Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

KRITIS-Sektor Gesundheit: Informationssicherheit in der stationären medizinischen Versorgung – Rahmenbedingungen, Status Quo, Handlungsfelder

Ergebnisse einer qualitativen Studie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: https://www.bsi.bund.de

Inhalt

Tabellenverzeichnis

1 Vorbemerkungen

Krankenhäuser und viele andere Einrichtungen des Gesundheitswesens tragen in mehrfacher Hinsicht eine besondere Verantwortung für ihre IT-Netze. Der Schutz sensibler Patientendaten muss ebenso zuverlässig gewährleistet sein wie die Versorgung von Patientinnen und Patienten mit Unterstützung modernster Computertechnologie. Öffentlich bekannt gewordene IT-Sicherheitsvorfälle zeigen, dass medizinische Einrichtungen gezielt und ungezielt Opfer eines Cyber-Angriffs werden können.

Nicht zuletzt aufgrund der zunehmenden Digitalisierung im Bereich der medizinischen Versorgung stehen vor allem Krankenhäuser vermehrt vor großen Herausforderungen im Hinblick auf die Absicherung ihrer IT-Systeme, -Prozesse und -Komponenten. Eine Vielzahl von Krankenhäusern fallen schon heute unter die Anforderungen aus dem BSI-Gesetz (BSIG) sowie der Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) und haben dem Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits einen ersten Nachweis über die Umsetzung von technischen und organisatorischen IT Sicherheitsmaßnahmen nach dem Stand der Technik erbracht. Doch auch für Krankenhäuser unterhalb des Schwellenwertes aus der BSI-KritisV rückt IT-Sicherheit immer stärker in den Fokus. In diesem Zusammenhang wird es auch zukünftig zwingend notwendig sein, dass Krankenhäuser als Kritische Infrastrukturen verstärkt den Prozess ihrer kritischen Dienstleistung analysieren, um diesen durch die Umsetzung von IT-Sicherheitsmaßnahmen bestmöglich schützen zu können.

Vor diesem Hintergrund hat das BSI die „Studie zur kritischen Dienstleistung: Stationäre medizinische Versorgung“ in Auftrag gegeben. Diese qualitative Studie wurde durch Goldmedia GmbH Strategy Consulting durchgeführt. Sie analysiert im KRITIS-Sektor Gesundheit die kritischen Dienstleistungen im Rahmen der stationären medizinischen Versorgung exklusive der damit verbundenen Labordienstleistungen. Auf Basis strukturierter Interviews mit IT-Verantwortlichen von Krankenhäusern und Kliniken wurden insbesondere die Darstellungen der Prozesse, wie sie in der Vorgängerstudie „KRITIS Sektorstudie Gesundheit“ des BSI ermittelt wurden, validiert, die Kritikalität der Aufgaben und Vorgänge eingestuft sowie der Stand der Technik in Bezug auf die IT-Sicherheit der Krankenhäuser evaluiert. Die Studie ist dabei in Teilen als Kompendium angelegt, mit dem Auswirkungen technischer Störungen oder Ausfälle in Krankenhäusern bewertet werden können. Die Studie ist als Verschlusssache[1] eingestuft und daher nicht öffentlich zugänglich.

Die hier vorliegende Publikation fasst die wesentlichen Ergebnisse der Studie zusammen und betrachtet insbesondere den Status quo der Informationssicherheit in Krankenhäusern. Neben Handlungsempfehlungen zur Erhöhung des Schutzniveaus erfolgt ein Ausblick zur Zukunft der IT Durchdringung und -Entwicklung innerhalb der stationären medizinischen Versorgung.

[1] VS–NUR FÜR DEN DIENSTGEBRAUCH

2 Rahmenbedingungen

2.1 Marktstrukturen

Die Grundstruktur der deutschen Gesundheitsversorgung basiert auf den Säulen Primärversorgung (ambulante Behandlung), Akutversorgung (stationäre Behandlung in Krankenhäusern), Rehabilitation und Prävention. In den Bereich der Primärversorgung fallen akute und routinemäßige ambulante Behandlungen und Untersuchungen durch (niedergelassene) Haus- und Fachärzte in Arztpraxen, Polikliniken, medizinischen Versorgungszentren bzw. in ambulanten Krankenhauseinheiten. Auch die Notfallbehandlung in Krankenhäusern zählt zur Primärversorgung. In der Akutversorgung werden die Patientinnen und Patienten in einem Krankenhaus stationär untergebracht, verpflegt und medizinisch behandelt. Medizinische Leistungen sind nur dann unter stationären Bedingungen zu erbringen, sofern eine ambulante Versorgung nicht möglich erscheint.

Statistische Daten zur Krankenhausversorgung

Nach Angaben des statistischen Bundesamtes stehen in Deutschland ca. 1.900 Krankenhäuser mit knapp 500.000 Betten zur Verfügung. Die Zahl großer Kliniken mit 600 und mehr Betten belief sich im Jahr 2017 auf 175. Pro Jahr werden etwa 19,5 Mio. Fälle behandelt. Rund 29 % der Krankenhäuser befinden sich in öffentlicher Trägerschaft, 34 % werden von Kirchengemeinden, Stiftungen oder Vereinen unterhalten (sogenannte freigemeinnützige Trägerschaft), 37 % privat betrieben. Da öffentliche Krankenhaushäuser im Schnitt dreimal so groß sind wie private Einrichtungen, stand fast jedes zweite Bett (48,0 %) in einem öffentlichen Krankenhaus. (Destatis, 2017)

Krankenhausplanung ist Ländersache

Die stationäre medizinische Versorgung durch Krankenhäuser ist in Deutschland grundsätzlich im Sozialgesetzbuch V (SGB V) geregelt. Die Planung von Krankenhäusern und die damit einhergehende Festsetzung stationärer Kapazitäten sowie die verschiedenen Leistungsangebote und die Sicherstellung der Notfallversorgung obliegt dabei den Bundesländern und wird von den Landesgesundheitsministerien verantwortet. Das Bundesgesetz zur wirtschaftlichen Sicherung der Krankenhäuser, das sogenannte Krankenhausfinanzierungsgesetz (KHG) sowie die Krankenhausgesetze der Länder bilden hierzu die gesetzliche Grundlage.

