# Guides de sécurité pour les petites entreprises

Clients, employés et entreprises :
**Qui souffre le plus d'une brèche des données ?**

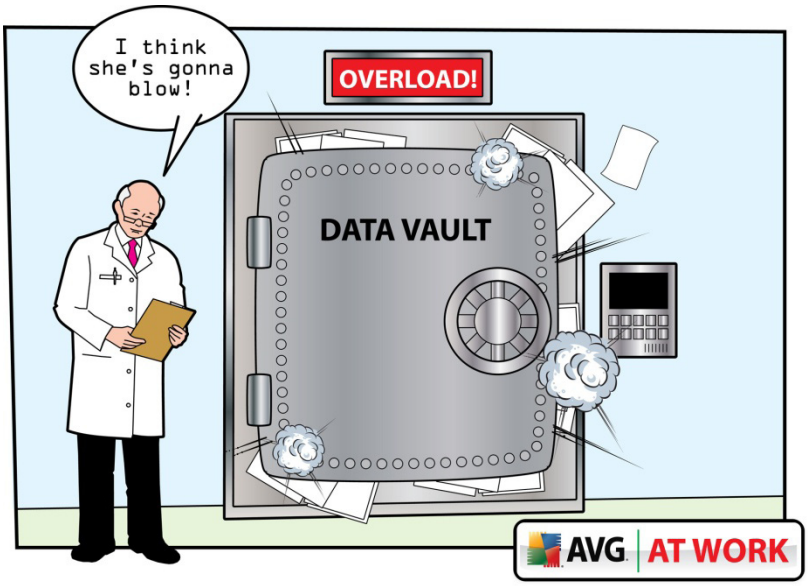
AVG AU TRAVAIL

# Clients, employés et entreprises : Qui souffre le plus d'une brèche des données ?

La protection des données présentes sur votre ordinateur est relativement simple, mais qu'en est-il des informations auxquelles votre entreprise se connecte et qui échappent au contrôle de votre service informatique ?

**Le saviez-vous**

- Les entreprises encourent une amende pouvant atteindre 571 000 € pour ne pas avoir correctement protégé les données de leurs clients
- Seules 28 pour cent des entreprises interrogées lors d'une enquête récente avaient mis en place des stratégies formelles concernant la sécurité sur Internet
- 330 millions de fichiers contenant des informations personnelles sensibles ont fait l'objet de brèches de sécurité des données depuis 2005




Pour assurer leur sécurité, les utilisateurs moyens de PC devraient notamment mettre à jour leur protection par antivirus, installer les correctifs de sécurité et éviter tous les liens qui leur semblent douteux. Toutefois, quels sont les risques pour les données qui échappent à notre contrôle centralisé ? De très nombreuses entreprises des secteurs public et privé détiennent des informations confidentielles à propos de différents éléments de notre société, et nous leur faisons confiance pour assurer leur sécurité. Malheureusement, cette confiance n'est pas toujours justifiée.

Les incidents de perte ou de vol de données dans une entreprise sont appelés brèches des données et leur nombre est en augmentation. Une étude récente réalisée par la United States National Cyber Security Alliance a révélé que 65 pour cent des petites entreprises interrogées détiennent des données concernant leurs clients et 33 pour cent d'entre elles ont reconnu stocker des informations relatives à des cartes de crédit. Même si elles reconnaissent qu'Internet est essentiel à leur activité, seules 28 pour cent des entreprises interrogées ont déclaré avoir mis en place des stratégies formelles de sécurité sur Internet. Plus inquiétant encore, seules 35 pour cent des entreprises ont déclaré organiser des formations à la sécurité sur Internet pour leur personnel, et 14 pour cent des entreprises seulement ont précisé qu'elles disposent d'un collaborateur qui se consacre uniquement à la sécurité sur Internet.

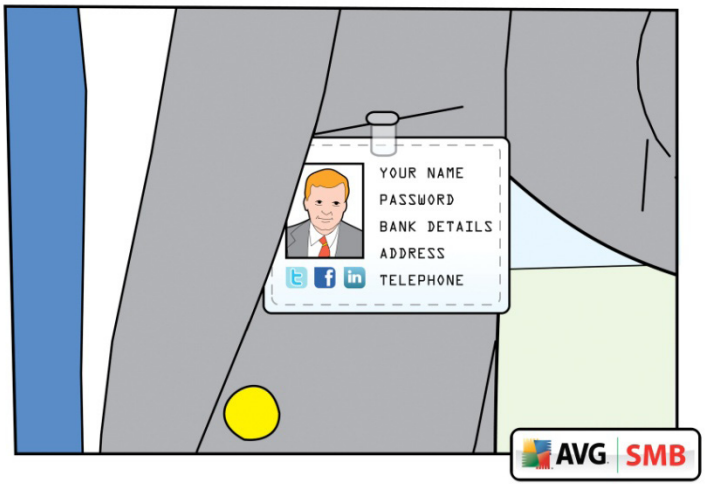
La taille et les caractéristiques de l'entreprise typique la plus susceptible de faire

