WHITE PAPER

Ihre letzte Verteidigungslinie gegen Ransomware

Quantum®

INHALT

Ihre letzte Verteidigungslinie gegen Ransomware ist nicht die, an die Sie gerade denken 3
Wie gelangt Ransomware in Ihre Umgebung? 4
Wie schützen Sie Ihre Daten vor Ransomwareangriffen? 4
Schutz für Ihren Systemschutz 4
Bietet die Cloud einen wirksamen Schutz vor Ransomware? 5
Ist Tape die letzte Verteidigungslinie? 6
Über den 3-2-1-Ansatz von Quantum 6

IHRE LETZTE VERTEIDIGUNGSLINIE GEGEN RANSOMWARE IST NICHT DIE, AN DIE SIE JETZT DENKEN

Ransomware ist in aller Munde. Erpressungstrojaner wie CryptoLocker oder Locky wurden zuletzt in den Schatten gestellt von WannaCry„ einem der schlimmsten Ransomware-Angriffe" (Trend Micro), den die Welt bisher erlebt hat. Die WannaCry-Attacke begann am Freitag, den 12. Mai 2017, und infizierte innerhalb eines Tages über 230.000 Rechner in mehr als 150 Ländern, darunter auch die Systeme zahlreicher internationaler Großunternehmen. Der Autohersteller Renault-Nissan musste infolge des WannaCry-Angriffs den Produktionsbetrieb in fünf Werken einstellen. Auch die Computer Dutzender britischer Krankenhäuser und Gesundheitsdienstleister, der US-amerikanische Paketzusteller FedEx Corp. und der japanische Konzern Hitachi Ltd. waren betroffen.

Ransomware ist eine Malware, die Nutzern den Zugriff auf ihre eigenen Computersysteme verwehrt oder einschränkt. Entweder friert der Bildschirm ein oder die Dateien werden gesperrt bzw. verschlüsselt, bis ein „Lösegeld" (engl. „ransom") für den Entschlüsselungs-Key bezahlt wird – meist in Form von Bitcoins.

Die erste bekannte Ransomware wurde 1986 entwickelt, 2006 tauchten die ersten raffinierteren Methoden auf Basis des RSA-Kryptosystems auf. Seit 2015 nimmt die Anzahl dieser Angriffe weltweit alarmierend zu. Internetkriminelle nehmen nicht nur Einzelpersonen, sondern zunehmend auch Unternehmensnetzwerke ins Visier. Hat sich eine solche Schadsoftware erst einmal auf Ihren Rechnern eingenistet, kann sie unbemerkt Ihr gesamtes System infizieren.

Ein gutes Beispiel hierfür ist Locky. Die in C++ geschriebene und mit Microsoft Visual Studio kompilierte 100 KB-Malware installiert sich selbst auf Ihrem System und löscht alle Windows-Dateien, über die Sie sonst vor verdächtigen Downloads aus dem Internet gewarnt werden. Die Ransomware nimmt dann Kontakt mit einem zentralen Server auf, um die erfolgreiche Infizierung zu melden. Sie erhält einen RSA-2048-Verschlüsselungs-Key und eine Kennung für das befallene System und kann nun mit der Verschlüsselung des Computers oder Servers beginnen. An diesem Punkt senden die Angreifer ihre Lösegeldforderung, um die Attacke zu beenden. Mittlerweile sind zahlreiche Varianten oder Klone von Locky oder CryptoLocker im Umlauf, die zwar nicht direkt mit dem ursprünglichen Trojaner in Verbindung stehen, aber allesamt ähnlich vorgehen.

Auch bei WannaCry handelt es sich um eine Ransomware. Was sie jedoch weit gefährlicher macht als andere gängige Ransomware-Typen, ist die Tatsache, dass sie sich extrem schnell über den Microsoft Windows Server Message Block (SMB), eine Standardtechnologie von PCs für das File Sharing, verbreiten kann. Besonders anfällig sind Schulen, Universitäten, Unternehmen, Krankenhäuser und andere netzwerkorientierte Organisationen. Zudem scheint WannaCry auch Computer außerhalb des Unternehmensnetzwerks zu befallen.

