ÉTUDE DE CAS

Un fournisseur de matériel lourd lutte et triomphe contre une attaque de ransomware avec Tanium

Après une attaque, Ring Power, un distributeur d'équipements Cat® basé en Floride, s'est appuyé sur Tanium pour éviter de payer une rançon, tout en remettant son data center et ses endpoints en état de fonctionnement.

Entreprise

Ring Power Corp.

Secteur

Fourniture d'équipements lourds

Siège

Saint Augustine, Floride, USA

Endpoints gérés

2 300

Solutions Tanium

- Chasse aux menaces
- Découverte et inventaire des actifs
- Supervision des données sensibles
- Gestion des risques et de la conformité
- Gestion des clients

Problématique

À la suite d'une attaque de ransomware, Ring Power s'est retrouvé avec un data center entièrement coupé du monde, et avec un nombre d'endpoints infectés inconnu.

Solution

Avec l'aide de Tanium, Ring Power s'est pleinement remis de l'attaque, et sans payer de rançon.

Résultat

Grâce à Tanium, Ring Power n'a pas eu à payer la rançon, et n'a même pas communiqué avec ses assaillants.

Tanium peut aider les organisations à se remettre rapidement et efficacement sur pied à la suite d'une attaque de ransomware.

Comment Ring Power s'est remis d'une attaque de ransomware grâce à Tanium

Un matin de septembre 2019, Kevin Bush a été réveillé par un coup de fil l'informant que Ring Power était victime d'une attaque de ransomware. Il a alors découvert que l'ensemble de son data center était désormais coupé du monde. En outre, un nombre inconnu de ses 2 300 endpoints étaient dangereusement infectés.

Avec l'aide de Tanium, Kevin Bush et son équipe informatique de 10 personnes ont pu désinfecter et restaurer entièrement l'infrastructure de Ring Power en quelques semaines. En outre, l'entreprise a accompli tout cela sans payer de rançon, et sans le moindre échange avec ses assaillants.

La veille au soir, un des responsables de Ring Power avait cliqué à son insu sur un e-mail de phishing.

Problématique

À 4h30 du matin, Kevin Bush, vice-président des systèmes d'information pour le fournisseur de matériel lourd Ring Power Corp., a été réveillé par un coup de fil qu'il redoutait plus que tout.

Son interlocuteur matinal, un représentant du fournisseur de services managés de Ring Power, avait de mauvaises nouvelles à annoncer. La veille au soir, un des responsables de Ring Power avait cliqué à son insu sur un e-mail de phishing. Durant les heures qui ont suivi, l'infrastructure de l'entreprise a été victime d'une attaque de ransomware. Le résultat : un nombre incertain d'endpoints infectés, et un data center pris en otage.

Tous ces incidents survenaient seulement 11 jours après son arrivée chez Ring Power. « Les ransomwares sont comme un cancer », explique-t-il. « Conscients de la menace, nous croisons simplement les doigts pour que cela ne nous tombe pas dessus. »

Solution

Avec l'aide de Tanium, M. Bush et son équipe ont restauré l'infrastructure de l'entreprise en quelques semaines. De plus, le groupe a accompli cela sans payer la moindre rançon, et en refusant d'échanger avec les attaquants.

« Grâce à Tanium, nous avons pu rétablir nos systèmes avec une grande simplicité », déclare Brian Hall, responsable des opérations de gestion des systèmes d'information de Ring Power, et membre de l'équipe informatique de Kevin Bush.

Kevin Bush et son équipe ont mis près de trois semaines à accomplir tout cela. Le matin où l'attaque a été signalée, leur première initiative après la conversation téléphonique a été de se rendre d'urgence au bureau pour évaluer l'étendue des dégâts. La situation n'était pas encourageante. Le data center de Ring Power, y compris ses 150 serveurs, était complètement coupé du monde.

