Ransomware-Schutz auf Zero-Trust-Basis durchsetzen

VMware NSX und VMware Ransomware Recovery

Der Status quo

Elf Sekunden.

Laut Schätzungen von Cybersecurity Ventures erfolgen Ransomware-Angriffe alle elf Sekunden[1] und verursachen weltweit Schäden in Milliardenhöhe. Bis 2031 findet voraussichtlich alle zwei Sekunden[2] ein Ransomware-Angriff statt. Darüber hinaus hat der eigene Threat-Intelligence-Service von VMware, Contexa, festgestellt, dass 44 % der Bedrohungen sich lateral ausbreiten, wodurch sich der Wirkungsradius des Angriffs vergrößert.

Um das Risiko von Ransomware zu minimieren, empfehlen Regierungsorganisationen wie die US-Behörde National Institute of Standards and Technology (NIST) die Implementierung eines robusten Schutzplans, der sowohl Maßnahmen zur Vorbeugung als auch zur Wiederherstellung vorsieht.

Die „neue Normalität“

Fakt ist, dass Ransomware-Angriffe zur neuen Normalität geworden sind.

Durch die Nutzung mehrerer Clouds vergrößert sich die Angriffsfläche eines Unternehmens und durch Inkonsistenzen beim Betriebsmodell steigt das Risiko von Cyberangriffen. Ransomware ist für viele Unternehmen zu einer existenziellen Bedrohung geworden und nutzt Schwachpunkte und Ineffizienzen vorhandener Schutzmechanismen aus, sowohl bei manuellen als auch bei automatisierten Abläufen. Nachdem Angreifer in ein Rechenzentrum eingedrungen sind, breiten sie sich lateral und dateilos über legitime Ports und Protokolle aus. Die Wiederherstellung nach einem Angriff ist langwierig und unplanbar, da die zahlreichen beteiligten Tools und Prozesse nicht automatisiert sind. Zur Abwehr von Ransomware benötigen Unternehmen einen Zero-Trust-Ansatz, der sowohl Vorbeugungs- als auch Wiederherstellungsmaßnahmen umfasst.

Ein Ransomware-Angriff erfolgt alle
11 Sekunden.[1]

44 %
der Bedrohungen breiten sich lateral aus.[3]

96 %
der Unternehmen, die Lösegeld gezahlt haben, haben den vollen Zugriff auf ihre Daten nicht wiedererlangt.[4]

Die durchschnittlichen Kosten eines Ransomware-Angriffs belaufen sich auf
4,62 Mio. USD.[5]

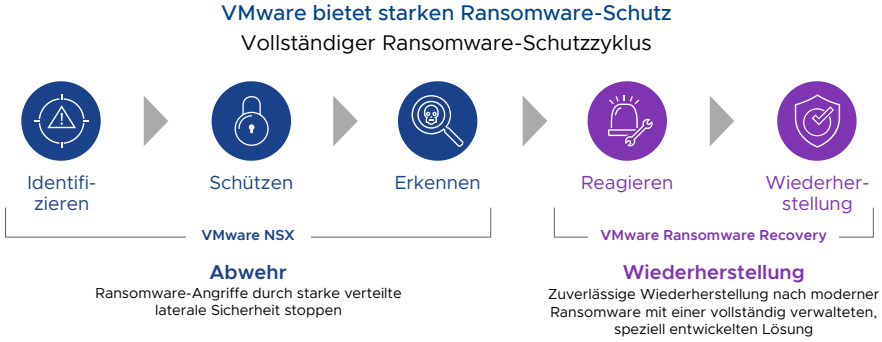

Abbildung 1: Ransomware-Schutzzyklus von VMware

Abwehr

Die Abwehr besteht aus Sicherheitskontrollen, die eine laterale Ausbreitung verhindern, Verhaltensanomalien erkennen und so Bedrohungen eindämmen.

