Une grande entreprise aérospatiale remporte la victoire contre des escrocs utilisant un ransomware

Comment HarcoSemco a déjoué une attaque CryptoLocker grâce à la facilité de bouton-poussoir de Barracuda Backup.

L'attaque

Depuis son apparition en 2013, le ransomware populaire CryptoLocker, ainsi que ses nombreuses versions, a été utilisé pour extorquer des milliards de dollars à des entreprises du monde entier. Mais lorsqu'il a été utilisé pour attaquer HarcoSemco, un important fabricant de composants aérospatiaux, le directeur informatique Brian O'Connor était déterminé à récupérer les données chiffrées et à laisser les criminels partir les mains vides.

« C'était terrible », dit O'Connor en décrivant le matin où les employés ont trouvé leurs fichiers inaccessibles et une image menaçante sur leurs ordinateurs de bureau en arrivant. « Tout le monde paniquait, mais nous étions décidés à ne pas payer la rançon. »

Selon O'Connor, l'attaque a infecté des dossiers publics et même un serveur contenant des données financières en direct, ce qui aurait créé une énorme responsabilité pour l'entreprise. Les dommages potentiels à la réputation de HarcoSemco à eux seuls auraient été intolérables.

> « Barracuda Backup a fonctionné exactement comme il se doit. Cela a été facile et rapide, et nos attaquants n'ont rien obtenu. »
>
> **Brian O'Connor**
> Responsable informatique,
> HarcoSemco

Profil

- Basée à Branford, au Connecticut
- Un fabricant de composants aérospatiaux de premier plan
- Plus de 60 ans d'expérience dans le secteur

Difficultés

- Récupération des données critiques verrouillées par CryptoLocker
- Forte rançon demandée par les attaquants
- Réduire au minimum les temps d'arrêt pendant la récupération

Solution

Barracuda Backup

Résultats

- Aucune rançon payée
- Aucun temps d'arrêt important
- Tranquillité d'esprit permanente

La réponse

Lorsque O'Connor a rejoint HarcoSemco, l'entreprise utilisait un système sur bande pour sauvegarder les données. Mais les limites intégrées de ces systèmes, qui nécessitent beaucoup de temps et de travail, évoluent mal, ne mettent pas à jour les fichiers de sauvegarde assez souvent et ne sont pas toujours fiables, l'ont rapidement amené à chercher une nouvelle solution.

« Notre société sœur en Californie utilisait Carbonite EVault; nous avons donc examiné cette solution », explique O'Connor. « Mais nous l'avons trouvée un peu mal conçue. Je me suis alors adressé à TBNG Consulting pour obtenir de l'aide et ils ont porté le produit Barracuda à notre attention. » Après une période d'essai réussie, O'Connor a commandé deux appliances Barracuda Backup 690. L'une a été installée dans le bureau de Branford et l'autre a remplacé la solution Carbonite de la société californienne. Chaque appliance a répliqué ses fichiers sauvegardés localement sur l'autre. Sept ans plus tard, la même solution est toujours utilisée, bien que HarcoSemco soit passée à des modèles 790 de plus grande capacité.

Ainsi, lorsque CryptoLocker a pris le contrôle des fichiers de l'entreprise, alors que certaines personnes paniquaient, O'Connor a tout simplement commencé à supprimer les fichiers infectés et à les restaurer à partir des fichiers de sauvegarde les plus récents. « Au début, je restaurais quelques éléments avant de réaliser l'ampleur des attaques », se souvient-il. « À la fin de la journée, j'ai finalement décidé de restaurer l'ensemble du serveur. Barracuda Backup a fonctionné exactement comme il se doit. Cela a été facile et rapide, et nos attaquants n'ont rien obtenu. »

Perspectives d'avenir

« Je suis toujours surpris d'entendre qu'une organisation a dû payer une rançon ou a perdu des données critiques à cause d'un ransomware », explique O'Connor. « Toute solution de sauvegarde convenable, moderne et bien gérée devrait rendre cela pratiquement impossible. Cela dit, Barracuda Backup se démarque des autres produits en raison de sa facilité d'utilisation, de la souplesse de ses options de réplication et de son évolutivité. »

HarcoSemco attend avec impatience certains changements qui pourraient rendre la souplesse mentionnée par O'Connor particulièrement utile. « Notre société sœur en Californie fermera bientôt ses portes », explique O'Connor, « donc toutes ses données seront transférées ici et nous devrons repenser notre stratégie de réplication. Ensuite, une nouvelle installation ouvrira ses portes au Mexique et nous devrons également l'intégrer au système. »

O'Connor fait face à une contrainte : se conformer à l'ITAR, la Réglementation américaine sur le trafic d'armes au niveau international. « Lorsque nous avons obtenu les appliances Barracuda Backup pour la première fois, nous pensions que l'utilisation de la fonction de réplication dans le cloud du produit pouvait nous exposer à des risques en termes de conformité ITAR », dit-il. « Nous réexaminerons probablement cela, lorsque le remaniement d'entreprise sera en cours. En supposant qu'elle soit conforme à l'ITAR, la réplication dans le cloud de nos sauvegardes de données pourrait être très utile en termes d'évolutivité et de continuité des opérations à long terme. »

> « Notre société sœur en Californie utilisait Carbonite EVault ; nous avons donc examiné cette solution. Mais nous l'avons trouvée un peu mal conçue. Je me suis alors adressé à TBNG Consulting pour obtenir de l'aide et ils ont porté le produit Barracuda à notre attention. »
>
> **Brian O'Connor**
> informatique
> HarcoSemco

En savoir plus sur Barracuda Backup

https://fr.barracuda.com/products/backup

Barracuda
Your journey, secured.