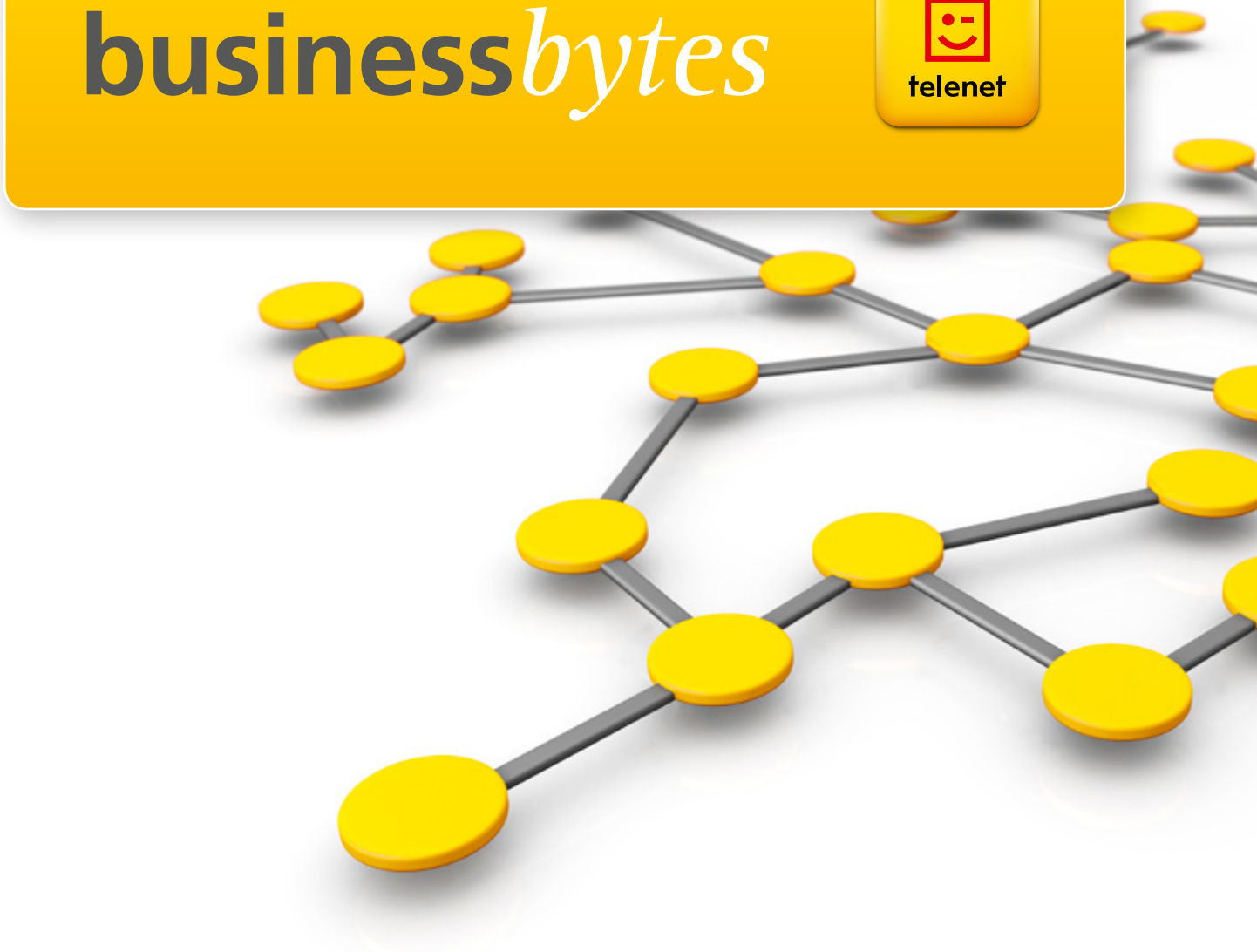
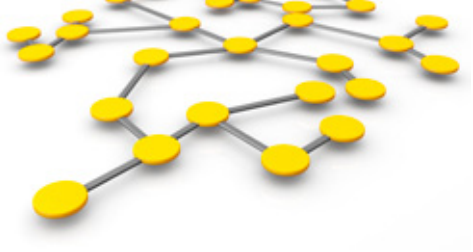
businessbytes

telenet



La sécurité de l'information
Tendances, dangers et solutions

dossier



Tendances

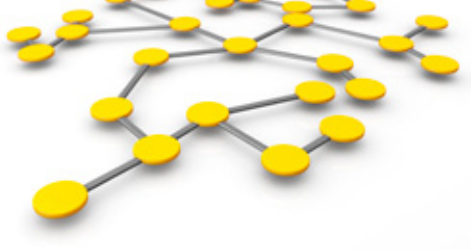
Dangers

Solutions

Quel est le degré de sécurité des nouvelles méthodes de travail ?

