ANTICIPER ET LIMITER LES RISQUES DE CYBERATTAQUES

Dans le cadre de la crise sanitaire liée au Covid-19, beaucoup d'entreprises ont déployé massivement le télétravail et modifié leurs usages numériques avec notamment **un recours accru à des outils de visioconférence, de partage via le cloud, ou encore des plateformes de chat**. De même, les connexions sur les réseaux sociaux se sont intensifiées. Cette situation hors norme à l'échelle internationale offre **de multiples occasions pour les hackers de mener des attaques contre les entreprises**, petites et grandes, en profitant de l'usage intensif de la dématérialisation des procédures.

Le contexte de Covid-19 et **la forte demande de moyens de protection** comme les masques, le gel hydroalcoolique ou les gants ont suscité d'autant plus d'opportunités d'attaques pour les hackers.

Etre **capable d'identifier et de mieux appréhender les risques** de cyberattaques peut renforcer votre capacité à **protéger l'activité** de votre entreprise, ses infrastructures, et **éviter des pertes** importantes dans cette période de crise où les équipes sont réduites, ou en télétravail.

Afin d'opérer de manière sécurisée votre reprise d'activité et installer un climat de confiance pour les tiers et fournisseurs, **nous vous invitons à mettre en œuvre les mesures de prévention présentées dans notre fiche d'informations,** tant au niveau de l'entreprise qu'au niveau des salariés.

Pour l'entreprise

› **Formation de sensibilisation des collaborateurs** : Il est important que les collaborateurs suivent une formation adéquate sur les campagnes de phishing (hameçonnage) et les procédures de sécurité. Ils doivent également connaître toutes les procédures nécessaires pour signaler un problème de sécurité si une attaque est soupçonnée ou identifiée. Soyez, dans tous les cas, facilement joignable.

› **Gestion des appareils :** Les ordinateurs portables, tablettes et mobiles des collaborateurs doivent être équipés d'une solution de gestion des appareils mobiles. La solution doit appliquer des contrôles de sécurité adéquats et créer un environnement virtuel crypté au sein de l'appareil afin de pouvoir stocker et traiter les informations de l'entreprise. L'utilisation des connexions bluetooth constitue potentiellement des brèches dans lesquelles les hackers peuvent également s'infiltrer.

› **Sécurisation des accès extérieurs** : L'utilisation d'un accès VPN (Virtual Private Network) avec une double authentification permet de sécuriser vos accès. Il existe des solutions faciles à mettre en place du côté de votre pare-feu.

› **Périmètre de protection Internet :** Les services informatiques doivent s'assurer que les pare-feux sont correctement configurés, et doivent surveiller la journalisation des pare-feux pour identifier les tentatives ou les réussites de connexion à partir d'adresses IP non autorisées ou suspectes.

› **Mise à jour du réseau, des logiciels et des applications :** Les technologies utilisées pour le travail à distance peuvent présenter des failles de sécurité et sont souvent le point d'entrée que les personnes mal intentionnées utilisent pour accéder à des informations protégées. Veillez à ce que tous les logiciels, l'antivirus et les applications soient mis à jour, et corrigez chaque faille de sécurité identifiée. Pensez également à réaliser des sauvegardes dès que possible, idéalement quotidiennement.

En prévision d'éventuelles attaques :

Il est fortement recommandé de reprendre l'ensemble des règles précitées dans le cadre plus global d'un Plan de Continuation d'Activité informatique et d'un Plan de Sécurité Informatique.

Pour le salarié

› **Liens & pièces jointes :** Cliquez seulement sur les liens et téléchargez les pièces jointes et logiciels provenant de sources sûres. Les personnes mal intentionnées tentent très souvent de masquer des liens malveillants sous des liens utiles et informatifs. Prétendant diffuser des informations relatives au Covid-19, des hackers peuvent vous entraîner sur des applications et/ou sites malveillants qui sont susceptibles d'aspirer vos données ou d'introduire des virus dans votre système : redoublez de vigilance avant de cliquer sur un lien ou d'installer une application. En cas de doute, utilisez un site de vérification d'adresse URL, comme *isitphishing.org*.

› **Informations personnelles :** Ne donnez aucune information bancaire à une source inconnue. Les institutions de confiance, comme les fournisseurs ou les vendeurs, doivent déjà disposer de cette information. N'envoyez jamais d'informations d'identification ou de mots de passe à des individus inconnus, et n'ouvrez jamais de documents présents dans des courriers non sollicités.

