Comment KPMG a aidé une entreprise mondiale de transformation des aliments au Canada à se remettre d'une attaque par rançongiciel

Défi client

Une entreprise mondiale de transformation des aliments dont le siège social est au Canada et qui emploie plus de 500 employés s'est retrouvée en crise en raison d'une attaque par rançongiciel débilitante. Lors de l'incident, les serveurs et les données dans l'environnement informatique du client ont été chiffrés, les activités essentielles de l'entreprise ont été interrompue de façon prolongée et il y a eu une atteinte aux renseignements confidentiels sur les recettes, ce qui a eu une incidence sur la production, la sécurité des employés et la confidentialité. L'organisation a immédiatemment fait appel à un conseiller juridique et un fournisseur de cyberassurance pour enquêter sur les incidents et la reprise des activités.

Solution

L'équipe de réponse aux cyberattaques de KPMG a réagi rapidement en lançant un appel dans un délai de 30 minutes avec le client et son conseiller juridique (conseiller en cas d'intrusion) pour déterminer l'étendue de l'incident et en faire le tri. En accordant la priorité à la confidentialité et à la protection des renseignements personnels conformément aux directives du cabinet juridique, KPMG a obtenu l'accès aux systèmes touchés. Les membres de l'équipe de KPMG ont mené de nombreuses activités de détection de menaces et déployé des outils de détection et de réponse aux points terminaux pour contenir l'intrusion et enquêter efficacement. KPMG a également effectué l'examen exhaustif de la collecte de journaux et des preuves. Conscient de l'urgence de l'incident, KPMG a mis en place une surveillance en tout temps de l'environnement informatique afin de prévenir d'autres attaques.

Afin d'aider davantage le client, KPMG et le conseiller juridique ont retenu les services d'un négociateur indépendant associé à la demande de rançon et ont fourni du soutien pour le déchiffrement et la récupération des serveurs et des données, y compris la vérification des clés de déchiffrement. KPMG a également aidé à la reconstruction des environnements de TI et de technologie opérationnelle en collaboration avec le client, au besoin. Notre approche a assuré la confidentialité des données tout en tenant compte des répercussions sur la production et les opérations.

Résultat : accroître la cyberrésilience

Dans le cadre de la prestation des services de KPMG, le client a reçu un rapport d'enquête technologique détaillé qui comprenait un échéancier d'incident illustrant les activités exécutées par l'auteur de menace. L'enquête de KPMG a permis de découvrir d'autres activités malveillantes exécutées dans l'environnement informatique du client, en plus du déploiement de rançongiciels qui n'avaient pas été détectés auparavant. Grâce à la collaboration avec KPMG, le client a non seulement rétabli ses activités, mais il a également amélioré ses capacités de réponse en cas d'incident ainsi que son savoir-faire en matière de surveillance et de détection. Notre approche globale a permis de corriger les vulnérabilités et de créer une feuille de route stratégique pour améliorer la sécurité globale du client. Nous avons fait des recommandations, comme divers investissements en matière de sécurité, ce qui a amené le client à choisir un fournisseur de services de sécurité gérés, à effectuer des tests de pénétration dans son environnement informatique et à réviser certains processus opérationnels. En collaborant avec KPMG, le client a protégé son environnement informatique contre les menaces futures, tout en soulignant son engagement envers la résilience en matière de cybersécurité.

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