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

ORACLE
Cloud

Die öffentliche Verwaltung unterliegt ebenso wie die gesamte Wirtschaft einem signifikanten Veränderungsdruck, durch IT-Konsolidierung des Betriebs, Modernisierung der IT-Verfahren, Bereitstellung neuer Services für die Verwaltung sowie für Bürger und Wirtschaft und letztendlich der immer aufwendigeren Abwehr von (Cyber-)angriffen. Cloud basierte Lösungen unterstützen bei der Lösung der skizzierten Aufgabenstellungen auf allen Ebenen und helfen dem Staat schnell auf Änderungen und äußere Einflüsse zu reagieren.

Oracle unterstützt die Umsetzung dieser Aufgabenstellungen mit Hilfe seiner bewährten Technologien. Der Fokus des vorliegenden Whitepapers liegt auf dem Thema Sicherheit. Sicherheitsfunktionalitäten werden in allen Oracle Produkten, ob Cloud oder in Ihrem Rechenzentrum, zur Verfügung gestellt. 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 unternehmenskritischen Anwendungen ein.

IT-GRUNDSCHUTZ, IT-SICHERHEITSGESETZ, DATENSCHUTZGRUNDVERORDNUNG

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. Dazu zählen die EU Datenschutz-Richtlinie von 1995, die Datenschutzgrundverordnung und die damit verbundene Anpassung lokaler Vorgaben wie BDSG, NIS und die damit verbundene Anpassung von KRITIS und lokale Vorgaben wie IT-Sicherheitsgesetz, IT-Grundschutz oder BSI C5. 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.

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 verschiedener Tools ist es so zum Beispiel möglich, Anforderungen aus der DSGVO oder aus dem IT-Grundschutz abzubilden und in ein übergreifendes ISMS einzubinden.

Ziel der Schutzmaßnahmen sind Prävention, Erkennung, Vorhersagen 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.

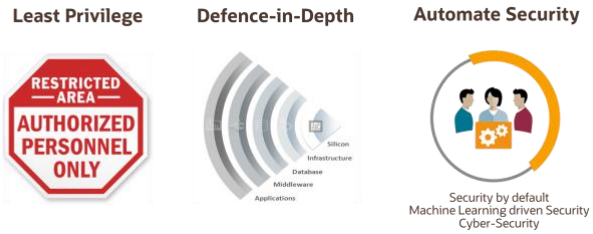
DATENSOURVERÄNITÄT UND CLOUD

Werden zur Lösung der Aufgabenstellung Cloud-Services genutzt stellt sich u.a. die Frage nach der Datensouveränität. Abgesehen von den Anforderungen durch Regularien, die den Schutz der Daten organisatorisch und technisch beschreiben gibt es auch Vorgaben für die Sicherstellung des Speicherorts und Umgang mit ggf. gesetzlichen Zugriffsmöglichkeiten durch deutsche Behörden oder ausländische Staaten.

Die Zugriffsmöglichkeiten auf Oracle Cloud Services sind in den sogenannten DPAs (Data Processing Agreements) dargelegt. Diese beinhalten auch die Beschreibung entsprechender staatlicher Interventionen als auch Meldepflichten. Ein Speicherort der Daten, z.B. nur in Deutschland, kann vertraglich bei den meisten Cloud-Services festgelegt werden. Die Oracle Cloud arbeitet mit einer HW-gestützten Trennung der Mandanten und automatischer Verschlüsselung. Soll ein hypothetischer Zugriff von Behörden verhindert werden so sind mögliche Schutzmassnahmen die Schlüssel der Verschlüsselung selbst zu speichern (Schutz gegen lesen) und Backups in weiteren Lokationen abzulegen (Schutz bei Unerreichbarkeit der Services). Oracle unterstützt dies in der Cloud. Sind diese Massnahmen nicht ausreichend gibt es auch die Möglichkeiten eine Oracle Cloud in Ihrem Rechenzentrum zu hosten oder eine der autarken Cloud-Appliances an einem beliebigen Standort zu nutzen.

