PRISMA
BY PALO ALTO NETWORKS

Mehr Sicherheit überall

Unverzichtbare Voraussetzungen für eine sichere Migration in die Cloud.

Die Cloud ist heute eine ganz normale Technologie. Schätzungen von Gartner zufolge wird der Gesamtwert des Cloud-Markts von 182,4 Milliarden US-Dollar im Jahr 2018 auf 331,2 Milliarden US-Dollar im Jahr 2022 ansteigen. Das entspricht einer jährlichen Wachstumsrate (CAGR) von 16,1 %.[1] Angesichts der nahezu unmittelbar spürbaren Vorteile überrascht das auch nicht: Durch die Cloud-Nutzung profitieren Unternehmen von allen wichtigen Voraussetzungen für ein langfristig erfolgreiches Geschäft, von der raschen Innovation über neue, schnelle Routen zum Markt bis hin zu effektiven Möglichkeiten, neue Kunden zu finden, zu bedienen und zu halten.

Doch trotz der immer schneller zunehmenden Cloud-Nutzung äußerten Sicherheitsexperten im Jahr 2018 verstärkt Bedenken rund um die Cybersicherheit. Bei einer Umfrage im Mai 2019 beschrieben sich neun von zehn Sicherheitsexperten als „über die Cloud-Sicherheit besorgt" – 11 % mehr als im Vorjahr.[2] Welche Schlussfolgerungen sollten Vorstandsmitglieder und andere Führungskräfte aus den zunehmenden Bedenken der Cybersicherheitsprofis ziehen?

> *„Im Moment werden Anwendungen und Workloads in geradezu fieberhafter Eile in die Cloud verlagert. Die entscheidende Frage ist: Wer wird davon profitieren und wer wird auf der Strecke bleiben?"*
>
> – 451 Research[3]

Die Cloud ist inzwischen fest als strategische Geschäftsinitiative etabliert und gilt in vielen Unternehmen als nächste Entwicklungsetappe. Das ändert jedoch nichts an der aktuellen Situation: Moderne Unternehmen sind weit verteilt. Ihre Benutzer greifen von überall und mit den verschiedensten Geräten auf Tools und Informationen zu, und ihre Daten und Anwendungen werden in verschiedensten Cloud-Umgebungen gehostet, unter anderem in IaaS-, PaaS- und SaaS-Lösungen (Infrastruktur, Plattform und Software as a Service) in privaten und öffentlichen Clouds.

Die Migration in die Cloud führt zu Unsicherheit und diese Unsicherheit führt zu Verzögerungen bei der Migration. Ein wichtiger Grund hierfür ist, dass die Verantwortlichen in Unternehmen mit der Migration in die Cloud Neuland betreten. Sie fühlen sich weniger sicher, alles im Griff zu haben. Der tatsächliche Verlust an Transparenz und Kontrolle verstärkt dieses Gefühl. Gleichzeitig wird die Unternehmensinfrastruktur durch die Cloud-Nutzung wesentlich komplexer. All das führt zu neuen Geschäftsrisiken und ineffizienten Prozessen.

Die herkömmlichen Ansätze für die Cloud-Sicherheit reichen nicht aus

Bei der Migration in die Cloud stehen zahlreiche Sicherheitsoptionen zur Auswahl, doch viele sind nur dazu gedacht, einen kleinen Teil der Herausforderungen in puncto Sicherheit zu bewältigen. Durch den Erwerb und Einsatz mehrerer Punktlösungen zum Schutz verschiedener Cloud-Umgebungen (öffentliche und private Clouds, SaaS-Umgebungen usw.) wird die Infrastruktur noch komplexer. Im schlimmsten Fall verschlingen die neuen Lösungen zudem das durch die Migration eingesparte Geld.

