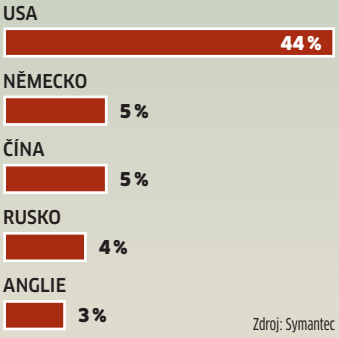
DATA A FAKTA

Barometr nebezpečí
v červenci

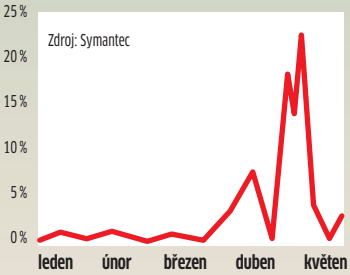
Původ phishingu



Bezpečně v čele: Velká většina phishingových stránek pochází z USA, přesto největší kritiku sklízí Čína...

Spam ve fotografiích

Útoky v roce 2009



Nová metoda: Spamovou zprávu obsaženou v obrazovém souboru rozpoznají spamové filtry jen obtížně.

Číslo měsíce

90 %

všech e-mailů je spam, tvrdí Symantec. Mimochodem, většina reklam přichází mezi devátou a desátou hodinou.

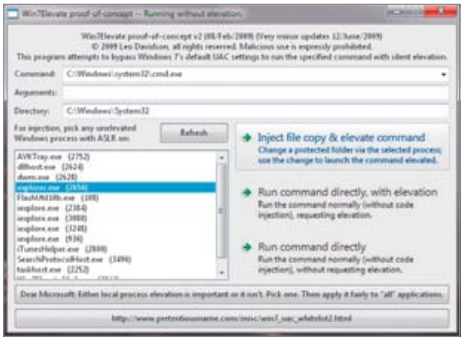
Windows 7: Pod palbou hackerů

ŘÍZENÍ UŽIVATELSKÝCH ÚČTŮ má de facto chránit před hackerskými útoky – jenomže právě tato funkce nyní podkopává bezpečnost systému.

FABIAN VON KEUDELL

22. října to vypukne – na trh přijde operační systém Windows 7. Microsoft tvrdí, že je bezpečnější, krásnější a rychlejší než Vista. Microsoft však už neříká, že od začátku vykazuje systém neodstranitelné bezpečnostní mezery! A Microsoft o tom ví už od zahájení beta fáze. Achillovou patou Windows 7 je Řízení uživatelských účtů (UAC).

Tato funkce byla poprvé zavedena ve Windows Vista a měla chránit před záškodnickým softwarem. Myšlenka UAC je prostá: Před Vistou byl každý uživatel vybaven oprávněním správce – každý směl v systému cokoliv měnit. Počínaje Vistou má běžný uživatel jen omezená práva. Jakmile nějaký program nebo uživatel chce provádět nastavení blízká úrovni systému, objeví se varovná zpráva UAC, která teprve až po potvrzení udělí potřebné oprávnění. Má to však jeden háček: Řízení uživatelských účtů pak svými vyskakovacími okny otravuje i při sebemenší aktualizaci. Nápravu mělo zjednat UAC ve Windows 7. Kdy má Řízení uživatelských účtů spustit poplach, o tom zde mohou uživatelé rozhodnout sami. V první beta verzi Windows 7 však přišel zpětný úder: postačil jednoduchý skript, aby se všechny programy daly spouštět s oprávněním správce, aniž by se o tom uživatel něco dozvěděl. Dnes jsou Windows 7 těsně před dokončením a někdejší problém UAC se skriptem je vyřešen – jenomže jen polovičatě. Dokonce i ve verzi označované jako „release candidate“ dokáží útočníci prostřednictvím „DLL injection“ UAC ošálit. Kliknutím myší pak každý program obdrží oprávnění správce. Zvláště fatální přitom je, že pokud útočník touto funkcí spustí Internet Explorer, ten vypne svůj chráněný režim a přestane blokovat hackerské útoky. A Microsoft se může jen stěží bránit.



Zrádné UAC: Řízení uživatelských účtů ve Windows 7 umožňuje útočníkům spouštět libovolné programy s oprávněním správce.

