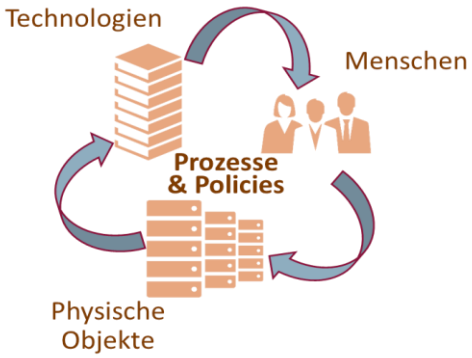
Oracle Public Cloud Security

Security in der Oracle Public Cloud für Iaas/PaaS und Cloud Security Services

Oracle betrachtet das Thema Cloud Security aus zwei Perspektiven:
- Sicherheit in den angebotenen Cloud Services, zum Beispiel Verschlüsselung
- Sicherheit der Cloud an sich

Es gibt viele Gründe, sich für Cloud Services zu entscheiden, sei es, um von vorgefertigten Anwendungen zu profitieren, CapEx Posten zu reduzieren, besser auf wachsende Datenmengen und Nutzerzahlen zu reagieren, schneller Services bereitstellen zu können, Kosten einzusparen oder Sicherheit zu erhöhen. Fast 60% der von IDC befragten Unternehmen trafen die Einschätzung, dass Cloud Service Provider eine bessere Absicherung bzw. höhere Sicherheit leisten können als die eigene IT.

Cloud Security kann in Bezug auf die eingesetzten Technologien, auf die Personen, die den Betrieb sicherstellen und auf die Rechenzentren, die diese Dienste bereitstellen, betrachtet werden. Prozesse und Richtlinien definieren dabei das Zusammenwirken.



Betrachtungsweise Cloud Security

Das eigene Rechenzentrum unterliegt vollständig der eigenen Verantwortung. Werden Cloud Services genutzt, teilt sich diese Verantwortung zwischen dem Kunden und dem Cloud Provider auf, dies wird als "Shared Responsibilities" definiert.

ECKPFEILER CLOUD SECURITY

Cloud Security besteht aus dem Bereitstellen sicherer Cloud Services und dem sicheren Betrieb

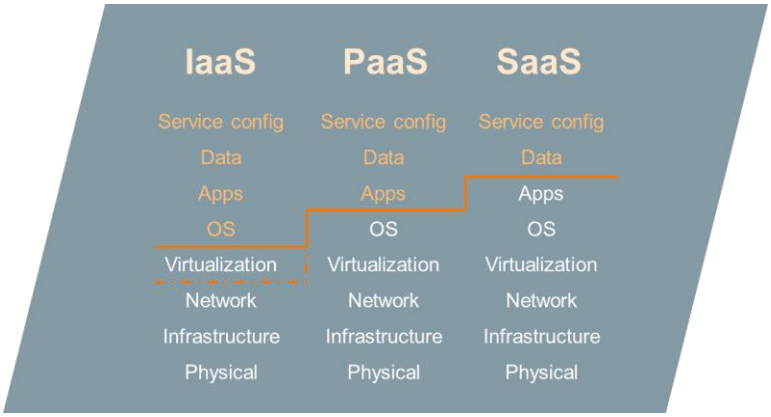
Grundlage von Services, die nicht von der eigenen Organisation bereitgestellt werden, ist die Auftragsdatenverarbeitung

„Shared Responsibilities“ ist das Modell um Verantwortlichkeiten unter anderem aus der Auftragsdaten-verarbeitung je Service zu modellieren

„Shared Responsibilites“ sind unter anderem in den Hosting Policies beschrieben

Die Basis der Nutzung von Angeboten eines Cloud Providers ist die sogenannte Auftragsdatenverarbeitung. Oracle ist dabei der Auftragsdatenverarbeiter (Data Processor) und nicht der Verantwortliche (Data Controller). Verallgemeinert bedeutet dies, dass der Kunde Eigentümer und Verantwortlicher der Daten ist und bleibt.

Die Aufteilung der Verantwortlichkeiten ist je nach Art des Cloud Services verschieden, wie das nachfolgende Bild illustriert. Die Trennlinie kennzeichnet die Verantwortlichkeiten von Oracle (weiß) und die des Service-Nutzers (orange).



Shared Responsibilities / Verantwortlichkeiten in unterschiedlichen Cloudtypen

Oracle stellt und managt die Basisdienste je nach Cloud Typ bzw. Service.

