RheinlandPfalz
MINISTERIUM FÜR SOZIALES, ARBEIT, GESUNDHEIT UND DEMOGRAFIE

RUNDER TISCH IT-SICHERHEIT
KRANKENHÄUSER

Maßnahmen und Empfehlungen der Projekt-gruppe

(11. März 2020)

PRÄAMBEL

Der Runde Tisch „IT-Sicherheit Krankenhäuser" hat in seiner Sitzung am 14. August 2019 auf Vorschlag von Gesundheitsministerin Sabine Bätzing-Lichtenthäler einvernehmlich beschlossen, eine mit Fachexperten der vertretenen Organisationen besetzte Projektgruppe ins Leben zu rufen. Aufgabe der Projektgruppe war es, konkrete Vorschläge, Maßnahmen und Empfehlungen zur Verbesserung der IT-Sicherheit in Krankenhäusern ausarbeiten. Rechtliche Grundlage hierfür waren die rechtlichen Vorgaben sowohl aus den IT-Sicherheitsgesetzen als auch aus den datenschutzrechtlichen Regelungen, die von den Krankenhäusern umzusetzen sind.

Die Projektgruppe hat in zwei Sitzungen am 19. September und am 27. November 2019 über Maßnahmen zum besseren Schutz vor Cyberangriffen auf Krankenhäuser beraten und sich sowohl auf übergeordnete Maßnahmen als auch auf konkrete Empfehlungen für die Krankenhäuser verständigt.

Ein wichtiges Handlungsfeld zur Verbesserung der IT-Sicherheit in den Krankenhäusern liegt vor allem im Kompetenzerwerb und der Sensibilisierung der Mitarbeiterinnen und Mitarbeiter. Gleichwohl müssen die Krankenhäuser angesichts der zunehmenden Professionalität der Cyberangriffe auch erhöhte und verbesserte technisch-organisatorische und personelle Vorkehrungen treffen, um sich vor Cyberattacken zu schützen. Die damit verbundenen hohen Kosten werden im derzeitigen Vergütungssystem nicht ausreichend refinanziert. Die Projektgruppe unterstreicht, dass über die hier vorgeschlagenen Maßnahmen hinaus im Zuge eines Sofortprogramms weiterhin auch eine Ausweitung der Strukturfondsförderung auf Krankenhäuser mit weniger als 30.000 Fällen und deren Aufstockung sowie Verbesserungen in der Betriebskostenfinanzierung entsprechend der Forderungen des Runden Tisches erforderlich sind. Denn auch

diese kleineren Einrichtungen sind datenschutzrechtlich verpflichtet, geeignete Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus der von ihnen verarbeiteten Gesundheitsdaten zu treffen.

Um die Umsetzung der Maßnahmen weiter zu konkretisieren und zu begleiten, wird vorgeschlagen, die Arbeit der Projektgruppe auch im Jahr 2020 mit einer weiteren Sitzung fortzusetzen.

ENTWICKLUNGEN AUF BUNDESEBENE

Teilweise parallel zu den Beratungen der Projektgruppe gab es für die IT-Sicherheit relevante Entwicklungen auf Bundesebene, die zu berücksichtigen sind.

Die DKG hatte sich bereits im Jahr 2018 dafür ausgesprochen, gemeinsam mit Fachexperten aus dem Bereich der Informationssicherheit und in Abstimmung mit dem BSI einen Branchensicherheitsstandard für deutsche Krankenhäuser zu erarbeiten. Dieser Sicherheitsstandard beschreibt Maßnahmen, wie die an der Versorgung der Patienten genutzten Prozesse und Systeme vor dem Hintergrund der branchenspezifischen Gefährdungslage im Krankenhaus geschützt werden, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen zu gewährleisten und damit die IT-Sicherheit in den deutschen Krankenhäusern zu verbessern. Der von der DKG zur Verbesserung der IT-Sicherheit in den Krankenhäusern erarbeitete Branchenspezifische Sicherheitsstandard („B3S") wurde dem Bundesamt für Sicherheit in der Informationstechnik am 3.6.2019 zur Eignungsfeststellung gemäß § 8a Abs. 2 BSIG vorgelegt. Das BSI hat zwischenzeitlich die Prüfung abgeschlossen. Die Feststellungsurkunde wurde seitens des BSI am 22.10.2019 an die DGK übergeben. Damit liegen für den Krankenhausbereich Maßnahmenempfehlungen für die IT-Sicherheit bzw. die Sicherheit der Verarbeitung vor, die dem Stand der Technik nach Art. 32 Datenschutz-Grundverordnung entsprechen.

