ZYXEL

www.zyxel.fr

Avis d'expert - Limonest, 30 janvier 2017

+ 51 % de cyberattaques en France en 2016 : comment limiter les risques ?

En 2016, le taux de cyberattaques a augmenté de 38 % dans le monde et, plus encore, de 51 % en France*. Malgré ces chiffres, le risque n'est pas suffisamment pris au sérieux, dans les entreprises françaises. Et pourtant... En 2015, 81 % d'entre elles déclaraient avoir subi une attaque informatique**. Manque de pédagogie ou d'informations ? Trop faible connaissance du sujet ? Comment reconnaître une cyberattaque ? Qui sont ces pirates dont il faut se méfier ? Quelles sont les menaces pour l'entreprise ? Comment limiter les risques ?... Des questions centrales auxquelles répondent les experts de Zyxel France : Pierre-Emmanuel Vincent, Directeur Technique et Charles Geismar, Chef de Produits sécurité.

Une cyberattaque, quésaquo ?

On a réellement commencé à parler de virus et de piratage informatiques dans les années 80. Globalement, ceci consiste à exploiter les failles de sécurité d'un système. Mais les moyens pour y parvenir ont changé, au fil du temps.

En 2016, **les attaques de type ransomware**, prenant en otage les données personnelles contre rançon, ont pris une importance accrue **(plus de 60 % des cyberattaques recensées)**. En concurrence directe, de nouvelles formes de piratage, nommées APT (Advanced Persistant Threat) ont vu le jour. Leur présence se multiplie, avec pour objectif de s'introduire dans un système et d'agir sur le long terme en toute discrétion (vol de données, expansion d'un virus, …).

Enfin, dernière menace en vogue, la guerre du **cyber-terrorisme** et de l'espionnage étatique qui font régulièrement la "une" des médias. Un enjeu majeur et croissant, avec des attaques persistantes et, dans certains cas, silencieuses.

D'où vient le problème ?

On imagine généralement la cyberattaque comme venant d'un tiers qui cherche à s'introduire à distance dans le système pour le verrouiller ou pour voler des données. Mais contre toute attente, l'origine est souvent bien plus proche ! Elle est même fréquemment interne à l'entreprise : **35 % des incidents sont générés par les collaborateurs !** En toute insouciance, ceux-ci cliquent sur un lien ou encore exécutent un programme malveillant qui endommage le système.

Objets connectés : le nid à microbes ?

Les objets connectés (smartphones, tablettes, etc.) que les collaborateurs utilisent accentuent le risque. En effet, lorsqu'ils sont connectés au réseau de l'entreprise, ces objets représentent autant de portes d'entrée dans le réseau que de failles de sécurité potentielles.

Face au **BYOD**, Bring Your Own Device, certaines entreprises ont fait le choix d'isoler un réseau WiFi dédié à ces équipements. D'autres optent pour le **CYOD**, Choose Your Own Device, dont le but pour l'entreprise est de laisser son collaborateur choisir son équipement pour s'assurer qu'il l'utilisera et qu'il ne cherchera pas à en connecter d'autre.

Cybersécurité : qui sont les acteurs ?

La cybersécurité consiste à implémenter des moyens de différentes natures (informatiques, humains,…) pour sécuriser un système ou un réseau informatique contre des attaques perpétrées par des pirates informatiques.
L'un des premiers acteurs de la cybersécurité, ce sont les constructeurs qui développent en permanence de nouvelles technologies. Par exemple, les 1ères générations de pare-feu permettaient uniquement de sécuriser une liaison Internet et d'établir des liaisons VPN. Elles disposent désormais de briques UTM et de services ATP (Advanced Threat Protection).
Mais les constructeurs ne sont pas les seuls concernés par cette problématique, loin de là ! Les pouvoirs publics jouent aussi un rôle prédominant. La réglementation se renforce et devient de plus en plus contraignante pour les « systèmes d'information d'importance vitale », tels que les opérateurs majeurs. On pense aussi à la **norme internationale ISO/CEI 27001** relative au système de management de la sécurité de l'information qui impose de nouvelles conditions.
Enfin, des organismes, à l'instar de **l'ANSSI** (l'Agence Nationale de la Sécurité des Systèmes d'Information), accompagnent les professionnels et les entreprises dans la sécurisation de leurs systèmes, en publiant des recommandations ou des certifications.

Quels standards adopter pour se protéger ?

