

Auteur: Evelyne Pintado  
Communication Architect – Navixia SA

## SÉCURITÉ DE L'INFORMATION: COMMENT SE PROTÉGER AU QUOTIDIEN?

L'actualité récente a fait la part belle aux effets du piratage informatique et de la fuite des données sensibles avec entre autres WikiLeaks, le «Sonygate» ou la cybercriminalité dans le domaine des paiements en ligne. Pour l'entrepreneur, il devient difficile dans un tel climat de faire la part des choses: quels sont réellement les risques, et comment protéger l'entreprise et ses collaborateurs au quotidien? Voici quelques pistes simples pour y voir plus clair.

La presse a beaucoup parlé de WikiLeaks en début d'année. Si elle a suscité la polémique, cette affaire surtout politique restait en définitive assez éloignée des préoccupations de l'entrepreneur ou de l'utilisateur d'un réseau informatique. Mais l'actualité vient de nous fournir un exemple plus proche de chacun d'entre nous: le «Sonygate». Pour rappel, l'entreprise Sony a été victime entre le 17 et le 19 avril 2011 d'un piratage sans précédent de son portail interactif, Sony Online Entertainment (SOE), qui relie la PlayStation 3 à des jeux ou des films en ligne.

Il s'agirait ici de la vengeance d'un groupe de «hacktivistes» (c'est-à-dire de pirates se considérant comme des redresseurs de torts); ils auraient voulu punir Sony, qui a poursuivi en justice deux jeunes hackers ayant réussi à pi-

rater le code de la PlayStation 3. Les conséquences ont été rudes. Sony a annoncé que des informations relatives à 24,6 millions de comptes SOE auraient été volées lors de cette opération, ainsi que les coordonnées bancaires de milliers d'utilisateurs. Certaines de ces dernières auraient été mises immédiatement en vente sur internet.

Cet exemple illustre bien une problématique très actuelle: le mode de stockage et de diffusion des informations. L'activité en ligne croissante des internautes ainsi que l'usage des forums participatifs et des réseaux sociaux ont considérablement accru pour tout le monde le risque d'exposition des informations professionnelles ou personnelles. Il est toutefois bien clair qu'en termes de sécurité, toutes les entreprises ne sont pas à la même enseigne. Logiquement,



le degré de protection à déployer dépend de la valeur des informations à protéger et des conséquences potentielles d'un piratage pour la société.

### Protéger quoi?

Protéger le système d'information, qu'est-ce que cela implique? C'est plus compliqué qu'autrefois. Alors qu'il y a quelques années les réseaux informatiques étaient des entités clairement délimitées, aujourd'hui leur périmètre est devenu beaucoup plus flou. Cela est dû essentiellement à la multiplication des appareils périphériques portables (laptops, smartphones, tablettes) utilisables partout, à la porosité de la frontière entre les usages professionnels et privés, à l'usage d'internet et à la virtualisation de certaines fonctionnalités du réseau. Il n'est ainsi plus possible de dresser une muraille unique autour du réseau informatique pour en assurer la sécurité: les différentes protections doivent intégrer avec une grande souplesse des facettes très diverses de l'infrastructure existante en fonction de l'utilisation qui en est faite. Les risques actuels les plus marqués sont:

La contamination possible du réseau par le biais de supports mobiles infectés ou par l'utilisation d'internet. Les infections de sites web constituent d'ailleurs actuellement le vecteur de diffusion de maliciels le plus répandu.

le vol ou la perte de données sensibles dont la publication ou la perte serait dommageable pour l'entreprise.

le blocage ou le ralentissement des services essentiels de l'entreprise, compromettant sa capacité à fonctionner normalement. On relève une forte recrudescence de ce type d'attaques. La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI estime même à ce propos dans son dernier rapport que «la sophistication des moyens utilisés et les dommages collatéraux qui s'ensuivent laissent songeur, même en Suisse. Il suffit de penser aux actes de représailles menés contre plusieurs entreprises suisses jugées hostiles au fondateur de WikiLeaks».



