Les cinq leçons apprises de l'attaque par ransomware que nous avons subie

Par Mark Hughes, vice-président senior, DXC Technology

En cas d'attaque par ransomware, il faut agir vite parce que l'interruption des systèmes impacte concrètement l'activité.

Il est bien démontré que les attaques par ransomware sont en augmentation et qu'elles peuvent avoir des conséquences graves sur tous les aspects d'une entreprise, ses clients, son exploitation, sa marque et même son conseil d'administration.

Dans le cadre de mes fonctions chez DXC Technology, je supervise les activités en rapport avec la sécurité et je m'occupe des attaques fréquentes dont sont victimes nos clients. Le samedi 4 juillet 2020, alors que je sortais de la voiture et que j'étais sur le point de démarrer mes vacances en famille, l'entreprise a été la cible d'une attaque par ransomware.

Était visée Xchanging, une filiale basée au Royaume-Uni, laquelle offre des services technologiques aux entreprises évoluant dans le secteur de l'assurance généraliste. Le cybercriminel a envoyé l'image souvent utilisée d'un personnage de dessin animé bien mignon faisant un geste obscène de la main accompagnée de ce message : « Nous avons vos données. Nous avons chiffré vos fichiers. Si vous voulez négocier, ça peut se faire par le biais d'un outil sécurisé ou par chat. »

Bien que le réseau utilisé par Xchanging était séparé de l'environnement beaucoup plus vaste de DXC, nous nous inquiétions néanmoins de l'impact possible sur les activités des clients de Xchanging lorsque les agences à Londres ouvriraient le lundi.

En cas d'attaque par ransomware, il faut agir vite parce que l'interruption des systèmes impacte concrètement l'activité. Emsisoft nous apprend qu'une attaque induit en moyenne un arrêt des systèmes de 16 jours et prévoit que les coûts liés aux attaques par ransomware pourraient atteindre 170 milliards de dollars dans le monde en 2020.

Dans le cas de Xchanging, le hacker était entré dans l'environnement juste deux jours plus tôt. Il n'avait accédé qu'à quelques-uns des systèmes, et nous avons pu rapidement isoler et neutraliser l'attaque. Aucun jeu de données n'a été volé et nous n'avons pas payé la rançon. Nous avons immédiatement informé nos clients et les autorités.

Le dimanche 5 juillet, nous avons nettoyé et restauré l'environnement impacté. Dès le lundi matin, Xchanging était en mesure de traiter des polices d'assurance.

Mes conseils pour rester en sécurité

L'enquête criminelle est en cours, et nous nous employons pleinement à réviser nos systèmes de contrôle et nos procédures. Tout ou presque a fonctionné comme prévu. Malheureusement, ce n'est pas le cas pour nombre d'entreprises.

Nous avons analysé ce qui s'est bien passé, ce qui s'est mal passé et nous réfléchissons à ce que nous pouvons améliorer.

Cinq points essentiels :

Connaître son infrastructure. Il faut mettre l'accent sur les systèmes de correctifs logiciels, et s'assurer que tous les réseaux et pare-feux disposent d'outils permettant de détecter les comportements malveillants. Dans notre cas, les hackers ont commencé par utiliser un outil de test de sécurité accessible au public que l'on qualifie de « grayware ». Le grayware n'est pas malveillant en soi mais il a été utilisé ici pour créer une porte dérobée afin d'exploiter Microsoft Windows et de déployer une nouvelle variante du malware de chiffrement. Bien que nous n'ayons pas empêché l'attaque, nous avons été alertés et su qu'il y avait un problème, nous avons ainsi pu déterminer quel endroit du réseau était attaqué.

Les autorités recommandent vivement de ne pas payer les rançons. En fait, les États-Unis et le Royaume-Uni travaillent sur une réglementation visant à punir, au civil et au pénal, ceux qui paient des rançons.

