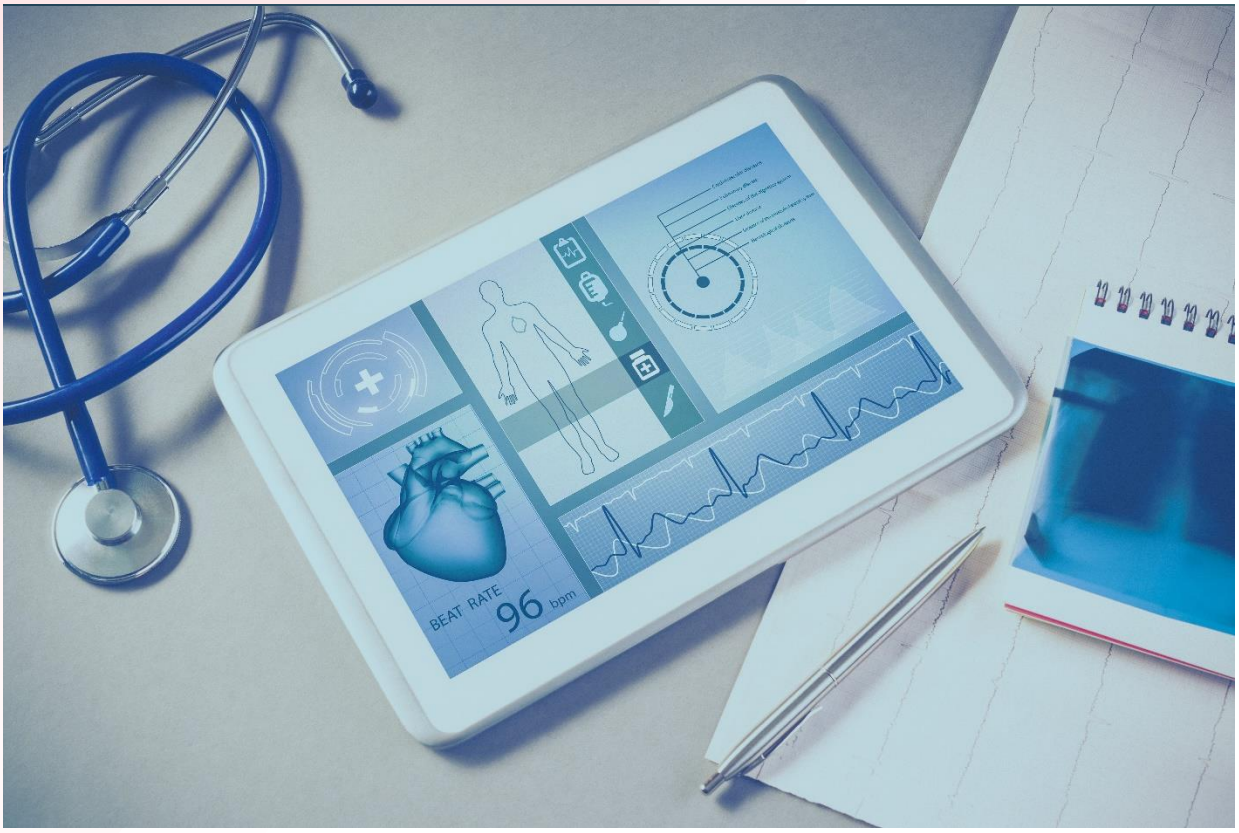

Sicherheitsrichtlinien im Gesundheitswesen… so unterstützen die Oracle Security Features

AUSGANGSLAGE

In Kürze

Neben den klassischen ISO27001 Zertifizierungen existiert seit Juli 2015 das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). Damit leistet die Bundesregierung einen wichtigen Beitrag dazu, die IT-Systeme und digitalen Infrastrukturen Deutschlands abzusichern (siehe Quelle 9). Insbesondere im Bereich der Kritischen Infrastrukturen (KRITIS) - wie etwa Strom- und Wasserversorgung, Finanzen, Ernährung aber auch das Gesundheitswesen - hätte ein Ausfall dramatische Folgen für die deutsche Gesellschaft. Dies war der Grund warum mit Wirkung zum 30.6.2017 unter anderem die Ergänzung der KRITIS Infrastrukturen um den Sektor Gesundheitswesen erfolgte.

Die Datenschutzbeauftragten der Länder haben für das deutsche Gesundheitswesen eine **Orientierungshilfe** für die Umsetzung existierender Sicherheitsrichtlinien erarbeiten lassen. Ergänzend hat sich auch die Deutsche Krankenhausgesellschaft (DKG) speziell dieser Thematik angenommen und Empfehlungen sowie Umsetzungshinweise für Krankenhäuser erstellt (siehe Quelle 10 + 11).