Bei Infrastructure as a Service (IaaS) stellt Oracle das Rechenzentrum und die Infrastruktur bestehend aus Netzwerk, Compute und Storage. Beim Storage wird eine entsprechende Redundanz transparent bereitgestellt. Um Server für Kunden verwalt- und nutzbar zu machen, kommen entweder Virtualisierungslayer (Verantwortlichkeit wie im Bild) oder Provisionierungskomponenten (Bare Metal Cloud, gestrichelte Linie) zum Ansatz. Alle weiterführenden Services stellt oder provisioniert der Kunde als Service-Nutzer selbst. Damit ist der Kunde für die sichere Konfiguration verantwortlich. Ausgehend von einem „alles-ist-verboten“ Ansatz konfiguriert der Kunde entsprechend Accounts, Zugänge, Netzwerke, Verschlüsselungen, Verfügbarkeiten sowie Backups. Je nach Service ist dabei auch Patching und Backup/Restore über die Weboberflächen möglich.

Platform as a Service (PaaS) stellt die Services “vorkonfiguriert” zur Verfügung. Je nach Art des Services ist der Kunde auch für Security und administrative Aufgaben verantwortlich. Abhängig vom PaaS Service ist ggf. ein Betriebssystem mit enthalten, zum Beispiel beim Provisionieren eines Service. Es wird ebenfalls von einem „nichts-ist-erlaubt“ Ansatz gestartet, bei dem Accounts, Zugänge, Netzwerke, Verschlüsselungen, Verfügbarkeiten sowie Backups konfiguriert und das Patching durchgeführt werden muss. Bei einem höherwertigen PaaS Service wie zum Beispiel DB Schema Service oder Content Cloud führt Oracle einen Teil der Aufgaben, wie Patching der Datenbank, durch.

Die detailliertere Beschreibung der Verantwortlichkeiten des Kunden findet sich in den Hosting Policies und den entsprechenden Servicedokumentationen (Link siehe weiterführende Informationen).

SHARED RESPONSIBILITIES

Die Aufteilung über die Shared Responsibilites erlaubt eine grobe Zuordnung der Verantwortlichkeiten

Die Aufteilung ist auch die Basis wenn es um Compliance und Regularien geht

Technische Massnahmen für die Security wie Verschlüsselung sind in nachfolgenden Seiten beschrieben

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

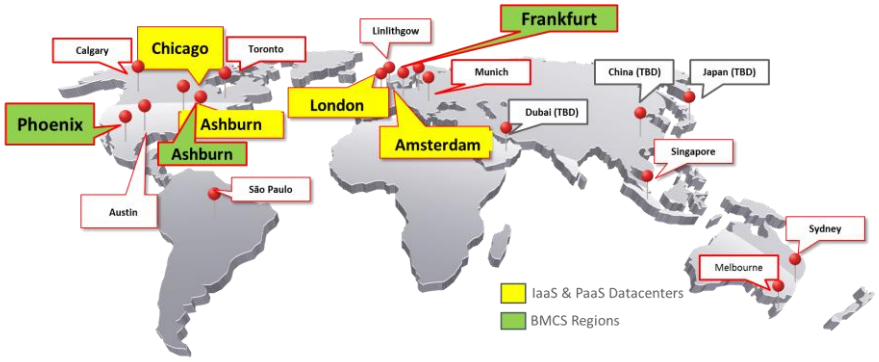
twitter.com/oracle

oracle.com

FOR MORE INFORMATION

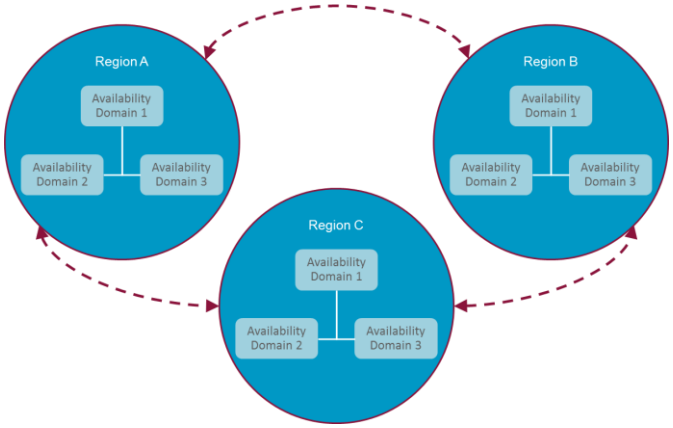
Contact: 1.800.ORACLE1

Oracle stellt die IaaS, PaaS und SaaS Services in 19 Datacentern zur Verfügung. Damit ist sowohl eine Redundanz innerhalb eines Datacenters als auch eine Redundanz über Standorte und Kontinente möglich. Bis auf das Datacenter in Austin nutzt Oracle Datacenter Facilities von Anbietern wie Equinix. Generell sind diese auf Tier III+ („Concurrent maintainable“: redundante Komponenten und mehrfache Anbindungen) ausgelegt, erfüllen teilweise auch Tier IV Standards.