Les travailleurs répondent à leurs mails professionnels depuis leur domicile et consultent de temps à autre une mise à jour Facebook au travail. Ils apportent leur appareil privé au bureau et partagent des fichiers dans le cloud. Ces nouvelles méthodes de travail accroissent la compétitivité des entreprises mais peuvent rendre leurs données plus vulnérables maintenant qu'elles ne circulent plus dans un système fermé. Les entreprises disposant de multiples appareils personnels et non contrôlés risquent non seulement de perdre d'importantes données, mais sont aussi plus exposées aux logiciels malveillants.

Comme de nombreux managers - voire certains experts IT - sont encore peu familiarisés avec les implications en matière de sécurité, ce dossier en expose les grandes lignes. Vous y apprendrez où résident les défis et à quels éléments votre entreprise devrait consacrer son attention. Nous vous aiguillerons également vers des solutions alliant confort d'utilisation, productivité et sécurité.



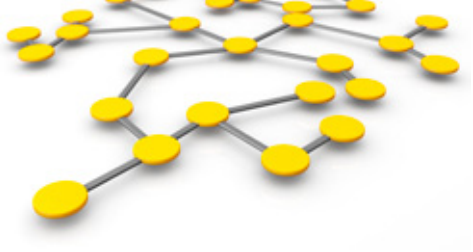
« Tout est interconnecté »

Christophe Huygens, consultant en sécurité et professeur à la K.U.Leuven

L'un des nouveaux termes à la mode dans le secteur des technologies est solomo. Cet acronyme désigne l'avancée et la fusion des médias sociaux, locaux et mobiles. Pour Christophe Huygens, expert en sécurité et professeur au département Informatique de la K.U.Leuven, c'est l'un des deux phénomènes importants à court terme pour la sécurisation des données et réseaux. Le second est le 'cloud computing' (informatique en nuage). À plus long terme, il estime que les principaux défis des experts en sécurité résideront dans l'évolution de l'Internet of Things (IoT) et de la communication machine-to-machine (M2M).

Solomo, le cloud et l'Internet of Things

«La principale tendance est sans conteste la disparition du périmètre de sécurité de l'entreprise», explique Huygens. «Vu le succès des appareils personnels tels que le smartphone, il n'est plus possible d'isoler hermétiquement une entreprise. Ce sont surtout les nouveaux dispositifs mobiles qui compromettent la sécurité. Les entreprises doivent y remédier en adaptant leur politique et en prenant des mesures directement axées sur les appareils. Ce sont essentiellement les applications qui posent problème. Chez Apple, la situation n'est pas trop préoccupante car leur App Store pour l'iPhone est un 'walled garden' (jardin clôturé) relativement sûr. On y contrôle encore ce qui entre. Mais ce n'est pas le cas pour Android : tout y est possible, ce qui alimente le débat en cours sur un 'kill switch', un système permettant d'effacer à distance des applications dangereuses sur un appareil. Les autorités européennes se montrent prudentes sur ce plan et je les comprends du point de vue de la protection du consommateur. Mais dans le contexte d'une entreprise, je pense qu'une telle intervention doit être possible. En tous les cas, les entreprises doivent établir une politique d'utilisation acceptable, de sorte que les travailleurs sachent ce qui est toléré ou interdit. Elles doivent certifier des applications pour le téléchargement afin que les travailleurs puissent discerner celles qui peuvent ou non se retrouver sur le réseau de l'entreprise.»



