AVG V PRÁCI

Průvodce zabezpečením

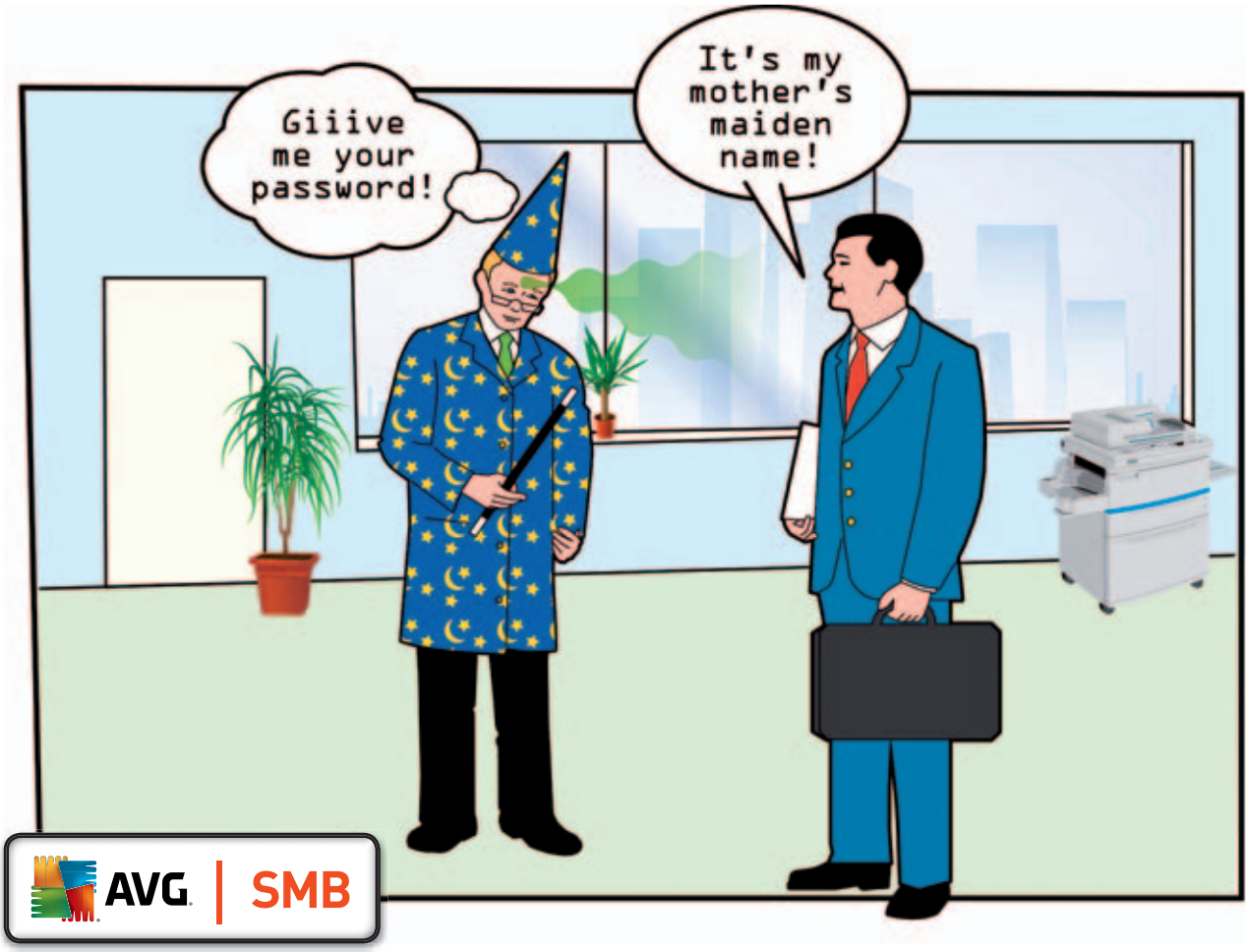
Sociální inženýrství:
Narušení lidí, nikoli strojů

Nejslabším článkem počítačového systému je téměř vždy člověk, který s ním pracuje, a to hackeři moc dobře vědí. Sociální inženýrství je všudypřítomné a často velmi účinné...

- Bezpečnostním expertům se podařilo přesvědčit pracovníky, aby jim odhalili svá hesla, výměnou za pero zdarma ***http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/***
- Více než polovina počítačových uživatelů dle nedávné studie společnosti AVG obdržela phishingové e-maily.

