Resilienz im Gesundheitswesen

Wie die nachhaltige Etablierung von Informationssicherheit und ein durchdachtes Krisenmanagement Leben retten können

Von Judit Schmidt und Ronald Koß

Das deutsche Gesundheitswesen gerät zunehmend ins Visier sowohl staatlicher als auch nicht-staatlicher Akteure. Mit über 1.800 Krankenhäusern, mehr als einer Million Beschäftigten und einem jährlichen Umsatz von weit über 100 Milliarden Euro, bildet es eine zentrale Stütze des Gesundheitssystems und zählt zu den Kritischen Infrastrukturen (KRITIS). Im Unterschied zu Angriffen auf die IT-Infrastruktur von Privatpersonen oder Unternehmen gefährden Cyberangriffe auf Gesundheitseinrichtungen, wie bspw. Krankenhäuser, direkt das Leben von Patienten. Fällt die IT einer Klinik aus, kann sie keine neuen Patientinnen aufnehmen und geplante Operationen müssen verschoben werden. Besonders kritisch wird es, wenn der Angriff vernetzte Systeme oder Geräte auf Intensivstationen, wie Beatmungsgeräte, betrifft – in solchen Fällen kann der Ausfall innerhalb von Minuten lebensbedrohliche Folgen haben.

Keywords: *Digitalisierung, IT, Krisenmanagement*

Ganze 73 Prozent der deutschen Gesundheitseinrichtungen waren 2022 von Cyber-Angriffen betroffen (Tendenz steigend), 33 Prozent davon mit moderaten bis erheblichen Auswirkungen. Insbesondere bei Gesundheitseinrichtungen sind Ausfälle besonders gravierend. Das Universitätsklinikum Düsseldorf wurde bspw. im Jahr 2020 Opfer eines Ransomware-Angriffs, bei dem die Täter die Daten des Klinikums verschlüsselten und das Wiedererlangen der Zugriffe an Lösegeld knüpften. Dieser Vorfall führte zu erheblichen Störungen des Krankenhausbetriebs. Viele Operationen mussten abgesagt werden und die Notaufnahme vorübergehend geschlossen werden. Der entstandene wirtschaftliche Schaden für das Krankenhaus ist enorm. Die Klinik selbst war insgesamt 13 Tage lang nicht in der Lage, den regulären Betrieb aufrechtzuerhalten.

Diese Art der Angriffe verdeutlichen nicht nur die wachsende Verwundbarkeit des Gesundheitssystems gegenüber digitalen Bedrohungen, die sowohl finanzielle als auch lebensgefährdende Konsequenzen haben können, sondern auch den Bedarf schnelle Ersatz- und Wiederanlaufprozesse einzuplanen. Die zunehmende Vernetzung und Digitalisierung der Gesundheitsbranche erfordert daher zum einen verstärkte präventive Sicherheitsmaßnahmen, um solche Vorfälle zu verhindern sowie zum anderen ein klares Notfall- und Krisenmanagement, um im Ernstfall schnell und zielgerichtet reagieren zu können (▶Abb. 1).

Gesetzliche Vorgaben und regulatorische Anforderungen steigen stetig

Die fortschreitende Entwicklung hin zu einem Smart Hospital mit telemedizinischen Lösungen, vernetzten Systemen, roboterassistierten Operationen und digitalen mobilen Endgeräten macht Informationssicherheit zu einem kontinuierlichen, sich ständig verändernden Prozess. Zudem hat sich die Anzahl der Zugriffe von mobilen Endgeräten und Heimcomputern durch Krankenhausmitarbeitende in den letzten Jahren stark erhöht. Durch Homeoffice und remote Arbeit ist die Steuerung interner IT-Systeme von externen Standorten zu einer zusätzlichen Herausforderung für die Krankenhaus-IT geworden. Jeder Fernzugriff auf das interne Netzwerk stellt ein potenzielles Einfallstor für Cyberkriminelle dar, wenn keine ausreichenden Sicherheitsvorkehrungen getroffen wurden. IT-Abteilungen sind somit nicht nur für die Beschaffung und Installation von Systemen verantwortlich, sondern auch für deren Überprüfung und Überwachung. Problematisch ist jedoch, dass die internen Mitarbeitenden oft überlastet sind und im Zuge des Einsatzes von externen Dienstleistenden die Verantwortlich-

keiten häufig nicht vollumfassend geklärt sind. Dies führt dazu, dass selbst identifizierte Sicherheitslücken oft nicht sofort behoben werden können, da die personellen Ressourcen oder die klaren Zuständigkeiten fehlen.

