Le Cabinet ACDL Expertise vous informe :

Avez-vous les bons réflexes en matière de cybersécurité ?

Contrairement à certaines idées reçues, près de huit cyberattaques sur dix viseraient les PME. Il est donc urgent d'acquérir les bons réflexes en matière de cybersécurité. Avec l'aide méconnue, aussi, des commissaires aux comptes.

Le savez-vous vraiment ? « Qui me menace et comment ? », « Quelles sont les conséquences pour les victimes de cyberattaques ? » ou encore « Quelles sont les règles d'or de la sécurité ? » Voici trois questions, parmi beaucoup d'autres, posées par le MOOC de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), accessible gratuitement jusqu'en avril 2020.

Au sommaire : des mini-cours, des quiz et surtout une mine d'informations pour s'initier aux bons réflexes en matière de cybersécurité, approfondir ses connaissances, et ainsi agir efficacement sur la protection de ses outils numériques.

« *La complexité des menaces, le coût, le manque de personnel et de temps sont souvent autant d'arguments pour justifier un moindre intérêt porté à la sécurité informatique au sein des petites structures*, prévient Guillaume Poupard, le directeur général de l'ANSSI dans le « Guide des bonnes pratiques » de l'informatique. *Ces questions sont pourtant essentielles et relèvent souvent de réflexes simples. Il ne faut pas oublier que devoir remédier à un incident dans l'urgence peut s'avérer bien plus coûteux que leur prévention.* »

Se poser les bonnes questions pour avoir les bons réflexes

« *Quand je rencontre un dirigeant, je lui demande souvent quelles sont les données critiques de l'entreprise*, observe Nathalie Malicet, expert-comptable et commissaire aux comptes auprès du cabinet Anexis à Bordeaux. *Il leur faut souvent un peu de temps pour me répondre. Or, c'est le premier réflexe à avoir : identifier ses informations sensibles pour mieux les protéger.* »

Selon la dernière étude Symantec sur les cybermenaces publiée en 2016, 77% des cyberattaques viseraient les PME. Il ne s'agit donc plus de savoir « si »… mais « quand » son entreprise peut être attaquée.

Chacun pourra déjà commencer avec des réflexes simples comme changer ses mots de passe régulièrement en pensant à mélanger majuscules, minuscules, chiffres et caractères spéciaux. Il faut non seulement télécharger ses logiciels sur des sites officiels, mais surtout les mettre à jour pour corriger certaines vulnérabilités.

Si les sites de stockage en cloud sont utiles pour sauvegarder ses données régulièrement, des supports externes, comme un disque dur externe dédié, constituent des précautions utiles. Enfin, il est impératif de savoir « chiffrer » ses documents (avec des programmes comme 7-Zip ou Peazip) pour « crypter » des données sensibles que l'on peut transporter sur un support, comme une clé USB, qui peut être perdue ou volée. Entre autres…

Avril 2019

Se faire aider par les commissaires aux comptes
Mais pour aller plus loin, les dirigeants pourront aussi, de plus en plus, compter sur les commissaires aux comptes.

« Pour certifier la qualité d'une information financière, il faut regarder les outils avec lesquels elle est construite. Or, avec l'émergence du numérique dans les systèmes d'information, le commissaire aux comptes a maintenant aussi pour mission de vérifier ce que l'entreprise fait pour sécuriser ses données »
Nathalie Malicet

Pour être plus performante, la profession peut désormais se former sur la plateforme CyberAUDIT.

« *Nous pourrons tous ainsi, avec nos clients, envisager les scénarios possibles, évaluer les conséquences financières et surtout recommander les bonnes pratiques à mettre en place…* », indique Nathalie Malicet, également vice-présidente de la Commission numérique et innovation à la Compagnie Nationale des Commissaires aux Comptes.

Publié le jeudi 11 avril 2019 à 09h03
Par Céline Chaudeau, Accroche-press' pour France Défi

Les collaborateurs du cabinet se tiennent à votre disposition pour tout renseignement complémentaire.

Votre expert-comptable : Guillaume GAHIDE 03.27.62.18.11 / ggahide@acdl.fr