2.2 Regulatorische Anforderungen

Krankenhäuser unterliegen einer Vielzahl regulatorischer Anforderungen. Sie reichen von der Qualität der Leistungserbringung über den sicheren Betrieb von Medizintechnik bis hin zu Anforderungen an die IT-Sicherheit.

Anforderungen an die Qualität

Die Qualitätsanforderungen an die Leistungserbringung ergeben sich in erster Linie aus dem Patientenrechtegesetz, das Krankenhäuser zu einem Risiko- und Qualitätsmanagement verpflichtet, sowie aus der Medizinprodukteverordnung oder dem Medizinproduktegesetz. Daneben gibt es zahlreiche weitere Regelungen, die sich auf die Qualität der Leistungen beziehen wie Sozialgesetzbuch (SGB) oder Industrienormierungen. Dabei werden die Anforderungen an die Qualität der Leistungserbringung innerhalb der stationären medizinischen Versorgung durch den vom Gesetzgeber beauftragten Gemeinsamen Bundesausschuss (G-BA) verantwortet. Zu den zentralen Aufgaben des G-BA innerhalb der Qualitätssicherung zählen bspw. das Festlegen von Grundelementen, die das Qualitätsmanagement von Dienstleistern in der medizinischen Versorgung aufweisen muss. Hierbei legt der G-BA für die verschiedenen Fachabteilungen in Form von Richtlinien fest, welche Anforderungen im Bereich der medizinischen Dienstleistungen zur Durchführung von Eingriffen in diesem Fachbereich erfüllt werden

müssen. Dies betrifft u.a. die räumliche und technische Ausstattung (z.B. OP-Räume), die Qualifikation der Beschäftigten (Strukturqualität) sowie der organisatorischen Abläufe und zeitlichen Vorgaben von der Aufnahme und Diagnose bis zur Durchführung des Eingriffs (Prozessqualität). Einrichtungen im Gesundheitswesen sind durch das SGB V verpflichtet, ein Qualitätsmanagement einzuführen und dieses auch nachzuweisen.

Anforderungen an die Medizintechnik

Die Anforderungen an medizintechnische Systeme bilden sich mittels der Medizinprodukteverordnung und zugehöriger Verordnungen in Bezug auf die Verarbeitung, Inbetriebnahme, den Betrieb und die Anwendung sowie die Kontrolle von Medizinprodukten ab. Im Wesentlichen betrifft dies die Regelungen der EU-Medizinprodukteverordnung (Medical Device Regulation - MDR), das deutsche Medizinproduktegesetz (MPG), die Medizinprodukte-Sicherheitsplanverordnung (MPSV) sowie die Medizinprodukte-Betreiberverordnung (MPBetreibV). Letztlich besteht das Ziel dieser Gesetze und Verordnungen in der Reglementierung des Handels und des Einsatzes von Medizintechnik zur Abwendung bzw. Minderung von Gefahren für Patienten und Patientinnen, Anwendern und Dritten. Die MDR wird dabei nicht mehr in nationales Recht überführt, sondern trat 2017 unmittelbar in Kraft.

Anforderungen an Krankenhäuser als Betreiber einer Kritischen Infrastruktur im Sinne des BSIG

Der KRITIS-Sektor Gesundheit ist von zentraler Bedeutung für das Funktionieren des Gemeinwesens und gehört deshalb zur Kritischen Infrastruktur. Bisher sind kritische Dienstleistungen in der stationären medizinischen Versorgung sowie in der Versorgung mit Arzneimitteln, Blut- und Plasmakonzentraten sowie lebenserhaltenden Medizinprodukten und die Laboratoriumsdiagnostik über das BSI-Gesetz (BSIG) reguliert, wenn die jeweiligen Anlagen die derzeit gültigen Schwellenwerte gemäß BSI-KRITIS-Verordnung (BSI-KritisV) erreichen oder überschreiten. Aktuell erreichen rund zehn Prozent der Krankenhäuser in Deutschland den Schwellenwert von 30.000 vollstationären Fällen pro Jahr und sind beim BSI als Betreiber Kritischer Infrastrukturen registriert.

Das BSIG verpflichtet die regulierten KRITIS-Betreiber, angemessene technische und organisatorische IT-Sicherheitsmaßnahmen nach dem „Stand der Technik“ umzusetzen und diese dem BSI alle zwei Jahre nachzuweisen. Dies erfolgt nach erfolgreicher Registrierung als Betreiber einer Kritischen Infrastruktur beim BSI und der Benennung einer Kontaktstelle. Das BSIG verfolgt das Ziel, Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Prozesse, Systeme und Komponenten zu vermeiden und die kritische Dienstleistung, in diesem Fall die stationäre medizinische Versorgung, aufrecht zu erhalten. Die Nachweiserbringung über die Umsetzung von IT-Sicherheitsmaßnahmen erfolgt üblicherweise in Zusammenarbeit mit einer geeigneten externen Prüfstelle. Der Betreiber übermittelt die Ergebnisse nach erfolgreicher Durchführung fristgerecht an das BSI. Das BSI wurde im Zuge des BSIG dazu ermächtigt, die Beseitigung von vorliegenden Sicherheitsmängeln bei Betreibern zu veranlassen und dies bei Nichterfüllung mit einem Bußgeld zu ahnden. Die regulierten KRITIS-Betreiber sind zudem durch das BSIG dazu verpflichtet, Störungen, welche die kritische Dienstleistung erheblich beeinträchtigen oder beeinträchtigen können, unverzüglich dem BSI zu melden.

