Guides de sécurité pour les petits entreprises

Comment les logiciels malveillants peuvent s'infiltrer dans les réseaux de votre entreprise et que faire pour y remédier

AVG AU TRAVAIL

Comment les logiciels malveillants peuvent s'infiltrer dans les réseaux de votre entreprise et que faire pour y remédier

Il existe une multitude de voies pouvant permettre aux virus, chevaux de Troie et autres types de codes malveillants de s'infiltrer dans votre entreprise et il est utile de se tenir informé à leur sujet.

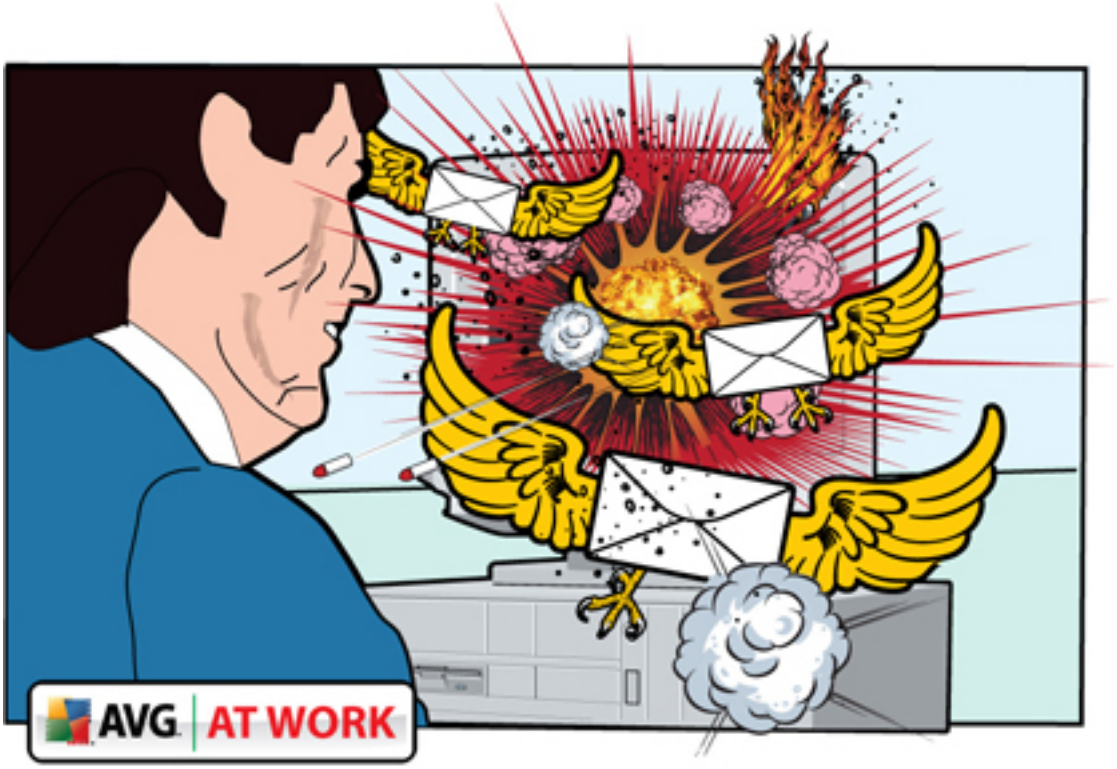
Le saviez-vous

- Quarante pour cent des entreprises permettent l'accès aux réseaux sociaux, mais seulement 23 pour cent disposent de stratégies de sécurité spécifiques
- Soixante-dix des 100 principaux sites Web ont hébergé des codes malveillants ou contenaient un lien vers des sites malveillants
- Le piratage Wi-Fi est la pratique consistant à chasser et à exploiter les réseaux sans fil non sécurisés

Le blocage complet de l'accès des utilisateurs à Internet pourrait permettre de maintenir les virus et autres logiciels malveillants hors de votre entreprise, mais cela ne serait pas très favorable à votre activité. Vous devez donc avoir conscience des moyens que les pirates peuvent utiliser pour accéder à vos informations précieuses – et prendre des mesures pour vous protéger.

Voici un aperçu des principales menaces et de la protection à utiliser contre elles.

