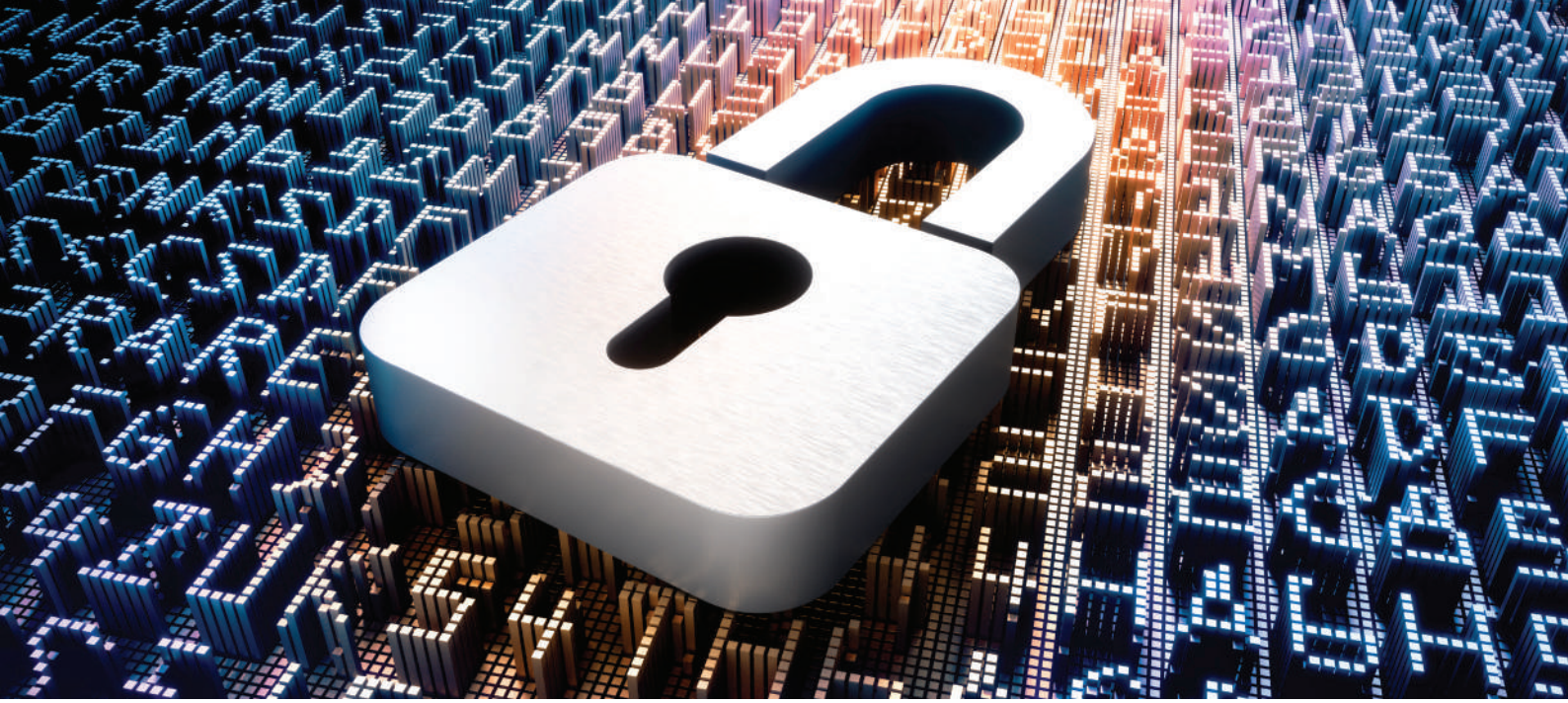

IT-Sicherheit in Kliniken:
Was Klinik-Chefs jetzt wissen müssen

Vom Diebstahl von Patientendaten bis zum Cyberangriff, der ganze Abteilungen lahmlegt und Leben gefährdet: Mit zunehmender Digitalisierung wird das Thema IT-Sicherheit für Kliniken, Krankenhäuser und Pflegeeinrichtungen immer wichtiger. Einrichtungen müssen jetzt sowohl für die entsprechenden technischen Grundlagen und Strukturen sorgen, als auch für das nötige Bewusstsein, zum Beispiel durch das Rekrutieren IT-versierter Führungskräfte. Handeln tut not: Einer aktuellen Studie nach war bereits fast jede zweite Klinik in Deutschland Ziel eines Hackerangriffs.