Für eine zielgerichtete Umsetzung der IT-Sicherheitsanforderungen aus dem BSIG wurde innerhalb der Branche ein branchenspezifischer Sicherheitsstandard (B3S) erstellt, der von den KRITIS-Betreibern als Prüfgrundlage für die Nachweisprüfung nach § 8a BSIG verwendet werden kann. Es können aber auch Krankenhäuser, die nicht durch das BSIG reguliert werden, vom B3S profitieren und durch die Umsetzung der Anforderungen ihr IT-Sicherheitsniveau deutlich verbessern.

3 Informationssicherheit in der stationären medizinischen Versorgung

3.1 Besonderheit: Kritische Dienstleistung

Die meisten Prozesse in einem Krankenhaus sind heute ohne IT-Unterstützung nicht mehr vorstellbar. Außerdem verlieren Medizingeräte zunehmend ihre ursprüngliche Eigenschaft als Spezialgerät und werden durch IT-Systeme bzw. –Komponenten mit medizinischer Verwendbarkeit ersetzt. Die Informationsverarbeitung muss ebenso zuverlässig funktionieren wie die zugehörige Technik, damit der Betrieb aufrechterhalten werden kann. Zugleich stellt die dynamische Cyber-Bedrohungslage neue Anforderungen an die Informationssicherheit. Um die Funktionsfähigkeit der betriebenen Kritischen Infrastruktur zu erhalten, muss jedes Krankenhaus daher ein individuelles und auf seine Anforderungen abgestimmtes Sicherheitskonzept erstellen, umsetzen und stetig überprüfen.

Erfahrungen aus der Praxis zeigen, dass es besonders zielführend ist, dabei den Fokus auf die kritische Dienstleistung (kDL) der stationären medizinischen Versorgung zu legen. Ausgehend von den relevanten Prozessen sowie den daraus resultierenden wechselseitigen IT-Abhängigkeiten lassen sich die Kritikalität der Aufgaben und Vorgänge einstufen sowie der Stand der Technik in Bezug auf die IT-Sicherheit evaluieren.

Prozesse und Aufgaben im Krankenhaus

Aus den Funktionsbereichen und Funktionsstellen sowie den Fach- und Funktionsabteilungen eines Krankenhauses ergeben sich in Anlehnung an die KRITIS-Sektorstudie Gesundheit des BSI aus dem Jahr 2016 die einzelnen Prozessschritte der kritischen Dienstleistung. Die primäre Versorgungsdienstleistung gliedert sich somit in fünf aufeinanderfolgende Prozessschritte auf, die jeweils wieder in Aufgaben und Vorgänge unterteilt sind.

Den ersten Prozessschritt stellt die **Aufnahme** von Patienten bzw. Patientinnen dar. Dieser Prozessteil umfasst vor allem organisatorisch-logistische Aufgaben. Die Notfallaufnahme zur Akutversorgung erlangt hier eine besondere Relevanz. Im Prozessschritt der **Diagnose** bestehen die Aufgaben in der Feststellung bzw. Bestimmung von Krankheiten, der Diagnoseerstellung auf Basis von Untersuchungen, Laboruntersuchungen sowie der Therapieplanerstellung und Medikation. Daran anknüpfend erstreckt sich der Prozessschritt der **Therapie**. Dieser untergliedert sich in Aufgaben mit verschiedenen interventionellen Behandlungsmethoden wie der medikamentösen und manuell-physikalischen Heilmethoden, gerätebasierter Heilmethoden sowie in der Bereitstellung von Medikamenten und Hilfsmitteln. Der nächste Prozessschritt umfasst die **Pflege**. Hier ist jedoch zu beachten, dass in der Realität die Pflege parallel und fortlaufend von der Aufnahme bis zur Entlassung des Patienten bzw. der Patientin erfolgt. Mit der **Entlassung** als finalem Prozessschritt erfolgt die Übergabe an eine andere Einrichtung.

Tabelle 1 Relevante Teilprozesse und Aufgaben der kritischen Dienstleistung medizinische Versorgung (BSI, 2016)

Prozessschritt	Aufgabe (Arbeitsschritte gem. Sektorstudie 2016)
Aufnahme des Patienten	Notfallaufnahme
	Aufnahme des Patienten
Diagnostik	Anamnese und Stellung von Verdachtsdiagnose(n)
	Diagnosestellung aufgrund von Funktionsdiagnostik
	Diagnosestellung aufgrund von Untersuchungen mit bildgebenden Verfahren
	Durchführung von Laboruntersuchungen

Prozessschritt	Aufgabe (Arbeitsschritte gem. Sektorstudie 2016)
	Erstellung eines Therapieplans & Verordnungen von Arznei-, Heil-, und Hilfsmitteln
Therapie	Anwendungen von Operationsverfahren (inkl. Sterilgutversorgung)
	Anwendungen von medikamentöser, physikalischer, manueller Heilmethoden
	Anwendung gerätebasierter Heilmethoden, Einsatz von lebenserhaltenden Technologien, Intensivstation
	Bereitstellung von Arznei- und Hilfsmitteln (inkl. Arzneimittel, Materialwirtschaft / Medikalprodukte
Pflege	Durchführung von pflegerischen Maßnahmen
	Sicherstellung Versorgung / Verpflegung / Hygiene (inkl. Reinigungsdienst)
Entlassung	Erstellung des Arztbriefes mit Medikationsliste, ggf. anschließende Therapieplanung
	Entlassung des Patienten und Erläuterungen / Sicherstellung der Medikamentenversorgung
	Sicherstellung der poststationären Versorgung, Kurzzeitpflege, etc.

