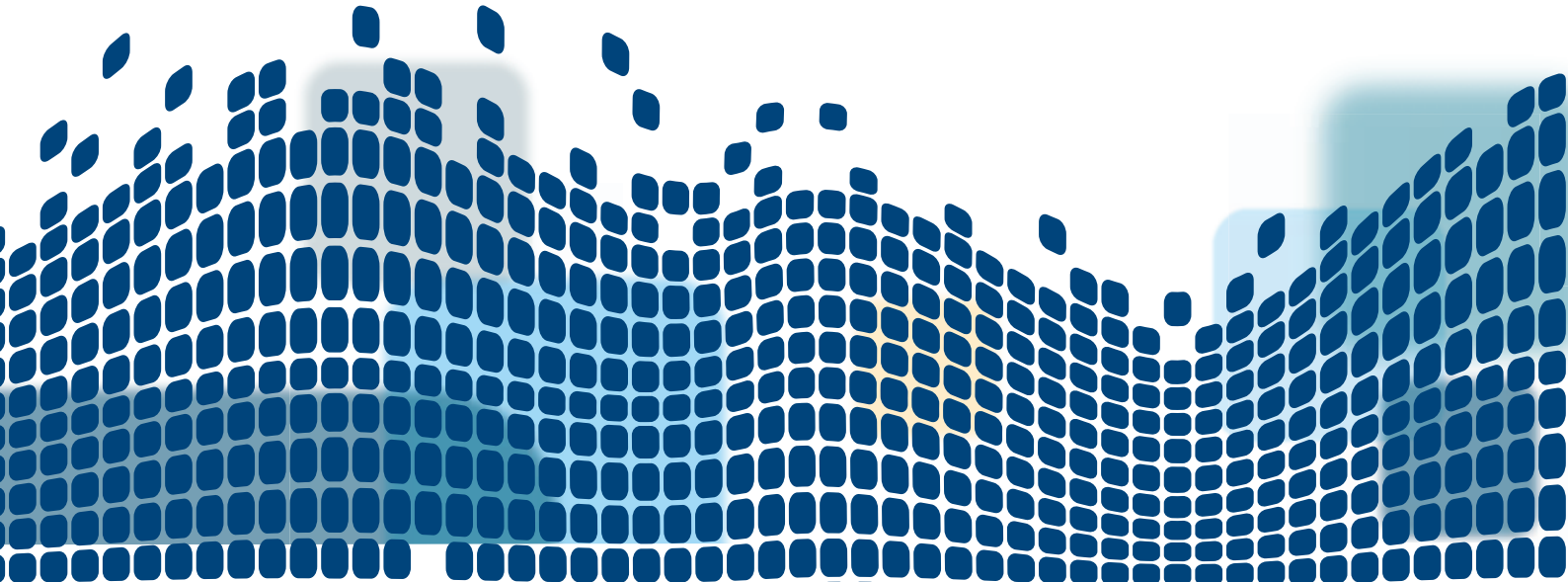
AVG V PRÁCI

Průvodce zabezpečením pro firmy

Jak se může malware vkrást do sítě vaší společnosti a jak se s ním vypořádat



Existuje ohromné množství způsobů, jak se viry, trojské koně a jiné typy škodlivého kódu mohou dostat do vaší firmy. Ochrana před nimi se vyplatí.

Víte o tom, že...

- ✔ Čtyřicet procent firem povoluje přístup k sociálním sítím, ale pouze 23 procent z nich má k tomuto přístupu stanoveny bezpečnostní zásady?
- ✔ Závažné procento ze 100 nejnavštěvovanějších webů obsahovalo škodlivý kód nebo odkazy na infikované weby?
- ✔ „War driving“ je postup vyhledávání a zneužívání nezabezpečených bezdrátových sítí?

Úplné zamezení přístupu uživatelů k internetu by bylo účinným způsobem, jak zabránit virům a jinému malwaru v přístupu do vaší sítě, avšak vašemu podniku by to mohlo uškodit. Proto je nutné seznámit se možnostmi ochrany proti přístupu zločinců k vašim cenným informacím a uplatňovat je.

Zde naleznete souhrn hlavních hrozeb a informace o tom, jak se před nimi chránit.

