Smart Backup Veeam

Was bewirkt die Sicherheitstechnologie Insider Protection for Veeam Cloud Connect?

Update 3 für Veeam Backup & Replication 9.5

Veeam hat mit Update 3 für Veeam Backup & Replication 9.5 eine neue Sicherheitstechnologie eingeführt: **Insider Protection for Veeam Cloud Connect.**

Warum wurde dieses Feature entwickelt?

Durch die Installation von sogenannter "Ransomware" auf Produktionsservern, versuchen Hacker alle Backup-Dateien von jeder Backup-Software zu löschen, die sie über die Benutzeroberfläche finden. Die meisten von ihnen wissen genau, worauf sie im Netzwerk achten müssen - viele geben in ihrem Austausch mit dem Opfer zu, dass sie gezielt nach Servern suchen, auf denen Veeam und andere bekannte Backup-Produkte laufen. Die Hacker verwenden ausgefeilte Netzwerkanalyse-Tools, um die Backup-Software im Netzwerk zu finden. Sie halten selten im Hauptrechenzentrum an, sondern suchen gezielt nach gespeicherten Cloud-Anmeldeinformationen, um die gesamten Backups mit all ihren Schnappschüssen und Repliken zu zerstören.

Welche Auswirkungen hat das Feature und wie können Sie davon profitieren?

An dieser Stelle greift die neue Sicherheitstechnologie. Sie ermöglicht, dass Ihre Daten bei uns nicht sofort gelöscht werden, sondern in den Papierkorb verschoben und somit vor dem Hackerangriff versteckt werden. Aus Kunden- und Hackeransicht sind die Daten vollständig gelöscht, der Angreifer nimmt also an, er habe sein Ziel erreicht. Somit haben wir eine Möglichkeit geschaffen, den Angreifer zu täuschen und Ihre Daten vor diesem Angriff zu schützen. Wenn Sie uns diese Verschiebung innerhalb von 7 Tagen melden, können wir Ihre Daten wieder in Ihr Veeam Cloud Connect Repository zurücksichern und Sie haben Ihre Daten auch nach einem "erfolgreichen" Angriff wieder im vollen Zugriff.

Wir haben die neue Sicherheitstechnologie bereits kostenlos für Sie aktiviert, sodass Sie dazu keine Veränderung Ihrer Einstellungen vornehmen müssen.

Ihr Hamburg-Cloud Team

Eindeutige ID: #1201