AVG V PRÁCI

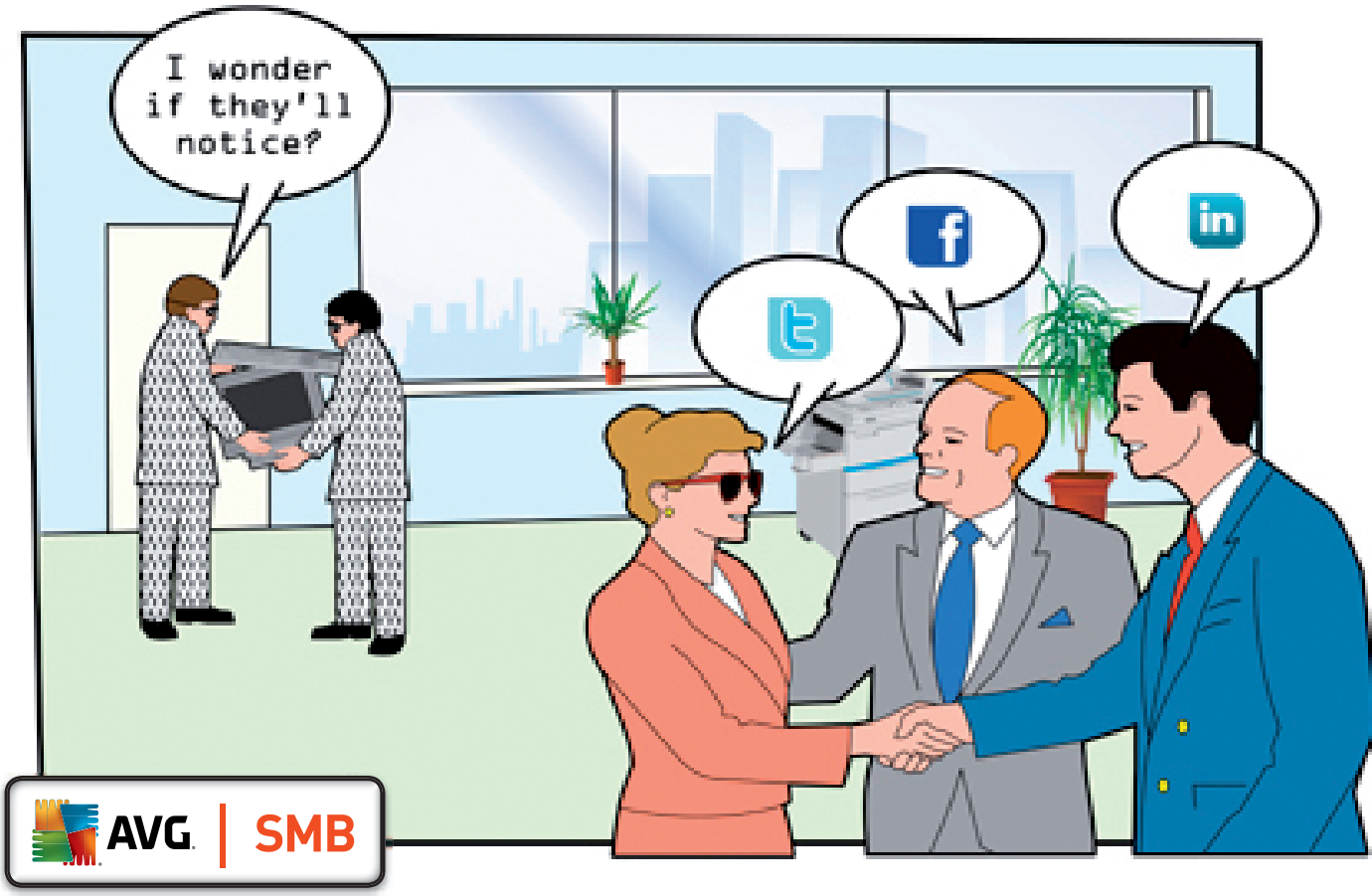
Průvodce zabezpečením

Odpovědi na vaše otázky
ohledně zabezpečení malých firem:
**Sociální sítě, citlivá data,
podnikové bankovnictví**

Otázka:

Pokud sociální sítě představují takové riziko, máme je prostě zablokovat?

Když se sociální sítě jako MySpace či Facebook objevily, některé podniky je považovaly za odvádějící od práce a zakázaly jejich používání. S rozšířením dalších sociálních formátů jako Twitter ale společnosti začaly využívat potenciálu sociálních sítí ke spolupráci. Sociální sítě se změnily z osobního prostředí na médium pro masovou komunikaci. Mnoho společností nyní vnímá služby jako například Twitter jako cenný marketingový kanál.



