

Les cyberrisques au premier rang des préoccupations des comités d'audit

L'automatisation et l'intelligence artificielle peuvent aider à s'attaquer aux cybermenaces et à la pénurie de main-d'œuvre

Par Hartaj Nijjar

La cybersécurité est l'un des enjeux en constante évolution les plus complexes auxquels sont confrontées les organisations. Selon une nouvelle [recherche menée par KPMG](#), seulement 38 pour cent des sociétés canadiennes croient que la cybersécurité est « profondément ancrée » dans tous les aspects de leurs processus de gouvernance et de gestion. Plus les cybermenaces deviennent élaborées, plus la responsabilité des comités d'audit à l'égard de la surveillance des risques liés à la cybersécurité s'accroît. Il est crucial que les comités d'audit aient une compréhension approfondie des vulnérabilités et des risques organisationnels associés au télétravail, à l'adoption des services infonuagiques et à la transformation numérique accélérée.

Menaces internes à la hausse

L'hameçonnage continue d'évoluer et de créer de nouveaux risques pour les organisations. Les cybercriminels déploient de nouvelles stratégies, comme la corruption d'employés, afin d'accéder à un réseau d'entreprise. Bien que la menace d'attaques internes n'ait rien de nouveau, il y a une hausse des inquiétudes concernant les employés mécontents qui refusent de se conformer aux politiques en matière de vaccination obligatoire du bureau et qui sont susceptibles d'accepter des pots-de-vin de la part de cybercriminels.

Nous avons constaté une hausse notable des attaques par hameçonnage et par rançongiciel depuis le début de la pandémie, lorsque les employés ont massivement

adopté le télétravail. Cependant, les cybercriminels ne ciblent pas uniquement les institutions financières et les multinationales; ils visent également les hôpitaux, les universités, les organismes gouvernementaux et les infrastructures essentielles. La récente attaque de Colonial Pipeline par un rançongiciel, qui a entraîné la fermeture du plus grand pipeline des États-Unis, était due à un seul mot de passe compromis¹.

Les comités d'audit doivent s'assurer que des contrôles sont en place pour identifier les menaces internes potentielles, détecter les activités malveillantes, y compris les cas



Le comité d'audit joue un rôle stratégique en matière de surveillance des activités de gestion des risques et des procédures de suivi liées à la cybersécurité. Ce rôle est d'autant plus essentiel en raison de la pratique accrue du télétravail, de l'adoption des services infonuagiques et de la transformation numérique accélérée.

Hartaj Nijjar

Associé, Cybersécurité
KPMG au Canada



¹ TURTON, William, MEHOROTRA, Kartikay. « Hackers Breached Colonial Pipeline Using Compromised Password », *Bloomberg*, 4 juin 2021.

où un employé fournit à un tiers externe non autorisé un accès au réseau, et répondre à une attaque. C'est pourquoi la gestion de l'identité constitue de plus en plus une composante cruciale de toute stratégie en matière de cybersécurité. Un cadre de « confiance zéro », par exemple, consiste à éliminer le facteur confiance et exige l'authentification, l'autorisation et la validation de tous les utilisateurs avant qu'ils obtiennent (et conservent) l'accès aux données et aux applications.

Gestion des risques liés à l'infonuagique

Parallèlement à cela, de nombreuses organisations ont accéléré leur passage au numérique au cours de la pandémie, notamment en déplaçant des services clés vers le nuage. Toutefois, dans bien des cas, ces organisations tentent de migrer vers l'infonuagique le plus rapidement possible ou de centraliser leurs services infonuagiques sans suffisamment tenir compte de la sécurité du nuage. Bien que les fournisseurs de services infonuagiques offrent un niveau de sécurité de base, c'est aux locataires qu'il revient de garantir la sécurité de leurs données, de leurs applications et des accès utilisateurs (et, selon le type de nuage, du trafic sur leur réseau virtuel). Nombre d'organisations s'appuient trop sur le fournisseur de services infonuagiques, sans reconnaître le partage de la responsabilité en matière de sécurité.

Certaines organisations déplacent leurs actifs névralgiques (aussi appelés « joyaux de la couronne ») vers le nuage alors que d'autres adoptent une stratégie plus pondérée : tout dépend de leur appétit pour le risque. Les comités d'audit doivent s'assurer que des contrôles sont en place pour déterminer quelles données et applications peuvent migrer vers le nuage et qui peut procéder à la migration, et que les données et les applications sont sécurisées dès lors qu'elles sont dans le nuage. Il n'y a cependant aucun guide ou cadre exhaustif expliquant la façon d'y parvenir, et ceux qui existent laissent place à l'interprétation, ce qui représente un enjeu supplémentaire pour les comités d'audit.

