AVG V PRÁCI

Small Business Průvodci zabezpečením

Kdo je větší hrozba?
Zaměstnanci nebo počítačoví zločinci

Podnikoví zaměstnanci jsou často vnímání jako větší hrozba pro zabezpečení podniku než externí hackeři. Platí to i dnes s ohledem na stále větší důmyslnost počítačových zločinců?

Víte, že:

- ✔ **Před deseti lety byly viry a jiné formy malwaru z velké části výsledkem práce mladých amatérských programátorů, kteří se pokoušeli upoutat na sebe pozornost.**
- ✔ **Výzkum provedený společností Verizon zjistil, že 74 % narušení dat bylo způsobeno někým zvenčí.**
- ✔ **Dle číselných údajů uváděných světovým ekonomickým fórem dosáhl objem škod způsobených krádežemi online v roce 2009 hodnoty 1 bilionu dolarů.**

Obecně je známo, že největší hrozbou pro většinu podnikových počítačových sítí jsou nespokojení zaměstnanci, nikoli skrývající se kybernetičtí zločinci. Zaměstnanci mají přístup k heslům.

Techničtí zaměstnanci mají dokonce správcovská oprávnění. Navíc ví, co mají hledat a co by se konkurenci mohlo hodit. Takzvanou koncepcí „vnitřních hrozeb" se odborníci v oblasti zabezpečení informačních technologií zabývají již dlouhou dobu. Je zčásti založena na studii FBI z počátku devadesátých let, která zjistila, že 80 % útoků na zabezpečení informačních technologií pochází zevnitř organizace.

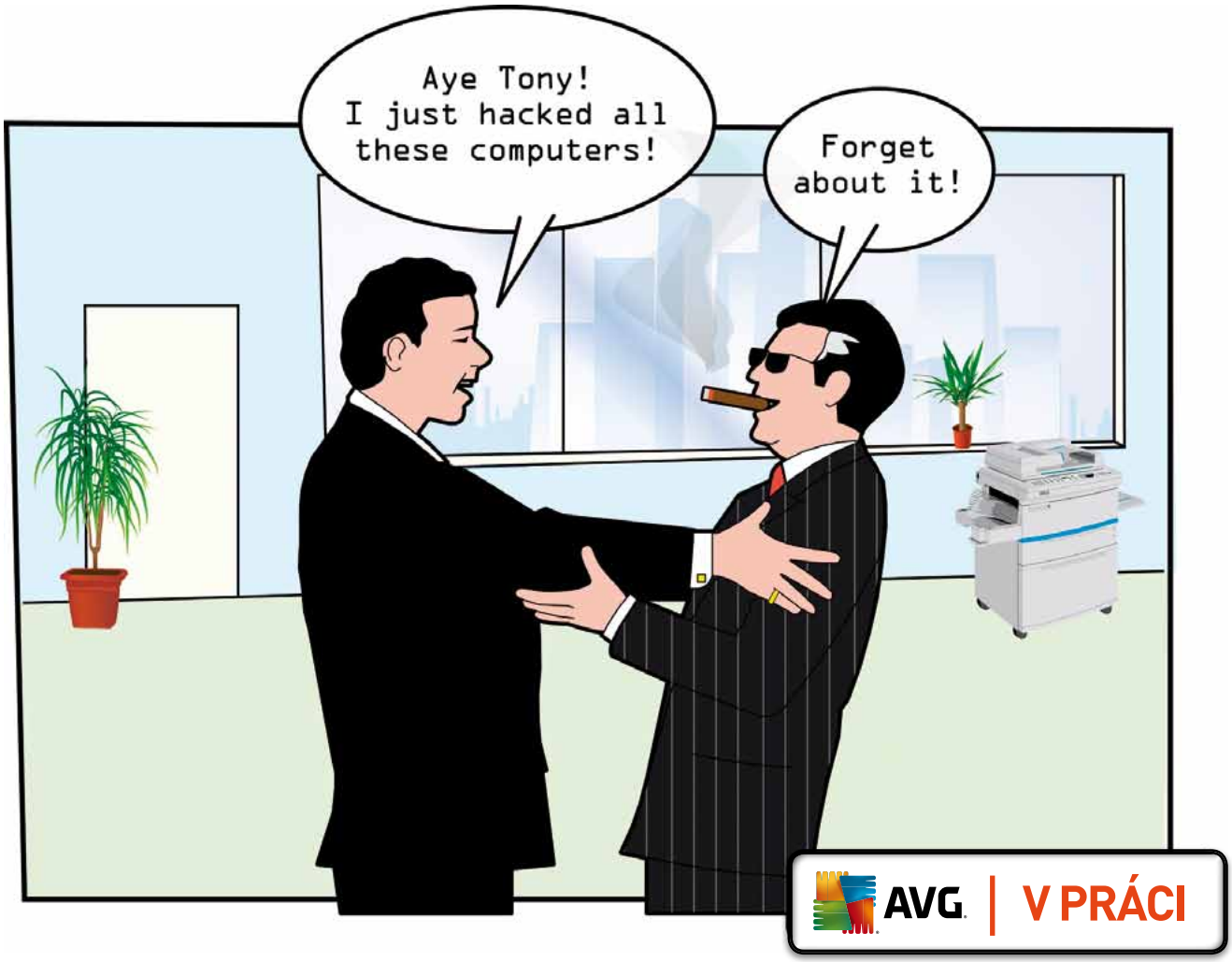
Za posledních dvacet let se toho ale hodně změnilo. Zatímco kdysi se hackingem a psaním virů zabývaly spíše děti, dnes kybernetický zločin dospěl a stal se velkým byznysem. Dle číselných údajů uváděných světovým ekonomickým fórem dosáhl objem škod krádeží online v roce 2009 hodnoty 1 bilionu dolarů. Tato účinná přeměna kybernetické kriminality v organizovaný zločin mohla mít vliv na vnímání toho, zda mají být „vnitřní hrozby" i nadále hlavní prioritou zabezpečení informačních technologií. Organizované zločinecké gangy, které se zaměřují na průniky do podnikových sítí, stejně jako se kdysi snažily o průnik do bankovních trezorů, možná mohou vypadat jako mnohem větší hrozba než nevyzpytatelný či nespokojený zaměstnanec.