1. Messagerie et spam : anciens, mais redoutables
La méthode choisie par les premiers auteurs de virus consistait à placer leurs produits dangereux dans des pièces jointes. Même si cela reste un mode d'attaque répandu, le niveau de prise de conscience concernant les logiciels malveillants envoyés par e-mail, ainsi que le renforcement des technologies de détection des virus, le rendent moins efficace qu'autrefois. « La messagerie était le principal vecteur des attaques et la simple installation d'un antivirus et la prudence lors de l'ouverture des pièces jointes ont permis d'atténuer la plupart de ces menaces », explique AVG dans son livre blanc intitulé « Pourquoi les solutions classiques contre les logiciels malveillants ne suffisent pas. »



La formation des employés à une bonne étiquette de sécurité de la messagerie est fondamentale et le CERT du gouvernement américain recommande aux utilisateurs de se méfier des e-mails non sollicités, même s'ils proviennent d'un contact connu. « De nombreux virus sont capables de « pirater » l'adresse de l'expéditeur, donnant ainsi l'impression que le message provient de quelqu'un d'autre. Si possible, vérifiez avec le prétendu expéditeur du message qu'il s'agit d'un e-mail légitime avant d'ouvrir toute pièce jointe », conseille l'organisation.

Les autres automatismes à enseigner au personnel comprennent la désactivation des options permettant de télécharger automatiquement les pièces jointes lorsque c'est possible. « Pour simplifier le processus de lecture des e-mails, bon nombre de programmes de messagerie permettent de télécharger automatiquement les pièces jointes. Vérifiez vos paramètres pour voir si votre logiciel propose cette option et assurez-vous qu'elle est désactivée », recommande le CERT américain.

2. Messagerie instantanée – Des conversations qui peuvent provoquer bien des problèmes

Même si elle n'est pas aussi répandue que l'e-mail, la messagerie instantanée (MI) présente certains risques de sécurité identiques pour les entreprises qui l'ont adoptée. Comme dans le cas des e-mails, des virus et autres logiciels malveillants peuvent être masqués dans des fichiers envoyés par MI. Certains employés peuvent ne pas être familiarisés avec la MI, et par conséquent, de cliquer sans se méfier sur des pièces jointes infectées : c'est la raison pour laquelle une formation s'impose. Microsoft dispense des conseils utiles à ce sujet et avertit les utilisateurs de ne jamais cliquer sur un fichier envoyé par un inconnu. Pour fermer la porte aux logiciels malveillants transmis par la MI, il faut également s'assurer que la messagerie des utilisateurs ne peut pas être identifiée facilement par leur nom d'utilisateur de MI. « Certains services de MI lient votre nom d'écran à votre adresse e-mail lorsque vous vous inscrivez. L'accès facile à votre adresse e-mail peut provoquer une augmentation des messages indésirables et des attaques par hameçonnage », avertit Microsoft.

3. Sites Web / réseaux sociaux – Pourquoi il est utile d'être antisocial

Constatant que la prise de conscience des dangers liés à l'ouverture de pièces jointes suspectes augmentait, les cybercriminels ont cherché de nouveaux moyens de répandre les codes malveillants. L'hébergement de logiciels malveillants sur des sites Web qui peuvent in-

fecter votre ordinateur en cas de simple consultation présente aujourd'hui une menace croissante pour les particuliers comme pour les entreprises.

