CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

À surveiller

Bulletin sur la cybersécurité à l'intention des administrateurs

Ce bulletin aborde cinq thèmes relatifs à la sécurité et à la confidentialité des données que tout administrateur doit connaître en 2019.

Thème 1 : Cybermenaces touchant les technologies opérationnelles et l'Internet des objets

On connaît bien les menaces relatives aux technologies de l'information (TI), comme le vol des données clients. Cependant, les administrateurs doivent savoir que les opérations des organisations sont, elles aussi, sujettes aux cybermenaces.

Chaînes de fabrication, génératrices, systèmes de climatisation d'entrepôts, systèmes de contrôle et d'acquisition de données (SCADA) et actifs de transport représentent divers exemples d'actifs, de systèmes et de réseaux de technologie opérationnelle (TO). Il y a quelques années, bon nombre de réseaux de TO étaient isolés des réseaux informatiques de l'organisation et, ainsi, inaccessibles aux pirates. Or, pour accroître l'efficacité et l'efficience des organisations, ces systèmes de TO sont de plus en plus numérisés et connectés, ce qui les rend vulnérables aux cyberattaques. En effet, la convergence des systèmes et des réseaux de TI et de TO facilite la vie des pirates informatiques, qui peuvent naviguer plus aisément dans les systèmes numériques des organisations.

Comme beaucoup d'organisations dépendent des TO d'une manière inattendue, les administrateurs peuvent être pris au dépourvu par les menaces. Par exemple, dans le secteur bancaire, les systèmes fondés sur des algorithmes, comme les plateformes de négociation et les programmes de conformité, pourraient être la cible d'attaques informatiques.

Voici quelques données intéressantes tirées du sondage Global State of Information Security® de 2018 de PwC.

- Peu d'organisations prévoient évaluer les risques liés à l'Internet des objets industriels dans leur écosystème d'affaires.
- La responsabilité des technologies émergentes, comme l'Internet des objets, l'Internet des objets industriels et la sécurité des TO, incombe à différents acteurs dans les organisations. Par exemple, dans les organisations interrogées, la sécurité des TO peut relever :
  - du responsable de la sécurité de l'information (29 %);
  - ou des ingénieurs (20 %);
  - ou du responsable de la gestion des risques (17 %).
- Afin de soutenir les activités internes :
  - 52 % des organisations embauchent un responsable de la sécurité de l'information;
  - 47 % embauchent des employés responsables de la sécurité;
  - 45 % embauchent un responsable de la sécurité.
- Peu d'organisations comptent des dirigeants en cybersécurité.

Ces données montrent que de nombreuses organisations n'ont pas bien cerné les systèmes les plus susceptibles d'être compromis, les conséquences probables d'une telle atteinte sur leurs activités ou encore les éventuels responsables de celle-ci.

Cybermenaces : conseils aux administrateurs

Les attaques de systèmes des TO peuvent paralyser les fonctions clés d'une organisation. Provoquer une panne d'un réseau électrique, bloquer le traitement des achats de consommateurs de partout dans le monde, fermer une usine ou compromettre des activités minières sont des exemples réels de piratage des TO qui se sont produits au cours des dernières années.

Beaucoup d'environnements de TO n'ont pas encore de contrôles de cybersécurité adéquats. Aussi les pirates informatiques visent-ils de plus en plus ces infrastructures. Voici quelques conseils pour aider les administrateurs à assurer une gouvernance efficace des TO :

- Demander à l'équipe de direction de quelle manière elle identifie et atténue les risques associés aux TO.
- Chercher des éléments probants attestant que l'équipe de cybersécurité comprend ou cherche à recruter des spécialistes en sécurité des TO capables d'élaborer des programmes efficaces pour assurer la sécurité des activités.
- Vérifier que la direction a instauré des règles de reddition de comptes en ce qui concerne la cybersécurité des TO, de l'Internet des objets industriels et des technologies émergentes.
- S'assurer que l'équipe de direction a dressé l'inventaire de ses actifs de TO essentiels et représenté, dans un diagramme, ses réseaux de TO, et s'assurer aussi qu'elle tient ces outils à jour.