3.2 IT-sicherheitsrelevante Herausforderungen

Das Schaffen der notwendigen Grundlagen für die Informationssicherheit stellt sowohl die regulierten KRITIS-Betreiber als auch andere Krankenhäuser nicht selten vor große Herausforderungen, die sich aus dem Klinikalltag und der besonderen (Infra-)Struktur ergeben. Der soziale Aspekt des medizinischen Berufes dominiert die Einstellung zur Arbeit: Der Patient bzw. die Patientin steht im Mittelpunkt – und das rund um die Uhr.

Sicherheitskultur im Krankenhaus

Bislang fehlt es in vielen Krankenhausorganisationen an einer IT-spezifischen Sicherheitskultur. Die Sicherheitskultur eines Krankenhauses ist vorrangig vom Bemühen um eine fehler- und schadensfreie medizinische Behandlung und Versorgung gekennzeichnet. Geprägt wird diese Sichtweise vor allem durch die Medizinethik, das Patientenrechtegesetz und durch Maßnahmen, wie der Einführung eines patientenorientierten Beschwerdemanagements, eines Qualitätsmanagements mit sachgerechtem Risiko- und Fehlermanagement sowie von Fehlermeldesystemen wie dem „Critical Incident Reporting System“ (CIRS).

Prinzipiell wird der schnelle Zugriff auf Patientendaten als wesentlich wichtiger beurteilt, als die Sicherheit des Zugangs zu Daten von IT-Anwendungen oder medizinischen Geräten, da der Informationszugriff allzu oft im Kontext der Behandlung erfolgt und in kritischen Situationen Zeitverluste durch Anmeldevorgänge oft nicht hinnehmbar sind.

Vermittlung und Umsetzung von Compliance-Vorgaben

Der Umstand von häufig wechselndem Personal aufgrund von Schichtwechsel, Teilzeitarbeit, Leiharbeit oder durch Belegärzte kompliziert die Sensibilisierung der Beschäftigten im Bereich IT-Sicherheit. Die Aus- und Weiterbildung von Medizinern und Pflegekräften erfolgt bislang ohne wesentliche Berücksichtigung

der digitalen Veränderung des Berufsbilds. Daneben erwecken stark regulierte Bereiche wie die Medizintechnik den Eindruck, dass Risiken weitestgehend ausgelagert sind, d. h. IT-Sicherheitsanforderungen implizit über die Geräte geregelt werden und es keiner organisationalen Einbindung mehr bedarf.

Auch wenn die Beschäftigten bereits in erheblichem Umfang medizinische Pflichtunterweisungen und Fortbildungen wahrnehmen müssen, wie zum Beispiel Einweisungen an Medizintechnik-Systemen sowie Fortbildungen in den Bereichen Hygiene, Abrechnungssysteme und Datenschutz, so existieren jedoch kaum Präsenzveranstaltungen oder elektronische Lernmedien bzw. Online-Seminare zum Thema IT-Sicherheit, die krankenhausspezifisch aufbereitet sind. Die hierfür notwendige Zeit bleibt in der Ressourcenplanung der Belegschaft häufig unberücksichtigt. Jede weitere Aufgabe wird als „Last" daher gegen die Aufrechterhaltung des Kerngeschäfts abgewogen.

Nutzung und Bereitstellung von Informations- und Medizintechnik

Die IT-Infrastruktur in Krankenhäusern ist nur selten systematisch und gleichmäßig mit den technischen Anforderungen und den mit ihr verbundenen IT-Sicherheitsaspekten gewachsen. Kliniken verfügen in der Regel über eine Vielzahl von IT-Anschlüssen, 30.000 Endgeräte sind keine Seltenheit. Durch Digitalisierungsprojekte kommen zahlreiche vernetzbare IT- und Medizingeräte hinzu bei gleichzeitiger Nutzung von (nicht mehr gepflegten) Altsystemen. Die Anforderungen, die sich aus dem Krankenhausbetrieb aufgrund des 24/7-Betriebs an die Verfügbarkeit der IT-Systeme selbst ableiten, schlagen sich nicht nur auf die Wartungsintervalle nieder, sondern auch auf die Nutzung der IT-Systeme durch das medizinische Personal. So wird das „ständige An- bzw. Ummelden" an IT-Systemen teilweise als zeitraubend und im Alltag als nicht praxistauglich empfunden, vor allem bei zeitkritischen Diagnosen und Behandlungen. Zudem sind Krankenhäuser in der Regel offene Einrichtungen, Zutrittsbeschränkungen lassen sich höchstens für den OP- oder Verwaltungsbereich realisieren.

Finanzielle Ressourcen

Auch finanzielle Aspekte spielen eine Rolle. Insbesondere bei den 1.800 öffentlichen, frei-gemeinnützigen und privaten Krankenhäusern in Deutschland, die nicht unter die KRITIS-Regulierung fallen, fehlen häufig finanzielle Mittel, um die notwendigen strukturellen Grundlagen für IT-Sicherheit zu schaffen. Dies betrifft gleichermaßen Investitionen in Hard- und Software, die Durchführung von Schulungen wie den personellen Aufwand zur Dokumentation, Überprüfung, Auditierung und kontinuierlichen Weiterentwicklung der Compliance-Regelungen.

Insgesamt machen die Rahmenbedingungen deutlich, dass die Krankenhäuser im Hinblick auf die Umsetzung von organisatorischen und technischen IT-Sicherheitsanforderungen besonderen Herausforderungen gegenüberstehen. Denn sie müssen letztlich einen Spagat meistern, indem sie auf der einen Seite die Anforderungen an die IT-Sicherheit umsetzen, ohne dass es auf der anderen Seite zu spürbaren Beeinträchtigungen des operativen medizinischen Betriebs kommt. Das alles lässt sich nur mit Hilfe eines etablierten, systematischen Vorgehens in moderne IT-Sicherheitsvorhaben integrieren.

