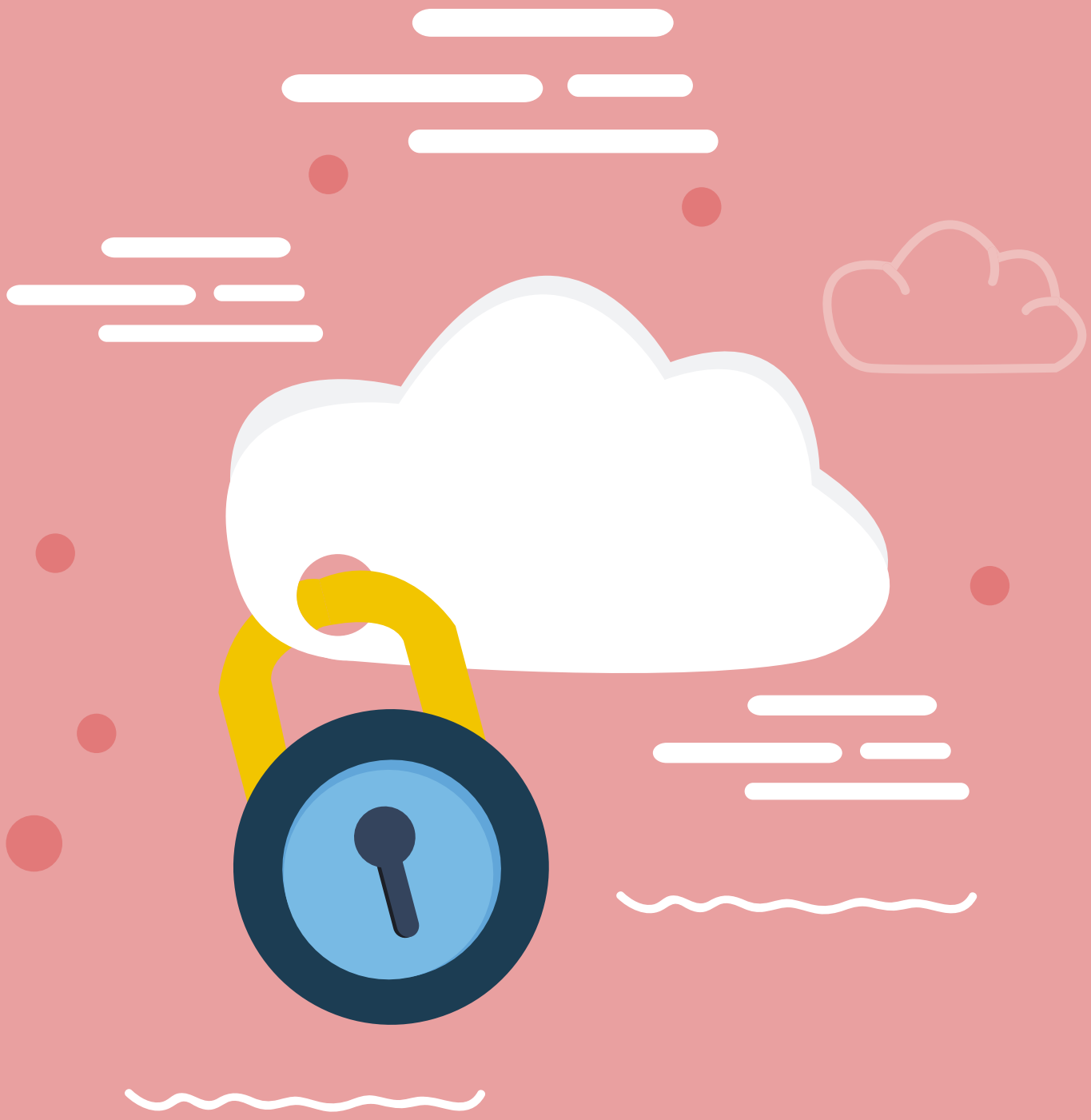
Oracle-Lösungen zur Datensicherheit

Ernst Lorenz, Oracle Deutschland B.V. & Co. KG



Am 25. Mai 2018 tritt die EU-Datenschutz-Grundverordnung in Kraft. Schon jetzt, in der Vorbereitungsphase, hat sich das Bewusstsein für IT-Sicherheit aufgrund der Häufung von Cyber-Crime-Attacken stark intensiviert. Kriminelle Angriffe auf Daten und Anwendungen sind in der Ausführung mittlerweile so raffiniert, dass auch der Schutz und die Abwehr „nachgerüstet" werden müssen. Seitens seiner Produktstrategie hat Oracle von Beginn an eine ganzheitlich angelegte Sicherheitsphilosophie verfolgt. Der Artikel zeigt auf, wo die von Oracle angebotenen Sicherheitstechniken möglicherweise helfen können, die Anforderungen und Ziele der EU-Datenschutz-Grundverordnung zu adressieren.

