DATA A FAKTA

Barometr nebezpečí
v říjnu:

Jak uživatelé chrání své sítě

1. Antivirový program
86,1 %

2. Antispywarové nástroje
44,8 %

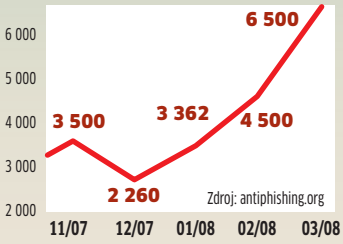
3. Bezdrátové šifrování
44,7 %

Zdroj: Webroot

Proti zneužití rádiové sítě se chrání heslem méně než polovina uživatelů.

Krádeže hesel

Počet phishingových URL



Rostoucí nebezpečí: Na stále větším počtu webových stránek hackeři vyzvídají hesla uživatelů.

BEZPEČNOSTNÍ WEB CHIPU

www.chip.cz

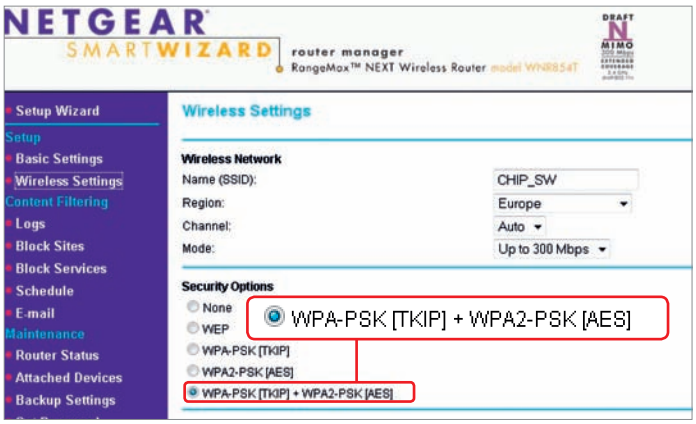
I na našem novém webu najdete zajímavé informace a tipy a triky z oblasti bezpečnosti.

Jak WLAN zničí sama sebe

Pomocí jednoduchého datového paketu dokáží hackeři proměnit bezdrátový router ve **VRAŽDÍCÍHO MANIAKA** a každou WLAN v několika sekundách ochromit.

FABIAN VON KEUDELL

Pouhých pět vteřin stačí Sohailu Ahmadovi na to, aby vaši bezdrátovou síť učinil nepoužitelnou. Jeho útok se dá přirovnat k lidské autoimunitě. Tak lékaři označují situaci, při níž imunitní systém napadá vlastní zdravé buňky a ničí je. U WLAN to funguje podobně – jediný zmanipulovaný datový paket dokáže změnit směrovač v zabijácký stroj, který nijak nerozlišuje mezi dobrem a zlem. Nepomůže proti tomu ani aktuální šifrování WPA2 s AES a 20místným klíčem, ani filtrování MAC adres, které do WLAN vpustí jen důvěryhodné koncové přístroje. Skutečná obrana proti útoku prominentního hackera tedy neexistuje. Zbývá chabá útěcha, že vlastní data nedokáže ze sítě vyčíst ani Ahmad. Umí jen přerušit momentální spojení mezi klientem a serverem a zabránit samočinnému opětovnému navázání spojení přístrojů. Tento nový druh DoS útoku (Denial of Service) znamená hrozbu především pro komerční WLAN, neboť síť může znovu zprovoznit jen hardwarový reset. To je u soukromých sítí sice nepříjemné, nicméně proveditelné. Komerční varianty však většinou mívají i několik set přístupových bodů...



Šifrování nepomůže: Ani sítě, které jsou chráněny aktuální šifrovací metodou WPA2-AES, nemají proti WLAN hackerům šanci.

