

## **Cyber-sécurité en entreprise : 6 idées reçues**

### **Sécurité**

Posté par : JulieM

Publié le : 28/5/2018 13:00:00

## **1 - Tous les emails que j'envoie sont sécurisés**

La messagerie électronique reste un des vecteurs les plus vulnérables aux cyber attaques. Les hackers redoublent d'ingéniosité utilisant l'usurpation d'identité, la réponse d'urgence ou encore le mail d'un collaborateur pour mener à bien leurs opérations.

D'après une étude de SANS, 46 % des attaques seraient exécutées par un employé ayant cliqué sur un lien contenu dans un email.

A l'instar d'une carte postale, le courriel, impliquant très souvent des données confidentielles, peut être lu par tout le monde s'il n'est pas chiffré. Même si de nombreuses solutions de sécurité existent, beaucoup d'entreprises ne procèdent pas à un chiffrement de bout en bout de leurs messageries.

## **2 - Une information personnelle n'est pas une information sensible**

C'est faux et c'est le RGPD - Règlement Général sur la Protection des Données - qui le dit. Texte de loi développé pour servir le droit fondamental de chaque citoyen à la protection de sa vie privée et de ses données personnelles, il sera mis en application le 25 mai 2018 et cible l'ensemble des sociétés, européennes ou mondiales, publiques comme privées, qui traitent des données à caractère personnel de personnes résidant en UE.

Utilisée à des fins de revente, d'usurpation d'identité ou d'espionnage, la donnée personnelle est devenue le nouveau graal des cybercriminels. Pour exemple, l'incident de sécurité en 2017 d'Equifax, une société de crédit américaine qui a mis en péril la confidentialité de 143 millions de personnes aux Etats-Unis.

## **3 - C'est le matériel informatique qui est le principal vecteur de fuite de données**

Identifier les risques et implémenter les meilleures solutions technologiques ne doit pas faire oublier le rôle que peuvent avoir les collaborateurs en matière de protection de leur entreprise. Les professionnels de l'informatique le savent : l'humain reste le maillon faible en termes de sécurité.

Selon un récent rapport Kaspersky : 46 % des incidents de sécurité seraient causés par des employés de l'entreprise et dans 40 % des organisations, ces derniers dissimuleraient même les incidents de sécurité à leur service informatique !

Certes, les programmes de sensibilisation aident les collaborateurs à améliorer leur connaissance autour des menaces environnantes pouvant les impacter directement mais pour être optimale, cette sensibilisation doit également se jouer au niveau des directions générales.

## **4 - Le système de sécurité de l'entreprise me protège de toutes les cyber-menaces extérieures**

Encore une fois l'humain peut devenir le vecteur d'infection. Capitalisant sur les faiblesses

humaines, le phishing ou tentative d'hameçonnage est une technique d'ingénierie sociale et l'une des armes de prédilection des cybercriminels pour atteindre leurs objectifs.

D'après un rapport de Webroot, 1 385 000 sites uniques de phishing sont créés chaque mois, la grande majorité des noms de domaines utilisant l'identité de sites de confiance pour tromper les utilisateurs.

Le spear phishing est une méthode d'attaque utilisant un courriel d'apparence légitime pour inciter le destinataire à transmettre des informations confidentielles ou lui demander de cliquer sur un lien qui téléchargera un logiciel espion ou un programme malveillant.

Pour que l'attaque réussisse, la source doit se présenter comme une personne connue ou de confiance, les informations contenues dans le message doivent être cohérentes et ne pas présenter d'anomalies typographiques ou syntaxiques et la demande de l'expéditeur doit s'inscrire dans une logique.

### 5 - Les virus existent seulement sur Windows

À la question les Macs et les iPhones sont-ils mieux protégés que les plates-formes Windows, on peut inévitablement répondre NON. À l'instar de l'ensemble des systèmes d'exploitation, Mac Os et Android possèdent des failles largement exploitées par les cybercriminels et tous les experts de la sécurité s'accordent à dire que ce phénomène ne va aller en s'accroissant.

DOK par exemple, fut l'un des premiers malwares sur Mac à utiliser une campagne de phishing à grande échelle et des smartphones Android chinois ont même hébergé leur insu un programme malveillant, passé sous les radars des antivirus.

### 6 - Je suis le seul à courir un risque si j'installe une application sur mon ordinateur

Les ordinateurs étant généralement connectés à un réseau, une application hébergeant un malware peut être ainsi le point de départ pour toucher l'ensemble de l'entreprise et se diffuser ensuite à travers le monde. L'exemple le plus marquant est le ransomware wannacry.

Utilisant une faille du système Windows pour infecter l'ensemble du parc informatique de l'entreprise ciblée, il chiffrait les données pour les rendre inaccessibles réclamant à l'entreprise une rançon en échange de leur déchiffrement.

Des grands groupes mondiaux comme Telefonica en Espagne, ou encore Renault, ont été touchés par ce ransomware dont la diffusion a été extrêmement rapide, scannant les réseaux internes et Internet pour se propager.