Die Datenschutz-Grundverordnung umfasst 99 Artikel und 173 sogenannte „Erwägungsgründe". Schon allein dieses Zahlenverhältnis von normativen Festlegungen zu Erläuterungen zeigt, wie komplex die Anwendungssachverhalte sind. Die eigentliche Herausforderung für die Umsetzung der Verordnung stellen jedoch die Varianz und Komplexität der heutigen IT-Systeme dar. Diese Systeme wurden nicht im juristischen Erwartungshorizont der EU-DSGVO entworfen. Um jetzt ab 25. Mai 2018 der Verordnung zu entsprechen und potenziell hohe Haftungsrisiken zu vermeiden, können Nachbesserungen bei der Sicherheit der IT-Systeme erforderlich sein.

Risikokategorien im Kontext der IT-Systeme

Der juristische Kontext der EU-DSGVO erwartet Sicherheit an verschiedenen Stellen der IT-Systeme. Wenn Unternehmen diesen Sicherheitsanforderungen nicht entsprechen, gehen sie nicht unerhebliche Risiken ein. Artikel 83 behandelt die „Allgemeine(n) Bedingungen für die Verhängung von Geldbußen" und bestimmt, dass getroffene technische Vorkehrungen bei der Entscheidung über Geldbußen berücksichtigt werden sollen.

Eines der größten Risiken im Sicherheitsverständnis der EU-DSGVO ist der Datendiebstahl. Unabhängig von den Sanktionen geht dieser häufig auch mit einem immensen Reputationsschaden für das Unternehmen einher. Die Kategorie „Datendiebstahl/ Data Breaches" soll hier als synonymer Begriff für alle Arten von Angriffen auf die zu schützenden personenbezogenen Daten verstanden werden. Weitere Erwartungen an die Sicherheit lassen sich den Kategorien „Sorgfalt in der IT" und „Meldepflicht" zuordnen. Technisch gesehen sind die drei Hauptbereiche wichtig:

- Verhinderung und Vermeidung von Datenschutzverletzungen
- Nachweiserbringung und Dokumentierung des Umgangs mit personenbezogenen Daten
- Bericht und Benachrichtigung im Pannenfall

Angriffe können sowohl von extern, also von außerhalb der IT-Systemgrenzen, als auch von autorisierten Benutzern innerhalb des Systems erfolgen. Aus technischer Sicht ist für die Auswahl geeigneter Sicherheitsmittel neben den Angriffsszenarien auch die Art der potenziell an den Daten verursachten Schäden maßgeblich.

Grundsätzlich können zwei Arten von Schutzverletzungen erfolgen: Diebstahl von Personendaten und deren Manipulation. Dabei kann sich die Manipulation als noch gravierender als der Datendiebstahl auswirken. Arti-

