EIN WEG ZU PERMANENTER KRITIS-KONFORMITÄT IM KRANKENHAUS

Im Juni 2017 trat die KRITIS-Verordnung der Bundesregierung in Kraft. Die Zeit läuft, doch auch ein knappes Jahr nach der Verordnung ist noch einiges unklar. Nicht unklar ist, dass sich Krankenhäuser und andere Gesundheitsbetriebe um die IT-Sicherheit kümmern müssen. Ein risikobasierter Ansatz zur Analyse und Priorisierung von IT-Sicherheitslücken in KRITIS-betroffenen Gesundheitsbetrieben.

TEXT: PIERRE GRONAU

Als am 30. Juni 2017 die KRITIS (KRITIS = kritische Infrastrukturen)-Verordnung des Bundesamts für Sicherheit in der Informationstechnik (BSI) in Kraft trat, fing in deutschen Krankenhäusern die Uhr an zu ticken. Noch rund ein Jahr bleibt den Betreibern, um den Anforderungskatalog zu erfüllen, ein gutes Jahr, um der Behörde die dazugehörenden Auditergebnisse zu präsentieren. Unter die neue Verordnung fallen aktuell alle Krankenhäuser mit mindestens 30 000 vollstationär betreuten Patienten pro Jahr. Sie müssen bis dahin ein sogenanntes Mindestsicherheitsniveau gemäß Stand der Technik erreichen und dies alle zwei Jahre auf den Prüfstand stellen.

ILLUTSTRATION: © GRONAU IT CLOUD COMPUTING

Bis der dazu ins Leben gerufene Branchenarbeitskreis „Medizinische Versorgung“ diese Mindestanforderungen im Rahmen eines branchenspezifischen Sicherheitsstandards (B3S) abschließend definiert, vergehen sicher noch einige Monate. Doch für die Krankenhausbetreiber läuft mit Inkrafttreten der BSI-KRITIS-Verordnung die Zweijahresfrist. Diesen Zeitrahmen vor Augen, hat der Branchenarbeitskreis nun als Vorabinformation zum späteren B3S eine konkrete „Handlungsempfehlung für die Verbesserung zur Informationssicherheit an Kliniken“ veröffentlicht. Das Dokument verfolgt den Ansatz, betroffenen Einrichtungen den Einstieg in das Thema IT-Informationssicherheit zu erleichtern und klarzustellen, dass dieses Thema nicht autark in IT-Abteilungen aufgehängt sein sollte.

STAND DER TECHNIK: BITTE NICHT AUSRUHEN

Laut BSI müssen KRITIS-Betreiber ihre IT-Prozesse, die sich für die Bevölkerung, in diesem Kontext Patienten, als kritisch erweisen können, nach dem Stand der Technik absichern und dies gegenüber dem BSI verpflichtend nachweisen. Begriff und Forderung nach besagtem Stand der Technik gibt das IT-Sicherheitsgesetz (IT-SiG) vor, wobei jedoch keine konkreten Aussagen damit verbunden sind, die den Begriff mit Leben füllen. Dieses Manko sieht auch der Bundesverband IT-Sicherheit e.V. TeleTrusT und reagiert mit einem verbandsinternen Arbeitskreis „Stand der Technik“, um Einrichtungen, Unternehmen und IT-Anbietern Orientierungshilfen und Handlungsempfehlungen anzubieten. Jenseits dieser Handlungsempfehlungen erfolgt die Nachweispflicht von Krankenhausbetreibern jedoch eigenverantwortlich; wahlweise in Form von Sicherheits-Audits, Prüfungen oder Zertifizierungen. Der Blick in die sich permanent erneuernde IT-Landschaft nebst wandlungsfähigen Bedrohungsbildern von außen macht klar, dass es sich um laufende Prüfungen von IT-Systemen und IT-Strukturen handeln muss. Eine tagesaktuell festgestellte Sicherheit und Konformität kann schon morgen überholt sein.

DAS SICHERHEITSKONZEPT: SECURITY AS A SERVICE

Nach aktueller Einschätzung agiert heutzutage nahezu kein Krankenhaus nach Stand der Technik, was aber die Basis für IT-Sicherheit darstellt. Darüber hinaus reicht bei Angriffen von außen, beispielsweise auf digitalisierte Patientenakten, der Stand der Technik zumeist nicht aus. Hier muss der Stand der Forschung für bestehende IT-Strukturen risikobasiert ermittelt und in sie integriert werden. Auf dieser Basis überprüfen Experten IT-Systeme kontinuierlich auf Sicherheitslücken, um Attacken wie zuletzt Meltdown oder Spectre abzuwehren.