Ransomware zielt jedoch längst nicht nur auf Windows-Systeme ab. Trojaner wie KeRanger oder Mabouia greifen Mac OS an, Linux.Encoder.1 oder FairWare haben sich auf Linux spezialisiert, und SynoLocker hat es auf NAS-Systeme abgesehen. Selbst Mobilgeräte und sogar Cloud-basierte Dienste für die Dateisynchronisierung bleiben nicht verschont. Erst vor kurzem wurden innerhalb von nur drei Wochen 30.000 Mobilgeräte mit der Ransomware-Variante ScareMeNot infiziert. Auch Windows-Volume Shadow Copy Services (VSS) oder Funktionen zur Systemwiederherstellung bieten keinen Schutz, da sie ebenfalls von der Ransomware deaktiviert werden können. Inzwischen konzentrieren sich Angreifer verstärkt auf Administratorkonten für Backups, um die Backups noch vor den Primärdaten zu verschlüsseln.

WIE GELANGT RANSOMWARE IN IHRE UMGEBUNG?

59 % aller Ransomware-Infizierungen sind auf E-Mails mit manipulierten Links und Anhängen zurückzuführen. Laut einer Umfrage von Osterman Research vom Juni 2016 ist die Wahrscheinlichkeit, durch Anklicken eines Links in einer E-Mail infiziert zu werden, mehr als doppelt so hoch wie ein Befall durch den direkten Besuch auf einer manipulierten Website. Zudem sagt fast jeder zweite Befragte aus, dass sein Unternehmen in den vorausgegangenen 12 Monaten von mindestens einer Ransomware-Attacke betroffen war. Nachdem Locky und andere neue Ransomware-Typen in Umlauf gekommen sind, meldete Symantec Ende 2016 rund 388.000 abgewehrte Angriffe pro Tag allein aus Exploit Kits.

Immer mehr Kriminelle haben diese Form der Malware als einfache Einnahmequelle erkannt und leisten damit der Entwicklung immer neuer Ransomware-Varianten Vorschub. Laut Trend Micro wurden allein in den ersten fünf Monaten des Jahres 2016 50 neue Ransomware-Familien ermittelt. Nach Schätzungen des FBI erzielen Internetkriminelle in diesem Jahr mit Ransomware Einnahmen in Höhe von 1 Mrd. US-Dollar. Da viele Betroffene die Attacken nicht melden, dürfte die tatsächliche Summe sogar noch höher liegen. Zu den besonders bekannten Fällen zählt das Hollywood Presbyterian Medical Center. Laut New York Post hat das Krankenhaus 17.000 US-Dollar an einen anonymen Hacker gezahlt, um sich von einer Cyberattacke freizukaufen.

Nicht zuletzt haben die Forscher von Invincea eine neue Ransomware-Variante entdeckt. Der Trojaner Cerber verschlüsselt nicht nur Dateien, sondern installiert auch ein Botnetz für die Durchführung von DDoS-Attacken (Distributed Denial of Service), die Online-Services durch Überflutung mit Traffic aus zahlreichen Quellen lahmlegen können. Das verdoppelt die Gefahr für die Betroffenen: Wird kein Lösegeld bezahlt, bleiben die Dateien verschlüsselt und das befallene System wird zudem als Teil eines Botnetzes für DDoS-Angriffe missbraucht – eine weitere lukrative Einnahmequelle für Internetkriminelle.

WIE SCHÜTZEN SIE IHRE DATEN VOR RANSOMWARE-ANGRIFFEN?

Schutz für Ihren Systemschutz

Angesichts der steigenden Anzahl an Ransomware-Attacken benötigen Sie eine Strategie, um Ihre Dateien vor diesen verheerenden Angriffen zu schützen. An erster Stelle steht dabei eine geeignete Datensicherungsstrategie. Ohne zweckmäßigen Backup-Plan halten Sie am besten gleich die Bitcoins zur Zahlung der Lösegeldsumme bereit. Natürlich wird von Zahlungen eigentlich abgeraten, da die Verbrecher ihre Versprechen, die Daten wieder zu entschlüsseln, nicht unbedingt einhalten. Dies musste laut Healthcare IT News im Mai 2016 auch das Kansas Heart Hospital erleben.