1 *E-MAIL A SPAM*

Stará známá písnička – Nejstarší a nejhorší způsob průniku do počítačů, ktery autori viru pouzivaji, je skrze přílohy e-mailů. Tato metoda útoků je stále populární, ale informovanost o malwaru v e-mailech a stále efektivnější metody prověřování zajistily podstatný pokles její účinnosti. „E-mail dříve býval primárním způsobem útoku. Používání antivirového softwaru a opatrnost při otevírání příloh ale většinu podobných hrozeb eliminovaly," vysvětluje bezpečnostní příručka společnosti AVG s názvem Proč již nejsou tradiční řešení ochrany před malwarem dostatečná. (***http://www.docstoc.com/docs/25405718/AVG-Whitepaper---Proč již nejsou tradiční řešení ochrany před malwarem dostatečná***).

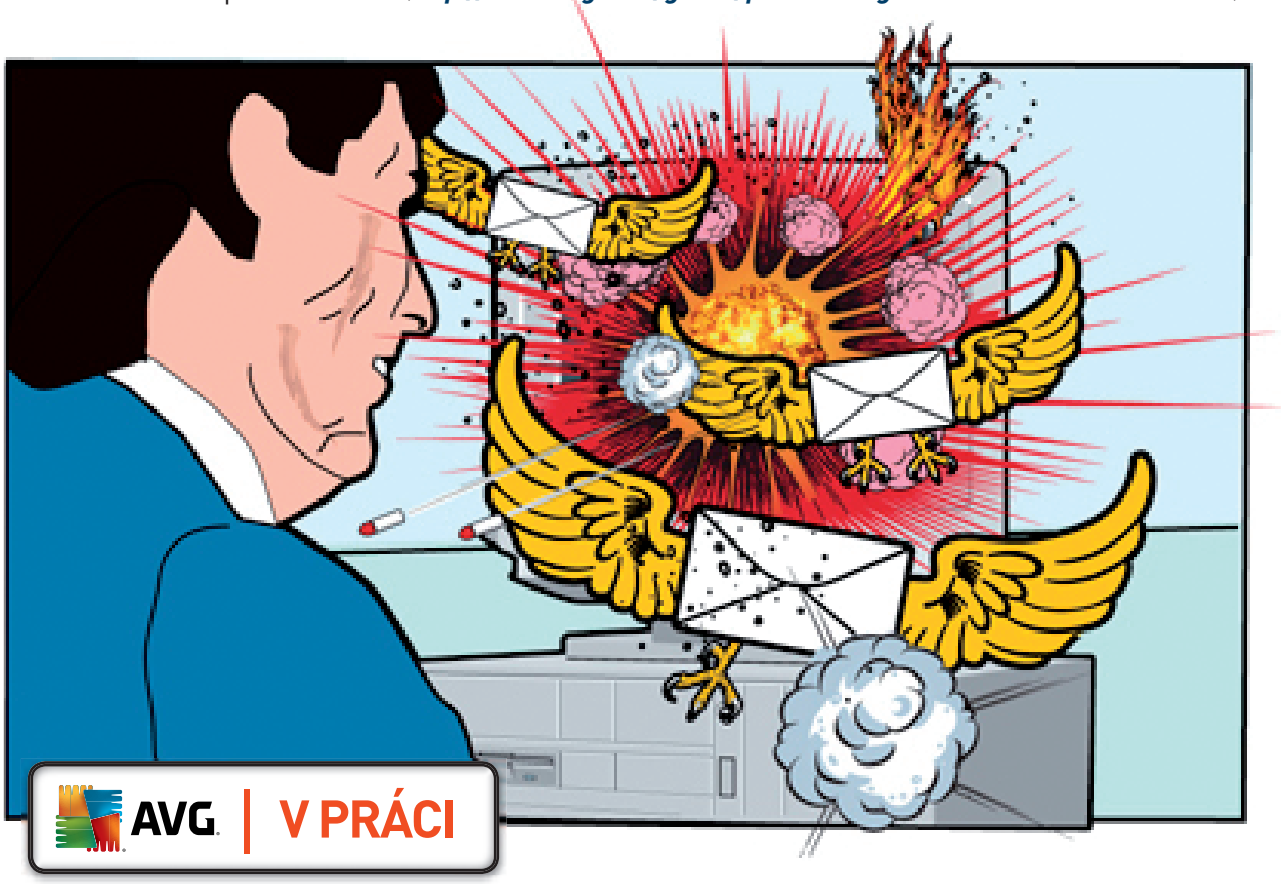
Poučení zaměstnanců o bezpečnostních postupech týkajících se e-mailů je nezbytné. Americká vládní organizace US CERT na svém webu doporučuje uživatelům, aby se vyhýbali otevírání nevyžádaných e-mailů, přestože jim je zaslala známá osoba.

