EU DS-GVO.
Beitrag von Oracle-Lösungen zur Datensicherheit.

Ernst Lorenz
Oracle B.V. & Co. KG
München

Schlüsselworte
EU Datenschutz-Grundverordnung, Data Breaches, Oracle Sicherheitsarchitektur, Oracle Sicherheitsstrategie, Datensicherheit, personenbezogene Daten, Personensicherheit, Identity Governance, Security Operation Center, Security Monitoring and Analytics

Einleitung

Kundendaten sind für Unternehmen besonders wertvoll und werden deshalb per se sehr aufwändig gepflegt. Ab Mai 2018 unterliegen sie dann, mit Gültigkeit der EU Datenschutz-Grundverordnung, auch einem stark erweiterten rechtlichen Schutz. Sicherheitsverletzungen müssen innerhalb von 72 Stunden gemeldet werden und können mit empfindlichen Strafen, bis zur Höhe von 4% des jährlichen Firmenumsatzes, sanktioniert werden. Gemäß den Regelungen der Verordnung gibt es Risiken in den IT Systemen. Der Vortrag betrachtet die Risiken und erläutert anhand der Artikel der Datenschutz-Grundverordnung welche Oracle Betriebsmittel helfen können, die Sicherheitsanforderungen der DSGVO, in komplexen und heterogenen IT Betriebsumgebungen, umzusetzen.

EU DS-GVO: Beitrag von Oracle-Lösungen zur Datensicherheit.

Mittlerweile ist über ein Jahr seit der Veröffentlichung der EU Datenschutz-Grundverordnung am 4. Mai 2016 vergangen. Im Gegensatz zur EU Datenschutzrichtlinie von 1995 erlangt die Verordnung ab dem 25. Mai 2018, am Ende der zweijährigen Übergangsfrist, ummittelbare Geltung und gilt vorrangig zu nationalem Recht. Dementsprechend wurde der Gesetzesentwurf zur Anpassung des Datenschutzrechts in Deutschland an die EU Verordnung am 27. April 2017 vom dt. Bundestag verabschiedet.

Mit der Verordnung legen die Juristen in gewisser Weise auch eine Architektur vor, deren 99 Artikel und Abschnitte, sowie den 173 Erwägungsgründen, mit einem IT Pflichtenheft zu vergleichen sind. Die Statik der Verordnung ist die Definition der sogenannten Akteure. In Artikel 4 der Verordnung werden zum Beispiel in den einzelnen Abschnitten diese Akteure definiert und die juristischen Kriterien, denen sie unterliegen, operationalisiert.

Die zwei zentralen Akteure sind der „Verantwortliche“ (Controller) und der „Auftragsverarbeiter“ (Processor). Daneben werden noch einige weitere Akteure definiert, über die sich insbesondere auch die neuen Internet und Cloud basierten Paradigmen regeln lassen. Alle Akteure stehen in juristisch definierten Verhältnissen zueinander, das in sehr detaillierter Weise Bezug auf ihre Verantwortlichkeiten, zum Schutz und zur Sichererung der personenbezogenen Daten, nimmt.

Oracle ist bei der Bereitstellung von Cloud Services ein Auftragsverarbeiter und speichert im Auftrag der Kunden personenbezogene Daten. Die Kunden sind im Sinne der DS-GVO Verantwortliche in Bezug auf die Verarbeitung der personenbezogenen Daten, die sie Oracle anvertrauen. Oracle unterstützt Kunden als Technologieanbieter mit Hilfe von Lösungen (Produkten und Services) dabei, ihre Complianceanforderungen umzusetzen.

Zwischen den beiden Akteuren besteht eine sogenannte „shared responsibility“, deren konkrete Ausgestaltung vom jeweilig verfolgten Betriebseinsatzszenario bestimmt ist. Die Betriebseinsatzszenarien lassen sich unterscheiden nach OnPremise, IaaS, PaaS oder SaaS Cloud Services und hybride Systeme.

Solche hybriden oder ausschließlich Cloud basierten Szenarien unterliegen vielfältigen Bedingungen, die sie von den bisherigen klassischen OnPremise Szenarien unterscheiden. In OnPremise Szearien muß sich der Kunde komplett um alles kümmern. Sowohl um den Datenschutz als auch um die Sicherheit der IT Systeme und die Verarbeitung, bis hinab ins letzte Betriebs- und Anwendungsdetail.