Il est fortement recommandé de construire une infrastructure réseaux solide pour contrer les cyberattaques. Selon l'ANSSI, **5 % à 10 % du budget d'une entreprise devraient être alloués à la sécurité informatique**. Bien que l'infrastructure idéale soit propre à chaque entreprise, il existe toutefois des standards, tels que :

1. L'installation d'une **passerelle réseau de sécurité** (firewall), qui fera le lien entre le réseau de l'entreprise et le monde extérieur. Cette passerelle doit absolument intégrer des règles d'ouverture et de fermeture des ports.
2. Des **services UTM** (Unified Threat Management) dont le rôle sera de contrôler le flux entrant et sortant : antivirus, antispam, filtrage de contenu, contrôle applicatif.
3. Une protection logicielle des postes de travail avec un **antivirus**.
4. Une **séparation des réseaux** internes et visiteurs par l'intermédiaire de LAN ou de VLAN, avec des règles de sécurité adaptées.
5. Un **chiffrage des échanges** à distance accédant aux données et aux applications de l'entreprise via des connexions VPN.

Sécurité du réseau : quelles sont les bonnes pratiques ?

Une fois l'infrastructure réseaux installée, des actions de prévention et de maintenance sont préconisées. Il est essentiel d'agir à différents niveaux :

1. **Mettre à jour régulièrement** la solution de sécurité. Le constructeur n'ayant plus la main sur les équipements qui ont été achetés et installés, il relève de la responsabilité du client et de son intégrateur d'exécuter cette tâche.
2. **Autoriser uniquement le nécessaire**, afin de réduire au maximum le nombre de portes d'entrée dans le réseau. Par exemple, si le réseau n'intègre pas de serveur HTML hébergeant un site Internet, il est recommandé de fermer les ports réseau non utilisés correspondants.
3. **Maîtriser et contrôler les différents accès**. Seuls les collaborateurs concernés doivent avoir les droits d'administrateurs afin d'éviter au maximum la diffusion des identifiants de connexion. Dans la mesure du possible, les mots de passe doivent également être modifiés régulièrement (1 fois par trimestre au minimum).
4. **Sensibiliser et former les collaborateurs aux bons réflexes**. Ils sont souvent la 1ère cible des pirates pour pénétrer dans le réseau. Ceux-ci tirent parti des petites erreurs classiques et a priori anodines : social engineering, connexion d'une clé USB trouvée, un identifiant et un mot de passe écrits sur un post-it,

un clic sur un email publicitaire reçu,…

Check list : que faire en cas de cyberattaque ?

Si l'entreprise doit faire face à une cyberattaque, il est important d'agir rapidement et de manière efficace :

1. **Isoler les données** sensibles et les données infectées, en déconnectant les serveurs, voire même le réseau de l'entreprise.
2. **Identifier les failles et les systèmes infectés** afin de mieux comprendre la source de l'attaque et les risques.
3. **Prendre contact avec les éditeurs et constructeurs** concernés pour mettre en œuvre les procédures correctives.
4. **Sécuriser les accès** qui auraient pu être corrompus par les pirates et changer les mots de passe.

** Selon une étude du cabinet PricewaterhouseCoopers.*
*** Selon un sondage OpinionWay.*

CONTACTS PRESSE : AGENCE OXYGEN - @OXYGEN_Lyon

Julie Munoz
juliem@oxygen-rp.com
06 24 70 07 70

Anne Masson
anne@oxygen-rp.com

A propos de Zyxel Communications : Fondée en 1989, ZyXEL Communications Corp. compte parmi les premières entreprises mondiales fournisseurs de solutions d'accès à Internet innovantes et de qualité. Pionnière dans la fabrication de modems, ZyXEL Communications Corp. a continuellement évolué. Elle fournit aujourd'hui des solutions réseaux adoptées par plus de 400 000 entreprises et 100 millions d'utilisateurs à travers le monde. Elle est l'une des rares sociétés dans le monde capables d'offrir des solutions réseau complètes (CPE et solutions xDSL, routeurs LTE, solutions de sécurité unifiées, hotspots, NAS, Switch, contrôleurs et points d'accès WiFi). Elle adresse aussi bien les opérateurs que les professionnels, de la TPE à la grande entreprise, que les particuliers. Les produits ZyXEL sont distribués dans 70 pays par 30 filiales. ZyXEL compte parmi le Top 20 des marques taïwanaises rayonnant à l'international.

A propos de Zyxel France : Créée en 1996 et basée près de Lyon (69), ZyXEL France compte une trentaine de collaborateurs au service de ses clients. La société commercialise les produits Zyxel via son réseau de distributeurs. Elle propose également un ensemble de services à ses clients, allant de la formation à la certification, ainsi qu'un service avant et après-vente technique pour l'assistance de ses clients.
Plus d'infos : www.zyxel.fr

Zyxel France est présent sur les réseaux sociaux !
Retrouvez toutes les nouveautés du marché IT ainsi que l'actualité ZyXEL :
événements, formations, promotions, nouveautés produits et services, success stories…