EU-DSGVO: Stand der Technik - Oracle Sicherheitsverständnis

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

Schlüsselworte
EU Datenschutz-Grundverordnung, IT-Sicherheitsgesetz, KRITIS, Cyber-Sicherheitsstrategie, Stand der Technik, OSI-Modell, Betroffenenrechte, technische Sicherheit, Datensicherheit, Datenschutz, Autonomie, Regularien, Regelkreis, Regeln, Künstliche Intelligenz, Machine Learning, Security Operation Center, Shadow IT, Oracle Sicherheitstechnologien

Einleitung

Die ***EU Datenschutz-Grundverordnung*** (EU-DSGVO) fokussiert auf den Schutz personenbezogener Daten. Neben der Sicherstellung der ***Betroffenenrechte***, wie sie sich aus Kapitel III DSGVO ergeben, stellen die ***Schutzerwartungen*** den Kern der Verordnung dar. Auch andere wichtige Regularien, wie z.B. das ***deutsche IT-Sicherheitsgesetz*** (ITSiG), referenzieren auf diese Erwartungen bezüglich Schutz und Sicherheit. Das ITSiG dabei insbesondere in Bezug auf die „***kritischen Infrastrukturen***“ in Deutschland, im Kontext der ***nationalen Cyber-Sicherheitsstrategie***.

Es zeigt sich, dass die weltweit entworfenen sicherheitstechnischen Regularien zunehmend konvergieren und in ihren Intentionen und Zielsetzungen weitestgehend gleichen Mustern folgen. Deshalb ist insbesondere auch die Frage interessant, welche Schnittmengen sich aufzeigen lassen.

Orientiert an der EU-DSGVO und dem deutschen IT-Sicherheitsgesetz kann dieser Fragestellung beispielhaft nachgegangen werden.

Konvergenz von Regularien

Die folgende Abbildung zeichnet die zeitliche Entstehungsgeschichte von EU-DSGVO und ITSiG nach.

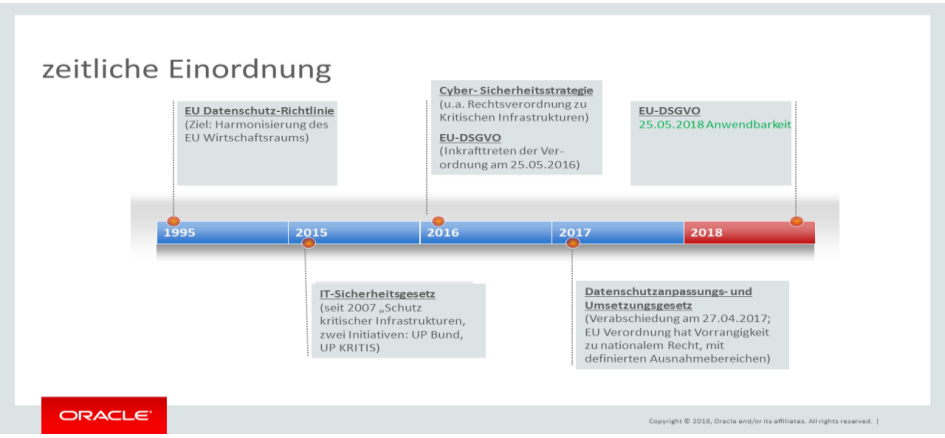

Abbildung „Zeithorizont der Regularien“

Im Sinne von Prävention und aktiver Angriffsabwehr kommt dem „***technischen Mitteleinsatz zur Herstellung von Sicherheit***“ eine entscheidende Bedeutung zu. Für dessen praktische Umsetzung orientieren sich beide Regularien sehr stark an internationalen Standards. Insofern thematisieren ITSiG

und EU-DSGVO für die Gefahrenabwehr auch identische vier IT-Handlungsfelder, die funktional abgedeckt werden müssen: „***Risikomanagement***“, „***Sicherheitsmittel***“, „***Betroffenenrechte***“ und „***Gefahrenabwehr***“.

