Regularien und jetzt? Datenschutz mit Oracle

Michael Fischer
Oracle Deutschland
München

Schlüsselworte
Oracle DB Security, Oracle DB Options, EU Datenschutzgesetz, Bundesdatenschutzgesetz, IT Sicherheitsgesetz, Verschlüsselung, Authentifizierung, Authorisierung, Auditing, Administration, Identity Management

Einleitung

Im Zuge der schärferen Diskussion um Regularien, zuletzt durch die Verabschiedung des EU Datenschutzgesetzes 2016 als auch durch bestehende Vorgaben wie Bundesdatenschutzgesetz oder IT Sicherheitsgesetz stellen sich oft zwei Fragen:

- Was steckt in diesen Regularien technisch gesehen im Kern drin und
- Welche Massnahmen könnten datenbankseitig umgesetzt werden damit bei einer eventuellen Prüfung oder einem Vorfall die IT in einem guten Licht steht.

Hierzu werden pragmatisch technische Massnahmen aufgezeigt die eine sinnvolle Basis für die Umsetzung sein können.

Disclaimer

Die Darstellung entspricht der Meinung des Autors und ist keine offizielle Darstellung von Oracle.

Scope

Im Folgenden wird das Thema Regularien und deren Umsetzung sowohl On-Premise, als auch in der Cloud betrachtet. Dies ist keine Anleitung um Compliance mit Regularien ganz oder teilweise zu erreichen. Vielmehr werden Mechanismen aufgezeigt die bzgl. Compliance helfen können. Für Unternehmen treffen in der Regel viele gesetzliche Regularien zu, beispielhaft werden hier die Folgenden herausgegriffen:

- Bundesdatenschutzgesetz gültig seit Dezember 1990, zwischenzeitlich mehrere Überarbeitungen, aktuelle Version 1.1.2016 (abgekürzt im Folgenden mit BDSG)
- EU Datenschutzverordnung in Kraft seit 14.4.2016, Umsetzung bis 2018 (abgekürzt im Folgenden mit EU-DP)
- IT-Sicherheitsgesetz verabschiedet im Dezember 2016, wartet auf Rechtsverordnung (abgekürzt im Folgenden mit IT-SIG)

Die Regularien sind typischerweise so formuliert, dass die technische Umsetzung nicht eindeutig beschrieben ist. Manche Vorgaben sprechen von "Schutz" andere nennen "Stand der Technik bei

Security" und führen technische Maßnahmen beispielhaft auf, z.B. Verschlüsselung. Andere Regularien wie EU Datenschutz bestehen aus Artikeln welchen Folge zu leisten ist und einer sehr viel grösseren Menge an Amendments/Ergänzungen, die versuchen Teile der Artikel zu konkretisieren. Amendments sind regulatorisch gesehen nicht verbindlich wie Artikel. Darüberhinaus gibt es auch noch EU Direktiven, die Vorgaben aufführen, die jedoch länderspezifisch umgesetzt werden sollen. EU Direktiven haben nicht den Stellenwert wie Regularien.
Deutschland hat durch das BDSG schon seit längerem eine im EU Vergleich strenge Datenschutzverordnung. Sie ist mittlerweile branchenübergreifend und wird durch bundeslandspezifische Datenschutzverordnungen (kurz LDSG) noch verschärft. Ferner gibt es in unterschiedlichen Branchen, z.B. mineralölverarbeitende Industrien, Verordnungen die BDSG/LDSG umfassen.

Vorgehen

Eine Betrachtung ist immer unternehmensspezifisch, Compliance oder Datenschutz auf Knopfdruck wird es nicht geben. Ein Vorgehen hinsichtlich der Technik könnte in folgenden Schritten durchgeführt werden:

- Klären welchen Regularien man unterliegt
- Klären ob Mindeststandards für die Branche vorliegen und was State of the Art ist
- Klassifikation der Daten und Systeme inkl. Risikobetrachtung
- Zusammenstellen der jeweiligen technischen Maßnahmen
- Umsetzungsplanung / Roadmap und Umsetzung

Um sich dem Thema pragmatisch zu nähern können technische Maßnahmen auch aus Vorgaben abgeleitet werden:

