Zeitschrift: Revue Militaire Suisse
Band: - (2018)
Heft: [2]: Numéro Thématique 2

Artikel: La cyber-hygiène
Autor: Pélissier, Albert
DOI: https://doi.org/10.5169/seals-823465

Cyber

La cyber-hygiène

Albert Pélissier
Président, Pélissier & Partners, Nyon

Selon une étude publiée par KPMG, 88% des entreprises auraient été victimes de cyberattaques en 2017 contre 54% l'année précédente. Le constat de cette étude est non seulement un révélateur de l'accroissement des menaces mais également de la protection au sein des entreprises en terme de cybersécurité. Ce chiffre aurait toutefois pu être réduit si les règles de base de cybersécurité avaient été respectées. En effet, bien qu'un bon nombre d'entreprises investissent dans des solutions de sécurité informatique, beaucoup d'entre elles ne suivent pas les règles de bases en matière de sécurité informatique.

Ces règles de bases constituent un guide d'hygiène informatique communément appelé: la cyber-hygiène. La Cyber-hygiène permet de garantir une protection des terminaux et systèmes informatiques et de mettre en œuvre les meilleures pratiques en matière de cybersécurité.

Avant toute chose, il est important de prendre conscience que la menace est partout et que chaque entreprise est une cible potentielle. Les entreprises de type PME-PMI minimisent le risque de subir une cyberattaque. Elles pensent souvent à tort, qu'elles ne sont pas assez importantes pour susciter l'intérêt des cybercriminels. Or, il apparaît que les petites et moyennes entreprises constituent en grande partie le résultat de l'étude susmentionnée. Qu'il s'agisse, par exemple, de malveillances visant à la destruction de données ou d'espionnage économique et industriel, les conséquences des attaques informatiques pour les entreprises sont généralement désastreuses et peuvent impacter leur pérennité.

Si les contraintes financières des petites structures restent un frein à la construction d'une cybersécurité optimale, il existe des bonnes pratiques peu coûteuses et faciles à mettre en œuvre permettant de limiter une grande partie des risques liés à l'usage de l'informatique.

La cyber-hygiène est à la portée de toutes les entreprises, qu'importe sa taille ou son secteur d'activité: les règles qu'elle préconise sont simples à appliquer. Le plus difficile sera peut-être de mettre en pratique ces habitudes essentielles qui relèvent pourtant de réflexes simples.

A propos de réflexes simples, nous en appliquons quotidiennement dans notre vie pour des raisons d'hygiène de vie par exemple. Cependant, pour les appliquer, il a fallu comprendre leur utilité, les apprendre et les mettre en pratique. Voici un parallèle très simple à titre d'exemple. Lorsque nous éternuons, le reflexe est de mettre notre main ou un mouchoir sur la bouche afin de ne pas propager nos microbes ou encore lorsque nous nous lavons les mains avant chaque repas ou à la sortie des toilettes... La cyber-hygiène est tout simplement l'équivalence de l'hygiène dans la vie virtuelle. Il s'agit ni plus ni moins de réflexes et automatismes à adopter afin de prendre soin de notre vie numérique. Une simple faille peut nous rendre vulnérable et dévoiler notre vie privée tout comme l'hygiène de vie peut aussi nous rendre vulnérable comme lorsque nous tombons malade: nous ne disposons pas de toutes nos facultés et des personnes malveillantes pourraient en abuser. Tout comme l'hygiène qui sert à prendre soin de soi, La cyber hygiène c'est prendre soin de la sécurité informatique de son entreprise.

L'un des exemples le plus parlant est sans doute l'attaque WannaCry. Les malwares de ce type se propagent rapidement en exploitant des vulnérabilités logicielles connues, que les entreprises ou individus ne prennent pas toujours le temps de corriger. Le botnet Mirai a ainsi utilisé environ 100'000 équipements connectés non sécurisés, à l'instar de caméras de sécurité, pour submerger le fournisseur de services Dyn, entraînant une panne gigantesque qui a mis hors ligne nombre de sites Web. En clair, WannaCry et Mirai ont pu se propager grâce à une hygiène informatique défaillante de la part des utilisateurs.

