Arbeitsteilung bei der Workload-Sicherheit

Vorgänge für Sicherheitsteams und IT-Administratoren operationalisieren und vereinfachen

vmware®

Inhaltsverzeichnis

Einführung

Sicherheitsteams brauchen die Hilfe des IT-Betriebs beim Schutz von Workloads

IT-Administratoren und Sicherheitsteams spielen beide eine Rolle bei der Gewährleistung der Sicherheit von Systemen, sind jedoch relativ isoliert voneinander. Die Umstellung auf Cloud-Umgebungen für Anwendungen und Workloads erzwingt eine Änderung der Art und Weise, wie diese Rollen ausgeführt werden.

Sicherheitsteams eines Unternehmens bestehen in der Regel aus Richtlinien- und Auditgruppen sowie aus Teams für die Bedrohungsbekämpfung und die Reaktion auf Vorfälle. Die tägliche Last der Sicherheit und Compliance fällt den IT-Betriebsmitarbeitern und Ressourcen zu, die nicht unbedingt sicherheitsorientiert sind. Laut einem Spotlight-Report von Forrester Consulting haben heute nur 33 Prozent der Unternehmen ein einheitliches Team für IT und Sicherheit, aber 47 Prozent glauben, dass die Vereinheitlichung in drei bis fünf Jahren die Norm sein wird.[1] Es gibt keinen besseren Zeitpunkt für einen neuen Ansatz, der den Zusammenhalt zwischen diesen Teams fördert.

Dieses White Paper behandelt die wichtigsten Konstrukte, mit denen sowohl Sicherheits- als auch IT-Teams die Angriffsfläche proaktiv reduzieren und Ressourcen härten können. Durch Einführung dieser Konstrukte wird die Kluft zwischen diesen Teams überbrückt, der Betrieb vereinfacht und die Workload-Sicherheit eine gemeinsame Aufgabe.

KERNKONSTRUKT	BESCHREIBUNG
Minimierung des Agent-Einsatzes	Müssen keine Agents auf Workloads installiert werden, wird der Wildwuchs an Sicherheits-Agents reduziert. Installationen und Neustarts werden minimiert und die Betriebskosten verringert. Dies vereinfacht die Bereitstellung von Sicherheit als Service für die IT.
Gemeinsamer Einblick in Schwachstellen	Eine einheitliche Ansicht der Sicherheitsdaten gewährleistet eine klare Kommunikation und ein klares Verständnis hinsichtlich der erkannten Schwachstellen.
Automatisierung der Risikopriorisierung	Um Alarmmüdigkeit vorzubeugen und überlastete Ressourcen zu minimieren, müssen beide Teams wissen, worauf sie sich konzentrieren müssen, um die größte Abwehrwirkung zu erzielen. Ein kontextbezogenes System, das Schwachstellen automatisch und unvoreingenommen priorisieren kann, ist entscheidend.
Optimierung von Workload-Prozessen	Dank teamübergreifender Transparenz und Risikopriorisierung profitieren sowohl Sicherheits- als auch IT-Teams von einer reibungslosen Erfahrung durch Automatisierung und Operationalisierung konsistenter Sicherheit als Teil der IT-Hygiene.

TABELLE 1: Vier Kernkonstrukte zur Reduzierung der Angriffsfläche und Härtung von Ressourcen

1. Forrester Consulting, von VMware in Auftrag gegeben, „Security As A Team Sport: A Spotlight On The Growing Role Of IT In Security Tasks", Mai 2020.

Die Herausforderung

Workloads sind zu einer offensichtlichen Schwachstelle geworden

Workloads werden zunehmend verteilt, da unsere Umgebungen immer umfangreicher und komplexer werden. Viele Cloud-basierte Anwendungen sind geschäftskritisch, aber anfällig für Sicherheitsverstöße, wenn ein Teil des Workload (Anwendung, Daten oder Betriebssystem) nicht ordnungsgemäß funktioniert. Natürlich besteht die Lösung nicht darin, einen Unternehmensserver herunterzufahren, wenn ein Vorfall eintritt. Sicherheit und IT-Betrieb sind der Geschäftsproduktivität untergeordnet. Das bedeutet, dass Schutz und Überwachung jedes Teils des Workload jetzt ein zusätzlicher – und wichtiger – Faktor beim Schutz Ihres Unternehmens sind.