Die DKG hatte parallel zur Erstellung des Sicherheitsstandards auch eine Studie in Auftrag gegeben, die den Umsetzungsaufwand der enthaltenden Maßnahmen in den Krankenhäusern ermitteln sollte. Demnach werden für die Bereiche Investition, Betrieb und Personal für ein Krankenhaus mit 30.000 vollstationären Fällen im Jahr initi-

ale Kosten in der Größenordnung von 1,5 bis 2 Millionen Euro erwartet, in den Folgejahren ist mit jährlichen zusätzlichen Belastungen in der Größenordnung von ca. 500.000 bis 600.000 Euro zu rechnen.

Die Projektgruppe spricht sich auch vor diesem Hintergrund dafür aus, durch bundesgesetzliche Änderungen eine Refinanzierung dieser Kosten zu bewirken.

MASSNAHMEN UND EMPFEHLUNGEN

Infolgedessen unterbreitet die Projektgruppe folgende Vorschläge für übergeordnete Maßnahmen und Empfehlungen an die Krankenhäuser:

Übergeordnete Maßnahmen

- Einstellen von fachspezifischen Informationen für die Krankenhäuser auf der Homepage der Krankenhausgesellschaft Rheinland-Pfalz,

- Schreiben an die Krankenhäuser mit Informationen über Ergebnisse des Runden Tisches, den Informationsangeboten (u.a. Hinweis auf Homepage) und konkreten Empfehlungen,

- Durchführung von Informationsveranstaltungen für Krankenhäuser zum Schutz vor Cyberangriffen (mit Best Practice-Empfehlungen und Möglichkeit für Erfahrungsaustausch bzw. regelmäßigen Austausch im Anschluss, insbesondere auch zwischen den Berufsgruppen); bereits konkret geplant ist eine gemeinsame Veranstaltung des MSAGD, des MdI (Verfassungsschutz) und des Landeskriminalamtes, die am 20. April 2020 in Mainz stattfinden wird,

- Aufgreifen des Themas IT-Sicherheit in Krankenhäusern als Tagesordnungspunkt auch bei weiteren Veranstaltungen, so etwa bei den regelmäßigen Tagungen des Verbandes der Krankenhausdirektoren Landesgruppe Rheinland-Pfalz/Saarland (VKD),

- Durchführung von regelmäßigen (jährlichen) Fachveranstaltungen für die IT-Leiter der Krankenhäuser seitens des Verbandes der Krankenhausdirektoren Rheinland-

Pfalz/Saarland: Konkret wird der VKD am 28. Mai 2020 einen zentralen Lehrgang für IT-Leiter, der sich mit den Gefahren durch Cyberattacken und Abwehrmaßnahmen befassen wird, durchführen,

- Durchführung von Übungen zur Abwehr und zum Umgang mit Cyberattacken: KRITIS-Betreiber sind eingeladen, sich an der in Deutschland vom BSI koordinierten und in 2020 auf den Gesundheitssektor fokussierenden Übung „Cyber Europe 2020" am 17./18. Juni 2020 zu beteiligen (Informationen unter www.cyber-europe.eu); das MSAGD wird im Mai 2021 unter Beteiligung eines Krankenhauses im Sinne des BSI-Gesetzes an der strategischen Länder- und Ressortübergreifenden Krisenmanagementübung LÜKEX 21 mit dem Szenario „Cyberangriff auf Regierungshandeln" teilnehmen,

- Im Falle eines Cyber-Vorfalls in einem Krankenhaus bietet das BSI Unterstützung bei der Krisen-/Vorfallsbewältigung an. Diese Unterstützung kann sich darstellen als
  - eine Telefonkonferenz mit BSI-Experten,
  - Verweise auf qualifizierte Dienstleister,
  - Unterstützung bei der Analyse einzelner Aspekte des Vorfalls, oder
  - ein Einsatz des sog. „Mobile Incident Response Teams" (MIRT) des BSI.

