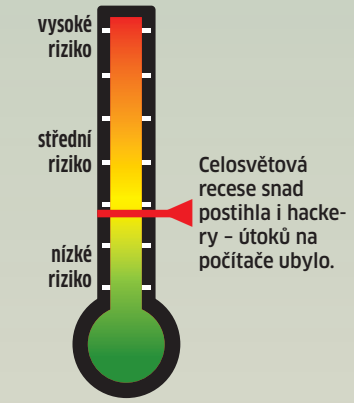
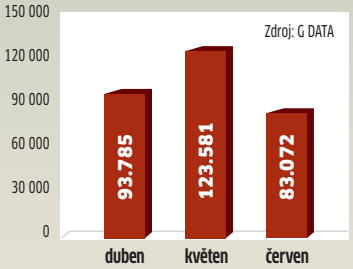
DATA A FAKTA

Barometr nebezpečí
v srpnu

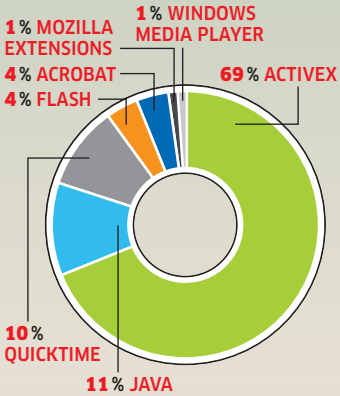


Malwaru je méně



Nebezpečí trvá: I přes pokles je výskyt malwaru děsivě vysoký.

Útoky na browsery



Nebezpečí z webu: Hackeři nejraději využívají mezer v plug-inech Microsoftu.

Číslo měsíce

500

eur stojí přístupová data k „hacknutému“ on-line účtu s vkladem přes 10 000 eur.

Nejhorší hesla všech dob

Chrání vás kvalitní firewall, máte nejnovější updaty operačního systému, používáte výborný antivir, a přesto byl váš počítač úspěšně napaden hackerem? Problém může být ve **ŠPATNĚ ZVOLENÉM HESLE**.

PETR KRATOCHVÍL

Útoky hackerů se vždy snaží zamířit na nejslabší článek řetězu – pokud má váš počítač kvalitní softwarovou výbavu, mohou se hackeři pokusit zaútočit na vaše přístupová hesla. Ačkoliv mezi nejčastější varování v článcích o počítačové bezpečnosti patří „zásada bezpečného hesla“ (varující před používáním jednoduchých hesel), jen málokdo se jí drží. To pravidelně potvrzují průzkumy bezpečnostních firem i vlastní zkušenosti uživatelů.

První hesla, vytvářená ve snaze o maximální zabezpečení nového počítače, bývají komplikovaná a opravdu bezpečná. Po čase ale ostražitost klesá a s ní se snižuje i komplikovanost hesel. To je nebezpečné riskování. Metod, jak uhodnout vaše heslo, je celá řada a většinu uživatelů určitě napadne „slovníková metoda“. Při ní hacker zkouší kombinace a variace slov ze slovníku daného jazyka – v ohrožení jsou tedy hesla typu „reflektor“ nebo „laparoskopie“. V praxi ale mají hackeři situaci ještě snadnější.

Tabule hanby: Najdete i vy své heslo v seznamu těch nejhorších, nebo si svých dat a soukromí vážíte více?

500 nejhloupějších hesel

Při vytváření knihy o heslech zjišťoval její autor Mark Burnett (na vzorku více než milionu uživatelů), jaká hesla uživatelé používají. Výsledky jeho výzkumu překonaly i ty nejhorší předpoklady: neuvěřitelné množství lidí používá stále se opakující primitivní hesla, která dokáže uhodnout i cvičená opice. K demonstraci lidské hlouposti sestavil Mark Burnett seznam 500 nejhloupějších hesel, která používá více než desetina uživatelů! Pojďme se podívat na některá z nich:

- 123456 – klasika, „náročnější“ uživatelé pokračují až k devítce, líní končí na čtyřce či pětce;
- password – „heslo“ jako heslo má být trik k ošálení hackerů, opak je bohužel pravda;
- 666666 – s alternativami v podobě sedmi sedmiček, pěti pětek, kreativitě se meze nekladou;
- zxcvbn – heslo „qwerty“ se uživatelům nezdá bezpečné, tak to zkouší v dolní části klávesnice;
- qazwsx – pokročilejší kreace předchozí metody, ovšem se stejnou bezpečnostní úrovní;
- ncc1701 – oblíbené heslo „nerdů“, skrývající označení kosmické lodi ze seriálu Star Trek;
- porsche – s alternativou v podobě značky vašeho vysněného vozu (ano, v seznamu je i ferrari).

