KRITIS im Krankenhaus: Komplex, aber machbar

(April 2019) Der Schutz kritischer Infrastrukturen im Gesundheitssektor ist nicht trivial, die Vorbereitungen auf den Stichtag 30.06. diesen Jahres laufen auf Hochtouren. Dank der Erkenntnisse sowie dem Informations- und Erfahrungsaustausch auf dem inzwischen sechsten KRITISchen Stammtisch Dresden haben die rund 35 Teilnehmer einen Wissensvorsprung, der ihre Aufgabe wesentlich vereinfacht.

Geteilt wurden insbesondere Tipps für den Fokus auf Kernprozesse, den Antrag auf Fördergelder und den Umgang mit Prüf-Ergebnissen.

Mit großem Interesse verfolgten die anwesenden Sicherheits-Experten den KRITISchen Stammtisch in der sächsischen Elbmetropole. Viele Kliniken haben sich schon intensiv auf den Stichtag vorbereitet, ihre ersten internen Audits womöglich bereits weitgehend hinter sich und sogar zusätzliche Schutzmaßnahmen getroffen. Vertreter einiger Häuser standen in Dresden Rede und Antwort, doch es gibt noch Unsicherheiten. So müsse klar sein, dass Prüfer, die nach Branchenspezifischen Sicherheitsstandards BS3 vorgehen wollen, nach wie vor auf die endgültige Fassung der Durchführungsverordnung warten müssen – obwohl im April die Auditierungen offiziell beginnen sollen. Zwar muss die Auditierung nicht nach den B3S vorgenommen werden, dies bietet allerdings den Vorteil, den neusten Stand der Technik in Kliniken höchstmöglich zu berücksichtigen.

Hans-Wilhelm Dünn zufolge, Präsident des Cyber-Sicherheitsrat Deutschland e.V., sind die Krankenhäuser noch nicht ausreichend gegen Angriffe von Cyberkriminellen gerüstet. Hier werde es voraussichtlich über den Stichtag hinaus noch Nachbesserungen geben müssen. Das liege aber nicht allein an den Häusern,

Herausforderungen.

Angesichts des nahenden Stichtags zur Jahresmitte rät Stammtisch-Mitinitiator Konrad Christoph zu Pragmatismus: „Jetzt handeln mit 80 Prozent Klarheit ist besser als bis zum Schluss zu warten und dann womöglich mit leeren Händen dazustehen." Bei der Beantragung von Fördermitteln berücksichtige der im neuen Pflegepersonal-Stärkungsgesetz ausgewiesene Strukturfond mit einer Laufzeit von vier Jahren (2019 bis 2022) auch Mittel für Verfahren und Maßnahmen im Bereich BSI Kritisverordnung. Auf Bundesebene werden jährlich 500 Millionen Euro aus der Liquiditätsreserve des Gesundheitsfonds bereitgestellt – ein Teil davon stehe für Vorhaben zur Verbesserung der informationstechnischen Sicherheit der Krankenhäuser zur Verfügung. Dabei muss der jeweilige Landeshaushalt zusätzlich 50 Prozent als Co-Finanzierung aus eigenen Mitteln aufbringen. Nach Erscheinen der Verwaltungsvorschrift liegt es, so Christoph, auch an der Kreativität der Häuser, diese Fördergelder entsprechend der zeitlichen Vorgabe zu beantragen.

Sebastian Junge, ISB der Heinrich-Braun Klinikum gemeinnützige GmbH (HBK),hielt Junge fest, dass das HBK einen BSI-Nachweis durch eine Kombination aus branchenspezifischem Sicherheitsstandard und der ISO/IEC 27001 anstrebt.

Laut Frank Engelking, ISB beim Carl-Thiem-Klinikum Cottbus, ist zu erwarten, dass es beim Audit eine Mängelliste geben werde, die mit dem Prüfer diskutiert werden könne. Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) muss die kommentierte Mängelliste vorgelegt werden. Das BSI erhält durch den Eingang der Prüfberichte einen generellen Überblick der Informationssicherheit in der Branche und werde darüber hinaus voraussichtlich stichprobenartig mit einigen Einrichtungen in Kontakt treten. Zukünftig könne das BSI einen Sachstand über die KRITIS-Fortschritte aufbauen.

René Salamon, Sektorverantwortlicher Gesundheit beim BSI, gab Einblicke, welche Vorfälle überhaupt gemeldet werden müssen. Ziel sei es, sich anhand der Menge und Inhalte der Fehlermeldungen ein Lagebild von besonders gefährdeter IT-Security der Hard- und Software zu schaffen, die entsprechenden Hersteller zu identifizieren und auf diese zuzugehen, um die Fehler zu beheben. Denn nicht selten ist es der Fall, dass Sicherheitsmängel in den Produkten von den SIBetreibern nicht kompensiert werden können, sondern herstellerseitig abgestellt werden müssen.

Salamon warb dafür, dem BSI im Störungsfall zu vertrauen. Die Anonymisierung von Daten sei möglich, es werde nichts

anhand der Mängelliste, sowie die Initiierung eines Veränderungsprozesses.

Ein Management, das bis dato noch immer keine Budgets freigestellt oder Fördermittel initiiert habe, gerate spätestens mit der Vorlage des Prüfberichts endgültig unter Druck. Generell begrüßte Salamon die bereits bestehende sowie die absehbare Kooperation zwischen Kliniken und BSI, nur so sei die Sicherheit kritischer Infrastrukturen sinnvoll zu erarbeiten und letztlich von Erfolg gekrönt.

Der nächste KRITISche Stammtisch der SHD GmbH wird am 11.09.19 stattfinden- mit den Schwerpunkten Auswertung der Audits und Strategien für das Abarbeiten der Mängellisten. Weitere Informationen werden auf https://www.shd-online.de/veranstaltungen/ bekanntgegeben.

Quelle Text: System Haus Dresden

Quelle Bild: Fotolia/kamasigns