SOMMET SUR LA GOUVERNANCE - ACATC 2021

Gouvernance du risque de cybersécurité

Presented By

Dan Michaluk

Le 10 juin 2021

BLG
Borden Ladner Gervais

Le degré et la nature du risque pour les conseils

Le degré et la nature du risque pour les conseils

BLG

Catalogue des problèmes de sécurité des données

- Cyber (extérieur > intérieur)
  - Rançongiciels / logiciels malveillants
  - Compromission et fraude du courrier électronique d'entreprise
  - Expositions dues à une mauvaise configuration
  - Déni de service distribué
- Autre (intérieur > extérieur)
  - Vol commis par des initiés
  - Fouinage
  - Courriels errants
  - Perte d'appareils, de papiers...

Le degré et la nature du risque pour les conseils

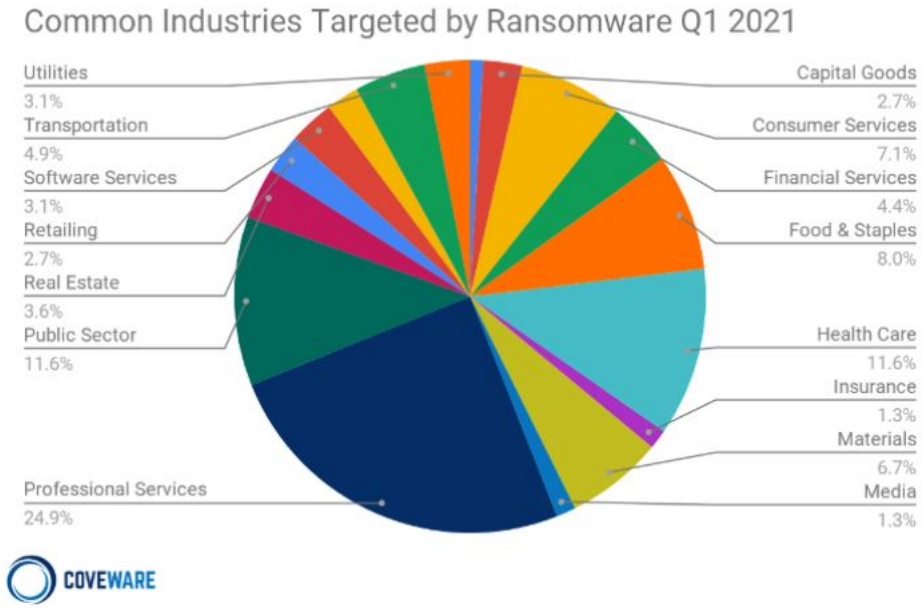
La menace de rançongiciels est très élevée

- Les attaques ont augmenté de 150 % en 2020
- Augmentation de plus de 300 % des paiements de rançons en 2020
- Double et triple menace d'extorsion
  - Verrouillage des données
  - Vol de données et demande de rançon
  - DDoS ou menace de divulgation de données personnelles
- Le marché de l'assurance devient plus rigide.
  - Augmentation des primes de 20 à 50 %.
  - Augmentation des franchises, des limites et de la coassurance
  - Nouvelles conditions de couverture et contrôles plus stricts

Le degré et la nature du risque pour les conseils

Le secteur public est une cible principale.

- Les pressions budgétaires ont tendance à affaiblir les défenses des entités du secteur public
- Les attaques contre le gouvernement et le secteur MUSH sont très courantes



Common Industries Targeted by Ransomware in Q1 2021

Le degré et la nature du risque pour les conseils

BLG

Manifestations du risque

- Défauts de conformité aux règles de confidentialité
- Problèmes de réputation
  - Quelles sont les conséquences sur le fonctionnement d'une rupture de confiance?
  - La législation sur l'accès à l'information invite à une transparence totale et sans faille
- Coûts de réponse
  - Drainage opérationnel
  - Coûts réels
- Responsabilité civile et responsabilité envers les employés

Cybersécurité 101 pour les administrateurs

Signification de la sécurité de l’information

- La pratique de la protection de l'information en atténuant les risques liés à l'information
- La valeur de l’information pour les organisations est dérivée de
  - Sa confidentialité
  - Son intégrité
  - Sa disponibilité

