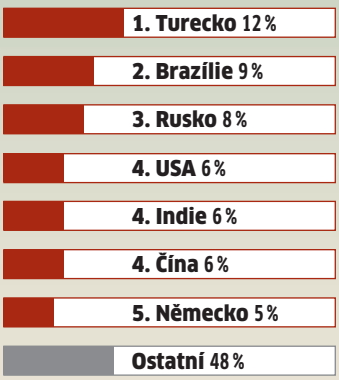
## DATA A FAKTA

### Barometr nebezpečí


Předvánoční období je ideální čas pro phishingové maily, lákající na domněle výhodné nabídky.

### Přední země zombie

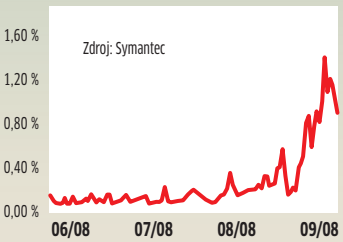



Zdroj: Symantec

V Turecku kontrolují hackeři bezmála každý devátý počítač.

### Viry v e-mailech

**Podíl v procentech**




**Nárůst:** Od června se podíl malwaru zvýšil o 12 %.

### Číslo měsíce

**7 000**

falešných antivirových programů koluje na webu. Tito domnělí pomocníci sami šíří viry.

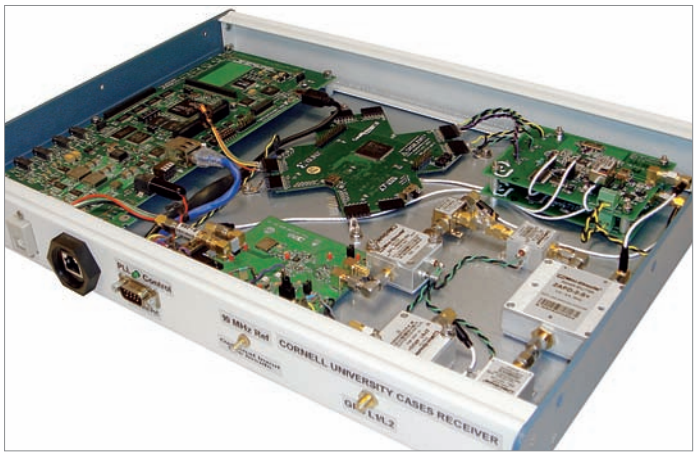
# Hackeři matou navigace

**RUŠIČKA GPS** se vejde do každého kancelářského kufříku a vsugeruje navigačním přístrojům libovolné zeměpisné souřadnice. Chránit se proti tomu není snadné.

FABIAN VON KEUDELL

Až vás v noci váš navigační přístroj náhle navede do nejbližší řeky, mohl by v tom mít prsty Paul Kinter. Kinter je profesorem na Cornellově univerzitě v USA a objevil možnost, jak zfalšovat signály GPS. Vědec chtěl původně sestrojit speciální přijímač, který měl zkoumat vliv slunečních erupcí na satelity systému GPS. Výsledkem však bylo něco jiného – hackerská GPS vysílačka. Manipulace s ní je až úděsně jednoduchá: GPS vysílačka funguje v prvním kroku jen jako jakýsi zesilovač přicházejících signálů. Dále se vysílačka musí nacházet v blízkosti oběti – podle síly signálu kolem 50 metrů. Poněvadž navigační přístroje vždy zpracovávají nejsilnější signál, hackerská vysílačka se pro ně po několika vteřinách stane hlavní frekvencí – a útočník tak má možnost zmanipulovat GPS údaje o poloze napadeného přístroje. Prozatím má vysílačka přibližně velikost běžného kancelářského kufříku, nicméně vědci nevylučují, že by brzy mohla být miniaturizována – na velikost krabičky cigaret.

Naštěstí není snadné takto napadnout navigační přístroje v autech: pohybují se příliš rychle, a vysílačka by proto musela být instalována přímo na voze. Kriminální živly by však mohly přístroj využívat k úplně jiným účelům, například ke zmanipulování „elektronických nožních pout“. To je zařízení, jímž orgány činné v trestním řízení v USA sledují u pachatelů odsouzených k domácímu vězení dodržování stanovených podmínek. Tyto osoby by se pak mohly volně pohybovat i mimo jim vymezenou oblast – stačí k tomu, aby hackerská vysílačka změnila GPS data pro elektronické pouto.




**Příruční rušička GPS:** Tento přístroj umí děsivě snadno zmanipulovat poziční údaje navigačního systému.

### Drahá obrana: Pomohou multiantény a šifrování

Kdo se teď začal obávat, že by se takovou vysílačkou daly zmanipulovat také pomocí GPS řízené zbraně, například rakety, naštěstí se mýlí. Armáda totiž používá speciální verzi sítě GPS, v níž satelity vysílají do navigačních přístrojů svá data v zašifrované podobě. Ačkoliv vojenská varianta už dlouho vykazuje dobré bezpečnostní funkce, civilní GPS signály šíří satelity ještě pořád v otevřené řeči. Pomohlo by tedy šifrování civilního signálu. Nestačí k tomu však jednoduchá aktualizace softwaru navigačních přístrojů. V mnoha případech musí být v přístroji zabudován speciální šifrovací čip.

