



# Cloud-Migration - aber sicher!

Security-Service-Plattform mit Rundum-Schutz



## HABEN SIE VOR DER MIGRATION AN DIE SECURITY GEDACHT?

Wenn Sie auf das vergangene Jahr zurückblicken, werden Sie womöglich feststellen: Der oft gehörte Spruch von der Krise als Chance ist gar nicht so dumm. Der „Lockdown“ und die veränderten Bedürfnisse Ihrer Kunden haben Sie vermutlich längst inspiriert, das Thema Service neu zu überdenken. Um schneller und flexibler agieren zu können und besser zu skalieren, wollen Sie Workloads in die Cloud migrieren.

Die meisten Einzelhandelsunternehmen entscheiden sich für AWS als Provider, weil sie dort viele nützliche Anwendungen „On Demand“ erhalten. Doch ganz gleich, welchen - oder wie viele - Public Cloud Services Sie nutzen: Wichtig ist, dass Sie bereits vor dem Umzug für angemessene Security sorgen. Systeme, die Sie in die Cloud verschieben, müssen während und nach der Migration genauso sicher sein wie On-Premises. Schließlich haben Sie es im Einzelhandel mit sensiblen Finanz- und Kundendaten zu tun, die nicht in falsche Hände geraten dürfen.

## HYBRIDE UMGEBUNGEN HABEN ES IN SICH

Aber kümmert sich nicht der Cloud Provider um die Security? Jein, denn in der Cloud gilt das Prinzip der geteilten Verantwortung: Der Provider sichert zwar die Infrastruktur, auf der der Cloud-Service ausgeführt wird. Alles, was Sie innerhalb der Cloud betreiben, müssen Sie aber selbst schützen. Sie stehen also vor einigen Herausforderungen:



Durch die Cloud-Transformation entsteht eine hybride IT-Umgebung. Neben Ihren On-Premises-Systemen müssen Sie jetzt auch noch Security-Lösungen in der Cloud aufbauen und managen. Das verursacht doppelten Aufwand.



Sie haben es mit zwei parallelen Security-Welten zu tun, in denen Sie Risiken individuell betrachten und Maßnahmen auswählen müssen.



Je größer und vielfältiger die IT-Umgebung, desto komplexer wird das Security-Management. Da kann schnell einmal ein Fehler passieren.



Jede Cloud hat ihre eigenen Besonderheiten, mit denen Sie sich auskennen müssen. Sonst kann es zu gefährlichen Konfigurationsfehlern kommen. Was, wenn Daten in einem S3-Bucket öffentlich zugänglich sind?



Cloud Security-Experten sind in Zeiten des Fachkräftemangels schwer zu finden.

## WAS TUN?

Sie brauchen eine Plattform-Lösung, die es Ihnen ermöglicht, die Security für Ihre gesamte hybride Multicloud-Umgebung einheitlich zu managen. Sie sollte Sicherheitsfunktionen sowohl für On-Premises-Systeme als auch für Cloud Services bereitstellen, Security-Prozesse automatisieren und sich bereits in die DevOps-Pipeline integrieren lassen.

So sind Workloads von Anfang an geschützt, egal ob sie sich im eigenen Rechenzentrum oder in der Cloud befinden. Die Lösung sollte auch Container und Serverless-Funktionen absichern und ein Cloud Security Posture Management bieten (CSPM). Dieses deckt automatisiert Fehlkonfigurationen auf und gibt Schritt für Schritt-Anleitungen, um sie zu korrigieren. Dabei prüft das CSPM die Einstellungen anhand von Regularien und Best Practices wie dem AWS Well-Architected Framework.

## ACHTEN SIE AUF NATIVE CLOUD-INTEGRATION

Wählen Sie eine Cloud-native Lösung, die sich mit wenigen Klicks direkt in Ihrer Public Cloud Umgebung ausrollen lässt. Das spart Zeit und erhöht die Effizienz. Wenn Sie AWS nutzen, sollten die Security-Funktionen über den AWS Marketplace als Service buchbar sein. So können Sie sie bequem über Ihr AWS-Konto abrechnen und flexibel skalieren.



# DARUM LOHNT SICH EINE CLOUD-SECURITY-PLATTFORM



- Sie etablieren Sicherheit über den gesamten Migrationsprozess hinweg.
- Indem Sie Ihr Security-Management unabhängig von der IT-Infrastruktur machen, gewinnen Sie maximale Flexibilität und können Systeme ganz nach Bedarf zwischen verschiedenen Umgebungen verschieben.
- Sie vereinfachen das Security-Management und haben die gesamte Sicherheitslandschaft Ihrer hybriden Umgebung von einer zentralen Management-Konsole aus immer im Blick. So können Sie schnell reagieren.
- Sie vermeiden Fehlkonfigurationen und behalten auch dynamisches Cloud-Wachstum sicher im Griff. Jeder neue Cloud-Space wird automatisch überprüft.
- Als AWS-Kunde beziehen Sie die Lösung als Service aus dem Marketplace und zahlen nur das, was Sie tatsächlich nutzen.

## DER PARTNER AN IHRER SEITE



Mit Cloud Security Lösungen 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).

Zwischen AWS und Trend Micro besteht eine langjährige, enge Partnerschaft. Seit 2012 ist Trend Micro „AWS Advanced Technology Partner“ im AWS Partner Network (APN) sowie „AWS Security Competency Partner“. Zudem hat Trend Micro den größten Marktanteil bei den Sicherheitsanbietern, die sich dem Schutz von AWS-Kunden widmen.

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.“



Copyright © 2023 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro Logo und das T-Ball-Logo sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- bzw. Produktnamen sind Unternehmenskennzeichen oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. Trend Micro, das Trend Micro Logo und das T-Ball-Logo tragen das Registered-Trade-Mark-Symbol der USA. Einzelheiten darüber, welche personenbezogenen Daten wir erfassen und warum, finden Sie in unserer Datenschutzerklärung auf unserer Website unter: [https://www.trendmicro.com/de\\_de/about/legal/privacy.html](https://www.trendmicro.com/de_de/about/legal/privacy.html)