IT-Security im Cloud-Zeitalter

T Systems

Let's power
higher performance

Einleitung

Lange wurde das Für und Wider der Cloud in Europa intensiv diskutiert. Neben der fehlenden Cloud-Expertise in Unternehmen waren es vor allem Sicherheitsvorbehalte und Herausforderungen für die Compliance, die Unternehmen zwangen, die (Public) Cloud als Sourcing-Modell sehr kritisch zu prüfen.

Heute hat sich die Waagschale zu Gunsten der Cloud geneigt: 70 Prozent aller deutschen Unternehmen nutzen Cloud Services in verschiedener Ausprägung[1] – beginnend bei IaaS über PaaS bis hin zu SaaS. Geschäftslogiken werden in Form von SaaS-Anwendungen aus der Cloud konsumiert, Infrastrukturen und Software-Plattformen werden dynamisch und elastisch als IaaS und PaaS in die Cloud verlagert.

Die wirtschaftlichen Vorteile der Cloud sind zu groß, um sie zu ignorieren. Durch das Pay-per-use-Prinzip können IT-Services bedarfsgerecht genutzt werden, ohne dass dazu Investitionen nötig wären. Diese bedarfsgerechte Verfügbarkeit reduziert Business-Risiken und erlaubt das schnelle Testen neuer Geschäftsideen. Darüber hinaus hat die Cloud eine weitere hochattraktive Eigenschaft für Unternehmen: Skalierbarkeit. Cloud-Ressourcen und -Services verschaffen Unternehmen damit ein Maximum an Agilität; das ist die Fähigkeit, schnell auf Anforderungen des Marktes zu reagieren.

Die Cloud-Nutzung ist heutzutage gelebte Realität. Zudem ist die Cloud ihren Kinderschuhen längst entwachsen. Der hohe Reifegrad im Umgang mit Cloud Services zeigt sich daran, dass sich gegenwärtig die Diskussion um die Cloud verlagert. Aktuell gehen Anwenderunternehmen den nächsten Schritt und etablieren aktiv Multi-Cloud-Landschaften. Sie wollen sich bewusst plattform-unabhängig aufstellen, Risiken und Vendor Lock-in reduzieren und die spezifischen Vorteile der Plattformen nutzen.

Die Rolle der Cloud als Enabler digitaler Geschäftsmodelle kann nicht überschätzt werden. Aber auch wenn die Diskussion um Sicherheit und Compliance zugunsten der Business-Mehrwerte in den Hintergrund gerückt ist – **kein Unternehmen, das Cloud Services einsetzt, kommt umhin, ein ganzheitliches Sicherheitskonzept für den Einsatz der Cloud vorzusehen**. Dieses Sicherheitskonzept muss ein integraler Bestandteil der Cloud-Strategie sein.

Zwar haben die Cloud Service Provider in den letzten Jahren kontinuierlich an der Sicherheit ihrer Plattformen gearbeitet und bieten zusätzlich eine Vielzahl von Sicherheitsfunktionen an. Aber in der Realität zeigt sich, dass damit mitnichten eine umfassende Sicherheit aus einer Hand entsteht. Denn mit der Cloud-Nutzung geht einher, dass auch sensible, unternehmenskritische und besonders schützenswerte Daten (z.B. personenbezogene Daten, Rechnungsdaten, Umsatzinformationen, Kundendaten etc.) die Unternehmensdomäne verlassen. Die Verantwortung für die Sicherheit der Daten und Anwendungen in der Cloud kann nicht auf den Cloud Service Provider übertragen werden, sondern liegt weiterhin beim Anwenderunternehmen. Das heißt: Das Anwenderunternehmen muss Sorge dafür tragen, dass auch in Multi- und Hybrid-Cloud-Ansätzen einheitliche Regelwerke und Compliance-Richtlinien durchgesetzt werden. Erst wenn Sicherheit und Digitalisierung Hand in Hand gehen, ist der Weg für das zukünftige Geschäft frei.

Der Weg in die Cloud

Noch vor zehn Jahren war das Standardmodell für die Erbringung von IT-Leistungen die traditionelle serverbasierte Infrastruktur. Diese Infrastrukturen residierten physisch in Rechenzentren, die teilweise in eigener Hand waren oder im Outsourcing betrieben wurden.