„Mnoho virů dokáže maskovat adresu odesílatele, aby to vypadalo, jako by zprávu odeslal někdo jiný. Pokud je to možné, před otevřením jakýchkoli příloh požádejte odesílatele zprávy o potvrzení, že vám zprávu skutečně poslal," radí organizace. Další nutností je, aby zaměstnanci zakázali automatické stahování příloh, kdekoli je to možné. „Za účelem zjednodušení procesu čtení e-mailů mnoho poštovních klientů poskytuje možnost automatického stahování příloh.

Zkontrolujte nastavení softwaru, zda tuto možnost poskytuje, a zakažte ji," doporučuje organizace US CERT. Viz také: Proč již nejsou tradiční řešení ochrany před malwarem dostatečná (***http://www.docstoc.com/docs/25405718/AVG-Whitepaper---Proč již nejsou tradiční řešení ochrany před malwarem dostatečná***)

Seznámení s antivirovým softwarem (***http://www.us-cert.gov/cas/tips/ST04-005.html***) AVG Anti-Virus Business Edition 2011.

Základní ochrana podnikové sítě (***http://www.avg.com/gb-en/product-avg-anti-virus-business-edition***)



2 *RYCHLÉ ZPRÁVY*

Jak si chatováním přivodit problémy. – Přestože není rychlé zasílání zpráv používáno v takové míře jako e-mail, představuje reálnou bezpečnostní hrozbu pro ty společnosti, které je používají. Viry a jiný malware se mohou skrytě šířit prostřednictvím rychlých zpráv, a to stejně jako v případě e-mailu. Někteří zaměstnanci si nemusí být vědomi toho, že se infikované přílohy mohou šířit i prostřednictvím rychlých zpráv. Školení v této oblasti bezpečnosti je proto nutností. Společnost Microsoft poskytuje v této oblasti množství dobrých rad a varuje uživatele, aby nikdy neotevírali soubory přijaté od osob, které neznají.

Dalším způsobem, jak zavřít dvířka malwaru šířenému přes rychlé zprávy, je zamezení možnosti identifikovat uživatele sítě IM podle e-mailové adresy. „Některé služby zasílání rychlých zpráv používají jako své uživatelské jméno vaši e-mailovou adresu. Snadná dostupnost vaší e-mailové adresy vede k vyššímu množství přijatého spamu a ***phishingových*** útoků," varuje společnost Microsoft.

Viz také: 10 tipů pro bezpečnější rychlé zasílání zpráv (***http://www.microsoft.com/uk/protect/yourself/email/imsafety.mspx***)

5 kroků, jak se vyvarovat virům v rychlých zprávách (***http://www.microsoft.com/uk/protect/computer/viruses/im.mspx***)

Bezpečné používání rychlých zpráv a chatovacích místností (***http://www.us-cert.gov/cas/tips/ST04-011.html***)

3 *WEBOVÉ STRÁNKY / SOCIÁLNÍ SÍTĚ*

Kdy se vyplatí být nesociální – Přestože informovanost o nebezpečích při otevírání podezřelých e-mailových příloh vzrostla, kybernetičtí zločinci přišli na nové způsoby šíření škodlivého kódu.

Malware přítomný na webových stránkách, který může váš počítač nakazit při jediné návštěvě, nyní představuje rostoucí hrozbu pro spotřebitele i firmy. Prohlížeče a jejich rozšíření obsahují spoustu chyb, které mohou kompromitovat webové stránky a infikovat nic netušící návštěvníky malwarem.

Výzkum provedený v roce 2008 zjistil, že 70 % ze stovky nejnavštěvovanějších webů obsahovalo buď škodlivý kód, nebo odkaz, který návštěvníky přesměrovával na infikovaný web. „Útoky jsou v dnešní době směrovány na webové stránky. Útočníci mají při využívání e-mailů k dispozici pouze omezený počet způsobů, jak mohou počítač napadnout. Mohou použít infikované přílohy nebo odkazy na webové stránky, které obsahují škodlivý kód. Zasílání těchto e-mailů sice stále pokračuje, ale ukázalo se, že Internet obecně (obzvláště sociální sítě) poskytuje mnohem větší nabídku možností, jak lze útok provést, vysvětluje studie společnosti AVG s názvem Proč již nejsou tradiční řešení ochrany před malwarem dostatečná.