Zpráva společnosti AVG s názvem ***Proč již nejsou tradiční řešení ochrany před malwarem dostatečná*** vysvětluje, proč by společnosti měly zvážit způsob nasazení svých prvků zabezpečení. „Před deseti lety byly viry nebo jiné formy malwaru z velké části výsledkem práce mladých amatérských programátorů (rádoby hackerů a zelenáčů v oboru), kteří se pokoušeli upoutat na sebe pozornost a získat věhlas v komunitách hackerů," uvádí tato zpráva a dále dodává: „V posledních letech se však tato oblast výrazně změnila." Organizované kriminální skupiny si uvědomily, že pomocí malware mohou přijít na slušné peníze. Začaly najímat zkušené programátory, kteří jim za tímto účelem vytváří škodlivé programy. Cílem těchto programů není působit potíže, ale umožnit krádeže peněz, dat nebo obojího. Výsledkem bylo vytvoření černého trhu, na kterém lze nelegálně nakupovat a prodávat data nebo programy určené k těmto krádežím." Přestože se externí hrozby díky vzniku kriminálních sítí staly mnohem organizovanější, nemůžeme říct, že převládly nad nebezpečími ze strany nespokojených zaměstnanců. Experti se v tomto ohledu dělí na dvě poloviny. Částečně je to dáno tím, že se neshodují na definici interních hrozeb a jejich rozdílu oproti externím hrozbám.

Zatímco se za posledních dvacet let změnila povaha kybernetického zločinu, změnilo se i fungování průměrných podniků. Společnosti se staly více fragmentované a čím dál více se spoléhají na konzultanty a odborníky zvenčí. Další faktory, jako je vyšší míra slučování a akvizic, učinily dříve stabilní hranice některých velkých společností nestálé, a to z důvodu slučování s konkurencí a přijímání zaměstnanců konkurence. Dawn Cappelli, vedoucí technická pracovnice týmu CERT (Computer Emergency Response Team) na univerzitě Carnegie Mellon University nedávno popsala, jak si musela její organizace upravit definici vnitřní hrozby, aby udržela tempo s obchodní praxí. „Naše definice vnitřní hrozby zní: aktuální či bývalý zaměstnanec a smluvní nebo obchodní partner," uvedla. „Na základě sledování posledních trendů jsme nedávno tuto definici rozšířili o obchodního partnera."

