DATA A FAKTA

Barometr nebezpečí v září

Hackeři vyhledávají bezpečnostní mezery stále více v sociálních sítích, aby jimi propašovali své záškodnické programy mezi běžné uživatele.

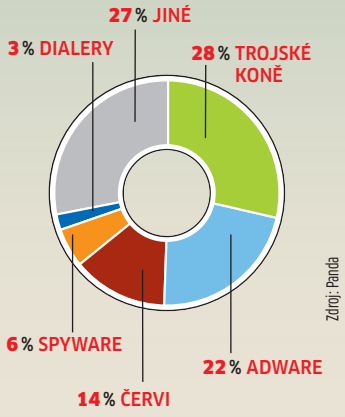
Cíle útoků

1. Browsery
2. Flash
3. ActiveX
4. SQL databanky
5. Adobe Reader

Zdroj: Websense

Nejčastějšími vstupními branami malwaru jsou bezpečnostní mezery v browserech, ve Flashi a v ActiveX.

Malwarové útoky



Zdroj: Panda

Nejúspěšnějšími druhy škůdců v roce 2008 jsou zatím trojské koně a adware.

Poplach pro Vistu: Systém prolomen

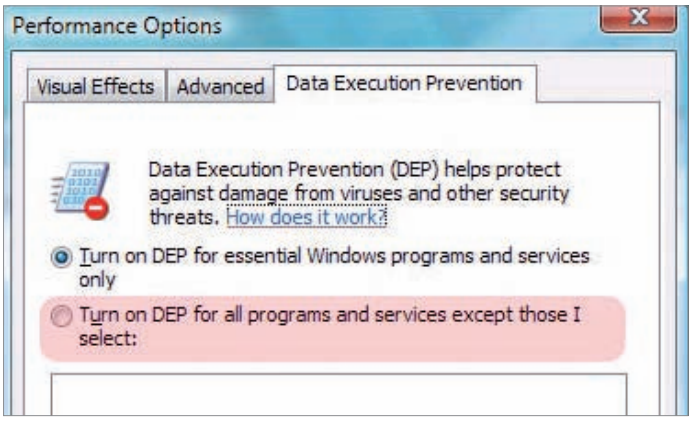
Vyvolat pod Vistou **PŘETEČENÍ BUFFERU** není tak jednoduché. Dva hackeři předvedli hned několik cest, jak toho lze přesto dosáhnout.

MARKUS MANDAU

Microsoft zavedl v posledních letech nové techniky, jimiž chce lépe zabezpečit správu paměti zejména ve Vistě. Cílem opatření je zneškodnit stav „buffer overflow" jako standardní nástroj hackerů. Toto tzv. přetečení bufferu signalizuje situaci, kdy se nějaká aplikace pokusí do vyhrazené oblasti paměti zapsat příliš mnoho dat. Dojde přitom k přepsání následujících oblastí, které jsou rezervovány pro jiné úlohy. Hackeři tak dokážou do sousední oblasti paměti dopravit záškodnický kód a také jej tam spustit.

Na bezpečnostní konferenci Black Hat nyní dva specialisté demonstrovali, jak lze účinnost každé z těchto nových technologií ochromit. Dva důležité ochranné mechanismy, DEP (Data Execution Prevention) a ASLR (Address Space Layout Randomization), je možné relativně jednoduše obejít za předpokladu, že v počítači je také nainstalován zranitelný software.

Při DEP označují Windows počínaje XP SP2 všechny oblasti, které obsahují spustitelný kód, jako chráněné proti zápisu. Teoreticky vzato je tedy přetečení bufferu nemůže postihnout. Bohužel však tuto techniku nezvládají některé velice rozšířené programy, jako IE7 a Firefox 2. V těchto případech Windows mechanismus DEP vypínají. Bezpečnější surfování zajistí Firefox 3 nebo také IE8 – oba browsery už DEP podporují. Ochranu DEP však znehodnotí také Java, neboť její správa paměti vždy zapíná povolení zápisu. Pro buffer overflow z Java appletů tedy překážka v podobě DEP nijak neplatí.



Pochybná ochrana: Pod Vistou může uživatel nastavit Data Execution Prevention. Pomůže to však jen u programů, které DEP podporují.

Bezcenná ochrana: Techniku Visty aplikace nepoužívají

Technika ASLR vypadá jako docela chytrý nápad. Při zavádění programu do operační paměti volí Vista pro části spustitelného kódu náhodně přidělené úseky paměti. Útočník pak nemůže vědět, kde musí vyvolat přetečení bufferu, aby mohl paměťovou oblast přepsat vlastními daty.

