Guides de sécurité pour les petites entreprises

Réseaux sociaux pour l'entreprise : **Risque ou retour sur investissement ?**

AVG AU TRAVAIL

Réseaux sociaux pour l'entreprise : Risque ou retour sur investissement ?

LinkedIn, Facebook, Twitter et les réseaux sociaux en général sont considérés par certains comme offrant des avantages commerciaux tangibles, mais ces canaux de communication sont-ils plus qu'une passerelle pour les risques commerciaux ou ont-ils le potentiel d'offrir un impact réel et positif sur le retour sur investissement (ROI) ?

Le saviez-vous ?

• Gartner, société de pointe dans le domaine de la recherche et du conseil, prévoit que les réseaux sociaux surpasseront la messagerie d'ici 2014 http://www.computerworlduk.com/management/onlince/new-media/news/index.cfm?newsid=21033

• Le nombre de membres de LinkedIn a augmenté de 40 % au cours du premier semestre 2010 http://econsultancy.com/blog/6205-revised-mind-blowing-social-media-statistics-revisited-and-20+-more

Selon le fondateur de Facebook, Mark Zuckerberg, « ...les gens sont aujourd'hui beaucoup plus détendus lorsqu'il s'agit de leur confidentialité en ligne. Les attitudes ont changé et les utilisateurs se sont « ouverts au Web », pour partager des informations personnelles sur des sites de réseaux sociaux. « ...Même si cette nouvelle orientation s'accompagne de risques pour la confidentialité personnelle, le véritable problème se pose lorsque les utilisateurs adoptent la même approche dans leur travail et se montrent tout aussi « ouverts » dans l'environnement d'une entreprise.

Le changement d'attitude perçu en termes de partage des informations personnelles dans sa base d'utilisateurs a incité Facebook à modifier ses règles de confidentialité à la fin 2009. Toutefois, même si ces changements ont été considérés comme audacieux et courageux par la direction de Facebook, certains de ses 350 millions d'utilisateurs à travers le monde ne partagent pas cette opinion et se sont plaints du fait que la société ne se montrait pas à la hauteur de leurs préoccupations bien réelles en matière de vol d'identité et de sécurité en ligne.

L'opinion du secteur semble indiquer que même si ces règles ont été adoptées sur Facebook (et peut-être plus encore sur LinkedIn et Twitter) en tant que réseau social au niveau professionnel, l'augmentation de la confidentialité mise en place par le géant des réseaux sociaux n'était pas à la hauteur des risques actuels qui menacent les grandes entreprises en réseau. Plus simplement, si nous utilisons les réseaux sociaux au sein d'une entreprise, une nouvelle stratégie de confidentialité ne suffit pas. Si nous ne nous attaquons pas directement aux problèmes de vol d'identité, de cybercriminalité et d'espionnage sur le Web, nous laissons la porte grande ouverte.

Dans le même temps, les réseaux sociaux semblent se concentrer sur la manière de rendre leurs sites plus attrayants, plus conviviaux et plus susceptibles de retenir l'attention des utilisateurs. Cela passe avant tout par l'incitation des utilisateurs à publier du contenu plus personnel et à communiquer davantage de renseignements confidentiels. Tout cela vient renforcer le profil et l'identité. Transposons cet exemple dans l'environnement de l'entreprise, et l'identité devient une propriété intellectuelle, laquelle doit impérativement être verrouillée.

Encore une fois, transposons cet exemple sur le lieu de travail, et vous pouvez voir les dangers qui vous guettent. L'envoi d'informations indiquant le nom des entreprises avec lesquelles vous êtes en contact dévoile à vos concurrents l'identité de vos partenaires professionnels et de vos prospects. Le fait de parler au monde entier des nouveaux produits de votre entreprise avant leur lancement officiel ne vous vaudra certainement pas le respect de vos collègues. Peut-être pire encore, les informations concernant les entreprises avec lesquelles vous ne supportez pas de traiter et dont vous détestez les produits pourraient vous rapprocher dangereusement d'un procès en diffamation.

Le danger inhérent à une approche imprudente des réseaux sociaux ne concerne pas seulement les risques pour les biens physiques au niveau personnel ou professionnel : le vol d'identité constitue également un danger sérieux. Le site StaySafeOnline du gouvernement américain (http://www.staysafeonline.org/) propose certains conseils utiles à propos de l'utilisation sécurisée des sites de réseaux sociaux. Selon ce site, « les réseaux sociaux en ligne ont été conçus pour les entreprises, les loisirs, les écoles et les groupes religieux. Correctement utilisés, ils constituent un outil de communication unique permettant de rester en contact avec des amis et des collègues. Toutefois, comme tout outil en ligne, les sites de réseaux sociaux sont susceptibles d'être infiltrés par des pirates et des cybercriminels. »

StaySafeOnline invite les utilisateurs occasionnels et professionnels à faire preuve de prudence quant aux informations qu'ils publient en ligne, car les criminels utilisent ces sites pour puiser des informations qu'ils pourront exploiter ; il est donc essentiel de se familiariser avec les paramètres et les outils de confidentialité proposés sur ces réseaux sociaux. En résumé, tous les employés devraient savoir quels sites sociaux une entreprise autorise ses employés à utiliser au cours des heures ouvrées.

