POINTS À CONTRÔLER

PANDÉMIE
PRÉVENTION DES SINISTRES CYBER – SÉCURITÉ DE L'INFORMATION

Ce document a pour objectif de fournir des préconisations en matière de prévention des sinistres cyber en période de pandémie. Pour assurer la continuité de vos activités, vous vous éloignez peut-être de vos pratiques habituelles en misant massivement sur le télétravail et en adoptant de nouvelles méthodes d'implication des collaborateurs. Parallèlement aux autres difficultés posées par une pandémie, ces déviations introduisent de nouveaux cyber-risques. Il existe toutefois des mesures de précaution et de sensibilisation éprouvées pour déjouer les tentatives de cyber-attaques contre votre entreprise.

Les cybercriminels continuent d'utiliser des techniques d'ingénierie sociale et de phishing (hameçonnage) pour accéder aux réseaux des entreprises. Le phishing reste le mode d'attaque le plus fréquent et le vecteur d'infection privilégié pour les malwares (logiciels malveillants) et les ransomwares (rançongiciels).

Ces recommandations sont destinées à vous aider à cibler vos efforts de prévention des sinistres cyber durant la pandémie, en conformité avec les procédures en place dans votre entreprise.

INGÉNIERIE SOCIALE

Les auteurs de menaces profitent des perturbations engendrées par la pandémie, notamment en termes de cybersécurité, pour lancer des attaques d'ingénierie sociale. Faites preuve de prudence si vous recevez un e-mail, un appel téléphonique ou un message instantané basé sur l'un des scénarios suivants :

- ☐ Un problème requiert une « vérification » au moyen de vos informations personnelles.
- ☐ Quelqu'un a besoin de votre aide en urgence.
- ☐ Une notification vous informe que vous avez gagné le gros lot dans le cadre d'un concours ou d'un tirage au sort.
- ☐ Un e-mail provenant a priori de votre responsable ou d'un collègue vous demande de lui envoyer des données internes sensibles.

PHISHING (HAMEÇONNAGE)

Pour tenter d'accéder aux réseaux de votre entreprise, un cybercriminel peut vous attirer sur un site Internet sérieux en apparence mais sous son contrôle, publier des offres d'emploi promettant de l'argent facile, ou encore lancer un appel aux dons au nom d'une fausse organisation affectée par la pandémie. Quelques conseils pour réduire les risques liés au phishing :

- ☐ Traitez les e-mails et pièces jointes envoyés par des expéditeurs inconnus avec autant de prudence chez vous que sur votre lieu de travail.
- ☐ Utilisez les sites Internet que vous consultez habituellement, moins susceptibles d'héberger des contenus malveillants.
- ☐ Vérifiez toujours l'expéditeur d'un e-mail.
- ☐ En cas de doute, ne prenez aucun risque. Appelez le service informatique de votre entreprise.

L'anxiété causée par cette situation sans précédent peut inciter des utilisateurs à ouvrir des e-mails de phishing relatifs à la pandémie, ce qui pourrait introduire des programmes malveillants sur le réseau de l'entreprise.

FM Global

PRÉVENTION DES SINISTRES LIÉS AUX DOMMAGES MATÉRIELS EN CAS DE PANDÉMIE : POINTS À CONTRÔLER

VISIOCONFÉRENCES

Les cybercriminels sont capables de pirater et voler en toute discrétion des informations confidentielles partagées dans le cadre de réunions en visioconférence. Les répercussions sur les activités de l'entreprise pourraient être considérables. Prenez les précautions suivantes dans la mesure du possible :

- ☐ Désactivez les paramètres par défaut qui permettent aux participants de partager leur écran sans qu'une autorisation de l'organisateur de l'événement soit nécessaire.
- ☐ Activez la protection par mot de passe pour empêcher toute personne non invitée de se connecter.
- ☐ Demandez à l'organisateur de se connecter avant le début de la réunion.
- ☐ Avant de partager votre écran, fermez les applications et documents sans lien avec la réunion afin d'éviter toute divulgation accidentelle.
- ☐ Autorisez uniquement la connexion de personnes dont l'adresse électronique est associée à un domaine de messagerie spécifique.

CORRECTIFS

Les cybercriminels tentent de tirer profit des vulnérabilités connues des systèmes d'exploitation et des applications. Dans la mesure où un nombre croissant de salariés utilisent leur ordinateur personnel pour télétravailler, il est primordial de garantir la sécurité des données auxquelles ils accèdent ou qu'ils stockent sur leur appareil. Pour sécuriser ces ordinateurs et protéger vos données :

- ☐ Installez toujours les mises à jour et correctifs de systèmes d'exploitation.
- ☐ Activez ou faites activer la mise à jour automatique si possible.
- ☐ Vérifiez que chaque utilisateur utilise la dernière version à jour des logiciels anti-virus et anti-malware et installe les correctifs.
- ☐ Harmonisez si possible les versions logicielles utilisées sur les ordinateurs personnels et professionnels.
- ☐ Sécurisez tout appareil qui pourrait interagir avec les réseaux et services de l'entreprise.

RESSOURCES UTILES

Télétravail : préparez votre entreprise et vos équipes
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail

Conseils aux utilisateurs
https://www.gouvernement.fr/risques/conseils-aux-usagers

En savoir plus sur les correctifs et les mises à jour logicielles
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour

Protégez votre ordinateur en télétravail
https://support.microsoft.com/fr-fr/help/4092059/windows-keep-your-computer-secure-at-work

AVIS DE NON-RESPONSABILITÉ RELATIF AUX LIENS EXTERNES

Bien que nous nous efforcions d'assurer l'exactitude, la validité et la pertinence de ces liens, FM Global ne saurait être tenue responsable de pages gérées par des fournisseurs externes.

Vous pouvez commander d'autres exemplaires de cette brochure ou d'autres ressources FM Global en ligne 24 h/24, 7 j/7, à l'adresse suivante : www.fmglobalcatalog.com.

W152550_20c_FRA © 2020 FM Global. (03/2020) Tous droits réservés. fmglobal.fr