AEC
DATA SECURITY COMPANY

Bulletin

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

AEC DATA SECURITY COMPANY

Vám přeje hodně úspěchů v novém roce

pour felicitae

ifpo ucerleait

200

Úvod

Milí přátelé!

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

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

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

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

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

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

Tomáš Přibyl, tomas.pribyl@aec.cz

Data do diáře: konference a akce AEC v roce 2002

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

Semináře Bezpečnost dat

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

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

Začátek seminářů je vždy v 9:30 hod.

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

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

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

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

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

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

Partnerský den AEC

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

Semináře a konference 2002

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

Konference Security 2002 (Praha)

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

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

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

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

Konference Bezpečnosť dát (Bratislava)

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

Workshop pro dealery

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

Roadshow Slovensko 2002

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

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

AEC roadshow 2002

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

AEC roadshow 2002 se bude konat na podzim 2002.

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

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

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

Počítačové viry v roce 2002

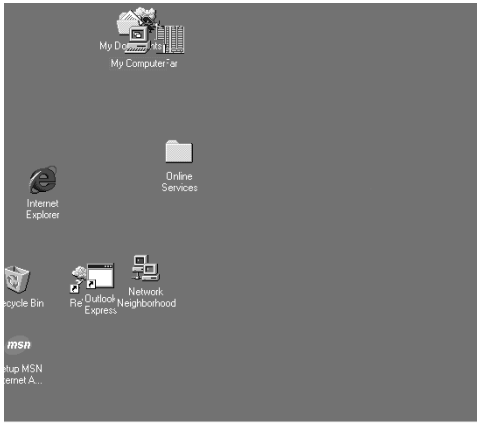
V roce 2000 jsme do říjnového čísla známého počítačového měsíčníku PC World připravili společně s jeho redakcí 64stránkovou brožurku „Svět elektronického podpisu“. Ani ve snu nás tehdy nenapadlo, jak velký ohlas (veskrze pozitivní) bude mít a jak velkého ocenění se na mnoha frontách dočká.

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

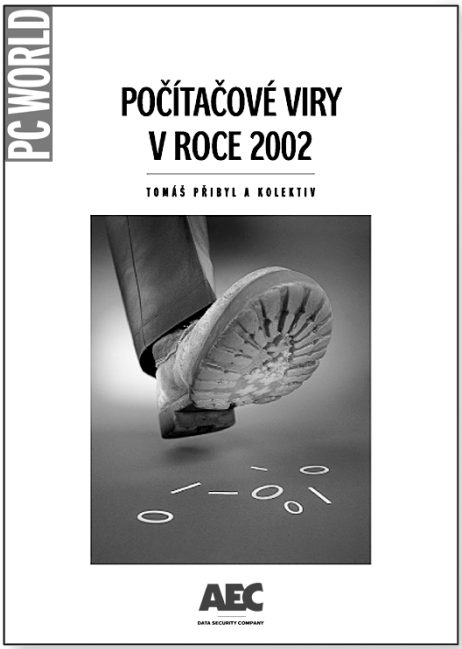
Její název by mohl svádět k domněnce, že bude pojednávat pouze o úzké oblasti škodlivých kódů, ale není tomu tak. Název „Počítačové viry v roce 2002“ byl zvolen proto, že jde o první z řady několika brožurek, které by se měly začít více či méně pravidelně (zhruba v jednoletých intervalech) objevovat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

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

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



Projev počítačového viru Magistr - „uhýbání“ ikonek.



BadTrans - tvrdý úder po půl roce

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

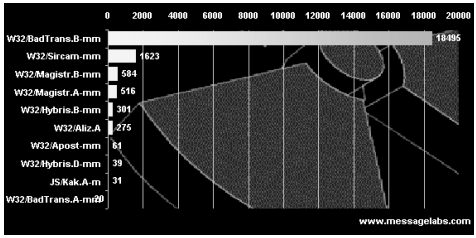
To, že je váš systém infikován virem BadTrans.B, poznáte bezpečně podle toho, že při pokusu o napsání velkého písmena s háčkem napíšete pouze dva háčky „ˇˇ“. Tento projev je způsoben programem pro snímání stisknutých kláves, který je taktéž součástí červa.

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

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

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

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



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

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

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

Zpráva vypadá takto:

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

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

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

Audit akreditovaných certifikačních autorit aneb workshop e-commerce

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

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

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

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

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

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

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

Hana Stojanová, hana.stojanova@aec.cz

V roce 2002 opět na CeBITu

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

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

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

Proč právě CeBIT?

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

Pro rok 2002 jsou na CeBITu připravena tato témata:

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

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

Takže: na shledanou na CeBITu!