Microsoft nepomůže: Komfort je důležitější než ochrana před hackery

„DLL injection“ hackerů zasahuje interní DLL soubory Windows, na nichž je celý systém postaven. Běžně jsou tyto knihovny ve Windows 7 chráněny právě prostřednictvím UAC, ovšem jen tehdy, je-li řízení účtů nastaveno na nejbezpečnější režim. Poněvadž si mnozí uživatelé stěžovali na protivné „pop-upy“, Microsoft konfiguraci UAC zmírnil – a umožňuje tak přístup k DLL souborům. I ten, kdo chce používat Windows 7 na cestách, se tedy musí rozhodnout mezi obtěžujícími zprávami a bezpečnostní mezerou. Slabou útěchou může být, že uživatelé jiných operačních systémů na tom nejsou o nic lépe: Mac OS a Linux vždy, když mají být provedeny změny v systému, vyžadují heslo správce. Pod novými Windows 7 stačí kliknutí myší.

INFO: www.microsoft.com

MAC OS X

Jablka v ohrožení

Na počátku srpna vydala společnost Apple patche, kterými opravila 18 bezpečnostních mezer v operačním systému Mac OS X. Záplaty jsou mimořádně důležité, protože zneužití sedmi (ze zmiňovaných 18) mezer může vést až k totálnímu vzdálenému převzetí kontroly počítače útočníkem. Hrozba je o to nebezpečnější, že uživatel nemusí udělat nic „podezřelého“ – stačí jen, aby si prohlédl speciálně upravený obrázek.

A příčiny? Za pěti ze sedmi „obrázkových děr“ stojí mezery v aplikaci ImageIO Framework, zbývající dvě má „na triku“ ColorSync a jeho komponenta „ImageRAW“. Zmiňované zranitelnosti vytvářejí takřka ideální podmínky pro útočníky, kteří mohou pomocí upravených souborů s formáty PNG, OpenEXR a RAW propašovat do počítače libovolný kód.

Další záplaty opravují chyby v kornelu OS X, přihlašovacím okně a jiných částech operačního systému. I tyto chyby lze zneužít ke spuštění libovolného kódu. Poslední z chyb se nachází v komponentě známé pod jménem XQuery a související s XML. Před podobnou zranitelností v open-source knihovnách XML, která postihuje enormní množství aplikací, varovali švédští výzkumníci už před několika dny (viz například článek na serveru The Register, **www.theregister.co.uk/2009/08/06/xml_flaws/**). Prozatím se ale neví, zda spolu obě zmiňované zranitelnosti úzce souvisí. Opravné záplaty, které přicházejí jakou součást OS X 10.5.8, také řeší chyby a problémy v MobilMe. Podrobnější informace o jednotlivých problémech a jejich řešeních najdete na webu firmy Apple.

INFO: zpravy.actinet.cz

NOVINKA OD AVG

Ochrana identity v češtině

Společnost AVG Technologies uvolnila do distribuce osm nových lokalizací aplikace AVG Identity Protection (IDP) včetně české verze. Aplikace IDP byla veřejnosti představena při uvedení verze AVG 8.5 na jaře tohoto roku poté, co společnost AVG Technologies akvizicí získala společnost Sana Security. Zatím však byla dostupná pouze v angličtině. Uživatelům, kteří dávají přednost českým verzím programů, se nyní otevírá snadná cesta, jak zajistit svému počítači neustálou ochranu před krádeží online identity, ale i před novými a dosud neznámými viry. Aplikace IDP je kompatibilní s většinou nejčastějších antivirů. Zároveň je také integrální součástí balíčku AVG Internet Security, který poskytuje komplexní ochranu při všech aktivitách na internetu.

Krádeže identity se ve světě již staly internetovým zločinem číslo jedna. Americká obchodní komise uvádí krádeže identity jako nejčastější důvod stížností spotřebitelů. V její „Zprávě o zneužívání identity“ za rok 2008 se uvádí, že pouze v USA se obětí stalo téměř 10 milionů lidí. Nástup tohoto trendu v ČR potvrzuje „Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2008“, vydaná počátkem letošního května ministerstvem vnitra.

Aplikace AVG Identity Protection přidává vrstvu ochrany, která zdokonaluje celkové zabezpečení před hrozbami nerozpoznatelnými pro běžné antivirové aplikace. Je přitom lhostejné, zda jsou na počítači nainstalovány produkty AVG, nebo jiné firmy. IDP pracuje vedle všech nejčastěji používaných antivirů spolehlivě a kdykoli. Brání cíleným útokům vedeným s cílem krádeže hesel, odcizení podkladů k internetovému bankovnictví, čísel kreditních karet a dalších cenných informací. Používá tzv. behaviorální analýzu, která zjišťuje odchylky od standardního chování programů v počítači. Pokud odhalí cokoli podezřelého, co by mohlo naznačovat pokus o krádež identity, odstraní hrozbu a ukončí danou aktivitu ještě před zasažením uživatelových dat.

