) název. Přitom tento skript obsahuje závažnou programátorskou chybu, takže se vůbec nešíří a existuje pouze v podobě laboratorních vzorků, které antivirovým firmám poskytl jeho autor. Zhruba o rok dříve byla podobná situace s virem Pikachu. Ten byl vytvořený už někdy koncem devadesátých let, ale protože se nešířil, antivirové společnosti jej zahrnuly do svých databází a celý případ tím uzavřely. Ale jakýsi novinář po loňské Pikachu-mánii zprávu o tomto viru kdesi „vyčaroval" a od něj už zuřivě opisovaly všechny „seriózní" tiskoviny.

CodeRed díky svému „samovolnému" šíření byl snad jediným z nejúspěšnějších škodlivých kódů, které se objevily v roce 2001 a který nevyužíval metod sociálního inženýrství. Jak již bylo uvedeno výše, v současné době není problém počítačový virus napsat, problém představuje jeho aktivace v cílovém počítači. Přestože známe první exempláře kódů aktivovaných při pouhém otevření e-mailové zprávy (tedy nikoliv po spuštění přílohy!), jedná se zatím jen o první varování. Drtivá většina škodlivých kódů pro svou činnost potřebuje - alespoň v prvním okamžiku - spolupráci neopatrného, nepoučeného či nepoučitelného uživatele.

Přímo čítankovým příkladem využití sociálního inženýrství byla jedna z variant viru Iloveyou (která se objevila už v květnu 2000). Škodlivý kód do zprávy elektronické pošty vypsal zhruba toto poselství: „Děkujeme Vám, že jste si u nás objednal květiny ke Dni matek. Květiny doručíme na Vámi uvedenou adresu. Částku 326 dolarů 90 centů strhneme z Vašeho účtu, doklad naleznete v přiloženém souboru. Děkujeme." Samozřejmě, že dotyčný si žádné květiny nikdy neobjednával (o to větší bylo jeho zděšení) a že v přiloženém souboru nebyl žádný platební doklad, ale virus. Ovšem člověk se v první chvíli vyděsí, zapomene na všechny dobré rady (Nespouštět podezřelé přílohy!) a neštěstí je hotovo.

V roce 2001 prakticky každý virus nějakým způsobem využíval metod sociálního inženýrství. A tak se velkého rozšíření dočkal virus Kurnikovová slibující atraktivní fotografii neméně atraktivní ukrajinské tenistky. Kód Naked_Wife zase měl nejen mnohoslibný název, ale i připojený text „má manželka nikdy nevypadala tak zajímavě" (jen mimořádně odolný jedinec by asi dokázal na přílohu u zprávy nepoklikat). Sircam zase - aby vypadal co nejdůvěryhodněji - náhodně vybíral z napadeného počítače jeden dokument, který pak odesílal. Desítky dalších škodlivých kódů se zase vydávaly za soubory s erotickým (ve většině případů) či jinak zajímavým obsahem.

Zcela samostatnou kapitolou v oblasti počítačové bezpečnosti jsou tzv. hoaxy - jakási e-mailová varování před viry, které neexistují. Správný hoax (toto slovíčko označuje v angličtině „smyšlenku" nebo „žert") je dopis elektronické pošty, který přijde do počítače a uživateli líčí hrůzostrašné chování nepředstavitelně nebezpečného viru. Na závěr je připojena žádost (někdy i opakovaná) o rozeslání této zprávy na co nejvíce lidem.

Problém spočívá v tom, že nicnetušící uživatel tak svým způsobem vykoná činnost prováděnou povětšinou právě viry - rozešle zprávu na všechny strany (mnoho virů se kromě šíření nijak neprojevuje, leč pod množstvím odesílané pošty „padají" přehlcené poštovní servery).

Typické znaky hoaxu:

- Popisuje nesmírně nebezpečný virus dosud nevídaných vlastností a schopností.
- Chybí v něm jakékoliv časová přesnost (termín „včera ráno" je použitelný dnes i za půl roku).
- Varuje před virem, který je nepředstavitelně nebezpečný, ale o kterém zároveň nikdo nic neví a se kterým si nikdo nedokáže poradit.
- Snaží se zaštítit jménem velké a důvěryhodné firmy, která toto varování údajně vydala.