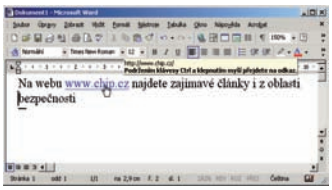
Alternativním řešením by mohla být varianta přístroje se zdvojenou anténou. Pak by elektronika měřením časového průběhu signálů dokázala zjistit, z kterého směru signál přichází, a hackera tak odhalit. Nejslibnější pomoc však podle všech předpokladů přijde z Evropy: navigační systém Evropské unie Galileo, který má být schopen nasazení v roce 2013 a šifrování má v základní výbavě.

**INFO: www.cornell.edu**

**MICROSOFT OFFICE**

# Nepřítel naslouchá

Pomocí zmanipulované CDO URL (Collaboration Data Objects) mohou útočníci načíst uživatelské informace z lokálního PC a spouštět libovolné skripty. Jakmile uživatel Office klikne na CDO URL, například aby otevřel webovou stránku nebo mailovou adresu, pošlou se v Office uložená osobní data hackerovi. Jakkoli je toto nedobrovolné předávání informací podlé, Microsoft to za nijak kritickou záležitost nepovažuje – mezera je hodnocena jako mírně nebezpečná. Postiženy jsou nejen verze Office pro Windows, ale i jejich varianty pro Mac. Po intervenci Chipu slíbil Microsoft rychlou aktualizaci, která krátce poté vyšla u příležitosti „patch day“. Objevilo se v ní jedenáct dalších bezpečnostních záplat, z nichž čtyři hodnotí výrobce jako kritické.




**INFO: www.microsoft.com**

## INFO

# Nová bezpečnostní rizika

### THUNDERBIRD

Pomocí upravené URL uvnitř zprávy mohou útočníci vyvolat v e-mailovém programu Thunderbird přetečení bufferu. Lze tak do počítače propašovat škodlivý kód. Řešením je upgrade na aktuální verzi 2.0.0.17.

**INFO:** www.mozilla-europe.org

### VIDEOLAN CLIENT

Prostřednictvím zmanipulovaných playlistů pro XSPF dokážou hackeři využít mezeru v přehrávacím modulu Media Playeru a vyvolat přetečení bufferu. Týká se to i vás? Pak si z webové stránky výrobce stáhněte aktuální verzi VLC 0.9.4.

**INFO:** www.videolan.org

### APPLE SAFARI

Ve webovém prohlížeči Safari společnosti Apple bylo nalezeno několik zranitelností. Tyto chyby mohou být mimo jiné zneužity ke kompromitování systému a mohou zapříčinit únik citlivých informací. Podrobný výpis chyb a další informace naleznete na webu Applu (**http://support.apple.com/kb/HT3298**). Uživatelé systému Apple Mac OS X si mohou update stáhnout přes utilitu Software update, ostatní jej naleznou na webu společnosti jako Safari 3.2.

**INFO:** zpravy.actinet.cz

### NERO SHOWTIME

Byla nalezena zranitelnost v Nero ShowTime, způsobující přetečení bufferu kvůli chybě při zpracování M3U souborů. Útočník tak může kompromitovat systém. Chyba byla oznámena ve verzi 5.0.15.0, ostatní verze nejsou potvrzeny. Více informací naleznete na serveru Secunia (**http://secunia.com/advisories/32850/**).

**INFO:** zpravy.actinet.cz

### SAFARI V IPHONE

Na serveru iPhonemania (**http://iphonemania.mobilmania.cz**) najdete informaci o zákeřné chybě v Safari na iPhone. Prohlížení webové stránky může způsobit vytočení telefonního čísla bez potvrzení uživatele. Chybu by měla opravovat aktualizace firmwaru vydaná na konci listopadu.

**INFO:** zpravy.actinet.cz

### ADOBE ACROBAT/READER

Ve starší verzi populárního softwaru pro prohlížení dokumentů ve formátu PDF byla objevena zranitelnost. Ta je způsobena chybou při zpracování řetězců v Javascript funkci util.printf(), může být zneužita k „stack-based buffer overflow“ útokům pomocí upraveného PDF souboru. Úspěšné zneužití umožňuje spuštění libovolného kódu. Zranitelnost je potvrzena u verze 8.1.2, další verze mohou být také zasaženy. Více informací naleznete opět na serveru Secunia (**http://secunia.com/secunia_research/2008-14/**).