Quelles questions les comités d'audit devraient-ils poser?

Avons-nous identifié les menaces les plus pertinentes pour notre organisation et notre secteur d'activité?

Comment évaluons-nous et surveillons-nous ces risques?

Comment nous tenons-nous au courant des risques en constante évolution, par exemple la corruption des employés?

Que faisons-nous pour accorder la priorité à l'atténuation des principaux secteurs de risques?

Quels moyens employons-nous pour nous assurer d'avoir notre juste part en matière de talents en cybersécurité?

Y a-t-il des domaines pour lesquels nous pourrions avoir recours à l'automatisation pour simplifier les contrôles?

Faire face à la pénurie de talents en cybersécurité

Un autre risque dont les comités d'audit doivent tenir compte est la grave pénurie de main d'œuvre dans le domaine de la cybersécurité. Toutes les organisations de tous les secteurs d'activité se disputent les mêmes talents, ce qui rend ardues l'embauche et la rétention des rares personnes qui savent comment repousser les menaces et exécuter un plan d'action en cas d'incident de cybersécurité.

L'intelligence artificielle et les solutions d'automatisation peuvent aider à combler la pénurie de talents et à bâtir une organisation plus résiliente, tout comme le fait de travailler avec des tiers fournisseurs de services de sécurité. Bien que l'automatisation ne remplace pas les employés, elle peut leur permettre de se concentrer sur les questions qui demandent une attention accrue.

Bâtir une base solide en matière de sécurité

Les organisations ne peuvent tout protéger et elles ne peuvent pas nécessairement empêcher toutes les atteintes; elles doivent donc adopter une approche fondée sur le risque à l'égard de la cybersécurité. Il s'agit donc de comprendre ce qui est important pour l'organisation et de connaître l'emplacement des données sensibles ainsi que l'identité de ceux qui y ont accès. Les organisations doivent également améliorer leur détection des activités suspectes et des comportements frauduleux. De plus en plus d'organisations bien établies investissent pour fusionner la cybersécurité avec d'autres sources de données afin de profiter d'une approche de nouvelle génération centrée sur l'information sur les menaces, l'analyse avancée et une technologie de pointe comme l'intelligence artificielle visant à détecter,

à examiner et à atténuer les menaces par le biais d'une plateforme unique intégrée.

Toutefois elles devront d'abord bâtir une fondation solide en matière de cybersécurité. Selon KPMG, seulement 39 pour cent des sociétés ont une « grande confiance » en leur capacité à détecter une attaque et à y répondre. Les comités d'audit doivent s'assurer que des fondations solides sont en place, puis identifier les lacunes (comme une incapacité à recruter des talents en cybersécurité ou à reconnaître les menaces internes potentielles). Afin que les organisations deviennent réellement résilientes, les comités d'audit doivent se concentrer sur la façon de répondre aux menaces, et non uniquement sur la prévention. Pour y parvenir, ils doivent s'assurer d'avoir une stratégie pour répondre à une cyberattaque et permettre la reprise des activités lorsque (et non « dans l'éventualité où ») l'organisation devra faire face à une telle cyberattaque.

Communiquez avec nous

Hartaj Nijjar

Associé, Cybersécurité
KPMG au Canada
416-228-7007
hnijjar@kpmg.ca

Yassir Bellout

Associé, Services-conseils
Cybersécurité, Montréal
KPMG au Canada
514-840-2546
ybellout@kpmg.ca

Marc Chaput

Associé, Services-conseils, Identité et
gestion des accès, Cybersécurité
KPMG au Canada
514-840-5674
mchaput@kpmg.ca

Guillaume Clément

Associé, Services-conseils
Cybersécurité et président
de EGYDE Conseils inc.
KPMG au Canada
418-653-5335
guilleumeclement@kpmg.ca

Pascal Fortin

Associé, Services-conseils,
Cybersécurité,
KPMG au Canada
514-840-2102
pfortin@kpmg.ca

Réalisons-le. home.kpmg/ca/audit-fr

© 2021 KPMG s.r.l./s.e.n.c.r.l., société à responsabilité limitée de l'Ontario et cabinet membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société de droit anglais à responsabilité limitée par garantie. Tous droits réservés. KPMG et le logo de KPMG sont des marques de commerce utilisées sous licence par les cabinets membres indépendants de l'organisation mondiale KPMG. 13478

