Oracle Beiträge zur IT- und Cyber-Sicherheit für die Öffentliche Verwaltung und das Gesundheitswesen

ORACLE
Cloud

IT-SICHERHEIT – BESTANTEIL DER NATIONALEN EGOVERMENT STRATEGIE

Die öffentliche Verwaltung unterliegt ebenso wie die gesamte Wirtschaft einem signifikanten Veränderungsdruck, der sich in IT-Konsolidierung des Betriebs, Modernisierung der IT-Verfahren und neuen Services für die Verwaltung sowie für Bürger und Wirtschaft niederschlägt. Cloud basierte Lösungen unterstützen die Konsolidierungsprozesse und die Effizienz von Dienstleistungszentren für ein breites und modernes Serviceangebot auf allen Ebenen der öffentlichen Verwaltung und helfen dem Staat schnell auf äußere Einflüsse zu reagieren. Die Sicherheit von Daten und Prozessen bekommt vor diesem Hintergrund einen deutlich höheren Stellenwert. Die Bedrohungen für die Bürgerinnen und Bürger sowie für Wirtschaft und Verwaltung durch Cyberangriffe machen zusätzlich erhöhte Schutz- und Abwehrmaßnahmen erforderlich.

In der Nationalen eGovernment Strategie für den Public Sector wird IT-Sicherheit mit hoher Priorität bewertet. Der IT-Planungsrat hat eine „Leitlinie Informationssicherheit“ verabschiedet, welche konkrete Ziele zur Gewährleistung von Datenschutz und Datensicherheit formuliert und Handlungsempfehlungen für Bund, Länder und Kommunen beschreibt. Diese bestehen im Wesentlichen aus:

- Einheitlichen Standards zum Einsatz sicherer, datenschutzgerechter und interoperabler Lösungen, Realisierung eines einheitlichen Informationssicherheitsmanagements sowie kontinuierliche Information und Qualifierung der Mitarbeiter
- Gewährleistung des technischen und organisatorischen Datenschutzes, insbesondere Verfügbarkeit, Vertraulichkeit, Integrität, Transparenz, Nichtverkettbarkeit (als technische Sicherung der Zweckbindung) und Intervenierbarkeit (als technische Gestaltung von Verfahren zur Ausübung von Betroffenenrechten)
- Sicherstellung der Funktionsfähigkeit des E-Government auch in Krisensituationen. Handlungsfelder hierfür sind insbesondere durch die Umsetzung der gemäß dem "Nationalen Plan zum Schutz der Informationsinfrastrukturen" notwendigen Maßnahmen im Rahmen des Umsetzungsplans KRITIS sowie die Umsetzung der zwischen Bund, Ländern und Kommunen gemeinsam definierten Verfügbarkeitsanforderungen und Maßnahmen

Oracle unterstützt die Umsetzung dieser Ziele mit Hilfe seiner bewährten Technologien. Sicherheitsfunktionalitäten werden in allen Oracle Produkten zur Verfügung gestellt und durch deren maßgeschneiderten Einsatz lassen sich die unterschiedlichsten Sicherheitsanforderungen abbilden.

Eine große Zahl von Behördenkunden in Deutschland und weltweit vertraut auf die Oracle Produkte und setzt diese in unternehmensskritischen Anwendungen ein.

IT-GRUNDSCHUTZ UND IT-SICHERHEITSGESETZ

Sowohl in Deutschland, als auch auf europäischer Ebene gibt es seit Mitte der 90er Jahre verstärkte Bestrebungen, die internationalen Sicherheits- und Schutzerwartungen an die Datenverarbeitung gesetzlich zu vereinheitlichen. Das ist nicht weiter verwunderlich, weil sich sowohl die kommerzielle IT als auch Geschäftsmodelle auf Basis von Sozialen Medien, in den 90`er Jahren durch das Internet und jetzt im Rahmen der Cloud Angebote massiv globalisiert haben. Sicherheit hat dadurch einen völlig neuen Stellenwert bekommen. Meilensteine in der Entwicklung dieser gesetzlichen Regelungen waren unter anderem die EU Datenschutz-Richtlinie von 1995 mit der Vorgabe, den EU-Wirtschaftsraum zu harmonisieren, sowie beispielsweise auch die Ausarbeitung der Schutzziele für „Kritische Infrastrukturen“ in Deutschland, im Kontext der nationalen Cyber-Sicherheitsstrategie. Seit 2007 wurden solche Schutzerwartungen, in Vorbereitung auf das 2015 verabschiedete deutsche IT-Sicherheitsgesetz (ITSiG), im Rahmen der zwei Initiativen „UP-BUND“ und „UP-KRITIS“, gesetzlich vorbereitet.

Insofern sind sowohl für die „Kritischen Infrastrukturen“ aber auch für Bundesbehörden ISMS und IT-Sicherheitskonzepte nach IT-Grundschutz, regelmäßige IS-Revisionen sowie die Meldung von Sicherheitsvorfällen verpflichtend.

Durch die starke internationale gesetzliche Verankerung von IT-Sicherheit und die hohen Auflagen, denen Behörden und Unternehmen bezüglich der Compliance in der Umsetzung und Einhaltung der Regelungen unterliegen, wird deutlich, dass IT-Sicherheit eine Führungsaufgabe ist und über den gesamten Lebenszyklus von IT-Verfahren und Architekturen berücksichtigt werden muss.

Oracle kann seine Kunden bei der Umsetzung und Implementierung der IT-Sicherheit durch den adäquaten Einsatz spezifischer Oracle Produkte unterstützen und entsprechend der Kritikalität der Anwendungen auf Basis gemeinsam vom Kunden mit Oracle durchzuführender Security Checks Empfehlungen aussprechen.

Mit Hilfe der Oracle Enterprise Management Funktionalitäten ist es so zum Beispiel möglich, Anforderungen aus dem BSI IT-Grundschutz abzubilden und in ein übergreifendes ISMS einzubinden.

Ziel der Schutzmaßnahmen sind Prävention und aktive Angriffsabwehr. Sowohl gegen Gefahren von außen, aber auch gegen kriminelle Manipulationen von innen. Alle Regularien verweisen im Zusammenhang mit der Herstellung von Sicherheit auf „TOM“, also auf den Einsatz adäquater technischer und organisatorischer Maßnahmen, um Missbrauch und fahrlässige Datenverluste zu verhindern. Das Kriterium der Geeignetheit der Maßnahmen wird dabei als „gemäß dem Stand der Technik“ verstanden. Die Regularien halten allerdings die Definition dessen, was „dem Stand der Technik“ entspricht, absichtlich sehr vage. Das ist unter praktischen Gesichtspunkten sehr gut nachvollziehbar, weil die jeweiligen IT-Umgebungen eine sehr hohe Heterogenität aufweisen, also sehr unterschiedlich sind und im Detail möglicherweise unterschiedlicher Sicherheitsmittel bedürfen.

EUROPÄISCHE DATENSCHUTZ GRUNDVERORDNUNG

Seit 25.05.2018 entfaltet die Europäische Datenschutz-Grundverordnung (EU-DSGVO) nach zweijähriger Einführungsfrist unmittelbare gesetzliche Wirksamkeit. Gemäß der DSGVO sind Behörden und Unternehmen aufgefordert, ihre Prozesse, Mitarbeiter und technischen Infrastrukturen „compliant“ zu den Vorgaben der Verordnung zu machen. Im Gegensatz zum ITSiG bezieht sich die DSGVO „nur“ auf „als besonders schützenswert eingeordnete“ personenbezogene Daten. Das ITSiG ist quasi das Pendant zur EU-DSGVO hinsichtlich der Daten ohne primären Personenbezug.