Dle nedávné studie „Zkouška ohněm", provedené poradenskou společností PWC, v sociálních sítích existuje vysoké riziko výskytu škodlivého kódu. Kolem 40 % společností uvedlo, že povolují přístup k sociálním sítím, avšak pouhých 23 % z nich aplikovalo potřebná bezpečnostní opatření, která by zamezila vzniku potenciálních problémů. „Dnešní nová generace zaměstnanců po celém světě mnohdy houfně přistupuje k sociálním sítím tak, aby o tom nevěděli správci sítě. Často tak činí obcházením tradičních opatření, která mnozí zaměstnavatelé používají," uvádí zpráva společnosti PWC. Firmy by jednak měly přehodnotit svou strategii zabezpečení informačních technologií, aby byly pokryty i hrozby ze sociálních sítí. Firmy hledají řešení a často využívají nástroje pro prověřování webu.

Technologie LinkScanner (***http://linkscanner.avg.com/***) od společnosti AVG například kontroluje každou stránku před jejím otevřením, zda neobsahuje infekce.

Viz také: Proč již nejsou tradiční řešení ochrany před malwarem dostatečná (***http://www.docstoc.com/docs/25405718/AVG-Whitepaper---Proč již nejsou tradiční řešení ochrany před malwarem dostatečná***)

Průzkum na sociálních sítích zjistil, že jsou uživatelé zranitelnější, než kdy jindy (***http://www.avg.com/gb-en/press-releases-news.ndi-224096***)

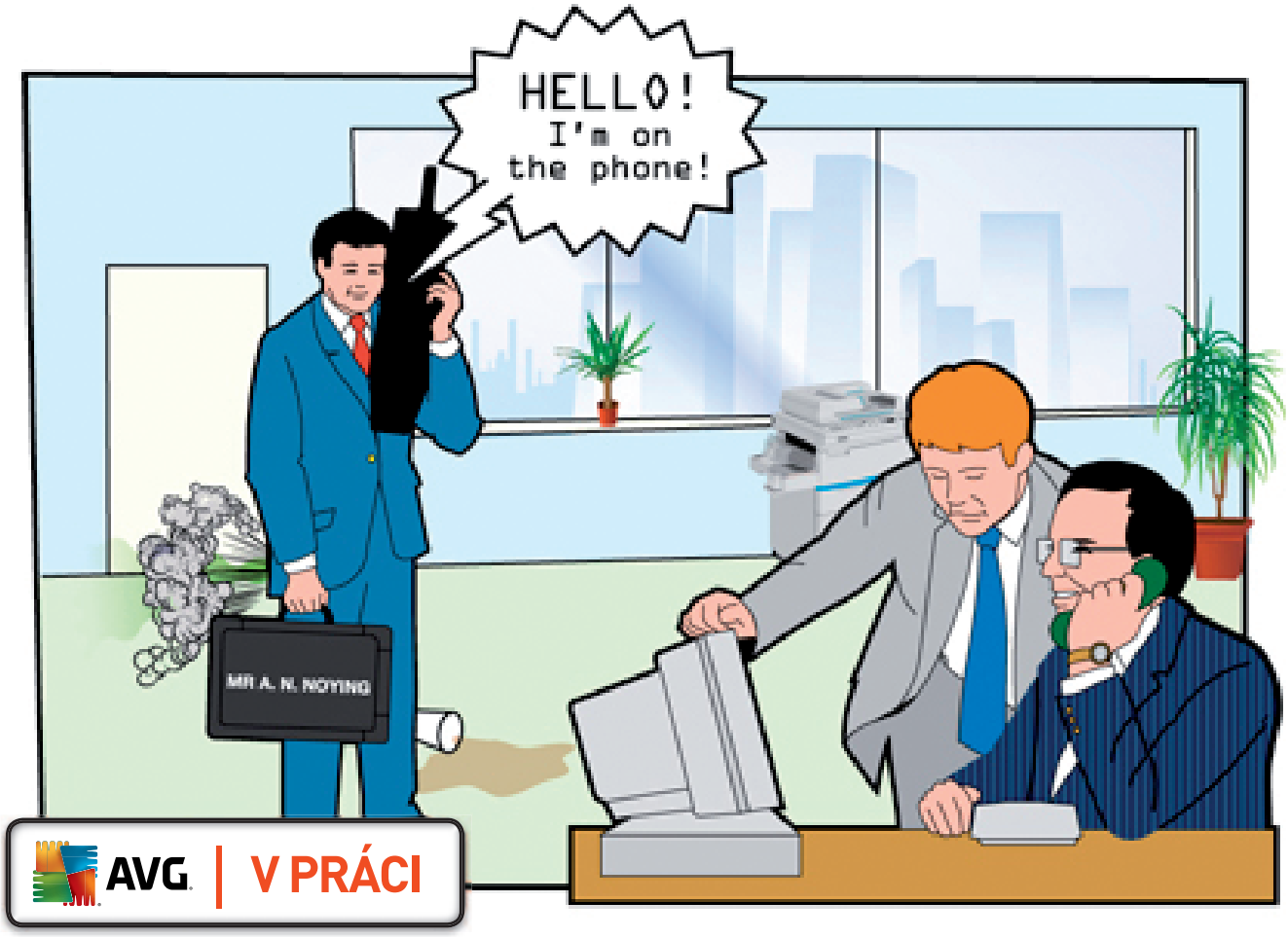
Zkouška ohněm od společnosti PWC (***www.pwc.com/en_GX/gx/...security-Survey/.../pwcsurvey2010_report.pdf***)