l'objet d'une brèche de données sont faciles à définir : toutes les entreprises sont concernées. Des petits commerçants et des partenariats à deux personnes jusqu'aux grands services administratifs et aux sociétés multinationales, les pirates qui se livrent à des intrusions aboutissant à des brèches de données ne font aucune distinction. Ils ne sélectionnent pas leurs cibles et voici pourquoi. Une petite entreprise peut détenir un grand nombre de données sensibles que les cybercriminels souhaiteront « récupérer », tout en ne disposant que d'une couche de sécurité des données relativement faible et poreuse pour se protéger.

Le ministère britannique des douanes et du revenu (HMRC) a fait l'objet d'une des violations de données les plus tristement célèbres de l'histoire récente, lorsque des dossiers concernant environ 25 millions de personnes ont été exposés à la suite de la disparition de deux CD. Les retombées qui ont suivi ont abouti à une enquête juridique portant sur les pratiques de manipulation des données en place au HMRC et dans l'ensemble des secteurs administratifs et à un résultat positif pour les consommateurs : un renforcement des pouvoirs du Commissaire de l'information britannique et de la Loi sur la protection des données qu'il est chargé de réglementer et d'appliquer.

L'ICO (Information Commissioner's Office) est désormais à même d'infliger aux entreprises des amendes pouvant atteindre 571 000 €, s'il s'avère qu'elles ont fait preuve de négligence dans la protection des données. « L'obtention du droit de protection des données n'a jamais été aussi importante qu'aujourd'hui », déclare le Commissaire de l'information, Christopher Graham. « En tant que citoyens, nous sommes de plus en plus fréquemment invités à effectuer des transactions en ligne, que ce soit avec l'administration, les banques et autres organismes utilisant d'énormes bases de données pour stocker nos informations personnelles. Lorsque les choses se passent mal, une brèche de sécurité peut s'avérer catastrophique et occasionner des préjudices considérables à des milliers de personnes. »

Le Commissaire de l'information conseille aux entreprises et aux particuliers britanniques de prendre contact directement avec toute entreprise qu'ils soupçonnent d'exercer un contrôle trop faible sur les données ou pire encore, d'avoir été victime d'une brèche de données. Si cette approche initiale n'aboutit pas à des mesures, le Commissaire de l'information peut alors intervenir pour le compte de l'entreprise ou du consommateur. « Au besoin, nous examinons la plainte. Si nous soupçonnons une infraction à la loi, nous pouvons donner des conseils à l'entreprise et lui demander de remédier au problème. Dans les cas les plus sérieux, nous pouvons lui en donner l'ordre », précise le Commissaire de l'information. Toutefois, l'organisation n'a pas le pouvoir d'octroyer directement tout type de compensation.




De leur côté, les États-Unis renforcent également la législation afin de réguler les entreprises qui se montrent négligentes avec les informations. Le législateur a récemment voté deux nouvelles lois visant à imposer aux entreprises de faire preuve de transparence en matière de brèches de données : la loi Personal Data Privacy and Security Act de 2009 (S.1490) et la loi Data Breach Notification Act (S.139). Un organisme de mise en application a également été constitué : il s'agit de l'Office of Federal Identity Protection, lequel fait partie de la Federal Trade Commission. Le législateur tenait à resserrer les efforts de protection des données, compte tenu du fait que certains experts estimaient que 330 millions de fichiers contenant des informations personnelles sensibles avaient fait l'objet de brèches de sécurité depuis 2005.

La campagne menée par la Cyber Security Alliance www.staysafeonline.org aux États-Unis a constitué un avertissement très solennel pour les entreprises qui ne prennent pas au sérieux la sécurité des informations de leurs clients. « Vos clients sont notre affaire. Vous ne les exposeriez jamais sciemment à des risques, mais des pratiques de sécurité informatique trop négligentes peuvent aboutir au même résultat », affirme l'organisation. « Comme nous l'ont démontré les récentes brèches de données très importantes, les clients n'apprécient pas que leurs informations soient perdues, volées ou compromises. Protéger les données sensibles de vos clients est à la fois une bonne stratégie et un atout commercial.