- Vyzývá k rozeslání tohoto varování co nejvíce lidem. (Svým způsobem metoda sociálního inženýrství: Kdo by nechtěl pomoci bližnímu svému varováním, které prakticky nic nestojí?)

Speciálním případem hoaxu je přitom zpráva, která varuje před souborem sulfbnk.exe. Ten je totiž regulérní součástí prakticky každé instalace Windows. Toto ovšem tuší málokterý uživatel, jemuž varování (zpravidla od důvěryhodné a známé osoby) přijde. Člověk neznalý se vyděsí, soubor sulfbnk.exe samozřejmě v počítači najde - a dle přiloženého návodu odstraní. Přestože je to regulérní součást Windows, sulfbnk.exe (naštěstí) nemá žádnou klíčovou či nenahraditelnou funkci - jedná se o program, který má převádět „dlouhé“ názvy programů na „krátké". Každopádně se ale jedná přímo o čítankový příklad pravidla, že „laický uživatel je mnohdy schopen (a ochoten) způsobit mnohem více škod než virus“.

Tolik tedy ve stručnosti k otázce problematiky počítačových virů v roce 2001. Zcela logicky vyvstává otázka: Co nás asi v roce nadcházejícím (či v letech příštích) v oblasti počítačových virů čeká? Nějakou převratnou revoluci asi očekávat nelze - bude se pouze měnit (rozšiřovat) rozsah platforem „podporujících“ počítačové viry, prostor dostanou na jedné straně komplexní a sofistikované škodlivé kódy, na druhé straně jednoduché a primitivní kusy programových kódů schopné přežít prakticky kdekoliv. Hlavním nosným médiem virů se nadále zůstane e-mailová pošta (či její deriváty). A v každém případě bude narůstat četnost útoků.

Rozhodně se můžeme „těšit“ na další škodlivé kódy, které se automaticky aktivují při pouhém otevření e-mailu či jeho náhledu (preview). Není už tedy nutné na nic klikat, nic spouštět! Toto umožňuje psaní zpráv elektronické pošty v HTML formátu - přitom HTML stránka může obsahovat nejrůznější skripty, a tyto skripty zase mohou obsahovat kdeco. Bezpečnostní chyby navíc umožňují skripty aktivovat doslova „bez zásahu lidské ruky". První prototyp podobného škodlivého kódu se jmenoval BubbleBoy a objevil se již v říjnu 1999. Na závěr roku 2001 už podobnou technologii disponoval (nebo se pokoušel disponovat) prakticky každý „lepší“ virus.

Další z cest, kterou by se škodlivé kódy v budoucnu mohly ubírat, ukázal v polovině roku 2001 Sircam. Ten si z napadeného počítače náhodně vybral jeden dokument, který si s sebou vzal „na cestu“ a za nějž se v cílovém počítači vydával. Že při této činnosti nedělal velkého rozdílu mezi daty soukromými či veřejnými, tajnými, důvěrnými apod. jistě není třeba dvakrát zdůrazňovat. Přímo se nabízí myšlenka využít počítačových virů k cíleným útokům na určité soubory či systémy. Ještě lákavější může být spojit tuto činnost s vydíráním - dešifrovací klíč k zašifrovaným souborům po útoku počítačového viru se často vyvažuje zlatem (a to nejen obrazně).

Škodlivé kódy a mobilní aplikace. Často je zdůrazňováno, že současné mobilní telefony se nějakého velkolepého útoku obávat nemusí. Maximálně lze mobily „zasypat“ přívalem SMS zpráv na veřejné brány jednotlivých operátorů. Ovšem s příchody nejrozmanitějších komunikátorů a PDA aplikací se samozřejmě velmi rozšíří možnosti jejich použití - a ruku v ruce s tím i možnosti jejich napadení. Mobilní telefony si zatím předávají pouze data (ať již ve formě SMS zpráv či hlasových dat), nikoliv kusy programového kódu - v takovém prostředí samozřejmě není pro viry místo.

Několik virů pro PDA sice již existuje (první z nich byl Phage v polovině roku 1999), ale protože tato zařízení nejsou navzájem propojena a propojována, dochází k jejich napadení výhradně prostřednictvím přenosu dat z počítače. Proto již bylo nutné vyvinout několik antivirových programů právě pro PDA. S nasazením sítí třetí generace dojde k mnohem větší výměně dat a dalších informací mezi jednotlivými „příručními“ digitálními pomocníky - pak se hrozba „zavirovaného“ mobilu stane reálnou. Máme se věru nač těšit.