Der besondere Charakter der DSGVO stellt allerdings die weltweite Gültigkeit der gesetzlichen Regelung dar, obwohl es sich nur um ein europäisches Gesetz handelt. Wenn europäische Datensubjekte Teil von IT-Prozessen außerhalb der EU sind, dann unterliegen diese Prozesse in den entsprechenden außereuropäischen Staaten auch den gesetzlichen Vorschriften der EU-DSGVO.

Wir gehen davon aus, dass ein robustes Fundament in den Bereichen Infrastruktur und Organisation die Basis für erfolgreiche Unternehmen und Verwaltungen ist, welches ihnen hilft, wirtschaftliche oder gesellschaftliche und politische Schocks abzufedern und sie vor existenzbedrohenden Krisen bewahrt.

Verstöße gegen die gesetzlichen Bestimmungen werden mit drakonischen Strafen geahndet.

Obwohl die Behörden von den unmittelbaren monetären Sanktionen ausgenommen sind, unterliegen sie trotzdem den gleichen Regeln der Sorgfaltspflicht wie Unternehmen, wenn es um den Einsatz der technischen Sicherheitsmittel geht.

Im juristischen Kontext der EU-DSGVO verweisen die Artikel 25 und 32 dediziert auf das Kriterium „Stand der Technik“. Als „Stand der Technik“ wird verstanden und akzeptiert, wenn sich die Umsetzung der gesetzlichen Regelungen auf internationaler Ebene, und durch die entsprechenden Gremien begutachtet, auf den „breiten“ Einsatz von Sicherheitsfunktionen der maßgeblichen Technologieanbieter stützt.

Die Generierung geeigneter Sicherheitsfunktionen ist insofern ein infiniter Prozess, als sich die IT-Umgebungen permanent verändern und die Angriffsszenarien immer ausgeklügelter werden. Das muss zwangsläufig zu Systemen führen, die „in sich“ intelligent und autonom agierend gemacht werden.

IT-Sicherheit im Sinne der Compliance zu den Regularien gemäß der EU-DSGVO und dem ITSiG muss daher permanent auf Geeignetheit und Effizienz überprüft werden, damit Behörden und Unternehmen ihrer Sorgfaltspflicht, wie sie zum Bespiel in Artikel 5 der DSGVO formuliert ist, entsprechen.

Oracle ist einer der internationalen Marktführer im IT-Bereich und Oracle Produkte können dabei helfen, die in der EU-DSGVO vorgesehenen Maßnahmen umzusetzen. Oracle nimmt seit Jahrzehnten eine unbestrittene Führungsrolle im Bereich der Datensicherheit ein. Oracle hat innovative Datensicherheitsprodukte entwickelt und hilft Organisationen dabei, Angriffe aus den verschiedensten Bedrohungsszenarien abzuwenden.

DER ORACLE ANSATZ

Seit Gründung von Oracle ist Sicherheit eine treibende Kraft – vor allem die Erfahrungen bei Sicherheitsbehörden haben wesentlich zum Erfolg des Unternehmens beigetragen und die Entwicklung der Oracle Produkte und Services nachhaltig geprägt.

Auf dem Weg zum Cloud-Computing und angesichts der Cyber Herausforderungen stellt Sicherheit nach Auffassung von Larry Ellison, Oracle's Chief Technology Officer und Chairman, die größte Herausforderung für die IT-Industrie dar. Oracle antwortet darauf mit sich selbst absichernden Systemen **(„self-securing" bzw. „autonomous")** und **technischen Sicherheitsfunktionen.**

Technische Sicherheitsfunktionen

Die technischen Sicherheitsfunktionen sind mit „End-to-End Security" bzw. Defense in Depth bekannt und lassen sich zusammenfassen in:

- Schutz jeder Schicht, von der Anwendung bis zur Hardware (protect every layer)
- Schutz beginnt so "tief" wie möglich (push down security the stack)
- Schutz im Standard (security should always be on)

Oracle bietet in den Komponenten der einzelnen Schichten die entsprechenden Funktionen wie beispielsweise Verschlüsselung in der Datenbank oder bei der Kommunikation mit der Datenbank.

„self-securing" bzw. „autonomous"

Sich selbst absichernde Systeme sind seit der Ende 2017 unter dem Begriff „autonomous" bei Oracle zu finden. Sie sind die Antwort auf die immer komplexer werdende Aufgabe bestehende und die stetig wachsende Anzahl von Systemen in On-Premises und Cloud-Umgebungen kontinuierlich abzusichern und der zunehmenden Intelligenz in Cyber-Attacken entgegenwirken zu können. Security relevante Merkmale dieser Systeme sind dabei:

- Automatisches einspielen von (Security) Patches
- Überwachung des Betriebs hinsichtlich interner und externer Threats und deren Abwehr
- Überwachung sicherheitsrelevanter Konfigurationen
- Hochverfügbarkeit und Disaster Recovery

Hier wird in großem Stil Machine-Learning eingesetzt, um auch außerhalb eines starren Regelwerks flexibel und automatisiert reagieren zu können.

Integration und Aufbau einer Sicherheitsarchitektur

Um Kunden eine höchstmögliche Effizienz bieten zu können besitzen die Oracle Komponenten eine Vorintegration in eine Sicherheitsplattform. Die Sicherheitsplattform teilt sich in den Bereich Monitoring (u.a. SIEM, IT Compliance, Identity SOC, Trust Fabric) und Durchsetzung von Policies (u.a. Identity& Access, Governance, Verschlüsselung). Selbstverständlich können die Komponenten auch einzeln eingesetzt und in andere Sicherheitsplattformen integriert werden.

Oracle Komponenten unterstützen die Verwendung einer gemeinsamen Sicherheitsarchitektur. Unabhängig davon wo die Komponenten laufen können meist die gleichen Policies und Mechanismen verwendet werden wie beispielsweise eine starke Authentifizierung abhängig des Kontexts bei sensitiven Services.

Durch die steigende Nutzung von Cloudansätzen sind oft mehrere Typen von Umgebungen im Einsatz. Klassische On-Premises Installationen, externe Cloudservices, gehostete Clouds (z.B. Cloud at Customer), interne Cloudansätze bzw. hybride Umgebungen. Oracle unterstützt diese Modelle teilweise naheliegend durch Verwendung identischer Produkte oder durch gemeinsam verwendete Standards bzw. Schnittstellen.

Oracle investiert nachhaltig und signifikant in den Security Bereich. Bestehende Produkte werden um Sicherheitsfunktionen weiterentwickelt, neue Security Services geschaffen, Automatisierung vorangetrieben und Firmen auch im Bereich Security akquiriert. Ziel ist die kontinuierliche Verstärkung der Absicherungsmöglichkeiten von Daten und Services.

Das Oracle Produkt- und Lösungsportfolio umfasst Unternehmenssoftware, Business Intelligence, Middleware, Identity Management, Standardsoftware für Datenbanken, Server und Storagesysteme sowie Cloud Services, Support und Consulting. Alle verfügbaren Innovationen in die IT-Sicherheit werden unseren Kunden im Rahmen von Supportverträgen über die Auslieferung neuer Releases und Erweiterungen angeboten. Auch in diesem Zusammenhang sind Investitionsschutz, Wirtschaftlichkeit, Vereinfachung und Beherrschbarkeit die Grundprinzipien unserer Produkt- und Lösungsentwicklung.

ORACLE IT-DATEN- UND ANWENDUNGSSICHERHEIT

Kaum eine Behörde arbeitet heutzutage ohne IT-Systeme. Durch die sukzessive Einführung von IT-Komponenten sind häufig Einzellösungen entstanden, die meist ihre eigene Anwender-, Rechteverwaltung und Datenschutz mitbringen. Die Verteilung der IT-Systeme im eigenen Rechenzentrum oder der Cloud birgt eine weitere Herausforderung. Diese verursacht bei der Verwaltung und Wahrung der Compliance einen hohen manuellen Aufwand und verhindert einen zentralen Blick auf den aktuellen Stand der IT-Datensicherheit.

