AEC
DATA SECURITY COMPANY

Bulletin

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

Úvod

Milí přátelé!

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

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

Příjemné čteni!

Tomáš Přibyl
tomas.pribyl@aec.cz

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

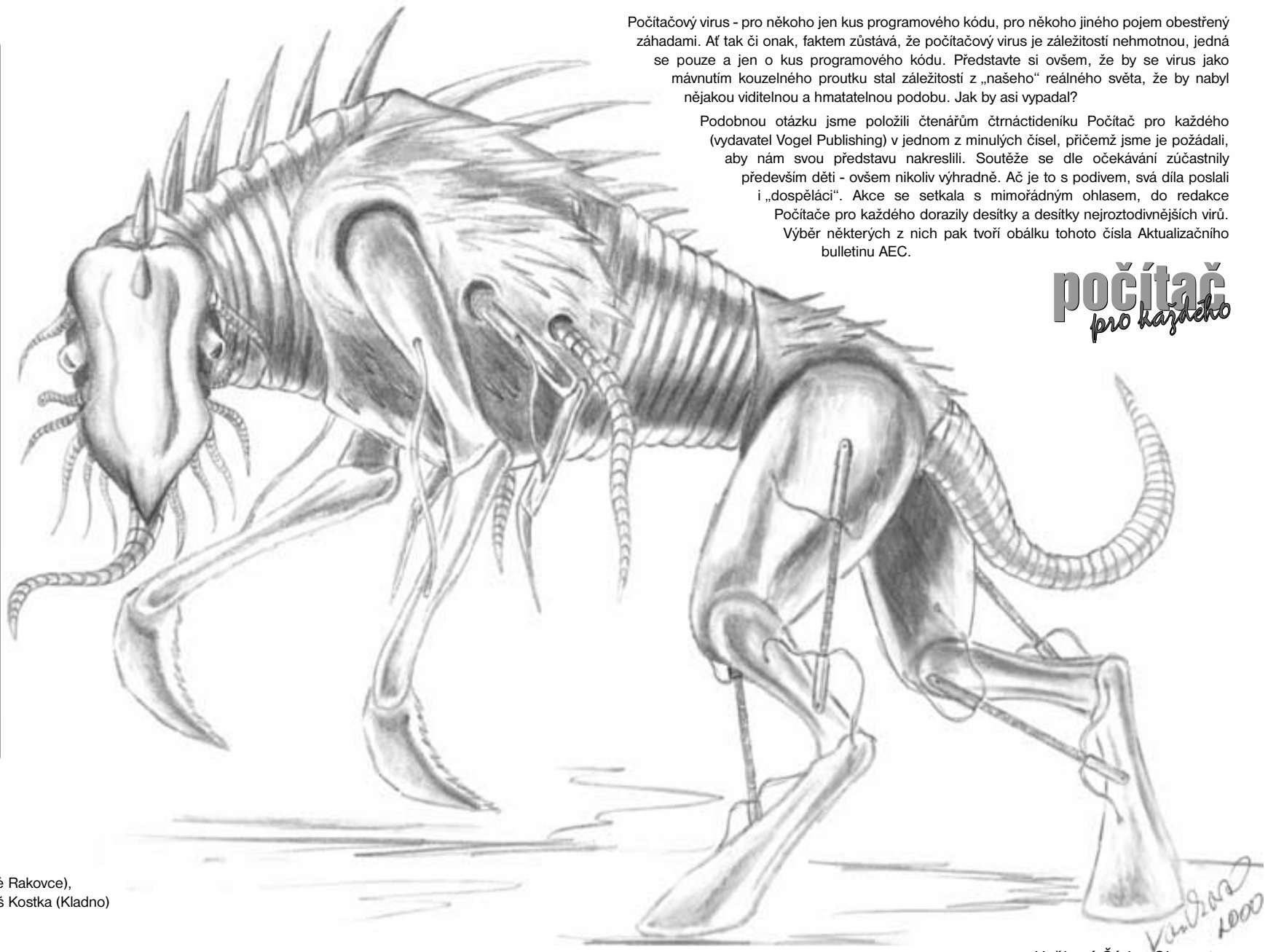
Foto na obálce: David Mráz a Jan Kroupa

Jak vypadá počítačový virus?

