› Bei einer Cloud-Migration lauern eine Menge Gefahren. Unternehmen sollten bereits vorher alle potenziellen Security-Lücken schließen und überwachen. (Foto: ozrimoz – shutterstock.com)

Sichere Cloud-Migration

Diese Sicherheitsrisiken lauern bei der Cloud-Migration

Security in einer On-Premises-Landschaft unterscheidet sich in wesentlichen Punkten von der Sicherheit in einer Cloud. Wir erklären, was bei einer Cloud-Migration zu beachten ist und wie Sie die Sicherheitsrisiken beim Umzug minimieren.

Bei der Cloud-Migration werden Daten, Anwendungen und andere digitale Ressourcen von einem lokalen Rechenzentrum in die Cloud verschoben. Dabei kann es sich um individuell erstellte Anwendungen oder um Systeme handeln, die das Unternehmen von einem Drittanbieter lizenziert hat. Es gibt verschiedene Ansätze für die Cloud-Migration, darunter:

- Anwendungen werden im Ist-Zustand verschoben – dies ist als „Lift and Shift" bekannt.
- Es werden kleine Änderungen an den Anwendungen vorgenommen, um deren Umzug in die Cloud zu ermöglichen.
- Neuaufbau oder Refactoring von Anwendungen, um sie für eine Cloud-Umgebung besser geeignet zu machen.
- Umstellung von Legacy-Anwendungen auf neue Programme, die die Cloud unterstützen oder von Cloud-Anbietern bereitgestellt werden.
- Das Erstellen neuer Anwendungen für die Cloud (Cloud-native Entwicklung).

Wie unterscheidet sich die Sicherheit in der Cloud von On-Premises?

Es gibt drei wesentliche Unterschiede zwischen der Sicherheit in der Cloud und On-Premises:

- **Geteilte Verantwortung:** Das Konzept der geteilten Verantwortung für Datenschutz und Cybersicherheit ist seit vielen Jahren Bestandteil der meisten Outsourcingvereinbarungen. Das hat sich jedoch mit der Einführung der Cloud verändert. Alle großen Cloud-Anbieter unterstützen die gemeinsame Verantwortung in der Cloud, aber nicht alle diese Modelle sind gleich. Ein Teil der Security in der Cloud liegt in der Verantwortung des Kunden. Dazu zählen Datenschutz, Identitäts- und Zugriffsmanagement (IAM), Betriebssystemkonfiguration, Netzwerksicherheit und Verschlüsselung. Zur Verantwortung des Cloud-Dienstleisters gehören die zugrundeliegenden Teile der Infrastruktur, einschließlich der Datenverarbeitungselemente, Hypervisoren, Speicherinfrastruktur, Datenbanken und Netzwerke.
- **Software:** Ein weiterer großer Unterschied zwischen der Sicherheit On Premises und in der Cloud besteht darin, dass in der Cloud alles softwarebasiert ist. Dies bringt spezielle Anforderungen an Kontrollen und Prozesse sowie potenziell neue Tools und Dienste zur Erfüllung der Sicherheitsziele mit sich. Auch hier ist der Cloud-Anbieter für die Verwaltung und Sicherung der Hardware verantwortlich, auf der seine Dienste beruhen – der Nutzer bekommt davon allerdings nichts mit.
- **Verwaltung:** Die Arbeitsabläufe und die Ausrichtung der Governance in der Cloud müssen viel flexibler und kontinuierlicher sein, wobei jederzeit verschiedene Interessengruppen und technische Disziplinen vertreten sein und sich miteinander abstimmen müssen. So muss jederzeit eine größere Anzahl von Interessenvertretern einbezogen werden, um Entscheidungen schneller treffen zu können als bisher üblich.

Sicherheitsrisiken der Cloud-Migration

Die Cloud-Migration erfordert eine sorgfältige Planung. Während der Migration werden sensible Daten übertragen, was diese anfällig für Angriffe macht. Darüber hinaus können Angreifer in verschiedenen Phasen eines Migrationsprojekts Zugang zu ungesicherten Entwicklungs-, Test- oder Produktionsumgebungen erhalten.

