



Phishing, hacking et autres cybercrimes

**La cybercriminalité,
la piraterie moderne**



Thijs Feryn (Combelle)

Des sites web proposant des ordinateurs piratés, une multinationale comme Sony régulièrement tourmentée par des pirates informatiques..., la cybercriminalité semble s'être bien installée dans nos temps modernes. Mais qu'a-t-on à perdre en tant qu'entreprise belge lorsque des cybercriminels vous cherchent noise ?

TEXTE **KATIA GROSEMANS**
PHOTO **TF**

**“Tous ensemble, nous
devons colmater les fuites.
Sinon nous n'arriverons
à rien”**

Il ressort de la '2011 Security Survey' de Symantec – fournisseur de solutions en matière de sécurité, de stockage et de gestion de système – que la sécurité est le risque réel le plus important auquel les départements IT sont confrontés aujourd'hui. L'augmentation rapide de l'utilisation des smartphones et des tablettes dans les entreprises et la grande popularité des médias sociaux engendrent de nouveaux défis sur le plan de la cybersécurité. Les hackers sont le plus grand souci des entreprises, suivis de leurs propres collaborateurs pleins de bonnes intentions. Quasi toutes les entreprises sont confrontées à des attaques informatiques, mais près de 29% les essuient de manière régulière. 92% des entreprises ont subi des dommages, parmi lesquels le vol d'informations sur l'identité d'un travailleur et le vol de propriété intellectuelle. Dans 84% des cas, ces pertes ont entraîné des préjudices financiers.

La cybercriminalité constitue donc un risque réel, y compris en Belgique. Un risque qui grandit à mesure que se développe Internet. Le fournisseur de technologie de réseau Cisco prévoit une multiplication du trafic Internet par quatre d'ici à 2015.

Dans son rapport international sur les e-menaces, BitDefender, spécialisé dans les solutions de sécurité, soutient que ce sont la Chine et la Russie, principalement, qui sont responsables des menaces. La Chine figure en tête de liste en termes de production et d'hébergement de logiciels malveillants, avec plus de 31% du total, suivie par la Russie (22%) et le Brésil (8%).

Internet peu sûr

L'entreprise gantoise Combelle propose des solutions d'hébergement et des services en ligne. Elle est constamment confrontée aux dangers de l'Internet. "L'Internet, tel qu'il existe aujourd'hui, n'a jamais été conçu pour être exploité commercialement", explique **Thijs Feryn**, porte-parole de Combelle. L'Internet a en effet été créé à des fins militaires, avant d'être ouvert aux entreprises et aux simples citoyens. La sécurité intégrée dès le début des années '60 est minime. "On voit clairement qu'il manque des composantes", précise Thijs Feryn. Remplacer les 'anciens' protocoles Internet par de nouveaux n'est pas (encore) une option. "Chaque serveur et chaque ordinateur dans le monde entier devraient être adaptés. Nous ne sommes pas prêts pour cela", poursuit-il. Il n'existe pas davantage une technologie sans faille pour nous protéger contre les abus sur Internet. "Les hackers

deviennent plus malins, et les entreprises qui veillent à la sécurité les rattrapent. Mais une fois le mouvement de rattrapage effectué, de nouvelles formes d'abus réapparaissent.”

Identité véritable

Diverses technologies protègent les entreprises et les consommateurs contre la cybercriminalité. Les certificats SSL (Secure Sockets Layer) vous garantissent que celui avec lequel vous communiquez est bien celui qu'il prétend être. “Lors d'une connexion sécurisée avec une boutique en ligne ou votre banque, par exemple, des certificats SSL protègent le cryptage des données de votre transaction. Le certificat SSL se présente sous la forme d'un logo dans la barre d'adresse. Si vous cliquez dessus, vous savez de quelle entreprise il s'agit.”

Un certain nombre de certificats SSL ont cependant récemment été piratés. “Il vaut donc mieux ne faire des affaires qu'avec les entreprises auxquelles vous faites confiance”, conseille le porte-parole de Combell.

Les enregistrements SPF (Sender Policy Framework) constituent une autre technologie de sécurité. “Une liste des expéditeurs pouvant envoyer des courriers électroniques à partir d'une adresse IP déterminée est tenue à jour sur Internet”, précise le porte-parole de Combell. “Une adresse IP est une forme d'identification d'une machine. Si on peut également y associer une identité, on sait avec certitude qu'il s'agit d'une personne définie, et non d'une autre personne.”

“Un autre terme à la mode est DNSSEC”, poursuit Thijs Feryn. “Les noms de domaine sont, en bout de parcours, convertis en adresses IP. On utilise à cet effet le protocole DNS. Lorsqu'un ordinateur local est piraté, la requête DNS peut être redirigée vers un autre serveur. Avec DNSSEC, on pourra garantir dans le futur que l'adresse IP reste liée au nom de domaine correct.” La redirection vers d'autres sites web deviendra alors impossible.

Spam

Tout le monde connaît les nombreux courriers indésirables qui inondent nos boîtes de réception. “C'est là que se situent les principales lacunes à l'heure actuelle”, estime Thijs Feryn. “Nous ne disposons pas d'une technologie concluante pour lutter contre les spam. Je peux par exemple programmer un script simple et me faire passer pour quelqu'un d'autre. Si j'utilise l'adresse e-mail de cette personne, je peux communiquer avec sa famille et ses amis sans qu'elle n'en sache rien. Un bon filtre anti-spam est très utile, tout comme un SPF. Des listes noires liées à des filtres anti-spam permettent d'éliminer les courriers non sollicités.”

