Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

KRITIS-Sektor Gesundheit: Informationssicherheit in Laboren – 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

Aufgrund der bedeutenden Rolle, welche die Laboratoriumsdiagnostik für die Diagnose und Therapiekontrolle sowohl in der ambulanten als auch in der stationären medizinischen Versorgung der Bevölkerung einnimmt, wurde diese vom Gesetzgeber als Erbringer einer „kritischen" Dienstleistung erfasst (BSI-Gesetz (BSIG)). Dabei fallen alle Labore, die einen Schwellenwert von 1,5 Mio. Laboraufträgen pro Jahr überschreiten, unter den Geltungsbereich der Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV). Als Labor wird dabei im Sinne der BSI-KritisV eine Einrichtung definiert, in der medizinische labordiagnostische Verfahren zur Diagnose und Therapiekontrolle in der Humanmedizin durchgeführt und fachärztlich befundet werden.

Das BSI hat diesbezüglich im Rahmen der „Studie zur kritischen Dienstleistung: Laboratoriumsdiagnostik" neben einer Übersicht über den Gesamtmarkt die relevanten Prozesse der Laboratoriumsdiagnostik sowie die daraus resultierenden wechselseitigen IT-Abhängigkeiten näher untersucht. Auf Basis von strukturierten Gesprächen mit IT-Verantwortlichen von Laboren wurden insbesondere die Prozessdarstellungen validiert, die Kritikalität der Aufgaben eingestuft sowie der Stand der Technik in Bezug auf die IT-Sicherheit der Labore evaluiert. Primär sollten dabei die eingesetzten IT-Systeme, deren Vernetzung und Abhängigkeiten genauer identifiziert werden mit dem Ziel, den IST-Zustand der technischen Systeme hinsichtlich möglicher Schwachstellen, Bedrohungen und Absicherungen genauer erheben zu können, um im Anschluss konkrete Handlungsempfehlungen zur Erhöhung des Schutzniveaus daraus abzuleiten. Diese Studie wurde durch Goldmedia GmbH Strategy Consulting und dem ALM – Akkreditierte Labore in der Medizin e.V. in Zusammenarbeit mit der WCG AG im Auftrag des BSI durchgeführt. 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 die Prozesse sowie den Status Quo der Informationssicherheit in den Laboren. Neben Handlungsempfehlungen zur Erhöhung des Schutzniveaus erfolgt ein Ausblick zur Zukunft der IT-Durchdringung und -Entwicklung.

[1] VS–NUR FÜR DEN DIENSTGEBRAUCH

2 Rahmenbedingungen

2.1 Marktstrukturen

In Deutschland existieren ca. 1.730 medizinische Labore. Dazu gehören Krankenhauslabore, Laborketten teilweise international tätiger Laborgruppen, die eine Vielzahl von Standorten betreiben, sowie inhabergeführte laborfachärztliche Labore mit einem oder mehreren Standorten.

Des Weiteren werden Laborleistungen durch niedergelassene Ärzte (z. B. Urologen, Gynäkologen) in deren Praxen erbracht. Im Gegensatz zu laborfachärztlichen Laboren erbringen diese Praxen nur ein kleines Spektrum an Leistungen – im Wesentlichen diejenigen Laboruntersuchungen, die „Kern des Fachgebiets" sind.

Tabelle 1 Organisationsformen medizinischer Labore in Deutschland (WCG-Datenerhebung 2018) (WCG, 2018)

Art des Labors	Anzahl Standorte	Organisationsstruktur/Betreiber
Krankenhauslabore	Ca. 400 Standorte in Deutschland	On-Premise-Labor in Eigenbetrieb des Krankenhauses
	Ca. 1.100 Standorte in Deutschland	On-Premise-Labor, betrieben durch externe Labordienstleister
Laborgemeinschaften	Ca. 200-230 Standorte in Deutschland	Zumeist als Gesellschaft bürgerlichen Rechts (GbR) organisiert. Gesellschafter sind einzelne Ärzte. Die Laborgemeinschaften sind rechtlich selbstständig, sie werden häufig gemeinsam mit einem ambulanten, gelegentlich auch mit einem stationären Facharztlabor betrieben (sog. integrierte Laborversorgung). An einem Facharztlaborstandort können eine oder mehrere Laborgemeinschaften angegliedert sein.
Laborfachärztliche Labore	Ca. 200-230 Standorte in Deutschland	a) Labore, die Teil einer Laborgruppe sind b) Inhabergeführte Einzellabore c) Inhabergeführte Labore mit mehreren Standorten in unterschiedlichen Organisations- und Rechtsformen

Art des Labors	Anzahl Standorte	Organisationsstruktur/Betreiber
Haus- bzw. fachärztliche Praxislabore/Präsenzlabore	Ca. 82.800 Haus- bzw. fachärztliche Praxen inkl. medizinische Versorgungszentren[2] ohne Laborfachärzte	Durchführung von: a) Akutparametern (zeitkritische Laboruntersuchungen, z. B. Verdacht auf Herzinfarkt) b) Begrenzte Laborleistungen aus dem Bereich des Basislabors
Eigenlaborerbringer	Teilmenge der ca. 18.300 Facharztpraxen (ohne Labor-fachärzte), vor allem aus der Gruppe der Gynäkologen, Orthopäden, Urologen und Dermatologen	Durchführung von Laborleistungen aus dem Bereich des Speziallabors. Die Abrechnung ist an eine Labor-Ermächtigung (Sonderqualifikation) für den Arzt, der die Untersuchung durchführt) bzw. den sog. Fachkundenachweis gebunden. Es gilt im GKV-Bereich eine Qualitätssicherungs-Richtlinie für das Speziallabor.

