Security im Oracle-Rechenzentrum in Frankfurt

Michael Fischer, ORACLE Deutschland B.V. & Co. KG

Oracle bietet seit mehreren Jahren Cloud Services in den Bereichen „IaaS", „PaaS" und „SaaS" an. Seit dem Jahr 2017 wird ein Teil der Services auch in Deutschland angeboten. Der Artikel beschreibt Sicherheitsmerkmale dieser Oracle Cloud Services im Frankfurter Rechenzentrum.

Der Anteil von Unternehmen, die Cloud-Angebote nutzen, steigt seit Jahren kontinuierlich. Sie benötigen dafür skalierbare, hybride Cloud-Lösungen, die die Sicherheits-, Datenschutz- und Compliance-Anforderungen erfüllen. Um diesen Anforderungen gerecht zu werden, hat Oracle unter anderem die Oracle Cloud Infrastructure entwickelt, eine Cloud-Plattform, die den Kunden ein virtuelles Rechenzentrum in der Cloud bietet. Die Oracle Cloud Infrastructure stellt eine Vielzahl von Cloud-Services bereit *(siehe Abbildung 1)*.

Unter „Compute" finden sich dedizierte Server (auch „Bare Metal") sowie virtuelle Maschinen (VM). Der Speicher steht mit „Storage" (in Form von Block, File, Object, Archive-Speicher) zur Verfügung. Oracle-Datenbanken gibt es in den verschiedenen Ausprägungen: Shared, dediziert, Exadata und Autonomous. Zugrunde liegen Software-definierte, virtuelle Cloud-Netzwerke (VCN), optional ergänzt um „Edge"-Services wie Load Balancing, DNS und weitere Services.

Für die Verwaltung werden in den Services Identitäts- und Zugriffsmanagement (engl. Identitiy and Access Management), Verschlüsselung, Monitoring und Auditierung bereitgestellt sowie ein Cloud-Tooling zur Unterstützung bei den typischen Tätigkeiten wie Erzeugen, Starten, Stoppen, Löschen von Services ebenso wie Backups, Restores oder Patching.

Für Unternehmenskunden, die eine Public Cloud nutzen wollen, sind die Datensicherheit und der Aufwand für die Migration bestehender Anwendungen von zentraler Bedeutung. Angesichts der Einschränkungen herkömmlicher öffentlicher Clouds migrieren Unternehmen normaler-

weise nicht-kritische Anwendungen in die Cloud und beschränken geschäftskritische Produktionsanwendungen und Daten weiterhin auf ihre lokalen Rechenzentren.

Oracle hat seine Cloud-Infrastruktur so aufgebaut, dass Unternehmen auch unternehmenskritische Anwendungen und Daten unter Berücksichtigung der Sicherheit migrieren und den Overhead beim Aufbau und Betrieb der Rechenzentrums-Infrastruktur reduzieren können. Mit der Oracle Cloud Infrastructure erhalten Unternehmenskunden die gleiche Kontrolle und Transparenz über ihre Workloads wie in ihren eigenen Rechenzentren.

Für Kunden, die eine vollständig isolierte und kontrollierte Umgebung benötigen, bietet Oracle Cloud Infrastructure sogenannte „Bare-Metal-Instanzen", also Maschinen, die vollständig vom Kunden verwaltet werden, ohne dass eine Software von Oracle auf der Instanz läuft. Kunden haben in diesem Fall sogar vollständigen Root-Zugang zu diesen Maschinen.

Seit dem Jahr 2017 ist die Oracle Cloud Infrastructure auch in den Rechenzentren in Frankfurt bereitgestellt. Dort werden drei örtlich getrennte Rechenzentren (in 5 bis 15 Kilometern Entfernung) genutzt, um eine entsprechende Ausfallsicherheit und Disaster-Recovery-Funktionen bereitzustellen.