Jenomže ASLR funguje jen v případě, že nějaký DLL soubor nastaví odpovídající příznak. To však činí právě jen DLL soubory patřící pod Windows. Externí aplikace tuto zásadu nedodržují důsledně. Jinou metodu, jak zneschopnit ochranu ASLR, představuje tzv. „sprejování": masovou duplikací a distribucí škodlivého kódu v paměti může útočník poměrně jistě zasáhnout oblast, kterou Windows metodou ASLR přidělila.

O těchto bezpečnostních mezerách zatím Microsoft mlčí. Ovšem oprava nejspíš nebude snadná, neboť problém často nespočívá v operačním systému, ale ve spolupráci Windows s externími aplikacemi.

INFO: www.microsoft.com

TRUSTPORT NET GATEWAY 5.2

Ochrana počítačových sítí

Společnost TrustPort přichází na trh s novou verzí serverového řešení TrustPort Net Gateway. Produkt TrustPort Net Gateway 5.2 se prodává od začátku října a je nástupcem TrustPort Internet Gateway 5.1, která bude podporována do konce ledna 2009.

TrustPort Net Gateway je řešení pro souhrnnou ochranu počítačové sítě před riziky, vyplývajícími zejména z internetové komunikace. Funguje jako bezpečná brána, monitorující veškerý poštovní a webový provoz mezi vnitřní sítí a vnějším světem. Zajišťuje spolehlivou autorizaci uživatelů a šifrování dat, takže nabízí věrohodnost a důvěrnost komunikačních kanálů.

Mezi zlepšení, která TrustPort Net Gateway 5.2 přináší, patří novinky v oblasti ochrany elektronické pošty i v oblasti prohlížení webových stránek. Došlo také k optimalizaci grafického uživatelského rozhraní a nápovědy. Novinkou je též zdokonalená analýza poštovního provozu, která poskytuje snadné dohledání ztracené zprávy v záloze nebo ve virové či spamové karanténě, s možností zprávu znovu poslat adresátovi. Pro plynulé odesílání odchozí pošty nabízí řešení funkci privilegovaného portu, užitečného v případě zahlcení serveru velkým množstvím příchozí pošty. Jako součást TrustPort Net Gateway 5.2, ale také samostatně, se dodává TrustPort WebFilter 5.2, řešení sloužící ke kategorizaci webových stránek, k monitorování a blokování nežádoucích stránek spadajících do definovaných kategorií.

BEZPEČNOSTNÍ SOFTWARE

Dvakrát více bezpečnosti

Před koncem roku je na trhu s bezpečnostními programy živo. Nám se dostaly do rukou dvě absolutní novinky, které jsme si nainstalovali a otestovali.

Blížící se zimu v redakci nepoznáme pouze podle listí padajícího na nedaleké hroby na Olšanech, ale také podle e-mailů plných superlativů. S pomalu přicházejícím koncem roku se totiž v našich schránkách začínají objevovat informace o produktech pro příští rok, které se ve většině případů vyznačují neuvěřitelným přebytkem nadšení a zoufalým nedostatkem soudnosti. U programů z oblasti bezpečnosti platí tento fakt obvykle dvojnásob – pokud bychom měli věřit všem reklamním slibům, surfovali bychom téměř bez zábran, bezpečnostní balíky by počítač vůbec nebrzdily a malware by absolutně neměl šanci. O smutné realitě se pak po nainstalování těchto programů může přesvědčit kdokoliv. Pomalu se „plazící“ systém, brzděný sebemenším náznakem aktivity bezpečnostního balíku, ve spojení s komplikovaným ovládáním – to je stručná charakteristika „dobře zabezpečeného“ počítače let minulých. Od tohoto podzimu ale může být všechno jinak…

Norton Internet Security 2009 (NIS 2009)

Ani letos nebyla tisková zpráva Symantecu nijak výjimečná. Slovíčky jako „vylepšení“, „rychlejší“ a „bezpečnější“ se to v ní jen hemžilo a míra optimismu několikrát překročila hranici dosažitelnou po požití alkoholu. I přesto, že s předchozí verzí programu (NIS 2008), vítězem našeho bezpečnostního testu, jsme byli až na pár drobností spokojeni, přistupovali jsme k novince poněkud s rozpaky. Opravdu to půjde ještě lépe? Vzali jsme tedy našeho loňského favorita a postavili jsme ho přímo proti nováčkovi.