Mit der Cloud löst sich die traditionelle Zuordnung von IT-Diensten zu spezifischer Hardware in kontrollierten Umgebungen auf. IT-Services werden im besten Sinne virtualisiert und unabhängig von der Infrastruktur. Servicebasierte integrierte Architekturen entstehen. IT wird as a Service genutzt.

Ein Entwicklungspfad hin zu cloud-nativen Architekturen und Services umfasst typischerweise verschiedene Zwischenschritte: Am Anfang stehen Lift & Shift-Ansätze, mit denen existente Workloads vom Rechenzentrum bzw. von On-Premise-Umgebungen migriert werden. Die Kosten für das Infrastrukturmanagement reduzieren sich, das Unternehmen erzielt mit der Migration erste Skalierungsoptionen. Im nächsten Schritt versuchen Unternehmen, die Time to Market zu reduzieren. Entwicklungszyklen von business-unterstützenden Applikationen werden durch den Einsatz von Cloud Services jenseits von Compute und Storage beschleunigt, beispielweise durch den Einsatz von Plattform-Diensten und Entwicklungswerkzeugen. Dabei kommen auch vereinzelt „serverless“ Designs zum Einsatz.

Mit der Re-Architect-Phase wird der Betrieb in einem dynamischen Umfeld vereinfacht. Schnelle Entwicklungszyklen werden unterstützt. Microservices, Container und „serverless“ Architekturen werden zum Standard. Damit ist die Grundlage für DevOps gelegt, eine agile Kultur, die Entwicklung und Betrieb von Software ganzheitlich und integriert lebt. Derartige Unternehmen releasen ihre Applikationen in schnellen Zyklen – bis hin zu mehrmals täglich.

Die Beschleunigung der Applikationsentwicklung erfordert den Einsatz von Ressourcen, die nicht komplett unter eigener Kontrolle stehen. Die Cloud als Zusammenarbeitsmodell fordert ein hohes Maß an Vertrauen in die Service-bereitstellenden Unternehmen – hin zu einem Shared-Responsibility-Modell. Die Nutzung cloud-nativer Ansätze bedeutet einen Paradigmenwechsel auch für den Umgang mit Sicherheit. In der Vergangenheit waren die Komponenten eines Service entlang ihres kompletten Lebens-zyklus bekannt, deren Beiträge nachvollziehbar. Mit der cloud-nativen Welt verteilen sich Verantwortung und Expertise auf viele Schultern. In dem Maße, wie sich die IT-Plattformen wandeln, sorgt der Wechsel hin zur Cloud-Architektur für eine andere Bedrohungslage.

Erschwerend kommt hinzu, dass durch die Digitalisierung Unternehmensprozesse intensiver mit IT verknüpft werden. Der Stellenwert, die Bedeutung, von IT steigt, während die Kontrolle über sie sinkt. Die Kombination dieser beiden Entwicklungen wirkt sich synergetisch auf das Risikopotenzial aus. Gleichzeitig bleiben Anwenderunternehmen für die Sicherheit von Daten und Anwendungen verantwortlich. Die Nutzung der Cloud erzeugt neue Herausforderungen in puncto Sicherheit – die als Zusatzanforderungen auf die existenten Herausforderungen „on top“ kommen.

Neue Sicherheitsherausforderungen im Zuge der Cloud-Transformation

Es sind im Wesentlichen drei Parameter, die die neue Bedrohungslage durch die Cloud kennzeichnen:

1. Exponierte Lage

Der klassische Perimeter hat ausgedient. Mit der Cloud verschiebt sich die Außengrenze des Unternehmens – und niemand kann sagen, wohin genau. Die Vorteile der Bereitstellung von Services aus der Cloud, (Bequemlichkeit des Teilens von Daten, reduzierte Reaktionszeiten, öffentliche Erreichbarkeit von Services) erzeugen neue Risikopotenziale: Zum einen können Angreifer per se die öffentlich zugänglichen Infrastrukturen erreichen, zum anderen können Daten leicht unbeabsichtigt veröffentlicht werden. Über menschliches Fehlverhalten hinaus erlauben APIs auch ungewollte nicht-humane Kommunikation, durch die Daten ungewollt abfließen können. Cloud-Architekturen fordern daher von Sicherheitsverantwortlichen, dass jede Anwendung ihren eigenen „Perimeterschutz“ erhält. Eine umfangreiche Aufgabe.

