eHealth: Nicht auf Kosten der Patientensicherheit

München, 19.11.2019: Bei der digitalen Gesundheit hinkt Deutschland im internationalen Vergleich gehörig hinterher. Laut einer Bertelsmann-Studie sind wir Vorletzter, nur Polen digitalisiert noch langsamer[1]. Experten führen verschiedene Gründe an. Unter anderem mangle es an einer sicheren Infrastruktur, die den rechtlichen Anforderungen gerecht wird.

Wenn von Digitalisierung und eHealth die Rede ist, geht es um mehr als die elektronische Patientenakte (ePA): Dienstleister mit digitalen Gesundheitsangeboten drängen auf den Markt; längst erleichtern Fitnesstracker und Smartwatches den Alltag vieler Deutscher. Die dazugehörigen Health-Apps erheben und verwerten sensible Daten, häufig mit Personenbezug. Bei der Umsetzung der gesetzlichen Datenschutzrichtlinien tun sich viele Anbieter jedoch noch schwer. Und mit dem Patientendaten-Implantationsregister steht bereits das nächste Mammutprojekt in den Startlöchern, bei dem Datenschutz-Probleme vorprogrammiert sein dürften[2].

Datenschutz durch Technik?

Während Ärzte und Apotheker der Schweigepflicht nach §203 StGB unterliegen, gelten für App-Anbieter, Dienstleister und Server-Betreiber meist andere Regeln. Selbstverständlich gibt es strenge Gesetze und Anforderungen für den Umgang mit personenbezogenen Daten, die vor allem in der EU-Datenschutzgrundverordnung (DSGVO) und im Bundesdatenschutzgesetz (BDSG-neu) geregelt sind. Diese erweisen sich in der Praxis allerdings häufig als wirkungslos, weil etwa organisatorische Schutzmaßnahmen (vgl. Art. 32 DSGVO) wie Rechte- und Rollenkonzepte relativ einfach umgangen werden können. Administratoren können sich in der Regel privilegierten Zugriff zu den Servern verschaffen und vertrauliche Daten einsehen, manipulieren oder entwenden. Bereits eine mögliche Kenntnisnahme sensibler Informationen stellt einen Verstoß gegen die Schweigepflicht dar und muss daher von vornherein ausgeschlossen sein.

Patientensicherheit durch IT-Sicherheit

Um personenbezogene Daten wie Patientendaten vor Kenntnisnahme, Manipulation oder Verlust zu schützen, braucht es eine rein technische, manipulationssichere und präventive Lösung, die jeglichen – auch privilegierten – Zugriff zuverlässig unterbindet. Zahlreiche Public-Cloud-Angebote und sogar viele Business Clouds tun sich damit jedoch schwer. Denn die meisten Server-Infrastrukturen sehen privilegierte Admin-Zugänge vor, beispielsweise zu Wartungs- oder Monitoring-Zwecken.

Einen anderen Ansatz verfolgen versiegelte Infrastrukturen[3]: Hier wurden die organisatorischen Schutzmaßnahmen vollständig durch technische Maßnahmen ersetzt, die sich auch mit hohem Aufwand nicht umgehen lassen. Die Server sind hermetisch abgeriegelt, ein privilegierter Admin-Zugriff ist nicht vorgesehen – eine Kenntnisnahme vertraulicher Daten ist ebenso ausgeschlossen wie Diebstahl und Manipulation. Das gilt nicht nur für Administratoren, sondern für alle externen und internen Angreifer.

---

[1] https://www.bertelsmann-stiftung.de/de/themen/aktuelle-meldungen/2018/november/digitale-gesundheit-deutschland-hinkt-hinterher/

[2] https://www.heise.de/tp/features/Der-fleissige-Herr-Spahn-Mit-Vollgas-gegen-den-Datenschutz-4556149.html

[3] https://de.wikipedia.org/wiki/Sealed_Cloud

„Gesundheitsminister Spahn fordert mehr Patientensicherheit. Langfristig werden wir diese nur durch bessere IT-Sicherheit realisieren können – und dazu muss sich IT-Sicherheit wie auch vom Gesetzgeber gefordert am Stand der Technik orientieren“, sagt Dr. Hubert Jäger, Datenschutz-Experte und CTO der Münchner TÜV SÜD-Tochter uniscon GmbH.

Als Beispiele für versiegelte Infrastrukturen nennt Jäger unter anderem die Versiegelte Cloud der Deutschen Telekom, die ucloud des Aachener TK-Providers regio iT sowie idgard® und die sealed platform der uniscon, eine hochsichere Cloud-Plattform, auf der sich schützenswerte Anwendungen rechtssicher und datenschutzkonform betreiben lassen.

Weiterführende Informationen zur sealed platform sowie druckfähiges Bildmaterial erhalten Sie auf Anfrage bei presse@uniscon.de.

uniscon – ein Unternehmen der TÜV SÜD Gruppe

Die uniscon GmbH ist ein Unternehmen der TÜV SÜD Gruppe. Als Teil der Digitalisierungsstrategie von TÜV SÜD bietet uniscon hochsichere Cloud-Anwendungen und Lösungen für sicheren und gesetzeskonformen Datenverkehr. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund ist uniscon in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zu Partnern und Produkt: www.uniscon.com

Pressekontakt

uniscon GmbH, Claudia Seidl
Ridlerstr. 57
80339 München
E-Mail: presse@uniscon.de
Internet: www.uniscon.com
Telefon: 089 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Julia Fehrle
Auf der Eierwiese 1
82031 Grünwald
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20