Comment l'équipe d'intervention en cas de cyberincident de KPMG a aidé une municipalité canadienne

Défi client

Une municipalité canadienne a subi une attaque par rançongiciel où l'acteur de menace externe a chiffré l'ensemble de son infrastructure informatique, y compris les services essentiels comme les systèmes de traitement de l'eau et de téléphonie. L'attaque a fait en sorte que les services quotidiens essentiels ont été indisponibles à la communauté. La municipalité n'avait pas suffisamment de personnel et de ressources technologiques pour réagir efficacement à l'incident. Plus précisément, la municipalité n'avait pas de surveillance en tout temps de son environnement informatique, ce qui limitait sa capacité à détecter l'attaque et à y répondre en temps opportun. En outre, des mécanismes d'enregistrement incomplets et des cycles limités de conservation des journaux ont entravé sa capacité à cibler l'incident, à l'analyser et à y réagir.

Solution

Pour répondre à l'incident, la municipalité a fait appel à l'équipe multidisciplinaire d'intervention en cas de cyberincident de KPMG, par l'entremise de son fournisseur de cyberassurance et de son conseiller juridique. KPMG a fourni une gamme complète de services, y compris des services de confinement des incidents, d'enquête, de soutien à la reprise des activités et de surveillance en tout temps. KPMG s'est mobilisé rapidement et a établi une communication claire avec la municipalité pour évaluer la situation et prioriser les activités de confinement des atteintes à la sécurité.

À l'aide d'outils de sécurité avancés, KPMG a mené une enquête approfondie sur l'environnement informatique de la municipalité afin de comprendre les activités de l'auteur de menace. Des mises à jour régulières de l'état d'avancement ont clarifié l'étendue et l'incidence de l'attaque. De plus, KPMG a analysé l'environnement de technologie opérationnelle de la municipalité pour bien comprendre l'incident, tout en déployant des activités de confinement appropriées.

Parallèlement, le cabinet a aidé la municipalité à récupérer des systèmes essentiels en procédant à une restauration à partir des sauvegardes disponibles et en formulant des recommandations pour perfectionner les contrôles de cybersécurité et la pile technologique de la municipalité. Il a également fourni un soutien pour la reconstruction des systèmes de téléphonie qui étaient devenus inopérants à la suite de l'attaque.

Résultat : accroître la cyberrésilience

Avec le soutien de KPMG, la municipalité a réussi à contenir l'incident et à rétablir les services essentiels. Dans le but d'améliorer sa position en matière de cybersécurité, une feuille de route stratégique a été élaborée. Cette feuille comprend des recommandations ciblées sur la technologie, les processus et la gestion du personnel.

KPMG a joué un rôle important pour aider la municipalité non seulement à se remettre de l'incident du rançongiciel, mais aussi à renforcer ses défenses contre les cybermenaces potentielles futures. Le cabinet a collaboré avec la municipalité pour mettre en place une surveillance en continu et fournir des services de tests d'intrusion – deux éléments importants pour la détection proactive des menaces et la cyberrésilience.

En plus de renforcer les mesures de sécurité interne, KPMG a amélioré la gestion des risques liés aux tiers en effectuant des évaluations détaillées de la dépendance de la municipalité à l'égard des applications et des infrastructures externes. Cela était important pour cerner et atténuer les risques associés aux tiers fournisseurs de services.

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