Pro Jahr werden durch die ambulanten Facharztlabore nach Schätzungen ca. 350 bis 400 Mio. Laboraufträge bearbeitet und befundet. Darin sind auch diejenigen Aufträge enthalten, die von Krankenhäusern an die ambulanten Facharztlabore überwiesen werden, wenn diese Laboruntersuchungen im eigenen Krankenhaus (mit/ohne eigenem Vor-Ort-Labor) nicht durchgeführt werden können. Hinzu kommen die Laboraufträge, die Krankenhäuser an ihre eigenen Labore geben. Dieses Volumen dürfte in etwa 25 bis 30 Prozent der Laboraufträge der ambulanten Facharztlabore entsprechen.[3]

Geht man davon aus, dass je Laborauftrag im Durchschnitt vier bis fünf Untersuchungen pro Probe anfallen (Mittel aus Laborgemeinschaftsanforderungen und Speziallaboranforderungen), so werden pro Jahr mehr als 2 Mrd. Einzellaboruntersuchungen in medizinischen Laboren durchgeführt.

2.2 Regulatorische Anforderungen

Labore unterliegen einer Vielzahl regulatorischer Anforderungen, die sich über mehrere Bereiche erstrecken. Diese reichen von der Qualität der Leistungserbringung über den sicheren Betrieb von Medizintechnik bis hin zu Anforderungen an die IT-Sicherheit.

Anforderungen an die Qualität

Mit der Verabschiedung der EU-Richtlinien zu Medizinprodukten 2002 wurde zwischen Bundesministerium für Gesundheit und Bundesärztekammer abgestimmt, die Medizinproduktebetreiberverordnung um Anforderungen zur Qualitätssicherung in medizinischen Laboratorien zu vervollständigen. In der Folge wurde ein Gesamtkonzept zur Qualitätssicherung aller laboratoriumsmedizinischen Untersuchungen entwickelt – die neue „Richtlinie der Bundesärztekammer zur Qualitätssicherung laboratoriumsmedizinischer Untersuchungen“, kurz: Rili-BÄK.

[2] Bundesarztregister und MVZ-Statistik (ohne psychologische bzw. psychotherapeutische Praxen) nach [KBV 2017] (KBV, 2017)

[3] Quelle: WCG-Datenerhebung, Stand 2018 (WCG, 2018)

Die Rili-BÄK regelt die Qualitätssicherung laboratoriumsmedizinischer Untersuchungen in der Heilkunde. Das in dieser Richtlinie beschriebene System hat das Ziel, die Qualität laboratoriumsmedizinischer Untersuchungen zu sichern.

Es soll insbesondere gewährleisten:

- Die Minimierung von Einflussgrößen und Störfaktoren in der Präanalytik,
- die fachgerechte Durchführung der laboratoriumsmedizinischen Untersuchungen, einschließlich der Erkennung und Minimierung von Störeinflüssen auf die Untersuchungen und
- die korrekte Zuordnung und Dokumentation der Untersuchungsergebnisse, einschließlich der Erstellung eines Berichts.

Die allgemeinen Anforderungen an ein Qualitätssicherungssystem orientieren sich an internationalen Normen und an Konzepten zur guten labordiagnostischen Praxis. Den Kern bilden die Beschreibungen der Qualitätssicherung laboratoriumsmedizinischer Untersuchungen, die dann in den speziellen Abschnitten des Teils B konkretisiert sind. Auch die Postanalytik mit Mindestanforderungen zur Erstellung eines Berichtes oder Befundes wird abgehandelt und es wird ein Qualitätsmanagementsystem für alle Einrichtungen beziehungsweise Personen vorgegeben, die laboratoriumsmedizinische Untersuchungen durchführen.

Darüber hinaus können Labore sich auf freiwilliger Basis akkreditieren lassen. Sie ist für die Anwendung durch medizinische Laboratorien bei der Entwicklung von deren Qualitätsmanagementsystemen und der Beurteilung ihrer eigenen Kompetenz bestimmt. Demnach geht es sowohl um Anforderungen an das Management als auch an die technischen Einrichtungen. Die EN ISO 15189 legt dabei die Anforderungen an die Qualität und Kompetenz in medizinischen Laboratorien fest. Die Akkreditierung medizinischer Laboratorien nach dieser Norm gilt international als „Goldstandard“ und ist eines der wichtigsten Verfahren zur externen Qualitätsüberprüfung. Nationale Regelungen können darüber hinaus zur einzelnen Themengebieten konkretisierende Vorgaben machen.