Wer ist für den Workload-Schutz verantwortlich?
Als Workloads noch in statischen Rack-Servern in On-Premises-Rechenzentren untergebracht waren, war es einfach, die Verantwortung für ihre Sicherheit zu übertragen. Heutzutage können Workloads auf physischen Servern, virtuellen Servern, in der Public Cloud oder sogar serverlos existieren. Außerdem können Workloads über all diese Umgebungen hinweg verschoben werden, wodurch es schwierig ist, sie zu verfolgen und zu verwalten. Sicherheit, IT-Administratoren, Cloud-Administratoren, VMware vCenter®-Administratoren, Site Reliability Engineers (SRE), DevOps und Entwickler können alle eine Rolle im Workload-Lebenszyklus spielen. Manchmal werden beim Umgang mit Workloads gemeinsame Ziele erreicht, zu anderen Zeiten können sich die Ziele der verschiedenen Parteien jedoch widersprechen.

IT-Administratoren können Workloads effizient schützen. Sie erkennen die meisten Workload-Schwachstellen jedoch nicht und verfügen definitiv nicht über den Kontext, um die Auswirkungen zu priorisieren. Da IT-Administratoren oft keine Kontrolle über die Cloud-Umgebung haben, werden die Rollen und Verantwortlichkeiten schwammig. Sicherheitsteams verfügen möglicherweise über einige der Informationen, die zur Identifizierung von Schwachstellen erforderlich sind, haben aber möglicherweise keine klare Risikopriorisierung oder keinen Kontext, um die Remediation effektiv zu verwalten.

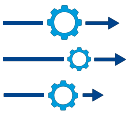
Mit anderen Worten: Die Workload-Sicherheit wird wahrscheinlich von niemandem ausreichend verwaltet.

Kann die Verantwortung geteilt werden?
Die Quintessenz ist, dass sowohl Sicherheitsteams als auch IT-Administratoren eine Rolle bei der Workload-Sicherheit spielen müssen. Um Schuldzuweisungen zu vermeiden, müssen beide Teams hinsichtlich der für Workloads spezifischen Prozesse, Informationen und Tools auf dem gleichen Stand sein.

Mit einem gemeinsamen Verständnis und einer Methodik zur automatischen Erkennung und Priorisierung von Schwachstellenkorrekturen wird es für IT-Administratoren viel einfacher, die Verantwortung für die Härtung und Reduzierung von Angriffsflächen zu teilen. Die Workload-Sicherheit kann operationalisiert werden, um Spannungen und Schuldzuweisungen zwischen diesen beiden kritischen Teams zu beseitigen. Es sind lediglich vier wichtige Schritte erforderlich, um dies Realität werden zu lassen.

SCHLÜSSELDATEN, DIE ZWISCHEN SICHERHEITSTEAMS UND IT-ADMINISTRATOREN AUSGETAUSCHT WERDEN SOLLTEN

- Indicators of Compromise (IOC)
- Taktiken, Techniken und Verfahren (TTP)
- Informationen zu blockierten und erkannten Angriffen
- Gewöhnliche Ereignisse, die im System auftreten
- Auswertung von mehr als 2.000 Workload-Konfigurationszuständen
- Bestandsaufnahme von Workloads und deren Schutzstatus
- Scanloser Schwachstellenkontext mit Risikobewertungen und Links zur National Vulnerability Database
- Verfolgung und Trends der IT-Hygiene im Zeitverlauf



Vier Schritte zum Operationalisieren und Vereinfachen der Workload-Sicherheit

Schritt 1: Minimierung des Agent-Einsatzes

Der Wildwuchs an aufgesetzten Sicherheits-Agents verursacht sowohl für IT-Administratoren als auch für Sicherheitsteams viele Probleme. Zu den gängigsten Herausforderungen zählen:

- Unterschiedliche Quellen für Sicherheitsinformationen verschlechtern die Kommunikation
- Erhöhter Wartungsaufwand und höhere Fehleranfälligkeit
- Zusätzliche Storage-Kosten für gesammelte Daten

Um diese Probleme zu beseitigen, sollten Sie die IT- und Sicherheits-Stacks konsolidieren, indem Sie mehrere Punktlösungen durch einen ganzheitlichen Sicherheitsansatz ersetzen – einen, der Daten über On-Premises- und Cloud-Umgebungen hinweg sammeln kann.

Wahl eines einzigen integrierten Agent

Die optimale Lösung besteht darin, einen einzelnen Agent im Virtualisierungs-Layer, der in Ihre bestehende Infrastruktur integriert ist, zu verwenden. So können die Ereignisse registriert werden, die für vollständige Transparenz in allen Umgebungen erforderlich sind. Mit einem einzigen Agent kommt die Sicherheitsüberwachung so nah wie möglich an einen minimalen Fußabdruck heran.

