CAS CLIENT

Commvault

BILTHOVEN BIOLOGICALS

Bilthoven Biologicals renforce sa protection contre les ransomwares avec Commvault et Commvault Cloud Air Gap Protect.

Bilthoven Biologicals
Cyrus Poonawalla Group

L'entreprise néerlandaise de santé reprend ses activités après des cyberattaques.

Secteur
Santé

Localisation
Pays-Bas

Site web
www.bbio.nl/fr

En bref
- Principal fabricant néerlandais de vaccins
- Produit une gamme de vaccins contre la polio de haute qualité pour prévenir les maladies mortelles

Principaux actifs protégés
- 60 To de données
- 300 machines virtuelles • Données Microsoft 365
- Microsoft Active Directory

L'environnement de sauvegarde
- Commvault Cloud Backup & Recovery
- Commvault Cloud Air Gap Protect

DÉFI

- Les utilisateurs ne pouvaient pas accéder aux fichiers en raison d'attaques par ransomware
- Nécessité d'un plan de reprise après sinistre pour prioriser les services importants et maintenir l'opérabilité tout en minimisant l'impact sur le processus critique de production de vaccins

SOLUTION

- Adoption de Commvault Cloud Backup & Recovery pour récupérer facilement les données dans Microsoft 365 et l'environnement virtuel à travers plusieurs bureaux et l'usine
- Intégration avec Commvault Cloud Air Gap Protect pour améliorer la sécurité des données et renforcer la protection contre les ransomwares

RÉSULTAT

- Reprise de tous les services en quelques jours après l'attaque
- Réduction du nombre d'étapes nécessaires pour restaurer une machine virtuelle ou une copie de sauvegarde grâce à un tableau de bord intuitif
- Renforcement de la sécurité et de la protection des données dans l'environnement hybride
- Permet une récupération rapide des données, assurant la continuité des opérations de fabrication

> **Nous adorons la simplicité du tableau de bord Commvault. En quelques clics, nous pouvons restaurer une machine virtuelle ou des sauvegardes après une attaque, ce qui est essentiel dans notre domaine en tant qu'entreprise pharmaceutique manipulant des données très sensibles. »**
>
> **Paul Vries, consultant en informatique**
> Bilthoven Biologicals

ATTÉNUATION DES RISQUES D'ATTAQUES PAR RANSOMWARE

Fondé par le groupe Cyrus Poonawalla après la privatisation de l'Institut Néerlandais des Vaccins en 2012, Bilthoven Biologicals (BBio) développe et fournit des vaccins contre la polio à l'Organisation Mondiale de la Santé, à l'UNICEF et à de nombreux pays dans le monde entier. Avec une équipe d'experts motivés travaillant sans relâche, BBio produit des vaccins abordables et de haute qualité qui contribuent à prévenir des maladies potentiellement mortelles.

Pour poursuivre sa mission de fabriquer des vaccins pour un monde meilleur, il est crucial pour BBio de protéger ses données contre les attaques par ransomware et d'assurer des opérations de fabrication sans interruption.

« On ne peut jamais être totalement préparé à un ransomware car on ne sait pas quand il va frapper. Les acteurs malveillants n'ont besoin que de trouver un seul point faible pour attaquer les données de votre organisation », a déclaré Paul Vries, consultant en informatique chez Bilthoven Biologicals. « En tant que département informatique, nous devons toujours nous assurer que tout est sécurisé. Avec Commvault, nous pouvons construire un mécanisme de défense pour prévenir les cyberattaques et permettre une récupération rapide. »

RESTAURATION DES DONNÉES EN TOUTE SIMPLICITÉ

BBio a subi sa première grande attaque par ransomware le 21 septembre 2022. Tout a commencé par des appels d'utilisateurs incapables de se connecter ou d'accéder à leurs fichiers. Après quelques recherches, Vries a découvert une note de rançon indiquant que leurs fichiers étaient cryptés et exigeant un paiement pour les décrypter.

« Le ransomware s'est propagé à travers le domaine et l'usine. En gros, tout ce qui était connecté à l'Active Directory était compromis », a déclaré Vries. « Nous avons dû agir rapidement pour stopper la propagation car nous n'étions pas sûrs de l'étendue exacte de l'impact. »

Vries a immédiatement pris contact avec la direction de BBio et l'équipe de cybersécurité, ainsi qu'avec KEMBIT, le prestataire de services gérés de l'entreprise, pour analyser la situation et déterminer les actions à suivre. Leur première réaction a été de déconnecter le réseau et d'éteindre les serveurs et les machines virtuelles infectés par l'attaque, tout en laissant les machines non affectées en fonction pour minimiser l'impact sur le processus de production de vaccins. Une autre étape importante a été d'informer les employés de ce qui se passait afin qu'ils comprennent la criticité de la situation.

Le deuxième jour de l'attaque, Vries et son équipe ont réussi à remettre en ligne l'Active Directory et l'environnement Commvault. Après avoir reconstruit le Commvault Cloud Backup & Recovery, Vries a déclaré qu'il était facile et simple de restaurer le service.

« Nous adorons la simplicité du tableau de bord Commvault. En quelques clics, nous pouvons restaurer une machine virtuelle ou des sauvegardes après une attaque, ce qui est vital dans notre domaine en tant qu'entreprise pharmaceutique manipulant des données très sensibles », a déclaré Vries. « Commvault nous donne confiance en la sécurité de nos données et en la rapidité de remise en service de nos services importants. »

Comme Commvault était si simple à utiliser, l'équipe a pu se relayer pour restaurer les services de l'entreprise tout au long de la nuit et jusqu'à ce que tout soit restauré. Grâce au partenariat entre l'équipe informatique, KEMBIT et Commvault, BBio a pu rétablir complètement le service dans plusieurs bureaux et son usine en seulement neuf jours.

« Si nous n'avions pas eu Commvault et que les sauvegardes n'avaient pas été faites avant l'attaque, la situation aurait pu être bien pire », a déclaré Vries.

> **Commvault nous donne confiance en la sécurité de nos données et en la rapidité de remise en service de nos services importants. »**
>
> **Paul Vries, consultant en informatique chez**
> Bilthoven Biologicals

ÉLABORATION D'UN PLAN DE RÉCUPÉRATION APRÈS SINISTRE

Depuis l'incident de ransomware, BBio et son équipe informatique ont tiré des enseignements importants.

« Nous n'avions pas de plan de récupération en place avant l'attaque », a déclaré Vries. « Nous travaillons désormais avec Commvault pour élaborer un plan de reprise après sinistre afin de mieux identifier les priorités de remise en service et l'ordre dans lequel elles doivent être effectuées. »

Certains fichiers n'ont pas été cryptés lors de l'attaque car BBio avait déplacé les agents médias hors du domaine. Avec la transition vers Microsoft 365, l'entreprise met également en place Commvault Cloud Air Gap Protect avec Commvault Cloud Backup & Recovery pour simplifier davantage les sauvegardes dans l'environnement hybride et renforcer la protection contre les ransomwares.

« Avec Commvault et Commvault Cloud Air Gap Protect, nous pouvons facilement gérer, protéger et récupérer des données dans le cloud et sur site, même dans le pire des cas », a déclaré Vries.

« Avec Commvault et Commvault Cloud Air Gap Protect, nous pouvons facilement gérer, protéger et récupérer des données dans le cloud et sur site, même dans le pire des scénarios. »

Paul Vries, consultant en informatique chez
Bilthoven Biologicals

To learn more, visit **commvault.com**