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 EU Medizinprodukte-Sicherheitsplanverordnung (MPSV), die EU-Medizinprodukte-Betreiberverordnung (MPBetreibV) sowie insbesondere die In-Vitro-Diagnostik Verordnung (EU 2017/746, IVDR). 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 bzw. Patientinnen, Anwendern und Dritten. Die IVDR und MDR werden dabei nicht mehr in nationales Recht überführt, sondern traten 2017 unmittelbar in Kraft.

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

Für Labore, die den Schwellenwert der BSI-KritisV von 1.500.000 Aufträgen pro Jahr erreichen oder überschreiten, leiten sich Anforderungen an die IT-Sicherheit aus dem BSIG ab. Das BSIG verpflichtet die 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 Laboratoriumsdiagnostik, aufrecht zu erhalten. Die Nachweiserbringung über die Umsetzung von IT-Sicherheitsmaßnahmen erfolgt üblicherweise in Zusammenarbeit mit einer geeigneten externen Prüfstelle. Der Betreiber übermittelt nach erfolgreicher Durchführung die Ergebnisse 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 Labore, 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 Laboratoriumsdiagnostik

3.1 Besonderheit: Kritische Dienstleistung

Viele Prozesse in der Laboratoriumsdiagnostik laufen teil- bzw. vollautomatisiert und sind auf IT-Unterstützung angewiesen. Gleichzeitig wird eine Vielzahl von Daten über Schnittstellen zu anderen Akteuren aus dem Gesundheitssektor wie Arztpraxen, Polikliniken, medizinische Versorgungszentren und Krankenhäuser übertragen. Die Informationsverarbeitung muss ebenso zuverlässig funktionieren wie die zugehörige Technik, damit der Laborbetrieb aufrechterhalten werden kann. Dabei stellt die dynamische Cyber-Bedrohungslage neue Anforderungen an die Informationssicherheit. Für den Erhalt der Funktionsfähigkeit der betriebenen kritischen Dienstleistung (kDL) muss jedes Labor daher ein auf seine Anforderungen abgestimmtes Informationssicherheitskonzept erstellen, umsetzen und stetig überprüfen.

Prozesse und Aufgaben

Im Vergleich zur KRITIS-Sektorstudie Gesundheit (BSI, 2016) wurde die dortige Unterteilung in Prozessschritte für die aktuelle Definition der Teilprozesse erweitert und begrifflich leicht angepasst, um Teilprozesse, Aufgaben und den Sprachgebrauch in den Laborbetrieben realitätsnah abbilden zu können. Die primäre Versorgungsdienstleistung gliedert sich somit in fünf aufeinanderfolgende Prozessschritte, die jeweils wieder in Aufgaben und Vorgänge unterteilt sind.

Der Prozessauslöser für die Erbringung von Laborleistungen ist die Indikationsstellung innerhalb des Teilprozesses **Veranlassung** durch den behandelnden Arzt bzw. behandelnde Ärztin auf Station im Krankenhaus oder in der Arztpraxis. In deren Folge wird dem Patienten bzw. der Patientin das entsprechende Probenmaterial (i.e. Blutprobe, Urinprobe, Stuhlprobe, Abstrich oder sonstiges Material) entnommen. Anschließend erfolgt der **Transport der Proben** in das analysierende medizinische Labor.

Erst der dritte Teilprozess der Laboratoriumsdiagnostik, der **Probeneingang**, findet innerhalb des Laborbetriebes statt. In der Terminologie der Laboratoriumsdiagnostik werden alle Aufgaben bis einschließlich des Probeneingangs auch unter dem Begriff „Präanalytik“ zusammengefasst. Während des Probeneingangs erfolgen verschiedene, vorbereitende Tätigkeiten, bevor die Proben im Teilprozess **Analytik** analysiert werden. Im sich anschließenden Teilprozess **Postanalytik** laufen hauptsächlich die Befundung und Übermittlung der Befundergebnisse an die Verordner (Kliniken und Arztpraxen) ab.

Tabelle 2 Relevante Teilprozesse und Aufgaben der kritischen Dienstleistung Laboratoriumsdiagnostik

Prozessschritt	Aufgabe (Arbeitsschritte gem. Sektorstudie 2016)
Veranlassung	Indikationsstellung
	Probenentnahme
	Transportvorbereitung
Transport	Transport
Probeneingang	Auspacken der Probe
	Auftragserfassung
	Probenidentifikation
	Probenvorbereitung
	Probenverteilung
Analytik	Vollautomatisierte Analytik

Prozessschritt	Aufgabe (Arbeitsschritte gem. Sektorstudie 2016)
	Teilautomatisierte und manuelle Analytik
	Notfallanalytik
	Technische Validation
Postanalytik	Medizinische Validation und ärztliche Befundung
	Befundübermittlung
	Probenarchivierung

3.2 IT-sicherheitsrelevante Herausforderungen

Sowohl KRITIS-Labore als auch Labore, die nicht durch das BSIG reguliert werden, sind (zunehmend) automatisiert und stehen deshalb bei der Schaffung der notwendigen Grundlagen für die Informationssicherheit vor den folgenden branchenspezifischen Herausforderungen.