Un nouveau terme à apprendre : données de passerelle

Comment un cybercriminel utilise-t-il les informations obtenues sur un profil Facebook ou LinkedIn pour accéder à un compte bancaire personnel ou d'entreprise, par exemple ? Her-

bert « Hugh »Thompson, professeur au département Sciences informatiques de l'université de Columbia à New York, a inventé le terme « données de passerelle » pour faire référence aux informations confidentielles recueillies auprès des sites de réseaux sociaux.

Thompson précise que tôt ou tard, le partage excessif d'informations via des réseaux sociaux entraîne inévitablement des conséquences. « Les cybercriminels doivent être en mesure d'exploiter les informations partagées par les utilisateurs pour leur nuire... et je pense que nous en sommes arrivés à ce stade », explique-t-il.

Les données de passerelle identifiées par Thompson peuvent être utilisées de différentes manières. Par exemple, la découverte du nom de jeune fille de la mère de quelqu'un sur Facebook pourrait être utilisée pour répondre à une question permettant de retrouver un mot de passe sur un compte de messagerie. Même s'il s'agit d'un compte personnel, l'utilisateur se met en danger et le pirate se rapproche dangereusement de toutes les informations professionnelles qu'il recherche.

Dès qu'un criminel parvient à accéder à la messagerie de l'utilisateur, il y a de bonnes chances qu'il y trouve des détails lui permettant par exemple de s'introduire dans un compte bancaire. Les données de passerelle peuvent également permettre d'utiliser un élément d'information, tel que les cinq premiers chiffres de la carte de crédit d'une entreprise, pour inciter l'utilisateur à révéler le numéro entier.

Un pirate procède en examinant de multiples fragments de données afin d'en extraire une information confidentielle importante. Par conséquent, la distinction entre vos données personnelles et professionnelles est beaucoup moins nette que vous ne pourriez le penser. En fait, elle est parfois quasi inexistante.

Outre le respect des approches sûres et raisonnables recommandées par StaySafeOnline, d'autres spécialistes déconseillent l'installation d'applications provenant de sites de réseaux sociaux, sauf si l'application elle-même émane d'une source sûre – et il s'agit là d'un jugement extrêmement subjectif : comment savoir à qui vous pouvez faire vraiment confiance et être sûr que cette société elle-même n'a pas été piratée ?

« Il faut acquérir une bonne dose de scepticisme », recommande Roger Thompson, respon-

sable de la recherche pour la société de sécurité Internet AVG. « Lorsque vous recevez l'une de ces offres vous invitant à regarder une vidéo, mais précisant que vous devez installer un programme pour y accéder : ne le faites pas. Cela n'en vaut pas la peine et vous ne devriez jamais avoir à effectuer ce genre d'opération. Ces applications inconnues sont susceptibles de contenir des codes malveillants tels que des virus ou des vers et une vidéo attrayante est précisément le genre d'outil que les cybercriminels tentent d'utiliser pour les disséminer sur le Web », ajoute Thompson.

AVG a également émis un avertissement concernant la popularité des URL abrégées sur les sites comme Twitter. « Le problème des liens abrégés tient au fait qu'ils ne ressemblent généralement en rien à l'URL d'origine, ce qui signifie que les utilisateurs ne savent pas toujours sur quoi ils cliquent. Les gens cliquent dans l'intention d'accéder à un site particulier, mais le lien peut facilement être piraté pour les envoyer vers un site contenant des chevaux de Troie, des logiciels espions, des rootkits et autres éléments dangereux », explique Thompson.

En résumé, les réseaux sociaux peuvent représenter une force positive au sein d'un environnement de communication d'entreprise et contribuer à la réalisation de bénéfices et à un ROI total de l'entreprise concernant son infrastructure informatique. Il faut seulement utiliser une couche de gestion, mettre en place des contrôles réglementaires et utiliser une certaine planification stratégique pour assurer la prise de conscience des utilisateurs et leur respect de la « voix de l'entreprise ».

AVG SMB group :
bit.ly/AVGSMB

Devenez un fan 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