

# So setzen Sie Cloud-Storage sicher ein

## File Storage Security



# CLOUD-STORAGE IST EIN NEUER ANGRIFFSVEKTOR

Die meisten Unternehmen nutzen heute Cloud-Storage, um ihre Infrastruktur kostengünstiger, flexibler und skalierbarer zu machen. Sie auch? Services wie Amazon S3-Buckets, Microsoft Azure Blob Storage oder Google Cloud Storage kommen häufig im Backup- oder Big Data-Bereich zum Einsatz und spielen mit Cloud-basierten Applikationen zusammen. Sie ermöglichen es zum Beispiel, Dateien mit Kunden oder Geschäftspartnern zu teilen.

So hat ein Zugunternehmen etwa einen Service entwickelt, über den Kunden Fahrplanauskünfte und Tickets anfordern können. Die Fahrkarte wird dann automatisiert erstellt und in Amazon S3 gespeichert, sodass der Kunde sie herunterladen kann. Doch was, wenn die Datei mit Ransomware infiziert ist und die Festplatte des Kunden verschlüsselt?

Das kann schnell dazu führen, dass Sie haftbar gemacht werden. Cloud-Storage aber auch Dropbox, Microsoft 365 und andere Software-as-a-Service (SaaS)-Anbieter in der Cloud stellen aus Security-Sicht neue Endpunkte dar, die Sie schützen müssen. Aus diesem Grund schreiben entsprechende Regularien den Einsatz von Antimalware vor. Denn Sie müssen dafür sorgen, dass Daten, die Sie zur Verfügung stellen, sauber sind. Umgekehrt ist Cloud Storage aber auch ein Angriffsvektor, über den Malware in Ihr Unternehmensnetzwerk eindringen kann - insbesondere, wenn externe Anwender Dateien hochladen dürfen.

## WER KÜMMERT SICH UM DIE MALWARE-PRÄVENTION?

Auch wenn der Cloud-Provider viele Security-Services bereitstellt, gilt in der Cloud das Prinzip der geteilten Verantwortung. Das heißt: Der Provider kümmert sich um die Absicherung von Hardware, Software, Netzwerk und Einrichtungen, auf denen der Cloud-Service ausgeführt wird. Für den Schutz Ihrer Applikationen, Daten und des Gesamtbetriebssystems müssen Sie dagegen selbst sorgen. Darunter fällt auch die Malware-Prävention. Das bedeutet:



Sie müssen alle Daten auf Malware scannen, die in Ihren Cloud Storage hochgeladen werden - sowohl intern als auch kundenseitig.



Sie brauchen eine Cloud-native Security-Lösung. On-Premises-Anti-Malware-Software lässt sich meist nicht ohne Weiteres in Cloud-Services integrieren.



Da Cloud-Storage häufig in automatisierte Workflows eingebunden ist, muss sich die Security-Lösung in diese Workflows integrieren lassen und darf sie nicht ausbremsen.



Sie müssen dafür sorgen, dass Ihr Cloud-Storage sicher konfiguriert ist. Gerade in großen Umgebungen verliert man schnell einmal den Überblick und es passieren Fehler - zum Beispiel falsch gesetzte Berechtigungen. Laut Gartner sind Fehlkonfigurationen das größte Sicherheitsrisiko in der Cloud.

## WAS TUN?

Gefragt ist eine Cloud-native Security-Lösung, die sich einfach in der Cloud bereitstellen lässt und über APIs in die Cloud-Services eingebunden ist. Außerdem sollte sie eine serverlose Architektur haben, sodass sie sich leicht in anwenderdefinierte Workflows integrieren lässt.

So können Sie Malware-Scans direkt in Ihrem AWS-Account und in Ihren Cloud-Applikationen durchführen. Anhand von Anti-Malware-Technologie prüft die Lösung alle Dateien beim Upload in den Cloud-Storage. Wichtig ist, dass sie dabei auf neueste, umfangreiche Threat Intelligence zugreift. Mithilfe von Algorithmen ist die Security-Lösung sogar in der Lage, verschleierte oder polymorphe Malware-Varianten zu entdecken. Verdächtige Dateien blockiert sie, steckt sie in Quarantäne und verständigt den Anwender und das Security-Team.

Ergänzen sollten Sie die Malware-Prävention durch ein Cloud-Security-Posture-Management (CSMP), das Ihren Cloud-Storage vor unsicheren Konfigurationen schützt. Es prüft die Einstellungen Ihrer Cloud-Services anhand von Compliance-Anforderungen, zentralen Frameworks, Unternehmensrichtlinien und branchenspezifischen Best Practices. Entdeckt die Lösung Sicherheitslücken, kann sie diese automatisiert schließen.



## TIPP: DENKEN SIE GANZHEITLICH!

Je mehr Einzellösungen Sie einsetzen, desto aufwändiger wird das Security-Management. Daher empfiehlt es sich, gleich eine Cloud-Security-Plattform zu wählen, die neben File Storage Security und Konformitäts-Check auch Module für alle anderen wichtigen Bereiche bietet: Container Security, Workload Security, Application Security und Network Security. So reduzieren Sie Komplexität und gewinnen Transparenz.

## DIESE VORTEILE BRINGT EINE CLOUD-SECURITY-PLATTFORM



- Sie können Ihren Cloud-Storage, ebenso wie Dateien, die Kunden herunterladen, vor Malware schützen.
- Sie können verhindern, dass Malware über den Cloud-Storage in Ihr Netzwerk eindringt.
- Sie haben die Sicherheit Ihres Cloud-Speichers von einer zentralen Konsole aus immer im Blick.
- Sie vermeiden unsichere Konfigurationen Ihrer Cloud-Services.
- Sie halten Compliance-Richtlinien ein und schützen sensible Daten vor unbefugten Zugriffen.

## 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. Die Plattform schützt Rechenzentrum, Cloud und Container mit einer umfassenden SaaS-Lösung. 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.

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).