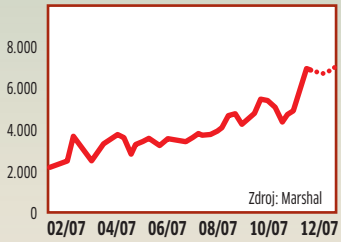
DATA A FAKTA

Barometr nebezpečí
v březnu

Krátká oddechová pauza: Phishing a ostatní útoky zažívají lehkou stagnaci. To ovšem nemůže být důvodem ke snížení obezřetnosti.

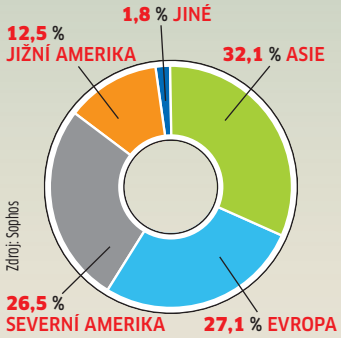
Trend spamu

Spamu stále přibývá



Ačkoliv před koncem roku 2007 došlo k mírnému poklesu, množství spamu trvale narůstá.

Původ spamu



Většina spamu stále pochází z asijského kontinentu. Nově se na druhém místě ocitá Evropa.

BEZPEČNOSTNÍ WEB CHIPU

www.chip.cz

I na našem novém webu najdete zajímavé informace a tipy a triky z oblasti bezpečnosti.

Přehrávače médií – nové nebezpečí

ÚTOKY z webu míří stále častěji na multimediální software. K nejoblíbenějším cílům patří QuickTime, RealPlayer a Windows Media Player.

VALENTIN PLETZER, AUTOR@CHIP.CZ

Jak hlásí americký bezpečnostní úřad SANS, počet bezpečnostních mezer ve Windows se postupně snižuje. Nebezpečných útoků přesto neubývá, neboť hackeři, místo aby si vylamovali zuby na stále lépe chráněných operačních systémech, si nyní berou na mušku aplikace.

Nejnovějšími terči programátorů malwaru jsou QuickTime, RealPlayer a Windows Media Player. Jejich obliba u hackerů má dva důvody: silnou rozšířenost a tím i obrovský počet potenciálních obětí a také to, že při vývoji multimediálních přehrávačů se často pracuje dost lajdácky a nedbá se na zabezpečení. A tak nyní zeje nebezpečná mezera i ve VLC Mediaplayeru.

Nejčastějším problémem přehrávačů je „buffer overflow" (přetečení bufferu) při zpracování videosouborů a streamů. Zneužití tohoto jevu způsobí, že jakmile oběť útoku otevře speciálně upravený soubor, spustí tak nejen video, ale zároveň si stáhne do paměti škodlivý kód. Ten pak většinou slouží k zavedení trojského koně.

Nebezpečná zábava: V přehrávači QuickTime musela být v loňském roce zaplatována většina bezpečnostních mezer – bylo uveřejněno 19 aktualizací.

Kdo si ovšem myslí, že se tomuto riziku vyhne používáním nějakého exotického přehrávače, je na omylu. Bezpečnostní problémy totiž ve většině případů nepostihují ovládací prostředí programu, nýbrž knihovnu videodekodérů. A poněvadž mnoho přehrávačů používá tutéž knihovnu, útok dopadá nikoli na jeden nástroj, ale vždy hned na celou řadu přehrávačů.

Další mrzutost: RealPlayer potají instaluje adware

Trampoty hrozí mediálním přehrávačům také z jiné strany. Už dlouho se zejména uživatelé programů QuickTime a RealPlayer pohoršují nad dotěrným chováním těchto nástrojů. Nyní už iniciativa StopBadware, sdružení IT firem a institucí, dokonce RealPlayer prohlásila za skutečný badware. Instituce svůj krok odůvodňuje tím, že tento software ve verzi 10.5 nedostatečně informuje uživatele o tom, že kromě přehrávače se instaluje také reklamní komponenta. Message Center v Realu pak vkládá reklamu, jestliže uživatel svůj mediální software dobrovolně nezaregistruje.

