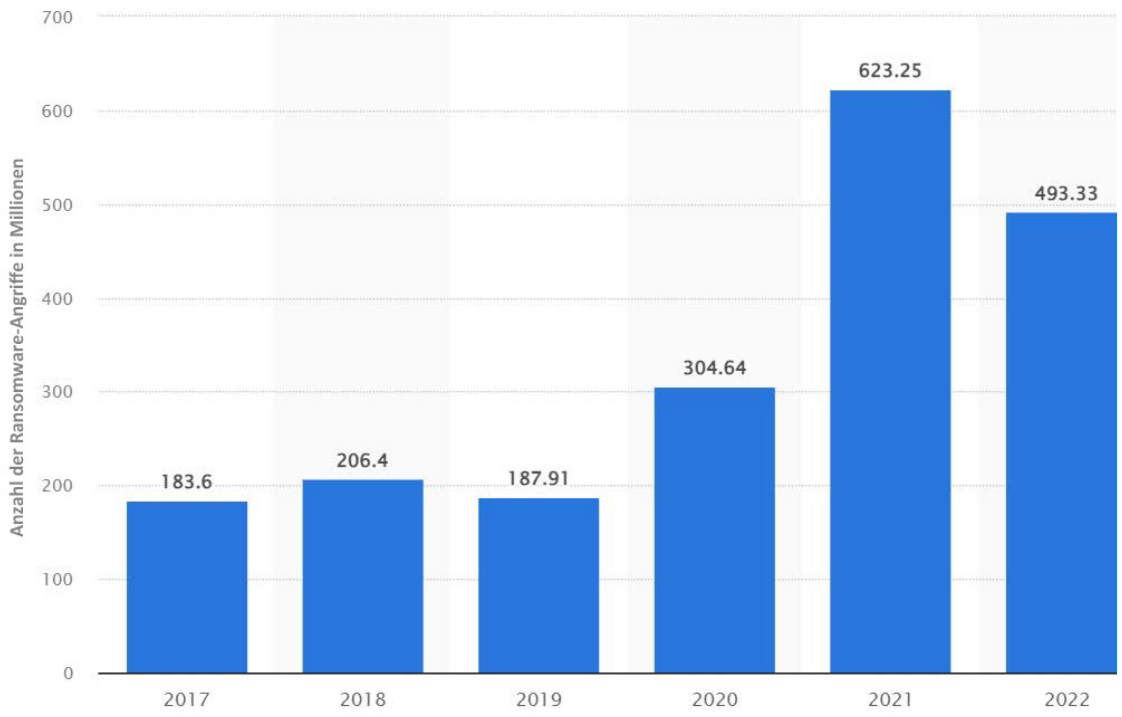
Wiederherstellung und Schutz vor Ransomware mit NetVault® Plus

Unternehmen und Non-Profit-Organisationen weltweit werden Tag für Tag Opfer von Ransomware-Angriffen und sehen sich im Zuge dessen mit enormen Beschädigungen und hohen Kosten konfrontiert. Gleichzeitig sollte man auch nicht die negativen Auswirkungen auf den Ruf der Marke sowie den Kundenservice außer Acht lassen. Zusammen genommen bedeutet jeder Ransomware-Angriff einen regelrechten Hurrikan.



Anzahl Ransomware-Angriffe gemäß Statista, 2022[1]

Obwohl die Anzahl der Ransomware-Angriffe im Jahr 2022 leicht abnahm, kam es dennoch zu rund 500 Millionen Angriffen weltweit. Aus dem IBM-Bericht „Cost of a Data Breach 2022“[2] geht hervor, dass sich das durchschnittliche Lösegeld für einen Angriff auf 812.360 USD beläuft. Das tatsächlich gezahlte Lösegeld macht jedoch nur einen kleinen Teil der Gesamtkosten eines Ransomware-Angriffs aus: Diese liegen laut IBM im Schnitt bei 4,5 Millionen USD. Zudem konnte IBM ermitteln, dass es im Vergleich zu anderen Cyberangriffarten in der Regel rund 49 Tage länger dauert, um Sicherheitsverletzungen aufgrund von Ransomware-Angriffen zu identifizieren und zu beheben.

Unternehmen benötigen eine Sicherungslösung, die zusätzliche Widerstandskraft beim Kampf gegen die Auswirkungen von Ransomware bietet. Quest® NetVault Plus bietet genau das. NetVault Plus ist eine umfassende Datenschutzlösung, die speziell für modernste Rechenzentrumsanwendungen und deren Infrastruktur sowie für Cloud-Lösungen wie Microsoft 365 entwickelt wurde. Zudem bietet es umfassende Schutz-, Wiederherstellungs- und Optimierungsfunktionen im Fall von Ransomware-Angriffen.

1 Statista
2 IBM

SCHÜTZEN

Um sich vor Ransomware-Angriffen zu schützen, ist ein mehrschichtiger Ansatz erforderlich. Gleichzeitig ist eine zuverlässige Sicherungs- und Wiederherstellungslösung Ihre letzte Verteidigungslinie gegen Angriffe, um das Geschäftsrisiko zu mindern.

