SHE Immer eine IT voraus.

Cloud, aber sicher!

Security-Herausforderungen in hybriden Szenarien meistern

Autor: SHE Informationstechnologie AG

September 2020

SHE Informationstechnologie AG
Bereich: IT-Security
Donnersbergweg 3 | 67059 Ludwigshafen | Germany
T+49 621 5200-150
E-Mail: daniel.dogan@she.net

Inhaltsverzeichnis

Cloud, aber sicher?

An Hybrid-Cloud-Infrastrukturen geht bei der Umsetzung der Digitalisierungsvorhaben kein Weg vorbei. Diese bringen neue und zusätzliche Anforderungen an die Security mit sich. Welche sind das und wie sollten Unternehmen sich ihnen stellen?

Workloads verlagern sich immer stärker in hybride Clouds. Das bestätigen auch die US-Marktforscher von Vanson Bourne. Sie haben im Auftrag des kalifornischen Anbieters von Datacenter-Lösungen Nutanix per Umfrage unter weltweit 2.300 IT-Entscheidern den Enterprise Cloud Index erstellt.

- In Deutschland nutzen demnach heute gut 20 Prozent der Befragten Hybrid-Cloud-Infrastrukturen für ihr Computing;
- in zwei Jahren soll sich dieser Wert mehr als verdoppeln.
- Traditionelle On-premise- und reine Private-Cloud-Szenarien sind dagegen dem Index zufolge deutlich auf dem Rückzug.
- Das trifft auch für Nutzungsszenarien in einer einzigen Public Cloud zu,
- während Anbieter-Mischungen (Multiple Public Clouds) für die CxOs und RZ-Chefs wichtiger werden sollen.

Das Institut für Management und Innovation an der Hochschule für Wirtschaft und Gesellschaft Ludwigshafen hat im SHE-Auftrag aktuelle IT-Fachpublikationen ausgewertet. Die Ergebnisse stützen die Nutanix-Prognose: Hybride Cloud-Infrastrukturen werden von einer Reihe von Autoren, etwa Forbes und Accenture, als Zukunft von Big Data und der Digitalisierung bezeichnet. Und das Thema Security werde weiterhin „von herausragender Bedeutung“ sein.
Sicher ist: Das Management von Hybrid Clouds entwickelt sich zu einer Standardaufgabe für immer mehr IT-Verantwortliche und –Abteilungen. Das umfasst die Security – zwingend.

Hybrid-Cloud-Security: die neue Standardaufgabe in drei Schichten

Ordnet man die damit zusammenhängenden Herausforderungen in einer dreischichtigen Pyramide an, bildet die unterste Ebene an traditionelle Aufgaben angelehnte Herausforderungen – in Hybrid-Szenarien zum Teil von kritischer Bedeutung als beim On-premise-Betrieb. Das beginnt mit der Zugangskontrolle – nicht einfach mit Benutzernamen und Passwort, sondern durch Multifaktor-Authentisierung, damit etwa sichergestellt werden kann, dass nur registrierte Geräte zugreifen. Dazu kommt die Gewährleistung der Datensicherheit: Werden Daten in der Cloud abgelegt, ist das Risiko, dass Versäumnisse bei der Verschlüsselung fatal wirken, viel höher. Drittens der Zugang zur Cloud in hybriden Szenarien abzusichern: zwischen eigenem RZ und Public Cloud traditionell über VPN oder Direct-Access, darüber hinaus mithilfe einer Cloud-Connect-Lösung.

In der mittleren Schicht der Pyramide stellt die Innovationsdynamik, mit der sich Technologieprovider wie Microsoft (Azure) oder Amazon (AWS) vom Wettbewerb abzuheben trachten, eine enorme Herausforderung dar. Fest steht: So neu wie die Technologie, so überschaubar ist die Erfahrung damit. Die Konfigurationsmasken der Public-Cloud-Angebote sind so komplex und verändern sich so schnell, dass Effekte auf die Security oft kaum vorauszusagen sind. Solche Risiken lassen sich nur beherrschen, wenn man mit sich dynamisch anpassenden Checklisten alle Eventualitäten abprüft – idealerweise nach dem Vier-Augen-Prinzip, wie zwischen Pilot und Co-Pilot vor dem Start.