ŘEŠENÍ: Pokud se přesto nechcete vzdát formátu RealVideo, měli byste sáhnout po alternativě, jako je VLC Mediaplayer, který alespoň neobsahuje žádnou reklamu. Dbejte však přitom na to, abyste tento software vždy měli v nejnovějším stavu. Většina programů k tomuto účelu nabízí automatické on-line aktualizace. Ty mějte bezpodmínečně aktivované. Jenom tak totiž časovou prodlevu mezi odhalením mezery a jejím uzavřením zmenšíte na absolutní minimum.

INFO: www.stopbadware.org

NOVÝ DRUH SPAMU

Už vás pozvali na schůzku?

„Společnost Trend Micro Incorporated varuje před novým typem spamu s názvem Meeting Invite (Pozvánka na schůzku). Během posledních dvanácti měsíců podchytila společnost Trend Micro nejrůznější formáty spamu, toto je však vůbec první případ, kdy byl k šíření spamu zneužit kalendářový systém Google. Spamové filtry jsou obvykle navrženy pro automatické filtrování spamu s přílohami nebo obrazového spamu, avšak tento nový způsob doručování pravděpodobně nezachytí.

Při tomto nejnovějším útoku rozesílají spammeři tzv. nigerijské dopisy a vyhýbají se antispamovým filtrům pomocí pozvánek na schůzku. E-mailové pozvánky jsou personalizovány, každému příjemci zobrazují odlišný odkaz a mohou být nastaveny tak, aby zasílaly i upozornění na schůzku. Tím se snaží obrátit pozornost ke spamované zprávě.

„Tuto metodu doručování spamu pravděpodobně využijí i další typy spamu, jako pump and dump, odkazy na webové hrozby apod.," uvedl Jamz Yaneza, manažer Trend Micro pro výzkumné projekty. „Je dobře možné, že po tomto prvním útoku budou následovat další, které budou k doručování nebezpečných odkazů a ke snaze odcizit citlivé informace dále zneužívat takové nástroje jako kalendář Google."

Trend Micro varuje všechny uživatele, aby věnovali zvýšenou pozornost neočekávaným pozvánkám na schůzku a dalším nevyžádaným mailům. Takové útoky znamenají zvýšené riziko pro příjemce včetně možnosti spuštění škodlivého kódu nebo jiného malwaru.

Další informace naleznete na malwarovém blogu Trend Micro na adrese.

INFO: http://blog.trendmicro.com

INFO

Nová bezpečnostní rizika

FIREFOX

Verze 2.0.0.11 prohlížeče vykazuje četné bezpečnostní mezery. Mezi nimi také trhlinu, která dovoluje útočníkům načíst surfovací historii, a přetečení bufferu případně umožňující vpašování škodlivého kódu. Řešením je pochopitelně aktualizace, protože nejnovější verze tyto mezery odstraňuje. Získáte ji prostřednictvím automatické aktualizace.
INFO: www.mozilla.org

ASUS EEE PC

Levný kompaktní notebook Eee PC firmy Asus si s sebou už z výroby nese několik závažných bezpečnostních mezer. Mezi jinými v síťové službě Samba pro sdílení ve Windows. Je na povážení, že chyby v přizpůsobeném Xandros Linuxu jsou už starší než rok. Do redakční uzávěrky ještě Asus žádný update k dispozici nedal.
INFO: www.asus.com

ADOBE READER

Zdá se, že už od konce ledna kolují po internetu PDF soubory, které využívají bezpečnostní mezeru v Adobe Readeru a počítač oběti infikují trojskými koňmi. Před nečetnými, ale nebezpečnými soubory varují výrobci antivirů. Řešení problému je snadné. Prostřednictvím příkazu Help | Check for Updates si nahrajte nejnovější verzi softwaru.
INFO: www.adobe.com

MCAFEE COMMON MANAGEMENT AGENT

McAfee Common Management Agent 3.6.0.574 a starší obsahuje zranitelnost ve FrameworkService.exe, která umožňuje případným útočníkům způsobit pád aplikace zasláním zákeřných požadavků na port 8081/TCP, na kterém CMA agent naslouchá. Na stránkách výrobce bylo zveřejněno dočasně řešení (viz **https://knowledge.mcafee.com/article/219/615324_f.SAL_Public.html**), na hotfixu MacAfee pracuje.
INFO: zpravy.actinet.cz

VISTA SP1

Trojský kůň místo pirátské kopie

„Zde najdete soubor, jímž můžete „kreknout“ Vistu vzdor Service Packu 1,“ slibuje e-mail. Kdo však připojený odkaz využije, nedostane slíbený nástroj, nýbrž stahovač. Ten pak obratem deaktivuje všechna bezpečnostní opatření a umístí do počítače trojského koně. Mnohé virové skenery tento malware identifikují jako XPack.Gen.