S těmito znalostmi tedy může být práce hackerů snadná a efektivní – zkuste si sami odhadnout, kolik počítačů tvoří zmiňovanou desetinu se snadno „odhalitelnými“ hesly. A jak jsou na tom vaše účty? Najdete i vy své heslo v seznamu 500 nejhloupějších hesel na adrese **www.whatsmypass.com/the-top-500-worst-passwords-of-all-time?**

LINUXOVÉ WEBSERVERY ÚTOČÍ

Nové triky malwaru

Ruský nezávislý bezpečnostní výzkumník a analytik Denis Sinegubko objevil skupinu infikovaných linuxových serverů, na kterých běží speciální druh botnetů. Ty poté rozesílají malware nic netušícím uživatelům surfujícím po webu. Takto postižené stroje sice na první pohled fungují zcela normálně a pracují na standardním TCP portu (80), vzápětí však využijí pro „tajný provoz“ port 8080.

Sinegubko ve své zprávě uvádí, že už dva poskytovatelé dynamického hostingu, DynDNS.com a No-IP.com, jejichž služby útočníci využívali, stihli na danou situaci zareagovat, a to aktivním vypínáním domén, které jsou k těmto útokům zneužívány. Dále však dodává, že to určitě není naposledy, co se s tímto fenoménem setkáváme , když každou hodinu přibývají dvě nové IP adresy...

Detailnější informace o dané problematice najdete na stránkách serveru The Register **(www.theregister.co.uk/2009/09/12/linux_zombies_push_malware/)**. Tento nález také poukazuje na neustály vývoj „záškodného“ softwaru, jehož oběťmi se už mohou snadno stát i velikáni jako Twitter, nebo dokonce Google Groups.

INFO: zprávy.actinet.cz

ANALÝZA SYMANTECU

Kyberzločinci na dovolené nebyli...

V měsíci srpnu si kyberzločinci pravděpodobně dovolenou nevybrali. A pokud ano, vzali na ni zcela jistě své notebooky. Vyplývá to z analýz State of spam a State of phishing společnosti Symantec, které sledovaly vývoj světového spamu a phishingových útoků v posledním měsíci letních prázdnin.

Stále platí, že jen v jednom případě z deseti není příchozí e-mail spam. V rozesílání spamu jsou nejaktivnější Spojené státy, odkud pochází čtvrtina veškeré světové produkce nevyžádané pošty, konkrétně 23%. Symantec během srpna zaznamenal nárůst spamu, který se vyznačuje zneužíváním důvěry lidí ke známým značkám. Jeden konkrétní lákal na profesionální spolupráci s Googlem, kdy člověku stačí pracovat jen hodinu denně z pohodlí domova, a pak v klidu zaplatí všechny své účty. Z aktuálních srpnových událostí stojí za zmínku 6. srpen, kdy uplynulo 200 dní od nástupu populární Obamovy administrativy. Této příležitosti se chopili spammeři a jeho jménem začali lidem nabízet levné léky. V červenci bylo například oblíbené nové filmové dobrodružství Harryho Pottera a nabídka jeho příběhů v elektronické podobě či snímky nahé Emmy Watson, filmové představitelky sexy čarodějky Hermiony. V srpnu se už také začal objevovat první spam věnovaný tematice Vánoc.

Pokud hodnotíme výskyt phishingových internetových stránek podle lokálního umístění, nelichotivé první místo drží s 33% podílem stále USA. Z evropských zemí se „nejlépe“ umístila Velká Británie, která se posunula v meziměsíčním srovnání ze sedmé na třetí příčku. Podrobné informace o vývoji světového spamu a phishingu naleznete v dokumentu se studií: **http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_09-2009.en-us.pdf**.
INFO: www.symantec.com

INFO

Nová bezpečnostní rizika

IRFANVIEW

Hackeři mohou využít mezeru v prohlížeči TIFF souborů k vyvolání „heap overflow“. Získají tak úplný přístup do PC. Řešením je upgrade na novou verzi 4.2.5, která nejen odstraňuje tuto mezeru, ale přináší také nové filtry pro různé souborové formáty.
INFO: www.irfanview.com

VIDEOLANCLIENT

Použitím příliš dlouhé URL pro playlist mohou útočníci vyvolat přetečení bufferu a poté propašovat do počítače škodlivý kód. Na aktualizaci se pracuje, podle vyjádření výrobce však bude k dispozici až za několik týdnů.
INFO: www.videolan.org/vlc