Innovationsdynamik erfordert neue Ansätze

Betrachtet man zusätzlich die Innovationen der Security-Lösungsanbieter, stellt man fest: „Lift and Shift“ greift zu kurz. Das einfache Übertragen von Security-Maßnahmen, die klassisch auf Firewalls basieren, in die Cloud ist nicht sinnvoll, wie die Erfahrung zeigt. So können etwa Umschaltprozesse zwischen unterschiedlichen Clustern zu Verzögerungen und erheblichen Performanceverlusten führen. Firewall-Anbieter haben das erkannt und reagieren. So hat sich etwa Checkpoint mit der Akquise des Unternehmens Dome9 spezielle Kompetenz in Sachen Cloud-Security, deren Visualisierung und Compliance-Checks ins Haus geholt. Und mit der Cloudguard-Suite verspricht Checkpoint verstärkten Schutz für Software-Anwendungen in der Cloud (SaaS), zum Beispiel durch Autoscaling. Dabei wird bei steigender Last auf dem Application Server die Leistung der Firewalls automatisch

angepasst. Auch die automatische Abwehr von offenbar unrechtmäßigen Login-Versuchen – etwa mit gleicher Kennung binnen kurzer Frist aus unterschiedlichen Regionen – erfüllt Cloud-spezifische Anforderungen.

DevSecOps: Entwickler müssen Security mitdenken

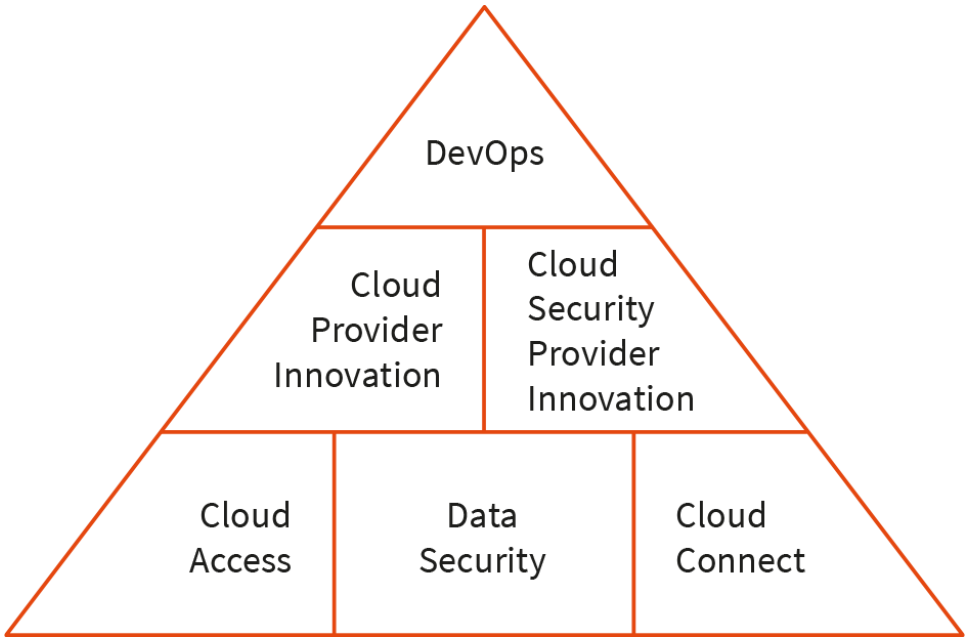
An der Spitze der Pyramide steht DevOps. In diesem Paradigma werden im Wesentlichen – auf agile Weise – die Anwendungen umgesetzt, die für die digitale Transformation von Geschäftsprozessen und Unternehmen stehen. Dabei geht es auch um Geschwindigkeit: so schaffte ein SHE-Team zum Beispiel in den ersten acht Monaten 2018 für den Kunden 48 Releases live zu schalten, wo früher höchstens eines pro Monat released wurde.
Was das Business zu schätzen weiß, weil es eine hohe Innovationsgeschwindigkeit mit sich bringt, lässt bei Security-Verantwortlichen die Alarmglocken schrillen. Da ist es umso wichtiger, dass das neue Paradigma mit einem technischen Ansatz realisiert wird, der auf das Konto „Sicherheit“ einzahlt: Containerisierung, beispielsweise mit Docker-Technologie. Die bewirkt, dass sich aus Infrastruktursicht bei einem neuen Release nichts ändert, denn der Container bleibt in seinen äußeren Eigenschaften gleich.

