Opter pour le télétravail c'est bien, protéger les données, c'est mieux !

Par Hamza Nassaf, Africa-Middle East CIO

En cette période de confinement, nombreuses sont les entreprises qui ont eu recours au télétravail pour assurer la continuité de leurs activités. Ce changement de mode de travail, jusque là inhabituel au Maroc, est non sans risque de cyberattaque ou de fuite de données.

Mazars retrace les 8 mesures incontournables à instaurer pour limiter ces risques d'atteinte à la Confidentialité, l'Intégrité et la Disponibilté des données.

1. Sécuriser le Réseau Wi-Fi

- Sécuriser votre réseau Wi-Fi domestique en renforçant son mot de passe et si possible en masquant l'affichage de son nom

- Changer le Nom et le Mot de passe par défaut de votre équipement Wi-Fi, ces valeurs peuvent être trouvées très facilement sur le site des constructeurs

- Eviter de vous connectez sur les réseaux Wi-Fi Publics. En cas de nécessité, il est fortement recommandé de ne pas autoriser que votre PC y soit visible et détectable

2. Renforcer les mots de passe

- Eviter d'utiliser le même mot de passe pour l'ensemble des comptes applicatifs (Personnels ou Professionnels)

- De nos jours, les mots de passe doivent être plus longs et plus complexes pour résister aux attaques, qui deviennent de plus en plus dangereuses. Par exemple, un mot de passe court, peut être cracké instantanément alors qu'un mot de passe long, complexe, et composé de différents caractères (chiffres, minuscules, majuscules, caractères spéciaux) peut résister de longues années avant d'être découvert par un logiciel spécialisé

Conseil > Evitez les mots de passe classiques (password, mypass, etc), les suites logiques (123456, azerty, etc) ou des mots issus des dictionnaires de toute langue confondue.

3. Vérifier la mise à jour de l'Antivirus

- S'assurer que votre antivirus est à jour et que la mise à jour est programmée avec une fréquence journalière, ceci protègera votre ordinateur même en cas d'apparition de nouveaux types de virus

4. Sécuriser les accès distants

- Pour les accès distants à vos applications ou réseaux internes, privilégier la mise en place de VPN (Virtual Private Network) entre votre ordinateur et le réseau local de votre entreprise

5. Chiffrer les documents sensibles

- Avant tout partage par e-mail ou sur un outil de partage en ligne, il est recommandé de protéger vos documents sensibles par un mot de passe

Procédure sur les outils Office > Fichier **>** Informations **>** Protéger le document **>** Chiffrer avec mot de passe

MAZARS

6. Sauvegarder les données

- Effectuer des sauvegardes régulières de vos données, en veillant à ce que l'emplacement de ces sauvegardes soit différent de celui de vos données d'origine

Astuce => Sauvegarder vos données sur un disque dur externe et placer le dans un lieu sûr, ou utiliser le stockage en Cloud si cela est autorisé, ceci vous permettra de récupérer vos données en cas de perte/vol de votre ordinateur

7. Verrouiller la session

- Il est nécessaire de verrouiller son écran à chaque fois que l'on s'absente, et ce même pour une courte durée

8. Enfin et surtout, Halte au Phishing

- Au vu des circonstances actuelles, plusieurs applications et sites web malveillants sont apparus exploitant le thème de Coronavirus afin d'infecter un nombre important de victimes. Suite à quoi, il est recommandé de :

o Se méfier des courriers électroniques demandant de saisir vos identifiants, de cliquer sur un lien ou de télécharger une pièce jointe pour accéder à des informations relatives à l'évolution ou au traitement du Coronavirus

o Se méfier des demandes inhabituelles (mot de passe, virement bancaire, document sensible), même provenant de sources connues

o Contacter l'expéditeur par téléphone, en cas de doute sur un courrier reçu de sa part

- En cas d'attaque :

o Changer immédiatement son mot de passe s'il a été introduit sur un site non fiable

o Déconnecter totalement son ordinateur du réseau s'il s'agit d'une infection virale

o Prendre contact dès que possible avec son responsable informatique pour l'informer de l'incident

Astuces > Les éléments ci-après doivent vous permettre de penser qu'il s'agit d'un potentiel e-mail de Phishing :
Objet vide / Erreurs d'orthographe ou de grammaire à répétition / Manque de personnalisation sur les formules de salutation

LE SAVIEZ-VOUS ?

- **94%** des malwares qui existent, sont véhiculés par courrier électronique*

- **3.5 Milliards de dollars**, est le montant** total des pertes relatives aux cyberattaques dans le monde en 2019

(*) Source : Le dernier rapport annuel concernant les investigations sur les fuites de données publié par VERIZON

(**) Source : Montant publié par le FBI sur son dernier « Internet Crime Report »

Pour toute demande de renseignement ou d'accompagnement, contactez nous sur l'adresse mazars@mazars.ma

MAZARS