OPENOFFICE.ORG 3.1.0

V oblíbeném kancelářském balíku OpenOffice.org 3.1.0 byly potvrzeny dvě zranitelnosti při zpracování dokumentů Microsoft Word, které mohou být zneužity pomocí upravených souborů. Ty mohou vést až k získání vzdáleného přístupu do systému. Více informací najdete na serveru Secunia **(http://secunia.com/secunia_research/2009-26/)**. Zranitelné mohou být také dřívější verze. Řešením je upgrade na verzi 3.1.1, kde jsou již zranitelnosti opraveny.
INFO: zpravy.actinet.cz

INFO

Nová bezpečnostní rizika

GOOGLE CHROME

Využitím bezpečnostních mezer v browseru od Googlu mohou hackeři získat přístup do PC. Opravný patch řeší zranitelnosti například v V8 JavaScript enginu nebo zpracování XML obsahu. Tyto zranitelnosti mohly vést k odhalení citlivých informací nebo až k získání přístupu do systému. Podle Googlu jsou slabiny natolik závažné, že podnik hodlá zveřejnit detaily až poté, kdy bude většina počítačů chráněna. Aktualizace je již u Googlu k dispozici.

INFO: www.google.com/chrome

MICROSOFT IIS FTP SERVER

V Microsoft IIS FTP serveru byla objevena zranitelnost, která umožňuje útočníkům po přihlášení se k serveru poměrně jednoduše způsobit DoS. Poté, co byl zveřejněn nový kód **(viz http://www.milw0rm.com/exploits/9587)**, který umožňuje způsobit DoS i uživatelům, kteří nemají práva k vytváření adresářů, se výrazně zvýšil počet útoků a očekává se, že stále poroste. Není vyloučeno, že se pádu aplikace nedá zneužít k dalším útokům. Zasaženy jsou pravděpodobně téměř všechny verze Microsoft IIS. Doporučuje se – tam, kde je to možné – vypnout ftp server. Více informací naleznete na stránkách Microsoftu **(www.microsoft.com/technet/security/advisory/975191.mspx)** nebo na webu TheRegister.co.uk **(www.theregister.co.uk/2009/09/04/microsoft_iis_attacks_go_wild/)**.

INFO: zpravy.actinet.cz

TCP PROTOKOL

Microsoft a Cisco vydaly updaty, které ošetřují nový druh DoS útoků, jenž vyžaduje jen malý přenos dat a může paralyzovat servery a routery i poté, co útok ustane. Chyba v TCP protokolu, kterou objevili a v říjnu 2008 zveřejnili Jack Louis a Robert E. Lee **(www.theregister.co.uk/2008/10/01/fundamental_net_vuln/)**, umožňuje útočníkům zahltit server požadavky na TCP spojení, což může donutit systém využít všech prostředků a odmítat další požadavky na spojení. Další společnosti, např. Check Point Software, oznámily, že aktualizovaly několik security gateway produktů. Linuxový distributor Red Hat zatím nabízí jiné řešení problému **(http://kbase.redhat.com/faq/docs/DOC-18730)**. Ne všichni hráči na trhu souhlasí se závažností problému, např. Juniper Networks, VMware a Clavister tvrdí, že jejich produkty nejsou zranitelné. Více informací naleznete na webu TheRegister.co.uk **(www.theregister.co.uk/2009/09/09/microsoft_cisco_patch_tcp_vuln/)**, informace o updatech jednotlivých produktů pak na serverech Microsoftu a Cisca.

INFO: zpravy.actinet.cz

NOVĚJŠÍ VERZE WINDOWS

Windows Vista a beta verze Windows 7 obsahují chybu ve zpracování SMB2 protokolu (více informací na webu The Register **(www.theregister.co.uk/2009/09/09/microsoft_windows_security_bug/)**, kterou může vzdálený útočník zneužít k ovládnutí systému. Microsoft slíbil opravit tuto chybu v záplatách, ale nestalo se tak. Podle původního článku Microsoftu **(www.microsoft.com/technet/security/advisory/975497.mspx)** útok ve většině případů skončí „modrou obrazovkou smrti“. Ve finální verzi Windows 7 a Windows Server 2008 R2 byla tato chyba opravena.

INFO: zpravy.actinet.cz

APPLE IPHONE

Viry z SMS

Mezera v SMS aplikaci iPhonu od Applu umožňuje útočníkům získat nad telefonem úplnou kontrolu. Podle bezpečnostního experta Charlie Millera stačí už jedna zmanipulovaná SMS, aby se přístroj změnil v „zombie“. Zvláště prekérní na tom je, že SMS aplikace je jedním z mála programů, které mají v iPhonu plná systémová práva. Většina ostatních nástrojů běží oddělene od systému v tzv. sandboxu. Na uzavření mezery už začal Apple pracovat. Podle zasvěcených však kvůli tomu musí být celá SMS aplikace přepsána. Aktualizace se proto pravděpodobně protáhne ještě na několik týdnů. Doutná však jiskřička naděje: Miller ujišťuje, že až do vydání updatu nezveřejní žádné podrobnosti.