2. Cloud Technologie und Governance

Das Teilen von Ressourcen ist in der Cloud üblich. Die eingesetzten Plattformen sind hochentwickelt und entsprechend komplex, damit sie Nutzern hohe Skalierbarkeit und die geforderten Geschwindigkeiten bereitstellen können. Auf die Art der Bereitstellung haben Nutzer nur minimalen Einfluss. Typische Probleme, die in solch komplexen Umgebungen entstehen, sind Fehler durch komplexe IAM-Strukturen oder Isolationsfehler zwischen verschiedenen Tenants. Die mangelnde Transparenz macht das Durchsetzen der hausintern geltenden Compliance schwierig, z.B. Regionsvorgaben, Datenschutzklassen oder Kennwort-Richtlinien. Zudem besteht die Gefahr, dass Nutzer „ungehärtete“ Betriebssystem- und Applikations-Images einsetzen, wodurch ungewollt Angriffspotenziale entstehen.
Doch der Agilitätsgewinn durch die Cloud wirft noch eine weitere Fragestellung auf: Unternehmen, die im agilen Modus häufig und schnell Updates für Applikationen ausrollen, müssen auch entsprechend schnelle Sicherheitsmechanismen etablieren. Bewährte Prozesse und Technologien für Sicherheit können diese Agilität nicht mitgehen. Es entsteht eine Lücke zwischen der technischen Machbarkeit hinsichtlich Applikationsentwicklung und -deployment auf der einen Seite und dem Gewährleisten eines adäquaten Sicherheitsniveaus auf der anderen Seite. Auf gut Deutsch: Die Sicherheit von Applikationen wird durch das immense Tempo von Entwicklung und Rollout abgehängt.

3. Vertrauen in den Cloud Service Provider

Shared responsibility lautet die Maxime innerhalb der Cloud – die Anwender sind (beim Einsatz eines IaaS) verantwortlich für ihre Applikation und die Daten, die sie in der Cloud betreiben. Der Cloud Provider übernimmt die Verantwortung für die Sicherheit der Plattform an sich – bis zu der Grenze, die das entsprechende Service-Modell vorgibt. Die Leistung des Cloud Service Providers erscheint bis zu dieser Grenze als „Black Box“ – der Anwender hat nur Transparenz jenseits der Grenzen der Black Box, in seiner Einflusssphäre. Er erhält also keine Einblicke darin, welche Schwachstellen die genutzten Cloud-Lösungen aufweisen – allzumal wenn er sich in komplexen Umgebungen bewegt. Darüber hinaus hat der Cloud Service Provider potenziell Zugriff auf die in seinen Rechenzentren stehenden Cloud-Ressourcen, ohne dass der Anwender dies bemerkt. Das umfasst die Hardware (z.B. Memory Dump, Storage Dump, Network Sniffing), die eingesetzten Cloud Management Tools und die APIs. Letztere können beispielsweise inoffizielle Backdoors aufweisen, die nur der Cloud Provider kennt.

Für viele Anwender ist die Cloud-Welt neu und muss erlernt werden – auch und besonders in puncto Sicherheit. Die Cloud Service Provider verlangen von ihren Anwendern, dass sie ganz im Sinne der Shared Responsibility ihren Anteil leisten, um Applikationen und Daten in der Cloud zu schützen. Doch noch ist diese Cloud-Sicherheitsexpertise nicht überall vorhanden. Gartner erwartet, dass bis 2025 99 Prozent aller Fehler in der Cloud von Anwendern verursacht werden[2]. Sicherheitsverantwortliche in den Anwenderunternehmen sollten daher mit eigenen Sicherheitsmechanismen vorsorgen.
Die Herausforderung der Cloud Security verschärft sich dadurch, dass Unternehmen in der Regel nicht „die eine“ Cloud nutzen, sondern dass Multi-Cloud-Ansätze mittlerweile gang und gäbe sind. D.h. Anwenderunternehmen müssen Sicherheitsexpertise für verschiedene Cloud-Architekturen vorhalten.