Jakmile je jednou aktivován, uhnízdí se škodlivý kód v adresáři Windows a PC se stane nedobrovolným účastníkem sítě botů. Tím se uzavře ďábelský kruh, neboť infikovaný počítač nyní sám začne vysílat spamové zprávy: e-maily slibující pirátské kopie, aby nalezly nové lehkomyslné oběti.
INFO: www.microsoft.com

PROMIS

Pornospam funguje

Nejdříve oběť obdrží e-mail od „Crazy Video Online“. Najde v něm obraz Britney Spears s vykasanou sukní a bez spodního prádla a kromě toho odkaz na weblog. V blogu je pak oběti slibováno video. Ovšem, jak tvrdí Crazy Video Online, nejprve je nutno nainstalovat speciální přehrávač. Za souborem pojmenovaným „player.exe“ se však neskrývá legitimní software, nýbrž zvláště zlomyslný bot. Kdo tento nástroj spustí, promění svůj počítač v rozesílatele spamu.

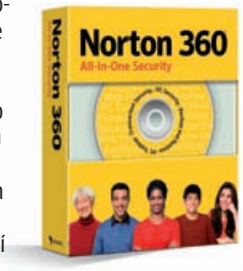
Tato finta je známa už dlouho, ale trik funguje tak dobře, že se všichni výrobci antivirů shodují v názoru, že zde vzniká nová síť botů. Armáda počítačů, která by nakonec mohla být větší než síť Storm Worm.
INFO: www.0-security.de

Norton 360

Společnost Symantec oznámila dostupnost aplikace komplexního řešení zabezpečení Norton 360 verze 2.0. Součástí nejnovější verze aplikace Norton 360 je nyní technologie ochrany prohlížeče (v patentovém řízení). Tato technologie chrání před automatickým stahováním z webu a jinými novými nebo neznámými hrozbami, které využívají zranitelná místa v aplikaci Internet Explorer. Jaké další novinky Norton 360 nabízí?

Ochrana identity

Součástí aplikace Norton 360 je nyní aplikace Norton Identity Safe, která bezpečně uchovává hesla a jiné osobní informace. Aplikace Norton Identity Safe nabízí také pohodlné funkce automatického vyplňování formulářů a přihlášení na důvěryhodné weby jedním kliknutím myší a spolupracuje s technologií ochrany identity aplikace Norton 360 při zajišťování ochrany před phishingovými weby.



Zabezpečení počítače

Novinkou v aplikaci Norton 360 je také sledování sítě. Tato funkce kontroluje stav zabezpečení bezdrátové sítě, mapuje připojená zařízení, upozorňuje uživatele, když se připojí k nezabezpečené síti, a nabízí odborné rady k usnadnění správy nastavení zabezpečení sítě. V aplikaci Norton 360 byla rozšířena funkce inteligentního plánovače na pozadí o schopnost zabránit automatickému spuštění úloh v režimu napájení z baterie a regulace šířky pásma při zálohování on-line nyní minimalizuje dopad na výkon. Uživatelé aplikace Norton 360 mají teď možnost ručně prověřit jednotlivé soubory a složky a vypnout počítač po skončení úlohy.

Zálohování

Zajímavým vylepšením aplikace Norton 360 je těsnější integrace s aplikací Windows Explorer. Uživatelé mají možnost zobrazit v aplikaci Windows Explorer stav zálohování každého dokumentu, hudebního souboru nebo fotografie. Prostřednictvím ikony je možné identifikovat položky, které byly zálohované, a položky, které na zálohování čekají. Jednoduché kliknutí pravým tlačítkem myši a výběr dává nyní uživatelům možnost přidat soubor do seznamu pro zálohování.

Vyladění počítače

Aplikace Norton 360 se nyní také pyšní funkcí mazání souborů z registru, která optimalizuje výkon počítače odstraňováním nepotřebných souborů. Aplikace poskytuje i diagnostickou zprávu, která umožňuje snadné odstraňování systémových potíží a řešení problémů.