Médias sociaux : pas pour les applications critiques

Le 'mo' de solomo est le principal souci en termes de sécurité. Huygens est moins préoccupé par les applications locales et sociales. Pour lui, la sécurisation des médias sociaux est 'très faible', mais le problème n'est pas d'ordre technique. «Twitter et Facebook connaissent des accidents presque chaque semaine. On pourrait pourtant renforcer considérablement la protection de ces réseaux. Mais le manque de sécurisation est étroitement lié au marketing, à l'effet inhibant des mesures de sécurité sur le nombre d'utilisateurs. Comme la valeur d'un réseau social augmente avec son affluence, leurs gestionnaires n'insistent pas trop sur la sécurité. Tant que l'utilisation de médias sociaux reste innocente, c'est encore acceptable. Si les entreprises n'utilisent les médias sociaux que comme canal de marketing et non pour des applications critiques comme la diffusion de mises à jour de logiciels, je n'entrevois pas de problèmes majeurs.»

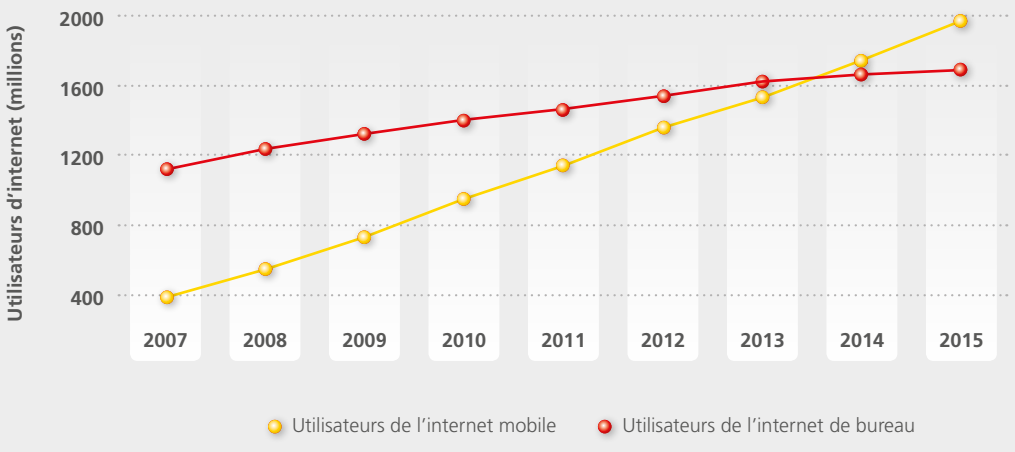
Sécurité dans le nuage

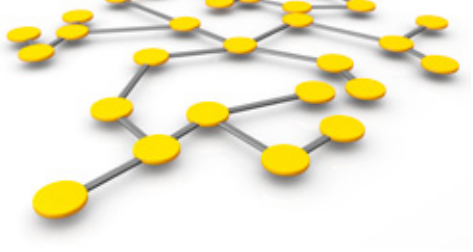
Huygens estime également le 'cloud computing' acceptable car sur le plan technique, il peut être utilisé en toute sécurité. Huygens pense néanmoins que beaucoup de gens évaluent mal son impact. «Si vous recourez au cloud computing, votre connexion internet devient nettement plus importante. Vous avez besoin de plusieurs connexions et

Expansion mobile

Pour la société américaine Morgan Stanley, l'expansion des dispositifs mobiles a pris une telle ampleur que dans quelques années, le nombre d'utilisateurs de l'internet mobile aura dépassé celui des utilisateurs de bureau. Cette évolution a également déplacé les pôles d'attention des criminels et oblige les experts en sécurité à se concentrer davantage sur la sécurisation mobile.

Évolution de l'utilisation d'internet





Services administrés

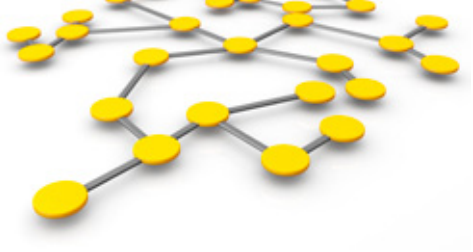
D'après le professeur Huygens, de nombreuses solutions peuvent offrir une protection adéquate aux réseaux et appareils des entreprises. Il s'agit néanmoins de solutions partielles qui doivent encore être intégrées, ce qui demande de l'expertise et des services de consultance. «La sécurisation est si spécifique que seules les très grandes entreprises peuvent acquérir et conserver les compétences appropriées en interne. Les services administrés constituent une solution bien plus opportune pour la plupart des entreprises. C'est alors un partenaire de confiance qui assume la protection des systèmes.»