Umfassende Cloud-Security-Strategie

Unternehmen, die die Cloud auch vor dem Hintergrund von Sicherheitserwägungen optimal einsetzen wollen, müssen vier Aspekte bei der Etablierung einer umfassenden Cloud-Security-Strategie berücksichtigen:

1. Grundlegend auf der **strategischen Ebene** sind Konzepte für Risikomanagement, Business Continuity Management und eine langfristige Planung des System Development Lifecycle. Ebenfalls wichtig ist das Design passender Metriken für die Cloud Security.

2. Auf der **Ebene der Prozesse** müssen Schwachstellen identifiziert und ein Compliance Management etabliert werden. Dieses umfasst u.a. Cloud Incident Response, die Einbindung von Sicherheits-fragestellungen innerhalb der DevOps-Ansätze und ein proaktives Cloud Threat Modelling.

3. Eine Auseinandersetzung mit **Cloud-Architekturen** ist eine weitere wichtige Komponente der Cloud-Security-Strategie. Neben der Kenntnis der Spezifika der verschiedenen Service-Modelle (IaaS, PaaS und SaaS) müssen gerade bei Cloud-Migrationsvorhaben wie Lift & Shift oder Re-Architect Sicherheitsaspekte integriert werden.

4. Der richtige Einsatz der passenden **Tools und Technologien** muss dieses Rahmenwerk flankieren. Dabei müssen zunächst die von Cloud Service Providern bereitgestellten nativen Sicherheitslösungen adäquat eingesetzt werden. Bestehende Lücken lassen sich mit zusätzlichen Sicherheitslösungen spezialisierter Hersteller schließen, insbesondere bei Herausforderungen im Multi- und Hybrid-Cloud-Umfeld. Zuletzt sollten Cloud-Anwender auch Machine-Learning-Mechanismen und automatisierte Response vorsehen.

Abb. 1: Individuelle und umfassende Cloud-Security-Strategie

Auf dieser Basis entstehen wesentliche Errungenschaften, die dazu beitragen, dass eine effiziente Cloud Security gebaut werden kann. Zunächst gewinnen Anwender Transparenz über ihre Daten. Sie wissen, wo welche Daten sind, wer und welche Anwendung sie verarbeitet und wohin sich Daten bewegen. Sicherheitsdefizite in der eigenen Organisation werden erkannt und können durch passende Gegenmaßnahmen ausgeräumt werden. Insbesondere können Anwenderunternehmen damit auch abwägen, in welchen Feldern sie notwendige Expertise durch passende Partnerschaften mit Sicherheitsexperten ergänzen sollten. T-Systems kann Ratsuchende in diesem Umfeld unterstützen.

Cloud Security: Kombination etablierter Mechanismen und neuer Werkzeuge

Die gute Nachricht ist: Für die neuen Herausforderungen an die Sicherheit im Umgang mit der Cloud gibt es bereits heute passende Lösungen.

Zwei Momente machen Sicherheit in der Cloud komplex: Zum einen die agilen Ansätze für Applikationsentwicklung und -bereitstellung, zum anderen die entstehenden Multi-Cloud-Landschaften. Kopfzerbrechen bereitet vielen Unternehmen, dass der Multi-Cloud-Einsatz nicht geplant entsteht. Nicht jeder Zugriff auf Ressourcen von Hyperscalern erfolgt auf offiziellem Weg. Es ist kein Geheimnis, dass die einfache Verfügbarkeit von Cloud-Services der Schatten-IT den Weg gebahnt hat. Mit der Schatten-IT, die außerhalb der offiziellen IT-Governance genutzt wird, entstehen neue Sicherheits- und Compliance-Risiken.

Eine ganzheitliche Cloud-Security-Strategie umfasst bewährte Schutzmethoden und ergänzt diese durch cloud-spezifische Sicherheitsmechanismen. Viele Hersteller haben sich mit ihren Lösungen auf konkrete Sicherheitsaspekte fokussiert. Zu den etablierten Schutzmaßnahmen gehören die Überwachung des Netzverkehrs durch Firewalls der neuesten Generation. Virtuelle Next Generation Firewalls stellen die Intrusion Prevention sicher und schützen vor Advanced Persistent Threats. Fortgeschrittene Web Application Firewalls, die sich ebenfalls als virtualisierte Services bereitstellen lassen, erweitern diesen Basisschutz auf die Applikationsschicht. Weitere etablierte Technologien überwachen die Aktivitäten von Datenbanken.