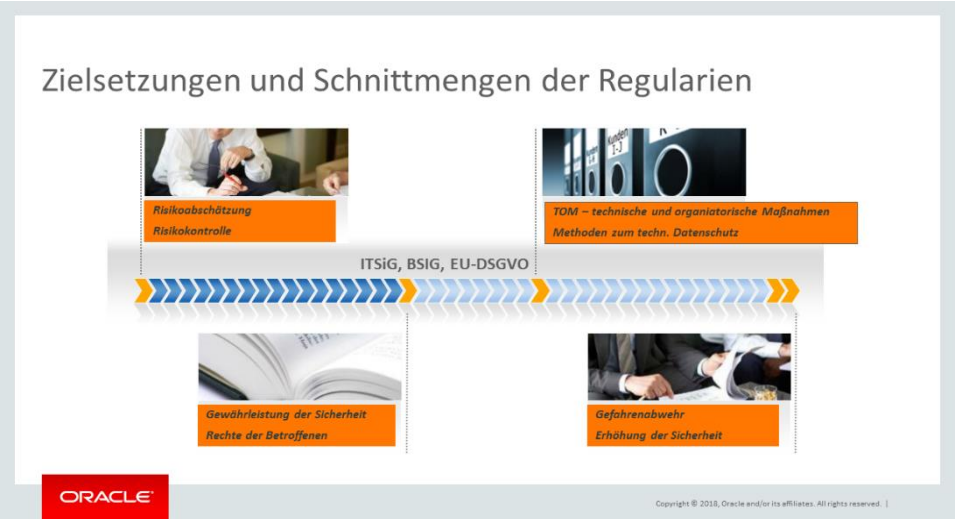

Abbildung „IT-Handlungsfelder zur Gefahrenabwehr“

Gefahrenabwehr gemäß dem „Stand der Technik“

In den Regularien wird auf das ***Auswahlkriterium*** „*gemäß dem Stand der Technik*“, für den Einsatz spezifischer technischer Mittel zur Gefahrenabwehr, Bezug genommen. Die Regularien halten die Beschreibung des Auswahlkriteriums, was „*Stand der Technik“* sei, aber absichtlich sehr vage. Das überrascht auf den ersten Blick. IT Pflichtenhefte tendieren normalerweise dazu ein geradezu akribisches Ausmaß an Detailliertheit zu entwickeln.

Unter praktischen Gesichtspunkten ist dieses Offenhalten der Technikmittel jedoch gut nachvollziehbar. Aufgrund des spezifischen historischen Aufwuchses in den IT Infrastrukturen der Unternehmen muss von Fall zu Fall entschieden werden, welche Sicherheitsfunktionen jeweilig zu kombinieren sind. Die Funktionen können dann im Detail variieren, aber sie müssen qualitativ dem jeweiligen „*Stand der Technik*“ entsprechen.

„Stand der Technik“ sagt aus, dass aufgrund weltweiter aktueller Erfahrungswerte mit den jeweilig ausgewählten Funktionen das angestrebte Sicherheitsniveau zu erreichen ist. Gemäß Vorschlägen des Bundesverbandes IT-Sicherheit e.V. ist „*Stand der Technik*“ als eine Mittelkategorie im Maßstab der Sicherheitserwartung zu verstehen. Ein nächst-schwächeres Niveau wird als „*allgemein anerkannte Regeln der Technik*“ definiert, ein nächst-höheres Niveau an Sicherheit wird als „*Stand von Wissenschaft und Forschung*“ kategorisiert.[1]