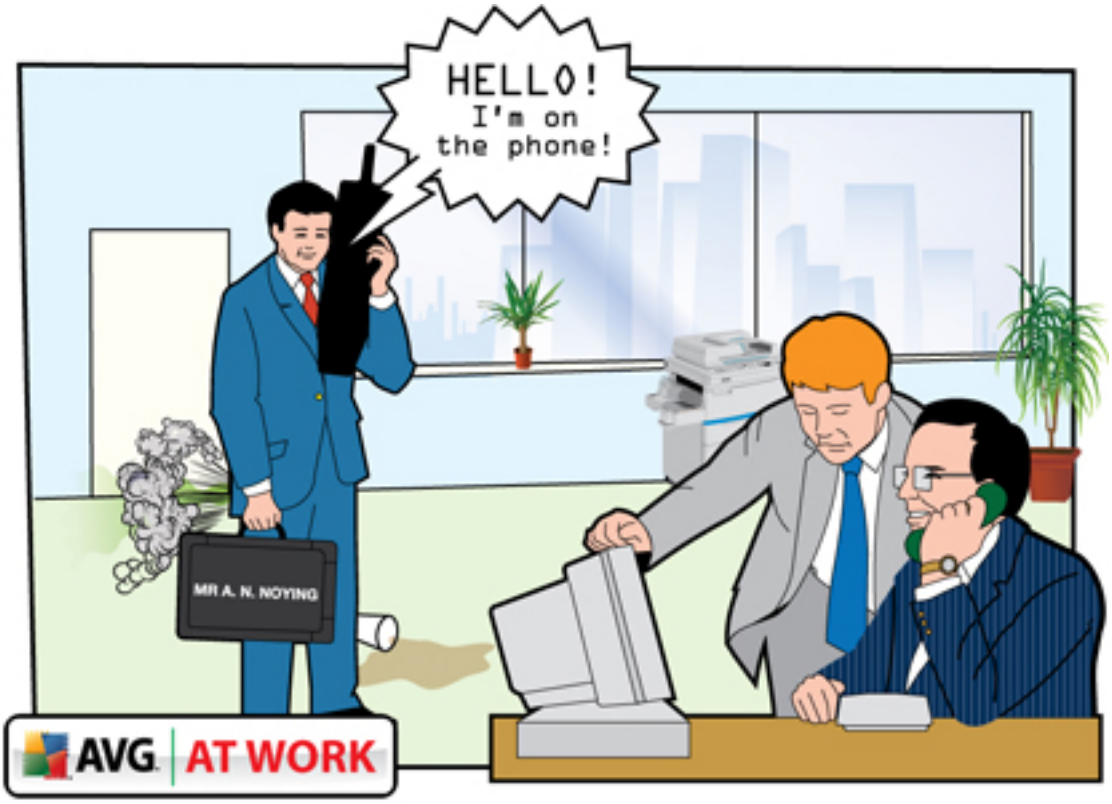
Les navigateurs et leurs ajouts associés fournissent une multitude de moyens de compromettre les sites Web et d'envoyer des logiciels malveillants à des visiteurs qui ne se doutent de rien. Des recherches réalisées en 2008 ont fait apparaître que soixante-dix des 100 principaux sites Web hébergeaient des codes malveillants ou contenaient un lien redirigeant les utilisateurs vers un site Web malveillant. « Le Web est devenu le vecteur de prédilection pour les attaques. Avec l'e-mail, les pirates ne disposaient que d'un nombre limité d'accès à un ordinateur : soit à l'aide d'une pièce jointe infectée, soit par un lien vers un site Web qui communique le logiciel malveillant. Si les pirates utilisent toujours l'e-mail, ils ont découvert que le Web en général – et les réseaux sociaux en particulier – leur offrait une gamme d'options beaucoup plus étendue, explique le livre blanc d'AVG intitulé « Pourquoi les solutions classiques contre les logiciels malveillants ne suffisent plus ».

Les navigateurs et leurs ajouts associés fournissent une multitude de moyens de compromettre les sites Web et d'envoyer des logiciels malveillants à des visiteurs qui ne se doutent de rien. Des recherches réalisées en 2008 ont fait apparaître que soixante-dix des 100 principaux sites Web hébergeaient des codes malveillants ou contenaient un lien redirigeant les utilisateurs vers un site Web malveillant. « Le Web est devenu le vecteur de prédilection pour les attaques. Avec l'e-mail, les pirates ne disposaient que d'un nombre limité d'accès à un ordinateur : soit à l'aide d'une pièce jointe infectée, soit par un lien vers un site Web qui communique le logiciel malveillant. Si les pirates utilisent toujours l'e-mail, ils ont découvert que le Web en général – et les réseaux sociaux en particulier – leur offrait une gamme d'options beaucoup plus étendue, explique le livre blanc d'AVG intitulé « Pourquoi les solutions classiques contre les logiciels malveillants ne suffisent plus ».

Outre la mise à jour de la stratégie de sécurité informatique de l'entreprise pour tenir compte de la menace présentée par les sites de réseaux sociaux, les entreprises peuvent naturellement choisir de bloquer tout simplement ces sites. Les entreprises qui cherchent une réponse plus subtile se tournent aujourd'hui vers les outils d'analyse du Web. Par exemple, la technologie LinkScanner (http://linkscanner.avg.com/) proposée par AVG vérifie chaque site à la recherche d'éventuelles infections avant d'en autoriser l'accès.

4. Menaces internes : connais ton ennemi, il est peut-être ton employé

Même si les entreprises peuvent s'inquiéter à juste titre des mystérieux cybercriminels, les employés présentent une menace équivalente, voire supérieure en termes de logiciels malveillants. Cette « menace interne » fait l'objet de nombreux débats dans le secteur de la sécurité informatique, mais qu'elle soit délibérée ou accidentelle, les employés sont responsables de l'introduction de la plupart des logiciels malveillants dans les réseaux d'entreprise.



Une formation aux pratiques de sécurité pourrait contribuer à réduire le nombre d'accidents, mais il est plus difficile d'empêcher les employés qui cherchent à introduire des logiciels destructeurs de le faire. On a recensé des cas où des employés installaient des logiciels malveillants sur le réseau de leur entreprise simplement dans le but de lui nuire ou d'en tirer un profit ultérieurement. Un exemple célèbre est celui de Michael John Lauffenburger, employé de General Dynamics Corporation, qui avait installé une bombe dite logique sur le réseau de la compagnie d'armement, dans l'espoir d'être embauché ultérieurement pour réparer les dégâts occasionnés.

