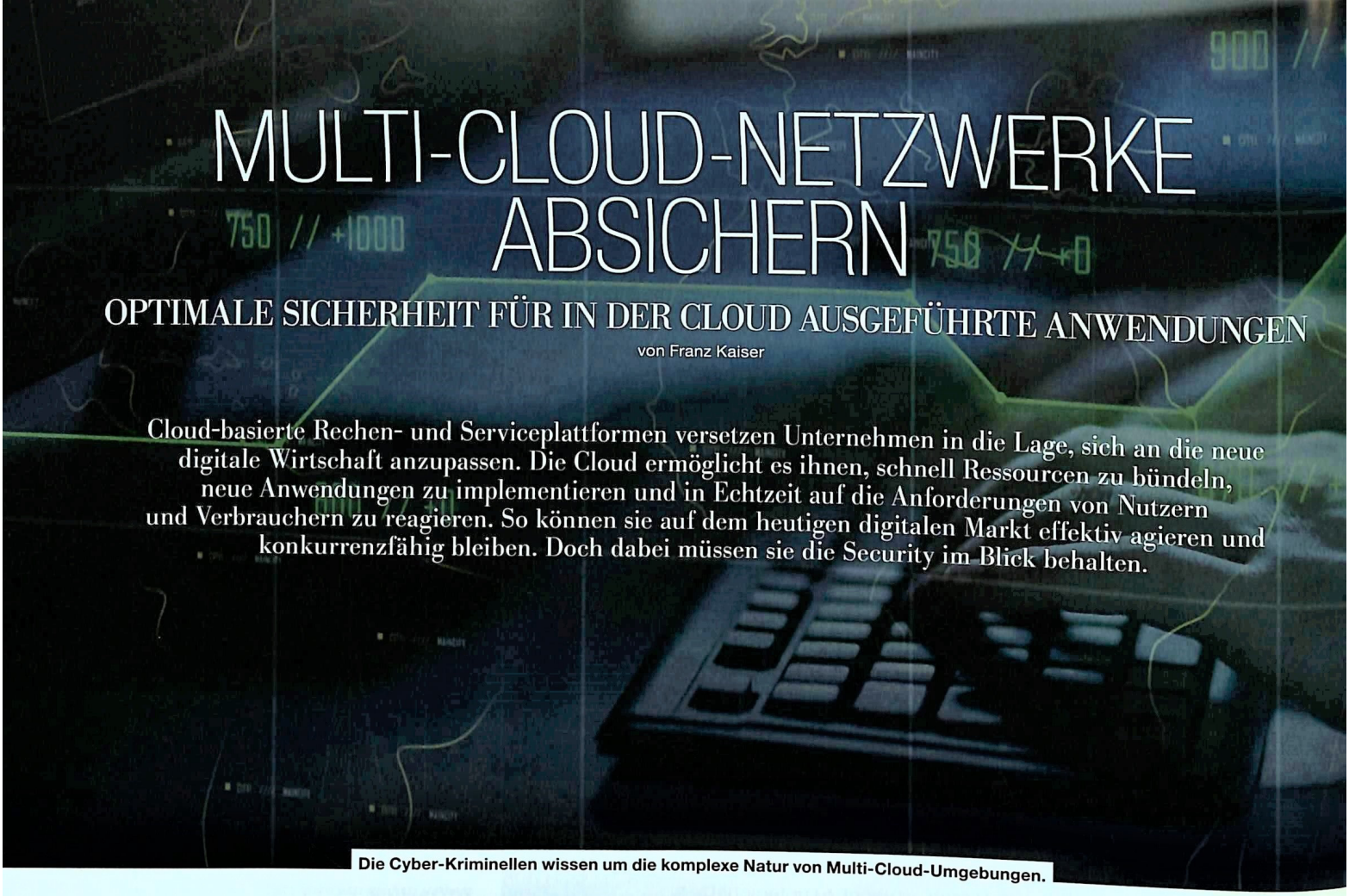
MULTI-CLOUD-NETZWERKE ABSICHERN

OPTIMALE SICHERHEIT FÜR IN DER CLOUD AUSGEFÜHRTE ANWENDUNGEN

von Franz Kaiser

Cloud-basierte Rechen- und Serviceplattformen versetzen Unternehmen in die Lage, sich an die neue digitale Wirtschaft anzupassen. Die Cloud ermöglicht es ihnen, schnell Ressourcen zu bündeln, neue Anwendungen zu implementieren und in Echtzeit auf die Anforderungen von Nutzern und Verbrauchern zu reagieren. So können sie auf dem heutigen digitalen Markt effektiv agieren und konkurrenzfähig bleiben. Doch dabei müssen sie die Security im Blick behalten.



