AVG V PRÁCI

Small Business Průvodci zabezpečením

Sociální sítě v podnikání: **Riziko nebo zhodnocení investice?**

Je sporné, zda portály LinkedIn, Facebook, Twitter a obecně sociální sítě přináší konkrétní výhody pro podnikání. Jsou tedy tyto komunikační kanály jen vstupní branou pro podniková rizika nebo jsou opravdu schopné zajistit jasný a pozitivní vliv na celkové zhodnocení investic?

Víte, že:

- **Vedoucí výzkumná a poradenská společnost Gartner předpovídá, že v roce 2014 dojde k překonání e-mailu sociálními sítěmi.** ***http://www.computerworlduk.com/management/online/new-media/news/index.cfm?newsid=21033***
- **Průzkum společnosti Manpower uskutečněný v lednu 2010 zjistil, že pouze 20 % společností po celém světě má stanovena svá pravidla pro používání sociálních sítí.** ***http://www.changeboard.com/resources/article/3404/social-media-the-employment-law-lowdown/***
- **Počet členů sítě LinkedIn během prvních šesti měsíců roku 2010 vzrostl o 40 %.** ***http://econsultancy.com/blog/6205-revised-mind-blowing-social-media-statistics-revisited-and-20+-more***
- **Nový průzkum společnosti Regus zjistil, že 40 % společností po celém světě úspěšně použilo sociální média ke svému rozvoji.** ***http://www.regus.presscentre.com/Press-Releases/34-Percent-of-Canadian-Businesses-Have-Used-Social-Media-to-Win-New-Business-38b.aspx***

Dle zakladatele sítě Facebook, Marka Zuckerberga, „....mají lidé uvolněnější vztah k soukromí online, než kdy dříve. Postoje se změnily a díky tomu, že na sociálních sítích lidé sdílejí informace o sobě, jsou mnohem otevřenější.Takové chování v sobě zahrnuje riziko ztráty vlastního soukromí, ale skutečný problém vzniká, když si uživatelé osvojí podobné otevřené chování vůči své práci a pracovnímu prostředí.

Tento posun v přístupu ke sdílení důvěrných informací mezi uživateli vedl na konci roku 2009 k rozhodnutí provozovatelů portálu Facebook změnit pravidla týkající se ochrany soukromí. Dle tvrzení pracovníků portálu Facebook se jednalo o skutečně odvážnou změnu. Část z 350 milionů uživatelů serveru po celém světě zastávala jiný názor a začala si stěžovat, že společnost učinila závažný krok mimo, který vede ke krádežím identity a narušení bezpečnosti na webu.
Dle názoru odborníků ve chvíli, kdy začal být portál Facebook (a dále zejména portály LinkedIn a Twitter) používán jako nástroj k sociální komunikaci na podnikové úrovni, přestala být rozšíření zásad soukromí zavedená tímto gigantem na poli sociálních sítí dostatečná k ochraně proti rizikům na úrovni podnikových sítí. Jednoduše řečeno, pokud jsou sociální sítě používány v podnikové síti, nové zásady týkající se soukromí jejich používání nezastaví. Pokud nebudeme reagovat přímo na problémy souvisejícími s krádežemi identity, kybernetickým zločinem a cílenými webovými špionážními útoky, necháváme otevřené dveře dalším potenciálním potížím.

Sociální sítě se momentálně zaměřují na to, jak se stát zábavnějšími, poutavějšími a jak zjednodušit správu, aby si udržely své uživatele. Snaží se především přimět uživatele k publikování důvěrnějšího obsahu a k odkazování na osobní informace. To vše vytváří profil a identitu. Přeneste tento příklad do podnikového prostředí a identita se rázem stává duševním vlastnictvím. To je třeba chránit.