Krankenhäuser, die jährlich mehr als 30.000 vollstationäre Fälle behandeln, sind gemäß dem Umsetzungsplan der kritischen Infrastruktur (UP KRITIS) verpflichtet, diese Standards umzusetzen. Der B3S-Standard, entwickelt von der Deutschen Krankenhausgesellschaft (DKG) in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), umfasst etwa 200 Empfehlungen und Anforderungen, um die Sicherheit der kritischen Dienstleistungen in Krankenhäusern zu gewährleisten. Laut dem BSI-Gesetz müssen KRITIS-Häuser regelmäßig nachweisen, dass ihre IT-Systeme dem Stand der Technik entsprechen. Seit dem 1. Januar 2022 sind zudem alle Krankenhäuser gemäß § 75c SGB V gesetzlich verpflichtet, entsprechende IT-Sicherheitsvorkehrungen zu treffen. Außerdem sind regelmäßige Audits verpflichtend, um den aktuellen Sicherheitsstandard zu überprüfen und damit einen ständigen Verbesserungsprozess herbeizuführen. Diese Regelungen haben das Bewusstsein für IT-Sicherheit in Kliniken deutlich gestärkt und die Bemühungen zur Umsetzung der empfohlenen Maßnahmen vorangetrieben.

Konkrete Maßnahmen zur Verbesserung der Informationssicherheit

Zur nachhaltigen Steigerung der Resilienz benötigt es – auf Basis einer festgelegten Informationssicherheitsstrategie – die Umsetzung vielseitiger technischer und organisatorischer Maßnahmen (▶Abb. 2):

- Mitarbeitenden-Schulungen und die Sensibilisierung für IT-Sicherheitsrisiken (auch auf Basis von Sicherheitsrichtlinien) spielen eine zentrale Rolle im Schutz von Krankenhäusern vor Cyberangriffen. Regelmäßige Schulungen helfen, das Personal für die Gefahren von Cyberbedrohungen wie Phishing-Angriffe zu sensibilisieren. Dabei lernen die Mitarbeitenden, potenzielle Risiken frühzeitig zu erkennen und entsprechend zu handeln.
- Eine Netzwerksegmentierung, bei der die IT-Infrastruktur in verschiedene Bereiche aufgeteilt wird (bspw. die Trennung von administrativen und klinischen Netzwerken), ermöglicht den Schutz kritischer Systeme. Gleichzeitig sollten strikte Zugriffskontrollen eingeführt werden, die den Zugang zu bestimmten Netzwerksegmenten überwachen und unberechtigte Zugriffe verhindern.
- Regelmäßige Sicherheitsupdates und Patches (bspw. automatisierte Updates) sorgen dafür, dass alle IT-Systeme stets auf dem neuesten Stand sind und bekannte Sicherheitslücken geschlossen werden. Ergänzt wird dies durch ein effektives Vulnerability Management, bei dem spezielle Tools kontinuierlich die IT-Infrastruktur überwachen und mögliche Schwachstellen identifizieren.
- Ein wesentlicher Bestandteil der IT-Sicherheit ist die Verschlüsselung sensibler Daten. Patientendaten sollten sowohl im Ruhezustand als auch während der Übertragung (kryptografisch) verschlüsselt werden, um unbefugte Zugriffe zu verhindern. Eine End-to-End-Verschlüsselung aller Kommunikationskanäle, die Patientendaten übertragen, gewährleistet zusätzlichen Schutz.
- Ein umfassendes Backup- und Disaster-Recovery-Konzept (Speicherung auf sicheren externen Speichermedien oder in der Cloud) sorgt dafür, dass kritische Daten (bspw. Patientendaten), regelmäßig und verschlüsselt gesichert werden. Darüber hinaus unterstützen Disaster-Recovery-Pläne dabei, im Falle eines Cyberangriffs eine schnelle Wiederherstellung des Klinikbetriebs zu ermöglichen.