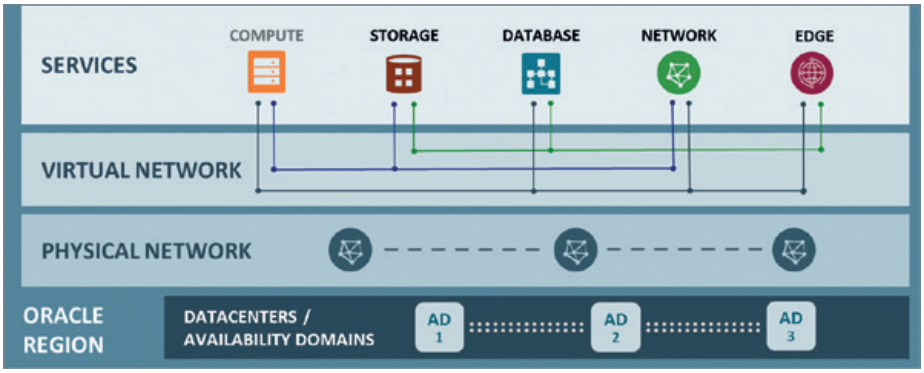

Abbildung 1: Funktionalitäten in der Infrastructure Cloud von Oracle

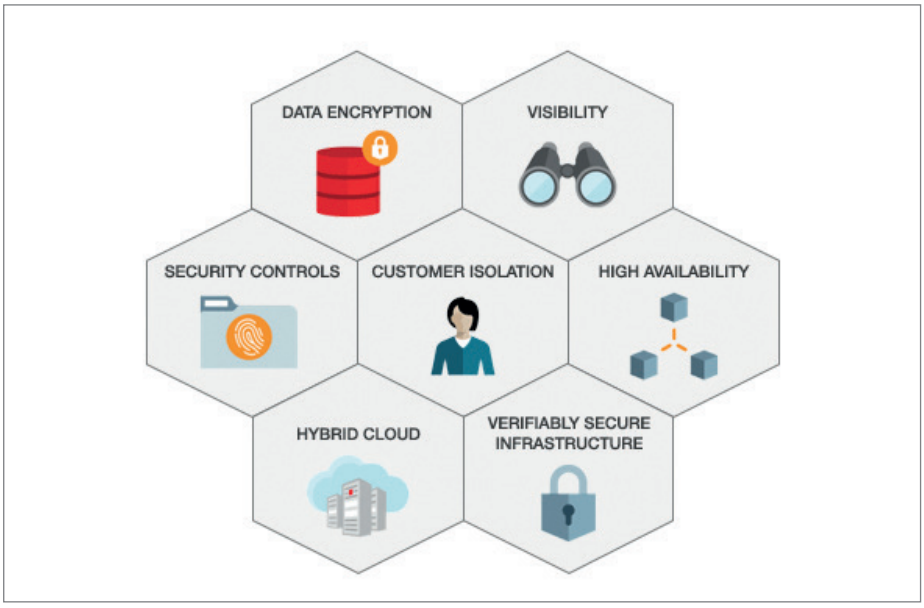

Abbildung 2: Die sieben Sicherheitsprinzipien

Die Sicherheitsprinzipien der Oracle Cloud Infrastructure

Oracle-Cloud-Infrastructure-Sicherheit umfasst folgende Prinzipien *(siehe Abbildung 2):*

- *Kundenisolierung*
  Anwendungs- und Datenbestände werden in einer Umgebung bereitgestellt, die von anderen Kunden und dem Oracle-Betrieb isoliert ist.

- *Verschlüsselung*
  Schutz der Daten am Speicherort und während der Übertragung durch Verschlüsselung. Transparenz bezüglich kryptografischer Algorithmen und Schlüsselverwaltung.

- *Security Controls*
  Funktionen zur Konfiguration von Sicherheit, die es ermöglichen, den Zugang zu Diensten einzuschränken (engl. „least privilege") und operative Verantwortlichkeiten zu trennen (engl. „segregation of duties").

- *Sichtbarkeit*
  Über Logdaten und Sicherheitsanalysen lassen sich die eigenen Ressourcen überprüfen und überwachen. Damit können Audit-Anforderungen erfüllt sowie Sicherheits- und Betriebsrisiken reduziert werden.

- *Sichere hybride Umgebungen*
  Vorhandene Sicherheitsmechanismen wie Benutzerkonten und Richtlinien sowie Sicherheitslösungen von Drittanbietern beim Zugriff auf Cloud-Ressourcen können weiterhin genutzt werden, um Daten in der Cloud abzusichern.

- *Hohe Verfügbarkeit*
  Bereits in der Standard-Konfiguration bieten die dreifach redundanten Rechenzentren hochverfügbare Scale-out-Architekturen und Resistenz gegen Netzwerk-Angriffe.

- *Überprüfbarkeit*
  Nachweis der Einhaltung der strengen Sicherheits-Standards von Oracle durch Audits, Zertifizierungen und Zertifikate von Drittanbietern. Eigene Cloud-Audits können beantragt werden.

- *Off-Box-Virtualisierung*
  Das virtuelle Netzwerk wird ausschließlich Software-basiert innerhalb der Cloud Infrastructure realisiert und nicht auf den auf den Maschinen laufenden Hypervisoren. Neben höherer Performance beim Netzwerk-Durchsatz bedeutet das auch den Wegfall von Sicherheitslücken durch potenzielle Exploits des Hypervisors auf der Netzwerk-Ebene.

Durch den Einsatz der Oracle Cloud Infrastructure profitieren Kunden direkt von der umfassenden Expertise von Oracle und den kontinuierlichen Investitionen in die Sicherheit. Die Entwicklung von Cloud Services erfolgt unter ISO-27001-Standards unter Berücksichtigung der ISO-27002-Controls für Information Security Management.

Die Rechenzentren, die die Cloud Services betreiben, sind zertifiziert nach ISO 9001, ISO 14001, OHSAS 18001, ISO 27001, ISO 50001 und PCI-DSS. Vom Typ sind sie ANSI/TIA-942-A Tier-III- oder Tier-IV-Standards des „Uptime Institute" und der Telecommunications Industry Association (TIA). Die Oracle Cloud Services in Frankfurt besitzen SSAE16/ISAE3402 (SOC-1 Typ 2), AT101 (SOC-2 Typ 2), SOC-3, PCI-DSS und HIPAA-Attestations sowie ISO/IEC-27001:2013-Zertifizierungen. Weitere (auch C5) sind in Planung.

