AEC Magazín – Viry, antiviry a bezpečnost

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 Vašich dat přeje

AEC, spol. s r.o.

Na veletrhu Invex jsme se zúčastnili semináře „Viry a antivirová problematika“, který pořádalo vydavatelství Vogel Publishing. Na snímku ing. Jiří Mrnuštík z AEC, spol. s r.o. přednáší na téma „Nové viry – nové výzvy pro způsob antivirové ochrany.“

Máme dvě nominace na Křišťálový disk!

Nejprestižnější soutěží na brněnském veletrhu informačních technologií a výpočetní techniky je bezesporu Křišťálový disk. Za bezpečnostní software IronWare® Security Suite jsme obdrželi hned dvě nominace na Křišťálový disk.

IronWare® Security Suite je komplexní modulární systém určený k ochraně informací. Je založen na PKI a mezinárodních otevřených standardech. K zabezpečení dat je použito silné kryptografie. Systém umožňuje zabezpečení dat z následujících hledisek:

- **Autentizace** – uživatel se do systému přihlašuje zadáním jména a hesla. Současně se může autentizovat i pomocí hardwarových přihlašovacích předmětů (čipové karty nebo snímače otisků prstů). Autentizační modul umožňuje i vlastnost jednotného přihlašování do sítě (single sign on).
- **PKI** – klíčová infrastruktura je základem celého systému a umožňuje komplexní manipulaci s uživatelskými atributy, klíči a certifikáty centrálně, na bázi technologie server/klient. Součástí PKI je i Certifikační autorita, která umožňuje vydávat a manipulovat s certifikáty a LDAP Server, který dovoluje přístup k certifikátům podle LDAP standardu.
- **Utajení** – obsah dat je účinně skryt před všemi uživateli mimo oprávněných.
- **Digitální podpis –** Program umožňuje vytvářet digitální podpisy pošty, zpráv a dokumentů podle platných mezinárodních standardů.
- **Integrita -** neporušenost dat předávaných systémem je kontrolována a je zaručeno, že žádný narušitel nemůže nepozorovaně data modifikovat či zaměnit.
- **Nonrepudiation** (Nepopiratelnost) – Program zabezpečuje, že data podepsaná a poslaná uživatelem tento nemůže odmítnou a popřít, že je jejich autorem či vlastníkem a že s obsahem souhlasí. Toto (mimo jiné) zaručuje digitální podpis.
- **VPN** – použitím modulů systému lze sestavit virtuální šifrovanou síť na bázi protokolu FTP, která umožňuje autentizovat uživatele a server podle normy X509 v.3 a bezpečně šifrovat přenášená data.
- **Shredder** – nedílnou součástí ochranného modulárního software je nejen data šifrovat, ale data také bezpečně a neobnovitelně smazat. Toto zaručuje modul IW Shredder. Samozřejmě je aplikován i implicitně pro mazání dat tam, kde to nevyžaduje uživatelovu volbu.
- **Otevřenost** – systém obsahuje tři programátorská definovaná a popsaná rozhraní, což dovoluje třetím stranám použít této technologie k vytváření vlastních aplikací založených na PKI.
- **Výlučnost a inovativnost** – již předchozí verze byla oceněna cenou EU za inovativnost. Ve výrobku jsou aplikovány nejmodernější informační technologie, je zde implementována eliptická kryptografie, což je unikátní technologie, kterou se podařilo ve světě implementovat pouze několika firmám. Produkt je komplexní a modulární a podporuje tvorbu bezpečnostních aplikací softwarovými firmami, které by jinak nebyly schopny zajistit

implementaci kryptografického jádra a PKI struktury. Reflektuje s předstihem na přijaté a připravované zákony ČR o bezpečnosti dat. Je kompatibilní se softwarem jiných producentů, kteří založili svoje výrobky na přijatých mezinárodních standardech S/MIME a dalších.

Více informací o systému IronWare® Security Suite naleznete na našich webovských stránkách, na e-mailové adrese info@aec.cz nebo na kontaktní adrese na konci tohoto „AEC Magazínu“.