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. Für Larry Ellison, Oracle's Chief Technology Officer und Chairman ist Sicherheit das oberste Ziel von Oracle. Zugleich ist Sicherheit auch eine der größten Herausforderungen für die IT. Wir bei Oracle sind überzeugt, dass wesentliche Verbesserungen beim Aufbau und Betrieb der IT notwendig sind um sich besser zu wappnen. Interne wie externe Services müssen Security und Compliance automatisch in alle Systeme und Anwendungen einbauen und eine fortwährende Selbstadaption nutzen. Oracle antwortet darauf mit **technischen Sicherheitsfunktionen** in allen Produkten und Architekturen und **sich selbst absichernden und verteidigenden** Systemen („self-securing" bzw. „autonomous")**.**



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

- Eine Basissicherheit sichert wie bisher jede Schicht in einer Architektur und die Kommunikation zwischen den Schichten ab („Defense in Depth"). Die Komponenten haben nach einer Installation bereits sichere Konfigurationen („Security by Default"), erlauben eine Begrenzung von Berechtigungen („least privilegues") und liefern Nachweise durch entsprechende Protokollierungen („Audit"). Oracle bietet in den Komponenten der einzelnen Schichten die entsprechenden Funktionen wie beispielsweise Verschlüsselung in der Datenbank oder bei der Kommunikation mit der Datenbank

  Speziell bei Cloud Services sind weitere Maßnahmen erforderlich, um die Mandanten logisch und physisch sowohl im Netz als auch auf/mit Systemen voneinander zu trennen und beim Aufsetzen von Systemen einen definierten sauberen Stand, auch der Firmware, sicherzustellen.

- Ergänzt wird dies durch ein dynamisches Modell, um während des Zugriffs kontextbasiert reagieren zu können, z.B. um Funktionalitäten einzuschränken.

- Um Services überhaupt erreichen zu können wehrt eine vorgelagerte Schicht, bei Oracle sogenannte Edge Services, im Vorfeld Angriffe ab. Diese können sowohl vor ein OnPremises Rechenzentrum als auch Cloud Services geschaltet werden.

Sich selbst absichernde Systeme sind seit der Ende 2017 unter dem Begriff „autonomous" bei Oracle zu finden. Eine Automatisierung zur Cyber-Crime Abwehr ist schon durch die fehlenden SOC Spezialisten notwendig. Die Automatisierung erfolgt maßgeblich durch künstliche Intelligenz. Diese lebt von einem sich ständig erweiternden Erfahrungsschatz von Oracle oder Dritten. Beispiele sind:

- Durch künstliche Intelligenz durchgeführtes Security-Patching laufender Systeme um die 85% der erfolgreichen Angriffe gegen ungepatchte Systeme abzuwehren.
- Mit User Entity Behaviour Analytics (UEBA) abweichendes Verhalten erkennen um Innentäter, Externe und missbrauchte Systeme und Threats/APTs aufzuspüren.
- Der Einbezug von zusätzlichen 3rd Party Services und/oder Daten für die Forensik hilft weitere Unrechtmäßigkeiten zu erkennen oder abzuwehren.
- Oracle setzt diese Konzepte und die Cyber-Crime Abwehr heute schon u.a. in autonomen Datenbanken, Cloud Access Security Broker (CASB), Web Application Firewall (WAF) und der Oracle Cloud um.

Security ist und bleibt in der DNA von Oracle und ist essentieller Bestandteil von Oracle und Oracle Cloud. 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. Zertifizierungen wie ISO27001 oder BSI C5 im Falle der Oracle Cloud weisen eine sichere Umsetzung nach. Analysten bestätigen die Strategie und Umsetzung im Bereich Security durch die Einstufung in den entsprechenden Leadership Kategorien.

INTEGRATION UND AUFBAU EINER SICHERHEITSARCHITEKTUR

Durch die sukzessive Einführung von IT-Komponenten sind bei Unternehmen 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 zusätzliche Risiken, bei der Verwaltung und Wahrung der Compliance einen hohen manuellen Aufwand und verhindert oft 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. Es reicht nicht aus nur den Perimeter, also die Firewall, zu verstärken. 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.

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/Reporting (u.a. SIEM, IT Compliance, Identity SOC) und Durchsetzung von Policies (u.a. Identity& Access, Governance, Verschlüsselung). Die Komponenten können auch einzeln eingesetzt und in andere Sicherheitsplattformen integriert werden. Oracle Komponenten unterstützen die Verwendung einer gemeinsamen Sicherheitsarchitektur. Unabhängig davon wo die Komponenten laufen, z.B. OnPremises oder in der Cloud können meist die gleichen Policies und Mechanismen verwendet werden. Beispielsweise ist das eine starke Authentifizierung abhängig des Kontexts bei sensitiven Services.