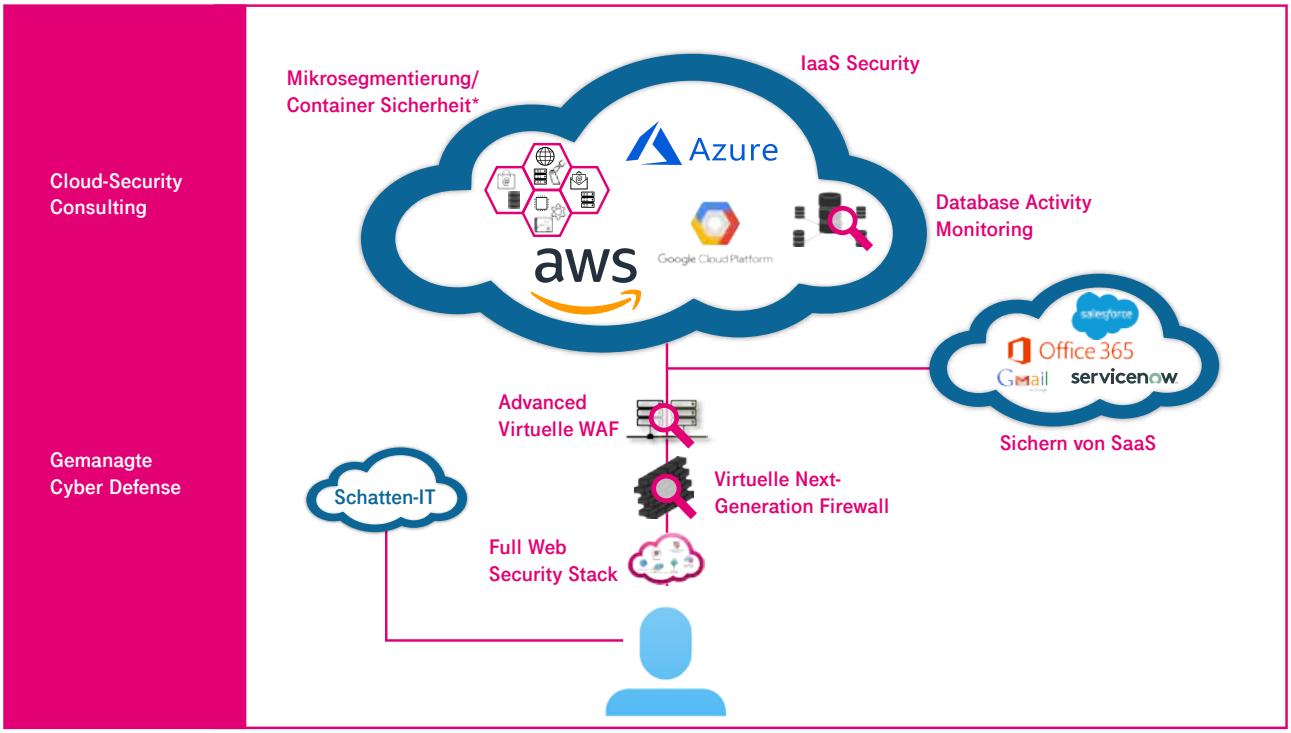

Abb. 2: Security für das Arbeiten in der Cloud-Ära

Spezifische Sicherheitslösungen für die Nutzung von Cloud Services – SaaS

Absicherung von SaaS

SaaS repräsentiert immer noch den Löwenanteil des Cloud-Marktes. SaaS richten sich speziell an Endnutzer und sind wegen ihrer einfachen Nutzung weit verbreitet. Speziell für die Nutzung von SaaS wie Salesforce oder Office 365 existieren Lösungen, die für den Malware- und Accountschutz eingesetzt werden können. Sie erlauben zudem die Verschlüsselung unstrukturierter Daten, bieten Funktionen für Data Loss Prevention und überwachen die Einhaltung regulatorischer Vorgaben.

Umfassende Lösungen (Full Web Security Stacks) integrieren verschiedene Sicherheitsmechanismen wie Virenschutz, Advanced Threat Protection, Web Security, Content/URL-Filtering und Firewalls als Komplettservice. Die Bereitstellung aus der Cloud hat den großen Vorteil, dass die Lösung direkt vor Ort – wo Cloud-Dienste produziert werden – jene überwachen kann. Das bringt den Nutzern der Cloud Services eine verbesserte User Experience gegenüber zentral bereitgestellten Lösungen, die im Corporate Network vorgehalten werden.