Die inneren Abläufe von Anwendungen schützen

Bei einem Zero-Trust-Ansatz wird davon ausgegangen, dass Bedrohungen bereits in das Netzwerk eingedrungen sind. Es geht darum, gefährliche Angreifer ausfindig zu machen und abzuwehren, bevor sie ernsthaften Schaden anrichten können – auch diejenigen, die legitime Ports und Protokolle nutzen. Dazu ist es zunächst erforderlich, die grundlegenden inneren Abläufe der Anwendungen zu verstehen. Das setzt einen genauen Einblick in die Anwendungen und Datenflüsse sowie die damit verbundenen Services, Verbindungen und Datenmuster voraus. Und was das Ganze noch komplexer macht: Dies gilt sowohl für herkömmliche Anwendungen, die größtenteils virtualisiert werden, als auch für moderne, meist containerbasierte und verteilte Anwendungen.

Ein wichtiger Bestandteil der Zero-Trust-Sicherheit ist die Mikrosegmentierung. Damit können Sicherheitsbarrieren implementiert werden, die Angreifer davon abhalten, definierte Netzwerksegmente im Rechenzentrum zu durchqueren. Das ist eine wirkungsvolle Methode, um bösartigen Datenverkehr zu stoppen. Angreifer wissen ihre Aktivitäten jedoch zu verschleiern und haben Techniken entwickelt, um sich über vertrauenswürdige Prozesse, Protokolle und Softwaremodule ungehindert lateral auszubreiten. Diese Bewegungen scheinen wie legitimer Traffic. Sie nutzen gängige Services wie Samba, RDP und PowerShell oder im Netzwerk gestohlene Kennwörter („Pass-the-Hash“). Ohne zusätzlichen Kontext und Threat-Intelligence-Mechanismen ist es so nicht leicht, zwischen Freund und Feind zu unterscheiden.

Ein genauer Einblick ist ein Muss

Um Bedrohungen im virtualisierten Rechenzentrum erkennen zu können, muss die Umgebung für die Sicherheitskontrollen transparent sein. In diesen Umgebungen durchquert der Datenverkehr von einer virtuellen Maschine (VM) zu einer anderen möglicherweise nicht das physische Netzwerk. Deshalb sind herkömmliche hardwarebasierte Firewalls oder Netzwerk-TAPs, die von Inline-Traffic oder Hairpinning ausgehen, bei virtualisierten Netzwerken schlicht unpraktisch. Sie erfordern mit Unterbrechungen verbundene Änderungen der Netzwerkkonfiguration. Außerdem sind die erfassten Daten unvollständig. Herkömmliche appliancebasierte Netzwerk-TAPs erfassen nur die Daten, die die Appliance durchlaufen. Das lässt den Traffic zwischen VMs völlig außer Acht. Daher weisen die heutigen leistungsstarken Server mit Kapazitäten für Hunderte von VMs potenziell zahlreiche Schwachpunkte auf, die Angreifer ausnutzen können, um sich unbemerkt lateral zu bewegen.

Einblick in alle Verbindungen und Datenaustausche

Wer gefährliche Angreifer ausfindig machen und abwehren will, muss einen genauen Einblick in seine Umgebung haben. Wenn die auf dem physischen Netzwerk basierenden Sicherheits- und Transparenzkontrollen bei virtualisiertem Netzwerkdatenverkehr nicht greifen, wird die Virtualisierungsebene selbst zum wichtigsten Tool für Sicherheitsexperten.

Die Sicherheitsmechanismen von VMware NSX® greifen genau hier. NSX erfasst, welche Verbindungen hergestellt und welche Aktionen bei diesen Verbindungen ausgeführt werden. Die Transparenz reicht dabei bis zu dem Prozess, der den Datenverkehr ausgelöst hat, selbst wenn er verschlüsselt ist. Dadurch werden sehr präzise Daten erfasst und jede Verbindung kann mit der verteilten IDS-/IPS-Lösung von VMware NSX auf signaturbasierte Bedrohungen geprüft werden. Und was noch wichtiger ist: VMware bietet eine softwarebasierte NDR- und NTA-Lösung sowie die einzige Netzwerk-Sandbox der Branche mit vollständiger Emulation. Mithilfe des grundlegenden Kontexts werden Anomalien erkannt, hinter denen ein Angriff stecken könnte. So können Bedrohungen erkannt werden, selbst wenn sie sich hinter vertrauenswürdigen Systemen und zulässigen Protokollen verbergen. Diese Funktionen, die als Lösung zur erweiterten Cyberabwehr bereitgestellt werden, haben als erste und einzige Lösung von SE Labs eine AAA-Zertifizierung für Netzwerkerkennung und -reaktion erhalten.

