SOPHOS

7 BEST PRACTICES ZUM SCHUTZ DER PUBLIC CLOUD

Wie Sie Ihre Daten und Ihr Unternehmen beim Einsatz von Public-Cloud-Anbietern wie Amazon Web Services, Microsoft Azure und der Google Cloud Platform schützen

1 Gemeinsame Verantwortung

Das Modell der gemeinsamen Verantwortung bedeutet: Public-Cloud-Anbieter sind für die "Sicherheit der Cloud" verantwortlich, d. h. auch für den physischen Schutz im Rechenzentrum sowie für die virtuelle Trennung von Kundendaten und Umgebungen. Sie selbst sind jedoch verantwortlich für die "Sicherheit in der Cloud", d. h. für alles (Daten, Workloads), was Sie in der Cloud ablegen.

2 Multi-Cloud-Planung

Gehen Sie bei der Planung Ihrer Sicherheitsstrategie davon aus, dass Sie mehrere Public-Cloud-Anbieter nutzen werden – wenn nicht jetzt, dann irgendwann in der Zukunft. So machen Sie Ihre Strategie zukunftssicher.

3 Transparenz

Was Sie nicht sehen können, können Sie auch nicht schützen. Deshalb ist es für Ihre Sicherheit enorm wichtig, volle Transparenz zu haben: über Ihre gesamte cloudbasierte Infrastruktur, Ihre Konfigurations-einstellungen, API-Aufrufe und den Benutzerzugriff.

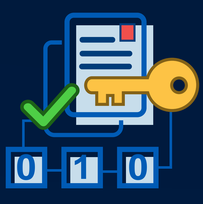
4 Kontinuierliche Compliance

Durch die Dynamik der Public Cloud lässt sich Compliance mit vielen Richtlinien nur durch eine kontinuierliche Überwachung sicherstellen. Am besten integrieren Sie Compliance in tägliche Abläufe, mit Echtzeit-Snapshots Ihrer Netzwerktopologie und Echtzeit-Warnmeldungen bei Änderungen.

5 Automatische Sicherheitskontrollen

Cyberkriminelle setzen bei ihren Angriffen zunehmend auf Automatisierung. Bleiben Sie Hackern einen Schritt voraus: Automatisieren Sie Ihre Abwehr, die Beseitigung von Schwachstellen und das Anomalie-Reporting.

6 Schutz aller Umgebungen (auch Dev und QA)



Aus den Medien bekannte Datenpannen betreffen meist Produktionsumgebungen in der Cloud. Für Aktivitäten wie Cryptojacking nehmen sich Angreifer aber genauso gerne Ihre Entwicklungs- oder QA-Umgebung vor.

7 Setzen Sie auf Bewährtes

IT-Sicherheit für lokale Systeme ist das Ergebnis jahrezehntelanger Erfahrung und Forschung. Schützen Sie Ihre cloudbasierten Server mit Firewalls und Server-Security vor Infektionen und Datenverlusten. Sorgen Sie außerdem dafür, dass Ihre Endpoint- und E-Mail-Security auf Ihren Geräten aktuell sind, damit Unbefugte keinen Zugriff auf Ihre Cloud-Accounts erhalten.

7 BEST PRACTICES ZUM SCHUTZ DER PUBLIC CLOUD

Zuverlässigen Schutz für die Public Cloud finden Sie unter

www.sophos.de/cloud-optix