Da die Ransomware Ihre Dateien still und heimlich verschlüsselt, besteht die Gefahr, dass Ihr Backup-Programm die frisch verschlüsselten Versionen der Dateien sichert. Sie benötigen also ein Programm mit Versionsverwaltung. Das dürfte kein größeres Problem darstellen, denn die meisten IT-Experten halten ohnehin mehrere Backups vor, um Anwendungen oder einzelne Dateien in einen Zustand vor der Verschlüsselung zurückversetzen zu können. Selbst diese älteren Versionen sind aber nutzlos, wenn es der Ransomware gelingt, sämtliche Dateien auf Ihrem Backup-Ziel oder sogar in einem externen replizierten Archiv zu verschlüsseln. (Die Ransomware kann nämlich über das Netzwerk auch andere Rechner infizieren.) Solange ein Nutzer keinen Schreibzugriff auf das Verzeichnis der Backup-Dateien (NAS-Share oder Veeam Backup & Replication-Archiv) hat, können Trojaner, die im Sicherheitskontext dieses Nutzers operieren, die Backup-Dateien nicht verschlüsseln. Eine Studie von Barkly aus dem Jahr 2016

ergab, dass von den IT-Experten, die einen Ransomware-Angriff erleben mussten, nur 42 % in der Lage waren, alle Daten aus den Backups wiederherzustellen. Ein Grund lag darin, dass auch die Backups verschlüsselt wurden.

Als Best Practice empfiehlt es sich, darauf zu achten, dass Administratoren ihre Konten mit erweiterten Berechtigungen nicht durchgängig nutzen. Sie müssen für einen wirksamen Schutz der Schutzbeauftragten sorgen und Sorgfalt bei der Verwaltung der Backup-Administratorkonten walten lassen. Besonders versierte – und motivierte – Angreifer versuchen, über Social Engineering oder andere Methoden an Administratorberechtigungen zu gelangen und so Zugriff auf Backups zu erhalten. Als mahnendes Beispiel dient der Fall einer bedeutenden amerikanischen Universität, die kürzlich einem sorgfältig geplanten Angriff von Internetkriminellen zum Opfer fiel. Die entsprechende Kundenreferenz finden Sie hier www.quantum.com/fighting-ransomeware.

In diesem Zusammenhang hat sich vor allem die erprobte 3-2-1-Backup-Regel bewährt, nach der Sie mindestens drei vollständige Kopien Ihrer Daten anlegen sollten, von denen zwei auf lokalen (aber unterschiedlichen) Medien/Geräten vorgehalten werden und mindestens eine sich an einem externen Standort befindet. Dieses Verfahren ließe sich nun noch auf eine 3-2-1-0-Regel erweitern: 3 Kopien, 2 Medien, 1 externer Standort und mindestens eine Offline-Kopie mit 0 Echtzeit-Konnektivität. Das insgesamt eher als unsexy bewertete Backup gewinnt damit als erste Verteidigungslinie mehr und mehr an Attraktivität.

Bietet die Cloud wirksamen Schutz vor Ransomware?
Kleinere Betriebe und Privatanwender setzen als letzte Verteidigungslinie immer häufiger auf Cloud-basierte Backups. Die Vermutung liegt nahe, dass Cloud-Speicherdienste wie Dropbox, Google Drive oder andere Cloud-basierte Backup-Services einen wirksamen Schutz Ihrer Daten vor Ransomware-Angriffen bieten.

Cloud-basierte Backups sind immer verfügbar – das Hochladen der Dateien braucht jedoch seine Zeit. Dieses langsame Tempo kann ärgerlich sein, bildet jedoch eine zusätzliche Schutzebene. So würde es Tage oder sogar Wochen dauern, bis alle verschlüsselten Dateien in die Cloud gelangen. Durch Deduplizierung, Komprimierung oder Techniken zur Bandbreitenoptimierung gelingt es jedoch, den Zugriff auf die Cloud zu beschleunigen. Das Problem besteht darin, dass der Großteil Ihrer Dateien bei Änderungen sofort synchronisiert wird. Sollten also Ihre Dateien infolge einer Ransomware-Attacke verschlüsselt werden, werden sie in verschlüsselter Form hochgeladen. Und mit Cloud-basierten Kollaborations-Tools wie Office 365 OneDrive for Business oder Google Drive potenzieren sich die Folgen eines Ransomware-Angriffs.