3.3 Status Quo – Ergebnisse der Betreiberbefragungen

Insgesamt zeigt sich bei der Umsetzung der Informationssicherheitsmaßnahmen, dass die Betreiber ihren Fokus primär auf die Umsetzung von technischen Maßnahmen zum Schutz ihrer kritischen Dienstleistung (kDL) gelegt haben. So sind relevante IT-Systeme und Komponenten zur Erbringung der kDL in der Regel redundant ausgelegt und durch klassische Abwehrmaßnahmen (z.B. Firewall, DMZ, zentraler SPAM- und Malware-Schutz, Routing, VPN/https, dezentrale Malware-Scanner) zum Schutz vor Angriffen sowie Schadsoftware technisch umgesetzt. Dennoch ergibt sich bei der Umsetzung von organisatorischen, wie auch einzelnen technischen IT-Sicherheitsmaßnahmen noch Verbesserungspotenzial.

Organisatorische Maßnahmen

Grundsätzlich wurde im Rahmen der Betreiberbefragungen festgestellt, dass sich ein systematisches IT-Risikomanagement in vielen Häusern noch nicht auf dem notwendigen Niveau bewegt. So werden IT-Sicherheitsmaßnahmen nur teilweise risikoorientiert geplant. In Bezug auf die IT-Risiken besteht bislang lediglich eine unvollständige Bedrohungsanalyse (auch unter Ausklammerung von Medizin- und Versorgungstechnik), mit der Folge, dass zumeist vor- oder nachgelagerte Prozesse eine zu geringe Berücksichtigung in der Risikoanalyse finden.

Schutzkonzepte und Compliance-Regelungen werden oftmals nur unvollständig entwickelt und eine darauf aufbauende Schulung findet häufig nicht im erforderlichen Umfang statt. IT-basierte Schulungen beschränken sich zudem in der Regel auf Datenschutz-Themen. Darüberhinausgehende Einübung von Bewältigungsmaßnahmen im Rahmen eines Notfallmanagements (bspw. für manuelle Ersatzverfahren, die bei einem stunden- oder tageweisen Serverausfalls angewendet werden müssten) finden kaum statt.

Systematische Zugangskontrollen für Besucherinnen und Besucher sind im Krankenhaus weiterhin eine Ausnahme. Schließsysteme mit elektronischen Ausweisen, die die Stationen vor unberechtigten Zugang schützen, existieren allenfalls bei besonders kritischen Abteilungen (Intensiv, Psychiatrie).

Technische Maßnahmen

Besonders bei der Umsetzung technischer Schutzmaßnahmen, die eine aktive Mitwirkung der Beschäftigten erfordern, kommt es vereinzelt noch zu Akzeptanzproblemen. Dies betrifft neben der Verschlüsselung mobiler Speichermedien vor allem die Verschlüsselung von E-Mails.

Eine (virtuelle) Netztrennung und Netzsegmentierung in Medizintechnik-Netz, Verwaltungsnetz, Applikationsnetz und Patienten-/Gästenetz ist oftmals noch nicht vollständig vollzogen. Es zeigt sich zudem, dass die Krankenhäuser häufig keine Tests- und Freigabeprozesse für neue Softwaresysteme oder Gerätetechnik durchführen. Darüber hinaus erfolgen Maßnahmen im Patch- und Änderungsmanagement immer wieder verzögert. Weitere Einschränkungen ergeben sich auch durch Restriktionen der Speichersysteme. Aufgrund der immer stärker zunehmenden Datenmengen kommt es schon jetzt zu Kapazitätsengpässen. Dieser Trend wird mittelfristig weiter zunehmen.

Maßnahmen zur Detektion und Reaktion wird bisher nur ein geringer Stellenwert eingeräumt. Dies gilt z.B. für das Netzwerkmonitoring (bei der eine Logfile-Analyse weder kontinuierlich noch zentral durchgeführt wird), aber auch für das (wenig genutzte) zentralisierte Scannen von E-Mails zum Mal-ware- oder Phishing-Schutz.

4 Handlungsfelder

4.1 Empfehlungen

Um das IT-Sicherheitsniveau in Krankenhäusern langfristig erfolgreich steigern zu können, bedarf es eines ganzheitlichen Ansatzes. Entscheidend ist dabei die Prozessanalyse der stationären Patientenversorgung. Die fünf aufeinander folgenden Teilprozesse mit ihren Aufgaben und Vorgängen dienen damit als Richtschnur für eine systematische Planung und Umsetzung von zielgerichteten technischen und organisatorischen IT-Sicherheitsmaßnahmen.

Managementsystem für Informationssicherheit systematisieren

Der Aufbau und Betrieb eines Informationssicherheitsmanagementsystems (ISMS) sowie dessen kontinuierliche Weiterentwicklung ist von entscheidender Relevanz für das Erreichen eines angemessenen IT-Sicherheitsniveaus. Das ISMS stellt mit seinen Richtlinien und Methoden eine Art Grundpfeiler hierfür dar. Ein ausgereiftes ISMS hilft dabei nicht nur bei der Sensibilisierung der Beschäftigten im Hinblick auf die Umsetzung von IT-Sicherheitsanforderungen, sondern signalisiert diesen ebenfalls, dass die Leitungsebene hinter den Sicherheitszielen steht und sich ihrer Verantwortung im Umgang mit Informationssicherheit bewusst ist. Ziel des ISMS muss es sein, dass die darin enthaltenen Richtlinien eng mit den technisch umgesetzten IT-Sicherheitsmaßnahmen abgestimmt sind. Durch die enthaltene Vorgabe in einer Richtlinie wird die technische Umsetzung einer IT-Sicherheitsmaßnahme sprichwörtlich von jener ummantelt.