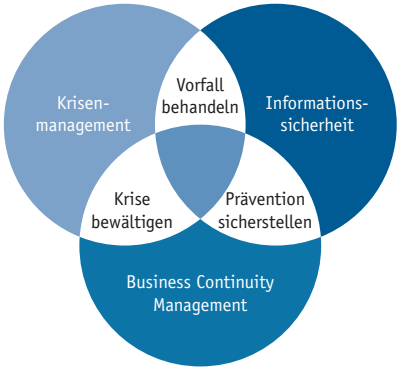

Abb. 1: Resilienz als Schlüssel zum Erfolg

- Ein Zero-Trust-Ansatz erhöht die Sicherheit zusätzlich, indem jeder Zugriff auf Systeme oder Daten individuell überprüft und autorisiert wird. Die Einführung von Multi-Faktor-Authentifizierung (MFA) stellt sicher, dass der Zugang zu kritischen Systemen durch eine zusätzliche Sicherheitsebene geschützt ist.
- Zur schnellen Reaktion auf Cybervorfälle können präventiv Incident-Response-Teams geschult und bereitgestellt werden, um im Falle eines Angriffs sofort Maßnahmen ergreifen zu können. Regelmäßige Simulationen von Cyberangriffen helfen dabei, die Einsatzbereitschaft des Teams zu verbessern und eventuelle Schwachstellen in der Reaktionsfähigkeit zu identifizieren.
- Um Cyberangriffe in Echtzeit zu erkennen und darauf zu reagieren, können Intrusion Detection Systems ▶

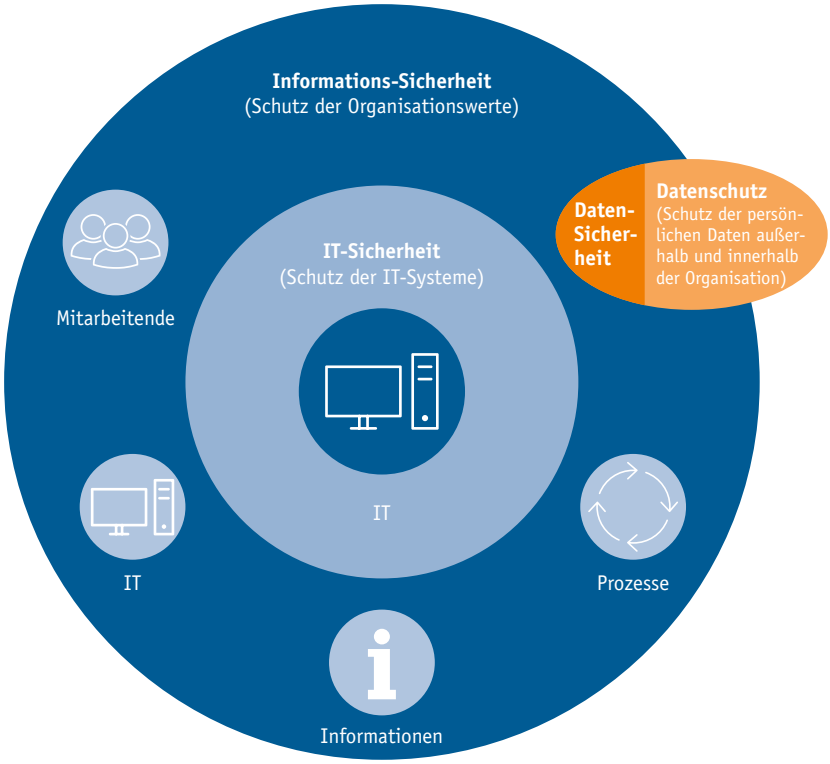

Abb. 2: Darstellung der verschiedenen technischen und organisatorischen Maßnahmen-Bereiche zur Steigerung der Resilienz

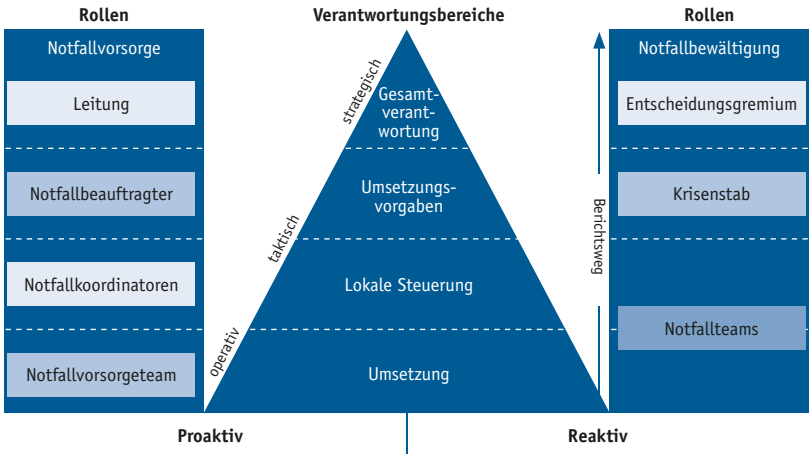

Abb. 3: Organisation des Notfallvorsorgekonzepts in Rollen und Verantwortungsbereiche

(IDS) und Intrusion Prevention Systems (IPS) implementiert werden. Unterstützend dazu kann ein Security Information and Event Management (SIEM) System eingesetzt werden, das sicherheitsrelevante Ereignisse zentral (auch durch den Einsatz von AI) überwacht und analysiert.