Dieser Beitrag formuliert einen risikobasierten Ansatz, um mindestens den Stand der Technik zu erreichen, damit den Minimalanforderungen der geforderten Sicherheit zu genügen und diese dauerhaft zu verbessern. Die Grundvoraussetzung für diesen Ansatz ist ein tragfähiges Sicherheitskonzept.

Das folgend dargestellte, auf Kontinuität ausgerichtete Sicherheitskonzept zielt darauf ab, die größten Schwachstellen und damit Gefahren für Sicherheitslücken in den IT-Strukturen einer KRITIS-betroffenen Gesundheitseinrichtung aufzudecken und Gegenmaßnahmen zu entwickeln. Die Bestandsaufnahme der Lücken, ihre Schließung und Dokumentation sowie der daraus folgende Nachweis der Datenkonformität sind als eindeutige Ziele formuliert. Es ist kein juristischer, übergeordneter Weg, sondern ein IT-getriebener Bottom-up-Weg.

SCHRITT 1: DEN RAHMEN ABSTECKEN

Die Transparenz einer Gesundheitseinrichtung bildet den Ausgangspunkt. Wie viele Mitarbeiter arbeiten im Krankenhaus? Welche IT-Systeme, Netze, Telekommunikationsanlagen und medizinischen Geräte sind im Einsatz? Wer zeichnet jeweils dafür verantwortlich und welche Mitarbeiter sowie externe Dienstleister wie zum Beispiel Reinigungskräfte haben Zugang? Sind diese Strukturen definiert, können IT-Sicherheitsbeauftragte ihre Taskforce bilden.

SCHRITT 2: INTERDISZIPLINÄRE TEAMBILDUNG

Die Absicherung von IT-Strukturen und der davon abhängende Schutz patientenbezogener Daten ist kein reines IT-Thema. Anwender medizinischer Devices, die Daten produzieren, kaufmännische Angestellte, Compliance-Verantwortliche und Datenschutzbeauftragte, das Legal Department, Krankenhausmanagement und IT-Leiter bzw. -Leiterin gehören sinnvollerweise zum IT-Sicherheitsteam. Es empfiehlt sich also die breite Aufstellung eines disziplinübergreifenden Teams von ungefähr zehn Personen aus Key-Anwendern, die den kompletten Prozess begleiten. Auch außenstehende Sicherheitsexperten ergeben Sinn, da diese Zusammenhänge ohne den hausinternen Tunnelblick betrachten. Aus der Teamarbeit ergibt sich der größte Lerneffekt über die zu analysierenden Strukturen, Systeme und Komponenten aus diversen Blickwinkeln.

Es sollten auch nicht nur Sicherheitsaspekte der primär identifizierten Systeme diskutiert, sondern auch >

ihre komplette IT-Umgebung sowie ihre Aspekte zum Gegenstand werden.

SCHRITT 3: IT-GETRIEBENE BESTANDSAUFNAHME

Die im Team erarbeiteten Erkenntnisse verdichten sich zu einer IT-bezogenen Bestandsaufnahme. Sie soll im Anschluss dazu führen, kritische Patientenversorgungsprozesse in der stationären Betreuung aufzuzeigen. Das können datenerzeugende medizinische Apparate wie EKGs oder Ultraschallgeräte sein, genau wie deren Schnittstellen zu IT-Systemen, Cloud-Diensten, Herstellersoftware und Dienstleistern. Jedes System, jede Komponente, die in diesem Rahmen identifiziert wird, sollte in puncto Schwachstellen und personenbezogene Daten analysiert werden, wobei ihnen je nach Art differenzierte Schutzziele zugewiesen werden müssen. Schließlich ist jede Komponente, IT-sprachlich jedes Asset, unterschiedlichen Risiken und Gefahren ausgesetzt. Wie wahrscheinlich ist ein Angriff, wie hoch die Motivation dafür und der damit verbundene Schaden? Das sind Fragen, die sich IT-Sicherheitsbeauftragte beantworten müssen, um Risiken einzuschätzen. Kundige gehen davon aus, dass ungefähr die Hälfte aller Sicherheitsprobleme von Fehlern in der Software und Fehlkonfigurationen der IT-Systeme herrühren. Diese entwicklungsbasierten Fehler sind der Ausgangspunkt für ungewollte Ereignisse oder Angriffe. So kann eine Schwachstelle dafür sorgen, dass beispielsweise personenbezogene Patientendaten eines medizinischen Geräts unverschlüsselt mit Klarnamen übertragen werden. Eine Schwachstelle wird zudem zum Sicherheitsrisiko, wenn jemand Interesse hat, diese für sich zu nutzen. Experten sprechen dann von „Vulnarability“, angreifbaren Schwachstellen, die Unbefugte nutzen, um schadhafte Codes auszuführen oder Datenpakete zu lancieren. In diesem ungeschützten Zustand stehen dem Angreifer Rechte zur Verfügung, die das Asset gefährden. So können beispielsweise Passwörter aus Datenbanken ausgelesen werden. Hier gilt es, Risiken, Schwachstellen und Bedrohungen zu enttarnen, zu klassifizieren und vor allem zu dokumentieren.