Die IT-Verantwortlichen und das Management von Krankenhäusern sind dadurch aufgefordert, über eine Umsetzung nachzudenken und Entscheidungen vorzubereiten.

In der Regel ist für die Nutzung der Security-Features bei der Erstellung einer Anwendung der jeweilige Software-Hersteller zuständig. Aufgabe des Kunden oder des Hosters ist üblicherweise die Organisation während des Betriebs. Dabei kommen Security-Features zum Einsatz. **Oracle bietet Security-Features an, die von Entwicklern und deren Kunden genutzt werden können, um die Anforderungen aus der Orientierungshilfe zu erfüllen.**

Die Anwendungsentwickler und insbesondere die Betreiber müssen die Anforderungen umsetzen. Die kürzlich erfolgte Ausschreibung des Bundeswehrkrankenhauses (siehe Quelle 2) ist sicherlich das deutlichste Signal hierfür. Der Landesbeauftragte für Datenschutz Rheinland-Pfalz machte in seinem Vortrag (siehe Quelle 6) die Aussage: „Bei Defiziten in der Verantwortung der KIS-Herstellers muss von einem angemessenen Übergangszeitraum für seitens der Hersteller erforderliche Anpassungen ausgegangen werden“. Diese Aussage bedeutet letztlich, dass Software-Hersteller oder die Betreiber in jedem Falle Security-Features einsetzen müssen, auch wenn es eine zeitliche Verzögerung für die Umsetzung geben sollte. Der Einsatz der Technologien von Oracle kann einen zeitlichen Vorteil für die Umsetzung bedeuten.

MAPPING SECURITY FEATURES

Allgemeine Forderung der Orientierungshilfe (s. Quellen)	**Oracle Produkt, Option oder Feature**
Gefordert ist: „... eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren ...“ Stand ist: „...ein Teil der ... angebotenen Lösungen bleibt ... in technischer Hinsicht gegenwärtig noch hinter den hier dargelegten Anforderungen zurück.“	Die Summe der Oracle Produkte, Optionen und Features bzgl. Security ermöglichen grundsätzlich die Einhaltung sämtlicher datenschutzrechtlicher Forderungen für den Bereich der Datenbank. Oracle Security Optionen werden unseres Wissens nach selten im KIS-Umfeld eingesetzt.

KONKRETES MAPPING SECURITY FEATURES

Forderung der Orientierungshilfe (s. Quellen)	**Oracle Produkt, Option oder Feature**
Datenaustausch in Verbindung mit externen Dienstleistern muss eine **Transport-Verschlüsselung** beinhalten.	**Oracle Datenbank (ODB)** kann transparent (d.h. ohne Änderung in der Anwendung) die Verschlüsselung jeglichen Netzverkehrs von und zur Datenbank eines Dienstleisters übernehmen.
Verschlüsselung der Daten in einer Datenbank (Encryption @Rest) u.a. der BSI Grundschutz sieht für besonders sensible Daten, wozu Patienten und Gesundheitsdaten ja zweifelsohne gehören) eine Verschlüsselung bei der Speicherung der Daten in einer Datenbank vor. (siehe Quelle 12 Kapitel APP.4.3.A24)	**Oracle Advanced Security Option (OAS)** verschlüsselt die Datenbestände in einer Oracle Datenbank hochperformant und transparent und ohne, dass eine Anwendung geändert werden muss bzw. diese Verschlüsselung vorsehen muss. Als Nebeneffekt werden dabei auch alle Backups und Datenexporte aus einer Datenbank verschlüsselt.
• Die **Zugriffsrechte und Eingriffsebenen der Administratoren** sind entsprechend ihren spezifischen Aufgaben zu begrenzen. Die Aktivitäten der Administratoren sind revisionsfest zu protokollieren. • Bei einer (Fern-)Wartung durch Dritte/Externe sind besondere Maßnahmen erforderlich, damit die Wartung **nur mit Wissen und Wollen** des Krankenhauses im zugelassenen Umfang stattfinden kann.	**Oracle Database Vault (ODV)** erlaubt die Zugriffsrechte für alle Benutzer bzw. Benutzergruppen inkl. Datenbankadministratoren genau zu steuern und bietet somit einen wirksamen Schutz um Dritte/Externe davon abzuhalten auf sensible Daten zuzugreifen. Mit **Oracle Audit Vault and Database Firewall (OAV)** können alle Zugriffe revisionssicher protokolliert und auswertbar zur Verfügung gestellt werden.
• „... für eine datenschutzgerechte Gestaltung einer angemessenen **Nachvollziehbarkeit der Verarbeitung** personenbezogener Daten.“ ... muss gesorgt werden. • „... muss sich ... bestimmen lassen, wer Daten wann erstellt und wer Daten wann wie modifiziert hat.“	Mit **Oracle Audit Vault and Database Firewall (OAV)** können alle Zugriffe revisionssicher protokolliert und auswertbar gemacht werden.
Personenbezogene Daten müssen **anonymisiert, pseudonymisiert** bzw. mit einem Alias versehen werden.	In Test- und Entwicklungsumgebungen kann **Oracle Data Masking (ODM**) das leisten.