Webové prohlížeče a jejich zabezpečení (***http://jrsmith.blog.avg.com/2009/12/web-browsers-and-web-browser-security.html***)

4 *VNITŘNÍ HROZBY*

Poznejte svého nepřítele, možná jej zaměstnáváte

Ačkoli se firmy oprávněně obávají skrytých kybernetických zločinců, jejich zaměstnanci mohou představovat stejnou nebo dokonce větší hrozbu, pokud jde o malware. Takzvané „vnitřní hrozby" jsou častým tématem mnoha debat odborníků na zabezpečení informačních technologií. Bez ohledu na to, zda se jedná o úmysl nebo o náhodu, zaměstnanci jsou odpovědní za vniknutí většiny malwaru do podnikových sítí.



Školení v oblasti bezpečnostních postupů může snížit množství nechtěných infekcí. Zastavení zaměstnanců, kteří malware přinášejí úmyslně, je však mnohem větší výzvou. Byly zaznamenány případy, kdy zaměstnanci nainstalovali malware do firemní sítě z čisté zlomyslnosti nebo z důvodu osobního prospěchu. Jedním z těch nejznámějších byl Michael John Lauffenburger, pracovník firmy General Dynamics Corporation, který nainstaloval takzvanou logickou bombu do sítě této zbrojařské společnosti, přičemž doufal, že později bude najat, aby následné škody opravil. (***http://www.nytimes.com/1991/06/27/us/computer-programmer-charged-in-sabotage-plot.html?pagewanted=1***).

Je třeba udržovat antivirové programy a jiný bezpečnostní software aktualizované, stejně tak je nutné zabránit, aby zaměstnanci instalovali malware do počítačů. Ve společnostech pracujících s velmi citlivými daty opravdu stojí za to provádět kontroly zaměstnanců na pozadí, nebo provádět psychometrické zkoušky, které mohou pomoci k rozpoznání typů osobností schopných sabotovat vlastní firmu. Snižování stavů zaměstnanců může některé pracovníky motivovat k tomu, aby do podnikového systému nasadili malware. Proto je nutné omezovat síťová oprávnění zaměstnanců, zejména správců sítě, a mít připravenu možnost je okamžitě těchto oprávnění zbavit.

Viz také: Kdo je větší hrozba? Zaměstnanci nebo počítačoví zločinci (***http://small-business.blog.avg.com/2010/05/whos-the-bigger-threat-staff-or-cybercriminals.html***) Výzkum hrozeb CERT Insider (***http://www.cert.org/insider_threat/***)

5 *VZDÁLENÍ PRACOVNÍCI*

Zabezpečení mimo dohled – Ochrana firmy před malwarem, který proniká do sítě díky zaměstnancům, je skutečně náročná, avšak mnohem náročnější je kontrola pracovníků, kteří k podnikové síti přistupují vzdáleně. Přístup těchto pracovníků k aktualizacím antivirového softwaru a systému je obvykle laxnější než u běžných zaměstnanců.

Pokud pracovníkům povolíte používat vlastní zařízení, riziko průniku malwaru do podnikové sítě se zvýší. Tohoto bezpečnostního rizika se nejsnadněji zbavíte tak, že zaměstnancům zakážete používat k práci vlastní počítače. Ovšem na druhou stranu některé společnosti, jako je specialista na virtualizaci společnost Citrix, ukázala, že pokud umožníte pracovníkům kupovat si vlastní zařízení a spravovat je, zajistíte si oproti vlastnictví podnikových počítačů dlouhodobé úspory.