Laborinformations- und Managementsystem (LIMS)

Das LIMS steht im Mittelpunkt des operativen Laborbetriebs, insbesondere wenn es als vollumfängliches Labor-Informations- und Management-System genutzt wird. Der Funktionsumfang eines LIMS kann von der Probenverwaltung bis zur Befunderstellung reichen. Für LIMS bestehen hohe Verfügbarkeitsanforderungen, ein Ausfall stellt ein kritisches Ereignis in einem Laborbetrieb dar. LIMS werden in der Regel auf dem Gelände des Laborbetriebs gehostet. Hierfür sind redundante, zugangsgeschützt aufgestellte Server-Systeme im Einsatz. Bei stark integrierten Laborgruppen können zudem auch Remote-Standorte an ein zentral organisiertes LIMS, das im Kern die Stammdatenorganisation übernimmt, angeschlossen sein. Der Wechsel des LIMS-Anbieters ist aufgrund des hohen Einrichtungs- und Individualisierungsaufwandes, seines zentralen Stellenwertes innerhalb des Labor-Setups und evtl. bereits geleisteter Software-Eigenentwicklungen sehr aufwendig und daher unüblich. Dieser Umstand kann zu einer Einschränkung bei Auswahl und Design von angemessenen IT-Sicherheitsmaßnahmen führen.

In-Vitro-Diagnostikgeräte (IVD-Geräte)

Die eigentliche Diagnostik erfolgt durch Untersuchungen mit IVD-Geräten in den unterschiedlichen Analysebereichen. Die Spannbreite der IVD-Geräte umfasst vollautomatisierte Analysegeräte mit hohem Probenaufkommen von bis zu mehreren hundert Proben pro Stunde („Massenparameter“), teilautomatisierte Geräte sowie manuelle Analysegeräte. IVD-Geräte innerhalb des Labornetzes weisen aufgrund ihrer Eigenschaft als Medizinprodukte sicherheitsrelevante Einfallsvektoren auf, die nur durch die jeweiligen IVD-Gerätehersteller gesichert werden können. Dies ist der Tatsache geschuldet, dass IVD-Geräte komplexe Zertifizierungsverfahren durchlaufen. Bis zur Markteinführung eines neu entwickelten Gerätes können bis zum Abschluss aller Zertifizierungs- und Zulassungsmaßnahmen bis zu 10 Jahren vergehen, dementsprechend lange sind auch die Nutzungszyklen von IVD-Geräten. Aus Sicht der IT-Sicherheit bereiten IVD-Geräte daher erhebliche Herausforderungen, da die zertifizierte Laufzeitumgebung mit statischen Betriebssystemen nicht ohne weiteres gepatcht bzw. aktualisiert werden kann.

Middleware-Systeme

Aufgrund des Koordinationsbedarfes bei mehreren IVD-Geräten in einem Analysestraßenverbund setzen die IVD-Gerätehersteller zur Steuerung, Prozessoptimierung und Qualitätssicherung zunehmend eine herstellerspezifische Middleware ein, um den Informationsfluss zwischen den verschiedenen Anlagenteilen und der Analysestraße zu koordinieren. Für jede Analysestraße bzw. jeden IVD-Gerätehersteller kommen jeweils eigene, proprietäre Middleware-Systeme zum Einsatz. Für Middlewares gelten hierbei dieselben strukturellen Probleme wie für IVD-Geräte: Sie sind potenziell anfällig für Angriffe, da sie aufgrund ihrer

zertifizierten Laufzeitumgebungen z.B. nicht in das lokale Virenschutz-Regime eingebunden werden können.

Insgesamt wird deutlich, dass Labore mit Geräten und Systemen vieler Hersteller und deren Anforderungen umgehen und gleichzeitig einen sicheren, täglich verfügbaren, hocheffizienten und hochqualitativen Betrieb aufrechterhalten müssen.

3.3 Status Quo: Ergebnisse der Betreiberbefragung

In der Gesamtschau lässt sich feststellen, dass Laborbetriebe aufgrund des fortgeschrittenen IT-Reifegrades und der hohen Verfügbarkeitsanforderungen über weitgehende Schutzmaßnahmen gegen Ausfälle verfügen. Die bislang erfolgte Formalisierung und Umsetzung der Sicherheitsmaßnahmen im Rahmen der BSI-KritisV hat zu einem wesentlichen Sprung im Reifegrad der betroffenen Laborbetriebe geführt. Labore, welche die aus der BSI-KritisV resultierenden Sicherheitsmaßnahmen bereits umgesetzt haben, erreichen in der Regel ein gutes Schutzniveau. Die ergriffenen Schutzmaßnahmen gegen Ausfälle der IT-Infrastruktur skalieren dabei in der Regel mit der Unternehmensgröße und der damit verbundenen Anlagenkritikalität. Die Befragung zeigt insgesamt, dass die Labore den Fokus vor allem auf die Umsetzung von technischen IT-Sicherheitsmaßnahmen gelegt haben. Bei der Umsetzung von organisatorischen IT-Sicherheitsmaßnahmen ist noch Verbesserungspotenzial erkennbar.