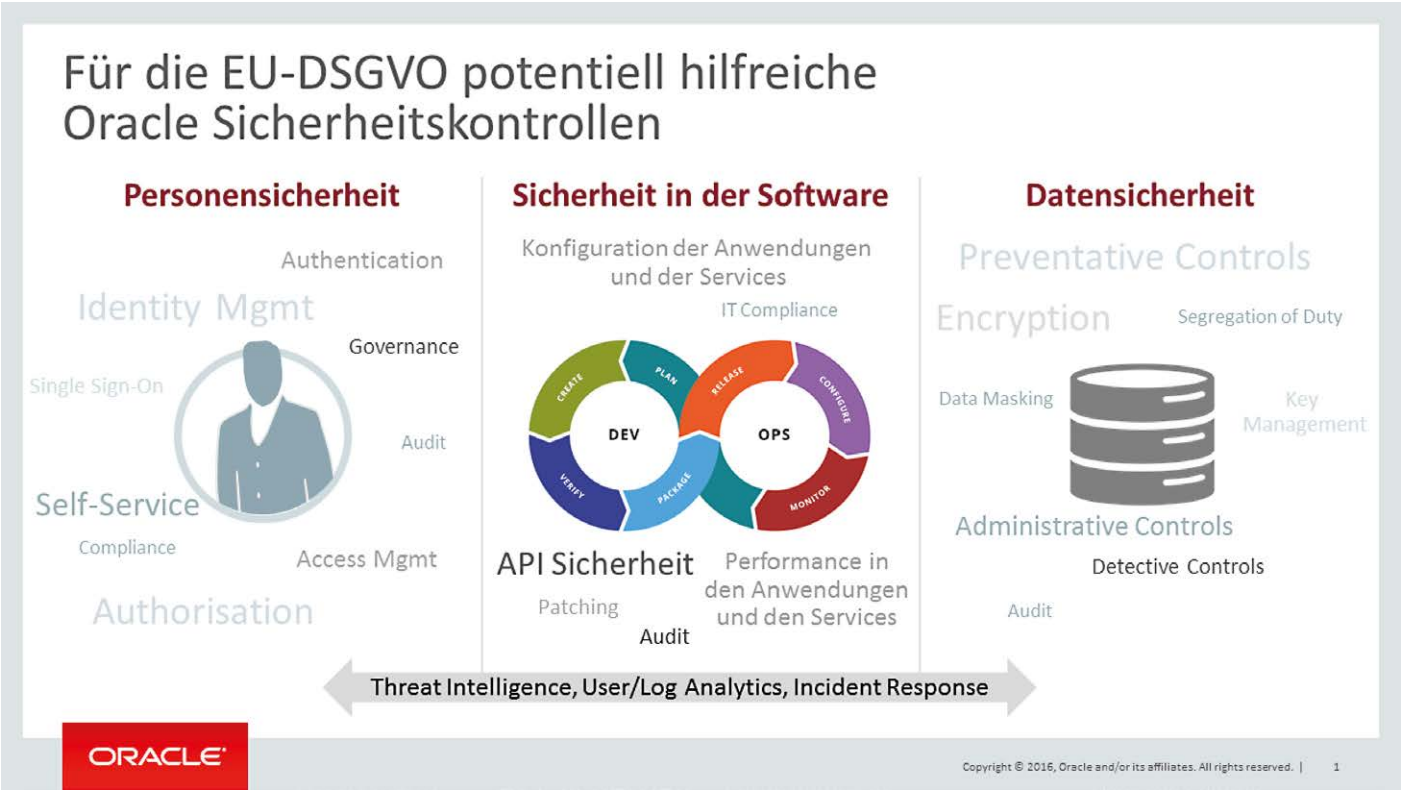


Abbildung 1: So können Oracle-Lösungen zur Datensicherheit beitragen

kel 34 der DSGVO über die „Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person" trägt dem Rechnung. Problematisch wird es insbesondere, wenn hochsensible Personendaten manipuliert werden, diese Manipulation aber nicht sofort erkannt wird. Im Falle spezieller Angriffe wie Ransomware fällt die Manipulation sofort auf, weil der Datenbestand des Unternehmens in krimineller Absicht verschlüsselt wird und nicht mehr zugänglich ist. Unternehmen müssen sich dann den Zugang zu ihren Daten wieder freikaufen.

Sorgfaltspflichten in der Verarbeitung, Dokumentation und Berichterstattung

In einer von IDC 2017 herausgegebenen Studie wird sehr pointiert dargestellt, warum sich die EU-DGSVO nicht nur auf die Verhinderung von Datendiebstahl und -manipulation reduziert [1]. Auch mangelnde Sorgfalt in der Datenverarbeitung kann beanstandet werden. Unternehmen sollten deshalb die drei Dimensionen „Angriffsabwehr", „Schadenminimierung" und „Sorgfalt im Verfahrensbetrieb" über den Einsatz technischer und organisatorischer Sicherheitsmittel absichern [2].

Aufgrund seiner langjährigen Erfahrung ist Oracle der Überzeugung, dass die Sicherheit am effizientesten gemäß den Prinzipien „Nearest to the data" und „Least privilege", also Daten- und Zugriffssicherheit, zu implementieren ist, weil das Angriffsziel immer direkt auf die Daten gerichtet ist. *Abbildung 1* zeigt dazu einen Funktionsüberblick.

Technische Oracle-Sicherheitsmittel

Verschlüsselung der Daten kann zum Beispiel im Fall eines Datendiebstahls das Risiko eines Schadens für betroffene Personen verringern. Die gestohlenen Daten sind unkenntlich gemacht und daher regelmäßig wertlos. Bei der Maskierung von bestimmten Feldinhalten werden bestimmte personenbezogene Informationen in der Verarbeitung verfälscht, um die negativen Auswirkungen eines Datenverlusts zu begrenzen. Werden Feld-Inhalte randomisiert, ist der eigentliche Informationsgehalt der Daten zerstört, sodass sie möglicherweise an Dritte weitergegeben werden können; dennoch ermöglicht es die Oracle-Lösung, die relationalen Datenbeziehungen für Test und Entwicklung zu erhalten. Beim Subsetting von Daten-Untermengen werden sensible Daten nur sehr gezielt und minimiert bereitgestellt. So lassen sich potenzielle Angriffsflächen verringern und damit der Schutz vergrößern. Eine ähnliche Strategie wird verfolgt, wenn auf kritische Feld-Attribute Label-Vergaben zur Bildung von Risiko-Kategorien erfolgen. Über das Label wird dann, analog zu den Risikozuordnungen, der Zugriff auf die Daten kontrolliert und protokolliert.