“La majorité des abus que l'on rencontre aujourd'hui trouvent leur origine chez les développeurs qui n'intègrent pas suffisamment de sécurité dans leur méthode de programmation”, ajoute encore Thijs Feryn. “Les hackers se servent des failles dans les codes. Ils pénètrent dans le système, installent un ‘mauvais’ code et le simple visiteur d'un site web en est la victime. Il télécharge des virus qui se multiplient et qui affectent à leur tour d'autres personnes.”

Phishing

Chaque type de cybercriminalité a son nom. Le (spear) phishing, l'hacktivisme et l'ingénierie sociale sont trois techniques très courantes utilisées par les cybercriminels. **Marc Blanchard**, un épidé- >



TENEZ LES CYBERCRIMINELS À DISTANCE

Il n'existe pas de garantie à 100%. Mais il est possible, en suivant un certain nombre de règles de base, de réduire à un minimum le risque de cybercriminalité et de pertes qui en découlent.

Quelles sont les mesures à prendre à cet effet ?

- Faites en sorte d'avoir une bonne politique en matière de sécurité dans l'entreprise. Communiquez clairement à vos collaborateurs les règles et responsabilités relatives à Internet et à la messagerie électronique et faites-leur bien comprendre que les mots de passe et les identifiants sont strictement confidentiels.
- Utilisez le plus possible les technologies existantes pour surfer en toute sécurité sur le net et protéger les boîtes de réception : logiciels anti-spam, anti-virus, certificats SSL, enregistrements SPF, DNSSEC, etc.
- Prévoyez des accords et une communication efficaces avec vos partenaires technologiques en matière de sécurité.
- Attirez régulièrement l'attention de vos collaborateurs sur les dangers de l'Internet, conscientisez-les à propos de la sécurité.

Que faire si vous recevez un courriel suspect ?

- Appelez la personne indiquée comme expéditeur avant d'envoyer votre réponse ou d'ouvrir des annexes ou un lien dans le courriel.
- Ne cliquez jamais sur un lien dans le courriel, mais copiez-le dans votre navigateur Internet.
- Ne communiquez jamais des données personnelles ou financières en réaction à une demande envoyée par courriel, quel que soit l'expéditeur du courriel. ◀



- miologiste français à la tête du laboratoire de BitDefender, qualifie le spear phishing de nouvelle forme d'espionnage industriel. "65% des logiciels malveillants qui étaient présents dans les entreprises en 2010 proviennent du phishing", signale-t-il.

Via le phishing, des personnes malhonnêtes essaient de vous tromper et de voler ainsi de précieuses données personnelles telles que le numéro de votre carte de crédit, les informations liées à votre compte ou autres. Le phishing se sert souvent de courriels semblant provenir d'un collègue ou d'une personne que vous connaissez, de sites de réseautage social, de faux sites web où des dons sont collectés pour des œuvres de bienfaisance, de sites web imitant des sites connus mais ayant des adresses légèrement différentes.

Comment prévenir le (spear) phishing ? "Il faut toujours contrôler si l'URL est correct", conseille Thijs Feryn de Combell. "Et ne pas oublier de vérifier le certificat SSL. S'il n'est pas juste, méfiance ! Les données personnelles doivent toujours être transmises par le biais d'une connexion cryptée et sécurisée. Un bon anti-virus aide aussi. Certains virus font en effet en sorte que vous surfiez vers l'URL de votre banque, mais qu'en coulisse, vous soyez redirigé vers un autre serveur. Les cybercriminels tentent alors de voler les tokens (identifiants) que vous utilisez

pour vous connecter auprès de votre banque."



Ingénierie sociale et hacktivisme

Dans le cas de l'ingénierie sociale, le pirate informatique tente d'attaquer des systèmes informatiques en soutirant des informations confidentielles ou secrètes à un travailleur, de sorte à avoir accès aux systèmes. L'ingénierie sociale ne craint pas les contacts sociaux directs. "Ce type de piratage est beaucoup moins courant dans le secteur", affirme Thijs Feryn. BitDefender constate toutefois au niveau mondial une hausse du nombre de hackers faisant usage de cette technique.

L'hacktivisme est une forme de piratage au service de certaines convictions. "Une pratique que j'ai déjà souvent vue", affirme Thijs Feryn. "Il y a deux ou trois étés, des hackers turcs ont détruit des leads (contacts commerciaux) et placé un message politique sur la page d'accueil d'un site web. Le terme utilisé à cet effet est 'défacement' (defacing). Il y a moins d'hacktivisme ces dernières années. Mais le piratage commercial est encore très courant", poursuit-il. "Un exemple est le détournement de noms de domaine. Dans ce marché florissant, des techniques sont utilisées pour faire grimper factuellement la valeur du nom de domaine en redirigeant illégitimement un grand nombre de visiteurs non réels vers le site en question par le biais du hacking. De ce fait, la valeur du nom de domaine augmente et le vendeur malhonnête peut demander un prix supérieur."

Problème technique ou erreur humaine ?

Que faire si l'on remarque une irrégularité ? "Prenez contact avec votre fournisseur d'accès et faites-lui constater ce qui se passe, conseille Thijs Feryn. Ce n'est qu'après que vous pouvez réfléchir aux causes et aux mesures à prendre."

Tant Marc Blanchard que Thijs Feryn s'accordent à dire que la sécurité est une question de bon sens, qu'il faut se faire conseiller par un expert et même se tenir au courant des pratiques des cybercriminels. "Nous avons encore beaucoup de travail pour rendre l'Internet étanche à la fraude, estime Thijs Feryn. De plus, il faut que tout le monde utilise les technologies de sécurité, car c'est tous ensemble que nous devons colmater les fuites. Sinon nous n'arriverons à rien." ◀

"L'Internet, tel qu'il existe aujourd'hui, n'a jamais été conçu pour être exploité commercialement"