Odborná pomoc jedním klepnutím

Součástí aplikace Norton 360 je funkce Odborná pomoc jedním klepnutím, která uživatelům umožňuje rychle získat pomoc jedním kliknutím přímo z rozhraní produktu. Uživatelé mohou rychle řešit obvyklé problémy pomocí funkce Autofix a mohou se obrátit na techniky odborné pomoci společnosti Symantec prostřednictvím telefonu, e-mailu a chatu, který je dostupný 24 hodin denně, 7 dní v týdnu.

Rodičovský zámek a ochrana před nevyžádanou poštou

Uživatelé aplikace Norton 360 mohou získat rodičovský zámek a ochranu před nevyžádanou poštou prostřednictvím volitelné doplňkové sady, kterou si mohou stáhnout zdarma. Rodičovský zámek nyní umožňuje provázat natavení jednotlivých uživatelů s existujícími uživatelskými účty systému Windows a nabízí možnost vybrat předdefinované profily nebo vytvořit vlastní profily, které je možno použít jednou nebo opakovaně. Funkce ochrany před nevyžádanou poštou nyní zahrnuje také zlepšené nastavení filtru nevyžádané pošty, načítání a slučování již existujících seznamů povolených a zakázaných adres z e-mailových adres v aplikaci Outlook a již existujících seznamů aplikace Norton AntiSpam.

Komentář redakce

Přehled novinek je opravdu působivý. Vzhledem k tomu, že část funkcí aplikace převzala i z námi doporučovaného balíku Norton Internet Security 2008, vkládáme do programu poměrně velké naděje. Otázkou pouze zůstává, jak se u Symantecu vypořádali s největší slabinou předchozí verze – velkými systémovými nároky. Poté, co aplikaci důkladně otestujeme, prozradíme vám odpověď na tuto i další otázky…

INFO

Nová bezpečnostní rizika

PRODUKTY FIRMY SYMANTEC

Byly nalezeny dvě závažné zranitelnosti v produktech firmy Symantec. První zranitelnost byla nalezena v ActiveX ovladači (SYMADATA.DLL) přiloženém v AutoFix Support Tool a může způsobovat Stack-Based Buffer overflow (přetečení zásobníku). Druhá chyba byla nalezena ve stejném ovladači a může být zneužita k načtení a spuštění libovolného kódu ze vzdáleného umístění. Zneužití obou zranitelností vyžaduje vedení DNS poisoning nebo Cross-site scripting útoku. Zasažena je celá řada produktů (např. Norton Internet Security 2006 – 2008, Norton 360), ale na webu Symantecu už je k dispozici oprava…

INFO: zprávy.actinet.cz

NOVELL NETWARE, DOS

Novell NetWare 6.5 obsahuje chybu, která může způsobit DoS serveru. Zranitelnost se může projevit například při zpracování určitých požadavků z aplikace iPrint na MacOS X. Více informací naleznete v původním oznámení výrobce (na **secure-support.novell.com**), update pak na serveru **http://download.novell.com**.

INFO: zprávy.actinet.cz

MICROSOFT INTERNET EXPLORER 7

Internet Explorer 7 dovoluje nastavení hlavičky na „Transfer Encoding:chunked“ v setRequestHeader a tím vystavuje prohlížeč „http Request Splitting/Smuggling“ útokům. Při úspěšném zneužití může dojít k ukradení dat uživatele (httponly cookies, autorizační data). Zranitelnost byla zveřejněna na serveru Minded Security (**www.mindedsecurity.com/MSA01240108.html**).

INFO: zprávy.actinet.cz

MALWAROVÝ ŽEBŘÍČEK FIRMY BITDEFENDER

Storm Worm zase úřaduje

Společnost BitDefender zveřejnila žebříček „Top 10 malware“ za měsíc březen. Po velkém oživení vévodí žebříčku trojský kůň Peed (alias Storm Worm). Podle zjištění výzkumných laboratoří společnosti BitDefender mají různé variace tohoto trojského koně na svědomí více než polovinu všech zaznamenaných výskytů malwaru za poslední měsíc. Storm Worm sice vede žebříček, ale dlouhodobě nejrozšířenějším malwarem, který se tentokrát umístil na třetí příčce, je BehavesLike:Trojan.ShellHook. Tento trojský kůň umožňuje útočníkovi spustit na počítači oběti škodlivý program v momentě, kdy uživatel spustí legitimní program či aplikaci.

