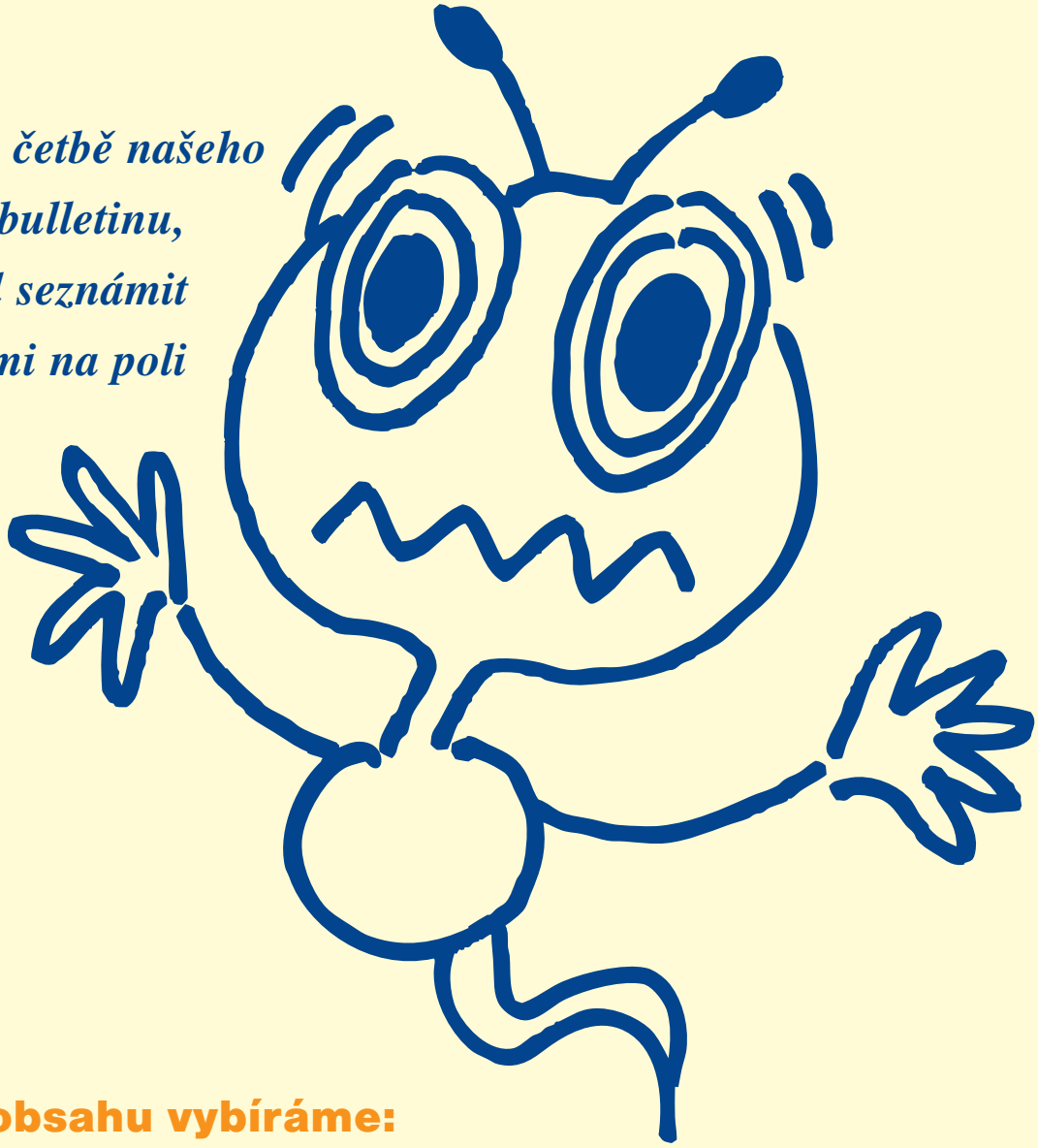
AEC
DATA SECURITY COMPANY

Magazín

Milí přátelé!
Vítáme Vás při četbě našeho informačního bulletinu, který má za cíl seznámit Vás s novinkami na poli virů, antivirů a bezpečnosti dat všeobecně.



Z dnešního obsahu vybíráme:

Příjemné počtení a co nejméně potíží s viry a zabezpečením dat přeje Vaše firma AEC, spol. s r.o.

JEDEN ZE SEDMI SET E-MAILŮ OBSAHUJE POČÍTAČOVÝ VIRUS!

Zatímco v lednu 2000 připadal na dva tisíce odeslaných zpráv elektronické pošty jeden virus, na konci téhož roku už obsahoval virus každý sedmistý e-mail!