IT-Risiken erkennen und managen

Im ISMS sollten neben Richtlinien zur technischen Umsetzung von IT-Sicherheitsmaßnahmen ebenso Rahmenbedingungen zum IT-Risikomanagement für Systeme und Komponenten der kDL festgelegt werden. Auch hier bietet die Prozessanalyse den Ausgangspunkt für die Risikobetrachtung. In der Praxis bedeutet dies, dass für jeden Vorgang einer Aufgabe im Prozessschritt diejenigen IT-Systeme und Komponenten analysiert werden müssen, die für den jeweiligen Vorgang der stationären Patientenversorgung maßgeblich sind. Daraus leiten sich letztlich die Verfügbarkeitsanforderungen an die einzelnen IT-Systeme und Komponenten ab, mit dem Ergebnis, dass sich diese schnell und einfach als kritische IT-Systeme und Komponenten der kDL identifizieren lassen. Im Anschluss daran kann eine vollständige Bedrohungsanalyse erfolgen, der Schutzbedarf festgelegt sowie passende technische und organisatorische IT-Sicherheitsmaßnahmen identifiziert und umgesetzt werden. Abschließend ist darauf aufbauend das IT-Notfallmanagement zu entwickeln.

IT-Notfallmanagement erweitern

Das IT-Risikomanagement und das IT-Notfallmanagement für IT-Systeme und Komponenten der kDL sollten eng miteinander verzahnt sein. Das bedeutet für die Sicherstellung der kDL, dass nicht nur IT-Systeme, sondern vor allem auch Komponenten der vernetzten Medizin- und Versorgungstechnik in die Betrachtung mit einbezogen werden müssen. Damit soll gemeint sein, dass neben Ausfällen von IT-Systemen, wie etwa dem Krankenhausinformationssystem (KIS), nicht nur auf manuelle Ersatzverfahren zurückgegriffen werden kann. Es müssen im Zuge einer ganzheitlichen Betrachtung und Absicherung der kDL bspw. auch Notfallpläne für Ausfälle oder Störungen an Dampfsterilisatoren in der Sterilgutaufbereitung oder Störungen des Kommissionierautomats in der Krankenhausapotheke vorhanden sein.

KRITIS-Sichtweise in der Organisation etablieren

Bei der Umsetzung von organisatorischen IT-Sicherheitsmaßnahmen sollte das Thema KRITIS noch stärker in den gesamtorganisationalen Kontext eingebettet werden. Dabei ist das IT-Risikomanagement der für die kDL notwendigen IT-Systeme und Komponenten stärker an das bereits vorhandene klinische Risikomanagement einzubinden. Dies hat den Vorteil, dass IT-Sicherheitsmaßnahmen risikoorientierter

geplant werden können und die Geschäftsführung in regelmäßigen Abständen über IT-Sicherheitsrisiken informiert wird.

Bei bereichsübergreifenden Prozessen IT-Anforderungen berücksichtigen

Darüber hinaus sollten übergreifende Prozesse zwischen einzelnen Bereichen im Krankenhaus enger miteinander abgestimmt werden, so dass zukünftig die IT-Abteilung bei der Anschaffung neuer Hard- bzw. Software einzelner Bereiche stärker mit eingebunden wird. Speziell bei der Einbindung von Medizintechnik-Systemen ins IT-Netz ergeben sich oftmals IT-Anforderungen, der einen größeren zeitlichen Puffer erfordern. Je größer die Vorlaufzeit für die IT-Abteilung ist, desto besser kann auf Schwachstellen im Hinblick auf die zu treffenden IT-Sicherheitsvorkehrungen wie Netzsegmentierung, Firewall-Freischaltungen, Verzeichnisdienst-Abgleiche bzw. Authentifizierungs- und Autorisierungstechniken reagiert werden. Schlussendlich können dadurch die IT-Systeme und vernetzten Medizingeräte sicherer in die bestehende IT-Infrastruktur eingebunden werden.

Netztrennung bzw. -segmentierung konsequent umsetzen

Die Wertschöpfung in der medizinischen Versorgung erfolgt zunehmend durch die Erhebung und Verknüpfung zahlreicher (Gesundheits-)Daten eines Patienten bzw. einer Patientin. Daraus resultiert eine gestiegene und weiterhin steigende Notwendigkeit der Vernetzung medizinisch genutzter Systeme (Diagnose, Therapie, Forschung), die sich in IT-Netzen unterschiedlichen Schutzbedarfs und unterschiedlicher Schutzmöglichkeiten befinden. Damit kommen einer ausgereiften IT-Netzinfrastruktur sowie ausreichend großen Speicherkapazitäten besondere Bedeutung zu. Dies betrifft sowohl die Anbindung über Kabel als auch die klinikweite Verfügbarkeit einer kabellosen Netzanbindung. Demzufolge bedarf es einer stringenten Netztrennung bzw. Netzsegmentierung. Einzelne Netzsegmente wie das Patientennetz (Klinik-Netz) sowie Netze der Medizintechnik sind von anderen Netzen wie dem Verwaltungsnetz, Alarmierungsnetz oder Gästenetz bestmöglich mit Hilfe klar definierter Routing-Regeln zu trennen, um dadurch den Schutz vor unberechtigtem Zugriff zu erhöhen, bzw. die netzübergreifende Ausbreitung von Schadsoftware einzudämmen. Prinzipiell sollten netzübergreifende Zugriffe ebenso wie Fernzugriffe protokolliert werden. Beim Aufbau von VPN-Verbindungen ist darauf zu achten, dass zum einen nur sichere Protokolle zum Einsatz kommen und zum anderen nur Dienste freigegeben werden, die auch tatsächlich benötigt werden.