Oracle Public Cloud Rechenzentren

Je nach Service ist eine Redundanz enthalten (zum Beispiel Storage) oder als Option verfügbar (zum Beispiel RAC im Falle der Datenbank). Dieses Dokument behandelt Bare Metal Cloud (BMC), IaaS und PaaS Services. Die Services besitzen unterschiedliche Hochverfügbarkeitsumsetzungen. In klassischen IaaS/PaaS kommt eine grundlegende Redundanz zum Tragen, Bare Metal Cloud „erweitert“ diese um ein Konzept bestehend aus Region und Availability Domains. Im Frankfurter Raum laufen beispielsweise drei Availability Domains, die alle örtlich getrennt sind.



Verfügbarkeit/Redundanz mit Domains und Regionen

DATACENTER

Weltweit sind 19 Datacenter für Oracle verfügbar

Datacenterfacilities kommen von namhaften Providern oder Oracle

Datacenter sind in einem geographischen Raum (zum Beispiel EMEA) mehrfach vorhanden

Eine Redundanz über Kontinente hinweg ist möglich

In Deutschland sind in Frankfurt und München SaaS Rechenzentren, im Frankfurter Datacenter werden „Bare Metal“ IaaS und PaaS aufgebaut

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

FOR MORE INFORMATION

Contact: 1.800.ORACLE1

ORACLE

Integrated Cloud Applications & Platform Services

Cloud Security im Überblick:
Personen, Technologien, Objekte, Prozesse und Policies

Die Oracle Cloud ist so ausgelegt, dass jede Schicht (Layer) abgesichert wird und sowohl Entwicklung der Cloud Services als auch Betrieb prozesstechnisch entsprechend ausgerichtet sind. Die fortwährenden Audits und Zertifizierungen (siehe auch nachfolgende Abschnitte) bestätigen dabei das Selbstverständnis, eine sichere Cloud anzubieten. Wie in der Abbildung „Betrachtungsweise Cloud Security“ beschrieben, sind die Bestandteile die

- Personen: Mitarbeiter die die Oracle Cloud betreiben werden fortwährend bzgl. Security und im Umgang mit sensiblen Daten geschult. Im Rahmen der gesetzlichen Möglichkeiten werden sie beim Einstellungsverfahren überprüft.
- Technologien: Security wird im Stack so tief wie möglich und in jeder der beteiligten Schichten implementiert (Oracle Modell „Defense in Depth“).
- Physischen Objekte: Dies umfasst die Datacenter, die Hardware im Datacenter, die Gebäudeüberwachung und den Zutrittsschutz.
- Prozesse und Richtlinien: Strenge stringente Sicherheitsrichtlinien und deren Kontrolle bzgl. der Mitarbeiter, Technologien und Datacenter. Diese werden übergeordnet überwacht durch das Oracle Security Oversight Committee.

Oracle benutzt parallel mehrere Methoden Prozesse, Technologien um Kundenumgebungen möglichst transparent für den Benutzer zu schützen. Zudem werden fortwährend Empfehlungen wie die 12 Punkte der Cloud Security Alliance für Cloud Provider und Kunden berücksichtigt.

CLOUD SECURITY IM ÜBERBLICK

Für die Cloud Security werden gemäß Abbildung „Betrachtungsweise Cloud Security“ kurz die Cloud Organisation und die technischen Maßnahmen beleuchtet

Technische Maßnahmen sind durchsetzt mit den Anforderungen der CIA Triade (confidentiality, integrity, availability) an die Security

Technische Maßnahmen sind teilweise quer durch alle Services vorhanden als auch spezifisch in einzelnen Services

Die Menschen hinter der Cloud: Organisation & Operations

Mehr als 1600 dedizierte Mitarbeiter von Oracle betreiben die Oracle Cloud. Die Oracle Cloud ist vom internen Oracle-Firmen-Netzwerk getrennt. Der Betrieb umfasst das Management von Applikationen, Plattformtechnologien und der Infrastruktur inklusive Netzwerk-Administration mit Switchen, Firewalls und Loadbalancer. Eine Überwachung erfolgt in einem 7x24 Operation “Nerve Center”.
Für Security & Compliance gibt es eine dedizierte Organisation bestehend aus Betrieb, Entwicklung, Auditoren und Testern. Sie sind verantwortlich für das Aufspüren und die Behandlung von Vorfällen inklusive deren Meldung und Nachverfolgung. Die Zusammenarbeit mit dem Kunden ist in den Oracle Hosting Policies beschrieben. Unterstützt wird der Betrieb darüber hinaus durch die Oracle Abteilungen Global Information Security, Global Product Security und der Rechtsabteilung Privacy & Security.