Podle statistiky firmy MessageLab byl nejhorším měsícem říjen, kdy bylo zaznamenáno 30678 e-mailů obsahujících virus. Následuje listopad s 23961 odhalenými zavirovanými e-maily a na třetím místě se umístil květen - především zásluhou kalamity "Iloveyou" (23290 zachycení). Symbolický "účet" roku 2000 pak hovoří o 155528 odhalených virech v e-mailech. (V této statistice jsou zaznamenány e-maily kontrolované právě společností MessageLab. Ovšem vzhledem k tomu, že kontroluje přes tři milióny zpráv denně, jedná se o statisticky dostatečně reprezentativní vzorek.)

Právě Iloveyou se stal nejrozšířenějším škodlivým kódem roku 2000. Hned za ním se umístil škodlivý kód Kakworm, následovaným virem ProLinem. Díky své rychlosti se viry šířené elektronickou poštou staly "hitem" roku 2000 - nyní na ně připadá přes osmdesát procent všech hlášených infekcí.

JEDENÁCTÁ KONFERENCE VIRUS BULLETINU V PRAZE!

Jedenácté setkání předních světových expertů v oblasti antivirové ochrany počítačů konané pod záštitou specializovaného měsíčníku Virus Bulletin se uskuteční v Praze! Odborníci se v našem hlavním městě sjedou 27. a 28. září v Hotelu Hilton Praha. Dva dny budou vyplněny přednáškami a diskusemi o všech možných i nemožných otázkách s problematikou virů souvisejících.

POZOR, MELISSA SE VRACÍ!

Odborníci na antivirovou problematiku z AEC varují před staronovým e-mailovým červem, který se jako lavina šíří světem a zasáhl i počítače v České republice. Oficiálně se mu dostalo

označení Melissa.W.

Je to nová verze jednoho z nejslavnějších škodlivých kódů v historii počítačových virů, který se poprvé objevil v březnu 1999. Jen pro rychlou rekapitulaci: Melissa se šíří tím, že se automaticky rozešle pomocí elektronické pošty od jednoho uživatele ke druhému. Aktivuje se spuštěním přílohy u e-mailové zprávy (wordovský dokument), čímž se zapíná makro uvnitř dokumentu a odešle elektronickou poštou soubor list.doc padesáti lidem, jejichž adresy byly uvedeny v poštovních aliasech souboru daného uživatele. Většina příjemců přitom takový soubor otevřela, protože přicházel od někoho důvěrně známého. A Melissa se vesele šířila dál dalším padesáti lidem z každého napadeného počítače…

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

Melissa.W ve skutečnosti není nějakou revoluční novinkou. Skoro by se dalo říci, že ve srovnání s původní Melissou je téměř stejná - změnila se pouze jedna (ovšem poměrně podstatná) věc. Infikovaný soubor Anniv.doc je MS Wordem pro počítače Macintosh. A v tom je celý problém: Jednak si některé antivirové programy s tímto rela

tivně novým formátem nedokáží poradit a jednak se jedná o první virus právě v tomto formátu. Soubor i virus jsou přitom plně funkční nejen pod Macintoshem, ale také windowsovými verzemi MS Office.

Jediným skutečným rozdílem ve funkčnosti mezi původní Melissou.A a současnou Melissou.W je skutečnost, že W-verze nemění automaticky úroveň nastavení ochrany před makry v Wordu 2000 na "nejnižší". Jinak se úplně stejně jako její starší sestřička rozesílá automaticky na prvních padesát adres v kontaktech MS Outlooku.

Melissa.W může do počítače přijít v jakémkoliv dokumentu, nemusí se nezbytně jmenovat Anniv.doc (o to větší pozornost proto trvale věnujte kontrole jakýchkoliv příloh u elektronické pošty). Červ je totiž schopen za určitých okolností odeslat z počítače další wordovské dokumenty dle náhodného výběru - v tom spočívá další nebezpečí tohoto škodlivého kódu, neboť samozřejmě nerozlišuje mezi dokumenty tajnými a "netajnými".

Jak z výše uvedeného vyplývá, nejedná se v případě Melissy.W o nic nového, problémy působí pouze změna ve formátech souborů Microsoftu. Efekty jsou přitom prakticky stejné jaké známe z dřívějška: Přetížení e-mailových serverů a občasná indiskrétnost při odesílání dokumentů z počítače.

Přitom nepotřebujete mít nainstalovaný MS Outlook k tomu, aby bylo možné spustit infekci. Melissa.W se ovšem nebude šířit dál, pokud MS Outlook nemáte (např. v případě instalace Outlook Expressu). Stejně tak není schopná pracovat pod Wordem 95. Může fungovat pod Windows 95, 98, Me, NT, 2000 a Macintosh.

HERMES, VIRUS S PŘÍCHUTÍ DOMOVINY

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

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

Červ používá MAPI funkcí, získává kontakty z Address Book a posílá na ně e-mailové zprávy s předmětem "Re:", přičemž v těle zprávy není nic jiného než jméno odesílatele. Příloha zprávy (tedy vlastní tělo viru) má jméno náhodně vybrané z následujícího seznamu:

· Seti@home 3.x to 4.0 upd.exe
· Seti@home_twk.exe
· Seti_patch.exe
· Lunetic!.exe
· CIH.exe
· Energy.exe
· ftip.exe
· Navidat.exe
· Click_ME!.exe
· Cenik.exe
· Lunetic.scr
· fucking.scr
· micro$haft.scr
· matrix.scr
· reboot.scr
· Pamela.scr
· techno.scr
· funny!.scr
· Hermes.scr
· School_in_da_flame.scr

Navíc se pokouší připojit na stránky našeho nejpopulárnějšího webovského portálu www.seznam.cz.