Společnost Citrix problémy s bezpečností obešla pomocí své vlastní virtualizační technologie, která v rámci hardwaru efektivně vytváří bezpečnou virtuální zónu. Takovou, jakou je například ambasáda v cizí zemi. Použití hostovaných nebo cloudových aplikací je jedním z dalších způsobů, jak obcházet problémy s počítači zaměstnanců, protože vše je umístěno na serveru a nikoli místně. (***http://community.citrix.com/display/ocb/2009/05/28/BYOC+Demystified++-+Part+1***)

Viz také: Plán Citrix BYOC ***http://community.citrix.com/display/ocb/2009/05/28/BYOC+Demystified++-+Part+1***
Konzola vzdálené správy aplikace AVG (***http://www.avg.com.au/products/avg-admin/***)

6 *PAMĚŤOVÁ ZAŘÍZENÍ USB*

Snadné šíření malwaru – Paměťová zařízení USB jsou častými šiřiteli malwaru. Oproti přenosným počítačům nebo smartphonům vypadají neškodně, ale dokážou pojmout několik gigabajtů kódu. „Protože jsou jednotky USB malé, okamžitě použitelné, levné a extrémně přenosné, jsou velmi oblíbeným médiem pro ukládání souborů a jejich přenos mezi počítači. Tyto charakteristiky z nich ale dělají oblíbené médium pro útočníky," tvrdí americká vládní bezpečnostní organizace CERT. (***http://www.us-cert.gov/cas/tips/ST08-001.html***)

Mezi organizace, které se nedávno staly obětí nákazy přenesené z paměťových zařízení USB, patří Greater Manchester Police, jejíž počítačové systémy byly několik dní nedostupné z důvodu infekce červem Conficker. Tony Anscombe, vedoucí oddělení společnosti AVG pro bezplatné produkty, poukazuje na to, že vyměnitelná zařízení lze automaticky kontrolovat pomocí softwaru AVG. Uživatelé mohou také před otevřením kteréhokoli ze souborů v paměťovém zařízení provést ruční kontrolu. Dále prohlásil: „Ponaučením z tohoto příkladu je, že byste měli být neustále ve střehu." (***http://free-product.blog.avg.com/2010/02/making-your-usb-memory-stick-safe.html#ixzz0fiXiwqgu***)

Organizace CERT radí ohledně malwarových infekcí prostřednictvím jednotek USB, abyste nepoužívali neznámá zařízení a abyste pracovní a osobní jednotky používali odděleně. „Nepoužívejte osobní jednotky USB v počítačích vlastněných vaší společností a nepřipojujte jednotky USB obsahující podnikové informace ke svému osobnímu počítači," radí organizace.

Viz také: Ani policie není imunní vůči virům (***http://obluk.blog.avg.com/***)

Opatrnost při používání jednotek USB (***http://www.us-cert.gov/cas/tips/ST08-001.html***)

7 *MOBILNÍ ZAŘÍZENÍ*

Chytřejší zabezpečení telefonů – Smartphony umožňující používání e-mailu představují pro podnikové sítě stejnou hrozbu jako stolní počítače. Ačkoli se samotné telefony jen zřídka stávají obětí virů a červů, mohou posloužit k rozšiřování malwaru do ostatních zranitelných zařízení v síti. Organizace US CERT uvádí, že jsou známy případy, kdy hackeři a zločinci zneužili textové zprávy k tomu, aby navedli nic netušící uživatele na webové stránky obsahující škodlivý kód. „Tyto zprávy, které se tváří, jako by byly odeslány legitimní společností, se vás mohou snažit přesvědčit k návštěvě infikovaného webu s tvrzením, že se vyskytl problém s vaším účtem nebo že jste se zaregistrovali v nějaké službě. Jakmile takový web navštívíte, můžete být požádáni o zadání osobních údajů nebo ke stažení infikovaného souboru," varuje organizace.

Dalším rizikem u smartphonů je stahování obsahu. Organizace CERT radí, abyste zaměstnance varovali před stahováním her a jiných nepotřebných aplikací do pracovních mobilních telefonů. „ Celá řada webových stránek nabízí hry a jiný software, který si můžete stáhnout do mobilního telefonu nebo zařízení PDA," uvádí organizace. „Tento software by mohl obsahovat škodlivý kód. Nestahujte soubory z webů, kterým nedůvěřujete. Pokud stahujete soubory z webu, který považujete za bezpečný, zkontrolujte jeho certifikát. Pokud stahujete soubory z webu před jejich otevřením, zvažte uložení v počítači a ruční prověření na přítomnost virů." Vedle e-mailu a webu existuje další způsob, jak může nebezpečný kód získat přístup do mobilního zařízení. Jedná se o technologii sítí pracujících na krátké vzdálenosti , která je známá jako Bluetooth. Organizace CERT radí, aby zaměstnanci vypínali technologii Bluetooth ve chvílích, kdy ji zrovna nepotřebují. „Ujistěte se, že využíváte všech výhod bezpečnostních funkcí, které vaše zařízení nabízí," tvrdí organizace. „Útočníci mohou zneužít rozhraní Bluetooth k získání přístupu do vašeho zařízení