Natürlich unterstützen einige Cloud-basierte Backup-Lösungen auch Versionsverwaltung. Der Teufel steckt jedoch im Detail: In den AGB eines führenden Public Cloud-Anbieters ist zu lesen, dass frühere Versionen nur Datei für Datei wiederhergestellt werden können. Den daraus resultierenden erheblichen Zeitbedarf für Restores müssen Sie bei Ihrer Backup-Strategie unbedingt berücksichtigen.

Hinzu kommt, dass Angreifer mittlerweile auch Cloud-Storage wie Dropbox anvisieren. Ohne es zu bemerken, laden Sie also vielleicht verschlüsselte Dateien herunter. Hacker benötigen inzwischen nicht einmal mehr Ihr Kennwort, um Zugriff auf Ihre Cloud-Daten zu erlangen. Stattdessen stehlen sie einfach Ihre Zugangsdaten und löschen oder verschlüsseln Ihre Cloud-Backups mit einem Angriff nach dem Man-in-the-Middle-Verfahren (das die Sicherheitsfirma Imperva jetzt als „Man in the Cloud“ bezeichnet).

Ist Tape die letzte Verteidigungslinie?
Durch Vorhaltung einer offline Kopie Ihrer Daten können Sie Ihre Backup-Strategie auf pragmatische Weise optimieren. Die letzte Verteidigungslinie muss immer ein Offline-Backup sein. Unter diesem Blickwinkel bietet Tape-Speicher die vielleicht größten Vorteile, denn er ist preisgünstig, mobil – und offline.

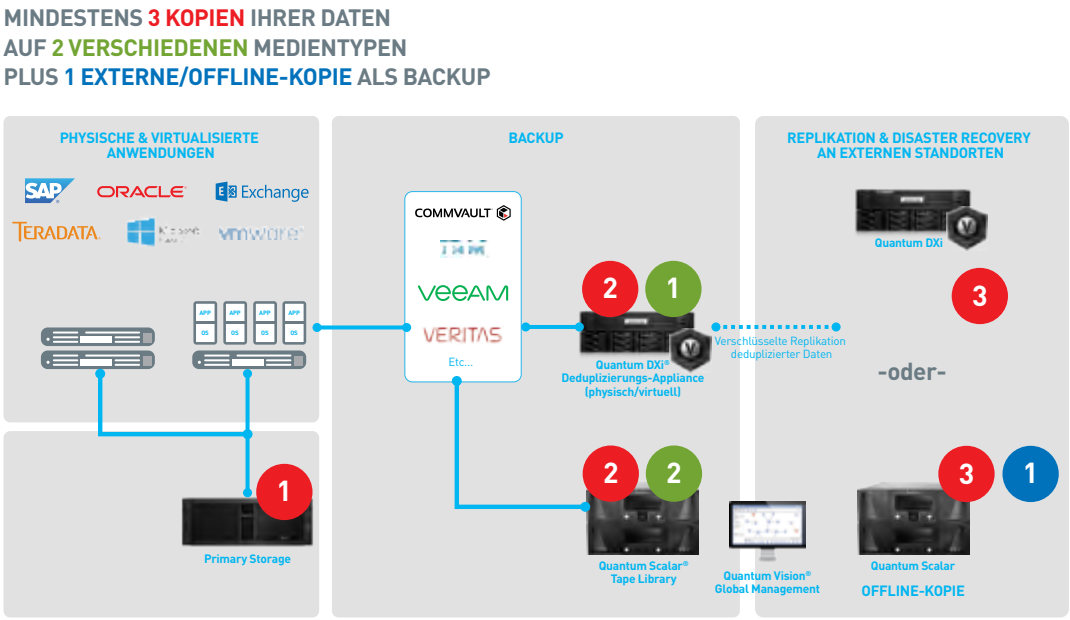
Mögliche Alternativen sind Replikationstechnologien und Speicher-Snapshots. Allerdings sind diese Modelle nicht vollständig offline, sondern sozusagen nur „zeitversetzt".

Tape ist Ihre letzte Verteidigungslinie – allein schon deshalb, weil Kriminelle keine Daten löschen oder verschlüsseln können, auf die sie nicht über das Netzwerk zugreifen können.

Voller Schutz gegen Ransomware ist nur möglich, wenn eine Infizierung von vornherein verhindert wird und regelmäßig Backups nach der 3-2-1-Methode erstellt werden, bei der die Kopien auf Offline-Medien wie etwa Tape repliziert und ausgelagert werden.