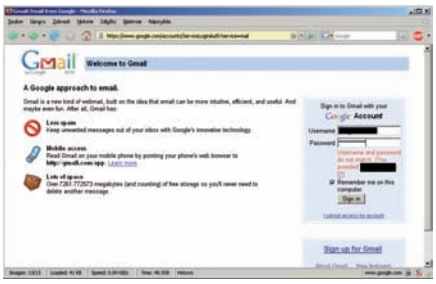
Útočník ani nemusí vynaložit žádné zvláštní úsilí: ve standardu WLAN je definována řídicí sada příkazů, které účastníka sítě žádají, aby se nově autorizoval. Donedávna hackerům stačilo jednoduše do sítě podstrčit takový řídicí paket, který opatřili MAC adresou routeru. Nyní už je však mnoho přístupových bodů proti tomuto útoku chráněno. Ahmadova metoda jde o krok dále: datový paket speciálně upraví a opatří jej MAC adresou odesílatele (ff:ff:ff), která není definována ve standardu IEEE-802.11. S tímto hackerským paketem pak požádá router o autentizaci klienta. Tento požadavek je stejně prostý jako zákeřný, neboť většina směrovačů na tuto zprávu reaguje příkazem pro odhlášení klientů v celé síti. Fatální je na tom to, že klienti už se samostatně k routeru nepřihlásí, protože ten nadále připojení odmítá. Výrobci už pracují na aktualizaci firmwaru. Dbejte proto, abyste ve svém směrovači vždy měli nainstalován nejnovější software. Chcete-li zkontrolovat, která verze ve vašem vysílači běží, otevřete jeho konfigurační stránku ve webovém prohlížeči na PC, většinou to bývá adresa »192.168.1.1«. Tam najdete – často pod »Firmware« – aktuální číslo. Není-li ještě update k dispozici, deaktivujte vysílací režim SSID.

INFO: airtightnetworks.com

GOOGLE MAIL

Hacking poštovní schránky

Vinou bezpečnostní mezery v poštovní službě Googlu mohou útočníci získat přístup k soukromým poštovním schránkám uživatelů.



Na bezpečnostní konferenci Defcon vysvětlil objevitel mezery Mike Perry potřebný postup: Předpokládejme, že ve veřejné síti, například prostřednictvím WLAN hotspotu, se oběť přihlásí na Google Mail přes šifrované HTTPS spojení a potom vyvolává libovolné další webové stránky. Hacker, který je připojen ke stejné síti, volání webové stránky rozpozná a do počítače oběti vyšle přesměrovávací datový paket. Napadený počítač se znovu hlásí u Googlu – tentokrát ovšem nechráněně prostřednictvím jednoduchého spojení HTTP. Pak může hacker „odposlouchat" přihlašovací údaje a zjistit jméno a heslo uživatele. Žádnou obranu proti tomuto útoku dosud Google nenabídl

INFO: www.googlemail.com

INFO

Nová bezpečnostní rizika

APPLE QUICKTIME

Celých devět kritických mezer v nástroji QuickTime mohou hackeři využít, aby do cizího počítače dopravili vlastní kód. Škodlivé programy je pak možno spouštět s oprávněním správce. Logickým řešením je update na aktuální verzi. Ve verzi QuickTime 7.5.5 jsou již chyby odstraněny...
INFO: www.apple.cz

NETBSD

V operačním systému NetBSD byla nalezena zranitelnost. Díky chybě v Neighbor Discovery protokolu může vzdálený útočník na stejné fyzické síti posílat tzv. ICMPv6 žádosti routeru, což může vyústit ve změnu směrovacích informací oběti. Následkem toho může útočník odříznout síťový provoz, případně způsobit DoS. Více informací naleznete na webu **www.netbsd.org**.
INFO: zpravy.actinet.cz

VLC MEDIA PLAYER

V populárním multimediálním přehrávači byla objevena zranitelnost. Ta je způsobena chybou při zpracování souborů TY, může být zneužita ke stack-based buffer overflow útokům a tím ke spuštění libovolného kódu. Zranitelnost je hlášena ve verzích 0.9.0 až 0.9.4, ostatní mohou být také zasaženy. Více informací naleznete na **www.videolan.org/security/sa0809.html**.
INFO: zpravy.actinet.cz

GOOGLE CHROME

Vyvoláním přetečení bufferu ve funkci »Uložit jako« může útočník nahrát do počítače spustitelný kód.
Řešením je instalace aktuální beta verze (v době psaní článku to byla verze 0.3.154.9). Na důležitých počítačích byste však měli počkat na finální verzi browseru.
INFO: www.google.com/chrome