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

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

počítač pro každého



Vaňková Šárka, Chomutov

Bezpečnost elektronického podpisu: Bouře ve sklenici vody

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

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

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

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

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

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

Není tedy naprosto žádný důvod propadat jakékoliv panice.

Rozšiřujeme nabídku: Panda Software

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

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

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

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

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

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

Andrea Koláčková
andrea.kolackova@aec.cz

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

CeBIT na vlastní kůži

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

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

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

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

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

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

Tomáš Přibyl
tomas.pribyl@aec.cz

Roadshow 2001 - aneb cesta do Košic a zpět

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

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

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

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

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

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

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

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

Petr Nádeníček
petr.nadenicek@aec.cz

Finanční ztráty způsobené útoky z Internetu se zvyšují

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

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

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

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

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

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

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

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

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

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

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

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

Petr Nádeníček
petr.nadenicek@aec.cz

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

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

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

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

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

Konference Bezpečnost dat *Hotel Holiday Inn, Bratislava*

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

Stránku připravila Hana Stojanová
hana.stojanova@aec.cz

Kde jsi byl(a) v noci?

15. března 2001,

Praha

Divadlo Bez zábradlí

Výborné představení končí, nekonečná děkovačka začíná.

Po celý večer bylo o dobré pití a zábavu postaráno.

Každý účastník dostal los, někteří účastníci byli vylosováni.

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

Konec dobrý, všechno dobré.

Bezpečnosť dát 2001

3.dubna 2001,

Bratislava

Hotel Holiday Inn

T minus deset minut a odpočítáváme…

Čas nula, startujeme!

Nacpaný konferenční sál bratislavského hotelu.

Raut po skončení konference ozdobil kulturní program.

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

Elektronický obchod á la AEC

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

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

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

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

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

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

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

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

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

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

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

Ale zpět k zabezpečení elektronického obchodu. Veškerá komunikace probíhá zabezpečená pomocí protokolu HTTPS. Autentizace se pak děje pomocí přihlašovacího jména a hesla (nebo certifikátu), které jsou jedinečné - jedná se o jakousi obdobu prokázání totožnosti a jejího potvrzení podpisovým vzorem v „kamenné“ bance. Samozřejmě, v reálném světě může někdo Váš podpis napodobit - kybernetickém prostoru to absolutně nehrozí. Heslo buď je platné nebo není. Tečka. Samozřejmě, že může dojít k jeho prozrazení (např. je příliš jednoduché nebo si jej uživatel přilepí na kus papíru na klávesnici zespod), ale to už je vina nesprávného chování uživatele (stejně jako třeba zapomenutý občanský průkaz v dopravním prostředku). Ovšem elektronický svět má jednu velkou výhodu - zatímco v reálném můžete s občanským průkazem dělat prakticky cokoliv, heslo v kybernetickém prostoru má velmi malé uplatnění. navíc ho můžete dle libosti měnit.

Stále ještě se vám zdá elektronické obchodování složité?

Autentizace spojení prostřednictvím webu

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

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

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

Autentizační modul firmy AEC poskytuje tyto výhody:

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

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

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

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

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

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

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

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

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

Olga Přikrylová
olga.prikrylova@aec.cz

Vyzkoušejte NORMAN VIRUS CONTROL

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

Norman získal Virus Bulletin 100%

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

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

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

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

Norman Virus Control 5

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

Jednodušší instalace

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

Jednoduchá správa

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

Transparentnost

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

Aktualizace přes Internet

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

Jitka Brandejsová
jitka.brandejsova@aec.cz

Nová produktová řada od Kaspersky Lab

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

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

V kategorii domácích uživatelů Kaspersky Lab nabízí:

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

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

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

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

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

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

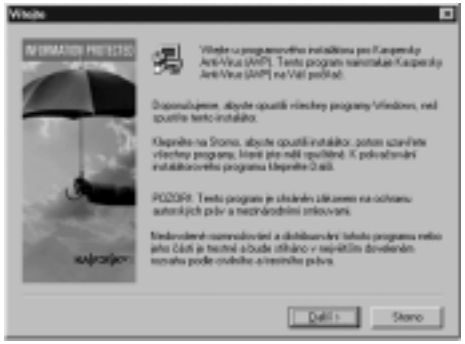
Pro velké firmy s rozsáhlými podnikovými sítěmi nabízí Kaspersky Lab balík **Kaspersky Corporate Suite**. Mimo podpory všech běžných operačních systémů a aplikací pro stanice, servery a e-mailové brány Kaspersky Corporate Suite poskytuje komplexní centralizovanou kontrolu síťového provozu (jak směrem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