Thème 2 : Obligation de communiquer toute atteinte à la cybersécurité

Selon le Commissariat à la protection de la vie privée du Canada, depuis le 1er novembre 2018, les organisations assujetties à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) doivent :

- déclarer au commissaire à la protection de la vie privée du Canada les atteintes aux mesures de sécurité concernant des renseignements personnels présentant un risque réel de préjudice grave à des individus;
- aviser les intéressés au sujet de ces atteintes;
- conserver un registre de toutes les atteintes.

Ces obligations nécessiteront l'apport de changements aux pratiques habituelles de gestion des atteintes à la vie privée et de protection des renseignements personnels chez les organisations touchées. Ne pas les respecter pourrait entraîner des conséquences négatives sur le plan de la réglementation, une couverture médiatique indésirable, une enquête ou un examen préventifs par l'autorité de réglementation du registre des atteintes, ainsi que des amendes pouvant aller jusqu'à 100 000 $. Ces coûts s'ajoutent aux mesures correctives mises en place après l'atteinte. (Selon le troisième rapport annuel du Ponemon Institute, le coût moyen d'une atteinte à la sécurité des données pour une entreprise canadienne s'élevait, en 2017, à 5,78 millions de dollars.) Avoir un plan d'intervention fonctionnel peut réduire les coûts et atténuer le risque d'atteinte à la réputation de l'organisation.

Devant l'augmentation des cyberattaques et de leur complexité, les organisations mettent sur pied des équipes d'intervention prêtes à agir, lesquelles sont composées de tiers experts en cybersécurité et de parties prenantes de divers secteurs, dont les suivants :

- gestion de la continuité de l'exploitation
- sécurité (TI et TO)
- conseil juridique et conformité à la réglementation
- relations avec la clientèle et relations publiques
- exploitation
- ressources humaines
- relations avec les gouvernements (dans le cas d'attaques provenant d'États étrangers)

Mesures en amont que peuvent prendre les administrateurs

- Connaître les responsabilités de l'organisation en matière de communication de l'information.
- Vérifier que la direction a un plan d'intervention complet ainsi qu'un guide comprenant la marche à suivre pour divers scénarios – par exemple, attaque par rançongiciel, interruption des activités ou perte de données.

- Demander si l'organisation dispose d'une équipe interne responsable des atteintes à la vie privée et a conclu une entente avec de tierces organisations pour obtenir du soutien au besoin.
- Vérifier que le service des relations publiques et des relations avec les investisseurs a un communiqué prêt pour publication rapide, afin d'atténuer le risque d'atteinte à la réputation de l'organisation.
- Confirmer auprès de la direction que des simulations sont réalisées au moins chaque année afin de vérifier que toutes les parties prenantes connaissent bien leur rôle.
- Savoir que la direction peut recouvrer les données perdues ou restaurer les systèmes corrompus dans les délais souhaités à partir d'une sauvegarde.
- Pour en savoir plus, consulter le site du Commissariat à la protection de la vie privée du Canada à https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee

Thème 3 : Risque d'atteinte à la cybersécurité commise par un tiers

Pensez aux nombreux prestataires de services externes auxquels se fie l'organisation pour mener ses activités de manière efficace et concurrentielle. Combien d'entre eux, par leur accès aux données, aux réseaux, aux applications ou aux activités de l'organisation, pourraient constituer une menace à la sécurité? La réponse pourrait vous étonner : entrepreneurs, entreprises de logistique, gestionnaires d'immeubles, fournisseurs de services de télécommunication et centres de stockage des données ne sont que quelques-uns de ces tiers.

Un bon nombre d'attaques visent d'abord des fournisseurs ou des entrepreneurs afin d'atteindre leurs clients importants. Les pirates savent que les petites sociétés de services, qui ont souvent accès aux réseaux de leurs clients, n'ont pas toujours mis en place des contrôles de sécurité rigoureux. En s'attaquant à ces cibles faciles, ils accèdent ensuite aux données de grandes entreprises. En 2014, Target, détaillant à grande surface aux États-Unis, a été victime de ce stratagème. Les malfaiteurs se sont d'abord attaqués à un petit entrepreneur de systèmes informatiques pour la climatisation, dans le but d'atteindre les données de Target. Résultat : des dommages estimés à 162 millions de dollars pour le détaillant.