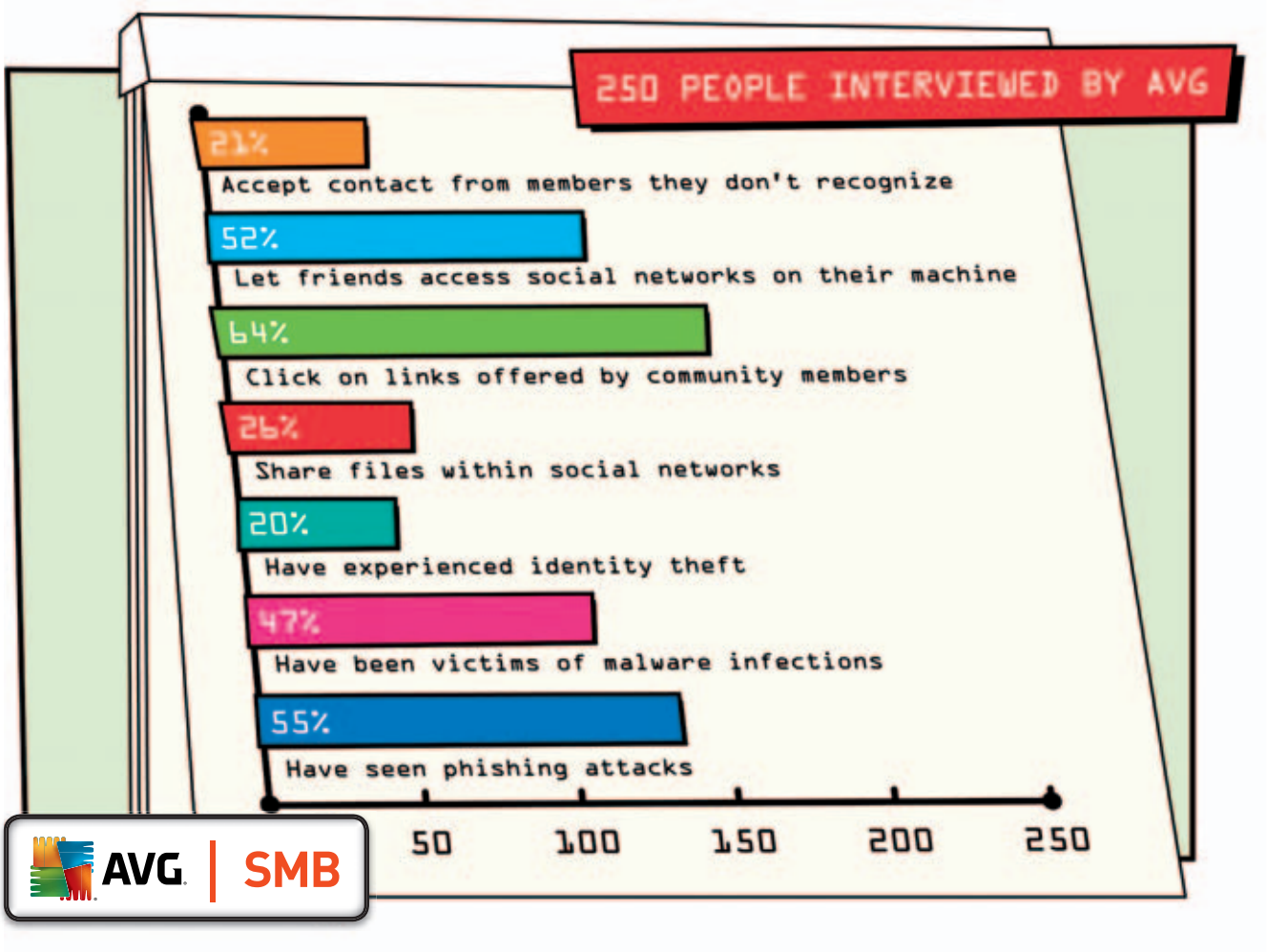
Hackery si často představujeme jako technické experty, kteří dosahují svých cílů pomocí velmi komplikovaného počítačového kódu. Ačkoli je na tom něco pravdy, získání přístupu k počítači může být docela jednoduché. Stačí jen někoho zmást natolik, aby vám sdělil své heslo. Tato taktika zneužití lidského faktoru k získání přístupu do počítače je známá pod pojmem sociální inženýrství a je všeobecně uznávána jako jedna z nejefektivnějších technik používaných kybernetickými zločinci. „Lidé jsou často nejslabším článkem v zabezpečení," varuje americký vládní poradenský web ***StaySafeOnline***. „Zločinci a hackeři to ví a patřičně toho zneužívají. Seznamte se se způsoby, jak odhalit jimi používané triky."