Vorrangiges Ziel für die IT-Architektur jedes Unternehmens ist, dass die Daten zuverlässig verfügbar sind (Ausfallsicherheit, Hochverfügbarkeit, Integrität) sowie jederzeit nur von berechtigten Personen einsehbar sowie zu bearbeiten sind. Weder sollen kritische Informationen aus dem Behördennetz oder der Cloud unberechtigt heraus gelangen, noch dürfen Daten von Unbefugten verändert werden können. Bedrohliche Sicherheitslücken sind nicht nur von außen zu schließen, sondern auch von innen.

Verschiedene Untersuchungen von "Angriffen" oder "Compliance Verletzungen" zeigen, dass es auch im Nachhinein nicht die eine Komponente gibt, die einen Rundumschutz gewährleistet hätte. Die Zunahme der Vorfälle bzw. deren Analyse zeigt auch, dass es nicht ausreicht den Perimeter, also die Firewall, zu verstärken. Im Rahmen der Digitalisierung beispielsweise muss es Zugriffe von außen durch die Firewall geben. Zudem können problematische Zugriffe auch von innen kommen. Neben der Zunahme einzuhaltender Regularien oder deren Konkretisierung kam nun im Rahmen des EU-Datenschutzgesetzes auch eine Auskunftspflicht hinzu. Behörden müssen u.a. nachweisen wie sie im Einzelnen die - hier personenbezogenen - Daten schützen und welche Daten sie gespeichert haben.

VORTEILE MIT ORACLE

Das Produktportfolio von Oracle zur IT-Sicherheit von Daten und Anwendungen erfüllt die Anforderungen, die heute an die Behörden-IT gestellt werden. Gleichzeitig schafft Oracle Mehrwerte wie:

- **Kostenersparnis:** Dank des integrativen Ansatzes wird der Verwaltungsaufwand über alle betroffenen IT-Systeme On-Premises und in der Cloud hinweg spürbar gesenkt. Zusätzlich wirkt sich die erreichte höhere Transparenz kostensenkend aus, z.B. beim Berichtswesen

- **Vereinfachte Nutzung:** Für den Endnutzer bedeuten einfachere und flexiblere Nutzung von Systemen eine deutliche Entlastung. Authentifizierung (inkl. SingleSignOn) und Kennwortmanagement werden vereinfacht, das Beantragen, Genehmigen, Anlegen, Ändern und Löschen von Benutzern und Rechten beschleunigt und verbessert. Der Endnutzer sieht Daten und Funktionen im Rahmen des erlaubten Kontexts (z.B. Zugriff nur mit registriertem Device). Administratoren werden vor einer Fehlnutzung geschützt

- **Erhöhte Sicherheit:** Der korrekte Umgang mit personenbezogenen Daten und das Einhalten von Sicherheitsrichtlinien wird erheblich erleichtert. Auch Dank eindeutiger Identifikation aller Beteiligten wird das „Sicherheitsbewusstsein“ in der Verwaltung gestärkt

- **Compliance:** Die Komponenten ermöglichen den revisionssicheren Nachweis ausreichender Risikovorsorge und legen die Grundlage für automatisiertes Auditing von IT-Prozessen. Dadurch kann das Haftungsrisiko verringert und das Vertrauen in Systeme und Prozesse gestärkt werden

Oracle ist aufgrund seiner eigenen Innovationsstrategie sowie durch den gezielten Zukauf von führenden Spezialanbietern in der Lage, ein Portfolio von Lösungskomponenten im Bereich IT-Datenschutz anzubieten, welche von Verschlüsselung, Anonymisierung, Datenseparation, Zugangskontrolle, Federation, Provisioning, API Management, Service Management bis zu Cloud Security Services reichen und die sich dank ihrer Offenheit sehr gut in bestehende Systemlandschaften integrieren lassen. Die Lösungs-Suite bietet Komponenten für On-Premises als auch als Cloud Service und unterstützt ein hybrides IT Sicherheitsmodell. Mit seinem Gesamtportfolio und seiner über Jahre hinweg erworbenen Lösungskompetenz ist Oracle der richtige Partner, wenn es darum geht, die Behörden-IT fit für die IT-Datenschutz-Anforderungen von morgen zu machen.

WOMIT BEGINNEN?

Der Fokus beim Einsatz ist natürlich abhängig von den Zielen und Anforderungen einer Verwaltung und immer individuell. Häufige Anforderungen, die genannt werden, sind:

- Umbau Silos in eine zentrale Anwenderkontenverwaltung und/oder SingleSignOn System
- sicherheitsrelevante Vorgaben für Mobile App Entwicklung
- Umgang mit DevOps und zentralen Sicherheitsvorgaben
- Integration von Blockchains in die Sicherheitsarchitektur
- Einführung einem aktuellen und zentralen Berichtswesen, um im Bereich Auditing und Compliance zu unterstützen
- Umsetzung von Schutzmaßnahmen je nach Klassifikation der Daten und Anwendungen
- Öffnung für Nutzung von kontrollierten Zugriffen durch mobile Endgeräte oder API Zugriffe sowohl für Mitarbeiter, Partner als auch Endkunden
- Aufbau oder Umbau einer sicheren Plattform für die Anforderung im Bereich Digitalisierung

- sichere transparente Nutzung von Cloudangeboten
- Integration sozialer Netzwerke

Oracle unterstützt eine Vielzahl von Lösungsansätzen und Herangehensweisen, exemplarisch sind das:

- Verschiedene Datentöpfe mit Anwenderinformationen für die Anmeldung virtuell, d.h. ohne Synchronisation und redundante Datenhaltung, zusammenführen (Oracle Virtual Directory)
- Den Zugriff auf Web-Applikationen konsolidieren und einschließlich Single Sign-On ermöglichen (Oracle Access Management Suite. Single Sign-On auch für Client-Server Applikationen, die nicht web-fähig sind ermöglichen (Oracle Enterprise Single Sign-On)
- Bewertung des Risikos beim Zugriff und dadurch gesteuert weitere Maßnahmen bei Applikationszugriffen (Oracle Adaptive Access Manager)
- Anwenderkontenverwaltung erleichtern sowie ein zentrales Berichtswesen aufbauen – wer hat was? (Oracle Identity Manager)
- Aufbau unternehmensübergreifender Netzwerke; kompatibel mit Standards wie SAML, WS-Federation, Liberty Alliance, OAuth/OpenIDConnect (Oracle Access Management)
- Unterstützung bei Audits, Re-Zertifizierungen und Prozessen bzgl. Compliance Anforderungen (z.B. SOX, MaRisk) (Oracle Identity Governance)
- Integrationsmöglichkeiten sozialer Netzwerke in z.B. das Behördenportal (Oracle Access Management)
- Absicherung bestehender APIs, z.B. im B-to-B Umfeld oder bei der Integration in Marktplätze. Bereitstellung vorhandener Services für Anwendungen/Apps auf mobilen Endgeräten (Oracle API Cloud Service)
- Aufbau, Integration oder Nutzung der Vorintegration von „permission-basierten“ Blockchains in eigene Anwendungen (Oracle Blockchain Service)
- Aufbau einer Plattform für Security Monitoring zur Erkennung von verdächtigem Verhalten interner und externer Benutzer sowie sicherheitsrelevanter Konfigurationsänderungen (Oracle Management Cloud Security Monitoring und Configuration Compliance)
- Unterstützung eines hybriden Identity Management (Oracle Identity Cloud Service)
- Überwachung der Nutzung Oracle und 3rd Party IaaS, PaaS und SaaS Cloud Services (Oracle Cloud Access Security Broker)

ÜBERBLICK ZUR IT-DATENSICHERHEIT IM BEREICH ANWENDUNGEN UND DATEN

Komponenten

IT-Daten- und Anwendungssicherheit im Portfolio von Oracle im Bereich Anwendungen und Daten hat drei Bereiche:

- Identity und Access Management mit Governance, Access und LDAP Directories
- Datenbank Security
- Cloud Security Services zur Absicherung von Cloud Services und On-Premises Systemen

Die folgende kurze Aufstellung der in den Säulen enthaltenen Komponenten bzw. Funktionen zeigt auf, welche Lösungen bei welchen Anforderungen hilfreich sind.