Zunächst bietet NetVault Plus Sicherung und Wiederherstellung der Enterprise-Klasse, auf die Tausende Unternehmen weltweit zum Schutz ihrer Daten vertrauen. Mit diesem Tool ist es möglich, eine Vielzahl von Systemen, Anwendungen und Daten sowohl lokal als auch in der Cloud zu schützen. Gleichzeitig bietet NetVault Plus inkrementelle CDP (Continuous Data Protection; kontinuierlicher Datenschutz), mit der Sie dauerhaft den Schutz virtueller VMware-Machinen sicherstellen, das Risiko für Datenverluste und -beschädigungen mindern und für eine schnellere Sicherung sorgen können.

NetVault Plus umfasst eine softwarebasierte Speicherkomponente für Deduplizierung, Komprimierung, Verschlüsselung, Replikation und Cloud-Verbindungen. Diese Speichertechnologie basiert auf einem unveröffentlichten Protokoll namens Rapid Data Access (RDA), das die Sicherungsdaten schützt. Im Gegensatz zum SMB (Server Message Block), das für Windows-Freigaben verwendet wird, ist RDA kein offenes Protokoll. Es kann nicht direkt über ein Betriebssystem aufgerufen werden und erfordert eine Authentifizierung, die außerhalb des lokalen Servers bzw. des domänengesteuerten Konstrukts erfolgt. Darüber hinaus bietet NetVault Plus Datenverschlüsselungsfunktionen, damit Sie sich sicher sein können, dass Ihre Daten jederzeit geschützt sind – sowohl lokal als auch in der Cloud. Zudem können Sie mit dem nach FIPS 140-2 zertifizierten NetVault Crypto Module dafür sorgen, dass behördliche Datensicherheitsanforderungen eingehalten werden.

Des Weiteren verbessert NetVault Plus Ihren Schutz vor Ransomware: Sicherungsaufgaben können als „unveränderlich“ markiert werden, sodass Sicherungsdaten während der Sicherungsaufbewahrungsfrist nicht überschrieben, geändert, gelöscht oder verschlüsselt werden können – auch nicht durch einen NetVault Administrator.

Bei Verwendung von NetVault Plus werden die Sicherungsdatenflüsse direkt von der Quelle zum Ziel geleitet. Es sind keine herkömmlichen Medienserver erforderlich. Dadurch wird einerseits die Komplexität und andererseits das Risiko für Datenverluste reduziert, da weniger Kernkomponenten angegriffen werden können.

Darüber hinaus nutzt NetVault Plus eine Secure Connect-Technologie, mit deren Hilfe die Datenübertragung und Steuerbefehle in einem sicheren TLS 2.0 Layer verpackt werden. Dies ist ein wichtiger Schritt zur Beschränkung des Zugriffs auf Ihre Sicherungsdaten durch Ransomware.

Außerdem können Sie mit Netvault Plus Sicherungsdaten schnell und sicher replizieren, um eine 3-2-1-Sicherungsstrategie für die Notfallwiederherstellung zu entwickeln. Für zusätzlichen Schutz bietet NetVault Plus zudem auch eine Möglichkeit zur Air-Gap-Bandsicherung.

Natürlich hat das NetVault Plus System selbst ebenfalls Zugriff auf die Sicherungsdaten, also muss auch das berücksichtigt werden. Bisher waren von Ransomware-Angriffen überwiegend Windows-basierte Systeme betroffen – einerseits aufgrund der Beliebtheit des Systems, andererseits durch die Anzahl vorhandener Benutzer-Clients und Endpunkte, die Ransomware-Angreifer nutzen können. NetVault Plus verringert dieses Risiko durch die Installation unterstützender Systeme unter Linux. Auch wenn es damit nicht komplett unangreifbar ist, wird durch die Installation des NetVault Plus Systems unter Linux die Anzahl potenzieller Bedrohungen reduziert.

Auch die Systemzugriffserteilung sollte nicht außer Acht gelassen werden. NetVault Plus verfügt über zwei Hauptmethoden der Zugriffserteilung: Integration in einen Verzeichnisservice oder eigene rollenbasierte Zugriffsmechanismen. Angesichts des hohen Risikos, das mit den bereits erwähnten Angriffen auf Active Directory-Gruppenrichtlinien und GPOs (Group Policy Objects; Gruppenrichtlinienobjekte) einhergeht, sollten wir berücksichtigen, dass eine solche Sicherheitslücke den Zugriff auf die Sicherungsanwendung ermöglichen kann, wo es zu systematischen Datenlöschungen kommen könnte. Obwohl Sie Ihren Systemzugriff auch ganz einfach über Active Directory steuern können, bietet NetVault Plus ebenfalls zuverlässigen, rollenbasierten Zugriff – und das ganz ohne die Notwendigkeit, Active Directory zu nutzen. Auch wenn dies etwas weniger komfortabel für die Festlegung von Benutzern und Gruppen ist, wird dadurch eine stärkere Trennung von der Produktionsumgebung erreicht und damit auch potenzielle Zugriffe durch nicht autorisierte Dritte verhindert.