**INFO:** zpravy.actinet.cz

### BLACKBERRY DESKTOP SOFTWARE

Byla nalezena zranitelnost v Microsoft ActiveX ovladači FlexNET Connect, který se používá k získávání a instalování záplat aplikací a který je zahrnut v BlackBerry Desktop Software. V ovladači se vyskytuje chyba způsobující přetečení zásobníku a může být spuštěna například při návštěvě stránky, která tento ovladač vyvolá. Chyba je opravena ve verzích 4.5–4.7, které si můžete stáhnout na stránkách výrobce (**www.blackberry.com**).

**INFO:** zpravy.actinet.cz

PRŮZKUM SPOLEČNOSTI SYMANTEC

# Zpráva o ekonomice šedé zóny

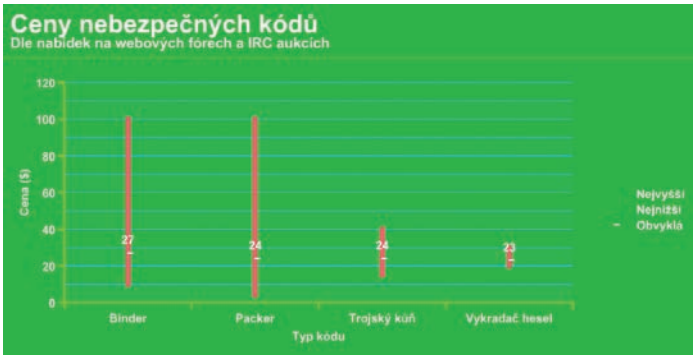
Společnost Symantec Corp. uvolnila svůj report věnovaný stínové ekonomice. Zpráva podrobně líčí stínovou ekonomiku na internetu, která již dospěla do stadia efektivního světového trhu, na němž je pravidelný zájem o nákup a prodej kradeného zboží a podvodných služeb. Cena nabízeného zboží jednotlivými obchodníky se počítá na miliony dolarů. Zpráva vychází z dat shromážděných organizací Symantec Security Technology and Response (STAR) v období mezi 1. červencem 2007 a 30. červnem 2008. Během sledovaného období pozoroval Symantec 69 130 různých aktivních prodejců a celkem 44 321 095 zpráv poslaných na fóra, kde se s těmito údaji obchoduje. Potenciální hodnota celkového množství nabízeného zboží deseti nejaktivnějších prodejců byla 16,3 milionu dolarů za kreditní karty a 2 miliony dolarů za bankovní účty. Nejaktivnější prodejce, kterého v daném období Symantec identifikoval, nabízel zboží s potenciální hodnotou 6,4 milionu dolarů.

## Zdroje a miliardy

Experti společnosti Symantec ve zmiňovaném období sledovali důležité servery a monitorovali IRC kanály a dospěli k následujícím zajímavým údajům: Potenciální hodnota nabízeného zboží byla ve stanoveném období větší než 276 milionů dolarů. Tato hodnota vychází z cen nabízeného zboží a služeb a porovnání, kolik by prodejce vydělal při prodeji kompletní nabídky. Nejčastěji nabízeným druhem zboží a služeb jsou informace o kreditní kartě, které představují 31% podíl celkového obchodu. Zatímco čísla ukradených kreditních karet se prodávají za relativně malé sumy (od 0,10 do 25 dolarů za kartu), limit pro čerpání z ukradené kreditní karty se v průměru vyšplhal až nad čtyřtisícovou mez. Symantec vypočítal, že potenciální hodnota všech kreditních karet nabízených v průběhu sledovaného období činila 5,3 miliardy dolarů. Popularita informací o kreditních kartách vyplývá z existence mnoha způsobů, jak získané informace využít pro podvody. Kreditní karty jsou snadno použitelné pro on-line nakupování, a proto je často obtížné pro obchodníka nebo poskytovatele úvěru rozpoznat a určit podvodné transakce předtím, než podvodníci kompletně dokončí transakci a obdrží své zboží. Kromě toho jsou informace o kreditních kartách často prodávány podvodníkům ve velkém, se slevami nebo volnými čísly poskytnutými s většími nákupy.


## Jak bezpečný je váš účet?

Druhou nejběžněji nabízenou kategorií zboží a služeb byly finanční účty, které tvořily 20 % z celku. Zatímco informace o ukradeném bankovním účtu se prodává za částky pohybující se mezi 10 a 1 000 dolary, průměrně nabízený zůstatek ukradeného účtu je téměř 40 000 dolarů. Spočteme-li průměrně nabízený zůstatek bankovního účtu s průměrnou cenou za ukradená čísla bankovních účtů, celková cena bankovních účtů nabízených během sledovaného období byla 1,7 miliardy dolarů. Informace o finančních účtech jsou populární díky potenciálně vysokým výplatám z těchto účtů a také díky rychlosti, se kterou se tyto výběry mohou uskutečnit. V jednom případě byl dokonce účet on-line převeden na nevypátratelné místo v méně než 15 minutách.




