ORACLE

EU-Datenschutz Grundverordnung DSGVO

Beitrag von Oracle-Technologien und Lösungen zur Datensicherheit

December 2020, Version 2.1

Am 25. Mai 2018 ist die EU Datenschutz-Grundverordnung in Kraft getreten. Damit und aufgrund der Häufung von Cyber Crime Attacken hat sich das Bewusstsein für IT-Sicherheit 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. In diesem Whitepaper zeigen wir auf, wo die von Oracle angebotenen Sicherheitstechniken möglicherweise helfen können, die Anforderungen und Ziele der EU Datenschutz-Grundverordnung zu adressieren.

Ausgangslagen und Überlegungen zur Sicherheitsstrategie

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 stellt jedoch die Varianz und Komplexität der heutigen IT-Systeme dar. Diese Systeme wurden nicht im juristischen Erwartungshorizont der EU-DSGVO entworfen. Um jetzt, ab 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 der EU-DSGVO 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 unter die Kategorien „Sorgfalt in der IT" und „Meldepflicht" subsumieren.

Angriffsszenarien und Verteidigungsstrategie

Technisch gesehen sind diese 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 Manipulation von Personendaten.** Dabei kann sich die Manipulation als noch gravierender als der Datendiebstahl auswirken. Artikel 34 der DSGVO über die „Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person" trägt dem Rechnung. Problematisch wird es insbesondere, wenn hoch sensible Personendaten manipuliert werden, diese Manipulation aber nicht sofort erkannt wird. Im Fall von speziellen Angriffen wie Ransomware fällt die Manipulation sofort auf, weil der Datenbestand des Unternehmens in krimineller Absicht verschlüsselt wird und nicht mehr zugänglich ist. Die betroffenen Organisationen 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 und Verwaltungen sollten deshalb die drei Dimensionen **Angriffsabwehr, Schadenminimierung und Sorgfalt im Verfahrensbetrieb** über den Einsatz technischer und organisatorischer Sicherheitsmittel absichern.

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

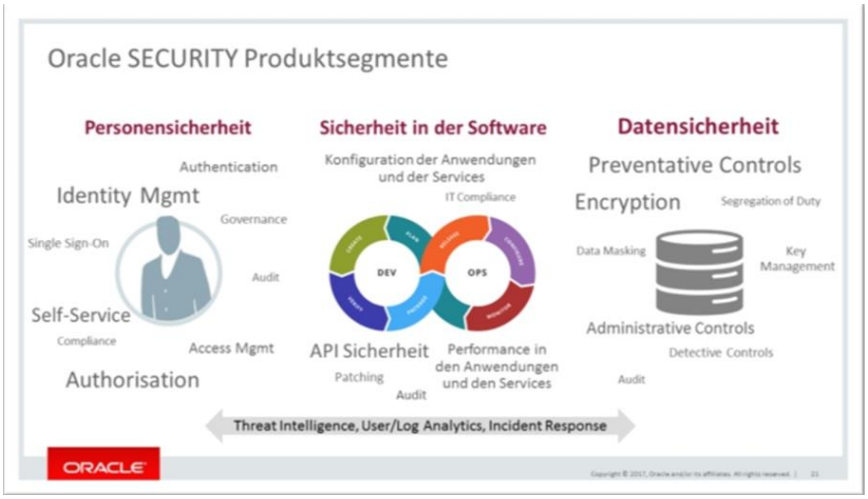

Abbildung 1: wie Oracle Lösungen zur Datensicherheit beitragen können

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

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

Ausgewählte Beispiele technischer Oracle Sicherheitsmittel

- Über **Verschlüsselung** der Daten kann zum Beispiel für den Fall eines Datendiebstahls das Risiko eines Schadens für betroffene Personen verringert werden. 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 Feldinhalte **randomisiert**, also der Personenbezug der Datenattribute nach dem Zufallsprinzip komplett überschrieben, so wird der eigentliche Informationsgehalt der Daten „zerstört", so dass sie dann möglicherweise an Dritte weitergegeben werden können; dennoch ermöglicht es die Oracle Lösung, die relationalen Datenbeziehungen für Test und Entwicklung zu erhalten.