Der Zugriff auf Systeme durch Mitarbeiter (IT Staff) erfolgt rollenbasiert mit dafür vorbereiteten Devices. Diese Devices sind speziell aufgesetzt und abgesichert durch Vollverschlüsselung, Firewalls, AntiVirus & AntiSpam. Der Zugriff erfolgt verschlüsselt (SSH, SFTP, SSL) über VPN Software mit 2-Faktor Authentifizierung. Ein Einzelfallnachweis als Begründung für einen Zugriff ist Voraussetzung. Beim Zugriff wird über ein VDI Image oder Bastian Hosts gearbeitet. Der Zugriff wird protokolliert (Keystroke Logging).

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

FOR MORE INFORMATION

Contact: 1.800.ORACLE1

ORACLE

Integrated Cloud Applications & Platform Services

Ausgewählte Prozesse

Patching

Die Verantwortlichkeit für die Durchführung des Patching ist je nach Service definiert. Wird Software auf einer Oracle Cloud Plattform von Kunden installiert, sind diese für das Patchen und das Bereitstellen der Patches verantwortlich. Im Falle von Oracle Cloud Services, die teilweise von Kunden verwaltet werden, wie zum Beispiel Database as a Service, werden Patches im Cloud Portal des Kunden bereitgestellt. Das Patching wird damit durch den Kunden gesteuert. Bei von Oracle gemanagten Services, wie zum Beispiel Oracle Database Schema Cloud Service oder Compute Hypervisor, werden die Patches von Oracle eingespielt. Dafür werden periodische Wartungsfenster definiert, zum Beispiel alle zwei Wochen für Bundle Patches, Service Packs, alle vier Monate für Upgrades von Anwendungen und jährlich für einen Infrastruktur Upgrade. Dabei werden Zeiten mit geringer Nutzung (21:00-06:00) gewählt. Die Planung ist im Cloud Customer Portal mit einem Vorlauf von fünf Tagen einsehbar, ausgenommen davon sind Notfall-Wartungsarbeiten.

Backup

In Produktionssystemen übernimmt Oracle die Backups von Datenbanken und für den unterliegenden Code. Logdaten werden archiviert. Beides sind interne Sicherungen, die in der Regel Oracle vorbehalten sind. Diese Sicherungen erfolgen täglich auf Platte und zweimal pro Woche auf Band. Die Aufbewahrung der Bänder erfolgt Off-Site durch einen „certified for tape vault“ Anbieter für fünf Wochen. Die Speicherung erfolgt verschlüsselt (AES 256). Der Wiederherstellungsprozess der Bänder wird regelmäßig getestet.

Ein Backup einzelner Services kann durch den Kunden durchgeführt werden. Entsprechende Funktionen sind je nach Service enthalten wie zum Beispiel beim DBaaS. Die Konfiguration übernimmt dabei auch der Kunde, zum Beispiel in Form eines Backups in die gleiche VM, auf einen externen Storage oder mit dem Datenbank Backup Service.

Disaster Recovery

Im gerade beschriebenen „internen“ Backup Prozess sind die Vorgaben zu den Service Level Objectives mit 99,95% einzuhalten (genaue Definition siehe Hosting Policies). Hierzu kann eine Erweiterung des Vertrags erfolgen, so dass ein Recovery Punkt nicht älter als eine Stunde ist und das Recovery nicht länger als 12 Stunden dauert. Kunden können das Disaster Recovery natürlich auch selbst aufsetzen, zum Beispiel mit kurzen Recovery Points oder Replikationsmechanismen.

Das Disaster Recovery wird regelmäßig getestet: wöchentlich in Laborumgebungen, vierteljährliche Verprobungen und periodisch mit destruktiven Tests.