Klassische Zugriffs- und Rechte-Steuerungen, wie Benutzername und Passwort, sind zwar nach wie vor notwendig, aber in den modernen Systemumgebungen bei weitem nicht mehr ausreichend. Wenn im Internet mit wechselnden Endgeräten auf die Daten zugegriffen wird, sollten die Daten zusätzlich, neben abgesicherten Zugriffskontrollen wie zum Beispiel der Zwei-Faktor-Authentifizierung, entsprechend obigen Sicherheitsmitteln geschützt sein. Die Internet-Verarbeitungsszenarien sind maßgeblich dafür verantwortlich, dass sich die klassischen Systemgrenzen der IT-Systeme zunehmend auflösen. Diese Unschärfe in der Abgrenzung der Systeme erfordert völlig neue Überwachungs- und Absicherungsmittel *(siehe Abbildung 2)*.

Deshalb müssen sich Unternehmen jetzt auch zunehmend überlegen, wie sie ihre Cloud-Strategie in Einklang mit den Erwartungen der EU-DSGVO bringen; insbesondere, welche Rolle die unterschiedlichen Cloud-Betriebsmodelle hinsichtlich Sicherheit und Risiko im IT-Aufbau für das Unternehmen darstellen. Wie wird zum Beispiel die Datensicherheit in hybriden Umgebungen (On-Premises, Cloud) hergestellt? Wie wird die Verarbeitung im Gesamtsystem überwacht, insbesondere wenn über sogenannte „Shadow-IT" potenziell Daten unkontrolliert abfließen können? Wie wird, analog zu den Vorgaben der DSGVO, die Verarbeitung auditiert und dokumentiert? Speziell auch hinsichtlich