Gestion de l’actif

- Le processus de gestion du déploiement, de l’entretien, de la mise à niveau et de l’élimination des biens informatiques
- Un bien informatique est un matériel, un logiciel ou un dépôt de données dans l’environnement technologique.
- Problèmes courants
  - Actifs qui ont été adoptés mais qui ne sont pas gérés
  - Les anciennes technologies peuvent être vulnérables et ne pas s’intégrer aux technologies de sécurité actuelles

BLG

Défense en profondeur

- L'utilisation de mesures superposées et redondantes pour protéger l'information et les systèmes en prévoyant que certaines mesures échoueront
- Obtenue par la mise en œuvre d'un ensemble de contrôles - physiques, administratifs et techniques
- Et obtenue par la superposition de couches - sécurité du périmètre >> sécurité au niveau du système
- Le travail dans le Nuage et à distance ont entraîné la mise en place de contrôles plus détaillés que le périmètre - la surveillance interne est désormais très importante
- La capacité à réagir aux événements et aux incidents est un autre aspect de la superposition.

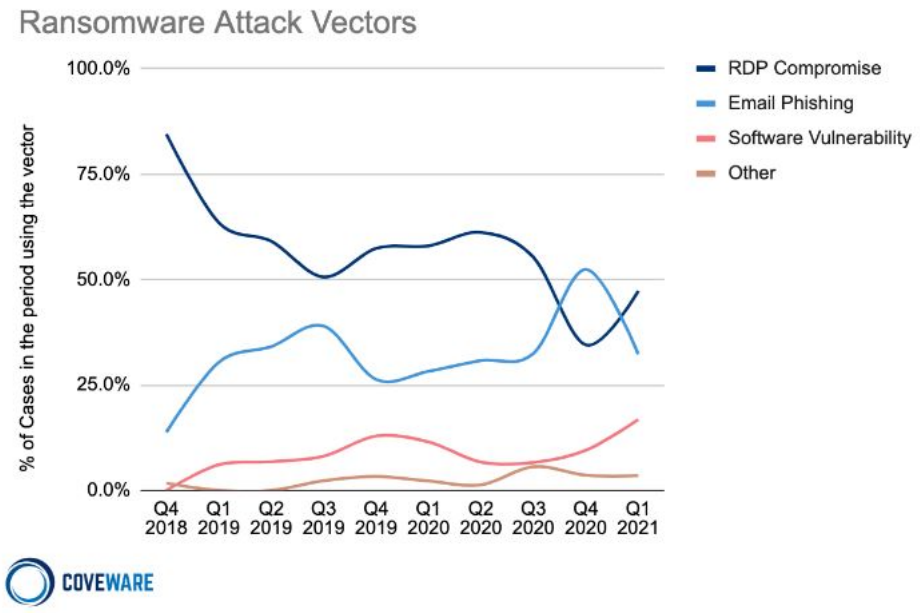
Événements, incidents et « effractions »

- Un événement de sécurité est un problème possible qui doit être évalué.
- Un incident de sécurité est un problème confirmé qui doit être géré par le processus de réponse aux incidents.
  - Cyber-attaque
  - Une mauvaise configuration
  - Une communication errante
- Une « effraction » est un concept juridique qui concerne l'accès non autorisé à des informations ou la perte, le vol...

Cybersécurité 101 pour les administrateurs

Problèmes courants

- Accès à distance non sécurisé
  - Protocole exposé du bureau à distance
  - Pas d’authentification multifactorielle
- Gestion des vulnérabilités et des correctifs
- Mauvaise mise en œuvre du principe de droits d'accès minimal
- Visibilité médiocre du réseau
- Procédures de sauvegarde insuffisamment mises en œuvre et non testées



Rapport Coveware du 1er trimestre de 2021 sur les rançongiciels

Surveillance de la cybersécurité

Surveillance de la cybersécurité

Vue d’ensemble

- Donner le ton au niveau supérieur
- Développer les cybercompétences du conseil d'administration
  - Comment informer les membres du conseil d'administration?
  - Qui doit être recruté?
- Discutez entre vous et référencez vos pratiques de surveillance
- Si le service informatique ou la sécurité informatique présente le rapport, n'excluez pas les autres cadres
- Envisagez d'utiliser le cadre de cybersécurité du NIST pour structurer le dialogue avec la direction.