Beispiel: Internet Protect Pro bei einem Maschinenbauer

Für neue Niederlassungen und einen wachsenden Mitarbeiterstamm nutzt der Maschinenbauer mit Googles G Suite aus der Public Cloud eine skalierbare Office-Lösung. Sie ist ortsunabhängig via Internet verfügbar und unterstützt das dynamische Wachstum des Unternehmens effizient. Doch Office-Systeme via Internet – das reicht im Enterprise-Umfeld in puncto Sicherheit nicht aus. Das Unternehmen setzte bislang auf eine zentrale Firewall im zentralen Rechenzentrum, die jeglicher Internet-Datenverkehr passieren muss. Die Security-Lösung passt damit nicht optimal zu der flexiblen Office-Lösung: Durch die Sicherheitsarchitektur entstehen hohe Laufzeiten für die Nutzung der Applikationen. Diese führen vor allem an entfernten Standorten des international agierenden Unternehmens zu einer schlechten User Experience.

Der Maschinenbauer entschloss sich, den zentralen Ansatz durch einen dezentralen abzulösen. Das MPLS-Netzwerk, wird nach wie vor für die businesskritischen Applikationen genutzt. Die Niederlassungen erhalten aber zusätzlich eigene Router, die ihnen einen direkten Internet-Breakout erlauben. Sie geben den Landesgesellschaften einen direkten Zugriff auf die Rechenzentren, aus denen die Office-Dienste bereitgestellt werden.

Doch wie sollte in dieser neuen Architektur eine angemessene Sicherheit gewährleistet werden? Eine Investition in neue Sicherheits-Hardware an den Standorten kam nicht in Frage. Der Maschinenbauer bezieht seine Sicherheit nun „as a Service“ aus der Cloud über Internet Protect Pro powered by Zscaler. Zscaler betreibt seine Sicherheitslösung als Cloud-Dienst in verschiedenen Rechenzentren der Welt. Der Datenverkehr der Office-Anwendungen läuft zunächst über die Sicherheitsfunktionen von Zscaler, bevor er auf die G Suite zugreift. Internet Protect Pro schützt den jeweiligen lokalen Internetzugang auf Basis eines mehrschichtigen Security-Konzepts.

Spezifische Sicherheitslösungen für die Nutzung von Cloud Services – IaaS, PaaS

Weitere spezielle Sicherheitslösungen für den Einsatz von Cloud Services im Unternehmen richten sich speziell an Entwickler, die IaaS-Ressourcen nutzen oder cloud-native Applikationen mit Containern entwickeln. Cloud-Nativität kennzeichnet einen der maßgeblichen Trends in der IT-Branche.

2021, so eine Prognose von IDC[3]**,** werden sich Applikationen in Richtung cloud-nativer, hyperagiler Architekturen bewegen. 80 Prozent der Entwicklungsarbeit erfolgen dann auf PaaS mithilfe von Microservices und Cloud-Funktionen. 95 Prozent aller neuen Applikationen werden in Containern deployed.

Die Cloud-Native Computing Foundation definiert „cloud-nativ" als Applikationen, die einen Open-Source-Software-Stack nutzen, um Applikationen als Microservices zu deployen. Die Teile werden in einzelne Container gepackt, die dynamisch orchestriert werden, um eine optimale Ressourcenauslastung zu erzielen.
Dieses Vorgehen hat gegenüber dem Einsatz einfacher Cloud-VMs einige Vorteile:

- Schnelle Bereitstellung neuer Releases
- Einfaches Management
- Reduzierte Kosten
- Höhere Zuverlässigkeit des Service
- Vermeidung eines Vendor Lock-in
- Unabhängigkeit von der Infrastruktur (cloud-native Applikationen können auch on-premises betrieben werden)

Cloud-nativ vereint also ein Bündel mehrerer moderner Technologien – über die Cloud hinaus: Container, Microservices und Orchestrierung. Der Trend hin zu cloud-nativen Ansätzen fordert auch Sicherheitsmechanismen, die diesen Weg mitgehen können.