## Comment peut-on se protéger?

Les technologies et les méthodes d'attaque évoluent si vite qu'il est vivement conseillé de faire appel à des professionnels qui pourront suggérer des solutions adaptées en connaissance de cause. Mais il existe un préalable incontournable à toute démarche de protection: l'entreprise doit établir des règles de sécurité claires et détaillées, puis sensibiliser ses utilisateurs aux risques que présente l'utilisation quotidienne du système d'information.

## L'utilisateur au centre de la politique de sécurité

En effet, il est inutile de déployer des protections sophistiquées si les utilisateurs sont susceptibles de cliquer sans méfiance sur des liens à risque, ou s'ils ne tiennent pas compte des règles de sécurité existantes parce qu'ils n'en comprennent pas l'utilité.

## Vous pensez que pour eux la prudence va de soi?

Plus que jamais aujourd'hui, les méthodes à base de phishing et d'ingénierie sociale restent une porte d'entrée privilégiée des hackers. Le phishing est une démarche qui permet à l'attaquant de profiter du réflexe qu'ont les utilisateurs de cliquer sur certains liens en apparence inoffensifs pour gagner accès aux systèmes de l'entreprise. Et c'est une tactique assez redoutable, comme l'a encore montré l'actualité récente: l'un des leaders mondiaux de l'authentification a fait l'objet d'une cyber-attaque qui a failli avoir des conséquences catastrophiques pour ses activités commerciales. Les pirates ont gagné accès à son infrastructure de manière simple: ils ont envoyé à certains employés un e-mail habilement formulé accompagné d'un document Excel infecté intitulé «plan de recrutement 2011». Il a suffi qu'une personne consulte le document pour installer, sans s'en douter, le cheval de Troie qui a ouvert la porte aux pirates...