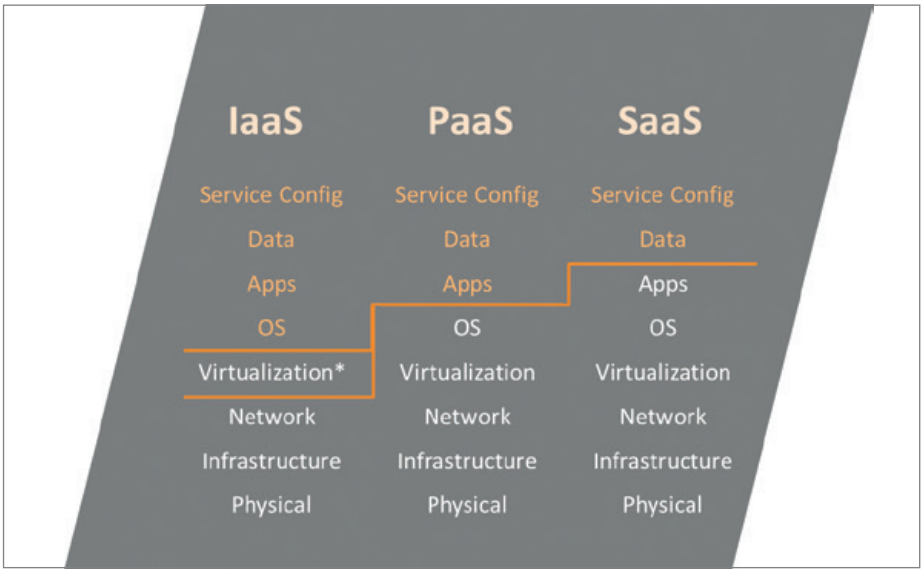

Abbildung 3: Die Aufteilung der Verantwortlichkeiten: Der weiß eingefärbte Teil liegt beim Cloud-Anbieter

Gemeinsame Verantwortung

Oracle stellt standardmäßig Cloud-Sicherheitstechnologien und betriebliche Prozesse zur Absicherung der Cloud Services bereit. Zusätzlich muss der Kunde darüber hinaus bei der Nutzung der Oracle Cloud auch selbst Verantwortung für Sicherheit und Compliance übernehmen, etwa in der sicheren Konfiguration der Cloud Services. Sicherheit in der Cloud ist somit immer eine gemeinsame Verantwortung, aufgeteilt zwischen dem Kunden und Oracle.

In der Cloud-Umgebung ist Oracle für die Sicherheit der zugrunde liegenden Cloud-Komponenten (wie Rechenzentrums-Einrichtungen, Hard- und Software-Systeme) verantwortlich, die Kunden hingegen tragen die Verantwortung für die Absicherung ihrer Workloads und die Konfiguration ihrer Services (wie Compute, Network, Storage und Database). Auf einem exklusiv genutzten Bare-Metal-Server erweitert sich die Verantwortung der Kunden auf den gesamten Software-Stack. In der Abbildung ist der Sonderfall mit Bare-Metal, dem Wegfall der Server-Virtualisierung durch den Cloud Provider, mit „*)" markiert *(siehe Abbildung 3)*.

Im Einzelnen lassen sich die Verantwortlichkeiten von Kunden und Oracle in die folgenden Bereiche unterteilen: Der Zugriff auf Oracle Cloud Services ist mit einem Identitäts- und Zugriffsmanagement (IAM) geschützt. Die Kunden sind für die Verwaltung und Überprüfung ihrer Accounts und für alle Aktivitäten im Rahmen der Nutzung verantwortlich. Oracle stellt lediglich das IAM zum Identitätsmanagement, zur Authentifizierung (inklusive Single-Sign-on über Federation), Autorisierung und Auditierung. IAM erlaubt über einen fein granularen Mechanismus, Zugriffsrechte auf Ressourcen-Anwendergruppen zu geben. Hierbei verfährt Oracle nach dem Least-Privilege-Grundsatz: Ein Nutzer hat per Default keine Rechte. Alle Rechte müssen explizit gesetzt werden.

Absicherung des Workloads: Kunden sind für den Schutz und die Sicherung des Betriebssystems und der Anwendungsschichten verantwortlich. Dieser Schutz umfasst, abhängig von den Services, das Patchen von Anwendungen und Betriebssystemen, die Konfiguration des Betriebssystems sowie den Schutz vor Malware und Netzwerkangriffen. Oracle bietet sichere Images mit aktuellen Patch-Levels an und ermöglicht im Rahmen der Kompatibilität mit den Services, Sicherheitslösungen von Drittanbietern, beispielsweise SIEM oder Firewall-Software-Appliances, aufzuspielen.

Datenklassifizierung und Compliance: Der Kunde ist für die korrekte Klassifizierung und Kennzeichnung seiner Daten und die Einhaltung der Compliance-Anforderungen verantwortlich. Auch die Überprüfung der Gesamtlösung hinsichtlich der Compliance ist in der Verantwortung des Kunden.

Sicherheit der Host- und Storage-Komponenten: Kunden sind für die sichere Konfiguration und Verwaltung ihrer Bare-Metal-, Compute- (virtuelle Hosts, Container), Storage- (Objekt-, lokale Storage-, Block-Volumes, File und Archive) und Plattform-Services (wie Datenbank-Konfiguration) verantwortlich. Oracle stellt die Basissicherheit dieser Elemente zur Verfügung.

Netzwerksicherheit: Kunden sind für die sichere Konfiguration von Netzwerk-Elementen wie virtuellen Netzwerken, Load Balancing, DNS und Gateways (Internet, VPN, Peering) zuständig. Oracle ist für die Bereitstellung einer sicheren Netzwerk-Infrastruktur verantwortlich. Oracle Cloud Infrastructure bietet dabei Kunden mit Security-Lists eine sehr feingranulare Konfigurationsmöglichkeit (welcher Traffic kann von wo nach wo über welchen Port erfolgen) ihrer Sub-Netze an.