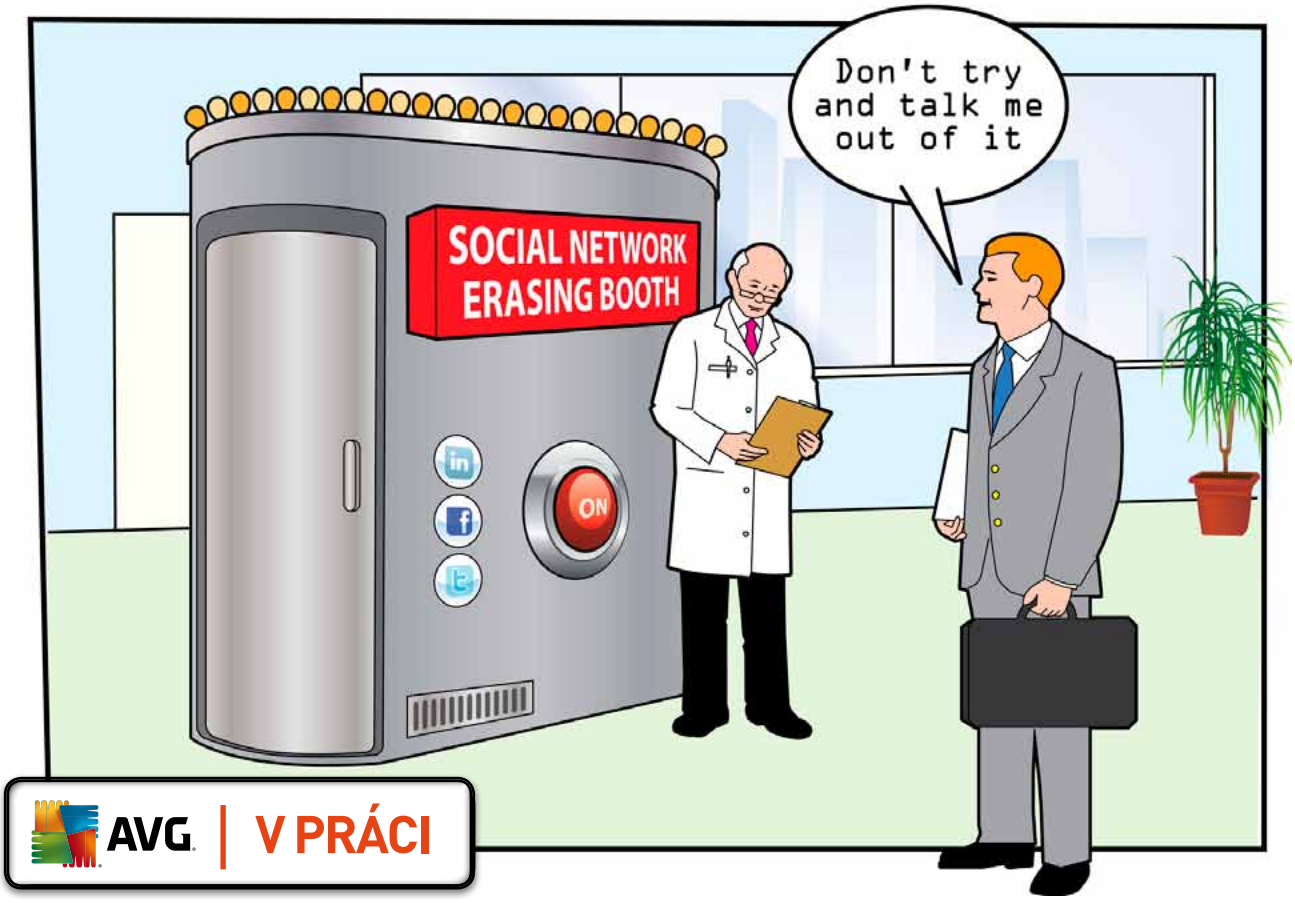
A ještě jednou přeneste tento příklad na pracoviště a uvidíte, kde se skrývají hrozby. Rozesílání informací o tom, se kterými společnostmi se stýkáte, se snadno dostane k vašim obchodním partnerům i konkurentům. Pokud světu oznámíte inovace produktů své společnosti dříve, než budou oficiálně uvedeny na trh, respekt kolegů si tím určitě nezískáte. A jako nejhorší varianta, pokud se někde zmíníte o tom, které společnosti nemůžete vystát a čí produkty nesnášíte, rázem se octnete jediný krok od obvinění z pomluvy.