Nechat se oklamat je snadné



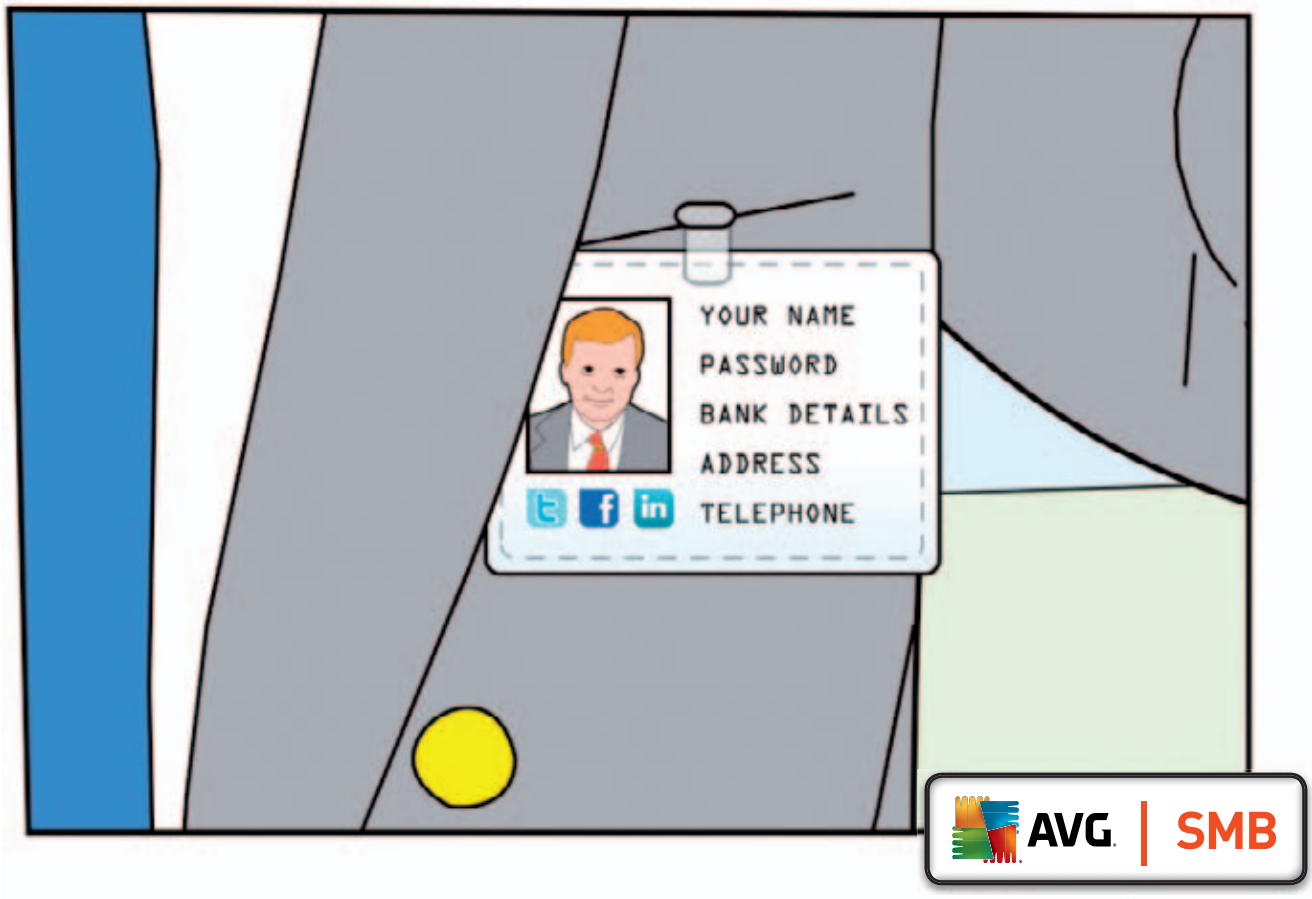
Je třeba si dávat pozor na velmi jednoduché taktiky, jako je telefonování na pomocí zdánlivě nevinných otázek vyloudit síťové heslo od osoby, která hov útočník není schopný získat dostatek informací od jedné osoby, může se pokusit kontaktovat jinou osobu ve stejné organizaci a přitom se spoléhat na informace získané od té první osoby, což mu dodá na důvěryhodnosti," varuje americká vládní bezpečnostní agentura ***US-CERT.***