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

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

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

Erik Borecký
erik.borecky@aec.cz



Průvodce světem VPN

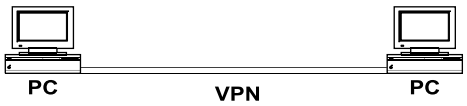
V poslední době se často objevují tato tři magická písmena v souvislosti s bezpečností dat. Co ale ve skutečnosti VPN je a jak pracuje? Na tuto otázku se Vám pokusím dát odpověď v následujícím článku.

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

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

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

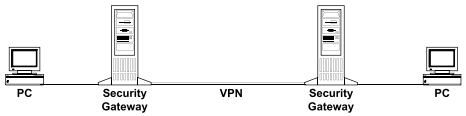
End - to - End Tunneling



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

Node - to - Node Tunneling

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



IP Security (IPSec)

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

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

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

Autentication Header (AH)

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

Encapsulating Security Payload (ESP)

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

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

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

Operační módy

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

Authenticated data	Encrypted Data

Barevné rozlišení

IP Header	AH	IP Peyload

AH Transport Mode

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

New IP Header	AH	Old IP Header	IP Peyload

AH Tunnel Mode

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

IP Header	ESP Header	IP Payload	ESP Footer	ESP Authenticated Data

ESP TransportMode

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

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

ESP Tunnel Mode

Virtuální privátní sítě

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

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

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

AH Transport Mode, ESP Tunnel Mode

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

Tomáš Kočnar
tomas.kocnar@aec.cz

Elektronický bulletin

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

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

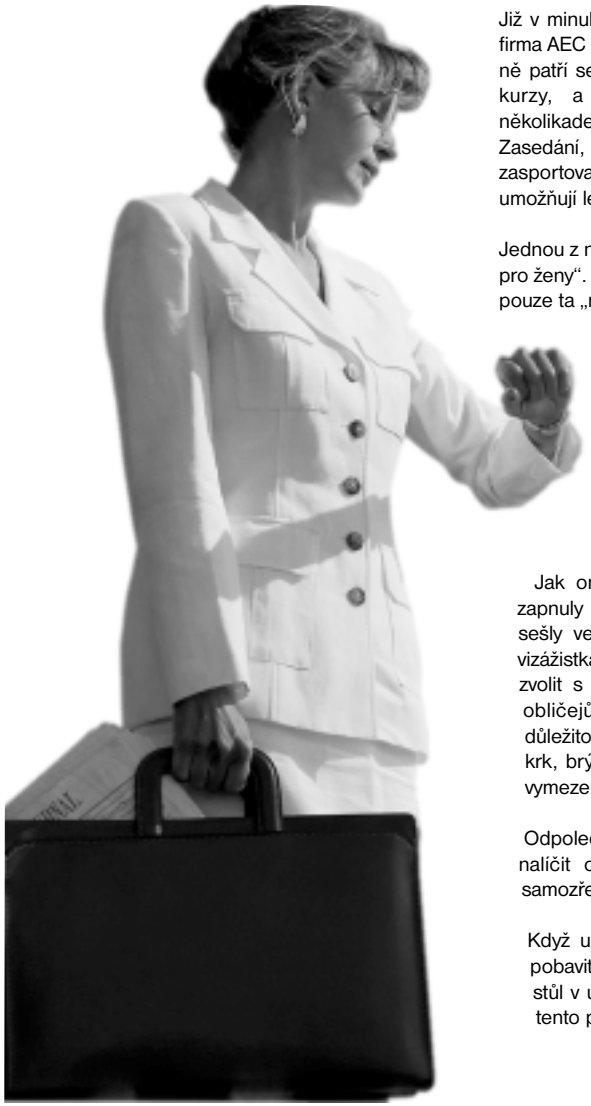
A právě především novinkám v oblasti počítačových virů a antivirových technologií stejně jako bezpečnosti dat vůbec, je věnovaný elektronický bulletin připravovaný společností AEC.

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

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

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

AEC zevnitř



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

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

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

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

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

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

Eva Šebková
eva.sebkova@aec.cz

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