Même s'il est vital de tenir à jour les logiciels antivirus et autres logiciels de sécurité, un autre moyen pour empêcher les employés d'introduire délibérément des logiciels malveillants dans l'entreprise consiste simplement à ne pas les embaucher. Pour les entreprises qui traitent avec des informations très confidentielles, des vérifications des antécédents du personnel – notamment du personnel technique – sont justifiées. Le recours à des tests psychométriques qui pourraient écarter les types de personnalités susceptibles de saboter leur propre entreprise constituent une autre option. De toute évidence, les licenciements et réductions de personnel peuvent inciter certains employés à placer des logiciels malveillants sur le réseau de l'entreprise par vengeance ; par conséquent, les droits d'accès informatiques, notamment les droits d'administrateur, devraient être limités ou révoqués dès que possible.

5. Employés distants – Une sécurité éloignée

Même s'il peut être difficile d'empêcher les employés de placer des logiciels malveillants sur le réseau d'une entreprise, il est encore plus complexe de contrôler les employés qui sont autorisés à accéder à distance au réseau de l'entreprise. Les particuliers adoptent généralement une approche plus laxiste que celle des entreprises lorsqu'il s'agit de mettre à jour les logiciels antivirus et d'installer les mises à jour du système. Le fait d'autoriser des employés à utiliser leur ordinateur personnel pour travailler augmente donc le risque d'implantation de logiciels malveillants sur le réseau de l'entreprise.

Une solution évidente pour combler cette lacune de sécurité particulière consiste à empêcher les employés d'utiliser leur ordinateur personnel. Toutefois, certaines entreprises comme le spécialiste de la virtualisation Citrix ont démontré que le fait de laisser les employés acheter

et gérer leurs propres périphériques constitue une option moins coûteuse à long terme que de leur remettre des machines appartenant à l'entreprise. Citrix a contourné le problème grâce à sa technologie de virtualisation, laquelle crée effectivement une zone sécurisée virtuelle dans le matériel - à l'instar d'une ambassade dans un pays étranger. L'utilisation d'applications hébergées ou de cloud est un autre moyen de contourner les machines des employés, puisque tout est hébergé sur un serveur central et non téléchargé localement.

6. Clés USB – Des logiciels malveillants en plug and play

Les cartes mémoire et les clés USB sont particulièrement efficaces pour propager les logiciels malveillants. Elles semblent inoffensives comparées à un ordinateur portable ou à un smartphone, mais peuvent contenir plusieurs gigaoctets de code. « Petites, disponibles partout, peu coûteuses et extrêmement portables, les clés USB sont très populaires pour stocker et transporter des fichiers d'un ordinateur vers un autre. Toutefois, ces mêmes caractéristiques les rendent attrayantes aux yeux des pirates », explique le CERT, organisme de sécurité du gouvernement américain.

Parmi les exemples récents d'organismes victimes de clés USB, on peut citer la police de la ville de Manchester, dont les systèmes informatiques ont été paralysés plusieurs jours en raison d'une clé USB contenant le ver Conficker. Tony Anscombe, directeur des produits gratuits chez AVG, explique que les périphériques amovibles peuvent être vérifiés automatiquement à l'aide de logiciels AVG. Les utilisateurs peuvent également procéder à une analyse manuelle avant d'accéder à tout fichier se trouvant sur la clé. « La morale de cette histoire est qu'il ne faut jamais baisser sa garde », conclut-il.

Les conseils du CERT quant à la manière d'éviter les infections par des logiciels malveillants par des clés USB comprennent l'avertissement suivant : ne pas utiliser de périphériques inconnus, mais aussi séparer les clés personnelles et professionnelles. « N'utilisez pas de clé USB personnelle sur un ordinateur appartenant à votre entreprise, et ne connectez pas de clé USB contenant des informations de l'entreprise sur votre ordinateur personnel », recommande l'organisme.