Aplikace AVG Identity Protection je založena na technologii, kterou společnost AVG Technologies získala po akvizici společnosti Sana Security počátkem tohoto roku. Analyzuje chování jednotlivých programů, proto nepotřebuje ke své aktualizaci popisy známých škodlivých kódů a předejde snaze útočníků odcizit uživateli on-line identitu. Software se navíc průběžně učí i z informací uživatelů o reálných útocích a zajišťuje jejich ochranu.

Veškeré produkty AVG 8.5 jsou k dispozici on-line, v obchodech a dalších prodejních kanálech. AVG Identity Protection stojí 595 Kč včetně DPH. Ceny ostatních produktů se nemění.

INFO: www.grisoft.cz

INFO

Nová bezpečnostní rizika

APPLE IPHONE OO

Byla potvrzena zranitelnost Apple iPhone OS 1.0 až 3.0, která umožňuje útočníkovi spustit v telefonu libovolný kód pomocí odeslání upravené SMS zprávy. Chyba je opravena ve verzi 3.0.1. Více informací naleznete na stránkách Apple.com (konkrétně na adrese **http://support.apple.com/kb/HT3754**) nebo v původním oznámení zranitelnosti na serveru **www.blackhat.com**.

INFO: zpravy.actinet.cz

ITUNES

Hudební software iTunes firmy Apple obsahuje dvě bezpečnostní mezery, které hackerům umožňují načíst uživatelské informace a program i celý počítač přivést ke zhroucení. Řešení je ale snadné: nainstalujte si verzi 8.1.

INFO: www.itunes.com

MOZILLA FIREFOX

V prohlížeči Mozilla Firefox byla nalezena zranitelnost umožňující zobrazení falešné URL v adresním řádku aplikace. Útočník tak může zranitelnosti zneužít např. takovým způsobem, že přesvědčí uživatele, že se pohybuje na jiném webu, než na kterém ve skutečnosti opravdu je, a ten mu nechtěně může při pokusu o přihlášení do svého účtu na podvodném webu odeslat své přihlašovací údaje k webu, za který se tento vydává. Zranitelnost je potvrzena ve verzích 3.0.12 a 3.5.1, ostatní verze mohou být taktéž zasaženy. Více informací na serveru Secunia.com (**http://secunia.com/advisories/36001/**). Řešením je aktualizace na novější verze prohlížečů (3.0.13 a 3.5.2)

INFO: zpravy.actinet.cz

WINDOWS

K proniknutí do cizích počítačů využívají hackeři také zmanipulované multimediální soubory. Další bezpečnostní mezera umožňuje třetím osobám webové přístupy uživatele bez jeho vědomí přesměrovat na libovolné stránky. Opravy slabých míst jsou však již k dispozici jako funkce Windows Update.

INFO: www.microsoft.com

INFO

Nová bezpečnostní rizika

CISCO IOS

Cisco vydalo opravné patche na dvě DoS zranitelnosti Cisco IOS. Napadnutelné jsou pouze verze, které používají podporou RFC4893 („BGP Support for Four-octet AS Number Space“). Více informací naleznete v oznámení na WWW stránkách výrobce (**www.cisco.com**).
INFO: zpravy.actinet.cz

VLC MEDIA PLAYER, MPLAYER

V oblíbeném multimediálním přehrávači byla nalezena zranitelnost, která je způsobena chybou ve funkci „real_get_rdt_chunk()“. Zranitelnost může být zneužita k heap-based buffer overflow útokům a v konečném důsledku ke spuštění libovolného kódu. Více informací naleznete v původním oznámení o zranitelnosti (**http://archives.neohapsis.com/archives/bugtraq/2009-07/0198.html**). Pro VLC Media Player 1.0.0 byl vydán opravný patch, pro Mplayer zatím pouze neoficiální.
INFO: zpravy.actinet.cz

CISCO WIRELESS LAN CONTROLLERS

V Cisco Wireless LAN Controllers bylo nalezeno několik chyb, které mohou způsobit DoS nebo restartování systému, a jedna, jejíž úspěšné zneužití může vést k úplnému převzetí kontroly nad zařízením. Více informací naleznete na stránkách **www.cisco.com**, případně na webu Secunia.com (**http://secunia.com/advisories/35982/**).
INFO: zpravy.actinet.cz