FCKEDITOR

FCKeditor (WYSWYG editor používaný v mnoha webových aplikacích) obsahuje zranitelnost dovolující upload libovolného souboru, jelikož nedostatečně kontroluje uživatelem poskytnutý vstup. Útočník toho může zneužít k nastrčení libovolného kódu a jeho spuštění v kontextu webserverového procesu. To může usnadňovat nejen neautorizovaný přístup nebo navýšení oprávnění uživatele, ale i další útoky. Více naleznete na webu SecurityFocus.com (**www.securityfocus.com/bid/31812/**).
INFO: zpravy.actinet.cz

WINDOWS MEDIA PLAYER 11

Bezpečnostní mezera v Media Playeru ve Windows umožňuje hackerům přenést programy do počítače oběti a převzít nad ním kontrolu. Řešení je snadné – nainstalujte si nejnovější verzi přehrávače prostřednictvím služby Windows Update.
INFO: www.microsoft.cz

GOOGLE CHROME

Další chyba nalezená v prohlížeči Google Chrome dovoluje útočníkům vést útoky typu spoofing – tedy vydávat webové stránky za jiné. Ačkoli je prohlížeč založen na jádru Safari od Applu, v Safari je tento problém ošetřen. Pravděpodobně se tedy jedná o chybu způsobenou chybným kódem použitým programátory Googlu. Podrobnější informace naleznete na portálu The Register (**www.theregister.co.uk/2008/10/26/google_chrome_address_spoofing/**).
Podle vyjádření Googlu se jedná o známý problém a opravu najdete již ve verzi 0.3.154.3.
INFO: zpravy.actinet.cz

DĚTI NA INTERNETU

Bezpečný internet s kampaní

Poradna bezpečného internetu, kterou provozuje Linka bezpečí, naplňuje záměry EU chránit děti na internetu. Problematika bezpečného internetu je v současné době velmi aktuální. K ochraně dětí na internetu může pomoci dětská poradna Internet Helpline, kterou provozuje Linka bezpečí a která je součástí tuzemského osvětového projektu Saferinternet.cz. Bezpečností dětí na internetu se v posledních dnech zabýval také Evropský parlament, který schválil návrh na uvolnění finančních prostředků pro projekty řešící bezpečný internet – prevenci a boj proti nebezpečnému obsahu a internetové kriminalitě.

Co si myslí o internetu rodiče?
Britská on-line studie společnosti Insight Research Group dokazuje, že si 91 % evropských rodičů myslí, že internet pomáhá dětem rozvíjet jejich schopnosti. Podle průzkumu agentury Gemius si rodiče většinou myslí, že vědí, co jejich děti na internetu dělají. Například 74 % dospělých se domnívá, že vědí o schůzkách svých ratolestí. Ve skutečnosti se však rodičům svěřuje pouze 22 % dětí. Výzkumy dále uvádějí, že zhruba 20 % lidí, se kterými se děti a mladí lidé po seznámení na síti sešli na reálné schůzce, jsou „jiné" osoby, než za koho se na internetu vydávali. V praxi to znamená, že každý pátý člověk na internetu se vydává za někoho jiného.

Problematika bezpečného internetu je tedy velmi aktuální a rodiče by měli vědět, co jejich děti na síti dělají. K tomu může pomoci například tuzemský kombinovaný projekt Saferinternet.cz včetně dětské poradny Internet Helpline.

Komentář redakce: *Bezpečnosti dětí se podrobněji věnujeme na jiném místě našeho časopisu (konkrétně na straně 126), přesto nelze nereagovat na nesmysly, které podobné podivné organizace vymýšlí za naše peníze. Je sice hezké, že se dozvíme, kolik procent dětí se nám „skutečně svěřuje", informace o bezpečnějším internetu ale bohužel musíte hledat jinde. Pokud to přesto zkusíte na webu* ***www.internethelpline.cz****, dozvíte se opravdové perly:*

► Naučte děti používat „child-friendly" vyhledávače, které jim bezpečně pomohou nejen s vypracováním domácích úkolů…

► Internetové účty vždy zadávejte pod svým jménem a jako rodiče si sami zvolte vhodné vstupní uživatelské jméno (login – primary screenname), kontrolní hesla (passwords) či použité zámky a filtrovací mechanismy (např. rodičovský zámek).

Zkoušeli jsme také použít telefonní helplinku, ale nad dotazem, pomocí jakých programů chránit děti, paní Kameníčková jen „krčila rameny" a odkazovala nás na vedoucí projektu. Ta slíbila zavolat a už se neozvala.