▸▸ d'une fiabilité supérieure. Vos priorités sont donc totalement différentes sur le plan des risques. Bien entendu, il faut tout crypter sans toutefois oublier d'adapter vos processus et procédures. Ainsi, vous aviez précédemment une maîtrise totale du back-up et de la restauration mais ce n'est plus le cas avec le cloud computing. L'exécution d'un audit devient aussi bien plus difficile. À cela s'ajoutent les implications juridiques. Si vos données se trouvent dans un autre pays, quelles en sont les conséquences ? La législation du Luxembourg n'est pas la même qu'en Irlande. Avant de se lancer dans le cloud computing, il faut répondre à ces questions.»

Internet of Things

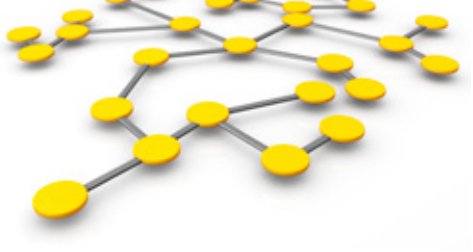
Un tout nouveau défi se profile également dans le long terme : l'Internet of Things. Divers objets, machines et emplacements sont connectés via internet, ce qui leur permet d'échanger des informations entre eux ou avec des gens. Cette tendance a déjà commencé. Christophe Huygens : «Tout sera interconnecté, ce qui entraînera une augmentation spectaculaire du nombre moyen d'appareils par personne - mille d'ici 2015-2020, d'après certaines estimations prudentes. Dans le secteur de la logistique, par exemple, nous pourrons équiper chaque paquet d'une plaquette active, afin de pouvoir le suivre à la trace. Dans les maisons de repos, les pensionnaires recevront un petit appareil permettant de les retrouver rapidement. Et sur un champ, on sèmera des milliers de dispositifs minuscules avec les semences afin de pouvoir mieux suivre la culture. Cette évolution suscite des questions inédites en termes de sécurité. Ainsi, par exemple, comment allons-nous établir une confiance dynamique entre des appareils au sein d'un réseau ? Comment allons-nous contrôler certaines opérations de machines ? Pour ce faire, nous aurons besoin d'analyses comportementales des appareils ainsi que de petits firewalls spécifiques aux applications et conformes aux politiques d'entreprises. Cette problématique fait d'ores et déjà l'objet de travaux intensifs, y compris dans notre centre de recherche.» ■

Christophe Huygens est consultant en sécurité et professeur à la K.U.Leuven. Il a contribué à la création de NetVision/Ubizen et collabore avec le groupe de recherche DistriNet de l'IBBT, spécialiste des systèmes informatiques distribués et de la sécurisation. À la K.U.Leuven, Huygens dispense des cours sur les réseaux informatiques et la sécurisation des ordinateurs et réseaux.



« Nous devons repenser entièrement notre modèle de sécurité »

Christian Van Heurck, analyste en sécurité et coordinateur de CERT.be



Les médias commentent régulièrement le thème de la cybercriminalité. Mais quelle est l'importance réelle de ces dangers et comment les abordons-nous ? CERT.be, la Computer Emergency Response Team belge, rassemble des informations sur les risques et menaces dans notre pays.

La sécurité internet en Belgique

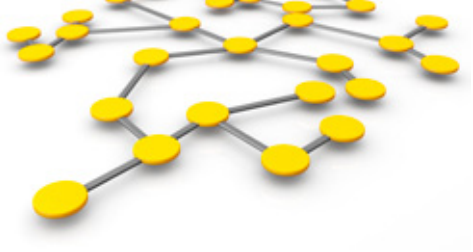
Pour Christian Van Heurck, coordinateur ad interim, l'époque 'romantique' du hacker individuel tentant de pénétrer dans le réseau d'une grande entreprise depuis son grenier est clairement révolue. Aujourd'hui, les dangers viennent essentiellement du crime organisé. Le piratage des protections d'une entreprise est devenu un business lucratif. Les cartes de crédit ou dossiers médicaux volés se négocient aisément sur le marché noir. Les logiciels malveillants sont même devenus des 'Software as a Service' (SaaS, logiciels en tant que service) que l'on peut louer avec des garanties. Pour illustrer l'ampleur des actes perpétrés par les criminels actuels, Van Heurck évoque le botnet Rustock, qui a diffusé chaque jour des milliards de spams vers environ un million d'ordinateurs infectés. «Ce type de botnet ne cesse de s'étendre et de gagner en puissance. Il sont de plus en plus difficiles à contrer car ils intègrent leur propre ▸▸