MOZILLA FIREFOX, THUNDERBIRD

V aplikacích Mozilla Firefox a Thunderbird byly zjištěny zranitelnosti, které mohou být zneužity k poškození paměti a potenciálně i ke spuštění zákeřného kódu. Ve Firefoxu, konkrétně ve verzích 3.5 a 3.0.12, již byly zranitelnosti opraveny. Více informací naleznete na adrese **www.mozilla.org/security/announce/2009/mfsa2009-34.html**. Pro Thunderbird zatím neexistují opravné patche. Výrobce doporučuje zakázat spouštění JavaScriptu, dokud patche nebudou k dispozici.
INFO: zpravy.actinet.cz

ADOBE READER/ACROBAT

Byla oznámena aktuálně zneužívaná zranitelnost v Adobe Readeru a Acrobatu verze 9.1.2 a dřívější 9.x verze pro Windows, Macintosh a UNIX. Jedná se o chybu v authplay.dll při zpracování SWF souboru, která může být zneužita k vykonání libovolného kódu. Doporučuje se odstranit přístup do authplay.dll knihovny a neotvírat nedůvěryhodné PDF dokumenty. Aktualizace bude dostupná 31. července. Více informací na **www.adobe.com**.
INFO: zpravy.actinet.cz

SUN SOLARIS XSCREENSAVER

Blíže nespecifikovaná chyba byla nalezena v operačním systému Sun Solaris, konkrétně v XScreenSaveru (xscreensaver(1)). Program může být zneužit k získání citlivých informací. Postižen je SPARC Platform a x86 Platform. Dosud nebylo vydáno konečné řešení. Více informací naleznete na webu **http://sunsolve.sun.com** pod kódem 264048.
INFO: zpravy.actinet.cz

ZÁPLATY A ZRANITELNOSTI

Mozilla Firefox a Thunderbird v servisu...

Mozilla vydala opravné patche pro Firefox, týkající se čtyř kritických chyb, včetně jedné, která útočníkům umožňovala vytvoření univerzálního certifikátu, díky kterému Firefox ověřil veškeré webové stránky a nevyžadoval po uživateli potvrzení bezpečnostního certifikátu. Moxie Marlinspike, jeden z výzkumníků, kteří zranitelnost objevili, uvádí, že většina softwaru, která používá SSL, je také zranitelná, takže můžeme očekávat další patche. Zranitelnosti byly opraveny ve verzích 3.5 a 3.0.13, zranitelné jsou i další produkty Mozilly – Thunderbird, SeaMonkey a NSS. Pro ně se patche připravují. Více informací naleznete na webu TheRegister.co.uk (**http://www.theregister.co.uk/2009/08/04/firefox_critical_update/**), případně na webu Mozilla.com.
INFO: zpravy.actinet.cz

STATISTIKY ESET

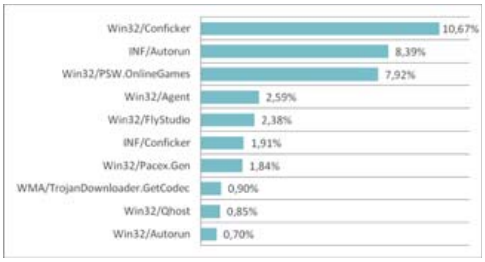
Nová hrozba útočí na prohlížeč

Podle statistického systému Eset ThreatSense.Net se v červenci nejvíce šířila infiltrace **Win32/Conficker**, a to s celosvětovým podílem 10,67 % ze všech detekovaných hrozeb. Ve vysokém počtu se stále šíří hrozby, které pro své spuštění využívají funkci autorun.inf operačního systému MS Windows. Takové škodlivé kódy mají většinou podobu trojských koní a Eset je souhrnně označuje jako **INF/Autorun**. V červnu byl jejich podíl na všech zachycených počítačových hrozbách 8,39 %. Třetí místo celosvětově v červenci patřilo opět různým variantám trojských koní útočících na on-line hry a jejich uživatele – **Win32/PSW.OnLineGames** (7,92 %).

