Cyberrisques

Supplément Relatif au Ransomware

Directives : Pour toute question dont la réponse est « non », veuillez songer à fournir des renseignements supplémentaires à la partie des commentaires figurant à la dernière page.

1. Prenez-vous les mesures suivantes pour protéger votre réseau contre les logiciels rançonneurs :

- Installer les correctifs de sécurité au cours des 30 jours suivant leur publication? ◯ Oui ◯ Non
- Marquer les courriels externes pour signaler aux employés que le message provient de l'extérieur de l'entreprise? ◯ Oui ◯ Non
- Mettre en œuvre les protocoles d'authentification SPF, DKIM et DMARC pour protéger votre entreprise contre l'hameçonnage : ◯ Oui ◯ Non
- Utiliser des applications de filtrage du Web pour bloquer l'accès à des sites Web malveillants connus? ◯ Oui ◯ Non
- Segmenter votre réseau en fonction du niveau de classification des données stockées sur ces systèmes? ◯ Oui ◯ Non
- Utiliser des systèmes d'exploitation ou plateformes qui ne sont pas pris en charge? ◯ Oui ◯ Non
- Utiliser un outil avancé de détection et d'intervention de point terminal? ◯ Oui ◯ Non
- Utiliser un système de gestion de la sécurité de l'information faisant l'objet d'une surveillance 24 heures sur 24, 7 jours sur 7 par un centre des opérations de sécurité? ◯ Oui ◯ Non
- Disposer d'un processus pour la mise hors service des systèmes inutilisés? ◯ Oui ◯ Non
- Si Office365 est exploité, utilisez-vous l'extension Protection avancée contre les menaces d'Office 365? ◯ Oui ◯ Non
- Mettez-vous en application les bonnes pratiques PowerShell présentées dans les recommandations de Microsoft? ◯ Oui ◯ Non

Commentaires supplémentaires :

_____

_____

2. Prenez-vous les mesures suivantes pour protéger vos employés contre les logiciels rançonneurs :

- Offrir une formation périodique en matière de sensibilisation à la sécurité (au moins deux fois par année)? ◯ Oui ◯ Non
  - À quelle fréquence? _____
- Mener une campagne d'information sur l'hameçonnage (au moins une fois par trimestre)? ◯ Oui ◯ Non
  - À quelle fréquence? _____
- S'assurer que les employés observent le principe de droit d'accès minimal en tout temps et ne font pas fonction d'administrateurs locaux : ◯ Oui ◯ Non
- Exigez-vous l'authentification à facteurs multiples? ◯ Oui ◯ Non
  - l'accès à distance au réseau?
  - protéger les comptes des utilisateurs privilégiés?
  - toutes les ressources infonuagiques, y compris Office 365?
  - tous les protocoles de poste de travail à distance (Remote Desktop Protocol) et toutes les situations d'infrastructure de poste de travail virtuel (Virtual Desktop)?

Commentaires supplémentaires :

_____

_____

3. Prenez-vous les mesures suivantes pour protéger les données contre les logiciels rançonneurs :

a) Effectuer régulièrement des sauvegardes complètes et incrémentielles des données commerciales? ◯Oui ◯Non

b) Tester les sauvegardes pour s'assurer qu'il est possible de les restaurer? ◯Oui ◯Non

c) Veiller à ce que les sauvegardes soient stockées physiquement hors site? ◯Oui ◯Non

d) Veiller à ce que les sauvegardes soient stockées hors ligne pour éviter toute infection? ◯Oui ◯Non

e) Disposer d'un plan d'intervention en cas d'incident mis à l'épreuve tous les ans et permettant de contenir rapidement un incident? ◯Oui ◯Non

f) Disposer de plans officiels de reprise après catastrophe et de continuité des activités mis à l'épreuve tous les ans? ◯Oui ◯Non

4. Prenez-vous les mesures suivantes pour protéger votre entreprise contre un fournisseur victime d'un logiciel rançonneur : ◯Oui ◯Non

a) Disposer d'un programme formel de gestion des fournisseurs qui répertorie et classe les types de données et le niveau d'accès de chacun des fournisseurs : ◯Oui ◯Non

Au besoin, selon la classe du risque :

b) Exiger par contrat aux tiers qu'ils protègent ces renseignements au moyen de mesures de protection aussi robustes que les vôtres? ◯Oui ◯Non

c) Faire preuve de diligence raisonnable à l'égard de chacun de ces tiers pour vous assurer que leurs mesures de protection des données sensibles répondent à vos normes (par exemple, effectuer des vérifications de sécurité et de confidentialité ou examiner les conclusions de vérificateurs indépendants en matière de sécurité et de confidentialité)? ◯Oui ◯Non

d) Effectuer des vérifications de ces tiers au besoin pour vous assurer qu'ils continuent de répondre à vos normes de protection des renseignements sensibles? ◯Oui ◯Non

e) Les obliger par contrat à vous défendre et à vous indemniser s'ils contribuent à une atteinte à la confidentialité ou à la vie privée? ◯Oui ◯Non

f) Les obliger à disposer de liquidités suffisantes ou à souscrire une assurance de responsabilité professionnelle d'un montant suffisant pour couvrir leur responsabilité découlant d'une atteinte à la vie privée ou à la confidentialité? ◯Oui ◯Non

Commentaires supplémentaires :

_____

_____

Veuillez décrire les mécanismes supplémentaires, la formation ou les autres mesures que votre entreprise met de l'avant pour reconnaître et atténuer les attaques par logiciel rançonneur.

Signature : _____

Nom en caractères d'imprimerie : _____

Titre : _____

Compagnie : _____

Date (mm/dd/yyyy) :_____

Pour de plus amples renseignements, veuillez communiquer avec votre souscripteur CNA local ou consulter notre site Web à l'adresse cnacanada.ca.