Hana Stojanová
hana.stojanova@aec.cz

Slovensko ve znamení počítačové bezpečnosti

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

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

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

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

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

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

Petr Nádeníček
petr.nadenicek@aec.cz

Roadshow aneb bezpečnost na cestách

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

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

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

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

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

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

Petr Nádeníček, petr.nadenicek@aec.cz

AEC
Data Security Day

9. a 11. října 2001
Slovenská republika

Vzpomínka na jarní roadshow - Košice.

Přednáším, přednášíš, přednášíme…

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

Vylosovaní výherci se těšili na získané ceny.

K boji s počítačovými viry vždy připraveni!

AEC roadshow 2001

30. října
až
15. listopadu 2001

Olomouc - velká roadshow začíná!

Na roadshow je cesta dlouhá…

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

Olga Přikrylová byla na roadshow skutečně "na roztrhání".

Tomáš Vobruba zaujal posluchače ve Zlíně.

Nebezpečí kybernetického prostoru jsou před námi

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

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

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

Nebezpečí útoků zevnitř

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

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

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

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

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

Hackeři

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

Hactivism - hackerský aktivismu

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

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

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

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

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

Pisatelé virů

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

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

Kriminální skupiny

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

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

Kyberterorismus

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

Informační válka

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

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

Tomáš Přibyl, tomas.pribyl@aec.cz

AEC představuje nový produkt

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

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

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

Antigen 6.0 pro Lotus Domino

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

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

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

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

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

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

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

Komponenty Antigenu pro Lotus Domino jsou následující:

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

Antigen pro Microsoft Exchange

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

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

Sybari

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

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

Produkt se skládá ze tří základních částí:

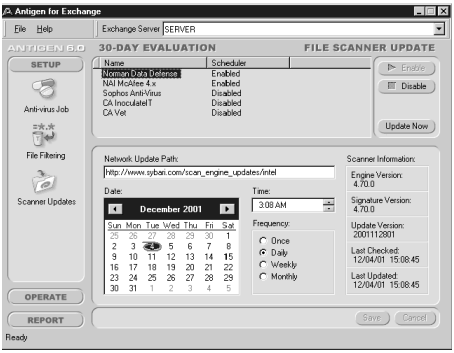
- Antigen Realtime Job - tato část slouží pro skenování probíhající v reálném čase, kdy zprávy jsou skenovány „za letu“ (on the fly). Tato část skenuje Storage Groups a databáze.
- Antigen SMTP/IMS Job - slouží pro ochranu příchozích a odchozích zpráv v reálném čase.
- Antigen Manual Scan Job - slouží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

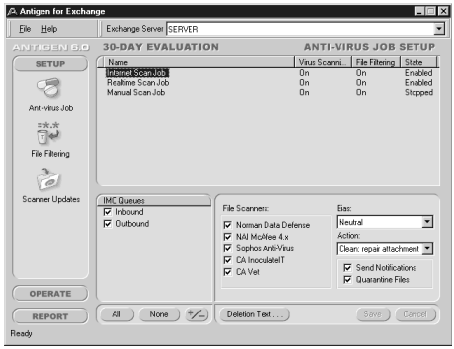
Oba tyto produkty jsou, jako ostatně všechny z nabídky AEC, dodávány spolu s technickou podporou, možností instalace, vyškolením obsluhy, auditů správného nasazení apod. Díky tomu, že tento produkt přesně zapadá do nabídky AEC, jsme schopni našim zákazníkům nabídnout nejen jedno antivirové řešení bezpečnosti,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

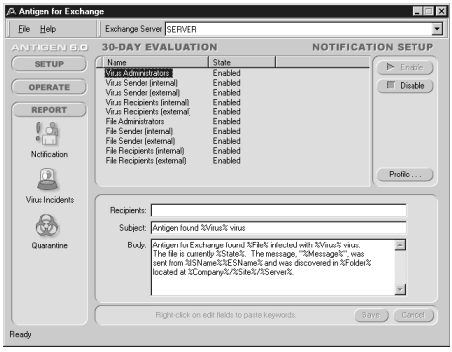
Teď už je jen na uživateli, aby specifikoval svoje potřeby v oblasti ochrany dat a tyto nám sdělil. Takže neváhejte a piště, telefonujte, faxujte a mailujte…

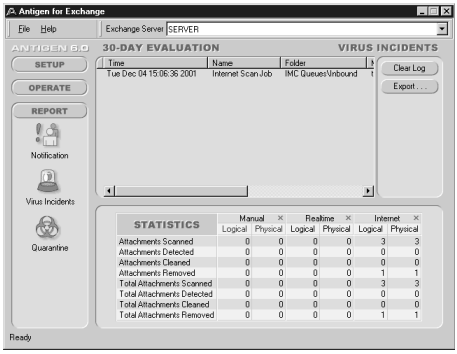
… a samozřejmě se mějte dobře.