Au cours de la dernière année, on a souvent entendu parler des risques d'atteinte à la sécurité liés aux tiers.

Questions clés dont les directeurs devraient discuter avec la direction

- Comment les équipes de direction peuvent-elles évaluer et atténuer les cyberrisques liés à des tiers?
- Comment l'organisation peut-elle s'assurer que les parties externes respectent leurs obligations contractuelles en matière de sécurité?
- Si la sécurité de l'organisation est compromise en raison d'un tiers, à qui incombe la responsabilité légale?

On recommande aux administrateurs de vérifier que l'équipe de direction a mis en place les contrôles suivants pour atténuer les risques de cybersécurité liés à des tiers :

- Ententes avec les tiers décrivant, d'une part, les obligations de chacun pour se protéger contre les atteintes à la sécurité et, d'autre part, la responsabilité en cas de non-conformité. (N'oublions pas que, malgré tous les efforts raisonnables déployés, la cybersécurité peut toujours être compromise; dans certains cas, il n'y a aucun responsable.)
- Processus de validation afin de s'assurer que les ententes contractuelles relatives à la sécurité sont respectées. (La capacité d'obtenir le niveau d'assurance recherché peut varier d'un tiers à l'autre.)
- Niveau d'accès minimal à accorder aux tiers (c'est-à-dire, donner l'accès au besoin seulement).

Thème 4 : Discuter des risques de cybersécurité avec les administrateurs

Comment les responsables de la cybersécurité peuvent-ils présenter les stratégies et les décisions relatives à la sécurité à leur conseil d'administration? À l'inverse, comment le conseil peut-il acquérir une meilleure compréhension de la stratégie de l'organisation en ce qui concerne les technologies et la cybersécurité?

La présentation d'un plan de cybersécurité technique et complexe au conseil d'administration peut s'avérer un exercice difficile. En fait, il n'est ni nécessaire ni souhaitable d'informer les membres du conseil des subtilités des modèles de segmentation réseau. Compte tenu du rôle de gouvernance des administrateurs, il serait préférable d'aborder la cybersécurité d'un autre point de vue.

La solution : traiter de la diminution des cyberrisques plutôt que des approches et des solutions techniques. Ainsi, l'analyse des risques actuels de l'organisation et l'établissement de cibles maximales de cyberrisques entraîneront des discussions très utiles.

EXEMPLE

Les administrateurs veulent connaître le niveau actuel de risque de pertes de données. La direction fournit alors un rapport d'évaluation des risques décrivant la probabilité et les conséquences d'une atteinte à la cybersécurité entraînant une perte de données importante. Elle présente aussi un niveau de risque souhaité (p. ex., faire passer le niveau de risque d'élevé à moyen ou faible sur une échelle d'évaluation). Il incombe ensuite au responsable de la sécurité de l'information d'assurer au conseil que des contrôles appropriés peuvent être mis en œuvre pour atteindre le niveau de risque souhaité. Si le conseil souhaite obtenir une autre validation, la direction peut mandater un tiers d'analyser le plan du responsable de la sécurité de l'information pour vérifier le bien-fondé des décisions techniques qui sont prises. Ainsi, la discussion porte sur les risques en tant que tels, et non sur les aspects techniques et complexes.

Le scénario ci-dessus ne dispense toutefois pas les administrateurs de veiller à acquérir de bonnes connaissances informatiques, notamment sur les questions de cybersécurité (et de protection de la vie privée). Les conseils devraient également compter au moins un membre connaissant très bien le sujet, afin de faciliter les discussions sur les risques et la surveillance de ceux-ci. Le comité d'audit est l'un des comités du conseil qui doit être au courant de l'analyse des risques de cybersécurité. En raison de leurs responsabilités de surveillance des documents déposés auprès des autorités en valeurs mobilières et des obligations d'information, les membres du comité d'audit doivent bien comprendre les cyberrisques et les obligations réglementaires en la matière.