Organisatorische Maßnahmen

Nahezu alle medizinischen Laborbetriebe sind durch die Deutsche Akkreditierungsstelle GmbH (DAkkS) akkreditiert. Eine grundlegende Risikovorsorge inkl. Asset Management und Wiederherstellungskonzepten ist bereits Voraussetzung für die DAkkS-Akkreditierung, mit der die Erfüllung der regulatorischen Vorgaben (u.a. RiliBÄK, DIN 15189, DIN 17025) bestätigt wird. Allerdings ist zu berücksichtigen, dass der Schwerpunkt der DAkks-Akkreditierung auf labormedizinischen Anforderungen liegt. Die Vorgaben zur IT-Sicherheit sind in der Akkreditierung nur generisch gehalten und bieten bei der technischen Implementierung im Detail Umsetzungsspielräume, sodass eine DAkks-Akkreditierung nicht mit einem erfolgreichen IT-Sicherheitsaudit gleichgesetzt werden kann.

Vor allem größere Labore verfügen über eine ausgeprägte IT-Dokumentation (Orgware), da sie auf eine stärkere Formalisierung der Prozesse betrieblich angewiesen sind. In größeren Laborbetrieben können mitunter 1.000 Standard Operating Procedures (SOPs) formalisiert sein. Sofern die Betriebe unter die Regulierung der BSI-KritisV fallen, ist die Prozessdokumentation zudem ein regulatorisches Erfordernis und Grundlage der Auditierung des B3S Labor. Die Umsetzung des B3S Labor erfordert die Dokumentation von derzeit rd. 800 Arbeitspaketen.

Aus dem Formalisierungsgrad der Prozesse und Schutzmaßnahmen lässt sich jedoch keine direkte Korrelation zur Wirksamkeit der ergriffenen Schutzmaßnahmen ableiten. So sind einzelne Schutzkonzepte (z.B. im Berechtigungsmanagement) noch nicht ausreichend entwickelt. IT-Sicherheitsschulungen finden häufig nicht im erforderlichen Umfang statt. Ein prozessgesteuertes Incident-Management ist nur vereinzelt und insbesondere in großen Laboren vorhanden, das Notfallmanagement ist vor allem in kleineren Laboren noch ausbaufähig.

Technische Maßnahmen

In der Regel sind Virenschutz und VPN in Laborbetrieben im Sinne des Stands der Technik umgesetzt. Maßnahmen im Patch- und Änderungsmanagement erfolgen zeitnah, sofern durch die Hersteller z.B. der Medizintechnik oder Peripherie-Geräte zur Verfügung gestellt. Die Datensicherung ist auf hohem Niveau realisiert, wenn auch Recovery-Tests und die großen Datenmengen Herausforderungen darstellen. In großen Laboren ist Netzsegmentierung und Virtualisierung trotz des höheren Kosten- und Personalaufwands durchgehend realisiert. In kleineren Laboren, die nicht der BSI-KritisV unterfallen, fehlt es hier jedoch oft an internem Know-how, so dass für Wartung und Betrieb Kosten durch externe

Dienstleister entstehen. Protokollierungsdaten fallen in Laborbetrieben in immer größerem Ausmaß an. Jede automatisierte Bewegung von Proben im Labor generiert in jedem Prozessschritt entsprechende Metadaten in den Routing- und Trackingsystemen. Eine strukturierte Auswertung (Monitoring) findet in den Laborbetreiben bislang kaum statt.

4 Handlungsfelder

4.1 Empfehlungen

Die Formalisierung der Prozesse ist in den Laboren bereits weit fortgeschritten. Im Zusammenspiel mit der in der Studie erarbeiteten Prozessanalyse können die fünf aufeinander folgenden Teilprozesse mit ihren Aufgaben und Vorgängen als Richtschnur für eine systematische Planung und Umsetzung von zielgerichteten technischen und organisatorischen IT-Sicherheitsmaßnahmen dienen. Auf diese Weise lässt sich das IT-Sicherheitsniveau in Laboren langfristig erfolgreich steigern

Managementsystem für Informationssicherheit für eine gelebte IT-Sicherheitskultur nutzen

Die kontinuierliche Weiterentwicklung des Informationssicherheitsmanagementsystems (ISMS) mit seinen Richtlinien und Methoden ist der Grundpfeiler für das Erreichen eines angemessenen IT-Sicherheitsniveaus. Ein ausgereiftes ISMS ist die Basis für die Sensibilisierung der Beschäftigten im Hinblick auf die Umsetzung von IT-Sicherheitsanforderungen und ein wichtiges Signal, dass die Leitungsebene hinter den Sicherheitszielen steht und sich ihrer Verantwortung im Umgang mit Informationssicherheit bewusst ist.