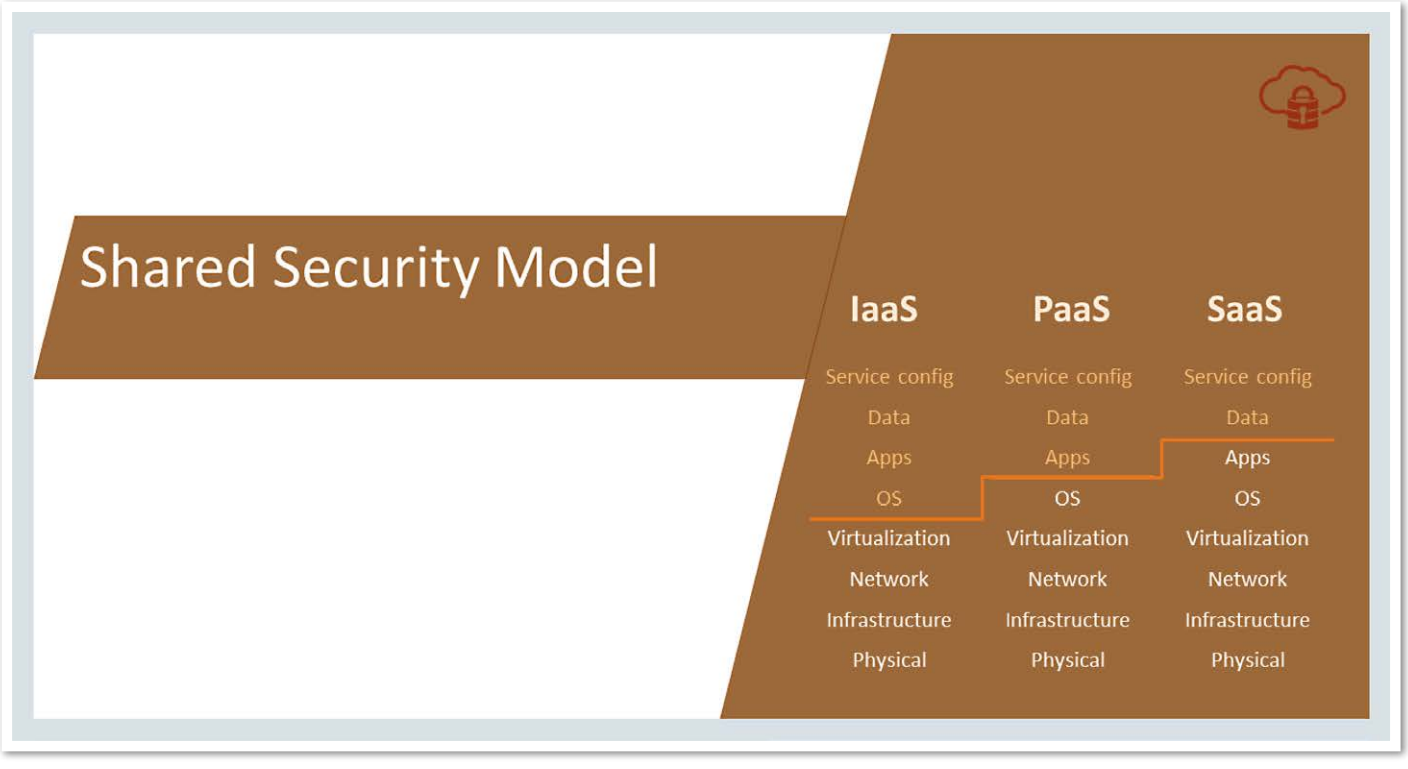


Abbildung 2: Unterschiedliche Betriebsmodelle und verteilte Verantwortung

der besonders zu schützenden personenbezogenen Daten, gemäß den Vorgaben der Verordnung nach den Artikeln 30 und 35 [3]. Dazu gehört dann auch die Vorbereitung darauf, wie Pannenfälle (Risiko-Kategorie „Meldepflicht“) zu dokumentieren sind und wie an die Aufsichtsbehörden berichtet wird.

Betriebsmodelle im Kontext der DSGVO-Akteure

Die EU-DSGVO weist eine sehr klare und eindeutige Architektur auf. Sie ähnelt einem Pflichtenheft, wie man es aus der Informatik kennt. In Artikel 4 „Begriffsbestimmungen“ und in den Erwägungsgründen 26 bis 37 werden unter anderem die Akteure der Verordnung und ihre juristischen Verhältnisse zueinander definiert. Dabei unterliegen die Akteure bestimmten Verantwortlichkeiten, sie müssen bestimmte Aufgaben erfüllen und unterliegen spezifischen Rollenerwartungen.

Den eigentlichen Kern der EU-DSGVO bilden die beiden Hauptakteure „Verantwortlicher“ und „Auftragsverarbeiter“. Der Verantwortliche muss entscheiden, welche Risiken im IT-System abzudecken und welche Datensicherungsmittel dafür einzusetzen sind. Gegenüber den Daten-Subjekten und ihren Rechten und Freiheiten an ihren personenbezogenen Daten existiert das Prinzip der „Beweislastumkehr“. Nicht das Daten-Subjekt muss nachweisen, dass seine/ihre Daten nicht ausreichend gesichert scheinen. Der Verantwortliche muss die rechtmäßige Verarbeitung und vor allem die erforderliche Datensicherheit nachweisen können, gegebenenfalls auch gegenüber der Aufsichtsbehörde (Artikel 5, Absatz 2).

Aus Sicht der Rollenverteilung der DSGVO ist das Unternehmen gerade auch im Betriebsmodell „On-Premises“ immer Verantwortlicher. Über Zulieferer, wie zum Beispiel Oracle, können für den On-Premises-Betrieb entsprechende ergänzende Sicherheitsprodukte zur Datenbank, zur Middleware, zum Identity Management, zur Überwachung und zum Reporting erworben werden. Wichtig für das Verständnis des On-Premises-Modells ist, dass die Entscheidung darüber, wie das datenschutzrechtlich geforderte Sicherheitsniveau herzustellen ist, ausschließlich in der Verantwortung des Unternehmens liegt.

Verlagert das Unternehmen Teile seiner IT in Cloud-Betreibermodelle, ist der Cloud-Betreiber Akteur im Sinne der DSGVO (Auftragsverarbeiter). Unternehmen können dann die von dem Cloud-Provider getroffenen Sicherheitsvorkehrungen bei der Prüfung ihrer Datenschutz-Compliance berücksichtigen. Oracle als On-Premises-Lösungsanbieter und Cloud Provider bietet seinen Kunden diesbezüglich die volle Durchgängigkeit der technischen Sicherheitsmittel über alle Betreibermodelle hinweg an. So werden zum Beispiel alle im Oracle-Cloud-Umfeld betriebenen Datenbanken per Default verschlüsselt.

Über Oracle Key Vault kann sich der Kunde zum alleinigen Besitzer aller benötigten Sicherheitsschlüssel machen und hat damit die vollständige Kontrolle über seine Daten. Dies wird ergänzt durch entsprechend starke und restriktive Authentifizierung- und Autorisierungs-Mechanismen sowie darauf aufbauende Zugriffskontrollen, über die kontrolliert werden kann, wer im On-Premises- und Cloud-Umfeld auf welche Instanzen und Daten zugreifen darf.

