AVG V PRÁCI

Průvodce zabezpečením

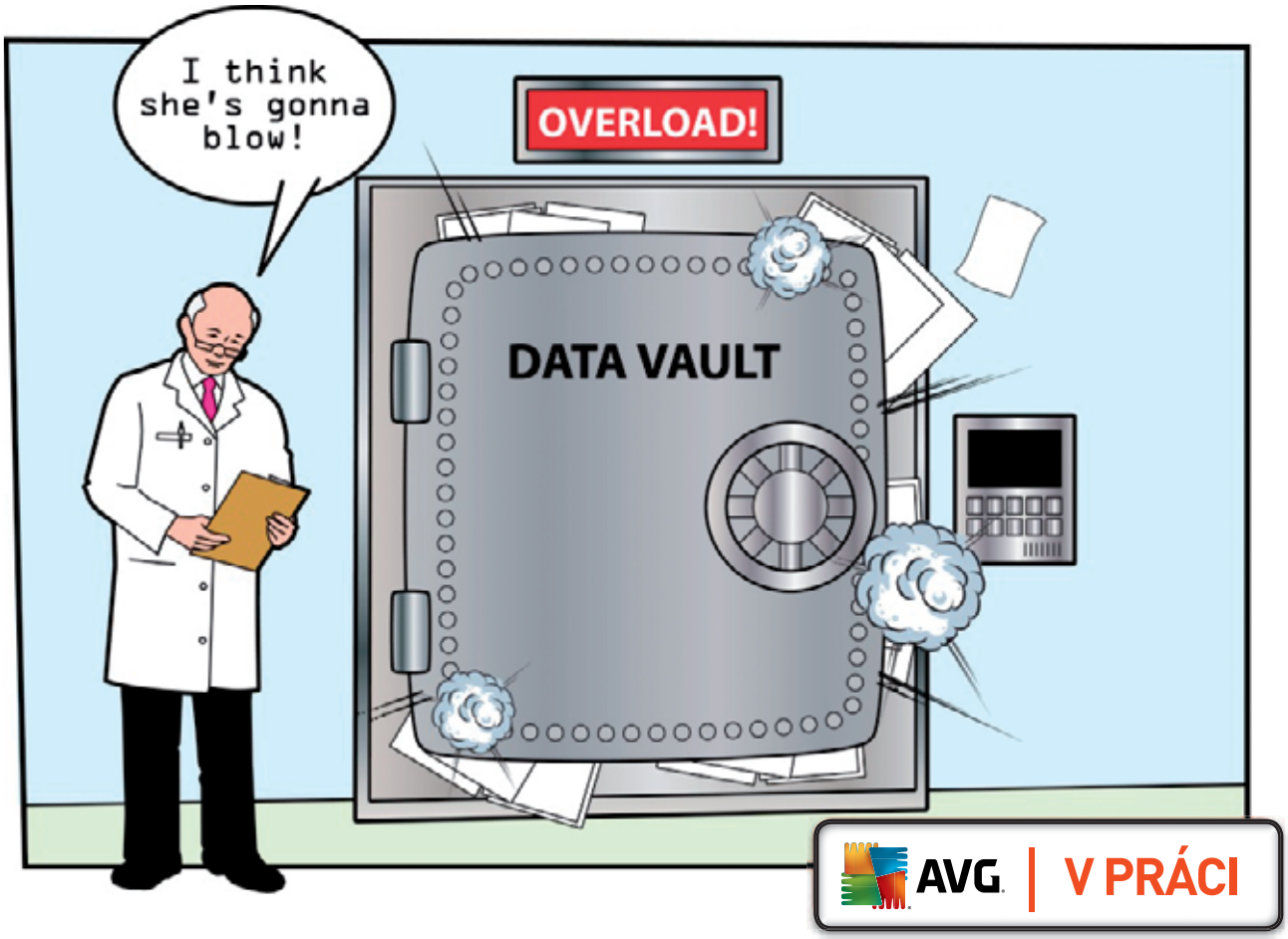
Zákazníci, zaměstnanci
a zainteresované strany:
kdo z nich utrpí následkem narušení dat?

AVG

Potřeba ochrany dat na vašem vlastním počítači je jasná, ale co s informacemi, které pro podnikání potřebujete a které se nenacházejí v dosahu vašeho oddělení IT?

