PERSPECTIVES SUR LES RISQUES

MITCHELL&ABBOTT INSURANCE BROKERS

NAVACORD®

www.mitchellandabbott.com | Mars 2020

Conséquences de l'épidémie du coronavirus dans les cyber-risques

L'épidémie de COVID-19 a provoqué une perturbation importante des activités commerciales et a déclenché la plus grande mobilisation de « télétravail » des dernieres décennies. C'est une nouvelle réalité pour beaucoup qui met à l'épreuve les équipes informatiques les plans de continuité des activités les plus solides.

Pendant que tout le monde s'efforce de garantir que les principales fonctions de l'entreprise restent opérationnelles et que les employés et leurs familles demeurent en sécurité, il existe un autre groupe de personnes qui travaillent tout aussi fort pour anéantir nos efforts: *les cybercriminels*.

La pandémie de COVID-19 a fourni la confusion et la distraction parfaites pour permettre aux cybercriminels d'attaquer votre entreprise et de commettre de graves perturbations, qui pourraient vous coûter des millions.

La création d'une culture de l'information et de la cybersécurité est désormais essentielle pour protéger votre entreprise. Nous recommandons aux entreprises de prendre les précautions suivantes afin d'assurer la protection de leurs réseaux, données et finances:

1. TESTER LES CAPACITÉS DE CONNEXION ET DE POINT DE TERMINAISON

Tous les appareils personnels et professionnels doivent être configurés pour un travail à distance sécurisé. Cela inclut la mise en oeuvre d'une authentification multifactorielle (AMF). L'AMF est un processus d'authentification qui nécessite plus qu'un simple mot de passe pour protéger un compte email ou une identité numérique. Elle est utilisée pour s'assurer qu'une personne est bien celle qu'elle prétend être en exigeant un minimum de deux données uniques pour corroborer son identité. L'AMF réduit considérablement les chances de réussite d'une cyberattaque.

En raison de la distance, il est plus difficile pour le personnel informatique de surveiller et de contenir les menaces à la sécurité du réseau. Pour mieux protéger les réseaux, les entreprises peuvent mettre en oeuvre un logiciel de détection et de réponse des Endpoints (EDR) qui peut être utilisé pour mettre en quarantaine les postes de travail à distance et limiter les possibilités de navigation des acteurs malveillants dans leur réseau.

2. FORMER VOS EMPLOYÉS SUR LES RISQUES DE LA CYBER-INGÉNIERIE SOCIALE

Le plus grand risque de sécurité pour les informations au sein d'une entreprise est l'erreur humaine, et avec autant d'employés travaillant en dehors de leur environnement habituel (à la maison, hors site, en utilisant des applications de bureau à distance, loin de leurs équipes ou services habituels, etc.), ces derniers sont potentiellement distraits, ce qui profite aux cybercriminels. **La formation aux risques de la cyber-ingénierie sociale est donc essentielle.**

Assurez-vous que vos employés connaissent et soient attentifs à:

- L'Hameçonnage sous toutes ses formes:

  Ces attaques sont des tentatives d'obtention d'informations sensibles par courriel (Hameçonnage), appels vocaux (vishing) ou SMS (smishing) par un cybercriminel. Le fraudeur envoie de faux courriels ou messages qui semblent provenir de sources fiables dans le but de tromper les utilisateurs et de les amener à révéler des informations financières personnelles ou professionnelles, ou à installer des logiciels malveillants ou des macros malveillantes.

  Il convient de faire attention aux:

  - Fausses adresses de courriel
  - Pièces jointes compressées
  - Messages impersonnels
  - Fautes d'orthographe ou de grammaire
  - Tactiques d'intimidation ou de réponse rapide
  - Imitations de marques connues

- Harponnage:

  Semblable à l'hameçonnage, il s'agit d'une attaque ciblée et personnalisée contre une entreprise ou un employé spécifique - généralement dirigée contre une personne qui aurait un accès spécifique à des informations confidentielles ou à des contrôles, potentiellement au sein de la finance ou de l'informatique.

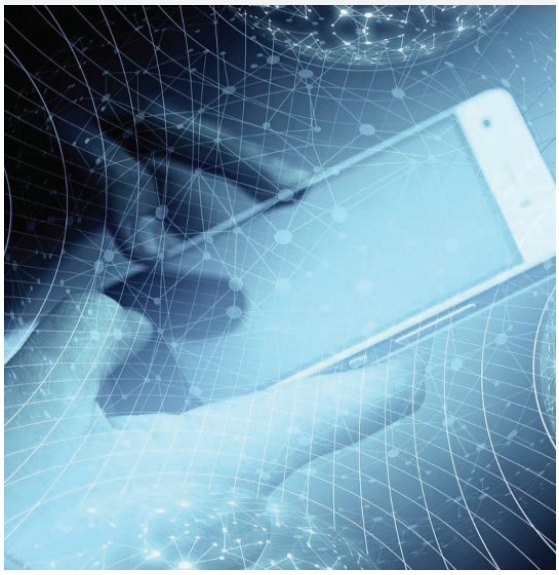
- Attaque de point d'eau:

  Cette attaque définit un cybercriminel qui étudie un groupe spécifique d'utilisateurs d'une entreprise et infecte des sites web que les membres du groupe visitent régulièrement. En infectant l'ordinateur d'un utilisateur, le cybercriminel peut ainsi accéder au réseau.

3. SE PRÉPARER AUX PERTURBATIONS

Préparez-vous au pire. La distance rend plus difficiles la surveillance et le confinement des menaces à la sécurité du réseau par le personnel informatique. Si une cyberattaque se produit dans votre entreprise, il est important de mettre en place un plan de réponse aux incidents. Si vous pensez qu'un employé a été victime d'un cyber événement ou d'un cybercriminel, informez la personne en charge de votre département informatique, le service financier et votre conseiller en assurance dès que possible.

C'est une nouvelle réalité pour beaucoup qui met à l'épreuve les équipes informatiques et de continuité des activités les plus solides



Si vous avez des questions spécifiques à votre entreprise, ou si vous souhaitez obtenir des informations complémentaires, n'hésitez pas à contacter votre conseiller Mitchell & Abbott.

LAISSEZ-NOUS VOUS AIDER À GÉRER VOS RISQUES

2000 Garth Street, Suite 202
Hamilton, ON L9B 0C1
1-800-463-5208

www.mitchellandabbott.com
www.navacord.com
info@mitchellandabbott.com

2020_03_COVID

Une touche locale. Une force nationale.[MC]