Comités d'audit et cybersécurité : adaptation

La direction doit mettre en place des pratiques de cybersécurité fondamentales.

Par Hartaj Nijjar

Chaque année, les organisations sont de plus en plus interconnectées sur le plan numérique et, chaque année, les cyberrisques évoluent. Les comités d'audit se voient de plus en plus confier la supervision de la gestion des cyberrisques. Ils ont donc intérêt à se tenir au fait des nouveautés dans ce domaine. Parmi ces cyberrisques, mentionnons les risques accrus liés aux chaînes d'approvisionnement, l'essor de l'utilisation de l'intelligence artificielle (« IA ») pour perpétrer et repousser des attaques et la prise de conscience croissante du fait que la cyberrésilience doit être soumise à une évaluation et à une gestion plus rigoureuses.

Les États-nations et le crime organisé demeurent les principales sources de menaces. Au cours de la dernière année, les perturbations géopolitiques mondiales ont entraîné une augmentation des cybermenaces commanditées par des États. Parallèlement, après une brève accalmie, l'activité du crime organisé a connu une résurgence sans pareil axée sur le recrutement d'initiés dans les entreprises, en plus des activités traditionnelles comme les attaques par rançongiciel. Les auteurs de menaces exploitent également les failles des produits numériques largement utilisés, ce qui leur permet d'atteindre plusieurs organisations à la fois sans en cibler une en particulier.

La chaîne d'approvisionnement au centre de l'attention

Les comités d'audit placent la sécurité de la chaîne d'approvisionnement en tête de leurs priorités depuis que plusieurs tiers prestigieux ont été victimes de compromissions, autrement dit, que leur environnement a été compromis par l'intermédiaire des systèmes informatiques d'un fournisseur. Face à l'intensification de la menace représentée par ces attaques, la direction ne

N'oubliez pas l'essentiel. Les nouveaux outils avancés de lutte contre les cybermenaces ne sont efficaces que si des pratiques fondamentales en matière de cybersécurité sont déjà en place.

Hartaj Nijjar
Associé, leader national de secteur de service, Cybersécurité

peut plus les traiter comme un simple point de défaillance parmi tant d'autres. Au contraire, elle doit réaliser une analyse en profondeur, penser de façon créative pour anticiper ces violations, tandis que les comités d'audit devraient évaluer si l'organisation prend des mesures suffisantes à des fins de prévention, d'identification et d'atténuation.

Tout d'abord, la direction devrait cartographier la chaîne d'approvisionnement de l'organisation de manière exhaustive afin de déterminer les points où les données et les composantes essentielles des systèmes interagissent avec les fournisseurs. De cette manière, il sera possible de mieux comprendre les dépendances critiques envers les fournisseurs et de repérer les points de défaillance potentiels. Partant de ce constat, les experts peuvent cibler les pistes de violations potentielles, recenser les domaines dans lesquels l'organisation est trop dépendante d'un fournisseur ou d'un ensemble de fournisseurs et diversifier les fournisseurs, si cela s'avère nécessaire.

Par ailleurs, les organisations pourraient avoir intérêt à revoir la façon dont elles établissent le profil des tiers. Les organisations qui s'appuient sur une liste de contrôle annuelle ou semestrielle, autrement dit, une liste de mesures et de pratiques exemplaires de sécurité décrivant comment protéger leurs systèmes, leurs données et leur infrastructure contre les cybermenaces, devraient envisager d'adopter une démarche plus exhaustive et continue. Une telle démarche les aiderait à comprendre pleinement si les contrôles communiqués chez le tiers sont réellement en place et s'ils répondent aux normes et aux attentes de l'organisation. Les comités d'audit devraient encourager la direction à réaliser un examen régulier pour vérifier si l'évaluation des tiers est effectuée avec la rigueur qui s'impose.

L'IA apporte son lot de nouveaux outils – et de nouveaux risques

Les auteurs de cybermenaces ont de plus en plus recours à l'IA pour cibler et adapter leurs attaques, et rechercher de nouvelles failles. Ils génèrent des hypertrucages avancés sous forme d'images, de vidéos et de voix, qu'ils utilisent pour inciter les gens à les aider. Par exemple, des utilisateurs ont été la cible de courriels et d'appels sophistiqués générés par l'IA dans le but de compromettre leurs comptes de courriel. Des centres d'appels de banques ont également été visés par des tentatives de collecte de renseignements sur leurs clients. Ces types d'attaques devraient s'intensifier considérablement, et c'est pourquoi la direction devra s'assurer de se tenir au fait des techniques d'attaque les plus récentes et des nombreux outils et services à sa disposition pour les détecter et les atténuer.

Des outils de pointe sont nécessaires pour lutter contre ces attaques. Si l'IA sert de plus en plus les auteurs des cybermenaces, elle aide également les organisations dans le cadre de la cyberdéfense. L'IA est capable de passer au crible d'énormes ensembles de données en temps réel, d'en tirer des renseignements exploitables et d'être entraînée à appliquer automatiquement des mesures défensives. Elle est utilisée pour améliorer la détection des incidents, évaluer les failles, gérer les accès et évaluer les risques liés aux tiers. Toutefois, l'IA comporte son propre lot de risques et révèle un nouvel angle d'attaque aux auteurs de menaces. Les comités d'audit doivent s'assurer que leur organisation utilise l'IA de façon sécuritaire et en atténuant les nouveaux risques liés à la confidentialité, à la réputation, à la réglementation et à la cybersécurité.