Daten nach Beendigung der Cloud Nutzung

Wird die Nutzung der Cloud beendet, wird Oracle die Umgebungen oder Daten so löschen, dass auf sie nicht mehr zugegriffen werden kann. Entsprechende gesetzliche Vorgaben werden berücksichtigt. Im Rahmen einer Karenzzeit ist es dem Kunden noch möglich die Daten ausgehändigt zu bekommen. Genaueres ist in den Oracle Hosting Policies beschrieben.

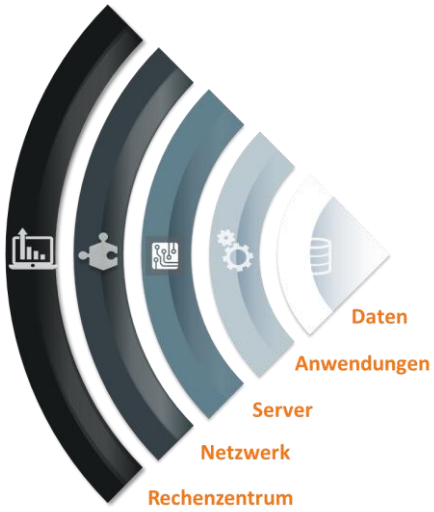
Auditing und Governance

Um die Governance hinsichtlich der Oracle Cloud zu prüfen, erfolgen täglich Scans der Services hinsichtlich der Vorgaben und möglicher neu entdeckter Schwachstellen. Täglich wird auch der eingesetzte Sourcecode gescannt. Einmal im Quartal findet eine gesonderte Überprüfung bezüglich Patches und Versionen statt.
Zugriffsrechte werden monatlich mit Hilfe eines webbasierten Prozesses verifiziert (im sogenannten Attestation Prozess). Die Zugriffe von Cloud Operations werden regelmäßig auf deren Rechtmäßigkeit hin überprüft.

Neben den eigenen Überprüfungen kommen noch regelmäßige Scans durch externe Auditoren hinzu, sowie entsprechende Zertifizierungen. Kunden ist es auch möglich, eigene Audits zu beantragen.

Eingesetzte Technologien und physischer Schutz: „Defense in Depth“

Am „Defense in Depth“ Modell von Oracle wird im Folgenden der logische Aufbau der Oracle Public Cloud kurz dargestellt.



Schalenmodell / Defense in Depth

Die Zufahrt und der Zutritt werden über **physische** Schutzmechanismen des jeweiligen Datacenters und Wachpersonal gesichert. Die Datacenter selbst sind an Versorgungen redundant angebunden. Die Verifikation erfolgt über Zutrittskarten und biometrische Erkennung gegen ein entsprechendes Berechtigungssystem. Der Zugang wird protokolliert. Innerhalb des Gebäudes erfolgt Videoüberwachung und eine Absicherung durch Bewegungsmelder. Es besteht eine weitere Unterteilung innerhalb des Gebäudes mit abgeschotteten Zonen.

Im **Netzwerk** sind verschiedene Zonen vorhanden, die durch Firewalls getrennt sind. Diese führen auch eine Paketinspektion durch. Die möglichen Protokolle für in- und outbound Netflows werden getrennt konfiguriert. Die Verbindungen sind in der Regel verschlüsselt. Whitelisting (erlaubte IP Adressen) wird eingesetzt. Beide Bereiche sind in einem gewissen Rahmen auch durch den Kunden konfigurierbar. Virtual Private Networks (VPN) stehen in der Regel für die Integration des Netzwerks zur Verfügung. Die Infrastruktur inklusive des Netzwerks wird überwacht und die Ereignisse an ein Security Information und Event Management übertragen. Network Intrusion Detection Systeme kommen zum Einsatz. Vorgeschaltet sind Systeme zur Verhinderung von Denial of Service (DOS) und Layer 3-7 Angriffen.

Auf den **Servern** werden in der Regel gehärtete Oracle Enterprise Linux Kernel eingesetzt. Verfügbare Protokolle sind limitiert, nicht benötigte Services entfernt oder ausgeschaltet, und unnötige Benutzeraccounts gelöscht. Es erfolgt ein „aggressives“ Patch Management und eine ausgewogene Protokollierung (Logging). Beim Härten werden die Vorgaben vom Center for Internet Security, National Institute of Standards and Technology und SANS Institute genutzt.
Für das Konfigurationsmanagement kommen Tools wie Chef bzw. Puppet zum Ansatz. Auf den Servern erfolgt ein File Integrity Monitoring. Es gibt ein gesondertes privilegiertes Benutzermanagement auf jedem Layer, Host, DBMS, Applikation. Bei der Nutzung der Privileged Accounts werden alle Aktionen in einem Auditlog festgehalten.