Medizintechnik sicher einbinden

Für die Verbindung medizinischer mit nicht-medizinischen IT-Netzen sind besondere Regeln an den Übergabepunkten notwendig, die mit Hilfe von eigenen Routern, Switches und Firewalls zum Schutz der Medizintechnik-Vernetzung umgesetzt werden. Gleichzeitig kann dadurch auch der Schutz der Standard-IT-Umgebung gewährleistet werden, da Schadsoftware sich in der Regel bidirektional auswirken kann und der Ausgangspunkt sowohl die Medizintechnik, als auch die Standard-IT sein kann. In diesem Zusammenhang ist neben der Trennung verschiedener Mandanten ebenfalls die Trennung von Gerätegruppen und die Kontrolle der Kommunikation durch den Einsatz von Firewall-Techniken entscheidend.

IT-Sicherheitsarchitektur weiterentwickeln

Daran anknüpfend liegen neben der redundanten Auslegung von IT-Systemen und Komponenten der kDL sowie Backup-Systemen weitere Erfolgsfaktoren einer ausgereiften IT-Sicherheitsarchitektur in der technischen Absicherung der IT-Infrastruktur durch Firewalls und Anti-Viren-Schutzlösungen. Dabei gilt es, genau zu analysieren, welche eingehenden und ausgehenden Verbindungen tatsächlich benötigt werden, um diese dann dediziert freizuschalten. Bei den Anti-Viren-Schutzlösungen ist darauf zu achten, dass vorhandene Signaturen zeitnah eingespielt werden. Dies gilt allgemein auch für das Einspielen von Patches. Nur so kann zeitnah auf aktuelle Bedrohungen und Schwachstellen reagiert werden. Auch die Perimeter-Absicherung hat einen wesentlichen Einfluss auf die IT-Sicherheitsarchitektur im Krankenhaus. So können bspw. E-Mails mit schadhaften Anhängen, Spam- oder Phishing-Angriffe schon frühzeitig über das Mail-Security-Gateway gescannt, detektiert und quarantänisiert werden. Letztlich bedingt das

Zusammenspiel technischer und organisatorischer IT-Sicherheitsmaßnahmen den Erfolg der IT-Sicherheitsarchitektur.

4.2 Ausblick

Die (zunehmende) Digitalisierung im Krankenhaus macht deutlich, dass der Erfolgsfaktor für ein hohes IT-Sicherheitsniveau in der ganzheitlichen Betrachtung der kritischen Dienstleistung liegt. Nur wer die kritischen Prozesse, Aufgaben und Vorgänge sowie die eingesetzten IT-Systeme und Komponenten klar identifiziert hat, kann ein angemessenes Schutzniveau erreichen. Das ist auch entscheidend für wesentliche Entwicklungstrends, die auf den Einsatz von IT-Systemen im Krankenhaus zukünftig wirken werden.

Implementierung eines volldigitalen Workflows

Gerade vor dem Hintergrund der zukünftigen Implementierung eines volldigitalen Workflows muss der IT-Sicherheit ein noch höherer Stellenwert beigemessen werden. Das ist insbesondere der Fall, wenn es um die Einführung der digitalen Kurve bzw. der digitalen Pflegedokumentation geht. Die elektronische Patientenakte des Krankenhauses als Bestandteil des KIS umfasst heute primär Vitalwerte (Kurven), An- und Verordnungen für Diagnostik und Therapie sowie die Ergebnis-Befunde der Untersuchungen und Maßnahmen. Die Abrechnungsdaten im Rahmen der Leistungsdokumentation können so aus dem KIS weitgehend elektronisch abgeleitet werden.

Parallel zu bereits teil-automatisierten Prozessen werden in den meisten Krankenhäusern häufig weiterhin papierbasierte Kurven geführt, in denen alle Vitalwerte und ärztliche Anweisungen handschriftlich vermerkt sind und im Rahmen der Visite verwendet werden. In dieser Papierkurve werden auch die Ausdrucke der elektronisch nicht verknüpften Systeme eingelegt. Dies gilt insbesondere für Spezialdokumentationen wie von EKG, CTG oder anderen Überwachungsanlagen. Laborwerte und radiologische Befunde sind dagegen weitgehend elektronisch verfügbar. Das bedeutet jedoch nicht, dass Schnittstellen zum KIS bestehen und diese Werte direkt in die elektronische Akte übernommen werden. Häufig werden elektronische Dokumente genutzt. Die vollständige Pflegedokumentation als Teil der Krankenhauspatientenakte erfolgt ebenfalls in der Mehrzahl der Krankenhäuser noch papierbasiert. Nur ein geringer Anteil der Krankenhäuser verfügt bereits über eine volldigitalisierte Kurven- und Pflegedokumentation mittels elektronischer Visitenwägen und mobiler Arbeitsplätze, die im WLAN agieren. Auch Laborwerte aus dem Laborinformationssystem sollen zukünftig direkt an das KIS angebunden werden.

Dem gegenüber steht oftmals das Bestreben einiger KIS-Hersteller, ihre Systeme in die Cloud zu migrieren. Krankenhäuser, die generell vor der Frage stehen, zukünftig Cloud-Computing zu betreiben, können an dieser Stelle auf den „Anforderungskatalog Cloud Computing (C5)“[2] des BSI zurückgreifen, der konkrete IT-Sicherheitsanforderungen zu Nutzung von Cloud-Diensten beinhaltet. Letztlich stehen die Krankenhäuser bis zur vollständigen Digitalisierung, d.h. die komplette Integration aller datenliefernden Systeme in das KIS und der elektronischen Akte, noch großen Herausforderungen gegenüber, die sowohl technischer als auch finanzieller Natur sind.