Persönliche Rechte, Überwachung, Auditing, Dokumentation und Benachrichtigung

Neben den bisher aufgezeigten Sicherheitserwartungen der EU-DSGVO gibt es zwei weitere Anforderungsbereiche. Diese betreffen die bereitzustellende Sicherheit im fachlich funktionalen Kontext. Die gesetzliche Grundlage dafür findet sich in den Artikeln 5 „Grundsätze für die Verarbeitung personenbezogener Daten“ und 7 „Bedingungen für die Einwilligung“ der Verordnung. In *Abbildung 3* sind beide sicherheitsrelevan-

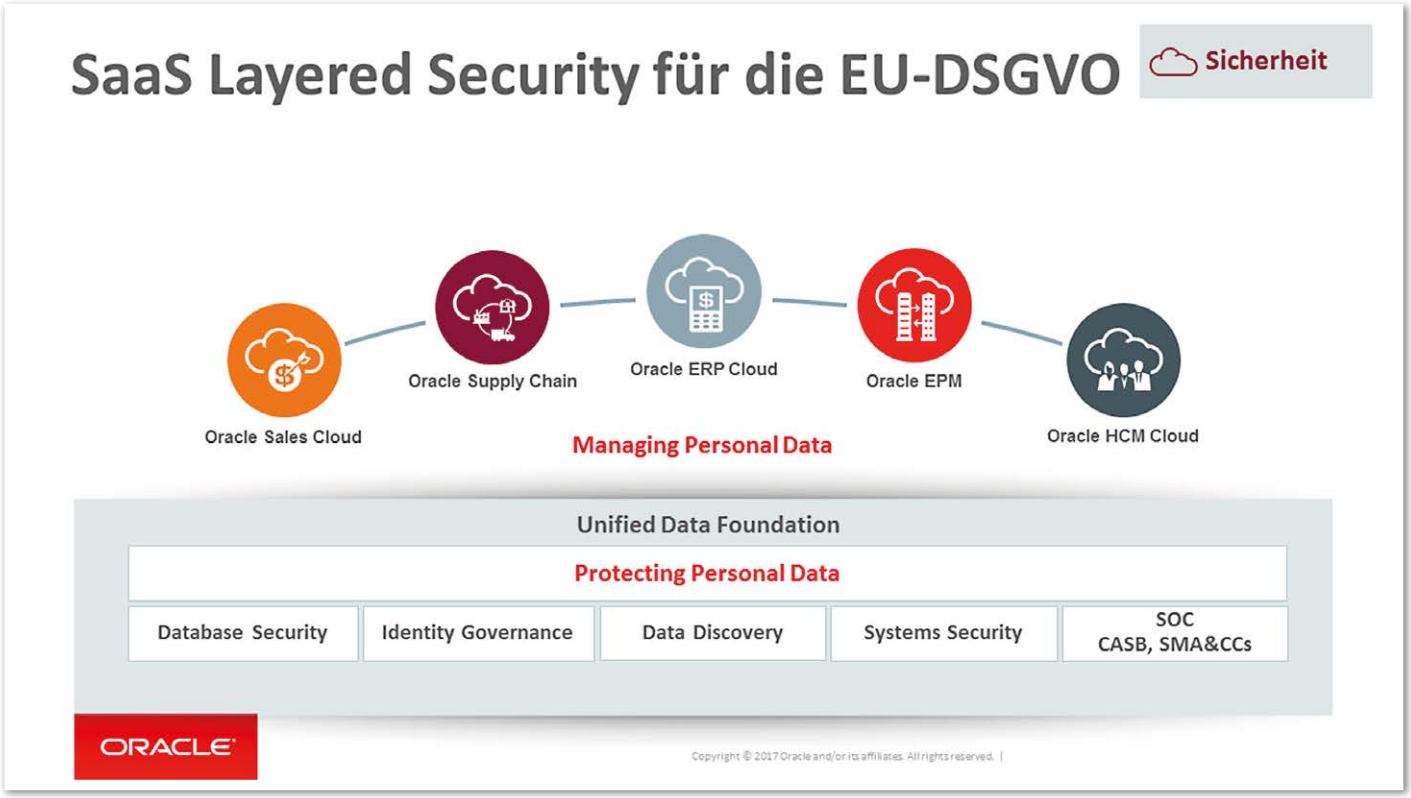


Abbildung 3: Sicherheit im fachlich funktionalen Bereich

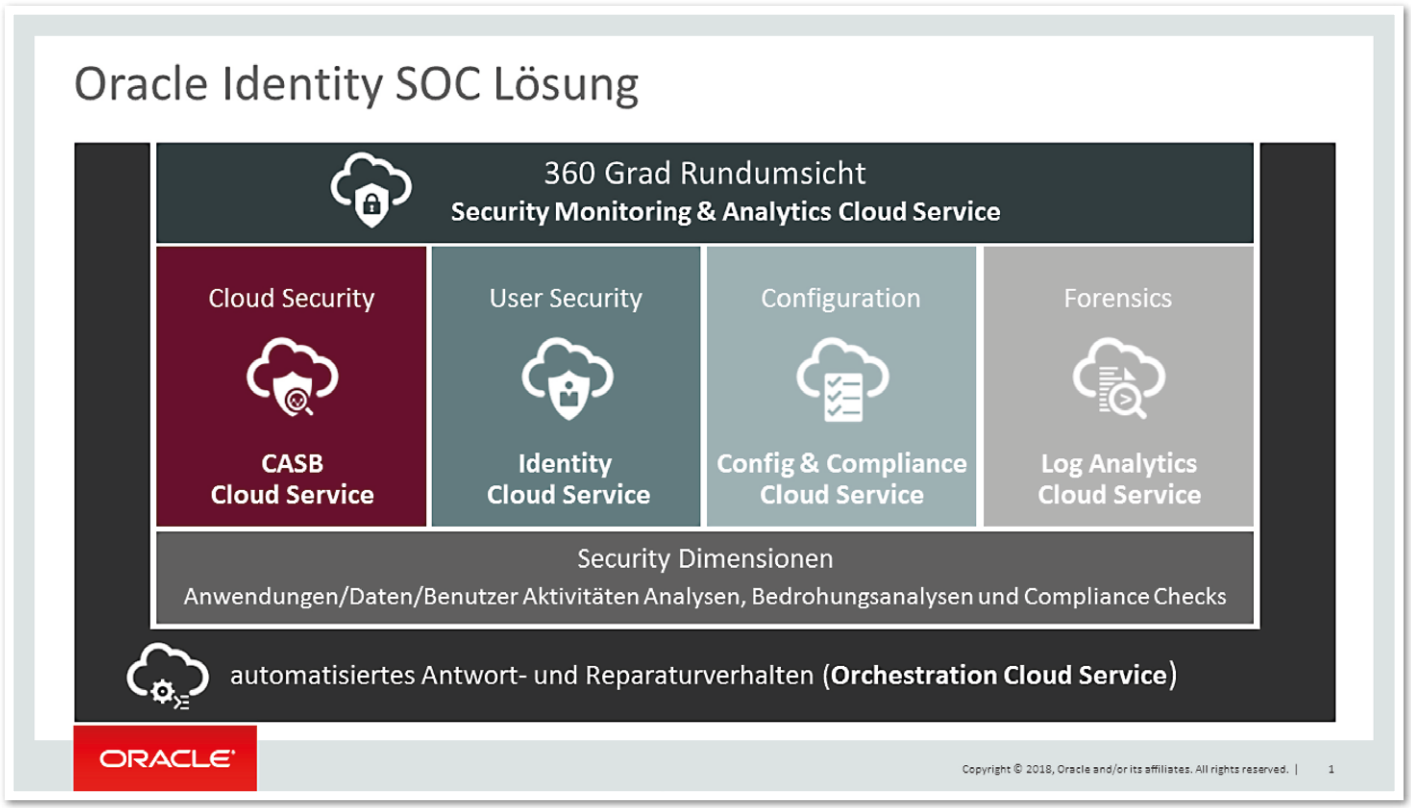


Abbildung 4: Angriffsabwehr und Systemschutz

ten Hauptkategorien in Beziehung zueinander gesetzt. Nach oben hin, in Richtung der Anwendungen, versteht sich Sicherheit als „Managing Personal Data". Nach unten hin, in Richtung der Infrastruktur, realisiert sich Sicherheit im Kontext der Infrastruktur als „Protecting Personal Data".