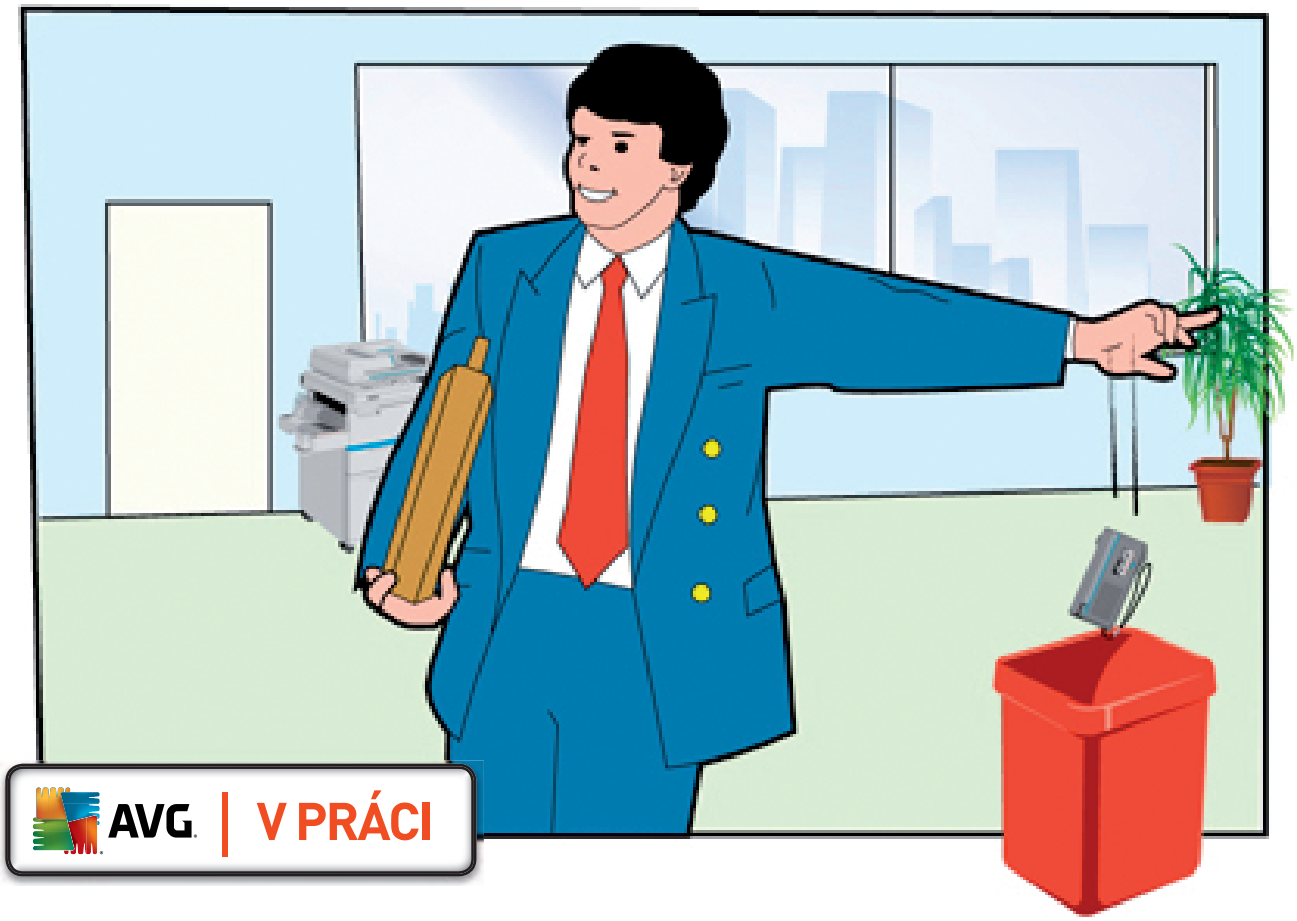
a ke stažení informací v něm uložených. Pokud rozhraní Bluetooth nepoužíváte, zakažte je, abyste předešli neoprávněnému přístupu do zařízení.“ Dalším problémem týkajícím se mobilních zařízení, jako jsou smartphony, je fakt, že jsou stále častěji používány k platbám za zboží a služby. Podle vedoucího pracovníka oddělení technologií ve společnosti AVG, Rogera Thompsona, to znamená, že na rozdíl od běžných virů, které se objevují čas od času, je skutečným problémem zákeřný kód. „Viry si vždy našly a čas od času si budou i nadále nacházet cestu do mobilních zařízení,“ prohlásil. „Jen minulý měsíc jsme objevili několik virů (přesněji červů) pro telefony iPhone. Virus, pokud se šíří, je pouhým virem. Software, který infikuje mobilní zařízení, je pak mnohem zákeřnější než obyčejný virus.“ Podle Thompsona mobilní malware zachycuje stisknutí kláves a přihlašovací údaje uživatelů. Dále uvádí: „Také se určitě objeví malware odesílající informace o internetových návycích uživatelů svým pánům, kteří pak tyto informace použijí k rozhodování, jaké reklamy se nám budou zobrazovat.“ „Je docela pravděpodobné, že si zločinci začnou vytvářet informační databáze, pomocí nichž si budou moci vytvořit náš profil, který pak následně mohou zneužít ke kriminální činnosti. ***http://thompson.blog.avg.com/2009/12/virus-migration-from-desktop-to-mobile.html#ixzz0fijzdgCD***