Das Oracle Produkt- und Lösungsportfolio umfasst für OnPremises und als Cloud-Service Unternehmenssoftware, Business Intelligence, Middleware, Identity Management, Datenbanken, Server und Storagesysteme sowie Support und Consulting. Alle verfügbaren Innovationen in die IT-Sicherheit werden unseren Kunden im Rahmen von Cloud- oder 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.

Die Komponenten unterstützen direkt oder integrativ die verschiedenen Betriebsmodelle On-Premises, Cloud, Cloud at Customer und Hybrid. Hier kann ein umfassender Schutz im Rahmen einer zentralen IT Sicherheitsarchitektur 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 werden 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 und verteidingende 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

Durch die breite Palette an Services und ihre Vorintegration ergeben sich Vorteile 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, z.B. SingleSignOn, automatisierte Rechtebeantragung. 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.

Auf den folgenden Seiten finden Sie weitere Informationen zu den Oracle Komponenten und Lösungen.

ÜBERBLICK ZUR IT-DATENSICHERHEIT IM BEREICH ANWENDUNGEN UND DATEN

Komponenten

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

- Identity und Access Management (IAM) 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.

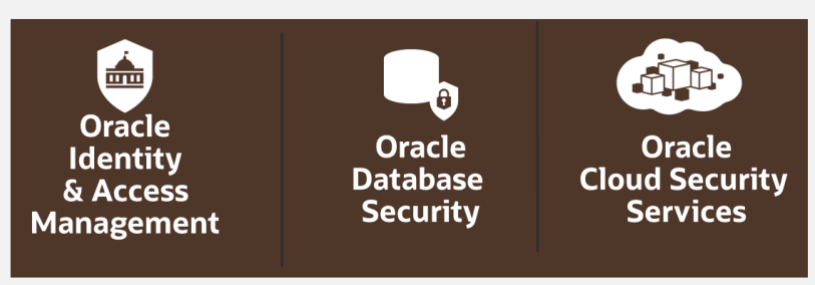


Abbildung 1: Oracle Komponenten für Datensicherheit bei Anwendungen und Daten

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.

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 Apps, 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 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. Der Identity Manager unterstützt auch hybrides Identity Management, so dass ein holistischer Blick und ein Identity Management über On-Premises und cloudbasierte System möglich ist. Identity Manager 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 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. Risikobasierte Zugriffskontrolle wird zur Verfügung gestellt. Zusätzlich werden Authentifizierungsmechanismen wie Einmal-Password für SMS oder via E-Mail, „Timebased OneTimeToken“ (TOTP) und Mobile Push 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 **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.

Typische Einsatzgebiete bei Behörden sind führende Anmeldeverfahren in zu webbasierten Applikationen onPremises und Cloud, starke Authentifizierung für Adminstratoren, Berechtigungsverwaltung von Mitarbeitern und Externen, Föderation mit anderen Behörden, Speicherung von Kundenaccounts und Umsetzung von IT Grundschutz.

DATENBANK SECURITY

Traditionelle Schutzmaßnahmen wie z.B. Firewalls und Virenscanner können allein keinen ausreichenden Schutz garantieren. Dem Oracle Ansatz folgend können die Datenbanken selbst und die Kommunikation daher zusätzlich abgesichert werden (siehe Defense in depth). Ergänzende Maßnahmen zur Gewährleistung einer umfassenden Datenbanksicherheit sind: Schutz der Daten, des Netzwerks und der Speichermedien mit Hilfe von Verschlüsselungstechnologien, Auditierung der Datenbank und kontinuierliche Prüfung der Einhaltung von Sicherheitsvorgabe. Es erfolgt zugleich die Abwehr von internen Bedrohungen. 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 Data-Redaction Komponente enthalten, die on-the-fly Rückgabemengen verfremden kann. Die Netzwerkverschlüsselung ist seit einigen jahren in allen Datenbank-Versionen enthalten.