Abb1: Gemeinsamer Nenner bei Regularien

Die Aufteilung 80/20 für technische Maßnahmen wurde lediglich zur Visualisierung gewählt um aufzuzeigen dass viele Regularien einen gemeinsamen Nenner haben. Diese Aufteilung ist jedoch mangels der technischen Spezifikation in den Regularien nicht belegbar. Auch über Auditoren oder Prüfer dürfte sich kein einheitliches Bild ableiten. Je nach technischem Hintergrund des Prüfers ist z.B. beim Schutz von sensiblen Daten für den einen Verschlüsselung "State-of-the-Art", für den anderen reicht ein definierter Personenkreis ähnlich einem Archivzugang.

Ist kein "Compliance" Projekt im Unternehmen aufgesetzt oder mit zu grosser Zeitverzögerung für bestimmte Bereiche, so kann auch ein präventives Vorgehen gewählt werden (Pfeil "präventiv" in der

folgenden Abbildung), um dann für spätere Compliance Prüfungen eine gute Ausgangsbasis zu haben. Gleichzeitig liegt damit auch im Bereich Cyber Security die Latte höher:

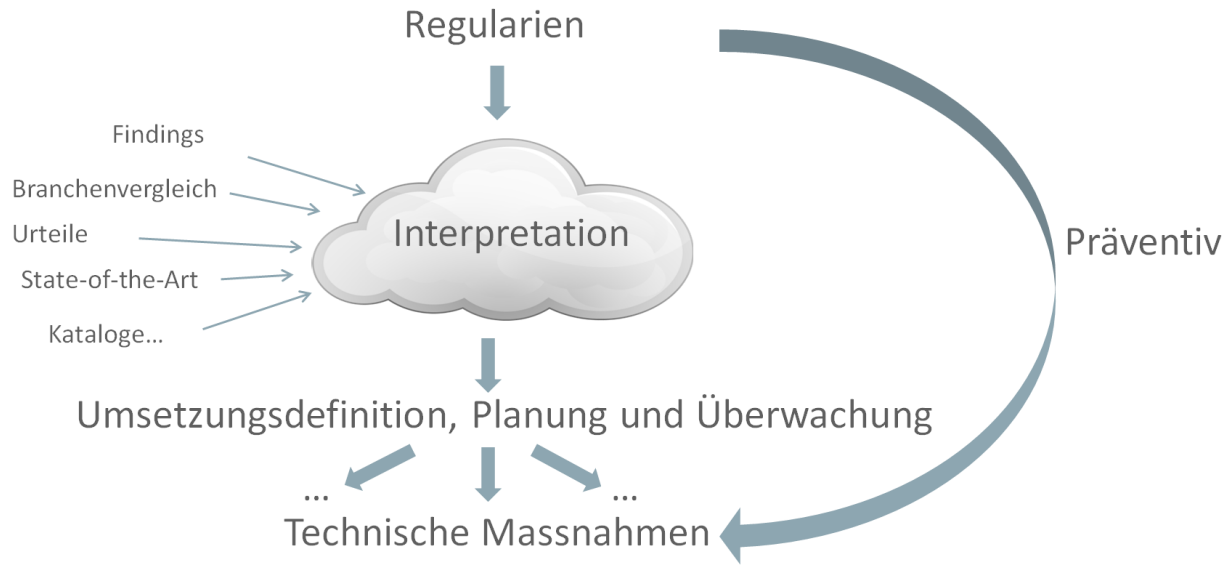

Abb.2: Präventive Massnahmen als Vorgriff

Exemplarisch umfassen die Anforderungen des EUDP foldende Punkte:

Abb.3: EUDP High Level Anforderungen

Die geforderten Security Best Practices (hier "Data Protection First") sind grob zusammengefasst:

1. Authentifizierung, Stärke nach Bedarf
2. Authorisierung inkl. Least Privilegue, Zweckgebundenheit und Duty Segregation (SoD)
3. Verschlüsselung, Pseudonymisierung, Masking
4. Monitoring und Audit für Nachweise und Informationen bei Meldepflicht, Nachweis der Berechtigungen
5. “State of the Art” und ähnliche Aussagen enthalten auch: Secure Configuration, Patching, SDLM (Dev.)

