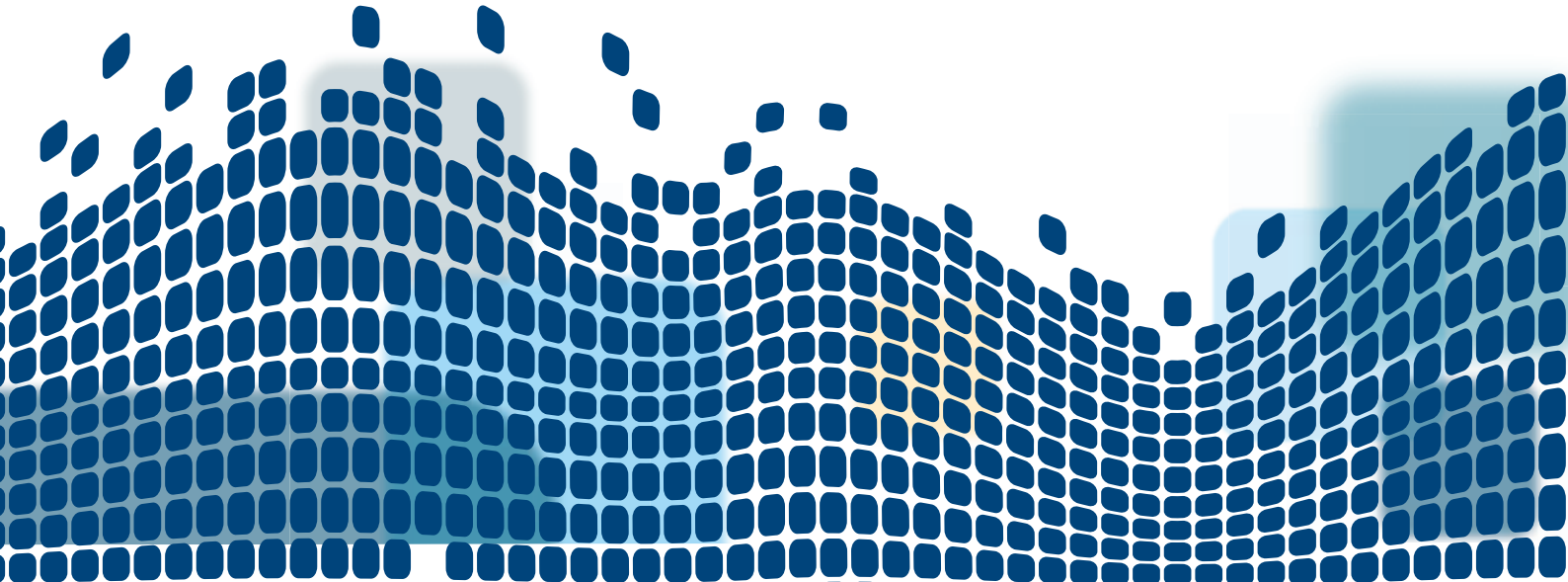
AVG V PRÁCI

Small Business Průvodci zabezpečením

Pět kroků pro zabezpečení webových stránek vašeho podniku a jejich obsahu



Pět kroků pro zabezpečení webových stránek vašeho podniku a jejich obsahu

Pokud podnikáte na Internetu, je váš podnik a jeho reputace vystavena většímu množství hrozeb. A čím jste úspěšnější, tím častěji se vaše webové stránky stávají terčem zločinců.

Zločinci se pokusí proniknout na váš web a použít jej k nalákání uživatelů na škodlivé stránky nebo na vaše stránky nainstalují programy typu exploit stahující data bez vědomí uživatele. Každý den se jim to daří na stovkách tisíc webových stránek.

Určitě nechcete, aby na váš web někdo pronikl, protože jste vynaložili značné investice do optimalizace pro vyhledávače (SEO) a marketingu ve vyhledávačích (SEM). O dobré jméno značky i loajalitu zákazníků můžete přijít ze dne na den.

Zločinci se rovněž pokusí využít chyb ve vašem webovém softwaru k tomu, aby se dostali k informacím o zákaznících v používaných databázích nebo aby zrealizovali podvodné transakce.

Společnost AVG právě uvedla do provozu informační portál, který vám pomůže zjistit, zda je váš web dobře zabezpečený. **Nástroj AVG Threat Labs** vám poskytne přehled o stavu webu v reálném čase, informaci, zda byl napaden, a pokud ano, jakým škodlivým kódem a z jakého zdroje.

Máte-li obavy o bezpečnost svého webu, zkontrolujte jej pomocí nástroje Threat Labs.

Pokud byl web napaden, můžete provést nutná opatření. Jakmile budou mezery v zabezpečení odstraněny, nástroj Threat Labs váš web vyhodnotí jako bezpečný. Další informace o nástroji Threat Labs pro provozovatele webů najdete **v Častých dotazech k nástroji Threat Labs**.

Základy pro podniky:

Pět kroků pro zabezpečení webových stránek vašeho podniku a jejich obsahu

1 Je možné, že jste vyvinuli vlastní řešení online. Pravděpodobně však využíváte služeb externího poskytovatele webových aplikací nebo řešení open source, jako jsou WordPress, phpBB, ZenCart apod. Ať už používáte jakékoli řešení, je třeba, abyste zajistili, že osoby odpovědné za zdrojový kód webu, provádění instalací a průběžnou správu jsou plně obeznámeny se **seznamem 25 nejnebezpečnějších softwarových chyb dle CWE/SANS za rok 2010**.

