MENACES NUMÉRIQUES : ÉVOLUTION DES ATTAQUES DANS L'ENTREPRISE, COMMENT SE PROTÉGER ?

A l'ère du tout connecté, tant en interne qu'à l'externe, la surface d'attaque possible s'élargit, offrant aux intrusions malveillantes la possibilité de transiter partout dans le système. Une cyber-attaque, avec des conséquences financières, juridiques ou réputationnelles, peut générer une crise majeure susceptible de remettre en cause la pérennité de l'entreprise. La sécurité informatique vise à prévenir les incidents et à les gérer mais ne prépare pas l'organisation à faire face aux conséquences.

Le salon Expoprotection (du 7 au 9 novembre 2016, Porte de Versailles – Pavillon 5), référent en matière de prévention et de gestion des risques, est l'occasion de décrypter les menaces numériques et les solutions techniques ainsi qu'organisationnelles pour s'en protéger. Le point sur les évolutions dans l'entreprise par le Clusif (Club de Sécurité de l'Information Français), partenaire de l'événement.

Dépendance de l'entreprise vis à vis de son système d'information

Le niveau de dépendance est la conséquence de l'automatisation des processus métier de l'entreprise. De ce fait, la taille, la complexité et donc la « surface attaquable » d'une structure a une tendance naturelle à s'élargir. Cette augmentation n'est pas mauvaise en soi puisque l'entreprise gagne en même temps en efficacité. Toutefois, ce gain n'est réel que si des mesures de protection appropriées sont mises en œuvre pour contrer les attaques et même les failles non intentionnelles.
Utilisés en local ou par l'intermédiaire des réseaux de télécommunication, les systèmes d'information présentent des fragilités liées à divers risques dont les sources peuvent être environnementales (météo, incendie…), intrinsèques (conception, technologies…) et humaines (internes, externes, délibérées, par erreur ou par négligence).

Ces vulnérabilités sont multipliées notamment par la complexité du système, le nombre d'utilisateurs, le volume et la diversité des informations traitées, le partage d'infrastructures communes ou encore les usages nomades. Le recours aux services du Cloud, de plus en plus fréquent dans les entreprises, ou encore l'augmentation des connexions des appareils internes ou externes vers le système d'information de l'entreprise ouvrent potentiellement de nouvelles brèches.

Les incidents de sécurité sur les systèmes d'information sont de nature à prendre connaissance, altérer et détruire les informations. Leurs impacts peuvent aller de la simple difficulté de fonctionnement d'un service durant quelques heures, au vol de données, à la dégradation de l'image et de la confiance, à l'atteinte à la personne, jusqu'à la destruction du système d'information et la faillite.

Typologie des attaques et leur évolution

L'entreprise, de plus en plus connectée (circuits logistiques et comptabilité numérique clients/fournisseurs…), est nécessairement plus ouverte en sortie mais également en entrée. L'attaquant dispose donc d'un grand nombre de canaux d'intrusion. Il peut être **interne,** des employés ou sous-traitants de l'entreprise qui agissent par méconnaissance, insouciance ou malveillance, ou **externe** avec, parfois, la collaboration de l'interne (recherche de profit). Enfin, notons que bien des attaques externes sont déclenchées depuis l'intérieur de l'entreprise, par le simple clic d'un employé sur une pièce jointe malveillante.
Les 4 principales catégories de menace sont les atteintes à l'image (défiguration d'un site ou déni d'accès), les vols de données ou des demandes de rançon, l'espionnage économique et le sabotage matériel.

Si le type d'attaque évolue peu d'un point de vue technologique – intrusion d'un Malware pour obtenir un mot de passe, des informations ou entrainer des dommages jusqu'au formatage du disque dur - l'intelligence des attaques augmente notamment dans le développement du Ransomware. Ce système logiciel permet l'intrusion d'un objet malveillant capable par une simple action de paralyser l'ensemble du système dont la maitrise sera restituée moyennant le versement d'une rançon.