INFO: www.apple.com

WEBSENSE

Hromadné napadení

Útočníci zmanipulovali několik desítek tisíc webových stránek a jejich návštěvníky přesměrovali na vlastní záškodnickou stránku. Tento masový útok odhalila bezpečnostní firma Websense. Zjistila, že útočníci použili metodu „SQL injection“, kterou do napadených stránek vpravili zmanipulovaný javaskript. Tak všechny návštěvníky stránek přesměrovali na vlastní domovskou stránku, na níž se nejrůznějšími postupy snaží do jejich počítačů nahrát záškodnický program. Útočníci se přitom zaměřují zejména na mezery v Adobe Readeru a v Internet Exploreru.

Ochranu by mělo zajistit udržování Windows a aplikací v aktuálním stavu. Kromě toho se vyplatí pohled na adresní řádek browseru: pravopisné chyby mohou naznačovat přesměrování na hackerskou stránku.

INFO: www.websense.com

TREND MICRO O HROZBÁCH:

Bredolab na vzestupu

21. srpna publikovali výzkumní pracovníci Trend Micro na blogu článek „Laptop Delivery Note Contains Malware“ (Dodací list k laptopu obsahuje malware), který přehledně shrnoval nedávnou sérii spamu se škodlivou přílohou, která se tváří jako faktura za nákup laptopu. Uvedená příloha ve skutečnosti spustí proces BKDR_BREDOLAB.AL, který otevře zadní dvířka a stáhne trojského koně RENOS (trojské koně RENOS jsou známé nástroje na stahování souborů a obvykle jsou maskovány jako falešné antiviry). **http://blog.trendmicro.com/laptop-delivery-note-contains-malware/**

Malware BREDOLAB si již upevňuje své pozice. Podle výzkumu Trend Micro zřejmě zločinci, kteří stojí za aktivitami běžně připisovanými kampani Zeus, vrhli do distribuce nový modul. Tento modul byl nazván Bredolab a v poslední době zaznamenali výzkumní pracovníci Trend Micro několik nových variant tohoto malwaru, které byly zachyceny ve velkých kriminálních kampaních, jako jsou spamové kampaně pod hlavičkou UPS a DHL.

Do počítače proniká pomocí útoků na slabá místa (např. PDF či SWF) z nebezpečných webových stránek a také přílohami, které jsou zasílané s nevyžádanou poštou. Jeho primární funkcí je stahování dalších programů a zpravidla je spojen s falešnými antiviry, rootkity, spamboty (jako je Cutwail) a dalšími nástroji pro krádež informací. Jakmile je malware Bredolab aktivován, začne komunikovat se skrytou soupravou nástrojů pro správu, která automatizuje stahování, instalaci a spouštění programů na napadeném počítači.

Naštěstí jsou již k dispozici technologie, které se těmto vzrůstajícím hrozbám dokáží postavit. Trend Micro například doporučuje řešení Smart Protection Network (více viz **http://us.trendmicro.com/us/trendwatch/core-technologies/smart-protection-network/**).

INFO: http://us.trendmicro.com/us/trendwatch/research-and-analysis/index.html

VÝZKUM AVG

Zranitelnější uživatelé sociálních sítí

Společnost AVG Technologies uvolnila ve spolupráci s CMO výsledky ankety „Jak přinést bezpečnost na sociální sítě“ (Bringing Social Security to the On-line Community). Z výzkumu vyplynulo, že uživatelé sociálních sítí mají sice obavy o bezpečnost při komunikaci, málokdo však podniká alespoň základní kroky k ochraně před on-line hrozbami. Jen necelá třetina respondentů se jim aktivně brání, téměř polovina se obává krádeží identity v on-line komunitách a také rostoucího množství phishingu, spamu i virových útoků.

Anketa na internetu shromáždila ve druhém čtvrtletí 2009 odpovědi náhodného vzorku více než 250 uživatelů. I přes masivní používání nejrůznějších sociálních sítí doma nebo v práci (86 %) nedodržuje většina uživatelů pravidelně ani následující základní bezpečnostní pravidla:

► změny hesel (64 procent zřídka nebo vůbec);
► úpravu nastavení soukromí (57 procent zřídka nebo vůbec);
► informování administrátora sociální sítě (90 procent zřídka nebo vůbec).