Diese Sicherheitslösungen verfolgen prinzipiell zwei Ansätze: eine Sorte von Lösungen fokussiert Compliance-Fragen. Mithilfe dieser Lösungen werden zentral Policies für die Sicherheit der entwickelten Anwendungen vorgegeben und über die genutzten Tenants in den eingesetzten Public Clouds überwacht. D.h. die Lösung kontrolliert, ob die entwickelten Microservices, Instanzen und Workloads entsprechend der vorgegebenen Policies arbeiten und alarmiert das Sicherheitsteam, falls sie Abweichungen feststellt.

Zentrale Policies für die Multi-Cloud einführen

Eine typische Policy könnte beispielsweise vorsehen, dass Daten im S3 Object Storage von Amazon Web Services (AWS) grundsätzlich verschlüsselt werden müssen. AWS stellt diese Sicherheitsfunktionalität als Plattformdienst bereit. Vergisst ein Entwickler, die Verschlüsselung bei einem Update seiner Anwendung zu implementieren, stellt die Sicherheitslösung dies automatisch fest und benachrichtigt das Sicherheitsteam, so dass eine sofortige Korrektur des Fehlers erfolgen kann. Fortgeschrittene Tools können falsche Einstellungen nicht nur identifizieren, sondern auch automatisch beheben (Automated Remediation). Das Elegante an dieser IaaS-Security-Lösung: Dieselbe Policy lässt sich – einmal etabliert – auf verschiedene Tenants in verschiedenen Public Clouds automatisch anwenden. D.h. eine Compliance-Kontrolle kann auch dann erfolgen, wenn der gesamte Service oder bestimmte Microservices in die Google Cloud, zu Azure oder in die Open Telekom Cloud verschoben werden. Ähnliche Policies können auch für die Ablage von Daten eingestellt werden, bspw. um die EU-DSGVO-Konformität zu gewährleisten. Die Policies sind zentral nach Richtlinien wie HIPAA, DSGVO oder Best Practice vordefiniert und können "out of the box" auf verschiedene Clouds angewendet werden. Für spezielle Anforderungen können individuelle Policies mit einem Policies-Generator geschrieben werden. Die Compliance-Überwachung verschafft insbesondere Unternehmen, die Applikationen von Dritten entwickeln und bereitstellen lassen, eine Möglichkeit zu überwachen, ob die Anwendungen entsprechend der Vorgaben designt wurden.

Den Container-Einsatz kontrollieren

Wie bereits beschrieben, sind Container einer der essenziellen Bestandteile cloud-nativer Ansätze. Sie bieten den Entwicklern ein Höchstmaß an Flexibilität. Die Überwachung der Container-Container-Kommunikation ist eine typische neue Herausforderung

für die Sicherheitsteams in den Anwenderunternehmen. Die Flexibilität der Container verschafft aber andererseits auch Angreifern einen großen Vorteil: Sie können die Container-Architektur ausnutzen. Der Angreifer nutzt eine Schwachstelle innerhalb einer Container-Umgebung und kann sich ohne entsprechenden Schutz innerhalb des Containers bewegen (Ost-/Westverkehr bzw. Lateral Movement), um so an relevante Daten zu gelangen.

In einem typischen Angriffsszenario kapert ein Angreifer einen Container, der eine öffentlich verfügbare Webseiten-Funktionalität bereitstellt. Von dort aus kann er via Container-Container-Kommunikation auf die im Backend liegende Kundendatenbank zugreifen.

Die Mikrosegmentierung ist eines der effizientesten und kostengünstigsten Verfahren, um derartige Angriffe zu unterbinden. Im Zuge der Mikrosegmentierung werden „erlaubte" Kommunikationspfade zwischen verschiedenen Teilservices festgelegt, die sich auf Container oder Container-Gruppen verteilen können. Über dieses so genannte Whitelisting erfolgt eine kontinuierliche Kontrolle der Container-Container-Kommunikation. Stellt das Tool fest, dass Container sich nicht entsprechend der Regeln verhalten, wird die Kommunikation blockiert. Im skizzierten Beispiel kann beispielsweise die (vorgesehene) Kommunikation der Webseite auf die Preisliste erlaubt werden; die weitere Kommunikation auf schützenswerte Daten im Backend aber kann verboten werden. Damit kommt der Angreifer nur auf die Preisliste, aber nicht auf die im Unternehmenssinne schützenswerten Kundendaten. Die Mikrosegmentierung erlaubt so die Einführung von Zero-Trust-Umgebungen. Ein weiterer Vorteil der Mikrosegmentierung liegt darin, dass sie software-basiert ist. Sie kann dynamisch aufgebaut werden, so dass das Regelwerk applikationszentrisch sogar bei einem Umzug der Anwendung mitwandern kann.