WIEDERHERSTELLEN

Dank NetVault Plus war Wiederherstellung noch nie schneller und einfacher. Administratoren finden schnell und einfach, was sie benötigen, um eine sofortige Wiederherstellung in die Wege zu leiten. Durch die Nutzung von NetVault Plus CDP für VMware profitieren Sie außerdem von Instant Restore, einer Funktion zur sofortigen Wiederherstellung einer virtuellen Maschine durch ein VM-Snapshot-Image, das direkt aus dem von NetVault Plus deduplizierten Sekundärspeicher-Repository installiert wird.

OPTIMIEREN

NetVault Plus umfasst leistungsstarke Automatisierungsfunktionen, mit deren Hilfe Datenschutz noch leichter gelingt und Ihre IT noch produktiver sein kann. Durch die quellseitige Datenduplizierung und -komprimierung lassen sich Sicherung und Wiederherstellung enorm beschleunigen, während gleichzeitig der erforderliche Speicherplatz reduziert und die Kosten um mehr als 90 % gesenkt werden können. Dabei ist die Deduplizierung von NetVault Plus weit mehr als „gewöhnlich“. Zunächst führt NetVault Plus bei sämtlichen Sicherungsprozessen eine Deduplizierung durch, um wirklich unternehmensweite Deduplizierung zu erreichen. Dabei verbindet es Deduplizierung mit variablen Blöcken mit einem inhaltssensitiven Algorithmus, der Muster innerhalb der Daten erkennt – auch wenn sich die Daten ständig verändern und gleichzeitig Daten im Datenstrom hinzugefügt oder gelöscht werden. Dies führt dazu, dass Sie nach abgeschlossener Deduplizierung von der bestmöglichen Speicherreduzierung profitieren, die es in der Branche gibt. Diese quellseitige Deduplizierung reduziert darüber hinaus die Datenmenge, die über das Netzwerk vom Clientrechner an den Speicher gesendet wird – und mindert so das von Datenerfassungstechnologien ausgehende Risiko.

Auch die Cloud-Tiering-Funktionen von NetVault Plus unterstützten Sie dabei, Ihre Sicherungsdaten zu optimieren, indem kürzlich durchgeführte Sicherungen lokal gespeichert werden, während ältere Sicherungen in die Cloud verschoben werden. Durch die Nutzung von Cloud-Speicher im Gegensatz zu lokalem Speicher lassen sich so enorme Kosteneinsparungen erreichen. Mit Cloud-Tiering nutzen Sie stets die neuesten Sicherungen von Ihren lokalen Laufwerken, um Ihre Daten noch schneller wiederherzustellen, während alle weiteren benötigten Daten aus der Cloud geladen werden.

WESENTLICHE VORTEILE

Letztendlich können sich selbst die am besten vorbereiteten Unternehmen nicht vollständig gegen Ransomware-Angriffe schützen. Sie können jedoch die Risiken minimieren, indem Sie eine Sicherungslösung verwenden, mit der Sie nicht nur alle Ihre Daten schnell wiederherstellen können, sondern die außerdem die folgenden Vorteile bietet:

- Minimierung der Risiken der Auswirkungen von Ransomware auf Ihr Unternehmen
- Reduzierung der Anzahl angreifbarer Kernkomponenten
- Minderung des von Datenerfassungstechnologien ausgehenden Risikos
- Zugriffsbeschränkung auf Sicherungsdaten für Ransomware

NetVault Plus bietet genau die Schutz-, Wiederherstellungs- und Optimierungsfunktionen, die anspruchsvolle IT-Manager und -Führungskräfte benötigen, um die Herausforderungen in der heutigen Bedrohungslandschaft erfolgreich zu bewältigen.

Weitere Informationen zu NetVault Plus finden Sie unter: www. quest.com/products/netvault-plus.

Über Quest

Quest stellt Softwarelösungen bereit, mit denen das volle Potenzial neuer Technologien in einer zunehmend komplexen IT-Landschaft ausgeschöpft werden kann. Von der Datenbank- und Systemverwaltung über die Migration zu und Verwaltung von Active Directory und Microsoft 365 bis hin zur Cyber Resilience: Quest hilft Kunden, bereits heute ihre IT-Herausforderungen von morgen zu bewältigen. Weltweit vertrauen mehr als 130.000 Unternehmen und 95 % der Fortune 500 Quest die proaktive Verwaltung und Überwachung der nächsten Unternehmensinitiative an. Quest soll außerdem die nächste Lösung für komplexe Microsoft-Herausforderungen finden, um für die nächste Bedrohung gewappnet zu sein. Quest Software. Where Next Meets Now. Weitere Informationen finden Sie auf www.quest.com.

Sollten Sie Fragen hinsichtlich der potenziellen Nutzung des Materials haben, wenden Sie sich bitte an:

www.quest.com/de-de/company/contact-us.aspx