Client- und Endpoint-Protection: Kunden nutzen verschiedene Hard- und Software-Systeme, wie mobile Geräte und Browser, um auf ihre Cloud-Ressourcen zuzugreifen. Kunden sind für die Absicherung aller Clients und Endgeräte verantwortlich, die sie für den Zugriff auf Oracle Cloud Infrastructure Services verwenden.

Physische Sicherheit: Oracle ist verantwortlich für den Schutz der globalen Infrastruktur, die alle in der Oracle Cloud Infrastructure angebotenen Services betreibt. Diese Infrastruktur besteht aus

Hardware, Software, Netzwerken und Einrichtungen, die Oracle Cloud Infrastructure Services betreiben. Oracle betreibt seine Cloud-Dienste innerhalb von Rechenzentren namhafter externer Betreiber, die mindestens ANSI/TIA-942-A Tier-3- oder Tier-4-Standards und einer N2-Redundanz-Methodologie folgen. Die Betreiber haben weder administrativen noch physischen Zugang zu den in Cages betriebenen Rechnern, es wird nur Housing, Energie, Kühlung und Brandschutz zur Verfügung gestellt.

Die Konzepte, Regionen, Redundanzen und Verfügbarkeit

Oracle Cloud Infrastructure bietet dem Kunden die Möglichkeit, sich sein Cloud-Datacenter aus den verschiedenen Cloud-Service-Lokationen auszusuchen, so zum Beispiel Frankfurt. Jede Region besteht aus drei Standorten mit eigenen Datacentern, den sogenannten „Availability Domains". Availability Domains innerhalb der gleichen Region sind durch ein sicheres, schnelles und latenzarmes Netzwerk verbunden, die Verbindungen sind verschlüsselt und je nach Servicetyp erfolgt transparent eine redundante Speicherung an mehreren Standorten.

Die Availability Domains sind physisch getrennte, von unterschiedlichen Anbietern gestellte Rechenzentren (jeweils 5 – 15 km voneinander getrennt). Es handelt sich also nicht nur um Availability Zones, die lediglich innerhalb eines Rechenzentrums durch Brandschutztüren voneinander getrennt sind. In Deutschland existiert als Region Frankfurt. Eine weitere EU-Region ist noch London, ein Ausbau weiterer EU-Regionen ist geplant.

Die Availability Domains können auch explizit vom Kunden genutzt werden, um hochverfügbare Anwendungen aufzubauen. Entsprechende technische Hilfsmittel wie Load Balancer oder Data Guard stehen zur Verfügung *(siehe Abbildung 4)*.

Zugriffsverwaltung und Auditing

Wird ein Cloud Account bei Oracle angelegt, bekommt der Kunde die notwendigen administrativen Accounts. Damit können Berechtigungsstrukturen definiert und weitere Accounts angelegt und verwaltet werden. Benutzer können entweder im Cloud Service über die Oberfläche angelegt, von außen provisioniert oder im Rahmen des Single-Sign-on (SSO) übernommen werden. Diese SSO-„on-the-fly"-Übernahme erfolgt optional basierend auf dem Federation Standard via SAML, etwa von einem Active Directory Federation Service aus. Passwort-Policies können bei Benutzern mit direkter Anmeldemöglichkeit definiert werden. Starke Authentifizierung und kontextbasierte Authentifizierung lassen sich im jeweiligen führenden Anmeldesystem konfigurieren.

Das Zugriffsmanagement ermöglicht so die Umsetzung des „least privilege"-Prinzips und optional die direkte Steuerung der Rechte vom lokalen oder fremden Identity Management System, etwa die Deaktivierung beim Verlassen des Unternehmens. Über die Steuerungsmöglichkeit können auch Abteilungen und/oder Test- und Produktions-Systeme abgebildet werden.

Alle Ressourcen sind standardmäßig geschützt und können nur mit entsprechenden Berechtigungen angelegt, geändert oder gelöscht werden. Dazu werden Gruppen definiert, Policies erstellt und die Gruppen den Benutzern oder Services zugewiesen. Die Architektur lässt den angemeldeten Account oder Service nur diejenigen Operationen ausführen, für die er berechtigt wurde. Das Berechtigungsmanagement wirkt übergreifend über Regionen.

Neben der Verwaltung der Cloud über die Web-Konsole bietet Oracle Cloud Infrastructure auch die Möglichkeit, über ein REST-API oder durch bereitgestellte SDKs (wie eine CLI für Shell-Skripte, Python, Java) Ressourcen zu verwalten. Zudem werden auch deklarative Infrastructure-as-Code-Technologien (IaC) wie Terraform unterstützt.