Respondenti zmiňovaného výzkumu definovali několik obvyklých praktik, které provádí navzdory zřejmým bezpečnostním rizikům při zapojení do sociálních sítí (tyto praktiky mohou nechráněné uživatele poškodit):

► 21 procent respondentů přijme nabídku na kontakt od členů sítě, které osobně nezná;
► 51 procent nechá známé či spolubydlící navštěvovat sociální sítě na svém osobním počítači;
► 64 procent respondentů kliká na odkazy od dalších členů sítě;
► 26 procent dotázaných sdílí prostřednictvím sociálních sítí soubory.

Výsledkem šíření odkazů, souborů a nevyžádaných kontaktů je, že se uživatelé sociálních sítí velmi často setkávají s nejrůznějšími hrozbami a narušením soukromí:

► téměř 20 procent již zažilo krádež identity;
► 47 procent se stalo obětí nákazy nějakým typem škodlivého kódu;
► 55 procent dotazovaných se setkalo s phishingovým útokem.

Ředitelka komunikace a vztahů s investory AVG Technologies Siobhan MacDermottová doufá, že se AVG podaří tento trend zvrátit na známých sítích, jako je Facebook nebo Twitter. „Naše kampaň Data Snatchers je virálním prostředkem, který by měl přimět uživatele přemýšlet o své osobní bezpečnosti. Poskytne jim také jednoduché nástroje, pomocí nichž mohou pro svou bezpečnost něco udělat, a zvláště pokud se pohybují v místech, kde se cítí zranitelní.“

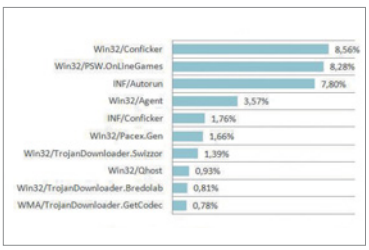
AVG Technologies také doporučuje šest jednoduchých kroků, které uživatelům pomohou zajistit bezpečí:

1. Nepotvrzujte pop-up okna či výzvy ke stažení softwaru, dokud váš počítač není vyzbrojen webovým štítem, jakým je například AVG LinkScanner **(http://free.avg.cz/linkscanner)**. Pomocí něj si zkontrolujte každou stránku ještě předtím, než na ni vstoupíte.
2. V sociální síti nikdy neuvádějte, neposílejte ani nepřikládejte žádná soukromá osobní data (například rodné číslo, údaje k bankovnímu účtu či zdravotní záznamy). Sociální sítě nevyžadují informace podobného typu k tomu, abyste se mohli stát jejich členem.
3. Měňte své heslo pravidelně, alespoň jednou za měsíc. Neměňte ho, když jste k tomu vyzváni. Mohlo by jít o trik třetí strany, která z vás chce heslo vylákat.
4. Nenechávejte své přátele, spolužáky, kolegy atd., aby navštěvovali sociální sítě z vašeho počítače, a ani vy je nenavštěvujte z cizího. Další osoby by svým neopatrným chováním mohly zanést do vašeho počítače infekci, případně by vaše přihlašovací údaje mohly být ohroženy prostřednictvím cookies, uložených na váš počítač.
5. Nikdy nevyužívejte automatického uložení vašich hesel a pravidelně mažte historii, alespoň jednou za týden.
6. Nikdy nepřijímejte nabídky na přátelství nebo o něj nežádejte osoby, které sami neznáte.

STATISTIKA FIRMY ESET

Počítačové hrozby: Conficker mírně na ústupu, roste podíl trojských koní

V celé východní Evropě Conficker konečně oslabuje. S podílem 8,56 % byl sice i v srpnu globálně nejrozšířenějším typem malwaru ze všech světově detekovaných hrozeb, ve srovnání s červencovými statistikami však zaznamenal pokles o více než dvě procenta. Silnější globální pozici naopak získala směs hrozeb sestávající převážně z trojanů útočících na hráče on-line her – Win32/PSW.OnLinegames (8,28 %). Nejrůznější trojské koně, které ke svému spuštění využívají funkci souboru autorun.inf, jsou stále rovněž v první trojici celosvětových hrozeb – v srpnu byla infiltrace INF/Autorun zaznamenána na 7,80 % počítačů. Varianty malwaru z rodiny Agent, schopné vykrádat informace z počítače, pak byly na čtvrtém místě, s výrazným odstupem za první trojicí a celkovým podílem 3,57 %. První pětku uzavírá INF/Conficker, který stejně jako INF/Autorun využívá autorun.inf v operačních systémech Windows k šíření infiltrace – konkrétně červa Conficker. Desítku celosvětově nejrozšířenějších počítačových hrozeb podle ESET ThreatSense.Net doplnily v srpnu škodlivé kódy Win32/TrojanDownloader.Swizzor (1,39 %) a Win32/TrojanDownloader.Bredolab (0,89 %). Cílem obou uvedených infiltrací je především stáhnout další malware a nainstalovat jej do infikovaného počítače.