„Toto je pohodlná cesta, jak spustit škodlivý kód, poskytující útočníkovi uživatelská práva, bez jakéhokoliv přičinění uživatele,“ vysvětluje Sorin Dudea, ředitel antivirového výzkumu společnosti BitDefender. „Nejedná se o příliš skrytý kód, což je běžná charakteristika různých typů současného malwaru. V každém případě tento patří k těm, pro něž byste legitimní využití hledali marně.“ Zbytek žebříčku obsadili už starší, ale přesto „nezlomní“ e-mailoví červi (mass maileři).

Top 10 malware za měsíc březen

1. Trojan.Peed.Gen	55,58 %
2. Win32.Netsky.P@mm	5,97 %
3. BehavesLike:Trojan.ShellHook	2,07 %
4. Win32.NetSky.D@mm	1,76 %
5. Win32.Netsky.AA@mm	1,54 %
6. Win32.Nyxem.E@mm	1,22 %
7. Win32.Netsky.B@mm	1,07 %
8. Win32.Netsky.C@mm	1,03 %
9. Trojan.Kobcka.CZ	0,83 %
10. Win32.Mydoom.M@mm	0,72 %
11. ostatní	28,21 %

Zdroj: BitDefender

USB hrozby jednoznačně vedou

Proces Windows AutoRun snižuje **BEZPEČNOST POČÍTAČE** – to potvrzuje i nový žebříček hrozeb. Chip vám dokonce doporučuje ho vypnout…

Top 10 hrozeb v březnu 2008

1.	INF/Autorun	10,30 %
2.	Win32/Adware.search.aid	4,42 %
3.	Win32/Adware.Virtumonde	2,81 %
4.	Win32/Toolbar.MyWebSearch	2,07 %
5.	Win32/TrojanDownloader.Agent.KGV	1,74 %
6.	Win32/IRCBot.AAH	1,67 %
7.	Win32/Adware.Virtumonde FP	1,55 %
8.	Win32/Agent.NHE	1,32%
9.	Win32/Agent	1,26 %
10.	Win32/Pacex.Gen	1,23%

Statistický systém ESET ThreatSense.Net vyhodnotil v březnu 2008 jako nejčastější hrozbu směs infiltrací INF/Autorun (10,3 %). Každá desátá zachycená hrozba tedy měla podobu škodlivého kódu, který využívá soubor autorun.inf s informací. Počítač je nakažen po vložení přenosného média, nejčastěji USB disku. Jakmile je přenosné médium se souborem autorun.inf, například USB klíč nebo CD/DVD disk, vloženo do počítače, dojde k automatickému načtení obsahu nebo spuštění instalačního procesu. Operační systém Windows v případě přítomnosti souboru autorun.inf na přenosném médiu spustí jeho instrukce, čehož útočníci využívají. Nakažený autorun.inf může způsobit nainstalování trojského koně, rootkitu nebo keyloggeru.

„Nárůst počtu tzv. USB hrozeb jsme zaznamenali před více než půl rokem. Počet zachycených infiltrací INF/Autorun tehdy dosahoval zhruba 2 % všech odhalených nákaz. Od začátku tohoto roku však jde o globální hrozbu," říká Juraj Malcho, vedoucí virusové laboratoře společnosti ESET.

Randy Abrams, šéf technického vzdělávání v ESET San Diego, tvrdí, že ponechání procesu Windows AutoRun v aktivní pozici dramaticky snižuje bezpečnost počítače, a doporučuje ji vypnout. Dokonce i v případě, že programy jako třeba iTunes žádají její aktivování.

Další hrozby

V březnu 2008 zůstal významnou globální hrozbou adware. Na druhém až čtvrtém místě ESET eviduje Win32/Adware.SearchAid (4,42 %), Win32/Adware.Virtumonde (2,81 %) a Win32/Toolbar.MyWebSearch (2,07 %). Pátou nejčastější počítačovou hrozbou je trojan, který slouží k vykrádání citlivých údajů a hesel z počítače uživatele – Win32/TrojanDownloader.Agent.KGV.

Top hrozby v Česku

Lokální statistika ESET ThreatSense.Net® za březen 2008 registruje jako top tři nejčastější hrozby v Česku adware Win32/Adware.SearchAid (7,49 %), HTML/Phishing.gen trojan (6,74 %) a INF/Autorun virus (2,95 %). Hrozba HTML/Phishing.gen trojan souvisí s vlnou phishingových útoků s cílem získat přístup k citlivým údajům klientů České spořitelny.