Celosvětově čtvrtý byl v červenci **Win32/Agent**. Eset tak označuje různé varianty rodiny Agent, které jsou schopné vykrádat informace z uživatelova počítače. Do první pětky se poprvé dostala zcela nová infiltrace – **Win32/FlyStudio**. Hrozba je navržena tak, aby modifikovala informace v internetovém prohlížeči. Je schopná měnit požadavky na vyhledávání s cílem doručit uživateli co nejvíce nevyžádané reklamy. FlyStudio je populární skriptovací jazyk především v Číně, kde patří Win32/FlyStudio mezi nejrozšířenější hrozby. Kromě Číny se zatím hrozba šíří nejvíce v USA, Mexiku a Argentině.

Česko a **Slovensko** zůstávají i v červenci regionálními výjimkami. V celé okolní Evropě vládne Conficker, u nás je to však novinka minulého měsíce Win32/TrojanDownloader.Bredolab.AA. V červenci ovládal místní 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. Trojan Bredolab se pomalu šíří i v okolních krajinách regionu, jedničkou tam však zůstává Win32/Conficker.

Například v **Polsku** a ve **Francii** v červenci dominovala směs trojských koní ohrožující virtuální identity hráčů on-line her Win32/PSW.OnLineGames. Severní Evropa a země Beneluxu jsou již delší dobu specifické místní dominancí trojanů pod názvem WMA/TrojanDownloader.GetCodec. Tyto trojské koně projdou všechny hudební soubory populárních audioformátů, které v počítači naleznou, a všechny mírně upraví. Při otevření se přehrávač následně pokusí stáhnout škodlivý obsah z internetové stránky, na kterou ho infikovaný soubor odkáže.
INFO: www.grisoft.cz



BEZPEČNOSTNÍ TIPY

Letní surfování přes Wi-Fi: Pozor na útoky

Léto je v plném proudu a často vídáme lidi, kteří si užívají volna nebo pracují s notebooky v městských parcích – chatují, blogují, sdílejí fotografie nebo jen tak surfují po internetu díky bezplatným Wi-Fi zónám. Ty se stávají čím dál tím běžnější součástí městského života, případně života přímořských letovisek. Čistě z pohledu výrobce bezpečnostního softwaru je třeba mít na mysli, že venkovní surfování není bezpečné (bezpečnost není zaručena). WEP šifrování, které se u Wi-Fi sítí často využívá, je slabé a snadno zneužitelné. Podle výzkumu ABI Research je Wi-Fi hotspotů stále více. Největší nárůst byl zaznamenán v Evropě, přičemž minimálně jeden Wi-Fi hotspot existuje v každém větším městě Evropy či na Blízkém východě.

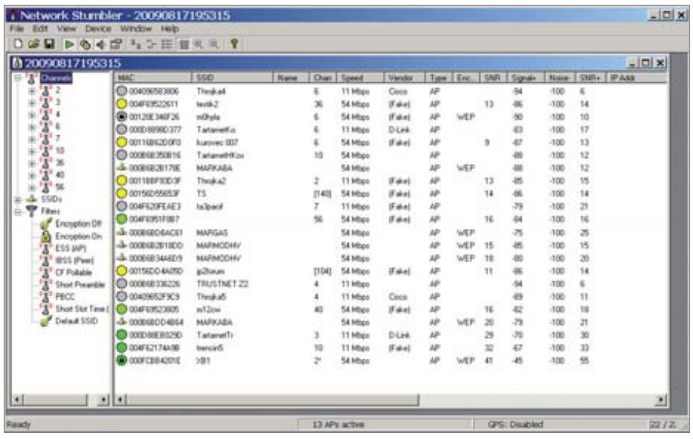
Podle Juraje Malcha, vedoucího Virus Labu společnosti ESET, je jednou z nejhorších hrozeb takzvaný man-in-the-middle útok. „Pokud je k síti připojen někdo jiný, může její směrování modifikovat tak, aby si uživatel myslel, že například komunikuje se svojí bankou, ale ve skutečnosti poskytuje údaje neznámému útočníkovi."

„Pracujeme-li s počítačem, je dobré používat šifrovaný (https) přístup k e-mailům. Uživatel by měl zvážit tzv. VPN přístup a vyhnout se přístupu na stránky, přes které posílá citlivé údaje (například při komunikaci s bankou)," dodává Juraj Malcho.

Existuje několik kroků, které může každý udělat, aby zvýšil ochranu před různými druhy počítačových infiltrací.

Druhy bezpečnostních ohrožení při používání Free Wi-Fi:

► **Evil twin login interception** (hackeři vytvoří síť, která připomíná legitimní Wi-Fi hotspot, při pokusech přihlásit se do jejich sítě získají přihlašovací údaje).
► **Útok přes dosud neznámou bezpečnostní díru** (zero-day útoky na operační systém nebo aplikace).
► **Sledování komunikace** (logování komunikace a přenos informací do sítě hackera).
► **Vykrádání dat** (man-in-the-middle útok).