API-Schwachstellen: Organisationen müssen Sicherheitskontrollen mit einem gewissen Grad an Automatisierung entwickeln, um sich während einer Cloud-Migra-

tion anzupassen und zu skalieren, einschließlich der Geschwindigkeit des laufenden Cloud-Betriebs. Dies wird meist durch die umfassende Nutzung der APIs von Cloud-Anbietern sowie durch spezielle Tools und Dienste erreicht, die bei der Rationalisierung und Integration der Sicherheitsautomatisierung für die gewünschten Anwendungsfälle helfen können.

Blinde Flecken: Der Wechsel in die Cloud bedeutet, dass Unternehmen die Kontrolle über einige Aspekte des Betriebs aufgeben. Deshalb sollte vor der Migration geprüft werden, welche Sicherheiten der gewählte Cloud-Anbieter bietet und wie diese gegebenenfalls mit Sicherheitslösungen von Drittanbietern ergänzen werden müssen.

Compliance-Anforderungen: Es muss sichergestellt werden, dass die Ziel-Cloud-Umgebung alle erforderlichen Compliance-Standards unterstützt. Dazu gehören Zertifizierungen durch den Cloud-Anbieter und Verfahren, die das Unternehmen selbst durchführt, um die Sicherheit von Cloud-Workloads, Daten und Zugriff zu gewährleisten. All dies kann und muss im Rahmen der Migration (oder der Vorbereitung dazu) geprüft werden.

Unkontrolliertes Wachstum: Die Cloud-Migration ist kein einmaliger Prozess. Nach der Migration von Anwendungen in die Cloud wird das Unternehmen wahrscheinlich weitere Ressourcen und Anwendungen hinzufügen sowie neue Cloud-Dienste in Anspruch nehmen. Es ist üblich, dass zusätzliche SaaS-Anwendungen genutzt werden, sobald die ersten bestehenden Anwendungen in die Cloud überführt sind. Diese neuen Dienste und Anwendungen müssen ordnungsgemäß abgesichert werden, was eine große betriebliche Herausforderung darstellt.

Datenverlust: Die Migration in die Cloud beinhaltet eine Datenübertragung. Es muss unbedingt sichergestellt werden, dass die Daten für den Fall von Fehlern im Migrationsprozess gesichert sind. Die gesamte Datenübertragung muss über verschlüsselte Kanäle erfolgen, wobei die Verschlüsselungsschlüssel sorgfältig zu verwalten sind.

Sicherheitsrisiken bei der Cloud-Migration minimieren

Auch wenn die Bewertung der Sicherheitsrisiken und der Gegenmaßnahmen immer individuell zu bewerten sind, enthält die folgende Aufzählung die gängigsten Empfehlungen zu den wichtigsten Sicherheitsmaßnahmen für Unternehmen, die eine Cloud-Einführung oder -Migration planen.

Baseline der Sicherheit vor der Migration: Viele Unternehmen arbeiten mit einer Sicherheitsarchitektur, die auf isolierten Sicherheitsgeräten, einer (zumeist) inkonsis-

tenten Anwendung von Sicherheitsrichtlinien und einer dezentralen Verwaltung von Sicherheitsstrategien beruht. Das Migrationsprojekt verschlimmert die Situation noch, da sich die Unternehmen für die Übertragung ihrer Anwendungen und Daten für den Einsatz von Tools entscheiden, die sowohl interne als auch entfernte Umgebungen sichern. Unter diesen Umständen muss ein Unternehmen den Sicherheitswildwuchs kontrollieren und eine zentralisierte Sicherheitsstrategie implementieren.

Backups und Strategien zur Wiederherstellung: Unternehmen, die in die Cloud migrieren, sollten verhindern, dass Benutzer die Erlaubnis erhalten, neue Angriffsflächen zu schaffen und Zugang zu Sandbox-Umgebungen zu erhalten. Die Aufbewahrung einer genauen und vollständigen Kopie des jetzigen Zustands ermöglicht es einem Unternehmen, Fehler bei der Datenexposition und Datenverluste schnell zu korrigieren, indem Dateien und Systeme in ihrem ursprünglichen Zustand wiederhergestellt werden.

Ordnungsgemäße Einrichtung und Schutz von Benutzeridentitäten: Unternehmen, die auf eine Cloud-Umgebung umstellen, sollten die Zugriffspunkte auf Daten und Anwendungen begrenzen. Die Gewährung des Zugriffs für viele Mitarbeiter kann dazu führen, dass ein Benutzer globale Berechtigungen aktiviert, die Daten für offene Verbindungen freigeben. In diesem Fall sollte sich ein Unternehmen darüber im Klaren sein, wer und was Zugang zu Daten und Anwendungen in der Cloud hat.