In der **Anwendungsschicht** erfolgt der Zugriff in der Regel verschlüsselt, meist via https/TLS. Der Anwendungsschicht liegt ein Identity- und Accessmangement zugrunde, das vorgefertigte Rollen bietet und eine Erweiterung um Rollen und Benutzeraccounts ermöglicht. Die Password Policies sind konfigurierbar und ermöglichen die Stärke der Authentifizierung (starke Authentifizierung), je nach eingesetztem Verfahren, zu ändern. Teilweise erfolgt eine Trennung in das Identity- und Accessmanagement der Cloud und das des Anwendungslayers, zum Beispiel bei der Content Cloud. Es stehen auch Technologien zur Verfügung um das Berechtigungssystem in das gegebenenfalls vorhandene lokale System zu integrieren, sei es mit Single Sign On oder mit der Benutzerverwaltung. Daten, die in der Anwendung verwendet werden können, sind in der Regel verschlüsselt und zugriffsbeschränkt. Typischerweise werden bei der Nutzung auf Basis des Netzwerks und an/in der Anwendung Logdaten gespeichert.

Die Speicherung der **Daten** und deren Zugriff erfolgt im Standardfall verschlüsselt, in der Datenbank mit Oracle Transparent Data Encryption (AES) und im Object Storage mit AES. Auch Cloud Backups zum Beispiel von Datenbanken unterliegen diesem Mechanismus, wobei hier in On-Premise Installationen nicht die entsprechende Datenbankoption (Advanced Security Option) benötigt wird. In allen Fällen kann/muss der Schlüssel lokal beim Kunden gelagert bzw. verwaltet werden.

Oracle Cloud Operations hat in der Regel keinen Zugriff auf die verschlüsselten Daten, die Virtual Machines oder Bare Metal Cloud Server der Kunden.

Von Kunden verantwortete Security

„Shared Responsibility“ ist die Basis der Cloud Modelle. Eine Basissicherheit ist im Service in Anlehnung an das Prinzip „Security Always On“ enthalten oder wird über Cloud Operations konfiguriert. Ein Kunde hat darüber hinaus die Möglichkeit, die im Service vorgesehenen sicherheitsrelevanten Funktionen zu konfigurieren und ist andererseits auch verantwortlich für die Absicherung der Services. Dies umfasst:

- Steuerung: Wer kann unter welchen Bedingungen auf welche Daten zugreifen (klassisches Identity und Access Management IAM), welche Systeme in der Cloud nutzen welche Protokollflüsse (Netzwerk- und Firewallkonfiguration VCN)?
- Prüfung: Welche sicherheitsrelevanten Konfigurationen wurden vorgenommen?
- Kontrolle: Wer hat wann zugegriffen?

Die Funktionen werden im Cloud-Portal für die übergreifende Verwaltung bereitgestellt und teilweise, soweit spezialisiert, innerhalb der Services angeboten.

Die Sicherheit kann auch mit zusätzlichen Services wie dedizierte Zugriffswege (Fast Connect) oder Cloud Security Services (zum Beispiel starke Authentifizierung mittels Identity Cloud Service) erweitert werden.

Zertifizierungen, gesetzliche Vorgaben und Security Reports

Oracle Public Cloud Security besteht in der Regel aus zwei Bestandteilen, dem Datacenter und den Cloud Services. Für Zertifizierungen und Regularien sind daher beide Teile relevant. Im Falle der Datacenterbetreiber sind die Informationen auf deren Webseite hinterlegt, im Falle von Oracle kann, sofern die Information nicht bei Oracle auf der Webseite verfügbar ist, beim entsprechenden Kontakt angefragt werden.

Das Vorgehen von Oracle sieht in einem ersten Schritt eine SOC1 und SOC2 Compliance inklusive der entsprechenden Reports vor, nachgelagert dann ISO 27001 und gegebenenfalls PCI-DSS, sowie andere spezifischere Zertifizierungen. In Bezug auf das EU Datenschutzgesetz (EU GDPR) finden entsprechende Überprüfungen statt (Stand 7/2017).

Die Zertifizierungen und Prüfungen sind je nach betrachtetem Service verschieden, so dass hier im Einzelfall spezifische Zertifizierungen angefragt werden können. Beispielsweise ist der Datenbank Service (PAAS – DBaaS) ISO27001 zertifiziert. Auch gibt es spezielle Cloud Umgebungen, für die andere Zertifizierungen vorhanden sind - wie UK Governance Cloud oder die Cloud@Customer.