Verstärkte Nutzung telemedizinischer Konsile

Weitere Zukunftspotenziale für Krankenhäuser liegen in der Telemedizinischen Behandlung. Aktuell entwickelt sich die Telemedizin innerhalb der Dimensionen „Eingesetzte Technologien“, „Anwendung im Klinikalltag“ und „Anschließend eingesetzte Pflegemodelle“ weiter. Während bisher auf den Einsatz neuer Technologien in etablierten Modellen gesetzt wurde, etwa die Videokonferenz am Krankenbett an Stelle persönlicher Visite, lassen sich nun hybride Modelle beobachten, die die Technologie als Treiber begreifen. Beispiele sind etwa Telerehabilitation eines Patienten zu Hause, die nur mit der Übertragung großer

[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf?__blob=publicationFile&v=2

Datenmengen funktioniert und den Patienten entlasten soll. Gleichzeitig werden bestehende telemedizinische Anwendungen flächendeckender in den Klinikalltag integriert u.a. in der Notfallmedizin oder der Behandlung chronischer Krankheiten. Kabellose Verbindungen ermöglichen zusehends, dass Untersuchungen nicht in der Videokonferenzumgebung, sondern am Point-of-Care, im Heim des Patienten, oder sogar an Unfallstellen stattfindet. Besonders vor dem Hintergrund der wachsenden Datenmengen müssen sich die Systeme der Telemedizin an die Übertragung digitaler Informationen anpassen.

Bei der verstärkten Nutzung von telemedizinischen Lösungen (und telemedizinischen Konsilen) stellt sich die Frage nach potenziellen „Man in the middle"-Angriffen. Auch wenn dies als eher unwahrscheinlich zu betrachten ist, könnten durchaus Verluste vertraulicher Daten zu thematisieren sein. Da sich die Angebote auf die KRITIS-Strukturen der Telekommunikations-Dienstleister beziehen werden, können diese Themen vermutlich nicht getrennt voneinander betrachtet werden. Hinzu kommt das Thema ausfallsicherer Internet-Verbindungen mit einem entsprechenden Quality-of-Service (QoS) und Service-Level-Agreements (SLAs). Solche Enterprise-Netzanbindungen sind in Krankenhäusern derzeit noch kaum vorhanden.

Das vom BSI veröffentlichte „Kompendium Videokonferenzsysteme"[3] kann Krankenhäusern bei der Wahl geeigneter Videokonferenzsysteme zur Durchführung telemedizinischer Behandlungen sowie einem damit verbundenen Austausch von Inhalten und Informationen mit erhöhtem Schutzbedarf unterstützen.

Zunehmender Einsatz von Point-of-Care-Analysen

Als ein weiterer Trend zeichnet sich ab, dass zukünftig vermehrt Point-of-Care-Analysen (Point-of-Care-Testing, POCT) zum Einsatz kommen sollen. Unter POCT wird eine unkomplizierte und patientennahe Sofortdiagnostik verstanden, unter Zuhilfenahme einfach zu bedienender und auf den Anwendungsbereich spezialisierten Gerätschaften. Zur Durchführung von POCT-Diagnosen werden zukünftig leistungsstarke, mobile Geräte benötigt, die mit einfach zugänglichem Probenmaterial ein möglichst großes Spektrum an Tests durchführen können. In diesem Zusammenhang sind neben der Benutzerfreundlichkeit vor allem Durchlaufzeiten entscheidend.

Die Entwicklung zu mehr POC-Diagnostik und ggf. Therapie stellt dabei einige Herausforderungen an die Netzinfrastruktur. Neben der vollständigen Inventarisierung der vernetzten Systeme kristallisieren sich vor allem spezielle Anforderungen heraus, welche die Kopplung von IT-Systemen und Medizintechnik in IT-Netzen betreffen. Hinzu kommt der sukzessive Anstieg der Nutzung privater Endgeräte, die vom medizinischen Personal vermehrt genutzt werden. Hier bedarf es zukünftig ebenfalls technischer und organisatorischer Maßnahmen, um die Digitalisierung in der medizinischen Versorgung sicher gestalten zu können.

IT-Sicherheit als notwendige Investition in die Funktionsfähigkeit der medizinischen Versorgung

Die Digitalisierung im Gesundheitswesen eröffnet große Chancen für eine bessere Versorgung der Patientinnen und Patienten in der stationären medizinischen Versorgung. Informationssicherheit ist dabei von Anfang an mitzudenken. Eine ganzheitliche und systematische Herangehensweise, die sich konsequent an der kritischen Dienstleistung orientiert, kann bei gleichzeitiger Steigerung des Sicherheitsniveaus mittel- und langfristig viel Aufwand sparen und darf nicht als bloßer Kostenfaktor abgetan werden. Das BSI als nationale Cyber-Sicherheitsbehörde des Bundes steht hier allen Akteuren im Sektor Gesundheit, insbesondere den Krankenhäusern, mit vielfältigen Unterstützungsangeboten zur Verfügung.

[3] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf?__blob=publicationFile&v=4

Literaturverzeichnis

[BSI. 2016] *Bundesamt für Sicherheit in der Informationstechnik: Kritis-Sektorstudie Gesundheit.* s.l. : Im Auftrag des Bundesamts für Sicherheit in der Informationstechnik erstellt von der PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft, zusammen mit der PwC Strategy (Germany), 2016.

[C5] Anforderungskatalog Cloud Computing (C5), BSI, C5:2016, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Kriterienkatalog/C5_Archiv/C5_Archiv_node.html

Destatis. 2017. Statistisches Bundesamt: Gesundheit — Grunddaten der Krankenhäuser 2016. 2017. [Online] 2017. https://www.destatis.de/DE/Publikationen/Thematisch/Gesundheit/Krankenhaeuser/GrunddatenKrankenhaeuser2120611167004.pdf?__blob=publicationFile.

[KoViKo] Kompendium Videokonferenzsysteme (KoViKo), BSI, 2020 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf?__blob=publicationFile&v=4