Beispielsweise werden diese in den Regularien wörtlich hier gefordert:

EU DP Art. 32 Security of Processing
Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data;

BDSG 3. Zugriffskontrolle: zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und ... Daten bei der Verarbeitung, Nutzung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Neben den direkt Security relevanten Anforderungen spielen andere Punkte ebenfalls in den Bereich Security, beispielsweise das "Recht auf Vergessen". Dafür gibt es technisch neben dem physischen Löschen (offener Punkt dabei Backups) auch andere Lösungen. Z.B. kann über Verschlüsselung und Tokenisierung erreicht werden dass mit dem Löschen des Schlüssels oder des Tokenmappings/-tabelle die Daten trotz Backup unbrauchbar sind.

Die meisten Unternehmen werden diese Massnahmen ganz oder in Teilen umgesetzt haben, da Vorgaben z.B. durch das BDSG schon länger bestehen und die möglichen technischen Hilfsmittel entsprechend lange verfügbar sind.

Oracle unterstützt durch folgende Komponenten die o.a. Anforderungen:

1. Authentifizierung, Stärke nach Bedarf:
   Einzelne Oracle Produkte unterstützen die Authentifizierungen auf unterschiedliche Art und Weise. Eine Oracle Datenbank unterstützt sowohl den Login mit User / Passwort als auch als starke Authentifizierung über Zertifikate oder Kerberos Tickets. Beim Anmelden am führenden System wie Kerberos können dort zusätzlich unterschiedlich starke Authentifizierungen hinterlegt werden. Andere Oracle Anwendungen unterstützen andere Verfahren oder lassen ein "universelles" Anmeldesystem (Oracle Access Management) und ggf. Benutzerverzeichnis (Oracle Directory Services) zu. In Oracle Access Management können kontextabhängig verschiedene Autentifizierungen vorgegeben werden. Beispielsweise ist ein Login auf ein HR System von aussen nicht möglich oder ein Admin Zugriff von einem nicht registrierten Gerät benötigt ein Einmalpasswort.

2. Authorisierung inkl. Segregation of Duties
   Die Authorisierung regelt den Zugriff auf Daten und Funktionen. Typischerweise ist diese in den jeweiligen Anwendungen integriert und das Management erfolgt in bereitgestellten Oberflächen oder von aussen über ein Identity Management. Um höher priorisierte Benutzer vor Fehlern zu bewahren können speziell für diese je nach System zusätzliche Mechanismen umgesetzt werden. Die Oracle Datenbank unterstützt beispielsweise die Daten von Usern so zu trennen, dass auch Admins sich nicht das Recht geben können auf Daten zuzugreifen oder in der Lage sind sich diese Rechte einfach zu beschaffen (Oracle Database Vault). Soll die Zweckgebundenheit beim Zugriff dokumentiert und kontrolliert werden kann dazu ein sogenanntes Privileged Account Management eingesetzt werden.

Hier können über vorher genehmigte Tickets oder hinterlegte Begründungen diese Accounts zeitlich befristet (und ggf. gemonitort) ausgecheckt werden. Das Oracle Werkzeug hierzu ist der Privileged Account Manager.
Eine weitere Form der Duty Segregation ist beim Zuteilen von Berechtigungen kritische Berechtigungskombinationen zu prüfen und diese ggf. zu verhindern. Dies funktioniert gleichzeitig über verschiedene Systeme hinweg. Ausnahmen können zeitlich befristet definiert werden, z.B. bei Urlaubsvertretungen. Auch ist es möglich diese Prüfungen adhoc gegen Systeme zu prüfen. Oracle stellt diese Funktionalitäten in der Oracle Governance Suite bereit.