- Beim **Subsetting von Datenuntermengen** werden sensible Daten nur sehr gezielt und minimisiert bereitgestellt. So können potenzielle Angriffsflächen verkleinert und damit der Schutz vergrößert werden.

- Eine ähnliche Strategie wird verfolgt, wenn auf kritische Feldattribute **Labelvergaben** zur Bildung von Risikokategorien erfolgen. Über das Label wird dann, analog den Risikozuordnungen, der Zugriff auf die Daten kontrolliert und protokolliert.

Klassische Zugriffs- und Rechtesteuerungen, 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 2-Faktor-Authentifizierung, entsprechend obigen Sicherheitsmitteln geschützt werden. 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.

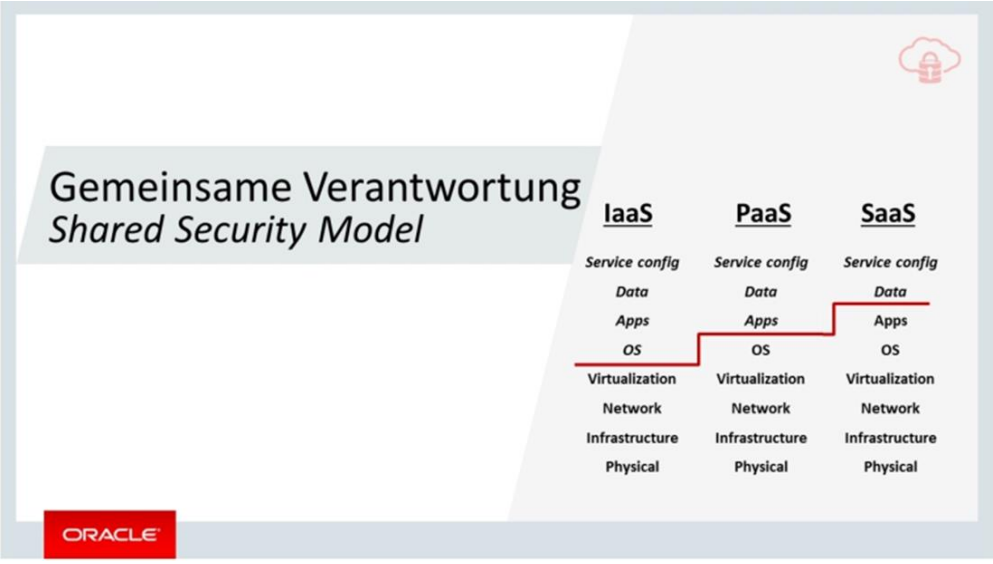

Abbildung 2: unterschiedliche Betriebsmodelle und verteilte Verantwortung

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 spielen. Wie wird zum Beispiel die Datensicherheit in hybriden Umgebungen (On-Premise, Cloud) hergestellt? Wie wird die Verarbeitung im Gesamtsystem überwacht, insbesondere wenn über sogenannte „Shadow-IT" potenziell Daten unkontrolliert abfließen können? Und wie wird, analog zu den Vorgaben der DSGVO, die Verarbeitung auditiert und dokumentiert? Speziell auch hinsichtlich 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" (Risikokategorie „Meldepflicht") zu dokumentieren sind und wie an die Aufsichtsbehörden berichtet wird.

Unterschiedliche Betriebsmodelle im Kontext der DSGVO Akteure

Die EU-DSGVO weist eine sehr klare und eindeutige Architektur auf. Sie ist ähnlich einem Pflichtenheft, wie man es aus der Informatik kennt, aufgebaut. In Artikel 4 „Begriffsbestimmungen" und den Erwägungsgründen 26 – 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 sind und welche Datensicherungsmittel dafür einzusetzen sind. Gegenüber den Datensubjekten und ihren Rechten und Freiheiten an ihren personenbezogenen Daten existiert das Prinzip der „Beweislastumkehr". Nicht das Datensubjekt muss nachweisen, dass seine / ihre Daten nicht ausreichend gesichert scheinen. Der Verantwortliche muss die rechtmäßige Verarbeitung, und vor allem die erforderliche Datensicherheit, nachweisen können, ggf. auch gegenüber der Aufsichtsbehörde (Art. 5 Abs. 2).