Die Cyber-Kriminellen wissen um die komplexe Natur von Multi-Cloud-Umgebungen.

Innerhalb von nur wenigen Jahren haben über 80 Prozent der Unternehmen zwei oder mehr Anbieter von Public-Cloud-Infrastrukturen in Anspruch genommen. Fast zwei Drittel nutzen drei oder mehr. Gleichzeitig werden kritische Daten über unterschiedlichste Cloud-basierte Anwendungen und Dienste verbreitet und verarbeitet. Doch der Performance darf dabei nicht die Security zum Opfer fallen. Es kann praktisch unmöglich werden, eine dynamische, hoch elastische Multi-Cloud-Umgebung mit herkömmlichen Sicherheitslösungen und -strategien angemessen zu sichern. Stattdessen brauchen digitale Umgebungen von heute ein integriertes, fabric-basiertes Security-Konzept, das das «Unmögliche möglich» macht.

Das Unternehmen Fortinet hat fünf Aspekte auf den Punkt gebracht, die Unternehmen helfen sollen, eine effektive Multi-Cloud-Security-Strategie zu entwickeln.

EINHEITLICHKEIT

Lassen sich Geräte nur isoliert verwalten, führt dies zu einer lückenhaften Security. Abwehrmassnahmen können dann weder koordiniert erfolgen, noch Sicherheitsrichtlinien oder -protokolle konsequent durchgesetzt werden. Unternehmen müssen nicht nur Sicherheitslösungen bereitstellen, die über Cloud-Ökosysteme hinweg konsistent funktionieren. Sie müssen auch in der Lage sein, die Automatisierung in Vorlagen zu integrieren, damit die Sicherheit konsistent bleibt und gleichzeitig in der Umgebung jedes Cloud-Anbieters angewendet werden kann. CISOs müssen daher für eine Automatisierung der gesamten IT-Infrastruktur sorgen, damit sich die Sicherheit dynamisch an die Workloads und Informationen innerhalb und zwischen verschiedenen Cloud-Umgebungen anpassen kann.

SCHNELLIGKEIT

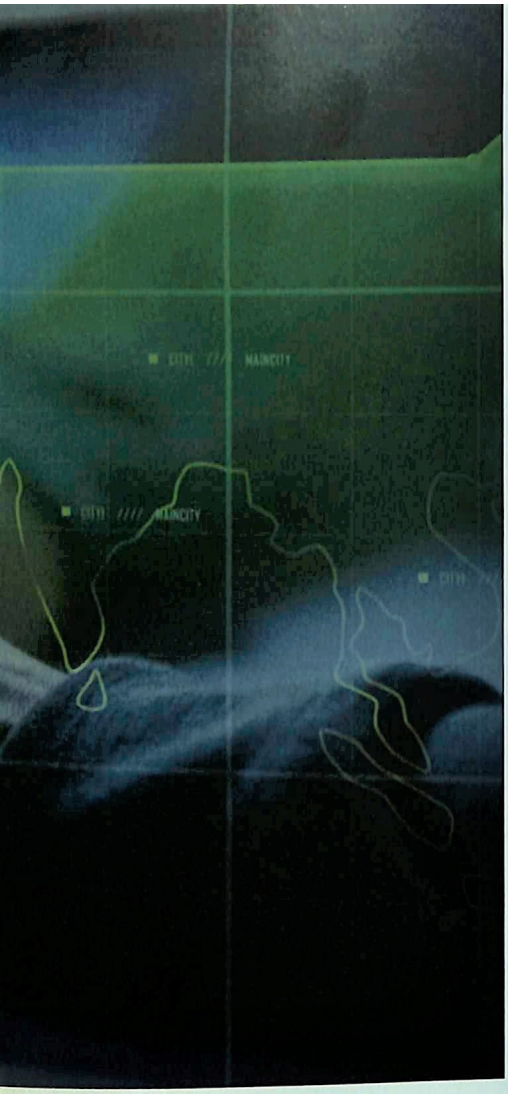
Der Einsatz von IoT-Geräten führt zu einem exponentiellen Anstieg des zu schützenden Datenvolumens. Software-as-a-Service-(SaaS)-Anwendungen arbeiten mit höheren Durchsätzen. Erschwerend kommt hinzu, dass über die Hälfte dieses Traffics mittlerweile verschlüsselt ist. Die SSL-Inspektion erfordert in diesem Umfang eine hohe Rechenleistung, was jedoch viele Sicherheitsgeräte in die Knie zwingt. Da gleichwohl der Erfolg in einer solchen Umgebung in Mikrosekunden gemessen wird, können sich Unternehmen keine Security leisten, die das Netzwerk ausbremst. Das richtige Sicherheitsframework stellt eine SSL-Inspektion in hoher Geschwindigkeit zur Verfügung.

