Resilienz

Datensicherheitssysteme im Gesundheitswesen

Notwendige Maßnahmen zur Erreichung der Belastbarkeit bzw. Resilienz von Datenverarbeitungssystemen

Der vom lateinischen „resilire" („zurückspringen" bzw. „abprallen") abgeleitete Begriff Resilienz wird in den verschiedenen Wissenschaftsbereichen zur Darstellung und Beschreibung der Widerstandsfähigkeit und Belastbarkeit von Menschen, Unternehmen, Materialien, sowie politischen, wirtschaftlichen, rechtlichen und technischen Systemen verwendet.

Mit der seit 25.05.2018 EU-weit für die Verarbeitung von personenbezogenen Daten geltenden Datenschutzgrundverordnung (DSGVO) hat das Thema Belastbarkeit bzw. Resilienz von Systemen auch Einzug in das Datenschutzrecht gehalten. Artikel 32 DSGVO fordert von denjenigen, die personenbezogene Daten verarbeiten (Verantwortliche und Auftragsverarbeiter), technische und organisatorische Maßnahmen zu ergreifen, die die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der IT-Systeme sicherstellen sollen. Eine Definition des Schutzzieles „Belastbarkeit" enthält DSGVO nicht. Die meisten Auslegungen des Begriffs „Belastbarkeit" gehen in Richtung „Robustheit" und verstehen darunter die Fähigkeit von datenverarbeitenden Systemen, erwartbare Störereignisse zu bewältigen. Der in der englischen Fassung der DSGVO verwendete Begriff „resilience" geht sogar weiter als Belastbarkeit und bedeutet Schutz und Maßnahmen vorzusehen, dass ein System auch in unvorhergesehenen Szenarien seine Funktionsfähigkeit aufrechterhalten kann.

Die Gefahren für die Datensicherheit im Gesundheitsbereich sind mannigfaltig. Hervorzuheben sind Hackerangriffe und der Missbrauch von Patientendaten durch Mitarbeiter der Gesundheitseinrichtung selbst, wie z.B. Veröffentlichung von solchen Daten auf Social Media-Plattformen oder der Verkauf von Patientendaten an Dritte. Datenleaks können aber auch durch veraltete IT-Systeme oder unzureichende technische Schutzsysteme für Daten verursacht werden. Um das Schutzziel Resilienz im Sinne einer Widerstandsfähigkeit zu erreichen, sind aus Sicht des Datenverarbeiters weitgehende Maßnahmen erforderlich. Zu diesen gehören die Einrichtung eines Compliance-Datenschutzsystems, Backup-Systeme, Vorkehrungen für das Krisenmanagement im Schadensfall, die Erstellung von Notfallszenarien, klare Vertretungsregelungen im Bereich IT bis hin zu Doppelbesetzungen von IT-Positionen. Eine empfohlene Maßnahme aus technischer Sicht ist auch, möglichst viele Einzelkomponenten zu verwenden, weil diese nach Ansicht von IT-Experten die Systeme weniger angreifbar macht. Weitere wesentliche Maßnahmen sind Schulungen der Mitarbeiter, Einrichtung von Authentifizierungssystemen (z.B. Zwei-Faktoren-Authentifizierung) und Pseudonymisierung.

Mit all diesen Maßnahmen soll ein möglichst hoher Grad an Datensicherheit erreicht werden. Wenn Patientendaten in die Hände unbefugter Dritter gelangen, kann dies für den Patienten dramatische Konsequenzen haben, die von Erpressung bis hin zu Verlust der beruflichen Existenz reichen können. Daraus können natürlich auch Schadenersatzansprüche des Betroffenen gegen die jeweilige Gesundheitseinrichtung entstehen. Die Diskussion, welche Maßnahmen nun tatsächlich zur Erreichung der Belastbarkeit bzw. Resilienz von Datenverarbeitungssystemen notwendig sind, ist noch nicht beendet, erst die ersten Entscheidungen zu Schadenersatzforderungen nach Störfällen werden mehr Klarheit bringen. Jedenfalls ist es aber für alle im medizinischen Bereich tätigen Personen und Unternehmen angebracht, die bisher getroffenen Maßnahmen zu evaluieren und nötige Verbesserungen und Anpassungen durchzuführen.

Dr. Gerald Ganzger,
Managing Partner bei Lansky, Ganzger + partner