Cloud-Security – Herausforderungen und ihre Lösungen

Ab in die Cloud

„Alles in die Cloud", so lautet das Paradigma vieler Unternehmen. Welche Probleme dabei auftreten können, nicht nur in Bezug auf Sicherheitsanforderungen, und wie verschiedene Anbietermodelle hierauf eingehen, erläutert der folgende Beitrag.

Von Sönke Freitag, Consist Software Solutions GmbH

Die Vorteile niedrigerer Betriebskosten, geringerer Kapitalbindung für Hardware und kleinerem Personalaufwand bei gleichzeitig verbesserter Ausfallsicherheit leiten viele Unternehmen in ihrer Entscheidung für die Cloud. Meist werden hierbei per „Lift and Shift" Applikationen von On-Prem-Umgebungen in die virtuelle Cloud geschoben. Ein Re-Design erfolgt sporadisch und oftmals dauert dieser Prozess deutlich länger als geplant. Insbesondere Probleme der Nebenläufigkeit von Microservices und der benötigte Kommunikationsaufwand werden zumeist unterschätzt. Aber auch die neuen Herausforderungen an die IT-Security und regulatorische Anforderungen sind häufig nicht vollumfänglich Teil der anfänglichen Betrachtungen.

Viele Hersteller bemühen sich mit ihren Produkten die vielfältigen Sicherheitsanforderungen abzudecken. Hierbei gibt es sowohl Software-as-a-Service-(SaaS)-Provider, Infrastructure-as-a-Service (IaaS) als auch klassische Anbietermodelle. Die folgende Betrachtung gibt einen Überblick über die Tools verschiedener Hersteller und Anbieter.

Verschlüsselung

Daten in der Cloud sollten verschlüsselt abgelegt werden – das hat nicht nur der CTO von Amazon bereits 2015 in einem Interview empfohlen, sondern vielfach wird dies auch in diversen Compliance-Anforderungs-Katalogen postuliert. Da die Daten in der Cloud innerhalb einer Struktur gehostet werden, die nicht im eigenen Hoheitsbereich steht, ist zudem eine Absicherung der Daten auch vor Insider-Angriffen, beispielsweise auf Backups und Containerimages notwendig.

Auf dem Weg in die Cloud stellen die wichtigsten Cloud-Anbieter über eine Transport Layer Security mit mindestens der Version TLS 1.2 einen gesicherten Zugang über die verschiedensten Protokolle bereit. Zusätzlich sollten aber auch alle selbst erstellten Kommunikationen zwischen einzelnen Containern oder Cloud-Komponenten (z. B. über REST-Schnittstellen oder Streaming-Systeme wie Kafka) stets verschlüsselt, authentisiert und signiert mit entsprechenden Gültigkeitszeiträumen erfolgen.

Amazon Web Services (AWS) bieten beispielsweise sowohl serverseitige (also von Amazon selbst durchgeführte) als auch clientseitige Verschlüsselungen mit CMK-Keys und auch mit eigenen Verfahren. Als eigene Verfahren kommen die klassischen Möglichkeiten der Transparent Drive Encryption (TDE) für Oracle- oder Microsoft-Datenbanken auf virtualisierten Servern in Betracht. Für Anwendungen, die auf Docker-Containern basieren, bieten Firmen wie Boxcryptor oder auch die Open-Source-Lösung Imgcrypt eine Docker Image Encryption.

Signierung

In Bereichen, in denen die Authentizität der Kommunikation nachzuweisen ist, bieten sich asymmetrische Public-Key-Verfahren im Rahmen einer Public-Key-Infrastruktur (PKI) an. Der internationale Markt der Anbieter hierfür ist sehr groß, beispielsweise mit Docusign und Globalsign. Deutsche Anbieter sind Postident, BV-Sign vom Bankverlag und D-Trust der Bundesdruckerei – letztere sind auch für den Zahlungsverkehr nach PSD2 zugelassen.

DDoS-Schutz

Dienstleister wie Cloudflare und Akamai versprechen hier, auch die größten DDoS-Angriffe abwehren zu können. Einige Cloud-Service-Provider, wie Google mit seiner Cloud Armor oder Amazon mit AWS Shield, bieten bereits ein eigenes Schutzsystem.

CASB

Um zu verhindern, dass in der Cloud Cryptomining stattfindet, sollte ein entsprechender Schutz implementiert sein. Cloud Access Security Broker (CASB) von Anbietern wie Cisco und Forcepoint sind Lösungen, die zwischen Cloud und Anwender geschaltet sind und solche Schutzfunktionen bieten.