Jan Novotný, jan.novotny@aec.cz









Projekt elektronické podatelny

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

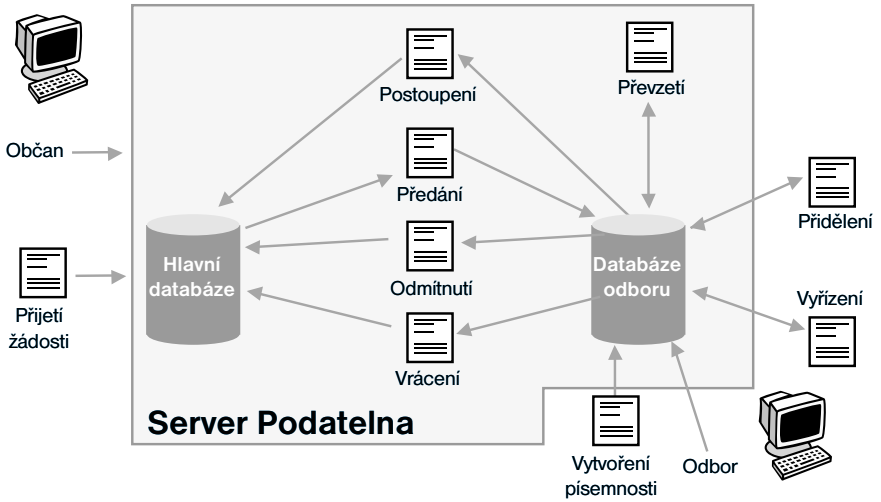
Jedná se o databázový systém, který umožňuje jednoduchou formou realizovat tzv. elektronické podatelny ve smyslu nařízení vlády ze dne 25. července 2001, kterým se provádí zákon o elektronickém podpisu. Řešení vychází z elektronické spisové služby, kterou doplňuje o možnost vytváření a ověřování elektronického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

Použité technologie v projektu elektronické podatelny

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

Jak funguje projekt elektronická podatelna?

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



Procesní diagram

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

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

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

Bezpečnost projektu elektronické podatelny

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

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

HOAX - otázky a odpovědi

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

Může být hoax nebezpečný?

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

Jak lze hoax poznat?

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

Jak se bránit?

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

Kde lze najít další informace o hoaxech?

Nejlépe na webových stránkách velkých antivirových firem.

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

McAfee VirusScan 6.0 - antivirový desktopový program určený pro domácí použití

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

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

McAfee - VirusScan 6.0

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

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

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

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

Systémové požadavky:

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

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

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

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

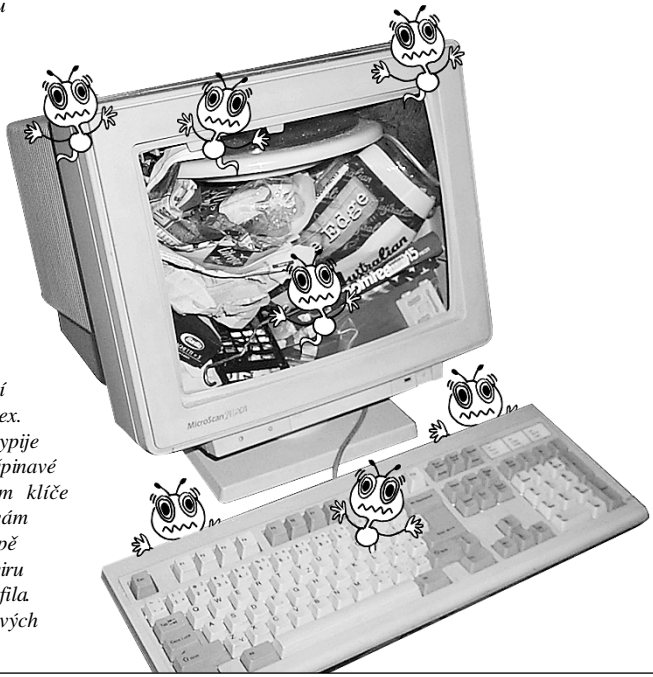
V případě jakýchkoli dotazů či zájmu o uvedené produkty kontaktujte naše obchodní či technické oddělení

Eva Šebková
eva.sebkova@aec.cz

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

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

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



Dejte přednost jistotě!

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

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

AEC

DATA SECURITY COMPANY

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

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

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