3. Verschlüsselung, Pseudonymisierung, Masking
   Eine Verschlüsselung kann in jeder Schicht der Anwendung erfolgen. Oracle's Philosphie ist diese möglichst nah an den Daten auszuführen (at rest). Eine Übertragung sollte verschlüsselt erfolgen (in transit). In Transit werden Kanalverschlüsselung, https/TLS oder bei DB und LDAP Kommunikation die jeweilige Protokollverschlüsselung eingesetzt. Eine Verschlüsselung am Speicherort wird entweder durch die Datenbank (Oracle Advanced Security TDE) oder durch das Filesystem erzielt. Die Masterkeys können dabei von einem zentralen Schlüsseltresor (Oracle Key Vault) verwaltet werden.
   Pseudonymisierung kann über Oracle Dataredaction umgesetzt werden. Dabei werden die Daten nur beim Verlassen der Datenbank pseudonymisiert und bleiben erhalten. Möchte man ein optional irreversibles Masking erzielen um beispielsweise Daten in Test und Entwicklungsumgebungen zu verwenden so stellt Oracle dafür Oracle Masking und Subsetting zur Verfügung.

4. Monitoring und Audit
   Um Nachweisfähig zu sein erfolgt typischerweise ein Logging. Diese Daten werden nach Bedarf aggregiert und ausgewertet. Im Bedarfsfall auch mit Auditdaten korreliert. Aufschluss über den Nutzer hinter den Aktivitäten liefert dabei entweder das Benutzerverzeichnis oder ein Identity Management System. Oracle unterscheidet hierbei in die Verwaltung von Accounts und Berechtigungen und dessen Auditlogs, den Auditlogs der Datenbanken und den Logs der Applikationen. Oracle Identity Gvernance liefert das Audit/Monitoring hinsichtlich der Berechtigungen, Oracle DB Audit Vault aggregiert und wertet DBLogs und Access Logs aus. Diese bzw. die relevanten Informationen können an ein SIEM weitergereicht werden.

5. “State of the Art” und ähnliche Aussagen erfordern darüber hinaus eine sichere Grundkonfiguration nach Best Practices, ein regelmässiges Patching vor allem bzgl. der Security Patches und einen sicheren Entwicklungsprozess (SDLM).
   Die Funktion mit Abgleich zu Best Practices, Patches und eigene Vorgaben erfolgt durch Oracle Life Cycle Manager. Dieser kann darüber hinaus auch Konfigurationen von Umgebungen vergleichen.

Oracle visualisiert die Komponenten in folgender Abbildung:

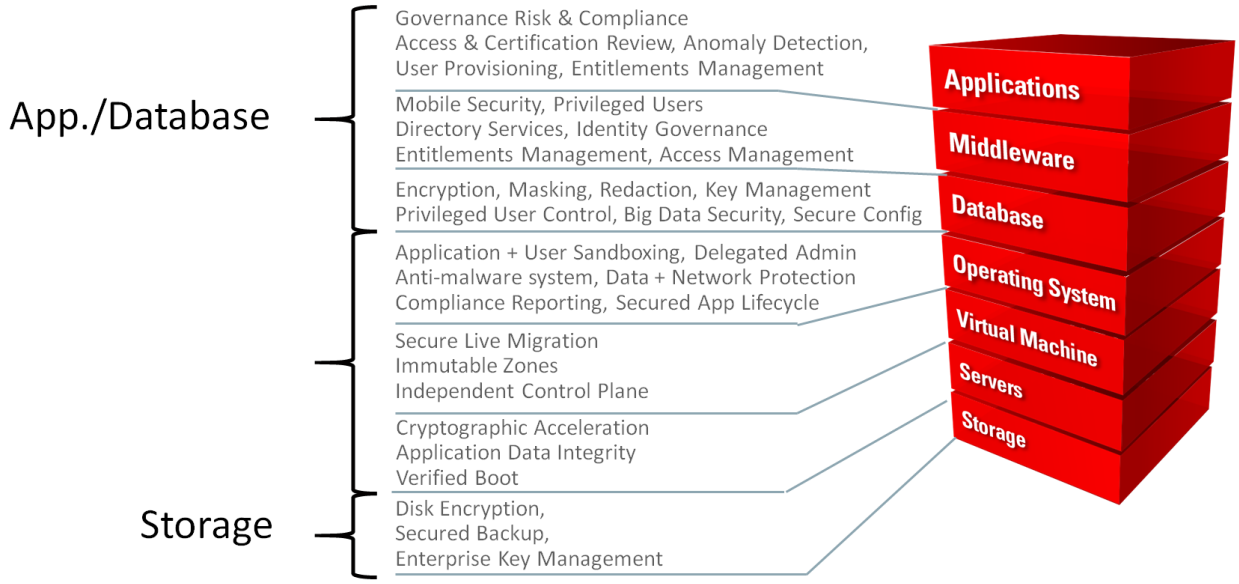

Abb.4: Oracle End-to-End Security für OnPremise, Hybird, Cloud

On-Premise und Oracle Cloud:

Oracle stellt diese Mechanismen On-Premise als auch in der Cloud zur Verfügung. Diese Mechanismen lassen sich auch in einem logischen System zusammenfassen,beispielsweise bei der Datenbank Verschlüsselung. Die Verschlüsselung der Oracle Datenbanken und der Oracle Datenbanken in der Cloud (DBaaS) ist dieselbe Funktionalität. Diese beruht jeweils auf Keys die über ein Wallet gespeichert werden. Diese Wallets mit den Keys können lokal liegen oder über einen zentralen Oracle Key Vault Server verwaltet werden. Ergebnis ist dass die Daten, die in der Oracle Datenbank gespeichert werden verschlüsselt sind. Diese Verschlüsselung bleibt auch im Backup erhalten, die Datenbanken sind dann sowohl On-Premise als auch in der Cloud ladbar.

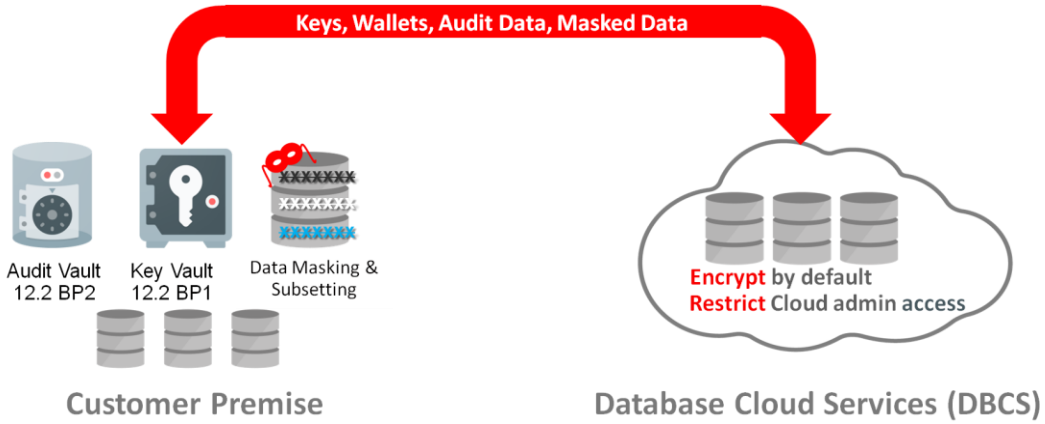

Abb.5: Oracle Security Komponenten in der Cloud als auch OnPremise

Die im vorhergehenden Abschnitt beschriebenen Produkte von Oracle sind entweder so oder in anderer Form bzw. unter anderem Namen in der Cloud vorhanden. Im Rahmen der Lizenzierung können auch Komponenten von OnPremise in die Cloud verschoben werden.

Wo anfangen?

Ist diese Betrachtung zu unternehmensübergreifend oder zu langwierig kann man beispielsweise mit den Datenbanken starten. Laut Verizon lagern 66% der sensiblen Daten eines Unternehmens in Datenbanken. Ein lohnendes Ziel also.

Abb.6: Oracle Security Einführungmodell für die Datenbank

und dies dann nach Bedarf um folgende Funktionen ausbauen:

- Personalisieren der Zugriffe, zentralisiertes Mgmt., least privilegue
- Nachweis und Prüfung der vorhandenen Berechtigungen, Access Reports
- SoD und Überwachen/Auswerten der Zugriffe

Oder nur nachsehen?