Nebezpečí nehlídaného přístupu k sociálním sítím není pouze rizikem v oblasti fyzického majetku na osobní či podnikové úrovni. Závažné riziko představují také krádeže identity. Americký vládní web StaySafeOnline (***http://www.staysafeonline.org/*** poskytuje užitečné rady k bezpečnému používání sociálních sítí. „Sociální sítě online se staly prostorem využívaným podniky, zájmovými skupinami, školami či náboženskými skupinami," uvádí tento web. „Pokud jsou používány správně, lze je považovat za jedinečný komunikační nástroj k tomu, abyste zůstali v kontaktu s přáteli a kolegy. Stejně jako ostatní nástroje online však mohou být sociální sítě zneužívány hackery a kybernetickými zločinci." Web StaySafeOnline varuje, že by si normální

i podnikoví uživatelé měli dávat pozor na to, co publikují online, protože zločinci používají web k získávání informací, které by mohli zneužít. Proto je nutné znát možnosti nastavení soukromí a nástroje pro ochranu soukromí dostupné v rámci sociálních sítí, které používáte. Základem je, aby všichni zaměstnanci věděli, které sociální sítě jim společnost povoluje používat v pracovní době.

Nový pojem k zapamatování – gateway data

Jak by například mohl zločinec zneužít informace v profilu na portálu Facebook nebo LinkedIn k získání přístup k podnikovému nebo osobnímu bankovnímu účtu? Herbert „Hugh" Thompson, profesor informatiky na Columbia University v New Yorku, vytvořil termín „gateway data" označující důvěrné informace shromážděné ze sociálních sítí. Thompson se domnívá, že musí dojít k výpadku z přemíry sdílení informací prostřednictvím sociálních médií. „Zločinci musí být schopní získat takové informace sdílené lidmi, aby jich mohli využít k dosažení svého cíle a uškodit díky nim – já si myslím, že jsme se dostali do situace, kdy je to pro ně jednoduché," prohlašuje. Thompsonův termín gateway data lze používat různými způsoby. Například zjištění jména něčí matky za svobodna pomocí portálu Facebook může vést ke správné odpovědi na bezpečnostní otázku k e-mailovému účtu. Přestože se jedná o pouhý osobní účet, došlo ke kompromitaci uživatele a hacker je o krok blíž k podnikovým informacím, které potřebuje.



Jakmile zločinec získá přístup k e-mailu uživatele, je vysoce pravděpodobné, že získá informace například k tomu, aby pronikl do bankovního účtu uživatele. Mezi další možnosti využití gateway dat patří použití částečných informací, jako například prvních pět číslic podnikové kreditní karty k navedení uživatele k tomu, aby zločinci sdělil celé číslo.

Hacker se bude obvykle snažit použít mnoho fragmentů dat k odhalení většího množství důvěrných informací. Proto není oddělení osobních a pracovních dat natolik zřetelné, jak si můžete myslet. V podstatě mezi těmito dvěma druhy dat nejsou žádné hranice. Kromě dodržování bezpečnostních postupů uvedených na stránkách StaySafeOnline někteří experti doporučují neinstalovat aplikace ze sociálních sítí, pokud nepochází z důvěryhodného zdroje. Rozhodování o tom, který zdroj je důvěryhodný a který ne, je však hodně subjektivní. Jak vlastně poznáte, komu můžete důvěřovat? A jak poznáte že takový zdroj nebyl kompromitován?

„Chce to zdravou dávku skepse," radí Roger Thompson, hlavní výzkumný pracovník internetové bezpečnostní společnosti AVG. „Jakmile obdržíte pozvánku ke sledování videa nebo výzvu k instalaci něčeho, abyste si dané video mohli přehrát, nedělejte to. Nestojí to za to a podobným instalacím byste se měli vždy vyhýbat. Tyto neznámé aplikace často obsahují zlomyslný kód, jako jsou viry nebo červi, a proto je vzrušující video přesně tím druhem nástrojů, které zločinci používají a rozšiřují ve formě virů na webu," dodal Thompson. Společnost AVG také varovala před popularitou zkrácených adres URL ve službách, jako je Twitter. „Problém se zkrácenými odkazy tkví v tom, že se obvykle nepodobají původním adresám URL, na které přesměrovávají. Uživatelé proto neví, na co klikají. Lidé na podobné odkazy klikají s tím, že se s jejich pomocí dostanou na určité stránky. Takové odkazy však lze snadno nabourat a přesměrovat na stránky obsahující trójské koně, spyware, rootkity nebo jiný malware," vysvětluje Thompson.

Když to shrneme, sociální sítě mohou mít kladný vliv na podnikové komunikační prostředí a mohou pozitivně přispět k fungování podniku či k návratnosti jeho investic do infrastruktury informačních technologií. Potřebují ale určitou míru dohledu, zavedení určitých uživatelských zásad a určitou míru strategického plánování, což dohromady zajistí dodržování podnikových postupů ze strany zaměstnanců.

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