Hned v úvodu vám prozradíme, že odpovědí na předchozí otázku je jednoznačné a překvapivé ANO. Jde to podstatně lépe. Při testech většiny programů se o instalaci příliš nezmiňujeme – jedná se o nudný a zdlouhavý proces, který většina uživatelů bere jako nutné zlo. Symantec překvapivě ukázal, že to jde i jinak – kompletní bezpečnostní balík byl i na starším a pomalejším počítači nainstalován za necelé tři minuty, a to prostřednictvím jediného kliknutí! To byl však pouze začátek. Dalším šokem byly systémové nároky – pokud NIS 2009 pracuje „v pozadí“, zabere méně než 10 MB paměti RAM, a i při náročnější práci (sken systému) se nároky pohybují okolo přijatelných 60 MB. Podobné jsou i nároky na procesor – „na pozadí“ se jednalo přibližně o 2 % výkonu, při skenování kolísaly na pomalejším počítači mezi 50 a 70 %. Na průměrně výkonném PC si činnosti programu téměř nevšimnete.

Zajímavě je také řešen systém aktualizací – na rozdíl od konkurence zde probíhá přibližně každých 10 minut tzv. pulzní aktualizace, která počítač téměř nezatěžuje. Ve finále se o aktuálnost produktu vůbec zajímat nemusíte, přičemž jeho stav máte neustále „na očích“ – elegantní a praktické.

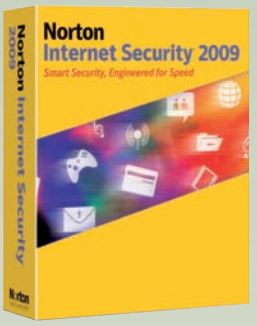
DALŠÍ NOVINKY Jako další zajímavou novinku lze označit vylepšenou prevenci proti škodlivým útokům pomocí multimédií – Intrusion Prevention System (IPS). Přímé útoky na operační systém začínají být pomalu, ale jistě nahrazovány útoky na „pomocné programy“ – často právě v oblasti multimédií. Filmoví nadšenci a hráči uvítají tzv. tichý mod, který automaticky odloží méně naléhavé úlohy a výstrahy, pokud uživatel zrovna hraje hru nebo sleduje film.

Funkcí, která nám v předchozích verzích NIS chyběla, je „obnovení systému“. Jde o sadu nástrojů, které dokáží v případě rozsáhlého napadení systému obno-

MCAfee Internet Security 2009: Novinka nejen v boji proti malwaru.

Norton Internet Security 2009: Příjemné překvapení letošního podzimu…

SHRNUTÍ



Norton Internet Security 2009

Doporučená cena: 1 459 Kč (licence pro 1 uživatele)

- ⊕ rychlá a bezproblémová instalace, minimální systémové nároky, minimální brzdění počítače při práci, přehledné ovládání
- ⊖ cena za licenci pro 3 uživatele by mohla být nižší…

McAfee Internet Security 2009

Doporučená cena: 1 699 Kč (licence pro 3 uživatele)

- ⊕ přijatelné systémové nároky, rychlost skenování
- ⊖ místy komplikovanější ovládání, zbytečně složitá instalace

vit a zabezpečit důležitá systémová data. Vylepšeno bylo také rozhraní a ovládání, ale vzhledem k tomu, že jsme s ním byli spokojeni už i v předchozí verzi, zde můžeme jen lehce souhlasně kývnout. Poslední funkcí, která stojí za zmínku, je vylepšená ochrana prohlížečů proti webovým útokům, přičemž kromě standardního Internet Exploreru chválíme i ochranu Firefoxu. I přes jeho stále rostoucí popularitu bývá často bezpečnostními nástroji poněkud přehlížen.

A to nejlepší na konec: Symantec nabízí bezplatnou technickou podporu e-mailem a po telefonu (zde platíte jen cenu hovoru). Pro zkušenější uživatele je navíc k dispozici diskusní fórum (Norton Users Forum beta – **http://community.norton.com/norton/**) s desítkami tisíc příspěvků.

ZÁVĚR Musíme přiznat, že v případě NIS 2009 jde jednoznačně o překvapení podzimu. Doposud jsme v redakci neměli žádný produkt podobného zaměření a rozsahu, který by se spokojil s tak nízkými systémovými nároky. V některém z příštích čísel Chipu se podíváme ještě více pod pokličku programu a otestujeme jeho bezpečnostní schopnosti ve srovnání s konkurencí, avšak už v této chvíli můžeme program bez nadsázky prohlásit za kandidáta na titul „Příjemné překvapení roku 2008“.