Zudem können derartige Ansätze auch kontrollieren, ob Entwickler beim Design von Containern auf gehärtete, d.h. sicherheitsgeprüfte, Images zurückgreifen. Die Überprüfung fordert vom Entwickler nur minimalen Aufwand. Sie erfolgt über Plug-ins in alle gängigen Entwickler-Tools. Das Sicherheitsteam kann damit schon auf einer sehr frühen Ebene mögliche Sicherheitsrisiken eindämmen. Schwachstellen-Scans bereits aktiver Container bzw. Container-Images erfolgen am besten auf der Ebene der Container Registries. Damit können auch im laufenden Betrieb neue Schwachstellen oder Security Alerts identifiziert werden. Aktive, verwundbare Container werden dann über Redeployments gepatcht. Mit diesen Lösungen wird der komplette Lebenszyklus eines Containers auf verschiedenen Plattformen übergreifend geschützt.

Fazit

Die Digitalisierung forciert den Einsatz von Clouds und cloud-nativen Methoden, damit Unternehmen in einem verschärften Wettbewerbsumfeld bestehen können. Doch dieser Paradigmenwechsel von der klassischen IT-Bereitstellung hin zu hoch-agilen Ansätzen fordert die Sicherheitsverantwortlichen in Unternehmen heraus. Sie stehen vor einer völlig neuen Situation – etablierte Sicherheitstools und -Verfahren haben in der agilen Cloud-Welt nur noch begrenzte Wirkung. Sie müssen neue Sicherheitslösungen finden, die mit der agilen Applikationsbereitstellung und Cloud-Nutzung Schritt halten können. Bereits heute sind am Markt verschiedene spezielle Lösungen verfügbar, die einzelne Aspekte der Cloud-Nutzung mit wirksamen Sicherheitsmechanismen unterstützen können. Doch im Einzelfall müssen Unternehmen genau prüfen, welche die für sie richtige Lösung ist. Cloud Security ist aber mehr als nur die Implementierung von spezifischen Sicherheitslösungen. Bereits beim Design der Cloud-Lösungen müssen alle Security-Aspekte ganzheitlich betrachtet werden. Dazu gehören die Architektur, Benutzer-, Rollen- und Berechtigungsverwaltung, Kommunikationsregeln, Einsatz von Verschlüsselung und zugehörigem Key Management, Überwachung und (automatisierte) Remediation. Der Austausch mit einem erfahrenen Security Provider kann helfen, eine ganzheitliche, effiziente und plattformunabhängige Security-Strategie für die Cloud-Welt zu entwickeln.

T-Systems als einer der führenden europäischen Dienstleister verfügt über ein ganzheitliches Security-Portfolio. T-Systems kann Anwenderunternehmen bei ihrem Weg in die Cloud auf zwei Ebenen unterstützen:

Wir definieren mit Ihnen gemeinsam Ihre Cloud-Sicherheits-strategie, identifizieren Lücken und finden passende Lösungen, um die Lücken zu schließen und das Unternehmen optimal auf die Cloud-Welt vorzubereiten. Im zweiten Schritt können wir Ihnen helfen, die entsprechenden Lösungen zu implementieren und auf Wunsch kontinuierlich zu betreiben.

Quellenangaben:
[1] "Cloud-Nutzung auf Rekordniveau bei Unternehmen", Umfrage von Bitkom Research im Auftrag der KPMG AG
[2] "Is the Cloud secure?", Gartner, Oct. 2019
[3] IDC FutureScape: Worldwide IT Industry 2018 Predictions, 2017
[4] "State of the Developer Nation 16th Edition – Q4 2018", Developer Economics, Slashdata, April 2019

Expertenkontakt

Andreas Pecka
Head of International Expert Sales & Presales Cyber Security
a.pecka@t-systems.com

Herausgeber

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Deutschland
E-Mail: cyber.security@t-systems. com
Internet: www.t-systems.com

T Systems Let's power higher performance