Musí problémům porozumět, zavést opatření k jejich zmírnění a provádět kontrolu funkčnosti těchto opatření. Naštěstí tzv. devět „monster mitigations“, uvedených ve výše zmiňovaném dokumentu, účinně odstraní nebo alespoň sníží závažnost 25 největších problémů a navíc ošetří mnoho dalších slabých míst, která v tomto seznamu nejsou uvedena.

2 Zajistěte, aby servery, které hostují váš web, byly neustále aktualizovány pomocí nejnovějších aktualizací softwaru a internetového zabezpečení. Zajistěte, aby byly aktualizovány i veškeré webové aplikace třetích stran či open source. Balíčky zabezpečení instalujte, jakmile jsou k dispozici.

3 Stejný postup proveďte se svou podnikovou sítí a s počítači v této síti. Dobré rady, jak správně postupovat, najdete v dokumentu „**35 strategií, jak zmírnit cílené kybernetické útoky**“ od australského vládního úřadu Defence Signals Directorate.

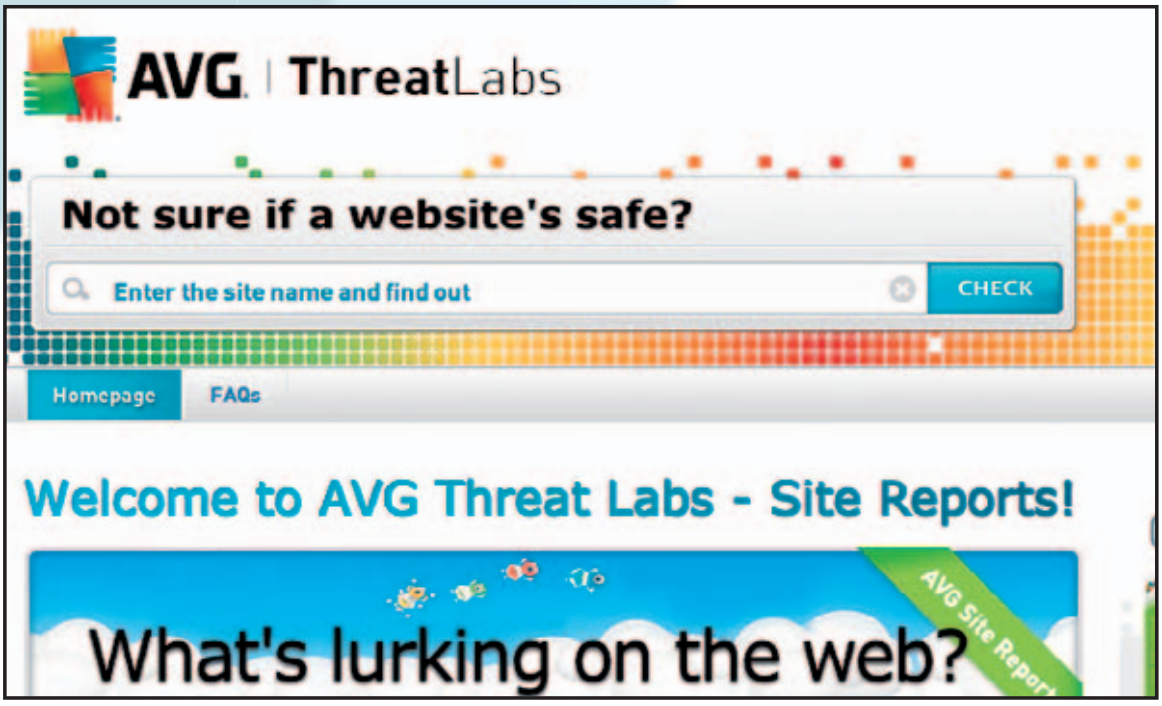
4 Zajistěte, aby se přístupová hesla k účtům pro správu webhostingu a administrativním částem vaší webové aplikace pravidelně měnila a aby se používala pouze „silná“ hesla. Více informací naleznete v dokumentu „**Pokyny ke zvolení správného hesla**“.

5 Ujistěte se, že znáte veškeré příslušné normy, požadavky nařízení a právní důsledky, včetně požadavků státu na ochranu soukromí a dat. Tyto požadavky se mohou v různých oblastech či zemích lišit. Pokud přijímáte, ukládáte nebo předáváte údaje o kreditních nebo debetních kartách, musíte splňovat požadavky standardu PCI. Více informací naleznete na webu organizace PCI.

Nejedná se o jednorázové záležitosti. Podnikání na Internetu vyžaduje značnou opatrnost, přičemž existuje několik dalších obvyklých chyb zabezpečení, kterých by si firmy měly být vědomy.

Musíte si dávat pozor na podvodné transakce. Přistupujte s podezřením ke všem objednávkám, které předpokládají platbu kreditní kartou a požadují odeslání zboží do zahraničí. Můžete dokonce zakázat pro zásilky do zahraničí platbu kreditní kartou online.

Požadujte platbu prostřednictvím služby PayPal, bankovního převodu nebo jiným bezpečnějším způsobem. Doporučujeme rovněž zvážit, zda nezablokujete veškeré objednávky z rizikových zemí, včetně rozvojových států, jako je Indonésie, Malajsie, Benin, Nigérie, Pákistán, Izrael, Egypt, Indie, Čína a některé východoevropské země. Další informace naleznete v dokumentu „31 způsobů, jak se vyhnout podvodům s kreditními kartami“.



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