Abbildung 1: Oracle Komponenten für Datensicherheit bei Anwendungen und Daten

Der Bereich IAM beinhaltet Werkzeuge zur Verwaltung von Benutzeraccounts, für Authentifizierungen und Benutzerspeicher. Im Rahmen der Verwaltung der Benutzeraccounts ist das Provisionieren und die Rezertifizierung (Attestierung) enthalten. Der Bereich Authentifizierungen stellt Services zur kontextbasierten Anmeldung, verschiedene Single-Sign On Mechanismen und Berechtigungsdurchsetzung. Benutzerspeicher sind die virtuelle oder physische LDAP Basis für Accounts.

Mit Database Security werden Datenbanken mit Hilfe von Verschlüsselung, Anonymisierung, Gewaltentrennung und Auditing abgesichert. Tools für das Assessment der Datenbanken sind verfügbar.

Cloud Security Services stellen spezielle cloudbasierte Services für On-Premises und cloudbasierte Systeme zur Verfügung. Dies umfasst Verwaltung von Accounts, das Security und Compliance Monitoring, API Security und Blockchains.

Werden spezielle Funktionalitäten bei der Anwendungsentwicklung benötigt, können die oben aufgeführten Funktionen auch als „Backbone“ verwendet werden. Entweder als Entwicklerbibliotheken oder als jeweilige (Webservice oder REST) Schnittstelle und Standardprotokolle wie z.B. SAML oder OAUTH.

BETRIEBSMODELLE

Die im vorangegangenen Abschnitt aufgeführten Komponenten unterstützen direkt oder integrativ die verschiedenen Betriebsmodelle On-Premises, Cloud, Cloud-On-Premises (Cloud at Customer) und Hybrid. Hier kann ein umfassender Schutz im Rahmen einer zentralen IT Sicherheit abgebildet werden.

Abbildung 2: Oracle Betriebsmodelle

Im Idealfall ist die IT-Sicherheitsarchitektur für On-Premises und Cloud identisch. Dies ist erreichbar durch Einsatz gleicher Komponenten, die dann die gleichen Security Maßnahmen umsetzen. Eine zentrale Architektur ermöglicht die einfachere Durchsetzung und Überprüfung der Richtlinien.

Beispiel für gleiche Komponenten sind Verschlüsselung und Management der Keys, die lokal zentral erfolgen kann, die Umsetzung der Gewaltentrennung in der Datenbank oder die zentrale Aggregation der Audit-Logs. Identity Management und Enterprise Manager können beide Umgebungen verwalten.

ZUSAMMENFASSUNG

Oracle bietet zur Umsetzung von IT-Sicherheit von Daten und Anwendungen einen konzeptionellen Ansatz und umfassende Komponenten. In Oracle Produkten und Oracle Cloud Services wird sowohl der Ansatz als auch die Komponenten verwendet.

Kernpunkte sind dabei:

- Schutz im Standard (security should always be on)
- Technische Funktionen zum Schutz in und zwischen jeder Schicht (protect every layer)
- Sich selbst sichernde Systeme (autonomous security, self-securing)
- Eine übergreifende IT Security Architektur über Systeme und Cloud hinweg
- Wahlmöglichkeit der Ablaufumgebung der Komponenten die Security nutzen: On-Premises, Cloud, Cloud at Customer oder Hybrid

BESCHREIBUNG DER KOMPONENTEN

Access Management, Identity Governance, LDAP Directories (IAM)

Das Thema IAM hat einen historischen und einen integralen Aspekt. Aus der Historie einer Behörde heraus wurden Anwendungen entwickelt oder zugekauft. Beide Fälle haben meist unabhängig voneinander das Thema Verwaltung von Accounts und Berechtigungen implementiert. Nicht selten sind daraus Silos entstanden, die sich über die Zeit vermehrt haben. Dadurch haben Benutzer mehrere Logins und die Verwaltungen einen hohen Aufwand bei der Ermittlung und Pflege der Berechtigungen. Fälle wie Eintritt/Austritt, Organisationswechsel seien hier genannt. Bei Lösungen über Helpdesks wurde der Aufwand nur in einen anderen Bereich verlagert.

Im Zuge der steigenden Nutzung von Anwendungen, z.T. auch aus der Cloud, neuen Services, wie MobileApps, einer weitergehenden Digitalisierung/Automatisierung sind die Fallzahlen und damit der Aufwand weiter in die Höhe geschnellt. Strenger ausgelegte Regularien wie IT-Grundschutz oder DS-GVO fordern auch eine hohe Sorgfalt und nicht zuletzt „state-of-the-art“ Sicherheit was oft zu einer Nachbesserung führt.

Das Oracle IAM Portfolio, ggf. ergänzt durch Cloud Security Services, helfen hier den Aufwand zu senken, Automatisierung zu erhöhen und weitere Sicherheitsmechanismen einzusetzen.

Oracle Identity Manager (OIM) ist die Komponente für das Provisionieren von Benutzern, Accounts und Berechtigungen. OIM liefert dabei u.a. Self-Services, Beantragungen, delegierte Administration, (periodische) Berechtigungsprüfungen, Genehmigungsworkflows und Berechtigungsmanagement über die angeschlossenen bzw. verwalteten Systeme. OIM unterstützt auch hybrides Identity Management, so dass ein holistischer Blick und ein Identity Management über On-Premises und cloudbasierte System möglich ist. OIM kennt die Berechtigungen in den Systemen und ermöglicht damit Berichte, (periodische) Berechtigungsprüfungen, Untersuchung von Berechtigungsverletzungen und über ein Zusatzmodul Role-Mining. Kritische Berechtigungsprüfungen (englisch SoD) können hinterlegt werden. Dashboards liefern die jeweilige Managementsicht.

Oracle Privileged Account Manager ermöglicht eine dedizierte Verwaltung von kritischen bzw. privilegierten Accounts, so dass auch nachweisbar ist, wer wann welche Accounts zur Nutzung (via CheckOut) freigeschaltet bekommen hatte.

Oracle Access Manager ist eine webbasierte Single-Sign On Lösung für Authentifizierung und Autorisierung. Durch die verwendeten Standards werden auch stark heterogene Umgebungen unterstützt. Hierbei trägt die zentrale Steuerung der auf den dezentralen Webserver geltenden Zugriffsrichtlinien zur effizienten Verwaltung bei. Single-Sign On wird dabei über mehrere Protokolle wie SAML, OAUTH und AccessToken hinweg unterstützt. SSO Mechanismen in Richtung mobiler Clients (Browser und Applikationen/Apps) werden bereitgestellt und können die Sicherheit abhängig des genutzten Gerätes steuern. Darüber hinaus können in die SSO Lösung soziale Netzwerke wie Facebook, Google, Yahoo, Twitter und LinkedIn hinsichtlich deren Logins und Identitäten integriert werden, so dass der Benutzer einen nahtlosen Übergang in Unternehmensapplikationen ohne erneute Registrierung oder Anmeldung hat. Eine nahtlose Integration in Cloud SSO ist natürlich auch möglich.

