CUSTOMER STORY

Commvault

BILTHOVEN BIOLOGICALS

Bilthoven Biologicals verstärkt den Schutz gegen Ransomware mit Commvault und Commvault Cloud Air Gap Protect

Bilthoven Biologicals
Cyrus Poonawalla Group

Das niederländische Gesundheitsunternehmen setzt den Betrieb nach Cyberangriffen fort.

Branche
Gesundheitswesen

Standort
Niederlande

Website
www.bbio.nl/de

Auf einen Blick
- Führender niederländischer Impfstoffhersteller
- Produziert eine Reihe hochwertiger Polio-Impfstoffe zur

Verhinderung lebensbedrohlicher Krankheiten
Wichtige geschützte Vermögenswerte
- 60 TB Daten
- 300 virtuelle Maschinen
- Daten von Microsoft 365
- Microsoft Active Directory
- Das Backup-Umfeld
- Commvault Cloud Backup & Recovery
- Commvault Cloud Air Gap Protect

HERAUSFORDERUNG

- Benutzer konnten aufgrund von Ransomware-Angriffen nicht auf Dateien zugreifen
- Notwendigkeit eines Katastrophenwiederherstellungsplans, um wichtige Dienste zu priorisieren und die Betriebsfähigkeit zu erhalten, während die Auswirkungen auf den kritischen Impfstoffproduktionsprozess minimiert werden

LÖSUNG

- Einführung von Commvault Cloud Backup & Recovery zur einfachen Datenwiederherstellung in Microsoft 365 und der virtuellen Umgebung über mehrere Büros und die Fabrik hinweg
- Integration mit Commvault Cloud Air Gap Protect zur Verbesserung der Datensicherheit und Stärkung des Schutzes gegen Ransomware

ERGEBNIS

- Wiederaufnahme aller Dienste innerhalb von Tagen nach dem Angriff
- Reduzierung der notwendigen Schritte zur Wiederherstellung einer virtuellen Maschine oder einer Sicherungskopie mit einem intuitiven Dashboard
- Verstärkte Datensicherheit und Schutz in der hybriden Umgebung
- Ermöglichte schnelle Datenwiederherstellung, um kontinuierliche Produktionsabläufe zu gewährleisten

> **Wir schätzen die Einfachheit des Commvault-Dashboards. Mit nur wenigen Klicks können wir eine virtuelle Maschine oder Backups nach einem Angriff wiederherstellen, was in unserer Branche als Pharmaunternehmen mit sehr sensiblen Daten von entscheidender Bedeutung ist."**
>
> **Paul Vries, IT Consultant**
> Bilthoven Biologicals

RISIKOMINDERUNG BEI RANSOMWARE-ANGRIFFEN

Nach der Privatisierung des Niederländischen Impfinstituts im Jahr 2012 gegründet, entwickelt und liefert Bilthoven Biologicals (BBio), eine Einrichtung der Cyrus Poonawalla Group, Polioimpfstoffe an die Weltgesundheitsorganisation, UNICEF und viele Länder weltweit. Mit einem Team motivierter Experten, die rund um die Uhr arbeiten, liefert BBio erschwingliche, hochwertige Impfstoffe, die lebensbedrohliche Krankheiten verhindern helfen.

Um seine Mission, Impfstoffe für eine bessere Welt herzustellen, fortzusetzen, ist es für BBio entscheidend, seine Daten vor Ransomware-Angriffen zu schützen und einen reibungslosen Produktionsbetrieb zu gewährleisten.

„Ransomware ist etwas, auf das man sich nicht vollständig vorbereiten kann, da man nicht weiß, wann es zuschlägt. Böswillige Akteure müssen nur eine Schwachstelle finden, um die Daten Ihrer Organisation anzugreifen", sagte Paul Vries, IT-Berater bei Bilthoven Biologicals. „Als IT-Abteilung müssen wir immer sicherstellen, dass alles sicher ist. Mit Commvault können wir einen Abwehrmechanismus aufbauen, um Cyberangriffe zu verhindern und eine schnelle Wiederherstellung zu ermöglichen."