	Zabraná RAM			Zatížení CPU		
	na pozadí	aktualizace	skenování	na pozadí	aktualizace	skenování
Norton Internet Security 2009	>10MB	>10MB	60MB	2%	>10%	30-70%
McAfee Internet Security 2009	58,6 MB	80	110 MB	>5%	40-70%	40-70%

McAfee Internet Security 2009 (MIS 2009)

I na druhé bezpečnostní novince, kterou jsme na našich počítačích testovali, je znát snaha o zrychlení a redukci systémových nároků. Výsledek sice není tak markantní jako v případě NIS, i tak jsou ale požadavky na procesor a paměť RAM podstatně nižší než u většiny konkurenčních produktů. Například při běhu na pozadí byla u pomalejšího počítače zátěž procesoru okolo 5%, při skenování se zvýšila na stále přijatelných 40–70%. O něco horší byly paměťové nároky. I ve „stavu nečinnosti“ balík zabral v paměti 60 MB, po aktivaci bezpečnostního centra (a poté při skenování disku) to bylo ještě o dalších 20 (40) MB více. Nutné je ovšem podotknout, že i na průměrně rychlém počítači budete moci bez problémů pracovat, aniž by vás kontrola zabezpečení brzdila.

NOVINKY A VYLEPŠENÍ McAfee Internet Security 2009 nabízí všechny důležité komponenty pro zabezpečení počítače – antivir, antispyware, antispam, firewall a ochranu identity. Balík také spolupracuje s rozhraními nejpoužívanějších vyhledávačů a blokuje škodlivý obsah již na této úrovni. Jako příjemný bonus lze označit funkci McAfee SiteAdvisor, která nabízí barevné označování webových serverů podle jejich důvěryhodnosti a uživatele tímto způsobem varuje před návštěvou nebezpečných nebo rizikových webů. Nabízí také funkci, která nalezne všechny soubory obsahující důvěrné informace a umožní je v případě potřeby z počítače odstranit. Ani zde nechybí tzv. tichý mod, nabízející režim, ve kterém MIS jen minimálním způsobem „komplikuje“ používání dalších programů (například pokud uživatel sleduje filmy nebo hraje hry). Automaticky se odloží také aktualizace, zobrazení varování nebo další činnosti bezpečnostního softwaru. Rodiče u MIS 2009 jistě ocení možnost definovat způsob, jakým mohou internet využívat děti – včetně zákazu definovaného typu webů (erotika, násilí…). Za zmínku stojí i nabídka automatického zálohování nejdůležitějších souborů na CD/DVD, USB nebo síťový disk.

ZÁVĚR McAfee Internet Security 2009 nešel ve snižování systémových nároků tak daleko jako Symantec, ale i tak nabízí povedený produkt s celou řadou zajímavých funkcí.

NOVÝ SOFTWARE

Kaspersky pro rok 2009

Společnost PCS, oficiální distributor Kaspersky Lab pro ČR a SR, oznámila uvedení nové generace bezpečnostních produktů Kaspersky.

Produkty Kaspersky Internet Security 2009 a Kaspersky Anti-Virus 2009 kombinují výhody nového antivirového jádra s podstatně vyšší rychlostí skenování a přelomové technologie HIPS, sloužící k blokování škodlivých programů ještě před přidáním signatur do antivirových databází. Kaspersky Internet Security 2009 se zaměřuje především na ochranu systému před nákazou, která je mnohem efektivnější než náprava následků.

Virtuální klávesnice ochrání hesla

Rovněž byla rozšířena nabídka nástrojů na ochranu důvěrných uživatelských dat. Nová generace produktů nyní brání důvěřivým uživatelům v přístupu na známé podvodné stránky. Zabraňuje také odcizení důležitých hesel a uživatelských jmen, ke kterému může dojít prostřednictvím softwaru typu keylogger. Kaspersky Internet Security 2009 obsahuje i virtuální klávesnici, která umožňuje uživatelům bezpečně zadávat jména a hesla. Kromě toho předchází Kaspersky Internet Security 2009 zcizení údajů přenášených prostřednictvím zabezpečených připojení (HTTPS, SSL). Může také odstranit všechny stopy po aktivitě uživatele na internetu (dočasné soubory, cookies atd.).

Všechny součásti dřívějších verzí produktu byly různými způsobem vylepšeny a rozšířeny – včetně firewallu, heuristického analyzéru, modulu rodičovské ochrany a antispamového modulu.

Kaspersky Anti-Virus 2009 a Kaspersky Internet Security 2009 byly vyvinuty s ohledem na systémové požadavky pro Windows Vista a jsou plně kompatibilní s 32bitovou i 64bitovou verzí tohoto operačního systému. Více informací o Kaspersky Anti-Virus 2009 a Kaspersky Internet Security 2009 naleznete na **www.kaspersky.cz**.

Bezpečněji: Kaspersky Internet Security 2009 také obsahuje virtuální klávesnici, která umožňuje uživatelům bezpečně zadávat jména a hesla.