Point de contact pour les problèmes de sécurité

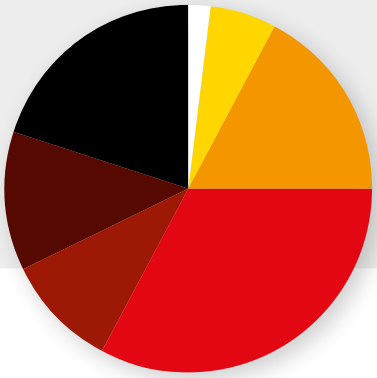
CERT.be est le point de contact national pour les menaces et vulnérabilités liées à internet. CERT.be collabore avec des organisations similaires à l'étranger. Christian Van Heurck : «Nous travaillons sur la base d'une confiance mutuelle, dans un groupe fermé de collaborateurs qui se connaissent personnellement. L'échange d'informations s'effectue par le biais de mailings restreints ou de contacts individuels, et toujours sans mention des données relatives aux entreprises concernées. Nous ne parlons entre nous que d'adresses IP.»

Signaler des incidents de sécurité
- Via CERT.be
- Par e-mail: cert@cert.be

Il est également possible d'envoyer un e-mail crypté, un fax ou de téléphoner.
Consultez www.cert.be pour plus d'informations.



Types d'incidents, premier semestre 2011



- Vol de compte ..... 2 %
- Attaques par déni de service ..... 6 %
- Spam ..... 17 %
- Piratage de systèmes ..... 33 %
- Vers et virus ..... 10 %
- Scans ..... 12 %
- Autres ..... 20 %

anti-antivirus et utilisent des techniques de cryptage et de communication toujours plus sophistiquées.»

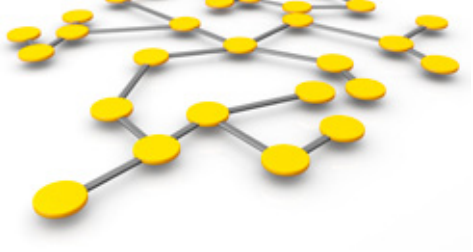
Pas de solutions miracles

Dans le contexte actuel, la sécurisation ne peut plus venir d'un produit unique, souligne Van Heurck. «Les managers d'entreprises pensent parfois qu'ils peuvent tout résoudre avec un seul produit, et certaines petites PME, qu'un antivirus récent fera l'affaire. Mais aujourd'hui c'est largement insuffisant pour pouvoir parler d'un environnement sécurisé. La tendance BYOD (Bring Your Own Device, apportez votre propre appareil) nous oblige à repenser entièrement notre modèle de sécurité. Elle a fait disparaître le périmètre de l'entreprise, de sorte qu'il n'y a, pour ainsi dire, plus aucun système de confiance. On peut difficilement lutter contre cette problématique et tout cadenasser ou interdire. Une sécurisation trop stricte peut nuire à la convivialité. Les utilisateurs vont alors chercher à la contourner, de sorte que vous favoriserez indirectement l'insécurité.» D'après Van Heurck, il n'existe pas de solutions miracles, mais bien de multiples solutions partielles. «C'est un peu comme pour les maisons et les voitures : on s'introduit d'abord là où c'est le plus facile.»