DATENWIEDERHERSTELLUNG MIT LEICHTIGKEIT

BBio erlebte seinen ersten großen Ransomware-Angriff am 21. September 2022. Es begann mit Anrufen von Benutzern, die sich nicht einloggen oder auf ihre Dateien zugreifen konnten. Nach einigen Nachforschungen entdeckte Vries eine Lösegeldforderung, die besagte, dass ihre Dateien verschlüsselt waren und eine Zahlung zur Entschlüsselung gefordert wurde.

„Die Ransomware verbreitete sich über das Domänenfeld und die Fabrik. Im Grunde war alles, was mit dem Active Directory verbunden war, kompromittiert", sagte Vries. „Wir mussten schnell handeln, um die Ausbreitung zu stoppen, da wir uns über das genaue Ausmaß der Auswirkungen nicht sicher waren."

Vries nahm sofort Kontakt mit dem Management und dem Cybersicherheitsteam von BBio auf, sowie mit KEMBIT, dem Managed Service Provider des Unternehmens, um die Situation zu analysieren und die nächsten Schritte zu bestimmen. Ihre erste Reaktion war, das Netzwerk zu trennen und die vom Angriff betroffenen Server und virtuellen Maschinen herunterzufahren, während nicht betroffene Maschinen eingeschaltet blieben, um die Auswirkungen auf den Impfstoffproduktionsprozess zu minimieren. Ein weiterer wichtiger Schritt war, die Mitarbeiter darüber zu informieren, was geschah, damit sie die Kritikalität der Situation verstanden.

Am zweiten Tag des Angriffs konnte Vries das Active Directory und die Commvault-Umgebung wieder online bringen. Nach dem Wiederaufbau von Commvault Cloud Backup & Recovery sagte Vries, dass es einfach und unkompliziert war, den Service wiederherzustellen.

„Wir lieben die Einfachheit des Commvault-Dashboards. Mit nur wenigen Klicks können wir eine virtuelle Maschine oder Backups nach einem Angriff wiederherstellen, was in unserer Branche als Pharmaunternehmen mit sehr sensiblen Daten von entscheidender Bedeutung ist", sagte Vries. „Commvault gibt uns das Vertrauen, dass unsere Daten sicher sind und unsere wichtigen Dienste schnell wieder laufen können."

Da Commvault so einfach zu bedienen war, konnte das Team abwechselnd die Dienste des Unternehmens über Nacht und bis zur vollständigen Wiederherstellung wiederherstellen. Dank der Partnerschaft zwischen dem IT-Team, KEMBIT und Commvault konnte BBio den Service in nur neun Tagen in mehreren Büros und seiner Fabrik vollständig wiederherstellen.

„Wenn wir Commvault nicht gehabt hätten und die Backups nicht vor dem Angriff gemacht worden wären, hätte die Situation viel schlimmer sein können", sagte Vries.

> **Commvault gibt uns das Vertrauen, dass unsere Daten sicher sind und unsere wichtigen Dienste schnell wieder einsatzbereit sein können."**
>
> **Paul Vries, IT Consultant**
> Bilthoven Biologicals

ERSTELLUNG EINES NOTFALL-WIEDERHERSTELLUNGSPLANS

Seit dem Ransomware-Vorfall hat BBio zusammen mit dem IT-Team wichtige Lektionen gelernt.

„Vor dem Angriff hatten wir keinen Wiederherstellungsplan", sagte Vries. „Wir arbeiten jetzt mit Commvault zusammen, um einen Notfall-Wiederherstellungsplan zu erstellen, damit wir besser verstehen, was zuerst und in welcher Reihenfolge wieder in Betrieb genommen werden muss."

Einige Dateien wurden während des Angriffs nicht verschlüsselt, weil BBio die Medienagenten außerhalb der Domäne verschoben hat. Mit dem Wechsel zu Microsoft 365 implementiert das Unternehmen auch Commvault Cloud Air Gap Protect zusammen mit Commvault Cloud Backup & Recovery, um die Backups für die hybride Umgebung weiter zu vereinfachen und den Schutz vor Ransomware zu verstärken.

„Mit Commvault und Commvault Cloud Air Gap Protect können wir Daten in der Cloud und on premise einfach verwalten, schützen und wiederherstellen, selbst im schlimmsten Fall", sagte Vries.

> Mit Commvault und Commvault Cloud Air Gap Protect können wir Daten in der Cloud und on premise einfach verwalten, schützen und wiederherstellen, selbst im schlimmsten Fall.“

Paul Vries, IT Consultant
Bilthoven Biologicals