Sicherstellen, dass der Cloud Computing Service den geltenden Cybersicherheitsvorschriften entspricht: Unternehmen sollten sich über die Auswirkungen der Einhaltung von Vorschriften im Klaren sein, bevor sie Cloud-Dienste in Anspruch nehmen. Diese Maßnahme ist besonders wichtig, wenn ein Unternehmen in einem stark regulierten Umfeld tätig ist, zum Beispiel im Gesundheits- oder Finanzwesen. Sicherheitsteams sollten ermitteln, wie Unternehmen die Anforderungen an Speicherung, Verschlüsselung, Backup und Übertragung erfüllen. Nahezu alle großen Cloud-Service-Anbieter verfügen über Compliance-Zertifizierungen für gängige Vorschriften wie PCI-DSS, GDPR (DSGVO) oder HIPAA.

Ordnungsgemäße Protokollierung und Überwachung: Unternehmen, die auf eine Cloud-Umgebung umstellen, sollten eine ordnungsgemäße Protokollierung, Überwachung und Sicherheitsanalyse in der Cloud einrichten, insbesondere bei der Übertragung von Daten und Anwendungen von internen Servern. Darüber sollten einfache Skriptfehler, die möglicherweise den Geschäftsbetrieb zum Erliegen bringen oder Schlupflöcher öffnen, die Hacker ausnutzen, erkannt werden.

Automatisierungsverfahren während der Cloud-Migration bringen unerwartete Probleme mit sich, die Unternehmen angehen sollten. Sicherheitsteams können den Zugriff auf und die Kontrolle über Cloud-Ressourcen granular überwachen. Security-Information und Event Management Solutions (SIEM) sind unverzichtbar, da sie

den Unternehmen die Zentralisierung von Warnungen und Protokollierung ermöglichen und gleichzeitig Analysen, Automatisierung und maschinelles Lernen einschließen, um ungewöhnliche Aktivitäten zu erkennen und zu kennzeichnen.

Benutzeranalyse- und Überwachungsplattformen helfen dabei, Verstöße schneller zu erkennen, indem sie das Verhalten analysieren, um ein Standardbenutzerprofil für einen Mitarbeiter und das Gerät zu erstellen, das für den Zugriff auf Cloud-Ressourcen verwendet wird. Wenn eine Aktivität von den Erwartungen des Benutzerprofils abweicht, sendet das Überwachungssystem sofort eine Warnung an die Sicherheitsteams und weist auf die Anwesenheit eines Außenstehenden hin.

Darüber hinaus ist es ratsam auch die offensichtlichen Maßnahmen zu ergreifen, welche auch für jedes andere Softwareprojekt unabhängig der technologischen Basis gelten:

- Datensicherung vor der Migration
- Phasenweise Migration
- Implementierung einer Disaster-Recovery-Strategie
- Sensibilisierung der Mitarbeiter

Viele der Sicherheitsrisiken der Cloud Migration entstehen auch bei normalen Migrationsprojekten von Software, es sollte aber nicht unterschätzt werden, dass das Gefahrenpotenzial wesentlich größer ist. So führen bei einer On-Premises-Migration falsch konfigurierte APIs vielleicht zu einem Sicherheitsrisiko innerhalb des Firmennetzwerks. In der Cloud-Welt stehen die APIs aber direkt ungeschützt der ganzen Welt offen. Diesen Aspekt sollte man immer im Hinterkopf behalten, auch wenn viele der Risiken und Gegenmaßnahmen einem bekannt vorkommen sollten.

Felix Weber

Felix Weber ist Doktorand am Lehrstuhl für Wirtschaftsinformatik und integrierte Informationssysteme mit den Forschungsschwerpunkten Digitalisierung, Künstliche Intelligenz, Preis-Promotion- und Sortiments-Management sowie Transformationsmanagement. An der Universität Duisburg-Essen ist er Leiter des SAP University Innovation Labs und gleichzeitig Berater für SAP Systeme im (Einzel-)Handel bei der Consenso Consulting GmbH.