Příklad, jak snadno lze lidi obelstít pomocí sociálního inženýrství, nedávno představili organizátoři konference InfoSecurity Europe. Expertům se povedlo přesvědčit 90 % pracujících, které zastavili na londýnském nádraží Waterloo Station, aby jim sdělili své heslo výměnou za pero zdarma. Někteří podezřívaví lidé nejdříve odmítli, ale nakonec odborníkům sdělili dostatek informací, aby zjistili správné heslo. Kevin Mitnick, jeden z nejznámějších hackerů všech dob, přiznal, že sociální inženýrství bylo základní součástí jeho práce. „Když si obyčejný člověk představí počítačového hackera, obvykle se mu vybaví nelichotivý obraz osamoceného a introvertního počítačového maniaka, jehož nejlepším přítelem je jeho počítač a který má problémy s běžnou konverzací s výjimkou konverzace pomocí rychlých zpráv," vysvětluje Mitnick ve své knize ***Umění klamu***. „Sociální inženýr, který je často vybaven hackerskými dovednostmi, má rovněž komunikační schopnosti k tomu, aby mohl využívat lidi a manipulovat s nimi těmi nejnemožnějšími způsoby, které mu umožní získat potřebné informace." Dávejte si pozor na podvodníky



Sociální inženýrství ale nemusí být uskutečňováno pouze osobně nebo telefonicky. Jednou z nejpopulárnějších technik sociálního inženýrství je phishing, který funguje následovně: Zločinci bombardují počítačové uživatele e-maily, které se tváří, jako by byly odeslány z bank nebo z jiných důvěryhodných institucí, kde si chráníte cenné informace pomocí hesel. Příjemci jsou vyzýváni k odpovědi na e-mail tím, že kliknou na zdánlivě legitimní odkaz a zadají své přihlašovací údaje. . „Útočník může rozesílat e-maily, které se tváří, jako by byly odeslány vydavatelem platebních karet nebo finanční institucí a které vyžadují poskytnutí informací o účtu, přičemž často tvrdí, že se vyskytl nějaký problém," vysvětluje US-CERT na svých webových stránkách. „Pokud uživatelé na tyto e-maily zareagují a poskytnou požadované informace, útočníci tyto informace mohou zneužít k získání přístupu k účtům.." Nedávný průzkum prováděný společností AVG zjistil, že kolem 55 procent z 250 dotazovaných uživatelů již obdrželo phishingové e-maily. Tento průzkum se zejména zaměřil na to, jak zvýšené používání sociálních sítí, jako je Facebook, Twitter nebo MySpace, přispívá k nárůstu výskytu phishingu a jiných bezpečnostních hrozeb. „

Vznik sociálních sítí vedl k prolínání hackerských technik založených na programování se sociálním inženýrstvím. Společnost AVG se touto hrozbou zabývá již od roku 2007. „Vývoj antivirových řešení se v posledních dvou či třech letech nacházel v přechodné fázi, protože se malware změnil z jednoduchých virů v komplexní webové hrozby, které kombinují útoky typu exploit a sociální inženýrství s cílem podvést nic netušících uživatele a získat jejich data," prohlásil Larry Bridwell, globální bezpečnostní stratég společnosti AVG Technologies. Důležitá je informovanost



Když je třeba se chránit před útoky pomocí sociálního inženýrství, software AVG může významně pomoci. Odborníci se ale shodují na tom, že základem je poučení zaměstnanců o bezpečnosti. „Informovaní pracovníci jsou hlavní linií obrany proti hrozbám online pro váš podnik," radí britská vládní kampaň ***GetSafeOnline*** . Agentura S-CERT tuto radu ještě upřesňuje: „Buďte podezřívaví vůči jakýmkoli nevyžádaným telefonátům, návštěvám nebo e-mailům jednotlivců, kteří se ptají na zaměstnance nebo jiné interní informace. Pokud neznámá osoba tvrdí, že přichází z legitimní společnosti, pokuste se ověřit její identitu přímo v dané společnosti."

Nejlepší strategií pro podniky je naučit pracovníky, že předávání jakýchkoli informací někomu, jehož motivy jsou podezřelé nebo neznámé, není dobrý nápad. Tento „paranoidní" přístup je třeba vštěpovat novým pracovníkům již od prvního dne v práci. Noví pracovníci jsou dle Kevina Mitnicka nejvíce náchylní podlehnout technikám sociálního inženýrství. „Noví zaměstnanci jsou oblíbeným cílem útočníků. Zatím totiž neznají mnoho lidí, neznají správné postupy a neví, co je ve společnosti zakázáno a co je povoleno. Ve snaze udělat dobrý dojem se horlivě snaží ukázat, jak umí spolupracovat a jak rychle dokážou zareagovat," varuje.

Vedle informovanosti zaměstnanců je nutná také ochrana. Proto by se firmy měly ujistit, že používají aktualizovaný bezpečnostní software. Software AVG 2011 obsahuje technologie, které dokážou rychle a přesně určit, zda daný web obsahuje phishingový útok či nikoli.

Zločinci si vždy najdou způsob, jak překonat kterékoli podnikové počítačové zabezpečení. Pokud si však budete dávat pozor na své zaměstnance i počítače, podstatně hackerům znesnadníte práci.

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