KPMG au secours d'un acteur mondial des télécommunications victime d'une cyberattaque

Le défi : répondre à une cyberattaque mondiale sophistiquée

Un fournisseur de services de télécommunications présent dans plus de 30 pays a fait face à un incident de cybersécurité grave impliquant des menaces persistantes avancées (APT). En effet, l'incident n'a pas été causé par un rançongiciel ou une autre technique perturbatrice classique, mais plutôt par une vaste opération visant le vol de renseignements stratégiques. Les cybercriminels ont exploité des vulnérabilités de l'équipement des chaînes d'approvisionnement pour cibler les systèmes de gestion des identités, ce qui leur a permis d'étendre l'opération à différentes régions du monde, dont l'Amérique du Nord, l'Afrique, l'Europe et l'Asie.

Plus tard identifiés comme faisant partie d'un groupe affilié à un État, les pirates ont utilisé des techniques hautement sophistiquées, telles que l'usurpation d'entités réseau légitimes et la reconfiguration de systèmes en temps réel sans interruption opérationnelle, ce qui rendait la détection de l'atteinte extrêmement difficile. Leur objectif était d'extraire des données confidentielles sur les abonnés – identité, emplacement et toutes les métadonnées pouvant être utilisées pour les surveiller et les cibler. Sans se faire repérer, ils ont utilisé l'accès du fournisseur de services Internet pour se déplacer latéralement jusqu'aux réseaux de clients importants. Après avoir repéré l'incident et compris la nature innovante et complexe de celui-ci, le client a reconnu le besoin de faire appel à KPMG pour endiguer la menace et protéger les données confidentielles de ses abonnés.

La solution : une intervention de bout en bout et un soutien en juricomptabilité

KPMG a fourni une gamme complète de services, y compris l'intervention en cas d'incident, l'analyse des données juricomptables, la détection de menaces et la gestion de crise. Pour contrer la menace, le cabinet a rapidement déployé une équipe interdisciplinaire de spécialistes pour soutenir l'intervention interne du client. L'équipe a fait appel à des juricomptables experts en vérification de réseau et d'hébergement pour suivre les mouvements des pirates et identifier les systèmes compromis.

En outre, des spécialistes des données ont été engagés pour gérer et analyser le volume considérable de données générées, et des ingénieurs en sécurité ont reconfiguré les mesures de surveillance existantes pour accélérer l'extraction des données et réduire le bruit causé par les résultats excessifs de requêtes, garantissant ainsi l'obtention d'information opportune et exploitable.

En parallèle, les équipes de détection de menaces ont identifié les indicateurs de compromission et cherché les activités cachées des pirates dans l'environnement numérique, tandis que les conseillers en gestion de crise et d'incident ont soutenu les communications et la prise de décisions au niveau de la direction, en veillant à ce que le client ait une compréhension claire de l'évolution des menaces et des mesures requises. KPMG a également fourni des rapports en continu et des recommandations stratégiques, y compris des mesures de confinement pour réduire la mobilité des pirates, des plans de mesures correctives pour remédier à l'obsolescence des systèmes et aux lacunes en matière de journalisation, ainsi que des améliorations aux pratiques de gestion des identités.

Au fur et à mesure que l'enquête avançait, l'étendue du soutien de KPMG s'est considérablement élargie : analyse des données, expertise en sécurité des centres opérationnels, extraction des données en vue de leur préservation, des améliorations de la surveillance, gestion des informations et des événements de sécurité (SIEM) et planification à long terme de la transformation de la cybersécurité. L'évolution de cette mission reflète la confiance croissante du client dans la capacité de KPMG à fournir des solutions de bout en bout qui répondent à la fois aux menaces immédiates et aux vulnérabilités systémiques.

Le résultat : un confinement efficace et le chemin vers une reprise sécurisée

Bien que l'enquête soit toujours en cours, l'intervention de KPMG a grandement réduit la capacité des pirates à manœuvrer dans l'environnement du client. Les systèmes essentiels ont été sécurisés et une feuille de route claire a été élaborée pour favoriser une reprise solide et la mise en place de mesures correctives à long terme. Grâce à des processus opérationnels améliorés et à une meilleure cyberrésilience, le client est désormais mieux outillé pour détecter les menaces futures et y répondre. La collaboration évolutive a également permis au client de profiter d'une gamme plus large de services, de la préservation des données à la transformation de la sécurité de ses centres opérationnels, ce qui lui assure un état de préparation mieux adapté aux défis de demain.

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