IT-Sicherheitsaudit als ideales Werkzeug zum Aufdecken möglicher Defizite in der IT-Sicherheit

Der Stellenwert der Informationstechnologie (IT) nimmt in allen Branchen und Lebensbereichen kontinuierlich zu. Unerlässlich werden Anwendungsbereiche durch neue IT-Systeme und Anwendungen erschlossen. Auch in Krankenhäusern ist die IT elementar für die Unternehmensprozesse. Die Erschließung von Anwendungsbereichen durch neue IT-Systeme und Anwendungen ist unerlässlich. Mit der wachsenden Zahl an eingeführten IT-Systemen steigt die Anzahl der IT-Nutzer. Somit wachsen auch die damit verbundenen Anforderungen an eine ganzheitliche IT-Sicherheit stetig. Durch die immer weitergehende Kommunikation, auch über die eigene Organisation hinaus, und die damit verbundene Öffnung steigt jedoch ebenfalls die Gefahr von Sicherheitslücken. Generell ist ein Nachholbedarf bei der IT-Sicherheit in deutschen Krankenhäusern zu beobachten.

Bereits vor der Corona-Krise war die IT-Sicherheit in Krankenhäusern von hoher Bedeutung und im Fokus vieler IT-Leitungen. Jedoch wurde ihre Relevanz gerade in der Krise und den damit an vielen Stellen einsetzenden Veränderungen in der IT-Landschaft verstärkt. So wurde beispielsweise in den Unterstützungsbereichen der Krankenhäuser vermehrt auf virtuelle Meetings und Homeoffice-Regelungen statt auf Besprechungen und Präsenzpflichten gesetzt. Viele IT-Abteilungen mussten hierfür unter hohem Zeitdruck schnelle Lösungen finden und setzten dabei oft auf cloudbasierte, die wenig physische Komponenten in den Rechenzentren der IT-Abteilungen benötigten. Durch den schnellen Handlungsbedarf und der Umstellung des Tagesgeschäfts wurden IT-sicherheitsrelevante Aspekte in den Hintergrund gestellt und notwendige sicherheitstechnische Anpassungen, beispielsweise von VPN-Zugängen und Rollen-/Rechtekonfigurationen etwa der Remote-Arbeitsplätze, fielen der Zeitknappheit bei der Umstellung zum Opfer. Letztlich führt die neue Situation in fast allen Bereichen zu neuen Lösungen in der IT-Landschaft. Obwohl die meisten Krankenhäuser und IT-Abteilungen die Schritte für den neuen Betrieb bereits gehen konnten und sich den neuen Gegebenheiten angepasst haben, bieten sich für Kriminelle eine Vielzahl an potenziellen Einfalltoren.

Die Corona-Krise wirkte in vielen Gebieten als Katalysator für die Digitalisierung im Krankenhaus und zeigte, wie wichtig eine funktionierende und sichere IT-Landschaft im Krankenhaus ist und welche Chancen durch die Digitalisierung im Gesundheitswesen entstehen. Nun ist der optimale Zeitpunkt für die IT-Abteilungen, den Fokus auf die IT-Sicherheit in zu richten, um sowohl die neuen Prozesse zu sichern als auch vermehrt in den Alltagsbetrieb übergehen zu können.

Das ideale Werkzeug, um den Status Quo der Krankenhaus-IT hinsichtlich der IT-Sicherheit zu erfassen, bietet ein IT-Sicherheitsaudit.

Mit Hilfe eines IT-Sicherheitsaudits kann der aktuelle Status in Bezug auf die IT-Sicherheit überprüft werden und Ansatzpunkte zur fortwährenden Verbesserung und Erhöhung aufgezeigt werden. Basierend auf dem Grundschutzkompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und weiterführenden branchenspezifischen Sicherheitsstandards, befasst sich das IT-Sicherheitsaudit mit Organisationsthemen und technischen Lösungen. Dazu werden zunächst organisatorische Abläufe im Krankenhaus unter anderem zu Notfallvorsorge-Konzepten, der Behandlung von Sicherheitsvorfällen und der Etablierung eines Informationssicherheitsmanagementsystems (ISMS) überprüft. Um die technischen Gegebenheiten zu untersuchen, werden die IT-Systeme, Netze und die Infrastruktur hinsichtlich der IT-Sicherheit geprüft. Ergänzt wird das IT-Sicherheitsaudit durch einen Penetrationstest. Hierbei werden mögliche Verwundbarkeiten durch Scans der Firewall und Router vom Internet aus (Black-Box-Tests) und Kontrolle der Systemkonfigurationen (White-Box-Tests) überprüft und gezielte Angriffe simuliert.

Aus dem IT-Sicherheitsaudit lassen sich anschließend der Schutzbedarf und notwendige Handlungsmaßnahmen ableiten, die von der IT-Abteilung umgesetzt werden können. Eine Priorisierungsempfehlung aus dem IT-Sicherheitsaudit ermöglicht die strukturierte Umsetzungsplanung.

Auch ohne bisherige Sicherheitsvorfälle kann kein Krankenhaus ausschließen, nicht selbst Opfer eines IT-Sicherheitsvorfalls, sei er mutwillig oder versehentlich herbeigeführt, zu werden und kann es sich daher nicht erlauben, seine IT-Sicherheit zu vernachlässigen. Gerade wenn durch die Corona-Krise Defizite in der IT-Sicherheit sichtbar wurden, sollten diese nun mit Hilfe eines IT-Sicherheitsaudits bewusst in den Fokus gestellt und untersucht werden. Dies legt den Grundstein für eine systematische Behebung der Defizite und eine Verbesserung der IT-Sicherheit im Krankenhaus.

Timo Braun,
Curacon GmbH