## Kde se skrývají?

Stínová ekonomika je závislá na zeměpisné poloze a generuje příjmy pro kyberzločince, kteří působí jako jednotlivci i jako dobře organizované a propracované skupiny. Během zkoumaného období bylo nejvíce takových serverů překvapivě zjištěno v Severní Americe – 45 % z celkového počtu; v regionu Evropa/Střední východ/Afrika bylo zjištěno 38 % serverů; následoval region Asie/Pacifik s 12 % a Latinská Amerika s 5 %. Zeměpisná poloha serverů stínové ekonomiky se neustále mění, čímž se ztěžuje jejich případné odhalení.

„Report o stínové ekonomice dokazuje, že dnešní kyberzločinci využívají informace, které shromažďují bez povolení zákazníků a obchodníků," řekl Stehen Trilling, viceprezident Symantec Security Technology and Response. „Vzhledem k tomu, že jednotlivci i skupiny pokračují ve vývoji nových nástrojů a technik k oklamání legitimních uživatelů po celém světě, musí se stát ochrana a snižování rizik proti útokům mezinárodní prioritou."

Kompletní zprávu o více než sto stranách najdete na webu společnosti Symantec, přesný odkaz přímo na zprávu také na našem webu.

**Komentář redakce:** *Internetové hrozby budou již v blízké budoucnosti patřit k největším světovým problémům. Určitým náznakem je již dnes fakt, že téměř polovina zločineckých serverů se nachází v Severní Americe, kde jsou zákony na potírání internetové kriminality velmi silné. O situaci u nás a na „divokém východě" svědčí cirkus okolo skupiny rBn (Russian Business network – nabízí hostingové služby), která je již několik let „podezřelá" z podpory phishingu, hackingu a podobných aktivit. A vzhledem k tomu, že ceny hackerských nástrojů jsou více než příznivé, čekají nás velmi „zajímavé" časy…*

**Příznivé ceny:** Ze necelých třicet dolarů seženete libovolný nástroj, prostřednictvím něhož můžete téměř anonymně krást a škodit. Klasičtí zločinci „se zbraní v ruce" mohou jen závidět….

GOOGLE CHROME

# Browser škodí PC

Nové internetové prohlížeče to mají na silně konkurenčním trhu těžké – zvláště když nejsou právě bezpečné. Google Chrome ještě nebyl na trhu ani dva celé dny, a už v něm hackeři našli první bezpečnostní mezery. Od té doby si výrobce Google hraje s útočníky na kočku a myš. Pár hodin po uveřejnění záplaty, která má mezery uzavřít, darebáci zpravidla odhalí nové vstupní brány. Teprve nedávno hackeři objevili mezeru typu DoS (Denial of Service), která jim umožňuje vyvolat nejen havárii browseru, ale také „vyvést z míry" celý počítač s Windows. Děje se tak funkcí javaskriptu windows.open, přes který Chrome otevírá četná nová okna, což má za následek vysoké zatížení paměti systému. Využitím slabiny v Chrome nyní útočníci také mohou zavírat různá okna browseru. Výrobce intenzivně pracuje na záplatě, v době uzávěrky ještě nebyla k dispozici.

**INFO: www.google.cz**

## INFO

## Nová bezpečnostní rizika

### MOZILLA FIREFOX

Krátce po updatu na verzi 3.0.2 se ve Firefoxu objevila nová mezera. Tentokrát je postižen správce hesel, který po aktualizaci nefunguje správně. Mozilla ale rychle zareagovala a nabízí opravenou verzi 3.0.3.

**INFO: www.mozilla-europe.org**

### MICROSOFT SECURITY BULLETINS

Microsoft vydal své pravidelné záplaty, které jsou opět hodny vaší pozornosti. Mimo jiné totiž obsahují i opravu jedné kritické chyby v Internet Exploreru a jedné důležité v protokolu Microsoft Server Message Block. Obě dovolují spuštění libovolného kódu. Více informací naleznete na webu Microsoft Technet.

**INFO: zpravy.actinet.cz**

### TRILLIAN

V instant messengeru Trillian bylo nalezeno několik zranitelností. V první řadě se jedná o chybu při generování XML tagů pro obrázky. Zde totiž hrozí zneužití a způsobení přetečení vyrovnávací paměti zasláním obrázku s příliš dlouhým názvem. Druhá chyba je ve zpracování kódu XML a může být zneužita k poškození interní datové struktury. Ve třetím případě se jedná o chybu v ohraničení při zpracování speciálních XML tagů, která může mít za následek přetečení haldy. Zneužití jakékoliv z těchto zranitelností může dovolovat spuštění libovolného kódu. Více naleznete na serveru Secunia (**http://secunia.com/advisories/33001/**). Novou verzi, opravující problémy, najdete na **www.ceruleanstudios.com/downloads/**.

**INFO: zpravy.actinet.cz**

### ZÁPLATY MICROSOFTU NA PROSINEC

Mimořádnou pozornost byste měli věnovat bezpečnostnímu updatu Microsoftu na měsíc prosinec. Obsahuje totiž důležité záplaty například pro Internet Explorer, Microsoft Office, Visual Basic, či Windows Search...