V souvislosti s událostmi 11. září se také často zmiňuje možnost kyberterorismus, jehož nebezpečí bývá mnohdy podceňováno. Vždyť škody způsobené nejúspěšnějšími škodlivými kódy se v současné době počítají na miliardy dolarů. A to jsou vlastně škody způsobené „jen tak mimochodem". Není asi těžké si představit nějaký kód, který by se napadal cíleně určité počítače, servery či databáze. Vždyť celý náš svět je postaven na informačních technologiích, které jsou zranitelnější než jsme si ochotni připustit…

Tomáš Přibyl

(Článek vyšel i v časopise Computerworld 3/2002.)

# Tretí ročník konferencie Bezpečnosť dát v Bratislave se blíži!


V stredu 17. apríla 2002 budeme svedkami ďalšej zaujímavej udalosti - prebehne už 3. ročník konferencie **„Bezpečnosť dát“** v Bratislave. Pokračovanie tejto akcie, ktorej prvý ročník prebehol v roku 2000, nesporne svedčí o jej kvalite a atraktívnosti diskutovaných tém. Popri spoločnosti **AEC Bratislava** sa na poriadaní podieľa tiež **Slovenská asociácia pre informačnú bezpečnosť (SASIB)** a mesačník **PC Revue** (www.pcrevue.sk). Tak ako aj v minulom roku, i tento rok sa konferencia uskutoční v reprezentatívnych priestoroch bratislavského hotela Holiday Inn.

Minulý rok bola konferencia rozdelená na tri tematické časti: „Bezpečnosť v počítačových sieťach“, „Bezpečnosť vo svete elektronického obchodu“ a „Antivírusová ochrana". Medzi prednášajúcimi odborníkmi bolo možné nájsť radu známych osobností z oblasti počítačovej bezpečnosti, napríklad Ing. Miroslava Trnku zo spoločnosti Eset alebo Ing. Jaroslava Pinkavu - známeho českého odborníka na kryptológiu. I v tomto roku bude na konferencii v podaní popredných českých i slovenských odborníkov preberaná rada zaujímavých tém. Program tohtoročnej konferencie Bezpečnosť dát je rozdelený do dvoch blokov: „Elektronickýpodpis v bezpečnosti IT“ a „Vírusy, antivírusy“. Prvý blok bude, ako už vyplýva z jeho názvu, venovaný hlavne problematike využitia elektronického podpisu v IT bezpečnosti. V rámci tejto časti konferencie prednesie svoje príspevky rada slovenských i českých odborníkov. Druhý blok bude venovaný príspevkom z oblasti antivírusovej ochrany.

Názvy jednotlivých prednášok, vrátane anotácií, nájdete v programe konferencie.
Naša spoločnosť týmto čo najsrdečnejšie pozýva všetkých záujemcov o informácie z oblasti bezpečnosti dát na bratislavskú konferenciu „Bezpečnosť dát 2002“. Prihlásenie je možné buď pomocou prihlasovacieho formulára, ktorý nájdete na **www.aec.sk**, alebo akýmkoľvek iným spôsobom v kancelárii AEC Bratislava (Pribinova 25, P.O.Box 79, 810 11 Bratislava, e-mail: **bratislava@aec.sk**, tel: +421 2 5063 3027, fax: +421 2 5063 3029)

# Konferencia v Bratislave

## Program konferencie Bezpečnosť dát 2002

**Kongresová sála hotela Holiday Inn, Bratislava, 17. 4. 2002**
**Organizuje AEC Bratislava, s.r.o. v spolupráci so SASIBom, mediálny partner PC Revue**

## Program

8:30 Prezentácia účastníkov konferencie (občerstvenie)

9:20 *Alena Mračková*
*riaditeľka AEC Bratislava, s.r.o.*
**Otvorenie konferencie**

### 9:30 Elektronický podpis v bezpečnosti IT

- **Elektronický podpis v archivácii dát**
  *Ing. Jiří Mrnuštík, riaditeľ vývojového oddelenia AEC, spol. s r.o.*

Prenikanie elektronického podpisu do stále väčšieho počtu oblastí sa stáva neoddiskutovateľným faktom. V súčasnosti ho mnohokrát nájdeme i tam, kde by sme jeho využitie skôr ani neočakávali. Tento fakt potvrdzuje najmä široké možnosti využitia technológie elektronického podpisu. Jeho aplikácia v súvislosti s archiváciou dát je obsahom tejto prednášky.