Deshalb empfehlen wir einen holistischen Ansatz für die Cloud-Sicherheit, bei dem die Zugriffskontrollen, die Datensicherheit und die Bedrohungsverhinderung und -abwehr für alle Cloud-Umgebungen und Infrastrukturen konsistent sind. Kernaspekte dieses Ansatzes sind einfaches Management und eine einfache Architektur. Dadurch werden der große Administrationsaufwand, die zahlreichen Bedienfehler und Fehlkonfigurationen und andere Probleme vermieden, die oft durch den Einsatz nicht miteinander verknüpfter Punktlösungen entstehen.

> *Gartner zufolge wird das Versagen der Cloud-Sicherheit bis Ende 2023 in mindestens 99 % der Fälle durch die Kunden verschuldet sein.[4]*

1. „Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019", Gartner, 2. April 2019, https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g.
2. „2018 Cloud Security Report", Cybersecurity Insiders, abgerufen am 22. Mai 2019, https://start.paloaltonetworks.com/cloud-security-report-2018.
3. „2019 Trends in Cloud Transformation", 451 Research, abgerufen am 22. Mai 2019, http://go.451research.com/2019-Cloud-Trends-Preview.html.
4. „Innovation Insight for Cloud Security Posture Management", Gartner, 25. Januar 2019, https://start.paloaltonetworks.com/innovation-insight-for-cloud-security-posture-management.html.

Ein holistischer Sicherheitsansatz – das fehlende Puzzleteil

Eine vor Kurzem von ESG durchgeführte Umfrage hat gezeigt, dass die Entscheidungsträger vieler Unternehmen die Anzahl der genutzten Anbieter und Technologien gern reduzieren würden. Weshalb? Die engere Verknüpfung der genutzten Lösungen hat eine ganze Reihe von Vorteilen für die Sicherheit.

Die drei wichtigsten Vorteile der Konsolidierung von Cybersicherheitsprodukten und -services auf Angebote eines Anbieters[5]		
44 % Effektivere Sicherheitsmaßnahmen	**34 %** Verstärkte Automatisierung von Prozessen	**34 %** Effizienterer Betrieb

Abbildung 1: Umfrageergebnisse von ESG

> *„36 % der Unternehmen nutzen zwischen 24 und 49 verschiedene Sicherheitsprodukte. 19 % nutzen sogar über 50 unterschiedliche Produkte von diversen Anbietern.“*
>
> – ESG[6]

Derzeit drängen sich über 1.000 Verkäufer auf dem Markt für Sicherheitstechnologien, darunter viele Spezialanbieter für eine Art von Sicherheitsfunktionen. Viele Kundenunternehmen suchen jedoch aktiv nach Produkt-Suites, mit denen sie solche Punktlösungen ersetzen und zu einem holistischen Sicherheitsansatz übergehen können. Infolgedessen zeichnet sich eine Verlagerung der Marktanteile zugunsten von Anbietern der Enterprise-Klasse mit einem breit gefächerten Produkt- und Serviceportfolio ab.

Innovation fördert die Komplexität

Verschiedene Unternehmen sind unterschiedlich weit mit der digitalen Transformation, doch unabhängig von der aktuellen Etappe spielt die Cloud eine wichtige Rolle bei der Neuausrichtung. Unternehmen können die Cloud nutzen, um etwaige Lücken zwischen ihren derzeitigen Fähigkeiten und zukünftigen Kundenerwartungen zu schließen. Die Skalierbarkeit, Flexibilität, Anpassungsfähigkeit und schnelle Weiterentwicklung von Cloud-Umgebungen fördern die Innovation. Für viele Unternehmen ist die Cloud-Nutzung auch eine Chance für einen Neuanfang mit einer strafferen und insgesamt weniger komplexen Infrastruktur.

Doch die Migration in die Cloud verläuft nicht in allen Unternehmen gleich, und Entscheidungsträgern stehen viele verschiedene Optionen zur Auswahl. Die daraus resultierende Komplexität ist der Sicherheit abträglich. Um unnötige Komplexität zu vermeiden und die Cloud erfolgreich zu nutzen, müssen Unternehmen auf Sicherheitstechnologien bestehen, die sich schnell und effektiv skalieren und an neue kommerzielle Anforderungen anpassen lassen.