Alle Zugriffe der Web-Konsole über IaC oder API/SDKs laufen am Ende über das gleiche API und werden daher identisch und vollständig durch den Oracle Cloud Infrastructure Audit Service protokolliert. Der Audit-Service stellt die Auditdaten über eine grafische Konsole und als JSON-Daten über ein authentifiziertes, filterbares Abfrage-API zur Integration in einem übergeordneten System bereit. Der Inhalt des Audit-Protokolls umfasst die

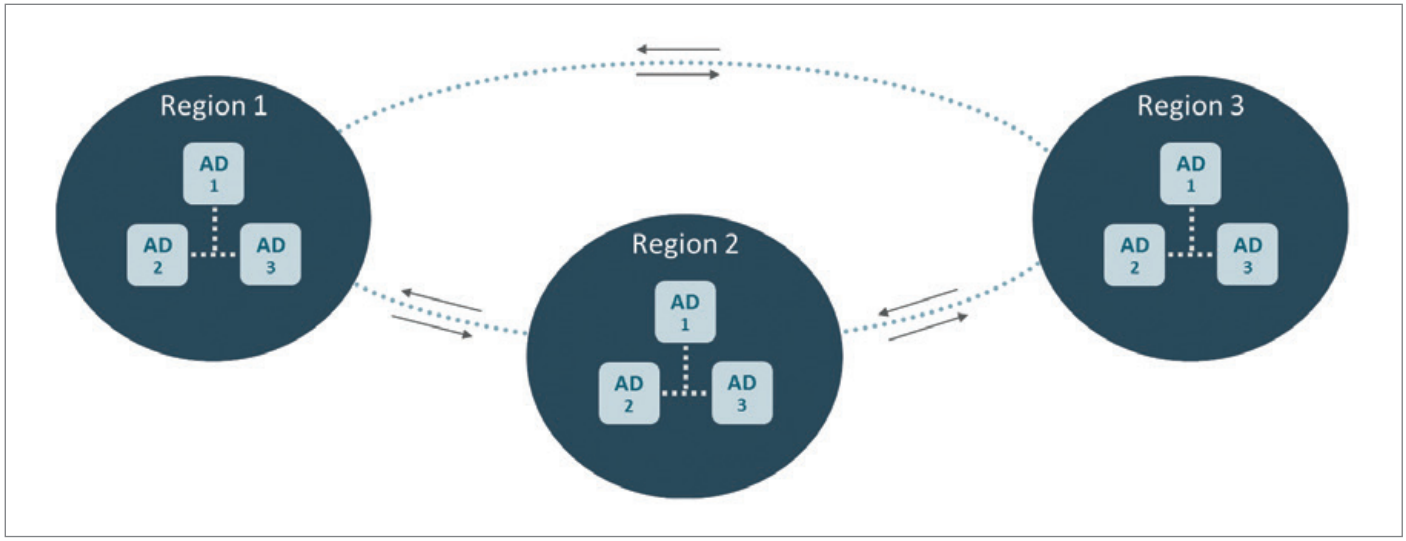

Abbildung 4: Das Konzept mit Regionen und Availability Domains

aufgetretene Aktivität, den Benutzer, der sie initiiert hat, das Datum und die Uhrzeit des Requests sowie die Quell-IP, den User-Agent und die HTTP-Header des Requests. Auditdaten von Services wie DB Auditlog oder Syslog sind wie bei On-Premises-Systemen über die entsprechenden Service-Schnittstellen verfügbar.

Instanzen

Die Oracle Cloud Infrastructure bietet Bare-Metal-, Virtual-Machine- und Datenbank-Instanzen in verschiedenen Ausprägungen:

- Bare-Metal-Instanzen (BM) sind dedizierte physische Server für einen einzelnen Kunden, der die volle Kontrolle über den Server hat. Es gibt keinen von Oracle verwalteten Hypervisor; Oracle-Mitarbeiter haben keinen Zugriff auf Speicher oder Storage. Die gesamte Netzwerk-Virtualisierung erfolgt off-box und nur der Oracle Integrated Lights Out Manager (ILOM) wird zum Hardware-Monitoring und -Reboot verwendet.
- Virtuelle Maschinen (VMs) sind mandantenfähige Kunden-VMs auf Oracle Hypervisor, der die Isolierung zwischen den Kunden bietet.
- Oracle-Datenbanken sind verfügbar als Exadata, Exclusive DB auf Bare-Metal-Instanzen, VM-DB-Instanzen und Autonomous DWH. DB-Systeme unterliegen der gleichen Zugriffsregelung wie die Instanzen beziehungsweise der Konfiguration der zugrunde liegenden Services (wie ADWC). Standardmäßig werden die Daten am Speicherort mit Oracle-TDE (AES) verschlüsselt, wobei die Hauptschlüssel in einem Oracle-Wallet auf jedem DB-System gespeichert sind. Wallets können ausgelagert oder zentral über Oracle Key Vault verwaltet werden. RMAN-Backups von DB-Systemen werden verschlüsselt und in kundeneigenen Buckets im Object Storage abgelegt.

Oracle-Cloud–BM-, -VM- und -DB-Instanzen verwenden als Standard schlüsselbasiertes SSH für die Verwaltung. Die Schlüssel werden vom Kunden festgelegt. Im Falle der Datenbank vergibt der Kunde zusätzlich die DB-Credentials. Andere Zugänge sind nicht vorkonfiguriert. Es können eigene oder von Oracle bereitgestellte gepatchte Images verwendet werden. Alle von Oracle bereitgestellten Images verfügen über sichere Standard-Einstellungen einschließlich Firewalls auf Betriebssystem-Ebene, die standardmäßig aktiviert sind.