Bezpečné surfování: Wi-Fi sítí přibývá, s jejich bezpečností je to ale horší...

Jak chránit svůj počítač při práci s Wi-Fi:

► Ujistěte se, že porty pro VPN jsou zapnuté, **nepovolte však porty s vysokým číslem,** přístupné pro všechny.
► Pro přístup k e-mailům **použijte šifrovaný protokol HTTPS**.
► Kdekoli je to možné, **vyhněte se protokolům, které nemají šifrování.**
► **Vypněte sdílení** souborů, aplikací apod.
► **Nevykonávejte aktivity, při kterých je nutné zadávat citlivá data,** jako například internet banking.
► **Ujistěte se, že máte zapnutý firewall, antivirus a antispyware.**

Pět věcí, které musíte letos v létě udělat pro svůj počítač

Ještě než začnete pracovat se svým notebookem na veřejných místech s bezplatným internetovým připojením, udělejte něco užitečného pro větší bezpečnost.
1. Aktualizujte si webový prohlížeč. Ujistěte se, že máte nainstalovanou nejnovější verzi svého oblíbeného, případně nejčastěji používaného internetového prohlížeče. Autoři počítačových infiltrací často zneužívají pro šíření svých „děl" právě nezabezpečená místa v internetových prohlížečích.
2. Změňte všechna přístupová hesla. Není to určitě nic příjemného, hlavně proto, že bude nutné si zapamatovat nové kombinace čísel a písmen, naštěstí to ale není zase tak složité. Změňte minimálně hesla pro přihlášení do počítače (jestliže nemáte nastaveno přihlašování do notebooku po jeho zapnutí, učiňte tak), dále změňte hesla k e-mailové schránce, k sociálním sítím a k jiným místům, kde se nacházejí vaše osobní údaje. Doporučujeme zvolit silná hesla, která mohou mít pro lepší zapamatování spojitost s něčím, co je vám blízké, ale snažte se kombinovat velká písmena s malými a s čísly.
3. Nastavte na notebooku běžný režim místo administrátorského. Počítač vám umožňuje vybrat si běžný režim, nebo s ním pracovat jako administrátor. Pro surfování na veřejných místech zvolte raději běžný uživatelský režim, který vám neumožní instalovat a přidávat do počítače nové aplikace či software. Aspoň se tím vyhnete případům, kdy vám bude nějaká počítačová infiltrace chtít do notebooku nainstalovat nebezpečnou aplikaci.
4. Zálohujte. Ještě než svůj notebook vezmete s sebou na dovolenou, do kavárny či do parku, zazálohujte si hodnotná data, jako například fotografie, hudbu, dokumenty, smlouvy, akademické práce apod., na CD nebo USB. Notebook je možné poškodit nebo odcizit. Zálohováním aspoň nepřijdete o cenná data.
5. Aktualizujte bezpečnostní software a průběžně skenujte. Ujistěte se, že máte aktualizovaný bezpečnostní software s nejnovější databází počítačových hrozeb a průběžně – po skončení práce v zóně Wi-Fi – notebook oskenujte, zda nejsou přítomné infiltrace.

MICROSOFT

Útok na klávesnici

Bezpečnostní specialisté Max Moser a Thorsten Schröder objevili možnost, jak odposlouchávat rádiové signály bezkabelových klávesnic. Postiženy jsou modely Optical Desktop 1000 a 2000 od Microsoftu. Přístroje vysílají na frekvenci 27 MHz a jsou zabezpečeny pouze 8bitovým šifrovacím kódem. Podstatou útoku je procesor TRF7900A firmy Texas Instruments, který se v modelech Microsoftu používá. Pro tuto CPU sestavili hackeři modifikovanou desku elektroniky, s níž lze signály klávesnic odposlouchávat.

