

# RÉSEAUX SOCIAUX: CINQ CLÉS POUR GÉRER LE RISQUE

CHAQUE ENTREPRISE PRÉSENTE SUR INTERNET PEUT DÉSORMAIS ÊTRE LA CIBLE D'ATTAQUES.

**Fabrice Perrin**

*Manager chez blue-infinity*

Dernièrement, le monde a pu constater la montée du pouvoir des réseaux sociaux dans les pays du Moyen-Orient, où ils auraient joué un rôle dans la coordination des manifestants et dans la diffusion d'informations concernant les agissements des autorités en place. Mais cette progression a également été ressentie dans les pays occidentaux avec le groupe Anonymous, qui mène les attaques de « soutien » à WikiLeaks.

Anonymus est un collectif qui agit de façon coordonnée sur Internet et lance des actions contre des sites ou des organisations. Les « hackers » utilisent le masque de « V pour Vendetta » pour leur communication et n'importe qui peut revendiquer son appartenance au groupe. Quiconque peut agir pour le groupe, sans être doté de connaissances techniques particulières, simplement en utilisant des logiciels comme LOIC ou Botnet. Ces programmes permettent de participer à des attaques en DoS (Denial of Service), qui consistent à saturer un site Internet en lui demandant des millions d'informations simultanément. Les participants sont des hackers chevronnés ou des internautes, qui pensent participer à une juste cause, sans forcément se rendre compte que ce jeu pourrait être très dangereux pour la sécurité de leurs données. Début décembre 2010, Anonymous avait indiqué les sites de Visa, Mastercard, Paypal et PostFinance sur son blog. Jugés « coupables » par le groupe de hackers de ne plus collecter les dons pour WikiLeaks, ces

sites ont été rendus indisponibles pendant plusieurs heures, créant ainsi un important préjudice d'image pour ces entreprises bancaires, qui montraient leur fragilité face aux attaques virtuelles.

Voici quelques pistes pour gérer le risque et réduire la vulnérabilité d'une entreprise...

## **Clé 1 : Soignez votre infrastructure technique**

Quand les sites bancaires ont été attaqués par Anonymous, ils se sont trouvés

dans l'incapacité de répondre aux milliers de demandes simultanées générées par les logiciels des hackers. Toute entreprise dont la visibilité sur Internet est critique devrait posséder un plan de contingence contre ce type d'attaques: possibilité pour le portail de passer en mode « dégradé », affichage d'un texte d'indisponibilité et surtout, existence d'une équipe de spécialistes capables de réagir et de reconfigurer serveurs et firewalls. Méfiez-vous également du « defacement »: rien de pire en termes d'image que de voir sa page

## LES ACTIONS D'ANONYMOUS

Le collectif Anonymous était auparavant connu pour plusieurs « faits d'armes » plus ou moins pertinents:

- Une attaque contre le site Internet du « White Supremacist » Hal Turner, qui aurait coûté des milliers de dollars en bande passante à ce dernier.
- La participation à l'arrestation du cyber-prédateur Chris Forcand. Les membres d'Anonymous avaient alerté la police sur les agissements de cet homme coupable d'attouchements sur un mineur.
- Une attaque contre YouTube avec le chargement massif de vidéos pornographiques le 20 mai 2009, pour protester contre la suppression des clips musicaux sur le site.
- Plusieurs autres attaques contre Gene Simmons du groupe Kiss ou la création de sites communautaires pour aider les Iraniens.

Anonymous a commencé à faire sérieusement parler de lui en 2008 avec le projet Chanology, lorsqu'il a menacé d'éradiquer l'Église de Scientologie. La vidéo postée à l'époque avait généré plus de 4 millions de visites...

d'accueil re-dessinée par un pirate. Des logiciels anti-intrusion correctement configurés doivent permettre de détecter toute activité suspecte, basculer en mode contingence et alerter les équipes techniques.

### Clé 2 : Écoutez les réseaux sociaux

Écoutez ce qui se dit sur vous. Faites appel à des sociétés d'écoute et d'engagement qui sauront identifier les réseaux vous concernant, entrer pour vous en contact avec les influenceurs et vous aider à prévenir les risques. C'est l'occasion d'anticiper les agressions et de gagner quelques heures: Anonymous annonce toujours sur son site qui sera sa prochaine cible. Cela permet aussi de comprendre ce que vos clients — ou l'opinion publique, d'une façon générale — pensent de vous, et d'agir dans le cas où leurs sentiments seraient négatifs. Mettez en place des procédures en cas d'intensification d'une rumeur ou si votre société était soudainement prise à partie sur des médias comme Facebook ou Twitter. Imaginez une campagne de dénigrement massive: comment arriveriez-vous à faire entendre votre point de vue sur ces réseaux? Vous devez vous poser la question avant que la crise n'arrive, étudier vos options et mettre en place les équipes adéquates.

### Clé 3 : Surveillez les noms de domaine

Soyez attentifs aux noms de domaine que l'on peut associer à votre société, à vos marques ou services. Des attaques de dénigrement de grande ampleur sont à attendre de ce côté. Et, pire encore, l'utilisation de votre nom dans le cadre de phishing (escroquerie en ligne) est tout à fait envisageable. Quelqu'un prétendant être [www.nom-de-votre-société-suisse.com](http://www.nom-de-votre-société-suisse.com) et reprenant votre logo et vos couleurs pourrait-il escroquer vos clients?

### Clé 4 : Formez vos équipes

Vos collaborateurs fréquentent forcément des réseaux sociaux, qu'ils soient professionnels (LinkedIn, Viadeo, etc.) ou non. Ils peuvent donc être confrontés à l'évocation de

vos entreprise en bien ou en mal, voire être jugés par d'autres internautes. Il est essentiel qu'ils soient formés, qu'ils sachent ce qu'ils peuvent dire ou non. Fournissez à vos collaborateurs des règles d'engagement sur les réseaux sociaux. Une base simple est celle des 3R : soyez clairs avec vos interlocuteurs sur ce que vous «représentez», soyez «responsables» de ce que vous dites et montrez-leur du «respect».

### Clé 5 : Méfiez-vous de l'«effet Streisand»

En 2003, Barbara Streisand a voulu faire interdire une image de sa propriété dans une collection de 12'000 photos. Résultat: l'informa-

tion a été diffusée, et dès le mois suivant, plus de 400'000 personnes se sont rendues sur le site pour connaître la raison de cette censure ! Vous êtes attaqués sur un forum ou dans le fil de discussion d'un article d'un magazine en ligne ? Attendez un peu avant de réagir. Parfois l'incendie s'éteint de lui-même. Chercher à l'étouffer immédiatement peut, au contraire, l'attiser ! Placez l'événement sous surveillance, déterminez quels critères (nombre de posts où vous êtes cités, propagation à d'autres sites, etc.) devront déclencher votre engagement, et pendant ce temps, préparez soigneusement votre réponse et vos explications, au cas où !



© edans