Novinky

Kaspersky Internet Security 2009 obsahuje inovační modul Application Activity Filter (filtr aktivit aplikací), který používá technologii HIPS (systém prevence napadení hostitele) s proaktivními obrannými prvky a zabudovaným firewallem. Tím je systém chráněn před všemi známými i neznámými typy hrozeb. Průběžně aktualizovaná „bílá listina" důvěryhodných aplikací podstatně snižuje nároky na interakci s uživatelem.

Další novinkou je indexovací systém, který slouží k přidělování bezpečnostního hodnocení neznámým aplikacím. Tak jsou omezena práva a funkce potenciálně nebezpečných aplikací – například přístup k systémovým souborům a složkám, k systémovému registru a k souborům vytvořeným uživatelem.

INFO

Nová bezpečnostní rizika

AVG ANTI-VIRUS

Skener antivirového stroje není odolný proti útokům typu „denial of service". Speciálně upravené archivní soubory mohou vyvolat nekonečné programové cykly, které zablokují CPU.
► **Řešení:** Mezeru odstraní aktualizace na verzi 8.0.156.
INFO: www.grisoft.cz

REAL PLAYER

Tento software vykazuje dvě velké slabiny: nespolehlivý plug-in pro ActiveX přivodí havárii browseru a v přehrávači lze po vyvolání přetečení bufferu spustit škodlivý kód. Výrobce na své webové stránce dává k dispozici opravy pro verze přehrávače 10 a 11.
INFO: www.real.com

SAFARI

Kvůli chybě ve správě cookies může útočník zjistit přístupová data uživatele. Týká se to surfování v doménách typu „com.au" a „co.uk". Záplata je v nedohlednu, zůstaňte na doméně .cz.
INFO: http://kuza55.blogspot.com

NOVELL EDIRECTORY

Bylo nalezeno několik zranitelností v databázi Novell eDirectory (více informací viz **www.novell.com/support/viewContent.do?externalId=3477912**), které mohou být zneužity ke kompromitování uživatelského systému a způsobit DoS. Tyto chyby postihují verzi 8.7.3 SP10. Jako řešení se doporučuje update na verzi 8.7.3 SP10 FTF1.
INFO: zpravy.actinet.cz

MPLAYER

Zranitelnosti jsou způsobeny chybami integer underflow ve funkci „demux_real_fill_buffer()" v ibmpdemux/demux_real.c. Mohou být zneužity k útokům buffer overflow a spuštění libovolného kódu pomocí upravených souborů Real Media. Více informací naleznete v původním oznámení na adrese **www.ocert.org/advisories/ocert-2008-013.html**. Zranitelnost je hlášena ve verzi 1.0rc2, ostatní verze mohou být také zranitelné.
INFO: zpravy.actinet.cz

MICROSOFT GDI+

V Microsoft GDI+ byla nalezena zranitelnost způsobující Denial of Service při zpracování ICO souborů. Vzdálený útočník toho může zneužít k zapříčinění pádu dané aplikace a odepřít tak tuto službu legitimním uživatelům. Více informací najdete na serveru Securityfocus **(www.securityfocus.com/bid/31432/info)**.
INFO: zpravy.actinet.cz

FLASH PLAYER

Updatový podraz

Většina videoportálů v poslední době sází na Flash Player firmy Adobe. To je pro hackery dostatečný důvod pro to, aby se touto cestou pokusili podstrčit uživatelům malware: na stránkách MySpace a Facebook se stále častěji objevují videa s typicky atraktivními pojmy ze světa celebrit, jako třeba „Paris Hilton". Klikne-li uživatel na takový odkaz, ocitne se na zfalšované stránce YouTube, která ho vyzve k aktualizaci Flash Playeru. Dvojité kliknutí na codecsetup.exe však ve skutečnosti nainstaluje červa Koobface. Ten pak napadené PC začlení do sítě botů. Podobně fungují také údajné maily televizní stanice CNN. Ty rovněž obsahují odkazy na videa s podvrženou aktualizací přehrávače. Adobe radí přezkoušet ve Vlastnostech souboru digitální certifikát aktualizace.
INFO: www.adobe.com

BEZPEČNOSTNÍ STUDIE

Nebezpečné komunitní weby

Společnost phion AG okomentovala průzkum na téma „Ochrana soukromí v platformách společenských sítí“, provedený Fraunhoferovým institutem.