Oracle Adaptive Access Manager beinhaltet eine risikobasierte Zugriffskontrolle inkl. forensischer Auswertung bei Zugriffsversuchen. Zusätzlich werden Authentifizierungsmechanismen wie Einmal-Password für SMS, interaktive Sprachauthentifizierung, via E-Mail und via Instant Messaging zur Verfügung gestellt.

Oracle Identity Federation und Oracle Secure Token Service (STS) ist ein Multi-Protokoll Federation Server der sich in ihre Access Lösung mit der Bereitstellung von weiteren Protokollen integriert.

Oracle Entitlement Server bietet das standardbasierte Auslagern von Berechtigungen und Policies für Anwendungen und Webservices eines Unternehmens (Stichwort XACML). So können feinstgranualare Berechtigungen modelliert und zentral bereitgestellt werden.

Oracle Enterprise Single Sign-On Plus stellt ein sogenanntes Desktop Single-Sign On zur Verfügung, das häufig dann genutzt, wird wenn sich eine Applikation nicht über einen SSO Standardmechanismus (vgl. Access Manager) integrieren lässt. Beispielsweise Mainframe Applikationen über Terminalemulationen.

Oracle Unified Directory und Oracle Internet Directory stellen jeweils hoch skalierbare LDAP Directory Services auf Basis der Berkley oder Oracle DB Technologien zur Verfügung. Eine LDAP Virtualisierung über LDAP, Text und DB Sourcen ist vorhanden. Eine Synchronisationskomponente wie ein Metadirectory ist ebenso vorhanden.

DATENBANK SECURITY

In Datenbanken werden die „digitalen Werte“ einer Behörde gespeichert; deren Verfügbarkeit und Integrität sowie der Schutz der Vertraulichkeit haben die höchste Priorität.

Traditionelle Schutzmaßnahmen wie z.B. Firewalls und Virenscanner können allein keinen ausreichenden Schutz garantieren. Daher sind ergänzende Maßnahmen zur Gewährleistung einer umfassenden Datenbanksicherheit erforderlich, die durch den kombinierten Einsatz verschiedenster kommerziell verfügbarer Funktionalitäten aufgebaut werden kann: Schutz der Daten, des Netzwerks und der Speichermedien mit Hilfe von Verschlüsselungstechnologien, Auditierung der Datenbank und kontinuierliche Prüfung der Einhaltung von Sicherheitsvorgaben wie z.B. IT Grundschutz. Abwehr von internen Bedrohungen mit Hilfe eines „Schutzschilds“ um die Datenbank und dem Management von Zugriffsberechtigungen auf Daten und Prozesse und vieles mehr.

Ausfallsicherheit und Hochverfügbarkeit werden mit Mitteln der Oracle Datenbanktechnologie herbeigeführt. Die Oracle Datenbank steht für höchste Performance, kürzeste Antwortzeiten und die Verarbeitung großer Datenmengen und Nutzerzahlen.

Oracle Advanced Security kombiniert Netzwerkverschlüsselung, Datenbankverschlüsselung und starke Authentifizierung. Applikationsdaten oder spezifische Spalten wie Kreditkartennummern können transparent verschlüsselt werden. Zudem ist ab Version 11.2 eine Dataredaction Komponente enthalten, die on-the-fly Rückgabemengen verfremden kann. Die Netzwerkverschlüsselung ist in allen Datenbank-Versionen enthalten.

Oracle Key Vault ist ein zentrales Speicher- und Verwaltungssystem (Key Management) für Schlüssel und Sicherheits Credentials, die bei der Verschlüsselung von Daten in einer Oracle Datenbank, auf den Kommunikationswegen und in den Anwendungen benötigt werden. Mit Hilfe von Oracle Key Vault kann das Keymanagement / die Schlüsselverwaltung deutlichst vereinfacht werden durch zentrale Backup-, Verteil- und Kontrollmöglichkeiten der Schlüssel und deren Nutzung.

Oracle Database Firewall: Oracle Database Firewall ist eine Firewall für Datenbanken, die auch Nicht-Oracle Produkte abdeckt. Sie monitort die Aktivität auf dem Netz und schützt vor unautorisiertem Zugriff, SQL Injections und anderen Angriffen. Sie nutzt positive (white list) und Ausschluss (black list) Securitymodelle, um SQL Kommandos zu validieren bevor sie die Datenbank erreichen.

Oracle Audit Vault sammelt die Logdaten von Systemen in einem Datawarehouse. Darüber können dann einfach Reports und Analysen erstellt werden und Threats oder Auditverletzungen entdeckt werden. Mit Audit Vault bietet Oracle eine vollwertige Database Activity Monitoring Lösung an, die Log- und Protokolldaten aus den Audit Trail Tabellen von Datenbanken, den Audit OS Files, SYS Logs und den Datenbanktransactions Logs der unterstützten Datenbanksysteme sammelt und in eine zentrales Datawarehouse konsolidiert. Auf diesem zentralen Warehouse können dann neben sehr hilfreichen Funktionen wie Notification und Alerting auch leistungsfähige vordefinierte aber auch eigene benutzerdefinierte Berichte benutzt werden um Bedrohungen und Incidents zu entdecken und zu analysieren.

Oracle Database Vault adressiert den Schutz von Daten vor hochprivilegierten Benutzern (Systemverwalter, DBA's), setzt Separation of Duty um und liefert erweiterte Steuerungsmöglichkeiten wer, wann und wie auf Daten zugreifen kann. Database Vault kann isoliert auf einer Oracle Datenbank eingesetzt werden, integriert sich in und nutzt automatisch ein evtl. vorhandenes Audit Vault System. Nachdem eine Zugriffskontrolle per Definitionem invasiv sein muss, bietet Database Vault zur Inbetriebnahme und zur Risiko Minimierung auch einen Simulationsmodus an, in den Zugriffsverletzungen nicht verhindert sondern nur protokolliert werden. Database Vault liefert zusätzlich extrem mächtige Berichtskomponenten, die von vielen Sicherheitsstandards gefordert werden - beispielsweise Entitlement Berichte um festzustellen und zu dokumentieren welche sicherheitsrelevanten Änderungen im Berechtigungswesen einer Datenbank über einen definierbaren Zeitraum erfolgt sind. Neben dem erweiterten Zugriffschutz für sensitive Daten erlaubt Database Vault eine Least Privilege Analyse um festzustellen welche Rechte tatsächlich von Benutzern benötigt werden im Vergleich zu den Rechten die ein Benutzer tatsächlich besitzt.durch privilegierte User (DBA), setzt Separation of Duty um und liefert Steuerungsmöglichkeiten wer, wann und wie auf Daten zugreifen kann.

Oracle Data Masking maskiert sensitive oder vertrauliche Daten beim Übertrag in andere Umgebungen, z.B. Development, Test oder Staging. Ein irreversibler Prozess ersetzt sensitive Daten über Masking Regeln.

CLOUD SECURITY SERVICES

Es gibt dedizierte Cloud Security Services im Bereich der Sicherheit. Diese sind nicht in Ergänzung zu bestehenden Cloud Services zu sehen, sondern es sind Services, die eigenständig genutzt werden können. Diese können mit Oracle oder 3rd Party Cloud Services als auch On-Premises Systemen integriert werden. Bereitgestellte Funktionsbereiche sind Benutzermanagements, Überwachung von Aktionen (SIEM) oder Konfigurationen (IT Compliance), Schutz von APIs (API Gateway) oder Blockchain Services.

Das Oracle Identity SOC Konzept (vorgestellt Ende 2016) oder die Oracle Trust Fabric (Mitte 2018) beschreiben schließlich Lösungsansätze über mehrere dieser Services hinweg um aktuelle Anforderungen wie fortwährende Absicherung der Services und kontinuierliches Security Monitoring zu adressieren. Automatisierung (autonomous, self-secure) spielt dabei in der Zukunft eine immer stärkere Rolle.