**INFO: www.microsoft.cz**


ADOBE FLASH

# Chyba v paměti

Využitím chyby v Adobe Flash Playeru mohou hackeři zmanipulovat oblast schránky v operační paměti. Ve Flashi obsažený ActionScript byl už častěji cílem hackerských útoků. U nyní zjištěné mezery stačí prohlížet si reklamní banner, který se objevuje na nějaké webové stránce. Až dosud jsou postiženy reklamní projevy časopisu Newsweek a televizní stanice NBC. Díky mezeře zapíší útočníci do paměti takovou URL, která odkazuje na domnělý on-line antivirový skener. Jestliže pak uživatelé vloží do webového prohlížeče metodou Kopírovat/Vložit nějaký odkaz, ve skutečnosti se projeví odkaz hackerů.

Adobe už o problému ví, zatím však pro Flash 9 žádnou záplatu neposkytuje. V nové verzi 10 už je chyba odstraněna.

**INFO: www.adobe.com**

VÝZKUM IBM

# Do banky z USB klíče

Prototyp USB zařízení v podobě paměťového klíče s integrovaným displejem z výzkumné laboratoře IBM v Curychu přináší novou úroveň zabezpečení pro uživatele on-line bankingu. Pilotní zařízení jsou už připravena na testování bankami. Zařízení Zone Trusted Information Channel (ZTIC) se připojí do USB portu jakéhokoli počítače a vytvoří přímý, bezpečný kanál k on-line transakčnímu serveru banky. Obchází přitom počítač, který může být napaden škodlivým softwarem (malwarem) nebo vystaven útokům hackerů.

Zákazník se může pomocí zabezpečeného USB klíče přihlásit a ověřovat všechny transakce na jeho displeji. USB zařízení je přitom bezpečně připojeno k serveru, takže je zákazník spolehlivě chráněn i před nebezpečnými formami útoků, které manipulují daty na pozadí bez vědomí uživatele i banky. Nové USB zařízení přidává další úroveň ochrany ke stávajícím řešením ověřování prostřednictvím čipové karty, kódu PIN nebo jednorázového ověřovacího kódu. Odvrací tak i nejnovější bezpečnostní hrozby založené na manipulacích s daty.

Hackeři jsou ve svých pokusech o napadení finančních transakcí na internetu čím dál tím náročnější. Stále častěji se objevují útoky typu „man-in-the-middle," kdy hacker nepozorovaně zachycuje a pozměňuje zprávy předávané mezi uživatelem a finanční institucí. Pozměněné zprávy vypadají jako oprávněné transakce finanční instituce a zprávy doručované bance vypadají jako zprávy od zákazníka.


**Bezpečněji:** Přístup do k bankovnímu účtu lze zabezpečit i pomocí USB klíče.

Téměř 90 procent on-line útoků zneužívajících identity míří na sektor finančních služeb. Mezinárodní studie instituce MELANI (Švýcarské zpravodajské a analytické centrum pro zajištění informací) z roku 2007 zjistila, že vzrostl počet úspěšných případů napadení malwarem a že v současnosti zavedené dvoufaktorové systémy ověřování (například ověřování pomocí transakčních čísel, kódů SecurID atd.) neposkytují dostatečnou ochranu před takovými útoky. V okamžiku, kdy je počítač zákazníka napaden malwarem, totiž nemohou být považovány za dostatečně zabezpečené.

Toto řešení efektivně přesouvá všechny kryptografické procesy a důležité procesy uživatelského rozhraní z počítače na zařízení ZTIC, čímž vzniká důvěryhodný koncový bod komunikace mezi bankovním serverem a uživatelem. Pomocí nového zařízení pak uživatel může bezpečně komunikovat s citlivými on-line službami, jako je bankovní server. V kombinaci s čipovou kartou, kterou lze do zařízení vložit, přináší nové řešení vyšší úroveň komplexního zabezpečení on-line bankingu.

To, co uživatel vidí na displeji zařízení ZTIC, je shodné s tím, co „vidí" server bez ohledu na nebezpečné útoky, k nimž může dojít v PC nebo při přenosu po internetu.

## Technologické specifikace

Vědci navrhli ZTIC jako USB zařízení o velikosti paměťového klíče. Pracuje s běžně používaným protokolem TLS/SSL. Hardware ZTIC se koncepčně skládá z procesorové jednotky, operační a permanentní paměti, malého displeje, alespoň dvou kontrolních tlačítek (OK a Storno) a volitelně i ze čtečky čipových karet. Ukázku použití v praxi najdete například na serveru YouTube (**www.youtube.com/watch?v=mPZrke-HMDJ8&fmt=18**).

VÝSLEDKY VÝZKUMU

# Největší hrozbou jsou vlastní zaměstnanci

Společnost GiTy provedla prostřednictvím agentury Ogilvy Public Relations vlastní výzkum. V rámci výzkumu byl osloven management více než 150 významných společností působících v České republice, a to s otázkami týkajícími se bezpečnosti v oblasti informačních technologií. Z výsledků výzkumu mimo jiné vyplývá, že největší hrozbou z pohledu firemní bezpečnosti IT jsou v 78 % vlastní zaměstnanci.