Dieselben Prinzipien gelten für moderne Anwendungen und Workloads, jedoch mit anderen Einbindungsmechanismen. Moderne Architekturen bestehen aus Microservices und APIs und können Hunderte oder sogar Tausende Endpunkte umfassen, die untereinander Daten austauschen. Wie auch bei herkömmlichen virtualisierten Umgebungen gelingt die Abwehr sich lateral ausbreitender Bedrohungen nur mit einem entsprechenden Einblick in diese Services und zugehörigen APIs. Und wie beim Hypervisor-Layer in virtualisierten Umgebungen bietet VMware sowohl Transparenz als auch Steuerelemente für moderne Anwendungsumgebungen. Mit dem Service-Mesh von VMware können IT-Teams APIs überwachen und analysieren und erhalten so einen genauen Einblick in ihre Schemas, Datenflüsse und Baselines des normalen Datenverkehrs. Wenn ein gefährlicher Angreifer versucht, einen Angriff zu verbreiten, beispielsweise eine anomale Datenabfrage, erkennt VMware-Security die Bedrohung und verweist den Angreifer aus dem Netzwerk.

Workloads sind in VMware Clouds sicherer

Für effektive laterale Sicherheit sind die richtigen Kontrollen zum Schutz von Multi-Cloud-Umgebungen erforderlich. Dazu gehören softwarebasierte Lösungen, um Workloads direkt zu schützen, ein genauer Einblick in die inneren Abläufe von Anwendungen sowie vollständige Automatisierung für einheitliches Management und einheitliche Richtlinien. Mit VMware Clouds können Sie hocheffektive laterale Sicherheitsmechanismen sowohl auf herkömmliche als auch auf moderne Anwendungsumgebungen anwenden – mit präziser Bedrohungserkennung und ohne Schwachpunkte im Netzwerk. Und durch die Bereitstellung und das Management in einem Cloud-Betriebsmodell erzielen Sie bessere Ergebnisse dank vollständiger Automatisierung und Konsistenz.

Wiederherstellung

Profitieren Sie nach einem Angriff durch moderne Ransomware von zuverlässiger Wiederherstellung als zusätzliche Schutzebene zur Zero-Trust-Sicherheit, falls unbefugte Operationen durchgehen.

VMware ermöglicht die Wiederherstellung nach moderner Ransomware

VMware Ransomware Recovery ist eine vollständig verwaltete Ransomware-Recovery-as-a-Service-Lösung für eine sichere Wiederherstellung nach moderner Ransomware. Damit wird das Verhalten aktiver Workloads in einer isolierten Wiederherstellungsumgebung (Isolated Recovery Environment, IRE) in der Cloud analysiert. Dank angeleiteter Workflow-Automatisierung können Sie mögliche Wiederherstellungspunkte schnell erkennen, mithilfe einer Live-Verhaltensanalyse validieren und eine Reinfektion durch Funktionen zur Netzwerkisolierung vermeiden.

Bei Disaster-Recovery- und Backup-Lösungen müssen Unternehmen heute darauf achten, dass sie Abwehrmechanismen gegen die Risiken moderner Ransomware bieten. Bei einem Angriff muss davon ausgegangen werden, dass die primären Datensätze und Backup-Kopien bereits infiziert wurden. Das heißt, Unternehmen müssen die Möglichkeit haben, ihre Backups schnell zu testen und die nicht infizierten zu finden, um eine saubere Wiederherstellung durchführen zu können.