Komentář redakce

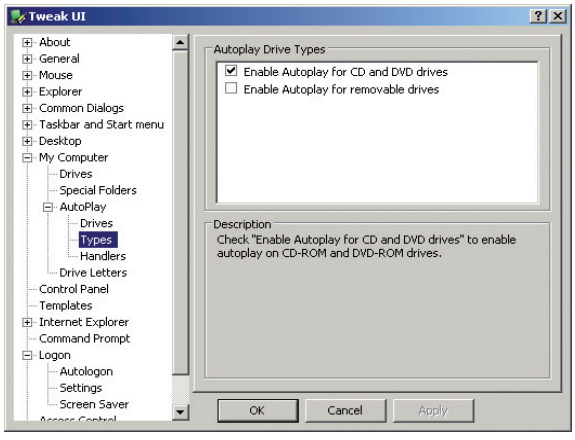
O rizikovosti povolení automatického spouštění médií jsme psali už několikrát. Ovšem teprve s masovým rozšířením USB disků začíná tento problém nabývat na palčivosti. Zatímco před instalací neznámého programu zaváhá alespoň část uživatelů, zasunutí cizího USB disku nedělá problémy téměř nikomu. A jak to vyřešit? Vypnutím funkce Autorun. Existuje celá řada možností, jak toho dosáhnout, ale tři z nich nám připadají jako nejrozumnější.

1) Klávesa Shift
Jestliže potřebujete (z jakéhokoliv důvodu) mít funkci autorun zapnutu, lze ji před zasunutím USB disku (krátkodobě) vyřadit z provozu stisknutím a podržením klávesy Shift.

2) TweakUI
Pokud si rádi hrajete se systémem, je optimálním řešením nástroj TweakUI, který kromě vypnutí funkce autorun umí i celou další řadu užitečných věcí…

3) Kompletní vypnutí funkce autorun pro všechny vstupy
Patří váš počítač k „ohroženým druhům"? Používáte často přenosné disky kamarádů, spouštíte vypálená CD a připojujete neznámá média? Pak doporučujeme vypnout funkci autorun zcela. Postup je snadný: spusťte editor registru a přejděte do větve HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer. V pravé části okna najdete hodnotu NoDriveTypeAutoRun, která má (šestnáctkovou) hodnotu 91. Změňte ji na 95, ukončete editor registru a restartujte počítač.

Bez šance: Samotná Windows zablokování automatického spouštění médií příliš neusnadňují…



Tweak UI: Umožňuje snadné vypnutí CD/DVD mechanik i vyjímatelných disků…

CSIRT.CZ
Poslední obranná linie?

Na počátku dubna byla zahájena činnost unikátního projektu CSIRT.CZ. Ten má v rámci grantového programu Ministerstva vnitra s názvem „Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů ČR“ zvýšit prostřednictvím tzv. CSIRT týmů schopnost českého internetového prostředí, efektivně řešit vzniklé bezpečnostní incidenty a podle možností jim předcházet. Předností nového pracoviště CSIRT.CZ je přímá spolupráce s ostatními světovými CSIRT týmy. To umožňuje ve velmi krátké době účinně řešit nejen útoky z různých částí světa, ale i prevenci samu.

CSIRT: Na webu projektu již lze nalézt například návod pro hlášení bezpečnostního incidentu.

Cesta vpřed?

Mezi nejdůležitější úkoly pracoviště patří budování distribuované sítě pracovišť CSIRT a nastavování vzájemných vazeb mezi těmito týmy. Do r. 2010 by v České republice měla vzniknout celá hierarchie týmů CSIRT. Dalším úkolem je příprava organizačních a legislativních podkladů pro provoz vrcholových týmů CSIRT v České republice, a to ve spolupráci s ostatními řešiteli grantového projektu (právníky, sociology) a Ministerstvem vnitra.