Americký Pentagon obětí útoku „neznámého“ viru

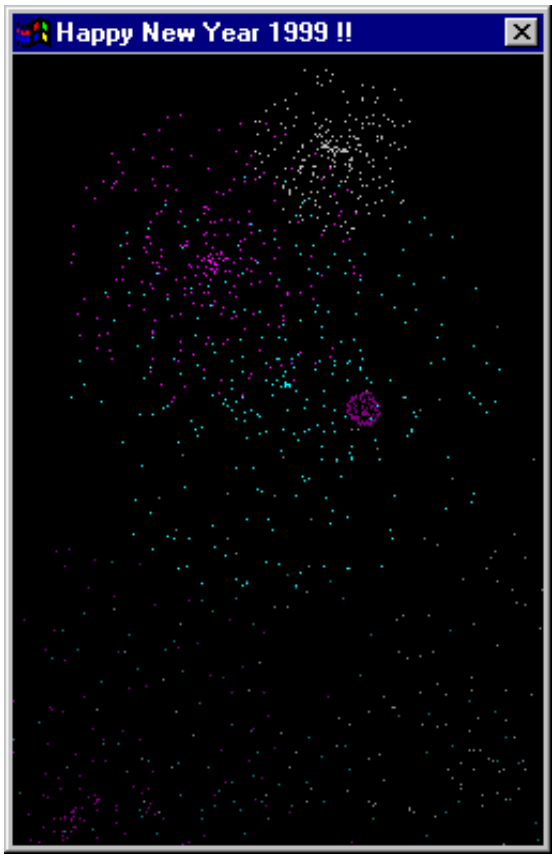
V pátek 22. října 1999 bylo ve vrchním velitelství amerického námořnictva v Pentagonu pěkně veselo. Zdejší počítačová síť se totiž stala terčem neznámého útoku. Několik hodin přitom nebylo jasné, odkud a jakým způsobem je útok vedený – „pouze“ se začala ztrácet citlivá data z počítačů. Mluvčí amerického námořnictva v první chvíli prohlásil, že jde o „ útok provedený novým způsobem nebo virem, o kterém ještě nikdo neslyšel.“

Pravda však byla poněkud prozaičtější – šlo o napadení červem „Zipped_Files.Exe“, který byl poprvé objevený v první polovině června letošního roku. Jedná se o červa (virus, který se šíří prostřednictvím elektronické pošty) s velmi destruktivními účinky. Je totiž schopen prohledat všechny lokální i síťové disky a pátrat po souborech s koncovkou .C, .H, .CPP, .ASM, .DOC, .XLS a .PPT. Nehledá je ovšem z dlouhé chvíle, ale proto, aby je zlikvidoval.

Zničení dat amerického námořnictva šlo velmi jednoduše zabránit. Stačilo, aby uživatelé nespouštěli neznámé přílohy u e-mailových zpráv (lidé jsou zkrátka nepoučitelní) a aby byly k dispozici antivirové programy s aktuálními databázemi virů.

AEC, spol. s r.o. varuje před vánočními a novoročními počítačovými viry

Blíží se doba svátků pokoje a míru a pravděpodobně i doba nepokoje v počítačových systémech kolem roku 2000. V této souvislosti bychom rádi varovali před počítačovými viry, které se mohou objevit právě v době letošních vánočních svátků a nového roku. Se vzrůstající oblibou zasílání přání pomocí elektronické pošty totiž roste riziko infikování počítače, což se děje prostřednictvím virů v přílohách (soubory EXE, DOC atd.). Přitom platí, že odesílatel zprávy vůbec nemusí o přítomnosti viru v systému vědět – některé viry se zcela „drze“ přidávají k odesílaným zprávám automaticky, jiné se distribuují za pomocí adresáře elektronické pošty.



Příkladem může být vir Happy99, který se začal šířit na počátku letošního roku. Na první pohled poměrně nudný ohňostroj, který se objevil po spuštění souboru HAPPY99.EXE v e-mailové zprávě. Ovšem v tomto okamžiku již byl v počítači instalovaný „záškodník“, který se automaticky rozesílal každému, komu uživatel počítače poslal e-mailovou zprávu. Happy99 je v současné době (deset měsíců po objevení!) nejrozšířenějším virem na světě – tomu napomáhá i skutečnost, že Happy99 kromě šíření nevykonává žádnou nebezpečnou činnost.

AEC, spol. s r.o. varuje, že nikdy nelze vyloučit přidání destruktivní rutiny (např. v návaznosti na nějaké konkrétní datum) – vir pak bude mít dost času se rozšířit a poté najednou zaútočit (podobně jako v případě viru CIH alias Černobyl, který byl známý a antivirovými programy detekovatelný deset měsíců – a přesto způsobil 26. dubna 1999 kalamitu, když na celém světě napadl několik miliónů počítačů).

Odborníci na problematiku počítačových virů z **AEC, spol. s r.o.** proto doporučují:

- Neotvírejte nevyžádané PŘÍLOHY u e-mailových zpráv (samotným přečtením e-mailu nemůžete nikdy virus aktivovat!). Žádný zdroj na Internetu není důvěryhodný, zpráva může „chytit“ vir kdekoliv.
- Pokud chcete posílat vánoční či novoroční blahopřání, neposílejte je ve formátu EXE, COM nebo DOC (či jiném potencionálním „nosiči“ virové nákazy), ale text napište přímo do e-mailu. Nemůžete sice odeslat žádné doprovodné efekty typu hezká animace nebo písnička, ale zároveň neriskujete šíření virové nákazy. Každý jistě ocení skromné přání, než honosnou zprávu, která mu vzápětí smaže veškerá data na pevném disku.