Evropa a zbytek světa

Stejně jako v červenci i v srpnu byl Win32/TrojanDownloader. Bredolab top hrozbou v Česku (7,06 %) i na Slovensku (5,25 %). V červenci ovládal lokální statistiky hrozeb s podílem 6,48 %. Tento malware se sám umisťuje do běžících procesů v počítači a snaží se vypnout bezpečnostní programy (uživatel o něm nemusí vůbec vědět). Je schopen se sám kopírovat do systémových souborů a spouštět se při každém zapnutí počítače. Zároveň komunikuje se vzdáleným serverem prostřednictvím HTTP. Pokud je tedy tento trojský kůň v systému, jeho hlavní úlohou je stahovat do infikovaného počítače další škodlivé kódy. Varianty červa Conficker jsou nejrozšířenější především na Ukrajině a v Rusku, ale i na jihu Afriky a ve Velké Británii.

Polsko je typické dominancí trojanů útočících na on-line hry Win32/PSW.OnLineGames. Ty mají stále vysoký podíl (13,59 %) mezi všemi hrozbami. I ve Francii (10,07 %), Turecku (13,7 %) a Spojených arabských emirátech (7,61 %) jsou uživatelé nejčastěji ohroženi trojskými koňmi souvisejícími s on-line hrami. Win32/Agent je nejrozšířenější počítačovou hrozbou v Dánsku (3,78 %) a Švédsku (3,49 %), přičemž v severských zemích je proti jiným evropským zemím zvláštně vysoký podíl specifického červa Koobface, útočícího na uživatele sociálních sítí typu Facebook či MySpace. Koobface je v Dánsku s podílem 2,59 % dokonce v první trojce, na Islandu je s 1,94 % v první pětce a první desítku okupuje i v Norsku a Švédsku.

OPERAČNÍ SYSTÉM PRO PDA

Microsoft Windows Mobile 6.5

Microsoft oficiálně oznámil, že 6. října 2009 uvede celosvětově na trh novou verzi operačního systému Windows Mobile 6.5. Ten zákazníkům přinese uživatelsky jednodušší prostředí, lepší možnosti při využívání internetu a přístup k zajímavým službám, včetně Microsoft My Phone a Windows Marketplace. Novinkou je také to, že všechny chytré telefony s jakoukoliv verzí Windows Mobile budou od 6. října 2009 nazývány Windows Phones.

Windows Phones nabídnou v České republice celkem čtyři výrobci. Jde o společnosti Samsung, HTC, Garmin-ASUS a společnost Mio. Majitelé zařízení Omnia firmy Samsung a některých modelů HTC budou moci využít bezplatného upgradu. S novou verzí bude mnohem jednodušší zařídit více věcí přímo z telefonu, jako například zkontrolovat si letenku či zaplatit účty.

INFO: **www.microsoft.cz**

CANON EOS 7D

Zrcadlovka s novým designem

Společnost Canon představila celé portfolio produktů (několik desítek), kterými hodlá oslovit podzimní trh. Patrně nejzajímavější novinkou pro pokročilé fotografy je nová zrcadlovka Canon EOS 7D se zcela novým designem, 18megapixelovým rozlišením, hned dvojicí obrazových procesorů Digic 4 a rozsahem citlivosti až do ISO 12 800. O rychlosti hovoří údaj, který uvádí, že fotoaparát dokáže v plném rozlišení pořídit až osm snímků za sekundu.

Fotoaparát EOS 7D je vybaven 19bodovým zaostřovacím senzorem křížového typu. Nastavení AF je uživatelsky přizpůsobitelné a umožňuje rychlou reakci na změny ve snímané scéně. Hledáček fotoaparátu Canon EOS 7D, nazvaný Intelligent Viewfinder, nabízí fotografům 100% pokrytí. Díky zvětšení 1,0x – poprvé u fotoaparátu EOS – vidí fotograf v hledáčku velký jasný obraz, umožňující plně se ponořit do pořizovaného záběru. Jde také o první model z řady EOS se zobrazením dvouosé elektronické vodováhy, která zobrazuje úhel naklonění i natočení – v hledáčku i na 3" LCD displeji. Režim EOS Movie umožňuje rychlé přepnutí do režimu filmování v rozlišení Full HD (kodek H.264). Uživatel může nastavit expozici a rychlost snímání – s možností filmovat rychlostí 24 snímků za sekundu. Tělo fotoaparátu je z hořčíkové slitiny. Předběžná cena byla stanovena cca na 38 000 Kč vč. DPH.