[1] *TeleTrustT*, https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

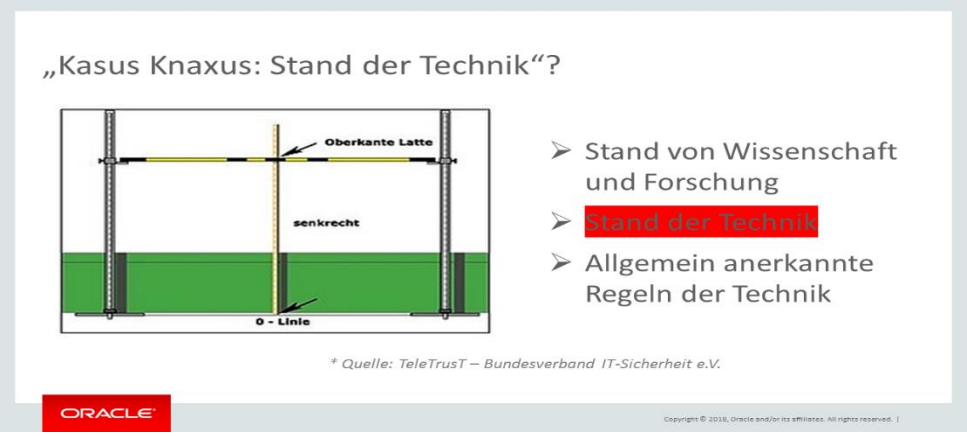

Abbildung „Kategorisierung von Sicherheit“

Bezugnahme auf den „Stand der Technik“ in der EU-DSGVO

Im juristischen Kontext der EU-DSGVO verweist der Artikel 25[2], zusammen mit dem Erwägungsgrund 78, dediziert auf das Kriterium „*Stand der Technik*“. Die Auswahlentscheidung für die einzusetzenden technischen und organisatorischen Mittel, gemäß dem „*Stand der Technik*“, hat demgemäß der „Verantwortliche im Sinne der Verordnung“ zu treffen. Die ***Geeignetheit der Sicherheitsmittel*** ist das Kriterium dafür, dass den ***Compliance Anforderungen der Verordnung***, hinsichtlich der Verarbeitung der personenbezogenen Daten, im Kontext der EU-DSGVO, entsprochen werden kann.

Auch der Artikel 32[3] und Erwägungsgrund 83 der DS-GVO verweisen auf dieses Qualitätskriterium des Mitteleinsatzes. Absatz 1d in Artikel 32 geht sogar insofern darüber hinaus, als zusätzlich auf die regelmäßig zu erfolgende Überprüfung, Bewertung und Evaluierung der Wirksamkeit der eingesetzten technischen und organisatorischen Maßnahmen, zur Gewährleistung der Sicherheit der Verarbeitung, hingewiesen wird.

Diese wiederkehrende und systematische ***Eignungsverifizierung*** der eingesetzten technischen Mittel im Sicherheitsmanagement war auch Forschungsgegenstand einer GARTNER Untersuchung aus dem Jahr 2017.[4] Das, in der Untersuchung herausgearbeitete, „CARTA“ Verständnis – „*CARTA - Continuous adaptive Risk and Trust Assessment*“ – läßt sich in Summe in etwa folgendermaßen charakterisieren: *„die Strategie des Verteidigungsansatzes muss der kontinuierlichen Risikoanpassung und der kontinuierlichen Prüfung, ob dem technischen Sicherheitssystem noch vertraut werden kann, folgen“*.

„Stand der Technik“ im Kontext eines Regelkreis-Modell

Das Zusammenwirken von Regularien und die Umsetzung durch technische Sicherungsmittel läßt sich als Regelkreis-Modell beschreiben. Insofern „bildet“ sich juristische Diktion, mit dem Einsatz entsprechender Sicherheitsmittel nach dem „*Stand der Technik*“ und, unter Kontrolle eines geeigneten IT-Sicherheitsmanagements, in die Laufzeit- und Überwachungsumgebung der operativen IT ab. Operative Erfahrungswerte und die Auswertung aktueller Angriffsszenarien fliessen dann, in Form neuer Standardisierungen beziehungsweise Benchmark Vorgaben, in den Regelkreis zurück.

---

[2] Artikel 25 „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“
[3] Artikel 32 „Sicherheit der Verarbeitung“
[4] Gartner Analysts Neil MacDonald, Felix Gaehtgens, 22 May 2017, ID G00332400 „Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats”

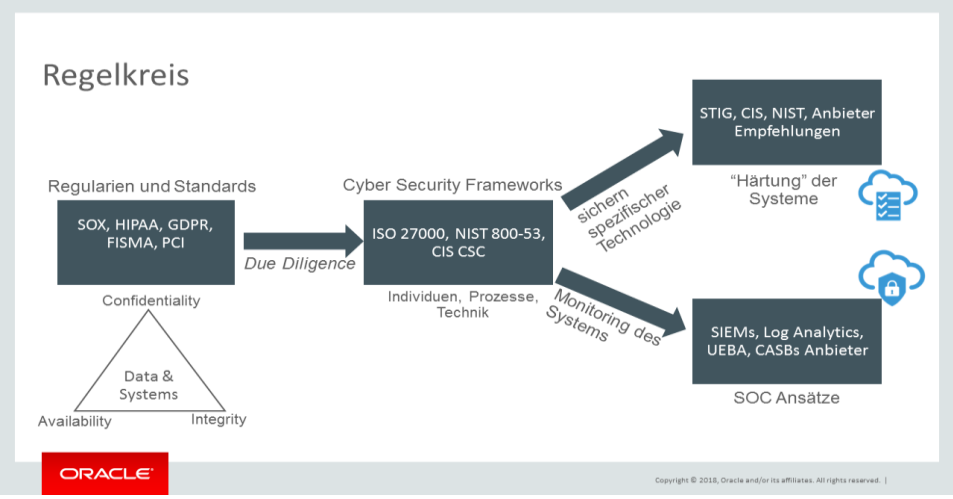

Abbildung „Regelkreis-Modell“

Im Regelkreis ist folgende Linearität wirksam:

a) die jeweiligen Zertifizierungen, Benchmarks und Controls grenzen die jeweiligen technischen Subsysteme ab und beschreiben deren sicherheits-technischen Erwartungshorizont
b) dieser sicherheits-technische Erwartungshorizont drückt sich in konkreten Beschreibungen und Funktionen aus, die den erreichten „*Härtegrad*“ der Systemumgebung beschreiben
c) der sicherheits-technische Erwartungshorizont wird in eine IT-Sicherheits-Managementumgebung abgebildet und wertet in Echtzeit sicherheits-relevante Systemaktiväten aus, beziehungsweise deckt Anomalien im Laufzeitsystem auf
d) auf sicherheits-relevante Anomalien wird manuell, teil-automatisiert oder sogar weitgehend autonom seitens des Systems reagiert

In die Funktionsbereiche c) und d) finden neuerdings verstärkt „***Machine Learning Eigenschaften***“ Eingang, um komplexes Systemverhalten, im sicherheitsrelevanten Kontext, „intelligent“ zu machen, also auch Sicherheit wo möglich zu „***autonomisieren***“.

Insofern wird damit jetzt auch „***Künstliche Intelligenz*** und Machine Learning“ als wesentlicher Teil der Funktionserbringung, zur Erreichung der Schutzziele, gemäß dem „Stand der Technik“, verstanden:

- zur Verhinderung von Angriffen unmittelbar auf die ***Dateninhalte***
- zur Verhinderung von Angriffen auf die ***Verfügbarkeit*** der jeweiligen Dienste und Daten
- zur Verhinderung unberechtigter ***Manipulationen*** der Betriebs- und Anwendungssysteme.

„Autonomie“ im Kontext von Regularien, Regeln, KI und Machine Learning

Zum Kontext der einzusetzenden Schutzmaßnahmen im IT-System gehört maßgeblich auch die Erkennung von Angriffen.

Die ***Angriffserkennung***, deren Evolution in „sich autonom verhaltende Systeme“ mündet, setzt das Zusammenspiel von (standardisierten) ***Regelwerken*** und deren „*intelligenter und lernender*“ ***Regelanwendung***, im Funktionskontext eines Security Operation Centers (SOC), voraus.

Die Konzeption des SOC ist dabei einem „***Informationssicherheits-Managementsystem***“ (ISMS) gleichzusetzen und stellt die Basis für die Regelanwendung her. Es ist orientiert an ***Normierungsvorgaben*** wie zum Beispiel ISO/IEC 27001.

Oracle spricht gegenwärtig von drei Funktionsbereichen, in denen sich ***Autonomie*** manifestieren kann: „***Self Driving***“, „***Self Securing***“ und „***Self Repairing***“.

„*Self Securing*“ berücksichtigt dabei insbesondere auch die beiden Unterkategorien ***„externe Attacken“*** und ***„interne Angriffe“***.

Auf dem Weg zu autonomem Systemverhalten stellen Regelwerke die „Operationalisierungen“ gesetzlicher Vorgaben dar. Über solche technisierten Regeln werden die vorgegebenen Schutz- und Sicherheitsziele quasi in die „IT technische Verarbeitbarkeit“ gebracht.[5] *„Regelwerke können somit als die Playbooks für die Good Guys verstanden werden. Sie sind niedergeschriebene und formalisierte Erfahrungswerte, auf Basis derer die Angriffe von „Bad Guys“ auf die IT Systeme abgewehrt werden können*“.

Die technische Umsetzung und Implementierung der Regeln wird als „***Härtung der IT-Systeme***“ deklariert.

Wenn sich bestimmte sicherheitskritische Eigenschaften dann, in komplexen IT-Laufzeitsystemen, „*aus sich selbst heraus auch noch verbessern lassen können*“, spricht man von „*Künstlicher Intelligenz*“ auf Basis von „*Machine Learning*“.

Das „intelligente und zielgerichtete Lernen“, auf eine bestimmte Zielerreichung oder Regelentsprechung hin, stellt eine wesentliche Voraussetzung für Systeme dar, die „autonom handeln“ sollen.

