www.medizin-edv.de ISSN 1619-0629 Preis: 12 Euro

Ausgabe 5 / 2019

Krankenhaus-IT JOURNAL

Fakten und Perspektiven der IT im Gesundheitswesen

KI programmiert das „Geschäftsmodell Krankenhaus“ neu

KH-IT-Herbsttagung 2019 skizzierte eHealth-Lösungen für die Praxis

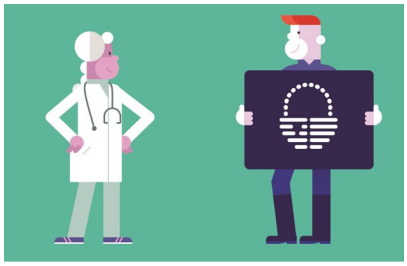
KH IT Bundesverband der Krankenhaus IT-Leiterinnen / Leiter e. V.

ENTSCHEIDERFABRIK

HL7

IHE DEUTSCHLAND Integrating the Healthcare Enterprise

KRITIS, DSGVO, Patientenrechtegesetz: Anforderungen im Krankenhaus umsetzen



Krankenhäuser müssen Verordnungen zum Schutz von Daten und IT-Infrastruktur umsetzen und die Übereinstimmung mit den Vorgaben nachweisen. Dafür benötigen sie Lösungen, die nicht nur Datenabfluss und den Eintrag von Schadcode verhindern, sondern auch die Umsetzung von Richtlinien erfassen und Datenübertragungen dokumentieren. Machtvolle Hilfsmittel dafür sind Lösungen für Data Loss Prevention.

Die Digitalisierung im Gesundheitswesen ermöglicht die Optimierung von Arbeitsabläufen, Diagnostik und Behandlung. Ihre Kehrseite ist die wachsende Anfälligkeit von Daten und Abläufen für Störungen. DSGVO, Patientenrechtegesetz und seit Juli 2019 die KRITIS-Verordnung geben den Rahmen für Maßnahmen vor, die die Risiken des zunehmend vernetzten, datengestützten Arbeitens verringern.

KRITIS-Verordnung

Sie regelt den Schutz der IT-Infrastruktur in den für das Wohlergehen der Bevölkerung wichtigen Branchen. Zu den KRITIS-Unternehmen gehören auch Kliniken und Krankenhäuser mit mehr als 30.000 vollstationären Fällen im Jahr. Sie machen jedoch nur einen Bruchteil der etwa 1.940 Einrichtungen in Deutschland aus. Ende Juni 2019 endete die Übergangsfrist, Maßnahmen zum Schutz ihrer IT-Systeme müssen nun umgesetzt sein.

DSGVO

Sie gilt unabhängig vom Wirtschaftszweig EU-weit für alle Unternehmen und Organisationen und regelt den Schutz von personenbezogenen Daten und von Gesundheitsdaten als besonders schützenswerten Informationen. U. a. muss sichergestellt sein, dass diese Daten nicht unkontrolliert abfließen und so unbefugten Personen nicht zugänglich sind bzw. nicht offengelegt werden.

Patientenrechtegesetz

Seit 2013 zielt es darauf ab, die Position von Patienten gegenüber Ärzten, Krankenhäusern und Krankenkassen u. a. durch Regelungen zur Dokumentation der Behandlung und zum Einsichtsrecht der Patienten in Krankenunterlagen zu stärken. Wann sie welcher Stelle Patientendaten in welcher Form übertragen haben, müssen die Leistungserbringer revisionssicher aufzeichnen und bei Audits nachweisen.

Die Risiken

IT-Infrastrukturen und Daten werden nicht nur durch Angreifer von außen bedroht, sondern auch durch die Beschaffenheit der IT-Infrastruktur und die Mitarbeiter. So haben PCs in Behandlungsräumen frei zugängliche USB Ports, werden vertrauliche Informationen wie Laborergebnisse via Webmailer versendet oder Daten beim Kopieren auf USB-Sticks nicht verschlüsselt.

Schutz durch DLP-Lösung

Für den Schutz sensibler Daten sind Sicherheitsrichtlinien auf Papier nur der erste Schritt. Für Konformität mit den Verordnungen sind technische und organisatorische Maßnahmen (TOM) umzusetzen. Die technische Überwachung von Vorgaben mittels Data Loss Prevention erlaubt die Kontrolle, ob Regeln eingehalten werden, und Reaktionen auf Verstöße. Typische TOM einer DLP Lösung ergänzen einander nahtlos:

- *Eine Daten-Abfluss-Kontrolle prüft bei Datentransfers via E-Mail, Web-Browser oder anderen Online-Diensten die Inhalte der Dateien. Unerwünschte Übertragungen werden unterbunden.*
- *Sensible Inhalte, die sich entgegen der Richtlinien lokal auf Arbeitsplatzrechnern befinden, werden via eDiscovery-Funktion entdeckt.*
- *Device Control-Funktionalität stellt sicher, dass Mitarbeiter ausschließlich firmeneigene USB-Sticks am Arbeitsplatzrechner verwenden. Dies verhindert das Ausschleusen von Daten bzw. das Eindringen von Schadcode über portable Datenträger.*
- *Mittels USB-Stick-Verschlüsselung ist der Schutz der Daten auf den Datenträgern gewährleistet.*

Revisionssichere Erfüllung von Nachweispflichten

Gute DLP-Lösungen protokollieren alle Dateiübertragungen revisionssicher. Auswertungen der Logfiles sind als Reports Grundlage für die Erfüllung von Nachweispflichten bei Audits und gegenüber der Datenschutzbehörde. Bei einem Datenverlust sind Krankenhäuser in der Lage, Verursacher und Umfang des Schadens sowie Austrittspunkte zu ermitteln, die Meldepflichten entsprechend DSGVO zu erfüllen und forensische Untersuchungen zu betreiben.

Fazit

DLP-Lösungen wie Endpoint Protector sind ausgereifte Systeme. Der Einsatz einer einzigen Lösung ermöglicht Kliniken die Umsetzung von TOM zum Schutz aller sensiblen Daten. So werden die Nachweispflichten entsprechend DSGVO, KRITIS, Patientenrechtegesetz und weiteren internationalen Standards erbracht. Es entsteht mehrfacher Nutzen bei einfachen Kosten.

Michael Bauner, Geschäftsführer, Endpoint Protector GmbH