INFO: **www.canon.cz**

INTERNETOVÉ NÁKUPY

Služba Srovname.cz se rozšířila

Do letošního léta se služba Srovname.cz zaměřovala převážně na obchody s elektronikou a zábavní technikou. V polovině prázdnin však webové stránky na adrese www.srovname.cz doznaly změn nejen po grafické stránce. Web je nyní přehlednější a pro uživatele přívětivější a kromě tradičního srovnávání cen například multimediálních zařízení je do porovnání zařazena i široká škála kategorií dalšího zboží. Například maminkám nyní server nabízí přehledné srovnání cen dětských kočárků, aktivním sportovcům umožní porovnání horských kol, cestovatelé si mohou srovnat nabídku stanů a zahrádkáři nabídku zahradnického náčiní. Srovname.cz nenabízí jen srovnání zboží, ale i nákupní rádce či službu hlídání ceny pro registrované uživatele.

INFO: **www.srovname.cz**

APPLE IPOD

Nano má kamerku

Společnost Apple představila nový MP3 přehrávač iPod nano, tentokrát obohacený o videokameru, mikrofon a reproduktor. Milovníci domácího videa teď mohou svá videa kdekoli natáčet, dívat se na ně na svém iPodu nano a snadněji je nahrávat z počítače na YouTube. iPod nano také nabízí vestavěné FM rádio s „živými pauzami" (živá pauza umožňuje zastavit a pak znovu zahájit poslech pořadu z rádia). Další novinkou je vestavěný krokoměr, který umí vést záznam o vašich krocích a spálených kaloriích. iPod nano má také větší 2,2" displej. K dispozici je ve verzi 8 GB za 3 990 Kč a 16 GB model stojí 4 690 Kč a dodává se v devíti barvách

INFO: **www.apple.cz**

LEXMARK S A PRO

S levným tiskem

Lexmark má v nabídce nové inkoustové multifunkce. Jejich hlavními novinkami jsou nízké provozní náklady (cena za stránku je při použití velkých kartridží 1 cent, tedy asi 25 haléřů), použití oddělených barevných inkoustů (u Lexmarku vůbec poprvé) a připojení k internetu (u některých modelů). Poprvé byla také u inkoustových tiskáren použita bezdrátová technologie 802.11n.

Osm nových multifunkčních zařízení je rozděleno do dvou řad. Pro domácnosti jsou určeny modely S305 až S605 s cenou od 2 200 Kč vč. DPH a pro malé firmy modely Pro205, Pro705, Pro805 a Pro905. Inkoustovou kartridž s vysokou kapacitou, s níž se při černobílém tisku můžete dostat až na cenu 25 haléřů za stránku, lze použít jen u nejdražších modelů Pro805 (6 850 Kč) a Pro905 (9 180 Kč), které tisknou rychlostí až 33 stránek za minutu. Model Lexmark Pro905 je zařízení „4-v-1" a nabízí bezdrátové rozhraní, dotykovou LCD obrazovkou s úhlopříčkou 4,3 palce, připojení k internetu, dva zásobníky papíru, automatický podavač dokumentů, úsporný režim Eco Mode a integrovanou funkci pro skenování vizitek. Díky připojení k internetu se mohou funkce tiskárny rozšiřovat – uživatel si například může vytvářet „makra" pro posílání naskenovaných dokumentů definovaným uživatelům, může si tisknout RSS kanály z internetu a k dispozici by měly být i nové aplikace pro multifunkční zařízení.

INFO: **www.lexmark.cz**

AUTOPŘÍSLUŠENSTVÍ

Držáky Brodit

Švédská společnost Brodit u nás začala prodávat své příslušenství do automobilů. Jedná se o držáky mobilních zařízení, jakou jsou mobilní telefony, PDA, navigace, ale i různé multimediální přehrávače.

V čem je Brodit odlišený, to je způsob uchycení držáku. Nejde cestou univerzálních držáků, ale pro každý typ automobilu má speciální držák, který mu byl vytvořen na míru. Výrobce využívá konstrukčních vlastností přístrojové desky každého automobilu a může tak vybrat nejvhodnější umístění pro držák mobilního zřízení.

Celý systém se skládá z podkladové destičky, která je určena pro specifický typ automobilu, a držáku mobilního zařízení, který je také vytvořen na míru danému produktu. Všechny držáky se instalují bez zásahu (vrtání) do přístrojové desky. Chválíme, že nabídka automobilů i podporovaných zařízení je zcela vyčerpávající. Na internetových stránkách firmy najdete konfigurátor.