Microsoftu je slabina bezkabelových klávesnic známa. Aktualizace by ovšem znamenala výměnu hardwaru, říká výrobce. Zabezpečeny proto mají být až další generace bezkabelových klávesnic. Modely jiných výrobců používají jiné čipové sady, a jsou proto proti takovému napadení imunní. Postiženy nejsou ani přístroje využívající Bluetooth. Oba hackeři jsou však podle vlastních vyjádření schopni odposlouchávat i 2,4GHz komponenty.
INFO: www.microsoft.com

ASUS TV MONITOR T1

Stylové monitory s TV tunerem

Společnost Asus uvedla na trh TV monitory řady T1, dostupné ve velikostech 22", 24" a 27", které jsou vybaveny vestavěným televizním tunerem, jenž umožňuje sledovat digitální (DVB-T) i analogové (PAL/SECAM) vysílání. Monitory jsou vybaveny dvojicí 7wattových reproduktorů a mnoha vstupními a výstupními porty (2× SCART, D-Sub, kompozitní, komponentní, S-Video, audiojack, výstup S/PDIF, zvukový výstup, výstup sluchátek a slot CI). Podporují Full HD 1080p rozlišení (1 920 × 1 080) a mají i dva HDMI vstupy. Technologie Asus Smart Contrast Ratio (ASCR) zvyšuje kontrast až na hodnotu 20 000:1. Jas je podle výrobce 300 cd/m^2. Monitory jsou dodávány s dálkovým ovladačem.

INFO: **ww.asus.cz**

SAMSUNG XL2370

LED monitor tenký jako prst

Společnost Samsung Electronics uvedla 23palcový monitor Samsung XL2370, který je vybaven technologií LED, je tenký jako prst a spotřebuje přibližně o 40 % elektrické energie méně než běžný monitor podobné velikosti. Monitor nabízí kontrastní poměr (5 000 000:1), má rozlišení Full HD (1 920 × 1 080) a doba odezvy je jen 2 ms (GTG). Velký důraz byl kladen na design. Rám monitoru omezuje světelné odrazy a odlesky. Lesklý černý podstavec doplňuje noha z čistého křišťálového akrylátu; monitor tak působí dojmem, že se vznáší. Orientační maloobchodní prodejní cena monitoru Samsung XL2370 činí 9 490Kč včetně DPH.

INFO: **www.samsung.cz**

MOBIL V HODINKÁCH

Samsung S9110

Samsung představil zajímavý mobilní telefon Samsung S9110, kterému designéři vtiskli podobu elegantních náramkových hodinek. Nejtenčí mobilní telefon tohoto typu na světě zaujme především originálním designem s 1,76“ plně dotykovým displejem, sponou z nerezové oceli nebo například koženým páskem. Samsung S9110 svému uživateli nabídne i řadu užitečných funkcí: Bluetooth 2.1, GPRS, MP3 přehrávač, rozpoznání hlasu, synchronizaci s počítačem nebo například možnost pracovat s maily přes Outlook.

INFO: **www.samsung.cz**

SONY CYBER-SHOT TX1 A WX1:

Fotografie i za šera

Od září letošního roku budou dostupné dva nové fotoaparáty firmy Sony: Cyber-shot TX1 a WX1. Zobrazovací vlastnosti obou fotoaparátů stojí na snímači Exmor R CMOS s rozlišením 10,2 megapixelu a na obrazovém procesoru Sony BIONZ. Snímač Exmor R využívá nové vnitřní uspořádání, podle výrobce dokáže zachytit více světla než klasická CMOS konstrukce. Fotoaparáty nabízí režim širokého panoramatu „Sweep Panorama“: stačí stisk spouště a pak fotoaparát plynule přesunout horizontálně nebo vertikálně z jedné strany na druhou, a funkce automaticky spojí sérii zachycených políček do jednoho velkého panoramatického snímku. Režim fotografování z ruky za soumraku (Handheld Twilight) zkombinuje šest sériově vyfotografovaných políček do jednoho optimalizovaného snímku s nižší hladinou šumu při špatných světelných podmínkách. Další funkcí je redukce rozmazání pohybem (Anti Motion Blur). Ta je určena pro fotografování rychle se pohybujících objektů při špatném osvětlení. Oba fotoaparáty natáčejí také videoklipy se zvukem v rozlišení 720p HD a se snímkovou frekvencí 30 fps. K dispozici je i optický stabilizátor a funkce detekce obličeje a úsměvu. Štíhlý model TX1 (tloušťka 14,1 mm) je k dispozici v pěti barvách a má velký, 3palcový dotykový displej. Cyber-shot WX1 je nová vlajková loď řady W. Má 5násobný optický zoom a 2,7" displej.