INFO: www.internethelpline.cz

INFO

Nová bezpečnostní rizika

SUN JAVA WEB START

Sun Java Web Start obsahuje zranitelnost dovolující útočníkovi spuštění libovolného příkazu na počítači nic netušícího uživatele. To může napomáhat dalším útokům. Více informací najdete na webu SecurityFocus (**www.securityfocus.com/bid/31916/**), a to včetně proof-of-concept exploitu. Řešení problému prozatím známo není.
INFO: zpravy.actinet.cz

POČÍTAČE LENOVO

Aplikace Lenovo Rescue and Recovery je náchylná k přetečení vyrovnávací paměti. Úspěšné zneužití dovoluje útočníkovi kompletně kompromitovat postižený počítač. Zasažena je verze Lenovo Rescue and Recover 4.20. Více informací najdete na webu SecurityFocus.com (**www.securityfocus.com/bid/31737/**). Řešením je update na verzi 4.21, která je k dispozici na adrese **www-307.ibm.com/pc/support/site.wss/MIGR-4Q2QAK.html**.
INFO: zpravy.actinet.cz

LOTUS QUICKR

IBM Lotus Quickr je náchylný k několika nespecifikovaným cross-site scripting zranitelnostem, jelikož nedokáže dostatečně ošetřit uživatelem poskytovaný vstup. Útočník může zneužít tyto problémy ke spuštění libovolného skriptu v prohlížeči v kontextu zasažené webové stránky. To mu může pomoci odcizit přihlašovací údaje založené na cookies a vést další útoky. Více naleznete na webu SecurityFocus (**www.securityfocus.com/bid/32212**) nebo přímo u výrobce (**http://www-01.ibm.com/support/docview.wss?uid=swg27013341**), kde najdete i vydanou záplatu.
INFO: zpravy.actinet.cz

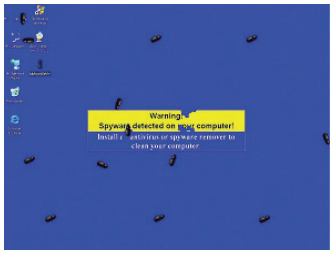
NOVÉ HROZBY

Falešné antiviry na 30 milionech infikovaných počítačů

Tento adware se začal šířit před necelým rokem a nyní je v oběhu více než 7 000 variant. Jeho cílem je přímý finanční zisk a „na lep" mu již sedlo několik milionů uživatelů.

Princip je jednoduchý – někdo vytvořil tisíce variant nového typu adwaru a rozšířil je po internetu. K infekci mohlo dojít různými způsoby – surfováním na erotických webech, při stahování na P2P sítích nebo instalací trojského koně. Dokonce již došlo ke zfalšování domácí stránky Googlu. Všechny typy tohoto malwaru však mají jedno společné: ohlásí uživateli, že jeho počítač je infikován. Poté se začnou spouštět spořiče, objevovat vyskakovací okna, falešné „modré obrazovky smrti", nebo dokonce švábi požírající pracovní plochu. Všechny tyto aktivity mají jediný cíl – donutit uživatele, aby koupil falešný antivir.

Zkušení uživatelé rychle pochopí, že jde o falešný antivir, a pokusí se ho odstranit. K charakteristickým rysům zmiňované hrozby však patří i mimořádně obtížná dezinfekce. Ne všichni uživatelé si ale všimnou, že něco není v pořádku. Stránky, na kterých se falešný produkt prodává, jsou technicky velmi kvalitní, což je ve spojení se zoufalou touhou uživatelů po vyčištění počítače smrtící kombinace.



Nejde tedy o žádnou novinku, přesto počet infikovaných počítačů rychle roste. Podle informací, které v Panda Labs získali, už bylo infikováno více než 30 milionů uživatelů. Podle aktuálních informací přibližně 3 % uživatelů skutečně „podlehlo" a poskytlo při „nákupu" autorům malwaru osobní informace a také zaplatilo 49,95 eura. Celkový zisk autorů malwaru se tak pohybuje v řádech desítek milionů eur. O budoucnosti čísel kreditních karet, které důvěřiví uživatelé použili k nákupu, se raději nebudeme ani zmiňovat…

INFO: www.pandasecurity.sk

APPLE

Sbohem, ochrano dat

Apple se v otázkách bezpečnosti těší velmi dobré pověsti – avšak pokud jde o iPhone, bohužel neprávem. Hackeři nyní objevili, jak mohou zjistit chráněná a soukromá data uživatelů telefonu. Hacker a bezpečnostní expert Jonathan Zdziarski zveřejnil dva postupy, které mu umožňují přístup k citlivým datům – normálně je iPhone proti neoprávněnému přístupu chráněn kódem PIN, avšak pomocí podvržené aktualizace firmwaru získá Zdziarski přístup do přístroje i bez PIN.