Vzhledem k tomuto novému legitimnímu využití ze strany firem se zdají být pravidla zakazující používání sociálních sítí kontraproduktivní. Přestože podobné nástroje hrají důležitou pracovní roli, společnosti by z bezpečnostních důvodů měly i nadále kontrolovat, jak je zaměstnanci používají. Bezpečnostní experti, jako je Herbert Thompson, profesor oddělení informatiky na Columbia University, varuje před nebezpečím publikování osobních informací v sociálních sítích. Lidé mohou publikovat osobní údaje, jako je jméno jejich matky za svobodna, které některé weby používají jako odpovědi na bezpečnostní otázky.

„Lidé publikují informace v sociálních sítích bez přemýšlení a ukazují se v různém světle. Došlo k velkému rozvoji technologií pro sdílení informací, avšak nikoli k rozšíření odpovídajících informací o tom, co můžeme sdílet," prohlásil.

Protože striktní zákaz používání sociálních sítí nemusí být tím správným krokem, firmy by měly zvážit vytvoření a prosazování pravidel jejich používání, zejména ve vztahu ke své oblasti působení. Nedávná studie uskutečněná španělskou školou IESE Business School, americkou E. Philip Saunders College of Business na Rochester Institute of Technology a britskou Henley Business School zjistila, že šest ze sedmi společností nemá vlastní formální pravidla upravující používání sociálních sítí při práci. „Ignorováním rostoucího využití a vlivu sociálních sítí a nástrojů Web 2.0 hrozí organizacím riziko zneužití, které může potenciálně vést k publikování citlivých informací nebo ke zkreslení obrazu společnosti," prohlásil Evgeny Kaganer, Ph.D., hlavní výzkumný pracovník a pomocný profesor na škole IESE Business School.

Podle ředitele oddělení výzkumu společnosti AVG, Rogera Thompsona, existuje vedle vytvoření přísných pravidel používání sociálních sítí také několik jednoduchých pokynů, které mohou vedoucí pracovníci zaměstnancům předat, a minimalizovat tak rizika.

„Fakt, že jsou uživatelsky velmi přívětivé, je činí nebezpečnými. Nevadí vám, že vaši přátelé ví, kde žijete, kdy máte narozeniny nebo jaké je jméno vaší matky za svobodna. Avšak pokud se zločincům povede nabourat do účtu vašich přátel, mohou se tyto informace dozvědět také," prohlásil Thompson.

Thompson radí používat jiná hesla pro každý web, která jsou také odlišná od přihlašovacích údajů k podnikovým systémům. I tak jednoduché opatření může být účinné. „Chcete-li být na těchto stránkách v bezpečí, měli byste pro každou z nich používat jedinečné ID uživatele a heslo nebo alespoň to jedinečné heslo," prohlašuje.

Mít obecné povědomí o tom, s kým pracovníci komunikují a jaké aplikace instalují, se opravdu hodí. „Rodiče vám kdysi říkali, abyste se nebavili s cizími lidmi. To samé platí i pro sociální sítě. Pokud daného člověka neznáte, nebavte se s ním," dodal. „Dávejte si pozor, které aplikace povolíte instalovat. Existuje ohromné množství lidí, kteří pro tyto sítě vyvíjejí aplikace, a něco mi říká, že ne všichni jsou ti hodní."

Více informací o bezpečnosti na sociálních sítích vám poskytne video (Co dělat a nedělat na sociálních sítích, Roger Thompson) (***http://www.youtube.com/watch?v=poHqIXvxmfg***)

Otázka:
Jak zodpovídám za ztrátu citlivých dat?

Odpověď na otázku, jakým zákonným opatřením mohou společnosti čelit v případě narušení nebo ztráty dat, závisí na celé řadě faktorů, včetně povahy dotyčných dat a místa, kde k incidentu došlo. Jakákoli ztráta dat může přinést negativní publicitu, pokud bude tato událost zveřejněna. Pokud jde o specifické právní úkony, nejpřísnější pravidla platí pro ztráty dat způsobené třetí stranou.

Například v USA, konkrétně v Kalifornii, byl již v roce 2003 jako první uveden v platnost zákon, který vyžaduje, aby společnosti v případě ztráty dat informovaly své zákazníky. Od té doby byla podobná legislativa přijata v dalších 44 státech. V současnosti se připravuje federální zákon H.R. 2221 s názvem Zákon o odpovědnosti za data (DATA). Ten však ještě nebyl schválen. Zákon DATA bude společnosti nutit, aby bez ohledu na to, ve kterém státě působí, informovaly každou osobu, „která je občanem nebo obyvatelem USA a jejíž osobní údaje byly získány neoprávněnou osobou jako výsledek narušení bezpečnosti". Dotyčná společnost navíc musí o narušení informovat Federální výbor pro obchod. Přestože zatím není jisté, v jaké formě bude tato legislativa přijata, na firmy, které se rozhodnou svá data šifrovat, se bude pohlížet příznivěji a nebude po nich vyžadováno informovat všechny zainteresované strany, pokud se prokáže, že jsou data chráněna či nečitelná.