Netzwerk und Storage

Im Oracle-Cloud-Infrastructure-Netzwerk gibt es keine Noisy-Neighbor-Probleme auf dem Netz und an den Instanzen. SLAs werden sowohl für Netzwerk-Bandbreiten als auch für Latenzzeiten zugesagt. Es erfolgt eine Isolierung der Kunden-Netzwerke auf Layer 3. Dies wird durch Software-Defined-Networks (SDNs) ermöglicht, die physisch auf einer speziellen Architektur (sogenannte „Clos-Netzwerke“) basieren und Off-Box-Netzwerk-Virtualisierung ohne zentralen Netzwerk-Hypervisor nutzen. Es erfolgt keine Over-Subscription.

Der Kunde definiert sein virtuelles Cloud-Netzwerk (VCN) unter Verwendung aller bekannten Sicherheits-Funktionalitäten wie IPs (public, private), Sub-Netzen (public, private), Routing-Tabellen und Security Lists (Firewalls). Durch Kunden konfigurierte Gateways kontrollieren die Netz-Übergänge mit dem Internet, einem VPN (IPSec), zwischen den Sub-Netzen und zwischen Regionen. Es kann eine private Verbindung zwischen dem Rechenzentrum des Kunden und der Oracle Cloud aufgeschaltet werden. Damit ist das Netzwerk vollständig unter der Kontrolle des Kunden.

Storage steht in verschiedenen Ausprägungen zur Verfügung. Sowohl physisch in den einzelnen Maschinen für High-Performance-Datenzugriffe (IOPS) als auch als externer Speicher. Externer Speicher und Boot Volumes sind immer AES-verschlüsselt. Externer Speicher ist für den Kunden transparent redundant. Weitere Redundanz kann konfiguriert werden. Die Storage-Typen sind im Einzelnen:

- *Lokaler Storage*
  NVMe-gestützter Speicher in den Dense-IO-Instanzen für maximale IOPS

- *Boot und Block Volumes*
  Über das Netzwerk angeschlossener Speicher (iSCSI) mit redundanter Speicherung in der jeweiligen Availability Domain

- *Object-Storage*
  Speicher aus Buckets und Objects, redundant über Availability Domains. Eine Authentifizierung ist beim Zugriff notwendig, es sei denn, es wird ein öffentlicher Zugriff festgelegt. Zugriffsschlüssel für andere Protokolle (wie Amazon S3) können über das integrierte Berechtigungsmanagement ebenso verwaltet werden wie vorauthentifizierte Benutzerzugriffe.

- *File-Storage*
  NFSv3-Endpunkt als Mount-Ziel im VCN-Subnetz jedes Kunden. Das Mount-Ziel wird durch einen DNS-Namen identifiziert und auf eine IP-Adresse abgebildet.

- *Archive-Storage*
  Speicherung langlebiger Daten mit nur seltenem Zugriff. Der Zugriff erfolgt wie bei Object-Storage (API, SDK, CLI), aber im Gegensatz zum Object-Storage stehen Daten nach einem Daten-Abruf erst mit einer Verzögerung von mehreren Stunden bereit.

Weitere Services

Weitere Services wie Load Balancer und Managed Domain Name Server (DNS) stehen zur Verfügung. Load Balancer können kundeneigene Zertifikate verwenden und unterstützen End-to-End-SSL, SSL-Tunneling oder SSL-Terminierung. Im Standard werden TLS 1.2 und Forward-Secrecy-Chiffre verwendet. Der Oracle-Cloud-Infrastructure-DNS-Service bietet dynamische, statische und rekursive DNS-Lösungen. Der DNS-Dienst arbeitet in einem globalen Anycast-Netzwerk mit 18 Points of Presence (PoP) auf fünf Kontinenten und bietet vollständig redundante DNS-Konstellationen sowie mehrere Tier-1-Transit-Anbieter pro PoP.

Sicherheits-Design und -Kontrollen

Das Oracle-Sicherheitsmodell basiert auf Menschen, Prozessen, Werkzeugen und

einer gemeinsamen Sicherheits-Plattform mit Methoden und Ansätzen *(siehe Abbildung 5)*. Einige Aspekte daraus sind:

- *Benutzer-Authentifizierung und Zugriffskontrolle*
  Der Zugang zu den Produktionssystemen unterliegt dem „least privilege"-Prinzip. Die Berechtigungen werden regelmäßig überprüft und sind auch mit dem HR-System gekoppelt. Der Zugriff auf Produktions-Umgebungen erfordert eine Multi-Faktor-Authentifizierung (MFA). Zugriffe auf Produktions-Systeme werden protokolliert und die Protokolle zur Sicherheits-Analyse gespeichert.

- *Change Management*
  Die Oracle Cloud Infrastructure folgt definierten Change-Management- und Deployment-Prozessen. Alle Änderungen, die in der Produktions-Umgebung vorgenommen werden, folgen einem Test- und Freigabe-Prozess. Die Integrität kritischer System-Konfigurationen wird überwacht, um sicherzustellen, dass sie mit dem erwarteten Zustand übereinstimmen.

- *Schwachstellen-Management*
  Sowohl interne Penetrationstests als auch Tests durch externe Branchen-Experten werden durchgeführt, um potenzielle Schwachstellen zu identifizieren. Oracle Cloud Infrastructure Hosts durchlaufen periodische Scans mit branchenüblichen Scannern.