Verschlüsselte Backups aus Sicherheitsgründen.	**Oracle Advanced Security Option (OAS)** verschlüsselt neben den eigentlichen Datenbeständen in einer Oracle Datenbank auch Backups und Datenexporte aus einer Datenbank. Falls OAS nicht eingesetzt werden soll, können Backups auch mit **Oracle Secure Backup (OSB)** verschlüsselt werden.
Für die gemeinsame Speicherung der Daten unterschiedlicher Krankenhäuser in einem KIS (z.B. in einem Klinikverbund), müssen sicherheitstechnische Mechanismen zur **Trennung der Daten** vorgesehen werden **(Mandantenfähigkeit).**	Je nach Szenario können **Oracle Virtual Private Database (VPD)** oder **Oracle Database Vault (ODV)** diese Aufgabe übernehmen. Der Einsatz von VPD setzt die EE voraus und bedeutet i.d.R. eine Einbindung der KIS-Entwicklung. Auch ODV setzt die EE voraus sowie die Lizenzierung der Option ODV.
Daten, die im Sinne der Patientenbehandlung erstellt werden, dürfen zum Zwecke von allgemeinen Auswertungen oder zur Aus- oder Fortbildung nur genutzt werden, wenn die Patienten **nicht identifizierbar** sind.	**Oracle Data Masking (ODM)** Oracle Label Security (OLS) Oracle Database Vault (ODV)
In das KIS sollte ein **Single-Sign-On-Dienst** integrierbar sein.	Sign-On möglich, z.B. mit **Oracle Access Manager (OAM)** bzw. **Oracle Identity Manager (OIM).**

FAZIT

Anwendungsentwickler und insbesondere die Betreiber müssen die Anforderungen umsetzen. Die kürzlich erfolgte Ausschreibung des Bundeswehrkrankenhauses (siehe Quelle 2) ist sicherlich das deutlichste Signal hierfür. Der Landesbeauftragte für Datenschutz Rheinland-Pfalz machte in seinem Vortrag (siehe Quelle 6) die Aussage: „Bei Defiziten in der Verantwortung der KIS-Herstellers muss von einem angemessenen Übergangszeitraum für seitens der Hersteller erforderliche Anpassungen ausgegangen werden“. Diese Aussage bedeutet letztlich, dass Software-Hersteller oder die Betreiber in jedem Falle Security-Features einsetzen müssen, auch wenn es eine zeitliche Verzögerung für die Umsetzung geben sollte. Der Einsatz der Technologien von Oracle kann einen zeitlichen Vorteil für die Umsetzung bedeuten.

AUSBLICK AUF KÜNFTIGE BETRACHTUNGEN

Wenn die oben aufgeführten, „offensichtlichen“ Punkte erfüllt sind, gibt es darüber hinaus weitere Möglichkeiten, in diesem Umfeld mit Oracle Security Features erfolgreich zu werden.

Weitere Forderungen ... „zwischen den Zeilen“ (s. Quellen)	**Oracle Produkt, Option oder Feature**
Sehr gute Kenntnisse der IT-Sicherheitsmechanismen in gängigen Softwareprodukten (Betriebssysteme, Datenbanken,) sowie TCP/IP-basierenden Netzen, durch alle Beteiligte, d.h. sowohl Administratoren als auch Entwickler. Endbenutzer müssen ebenfalls sicherheitstechnisch geschult werden.	Schulung / Ausbildung / Dienstleistung, aber auch der komplette Lizenz-Stack der Security Features von Oracle: **Access Management:** - Oracle Access Manager (OAM) - Oracle Adaptive Access Manager (OAAM) - Oracle Entitlements Server (OES) - Oracle Enterprise Single Sign-On (OeSSO) Plus - Oracle Mobile and Social Services …

	Directory Services: - Oracle Unified Directory (OUD) - Oracle Directory Services Enterprise Edition (ODSEE) - Oracle Virtual Directory (OVD) - Oracle Internet Directory (OID) … **Identity Governance:** - Oracle Identity Manager (OIM) - Oracle Privileged Account Manager (OPAM) … **Cloud Security Services:** - Oracle Identity Cloud Service - Cloud Security Access Broker (CASB) - Oracle Identity & Log Analytics (OIA) - Oracle Platform Security Services (OPSS) … **Oracle Database (ODB):** - Netzwerkverschlüsselung - Oracle Total Recall/Flashback Data Archive (OTR) - Oracle Virtual Private Database (VPD) … **Oracle Datenbank Optionen:** - Oracle Advanced Security (OAS) - Oracle Database Vault (ODV) - Oracle Label Security (OLS) - Oracle Data Masking (ODM) - Oracle Audit Vault and Database Firewall (OAV) … **Oracle Secure Backup** (OSB) **DBSAT** (Database Security Assesment Tool) **Oracle Enterprise Manager (OEM)** - Oracle Tuning & Diagnostic Pack - Lifecycle Management Pack…