Software Defined Perimeter Security

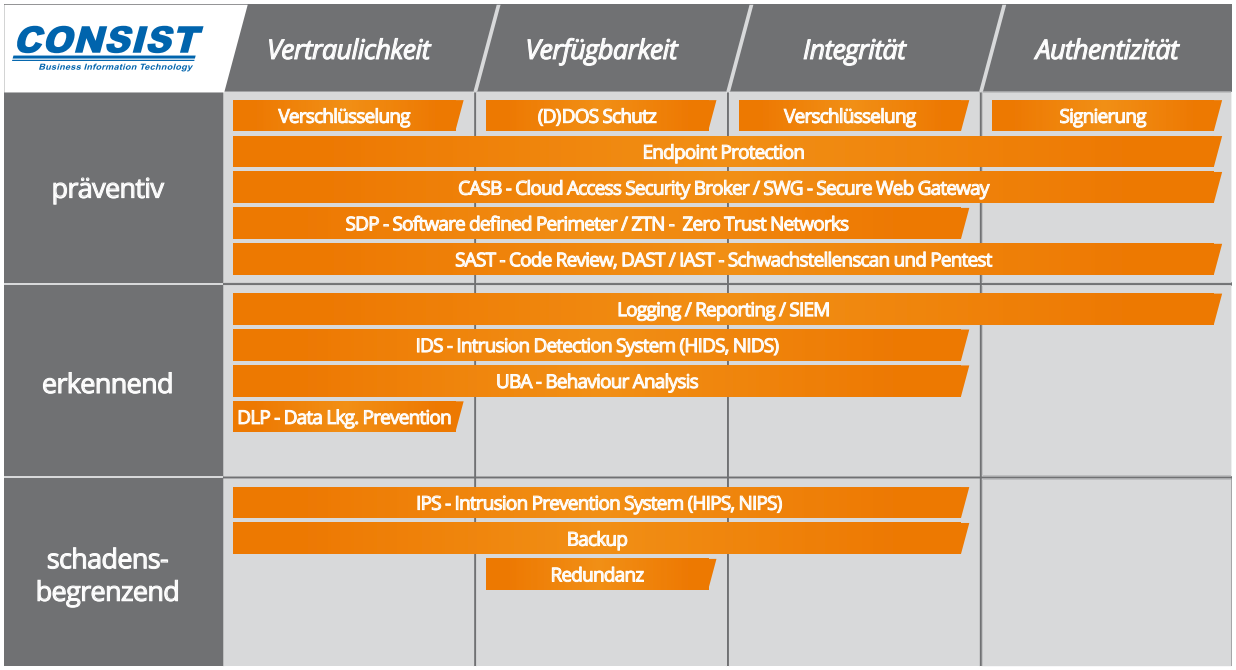
Cloud-Strukturen erlauben keine klaren Zonengrenzen. Vertrauenswürdige interne Zonen, wie bei On-Prem-Installationen üblich, oder feste IP-Adressen lassen sich kaum mehr festlegen. Im Rahmen des Software Defined Perimeter Projekts (SDP Zero Trust Netorks) der Cloud-Security Alliance (CSA) werden für Kommunikationsstrukturen genaue zulässige Pfade festgelegt, die zuerst eine Authentisierung vor dem Kommunikationsaufbau erfordern und sonst keine Kommunikation zulassen. Diese relativ neue Technik wird in unterschiedlichen Ausprägungen am Markt angeboten – Perimeter81, ZScaler, NetMotion, Illumo aber auch größere Hersteller wie Cisco und Fortigate bieten derartige Lösungen an, die klassische Perimeter-Firewalls ergänzen oder sogar ersetzen können.

Code Review, Schwachstellenscan und Pentest

Mit sicherheitsfokussierten Code Reviews (Static Application Security Testing, SAST) werden Schwachstellen in der Verarbeitung von Daten durch eigene Programme im Quellcode aufgedeckt. Eine fehlerhafte Codierung könnte sonst beispielsweise einen SQL-Injection-Angriff oder CSRF- und XSS-Angriffe ermöglichen. Code Reviews erfolgen manuell oder (teil-)automatisiert mit Tools wie CheckmarX, SynopSys oder Veracode.

Dynamische Schwachstellenscans (Dynamic Application Security Testing, DAST), wie von den Marktführern Tenable, Qualys und Rapid7, bewerten die Funktion und Sicherheit des Systems aufgrund von generierten Abfragen, zum Beispiel auf Web-Oberflächen oder IP-Strukturen. Zusätzlich zu den in der Breite scannenden Tools gibt es auch auf bestimmte Anwendungstypen, beispielsweise für Web/Intranet, spezialisierte Unternehmen wie Acunetix oder Burp Suite.

Der klassische Pentest wird manuell ausgeführt, wobei sich der Pentester in die Rolle eines Angreifers versetzt, der versucht, das System zu korrumpieren. Ein Pentest ist nicht durch einen reinen Schwachstellenscan zu ersetzen. Die Einzigartigkeit jeder Installation und Anwendungsstruktur mit ihren jeweiligen Abhängigkeiten ist im Vorfeld nicht komplett durch automatische Tools abbildbar.