Ce type de manipulation relève de ce qu'on appelle l'«ingénierie sociale». Il

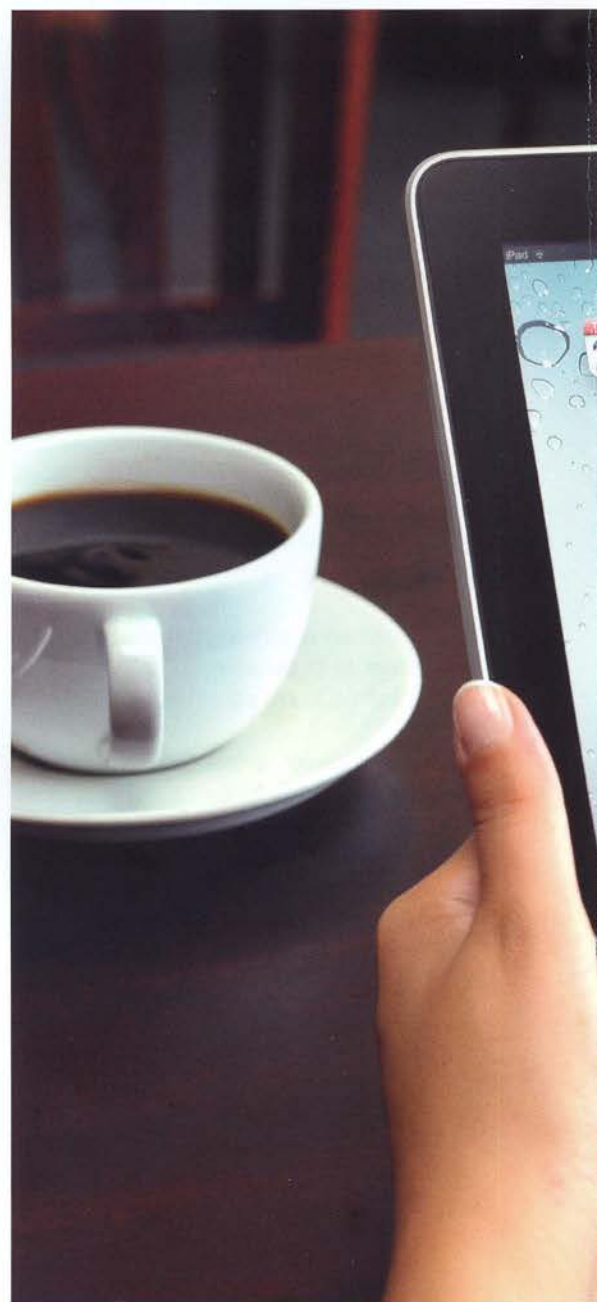


s'agit pour le pirate d'exploiter les faiblesses, la crédulité ou les automatismes des utilisateurs, et d'obtenir ainsi à leur insu les informations souhaitées ou de gagner un accès direct à leur réseau. L'utilisateur est trompé sans s'en apercevoir, d'où l'importance de le sensibiliser aux risques potentiels: seules sa perspicacité et sa méfiance lui permettront de ne pas tomber dans le panneau.

## Les smartphones et les tablettes: un nouveau risque

Ces méthodes d'ingénierie sociale vivent par ailleurs de plus en plus les nouveaux appareils périphériques portables. Il s'agit en effet d'une cible sensible. Non seulement les systèmes d'exploitation de ces appareils n'ont pas fait l'objet de recherche de vulnérabilités poussées, mais l'utilisateur entretient un rapport de confiance souvent excessif avec son téléphone mobile ou sa nouvelle tablette, sur lesquels les usages professionnels et privés sont souvent mêlés.

De plus, de nombreuses applications pour mobiles sont disponibles au téléchargement avec les risques que cela entraîne. On apprenait par exemple le mois dernier cette information inquiétante: des intervenants malveillants avaient sélectionné plusieurs dizaines d'applications gratuites pour Android disponibles sur Google Market. Ils y avaient injecté un maliciel permettant





non seulement d'extraire toutes les informations du smartphone, mais aussi d'y installer potentiellement du code additionnel. Ils les avaient ensuite remis à disposition en ligne. Bilan après quelques jours: des centaines de milliers de téléchargements effectués, et autant d'utilisateurs qui avaient ainsi compromis leur smartphone sans le savoir.

Selon une étude récente, les utilisateurs mobiles sont jusqu'à trois fois plus vulnérables au phishing que les autres. Diverses raisons à cela: ils ont un accès immédiat à l'information; la taille de l'écran ne permet pas une bonne visibilité des indices trahissant le phishing; les URLs s'ouvrent automatiquement...



Par ailleurs, les utilisateurs d'iPhones auraient huit fois plus de chances de se rendre sur des sites de phishing que les utilisateurs de Blackberries, dont l'usage est plus fréquemment limité au domaine professionnel.

Pour un pirate, les smartphones et les tablettes sont donc un vecteur assez idéal pour accéder au cœur des entreprises. Ces dernières sont d'ailleurs toujours plus nombreuses à en prendre conscience.

Les smartphones devraient être considérés comme des terminaux à part entière dans l'infrastructure informatique de l'entreprise, et sécurisés comme tels. En dehors de toute autre mesure, la recommandation impérative reste: former les utilisateurs à ne pas cliquer sur des liens internet via un smartphone, et soumettre l'usage des périphériques mobiles à des règles de sécurité claires.

### Pour conclure

Les risques liés à l'utilisation du système d'information, même nombreux, sont pondérés par la valeur des informations à protéger, qui varie d'une entreprise à l'autre. Il faut rester pragmatique!

Mais la première démarche, simple et indispensable pour renforcer la sécurité de l'entreprise, c'est d'y sensibiliser tous les utilisateurs. Si l'entreprise ne dispose pas des ressources internes lui permettant de mettre en place elle-même de telles sensibilisations, des entreprises externes spécialisées pourront l'y aider. De telles mesures sont extrêmement efficaces.

A surveiller également de très près, l'augmentation des risques liés à l'utilisation des périphériques mobiles, qui seront de plus en plus la cible des pirates dans les futur et risquent de devenir le point faible potentiel de nombreuses entreprises.

Là aussi, une aide extérieure peut être très profitable pour déterminer l'exposition réelle au risque et les mesures de prévention possibles.