„Stand der Technik“ im Oracle Verständnis

Generell läßt sich Sicherheit in a) ***statische Mittel*** zur Herstellung von Sicherheit in der Laufzeitumgebung und b) ***dynamische Reaktionen*** auf sicherheitsrelevante Vorkommnisse, im Zuge des Betriebes, unterschieden. Für die statische Sicherheit setzt Oracle auf Funktionen folgender Teilbereiche:

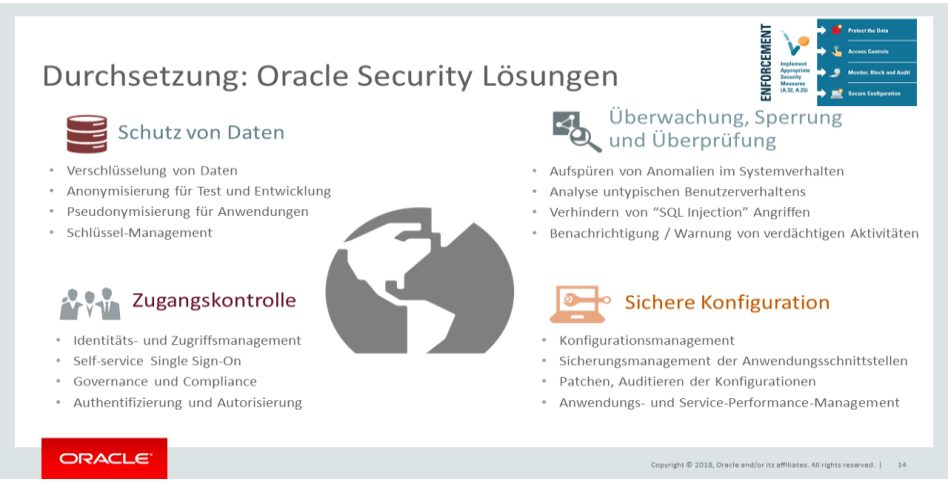

Abbildung „Oracle Security Lösungen“

Statische Sicherheitsmittel und organisatorische Maßnahmen stellen allgemein die Grundlage der Gefahrenabwehr dar und erhöhen die Systemsicherheit. Die vier in der Abbildung aufgeführten

[5] *CIS / Center for Internet Security, “CIS Controls”* https://www.cisecurity.org/controls/, *“CIS Benchmarks”* https://www.cisecurity.org/cis-benchmarks/

Funktionsbereiche ergänzen sich und sind aufeinander abgestimmt. Sie zielen auf die Bereiche „***Datensicherheit***“, „***Zugriffssicherheit***“, die „***Absicherung von Schnittstellen*** und ***Zugriffskanälen***“ und „***Sicherheit in der Infrastruktur***“.

Im Rahmen seines SOC Ansatzes bietet Oracle dafür ein ganzes Bündel von Funktionen an.

In seinem Kern definiert sich das SOC durch Konzepte gemäß ***SIEM*** (Security Information and Event Management) und ***UEBA*** (User and Entity Behavior Analytics).

UEBA kann dabei als ein Typus eines „*Machine Learning Modells*“ verstanden werden. Über das Aufdecken von ***Sicherheitsanomalien*** hilft das Modell Cyber Attacken zu identifizieren. Dazu müssen alle sicherheits-relevanten Daten gewisserweise standardisiert, also vergleichbar und aufeinander beziehbar gemacht werden. Das betrifft sehr große Datenmengen, u.a. auf Basis von Konfigurations-, Log- und Laufzeit-Parametern. Auf Basis dieser Daten „*lernt*“ das System sozusagen, „*normales Verhalten*“ von Abweichungen zu unterscheiden und diese „Anomalien“ zu identifizieren und aufzudecken.

In Ergänzung zu UEBA ist SIEM ein Ansatz eines Sicherheits-Managements, der darauf abzielt, eine ganzheitliche Sicht auf die Sicherheit der Informationstechnologie (IT) einer Organisation zu entwickeln.

Das SOC ist von seinem Ansatz her „*räumlich*“ zu verstehen. „*Moderne Angriffsvektoren*“ setzen nicht mehr nur eindimensional an, sondern versuchen Schwachstellen im IT System parallel anzugreifen. In Übereinstimmung mit dem UEBA Konzept werden deshalb auch nicht nur alle klassischen Benutzer, sondern alle „Entitäten“ eines Systems entsprechend überwacht. Entitäten sind so z.B. auch sogenannte „*managed or unmanaged endpoints*“ oder Anwendungen.