> *„Heutzutage ergibt sich der Mehrwert der Cloud aus der Zuverlässigkeit und Stabilität von Cloud-Umgebungen und daraus, dass dort Dinge möglich sind, die Unternehmen sonst nirgendwo tun könnten.“*
>
> – 451 Research[7]

Prisma von Palo Alto Networks

Palo Alto Networks Prisma™ ist das branchenweit umfassendste Angebot zur Bewältigung der aktuellen und zukünftigen Anforderungen rund um die Cloud-Sicherheit. Neben der für Cloud-Plattformen typischen Schnelligkeit und Flexibilität bietet Prisma einen beispiellosen Überblick über Daten, Ressourcen und Risiken sowie kompromisslose Zugriffskontrollen für Daten und Anwendungen. Gleichzeitig reduziert es durch seine radikal einfache Architektur die Komplexität und die Kosten.

Prisma sorgt für Sicherheit bei der Migration in die Cloud, unabhängig davon, wie Ihr Unternehmen diese angeht:

- **Sicherer Zugang:** Zweigstellen und mobile Benutzer in aller Welt profitieren von sicherem Zugang zur Cloud, ohne Beeinträchtigung der Benutzererfahrung.
- **Sichere SaaS-Lösungen:** Prisma vereint Datensicherheit, Governance und Compliance für die sichere Nutzung von SaaS-Angeboten.
- **Sichere Nutzung öffentlicher Clouds:** Kontinuierliches Sicherheitsmonitoring, Compliance-Prüfungen und ein sicherer Cloud-Speicher unterstützen die sichere Nutzung von Multicloud-Umgebungen. Diese Funktionen werden durch effektive, auf umfassende Bedrohungs- und Kontextdaten gestützte Maßnahmen zur Bedrohungsprävention und -abwehr ergänzt.

5. „Toward Enterprise-class Security“, ESG, Mai 2019.

6. Ebd.

7. „What's on the Minds of Cloud-Focused CTOs in 2018?“ 451 Research, abgerufen am 22. Mai 2019, http://go.451research.com/what-is-on-mind-of-cloud-focused-CTOs.html.

Darüber hinaus enthält Prisma Komponenten für spezifische Anwendungsbereiche, mit denen Sie bei jeder Etappe der Migration in die Cloud optimale Ergebnisse erzielen können.