„Managing Personal Data" muss im Sinne der EU-DSGVO die fachlichen Rechte der Person an ihren Daten umsetzen. Das beginnt mit Funktionen zur Verwaltung der Einwilligung, die eine Person für die Verarbeitung ihrer personenbezogenen Daten abgibt. Dazu gehört auch die Implementierung für die Daten-Migration, entsprechend dem Recht auf Datenübertragbarkeit gemäß Artikel 20. Die Artikel 16 bis 19 der Verordnung [4] spezifizieren das Recht auf Berichtigung, auf Löschung, auf Einschränkung in der Verarbeitung sowie auf entsprechende Mitteilungspflicht im Verarbeiten der personenbezogenen Daten.

Im Kontext der funktionalen Sicherstellung dieser individuellen Rechte der Person gewinnen dann insbesondere auch die Auflagen der EU-DSGVO hinsichtlich Auditing, Dokumentation und Benachrichtigung ihre hohe Bedeutung. Nicht nur die EU-DSGVO, auch andere Compliance-Regelungen schreiben diesbezüglich den Unternehmen im Rahmen ihrer branchenüblichen Vorgaben [5] ein detailliertes Reporting in der Datenverarbeitung vor. Rechte sind also nicht nur entsprechend funktional abzubilden, sondern es ist auch die detaillierte Nachvollziehbarkeit und Berichtsführung hinsichtlich der Compliance gefordert.