Navíc se ještě pokouší o zápis do registrů systému Windows, ale zásluhou chyby v programovém kódu nemá úspěch.

SPOLEČNOST NETWORK ASSOCIATES (NAI) NA PRAHU NOVÉHO MILÉNIA

V poslední době došlo v americké společnosti Network Associates (dále jen NAI) k několika personálním změnám, které jsou některými konkurenčními firmami tendenčně vykládány jako příznak krize. Proto český distributor produktů NAI, AEC Data Security Company, považuje za nutné se k současné situaci vyjádřit.

NAI ohlásila v minulých dnech změny ve vedení společnosti: Edwin Harper (ředitel společnosti od r. 1993) se stal předsedou správní rady. K poslednímu dni loňského roku zároveň odešli z vedení prezident společnosti Peter Watkins stejně jako finanční ředitel Prabhat Goyal.

Společnost NAI vzápětí nato jmenovala nového výkonného ředitele George Samenuka, který byl také jmenován do správní rady této firmy. Samenuk pracoval dosud jako prezident a výkonný ředitel společnosti Tradeout. Před příchodem do Tradeout působil na rozličných pozicích ve vedení IBM (přes 22 let). Edwin Harper předseda správní rady NAI o něm prohlásil, že je ideálním mužem na tuto pozici vzhledem ke svým dlouholetým zkušenostem. Správní rada NAI dále jmenovala Terryho Davise finančním ředitelem Network Associates.

"Jedná se o personální změny, k jakým dochází na celém světě dnes a denně. Lidé zkrátka přicházejí a odcházejí. Na celé situaci nevidím nic zvláštního," komentuje celou situaci ředitelka společnosti AEC Alena Řezníčková.

Je sice pravdou, že se akcie společnosti NAI výrazně propadly - zde ale jde o trend celého technologického oboru (akciový index NASDAQ se v roce 2000 propadl o největší hodnotu za dobu své existence). Nejvýraznější jednorázový propad pak nastal v prosinci, kdy byly za poslední kvartál oznámeny horší než analytiky očekávané hospodářské výsledky. Po oznámení změn ve vedení NAI se ovšem její akcie vydaly směrem vzhůru.

F-SECURE WORKSTATION JE FINALISTOU V OCENĚNÍ CELLENCE AWARDS

Antivirový program F-Secure Workstation se stal finalistou v nově vznikajícím ocenění Excellence Awards odborného časopisu Information Security.

Produkt byl v prvním kole nominovaný čtenáři časopisu, vzápětí nato jej museli mezi finalisty ocenění Excellence Awards potvrdit ještě analytikové a profesionálové z oblasti ochrany počítačových dat. Finalisté ceny reprezentují nejlepší bezpečnostní řešení a produkty v osmi různých kategoriích - F-Secure Workstation Suite je přitom finalistou v kategorii "Antivirus and Content Inspection products" (Antiviry a programy na kontrolu obsahu).

Andy Briney, šéfredaktor časopisu Information Security, prohlašuje, že nominovaní reprezentují přední produkty a řešení na dnešním trhu bezpečnostních produktů. "Jak vidíme na prudkém nárůstu nejrůznějších incidentů, nasazení a efektivní využití bezpečnostních technologií je velmi důležité," uvedl Briney. "Nominované produkty byly vybrány profesionály, kteří budují, aplikují a využívají bezpečnostní řešení. Vítězi se tak skutečně stanou jen ti nejlepší z nejlepších."

Finálovou účast produktu F-Secure Workstation komentuje též Risto Siilasmaa, prezident a CEO F-Secure Corporation: "V jakémkoliv podnikání není nic důležitějšího, než spokojenost zákazníka. Hned na druhém místě je ale ocenění a uznání. Být nominováni bezpečnostními analytiky a profesionály, kteří budují a chrání klíčové systémy pro 21. století, je skutečná čest."

Vítězové Excellence Awards budou oznámeni na galavečeři v únoru v MIS Training Institute na konferenci InfoSec World v Orlandu (stát Florida).

O FIRMĚ
AEC, SPOL. S R.O.

Firma AEC, spol. s r.o. byla založena v roce 1991. Dnes je jedním z předních poskytovatelů software a služeb pro komplexní zabezpečení osobních počítačů jak z hlediska utajení informací, tak antivirové ochrany. Za své produkty obdržela několik prestižních ocenění a také certifikace ISO-9001 a TickIT. V současnosti disponuje prodejní sítí, pokrývající Českou republiku i Slovensko s kancelářemi v Praze, Brně a Bratislavě.