INFO: **www.sony.cz**

PORTÁLY

Aukro.cz prodává nemovitosti

Servery Bezrealitky.cz a Aukro.cz se spojily a nemovitosti je nyní možné nakupovat i na aukčním portálu Aukro.cz. Návštěvníkům portálu Aukro.cz novinka přinese větší uživatelský komfort. Pokud hledají nemovitost, nemusí chodit na jiné webové stránky, širokou nabídku v řádu tisíců položek najdou na jednom místě. Aukce v sekci Nemovitosti probíhají stejným způsobem jako standardní aukce. Rozdíl je však v tom, že výhra v aukci uživatele Aukra nezavazuje k uzavření smlouvy o prodeji nebo pronájmu. Systém v tomto případě funguje pouze jako zprostředkovatel mezi prodávajícím a potenciálním zájemcem.

INFO: **www.aukro.cz**

PRESTIGIO DATARACER II

Od designéra Alfy Romeo

Společnost Prestigio představila nový přírůstek do své produktové řady Racer – externí pevný disk Prestigio DataRacer II (DR2). Od předchůdce DataRacer I se liší dravějším designem, který vytvořili návrháři z kyperského studia Demades Design pod vedením Nicolase Demadese. Prestigio DR2 je výkonným přenosným 2,5” eSATA diskem s kapacitou až 500 GB a rychlostí do 7 200 ot./min. Disk je vybaven eSATA portem pro maximální přenosovou rychlost a k napájení využívá druhý USB 2.0 port. Pro zvýšení přenosové rychlosti je vybaven softwarovým modem Turbo od společnosti FNet. Rozměry disku jsou 148 × 94 × 24 mm.

INFO: **www.prestigio.cz**

CANON HYBRID IS

Hybridní optický stabilizátor obrazu

Společnost Canon oznámila, že vyvinula hybridní stabilizátor obrazu (Hybrid IS) – první optický stabilizátor obrazu, který vyrovnává rotační i lineární roztřesení snímku. Nová technologie bude poprvé použita ve výměnném objektivu pro jednooké zrcadlovky (SLR), jehož prodej bude zahájen před koncem roku 2009.

Společnost Canon zahájila výzkum metod kompenzace roztřesení snímku v 80. letech. V roce 1995 uvedla na trh objektiv EF 75–300 mm f/4–5,6 IS USM, výměnný objektiv pro jednooké zrcadlovky opatřený mechanismem vyrovnání roztřesení fotoaparátu. Nově vyvinutá technologie hybridní stabilizace obrazu Canon optimálně vyrovnává rotační roztřesení snímku (úhlové) i lineární roztřesení snímku (posuvné). Při standardním fotografování mohou náhlé změny v natočení fotoaparátu způsobit značné rozmazání snímku, zatímco roztřesení lineární, při kterém se fotoaparát pohybuje paralelně s fotografovaným objektem, je zřetelnější v makrofotografii a při fotografování detailů.

INFO: **www.canon.cz**

Archiv TV Nova ve Viera Cast

V polovině července zprovoznila společnost Panasonic kompletní archiv TV Nova ve své aplikaci Viera Cast, implementované v televizorech. Diváci v České a Slovenské republice si tak mohou na televizoru spustit jakýkoli pořad či seriál z portálu nova.cz v kvalitě digitálního vysílání.

Služba Viera Cast je k dispozici zdarma v nových modelových řadách televizorů Panasonic Viera G15, V10 a Z11, ale i v domácích kinech a všech Blu-ray přehrávačích představených letos na jaře. Stisknutím tlačítka na dálkovém ovladači se divák dostane k oblíbenému internetovému obsahu. Viera Cast kromě archivu TV Nova již nyní nabízí přístup na videoserver YouTube.com, server pro ukládání fotografií Picasa.com, ke kanálu Eurosport nebo informacím agentury Bloomberg.

INFO: **www.panasonic.cz**

2,5" PEVNÉ DISKY

Verbatim rozšiřuje řadu barevných disků

Verbatim přidává do svého portfolia přenosných 2,5" pevných disků pět nových barevných modelů – Sun kissed Yellow, Eucalyptus Green, Hot Pink, Caribbean Blue a Volcanic Orange. Uživatelé mohou věnovat větší pozornost designu a mohou přizpůsobit vzhled svého počítače podle svých představ. Disky se připojují přes USB port, mají hmotnost 161 g, kapacitu 500 GB a v obchodech jsou již k dostání za 2 859 Kč. Na discích najdete předinstalovaný software Nero BackItUp 4 Essentials, který umožňuje pravidelné zálohování souborů z notebooku či PC na přenosný pevný disk.

INFO: **www.verbatim-europe.cz**