

Guides de sécurité pour les petites entreprises

Cinq étapes pour
sécuriser le site Web de
votre entreprise et son
contenu

Cinq étapes pour sécuriser le site Web de votre entreprise et son contenu

Si vous dirigez une entreprise en ligne, les menaces qui pèsent sur votre entreprise et votre réputation sont beaucoup plus nombreuses. Et plus vous aurez de succès, plus il est probable que des personnes malveillantes s'attaquent à votre site Web.

Les criminels tenteront de pirater votre site Web et de l'utiliser pour hameçonner des utilisateurs vers des pages Web infectées, ou même de pirater votre site Web et de placer des exploits de téléchargement dans vos pages Web. Ils réussissent ainsi à infecter des centaines de milliers de pages Web par jour.

Il faut éviter que votre site Web ne soit piraté ainsi, car tout l'argent que vous avez investi dans l'optimisation pour les moteurs de recherche (SEO), le marketing des moteurs de recherche (SEM), la réputation de la marque et la fidélisation des clients peut s'envoler du jour au lendemain.

Les pirates tenteront également d'exploiter les erreurs logicielles du site Web pour accéder aux informations des clients dans les bases de données utilisées par le site Web, ou d'effectuer des transactions frauduleuses.

AVG vient de lancer un portail d'information en ligne qui vous aidera à déterminer si votre site Web est sécurisé ou pas. [AVG Threat Labs](#) vous offre un rapport de site pour connaître l'état en temps réel de votre site, savoir s'il a été compromis, si oui, par quoi et d'où provient le code malveillant.

Si vous avez des craintes pour la sécurité de votre site Web, consultez [Threat Labs](#).

Si le site a été compromis, vous pouvez prendre des mesures et dès que les problèmes de sécurité seront résolus, Threat Labs indiquera à nouveau que le site est sûr. Pour plus d'informations à propos de Threat Labs pour les propriétaires de sites Web, consultez cette [Threat Labs FAQ](#).



Les bases de l'entreprise :

Cinq étapes pour sécuriser le site Web de votre entreprise et son contenu

1. Peut-être développez-vous vos propres solutions en ligne. Il est plus probable que vous utilisiez un fournisseur d'applications Web externe ou simplement des solutions en open source telles que WordPress, phpBB, ZenCart etc. Quoi qu'il en soit, vous devez vous assurer que les personnes chargées du code du site Web, de son installation et de sa gestion continue connaissent parfaitement la [liste 2010 CWE/SANS des 25 erreurs logicielles les plus dangereuses](#).

Il est indispensable qu'ils comprennent les problèmes, mettent en place les mesures d'atténuation nécessaires pour y remédier et continuent à vérifier leur bon fonctionnement. Fort heureusement, les neuf « principales mesures d'atténuation » figurant dans le document ci-dessus sont efficaces pour éliminer ou réduire la gravité des 25 principaux problèmes et pour traiter de nombreuses lacunes qui ne figurent même pas dans la liste.

2. Assurez-vous que les serveurs qui hébergent votre site Web sont tenus à jour avec les dernières mises à jour des logiciels et l'installation de logiciels de sécurité Internet. Veillez à ce que les éventuelles applications tierces ou en open source soient également tenues à jour. Appliquez les éventuels correctifs de sécurité dès qu'ils sont disponibles.
3. Procédez maintenant de la même manière sur votre propre réseau professionnel et les PC qui y sont connectés. Pour trouver d'excellents conseils sur la procédure à suivre, consultez le document « [35 stratégies à appliquer pour atténuer les cyber-intrusions ciblées](#) » publié par le Defence Signals Directorate du gouvernement australien.
4. Assurez-vous que les mots de passe utilisés pour accéder à vos comptes d'hébergement sur le

Web et les zones d'administration de vos logiciels d'applications Web sont régulièrement changés et sont « solides ». Voir « [Le Guide des bonnes pratiques des mots de passe](#) ».

5. Vérifiez que vous êtes familiarisé avec toutes les normes pertinentes, les exigences de conformité et les implications juridiques, y compris les exigences de votre gouvernement en matière de confidentialité et de protection des données.
6. Ces règles peuvent varier selon les territoires et les pays. Si vous acceptez, stockez ou transmettez des données de cartes de crédit ou de débit, vous devez être compatible PCI : consultez le [site Web de PCI](#) pour plus d'informations.

Il ne s'agit pas d'une vérification ponctuelle. Elle nécessite une vigilance extrême et il existe de nombreuses autres lacunes de sécurité courantes dont les entreprises qui opèrent en ligne doivent avoir connaissance.

Vous devez être constamment à l'affût des transactions frauduleuses. Traitez avec méfiance toute commande réglée par carte de crédit et vous invitant à expédier des produits à l'étranger. Vous

pouvez aller jusqu'à interdire les règlements par carte de crédit pour les expéditions à l'étranger.

Invitez vos clients à utiliser PayPal, un virement bancaire ou un autre moyen de paiement plus sécurisé. Vous pouvez même envisager de bloquer toutes les commandes émanant de pays à risque, y compris certaines nations en développement comme l'Indonésie, la Malaisie, le Bénin, le Nigeria, Israël, l'Égypte, l'Inde, la Chine et certains pays d'Europe de l'Est. Pour plus d'informations à ce sujet, vous pouvez consulter le document « [31 moyens de minimiser les fraudes à la carte de crédit](#) ».





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/affiliate



Regardez notre chaîne :
youtube.com/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

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

 **AVG. AU TRAVAIL**

© 2011 AVG Technologies France. Tous droits réservés. AVG est une marque déposée d'AVG Technologies CZ, s.r.o.