Die Änderungen finden im Container selbst statt, als Bestandteil der Softwareentwicklung. Die Folge, wenn das funktioniert, ist „Security by Design“ – eine traditionelle Idealvorstellung von konzeptionell sicheren Produkten, die nicht mit hohem Aufwand nachträglich „gehärtet“ werden müssen.

Diese Lösung birgt freilich gleichzeitig eine Herausforderung, denn Entwicklungsteams brauchen nun solides Security-Wissen. Dieses klassisch „beizubringen“ funktioniert nicht, denn die Entwickler sind tendenziell derart überlastet, dass dafür kaum Zeit dafür ist. Außerdem: Erfahrung kann man nicht durch Schulung kompensieren. Die Lösung lautet: Security-Know-how muss in die Teams integriert werden.

Fazit

Werden Teile der Zuständigkeit für eine sichere Infrastruktur an Entwickler übertragen, folgen Konsequenzen für die Führung und die Organisation. SHE darf von sich behaupten, hier gut positioniert zu sein, denn hier sind schon immer Entwicklung, Betrieb und Infrastruktur unter einem Dach angesiedelt. Was Hybrid-Cloud-Security angeht, heißt das: Kompetenz in allen drei Schichten der Pyramide.



1 Referenzmodell Cloud-Security Pyramide: Analogien zur klassischen Security-Welt (unten), Besonderheiten in Cloud-Umgebungen (Mitte), DevOps an der Spitze

Über SHE

Wir sind die Macher der Digitalisierung

Mit über 200 Mitarbeitern in Deutschland und in Cluj (Rumänien) unterstützt SHE Unternehmen bei der Umsetzung ihrer Digitalisierungsstrategie.

Wir sind Experten für Konzeption, Umsetzung und Betrieb innovativer IT-Anwendungen und sicherer IT-Infrastrukturen (Security / Cloud & Infrastructure).

Die kurzfristige und pragmatische Bereitstellung moderner Arbeitsplätze (Digital Workspace) ermöglicht Unternehmen nachhaltig kostengünstig und flexibel zu arbeiten, was sich gerade anlässlich der Covid-19-Pandemie bewährt hat. Unsere Software-Entwicklungs-Teams im EU-Land Rumänien (Agile Nearshoring) helfen IT-Kosten zu senken und anspruchsvolle Herausforderungen umzusetzen. Wir beschaffen Software-Lizenzen, Hardware und Wartungsverträge zu attraktiven Konditionen. Mit der Realisierung von überzeugenden digitalen Kundenerfahrungen (Digital Customer Experience) fokussieren wir uns darauf, was im Mittelpunkt moderner Digitalisierungsstrategien steht: die Kunden unserer Kunden.

Unternehmenskontakt

Daniel Dogan	SHE Informationstechnologie AG
Teamleiter Cyber Security	Donnersbergweg 3
+49 621 5200-150	67059 Ludwigshafen
daniel.dogan@she.net	https://www.she.net