Cette nouvelle forme de « racket » d'abord utilisé auprès des consommateurs s'attaque désormais aux entreprises. Aussi, les pirates font évoluer leurs méthodes de « rançons » - menaces de blocage, de destruction, de vol et de divulgation d'informations sensibles… via des trojans (cheval de troie) type Cryptolocker de plus en plus sophistiqués. Ces derniers sont capables de chiffrer la sauvegarde puis le disque dur et donc des données auxquelles il n'est plus possible d'avoir accès sans acheter la clé de décryptage. La garantie de voir le chiffrement des données rétabli après règlement étant très faible.

Toute cette intelligence est de plus en plus facile d'acquisition sur les marchés noirs des outils d'attaques numériques, Darkweb.

Comment les entreprises font face aux menaces numériques

Les grandes entreprises, notamment celles qui en raison de la nature de leurs activités ont une culture de sécurité très forte, déploient d'importants moyens humains, technologiques et d'organisation en matière de lutte contre la cybercriminalité.

Les structures comme **les OIV** (Opérateurs d'Importance Vitale) ou **les SAIV** (Secteurs d'Activité d'Importance Vitale) sont soumises à des réglementations de sécurité numérique spécifiques (loi de programmation militaire 2013). Ce cadre réglementaire complété depuis janvier 2016 par la directive Européenne NIS (Network and Information Security) devra être transposée dans le droit français **d'ici 2018.** Celle-ci concerne, **outre les OIV** (dont la qualification s'élargit à la notion d'opérateurs essentiels), **les fournisseurs de services numériques** comme les moteurs de recherche, les sites de e-commerce ou encore les fournisseurs de Cloud.
Enfin, **les entreprises qui collectent, traitent et stockent les données personnelles** devront se conformer au règlement européen de protection des données personnelles voté en avril 2016 et applicable en 2018.

Si les grands groupes développent des dispositifs structurés de cyber-sécurité, **les ETI, PME et TPE ne disposent pas, pour la plupart, de moyens suffisants pour s'organiser. A minima, elles mettent en place des solutions de protection périmétrique** pour se protéger des menaces extérieures. La sécurité de leurs réseaux est assurée par une ligne pare-feu et autres équipements défensifs (Firewall, antivirus, antispam), par le choix de services internet (type messagerie) sécurisés ou encore d'outils de gestion des connexions à l'entreprise et de contrôle d'accès au système. Cependant, les utilisateurs, étant de plus en plus hors site, se connectent via Internet ou des terminaux et services mobiles. Les données et applications des entreprises résident souvent dans le Cloud. **La menace qui se réalise à l'intérieur de l'entreprise est une réalité de plus en plus prononcée**, qu'elle trouve son origine dans une malveillance assumée ou bien dans une compromission bien involontaire (méconnaissance, erreur ou négligence).

Sensibilisation pour prévenir et Cyber-résilience pour corriger

Le personnel interne doit être en mesure de défendre l'entreprise et non risquer de l'attaquer. Les **actions de sensibilisation** n'ont plus pour objectif la transmission des simples bonnes pratiques mais doivent rendre le personnel véritablement réceptif à « l'existence du mal » (malveillance, négligence, méconnaissance, erreur, non prévisible…) à travers divers champs : protection du poste, intrusion réseaux, malveillance téléphonique, fuite d'information, protection des informations, bons usages et réactions…

Malgré les dispositifs défensifs, le système d'information reste un monde ouvert dans lequel l'attaque ne pourra pas toujours être évitée. Il est nécessaire de privilégier à la protection, la mise en place d'un processus de résilience.