Sicherheitsanforderungen an die Cloud, Bild: Consist Software Solutions GmbH

Logging, Reporting und SIEM

Innerhalb der meisten hier besprochenen Sicherheitssysteme und auch von Seiten der Cloud-Anbieter werden Logdateien angeboten. Da es manuell kaum möglich ist, die verschiedenen Formate zu konsolidieren und bestimmte sicherheitsrelevante Vorgänge über diverse Sicherheitssysteme hinweg zu erkennen oder zu verfolgen, werden hierfür hochgradig flexible Logging-Systeme eingesetzt, die die verschiedenen Datenquellen vereinheitlichen und in einer schnell zugreifbaren Datenbank vorhalten.

Ein Sicherheitsinformations-Management-(SIEM)-System wie Splunk ES (Enterprise Security) verarbeitet die zugrundeliegenden Daten in der Cloud zu aussagekräftigen Informationen, die von einem Security Operations Center-(SOC)-Team weiterbearbeitet werden können. Als führende SIEM-Unternehmen identifiziert der Gartner-Report-2020 Splunk, IBM, ExaBeam und Securonix.

IDS und IPS

Intrusion-Detection-Systme (IDS) können sowohl hostbasiert (HIDS) als auch netzwerkbasiert (NIDS) agieren und sollen Einbrüche in die eigene Anwendungsstruktur entdecken. Anders als ein IDS beschränkt sich ein Intrusion-Prevention-System (IPS) nicht nur auf das Erkennen von Einbrüchen, sondern auch auf deren Verhinderung beziehungsweise die Schadensbegrenzung nach dessen Erkennung. Zumeist werden IDS/IPS-Systeme vom gleichen Hersteller bezogen und zusammen betrieben. Systeme kommerzieller Anbieter, wie Cisco FirePower, FireEye, Trend Micro TippingPoint, aber auch Public-Domain-Software, wie Suricata und Snort, finden sich hier am Markt.

UBA und DLP

User Behavior Analytics (UBA) wird meist als ein Plug-in für SIEM-Systeme wie SPLUNK ES angeboten und entdeckt ungewöhnliche User-Aktionen mit Methoden des Maschinenlernens. So können beispielsweise ungewöhnliche Häufungen von Transaktionsschritten oder ungewöhnliche Datenbewegungen schnell entdeckt und somit korrumpierte Accounts erkannt werden.

Neben nativen Data-Loss-Prevention-(DLP)-Lösungen größerer Cloud-Anbieter wie Google, bieten diverse Unternehmen, wie Forcepoint, Cisco (Cloudlock) und Symantec, Cloud-DLP-Lösungen in ihrem Portfolio an. Einige weitere kleinere Firmen, wie Endpointprotector und Nightfall, verfolgen interessante Ansätze, wie zum Beispiel künstliche Intelligenz (KI), in der Erkennung von Data-Leakages.

Backup und Redundanz

Gartner identifiziert Veeam, Comvault, Veritas, Dell, IBM, Rubrik und Cohesity im Juli-2020-Report als führende Backup-Software-Anbieter für Datacenter/Cloud-Strukturen.

Größere Cloud-Anbieter erfüllen in der Regel die regulatorischen Anforderungen (z. B. zwei unabhängige Rechenzentren mit mindestens 10 km Abstand), daher ist die Redundanz-Anforderung an Cloud-Strukturen relativ leicht umzusetzen. Hinzu kommt, dass die Container-Strukturen die redundante Auslegung von Anwendungen in der Cloud erleichtern.

Impressum

DATAKONTEXT GmbH

Augustinusstraße 9d, 50226 Frechen (DE)
Tel.: +49 2234 98949-30,
Fax: +49 2234 98949-32
redaktion@datakontext.com,
www.datakontext.com

Geschäftsführer: Hans-Günter Böse,
Dr. Karl Ulrich

Handelsregister:
Amtsgericht Köln, HRB 82299

Bankverbindung: UniCredit Bank AG, München,
IBAN: DE34 7002 0270 0015 7644 54

Zurzeit gültige Anzeigenpreisliste:
Nr. 38 vom 02. Januar 2020

Anzeigenleitung: Birgit Eckert
(verantwortlich für den Anzeigenteil)
Tel.: +49 6728 289003, anzeigen@kes.de

Media-Daten: Unsere Media-Daten finden Sie online auf www.kes.info/media/.

Herstellungsleitung und Vertrieb:
Dieter Schulz, dieter.schulz@datakontext.com,
Tel.: +49 2334 98949-99

Satz: BLACK ART Werbestudio
Stromberger Straße 43a, 55413 Weiler

Druck: QUBUS media GmbH,
Beckstraße 10, 30457 Hannover

Titelbild: 10-IMAGES auf Pixabay