Diagnosen, Blutwerte, Krankheitsverläufe, ärztliche Behandlungen: Daten rund um die eigene Gesundheit gehören zu den sensibelsten Informationen des Menschen. Gerade in Kliniken müssen sie sorgsam vor unbefugtem Zugriff geschützt werden. Das kann sowohl gezieltes Kopieren durch Einzelne sein oder auch ein massenhafter Datendiebstahl.

Dabei ist dies nur eines von vielen IT-Risiken im Gesundheitswesen. Angesichts einer zunehmenden Digitalisierung und Vernetzung kompletter Abläufe und Prozesse können Sicherheitslücken in der Informationstechnik auch zu schwerwiegenden Ausfällen führen. Im November 2018 etwa sorgte ein Verschlüsselungstrojaner dafür, dass in einem Krankenhaus in Fürstenfeldbruck bei München über längere Zeit kein einziger PC und Server funktionierte – eines von zahlreichen Beispielen, wie sie sich regelmäßig in deutschen Kliniken ereignen. Das bestätigt auch eine 2018 von Rochus Mummert erhobene Umfrage unter 362 Führungskräften deutscher Krankenhäuser und Pflegeeinrichtungen. Sie ergab unter anderem:

- 43 Prozent aller Einrichtungen waren bereits Ziel eines Hackerangriffs
- 48 Prozent der Befragten fühlen sich vor entsprechenden Attacken nicht ausreichend geschützt.

»Auch beim Recruiting wird in der Praxis zu wenig auf IT-Wissen und IT-Sicherheits-Know-how geachtet.«

Führungskräfte in Kliniken müssen IT-kompetent sein

Gleichzeitig gilt es, mit aktuellen Datenschutzvorschriften wie der DSGVO ein anspruchsvolles Regelwerk rechtssicher umzusetzen

und auf aktuellem Stand zu halten. Mit dem E-Health-Gesetz hat der Staat speziell für diesen Bereich weitere Vorgaben samt Fristen erlassen, was Kliniken jetzt tun müssen. Für mich ergeben sich daraus vier wesentliche Qualitäten, die Einrichtungen jetzt erfüllen müssen:

- Führungskräfte im Gesundheitswesen – allen voran die Klinikgeschäftsführer – müssen über profundes Digital-Know-how verfügen, inklusive fundiertem Verständnis zu IT-Sicherheitsthemen.

- Personalentscheider in Kliniken benötigen das richtige Know-how, um IT-Kenntnisse von Bewerbern für Führungspositionen kompetent bewerten zu können. Diese müssen sowohl im kaufmännischen als auch im medizinischen Bereich Voraussetzung sein.

- Im Führungsalltag brauchen Klinik-Entscheider das nötige Wissen, wie man komplexe Digitalisierungsprojekte federführend leitet und externe Dienstleister und interne Spezialisten steuert und koordiniert.

- Führungskräfte aller Bereiche und Ebenen müssen regelmäßig Gelegenheit haben, ihr Wissen zu aktuellen Entwicklungen und IT-Risiken auf den neuesten Stand zu bringen.

Last but not least ist für mich auch das Kultivieren einer visionären Leader-Persönlichkeit gefordert – sprich Führungskräfte, die Agilität, Innovation und Vernetzung konsequent vorleben. Aus eigener, echter Überzeugung.

Nachholbedarf von Ausbildung bis Recruiting

Betrachtet man die Realität im Gesundheitswesen, zeigen sich hier gleich mehrere Herausforderungen. Besonders gravierend sind für mich folgende:

- Es bestehen massive Defizite in der medizinischen und pflegerischen Ausbildung an Universitäten und Fachschulen – Digital-Know-how spielt dort meist nur eine geringe Rolle.

- Von den deutschen Gesundheitseinrichtungen hatte laut der eingangs zitierten Studie auch 2018 weit mehr als die Hälfte (!) keine unternehmensübergreifende Digitalstrategie. Sie wäre für das Thema IT-Sicherheit die nötige zentrale Plattform.

Auch beim Recruiting wird in der Praxis zu wenig auf IT-Wissen und IT-Sicherheits-Know-how geachtet. Laut unserer Studie sind entsprechend fundierte Kenntnisse von Kandidaten bei nur 29 Prozent der Einrichtungen Einstellungskriterium. Alle anderen beabsichtigten hier erst noch, nachzuziehen. Höchste Zeit, finde ich.

Autor:
Dr. med. Peter Windeck
Geschäftsführer
Rochus Mummert
Healthcare Consulting GmbH
Peter.Windeck@rochusmummert.com