Renforcer la cyberrésilience

Comment une compagnie d'assurance a transformé sa cybersécurité après une attaque par rançongiciel

Donner aux assureurs les moyens de gérer leur cybersécurité en toute confiance

Le défi : une attaque par rançongiciel compromet les données d'un assureur

Une compagnie d'assurance a dû confronter un défi de taille lorsque ses activités et ses données ont été compromises lors d'une attaque par rançongiciel. L'assureur a fait appel à l'équipe Intervention en cas d'incident de KPMG au Canada, qui s'est rapidement mobilisée pour contenir l'atteinte. Sa prompte réaction a permis de déterminer la nature de l'attaque et de limiter son impact.

Cet incident a incité l'assureur à renforcer ses mesures de cybersécurité pour réduire le risque d'attaques futures ainsi qu'à mettre en place des services de surveillance en continu pour détecter les cyberincidents et y réagir.

La solution : une approche globale et personnalisée

Consciente de ses difficultés, la compagnie d'assurance a jugé utile d'entretenir une relation de collaboration avec l'équipe Cybersécurité de KPMG au Canada. Ensemble, l'équipe du cabinet et l'assureur ont élaboré une feuille de route qui priorisait la mise en place de contrôles à l'appui des objectifs d'affaires et des aspirations de ce dernier en matière de cybersécurité accrue, et favorisait le passage d'une approche tactique à une approche stratégique.

Les mesures suivantes ont été prises en étroite collaboration avec les membres des équipes de la cybersécurité, des TI et de la direction de l'assureur :

01 Réalisation de tests de pénétration exhaustifs pour simuler des cyberattaques, cerner les lacunes de sécurité dans les systèmes et les applications, et dévoiler des vulnérabilités critiques que les équipes internes pourraient avoir négligées. Cela a permis d'effectuer une évaluation réaliste de la cybersécurité de l'assureur.

02 Amélioration du programme de gestion des vulnérabilités grâce à la mise en œuvre de processus qui visent à cerner, à évaluer, à prioriser et à corriger les lacunes en matière de sécurité au moyen des méthodes éprouvées de KPMG. Cela a aidé l'assureur à réduire les risques et à améliorer les mesures correctives au-delà des tests ponctuels.

03 Élaboration d'une feuille de route et d'un plan stratégique en matière de sécurité infonuagique qui décrivent clairement les étapes, les technologies et les politiques nécessaires pour assurer la sécurité de l'environnement infonuagique.

04 Conception et mise en œuvre d'une série de contrôles de sécurité des données pour protéger les données tout au long de leur cycle de vie, du stockage à l'utilisation. Nous avons adopté des pratiques de pointe et des contrôles de conformité, comme la loi 25, pour veiller à ce que les actifs informationnels essentiels des clients soient protégés contre les violations et respectent les exigences réglementaires.

05 Gestion améliorée des identités et des accès pour renforcer la sécurité quant aux utilisateurs, notamment en contrôlant qui peut accéder à quelles ressources en fonction du principe d'accès minimal, ce qui permet de réduire le risque d'accès non autorisé et de vol de données.

06 Déploiement du service de protection des renseignements personnels pour fournir un soutien et un savoir-faire opérationnels continus. Cela permet de gérer les obligations en matière de protection des renseignements personnels, y compris les exigences de conformité, les demandes des personnes concernées et la mise en correspondance des données.

07 Activation du service de renseignement sur les cybermenaces, qui surveille les forums cachés comme le web invisible pour détecter les signes de campagnes de cybermenaces ou de fuites de données, et qui permet une défense proactive en anticipant les menaces avant qu'elles n'aient des conséquences sur une organisation.

08 Intégration du service de recherche de menaces pour détecter de façon proactive les menaces qui pourraient avoir contourné les contrôles automatisés existants. L'assureur a ainsi pu compter sur notre personnel et notre technologie pour rechercher activement des menaces sophistiquées et cachées.

09 Établissement du service de détection et de réponse gérées, qui combine la technologie et le savoir-faire humain pour assurer une surveillance continue, une détection des menaces, une procédure d'enquête et une intervention coordonnée. Nous avons ainsi fourni à l'assureur des capacités de surveillance de la sécurité et de réponse rapide aux incidents en tout temps, soit une protection améliorée sans la complexité et les coûts associés à la création d'un centre opérationnel de sécurité interne.

Le résultat : une cybersécurité transformée

Au cours des cinq dernières années, la relation de confiance entre KPMG au Canada et l'assureur a grandement contribué à l'amélioration de la cyberdéfense globale de ce dernier. En outre, la compréhension mutuelle établie a permis de veiller à ce que les services répondent aux exigences de l'assureur et s'adaptent à ses besoins qui évoluent.

L'assureur exerce maintenant ses activités avec un sentiment de sécurité renforcé, et a confiance en sa capacité à gérer les risques liés à la cybersécurité ainsi qu'à relever efficacement les défis. Il est outillé pour explorer en toute sécurité de nouvelles occasions sur le marché, mobiliser ses clients et faire face aux défis qui se présentent.

L'assureur considère maintenant KPMG au Canada comme un conseiller de confiance sur lequel s'appuyer dans le contexte complexe de la cybersécurité.

Découvrez comment nous pouvons vous aider à renforcer votre position en matière de cybersécurité et apprenez-en davantage sur nos services.

Communiquez avec nous

Notre équipe dévouée est là pour répondre aux besoins uniques de votre organisation :

Guillaume Clément
Associé,
Services-conseils,
Cybersécurité
KPMG au Canada
+1 418 653 5335
guillaumeclement@kpmg.ca

René Bouchard
Directeur principal,
Services en gestion des risques,
Services gérés en cybersécurité
KPMG au Canada
+1 418 577 3426
rbouchard@kpmg.ca