„Výsledky průzkumu Fraunhoferova institutu jasně ukazují, že nedostatečné využívání šifrování a často nedostatečné ověřování uživatelů na platformách společenských sítí umožňuje špehovat citlivá uživatelská data a otevírá dveře pro kriminální aktivity s uživatelskými identitami a důvěrnými uživatelskými daty. Členové komunitních portálů se přímo vystavují nebezpečím, o nichž často nemají potuchy. Zatímco on-line bankovnictví, krádežím a zneužití dat se média často věnují a příslušné formality a regulace předepisují velmi vysoký stupeň zabezpečení, pro platformy společenských sítí to v žádném případě neplatí. Výsledkem je nedbalé nakládání s citlivými daty. Komunitní portály jsou sice obecně koncipovány jako otevřené platformy, ale zároveň slouží jako datová centra, kde jsou uloženy důvěrné informace. Proto představují atraktivní cíl pro útočníky. Provozovatelé společenských sítí by měli mít povinnost zajistit bezpečné nakládání s důvěrnými daty.

Je to něco, k čemu vyzýváme nejen komunitní portály využívané k soukromým účelům, ale také v daleko seriózněji tónu pro podnikové platformy. Zaměstnanci mnoha společností totiž tyto platformy čím dál častěji využívají jako rozšíření systémů CRM k navazování dialogu se zákazníky, obchodními partnery a dalšími cílovými skupinami. V důsledku potom důležitá podniková data, například informace relevantní pro prodej, nejsou při přenosu vůbec chráněna. Veškeré předchozí snahy společnosti o ochranu podnikových dat před neoprávněným přístupem tak přicházejí nazmar. phion proto společnostem doporučuje formulovat jasná pravidla, která zakážou zaměstnancům komunikovat prostřednictvím společenských sítí informace obchodního charakteru. Jednotlivcům phion radí, aby si pečlivě rozmysleli, které informace chtějí na soukromých komunitních portálech zveřejnit. I ze zdánlivě neškodných informací lze totiž sestavit velice přesvědčivý profil a udělat z nich potenciálně zajímavý terč kriminálních aktivit, od zasílání spamu až po promyšlené sociální inženýrství, kdy útočník využije informace o uživatelích k vlastnímu prospěchu.

Provozovatelům komunitních platforem phion doporučuje podniknout kroky ke zlepšení standardu zabezpečení. Vodítkem by mohla být norma Payment Card Industry Standard (PCI DSS), definovaná vydavateli kreditních karet za účelem zvýšení bezpečnosti webových aplikací. Domníváme se, že se tyto normy mohou uplatnit nejen v bankovnictví a při zpracování transakcí kreditními kartami, ale i v prostředí Webu 2.0 pro všechny strany, které pracují s citlivými uživatelskými daty.

Komentář redakce: *Asi nikoho z nás nepřekvapí fakt, že výsledky evropských komunitních portálů se od těch našich příliš lišit nebudou. A když se podíváte na libovolný český komunitní portál, budete šokováni, jaké informace zde o sobě uživatelé vystavují. Adresy, telefonní čísla, elektronické kontakty (e-mail, ICQ, Skype…), záliby, vybavení bytu – zkrátka pro zloděje přímo zlatý důl. Ano, většina těchto aktivit padá na vrub hlouposti samostatných uživatelů, ovšem svůj podíl zde mají i provozovatelé. Metody zabezpečení jsou zastaralé a je jen otázkou času, kdy se tato data objeví v hledáčku lovců informací. A co o sobě na internetu prozrazujete vy?*

INFO

Nová bezpečnostní rizika

WIN FTP SERVER

Win FTP server je náchylný ke vzdálenému zapříčinění Denial of Service (www.securityfocus.com/bid/31421/info). Útočníci mohou této chyby zneužít k zablokování přístupu ostatním uživatelům. Zranitelnost je zaznamenána ve verzi 2.3.0, ostatní verze mohou být také zasaženy.
INFO: zpravy.actinet.cz

MICROSOFT WINDOWS MOBILE

V operačním systému Microsoft Windows Mobile, hojně využívaném na mobilních telefonech a Pocket PC platformě, byla nalezena chyba, a to v jeho předposlední verzi 6.0. Chyba je způsobena neschopností ověřit uživatelem poskytnutý vstup při zadání příliš dlouhého jména Bluetooth zařízení. Útočník může tento problém zneužít k zapříčinění pádu zařízení (více na **www.securityfocus.com/bid/31420/info**). Soudě z povahy chyby se dá usuzovat, že by mohla být zneužita i ke spuštění libovolného kódu, to ovšem nebylo potvrzeno.
INFO: zpravy.actinet.cz

MAC ILLUSTRATOR CS2

Společnost Adobe Systems oznámila chyby v Illustratoru CS2 pro Macintosh. Chyby mohou být zneužity k vytvoření upraveného souboru, který při otevření spustí libovolný kód. Jako řešení se nedoporučuje otvírat soubory z nedůvěryhodných zdrojů. Adobe Illustrator CS3 a CS4 tuto chybu neobsahují.
INFO: zpravy.actinet.cz