Le conseil devrait adopter un cadre de gouvernance de la cybersécurité afin de fournir une taxonomie et un processus d'évaluation des cyberrisques au sein de son organisation. Ce type de cadre soulève des questions et des sujets pertinents reliés aux domaines importants visés par les risques de cybersécurité. (Voir, par exemple, le cadre de PwC, en anglais[1].)

EXEMPLE

L'une des techniques de transfert des risques de cybersécurité est de souscrire une assurance cybersécurité. Au cours des dernières années, les assureurs de cyberrisques pour les entreprises ont resserré leurs exigences. Les administrateurs devraient demander des conseils indépendants sur la structure et l'étendue de la couverture de cyberassurance de l'organisation. Vous trouverez plus d'information à ce sujet dans le guide *20 Questions que les administrateurs devraient poser sur la cybersécurité*, que publiera bientôt CPA Canada.

Thème 5 : Convergence de la cybersécurité et de la protection de la vie privée

Les organisations gèrent habituellement les processus de cybersécurité et de protection de la vie privée séparément : la cybersécurité relève d'équipes techniques alors que la protection de la vie privée est du ressort des services juridiques, de la conformité et des ressources humaines. La collaboration entre ces équipes varie surtout en fonction des besoins.

Toutefois, en raison des récentes menaces et atteintes à la cybersécurité, ces équipes ont dû collaborer plus activement. Or, le libellé des lois et des politiques de protection des renseignements personnels est bien différent du langage utilisé dans les services de TI. Ainsi, seule une poignée d'organisations ont créé une équipe intégrée responsable de la gestion de la sécurité et de la protection de la vie privée. Pourtant, plus les exigences d'observation sont nombreuses, plus s'accroît le besoin d'avoir des politiques, des processus et des ressources intégrés.

L'Accord Canada–États-Unis–Mexique (ACEUM), conclu à la fin de septembre 2018, pourrait avoir une incidence majeure sur les programmes de cybersécurité et de protection de la vie privée. Le chapitre 19 prévoit l'établissement d'une zone de libre-échange continentale pour

1 *PwC's Board Cybersecurity Governance Framework* : www.pwc.com/ca/en/consulting/publications/20160310-pwc-reinforcing-your-organizations-cybersecurity-governance.pdf

les biens et services numériques. Cet objectif renforce l'importance des règles de protection des renseignements personnels et encourage la collaboration des trois pays sur les questions de cybersécurité et de protection des renseignements personnels. Surtout que l'ACEUM limite l'imposition d'exigences relatives à la localisation des données, favorisant la libre circulation des données entre les frontières.

Cet accord entraîne des défis et des possibilités pour les organisations exerçant leurs activités en Amérique du Nord (et sur la scène internationale), dont les suivants :

- Renforcer les capacités en matière de cybersécurité aux fins de la protection des données personnelles.
- Favoriser des règles de protection des renseignements personnels adaptées à la circulation des données, ce qui nécessite le respect des règles du pays d'origine pour l'utilisation et la protection des données reçues de l'étranger par une organisation; cette mesure encouragera les trois pays à harmoniser leurs lois sur la protection des renseignements personnels, dans la mesure du possible.
- Tirer parti des cadres de gestion de données existants afin de susciter la confiance des clients et des autorités de réglementation, ainsi que de profiter au maximum du libre marché des biens et des services numériques.

À la lumière de ces éléments, les organisations devraient considérer comme une pratique exemplaire la mise sur pied d'un comité directeur de protection des renseignements personnels et de sécurité qui aurait pour mandat de créer des politiques et des processus tenant compte des exigences législatives et techniques afin de stocker, de transmettre et de disposer des données efficacement.

Pour en savoir plus sur le sujet, ne manquez pas le nouveau guide de CPA Canada, *20 Questions que les administrateurs devraient poser sur la cybersécurité*, qui sera publié à l'automne 2019.

À propos de l'auteur : Richard Wilson, associé, Cybersécurité et protection des renseignements personnels, chez PricewaterhouseCoopers au Canada, se spécialise dans la gouvernance, pour les conseils d'administration, de la cybersécurité et de la protection des renseignements personnels. Pour le joindre, écrivez à **richard.m.wilson@pwc.com**.