Starke Sicherheit während der gesamten Migration	
Anwendungsbereich	**Ergebnis mit Prisma**
Cloud-Zugriff für mobile Mitarbeiter	VPN für den Fernzugriff wurden nicht für Cloud-Anwendungen entwickelt. Auch bei Proxys, sicheren Web-Gateways und DNS-Filtern waren lückenloser Schutz und eine hervorragende Benutzererfahrung nicht die wichtigsten Designziele. *Doch Ihre mobilen Mitarbeiter benötigen unterbrechungsfreien, sicheren Cloud-Zugriff, unabhängig davon, wo in der Welt sie sich befinden. Prisma Access (früher GlobalProtect™ Cloud Service) bietet cloudbasierten Schutz für den sicheren Zugriff auf Cloud-Umgebungen.*
Cloud-Anbindung für Zweigstellen	Wenn Ihr Unternehmen die Cloud intensiv nutzt, müssen Sie vermutlich die Netzwerkstrategie für die Anbindung der Zweigstellen überarbeiten. Achten Sie dabei darauf, dass auch die Sicherheitsstrategie an die neuen Bedingungen angepasst werden kann. *Prisma Access schützt Zweigstellen und Ladengeschäfte mit cloudbasierten Sicherheitsmaßnahmen, wo immer diese benötigt werden.*
Cloud-Sicherheit nach dem „Zero Trust"-Prinzip	Wenn Sie Ihre Anwendungen in die Cloud verlagern, können Sie sich nicht länger auf herkömmliche Maßnahmen für die Netzwerksicherheit verlassen. Das bedeutet jedoch nicht, dass Sie die Kontrolle aus der Hand geben müssen. *Mit Prisma Access bekommen Sie Ihre Cloud-Umgebungen unter Kontrolle. Wenden Sie das „Zero Trust"-Prinzip für den sicheren Zugriff auf öffentliche und private Clouds und SaaS-Anwendungen an.*
Cloud-Governance und -Compliance	Mit der zunehmenden Nutzung von Cloud-Services wird die Erfüllung der Compliance-Anforderungen immer schwieriger. *Prisma überwacht Ihre verteilten Multicloud-Umgebungen und SaaS-Anwendungen pausenlos, weist Sie proaktiv auf alle Fehlkonfigurationen und Compliance-Verstöße hin und behebt diese automatisch, sodass Sie die Cloud ohne Bedenken nutzen können.*
Datensicherheit in der Cloud	Die Daten eines modernen Unternehmens sind typischerweise auf verschiedene Cloud-Umgebungen und SaaS-Anwendungen verteilt, die ein unterschiedliches Maß an Transparenz und Kontrolle bieten. Dadurch lässt sich kaum genau ermitteln, wie groß das Risiko eines Angriffs, Datendiebstahls oder eines versehentlich verursachten Datenverstoßes ist. *Prisma enthält Tools für die automatische Erkennung, Klassifizierung, Überwachung und Sicherung von Daten und die proaktive Verhinderung von Datenlecks.*
Schutz vor Bedrohungen in der Cloud	Voneinander isolierte Sicherheitsmaßnahmen verfügen nicht über die erforderlichen Kontextinformationen, um komplexe Bedrohungen zu erkennen. Stattdessen tragen sie mit ihren zahlreichen Benachrichtigungen zur Warnungsmüdigkeit der Sicherheitsteams bei. *Prisma vereinfacht den Betrieb der Sicherheitsinfrastruktur und bietet ununterbrochenen, effektiven Schutz vor Bedrohungen, der auf umfassenden Kontextdaten basiert.*
Sicherung der DevOps-Prozesse	Die Integration von Sicherheitsmaßnahmen in einem möglichst frühen Stadium der Softwareentwicklung erfordert, dass diese Maßnahmen automatisierbar und API-basiert sind. *Prisma stellt offene Sicherheits-APIs und automatisierte Sicherheitsmaßnahmen zur Verfügung, die Sie in Ihre CI- und CD-Zyklen integrieren können.*

Die digitale Transformation ist ein Balanceakt für die Führungsriege. Ob die Cloud genutzt werden sollte oder nicht steht vermutlich nicht mehr zur Debatte. Doch viele Fragen rund um das wie, was und mit wem müssen noch beantwortet werden. Gleichzeitig muss die Führungsriege ihren Beitrag zur Sicherung der digitalen Transformation leisten. Bei richtiger Planung kann die Migration in die Cloud Geschäftsbereichen, die normalerweise nicht viel miteinander zu tun haben, ein gemeinsames Ziel geben und sie enger zusammenbringen. Dabei spielt das Sicherheitsteam eine zentrale Rolle. Sicherheitsteams galten für lange Zeit als Hindernis für die Innovation, können heute aber ein strategischer Partner für die Geschäftsbereiche sein und sie bei der Implementierung wichtiger Funktionen unterstützen. Mit einer Cloud-orientierten Denkweise und der richtigen Suite integrierter Sicherheitsmaßnahmen können sie Ihrem Unternehmen helfen, ohne Sicherheitsbedenken von der Cloud zu profitieren.

Weitere Informationen finden Sie im **Prisma Resource Center**.

PRISMA™
BY PALO ALTO NETWORKS

Oval Tower, De Entrée 99 -197
1101HE Amsterdam
Niederlande
Telefon: +31 20 888 1883
www.paloaltonetworks.de

© 2019 Palo Alto Networks, Inc. Palo Alto Networks ist eine eingetragene Marke von Palo Alto Networks. Eine Liste unserer Marken ist unter https://www.paloaltonetworks.com/company/trademarks.html verfügbar. Alle anderen hier erwähnten Marken können Markenzeichen der jeweiligen Unternehmen sein. prisma-executive-summary-ds-053119-de