Möchte man um ein Bild zu bekommen "einfach" den Status Quo prüfen gibt es hierzu auch Hilfestellungen. Verschiedene Werkzeuge von Oracle ermöglichen z.B. eine Prüfung der Oracle Datenbanken gegen Best Practices, empfohlene Patches oder gegen (bereitgestellte) Compliance Regeln. Einige der Möglichkeiten sind:

- Durch den Verantwortlichen kann verifiziert werden dass in Testsystemen / auf Testdaten / für externe Entwicklung keine sensitiven Produktivdaten verwendet werden. Um Produktivdaten zu anonymisieren und referentielle und implizite Integritäten zu erhalten gibt es das Oracle Masking und Subsetting für die Datenbank.
- Werden in Produktivsystemen sensitive Daten angezeigt obwohl diese nicht im Klartext lesbar sein sollen und eine Änderung der Anwendung zu aufwendig ist, besteht die Möglichkeit in

der Datenbank Pseudonymisierung mit Hilfe der Data Redaction einzuschalten um die Daten on the fly zu maskieren (z.B. Geburtsdatum oder Kreditkartennummer).

- Möchte man die verwendeten, also nicht nur zugewiesenen, Privilegien in der Datenbank montitoren, um in einem Folgeschritt Berechtigungen auf die nur tatsächlich benötigten Rechte zu beschränken wird diese Funktion über Database Vault bereitgestellt. Auch ein "Test" zugeschnittener Rollen ist über einen Simulationsmodus mit Database Vault möglich.

- Oracle Kunden mit Datenbanksupport haben die Möglichkeit ein Tool (Scripts) über Ihren Supportzugang kostenfrei herunterzuladen und es gegen Ihre Datenbanken zu testen, Das Ergebnis (Findings) wird sowohl in Rohform als auch in Reports dargestellt. Typische Prüfungen umfassen default Schemas in Produktion, nicht geänderte oder schwache Passwörter, hohe Berechtigungen etc.

- Kunden mit dem Oracle Enterprise Manager Lifecycle Pack haben die Möglichkeit Ihre Datenbank gegen Best Practices, empfohlene Patches zu prüfen. Auch Konfigurationsunterschiede zwischen Umgebungen können so ermittelt werden. Eine weitere Komponente ist das enthaltene Compliance Framework. Hier sind Regeln enthalten (z.B. STIG) die geprüft werden und dessen Ergebnisse für eine Weiterverarbeitung webbasiert bereitgestellt werden. Das Regelwerk kann beliebig angepasst werden.

- Auch ein Montoring über Datenbanken verschiedener Hersteller hinweg kann helfen sich einen Überblick zu verschaffen was passiert. Dabei kann auf die Log Informationen der Datenbanken zurückgegriffen oder diese vor den Datenbanken abgegriffen werden. Die Monitoring Daten werden aggregiert, so dass auch komplexere problematische Aktivitäten erkannt werden können (z.B. loginversuche gegen alle gefundenen Datenbanken). Oracle Database Firewall bietet darüber hinaus die Möglichkeit SQl Zugriffe zu verändern (z.B. SQL Injections zu behandeln) oder zu blocken.

Weitere Funktionen wie die Analyse nach sensitiven Daten etc. sind enthalten aber nicht weiter aufgeführt.

Fazit

Datenschutz wie durch viele Regularien gefordert gibt es leider nicht auf Knopfdruck. Technische Vorgaben wie eine Checkliste sind nicht enthalten so dass es auf die spezifische Auslegung ankommt. Die gute Nachricht dabei ist dass der Kern der Regularien eine grosse Übereinstimmung hat und die abgeleiteten technischen Massnahmen kein Hexenwerk sind und vorab umgesetzt werden können. Viele Kunden nutzen erfolgreich Oracle Komponenten um Compliance zu erlangen bzw. Anforderungen von regularien zu erfüllen. Dies umfasst nicht nur die o.a. Regularien sondern geht weiter über SOX, PCI etc.

Kontaktadresse:
Michael Fischer
ORACLE Deutschland B.V. & Co. KG
Riesstr. 25
80992 München

Telefon: +49 (0)172 8323654
E-Mail michael.fischer@oracle.com
Internet: www.oracle.de