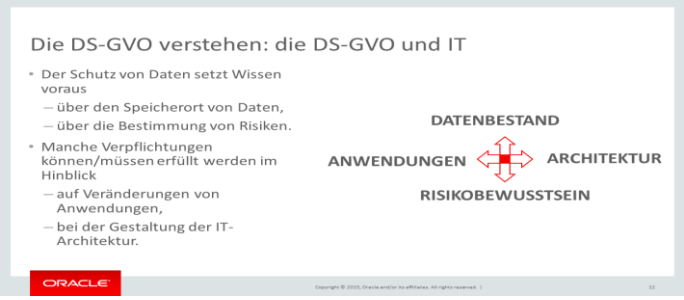
Aus Sicht der IT lassen sich im Kontext der EU Datenschutz-Grundverordnung im Wesentlichen drei zentrale Risikofelder identifizieren. Das augenfälligste Risiko sind „Data Breaches“, also Einbruchsszenarien die auf den Diebstahl, die Zerstörung oder die kriminelle Manipulation der schützenswerten personenbezogenen Daten zielen. Solche Angriffsszenarien auf die Daten können sowohl von außerhalb der IT Systeme als auch von Innen, durch die Mitarbeiter, erfolgen.

Das zweite Risiko leitet sich von dem Freiheitsgrundsatz ab, daß die Daten dem Individuum, also dem Datensubjekt gehören und nicht dem Unternehmen, der Behörde oder dem Auftragsverarbeiter. In der Verarbeitung der Daten, also sowohl in der Speicherung als auch in den Geschäftsprozessen, müssen die Unternehmen und die Behörden deshalb eine besondere Sorgfaltspflicht an den Tag legen, die gegenüber den Aufsichtsbehörden zu dokumentieren ist. Der Artikel 35 der Verordnung spricht in diesem Zusammenhang explizit von der nachzuweisenden „Datenschutz-Folgenabschätzung“. Diese zweite Risikokategorie für die Unternehmen und die Behörden besteht darin, daß die Aufsichtsbehörden die Dokumentation der sicheren Behandlung der personenbezogenen Daten im

Unternehmen und der Behörde detailliert aufgezeigt bekommen müssen, wenn das von den Datensubjekten eingefordert wird. Im Falle des Artikel 35 muß die Dokumentation pro-aktiv erfolgen.

Das dritte Risiko für die IT Verarbeitung besteht im Audit und der Reaktionszeit, wenn tatsächlich Datenpannen eingetreten sind oder kriminelle Machenschaften an den Daten erfolgreich waren. Verstöße müssen den Aufsichtsbehörden innerhalb von 72 Stunden gemeldet werden. Zugleich müssen die betroffenen Daten aufgezeigt werden und die, von den Datenschutzverstössen betroffenen Datensubjekte, ohne schuldhaftes Verzögern benachrichtigt werden. Die Kontrolle dieses Risikos setzt in den IT Systemen voraus, daß die Verstösse erkannt werden und sehr schnell nachvollzogen werden kann, welche Daten und welche Individuen davon betroffen sind.

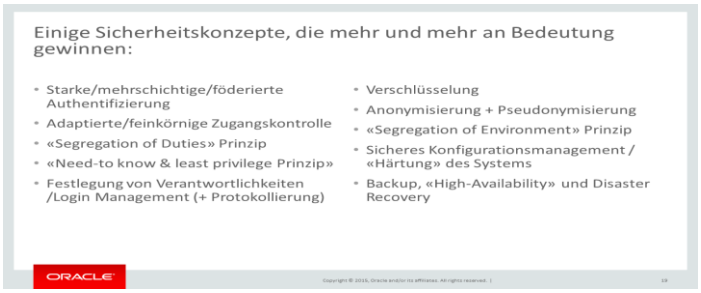
Die Sanktionsfälle, unter Androhung empfindlicher Strafen und die Festlegung der Bedingungen zur Regelung von Schadenersatzansprüchen, werden im Rahmen des Artikel 83 der Verordnung bewertet und entschieden. Auf Basis des Artikel 83 „Allgemeine Bedingungen für die Verhängung von Geldbußen“ untersuchen die Aufsichtsbehörden den Grad der Verantwortlichkeit der Hauptakteure und nehmen Bezug auf den Schaden beziehungsweise Verstoss gegen auferlegte Sorgfaltspflichten im Umgang mit den Daten. Der Umgang mit den Daten bestimmt sich wiederum maßgeblich durch die eingesetzte IT.