TRANSPARENZ UND SKALIERBARKEIT

Die Stärke einer Cloud-basierten Unternehmensumgebung liegt in ihrer Skalierbarkeit und Elastizität. Das führt allerdings häufig zu einem unvorhersehbaren Datenfluss, was für viele Security-Lösungen problematisch ist. Multi-Cloud-Security muss daher integriert funktionieren, um effektiv zu sein. Die Integration von Sicherheitstools ermöglicht eine plattformübergreifende Transparenz und konsistente Security. Die Cloud-Sicherheitsarchitektur muss ausserdem dynamisch, flexibel und in der Lage sein, sich mit Cloud-Workloads und Anwendungen bei deren Erweiterung zu bewegen.

AUTOMATISIERUNG

Cyber-Kriminelle wissen um die komplexe Natur von Multi-Cloud-Umgebungen und nutzen Sicherheitslücken zwischen verschiedenen Netzwerk-Segmenten und -Umgebungen aus. Indem Unternehmen Bedrohungs-Feeds nutzen und die



nativen Sicherheitsfunktionen aller Clouds in das Multi-Cloud-Sicherheitsframework integrieren, können sie ihre Cloud-Security multiplizieren. Sobald Sicherheitsvorgänge automatisiert sind, kann beispielsweise eine automatische Koordination der Bedrohungsreaktion erfolgen. Dazu gehören die Isolierung infizierter Geräte, die Identifizierung und Abschaltung von Malware und die Ausweitung des Schutzes auf die gesamte Multi-Cloud-Umgebung.

BEDROHUNGSAUSTAUSCH

Security-Technologien müssen zudem gesammelte Bedrohungsdaten – sogenannte Threat Intelligence – automatisch austauschen können. Unternehmen, Security Operation Center (SOCs) und Managed Security Service Provider (MSSPs) profitieren hier gleichermassen von integrierten SIEM-Technologien (Security, Information and Event Management). Diese verbessern die Erkennung raffinierter Bedrohungen, erleichtern die Priorisierung und ermöglichen die Automatisierung einer gemeinsamen Reaktion.

SCHUTZ ALLER DATEN

Die digitale Transformation verlangt nach dem Umstieg auf Multi-Cloud-Netzwerke und erfordert eine entsprechende Transformation der Security. Unternehmen müssen jetzt mit der Implementierung eines Fabric-basierten Security Frameworks beginnen. Nur so lassen sich Daten, Workflows und Ressourcen schützen und zugleich die Herausforderungen an Performance, Skalierbarkeit und Komplexität einer sich ständig weiterentwickelnden Multi-Cloud-Umgebung erfolgreich meistern. ●

FRANZ KAISER

ist seit 2004 Country Manager Switzerland für den Sicherheitsspezialisten Fortinet.

www.fortinet.com