Impliquer les dirigeants dès le début. Notre équipe de crise globale s'est réunie pour évaluer la situation. Ceci a été essentiel pour nous car nous avons directement impliqué les hauts dirigeants pour que les décisions cruciales puissent être prises rapidement. Il fallait par exemple interrompre les accès à distance, j'ai donc pris la décision de couper toute connectivité avec les systèmes de Xchanging. Bien que cela semble facile, l'action urgente de nos équipes informatiques au Royaume-Uni et en Inde était nécessaire. Impliquer les responsables de ces équipes a permis une coupure de connectivité rapide et efficace. Pendant l'événement, toute la direction - notre PDG, Mike Salvino, également - a participé au travail d'évaluation de la situation et a pris les décisions clés. Dans pareilles circonstances, il est crucial d'avoir une bonne gouvernance. Si les responsabilités des uns et des autres ne sont pas établies et si on ne sait pas clairement qui fait quoi, on perd de précieuses minutes dont les hackers profitent.

Travailler tôt avec les autorités et les experts. La police et les experts en sécurité peuvent offrir des informations précieuses permettant de contrer une attaque et de bénéficier d'une intervention judiciaire rapide. Dans le cas présent, le ransomware était configuré de façon à envoyer les données de Xchanging vers des domaines internet aux États-Unis. J'ai donc contacté les responsables de la police qui travaillaient pendant ce jour férié. Le soir même, nous avons obtenu une décision de justice nous permettant de prendre le contrôle des domaines internet des hackers.

S'organiser au mieux et ne pas payer la rançon. Les Autorités recommandent vivement de ne pas payer les rançons. En fait, les États-Unis et le Royaume-Uni travaillent sur une réglementation visant à punir, au civil et au pénal, ceux qui paient des rançons. Dans notre cas, les hackers n'ont pas tout de suite demandé de l'argent. Ils voulaient négocier. Nous savions que nous avions stoppé l'attaque, nous savions qu'ils n'avaient pas nos données et nous savions que nous avions des sauvegardes. Nous étions en position de force, nous n'avions donc pas besoin de négocier. Si vous

décidez de négocier avec des cybercriminels, n'y allez pas seul. Mettez en place un négociateur expérimenté, de préférence quelqu'un faisant partie de l'équipe d'intervention, avant d'être attaqué.

Être transparent. Vous n'avez pas à tout dévoiler, mais il est généralement bon d'être ouvert. Nous avons communiqué à des centaines de clients les indicateurs de compromission (IOC) du hacker. Bien qu'il y ait des informations que vous ne pouvez pas transmettre (par exemple, si vous êtes soumis à des obligations de confidentialité ou si la police vous le demande), partager les informations quand cela est possible permet non seulement de protéger les autres, mais aussi de bénéficier de l'aide d'un grand nombre de vos collègues, des Autorités et de la communauté engagée autour des questions de sécurité. Le dimanche 5 juillet, nous avons publié un communiqué de presse pour informer les marchés, et nous avons renouvelé la démarche quelques semaines plus tard pour confirmer que le problème avait été réglé.

Les responsables de la police auxquels j'ai parlé ce weekend-là étaient surpris d'apprendre que l'attaque était déjà contrée. La plupart des appels qu'ils reçoivent proviennent de PDG parce que les équipes informatiques et de sécurité sont très occupées, et que l'entreprise en est généralement à son troisième ou quatrième jour d'interruption des systèmes et que la reprise n'est pas en vue.

Nous savons que l'attaque du 4 juillet aurait pu être bien pire. L'association des actions rapides de notre équipe d'intervention, des contrôles de sécurité et d'une bonne gouvernance, ainsi que le recours à des outils techniques et aux bonnes pratiques du secteur nous ont donné un avantage.

Le « new DXC » qui a émergé a montré sa force et sa capacité à faire face, et a prouvé que ses clients sont sa priorité à chaque instant.

C'est ainsi que j'ai passé mes vacances d'été.

Ne manquez rien des dangers qui menacent vos systèmes. Pour recevoir notre Security Threat Intelligence Report, abonnez-vous sur **www.dxc.technology/threats_HBR**.

L'auteur

Mark Hughes est vice-président senior chargé des offres et des partenaires stratégiques chez DXC Technology. Il est responsable de la sécurité globale et des solutions associées, pour la cyberdéfense, l'infrastructure sécurisée, l'identité numérique et la protection des données notamment. Il a occupé le poste de PDG chez BT Security.

DG_8078a-21. décembre 2020