VMware Ransomware Recovery bietet eine zuverlässige und agile Wiederherstellung nach moderner Ransomware. Unternehmen profitieren von einem dedizierten Workflow für die Wiederherstellung nach Ransomware mit nahtlos integrierten Automatisierungsfunktionen, darunter eine verwaltete IRE, um die Reinfektion von Produktions-Workloads zu vermeiden, die angeleitete Auswahl von Wiederherstellungspunkten sowie eingebetteten Virenschutz der nächsten Generation mit Verhaltensanalyse von aktiven Workloads.

Als Grundlage dienen die umfassenden Basisfunktionen, die VMware Cloud Disaster Recovery bereits für eine schnelle Wiederherstellung nach Ransomware bietet, etwa unveränderliche VM-Snapshots, tägliche Prüfungen der Datenintegrität, Wiederherstellung auf Datei-/Ordnerebene sowie Instant Power-On von VMs für die schnelle Iteration von Wiederherstellungspunkten.

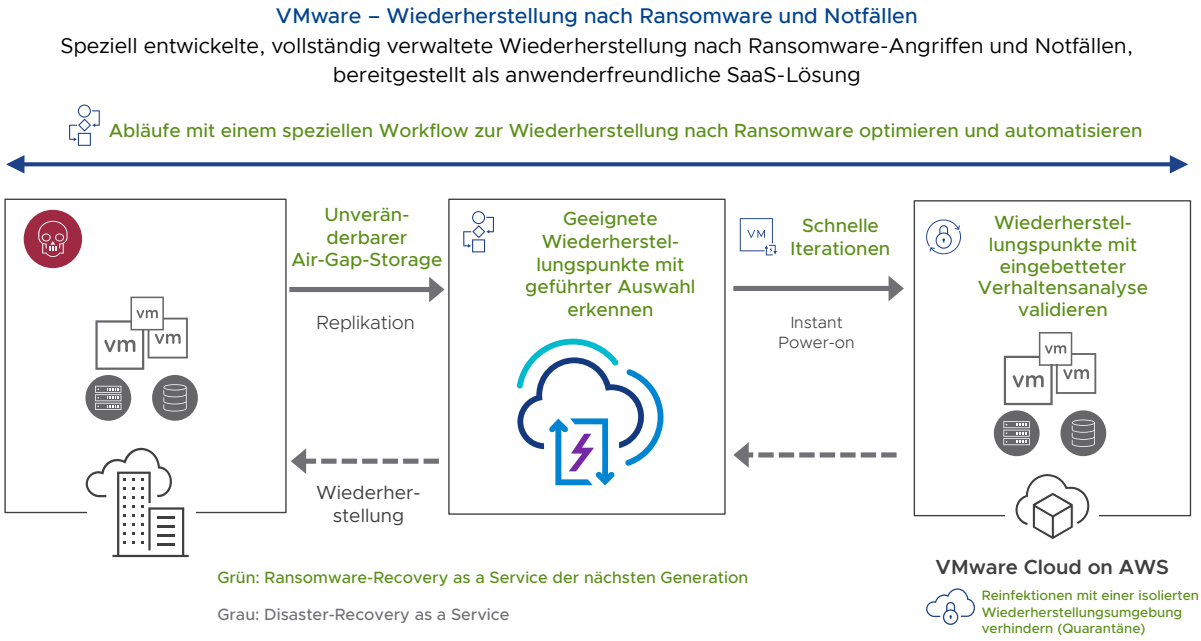

Abbildung 2: VMware – Wiederherstellung nach Ransomware und Notfällen

Zuverlässige Wiederherstellung nach existenziellen Bedrohungen

Mit den umfassenden Funktionen von VMware Ransomware Recovery können Sie eine IRE direkt über die Produkt-UI bereitstellen. Diese IRE wird von VMware verwaltet. So müssen Anwender ihre Wiederherstellungsumgebung nicht selbst erstellen, schützen und verwalten, die Wiederherstellung ist einfacher und der Aufwand für die IT ist erheblich geringer.