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 (z.B. Geräte oder IoT) verwaltet und angebunden werden. Durch vorgefertigte Integrationen sowohl bzgl. der Anbindung von On-Premises 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 eingebunden. Ein mit OPC bestehender IDCS Service kann, je nach Lizenz, dann auch für andere Dinge genutzt werden.

Mit dem Cloud Access Security Broker (CASB) kann die Nutzung der Oracle und 3rd Party 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, z.B. den IDCS, um Rückschlüsse auf den eingeloggten Benutzer ziehen zu können und im Rahmen des Vorfalls entsprechende Vorschläge machen zu können (z.B. Deaktivieren des Accounts im IDCS oder Rücksetzen der Konfiguration in einem Account).

Oracle Management Cloud Security Monitoring Services sowie Configuration und Compliance Service dienen zur Überwachung verdächtiger Operationen in Cloud und On-Premises Umgebungen. Beide Services werden die Log- bzw. Konfigurationsdaten mit Hilfe von Machine Learning aus um Abweichungen und Kausalketten entdecken zu können. Über den integrierten Orchestration Service können Aktionen automatisiert ausgeführt werden, beispielsweise eine Deaktivierung von Accounts.

Der API Platform Cloud Service ermöglicht die Administration von API Schnittstellen wie Bereitstelltung, Freischaltung und Monitoring. Der Service besteht aus zwei logischen Komponenten, eine zur Administration und eine für die Durchsetzung der Policies (Enforcement). Diese Enforcement Points, API Gateways, können sowohl in der Cloud als auch On-Premise deployed werden. Mit Hilfe dieses Services kann sichergestellt werden, dass allein der richtige User die richtigen Ressourcen nutzt. Er hilft ebenso zur Vorbereitung bei der Abwehr von potenziellen Attacken auf die Infrastruktur

·acle Blockchain Cloud Service bietet die Nutzung von permission-based Blockchains auf Basis von Hyperledger. Blockchain löst das Problem des Vertrauens zwischen Organisationen, indem es eine unabhängige Validierung durch ein manipulationssicheres, peer-distributed Ledger ermöglicht und somit die Notwendigkeit eines Offline-Abgleichs eliminiert. Vorkonfigurierte Blockchain-Codes sind für viele Standardgeschäftsprozesse einschließlich ERP-Transaktionen zur Nutzung vorkonfiguriert. Das Benutzer/Vertrauensmanagement erfolgt über den bereitgestellten Identity Cloud Service.

IDENTITY SOC UND TRUST FABRIC KONZEPT

Das Oracle Identity SOC Konzept (vorgestellt Ende 2016 auf dem Gartner IAM Summit) oder die Oracle Trust Fabric (Konzept wurde 2018 vorgestellt) beschreiben schließlich Lösungsansätze, die dem Wandel der IT inklusive der optionalen Nutzung von Cloud Services Rechnung tragen. Für beide Konzepte ist die Automatisierung einer der Schlüssel. Automatisierung erfolgt so weit, dass die Systeme „autonomous“ agieren, d.h. selbst mit Hilfe von Machine-Learning analysieren, Entscheidungen treffen können und damit auch Aktionen durchführen (auch self-securing oder self-healing genannt). Vereinfacht zusammengefasst sind die Anforderungen aufgrund des Wandels:

1. Eine immer schneller steigende Anzahl von Systemen sind abzusichern und hinsichtlich sicherheitsrelevanter Belange zu monitoren. Dies umfasst sowohl zeitnahes Security Patching als auch die Auswertung von Logs über Systeme und verschiedene Accounts hinweg

2. Dezentralisierung der Kontrollpunkte bzw. des „Perimeters“: die Firewalls des Unternehmens reichen für einen Schutz nicht mehr aus. Vielmehr wird der Schutz stärkst-möglich bereits beim Benutzen bzw. Benutzer der Services benötigt und an allen weiteren Punkten im Zugriffsweg

3. Kontinuierlich gewieftere, teilweise automatisierte Zugriffsversuche auf Systeme, auch von Behörden zu entdecken und zu bekämpfen. Bereits über 2/3 aller deutschen Unternehmen/Behörden stimmten zu, schon unberechtigte Datenabflüsse entdeckt zu haben. Dunkelziffer nicht eingerechnet

Das Identity SOC Konzept bzw. Framework adressiert diese drei Anforderungen durch die Nutzung von mehreren der Cloud Security Systemen zusammen, damit:

- verdächtige Aktivitäten, policy-basiert oder abweichend vom Standardverhalten, entdeckt und automatisiert adressiert werden können (Security Monitoring, CASB, Identity Cloud Service)

- Accounts unter einem Benutzer korreliert werden können, damit sichtbar wird, wenn ein Benutzer gehackt wird, z.B. durch Social Engineering oder Phishing (Identity Cloud Service)

- APTs (Advanced Persistent Threats) frühzeitig entdeckt werden (Security Monitoring, CASB)

- Datenabfluss durch DLP unterbunden werden (CASB)

- durch absichtliche oder unabsichtliche Konfigurationsabweichungen Problemstellen rechtzeitig erkannt und beseitigt werden können (Configuration Compliance)

- Kontinuierliches Monitoring ermöglicht wird, das auch im Rahmen von Regularien die entsprechende Sorgfalt nachweist (Configuration Compliance)

Diese Services werden je nach gewünschter Nutzung in einer Oberfläche wie z.B. der Oracle Management Cloud bereitgestellt. Abgedeckt werden je nach Zusammenstellung klassische SIEM, DLP, IT Compliance, UEBA und CASB. Sie bilden ein Security Operations Center (SOC) Framework oder können natürlich auch als Input für ein bestehendes Security Information und Event Management (SIEM) System genutzt werden. Soll ein SOC mit diesem Framework betrieben werden, können bei Oracle über die „Managed Services“ solche personalbasierten Dienste mit hinzu beauftragt werden.

Trust Fabric beschreibt als Konzept die Antwort der Anforderungen unter 1, 2 und 3 mit dem Identity SOC Framework als Teil der Lösung. Auch hier besteht ausgehend von der geänderten Kontrollmöglichkeit (keine zentralen Firewalls mehr, der Benutzer ist der größte gemeinsame Nenner bei der Nutzung von IT), die Herausforderung in der verteilten Security. In Erweiterung zum Identity SOC wird hier verstärkt auf Proaktivität, Schnelligkeit und Automatisierung im Sinne von Autonomous Wert gelegt. Maßgeblich dazu beitragen wird künstliche Intelligenz vor allem im Bereich Machine Learning, durch die auch neue Probleme/Angriffe selbständig erkannt und adressiert werden können. Die dabei eingesetzte Produktpalette ist die rund um das Identity SOC, ergänzt um Komponenten im Bereich „Autonomous“ (selbständige Adaption), API Schutz und Blockchains.

Beide Konzepte adressieren die Nutzung von heterogenen und Multi-Cloud Umgebungen und helfen bei der Erfüllung der typischen SOC Aufgaben durch Automatisierung und gesamtheitliche Sicht über alle Systeme.

ORACLE PUBLIC CLOUD SECURITY

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 normalerweise 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 Rechenzentrumsinfrastruktur reduzieren können. Mit der Oracle Cloud 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: Das sind 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. Die bekannten Oracle Engineered Systems sind ebenfalls in der Cloud Verfügbar.

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

Oracle bietet mit der Oracle Cloud die Nutzung von sicheren IaaS, PaaS und SaaS Cloudservices. Diese werden entweder aus einem Cloud Rechenzentrum heraus oder mit der Oracle Cloud Machine (Cloud at Customer) bei Kunden oder deren Hoster bereitgestellt. Nicht alle Services sind auf allen Umgebungen verfügbar. Durch Verwendung gleichartiger Technologien in den Cloud Services wie in lokal installierten Oracle Produkten kann das schon gewonnene Knowhow weitergenutzt und mit den gleichen Security Policies abgesichert werden. Auch lassen sich Szenarien wie ein Verschieben in die Cloud, Lift&Shift, Testumgebungen oder hybrider Betrieb abbilden.