- Novoroční či vánoční přání můžete poslat v „bezpečné“ formě RTF nebo obrázku (JPEG, GIF, BMP). Pozor na wordovské soubory přejmenované z DOC na RTF! Pozor také na obrázky v některých aplikacích schopných hostit makroviry (přípony PPT, CDR…)!
- Zálohujte data! Ušetříte si tak spoustu potíží – i v souvislosti s možnými komplikacemi kolem roku 2000.
- Používejte kvalitní antivirový program s nejčerstvější aktualizací, který dokáže „hlídat“ příchozí elektronickou poštu (pozor, ne každý antivir tuto operaci zvládá!). V nabídce antivirových programů **AEC, spol. s r.o.** je to například antivirový program **Norman Virus Control,** do konce letošního roku nabízený za mimořádně zajímavých podmínek (a kromě toho je k dispozici v lokalizované verzi – v češtině).

Thus.A udeří 13. prosince

Na první pohled je W97M/Thus.A (nebo též W97M/Thursday) „obyčejný“ makrovirus. Ovšem zaznamenaný byl již ve více než desítce zemích světa a šíří se především mezi bankovními a pojišťovacími institucemi, tedy mezi . Zatím nikdo nedokáže vysvětlit, proč a jakým kanálem napadl právě tyto organizace.

Jedná se o Word97 makrovirus, který infikuje šablonu Normal.dot a jeho cílem je smazat všechny soubory na pevném disku, je-li systémové datum nastaveno na 13. prosince. Pro banky a pojišťovny by se tak třináctý prosinec letošního roku mohl stát „černým pondělkem“. Všechny antivirové programy v nabídce AEC, spol. s r.o. jsou schopny se s tímto „černým morem“ vypořádat: AVP, F-Secure AntiVirus, Norman i VirusScan.

Ještě jedno varování před virem Kriz

O počítačovém viru Kriz jsme Vás již informovali v říjnovém vydání našeho „AEC Informačního magazínu“. Nicméně – opakování jest matkou moudrosti a v době, kdy se Vám tento materiál dostane do rukou (prosinec) bude nejvyšší čas se ještě jednou přesvědčit, zda skutečně nehrozí napadení právě od tohoto viru. Udeří totiž 25. prosince.

Vir W32.Kriz je rezidentní, navíc své tělo kóduje, čímž ztěžuje možnosti detekce antivirovými prostředky (všechny námi dodávané antivirové programy řady AVP, F-Secure AntiVirus a VirusScan si s ním hravě poradí). Vir napadá knihovnu KERNEL32.DLL, kde se „zavěsí“ na šestnáct jeho funkcí (např. otevřít soubor, nakopírovat, smazat, číst, zapisovat...). Každý soubor, s nímž je některá z těchto funkcí vykonána, napadne. W32.Kriz si přitom hlídá jméno souboru a jako čert kříži se vyhýbá souborům vytvořeným a využívaným některými antivirovými programy.

Kriz je mimořádně nebezpečný – především v případě, že jej budete mít v počítači ke dni 25. prosince. V tento den při otevření jakéhokoliv infikovaného dokumentu dochází k likvidaci CMOS, přepsání dat na všech dostupných discích a následné likvidaci Flash BIOSu stejnou rutinou, jakou využíval dnes již legendární vir CIH.

Přejeme Vám Veselé vánoce bez viru W32.Kriz.

O firmě AEC, spol. s r.o.

AEC, spol. s r.o. je jedním z předních poskytovatelů a výrobců software pro komplexní zabezpečení osobních počítačů jak z hlediska utajení informací, tak antivirové ochrany. Za své produkty obdržela několik prestižních ocenění a také certifikací ISO-9001 a TickIT. Společnost byla založena v roce 1991. Jedná se o ryze českou firmu bez účasti zahraničního kapitálu. V současnosti disponuje prodejní sítí, pokrývající ČR i SR s kancelářemi v Praze, Brně a Bratislavě. Důkazem toho, že Slovensko není jediným zahraničím, ve kterém AEC, spol. s r.o. působí, je distribuční síť v Austrálii, Belgii, Holandsku, Kanadě, Lucembursku, Maďarsku, Německu a v dalších zemích.

Kontakty:

AEC, spol. s r.o.
Bayerova 30, 602 00 Brno
Tel.: 05 / 4123 5466-7
Fax: 05 / 4123 5038
e-mail: info@aec.cz

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

AEC Bratislava, spol. s r. o.
POB 79, Pribinova 25, 810 11
BRATISLAVA, SK
Tel.: +421 (0)7 50633 027
Fax: +421 (0)7 50633 029
e-mail: bratislava@aec.sk

Autorem „AEC Magazínu“ je Tomáš Přibyl: tomas.pribyl@aec.cz