Activité	Catégorie
Identifier (ID)	Gestion des actifs
	Environnement métier
	Gouvernance
	Évaluation des risques
	Stratégie de gestion des risques
Protéger (PR)	Contrôle d'accès
	Sensibilisation et formation
	Sécurité des données
	Processus et procédures de protection d’information
	Maintenance
	Technologie de protection
Détecter (DE)	Évènements et anomalies
	Surveillance continue de la sécurité
	Processus de détection
Réagir (RS)	Planning de réaction
	Communications
	Analyses
	Atténuation
	Améliorations
Récupérer (RC)	Planning de récupération
	Améliorations
	Communications

Surveillance de la cybersécurité

Identifier

- Développer une compréhension organisationnelle pour gérer le risque de cybersécurité pour les systèmes, les personnes, les actifs, les données et les capacités.
  - Avons-nous des inventaires des biens? Avec un système de classification? Quand ont-ils été mis à jour pour la dernière fois?
  - Nos rôles et responsabilités sont-ils clairement et correctement attribués? Par quelles politiques? Quand ont-ils été mis à jour pour la dernière fois?
  - Avons-nous des processus d'évaluation continue des risques? Quels sont-ils? Avons-nous recours à des tiers, et comment?
    - *Globalement*
    - *Chaîne d'approvisionnement*

Surveillance de la cybersécurité

Protéger

- Élaborer et mettre en œuvre des mesures de protection appropriées pour garantir la prestation des services essentiels.
  - Quelles sont nos données les plus critiques?
  - Où sont-elles sauvegardées?
  - Avons-nous testé notre procédure de sauvegarde?
  - Qui y a accès?
  - Comment nous assurer qu'ils sont bien qui ils sont?
  - Comment savons-nous que nous pouvons leur faire confiance?
  - Que faisons-nous pour les former?

Surveillance de la cybersécurité

Détecter

- Élaborer et mettre en œuvre des activités appropriées pour identifier la présence d'un événement de cybersécurité.
  - Comment obtenir une visibilité dans notre activité de réseau?
  - Quelles données collectons-nous?
    - *Internes*
    - *Externes (renseignements sur les menaces)*
  - Qui les analyse?
  - Qui décide si nous avons un incident? Quelle est la limite? Que se passe-t-il ensuite?

Surveillance de la cybersécurité

Réagir

- Élaborer et mettre en œuvre des activités appropriées pour prendre des mesures concernant un incident de cybersécurité détecté.
  - Avons-nous un plan d’intervention en cas d’incident?
  - Quand a-t-il été mis à jour pour la dernière fois?
  - L’avons-nous mis à l’épreuve par des scénarios?
  - Qui fait partie de l’équipe d’intervention en cas d’incident?
  - Ont-ils été formés?
  - Avons-nous fait appel à des fournisseurs externes?
  - À quand remonte notre dernier incident? Qu’avons-nous appris sur notre capacité d’intervention?
  - Notre plan en tient-il compte?

Surveillance de la cybersécurité

Récupérer

- Élaborer et mettre en œuvre des activités appropriées pour maintenir les plans de résilience et rétablir les capacités ou les services qui ont été détériorés en raison d'un incident de cybersécurité.
  - À quand remonte notre dernier incident?
  - Avons-nous fait un compte rendu? Comment?
  - Qu’avons-nous appris sur notre capacité d’intervention?
  - Notre plan en tient-il compte?
  - Avons-nous communiqué à nos intervenants ce que nous avons appris?

Questions?

Thank You

For more information, contact:

Dan Michaluk
Associé
416.367.6097
dmichaluk@blg.com

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this presentation. No part of this presentation may be reproduced without prior written permission of Borden Ladner Gervais LLP.

© 2021 Borden Ladner Gervais LLP. Borden Ladner Gervais is an Ontario Limited Liability Partnership.

BLG
Borden Ladner Gervais