Die Zertifizierungen und Reports können über den zuständigen Oracle Ansprechpartner angefordert werden. Daneben gibt es weitere Reports für Cloud Kunden:

- Cloud Security Alliance Questionnaire v3 (cloudsecurityalliance.org)
- Disaster Recovery Test Report
- 3rd party Penetration Test Report & Application Security Assessment Report
- Infrastructure Security Scanning Report

Kunden können außerdem eigene Audits und/oder einen Besuch des entsprechenden Datacenters anfragen.

Anbindung an das Kundennetzwerk/VPN

Je nach Cloud Service und Datacenter stehen verschiedene Möglichkeiten zur Integration der Nutzer und Provider-Netzwerke zur Verfügung.

VPN durch Kunden installiert

Für einen Teil der IaaS und PaaS Services hat der Kunde einen SSH Zugang. Über diesen kann Software installiert werden wie zum Beispiel ein eigenes VPN. Im Cloud-Portal können entsprechende Zugänge freigeschaltet werden.

Oracle Corrente VPN

Mit Oracle Corente steht eine cloudbasierte Software zur Verfügung, mit der ein Kunde eine VPN Lösung ohne Hardwareappliance nutzen kann. Das Corente Services Gateway (CSG) bietet als virtuelle Appliance die sichere End-to-End Verbindung für IP Netzwerke. Mit dem Service Control Point (SCP) können Einstellungen getroffen werden, um policy-basiert Services zu vermitteln, zu steuern (Servicebroker), virtuelle Netzwerke zu orchestrieren, zu monitoren und zu protokollieren.

Oracle Network Cloud Service

Dies ist ein Site to Site VPN auf Basis von IPSec. Mit dem Oracle Network Cloud Service kann ein virtueller Tunnel zwischen dem lokalen Datacenter des Kunden und Oracle's Cloud Datacenter bereitstellt werden.

FastConnect

FastConnect ist ein Hardware VPN um ein Datacenter bzw. Netzwerk des Kunden direkt mit einem Oracle Cloud Rechenzentrum zu verbinden. Dies nutzt die Leitungen bzw. Bandbreiten die durch Provider wie Equinix bereitgestellt werden. Die Strecke Datacenter – Equinix Hub wird durch den Netzbetreiber des Kunden bereitgestellt.

Wahlfreiheit der Umgebung: Cloud@Customer

Für die Oracle Cloud-Umgebung ist es möglich das Datacenter selber zu wählen. Es gibt europäische Rechenzentren, zum Beispiel in Amsterdam (live) und Frankfurt. Die Rechenzentrums-Infrastruktur wird größtenteils von einem der großen Betreiber wie beispielsweise Equinix verwaltet und betrieben. Die IaaS/PaaS/SaaS Umgebungen werden von Oracle Public Cloud Operations betrieben.

Für diejenigen, die Cloud Services im eigenen Rechenzentrum betreiben wollen oder müssen, bietet Oracle mit „Cloud@Customer" (ehemals Oracle Cloud Machine) eine Appliance (Hardware und Software) an. Es handelt sich dabei um ein Abbild der Oracle Public Cloud mit einer Auswahl von Oracle IaaS und PaaS Services. Vorteile neben der "fertigen" Cloud Appliance sind das flexible Lizenzmodell der Oracle Public Cloud und die Verwaltung der Appliance durch Oracle. Beim Management profitieren Oracle Cloud Machine Kunden von der gleichen Erfahrung, Servicequalität sowie den neuesten Innovationen, die die Oracle Cloud kennzeichnen.

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

FOR MORE INFORMATION

Contact: 1.800.ORACLE1

ORACLE

Integrated Cloud Applications & Platform Services

Spezielle Cloud Security Services

Es gibt dedizierte Cloud Security Services, die keine Add-Ons zu bestehenden Cloud Services sind, sondern Services, die eigenständig genutzt werden können. Eine Integration einer Benutzerverwaltung und eines Monitoring kann damit auch für 3rd Party Clouds vorgenommen werden.

Es handelt sich um folgende Cloud Security Services:

» **Oracle Identity Cloud Service (IDCS)** stellt eine cloudbasierte Identity und Access Management (IAM) Plattform zur Verfügung. Damit können sowohl Mitarbeiter, Externe, Partner, Kunden und Dinge (zum Beispiel Geräte oder IoT) verwaltet und angebunden werden. Durch vorgefertigte Integrationen, sowohl bzgl. der Anbindung von On-Premise IDM Systemen als auch SSO Systemen ist eine einfache Nutzung möglich. Für den Benutzer ist der Service Dank SSO transparent. Oracle selbst hat diesen Service in seine neuen Oracle Public Cloud Services (OPC) eingebunden und die bestehenden OPC werden auf diese Plattform migriert. Ein mit OPC bestehender IDCS Service kann, je nach Lizenz, dann auch für andere Dinge genutzt werden.