Získané výsledky korespondují v mnoha ohledech s podobnými zahraničními průzkumy a ukazují, že firmy berou riziko ohrožení svých IT stále vážněji. Více než polovina (57,5 %) z nich považuje 100% bezpečnost za maximálně důležitou s ohledem na primární byznys. Přesto 20 % dotázaných potvrdilo, že se této oblasti u nich ve firmě nevěnuje dostatečná pozornost. Prostor pro zlepšení zabezpečení vlastních IT vidí 80 % dotázaných.

Marek Chlup, IT Expert GiTy: „Z vlastní zkušenosti víme, že naši technici řeší zhruba 10krát do měsíce výjezd do terénu za účelem záchrany dat z pracovních stanic a serverů. Hodnota dat je pro každou společnost velmi důležitá, bohužel si to většinou uvědomí až v případě nastalých problémů. Základem pro kvalitní zabezpečení IS/IT je zavedení uceleného systému informační bezpečnosti, který je pravidelně aktualizován."

## Někteří stále ještě pravidelně neaktualizují bezpečnostní politiku

Základem kvalitního zabezpečení IS/IT je kvalitní interní bezpečnostní politika. Vzhledem k vývoji počítačové kriminality je nutné ji také pravidelně aktualizovat. Zde si české firmy vedou velmi dobře a průměrně 2,5krát do roka ji aktualizuje na 73 % dotázaných. Pouze 3 % aktualizují až na základě reakce na novou nebo očekávanou hrozbu. Primárně je bezpečnost firem zaměřena na bezpečnost síťovou, a to téměř v polovině případů (48 %), komplexní bezpečnostní politiku zastává jen 20 % dotázaných.

## Každá pátá firma již byla nějakým způsobem ohrožena

Z výsledků průzkumů vyplývá, že u 23 % firem byla v poslední době ohrožena bezpečnost jejich IS/IT. Jako hlavní důvod jsou uváděny počítačové viry. 18 % dotázaných se do problémů dostalo kvůli selhání výpočetní techniky. Finanční ztráty se v těchto případech pohybují v desítkách tisíc za rok. Výzkum, který pro společnost GiTy provedla agentura Ogilvy PR, proběhl mezi nejvýznamnějšími firmami, které působí na českém trhu (například United Bakeries, Penam, Telefónica O2, Siemens, Finep, Česká spořitelna, ČSOB, Komerční banka, Czechinvest, České radiokomunikace, Shell, DB Schenker a další). Osloveno bylo více než 150 firem, a to primárně na úrovni managementu. Cílem výzkumu bylo zjistit, jak firmy pohlížejí na možná bezpečnostní rizika spojená s jejich infrastrukturou IT.

## Komentář redakce:

Pro většinu firem je investice do bezpečnosti rovna nákupu drahého softwaru a hardwaru. Jen málo z nich věnuje z hlediska bezpečnosti pozornost tomu nejdůležitějšímu – vlastním zaměstnancům. Předpokládá se, že zatímco v oficiálních statistikách hrají stále velkou pozornost viry a útoky „hackerů", ve skutečnosti mohou být největším problémem právě vlastní zaměstnanci. Odborníci odhadují, že naprostou většinu bezpečnostních „průšvihů" se firmám podaří utajit a z obavy o vlastní prestiž se zmiňované informace nikdy na veřejnosti neobjeví.

HROZBA BUDOUCNOSTI

# Robotický hmyz a inteligentní bakterie

Nová zpráva společnosti Canon Europe varuje před robotickým hmyzem, umělou inteligencí a chytrými bakteriemi. Tyto prostředky budoucnosti se mohou stát nástroji špionáže zaměřené na získání citlivých informací.

Vedoucí týmu, futurolog Ian Pearson, předpověděl, jak bude vypadat kancelář budoucnosti a jaké hrozby budou ohrožovat její existenci. Předpokládá se, že pro vojenské účely vznikne malý robotický hmyz, který bude zneužíván na špehování v kanceláři a k přenosu nebezpečného softwaru nebo hardwaru ke klíčovým zařízením. K výrobě sofistikovaných virů může být použita i umělá inteligence. Předpověď také říká, že by mohla být vyvinuta nebezpečná bakterie zaměřená na sběr důležitých informací v rámci kanceláře.

Radka Palánová, CBS & Corporate Marketing and Communication Manager Canon CZ, říká: „Může to znít jako scénář k nějakému hollywoodskému trháku, ale inteligentní bakterie, umělá inteligence a robotický hmyz představují skutečnou hrozbu bezpečného obchodování v budoucnu."