IT-Risikomanagement und IT-Notfallmanagement systematisch ausbauen

Im ISMS sollten neben Richtlinien zur technischen Umsetzung von IT-Sicherheitsmaßnahmen ebenso Rahmenbedingungen zum IT-Risikomanagement für Systeme und Komponenten der kDL festgelegt werden. Hier sollte die Prozessanalyse den Ausgangspunkt für die Risikobetrachtung darstellen. 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 Laboratoriumsdiagnostik 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 werden sowie die Umsetzung von technischen und organisatorischen IT-Sicherheitsmaßnahmen erfolgen. Abschließend ist darauf aufbauend das IT-Notfallmanagement zu errichten.

Netzsegmentierung und Virtualisierung weiterentwickeln

Aufgrund der umfangreichen zu verarbeitenden Datenmengen sind vor allem ausreichend große Speicherkapazitäten sowie eine ausgereifte IT-Netzinfrastruktur entscheidend. Demzufolge bedarf es einer stringenten Netztrennung bzw. Netzsegmentierung. Die unterschiedlichen Sicherheitszonen werden über logische Teilnetze als Virtual Local Area Network (VLAN) realisiert. Eine übliche Konfiguration trennt dabei das administrative Büronetz vom produktiven Labornetz. IVD-Geräte nehmen eine Sonderstellung ein, sie befinden sich hiervon abgetrennt in einem dritten Subnetz. Zusätzlich werden auch weitere Elemente des IT-Netzes mithilfe von Hypervisoren virtualisiert, insbesondere die Server-Virtualisierung kommt aus Sicherheitsgründen beim Betrieb von IVD-Geräten zum Einsatz. Einzelne Netzsegmente sind mit Hilfe klar definierter Routing-Regeln voneinander zu trennen, um dadurch den Schutz vor unberechtigtem Zugriff zu erhöhen, bzw. die netzübergreifende Ausbreitung von Schadsoftware einzudämmen.

Monitoring etablieren

Eine strategische Herausforderung stellen die im Laborbetrieb anfallenden Datenmengen und deren Archivdauer (mind. 10 Jahre, bei Untersuchungen nach dem Transfusionsgesetz bis zu 30 Jahre) dar. IVD-Geräte können während der Analyse z. T. Rohdaten in erheblichem Umfang produzieren.[4] Um einem

[4] Ein einzelnes Blutbild mit einer Analyse von 15 Eigenschaften pro Blutzelle generiert bei durchschnittlich 45 Tsd. in der Probe enthaltenen Zellen bereits über 0,5 Mio. Datenpunkte. Zudem werden viele Blutproben mehreren Analysen unterzogen. (BSI, 2020)

Datenverlust vorzubeugen, werden Backups der LIMS-, OE- und der Analysedaten in den IVD-Geräten in immer kürzeren Abständen gezogen (aktuell etwa alle 15 Minuten).

Auch Protokollierungsdaten fallen in Laborbetrieben in immer größerem Ausmaß an. Die Gründe hierfür liegen u.a. in einem gestiegenen Anspruch an die umfassende Rückführbarkeit des gesamten Analyseprozesses sowie des hohen Automatisierungsgrads. Jede automatisierte Bewegung von Proben im Labor generiert in jedem Prozessschritt entsprechende Metadaten in den Routing- und Trackingsystemen.

Eine strukturierte Auswertung findet in den Laborbetrieben bislang kaum statt. Eine Speicherung und Analyse der Protokollierungsdaten kann aufgrund der Datensensibilität und einschlägiger Bestimmungen (z. B. RiliBÄK, DIN 15189, DIN 17025) auch kaum an ein externes Security Operations Center (SOC) zur Analyse transferiert werden. Ein zentraler Protokollserver würde die automatisierte Suche nach Fehlern und Integritätsproblemen sowie die Erkennung von (drohenden) Systemausfällen ermöglichen. Ein zentralisiertes Protokollierungsdaten-Management für Laborbetriebe ist daher sinnvoll und sollte in den Betrieben mittel- bis langfristig aufgebaut werden. Auch wenn die strukturierte Analyse aufgrund der künftig weiter zunehmenden Anforderungen an Speicherplatz und Schreibperformance für Backup/Recovery und Protokollierungsdaten sowie der wachsenden Datenmengen absehbar mit erheblichen Anstrengungen für ein sinnvolles internes Data-Warehousing im Labor verbunden bleibt, welches selbst größere Laborbetriebe vor Herausforderungen stellt, ist ein zentralisiertes Protokollierungsdaten-Management sinnvoll.