Für eine zuverlässige Validierung möglicher Wiederherstellungspunkte und die Identifizierung von Formen moderner Ransomware bietet VMware Ransomware Recovery die Live-Verhaltensanalyse aktiver Workloads in der Cloud. Das ist besonders effektiv bei der Erkennung von dateilosen Techniken, die heute den Großteil der Angriffsvektoren ausmachen.

Um die laterale Ausbreitung von Ransomware in der Wiederherstellungsumgebung zu verhindern, bietet VMware Ransomware Recovery integrierte Networking-Funktionen, mit denen Sie VMs per Knopfdruck voneinander isolieren können.

Schnelle Wiederherstellung dank angeleiteter Automatisierung

Mit dem dedizierten speziellen Workflow zur Wiederherstellung nach Ransomware, der direkt über die SaaS-Konsole verfügbar ist, werden Sie durch den gesamten Wiederherstellungsprozess geleitet. Dabei werden Wiederherstellungspunkte automatisch identifiziert, validiert und wiederhergestellt. Durch diesen angeleiteten Workflow wird der Wiederherstellungsprozess vereinfacht und automatisiert. So werden in einer Situation, die schon schwierig genug ist, fehleranfällige manuelle Abläufe ersetzt.

Zur Identifizierung geeigneter Wiederherstellungspunkte werden verschiedene Informationen zur Verfügung gestellt, beispielsweise die VMDK-Änderungsrate und Dateientropie sowie die Snapshot-Zeitachse.

Dank VM-Netzwerkisolation auf Knopfdruck in mehreren Stufen müssen Firewallregeln und Richtlinien nicht mehr manuell konfiguriert werden und die Wiederherstellung wird beschleunigt.

Durch die schnelle Iteration von Wiederherstellungspunkten können Sie in einem Prozess, der mehrere Backup-Kopien durchläuft, rasch saubere Wiederherstellungspunkte und Daten finden.

Die Lösung ermöglicht eine schnelle Wiederherstellung, da keine Daten vom Cloud-Storage kopiert und auf VMware Cloud on AWS-Hosts aktiviert werden müssen (Instant Power-On durch Live-Mount von NFS- auf SDDC-Cluster). Instant Power-On ist ein leistungsstarkes Tool, mit dem Sie einfacher identifizieren können, welche Snapshots kompromittiert und welche Wiederherstellungspunkte geeignet sind.

Vereinfachte Wiederherstellungsabläufe

VMware Ransomware Recovery verbindet Verfügbarkeits-, Sicherheits- und Networking-Funktionen in einer Lösung zur zuverlässigen und schnellen Wiederherstellung nach moderner Ransomware.

Sie müssen sich nicht mit neuen Betriebsabläufen oder Tools vertraut machen. Sowohl die Produktionsstandorte als auch die Standorte zur Wiederherstellung nach Ransomware werden in einer vertrauten VMware-Umgebung verwaltet.

Die Lösung umfasst eine SaaS-basierte Managementkonsole. Diese vereinfacht die Wiederherstellungsabläufe nach Ransomware und Kunden müssen sich nicht mehr um das Software-Lebenszyklusmanagement kümmern. Sie können sich einfach durch den angeleiteten Workflow klicken, in dem automatisierte Wiederherstellungsabläufe nahtlos integriert sind.

Nachdem Wiederherstellungspunkte identifiziert und validiert wurden, unterstützt die Lösung die effiziente und orchestrierte deltabasierte Wiederherstellung von VMware Cloud on AWS am ursprünglichen Produktionsstandort.

VMware NSX und VMware Ransomware Recovery

Einheitliche Sicherheit und Resilienz durch Automatisierung

Die Instrumentierung von VMs und Containern hat sich mit der Cloud radikal verändert. Im „Cloud-Betriebsmodell“ können neue Workloads und die zugrunde liegenden Infrastrukturen einschließlich Switching, Routing und Lastausgleich dank Automatisierung und Effizienz per Knopfdruck bereitgestellt werden. Sicherheit muss ebenso Teil dieses Modells sein, sodass sowohl herkömmliche als auch moderne Anwendungen einheitlich geschützt sind.