En effet, le périmètre de cyber-sécurité couvre essentiellement la réduction des risques et la résolution des incidents de sécurité de l'information. **La cyber-résilience est beaucoup plus large et couvre à la fois la préparation à subir des attaques (prévention) et par-dessus tout à pouvoir continuer et reprendre une activité normale (correction)** très rapidement **après une attaque**. Elle vise à gérer la sécurité en adoptant une approche globale impliquant à la fois les individus, les processus et la technologie. Elle impose une méthodologie à la fois solide et évolutive de gestion, d'analyse et d'optimisation des risques. Elle s'appuie sur cinq piliers que sont la **préparation/identification, la protection, la détection, la résolution des problèmes et la récupération**. Les entreprises doivent absolument accepter de passer de la cyber-sécurité à la cyber-résilience et en tirer des avantages stratégiques mais grand nombre d'entre elles trouveront difficile de faire la transition par elles-mêmes. Elles pourront faire appel à un partenaire, consultant externe, s'appuyant sur des processus et des outils avancés.
(Sources le Clusif : https://www.clusif.fr/)

A propos de
Le CLUSIF, Club de la sécurité de l'information français, est un club professionnel constitué en association indépendante (Association Loi 1901). Ouvert à toutes les entreprises et collectivités, ce club rassemble des Offreurs et des Utilisateurs issus de tous les secteurs de l'économie. L'objectif principal du CLUSIF est de favoriser les échanges d'idées et de retours d'expériences au travers de groupes de travail, de publications et de conférences thématiques. Les sujets abordés, en relation avec la sécurité de l'information, varient en fonction de l'actualité et des besoins des membres de l'association.
Le CLUSIF a pour finalité d'agir pour la sécurité de l'information, facteur de pérennité des entreprises et des collectivités locales. L'enjeu actuel est donc de contrôler l'exposition au risque général, et au risque associé au système d'information en particulier.

A DÉCOUVRIR SUR EXPOPROTECTION 2016

DES EXPERTS EXPOSANTS/PARTENAIRES DU SALON EXPOPROTECTION 2016

Spécialistes dans leur métier, ils se tiennent à la disposition des médias pour faire le point et échanger sur les problématiques de Cyber-attaques.

Club de Sécurité de l'Information Français (Clusif) - https://clusif.fr/
Contact presse : Audrey Thiemonge - audreyd@oxygen-rp.com

Information Systems Security Association (Issa) - http://securitytuesday.com/
Contact presse : Diane Rambaldini – diane@securitytuesday.com

Corpguard - http://www.corpguard.com/fr/
Contact : 04 26 02 48 13

A propos du Salon Expoprotection

Expoprotection est l'unique événement en France qui rassemble les meilleurs spécialistes internationaux, les équipements et solutions les plus innovants, qui associe des conférences et des espaces de rencontres, au sein de deux univers complémentaires : risques professionnels, naturels & industriels et risques malveillance & feu.

***Rappel des chiffres de l'édition 2014** : 690 exposants, dont 39 % d'internationaux, 21 340 visiteurs uniques dont 17 % d'internationaux en provenance de 100 pays*

A propos de REED EXPOSITIONS - www.reedexpo.fr

Présent sur 20 secteurs d'activité, avec 52 salons leaders dont Batimat, EquipHotel, IFTM-Top Resa, Expoprotection, Pollutec, Midest, SITL, Maison & Objet, Fiac, Paris Photo, Nautic... et 51 sites internet, Reed Expositions apporte à ses clients les contacts, les contenus et les réseaux pour accélérer leur développement. Plus de 24 400 entreprises et 1,58 million d'acheteurs français et étrangers sont clients de ses événements.*

Reed Expositions fait partie du groupe Reed Exhibitions, premier organisateur mondial de salons et leader sur le marché français avec plus de 60 manifestations et 2 filiales, Reed Expositions France et Reed Midem.

**organisé par la SAFI, filiale de Reed Expositions et d'Ateliers d'Art de France*

Reed Expositions France
Laila Boudrar >> laila.boudrar@reedexpo.fr

CLC Communications
6 rue de Rome 75008 Paris – 01 42 93 04 04
Jérôme Saczewski >> j.saczewski@clccom.com
Anne-Claire Berthomieu >> ac.berthomieu@clccom.com
Ségolène Thion >> s.thion@clccom.com