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

Verlagert das Unternehmen bzw. die Verwaltung Teile ihrer IT in Cloud Betreibermodelle, ist der Cloud Betreiber Akteur im Sinne der DSGVO (Auftragsverarbeiter). Unternehmen und Verwaltungen können dann die von dem Cloud Provider getroffenen Sicherheitsvorkehrungen bei der Prüfung ihrer Datenschutz-Compliance berücksichtigen. Oracle als On-Premise 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 Autorisierungsmechanismen sowie darauf aufbauende Zugriffskontrollen, über die kontrolliert werden kann, wer im On-Premise und Cloud Umfeld auf welche Instanzen und Daten zugreifen darf und wie zugegriffen wird.

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 der Abbildung 3 werden beide sicherheitsrelevanten 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.

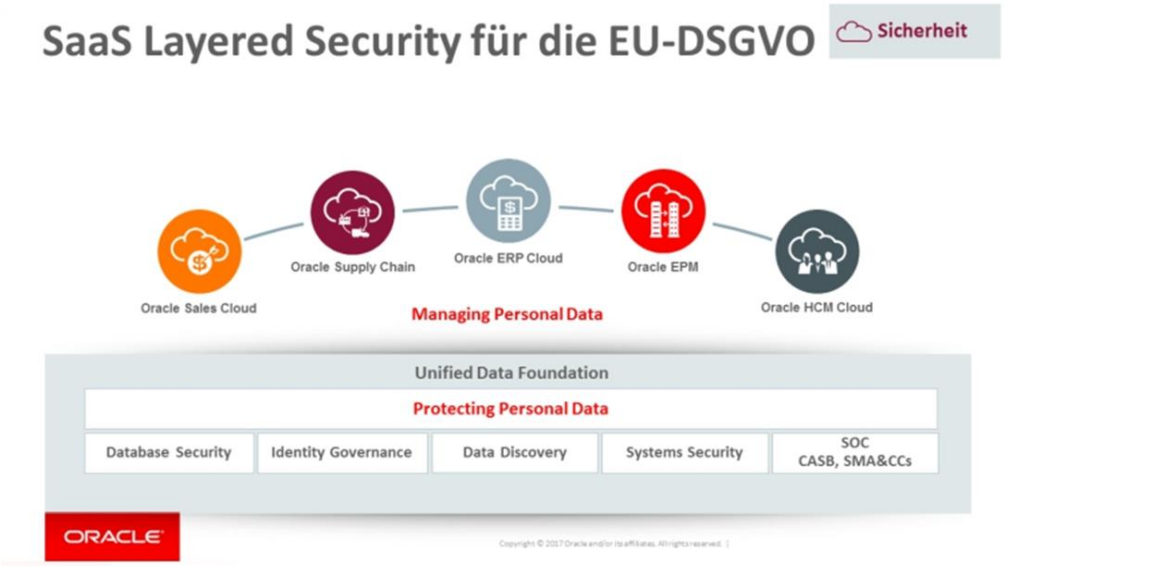

Abbildung 3: Sicherheit im fachlich funktionalen Bereich

„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 Datenmigration, entsprechend des „Recht(s) auf Datenübertragbarkeit“ gemäß dem Artikel 20. Die Artikel 16 – 19 der Verordnung4 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 und Verwaltungen, 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 Basis der Audit Logs 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-Premise als auch von Cloud Datenbanken sammeln. Es können sowohl Oracle als auch Non-Oracle Datenbanken protokolliert werden, ebenso wie Operating System Logs, Network Logs und die Log Dateien der Anwendungen. Auf Basis dieser Log-Dateien können über den **Audit Vault Database Firewall Server (AVDF) Audit Reports** erstellt werden. Diese Audit Reports sind als Nachweise, im Rahmen der Compliance Regelungen, verwendbar.

