Digitale Transformation (Teil 6)

Informationssicherheit dauerhaft gewährleisten

Wie gelingt es einem Krankenhaus Informationen zu jederzeit sicher zu steuern? Die Antwort ist so simpel wie komplex: Mit einem Informationssicherheitsmanagementsystem (ISMS). Das Beispiel des AWO Psychiatriezentrum Königslutter zeigt, wie die Umsetzung gelingen kann.

Die zentrale Herausforderung der Digitalisierung liegen nicht im Vorhandensein von Tools und Instrumenten, wie einer formulierten IT-Betriebsstrategie zum sicheren Betrieb von Hard- und Software. Vor allem bedingt sie ein Prozess der Bewusstseinsbildung hinsichtlich der damit verbundenen Dekonstruktion etablierter Geschäftsprozesse. Hinsichtlich der Informationssicherheit muss nicht nur mehr investiert, sondern der Managementfokus stärker in den Mittelpunkt rücken. Stichwort ist hier die Einführung von IT-Sicherheitsbeauftragten sowie einer CIO-Position an der Spitze von IT-Bereichen. Über eine so aufgebaute Steuerung sollte in Vereinbarung mit der Datenschutzgrundverordnung (DSGVO) und dem Branchenspezifischen Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (B3S) mit dem Datenschutzbeauftragten (DSB), dem Qualitätsmanagement, dem Risikomanagement und dem Informationssicherheitsbeauftragten (ISB) ein Informationssicherheit-Managementsystem (ISMS) institutionalisiert werden. Dieser Zusammenschluss sollte am Anfang in der Leitlinie zur Informationssicherheit verdeutlicht werden um für das weitere Vorgehen eine solide Basis zu bieten.

Der Weg am AWO Psychiatriezentrum Königslutter

Die Gestaltung einer digitalen Agenda als weitere Dimension der Unternehmensstrategie mit den Fokusbereichen Digitalstrategie, Digital Business, Digital Patient Relationship Management und „last but not least“ den Mitarbeitendenfokus Digital Work führte das AWO Psychiatriezentrum Königslutter 2019 zur Mitgliedschaft in der Hospitalgemeinschaft Hosp.Do.IT (Hosp). Zu Beginn wurden alle Fokusbereiche mit gleicher Wichtigkeit und Dringlichkeit entwickelt. Das Krankenhauszukunftsgesetz (KHZG) und die Krankenhausstrukturfondsverordnung (KHSFV) legte die Dringlichkeit auf das Mapping der Digitalstrategie auf die KHZG-Fördertatbestände (BAS Q 3). Da auch das KHZG der Informationssicherheit eine hohen Stellenwert beimisst – u.a. müssen in den sanktionsbewährten Fördertatbeständen (FTB) § 19 (1) Nr. 2 bis 6 mindestens 15 Prozent für Informationssicherheit ausgegeben werden – bleibt die digitale Agenda ein Bestandteil der Gesamtausrichtung des AWO Psychiatriezentrums.

Die Bestandteile des Managementsystems im Bereich der Informationssicherheit in Umsetzung des B3S und somit in Anlehnung an die ISO 27001 sind mindestens

- die Beschreibung des Kernprozess der Wertschöpfung, d.h. der Patientenversorgung,
- sämtliche Assets nach B3S, d.h. aus den Bereichen kritische branchenspezifische Anwendungssysteme, Informations-, Kommunikation-, Medizin- und Versorgungstechnik (IKMVT),
- eine Matrix der Schutzbedarfsfeststellungen der Assets mit Auswirkungswert bezogen auf die Bereich Vertraulichkeit, Integrität, Verfügbarkeit, Behandlungseffektivität und Patientensicherheit sowie
- ein Datenschutzkonzept.