Um letztlich auf die Risiken reagieren und pro-aktiv Vorsorge für die Sicherheit treffen zu können, ist es für die Unternehmen, die Behörden und deren Data Protection Officers notwendig zu verstehen und zu analysieren, in welchen Anwendungen und Prozessen die personenbezogenen Daten stecken und wie sie verwendet werden. Das ist das „magische Viereck“ analog dem analysiert, bewertet und dann entsprechend strategisch verfahren werden muß, um die IT auf die Anforderungen der Datenschutz-Grundverordnung abzugleichen.

Die vier „Zielkategorien“ beziehen sich gemäß dem Artikel 30 auf a), daß jeder Verantwortliche bzw. jeder in der Sphäre des Verantwortlichen Handelnde im Sinne der Verordnung, ein „Verzeichnis aller Verarbeitungstätigkeiten“ für seinen Verantwortungsbereich führen muß, b) gemäß dem Artikel 35 das Risiko für den Betroffenen kennen und abschätzen muß, c) die „Rechte der Betroffenen“, im Sinne der „Zweckbindung“ der Daten, in der Verarbeitung durch die IT sicherstellen muß und d) einigen Bestimmungen der Verordnung unmittelbar genügen muß, in denen geeignete technische und organisatorische Maßnahmen, bezüglich der Implementierung in der IT, eingefordert werden.

Natürlich liegen auf Basis bereits bestehender anderer weltweiter Regulierungen, im Rahmen internationaler Best Practices, mittlerweile bereits vielfältige Erfahrungen darüber vor, welchen Sicherheitsprinzipien unbedingt gefolgt werden sollte:

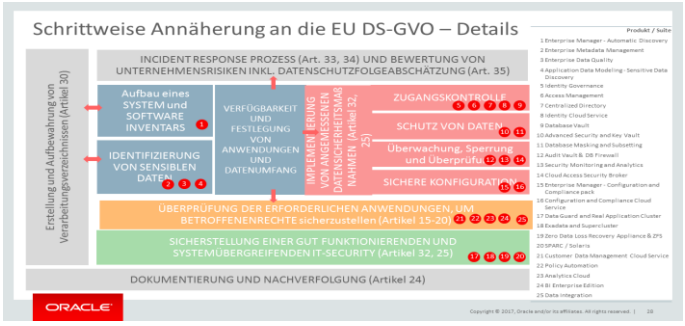


Das „Mantra“ der Oracle Sicherheitsphilosophie folgt dabei den Prinzipien „Security nearest to the data“ und „Security by default“.

Über das Oracle Produktportfolio werden vier Handlungsfelder zur Unterstützung in den Sicherheitsfragen der IT adressiert: a) die Datensicherheit, b) die Identity Governance, c) die Sicherheit des IT-Gesamtsystems sowie d) das Security Monitoring und die Analytik, in Verbindung mit der Überwachung der Konfigurationsumgebungen und zur Einhaltung von Compliance. Alle vier Handlungsfelder verstehen sich sowohl in Abbildung auf OnPremise Szenarien, als auch auf das Cloud Betreiberparadigma, oder für hybride Umgebungen.

Durch die Produkt-Vielseitigkeit und die Abstimmung der Funktionen aufeinander kann Oracle mit seinem Portfolio zur Sicherheit in allen Bereichen der Datenschutz-Grundverordnung Hilfestellung leisten.

Auf dieser abschließend dargestellten Folie sind die Oracle Sicherheitsprodukte und -funktionen den jeweiligen Regularien der Datenschutz-Grundverordung thematisch zugeordnet. Erst aus dem Zusammenspiel der unterschiedlichen Funktionen lassen sich die vielfältigen rechlichen Anforderungen der Verordnung gezielt und, auf Basis eines durchgängigen Sicherheitskonzeptes aufeinander abgestimmt, operationalisieren.



Kontaktadresse:
Ernst Lorenz
Oracle B.V. & Co. KG
Riesstr. 25
D-80992 München

Telefon: +49 (0) 89-1430-2850
E-Mail ernst.lorenz@oracle.com
Internet: www.oracle.com