La cybersécurité évolue rapidement et sûrement. C'est pourquoi les règles sont toujours plus nombreuses. Afin de comprendre les bases de la cyber-hygiène, voici un petit « échantillon » des règles importantes qui devraient être appliquées par toutes les entreprises.

Le choix d'un mot de passe

Un mot de passe unique doit être défini pour chaque compte. Les mots de passe protégeant des contenus sensibles ne doivent jamais être réutilisés pour d'autres services.

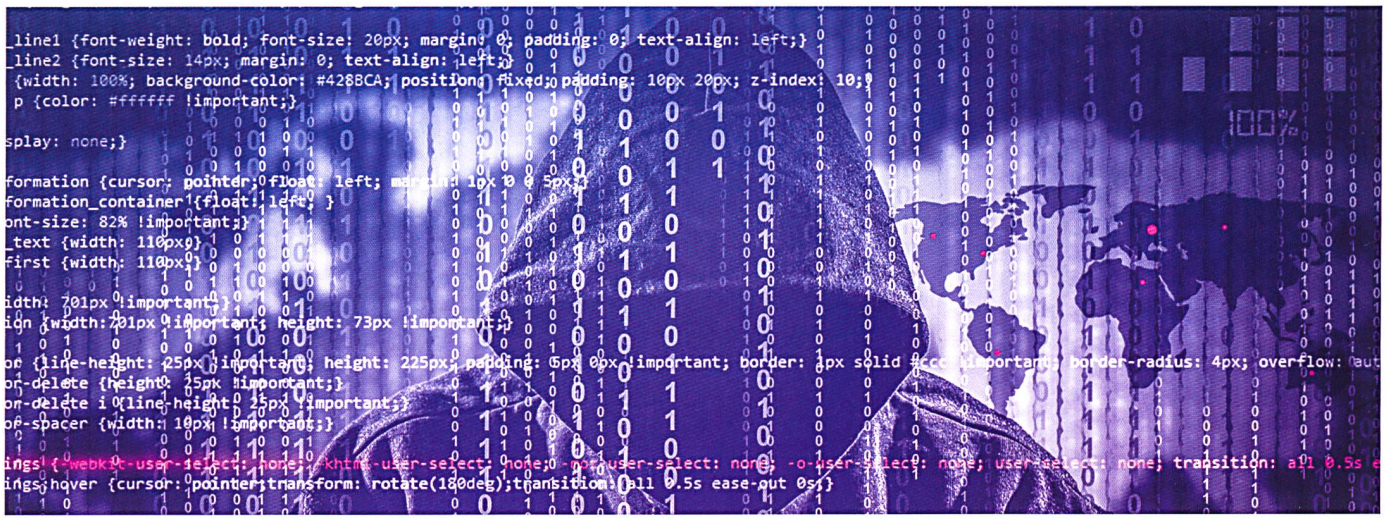
Il est souvent recommandé d'adopter un mot de passe d'au moins dix caractères, agrémenté de nombreux caractères spéciaux. C'est pour cela que de nombreux experts conseillent de choisir ce que l'on appelle une phrase de passe plutôt qu'un mot de passe. Un bon mot de passe est un mot de passe complexe et voit sa sécurité augmenter lorsqu'on y ajoute des caractères spéciaux, il est donc également vivement recommandé d'agrémenter sa phrase de passe de quelques caractères spéciaux ; un seul (un point, un guillemet ou autre) peut suffire à compliquer la tâche de ceux qui essaieraient de le deviner. Idéalement, le changement de mot de passe doit se faire tous les trois mois.

Connaissance des prestataires et utilisateurs

Afin que la sécurité soit optimale au sein d'une entreprise, il s'agit de connaître les droits d'accès de tous les utilisateurs. En effet, les droits d'accès doivent être à jour en permanence. Le service IT doit être informé sur les départs et arrivées des collaborateurs afin que leurs droits d'accès soient correctement définis. La meilleure méthode pour ne pas se perdre est de tenir un fichier à jour avec les droits relatifs à tous les collaborateurs de l'entreprise. De cette façon, le responsable pourra supprimer les droits d'accès du collaborateur sortants. Il faut une révision complète des droits utilisateurs au sein de l'entreprise. En effet, les collaborateurs ont bien souvent accès à des données dont ils n'ont pas besoin et cela peut s'avérer dommageable pour l'entreprise.

