

Sicher in die Cloud umziehen

Cloud Migration und Hybrid Cloud



HOHE SICHERHEITSSTANDARDS SIND FÜR SIE KEIN NEULAND

Als IT-Security-Verantwortlicher bei einer Bank, Versicherung oder einem Finanzdienstleister sind Sie daran gewöhnt, hohe Sicherheitsstandards einzuhalten. Schließlich gehört Ihr Unternehmen zu den KRITIS-Organisationen und steht verstärkt im Visier von Cyberkriminellen. Aber jetzt wird Ihre Arbeit noch schwieriger, denn Teile des Rechenzentrums sollen in die Cloud ausgelagert werden.

Keine Frage, das bringt bekannte Vorteile wie bessere Skalierbarkeit und mehr Flexibilität. Hardware-Kosten und Administrationsaufwand können gespart werden. Doch anders, als so mancher Kollege meint, ist die Cloud kein Rundum-Sorglos-Paket und darüber hinaus erschweren disruptive Entwicklungen den Umzug. So eröffnet beispielsweise die zweite Zahlungsdienstrichtlinie der EU - kurz PSD2, den Zahlungsverkehr gegenüber Drittparteien.

Für diese Form des Open Banking benötigen Banken völlig neue Sicherheitskonzepte, um Kundendaten zu schützen. In puncto Security gilt demnach das Prinzip der geteilten Verantwortung: Der Provider sorgt für die Absicherung von Hardware, Software, Netzwerk und Einrichtungen, auf denen der Cloud-Service ausgeführt wird. Für alles, was Sie innerhalb der Cloud betreiben, also Ihre Applikationen, Daten und das Gesamtbetriebssystem, sind Sie aber selbst zuständig.



BEI DER CLOUD-MIGRATION AN DIE SICHERHEIT DENKEN

Jetzt müssen Sie also zwei Welten gleichzeitig schützen: die bestehenden On-Premises-Systeme und die neuen Public-Cloud-Services. Und das schon vor der Migration, damit beim Umzug nahtlose Sicherheit gewährleistet ist. Die Hybrid Cloud bringt zahlreiche Herausforderungen mit sich:



Sie müssen in den unterschiedlichen Umgebungen verschiedene Security-Systeme aufbauen und managen. Das verursacht einen enormen Aufwand und erschwert einen ganzheitlichen Blick auf die Sicherheitslandschaft.



Sie müssen die Risiken in beiden Welten individuell bewerten und angemessene Maßnahmen ergreifen. Welche Daten dürfen zum Beispiel wohin verschoben werden und wie?



Das größte Risiko in der Cloud sind Fehlkonfigurationen. Gartner geht davon aus, dass 99 Prozent aller Cloud-Sicherheitsvorfälle im Jahr 2023 darauf zurückgehen werden. Aber alle unsicheren Einstellungen zu finden und zu beheben, scheint nahezu unmöglich. Denn ein AWS-Set-Up kann schnell einmal über 160 Services mit jeweils granularen Autorisierungsrichtlinien umfassen. Dazu kommt, dass sich Cloud-Umgebungen meist sehr dynamisch entwickeln.



Cloud Security erfordert spezialisiertes Know-how. Doch solche Experten sind in Zeiten des Fachkräftemangels rar.

WAS JETZT?

Sie brauchen eine Security-Lösung, die die Absicherung der Hybrid Cloud so einfach macht, wie die der gewohnten On-Premises-Umgebung. Sie sollte Sicherheitsfunktionen von einer zentralen Plattform aus für die komplette Infrastruktur bereitstellen - egal ob sich Systeme im eigenen Rechenzentrum oder in der Cloud befinden.

So können Sie Workloads sicher und ganz nach Bedarf zwischen der On-Premises-Umgebung und Public-Cloud-Providern verschieben. Das Security-Management ist unabhängig von der IT-Infrastruktur und bleibt immer gleich.

Um vor Cloud-spezifischen Risiken zu schützen, ist ein **Cloud Security Posture Management (CSPM)** unverzichtbar: Es prüft die Cloud-Umgebung kontinuierlich auf Fehlkonfigurationen, deckt Sicherheitslücken auf und kann sie automatisiert schließen. Kommen neue Cloud-Services hinzu, werden diese sofort erkannt und gescannt. Dabei gleicht das CSPM die Einstellungen permanent mit zentralen Frameworks, regulatorischen Anforderungen, branchenspezifischen Best Practices und Unternehmensrichtlinien ab.

EINE PLATTFORM FÜR ALLES

Wählen Sie eine Plattform-Lösung, die Automatisierung bietet und künstliche Intelligenz einsetzt. So können Sie Prozesse beschleunigen, Mitarbeiter entlasten und die Absicherung der Hybrid Cloud erheblich verbessern. Lesen Sie dazu auch die Gartner [„Top Security and Risk Management Trends“](#).

DAS BRINGT'S



- Dank einfachem, zentralem Security-Management haben Sie die gesamte Infrastruktur der Hybrid Cloud immer im Blick und können schnell reagieren.
- Wenn Sie Workloads in die Cloud verschieben, sind diese automatisch abgesichert.
- Sie können Workloads auch zwischen verschiedenen Public-Cloud-Providern verschieben - das Security-Management bleibt gleich. So gewinnen Sie maximale Flexibilität.
- Sie vermeiden Fehlkonfigurationen - und damit das größte Risiko in der Cloud. Das CSMP erkennt unsichere Einstellungen in Cloud-Services und kann sie automatisiert beheben.
- Auch dynamisches Cloud-Wachstum behalten Sie sicher im Griff. Jeder neue Cloud-Service wird automatisch erkannt und auf Sicherheitslücken gescannt.

DER PARTNER AN IHRER SEITE



Mit Cloud One von Trend Micro erhalten Sie Best of Breed-Lösungen vereint aus einer Hand von einem Marktführer. Trend Micro hat laut IDC mit 29,5 Prozent den mit Abstand größten Marktanteil im Bereich Hybrid Cloud Workload Security und wurde im Forrester Wave™: Cloud Workload Security als Leader genannt (4. Quartal 2019).

Trend Micro (börsennotiert in Tokyo) hat über 30 Jahre Erfahrung als Spezialist für Sicherheitslösungen. Das Unternehmen wird seit 15 Jahren erfolgreich von seiner Mitgründerin Eva Chen geleitet, die als Leading Woman in IT international anerkannt ist. Seit der Gründung im Jahr 1988 achtet sie mit ihrem Managementteam darauf, dass das Unternehmen gesund wächst und reinvestiert auch in Krisenzeiten umfangreich in Forschung und Entwicklung.

Ihr Credo: „Unsere einzige Konkurrenz sind Cyberkriminelle, denen man Einhalt gebieten muss.“



©2021 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo, OfficeScan and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. For details about what personal information we collect and why, please see our Privacy Notice on our website at: <https://www.trendmicro.com/privacy>