- *Sicherheits-Protokollierung und -Überwachung*
  Sicherheitsrelevante Ereignisse (wie API-Aufrufe und Netzwerk-Ereignisse) werden protokolliert und die Protokolle auf anomales Verhalten überwacht. Alarme, die ein Überwachungsmechanismus auslöst, werden vom Sicherheitsteam verfolgt und ausgewertet.

- *Netzwerk-Sicherheit*
  Standardmäßig erfolgt die Kundenkommunikation mit Oracle Cloud Infrastructure Services unter Verwendung aktueller TLS-Chiffren und Konfigurationen, um Kundendaten während der Übertragung zu schützen und Man-in-the-Middle-Angriffe zu verhindern. Aufrufe von Diensten sind mit öffentlichen Schlüsseln digital signiert, um Manipulationen zu verhindern. Es werden Tools und Mechanismen eingesetzt, um verteilten Denial-of-Service-Angriffen (DDoS) zu begegnen und eine hohe Verfügbarkeit zu erreichen.

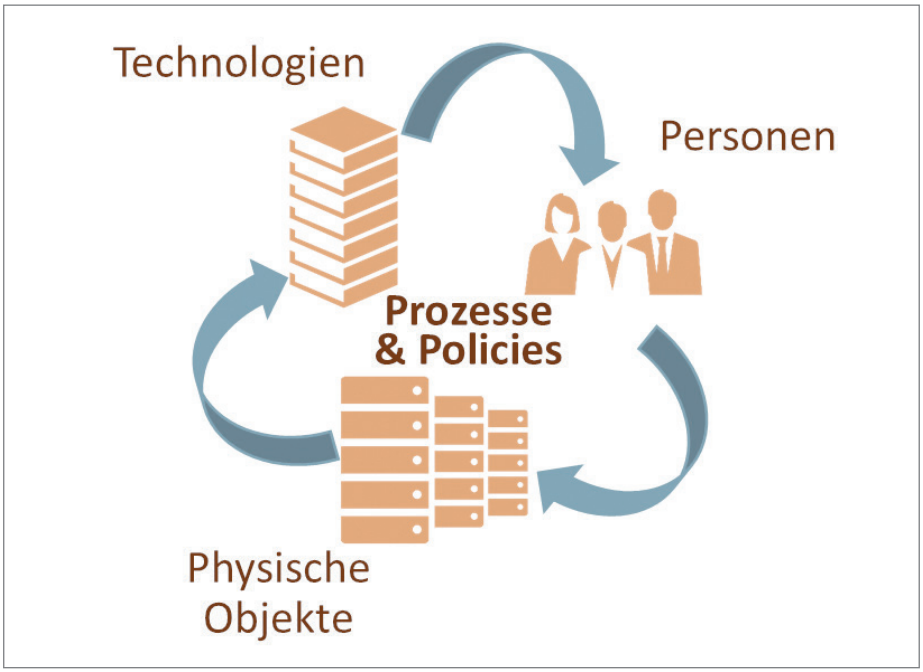

Abbildung 5: Sicherheitsmodell Oracle Cloud

- *Reaktion auf Vorfälle/Incidents*
  Innerhalb der Oracle Cloud wird ein Monitoring eingesetzt, um Incidents (dt. Vorfälle) zu erkennen. Abhängig von der Art des Vorfalls sind Eskalationspfade und Reaktionsteams definiert, um den Vorfall zu beheben. Oracle arbeitet mit dem Kunden, mit den entsprechenden technischen Teams und gegebenenfalls mit externen Strafverfolgungsbehörden zusammen, um auf den Vorfall zu reagieren. Das Ziel ist es, die Vertraulichkeit, Integrität und Verfügbarkeit der Cloud-Services-Umgebung wiederherzustellen und Ursachen und Abhilfemaßnahmen zu ermitteln. Mit dem sogenannten „CAPA-Prozess" (Corrective Action/Preventative Action) erfolgt die Ursachen-Analyse, um bei Bedarf Änderungen für die Produktion, technische Maßnahmen oder Prozess-Änderungen abzuleiten und sicherzustellen, dass das Problem nicht erneut auftritt. Verantwortlich dafür ist ein 24/7-Incident-Response-Team, die Kommunikation zum Kunden übernimmt die Oracle Global Information Security (GIS). Der Auftragnehmer wird den Auftraggeber im Falle eines Sicherheitsverstoßes, in dem der Auftraggeber gemäß geltendem Recht eine Benachrichtigung erhalten muss, innerhalb von 24 Stunden oder früher informieren. Wenn Informationen gesammelt oder anderweitig verfügbar sind, wird Oracle dem Auftraggeber eine Beschreibung des Sicherheitsverstoßes zur Verfügung stellen, sofern dies nicht gesetzlich untersagt ist.

- *Trennung der Cloud-Entwicklung von der Produktion*
  Die Vorproduktions-Umgebungen (wie Entwicklung, Test und Integration) sind von den Produktions-Umgebungen getrennt, sodass die Entwicklungs- und Test-Aktivitäten keine Auswirkungen auf die Produktivsysteme haben.

- *Löschung und Medienvernichtung*
  Die Oracle-Cloud-Infrastructure-Instanzen werden nach der Freigabe der Hardware durch den Kunden sicher gelöscht und neu initialisiert. Wenn die zugrunde liegende Hardware das Ende ihrer Lebensdauer erreicht hat, wird sie sicher zerstört. Vor dem Verlassen der Oracle-Rechenzentren werden die entsprechenden Laufwerke durch den Einsatz branchenführender Medienvernichtungsgeräte unbrauchbar gemacht.