„Protecting Personal Data“ umfasst im Kern die bereits unter der Überschrift „ausgewählte Beispiele technischer Oracle Sicherheitsmittel“ beschriebenen Funktionen zur Datensicherung. Datensicherung, entsprechend der Kategorie **„Database Security“,** heißt aber zugleich auch immer entsprechende Datenzugriffskontrolle und Wahrung der Identität derer, die auf diese Daten Zugriffsberechtigungen haben. Als Begriff dafür hat sich die Kategorie **„Identity Governance“** etabliert. Aus methodischer Sicht ist die Voraussetzung für die Database Security und die Identity Governance eine entsprechend im IT-System zu verankernde **„Data Discovery“.** Äquivalente Konzepte zur Data Discovery werden auch unter den Stichworten **„Data Quality Management“** diskutiert und entwickelt. Im Kern geht es, im Kontext des Lifecycle-Management, um die stetige Qualifizierung der Daten, also die Einordnung und Bewertung dessen, welche Schutzmechanismen für welche Datenattribute im IT-System eingebaut werden müssen. Die im System implementierten Funktionen dafür werden unter dem Begriff der **„Sensitive Data Discovery“** zusammengefasst. Oracle hat eine ganze Reihe von Produkten im Angebot, die eine solche Datenqualifizierung Repository gestützt erlauben. Die Kategorie **„Systems Security“** eröffnet den Blick auf die Daten- und Zugriffssicherheit primär aus Sicht der Funktionsbereitstellung durch die Hardware. Im Rahmen seiner Betriebssystem- und Prozessorentwicklung (M7, Unix, Sparc) stellt Oracle Sicherheitsfunktionen bereit, die Daten- und Zugriffsschutz bis auf die Ebene der Hardware implementieren. Die von Oracle verfolgte Strategie dafür wird als **„Defense in Depth“** bezeichnet. Zu guter Letzt geht es dann noch darum, das IT-System als Ganzes entsprechend abzusichern.

Schutz des IT-Gesamtsystems

Insbesondere 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 wird. Wichtige Prinzipien, denen der SOC Ansatz maßgeblich folgt, sind:

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

Abbildung 4 fasst diese Gesamtsicht nochmals abschließend zusammen.

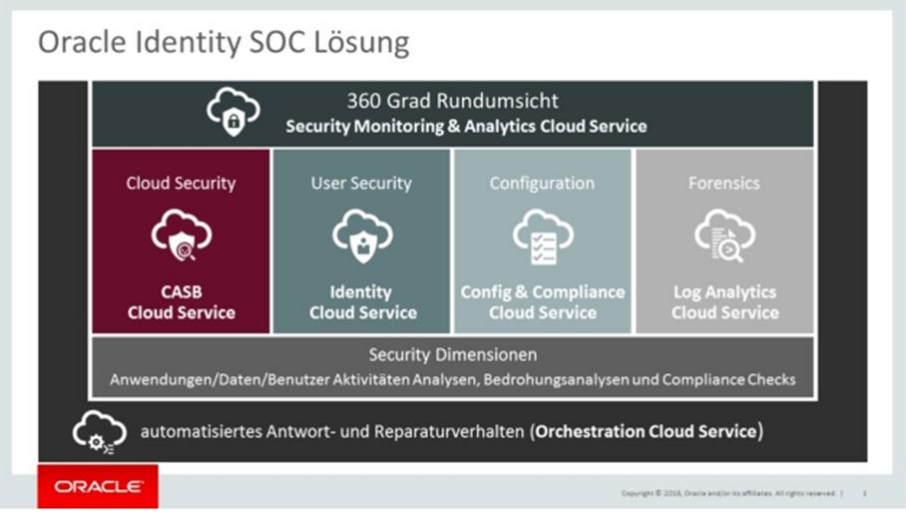

Abbildung 4: Angriffsabwehr und Systemschutz

Die Konzepte für das **SOC** gibt es mit **SIEM6** und **UEBA7** schon seit einigen Jahren. Mit „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 der Typus eines „Machine Learning Modells“ 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 werden.

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, ob dem System noch vertraut werden kann, folgen“.

In komplexen Systemen geht das nur über Machine Learning Ansätze. Wie lernt die Maschinenumgebung? Indem standardisiert wird und permanent auf Abweichungen überwacht wird. „CARTA“ steht für „Continuous Adaptive Risk and Trust Assessment“.