Große Vorteile durch einen Agent

Die Konsolidierung von Sicherheitslösungen auf einen Agent – eine einzige, umfassende Datenquelle – trägt entscheidend zur Verbesserung der Workload-Sicherheit bei:

- Erleichtert die Operationalisierung des Agent-Managements für die IT
- Lässt die Integration von Workflows und die gemeinsame Nutzung von Daten in verschiedenen Teams zu
- Liefert kontextbezogene Informationen und führt zu besser umsetzbaren Ergebnissen
- Macht Point-in-Time-Prüfungen auf Schwachstellen überflüssig, wodurch die Performance verbessert und die Reaktionszeit bei Angriffen verkürzt wird
- Verringert Storage-Kosten und Wartungsaufwand

Schritt 2: Gemeinsamer Einblick in Schwachstellen

Selten ist die Gruppe, die für das Patchen verantwortlich ist, auch die Gruppe, die sich mit den Sicherheitsauswirkungen von Schwachstellen beschäftigt. Klassische Scannerdaten sind schnell nicht mehr synchron und die Ticketing-Systeme sind langsam, was zu unterschiedlichen Interpretationen der erforderlichen Korrekturen führt.

IT-Administratoren nutzen Datenquellen, die von denen, die das Sicherheitsteam verwendet, getrennt sind. Es wird jedoch erwartet, dass auch sie zu umfassenderen Sicherheitsprozessen Informationen beitragen. Dies führt zu Missverständnissen und schlechten Hygieneergebnissen.

Eine einheitliche Ansicht der Sicherheitsdaten gewährleistet eine klare Kommunikation und ein klares Verständnis der erkannten Schwachstellen und der damit verbundenen Risikostufe.

Eine einheitliche Ansicht für effektive Risikoreduzierung

Die Konsolidierung auf einen einzigen Agent in Schritt 1 erzeugt Sicherheitsdaten, die leicht zwischen IT-Administratoren und Sicherheitsteams ausgetauscht werden können. Idealerweise sollten diese Informationen in den Tools dargestellt werden, die diese Teams täglich verwenden, wie Virtualisierungstools (z.B. VMware vSphere® und vCenter).

Wenn alle Teams dieselben Daten und Auswertungsergebnisse haben, wird die Kommunikation und Zusammenarbeit verbessert. Der wichtigste Punkt ist, immer aktuelle Schwachstellendaten zur Hand zu haben, anstatt eine Point-in-Time-Prüfung durchführen zu müssen. So wird sichergestellt, dass die Teams immer auf dem gleichen Stand sind. Eine gemeinsame Bestandsaufnahme der Workload-Schwachstellen, die nach Risiko geordnet ist, stellt sicher, dass Ressourcen auf die Lösung der kritischsten Probleme ausgerichtet werden.

Schritt 3: Automatisierung der Risikopriorisierung

Die Verwendung eines einzigen Agent und die umfassende Transparenz der Sicherheitsdaten verbessern das Management der Workload-Sicherheit erheblich. Der Zugang zu bekannten Schwachstellen allein bedeutet jedoch noch nicht, dass es ein gemeinsames Verständnis darüber gibt, wo die Ressourcen zu konzentrieren sind.

Der nächste logische Schritt ist eine standardisierte Methode für das Risiko-Assessment. Ziehen Sie eine Sicherheitslösung in Betracht, die Assessment und Priorisierung von Risiken automatisch durchführt.

Risikopriorisierte Daten innerhalb aktueller Tools für umsetzbare Ergebnisse
Ein Risiko-Assessment, das allein auf dem Common Vulnerability Scoring System basiert, ist nicht ausreichend. Kontextdaten, die aus benutzerdefinierten Bedrohungsdatensätzen kuratiert werden – einschließlich Exploit- und Threat Intelligence-Feeds und mehr als 7 Milliarden verwalteter Schwachstellen – geben Unternehmen die Möglichkeit, prädiktive Modelle anzuwenden, um neue Schwachstellen zu prognostizieren und Remediation-Aktivitäten auf der Grundlage des Kritikalitätsgrads zu priorisieren.

Idealerweise sollten IT-Administratoren innerhalb ihrer vCenter-Konsole einen Überblick über die häufigsten Exploits und Schwachstellen, die ein hohes Risiko darstellen, haben. Damit lässt sich die Workload-Härtung leicht in die täglichen Hygienemaßnahmen integrieren.

Außerdem benötigen IT-Administratoren Auditinformationen über den aktuellen Systemzustand, damit sie gemeinsam mit Sicherheitsteams an der Beseitigung von Bedrohungen arbeiten können. Mit einer gemeinsamen Ansicht dieser Informationen können diese Teams zusammenarbeiten, um Patches nach Priorität anzuwenden oder alternative Maßnahmen zu ergreifen, wie z.B. das Herunterfahren anfälliger Systeme.