Víte, že

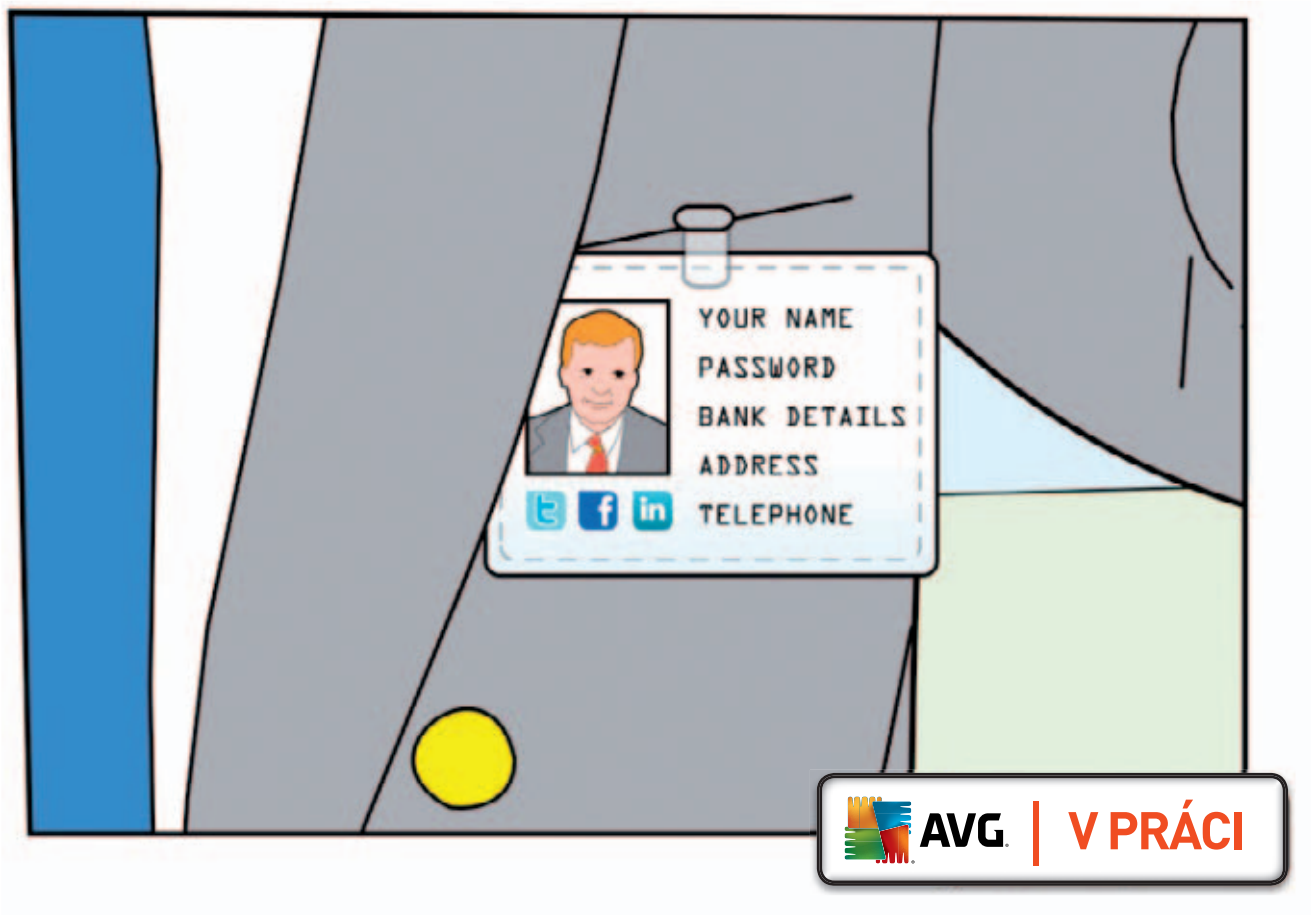
společnosti mohou dostat za neúčinnou ochranu uživatelských dat pokutu až do výše 500 000 liber? Podle nedávného průzkumu pouze 28 procent podniků zavedlo formální pravidla pro bezpečnost na internetu, ale u 330 milionů záznamů obsahujících citlivé osobní údaje došlo od roku 2005 k narušení zabezpečení dat.