Oracle Key Vault ist ein zentrales Speicher- und Verwaltungssystem (Key Management) für Schlüssel und sicherheitsrelevante 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 durch zentrale Backup-, Verteil- und Kontrollmöglichkeiten der Schlüssel und deren Nutzung stark vereinfacht werden.

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 Database Vault adressiert den Schutz von Daten durch privilegierte User (DBA), setzt Separation of Duty um und liefert Steuerungsmöglichkeiten wer, wann und wie auf Daten zugreifen kann.

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. Jede Oracle Datenbank hat unabhängig davon natürlich eine eigene Audit Funktionalität.

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.

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. Mit Data Subsetting kann der jeweilige Bereich von Daten der maskiert oder übertragen werden soll bestimmt werden.

Oracle Labeld Security ermöglicht die Definition welche Benutzer welche Daten auch innerhalb einer Tabelle sehen können. Dazu werden „Labels“ definiert und zugeordnet. Diese Funktion ist zum Teil als Virtual Private Database verfügbar.

Das für Oracle Kunden **kostenfreie DBSAT** Tool ermöglicht ein Assessment der Datenbank gegen Oracle Best Practices und Vorgaben der DSGVO, CIS und STIG. Darüber hinaus wird das Datenmodell auf potentiell sensitive Daten untersucht, die typischerweise einem höheren Schutzbedarf unterliegen. DBSAT basiert auf Scripten und ist daher non-invasiv. Das Tool kann mit Hilfe des Oracle Support Zugangs heruntergeladen werden.

Typisches Einsatzgebiet bei Behörden ist die Verschlüsselung der Daten die ein Lesen der OS Files oder Backups verhindert. Die weiteren Funktionen wie DBVault werden für die Umsetzung des IT-Grundschutzes eingesetzt.

CLOUD SECURITY SERVICES

Es gibt dedizierte Cloud Security Services im Bereich der Sicherheit. Diese sind zum Teil zur Absicherung der Oracle Cloud Services, z.B. Key Management als auch zur eigenständigen Nutzung von Cloud oder On-Premises Systemen. Bereitgestellte Funktionsbereiche sind Benutzermanagements (IdaaS), Überwachung von Aktionen (SIEM) oder Konfigurationen (IT Compliance), Schutz von APIs (API Gateway) oder Blockchain Services.

Oracle Identity Cloud Service (IDCS) stellt eine cloudbasierte Identity und Access Management Plattform zur Verfügung (IdaaS). 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 Cloud Services eingebunden. Ein mit Oracle Cloud bestehender IDCS Service kann, je nach Lizenz, dann auch für andere Dinge genutzt werden.

Mit dem **Cloud Access Security Broker (CASB)** können Oracle und 3rd Party Clouds bezüglich Missbrauch/Angriffen gemonitort und die Konfiguration überwacht werden. 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).

Der **API Platform Cloud Service bzw. API Gateway** ermöglicht die Administration von API Schnittstellen: 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 im Falle API Platform 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

Oracle **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.

Oracle Cloud Key Management Service (KMS) ermöglicht die Verwaltung der Schlüssel die in der Oracle Cloud für Storage (Object, File, Block) verwendet werden durch den Kunden. Die Oracle Cloud verschlüsselt den Storage per default. In die KMS können auch eigene Schlüssel importiert werden, die dann bei der Verschlüsselung angegeben werden können. Im Standard erfolgt dabei die Speicherung in einer HSM (FIPS3 compliant) in einer eigenen Partition. Abweichende Konfigurationen sind möglich wie Virtual Vaults. Durch den KMS kann der Kunde diese Schlüssel auch rotieren. Geplant ist auch die DB Keys zu verwalten was aktuell nur lokal oder zentralisiert mit Oracle Key Vault möglich ist. Weiterhin ist in Planung andere Secrets zu verwalten, z.B. für kubernetes.

Oracle Edge Services:

Die **Internet Intelligence Map** wertet Informationen des Traffic im WWW auf Störungen aus, z.B. als Auswirkung von Ereignissen wie Naturkatastrophen oder staatlich veranlassten Unterbrechungen, visualisiert. Störungen im Internet können Unternehmen, Regierungen und Netzwerkbetreiber in schwerwiegendem Ausmaß beeinträchtigen, sei es durch Nicht-Erreichbarkeit oder durch „Umleitungen“ zur Analyse des Datenstroms. Mit den bereitgestellten Informationen können diese Störungen in Echtzeit analysiert oder Angriffe rückverfolgt werden, um darauf z.B. im Rahmen der SOC Tätigkeiten reagieren zu können. Bei Oracle werden diese Informationen beim Routing auch automatisch durch den DNS Service verwendet.