Oracle-Datenbanken auditieren alle Zugriffe auf die Datenbanken im sogenannten „Audit-Log". Auf dessen Basis können dann Sicherheitshinweise bei sicherheitskritischen Ereignissen an die Administration gemeldet werden oder nachträglich forensische Untersuchungen, im Falle von Datenmissbrauch, durchgeführt werden.

Die von Oracle angebotene Audit-Vault-Lösung kann Verarbeitungsdaten sowohl von On-Premises- als auch von Cloud-Datenbanken sammeln. Es lassen sich Oracle- und auch Nicht-Oracle-Datenbanken protokollieren, ebenso wie Operating-System- und Network-Logs sowie die Log-Dateien der Anwendungen. Auf deren Basis können über den Audit Vault Database Firewall Server (AVDF) Audit-Reports erstellt werden. Diese sind im Rahmen der Compliance-Regelungen als Nachweis verwendbar.

Schutz des IT-Gesamtsystems

Durch die Häufung der kriminellen Angriffe wird das für die Unternehmen auch insbesondere im Blickwinkel der Datenschutz-Grundverordnung wichtig. Als Cloud-Provider muss sich Oracle mittlerweile auch verstärkt auf das Sicherheitsmanagement im IT-Gesamtzusammenhang konzentrieren, das unter dem Begriff „Security Operation Center" (SOC) zusammengefasst ist. Wichtige Prinzipien, denen der SOC-Ansatz maßgeblich folgt, sind:

- Zentralisierung und Standardisierung der sicherheitsrelevanten Informationen
- Machine Learning für die Überwachung und Krisenintervention

Die Konzepte für das SOC gibt es mit SIEM [6] und UEBA [7] schon seit einigen Jahren. Bei SIEM wird ein Ansatz des Sicherheitsmanagements verfolgt, der darauf abzielt, eine ganzheitliche Sicht auf die Sicherheit in der Informationstechnologie eines Unternehmens zu entwickeln. UEBA ist ein Machine-Learning-Modell, das helfen kann, Sicherheitsanomalien aufzudecken und Cyber-Attacken zu identifizieren. Im großen Stil eines RZ-Betriebs geht das nur, wenn alle die Sicherheit betreffenden Daten standardisiert und vergleichbar gemacht sind.

Im Jahr 2017 hat Gartner im Rahmen einer Forschungsarbeit dieses komplexe Zusammenspiel der Angriffsabwehr beschrieben. Entsprechend Gartner lässt sich das

„CARTA-Verständnis“ [8] folgendermaßen zusammenfassen: „Die Strategie des Verteidigungsansatzes muss der kontinuierlichen Risikoanpassung und der kontinuierlichen Prüfung darauf, ob dem System noch vertraut werden kann, folgen.“ In komplexen Systemen funktioniert das nur über Machine-Learning-Ansätze, bei denen standardisiert und permanent auf Abweichungen überwacht wird. „CARTA“ steht für „Continuous Adaptive Risk and Trust Assessment“. *Abbildung 4* fasst diese Gesamtsicht nochmals abschließend zusammen.

Weitere Informationen

[1] IDC Perspective – „Ten Myths regarding GDPR: Sifting Fact from Fiction“, Kuan Hon, Duncan Brown, June 2017, IDC #EMEA42628217

[2] Artikel 25 „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“.

[3] Artikel 30 „Verzeichnis von Verarbeitungstätigkeiten“, Artikel 35 „Datenschutz-Folgenabschätzung“

[4] Artikel 16 „Recht auf Berichtigung“, Artikel 17 „Recht auf Löschung“, Artikel 18 „Recht auf Einschränkung der Verarbeitung“, Artikel 19 „Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung“

[5] Zum Beispiel „Health Insurance Portability and Accountability Act“ (HIPAA) oder „Sarbanes-Oxley Act“ (SOX)

[6] „Security Information and Event Management“ (SIEM)

[7] „User and Entity Behavior Analytics“ (UEBA)

[8] Gartner – „Use a CARTA Strategic Approach to embrace Digital Business Opportunities in an Era of Advanced Threats“, Neil MacDonald, Felix Gaehtgens, May 2017, ID #G00332400

Ernst Lorenz
ernst.lorenz@oracle.com

In sieben Schritten zu EU-DSGVO-Verfahrenshandbuch & Co.

Mag. Wolfgang Klinger und DI (FH) Ernst Stippl, Sphinx IT Consulting GmbH

Es gibt viele Gründe, sich nicht mit langweiliger Dokumentation zu beschäftigen. Doch die DSGVO ist in diesem Punkt ganz klar: Personenbezogene Daten und deren Verarbeitungen müssen dokumentiert sein. Dieser Leitfaden hilft in sieben Schritten, die DSGVO-relevanten Dokumente rechtzeitig fertigzustellen, um auch nach dem 25. Mai 2018 ruhig schlafen zu können.