Aktualizace antivirové ochrany, instalace bezpečnostních záplat a předpoklad, že jakýkoli pochybný odkaz na webu může být nebezpečný, to jsou jen některé ze způsobů, jak by se běžní počítačoví uživatelé měli chránit. Jaká rizika ale hrozí datům mimo naši kontrolu? Celá řada veřejných a soukromých společností uchovává důvěryhodné informace týkající se různých fází naší vzájemné spolupráce a my jim důvěřujeme, že tyto informace uchovávají v bezpečí. Občas bohužel důvěřujeme těm nesprávným lidem. Incidenty, při nichž dochází ke ztrátě nebo krádeži dat ze společnosti, jsou nazývány narušení dat. Tyto incidenty jsou na vzestupu. Nedávná studie organizace United States National Cyber Security Alliance zjistila, že 65 procent dotazovaných malých podniků uchovává data o zákaznících, přičemž 33 procent z nich připustilo uchovávání informací o kreditních kartách. Navzdory tomu, že dotazované společnosti připustily důležitost Internetu pro své fungování, pouhých 28 % z nich zavedlo formální pravidla pro bezpečnost na internetu. A co je závažnější, pouhých 35 % těchto společností uspořádalo pro své pracovníky školení v oblasti bezpečnosti na internetu a pouhých 14 % z nich mělo na zabezpečení svých informačních technologií vlastní pracovníky.

Velikost a charakteristiky typické společnosti, které hrozí narušení dat, lze definovat snadno. Toto riziko totiž hrozí všem podnikům. Nebezpečí průniku hackerů a výrazného narušení dat hrozí všem, od obyčejných obchodníků a firem se dvěma obchodními společníky až po vládní organizace a velké podniky. Hackeři své cíle nerozlišují. Vysvětlíme vám, proč. Malé společnosti mohou vlastnit větší množství cenných podnikových dat, která kybernetičtí zločinci chtějí získat. Tato data jsou obvykle chráněna relativně chatrným zabezpečením.

Britský úřad HMRC (Revenue and Customs Department) se stal terčem jednoho z ***nejznámějších úniků dat*** v poslední době, kdy byly po ztrátě dvou disků CD vystaveny riziku záznamy 25 milionů osob. Poté, co se tento incident provalil, došlo v úřadu HMRC a ve státním sektoru k policejnímu vyšetřování postupů ohledně dat, což vedlo z pohledu spotřebitele ke kladným výsledkům: Britský informační komisař získal více pravomocí a byl přijat zákon na ochranu dat, který stanovuje pravidla pro ochranu dat. ***Úřadu informačního komisaře (ICO)*** byla nedávno přidělena pravomoc k udělování pokut společnostem, které zanedbaly ochranu dat, až do výše 500 000 liber. „Správná ochrana dat nebyla nikdy tak důležitá, jako je tomu dnes," prohlásil informační komisař Christopher Graham. „Po občanech je čím dál častěji požadováno, aby prováděli transakce online – se státem, s bankami či jinými organizacemi. To vše vyžaduje použití rozsáhlých databází k uchovávání osobních údajů. Pokud se něco pokazí, narušení zabezpečení může způsobit citelné škody a velké potíže tisícům lidí."Úřad ICO radí, aby se britské podniky a spotřebitelé obrátili přímo na společnost, kterou podezřívají z nedostatečného zabezpečení dat nebo u které došlo k narušení dat. Pokud podniky či spotřebitelé neuspějí, úřad ICO může zasáhnout jejich jménem. „V případě nutnosti stížnost posoudíme. Pokud budeme mít podezření na porušení zákona, poskytneme dané společnosti potřebné rady a požádáme ji o odstranění problému. V nejzávažnějších případech jí to můžeme i nařídit," vysvětluje úřad ICO. Tato organizace ale nemá žádné pravomoci k přímému odškodňování.



Spojené státy americké podobně upravují legislativu, aby regulovaly společnosti s nedbalým přístupem k datům. Zákonodárci nedávno představili dva nové návrhy zákona, které společnosti nutí narušení dat hlásit – zákon o soukromí a bezpečnosti osobních dat z roku 2009 (S.1490) a zákon o oznamování narušení dat (S.139). Rovněž byl vytvořen kontrolní orgán s názvem Federální úřad pro ochranu identity, který je součástí Federálního výboru pro obchod. Zákonodárci byli motivováni, aby více usilovali o ochranu dat, což bylo dáno tím, že podle odhadů některých expertů došlo od roku 2005 k narušení zabezpečení dat u 330 milionů záznamů obsahujících citlivé osobní údaje. Kampaň ***StaySafeOnline*** americké organizace Cyber Security Alliance rázně varuje podniky, které neberou bezpečnost dat svých zákazníků příliš vážně. „Vaši zákazníci jsou váš byznys. Vědomě byste je sice nikdy nevystavili riziku, ale kvůli laxnímu přístupu k počítačové bezpečnosti se vám to může snadno povést," uvádí organizace. „Jak jsme mohli pozorovat u nedávných případů rozsáhlého narušení dat, zákazníkům se ztráty, krádeže či kompromitace jejich údajů příliš nelíbí. ***Ochrana citlivých dat vašich zákazníků*** je jednak dobrý postup a jednak dobrý byznys."