Wenn Sie einem Ransomware-Angriff zum Opfer gefallen sind, besuchen Sie die Website www.nomoreransom.org, um herauszufinden, ob es für den jeweiligen Typ von Ransomware bereits ein Entschlüsselungs-Tool gibt.

Über den 3-2-1-Ansatz von Quantum



Beispiel des 3-2-1-Ansatz von Quantum

Die einzigartigen mehrstufigen Speicherlösungen von Quantum gewährleisten maximale Verfügbarkeit und Performance Ihres Produktionssystems und tragen gleichzeitig zum Abbau von Speicherkosten bei. Das Kernstück unserer Lösung bildet die DXi-Deduplizierungs-Appliance. Die DXi ist als physische oder virtuelle Appliance erhältlich und sorgt dank patentierter Deduplizierungstechnologie mit Datenblöcken variabler Länge für höchste Datenreduktion und Einsparungen der Netzwerkbandbreite ohne Leistungseinbußen bei Backups und Restores. Die DXi®-Software ermöglicht schnelle Backups und bietet Unterstützung für fortschrittliche Features wie Commvault Continuous Data Replicator (CDR) oder Concurrent Optimized Duplication zur schnelleren Replikation für Nutzer von Veritas NetBackup. Darüber hinaus unterstützt die DXi-Software den Veeam Data Mover Service (VDMS) bei der Verwaltung von Vollsicherungen, inkrementellen Sicherungen und synthetischen Vollsicherungen. So stehen zusätzliche

Ressourcen für den Veeam Backup-Server, das Netzwerk und den Primärspeicher zur Verfügung. Gleichzeitig wird mit dem „Veeam-ready Repository", einer Appliance mit Deduplizierung auf der Basis variabler Blocklängen, die Datenreduktion maximiert. Damit profitieren unsere Kunden von schnellen Backups und Restores sowie einer schnellen Replikation und sichern sich alle Vorteile deduplizierter Backups.

- Die DXi kann Daten auf andere DXi-Appliances oder in die Cloud replizieren und auch auf Tape ablegen.
- Eine Offline-Backup-Kopie auf Tape stellt den wirksamsten Schutz Ihrer Daten vor Ransomware-Angriffen dar.
- Über einen Zeitraum von drei Jahren betrachtet sind die Speicherkosten pro Petabyte mit Tape acht mal geringer als mit Disk – und mit einer Funktionsdauer von 30 Jahren ist Tape auch das ideale Medium zur langfristigen Vorhaltung.

Quantum bietet einzigartige Möglichkeiten zur Tape-Speicherung für zahlreiche Backup-Anwendungen. Dazu zählen neben der Direct-to-Tape-Pfad Option in Veritas NetBackup-Umgebungen auch unsere neue konvergente Tape-Lösung für Veeam Umgebungen, die den Verzicht auf einen physischen Veeam Tape-Server erlauben.

In allen Fällen überzeugen die Quantum Scalar® Tape-Storage Lösungen durch die höchste Tape-Speicherdichte zu den geringsten Kosten sowie durch einfache Skalierbarkeit und proaktive Scalar iLayer™-Diagnosen zur leichteren Verwaltung.

Weitere Informationen erhalten Sie unter www.quantum.com/de oder telefonisch unter +49 (0) 89 94303-0.

Quantum®

ÜBER QUANTUM

Quantum ist ein führender Anbieter von spezialisierten Lösungen für Scale-out-Tiered-Storage, Archivierung und Datensicherung, die die Erfassung, gemeinsame Nutzung und Vorhaltung von digitalen Inhalten über den gesamten Datenlebenszyklus gewährleisten. Mehr als 100.000 Kunden – vom kleineren Unternehmen bis zum multinationalen Konzern – vertrauen auf Quantum, wenn es um die Herausforderungen selbst anspruchsvollster Daten-Workflows geht. Mit der mehrstufigen End-to-End-Speicherlösung von Quantum können sie die Wertschöpfung aus ihren Daten maximieren und Kosten sowie Komplexität reduzieren. Weitere Informationen erhalten Sie unter **www.quantum.com/de/customerstories**.

www.quantum.com/de • + 49 (0)89 94303-0

Quantum®

WP00221G-v03 Juni 2018