VMware bietet bessere und konsistentere Sicherheit für das Cloud-Betriebsmodell. Dasselbe Modell wird für die Automatisierung von verteiltem Firewalling (für Segmentierung und Mikrosegmentierung), IDS/IPS, NDR, NTA sowie für das Netzwerk-Sandboxing zur erweiterten Cyberabwehr verwendet. Diese Sicherheitskomponenten sind in vorhandene Automatisierungsprozesse integrierbar und werden für neue Anwendungen als Software in einer Architektur mit horizontaler Skalierung angewendet. In Multi-Cloud-Umgebungen bietet das Cloud-Betriebsmodell optimale betriebliche Effizienz und bessere Sicherheit – ohne Support durch das SecOps-Team und ohne weitere Hardware-Appliances. Ein zusätzlicher Vorteil des Modells besteht darin, dass das Rechenzentrum vollständig intakt zu einem anderen Anbieter portiert werden kann, einschließlich Sicherheitskontrollen und -richtlinien.

VMware unterstützt auch die automatisierte Wiederherstellung nach moderner Ransomware mithilfe von angeleiteten Workflows, eingebundenen Auditberichten und täglichen Prüfungen der Datenintegrität. Unsere Lösung schützt sowohl on-premises ausgeführte Workloads als auch Cloud-Umgebungen. Letztere werden als Greenfield-Recovery-Standorte genutzt, um VM-Snapshots sicher zu iterieren und die Reinfektion von Produktionsstandorten zu vermeiden.

Ransomware-Schutz auf Zero-Trust-Basis durchsetzen

Worst-Case-Szenarien einzuplanen ist ein wichtiger Bestandteil jeder Multi-Cloud-Strategie. Stoppen Sie Ransomware-Angriffe – auch diejenigen, die legitime oder verschlüsselte Kanäle nutzen – mit starker verteilter lateraler Sicherheit, einschließlich Mikrosegmentierung und KI-/ML-gestützter NDR-Lösung für einen unternehmensweiten Einblick in die Umgebung sowie cloudübergreifend einheitlicher Richtlinien.

Und wenn doch einmal ein Angriff durchkommt, profitieren Sie von einer zuverlässigen Wiederherstellung mit einer vollständig verwalteten Lösung speziell für diesen Zweck. Wiederherstellungspunkte werden identifiziert, bereinigt und validiert und während des Wiederherstellungsprozesses wird dank Live-Verhaltensanalysen und IREs in der Cloud eine Reinfektion vermieden.

Außerdem unterstützen VMware Professional Services Sie gern bei der Erstellung und Implementierung einer umfassenden Strategie für Ransomware-Schutz und Wiederherstellung, die an Ihre speziellen Anforderungen angepasst ist.

Jetzt loslegen

Setzen Sie mit einem einzigen Technologiestack Ransomware-Schutz auf Zero-Trust-Basis durch und profitieren Sie von folgenden Vorteilen: starke verteilte laterale Sicherheit, speziell entwickelte Wiederherstellung nach Ransomware, attraktive TCO/Wirtschaftlichkeit und cloudübergreifende Konsistenz – ohne proprietäre Appliances, ohne Tickets zur Bereitstellung von Workloads, aber mit Zero-Trust.

VMware NSX Distributed Firewall

Ransomware Defense PoV on TestDrive

VMware Ransomware Recovery

VMware Cloud Disaster Recovery

1. Cybersecurity Ventures: „Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) by 2021“, Steve Morgan, 21. Oktober 2019
2. Cybersecurity Ventures: „Ransomware Will Strike Every 2 Seconds By 2031“, Steve Morgan, 3. Januar 2023
3. VMware Contexa
4. Sophos-Studie „The State of Ransomware 2022“
5. IBM, „Kosten eines Datenschutzverstoßes 2022“