English

CAPSULE # 1 – 16 mars 2020

Enjeux de cybersécurité

LE TÉLÉTRAVAIL EN TOUTE SÉCURITÉ DANS LE CADRE DU COVID-19

Dans le cadre des mesures à prendre face à la COVID-19, il est important de traiter des enjeux de cybersécurité relatifs au télétravail et des abus potentiels par les acteurs malveillants.

Les travailleurs à distance ont un accès privilégié aux données, aux informations et aux ressources du réseau, une augmentation des tentatives d'hameçonnage est ainsi à prévoir, en particulier celles ciblant des comptes sensibles.

En outre, il faudra porter une attention particulière à toute demande (par courriel ou par téléphone) qui enfreint la politique de l'entreprise et/ou qui incite à accéder à des informations de l'entreprise, tout particulièrement s'il y est fait mention de la COVID-19.

PRÉCAUTIONS À PRENDRE

- **Prenez vos précautions lorsque vous travaillez dans un endroit public, afin d'éviter le vol d'appareils et de données (toutes les connexions doivent être chiffrées).**

- **N'utilisez que des réseaux Wi-Fi fiables.**

- **N'utilisez que des dispositifs et des services autorisés par l'entreprise :**

    - des technologies de travail à domicile approuvées ;
    - un réseau virtuel privé (VPN) d'entreprise ;
    - aucun service tiers si vous ne pouvez accéder autrement à vos systèmes standard ;
    - des systèmes et des services approuvés pour communiquer et transférer des informations

- **Si vous avez besoin d'appareils de l'entreprise pour travailler à domicile, assurez-vous :**

    - de détenir une approbation formelle pour l'emprunt de ce matériel ;
    - que le(s) solution(s) de sécurité requise(s) est ou sont correctement installée(s) ;
    - d'utiliser un VPN et une connexion chiffrée lorsque cela est possible, afin de protéger à la fois les données de l'appareil et les systèmes de l'entreprise.
    - Les dispositifs personnels sont généralement contraires aux politiques des organisations, mais en cas d'autorisation spéciale, veillez à ce que :
    - les systèmes soient correctement mis à jour ;
    - les systèmes et les logiciels disposent d'une solution antivirus à jour ;
    - les données inutiles ne soient pas sauvegardées (ex. : documents Office) ;
    - toutes données liées à l'entreprise soient supprimées dès qu'elles ne sont plus requises.

- **Les dispositifs personnels sont généralement contraires aux politiques des organisations, mais en cas d'autorisation spéciale, veillez à ce que :**

    - les systèmes soient correctement mis à jour ;
    - les systèmes et les logiciels disposent d'une solution antivirus à jour ;
    - les données inutiles ne soient pas sauvegardées (ex. : documents Office) ;
    - toutes données liées à l'entreprise soient supprimées dès qu'elles ne sont plus requises.

- **Soyez attentif aux tentatives d'hameçonnage - traitez les courriels portant sur la COVID-19 avec la plus grande prudence :**

    - méfiez-vous des messages qui inspirent un sentiment d'urgence, en particulier ceux qui sont accompagnés de pièces jointes ou qui comportent des liens cliquables « pour plus d'information » ;
    - méfiez-vous également de l'utilisation abusive de marques légitimes, dans le but de fournir des informations relatives à la COVID-19 ;
    - soyez attentif aux communications qui prétendent provenir des Centres de contrôle et de prévention des maladies (CDC) ou de l'Organisation mondiale de la santé (OMS).

NOTE AUX SERVICES DES T.I. DES ORGANISATIONS CONCERNÉES

- **Il est fortement suggéré d'utiliser une authentification forte pour les services d'accès à distance et les services infonuagiques. Ce type d'authentification, aussi appelée « multi-factor authentification (MFA) », consiste à utiliser, en plus d'un mot de passe, un second facteur d'authentification comme par exemple un code envoyé par SMS sur le téléphone cellulaire, afin de procéder à vos différentes connexions.**

PARLEZ-NOUS

Nous sommes là pour réfléchir avec vous. Pour lancer la conversation, communiquez avec vos équipes de professionnels chez KPMG, écrivez-nous une note à continuite@kpmg.ca et/ou visitez notre Centre de ressources KPMG sur la COVID-19.

N'hésitez pas à contacter directement Francis Beaudoin, Associé et Leader National,

Services-conseils en risques technologiques, ainsi que Yassir Bellout et Guillaume Clément, Associés, Cybersécurité.

LIENS UTILES

www.quebec.ca/coronavirus
www.canada.ca/coronavirus
Centre de ressources KPMG sur la COVID-19

---

kpmg.ca/fr