Druhé bezpečnostní riziko vlastně představuje jedna z vymožeností iPhonu. Jakmile v něm uživatel uzavře nějakou aplikaci, přístroj ji grafickým efektem „vyzoomuje“. Aby mohl tento efekt zobrazit, musí si ovšem telefon vytvořit snímek displeje. Háček však spočívá v tom, že tyto screenshoty aplikací se dají načíst jednoduchými forenzními nástroji, které jsou volně k dispozici na internetu. Vymazat tato data manuálně přitom nelze. To, zda se Apple chystá takovou funkci doplnit, nám výrobce iPhonu nechtěl prozradit.

INFO: **www.apple.cz**

BEZPEČNOSTNÍ SOFTWARE

TrustPort PC Security 2009

Společnost TrustPort, výrobce bezpečnostního softwaru pro ochranu počítačů i firemních sítí, oznamuje vydání ostrých verzí TrustPort PC Security 2009 a TrustPort Antivirus 2009. Do prodejní sítě vstupují na začátku listopadu, stejně jako předchozí verze jsou k dispozici s licencí pro 1, 3 a 5 instalací nebo v multilicenci pro větší počet pracovních stanic v síti.

TrustPort PC Security je ucelené řešení, poskytující ochranu počítače a dat v něm uložených proti rizikům přicházejícím zejména z prostředí internetu. Antivirus a antispam chrání proti škodlivým kódům, tedy proti virům či spywaru, a blokuje nevyžádanou poštu; personální firewall dohlíží na veškerou komunikaci mezi počítačem a internetem. Řešení nabízí antivirovou kontrolu na vyžádání, prověřování souborů při jejich otvírání, on-line kontrolu dat stahovaných z internetu.

Součástí TrustPort PC Security jsou moduly pro spolehlivé šifrování dat, využití elektronického podpisu, nevratnou skartaci citlivých dat. Další novinku představuje rodičovský zámek, umožňující blokování internetových stránek s obsahem nevhodným pro děti. Kategorie nevhodných stránek jsou definované výrobcem a uživatel si vybírá, které kategorie si přeje blokovat. Uživatelé pracující na více počítačích uvítají možnost vytvoření mobilní verze antiviru na USB klíčence. Další novinkou je záchranný disk, který si uživatel předem vytvoří a použije k zotavení zavirovaného počítače.

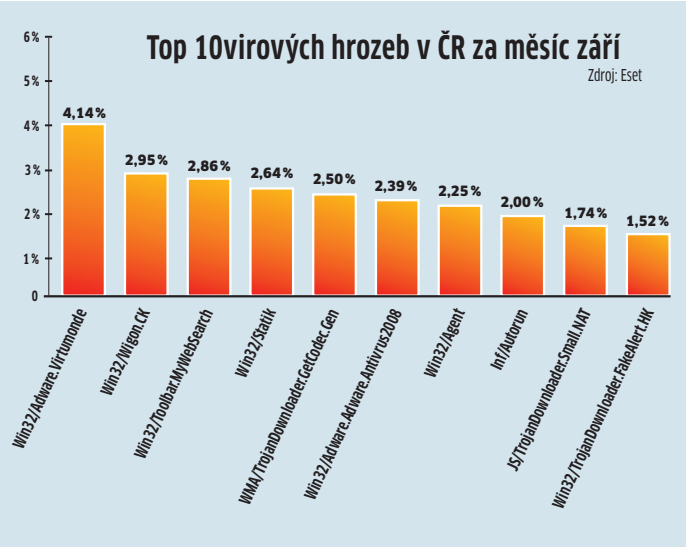
INFO: **www.trustport.cz**

STATISTIKY ESETU

Ve světě řádí zloději dat, v Česku adware

Zářijová analýza ThreatSense.Net, statistického systému společnosti ESET, odhalila, že nejvíce detekcí zaznamenal opět malware označovaný jako Win32/PSW.OnLineGames.