Datenschutz

Der Oracle Cloud liegt die Auftrags-Datenverarbeitung zugrunde. Bei der Nutzung der Oracle Cloud akzeptiert der Kunde diese und weitere Verträge zur Nutzung der Oracle Cloud. Oracle ist Auftrags-Datenverarbeiter („Processor") und der Kunde bleibt der Auftrags-Datenverantwortliche („Controller"). Die Oracle Cloud Infrastructure hat zwei Kategorien von kundenbezogenen Daten:

- *Informationen zum Kundenkonto*
  Dies sind Informationen, die für den Betrieb des Oracle-Cloud-Infrastructure-Kontos des Kunden erforderlich sind und in erster Linie zur Kontaktaufnahme und Abrechnung verwendet werden. Die Verwendung der persönlichen Daten, die Oracle vom Kunden zum Zwecke der Kontoführung sammelt, wird durch die Oracle-Datenschutz-Richtlinie geregelt. Die Oracle Cloud Infrastructure fungiert in diesem Fall als Controller.

- *Durch den Kunden gespeicherte Daten*
  In Daten, die Kunden in der Oracle-Cloud-Infrastruktur speichern, wozu auch personenbezogene Daten gehören können, hat Oracle keinen Einblick. Zusätzlich bestehen keine Einflussmöglichkeiten auf die Entscheidungen des Kunden über deren Erhebung und Verwendung. Oracle hat keine direkte Beziehung zu den betroffenen Benutzern, der Kunde ist der Auftrags-Datenverantwortliche und verwaltet die Daten. Oracle Cloud Infrastructure ist nur der Auftrags-Datenverarbeiter.

Oracle als amerikanischer Anbieter hält sich zum Zeitpunkt der Erstellung des Dokuments an das EU-U.S. Privacy Shield Framework beziehungsweise das U.S.-Swiss Safe Harbor Agreement des US-Handelsministeriums bezüglich der Erfassung, Verwendung und Speicherung von personenbezogenen Daten von Bürgern der Europäischen Union beziehungsweise der Schweiz. Oracle ist auch dafür verantwortlich, dass Dritte, die im Auftrag von Oracle handeln, dies auch tun.

Bezüglich auf beispielsweise in der DSGVO aufgeführte Anforderungen wird in den Cloud Policies (Data Processing Agreement) Transparenz geschaffen. Ergänzende Informationen wie Datenbank-Funktionen, Konfigurationen und Komponenten, die bei der Umsetzung helfen können, finden sich in verschiedenen Oracle Whitepapers. Das Oracle Cloud Infrastructure GDPR Whitepaper beispielsweise konzentriert sich auf Kundenservice-Daten und alle persönlichen Informationen im IaaS Service.

Fazit

Oracle stellt mit der Oracle Cloud Infrastructure in Frankfurt eine Cloud-Umgebung bereit, mit der unternehmenskritische Workloads unter Wahrung der Sicherheits-Anforderungen in die Cloud verlagert werden können. Kunden erhalten Kontrolle und Absicherung unter anderem durch:

- Security per Default: Verschlüsselung am Speicherort und beim Zugriff; Zugriffsbeschränkung im Standard ausgehend von einem Nichts-ist-erlaubt-Ansatz.
- Wahlmöglichkeit bezüglich Datenhosting: weltweit, EU, Deutschland oder On-Premises.
- Isolation der Kunden durch Layer3-Off-Box-virtualisierte Netzwerke und Einsatzmöglichkeit dedizierter Maschinen. Dadurch gibt es kein Noisy-Neighbor-Problem im Netzwerk oder auf dem Server.
- Compliance: Security-Zertifizierungen der Cloud durch Unabhängige, Hilfestellungen für GDPR und andere Regularien. Protokolldaten für Monitoring und Auditierungen sind zugreifbar.
- Cloud Security Services: Zusätzliche Services von Oracle, um Oracle oder 3rd-Party-Clouds/-Umgebungen abzusichern. Einsatzmöglichkeit von Software-Lösungen von Drittanbietern zum Schutz der Daten und Ressourcen in der Cloud.
- Redundante Rechenzentren, die hochverfügbare Scale-out-Architekturen ermöglichen und Netzwerk-Angriffe abwehren.

Oracle investiert weiterhin in die Entwicklung von Cloud Services und Sicherheits-Technologien. Funktionale Erweiterungen auch im Bereich „Security" finden in der Cloud permanent statt, beispielsweise die Erweiterung einer Web-Application-Firewall.

Weitere Informationen

- Oracle IaaS Security Security and Compliance, Informationen und Whitepaper: *https://cloud.oracle.com/iaas_compliance*
- Cloud-Verträge: *http://www.oracle.com/us/corporate/contracts/cloud-services/index.html*
- GDPR Whitepaper: *https://cloud.oracle.com/iaas/whitepapers/oci-gdpr.pdf und oracle.com/goto/gdpr* und *oracle.com/goto/gdpr-newsletter*
- Services Security Documentation: *https://docs.oracle.com/en/cloud*
- Blogeinträge: *https://blogs.oracle.com/cloud-infrastructure*, *https://blogs.oracle.com/coretec* und *https://www.oraclecloud.de*

Michael Fischer
michael.fischer@oracle.com