- **Národný bezpečnostný úrad SR a elektronický podpis**
  *JUDr. Sudor, NBÚ SR*

  Právne postavenie NBÚ vo vzťahu k zákonu o elektronickom podpise. Pôsobnosť NBÚ pri aplikácii zákona o elektronickom podpise. Práva a povinnosti NBÚ, právnických osôb a fyzických osôb vyplývajúce zo zákona o elektronickom podpise.

- **Zákon o elektronickom podpise, východiská, problémy a riešenia**
  *Doc. RNDr.Daniel Olejár, CSc.; Mgr. Jaroslav Janáček, FMFI UK*

  Zákon o elektronickom podpise vyvolal v poslednom čase veľa pozornosti. Autori príspevku, ktorí sa podieľali na vypracovaní poslaneckého návrhu zákona, objasnia základnú filozofiu zákona a poukážu na problémy vyplývajúce z nesúladu Direktívy EÚ 1999/93/EC, existujúcej slovenskej legislatívy a možností dostupných technológií. Naznačia možnosti riešenia uvedených problémov a ako sa tieto riešenia odrazili v návrhu zákona. Podrobnejšie sa zaoberajú otázkami, ktoré vzbudili najviac pozornosti - bezpečnosti, zaručenému elektronickému podpisu a spôsobu organizácie PKI.

- *Prestávka (občerstvenie)*

- **Bezpečnostné požiadavky na zariadenia elektronického podpisu**
  *Doc. Ladislav Hudec, FEI STU*

  Zariadenia na elektronický podpis musia vyhovovať istým bezpečnostným požiadavkám. Hlavné bezpečnostné požiadavky vyplývajú zo štandardov ISO 17799 alebo ISO/IEC TR 13 335 z hľadiska systémovej informačnej bezpečnosti, ISO 15 408 z hľadiska stanovenia úrovne informačnej bezpečnosti a štandardu FIPS 140-2 (NIST) z hľadiska použitia nosiča na uloženie informácie na vyhotovenie elektronického podpisu.

- **Využitie elektronického podpisu pri zavedení nových identifikačných preukazov občanov**
  *Ing. Miroslav Milán, ICL Slovakia*

  Aktuálny stav legislatívy vo vzťahu k identifikácii občana. Obmedzenia vyplývajúce zo súčasnej legislatívy. Potreba nahradenia rodného čísla nevypovedajúcim identifikátorom. Elektronický podpis - nové možnosti v jednoznačnej identifikácii občana. Trendy v EU vyplývajúce z využitia EP vo vzťahu k identifikácii občana (Francúzsko, Fínsko ...). Príprava prostredia na zavedenie identifikačných dokladov občana využitím EP vo väzbe na EU.

- **Bezpečnostný problém menom človek**
  Olga Přikrylová, Technical support,
  AEC, spol. s r.o.

  Väčšina celosvetových (i tuzemských) prieskumov, výsledkov bezpečnostných analýz a štatistík dokazuje, že prevažujúcou hrozbou bezpečnosti

informačných systémov je Homo sapiens sapiens (človek), či už sa jedná o vlastných zamestnancov organizácii, o pracovníkov na vedúcich postoch, o vonkajších nepriateľov, alebo o počítačových útočníkov (hackeri, crackeri atď.). Ľudský faktor sa na bezpečnostných incidentoch všeobecne podieľa tou najväčšou mierou. Ľudské chyby, trebárs i neúmyselné, spôsobujú veľké straty spoločnostiam, ktoré podceňujú toto riziko a z rôznych dôvodov nie sú schopné rešpektovať a uplatňovať všeobecné zásady a pravidlá bezpečnostnej politiky. V informatike rovnako ako kdekoľvek inde v živote platí doslova ono známe „dôveruj, ale preveruj", a to sa týka nielen systému (HW, SW, dáta), ale tiež, a hlavne, ľudí, pretože nadsadene môžeme povedať: čo človek, to užívateľ. A nielen týmto pravidlom vo vzťahu k bezpečnosti IS sa zaoberá prednáška na uvedenú tému.