V Česku virová laboratoř ESET nejvíce zachytávala agresivní adware (nevyžádanou reklamu). Podle statistik se globálně i v Česku čím dál tím více šíří trojské koně využívající k napadení počítače hudební soubory.



V průběhu září 2008 bylo téměř 19,47 % všech světových detekcí virových hrozeb označeno jako Win32/PSW.OnLineGames, což je v porovnání se srpnem další znatelný nárůst. Uvedená rodina Win32/PSW.OnLineGames představuje trojské koně s typickými keylogg a rootkit funkcemi, které získávají informace a uživatelské přístupy související s on-line hrami. Získané informace pak odesílají do počítače vzdáleného útočníka, který je dále zneužívá.

Účastníci nejrůznějších on-line multiplayerových her typu World of Warcraft a Lineage či uživatelé působící ve virtuálních světech jako Second Life by měli být na pozoru. Nejde jen o neškodné útoky, ale především o phishing a jiné podvodné techniky, které následně způsobí uživateli reálnou finanční ztrátu v reálném světě. Jejich úkolem je v těchto případech krást přihlašovací údaje či cenné virtuální ikony ve zmíněných hrách. Ty pak útočníci nabízí na černém trhu či aukčních serverech typu eBay.

Druhé místo v září patřilo hrozbám INF/Autorun (3,53 %). Uvedené detekční označení se používá pro celou řadu počítačových infiltrací, které jako cestu k napadení systému zneužívají soubor Autorun.inf. Win32/Toolbar.MywebSearch je potenciálně nechtěná aplikace (PUA – Potentially Unwanted Application) neboli méně nebezpečný typ adwaru, který si uživatel nainstaluje na počítač běžně jako součást licenčních podmínek jiné aplikace. Konkrétně v tomto případě se jedná o přídavnou lištu, která do internetového prohlížeče přidá vyhledávací okno směrující veškeré vyhledávání přes stránku MyWebSearch.com. Tento adware byl v září třetí nejrozšířenější hrozbou s podílem 3,28 %. Na čtvrtém místě s progresivním tempem růstu byl v září WMA/TrojanDownloader.Wimad.N (2,58 %). Jedná se o Windows Media soubor (WMA), který přesměruje multimediální přehrávač na útočníkovu stránku, aby následně stáhl a nainstaloval škodlivé komponenty včetně adwaru. Tento downloader je na P2P výměnných sítích označován jako populární skladby ve formátu MP3, čímž se snaží oklamat uživatele ke svému stažení. První pětku globálních počítačových infiltrací za měsíc září uzavírá Win32/Pacex.Gen (1,82 %). Tato hrozba slučuje široké rozpětí škodlivých souborů, které používají specifickou krycí vrstvu. Používá se hlavně v trojských koních zaměřujících se na krádeže uživatelských údajů a hesel.

Výsledky statistik v České republice se od globálních již několik měsíců liší. V září českému žebříčku opět vládl agresivní adware Win32/Adware.Virtumonde s 4,14 %. V první pětce se umístil také WMA/TrojanDownloader.GetCodec.Gen (2,50 %, páté místo), který v napadeném počítači mírně upraví všechny hudební soubory a následně se při jejich spuštění přehrávač pokusí stáhnout další škodlivý obsah z nastavené internetové stránky. Takto upravená písnička si svou škodlivou součást nese dále s sebou. Infikovány jsou všechny hudební soubory, které trojský kůň v počítači nalezne. Není tedy možné říci, že by konkrétní druhy písniček byly více či méně nebezpečné. Je tak možné najít nakažené nejnovější hity i klasickou hudbu.

NOVINKY V ZABEZPEČENÍ

KERIO MAILSERVER 6.6

Společnost Kerio Technologies oznámila vydání produktu Kerio MailServer 6.6, který nabízí řešení správy zdrojů a nový nástroj pro migraci uživatelů a dat ze serveru Microsoft Exchange. S tímto vydáním také společnost Kerio uvádí na trh komplexní řadu nástrojů pro spolupráci.