7. Périphériques mobiles – Une sécurité plus intelligente sur les téléphones

Les smartphones équipés de l'e-mail présentent pour les réseaux d'entreprise des risques similaires à ceux des ordinateurs de bureau. Même si les téléphones eux-mêmes sont rarement victimes de virus ou de vers, ils peuvent contribuer à propager les logiciels malveillants sur d'autres périphériques vulnérables du réseau. Selon le CERT américain, ces pirates et les criminels sont également capables d'utiliser des SMS pour guider des utilisateurs ignorants vers des sites Web contenant des codes malveillants. « Ces messages, qui semblent provenir d'une entreprise légitime, peuvent tenter de vous inciter à visiter un site malveillant en affirmant qu'un problème a été constaté sur votre compte ou que vous avez été abonné à un service. Dès que vous accédez au site, vous pouvez être invité à fournir des informations personnelles ou à télécharger un fichier malveillant », précise le CERT.

Les smartphones sont exposés à d'autres risques en cas de téléchargement de contenu. Le CERT recommande d'avertir les employés de ne pas télécharger de jeux ni d'autres applications inutiles sur leur téléphone portable professionnel. « De nombreux sites proposent des jeux et autres logiciels à télécharger sur un téléphone portable ou un PDA », précise l'organisme. « Ces logiciels peuvent contenir un code malveillant. Évitez de télécharger des fichiers depuis des sites auxquels vous ne faites pas confiance. Si vous vous procurez des fichiers auprès d'un site supposément sécurisé, recherchez son certificat de site Web. Si vous téléchargez un fichier à partir d'un site Web, envisagez de l'enregistrer sur votre ordinateur et de l'analyser manuellement pour rechercher les virus avant de l'ouvrir. »

Outre la messagerie et l'accès à Internet, des codes malveillants peuvent s'infiltrer sur un périphérique mobile grâce à la technologie de mise en réseau de proximité appelée Bluetooth. En ce qui concerne le Bluetooth, le CERT recommande de s'assurer que les employés savent qu'ils doivent le désactiver lorsqu'ils ne l'utilisent pas. « Assurez-vous de bien profiter des fonctions de sécurité proposées sur votre périphérique », recommande l'organisme. « Les pirates peuvent profiter des connexions Bluetooth pour accéder ou télécharger des informations sur votre périphérique. Désactivez Bluetooth lorsque vous ne l'utilisez pas pour éviter tout accès non autorisé. »

Autre problème lié aux périphériques mobiles tels que les smartphones : ils sont de plus en plus fréquemment utilisés pour payer des produits et des services. Cela signifie que même si certains virus détectables apparaîtront de temps à autre, la véritable préoccupation est liée à un code malveillant plus subtil, selon le responsable de la technologie chez AVG, Roger Thompson. « Des virus se sont toujours infiltrés et continueront à s'infiltrer occasionnellement sur des périphériques mobiles », dit-il. « Le mois dernier encore, nous avons découvert deux virus sur les iPhone (plus précisément des vers), mais un virus n'est réellement un virus que s'il se propage et le logiciel malveillant que nous verrons infecter les périphériques mobiles sera bien plus subtil que les virus classiques. »

Les logiciels malveillants mobiles enregistreront les frappes sur les touches et pirateront les identifiants et les mots de passe des utilisateurs, selon M. Thompson, d'AVG. « On verra des logiciels malveillants transmettre des informations concernant nos habitudes sur Internet à

leurs propriétaires, lesquels utiliseront ces informations pour décider des publicités à nous envoyer », dit-il. « Selon toute probabilité, les virus les plus néfastes généreront des bases de données d'informations de fond nous concernant, qu'ils utiliseront pour nous profiler en vue de leurs activités criminelles futures.

8. Réseaux sans fil – Ce que vous ne voyez pas peut vous nuire

Dans la mesure où ils ont la possibilité de diffuser en dehors des confins d'un immeuble de bureau, les réseaux sans fil offrent aux pirates une voie d'accès tentante. Selon le CERT américain, certains criminels se spécialisent dans le ciblage des réseaux sans fil non sécurisés. Pour combler cette lacune, il faut être attentif aux paramètres de sécurité du réseau. « Une pratique appelée piratage Wi-Fi requiert des individus équipés d'un ordinateur, d'une carte sans fil et d'un dispositif GPS, qui explorent les zones à la recherche des réseaux sans fil et identifient les coordonnées spécifiques d'un site de réseau. Ces informations sont ensuite généralement publiées en ligne », avertit le CERT.

Le CERT américain dispense également des conseils relatifs à la gestion des pare-feu pour bloquer les attaques sans fil. « Même si l'installation d'un pare-feu sur votre réseau est une bonne pratique de sécurité, vous devriez également installer un pare-feu directement sur vos périphériques sans fil (un pare-feu basé sur l'hôte). Les pirates qui puisent directement dans votre réseau sans fil peuvent être à même de contourner votre pare-feu de réseau – un pare-feu hébergé sur l'hôte ajoute une couche de protection aux données présentes sur votre ordinateur. »

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