Úkoly a zdroje

CSIRT.CZ bude zároveň sloužit jako místo „poslední záchrany“ v případě útoku, kdy napadená síť nedokáže kontaktovat správce sítě, jenž je zdrojem útoku, nebo kdy správa dané sítě na hlášení nereaguje. Pokud je detekován útok z jiného státu, CISRT.CZ zahájí v rámci internetové sítě okamžitou mezinárodní spolupráci, která povede k vyřešení problému. Spolupráce s CSIRT.CZ ve věcech internetového útoku však vyžaduje jistý stupeň profesionální komunikace a znalostí, tudíž je tato pomoc určena pro ostatní CSIRT týmy jako poslední instance při řešení útoku, nikoliv jako „helpline“ pro běžného uživatele. Nejčastější nebo nejzávažnější útoky budou spolu s dalšími informacemi zveřejňovány na internetových stránkách **www.csirt.cz**, stejně tak jako potřebné metodické, analytické a další materiály. Celý program profesionálně zajišťuje sdružení CESNET, které je zodpovědné za metodiku programu, a společnost NESS Czech, která se stará o provozní stránku. Hlavním koordinátorem českého grantového projektu je doc. Ing. Václav Jirovský, CSc., který zároveň zastupuje Českou republiku v bruselském výboru, pokud jde o bezpečnost.

Historické kořeny

Potřeba systému CSIRT v každé rozsáhlejší komunikační a informační infrastruktuře byla identifikována již v roce 1988 v USA, kdy se objevil první počítačový červ (program, který napadá počítače v síti) – tzv. Morrisův červ. Dokázal zahltit značnou část tehdejší sítě (z ní později vznikl internet), a aby tuto situaci bylo možné zvládnout, byl na Carnegieho-Mellonově univerzitě v Pittsburghu ustaven bezpečnostní tým Computer Emergency Response Team Coordination Center (CERT). Na základě dlouholetých zkušeností tohoto týmu byly popsány modely fungování CSIRT, nejlepší modely v oblasti řešení bezpečnostních počítačových incidentů. Týmy CSIRT jsou zakládány ve všech vyspělejších státech světa – pro ně jsou totiž, v důsledku jejich vysoké informatizace, počítačové incidenty skutečnou hrozbou.

Komentář redakce:

O potřebnosti a důležitosti takovéto instituce nemůže být nejmenších pochyb. Velkým problémem je však nulová podpora v současných zákonech. Podle zveřejněného plánu končí „pilotní provoz“ projektu 1. ledna 2011 a je silně nepravděpodobné, že do té doby dojde ke změně zákonů. Dá se tedy říci, že minimálně čtyři roky bude organizace bezzubá. Ve chvíli, kdy zjistí závažnější problém, vyžadující například „odstřižení serveru“, bude muset kontaktovat policii a nechat akci na ní. Důsledky takového jednání je asi zbytečné rozvádět…

INFO

Význam zkratek

CSIRT (COMPUTER SECURITY INCIDENT RESPONSE TEAM)
subjekt, jehož primárním úkolem je řešit bezpečnostní incidenty, koordinovat jejich řešení a předcházet jim.

CERT (COMPUTER EMERGENCY RESPONSE TEAM)
jedná se o synonymum pro CSIRT; CSIRT je chráněnou značkou Carnegieho-Mellonovy univerzity.

TF-CSIRT
mezinárodní fórum umožňující spolupráci týmů CSIRT na evropské úrovni. Dělí se na skupinu uzavřenou, jež je přístupná pouze akreditovaným týmům, a skupinu otevřenou, přístupnou všem zájemcům o práci těchto týmů. TF-CSIRT se schází obvykle několikrát ročně.

FIRST (FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS)
světové fórum týmů CSIRT.

NOVÝ PRODUKT

Avast! 4.8 antivirus i proti spywaru a rootkitům

Na konci března firma ALWIL Software oznámila vydání nové verze programu avast! antivirus, a to verze 4.8. Mezi novinky přidané do programu patří antispywarové ochrany, certifikované procedurou Checkmark West Coast Lab, a antirootkitová technologie. Program avast! 4.8 antivirus také přidává „sebeobranu“, která znemožňuje útoky proti programu samému. Program je možné stáhnout ze stránek **www.avast.com** a je dostupný ve třech edicích. Pro domácí nekomerční použití je k dispozici zdarma avast! Home Edition. Pro komerční využití je určen avast! Professional Edition a pro domácnosti a domácí kanceláře avast! Professional Family Pack, „pokrývající“ až deset počítačů a jeden Windows Home Server. Obě placené edice si lze vyzkoušet – jsou dostupné na stránkách **www.avast.com**. Dosavadní uživatelé programů avast! Home a avast! Professional mohou svůj avast! aktualizovat přímo z uživatelského rozhraní programu bez nutnosti nové instalace.