Viz také: Ochrana mobilních telefonů a zařízení PDA před útoky (***http://www.us-cert.gov/cas/tips/ST06-007.html***)

Roger Thompson: Migrace virů ze stolních počítačů do mobilních zařízení (***http://thompson.blog.avg.com/2009/12/virus-migration-from-desktop-to-mobile.html#ixzz0fijzdgCD***)

AVG J.R. Smith: Mobile World Congress (***http://jrsmith.blog.avg.com/2010/02/mobile-world-congress---vision-in-action.html***)

Jaký mají vliv chytré telefony a sociální sítě na kybernetický zločin? (***http://jrsmith.blog.avg.***



8 *BEZDRÁTOVÉ SÍTĚ*

I to, co nevidíte, vám může uškodit – Bezdrátové sítě jsou skutečným lákadlem pro hackery, jelikož mohou bez omezení rozšiřovat pole své působnosti i za zdi budov. Organizace US CERT varuje, že se někteří zločinci zaměřují na nezabezpečené bezdrátové sítě. Proto organizace upozorňuje, že je potřeba dbát na nastavení zabezpečení těchto sítí. „Praktika zvaná wardriving je prováděna osobami vybavenými počítačem, bezdrátovým zařízením a zařízením GPS. Tyto osoby projíždí městy, vyhledávají bezdrátové sítě a určují jejich souřadnice. Získané informace pak obvykle publikují online," varuje organizace US CERT. Organizace US CERT také radí, jak nastavit brány firewall, aby blokovaly útoky prostřednictvím bezdrátové sítě. „Bránu firewall je dobré nainstalovat nejen v síti, ale také přímo v bezdrátových zařízeních (tzv. hostitelská brána firewall). Útočníci, kteří dokážou přímo proniknout do bezdrátové sítě, mohou být schopní síťovou bránu firewall obejít. Hostitelská brána firewall pak brání data v jednotlivých počítačích."

Viz také: Zabezpečení sítí WiFi: Kampaň GetSafeOnline varuje před nebezpečími techniky piggybacking (***http://www.datamonitor.com/store/News/wifi_security_getsafeonline_warns_of_piggybacking_dangers?productid=44C2E8BD-EDB6-4EF0-9EB3-5954593F7D81***)

Zabezpečení bezdrátových sítí (***http://www.us-cert.gov/cas/tips/ST05-003.html***)

Skupinu AVG SMB najdete na adrese:
bit.ly/AVGSMB

Staňte se fanouškem společnosti AVG na adrese:
facebook.com/avgfree

Přečtěte si naše blogy na adrese:
blogs.avg.com

Sledujte nás na adrese:
twitter.com/officialAVGnews

Staňte se partnerem společnosti AVG na adrese:
avg.com/gb-en/affiliate

Sledujte náš videokanál na adrese:
youtube.com/user/officialAVG

AVG Technologies CZ, s.r.o.
Holandská 4, 639 00 Brno
Česká republika
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA
www.avg.com/us-en/homepage

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
Velká Británie
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Německo
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosia, Cyprus
Fax: +357 224 100 33
www.avg.com