› **Mots de passe :** De nombreuses personnes utilisent plus ou moins toujours le même mot de passe, que ce soit au travail ou à la maison. Malheureusement, cela signifie qu'en cas de vol d'un mot de passe, il peut être réutilisé sur plusieurs sites pour débloquer des dizaines de comptes. Utilisez un logiciel de gestion des mots de passe pour générer des identifiants forts et uniques à chaque fois.

› **Visioconférence :** N'autorisez que les participants qui sont invités à participer à la visioconférence, en ajoutant leurs adresses électroniques à l'invitation, lors de la programmation de l'appel. Il est important de définir un mot de passe de réunion, généralement en option lors de la création de la réunion, que les invités devront saisir. Vous pouvez aussi placer les participants dans une « salle d'attente » virtuelle et approuver la connexion de chacun d'eux. Si des transferts de fichiers sont nécessaires, envisagez de limiter les types de fichiers qui peuvent être envoyés et ne partagez pas, dans la mesure du possible, de documents au contenu stratégique et/ou sensible.

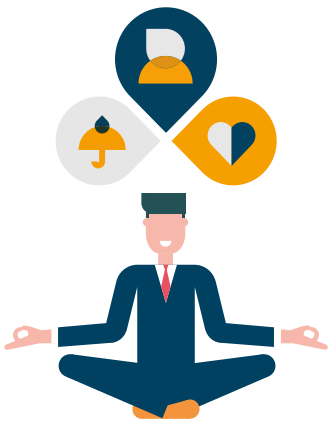
› **Réseaux :** Si vous vous connectez à votre box via le wifi, vérifiez qu'il est sécurisé par une clé secrète, et si ça n'est pas le cas, activez le chiffrement, puis déconnectez et reconnectez votre ordinateur.
Par ailleurs, en cette période de confinement, vous travaillez peut-être de chez vous avec d'autres membres de votre foyer qui sont connectés au même réseau : veillez à ce qu'ils soient équipés d'un antivirus avec une base de signature à jour, que le système d'exploitation des ordinateurs soient à jour des patchs de sécurité et que la fonctionnalité de mise à jour automatique soit activée. Lancez régulièrement des scans antivirus sur ces matériels pour vérifier qu'ils ne risquent pas d'infecter tous les matériels connectés sur votre réseau familial et votre box.

› **Vigilance :** Puisque beaucoup de monde travaille à distance, vous pourriez être victime d'une fraude à l'usurpation d'identité : ces tentatives consistent notamment à usurper l'identité d'un dirigeant, d'un client, d'un partenaire ou d'un fournisseur pour obtenir la réalisation de transactions financières. Ces usurpateurs sont très bien renseignés et préparés, ce qui rend leurs techniques très efficaces. Ces tentatives peuvent se faire aussi bien par téléphone que par email. En cas de doute, effectuez une vérification en recontactant votre interlocuteur habituel.

› **Activité suspecte *:*** Signalez tous les courriers électroniques suspicieux au service informatique de l'entreprise.

APRIL Entreprise, votre partenaire conseil

Chaque jour, votre entreprise fait face à de nouveaux défis pour se développer dans un environnement toujours plus complexe et mouvant. Il est aujourd'hui essentiel de se prémunir. C'est pour cette raison qu'APRIL Entreprise, filiale du Groupe APRIL, forte de plus de **30 ans d'expérience**, vous conseille et vous apporte son expertise afin de prévenir, piloter et gérer l'ensemble de vos dispositifs et services en protection sociale.



Notre mission : libérer votre entreprise de ses contraintes réglementaires et protéger vos collaborateurs.

Avec **une équipe d'experts techniques et juridiques** à votre écoute, nous vous accompagnons sur tous les sujets de protection sociale complémentaire ou de prévention, avec une approche personnalisée permettant une optimisation et une différenciation de votre politique des Ressources Humaines.

april | entreprise **Siège social : 90 avenue Félix Faure – CS 73344 – 69439 Lyon cedex 03 – Tél. : 04 37 46 46 46**
www.april-entreprise.fr

SAS au capital de 7 842 160 € - RCS Lyon 338 399 439 – Courtier en assurances immatriculé à l'ORIAS sous le n° 07 008 043 - www.orias.fr
N° TVA intra communautaire FR 15 338 399 439
Entreprise soumise au Contrôle de l'Autorité de Contrôle Prudentiel et de Résolution – 4 place de Budapest CS 92459 - 75436 Paris Cedex 09