  Tests mit dem Identity Cloud Service sowie weitere Informationen und Dokumentation unter https://cloud.oracle.com/en_US/identity. Der Service ist aktuell (Juli 2017) in den Oracle Rechenzentren in den USA und für EMEA in Amsterdam verfügbar

» Mit dem **Cloud Access Security Broker (CASB)** kann die Nutzung der Cloud Services überwacht werden, um einerseits eine Schatten-IT zu entdecken, und um andererseits die Cloud Nutzung bzgl. Missbrauch/Angriffen zu monitoren. Gängige Services wie Salesforce, Office365 oder AWS sind vorintegriert. CASB nutzt ein Identity Management System, zum Beispiel den IDCS, um Rückschlüsse auf den eingeloggten Benutzer ziehen zu können und im Rahmen des Vorfalls entsprechende Vorschläge machen zu können (zum Beispiel Deaktivieren des Accounts im IDCS oder Rücksetzen der Konfiguration in einem Account).

  Weitere Informationen hierzu: https://cloud.oracle.com/en_US/casb

» **Cloud Security Monitoring Services** sollen zur Überwachung verdächtiger Operationen in Cloud und On-Premise Umgebungen eingesetzt werden. Hierbei ist meist der vermeintlich genutzte Account und dessen Berechtigungen oder die Berechtigungshistorie von Interesse. Der Service war im Juli 2017 noch nicht freigeschaltet.

  Weitere Informationen hierzu:
  Security Monitoring https://cloud.oracle.com/en_US/security-analytics
  Compliance zu Konfigurationen: https://cloud.oracle.com/en_US/compliance

Mit CASB und den Monitoring Services können in einem Security Operations Center (SOC) die Cloud Umgebungen überwacht bzw. Richtlinien zur sicheren Konfiguration umgesetzt werden. Diese Services können natürlich auch als Input für ein bestehendes Security Information und Event Management (SIEM) System genutzt werden.

Technologische Prinzipien auf einen Blick

Aus technologischer Sicht kommen folgende Prinzipien zum Tragen:

- Schutz jeder Schicht („protect every layer“)
- Schutz beginnt im Stack so früh wie möglich („push down security the stack“)
- Schutz als Standard (security should always be on”)
- Eine übergreifende IT Sicherheitsarchitektur über Systeme (On-Premise) und Cloud hinweg
- Wahlmöglichkeit der Ablaufumgebung der Komponenten: On-Premise, Cloud, Cloud@Customer, Hybrid
- Spezielle Cloud Security Services zur Absicherung der Oracle und 3rd Party Clouds

Fazit

Oracle bietet mit der Oracle Cloud die Nutzung von sicheren IaaS, PaaS und SaaS Cloud-Services. Diese werden entweder aus einem Cloud Rechenzentrum heraus oder mit der Oracle Cloud Machine (Cloud@Customer) im Rechenzentrum des Kunden oder dessen Hoster bereitgestellt.

Durch Verwendung gleichartiger Technologien in den Cloud Services wie in lokal installierten Oracle Produkten kann das schon gewonnene Know How weitergenutzt und mit den gleichen Security Policies abgesichert werden. Auch lassen sich Szenarien wie das Verschieben in die Cloud, Lift&Shift, Testen in Cloudumgebungen oder eine hybride Nutzung abbilden.

Zusammengefasst besteht die Oracle Cloud aus sicheren Produkten, die in einer Sicherheitsarchitektur bereitgestellt werden. Sie wird unter Berücksichtigung von Sicherheitsgesichtspunkten ausgerollt, sicher betrieben und regelmäßig durch Unabhängige überprüft. Das folgende Bild zeigt die Adoption durch unsere Kunden:

Snapshot Oracle Cloud Betrieb

Weitere Informationen

- Oracle Cloud sowie weitere Informationen und Dokumentation unter https://cloud.oracle.com
- Definition der Oracle Public Cloud, die Policies: http://www.oracle.com/us/corporate/contracts/cloud-services/index.html
- Weiterführende Informationen zu Security & Oracle finden Sie im Internet unter http://www.oracle.com/security.