Pour limiter les dégâts, M. Bush et son équipe ont pris des mesures immédiates : ils ont éteint tous les serveurs, protégé leurs systèmes de sauvegarde en les déconnectant, et contacté les 26 sites de l'entreprise par téléphone pour inciter le personnel local à tester ses ordinateurs à la recherche d'infections. S'il leur était possible d'ouvrir Word ou Excel, cela signifie que la machine utilisée était saine. En revanche, si l'icône « Ryuk » s'affichait à l'écran, cela voulait dire que la machine était infectée. Dans ce cas, les employés avaient pour instruction d'éteindre leurs ordinateurs, de les mettre dans une boîte, et de les envoyer au siège de Ring Power, où la machine pouvait faire l'objet d'une désinfection.

Une fois cette opération effectuée, l'étape suivante a été de restaurer les systèmes. Redémarrer 150 serveurs, redéployer près de 200 applications et remettre environ 2 300 endpoints en service n'a pas été une mince affaire. Kevin Bush et son équipe ont travaillé 80 heures par semaine pendant deux longs mois.

Ensuite, l'entreprise a choisi d'installer Tanium sur tous les endpoints sains. Ring Power venait de signer un contrat pour bénéficier de la solution Tanium as a Service (TaaS), mais n'avait pas eu le temps de lancer la phase d'installation. L'équipe informatique a chargé les outils Tanium sur un grand nombre de clés USB, et les a expédiées vers les différentes succursales avec des instructions.

« Nous avons déployé Tanium partout où nous le pouvions. »

> Tanium offre à l'ensemble de notre équipe une visibilité centralisée. Sans cela, il nous est impossible de dormir sur nos deux oreilles.
>
> **Kevin Bush**
> Vice-président des systèmes d'information chez Ring Power Corp.

« Tanium a joué un rôle clé dans le rétablissement de nos systèmes »

Kevin Bush, vice-président des systèmes d'information chez Ring Power Corp, un fournisseur de matériel lourd basé à Saint Augustine (Florida).

> J'aime ce que Tanium nous apporte. Nous pouvons configurer la solution comme nous le voulons, et elle fonctionne, tout simplement. Il suffit de la configurer et de la laisser agir.

Brian Hall
Responsable des opérations de gestion des systèmes d'information chez Ring Power Corp.

Résultat

Une fois Tanium installé sur les ordinateurs des utilisateurs, ces derniers ont pu redéployer eux-mêmes leurs applications. Kevin Bush et son équipe n'ont donc pas eu à effectuer le travail manuellement — un atout remarquable pour Ring Power, compte tenu de ses nombreux sites, utilisateurs et systèmes.

En outre, l'entreprise n'a pas dû payer la moindre rançon. Elle n'a même jamais eu à communiquer avec ses assaillants. M. Bush a simplement transmis l'adresse e-mail des attaquants au FBI. Par la suite, l'agent fédéral en charge de l'affaire a estimé que Ring Power était mieux préparé que 90% des entreprises. Cette évaluation prend toute sa valeur lorsque l'on sait que l'agent en question reçoit en moyenne 4 nouvelles affaires par jour.

Grâce à Tanium, Ring Power a également grandement accru sa visibilité sur les endpoints de son réseau. L'entreprise envisageait d'utiliser l'outil de gestion de systèmes SCCM de Microsoft, mais a découvert que celui-ci était bien plus complexe que l'offre de Tanium.

« Tanium est extrêmement simple à gérer », explique Brian Hall. « En outre, la solution propose de nombreux modules et fonctionnalités qui font défaut à SCCM. Nous n'avons donc eu aucun mal à faire notre choix. »

Tanium a également permis à Ring Power d'automatiser la gestion des patchs et mises à jour. Auparavant, l'équipe de gestion des systèmes d'information procédait manuellement, ce qui lui prenait un temps considérable. Désormais, Tanium s'occupe de tout. L'entreprise a ainsi récupéré l'équivalent d'une heure et demie de travail par jour.

Envie d'en savoir plus ? Rendez-vous sur **www.tanium.com**.