Trend využívání čím dál tím menších a kapacitně výkonnějších externích pamětí představuje hrozbu pro kanceláře budoucnosti. Používáním malých externích paměťových jednotek, jako je USB nebo přenosný multimediální přehrávač, mají zaměstnanci možnost vynést z kanceláře velké množství citlivých informací. Aby se podobným případům zabránilo, bude vyvinuta nová technologie umělé inteligence, která bude podobná bezpečnostnímu systému na letištích a která zabrání podezřelému chování zaměstnanců. Přes tyto trendy varuje Ian Pearson před implementací podobných bezpečnostních systémů. „Bezpečnost by se nikdy neměla stát bariérou pro práci," říká. „Přílišná ochrana a bezpečnost v korporacích jsou samy o sobě hrozbami. Příliš striktní pravidla omezují výkon a produktivitu zaměstnanců. Ochrana by měla být vybalancovaná, aby chránila před hrozbami a zároveň dávala zaměstnancům pocit, že práci vykonávají svobodně."

Jako odpověď na tyto hrozby budoucnosti se zdokonalují systémy sloužící k autentifikaci uživatelů. Jednou z oblastí bezpečnosti je navržení tiskových elektronických okruhů, které mohou tisknout přímo na pokožku a které v kombinaci s ochranou pomocí otisků prstů vytvoří jedinečný systém identifikace uživatele. Jinou možností ochrany je používání speciálního neviditelného inkoustu k zabezpečení maximální ochrany dokumentů před kopírováním.


## Vize budoucnosti

Podle odhadů bude kancelář budoucnosti méně využívat osamocenou práci za pracovním stolem, mnohem víc prostoru bude věnováno práci ve skupinách a meetingům. Monitory počítačů budou nahrazeny videoclonou nebo aktivní čočkou, 3D tiskárny a monitory budou schopny během chvilky generovat 3D modely. Administrativa se díky pokroku v inteligenci strojů více zautomatizuje a práce už nebude tolik vázána na pracovní stůl. Výsledkem bude práce mimo centrální kancelář, ve speciálních pracovních centrech, která budou disponovat komplexnějším vybavením, jako jsou například velká multifunkční tiskařská centra, která zabezpečí bezpečné a efektivní sdílení informací. V situaci, kdy budou vedle sebe pracovat lidé z různých divizí a podniků, vzroste otázka bezpečnosti ještě víc. Pracovní skupiny budou naproti tomu tvořit lidé, kteří se v skutečnosti nikdy nepotkají.

Radka Palánová uzavírá: „Kancelář budoucnosti bude založena na bezpečné komunikaci pomocí kancelářských zařízení a technologií. Inovace v inteligentní tiskařské technologii a řízení dokumentů zabezpečí bezpečnost napříč různými úrovněmi: od bezpečnosti dokumentu a uživatele po bezpečnost celé firemní sítě a úschovy dat."

RÁDIA PŘES INTERNET

## Play.cz s novými funkcemi

S nárůstem domácností připojených k internetu pomocí vysokorychlostních linek vyměnili mnozí uživatelé své klasické rádiové FM přijímače za webové prohlížeče. Ty jim umožňují nalézt a následně přehrávat rozmanitou škálu stanic podle mnoha preferencí, jako jsou například hudební žánry či územní rozmístění. S nabídkou stanic se pak pochopitelně objevuje otázka jejich co možná nejsnazšího vyhledávání a třídění. Nepostradatelnou pomůckou se v takovém případě stává server Play.cz (**www.play.cz**), který před pár týdny prošel proměnou svých webových stránek a který tak nyní přichází s mnohem interaktivnějším zážitkem ze světa multimédií. Do nového obsahu byly například integrovány inteligentní systémy dohledávání multimediálního obsahu podle kritéria aktuálně hrané skladby.

V přehrávači se tak uživatelům zobrazují související videa ze serveru YouTube a nabídka mp3 ke stažení.


PŘEHRÁVÁNÍ VIDEA

## Videa na YouTube ve formátu 16:9

Jedna z nejpopulárnějších stránek na internetu, server YouTube, změnila formát videí. Zatímco doposud se videa zobrazovala v klasickém formátu 4:3, v současnosti jsou dostupné v širokoúhlém formátu 16:9 při rozměrech 640 × 360 bodů.

Původně nahraný soubor s poměrem stran 4:3 se tedy divákům zobrazí s černými pruhy po obou stranách. Kromě této novinky přináší YouTube i přehrávání 720p (HDTV) videí, které jsou díky novému širokoúhlému formátu větší a tedy i atraktivnější pro diváka.

**INFO:** **www.youtube.com**

MIVVY DUAL TV

## Mobil s televizí


Na trh přichází nový GSM mobilní telefon mivvy dual TV. Kromě podpory dvou SIM karet najednou nechybí schopnost přijímat analogový televizní signál, podpora Bluetooth s profilem A2DP pro bezdrátová stereo sluchátka, nebo program pro synchronizaci kontaktů MivvySync.