Absicherung der Fernwartung weiterentwickeln

Auf absehbare Zeit bleibt die Absicherung der Fernwartungszugänge zu den IVD-Herstellern eine zentrale Aufgabe im Sinne der IT-Sicherheit in den Laboren. Hierfür besteht die Notwendigkeit, dass grundsätzlich Auftragsdatenverarbeitungsverträge zwischen Laborbetrieben und IVD-Herstellern abgeschlossen werden, um der Tatsache gerecht zu werden, dass neue Wege der Datenverarbeitung etabliert werden. Zudem muss technisch wie vertraglich durch Zugriffs- und Berechtigungskonzepte sichergestellt werden, dass im Laufe des Remote-Zugriffes keine Einsicht in Patientendaten erfolgen kann.

Es kommt im Markt aktuell zu Konstruktionen, dass der VPN-Zugriff des Herstellers auf seine Geräte nur temporär, durch manuelle Freigabe des Labors erfolgt. Dies kann als Ad-hoc-Lösung betrachtet werden, in Ermangelung eines übergreifenden Branchenverständnisses oder einer grundlegenden „Branchenvereinbarung“ zur weitergehenden Absicherung der Fernwartungszugänge. Hersteller und Laborbetreiber müssen sich individuell darüber vertraglich einigen, wie die Nutzung von Fernwartungszugängen ausgestaltet wird. Aus Sicht der Laborbetreiber wäre eine grundlegende Vereinbarung bzw. Regulierung zum Fernzugriff im Kontext von IVD-Geräten sehr sinnvoll.

4.2 Ausblick

Angesichts der fortschreitenden Digitalisierung und der damit verbundenen Automatisierung der Labore ist der entscheidende Faktor für ein hohes IT-Sicherheitsniveau die ganzheitliche Betrachtung der kritischen Dienstleistung. Wer die kritischen Prozesse, Aufgaben und Vorgänge sowie die eingesetzten IT-Systeme und Komponenten klar identifiziert, erreicht nachhaltig ein angemessenes Schutzniveau – auch mit Blick auf wesentliche Entwicklungstrends, die auf den Einsatz von IT-Systemen zukünftig wirken.

IVD-Verbundsysteme statt Analysegeräte

Die Analysegeräte zur In-Vitro-Diagnostik werden sich künftig noch stärker zu modularisierten Verbundsystemen entwickeln, die nach den individuellen Anforderungen eines Laborbetriebs zusammengestellt und als Verbundeinheit betrieben werden. Durch den vernetzten Betrieb der einzelnen IVD-Geräte wird eine weitere Erhöhung des Probendurchsatzes erreicht. Neben dem allgemeinen technologischen Fortschritt ist auch eine weiter gesteigerte Effizienz innerhalb der Analysestraßen durch eine optimierte Anlagensteuerung im Verbundbetrieb zu erwarten. Zudem wird das Analysespektrum der

Verbundeinheiten größer, sodass umfangreichere Analysen gefahren werden können, ohne dass sich die Analysezeiten deutlich verlängern. In diesem Zusammenhang kommt es zu einer stärkeren Integration und damit Reduzierung der zurzeit noch halbautomatisch/manuell durchgeführten Analysen. Unabhängig von Effizienzsteigerungen im Laborbetrieb durch Verbundeinheiten werden insbesondere patientennahe Einzelanalysensysteme (Point-of-Care-Testing, POCT) in Praxen bzw. in Notaufnahmen verstärkt zum Einsatz kommen. Die beschriebenen Herausforderungen im Bereich der IT-Sicherheit durch den Betrieb von IVDs und Middleware werden also für einen noch größeren Teil des Laborbetriebs gelten.

Auslagerung der Analysetätigkeit in die Cloud

Die zunehmend algorithmenbasierte Prozessierung von Labordaten mit statistischen und lernenden Methoden wird dazu führen, dass vermehrt Labordaten außerhalb des On-Premise-Laborrechenzentrums in der Cloud durchgeführt werden. Insbesondere bei sogenannten Konstellationsauswertungen, bei denen mehrere, (typischerweise 5-6) Merkmale gemeinsam ausgewertet werden, kommen bereits entsprechende Cloud-Lösungen zum Einsatz.

Auch sind neuartige Laborinfrastrukturen zu erwarten, bei denen das LIMS vollständig von einem lokalen Rechenzentrum in die Cloud verlagert wird. Bereits heute gibt es die Möglichkeit, ein LIMS als „Software as a Service“ (SaaS) zu betreiben und Marktteilnehmer, die mit diesen Möglichkeiten experimentieren. Allerdings ist die vollständige Verlagerung des LIMS in die Cloud ein Szenario, das mittelfristig kaum in der Breite zur Anwendung kommen wird. Neben der Tatsache, dass LIMS-Migrationen nur selten in gewachsenen Strukturen unternommen werden, stellen vernetzte IVD-Geräte besonders hohe Anforderungen an geringe Latenzzeiten, die den Cloud-Betrieb technisch anspruchsvoll gestalten. Trotz der technischen Hürden bei der Echtzeit-Kommunikation, die SaaS im Laborumfeld mitunter Hürden bereiten können, werden externe Rechenzentrumslösungen weiter zunehmen. Damit wird die Zahl der Akteure wie Cloud-Dienstleister oder Telematik-Infrastrukturbetreiber, die Labordaten im Auftrag verarbeiten, ansteigen.