Par ailleurs, les entreprises devraient se munir d'une charte informatique afin que tous les collaborateurs puissent avoir à disposition un référentiel en terme de sécurité informatique au sein de l'entreprise.

De plus en plus d'entreprises, de nos jours, s'équipent d'un centre d'analyse cyber afin de prévenir autant que faire se peut les attaques. Mais ces moyens en « bout de chaîne » sont peu efficaces sans une prise de conscience de la responsabilité et une formation adéquate des employés.



Mise à jour des logicels

Procéder aux mises à jour des logiciels signifie corriger différentes failles de sécurité afin que de potentielles cyberattaques puissent être évitées.

Pour se faire, l'entreprise doit définir une politique de mises à jour régulières afin que tous les collaborateurs puissent utiliser leurs logiciels en toute sécurité. De plus, la plupart des mises à jour peuvent être automatiquement paramétrées. Si ce n'est pas le cas, il faut télécharger les correctifs de sécurité disponibles, les appliquer régulièrement et sans délai à toutes les applications. Les systèmes non à jour des correctifs représentent l'un des principaux facteurs de risque d'attaque. L'entreprise devra également veiller à mettre à niveau les infrastructures et systèmes vieillissants.

Sauvegardes régulières

On réalise souvent l'importance de procéder à des sauvegardes régulières trop tard, une fois confronté à une panne de disque dur ou au vol de son téléphone portable. S'astreindre à des sauvegardes n'est pas si contraignant. La sauvegarde de données se résume en trois questions : quoi ? Quand ? Et comment ? En premier lieu, il s'agit de définir les données que l'on souhaite sauvegarder. Ensuite, il faut décider à quelle fréquence ces données seront sauvegardées et enfin de la façon dont elles seront sauvegardées.

Données et mobilité

La mobilité a ouvert une brèche dans le système de protection des entreprises. Quel que soit le secteur d'activité, adapter ses procédures et ses outils devient une priorité. il est en effet complexe de sécuriser parfaitement des données tout en laissant les collaborateurs y accéder à distance.
Les collaborateurs doivent savoir identifier les données dont ils n'ont pas besoin en déplacement.
Ceci peut réduire considérablement l'impact dans le cas où vos appareils seraient volés ou perdus.

Limiter le facteur humain

Même avec la meilleure protection du monde, le risque pour votre entreprise de figurer sur la liste des prochaines victimes d'attaques au rançongiciel, de violations de données et autres menaces de cybersécurité ne sera jamais écarté. C'est pourquoi il est si important de limiter le facteur humain en automatisant autant que possible les pratiques de sécurité.

L'utilisation d'identifiants de connexion à double authentification avec mots de passe complexes, le blocage de certains types de fichiers et le test des connaissances des utilisateurs en matière de sécurité sont des mesures que toutes les entreprises peuvent prendre pour protéger les réseaux diversifiés actuels.

Les règles susmentionnées ne comptent qu'une infime partie des règles de cyber-hygiène. Chacune d'entre elles est essentielle pour le bon fonctionnement d'une entreprise.

Le bon sens et la vigilance de l'utilisateur sont et resteront toujours les armes les plus redoutables. Par ailleurs, la sensibilisation et la formation aux bonne pratiques des collaborateurs de l'entreprise aussi car comme nous l'avons précédemment mentionné, le facteur humain est bien souvent le plus sensible : il ne faut donc pas minorer les risques qu'il peut engendrer. C'est à l'entreprise d'inculquer les bonnes pratiques au même titre que les valeurs de l'entreprise. Il est également important de savoir qu'une bonne sensibilisation permettra d'accroitre la vigilance de l'utilisateur. Se sensibiliser permet effectivement de favoriser la réflexion et suscite bien souvent une prise de conscience.

La protection de nos organisations passe par la sensibilisation et la formation de chaque collaborateur, car être bien informé est déjà le premier pas vers une meilleure protection.

A. P.