Displej 2,6“ (320 × 240 bodů) je dotykový. Mobil je vybaven gyroskopickým senzorem, takže pozná, když ho v ruce otočíte. Displej se automaticky přizpůsobí, takže třeba právě při sledování televize se sám přepne na šířku. Multimediální výbava pokračuje rádiem, MP3 a MP4 přehrávačem, VGA fotoaparátem s možností záznamu videa ve formátu MPEG-4 a končí třeba MMS zprávami nebo prohlížečem WAP. Mivvy dual TV se prodává za 3 697 Kč včetně DPH.

**Komentář redakce:** *Dobře vybavený telefon za velmi zajímavou cenu. Problematické je použití analogové televize, která je u konce životního cyklu. Sice zde ještě nějakou dobu bude, ale neposkytuje takovou kvalitu, jako DVB-T. Pro řadu uživatelů by mohlo být lákadlem použití 2 SIM karet. Podobný mobil nabízí i Evolve, jeho kvalita a provedení jsou ovšem otřesné.*

SONY XEL-1

## Sony uvádí na trh OLED TV

V podobě nového „televizoru budoucnosti“ nazvaného XEL-1 převádí firma Sony technologii OLED z oblasti displejů mobilních telefonů do oblasti televizorů. Ve srovnání s LCD konkurencí vyzařuje organická dioda světlo s až o 25 procent větším barevným prostorem a také – což je podmíněno velmi tmavou hodnotou černé – s přehnaně vysokými kontrasty; výrobce udává více než milion ku jedné. Protože však OLED pixely v případě černé snadno nastavují vyzařování, je tento vysoký kontrast málo vypovídající. Praktičtější hodnotou je šachovnicový kontrast, poměr činí 982:1. To je téměř desetkrát více, než umožňují LCD obrazovky. Největší dojem dělá přímé srovnání: na LCD obrazovce lze vidět „plavající“ bílý čtverec v šedé ploše, u OLED technologie je naproti tomu vidět pouze bílý čtverec, zatímco černá barva zmizí v temnotě. Stejně tak potěšitelné je i zobrazení barev, které svou brilancí dokonce zastíní plazmové obrazovky. Trochu zklamáni jsme ale byli energetickou efektivitou obrazovky. OLED technika je všeobecně považována za úspornou, protože energie je potřeba pouze tehdy, když pixely produkují světlo. Přesto jsme změřili v průměru potřebu energie od 28 wattů. Pro srovnání: 22palcový TFT monitor potřebuje kolem 40 wattů.

Televizor XEL-1 stojí zatím v přepočtu zhruba 45 000 Kč, což je na 11palcový (27 cm) displej opravdu hodně, na druhou stranu stojí výrazně méně než první LCD a plazmové panely. Díky jednoduššímu výrobnímu procesu lze čekat, že se OLED televizory stanou v příštích letech atraktivní i cenově.

**INFO:** **www.sony.cz**

**Supertenký:** Nový OLED displej od Sony je silný pouze tři milimetry.

OVLÁDÁNÍ MOBILŮ

## Nový MOBILedit!

Program MOBILedit! umožňuje ovládat mobilní telefony prostřednictvím kabelu, infračerveného portu nebo Bluetooth. Můžete snadno kopírovat fotografie z telefonu, nahrávat loga, vyzvánění, MP3 i přenášet dokumenty. Dále můžete vytáčet čísla, přijímat a posílat SMS, organizovat kontakty, zálohovat, hlasovat, hrát hry a mnoho dalšího.

Nová verze 3.0 přináší celou řadu nových funkcí. Samozřejmě je rozšířena podpora nejnovějších mobilních telefonů, ale především byla přidána podpora mobilních telefonů s operačním systémem Windows Mobile a iPhonu první generace. Navíc je jedno, jaká Windows Mobile používáte, protože program si poradí s verzí 5.0, 2003, 6 i nejnovější 6.1.

**Komentář redakce:** *MOBILedit! je velmi zajímavou alternativou k originálním programům dodávaným samotnými výrobci telefonů. I když třeba Nokia Suite nabízí celou řadu dobrých funkcí, MOBILedit! ji prakticky ve všem trumfne a nabídne více. Od verze 3.0 nejsou navíc ochuzeni o praktické funkce ani majitelé PDA či MDA. Kdo chce nový MOBILedit! 3.0 používat, najde jeho plnou verzi na Chip DVD.*

LETENKY A VÝLUKY

## Jízdní řády s novinkami

Vyhledávač dopravního spojení, server Jizdnirady.cz (**www.jizdnirady.cz**), nabízí dvě novinky. První je možnost vyhledávání v letových řádech, které server čerpá ze systému Galileo. Součástí databáze jsou tedy letové řády všech letišť v České a Slovenské republice a velkého množství letišť na celém světě. Uživatelé si mohou letenky rezervovat a rovnou zaplatit, a to převodem na účet, online platební kartou nebo platebním systémem Paysec. Další novinkou serveru Jizdnirady.cz je integrace systému výluk Českých drah. Návštěvníci jsou tak nyní informováni o tom, zda dopravní spojení, které si vyhledali, je dotčeno výlukou, a současně dostávají odkaz na podrobné informace o výluce/výlukách na trati.