Étude de cas

Kroll Ontrack aide un groupe pharmaceutique mondial à restaurer 400 disques virtuels suite à une cyberattaque perpétrée par un employé mécontent

Une grande compagnie pharmaceutique a été confrontée au piratage de ses systèmes informatiques, menaçant la fourniture de médicaments vitaux.

Client

Une grande compagnie pharmaceutique a perdu l'accès à toutes ses données suite à une cyberattaque malveillante par un ancien employé.

Situation

Le client était en plein rachat d'une autre entreprise, dont la plupart des systèmes étaient virtualisés.

Lorsque les utilisateurs de l'entreprise ont quitté les locaux le vendredi, tous les systèmes étaient opérationnels, mais lorsqu'ils sont revenus le lundi matin, ils n'avaient plus accès aux machines virtuelles.

Le client a contacté les équipes de support de HP et de VMware et, après une enquête initiale, a découvert que les machines virtuelles et leurs instantanés avaient été supprimés des volumes source. Les volumes contenant les sauvegardes avaient été réinitialisés, écrasant les fichiers de sauvegarde.

Il a alors été recommandé au client de s'adresser à Kroll Ontrack en vue de la récupération des données.

Solution

Comme l'entreprise suspectait un acte malveillant, l'équipe de sécurité de Kroll Ontrack a été déployée dans les locaux du client pour démarrer une enquête pendant la récupération des données. L'équipe de sécurité a verrouillé le centre de traitements et installé des systèmes de surveillance, avant de lancer une investigation complète sur la brèche de sécurité suspectée.

L'équipe a rapidement déterminé qu'un individu s'était connecté à un système depuis l'extérieur de l'entreprise, avant de se connecter à une série de systèmes. Une fois que cet individu a atteint le serveur VMware, il a supprimé délibérément les disques virtuels et les sauvegardes. Il est parvenu à accéder à 27 des 28 numéros d'unité logique (LUN).

Kroll Ontrack a proposé une solution de récupération de données à distance. Plusieurs machines ont été connectées et, une fois la connexion établie, Kroll Ontrack a procédé à une évaluation des LUN fournis et a confirmé que les données avaient été supprimées du volume.

Toutes les données récupérables ont ensuite été identifiées sur chaque LUN.

Kroll Ontrack

L'évaluation s'est avérée très complexe, car le client avait une documentation limitée, des noms de machines virtuelles inconnus, du contenu inconnu sur les disques virtuels et des systèmes d'exploitation également inconnus. En outre, il n'avait aucun plan de reprise après sinistre en place pour ce système, de sorte que les priorités ont changé au cours de l'évaluation.

Ayant identifié l'ampleur du problème, qui signifiait que l'entreprise ne pouvait plus fournir des médicaments vitaux ni d'autre matériel médical, Kroll Ontrack a mis en place une équipe virtuelle utilisant les ressources de huit centres de récupération de données répartis à travers le monde. Après consultation des rapports fournis et approbation du client, les équipes de Kroll Ontrack ont extrait les données supprimées et le contenu requis des disques virtuels altérés vers un nouvel emplacement de stockage fourni par le client.

Coupable

L'administrateur système principal de l'entreprise rachetée avait quitté son emploi avant le début des pourparlers de fusion, emmenant avec lui toutes les informations système. L'entreprise a été contrainte de le réembaucher en tant que prestataire pour qu'il partage ses connaissances avec les employés restants.

Pendant cette période, il a installé un système vCenter malveillant sur le réseau de l'entreprise, sans qu'aucun des autres employés ne le sache. Il a ensuite terminé son contrat et quitté l'entreprise sans incident. Peu après qu'il ait quitté l'entreprise pour la seconde fois, cette dernière a fusionné avec une compagnie pharmaceutique plus grande. Au cours de la fusion, certains employés ont été licenciés, parmi lesquels un ami de l'administrateur.

Durant l'enquête de sécurité menée par Kroll Ontrack, les enquêteurs ont trouvé une entrée non autorisée provenant de l'extérieur du réseau dans l'un des journaux d'un routeur. Cette entrée les a conduits jusqu'au système vCenter malveillant et, de là, après avoir travaillé avec l'équipe de support de VMware, ils ont déterminé qu'il s'agissait du système utilisé pour supprimer tous les disques virtuels et leurs instantanés.

L'équipe de Kroll Ontrack a alors contacté le FBI et, en travaillant avec leur équipe, a réussi à déterminer que l'adresse IP externe appartenait à AT&T. Le FBI a contacté AT&T et appris que l'adresse IP correspondait à un McDonalds. Le FBI a envoyé des agents de terrain au McDonalds en question et découvert la preuve qu'un de leurs suspects y était présent le jour où l'incident s'était produit. Une fois les agents de terrain en possession de la preuve, ils sont allés trouver le suspect, qui a avoué.

En parcourant les écrits et les comptes rendus d'audiences, l'équipe a appris que l'administrateur principal avait décidé de venger le licenciement de son ami et de donner une leçon à son ancienne entreprise. Un dimanche matin, il a pris sa voiture, s'est rendu au McDonalds en question, y a acheté son petit-déjeuner avec sa carte de crédit, puis s'est connecté au Wi-Fi public. Là, il a établi une connexion au système vCenter malveillant et s'est mis à supprimer toutes les machines virtuelles, ainsi que les sauvegardes.

Epilogue

Kroll Ontrack est parvenu à récupérer toutes les machines virtuelles cruciales et à remettre les données au client en un temps record. Au total, le délai de récupération s'est élevé à environ trois semaines.

Le prévenu (l'administrateur principal) a été condamné à 41 mois de prison et s'est vu infliger une amende de 812 000 dollars.

France : 0 800 10 12 13
www.ontrack.fr

Belgique : +32 (0)2 512 30 22
www.ontrackdatarecovery.be

Kroll Ontrack.