Eine gemeinsame Sicht auf aktuelle Bedrohungen und Schwachstellen sowie die damit verbundenen Risiken erlaubt eine klare Priorisierung und Fokussierung der Bemühungen. Dies führt zu einer schnelleren Beseitigung bestehender Bedrohungen und einem besseren Schutz vor zukünftigen Angriffen.

Schritt 4: Optimierung von Workload-Prozessen

Prüfungen auf Schwachstellen wurden in der Vergangenheit monatlich oder vierteljährlich durchgeführt. Diese Point-in-Time-Aktionen sind jedoch nicht ausreichend. Mit der kontinuierlichen Ausweitung von Workloads in Multi-Cloud-Umgebungen liefern diese Prüfungen nicht so umfassende und zeitnahe Informationen, wie sie für die Minimierung kritischer Sicherheitsrisiken erforderlich sind.

Nach teamübergreifender Transparenz und Risikopriorisierung besteht der nächste Schritt für Sicherheits- und IT-Teams darin, Workload-Sicherheit zu einem regelmäßigen Bestandteil der IT-Hygiene zu machen.

Operationalisierung der Workload-Sicherheit
Die Operationalisierung der Workload-Sicherheit erfordert von IT-Administratoren, die Angriffsflächen als Teil der Standard-IT-Hygienepraktiken kontinuierlich zu reduzieren. IT-Administratoren müssen auf Auswertungen von Tausenden von Konfigurationszuständen ihrer Workloads zugreifen können und die Informationen und Anweisungen zur Beseitigung entdeckter Schwachstellen erhalten.

Das IT-Management sollte Zugriff auf eine gemeinsame Ansicht der IT-Hygienetrends im Zeitverlauf haben. Dadurch werden Diskussionen im Team über das Management von Schwachstellen und Performance-Messung gefördert. IT-Manager sollten mithilfe dieser Informationen sicherstellen, dass Prioritäten befolgt und Ressourcen entsprechend zugewiesen werden, um Workloads kontinuierlich zu härten.

Nächste Schritte

Weniger Angriffe durch Ausrichtung der IT auf Workload-Sicherheit

Sicherheitsteams und IT-Administratoren können gemeinsam an der Verbesserung der Workload-Sicherheit arbeiten. Mit den richtigen Sicherheitsfunktionen kann diese Zusammenarbeit einfach und mühelos in der täglichen Praxis umgesetzt werden. Um diese Chance zu nutzen, sollten Sie sicherstellen, dass diese Teams:

- Eine integrierte Lösung mit einem einzigen Agent verwenden
- Über eine einheitliche Ansicht der Sicherheitsdaten verfügen, die in ihre aktuellen Arbeitstools eingebettet sind
- Über den notwendigen Kontext und die kontinuierliche Überwachung auf Schwachstellen mit automatischer Risikopriorisierung verfügen
- Von Führungskräften unterstützt werden, um die Operationalisierung der Workload-Härtung sicherzustellen

Drei Schlüssel zur Verbesserung der Workload-Sicherheit

1. Bringen Sie IT-Administratoren und Sicherheitsverantwortliche zusammen, um eine mögliche Zusammenarbeit zur Reduzierung von Angriffen zu diskutieren.
2. Identifizieren Sie aktuelle Lücken in der Datenerfassung und -transparenz, um Schwachstellen besser priorisieren und Workloads härten zu können.
3. Erkunden Sie Lösungen, die IT-Administratoren und Sicherheitsteams teamübergreifende Transparenz und den nötigen Kontext bieten, um erfolgreich zu sein.

Höhere Workload-Sicherheit bringt große Vorteile mit sich

- Abdeckung und Transparenz über alle Workloads hinweg
- Vereinfachung des IT-Sicherheits-Stack
- Die Fähigkeit, durch Früherkennung schneller auf Probleme zu reagieren
- Besser gehärtete Ressourcen
- Bessere Verhinderung von Malware sowie unerwünschter Software und unerwünschten Prozessen
- Vollständige Beseitigung von Nicht-Malware
- Verbesserung der Sicherheit für die Zukunft – moderne Umgebungen und Workloads

Weitere Informationen

In diesem Datenblatt erfahren Sie, wie VMware Carbon Black Cloud™ IT und Sicherheit dabei unterstützt, die Workload-Sicherheit gemeinsam zu verbessern.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Zweigniederlassung Deutschland Willy-Brandt-Platz 2 81829 München Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de