Durch den Einsatz der Oracle Cloud 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.

Oracle Cloud Services besitzen unterschiedliche Attestierungen bzw. Zertifizierungen. Für die Oracle Cloud in Frankfurt sind dies SOC1, SOC2, SOC3, ISO27001, PCI-DSS und HIPAA. Weitere, auch BSI C5 sind in Planung. Nicht alle Services besitzen gleichzeitig alle Attestierungen bzw. Zertifizierungen, diese z.B. hier einsehbar: https://cloud.oracle.com/iaas-paas-compliance.

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 Telecommunications Industry Association (TIA). Rechenzentren sind sowohl in Deutschland, als auch in der EU und weltweit verfügbar.

Oracle stellt mit der Oracle Cloud eine Umgebung bereit, mit der Kunden Kontrolle und Absicherung unter anderem durch folgende Punkte erhalten:

- Security per default: je nach Service 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 virtualisierte Netzwerke und Einsatzmöglichkeit dedizierter nicht virtualisierter Maschinen
- Compliance: Security Zertifizierungen der Cloud durch Unabhängige sowie Hilfestellungen für GDPR und andere Regularien. Protokolldaten für Monitoring und Auditierungen sind zugreifbar. Eigene Audits sind möglich
- Cloud Security Services: Zusätzliche Services von Oracle, um Oracle oder 3rd Party Clouds/Umgebungen abzusichern. Einsatzmöglichkeit von Softwarelösungen von Drittanbietern zum Schutz der Daten und Ressourcen in der Cloud
- Redundante Rechenzentren, die hochverfügbare Scale-Out Architekturen ermöglichen und gegen Netzwerkangriffe abwehren

Oracle investiert weiterhin in die Entwicklung von Cloud Services und Sicherheitstechnologien. Funktionale Erweiterungen auch im Bereich Security finden in der Cloud permanent statt, beispielsweise um die Erweiterung einer Web-Application Firewall oder des DNS Dienstes DynDNS.

Zusammengefasst besteht die Oracle Cloud aus sicheren Produkten, die in einer Sicherheitsarchitektur bereitgestellt werden. Ausgerollt unter Berücksichtigung von Sicherheitsgesichtspunkten, sicher betrieben und das Ganze regelmäßig durch Unabhängige überprüft.

ORACLE CLOUD AT CUSTOMER: CLOUD ON-PREMISES

Das Potential von Cloud Computing als Schlüssel-Technologie der Zukunft ist auch in Deutschland längst erkannt; trotzdem sind viele Behörden beim Gang in die Cloud aus Gründen der Sicherheit und Kontrolle noch zögerlich. Oracle adressiert die größten Hemmnisse und stellt als erster Anbieter neue Services vor, dank derer Kunden ihre Daten und Prozesse nahtlos in die Cloud migrieren können. Oracle bietet mit „Cloud at Customer“ eine Appliance (Hardware und Software) als Lösung an, bei der die Oracle Public Cloud Plattform im Hause des Kunden steht. Damit ist dieser der Betreiber der Cloud Plattform im eigenen Haus und profitiert zusätzlich vom flexiblen Abonnement-basierten Lizenzmodell. Das Besondere: Die Oracle „Cloud at Customer“ ist eine vollständig gemanagte Lösung, d.h. Kunden partizipieren an der gleichen Erfahrung, Servicequalität und den neuesten Innovationen und Updates, die die Oracle Cloud kennzeichnen.

Mit Oracle „Cloud at Customer“ bekommen CIOs ganz neue Optionen, wenn es um Architektur, Einsatz und Betrieb ihrer Anwendungen geht. Sie können sich alle Vorteile der Oracle Cloud Services wie Skalierbarkeit, Agilität, Performance und die einfache Nutzung mit einem Abonnement-basierten Preismodell in ihr eigenes Rechenzentrum holen und behalten gleichzeitig die Kontrolle über die Infrastruktur. Sie können ihre Services genau dort betreiben, wo sie möchten – in ihrem eigenen Rechenzentrum oder in der Oracle Cloud.

Die Erweiterung der Oracle Cloud auf das eigene Rechenzentrum bringt den Kunden folgende Vorteile:

Sie behalten die vollständige Kontrolle über ihre Daten, können die Anforderungen im Bereich Datenhoheit und Datenhaltung besser erfüllen und profitieren trotzdem von den Vorteilen der Cloud. Denn: Mit der Oracle „Cloud at Customer“ verlässt kein Bit an Kundendaten das eigenen Rechenzentrum – und schon gar nicht das Land.

- Existierende Workloads können ganz einfach von On-Premises Infrastrukturen in die Cloud migriert werden – die Umgebungen, Toolsets und APIs sind absolut identisch

- Sowohl Oracle Workloads als auch Workloads anderer Anbieter können entsprechend den sich verändernden Geschäftsanforderungen zwischen selbstverwalteter Hardware und Cloud verschoben werden
- Die Services sind konform mit den gesetzlichen Regelungen hinsichtlich Datenschutz und -sicherheit, wie beispielsweise dem Bundesdatenschutzgesetz, dem PCI-DSS (Regelwerk für Kreditkartentransaktionen) sowie anderen branchen- oder länderspezifischen Vorschriften

BETRIEBSSYSTEME UND JAVA

Java Security

Java Sicherheits Technologien stellen dem Entwickler beim Erstellen von Applikationen ein vollständiges Sicherheits Framework zur Verfügung. Die Administratoren können ein Paket von Werkzeugen nutzen, um Applikationen sicher einzusetzen, incl. Verschlüsselung, Public Key Infrastrukturen, sicherer Kommunikation, Authentifizierung und Zugriffs Kontrolle.

Die erweiterten Sicherheitsmerkmale der Oracle Engineered Systems werden verstärkt, sowohl für Oracle Solaris als auch Linux Betriebssysteme zum Erreichen einer vollständigen Sicherheit auf Infrastruktur Ebene – innerhalb der Firewalls einer Behörde aber auch in der Cloud.

Oracle Solaris

Oracle Solaris 11.3 ist weltweit das fortschrittlichste Betriebssystem. Es liefert Sicherheit, Geschwindigkeit und einfache Bedienbarkeit für Enterprise Cloud Umgebungen.

Im Hinblick auf den Betrieb konsolidierter kritischer Umgebungen bietet Oracle Solaris verschiedene Technologien. Herausgehoben werden sollen hier:

Solaris Container: Isolierte Laufzeitumgebungen innerhalb einer Oracle Solaris Installation mit eigenem Namensraum (Benutzerverwaltung usw), mit eigener Netzwerkverwaltung unter der Kontrolle des umgebenden Solaris. Die Isolation unterbindet jegliche unerwünschte Kommunikation zwischen verschiedenen Containern innerhalb derselben Solaris Instanz. Zusätzlich können diese Container auch gegen jede Veränderung geschützt werden

Solaris Compliance Framework: Solaris bietet eine OpenSCAP kompatible Auditierung einer Betriebssystem Installation, es kann manuell oder automatisch eine vorhandene Installation auf die Einhaltung bestimmter Regeln überprüft werden (in einer Standardinstallation enthalten ist z. B. auch ein Regelwerk zu PCI-DSS) Es kann systematisch die Integrität beliebiger Files, insbes. von Betriebssystem-eigenen Files per Prüfsumme überprüft werden. Weiter bietet Solaris ein serienmäßiges Audit Framework, sämtliche Änderungen und Zugriffe auf ein Solaris können protokolliert werden.