GOOGLE

Zdroj spamu

Google se stále více stává platformou pro spam. Například 27 % všech zpráv odeslaných přes Gmail představuje nežádoucí poštu. Příčinou nárůstu je skutečnost, že spammeři dokázali zneužít mechanismus CAPTCHA při přihlašování nových účtů u Googlu. CAPTCHA je kombinace písmen a číslic vyjádřená obrazově (často ve zdeformované podobě), kterou jako text dokáže přečíst člověk, ale žádný software; zabezpečení spočívá v tom, že uživatel musí znaky z předloženého obrázku přepsat do textové podoby.

Weboví zločinci však už proti tomu vymysleli vychytralou fintu. Na internetu nabízejí série různých oplzlých fotografií, z nichž divák tu následující uvidí teprve poté, co zadá CAPTCHA. Přitom ovšem netuší, že tím právě pro spammera založil nový gmailový účet. Podle bezpečnostní služby MessageLabs si tak nyní spammeři také opakovaně přivlastňují službu Google Sites.
INFO: www.messagelabs.com

INTERNETOVÁ MAFIE

Klikací podvody

S tzv. zaparkovanými doménami a sítí botů se dnes dá skvěle vydělávat. Ptáte se jak? Provozovatel si zaregistruje stránky jako **www.symanzec.com** nebo **www.kaspesky.com**, které mnozí uživatelé vyvolají jen proto, že se prostě překlepli, a tam kliknou na reklamní banner zamaskovaný jako menu. Poněvadž majitel webové stránky je za každé kliknutí placen, například prostřednictvím Google AdSense, mají takové domény cenu zlata.
Takové příjmy se však dají lehce zmnohonásobit: stačí, aby hacker dokázal počítače ve své síti botů řídit tak, aby pokud možno často samočinně klikaly na reklamní bannery na jeho webové stránce. Jak tvrdí bezpečnostní specialisté společnosti ClickForensics, v současné době má už 25 % všech těchto podvodů pocházet ze sítí botů, a to přesto, že je tato finta ještě relativně nová.
INFO: http://clickforensics.com

KRÁTKÉ ZPRÁVY

GEFORCE VYPOČÍTÁVÁ HERNÍ FYZIKU

Výrobce grafických čipů nVidia umožňuje se svým novým ovladačem 177.93 urychlování fyzikálního prostředí ve hrách. Grafické karty GeForce řady 8, 9 a GTX tak mohou převzít vypočítání realistických efektů ve hrách s podporou PhysX – speciální hardware již není potřeba.

INFO: WWW.NVIDIA.COM

LG PŘEDSTAVUJE BLU-RAY PŘEHRÁVAČ S VIDEEM NA PŘÁNÍ

Firma LG představila hybridní přehrávač nejnovější generace: BD3000 nepřehrává pouze Bluray disky a DVD, ale je možné jeho pomocí vyvolat z webu video na přání. Prvním dodavatelem obsahu je Netflix. Díky streamingu není třeba čekat déle než 30 sekund na start filmu. Přístroj bude v USA k dostání od podzimu.

INFO: HTTP://CZ.LGE.COM/

MICROSOFT MOUSEPAD SI VYSTAČÍ BEZ MYŠI

Jako mousepad bez myši vyhlíží nové vstupní zařízení z výzkumné laboratoře Microsoftu. Multidotyková fólie se jednoduše položí na stůl a je ovládána pomocí prstů. Dokáže dokonce rozlišit rozdílně silný tlak a je možné ji vyrobit mimořádně levně. To, kdy přesně bude produkt dostupný, však zatím firma nechává otevřené.

INFO: WWW.MICROSOFT.COM

PROHLÍŽEČ FOTOGRAFIÍ JAKO PŘÍVĚSEK NA KLÍČE

Společnost Digital Foci nabízí zajímavý produkt v podobě přívěsku na klíče. Netradiční přívěsek umožňuje na 1,5palcovém displeji s rozlišením 128 × 128 prohlížet obrázky ve formátech JPG a BMP. Prohlížení lze realizovat manuálně nebo automaticky s časovým intervalem 5 vteřin až 2 minuty. Zařízení je napájené 3,7 V nabíjitelnou baterií i prostřednictvím USB. Životnost baterie je až 9 hodin.

