

IT-Sicherheit im Krankenhaus

## »Die Situation ist paradox«

14.12.2018

Kritischer Stammtisch Dresden

**Die meisten der 130 unter die KRITIS-Verordnung des Bundesamtes für Sicherheit in der Informationstechnik fallenden Großkliniken sind auf der Zielgeraden, was die Umsetzung betrifft. Aber auch die kleineren und mittleren Krankenhäuser müssen sich schützen. Problem: fehlendes Budget.**



© Pixabay

*Mehr Digitalisierung bedeutet auch höhere Anforderungen an die Datensicherheit.*

Sprinter im KRITIS-Rennen sind die Teilnehmer des Kritischen Stammtisches in Dresden. Der mitteldeutsche Arbeitskreis für den Erfahrungsaustausch zur Umsetzung der KRITIS-Anforderungen hat sich laut Veranstalter nach der inzwischen 5. Auflage zur Expertise-Plattform gemausert. Mittlerweise nehmen über 10 Prozent der deutschlandweit unter die KRITIS-Verordnung fallenden Kliniken am Stammtisch teil. Hinzu kommen Experten aus dem LKA, der Medizintechnik sowie ISMS-Berater und Auditoren.

Konrad Christoph, Experte für IT-Sicherheit im Gesundheitswesen bei SHD, hat die Runde Mitte 2017 gemeinsam mit der Uniklinik Dresden ins Leben gerufen und sagt heute: »Alle unter KRITIS fallenden Häuser haben eine Strategie für sich gefunden, aber bezüglich Umsetzung fehlen an vielen Stellen immer noch die Ressourcen, finanziell wie personell.« Dadurch werde für alle die Zeit bis zum Stichtag Ende Juni 2019 knapp. Hinzu kommt die Lage bei mittleren und kleinen Häusern, die zwar nicht unter KRITIS fallen, sich aber ebenfalls schützen müssen. »Die Situation ist einigermaßen paradox.« Politik, Verbände, Vorstände und selbstverständlich die ISB (Informationssicherheitsbeauftragte) selbst kennen das schwelende Problem seit Langem. Aber das Nadelöhr Finanzierung bleibt bestehen.

### **Finanzielle Ressourcen sind da**

Immerhin haben die Teilnehmer des Stammtisches gemeinsam mit der Krankenhausgesellschaft Sachsen Ende November einen Lichtblick ausgemacht: Der im neuen Pflegepersonalstärkungsgesetz ausgewiesene Strukturfonds 2 (Laufzeit von 4 Jahren, ab 2019 bis 2022) berücksichtigt auch Mittel für Verfahren und Maßnahmen im Bereich KRITIS und Digitalisierung. Auf Bundesebene werden jährlich 500 Millionen Euro aus der Liquiditätsreserve des Gesundheitsfonds bereitgestellt – ein Teil davon steht für Vorhaben zur Verbesserung der Informationstechnischen Sicherheit der Krankenhäuser zur Verfügung.

Wobei der jeweilige Landeshaushalt zusätzlich 50 Prozent als Co-Finanzierung aus eigenen Mitteln

aufbringen muss. Nach Erscheinen der Verwaltungsvorschrift liegt es Christoph zufolge nun auch an der Kreativität der Häuser, diese Fördergelder sofort und vor allem adäquat zu beantragen. Dr. Stephan Helm, Geschäftsführer der Krankenhausgesellschaft Sachsen, erwartet hier einen regelrechten Run auf den Fördertopf und empfiehlt, schnell zu handeln.

Aus Sicht der Deutschen Krankenhausgesellschaft (DKG) sei es ausdrücklich zu begrüßen, dass hiermit ein erster Schritt zur Refinanzierung entstehender Kosten gegangen wurde. Darüber hinaus setzt sich die DKG jedoch auch dafür ein, Krankenhäusern, die nicht unter die KRITIS-Verordnung (Schwellenwert: 30.000 stationäre Behandlungen jährlich) fallen, eine Refinanzierung für Maßnahmen rund um die Erhöhung der IT-Sicherheit zu ermöglichen.

### **Weiterer Engpass: fachlich versierte Auditoren**

Beim Stammtisch erläuterte Matthias Lohmann, Auditor aus Bergisch-Gladbach, den Aufwand für eine Zertifizierung. Dieser gehe von den notwendigen Vorbereitungen über die Durchführung des Audits bis zur Meldung und Dokumentenübergabe an das BSI und dauere im Schnitt vier Monate. Auf Basis dieser Zeitschiene empfiehlt er Nachzüglern, die Auditvorbereitungen spätestens im Ende Februar 2019 zu beginnen.

Zu beachten sei dabei, dass für die Prüfung der Häuser Fachexperten einbezogen werden müssen. Das ist aus Sicht von Lohmann ein echter Engpass: »Zwar gibt es genug Zertifizierungsstellen, aber diese haben keine Kontakte zu den für die Prüfung notwendigen Spezialisten mit mehrjähriger Branchenfachkompetenz. Und auch KRITIS-Auditoren sind fast ausgebucht!« Hier eventuell noch frei schwebende Kapazitäten will das SHD gerne vermitteln. »Experten mit mindestens drei Jahren Berufserfahrung im Klinikumfeld in den vergangenen fünf Jahren können sich bei Interesse an Auditbegleitung gern bei mir melden«, Christoph.

### **Software-Werkzeuge unterstützen eine strukturierte Vorgehensweise**

Generell sind bei der internen Vorbereitung nach Auffassung der Teilnehmer geeignete Software-Werkzeuge entscheidend wichtig: Wer hier immer noch mit statischen Tabellenkalkulations- oder Textverarbeitungs-Programmen arbeite, sollte sich schnell auf die Suche nach dynamischen Tools machen, die durch ihre Darstellung und Verwaltbarkeit funktionaler Zusammenhänge die Arbeit der ISB enorm erleichtert.

Beim SHD gibt es neben einem entsprechenden Tool auch ein spezielles Angebot für alle Kliniken: Um die bei den Expertentreffen gebündelte Kompetenz weiter zu geben, bietet das Unternehmen interessierten ISBs persönliche Telefonate von einer Stunde mit Christoph an, in dem Problemstellungen verglichen und bereits erprobte Lösungswege skizziert werden können.

Eines sei bei dem Ganzen aber auch sicher: Im Zuge der KRITIS-Vorkehrungen wird die Sicht auf Abläufe und Schnittstellen an Bedeutung gewinnen. Denn die intensive Beschäftigung mit der Absicherung lenkt den Blick automatisch auf sinnvoll vernetzte Infrastrukturen, saubere Prozesse und flexible Nutzungsmethoden. Und das erhöht nicht nur die IT-Sicherheit, sondern schafft echte Mehrwerte bei der Zusammenarbeit aller Bereiche im Klinikum. *(me)*