Spojené království rovněž plánuje zpřísnit svá pravidla ochrany citlivých dat. Úřadu komisaře pro informace byl svěřen úkol ochrany dat ve Spojeném království a jeho pravomoci postupně kvůli řadě narušení zabezpečení vládních organizací narůstají. Od dubna 2010 má tato organizace možnost udělit podnikům pokutu do výše až 500 000 liber, pokud nedokážou odpovídajícím způsobem ochránit data zákazníků.

Ztráta dat je problémem také pro malé podniky, které obvykle nemají prostředky na zabezpečení informačních technologií. Dle průzkumu prováděného v roce 2009 americkou organizací National Cyber Security Alliance nemělo 86 procent dotazovaných malých společností žádného pracovníka vyhrazeného pro správu zabezpečení informačních technologií a pouhých 28 procent z nich připustilo, že u nich platí alespoň nějaká formální pravidla pro počítačové zabezpečení. Průzkum rovněž zjistil, že 66 procent společností povoluje používání zařízení PDA a počítačů obsahujících citlivé informace mimo pracoviště. ***http://www.staysafeonline.org/content/2009-smb-securitystudy***)

Otázka:
Jak je bezpečné podnikové bankovnictví online?

Flexibilita internetového bankovnictví je pro firmy i spotřebitele velmi přitažlivá, ale je třeba si uvědomit, že tento skvělý nástroj s sebou přináší specifická rizika. Například ředitel FBI, Robert Mueller, nedávno oznámil, že mu manželka zakázala používání jeho internetového bankovnictví, když se málem stal obětí phishingového podvodu.

Muellerova manželka byla zřejmě znepokojena oprávněně. Číselné údaje za rok 2008 pouze pro Spojené království uvádějí, že míra podvodů online oproti roku 2007 vzrostla o 132 procent. Dle britské bankovní skupiny APACS dosáhly internetové podvody celkové hodnoty 52,5 milionu liber.

Pro podniky mohou být hrozby plynoucí z používání internetového bankovnictví ještě více alarmující, což je dáno existencí takzvaných „vnitřních hrozeb". Odborníci na počítačovou bezpečnost dlouho tvrdili, že zaměstnanci představují větší kriminální hrozbu než hackeři zvnějšku. Toto tvrzení již nemusí být úplně správné, protože od poloviny devadesátých let vznikají organizované kriminální gangy a kybernetičtí zločinci používají stále sofistikovanější metody; v takovém prostředí představuje internetové bankovnictví pro zločince zevnitř i z vnějšku nový způsob, jak ukrást peníze nebo důvěrné informace.

Nedávný průzkum společnosti AVG ve Spojeném království zjistil, že počty finančních transakcí na internetu vzrůstají. 85 procent dotázaných lidí nyní nakupuje na internetu a více než dvě třetiny z nich používají internetové bankovnictví. Výzkum rovněž zjistil, že obavy z kybernetických krádeží narůstají. 43 procent dotázaných prohlásilo, že si na kybernetické krádeže dávají větší pozor než na běžné zloděje či zločince.

Průzkum společnosti AVG ale zjistil, že navzdory těmto obavám se přibližně 30 procent respondentů domnívá, že jejich ochranná opatření nejsou adekvátní. Také banky by pro ně mohly udělat víc. Například použití rozevíracích nabídek při procesu přihlašování může pomoci proti použití takzvaných keyloggerů. Zločinci tento software používají k záznamu stisknutí kláves. Rozevírací nabídky tímto způsobem nelze zaznamenávat, protože jsou aktivovány myší uživatele. Mezi další možnosti zabezpečení patří použití externích zařízení, která zákazníci obdrží od poskytovatele služeb a která při každém přístupu uživatele k účtu generují jedinečný kód PIN.

Mezi lidmi panuje obecná informovanost alespoň o některých rizicích týkajících se internetového bankovnictví a znalost nástrojů, které proti těmto rizikům lze použít. Tato informovanost a znalost musí růst na obou stranách a, co je důležitější, nesmí být ignorována.

Další informace o bezpečných transakcích online naleznete na stránce **Jak se mohu ochránit před kybernetickými krádežemi?** (http://www.avg.com/77954).

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