

Sophos-Integration mit Veeam

Schützen Sie kritische Backup-Daten aktiv vor Bedrohungen

Bei 75 % der Ransomware-Angriffe gelang es Bedrohungsakteuren im vergangenen Jahr, Sicherungsverzeichnisse zu beeinträchtigen¹. Sie manipulierten dazu Backups und löschten Daten, um eine Wiederherstellung zu verhindern. Sophos und Veeam vereinfachen den Schutz und stärken die Cyber-Resilienz: Sie tauschen nahtlos Sicherheitsdaten aus, wenn eine Bedrohung auftritt, die Ihre Backup-Daten gefährdet. Dies sorgt für mehr Transparenz bei der Bedrohungserkennung, -analyse und -reaktion.

Anwendungsfälle

1 | SCHUTZ VOR RANSOMWARE

Gewünschtes Ergebnis: Stärkster Schutz vor Ransomware-Angriffen.

Lösung: Sophos bietet branchenführende Technologie, die Ransomware erkennt und stoppt, bevor Ihre Systeme Schaden nehmen – auch neue Varianten sowie lokale und Remote-Verschlüsselungsangriffe. Dank der modernen Erkennungs- und Abwehrfunktionen von Sophos in Kombination mit unveränderlichen Backups und der Versionierung von Veeam bleiben Ihre Backup-Daten sicher und wiederherstellbar.

2 | MEHR EINBLICK IN DIE BEDROHUNGSLAGE

Gewünschtes Ergebnis: Potenzielle Bedrohungen erkennen, die Ihre Backup-Daten gefährden könnten.

Lösung: Die Integration von Sophos mit Veeam ist für den Sophos MDR (Managed Detection and Response) Service und die Lösung Sophos XDR (Extended Detection and Response) verfügbar. Sie bietet Einblick in schädliche Aktivitäten, die Ihre Backups gefährden, u. a. Versuche, Backup-Verzeichnisse zu löschen, die Multi-Faktor-Authentifizierung zu deaktivieren und Verschlüsselungspasswörter zu ändern.

3 | INTEGRITÄT UND VERFÜGBARKEIT VON BACKUPS

Gewünschtes Ergebnis: Verfügbarkeit und Schutz von Backup-Daten jederzeit sicherstellen.

Lösung: Mit unserer leistungsstarken Integration können Sie Bedrohungen erkennen, verdächtige Aktivitäten analysieren und Daten bei Bedarf schnell wiederherstellen, um für einen unterbrechungsfreien Geschäftsbetrieb zu sorgen. Mit Sophos und Veeam können Sie die Integrität und Verfügbarkeit Ihrer Backups sicherstellen und dabei das Risiko von Datenverlusten aufgrund von Malware, versehentlichem Löschen, internen Sicherheitsbedrohungen und anderen Datenverlust-Szenarien minimieren.

4 | SCHNELLERE REAKTION AUF BEDROHUNGEN

Gewünschtes Ergebnis: Ausfallzeiten minimieren und die Geschäftskontinuität gewährleisten.

Lösung: Sophos MDR ist ein von Experten bereitgestellter Service für 24/7 Threat Prevention, Detection and Response, der Unternehmen und Organisationen vor hochkomplexen Angriffen schützt. Sophos-Experten führen Threat Hunts durch, um Angreifertechniken zu identifizieren, bei denen versucht wird, Abwehrtools zu umgehen. Außerdem ergreifen sie Reaktionsmaßnahmen, um bestätigte Bedrohungen zu stoppen. Dabei reagieren die Sophos-Experten in durchschnittlich nur 38 Minuten – 96 % schneller als der Branchenstandard.



Die Gartner „Customers' Choice“-Wahl für Managed Detection and Response Services

Gartner

2023 zum dreizehnten Mal in Folge als ein Leader im Magic Quadrant for Endpoint Protection Platforms eingestuft

MITRE ATT&CK.

Ein führender Anbieter in der MITRE ATT&CK-Evaluation für Managed Security Services

Mehr erfahren:

www.sophos.de/mdr

www.sophos.de/xdr

¹Veeam Ransomware Trends Report 2023