INFO: **www.brodit.cz**

ÚSPORNÝ FUJITSU ESPRIMO

Stand-by s nulou

Úspora elektrické energie je hitem, a proto není divu, že se výrobci IT snaží i v této oblasti. Nejnovějším ekologickým krokem jsou nové modely PC společnosti Fujitsu: Esprimo P7935 0-Watt (minitower) a Esprimo E7935 0-Watt (desktop). Jedná se o speciálně navržené počítače s patentovanou technologií, které v režimu stand-by nespotřebovávají žádnou elektrickou energii. Uživatel přitom nemusí používat tvrdé (hardwarové) vypnutí, PC se do nulové spotřeby uvede samo po standardním softwarovém ukončení práce. Pro informaci: Běžné počítače spotřebovávají ve vypnutém stavu obyčejně více než 1 W. Úsporné modely Esprimo jsou díky optimalizovanému konceptu ventilátorů (procesor má pouze pasivní chladič) extrémně tiché a jsou vybaveny i dalšími funkcemi, jako je spínaná zásuvka monitoru a správa úspory napájení. Nulová spotřeba ve vypnutém režimu by neměla znesnadňovat administraci v počítačových sítích: administrátor si může vzdáleně nakonfigurovat časový úsek, kdy bude možné PC řídit.

INFO: www.fujitsu.cz

TIPY A NÁVODY

Poradna pro uživatele produktů Apple

V polovině srpna byl spuštěn nový projekt ApplePoradna.cz (www.appleporadna.cz), který má za cíl pomoci začínajícím uživatelům výrobků Apple a pokročilejší uživatele upozornit na zajímavé tipy a triky týkající se jejich přístroje značky Apple. Užitečné rady se dnes ztrácí v nepřehledných fórech na několika místech. Ambicí tvůrců nového webu je tyto informace uspořádat a v přehledném konceptu předat uživatelům. Postupně tak chtějí návody doplňovat, aby byl server užitečný jak pro začátečníky, tak i pro pokročilé uživatele. Obsah budou hlavně zpočátku tvořit sami uživatelé. Postupně se bude tvořit i tým odborných poradců a s obsahem budou pomáhat i univerzitní Apple iKnow kluby. Prioritou pro prvních několik týdnů bude tvorba obsahu a vhodná organizace do kategorií.

INFO: www.appleporadna.cz

SLUNEČNICE.CZ

Co se stahuje

Jedním z nejpopulárnějších programů určených ke komunikaci přes síť je dnes software ICQ 6.5. Tento program byl také v červenci nejčastěji stahovaným „kecálkem“ ze serveru Slunečnice.cz v kategorii Komunikační programy. Jeho stávající verze nabízí uživatelsky přívětivé prostředí, k dispozici je mimo jiné hlasová komunikace, posílání SMS, konferenční textová komunikace a řada dalších zajímavých funkcí. Česká lokalizace tohoto programu, Atlas ICQ 6.5, obsadila třetí místo. Stříbrná příčka patří programu Skype, jehož hlavní a nejvyužívanější funkcí je telefonování. Velkým konkurentem klasického ICQ je QIP 2005 (čtvrté místo), který však již není dále vyvíjen, pouze aktualizován při změně protokolu ICQ. Jeho nástupcem je QIP Infium (šestá pozice), který umí komunikovat jak v síti ICQ, tak v síti Jabber. Dalším alternativním programem pro on-line komunikaci je Miranda IM (sedmé místo). Jde o software s otevřeným zdrojovým kódem neboli open-source, který vyniká především jednoduchostí, snadnou instalací a absencí reklamních sdělení. Neméně zajímavá je aplikace Jimm ICQ (devátá pozice), určená k použití v mobilních telefonech.

VOIP TELEFON

WELL 3195IF

Telefon s nadčasovým designem nabízí plnohodnotné „české“ prostředí, praktický podsvícený displej a pět programovatelných tlačítek pro rychlou volbu. Je předurčen pro kanceláře, avšak díky své přehledné obsluze je velmi vhodný i do domácností. Přístroj disponuje adresářem o kapacitě 99 záznamů a má paměť pro seznam posledních 80 odchozích volání, 80 příchozích volání a 80 zmeškaných volání. Údaje do „telefonního seznamu“ telefonu lze jednoduše přidat přes klávesy telefonu nebo je možné použít webový management. Telefon umožňuje volbu z devíti vyzváněcích melodií. Výhodou tohoto telefonu je také vestavěný firewall a integrace NAT a DHCP serveru. Jeho cena je cca 1 500 Kč vč. DPH.

INFO: www.joyce.cz