Z toho vyplývá, že podniková data jsou stejnou součástí jmění firmy jako její duševní vlastnictví, její pracovníci, její know-how a její pevné náklady, od koberců až po kopírky. Proto s nimi musí být nakládáno stejným způsobem. Firma si musí uvědomit důležitost tohoto základního přístupu k modernímu byznysu, v opačném případě mohou rovnou publikovat celou podnikovou databázi na webu a bude to mít stejný výsledek. Podniky nesou plnou odpovědnost za ochranu svého datového centra a dodržování stanovených pravidel ze strany těch, kteří k němu mají přístup.

Kampaň StaySafeOnline radí firmám, aby zavedly svá pravidla pro ochranu zákaznických dat. Rovněž prosazuje celou řadu opatření týkajících se zabezpečení vlastních informací podobných těm, která by měli uživatelé dodržovat doma. „Ochrana zákaznických dat vyžaduje, aby byly všechny vaše počítačové systémy plně chráněny," radí organizace. „Ani ta nejlepší pravidla na světě vaše zákazníky neochrání, pokud vaší síti nebo prostředkům hrozí riziko útoku nebo odvratitelných selhání." Ačkoli je dobré se řídit tím, co vláda podniká, aby se ujistila, že firmy svá data hlídají, je třeba také znát způsoby, jak se dozvědět o narušení dat společnosti, která přechovává vaše data. Dle amerického týmu CERT (Computer Emergency Readiness Team) existuje několik ***signálů, kterých je třeba si všímat***: – neobvyklé nebo nevysvětlitelné poplatky na účtech – telefonní hovory nebo faktury k účtům, produktům či službám, které nemáte – nedodržení pravidelných účtů či pošty ve stanovenou dobu – nové či nevysvětlitelné položky na fakturách – neočekávaná odmítnutí firemních kreditních karet. Pokud mají firmy na základě těchto signálů podezření, že jejich data mohla být u jiné společnosti vystavena útoku, měly by tuto společnost v případě nutnosti nejdříve telefonicky či písemně kontaktovat. Kontaktování hlavních společností zabývajících se hlášením problémů s kreditními kartami, jako jsou Equifax, Experian nebo TransUnion, je rovněž chytrý krok – stejně jako podání oznámení na místní policii. Díky tomu aspoň vznikne oficiální záznam události.

Také je třeba zvážit, zda narušení v jedné organizaci nebude mít dopad na jiné důvěrné informace. Tým CERT uvádí, že pokud například zloděj získá přístup k zaměstnancovu číslu sociálního pojištění, společnost by měla kontaktovat správu sociálního zabezpečení. Odpovědné oddělení podniku či samotní zaměstnanci by měli v případě krádeže řidičského průkazu nebo poznávací značky kontaktovat dopravní úřad. Existuje mnoho organizací a agentur, které vám mohou pomoci, pokud si myslíte, že vaše zaměstnanecká či podniková data nejsou správně chráněna. Jak to už ale chodívá, prevence je často účinnější než léčba. Pokud existuje mnoho kanálů, pomocí nichž může dojít k narušení vašich či zákaznických dat, nejlepším postupem je sdílet informace pouze s těmi společnostmi, kterým důvěřujete. Pokud tento přístup dokážete uplatnit jako standard pro pracovní postupy své společnosti a zajistíte jeho dodržování ze strany všech zaměstnanců, učiníte ten nejlepší krok k ochraně podnikových dat.

Nakonec se vraťme k naší úvodní otázce – Zákazníci, zaměstnanci a zainteresované strany: kdo z nich utrpí následkem narušení dat? Odpověď je nám teď zcela jasná. Následky útoků vedoucích k únikům dat pocítí všichni. Podniky z provozního hlediska utrpí potencionální ztrátu zisku, z níž následně vyjdou hůře akcionáři z řad podniků i jednotlivců. Zaměstnanci jsou kompromitování a zákazníci ztratí důvěru ve fungování společnosti, i přes snahu společnosti pracovat co nejlépe. Jedná se o bludný kruh a cestu do pekel. Přitom se tomu všemu dá předcházet. Ochraňte svá data ještě dnes!

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