SCHRITT 4: RISIKOANALYSE MIT PENETRATIONSTESTS

In der Risikoanalyse ermitteln Projektbeteiligte systematisch zu schützende Software, Schnittstellen zu angrenzenden Systemen sowie weitere Entitäten: potenzielle Angreifer, Umwelteinflüsse wie Hochwasser, Administratoren und ungeschulte Anwender. Ein wesentliches Mittel hierbei sind Penetrationstests, die von Externen durchgeführt werden sollten, die mit diesen Verfahren vertraut sind. Dabei dringen IT-Sicherheitsexperten mit den gleichen Methoden in das System ein, die auch ein interner oder externer Angreifer nutzen würde, um sich unautorisiert Zugriff zu verschaffen. Der fingierte Livehack legt sozusagen den Finger in die Wunde und ermittelt die Empfindlichkeit des zu testenden Systems gegen aktuelle Angriffsmuster. Penetrationstests identifizieren Schwachstellen, decken Anwender- wie auch Softwarefehler auf und erhöhen nach Auswertung und Beseitigung die IT-Sicherheit. Regelmäßig ausgewertete Schwachstellentests eines externen Dritten ergeben zudem einen permanent steigenden Level an IT-Sicherheit. Sie ist nichtsdestotrotz eine Momentaufnahme, denn durch immer neue sicherheitsrelevante Aspekte können Systeme trotz jüngst gestopfter Sicherheitslücken an anderen Punkten dennoch verwundbar sein. Wo jedoch Entwick-

ILLUSTRATION: © GRONAU IT CLOUD COMPUTING

lungsfehler seitens der Hersteller, Anwenderfehler oder falscher Software-Einsatz durch Pen-Tests aufgedeckt werden, lassen sich daraus klare Gegenmaßnahmen und Konsequenzen ableiten, die durch Dokumentationen zu einer erhöhten und nachweisbaren Sicherheitsstufe führen. Identifizierte Schwachstellen und Bedrohungsszenarien können anhand von Informationen aus der verfügbaren Dokumentation mitigiert, also abgeschwächt oder bestenfalls eliminiert werden. Kommen wir zurück zum Beispiel der entwendeten Passwörter, könnte in der Dokumentation zum Beispiel vermerkt sein, dass Passwörter zukünftig in einer verschlüsselten Datenbank gespeichert werden, was die Gefahr des Passwortdiebstahls mitigiert.

SCHRITT 5: MASSNAHMEN-BASIERTES ERLANGEN VON IT-SICHERHEIT

Neben der im oberen Abschnitt erwähnten lückenlosen Dokumentation ist auch eine klare Zuordnung von Verantwortlichkeiten innerhalb des Krankenhauses eine wesentliche Maßnahme zur Erlangung von IT-Sicherheit. Damit einher geht die Einrichtung einer Meldestelle, die bei beobachteten Unregelmäßigkeiten wie fehlerhaftem Umgang mit nicht verschlüsselten Patientendaten, Ausfällen datenproduzierender medizinischer Geräte oder bei Cyberangriffen mit Notfallkonzepten reagiert. Es muss also Teil des Sicherheitskonzeptes sein, IT-bezogene Schulungen für das Personal anzubieten und das im Rahmen des Konzeptes erworbene Wissen über die eigenen Strukturen in die Abteilungen zu tragen. Erst diese tiefe Verankerung schließt den Kreislauf und stützt das Bottom-up-Konzept. ■

■ **PIERRE GRONAU**

Gründer und Inhaber
Gronau IT Cloud Computing GmbH Berlin

www.gronau-it-cloud-computing.de

Kontakt: kontakt@gronau-it-cloud-computing.de