Dans ce cas précis, le message est le suivant : les données de l'entreprise font partie de ses actifs, au même titre que sa propriété intellectuelle, son personnel et sa base de compétences, ou encore ses biens mobiliers, des tapis à la photocopieuse, et elles doivent être traitées comme telles. Le fait de ne pas comprendre la gravité de ce principe essentiel des entreprises modernes équivaut à publier l'intégralité de la base de données de l'entreprise sur la page d'accueil du site Web de la société. Les entreprises ont pour responsabilité commerciale de fermer la porte du centre de données, de la maintenir verrouillée et de veiller à ce que des stratégies régissent le choix des personnes qui détiennent la clé.

StaySafeOnline conseille aux entreprises de mettre en place des stratégies visant à protéger les données de leurs clients, mais recommande également une série de mesures similaires à celles que certains particuliers devraient adopter en matière de sécurisation de leurs propres informations. « Le maintien de la sécurité de vos clients requiert une sécurisation totale de vos propres systèmes informatiques », explique l'organisation. « Les meilleures stratégies au monde ne protégeront pas vos clients si

votre réseau et vos ressources sont exposés à des risques d'attaques ou de pannes qui auraient pu être prévenues. »

Même s'il est utile de garder une longueur d'avance sur les mesures prises par le gouvernement pour s'assurer que les entreprises protègent vos données, il est tout aussi important de savoir si une entreprise qui détient des informations concernant la vôtre a fait l'objet d'un piratage. Selon l'équipe américaine de préparation aux urgences informatiques, la US Computer Emergency Readiness Team (CERT), il existe certains indices significatifs à détecter :

- dépenses inhabituelles ou inexplicables sur les factures
- appels téléphoniques ou factures concernant des comptes, des produits ou des services que vous ne possédez pas
- non-réception de vos factures régulières ou de votre courrier
- nouveaux comptes étranges apparaissant sur les factures
- rejet inattendu des cartes de crédit de l'entreprise

En fonction de ces signes, si les entreprises américaines soupçonnent que leurs informations peuvent avoir été exposées à une attaque de sécurité, elles devraient, dans l'exemple britannique, prendre contact avec la société concernée d'abord par téléphone, puis par courrier, le cas échéant. Il est également utile de contacter les principales sociétés de surveillance des crédits – Equifax, Experian et TransUnion – et de porter plainte auprès de la police locale afin que l'incident soit officiellement enregistré.

Il convient en outre de se demander si une brèche dans une entreprise a pu avoir un impact sur d'autres informations confidentielles. Le CERT recommande par exemple que, si un pirate a accédé au numéro de Sécurité Sociale d'un employé, l'entreprise prenne contact avec l'administration de la Sécurité Sociale. Le service du personnel de l'employé lui-même devrait également contacter le service des véhicules en cas de vol d'un permis de conduire ou d'une carte grise.

De nombreux organismes et agences peuvent vous aider si vous pensez que les données de vos employés ou de votre entreprise n'ont pas été correctement protégées, mais, comme dans bien d'autres domaines, mieux vaut prévenir que guérir. Par conséquent, lorsqu'il existe de nombreux canaux pouvant permettre à des pirates de voler vos données et celles de vos clients, la meilleure approche consiste à ne communiquer vos informations qu'à des entreprises auxquelles vous faites confiance. Si vous pouvez normaliser cette pratique dans les procédures opérationnelles principales de votre entreprise et vous assurer que ces méthodes sont communiquées à l'ensemble du personnel, vous adopterez les mesures les plus sûres possible pour préparer l'avenir.

En conclusion, revenons à notre première question : clients, employés et parties prenantes : qui souffre le plus d'une brèche des données ? La réponse devrait être claire maintenant. Tout simplement, tout le monde souffre des agissements des pirates qui aboutissent à des fuites de données. Sur le plan opérationnel, l'entreprise souffre directement de la perte potentielle de bénéfices commerciaux, ce qui nuit à la fois à l'entreprise et aux parties prenantes. Les données des employés sont compromises et les clients perdent confiance en l'aptitude de l'entreprise à fonctionner à un niveau vaguement proche des bonnes pratiques. Il s'agit d'un cercle vicieux et d'une spirale descendante, mais le plus regrettable est que cela aurait pu être évité. Nous vous invitons à verrouiller vos données dès maintenant.

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 CZ, s.r.o.**
Lidická 31, 602 00 Brno
République Tchèque
www.avg.cz

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

**AVG Technologies UK, Ltd.**
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
Royaume-Uni
www.avg.co.uk

**AVG Technologies GER GmbH**
Bernhard-Wicki-Str. 7
80636 München
Allemagne
www.avg.de

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


AVG AU TRAVAIL