Surmonter une atteinte à la cybersécurité dans le secteur de l'éducation

Défi client

Un important établissement d'enseignement postsecondaire au Canada, comptant plus de 500 employés et 5 000 étudiants, a été aux prises avec un incident de cybersécurité important causé par une menace interne. L'auteur de menace – un employé de confiance – a exploité son accès à des systèmes sensibles pour exfiltrer les données confidentielles des employés et des étudiants vers un appareil personnel. De plus, l'employé a compilé un rapport détaillant les vulnérabilités de l'institution.

Au moment de l'incident, l'établissement travaillait à l'amélioration de ses mesures de cybersécurité, y compris la mise à niveau de son système de détection et de réponse aux points terminaux (EDR). Bien que l'outil EDR était opérationnel, l'auteur de menace l'a contourné sans être détecté. Cette exploitation lui a permis de manipuler librement les vulnérabilités des systèmes de l'institution. Toutefois, au fur et à mesure que la nouvelle solution EDR a été déployée, elle a commencé à déclencher des alertes concernant les activités non autorisées effectuées par l'employé. Consciente des répercussions sur les renseignements personnels et la confidentialité, l'institution a rapidement évalué les alertes et avisé les personnes touchées de l'atteinte.

Solution

Dans les 24 heures suivant la découverte de l'atteinte, l'institution a fait appel à KPMG pour obtenir de l'aide. Nous avons rapidement réagi en tirant parti de notre relation préétablie avec l'établissement et de notre savoir-faire dans le secteur de l'éducation.

KPMG a amorcé l'enquête en procédant à un triage afin de comprendre l'incident, suivi d'une phase d'évaluation approfondie. Ensuite, notre équipe multidisciplinaire d'intervenants et d'analystes en cas d'incident a accédé aux technologies et aux registres de l'établissement, ce qui a rendu possible un examen détaillé des activités signalées. Notre analyse technologique approfondie comprenait un examen complet des journaux du système afin de détecter les actions malveillantes et d'évaluer les preuves de façon critique. Une équipe dévouée de cinq professionnels de KPMG, chacun spécialisé dans des domaines comme l'intervention en cas d'incident, les enquêtes technologiques et le renseignement sur les menaces, a dirigé l'établissement au cours de cette phase difficile.

Au cours de l'enquête, KPMG a découvert que l'employé malveillant avait exécuté des scripts personnalisés pour extraire des informations sensibles du progiciel de gestion intégré de l'établissement, recueilli des renseignements sur les comptes d'utilisateurs (y compris des mots de passe hachés), falsifié des courriels de dirigeants et effectué un test de pénétration dans son environnement, pour finalement compiler un rapport de ses constatations. KPMG a documenté ces découvertes dans un rapport officiel à l'intention des conseillers juridiques en matière d'intrusions. Ce rapport s'est avéré essentiel pour aider le cabinet juridique à fournir des conseils à l'établissement.

En collaboration avec le conseiller en cas d'incident, KPMG a fourni des renseignements essentiels qui ont mis en évidence les risques et les répercussions de l'intrusion, en veillant à ce que l'établissement reçoive des conseils juridiques exploitables adaptés aux circonstances particulières de l'incident. Dans l'intérêt de l'établissement, nous lui avons fourni une analyse complète des constatations techniques, y compris un calendrier détaillé des activités de l'auteur de menace. Nos recherches proactives de menaces ont permis de relever des indicateurs de compromission au sein de l'environnement de l'établissement, chacun d'entre eux ayant été solidement documenté dans notre rapport d'analyse technique.

Les renseignements détaillés fournis par KPMG ont permis à l'établissement de mieux comprendre l'incident et d'apporter les ajustements nécessaires à ses mesures de sécurité. Cette affaire souligne l'importance de la vigilance, de la recherche proactive de menaces et des stratégies d'intervention robustes en cas d'incident dans un contexte de cybersécurité en constante évolution.

Résultat : accroître la cyberrésilience

Le résultat de notre intervention a été transformateur pour l'institution. Nous avons établi une relation de confiance avec le collège, démontrant ainsi notre engagement à non seulement fournir des preuves, mais aussi à formuler des recommandations concrètes. Le collège est sorti de cet incident plus cyberrésilient, équipé d'une compréhension claire de ses vulnérabilités et rassuré qu'il avait une équipe réactive et proactive dédiée à le protéger. Cette protection est particulièrement essentielle compte tenu de la nature sensible de la clientèle dans le secteur de l'éducation, soit des étudiants et des mineurs.

Le conseiller en cas d'incident a pu aider le client en s'appuyant sur les constatations découlant de nos recherches. Cette collaboration a consolidé notre réputation de conseiller de confiance aux yeux du collège grâce à des stratégies efficaces de gestion des incidents et d'amélioration de la sécurité adaptées à son environnement particulier.

Pour en savoir plus sur nos services d'intervention en cas de cyberincident et sur la façon dont nous pouvons aider votre organisation, consultez notre site web : Intervention en cas de cyberincident.

Si vous avez vécu un cyberincident ou si vous avez des questions à ce sujet, communiquez avec notre équipe de professionnels en intervention en cas de cyberincident par courriel à cyberincident@kpmg.ca ou par téléphone au numéro sans frais 1-844-576-4911.

Contactez-nous

Alexander Rau
Associé, Services-conseils en cybersécurité
KPMG au Canada
+1 416-777-3450
alexanderrau@kpmg.ca

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