• Ergänzende Mitbehandlung durch andere Organisationseinheiten (so genannter Konsiliardienst) muss sicherheitstechnisch geregelt werden.	Oracle Label Security (OLS)
• Belegärzte erhalten nur Zugriff auf die Daten ihrer Patienten. • Mitarbeiter fachrichtungsübergreifender Funktion (z.B. Anästhesie, Physiotherapie, OP, Diagnostik, Pathologie, Labor) muss sicherheitstechnisch geregelt werden.	Oracle Label Security (OLS) Oracle Virtual Private Database (VPD)
Für den Zugriff auf medizinische Daten ist ein Rollen- und Benutzerkonzept einzusetzen, das sich an den jeweiligen	Oracle Database (ODB) Oracle Virtual Private Database (VPD) Oracle Access Manager (OAM)

persönlichen Aufgaben der Mitarbeiter orientiert.	Oracle Identity Manager (OIM)
Daten von Patienten die • Mitarbeiter des behandelnden Krankenhauses, • bekannte Personen des öffentlichen Lebens, • Personen mit besonderer Gefährdung etc. sind, benötigen im Rollen- und Berechtigungskonzept besondere Zugriffsregelungen.	Oracle Database Vault (ODV) Oracle Label Security (OLS) Oracle Audit Vault and Database Firewall (OAV)

QUELLEN

1. Entschließung der Konferenz der DSB Bund / Länder vom 16./17. März 2011
http://www.baden-wuerttemberg.datenschutz.de/lfd/konf/2011/03_16_1.htm

2.Ausschreibung Bundeswehrkrankenhaus:
Konzeption der IT-Sicherheit für das Projekt KIS (Krankenhausinformationssystem)
http://www.bund.de/IMPORTE/Ausschreibungen/EDITOR/Bundesamt-fuer-Informationsmanagement-und-Informationstechnik-der-Bundeswehr/2011/04/231985.html

3.Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
http://www.bfdi.bund.de

4.Die Landesbeauftragten für den Datenschutz
http://www.baden-wuerttemberg.datenschutz.de/links/beauftragte.html

5.Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Schutz des Patientengeheimnisses
https://www.datenschutzzentrum.de/material/tb/tb33/kap04_6.htm

6.Infoveranstaltung Landesbeauftragter für Datenschutz Rheinland-Pfalz: Datenschutz im Krankenhaus
http://www.datenschutz.rlp.de/de/aktuell/2011/images/20110609_kis/07_-_Heusel-Weiss_-_OH_KIS_2011-Juni.pdf

7.Berliner Beauftragter für Datenschutz und Informationsfreiheit: Konferenz der Datenschutzbeauftragten
http://www.datenschutz-berlin.de/content/deutschland/konferenz

8.Orientierungshilfe Krankenhausinformationssysteme der Bundes- und Landesdatenschutzbeauftragten
http://www.datenschutz-berlin.de/attachments/771/Orientierungshilfe_Krankenhausinformationssysteme.pdf?1307102606

9.IT-Sicherheitsgesetz
https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/it_sig_node.html

10.IT-Sicherheitsgesetz: Schutz Kritischer Infrastrukturen, 1. Änderungsverordnung zur BSI-KritisV ("Korb 2")
https://www.dkgev.de/dkg.php/cat/283/aid/31971/title/IT-Sicherheitsgesetz%3A_Schutz_Kritischer_Infrastrukturen_-_Umsetzungshinweise_der_DKG

11.IT-Sicherheitsgesetz: Schutz Kritischer Infrastrukturen - Umsetzungshinweise der DKG
https://www.dkgev.de/media/file/70091.ITSiG_Kritis_Umsetzungshinweise_BSIG_v0.9.pdf

12.BSI IT Grundschutz Kompendium relationale Datenbanken
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_4_3_Relationale_Datenbanksysteme.html

ORACLE

ORACLE Deutschland B.V. & Co. KG
Riesstraße 25
D-80992 München

Telefon: 0800 1 824145
Fax: 0180-2-ORAFAX

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Titel: Orientierunghilfe - Sicherheitsrichtlinien im Gesundheitswesen… so unterstützen die Oracle Security Features

Juni 2018

Oracle is committed to developing practices and products that help protect the environment