Auf welche Überwachungskategorien zielt der SOC Ansatz?

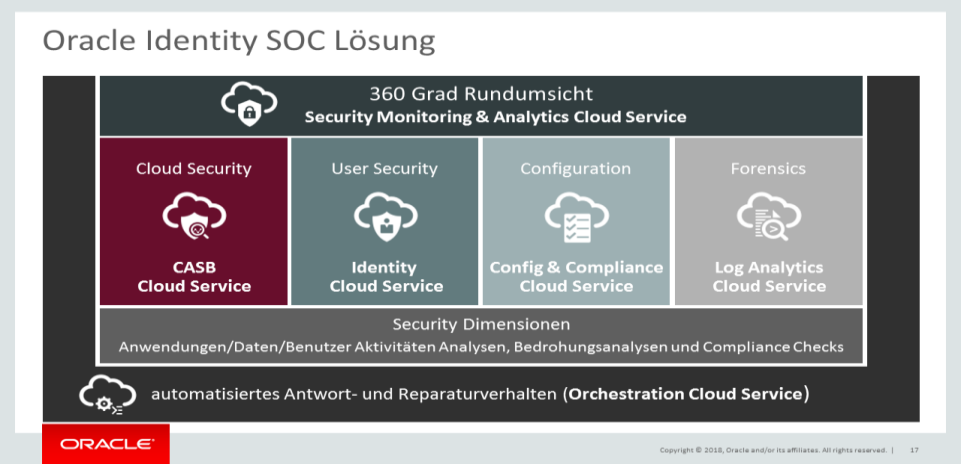

Abbildung „Oracle Identity SOC Lösung“

Da ist einmal das Phänomen sogenannter „***Shadow IT***“, also bestimmer Datenverarbeitungen, die an der Zentral-IT „*vorbeilaufen*“. Durch die zunehmende Inanspruchnahme von CLOUD Angeboten zeigt sich in den Unternehmen ein ähnliches Phänomen, wie zu Ablösungszeiten der Mainframe-Technologien durch die Client-Server Abteilungsrechner. Nachdem, aus Sicht der Abteilungen, die zentrale IT in der Umsetzung der Anforderungen als zu langsam wahrgenommen wurde, haben sich

viele Abteilungen mit dezentraler IT mehr oder weniger verselbständigt. Das führte zwar zur Erhöhung der Effizienz in den Abteilungen, lies aber zugleich den Aufwand an Integration exponenziell ansteigen.

„*Shadow IT*“ ist insofern gefährlich, als einerseits Daten unkontrolliert abwandern können und andererseits die Einfallstore in die eigene IT nicht ausreichend abgesichert sind. Um das zu verhindern hat sich eine Technologie etabliert, die als „***Cloud Access Security Broker***“ (CASB) bezeichnet wird. CASB überwacht und reagiert unter anderem auf sogenannte unerwünschte und wahrscheinlich auch unerlaubte „***Datenabflüsse***“ (DLP´s, Data Leakage Protection).

Die zweite Überwachungskategorie des SOC richtet sich auf die „***Identity Governance***“. Identity Cloud Service konsolidiert und überwacht, im Sinne von UEBA, die Benutzer und Entitäten des gesamten IT-Environment. Das spielt zusammen mit den Entitäten, die auf Basis der Konfigurationsdateien überwacht werden. Das ist unabdingbar weil es sich gezeigt hat dass, über das „*Verbiegen von Konfigurationsdateien*“, Systeme extrem verwundbar werden. Das wird neuerdings als „***Configuration Drift***“ bezeichnet.

Mit ***Forensics*** wird eine Kategorie umschrieben, die auf die weiterverfolgende Analyse, insbesondere nach Fehlervorkommnissen im weitesten Sinne, zielt. Durch das Zentralisieren der sicherheits-relevanten Daten und die Auswertung und Analyse dieser Daten nach dem SIEM Prinzip, kann dann zugleich, durch die automatisierte Erstellung von Berichten, der Compliance entsprochen werden.

Fazit

Es sollte deutlich geworden sein, dass sich der Begriffskontext von „*Stand der Technik*“ nicht nur auf die Bestimmung spezifischer Qualitäten, im Kontext technischer Sicherungsmittel, bezieht. „*Stand der Technik*“ umfasst zugleich einen Vorgehensvorschlag, um Systeme im sicherheitskritischen Bereich, auf eine systematische Art und Weise, aufgrund gesteigerter Bedrohungsszenarien, noch effizienter abzusichern.

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