Pompiers

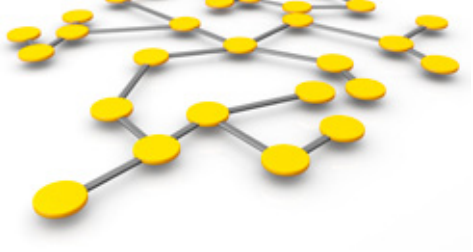
CERT.be ne donne pas d'avis concret sur les solutions de sécurisation. Van Heurck : «Nous sommes avant tout un point de contact neutre. Les entreprises ayant un problème de sécurité peuvent nous le signaler en toute confiance. Il faut nous considérer comme les pompiers et non la police. À la police, vous devez faire une déclaration. Les gens ne savent pas toujours comment procéder ; ils ont besoin de l'autorisation du haut management et craignent parfois une altération de leur image. Chez nous, ces seuils n'existent pas. Nous maintenons une confidentialité totale. Lorsque des entreprises viennent nous signaler des problèmes, nous pouvons affiner notre vue du grand ensemble et apporter une aide plus efficace. Si plusieurs parties rencontrent les mêmes problèmes, nous pouvons notamment trouver plus vite et plus aisément leurs causes communes.» ■

Christian Van Heurck est analyste en sécurité et coordinateur de CERT.be.
Il a travaillé précédemment en tant que manager de systèmes et d'applications chez CultuurNet Vlaanderen, et IT Manager chez Telepolis.



« Les managers et les utilisateurs finaux sont des maillons cruciaux de la chaîne »

Xavier Mertens, Principal Security Consultant chez Telenet



La sécurité est bien plus qu'une solution technique, déclare Xavier Mertens, Security Consultant chez Telenet. Pour assurer une protection efficace, il est extrêmement important que les managers d'entreprises et experts en sécurité se comprennent et que les utilisateurs finaux soient conscients de toute la problématique en termes de sécurité. «Beaucoup de choses sont possibles sur le plan technique, mais les managers et utilisateurs finaux ont aussi un rôle à jouer.»

Gestion des risques dans la pratique

Xavier Mertens : «Un manager qui n'a pas connu (beaucoup) d'incidents en matière de sécurité s'intéressera au coût de la protection et se demandera – très logiquement - si elle est absolument nécessaire. À titre d'exemple, un système de gestion de journal de bord, qui permet de suivre les événements de votre réseau, est indispensable sur le plan de la sécurité. Avec un tel système, vous pouvez en effet voir ce qui s'est passé et qui est concerné. Il y a, évidemment, des coûts à la clé qui rendent certains managers réticents. Mais il faut considérer un tel système comme une assurance. Le risque que votre maison prenne feu est relativement limité. Pourtant, tout le monde paie une prime d'assurance pour en être préservé. Il en va de même pour la protection des données et réseaux. Un seul incident peut avoir un profond impact sur le fonctionnement et l'image de votre entreprise. Vous avez donc besoin de systèmes de sécurité adéquats.»

Sensibilisation

Les utilisateurs finaux ne perçoivent pas toujours non plus l'intérêt d'une protection. Ils ne veulent ▸▸

Approche de l'architecture par Telenet

La méthode de Telenet en matière de sécurisation est fondée sur une connaissance approfondie de l'architecture. Nous assurons la sélection et la mise en oeuvre des composantes les plus adéquates sur la base d'une analyse de l'infrastructure existante et des besoins.
Pour plus d'informations, surfez sur www.telenet.be/security/surmesure

Formules de sécurisation pour petites entreprises

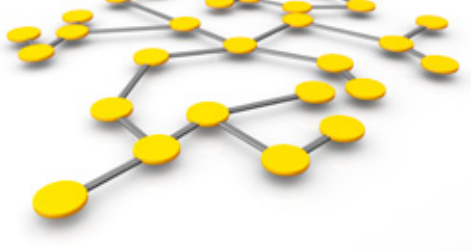
Telenet commercialise diverses solutions de nouvelle génération permettant aux petites entreprises de mieux protéger leur connexion internet. Ainsi, vous pouvez notamment bloquer certaines applications internet (Facebook, par exemple) sans couper la totalité de la connexion. Il s'agit de solutions administrées dont Telenet assure l'installation et la gestion. Elles ne requièrent ni connaissances ni investissements en matériel informatique.
www.telenet.be/security/formules