Questions que les comités d'audit devraient poser :

- Évaluons-nous de façon exhaustive les risques liés aux tiers?
- Notre utilisation de l'IA est-elle sûre et respecte-t-elle les normes de confidentialité?
- Testons-nous rigoureusement notre intervention en cas d'incident et procédons-nous à une vérification approfondie de notre fournisseur de services de sécurité gérés (« FSSG »)?
- L'organisation possède-t-elle les compétences nécessaires pour mettre en œuvre et gérer des solutions d'IA, et le comité d'audit possède-t-il suffisamment de connaissances ou a-t-il suffisamment accès à des experts externes pour les évaluer?
- Nos rapports sur la cybersécurité sont-ils suffisamment exhaustifs et opportuns?

Dans notre sondage intitulé *Perspectives des chefs de la direction en 2024,* 80 % des chefs de la direction canadiens conviennent que la façon d'intégrer l'IA repose essentiellement sur l'établissement d'une culture axée sur la cybersécurité. [1]

L'IA doit être spécifiquement conçue pour la tâche de cybersécurité à accomplir, et seules des données de grande qualité doivent être utilisées pour entraîner les modèles. Des protocoles rigoureux d'intégrité des données et de protection des renseignements personnels doivent être en place, et il convient de contrôler l'accès aux données et aux algorithmes. Les comités d'audit devraient interroger la direction sur la façon dont elle gère l'utilisation non autorisée et non régie de l'IA par le personnel en milieu de travail et sur la façon dont elle assure le suivi de la myriade de règlements en évolution qui régissent l'IA et s'y conforme. Pour développer des applications d'IA sécurisées, les organisations devront perfectionner leurs compétences ou recourir à l'externalisation, tout comme les comités d'audit chargés de s'assurer que la direction a correctement évalué la sécurité de l'IA.

En première ligne : détection des incidents et intervention

La détection des incidents est l'une des premières lignes de défense dans la lutte contre les cyberattaques. Il est essentiel que les organisations soient en mesure de repérer les activités suspectes et de déterminer le type d'attaque qui se produit afin de pouvoir réagir rapidement. La création d'un environnement dans lequel les activités suspectes peuvent être rapidement détectées est une tâche complexe qui s'appuie sur des renseignements concernant les cybermenaces, l'élaboration de cas d'utilisation, la consignation, la surveillance et l'intervention. La détection des incidents implique de plus en plus l'automatisation et l'utilisation de l'IA.

Certaines organisations exécutent cette fonction à l'interne, à l'aide des outils à leur disposition sur le marché. Bien qu'utiles, ces outils ne valent que pour les cas d'utilisation pour lesquels ils ont été conçus, et ils doivent être surveillés par des professionnels qualifiés pour s'assurer que les alertes qu'ils envoient font l'objet d'une enquête. Les organisations risquent également de trop se

[1] KPMG au Canada, « Retour aux activités de base », consulté le 31 octobre 2024. https ://kpmg.com/ca/fr/home/insights/2024/10/this-means-core.html

fier à ces outils plutôt que de se concentrer sur le processus de détection des menaces et sur l'intervention.

Compte tenu de ces défis, il est courant d'impartir ces fonctions en faisant appel à des tiers, comme des fournisseurs de services de sécurité gérés (« FSSG »). Toutefois, de nombreuses organisations ne parviennent pas à évaluer leur FSSG, qui, bien souvent, ne répond pas à leurs besoins. Deux tiers des cadres interrogés ont exprimé des doutes par rapport à leur choix de FSSG, particulièrement en ce qui concerne la détection et la réponse gérées (« DRG »). [2]

Les lacunes tant dans la détection des incidents gérés en interne que dans les services de tiers rendent de nombreuses organisations aveugles à certaines attaques. Afin d'aider à atténuer ce risque, il est impératif que les comités d'audit encouragent la direction à mettre en œuvre des exercices de cybersécurité entre les équipes de cybersécurité offensive et défensive, telles que l'« équipe rouge » et l'« équipe mauve ». Ces exercices permettent de simuler des attaques, des détections et des interventions pour favoriser la collaboration et renforcer les capacités offensives et défensives. Les comités d'audit doivent également s'assurer que la direction fournisse de l'information exhaustive et en temps opportun sur les menaces, les incidents et les mesures prises.

Couvrir les principes fondamentaux

Bien que les cybermenaces soient de plus en plus sophistiquées, les principes fondamentaux en matière de cybersécurité demeurent essentiels à la sécurité d'une organisation. Il est primordial de disposer de contrôles de sécurité fondamentaux solides, comme la gestion des vulnérabilités, la surveillance de la configuration et de la conformité, ainsi qu'une bonne gouvernance. Pourtant, de nombreuses organisations ne disposent pas complètement de ces contrôles de sécurité fondamentaux. Par exemple, certaines ont encore des difficultés à gérer les correctifs de sécurité en temps opportun. Les comités d'audit devraient interroger la direction sur la question de savoir si l'organisation a appliqué les exigences fondamentales pour un environnement de cybersécurité sain.

Les comités d'audit sont de plus en plus appelés à jouer un rôle de premier plan dans la surveillance de la cybersécurité. Pour y parvenir efficacement, ils doivent développer leurs propres compétences en cybersécurité et interroger la direction pour comprendre les nouvelles voies que les auteurs de menaces peuvent emprunter et les nouveaux outils pour les contrer. Ils doivent également s'assurer que les pratiques de base en matière de cybersécurité demeurent la base sur laquelle les nouveaux outils et les nouvelles techniques sont appliqués.

Contactez-nous

Hartaj Nijjar
Associé, leader national de secteur de service, Cybersécurité,
KPMG au Canada
416-228-7007
hnijjar@kpmg.ca

[2] KPMG au Canada, « Le rôle des FSSG fiables et innovants dans le renforcement de la cybersécurité au Canada ». consulté le 31 octobre 2024. https ://kpmg.com/ca/fr/home/insights/2024/03/role-of-trusted-and-innovative-mssps.html