Plattformunabhängigkeit: Oracle Solaris ist sowohl auf Oracle Solaris als auch auf x86 Systemen erhältlich. Diese Plattformunabhängigkeit wird durch ein plattformunabhängiges Programmiermodell erreicht, das u. a. auch eine höhere Softwarequalität erreicht.

Netzwerkbasiertes Installationsmodell: Solaris beruht auf einem netzwerkbasierten Installationsmechanismus, der allerdings keine Verbindung zum öffentlichen Internet erfordert. Die netzwerkbasierte Installation erleichtert die Administration einer großen Zahl von Systemen erheblich, überprüft transparent die Integrität von Softwarepaketen und enthält eine automatische Prüfung und Auflösung von Abhängigkeiten zwischen Softwarepaketen. Alternativ kann die Betriebssysteminstallation auch von einem lokalen Medium erfolgen

Oracle Linux

Dieses Betriebssystem ist ausgelegt für unternehmenskritische Auslastung in der Cloud, optimiert für Oracle Engineered Systems und bewährt im Einsatz bei einer Vielzahl von Kunden.

Es ermöglicht eine beschleunigte Cloud Entwicklung durch:

- Vollständige Virtualisierung, Linux Container und OpenStack for next-generation cloud
- Bewährtes und getestetes Cloud Deployment mit 5.5 Millionen Usern in der Oracle Cloud
- Einfaches Cloud Deployment mit Docker und Linux Containern
- Einsatz einer sicheren risikoarmen Foundation
- Bewiesene Verfügbarkeit mit 128,000 Stunden Nutzung durch Oracle Entwickler pro Tag

SERVER UND STORAGE

Oracle's SPARC Server

Die Oracle SPARC Architektur wurde 1987 erstmals veröffentlicht, sie blickt also auf eine mehr 25-jährige Geschichte zurück. Durch diese Erfahrung hat sie eine hohe Reife erreicht, die sich in der Verwendung in einer Vielzahl von extrem kritischen Systemen niederschlägt.

In der jüngeren Vergangenheit hat sich Oracle darauf konzentriert, die SPARC Architektur in Richtung einer optimalen Plattform für Oracle Softwareprodukte weiter zu entwickeln. Dabei waren insbesondere zwei Aspekte von zentraler Bedeutung: Optimierung der Verarbeitung sehr großer Datenmengen im Hauptspeicher und Erhöhung der Sicherheit beim Betrieb beliebiger Softwareprodukte.

Die aktuellen Oracle SPARC CPUs M7 (32 Kerne) und S7 (8 Kerne) beschleunigen 15 verschiedene Verschlüsselungs- und Signaturalgorithmen durch spezialisierte Einheiten in jedem CPU Kern, darunter AES, DH, RSA, ECC, oder SHA-512. Damit wird der Leistungsverlust durch Einsatz von Verschlüsselung vernachlässigbar, z. B. beträgt der Leistungsverlust pro Kern im SPECj Enterprise2010 Benchmark nur 2% pro Kern zwischen voll verschlüsseltem und Klartext[1].

Da Software Produkte auch (noch) unentdeckte Fehler beinhalten können, wurde für die aktuellen SPARC M7 und S7 CPUs eine Technologie entwickelt, die eine weit verbreitete Methode zum Eindringen unterbindet, Silicon Secured Memory ("SSM"). SSM wurde ursprünglich entwickelt, um sämtliche Hauptspeicherzugriffe in Echtzeit kontrollieren zu können, zur Entdeckung und Beseitigung sog. "memory reference errors". Diese Fähigkeit erlaubt wesentliche Verbesserungen in der Softwarequalität, sowie die Weiternutzung im produktiven Betrieb jenseits der Qualitätssicherung beim Softwarehersteller.

SSM erlaubt die fein granulierte Markierung des gesamten Hauptspeichers und transparente Prüfung dieser Markierungen bei jedem Hauptspeicherzugriff. Bei Abwesenheit von Fehlern oder Eindringversuchen verursacht SSM so gut wie keinen Leistungsverlust, im Falle eines illegalen Zugriffs wird dieser unterbunden und signalisiert. Dieser illegale Zugriff kann entweder durch einen Softwarefehler oder durch einen Angriff auf das System verursacht worden sein. Beispiele für solche illegalen Zugriffe wären "buffer over-reads" oder "buffer over-writes". In bestimmten Fällen können sogar existierende Programme ohne irgendwelche Änderungen oder erneute Übersetzung von SSM profitieren.

[1] *https://blogs.oracle.com/BestPerf/entry/20160629_jent_sparc_s7_2*

ORACLE ENGINEERED SYSTEMS

Komplexitätsreduzierung ist ein wesentlicher Vorteil, wenn es um IT-Sicherheit geht.

Weniger Komplexität, weniger Kosten: Integrierte Systeme sind für die Zusammenarbeit konzipiert, integriert, getestet und optimiert - mit dem Ziel, Komplexität zu verringern und Kosten einzudämmen. Auf diese Weise wird für eine Vereinfachung von Bereitstellung und Upgrades sowie ein effizienteres Systemmanagement gesorgt.

Schnellerer Geschäftsbetrieb dank vereinfachter IT: Oracle Engineered Systems sind auf allen Ebenen des Technologie-Stacks vorgefertigt. Die Integrationsaufgaben nehmen wir unseren Kunden ab, damit neue Services schneller online gehen können. Das IT-Team des Kunden kann sich auf die Verbesserung von Services und Serviceniveaus konzentrieren und so für einen Mehrwert sorgen.

Herausragende Performance auf allen Ebenen des Technologie-Stacks: Herausragende Performance bedeutet, dass Aufgaben schneller, besser und effizienter als je zuvor erledigt werden. Dies ist das Kennzeichen der Engineered Systems von Oracle und ultimativer Ausdruck des Strebens von Oracle, die IT zu vereinfachen.

ORACLE STORAGE

Oracle **ZFS Storage Appliances** sind eng mit den Oracle Serversystemen und der Oracle Software integriert.

Zur Vermeidung der Risiken von Sicherheitsbrüchen werden sichere, granulare und leicht zu implementierende Verschlüsselungen für die Oracle ZFS Storage Appliances angeboten:

Erweiterter Datenschutz mit AES 256-bit Datenverschlüsselung

- Vermeidend Sicherheitsbrüche mit hoch verfügbarer 2-Ebenen Schlüssel Architektur
- Schnelle Inbetriebnahme “one-click” Implementierung
- Granulare Wirksamkeit und Kontrolle durch Verschlüsselung auf Projekt-, Share-, or LUN Level
- Flexibles lokales oder zentralisiertes Schlüsselmanagement
- Hoch sicherer, skalierbarer und kostengünstiger unternehmensweiter Datenschutz

VERSCHLÜSSELUNG

Oracle unterstützt die Nutzung von Verschlüsselungsalgorithmen in verschiedenen Produktebenen

- Datenbank
- Middleware
- Java
- Server
- Prozessor
- Storage

Die Verwaltung von Schlüsseln wird durch das Produkt Oracle Key Manager (Oracle Key Vault) unterstützt.

KUNDENBEISPIELE

Bei unseren Kunden werden Oracle Technologien und Lösungen in vielfältigster Ausprägung und Kombination und unterschiedlichsten Architekturen eingesetzt, um der jeweiligen Kritikalität der Aufgaben gerecht zu werden.

Bitte sprechen Sie uns an.

ORACLE Deutschland B.V. & Co. KG
Riesstraße 25
D-80992 München

Telefon: 0800 1 824145
Fax: 0180-2-ORAFAX

CONNECT WITH US

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

Integrated Cloud Applications & Platform Services

Titel: Oracle Beiträge zur IT- und Cyber-Sicherheit für die Öffentliche Verwaltung und das Gesundheitswesen

Stand August 2018