INFO: WWW.DIGITALFOCI.COM

DIGITAL IXUS

Canon má dva přírůstky

Canon posílil řadu kompaktních fotoaparátů Digital IXUS o dva nové přírůstky: Digital IXUS 980 IS a Digital IXUS 870 IS. 14,7megapixelová vlajková loď Digital IXUS 980 IS přináší několik novinek, včetně manuálního ovládání rychlosti závěrky a clony. V situacích, kdy je zachycení záběru otázkou zlomku sekundy, se uplatní další nový režim QuickShot, který pro kompozici a ostření využívá optický hledáček a prakticky eliminuje zpoždění závěrky.

10megapixelový Digital IXUS 870 IS je vybaven širokoúhlým objektivem (28 mm) s 4násobným optickým zoomem a 3,0" displejem. Bude nabízen ve dvou variantách – zlaté a stříbrné. Oba fotoaparáty používají nový procesor Canon DIGIC 4, který zajišťuje jejich rychlý chod a pružnou odezvu, a jsou také vybaveny optickým stabilizátorem. Pro snímání portrétů a skupinových fotografií je k dispozici vylepšená technologie detekce obličeje. Oba fotoaparáty umožňují natáčení VGA videa frekvencí 30 snímků za sekundu.

INFO: www.canon.cz

OTEVŘENÁ ENCYKLOPEDIE

Knol: Soupeř Wikipedie

Nový vědomostní portál Googlu je v současnosti již dostupný online jako beta verze. Knol není jenom název služby, ale podobně jako pojem „Wiki" odkazuje na vědomosti. Na rozdíl od Wikipedie jsou jednotlivá hesla označena jménem autora a mohou být uzamčena pro jiné autory. Na Knolu tak existuje více textů o jednom tématu – a také se zcela různými pohledy.

Autoři se dokonce mohou – na rozdíl od jiných projektů otevřených encyklopedií – podílet i na příjmech z reklamy, kterou mohou umístit do svých hesel. Ačkoli se většina pojmů vztahuje k oblasti medicíny, je zde také možné informovat se o tom, jak opravit toaletu, jak se připravit na závod Ironman nebo jak se postarat o trávník.

INFO: www.google.com

PANASONIC LUMIX G1

Zrcadlovka bez zrcadla

První digitální „zrcadlovku" bez zrcadla představila firma Panasonic. Jde o SLR fotoaparát Lumix G1 založený na standardu Micro 4/3 s výměnnými objektivy. G1 je fotoaparátem pro všechny nadšence, kteří nechtějí cestovat s těžkým batohem, ale s fotografováním to myslí vážně a rádi experimentují. Novinka totiž dokáže poskytnout fotografům výhody digitálních zrcadlovek (jako je kvalita, možnost výměny objektivů, bohaté příslušenství a plně manuální funkce), a přitom nabízí kompaktní rozměry, výrazně nižší hmotnost, mobilitu i řadu funkcí, které dosud v digitálních zrcadlovkách nenašli.

Model vychází z nového standardu Micro 4/3. Převratným prvkem tohoto konceptu je nahrazení tradičního systému hranolu a zrcadla (zrcátko mimo jiné vyvolává nežádoucí otřesy) novým rozměrným digitálním hledáčkem Panasonic Live View Finder s vysokým rozlišením, rychlou odezvou a funkcí tzv. pravého živého náhledu Live View. Přístroj G1 je možné používat jak s výměnnými objektivy standardu Micro 4/3, tak se staršími výměnnými objektivy standardu 4/3 (se speciálním adaptérem). Panasonic představil pro fotoaparát G1 dva výměnné objektivy – standardní zoom objektiv Lumix G Vario 14-45mm/F3.5–5.6./Mega O.I.S., který má univerzální použití, a teleobjektiv Lumix G Vario 45-200mm/F4.0–5.6/Mega O.I.S., který nabízí zoomový rozsah 45–200 mm (ekvivalent 35mm filmu: 90–400 mm).

INFO: www.panasonic.cz

OKŘÍDLENÝ WEB

Stránky pražského letiště v novém

Plánujete-li cestu letadlem, první kroky vedou ve většině případů na webové stránky Letiště Praha (**www.prg.aero**). I díky jejich novému designu a struktuře zde snadno najdete rady, kde nejlépe zaparkovat či jak si koupit letenku, a samozřejmě také to nejdůležitější – kdy vám to letí. Výsledkem redesignu webu je přehledná a logická struktura, v níž každý rychle najde to, co potřebuje – počínaje informacemi, kde nakoupit a kde se dobře a levně najíst, konče radami, jak absolvovat kurz létání beze strachu. Zajímavou „vychytávkou" je infotabule s přílety a odlety na hlavní stránce, která se po „najetí" přiblíží – hned tedy můžete vidět, kdy odlétáte na dovolenou.