CERT jako jedna z hlavních amerických organizací zabývajících se počítačovou bezpečností i nadále podporuje tvrzení, že jsou to právě vnitřní hrozby, na které by se společnosti v rámci zabezpečení informačních technologií měly zaměřit. Organizace tomuto problému na svém webu vyhradila zvláštní sekci s názvem Výzkum vnitřních hrozeb. „Interní pracovníci díky svému legitimnímu přístupu k informacím, systémům a sítím dané organizace představují

pro zaměstnavatele podstatné riziko. Zaměstnanci potýkající se s finančními problémy mohou velmi snadno zneužít systémy, které denně používají, ke spáchání podvodu," uvádí organizace ve své zprávě s názvem „Velký přehled o sabotážích IT provedených zevnitř. ***(www.cert.org/archive/pdf/08tr009.pdf)***



Zatímco organizace jako CERT zaujaly v oblasti vnitřních hrozeb jasné stanovisko, jiné společnosti se domnívají, že sofistikovanější způsoby a větší organizace kybernetických zločinců vedla k nevratným změnám ve způsobu nahlížení na problém zabezpečení. Komunikační společnost Verizon zcela jasně uvádí, že by se společnosti měly zaměřit na externí hrozby. Zpráva společnosti Verizon o vyšetřováních narušení dat v roce 2009 ***(www.verizonbusiness.com/uk/products/security/risk/databreach)*** uvádí, že 74 % narušení dat pocházelo zvnějšku, zatímco 32 % bylo provedeno obchodními partnery. „Zevnitř bylo uskutečněno pouze 20 % narušení, což hovoří proti některým běžně uváděným tvrzením," oznámila zpráva. Zpráva společnosti Verizon připouští, že mnohá narušení zabezpečení zevnitř nebyla oznámena, protože podniky nestojí o negativní publicitu, které by se po zveřejnění takového incidentu mohly dočkat. Avšak společnost svou zprávu uzavírá s tím, že ačkoli menší množství interních incidentů nebylo oznámeno, její výzkum prováděný po dobu několika let

podporuje její tvrzení, že větší nebezpečí hrozí ze strany externích útoků. „Výsledky, které jsme získali zkoumáním 600 případů za období 5 let, popírají stávající dlouhodobě a široce prosazované tvrzení o tom, že za většinou narušení stojí útoky zevnitř," uvádí společnost. Zatímco někteří bezpečnostní specialisté se zaměřují na vymezení externích a interních hrozeb, jiní experti se domnívají, že přílišné zaměření na původ útoku může nebezpečně odvádět pozornost. „Celá debata o vnitřních a vnějších hrozbách byla vždy spíše záležitostí sémantiky než čehokoli jiného," prohlásil bezpečnostní guru Bruce Schneier na svém blogu. „Pokud porovnáte počty útoků, zjistíte, že vnější útoky převažují, protože vnějších útočníků je mnohem více. Pokud porovnáte počty incidentů, čísla se začínají sbližovat: v tomto případě je to 75 procent a 18 procent.

Pokud porovnáte výsledné škody, útoky zevnitř mají mnohem vyšší účinnost – zejména proto, že jejich původci mají mnohem více podrobných informací a mohou své útoky lépe cílit." (***http://www.schneier.com/blog/archives/2008/06/it_attacks_insi.html***) Schneier se domnívá, že společnosti by měly uplatňovat celkový přístup k zabezpečení informačních technologií a měly by se zamyslet nad tím, jak ochránit svá data a systémy před útoky, a to bez ohledu na původ takových útoků.

„Vnitřní i vnější hrozby jsou bezpečnostní rizika, proti kterým je třeba se bránit. Snaha o jejich hodnocení není příliš užitečná," uvádí.

Přestože to vypadá, že nebezpečí hrozící od kybernetických zločinců používajících stále více sofistikované praktiky v posledních letech vzrostlo, stále větší fragmentovanost struktury mnoha společností vede k tomu, že také jejich zaměstnanci, partneři a dokonce i zákazníci představují závažnou hrozbu. Přestože podnikům může prospět nasazení různých taktik vůči jednotlivým skupinám útočníků (kybernetičtí zločinci nebo vnitřní hrozby), nejlepším řešením je pořídit si robustní a adaptivní bezpečnostní strategii, která drží krok s rychle se vyvíjejícím zabezpečením informačních technologií.

Robert Gorby

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