  Sobald ein Haus erkennt, dass es den Cyber-Vorfall nicht oder nur eingeschränkt allein bewältigen kann, kann es im ersten Schritt eine grundsätzliche Unterstützungsanfrage beim BSI stellen.

  Als sog. „Single Point Of Contact" (SPOC) fungiert hier die Meldestelle der „Allianz für Cyber-Sicherheit" (ACS). Von dort wird dann an das Lagezentrum bzw. das CERT im BSI eskaliert und geprüft, in welcher Form die Unterstützung erfolgen kann/muss bzw. sinnvoll ist.

Informationen zur Aufgabe der Meldestelle der ACS, sowie zur Kontaktaufnahme finden Sie auf der Website der ACS (www.allianz-fuer-cyber-sicherheit.de <http://www.allianz-fuer-cyber-sicherheit.de>) unter dem Menüpunkt „Meldestelle"
(Deep-Link: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/meldestelle.html)

- Bestehende Unterstützungsangebote, Handlungsempfehlungen und Kontaktstellen transparent machen (LKA, BSI, Datenschutzaufsicht); sowohl der Branchenarbeitskreis (BAK) "Medizinische Versorgung" des UP KRITIS, die staatlichen Datenschutzbeauftragten als auch der "Arbeitskreis IT-Sicherheit" des Deutsche Hochschulmedizin e.V. (für Universitätskliniken) haben bereits krankenhausspezifische Handlungsempfehlungen verfasst.

- Das MSAGD setzt sich dafür ein, im Rahmen des Krankenhausstrukturfonds Maßnahmen zur Verbesserung der IT-Sicherheit für „KRITIS-Krankenhäuser" in Rheinland-Pfalz finanziell zu fördern. Darüber hinaus wird an der Forderung festgehalten, über eine bundesgesetzliche Änderung zukünftig auch kleineren Krankenhäuser mit weniger als 30.000 Fällen eine Strukturfondsförderung für Maßnahmen im Bereich der IT-Sicherheit grundsätzlich zu ermöglichen.

Empfehlungen an die Krankenhäuser

- Mitgliedschaft der Krankenhäuser in der Allianz für Cyber-Sicherheit beim BSI (kostenfrei): Teilnehmer erhalten Zugriff auf erweiterte Informationen zur Cyber-Sicherheitslage, Warnmeldungen, Fortbildungsangebote und Workshops sowie weitergehenden Hintergrundinformationen,

- KRITIS-Betreiber können und sollten Mitglied des UP KRITIS des BSI werden und am Informationsaustausch sowie an Branchenarbeitskreisen teilnehmen (kostenfrei),

- Sensibilisierung der Mitarbeiter für die Gefahren und Abwehrmöglichkeiten u.a. im Rahmen regelmäßiger Schulungen,

- Interne Verfahrensanweisungen etablieren zum Umgang mit auffälligen Vorfällen (e-mails etc.) und Transparenz über interne Meldewege u.a. im Wege von Mitarbeiterschulungen,

- IT-Sicherheit als Management- und Führungsaufgabe: Etablierung zentraler (ggf. externer) IT-Sicherheits- und Datenschutzbeauftragter und eines Informationssicherheits- und Datenschutzmanagementsystems,

- Orientierung am branchenspezifischen Sicherheitsstandard B3S, ISO27.001 oder BSI Grundschutz,

- Technische Vorkehrungen (u.a. Next-Generation-Firewalls) zur Analyse der internen Netzwerkkommunikation zwecks Angriffserkennung und –vermeidung,

- Umsetzung von Maßnahmen, die einen schnellen Wiederanlauf von IT-Systemen zur Patientenversorgung ermöglichen.