DNS Trafficsteuerung (ehemals Dyn): Um auf URLs zugreifen zu können, werden die Domains (z.B. www.oracle.com) auf eine IP Adresse abgebildet. Diese Abbildung wird durch die Domain Name Systeme (DNS) durchgeführt. Der DNS Service leistet neben der Auflösung auch eine DNS Trafficsteuerung wie Loadbalancing, Ausfallerkennung/-umleitung, Netzabhängige Steuerung etc.

Oracle Web Application Firewall (WAF) ist ein cloudbasierter Service, der Anwendungen vor böswilligem und unerwünschtem Internetverkehr schützt. Oracle Cloud Infrastructure WAF kann jeden mit dem Internet verbundenen Endpunkt, ob On-Premises, in der Oracle oder einer anderen Cloud, schützen und eine konsistente Durchsetzung der Regeln in den Anwendungen eines Kunden gewährleisten.Mit Oracle WAF können Layer7 DDos Abwehr und bereitgestellte Policies zur Abwehr von Cross-Site Scripting (XSS), SQL Injection und andere von OWASP (CRS 3.0) definierte Sicherheitslücken genutzt werden. Eine eigene Bot Erkennung und Abwehr ist vorhanden.

Werden alle Edge Services genutzt, findet zuerst eine DNS Steuerung bei der Auflösung der URL in eine IP statt. Der nächste Kontaktpunkt ist die WAF, die entsprechende Prüfungen vornimmt. Erfolgreiche Prüfungen der WAF lassen dann den Request auf den adressierten Server oder Loadbalancer oder API Gateway in der Cloud oder On-Premises, durch. Für das Monitoring stehen sowohl die Log-Informationen aus den aufgerufenen Services, der WAF und den „Health Checks“ zur Verfügung.

Weitere Cloud Services sind angekündigt, **Oracle Cloud Guard und Oracle Maximum Security Zones**. Beide dienen der Überwachung der Oracle Cloud und führen zum Teil selbständig Korrekturen in der Cloud durch um Angriffe abzuwehren. Durch die Vorintegration der Cloud Services ist damit eine zentrale Stelle für das Monitoring und Threat-Hunting vorhanden.

Cloud Services mit der **Autonomous** Kennzeichnung beinhalten Security Funktionen wie automatisches oder geschedultes Security Patching und Prüfung auf verdächtiges Verhalten. Aktuell sind das die Oracle Datenbank und Oralce Linux. 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).

ORACLE 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 Maschine läuft. Kunden haben in diesem Fall 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 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, ISO27017/18, BSI C5, PCI-DSS und HIPAA. Weitere 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 anderen 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 zum Monitoring und sicherer Enklaven.

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

ORACLE CLOUD ON-PREMISES: DEDICATED REGION ODER CLOUD AT CUSTOMER APPLIANCES

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 Services bereit, dank derer Kunden ihre Daten und Prozesse nahtlos in die Cloud migrieren können.

- Oracle bietet mit „Dedicated Regions“ an eine Oracle Cloud in ihrem Rechenzentrum oder einem Ihrer Provider aufzubauen. Für die Verwaltung der Cloud gibt es dabei mehrere Optionen.
- Oracle bietet mehrere Appliances, d.h. kein vollständiges funktionales Abbild der Oracle Cloud an. Dies sind „Cloud at Customer“ (wie Exadata) oder der „Cloud Appliance“ oder Tactical Edge Cloud. Das sind Appliances Hardware und Software, bei der die Oracle Cloud Plattform im Hause des Kunden steht.

Mit diesen Optionen ist dieser der Betreiber der Cloud Plattform im eigenen Haus und profitiert zusätzlich vom flexiblen Abonnement-basierten Lizenzmodell. Diese Cloud Plattformen sind teilweise vollständig gemanagte Lösungen, d.h. Kunden partizipieren an der gleichen Erfahrung, Servicequalität und den neuesten Innovationen und Updates, die die Oracle Cloud kennzeichnen. 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. 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.

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 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