rien perdre en convivialité ou fonctionnalités pour un surcroît de sécurité. Xavier Mertens estime qu'ils constituent le maillon faible dans la chaîne de sécurité. «Pour commencer, vous courez toujours le risque que des utilisateurs malintentionnés circulent dans votre organisation. Ou des gens qui altèrent volontairement la sécurité, par exemple parce qu'ils viennent d'être licenciés. Il est important de gérer correctement ces situations en tant qu'entreprise et de bloquer immédiatement tout accès à l'infrastructure en cas de licenciement, par exemple. Mais ce n'est pas là que résident les principaux risques, car il ne s'agit que d'un très petit groupe. Bien plus de gens compromettent la sécurité alors qu'ils agissent en toute bonne foi. Des gens qui veulent encore travailler le soir et, par exemple, emmènent des données de l'entreprise sur une clé USB. Ce sont de bons collaborateurs très motivés, mais qu'adviendra-t-il en cas de perte ou de vol d'une telle clé non protégée ? Qu'adviendra-t-il si les données sont chargées sur un ordinateur non protégé à la maison ? Les programmes de sensibilisation sont très importants pour attirer l'attention des collaborateurs sur ce type de problèmes. Parfois aussi, certaines personnes agissent de façon dangereuse car autrement, elles ne pourraient tout simplement pas travailler. À titre d'exemple, elles donnent leur mot de passe parce qu'il est indispensable à un collègue. Dans pareils cas, il faut évidemment adapter votre système.»

Collaboration

Pour aboutir à une solution satisfaisante pour les managers comme pour les utilisateurs finaux, il ne faut pas lésiner sur la communication, explique Xavier Mertens. «En définitive, une protection est toujours établie dans le cadre d'une concertation. En tant que partenaire, nous devons tenir compte des préoccupations budgétaires des managers, bien connaître l'infrastructure et nous imprégner des processus de l'entreprise. C'est seulement ensuite que nous allons déterminer les applications de sécurité spécifiques que nous pouvons intégrer. Et si nous optons ensemble pour une solution de sécurisation donnée, nous devons aussi pouvoir expliquer nos choix à tous les collaborateurs dans un langage intelligible. Notre tâche d'expert en sécurité va donc bien plus loin que les aspects techniques.» ■

Xavier Mertens est Principal Security Consultant chez Telenet. Véritable passionné de la sécurisation, il s'est spécialisé en Security Monitoring, Reporting et Auditing ces dernières années. À l'instar des autres experts en sécurité de Telenet, il affine ses connaissances en permanence. Xavier a ainsi décroché de nombreux certificats agréés à l'échelon international en matière de sécurité.



Glossaire

Acceptable Use Policy (AUP)
Document spécifiant les règles à respecter, les utilisations autorisées et interdites dans un réseau d'entreprise. Les collaborateurs doivent signer l'AUP pour accéder au réseau.

Botnet
Réseau d'ordinateurs infectés régi par un point de commande central afin de procéder à des activités criminelles. Un ordinateur infecté est intégré dans un botnet à l'insu de son propriétaire.

Bring Your Own Device (BYOD)
BYOD est un modèle d'entreprise permettant aux collaborateurs d'utiliser un appareil personnel (ordinateur portable, smartphone, tablette) au travail. L'intégration du BYOD est due au fait qu'il est économique pour l'employeur et rend les travailleurs plus mobiles et productifs. Cela demande néanmoins une approche spécifique de la sécurité.

Cloud computing
Utilisation partagée de serveurs, applications et autres ressources à distance, via un accès réseau simple et convivial.

Denial of service (DOS) attack
Attaque par déni de service : un grand nombre d'ordinateurs infectés, régis par un point de commande central, établissent simultanément une connexion avec un serveur, ce qui le rend indisponible ou le fait 'planter'.

Internet of Things (IoT)
Connexion d'objets, machines et lieux via internet, ce qui leur permet d'échanger des informations entre eux ou avec des utilisateurs.

Logiciels malveillants
Nom générique pour les logiciels créés avec une intention de nuire, comme les virus, vers, botnets et spywares.

Social engineering
Vol d'informations confidentielles ou secrètes en mystifiant des utilisateurs d'ordinateurs. Les e-mails demandant au destinataire de transmettre son numéro de carte de crédit ou ses mots de passe sont des formes de social engineering. Les sites de phishing (copies conformes de véritables sites Web), où les visiteurs se connectent en toute bonne foi avec des données confidentielles, en sont un autre exemple.

Solomo
Avancée et fusion des médias sociaux, locaux et mobiles. Néologisme lancé lors d'un événement chez Google, début 2011.

Walled garden
Environnement d'applications et de fichiers contrôlé. Le téléchargement à partir d'un walled garden offre davantage de garanties en termes de sécurité.