Conseils en cyber-résilience

La récente épidémie mondiale de rançongiciels WannaCry et NotPetya (ou « Nyetya » pour certains) a mis en évidence à la fois la menace croissante des défaillances en matière de cybersécurité et l'importance des systèmes TI pour toutes les facettes de l'entreprise. L'objectif de ce document est de rappeler et renforcer les pratiques qui créent la cyber-résilience. Ce document n'est pas un examen approfondi des virus mentionnés ci-dessus ; ces informations sont facilement accessibles par d'autres sources.

QUE PEUT FAIRE VOTRE ENTREPRISE ?

- Inventorier tous les systèmes dans votre environnement, en accordant une attention particulière à l'identification des systèmes en fin de vie. Migrer vers des versions et supports plus récents dès que possible, s'assurer que le risque est compris et que des contrôles compensatoires supplémentaires ont été engagés jusqu'à ce que la migration puisse avoir lieu. Ne pas s'appuyer sur les produits les plus anciens et obsolètes pour les applications les plus importantes et l'accès aux données.
- Faire de l'application des correctifs systèmes de manière régulière et en temps opportun une priorité. La grande majorité des programmes malveillants (malware) exploitent les vulnérabilités connues des systèmes d'exploitation ou des applications pour lesquelles des correctifs sont disponibles. Ne pas effectuer les mises à jour signifie que ces systèmes restent vulnérables.
- Analyser de façon externe l'environnement, en accordant une attention particulière aux services et aux ports ouverts. Les attaquants font la même chose, à la recherche de ports ouverts à l'internet. Avoir des ports ouverts à l'internet inutilement est une mauvaise pratique de sécurité et ce processus peut identifier des services en cours d'exécution ne servant pas une activité précise (une surface d'attaque inutile).
- Former les employés sur la manière d'identifier les courriels d'hameçonnage. De nombreuses attaques de rançongiciel se propagent par des courriels d'hameçonnage, dont beaucoup sont conçus pour leurrer les victimes et les inciter à cliquer sur un lien ou à ouvrir un dossier. Une formation des employés à la vigilance est conseillée pour éviter d'accueillir d'autres cyber-attaques.
- Suivre le principe de la séparation des privilèges : ne pas donner aux comptes d'employés ou services des droits dont ils n'ont pas besoin. En particulier, limiter les « privilèges d'administrateur local » aux seuls employés qui en ont vraiment besoin.
- Pratiquer une bonne hygiène de mot de passe. Ne pas utiliser le même mot de passe pour plusieurs comptes d'administration ou service et s'assurer que les mots de passe sont assez longs et complexes.
- Mettre à jour les antivirus sur les serveurs et les postes et les configurer pour qu'ils effectuent automatiquement des analyses régulières. Cela protège l'infrastructure si la signature de l'attaque est connue.
- Segmenter correctement le réseau. Identifier les données et les actifs les plus importants et les séparer par segmentation du réseau et contrôle d'accès strict. Chaque barrière de sécurité entre les segments représente un obstacle pour les attaquants et une possibilité pour les entreprises d'atténuer une attaque.
- S'assurer que les fichiers et systèmes importants disposent de sauvegardes à jour. Ceci fournit la meilleure protection contre la perte de données due à un rançongiciel. Les sauvegardes doivent être protégées et testées pour la capacité de restauration.
- Disposer d'un plan et processus d'intervention d'urgence en cas d'incident à jour et testé. La gravité de nombreux incidents augmente inutilement en raison de l'absence de réponse rapide et appropriée.

QUE PEUT FAIRE AIG POUR LES ENTREPRISES ?

Les assurés d'AIG devraient profiter des services clés gratuits offerts (si ce n'est pas déjà le cas), à savoir :

- Blocage d'IP inscrites sur la liste noire
- Formation en ligne de sensibilisation des employés à la sécurité
- Analyse de la vulnérabilité de l'infrastructure

Nous proposons également des services supplémentaires sur honoraires qui prennent directement en charge l'évaluation de la vulnérabilité de l'entreprise à ce type d'attaque, dont une évaluation des systèmes face à Internet, un examen de la cyberdéfense et des services d'évaluation optimisés par BitSight et Security Scorecard.

Ces services ont été spécialement sélectionnés sur la base de nos près de 20 ans d'expérience et la manière dont ils peuvent contribuer à renforcer la maturité de la cybersécurité d'une entreprise.

Commencez dès aujourd'hui. Visitez www.aig.ca/cyberedge.

12/17 6071T