Kerio MailServer 6.6 nyní zahrnuje plánování zdrojů, které uživatelům umožňuje prohlížet, přihlašovat, delegovat a rezervovat sdílené zdroje, jako jsou například konferenční místnosti a audiovizuální vybavení. Organizátor může v reálném čase sledovat dostupnost zdrojů a má možnost je ihned rezervovat pro plánovanou událost nebo činnost. Plánovač zdrojů poté automaticky odešle uživateli odpověď s potvrzením nebo zamítnutím rezervace. Každý zdroj může zahrnovat vlastní oprávnění konfigurované správcem IT, včetně možnosti omezit právo provádět rezervace na jednotlivé uživatele nebo možnosti stanovit „správce rezervací“ pro přidávání a odstraňování událostí přímo z kalendáře příslušného zdroje. Adresy zdrojů jsou dostupné ve složce Veřejné kontakty. Uživatelé si také mohou prohlížet nasdílené kalendáře každého zdroje v aplikacích Apple iCal, Microsoft Entourage, Kerio WebMail a Microsoft Outlook.

Podniky využívající Kerio disponují snadným přístupem k veškerým groupwarovým datům prostřednictvím smartphonů Apple iPhone, Windows Mobile, Palm, Symbian a Blackberry. Tato nová verze umožňuje uživatelům zobrazovat přílohy a HTML e-maily na přístrojích iPhone a Windows Mobile s využitím nejnovější aplikace Exchange ActiveSync 12. Nový nástroj Kerio Exchange Migration Tool nabízí rychlý a transparentní způsob migrace dat z Exchange na Kerio MailServer. Kerio MailServer 6.6 je určen pro celou řadu platforem – od Windows XP a 2003 přes Windows Vista a Mac OS X Tiger až po SUSE Linux.

INFO: www.kerio.cz

MICROSOFT BITLOCKER

Otevřená ochrana

Hesla softwaru pro šifrování pevných disků jako BitLocker se dají získat velmi snadno. Programy, které šifrují celý pevný disk, byly až dosud považovány za bezpečné. Nyní však pracovníci bezpečnostní firmy iViZ Techno Solutions zjistili, že si tyto nástroje ukládají heslo vždy na stejnou paměťovou adresu 0x40:0x1e – aniž by heslo později vymazaly.

Trojský kůň s oprávněním správce pak může v počítači bez problémů heslo načíst a odeslat jej útočníkovi. Výrobci šifrovacích programů o problému vědí a v řadě případů už zveřejnili aktualizaci. Microsoft aktualizoval BitLocker v SP1 pro Vistu. Nástroj pak po bootování vymaže heslo z paměti – hackeři jej tedy nemohou zjistit.

INFO: www.microsoft.cz

VÝZKUM RSA

Nebezpečné Wi-Fi sítě

Sedmý výroční průzkum zaměřující se na zabezpečení bezdrátových sítí společnosti RSA ukazuje, že ačkoli se ve velkých městech situace zlepšuje každým dnem, více než polovina obyvatelstva stále hazarduje se slabým zabezpečením bezdrátových sítí WEP, které při míře sofistikovanosti dnešních zločinců poskytuje jen velmi malou ochranu. Dostatečná ochrana sítí přitom nebyla nikdy tak nezbytná jako dnes, kdy je v každém větším městě možné zachytit Wi-Fi signál na každém rohu. Díky společnostem i jednotlivcům nepoužívajícím technologie poskytující vyšší stupeň zabezpečení, včetně WPA a WPA2, se doposud američtí hackeři údajně obohatili o více než 40 milionů čísel kreditních karet. Více informací naleznete ve zprávě společnosti RSA, která je k dispozici na adrese **www.rsa.com/press_release.aspx?id=9725**.

INFO: zpravy.actinet.cz

HROZBA

Nebezpečné klávesnice

Tým ze Security and Cryptography Laboratory (LASEC), sídlící ve švýcarském Lausanne, našel čtyři různé způsoby, jak získat kompletní nebo částečná data přenášená z klávesnice do počítače, a to na vzdálenost až 20 metrů, dokonce i skrz zdi. Testováno bylo jedenáct různých „drátových“ klávesnic zakoupených v letech 2001 až 2008, připojených přes USB a PS2. Všechny jsou zranitelné alespoň jedním ze čtyř útoků. Útoky jsou založeny na odposlouchávání elektromagnetického záření. Více informací včetně dvou videí naleznete na webu **http://lasecwww.epfl.ch/keyboard/**.