- *Prestávka (občerstvenie)*

- **Bezpečnosť bezdrôtových technológií**
  *Ing. Petr Nádeníček, IT security conslultant, AEC, spol. s r.o.*

  S rozvojom nových mobilných zariadení sa stále častejšie stretávame s problémami spojenými s riešením ich bezpečnosti. Bezdrôtové prenosy dát, nové generácie sietí mobilných telefónov a nové služby v týchto sieťach, to všetko môže byť v budúcnosti terčom mnohých útokov vrátane hackerov alebo nových počítačových vírusov. V prednáške budú poslucháči zoznámení s novými trendmi v oblasti mobilných zariadení a potenciálnymi hrozbami s nimi spojenými.

## 14:00 Vírusy, antivírusy

- **Čo trápi antivírusové firmy ?**
  *Ing. Tomáš Přibyl, IT security consultant, AEC, spol. s r.o.*

  Pokiaľ by niekto na otázku „čo trápi antivírusové firmy?" odpovedal „predsa počítačové vírusy", nemal by pravdu ani z polovice. Problematických otázok v oblasti antivírusovej ochrany je totiž celý rad - počnúc bezpečnostnými nedostatkami v software cez nepoučiteľných užívateľov a administrátorov až trebárs po nutnosť vytvoriť antivírusový program so zodpovedajúcim pomerom rýchlosť/výkon. Cieľom prednášky je zoznámiť poslucháčov s úskaliami boja proti škodlivým kódom z pohľadu antivírusovej firmy.

- **Windows živná pôda pre vírusy**
  *Ing. Patrik Drugda, AEC Bratislava, s.r.o.*

  Operačný systém Windows, nech hovoríme o ktorejkoľvek z jeho verzií, v sebe skrýva množstvo „temných zákutí", zneužívaných alebo potenciálne zneužiteľných počítačovými vírusmi. Tieto „temné zákutia" môžu mať podobu nielen rôznych bezpečnostných dier, ale tiež regulérnych súčastí systémov, akou je trebárs implementovaná podpora makrojazykov. Čo všetko Windows „ponúka" existujúcim i potenciálnym počítačovým vírusom, sa dozviete v tejto prednáške.

- **Počítačové infiltrácie šírené elektronickou poštou a ochrana proti nim**
  *Ing. Miroslav Trnka, Eset s.r.o.*

  Príspevok opisuje históriu šírenia infiltrácií pomocou elektronickej pošty od začiatkov až po dnešný stav. Infiltrácie rozdeľuje na jednotlivé druhy a v krátkosti oboznámi poslucháčov s príkladmi najvýznamnejších vírusov, červov a trójskych koní z hľadiska rozšírenia a nebezpečnosti. V záverečnej časti príspevok opisuje rôzne prístupy k ochrane proti infiltráciám tohoto druhu v podnikovom prostredí.

- *Prestávka (občerstvenie)*

- **Nasadzovanie antivírusovej ochrany vo veľkých spoločnostiach**
  *Ing. Jozef Chebeň, EMM, spol. s r.o.*

  Veľké firmy sa vyznačujú špecifickými podmienkami pri implementácii prostriedkov antivírusovej ochrany vyplývajúce z ich veľkosti. V takýchto firmách musia byť aplikované špecifické organizačné a technologické opatrenia.

- *Diskusia*

- *Recepcia*
  (pozvanie pre všetkých účastníkov na čašu vína s malým občerstvením).

# Bezpečnostní řešení z vývojových laboratoří AEC

## TrustPort Certifikation authority

Systém určený pro vydávání certifikátů.

## TrustPort Encryption

- šifrování souborů a adresářů na PC a PDA.

## DataShredder

- „skartovačka", která zaručuje neobnovitelné smazání elektronických dat.

## TrustMail

- vytváření a ověřování elektronického podpisu a šifrování dat.


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

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

**BRATISLAVA:** AEC Bratislava, s.r.o.
Pribinova 25, P.O.Box 79, 810 11 Bratislava, Slovenská republika
tel.: + 421 2 50 63 30 27, fax: + 421 2 50 63 30 29
e-mail: bratislava@aec.sk, www.aec-security.com