Aus der zunehmenden Komplexität der vernetzten Kommunikation mit medizinischen und nicht-medizinischen Leistungserbringern resultieren technische wie organisatorische Hürden, insbesondere bei der künftigen Organisation des Datenschutzes und der Datensicherheit. Zusätzliche Akteure und ein höherer Vernetzungsgrad bedeuten einerseits eine Zunahme der Angriffsmöglichkeiten und eine Erhöhung des abstrakten Gefährdungspotentials. Anderseits bieten zentral gemanagte Ressourcen Vorteile beim Sicherheitsmanagement und bei der Auditierung. Die Überwachung des abgehenden Netzverkehrs über bestimmte, besonders schützenswerte Netzübergange würde stattdessen eine zentrale, zertifizierte Instanz übernehmen, was Skalenvorteile bietet und zudem die Ressourcen im Sicherheitsmanagement der Labore entlasten würde.

Harmonisierung digitaler Schnittstellen und Übertragungsstandards

Der Erfolg der weiteren digitalen Transformation in der Laboratoriumsdiagnostik hängt wesentlich von der erfolgreichen Strukturierung und Standardisierung der Daten über Betriebsgrenzen hinweg ab. Obwohl die Digitalisierung im Laboralltag selbst schon weit fortgeschritten ist, bereitet der Datenaustausch zu anderen Teilnehmern des Gesundheitswesens weiterhin große Herausforderungen. Eine sektorenübergreifende Standardisierung von Gesundheitsdaten für eine fall- und einrichtungsübergreifende Dokumentation fehlt derzeit noch.

Nach wie vor kommt es zu Medienbrüchen in Arztpraxen und Krankenhäusern, falls die Order-Entry-Systeme der Labore nicht oder nicht hinreichend in die AIS- und KIS-Systeme integriert sind. Als Basis kommen zwar nur wenige Standards in Frage, etwa IHE/FIHR (mit Erweiterungen), HL7 (in Teilen), DICOM (übersteigt derzeit Möglichkeiten der eGA) und XML/xDT. Allerdings müssen auch bei einem einheitlichen Standard für die Übernahmen der Daten aus einem Aktensystem in ein anderes stets Übersetzungstabellen für das Mapping programmiert werden.[5] Aufgrund fehlender Mapping-Tabellen können die tabellierten Befundwerte derzeit noch nicht in die Informationssysteme übernommen werden, obwohl die Kommunikation über eine standardisierte Schnittstelle grundsätzlich möglich ist.

Informationssicherheit als notwendige Voraussetzung für eine erfolgreiche Digitalisierung

Die hier zusammengefasste Studie zeigt, dass ein branchenspezifischer Sicherheitsstandard (B3S) zur deutlichen Steigerung des Reifegrades im Bereich Informationssicherheit beiträgt. Damit sind die Labore, die sich daran orientieren, bereits gut auf die fortschreitende digitale Transformation vorbereitet. Diesen Vorsprung gilt es auszubauen. Eine ganzheitliche und systematische Herangehensweise, die sich konsequent an den Prozessen der kritischen Dienstleistung orientiert, kann bei gleichzeitiger Steigerung des Sicherheitsniveaus mittel- und langfristig Ressourcen sparen. Das BSI als nationale Cyber-Sicherheitsbehörde des Bundes steht hier allen Akteuren im Sektor Gesundheit, insbesondere den Laboren, mit vielfältigen Unterstützungsangeboten zur Seite.

[5] Bislang funktioniert übergreifend nur der Austausch der Versicherungsstammdaten über den Versichertenstammdatendienst (VSD). Seit Jahresbeginn 2019 müssen Arztpraxen die Stammdaten, die auf der Versichertenkarte gespeichert sind, mit dem VSD der jeweiligen Krankenkasse abgleichen. Sollten sich Daten wie bspw. die Adresse geändert haben, wird der Daten-Chip der Karte in der Arztpraxis mit den aktuellen Daten überschrieben. Dieser Vorgang benötigt keine harmonisierten eGA-Systeme. (BSI, 2020)

Literaturverzeichnis

BSI. 2020. *Bundesamt für Sicherheit in der Informationstechnik: "Studie zur kritischen Dienstleistung: Laboratoriumsdiagnostik".* s.l. : Im Auftrag des Bundesamts für Sicherheit in der Informationstechnik erstellt von der Goldmedia GmbH Strategy Consulting und dem ALM – Akkreditierte Labore in der Medizin e.V. in Zusammenarbeit mit der WCG AG, 2020.

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.

KBV. 2017. *Statistik der Kassenärztlichen Bundesvereinigung.* 2017.

WCG. 2018. *WCG Datenerhebung Stand 2018 .* 2018.