

Guides de sécurité pour les petites entreprises

Principaux conseils
pour sécuriser la
réputation de votre
entreprise

Principaux conseils pour sécuriser la réputation de votre entreprise

J'ai lu avec intérêt les rapports récents indiquant qu'un piratage sur Twitter avait touché certaines personnalités politiques bien connues, en émettant des Tweets embarrassants à partir de leurs comptes personnels. Même si ces gros titres peuvent sembler amusants, il faut tenir compte de l'impact potentiel de ce genre de piratage pour la réputation de votre entreprise. La réputation est l'atout majeur d'une petite entreprise et il faut souvent des années pour l'établir. Le fait d'être la cible d'un piratage de ce genre peut avoir un effet négatif sur la réputation de votre entreprise. Dans une enquête récente de la NCSA (National Cyber Security Alliance) portant sur la sécurité des petites entreprises, 69 % des propriétaires de PME ont déclaré qu'ils informeraient leurs clients s'ils étaient victimes d'une brèche de sécurité, alors que près de la moitié d'entre eux ont avoué que leurs clients étaient inquiets quant à la sécurité informatique de leur entreprise portant sur la sécurité des petites entreprises, 69 % des propriétaires de PME ont déclaré qu'ils informeraient leurs clients s'ils étaient victimes d'une brèche de sécurité, alors que près de la moitié d'entre eux ont avoué que leurs clients étaient inquiets quant à la sécurité informatique de leur entreprise.



Savoir que l'infrastructure informatique d'un fournisseur n'est pas aussi sécurisée qu'elle devrait l'être inquiéterait la plupart des gens, notamment s'ils partagent des données professionnelles stratégiques avec ce fournisseur/cette entreprise. Pourtant, à l'heure où tant d'entreprises utilisent des réseaux sociaux économiques pour faire leur publicité, la menace concernant l'envoi de messages inappropriés à vos clients par le compte d'un réseau social d'un ou plusieurs de vos employés est bien réelle et son impact potentiel sur votre réputation (en détruisant la confiance de votre client en votre aptitude à protéger ses données) est énorme.

Par conséquent, pour préserver la réputation de votre entreprise, voici quelques conseils qui vous permettront de bénéficier au mieux de votre logiciel de sécurité en vous permettant de vous concentrer sur le renforcement de votre réputation et non sur les moyens de la réparer :

1. Assurez-vous que votre logiciel de sécurité est robuste et à la hauteur de la tâche. AVG software est certifié par les plus grands organismes indépendants de certification de sécurité comme étant efficace contre une multitude de menaces.
2. Sécurisez votre réseau contre le comportement périlleux des employés. Vous ne pouvez pas toujours contrôler les sites Internet consultés par vos employés au bureau (si c'était le cas, vous auriez sans doute une rébellion sur les bras). AVG Business Edition contient LinkScanner® qui empêche les utilisateurs de consulter des sites Web infectés susceptibles de laisser des pirates infiltrer votre réseau. Assurez-vous donc que ce logiciel est installé sur chaque PC.
3. Réglez votre logiciel de sécurité pour qu'il se mette à jour au moins une fois par jour. Protégez-vous des virus nouveaux et inconnus qui surgissent entre deux mises à jour en vous assurant que AVG Data Protection est actif sur tous les postes de travail. AVG Business Edition Internet Security contient le module Data Protection.
4. Veillez à définir le niveau de sécurité le plus élevé sur les ordinateurs portables que les employés emportent chez eux ou en déplacement. Une fois déconnectés du réseau, ces PC échappent à votre contrôle. Utilisez donc la puissance des modules de mise à jour Internet d'AVG pour maintenir la solidité de leur protection.
5. Traitez les problèmes de sécurité informatique dès qu'ils apparaissent. AVG peut vous alerter dès qu'il détecte un problème – de jour comme de nuit – et prendre les mesures nécessaires pour protéger automatiquement votre réseau : vous n'avez rien à faire. Si vous avez le temps, consultez le fichier journal : il peut vous fournir des informations précieuses à propos de la formation des employés ou d'autres mesures préventives qui contribueront à améliorer la sécurité.

La réputation de votre entreprise a-t-elle souffert d'un piratage en ligne ? Quelles mesures avez-vous prises pour empêcher qu'il ne se répète ?



AVG SMB group :
bit.ly/AVGSMB



Devenez fan d'AVG :
facebook.com/avgfree



Lisez nos blogs :
blogs.avg.com



Suivez-nous sur :
twitter.com/officialAVGnews



Devenez un affilié
AVG :
avg.com/gb-en/affiliate



Regardez notre chaîne :
youtube.com/user/officialAVG

AVG Technologies France

1, Place de la Chapelle
64600 Anglet
France
www.avg.fr

AVG Technologies UK, Ltd.

Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
Royaume-Uni
www.avg.co.uk

AVG Technologies CZ, s.r.o.

Lidická 31, 602 00 Brno
République Tchèque
www.avg.cz

AVG Technologies GER GmbH

Bernhard-Wicki-Str. 7
80636 München
Allemagne
www.avg.de

AVG Technologies USA, Inc.

1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
États-Unis
www.avg.com/us-en/homepage

AVG Technologies CY Ltd.

Arch. Makariou III.
2-4 Capital Centre
1505, Nicosie, Chypre
www.avg.com