Die Umsetzung der Leitlinie zur Informationssicherheit findet sich im ISMS wieder und der Nutzen liegt nicht nur

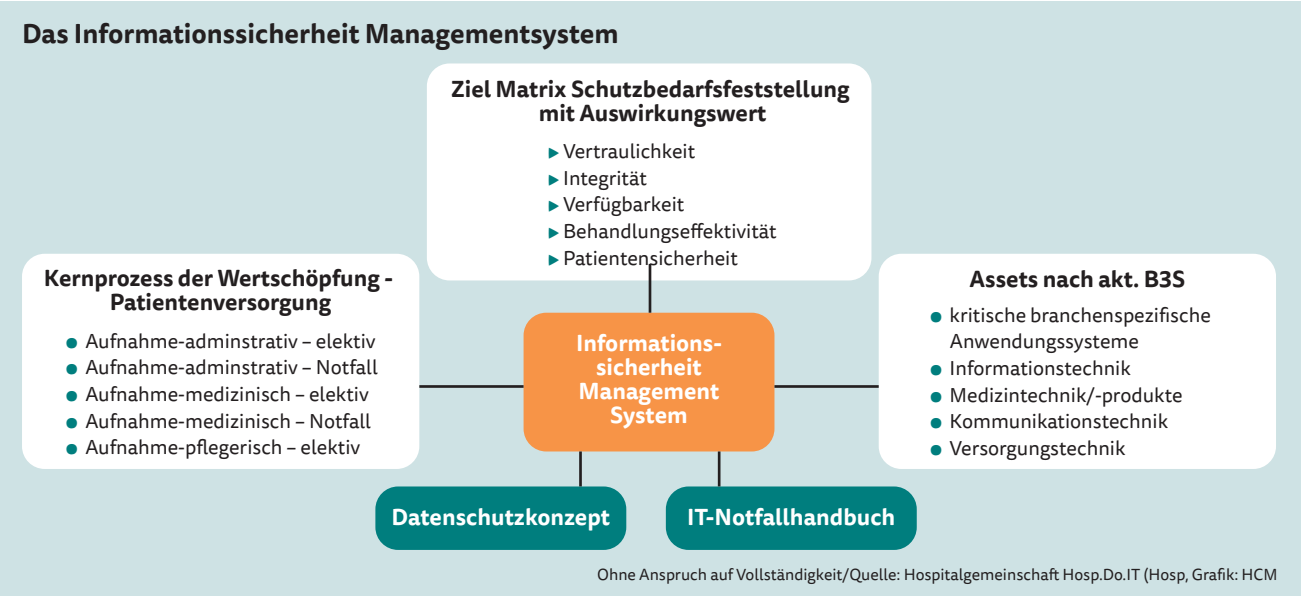
Björn Seelhorst

CHCIO, 1Geschäftsbereichsleiter IKT, AWO Psychiatriezentrum, **Kontakt: Bjoern.Seelhorst@awo-apz.de**

Dr. Pierre-Michael Meier

Generalbevollmächtigter, Hospitalgemeinschaft Hosp.Do.IT, **Kontakt: pierre-michael.meier@hosp.do.it.de**

Bilder: privat



Aufbau und Bestandteile eines ISMS.

darin, dass sich die Organisation mit der Informationssicherheit regelmäßig nach innen beschäftigt. Auch mit Blick auf die Klinische Dokumentenklassen-Liste (KDL), nach außen zu Vertragspartnern wie Software- und Hardwarelieferanten. Ebenso Versicherungen, die sich z.B. nur in der Verantwortung sehen, wenn ein ISMS institutionalisiert ist und für größten Risiken Notfallpläne vorliegen, die auch institutionalisiert sind, wie für Hackerangriffe.

Zur Vermeidung einer Störung der Informationssicherheit vom Geschäftsbereich IKMVT sind folgende Maßnahmen nach den Erfahrungen des AWO Psychiatriezentrums vorzunehmen:

- eine strukturierte sichere Datensicherungsstrategie anwenden,
- Form und Struktur der Daten auf dem Sicherungsträger in der Art aufbereiten, dass deren Rücksicherung technisch möglich ist,
- mindestens einmal täglich eine Datensicherung durchführen,
- Firewalls und Virenscanner durch Updates aktuell halten,
- durch Patch-Management zeitnah Sicherheitsupdates und -patches gewährleisten,
- Betriebssysteme und Programme, einschließlich Antivirensoftware und Firewalls verwenden, für die Updates bereitgestellt werden,
- Updates installieren, sobald diese vorliegen,
- eine solide Zugriffsstruktur, v.a. für die Administratoren aufbauen,
- Zugriff auf personenbezogene und andere sensible Daten mit Zugangsberechtigungen, Verschlüsselung und/oder Passwörtern sichern,
- von Vertragspartnern vorgegeben vorgegebene Prozesse zur Schadenmeldung und -bewältigung befolgen.