- Zusätzlich können Krankenhäuser von der Zusammenarbeit mit externen Partnern profitieren. Managed Security Services bieten spezialisierte Unterstützung bei der Überwachung von Bedrohungen und der Abwehr von Angriffen (bspw. durch Einsatz von Predictive Analytics). Der branchenübergreifende Austausch von Informationen über Bedrohungen und Best Practices mit anderen Gesundheitseinrichtungen trägt ebenfalls zur Stärkung der IT-Sicherheit bei.
- Schließlich sind regelmäßige Audits der IT-Sicherheitsmaßnahmen entscheidend, um bestehende Schutzvorkehrungen zu überprüfen und Schwachstellen zu identifizieren. Ein konsequentes Compliance-Management stellt sicher, dass alle relevanten Datenschutz- und Sicherheitsvorschriften, wie die Datenschutz-Grundverordnung (DSGVO), eingehalten werden.

Ein Notfallkonzept zur Vorbereitung auf den Ernstfall

Die Entwicklung eines umfassenden Notfallhandbuchs und -vorsorgekonzepts, die Erledigung aller notwendigen Vorarbeiten (bspw. Business Impact Analysen) sowie die Erprobung der definierten Meldewege und Prozesse bilden die Grundlage für eine schnelle und reibungslose Notfallbewältigung im Ernstfall (▶Abb. 3).

- Organisation und Vorgehensmodell: Neben der Festlegung hausinterner Definitionen, der Übernahme von Verantwortung durch die Leitungsebene sowie dem Commitment zu Zielbild, Zuständigkeiten und Ablauforganisation bedarf es auch der Integration der festgelegten Werte in die eigene Organisation, der Nutzung von Synergien mit festgelegten Ausweichstandorten sowie der Sicherstellung ihrer Erreichbarkeit.
- Geschäftsprozess- und Schadensanalyse: Es müssen Notfallszenarien und deren Auswirkungen, die kritischen Geschäftsprozesse und deren Wiederanlauf-Anforderungen (bspw. Zeiten, Reihenfolgeplanung) sowie Kontinuitätsstrategien (Wiederherstellung und Geschäftsfortführung) ebenso wie der benötigte Ressourceneinsatz für Normalbetrieb und Notfallbetrieb festgelegt werden.
- Sofortmaßnahmen und Krisenmanagement: Konkrete Rollen, Zuständigkeiten, Kompetenzen, Aufgaben, Handlungsanweisungen, sowie Melde- und Eskalationswege (inkl. Kommunikation intern und extern) müssen festgelegt und vorbereitet sowie eine systematische Dokumentation als Schnellzugriff sichergestellt werden.
- Aufrechterhaltung und Kontrolle: Die kontinuierliche Verbesserung des Notfallmanagements durch Übungen und Testläufe, Pflege und Überarbeitung der Notfallvorsorge- und -bewältigungsmaßnahmen sowie die Festlegung der Steuerung und Kontrolle des Notfallmanagements, auch mit der Unterstützung von entsprechendem Tool-Einsatz, sind letztendlich fester Bestandteil zur erfolgreichen Umsetzung eines umfangreichen Notfallkonzepts.

Abschließend lässt sich festhalten, dass die Herausforderungen im Bereich der IT-Sicherheit im Gesundheitswesen im Allgemeinen und in Krankenhäusern im Speziellen durch die zunehmende Digitalisierung und Vernetzung weiter steigen werden. Daher sind eine proaktive Sicherheitskultur und kontinuierliche Anpassungen an neue Bedrohungslagen unerlässlich, um sowohl den Betrieb der Einrichtungen als auch die Sicherheit der Patientendaten langfristig zu gewährleisten und damit schlussendlich eine reibungslose Versorgung eines jeden einzelnen sicherzustellen. Nur durch ein Zusammenspiel von technischen und organisatorischen Maßnahmen können Kliniken in der Lage sein, den wachsenden Cyberbedrohungen resilient entgegenzutreten. Letztlich geht es nicht nur um den Schutz der IT-Systeme, sondern auch um den Schutz von Menschenleben. ■

Judit Schmidt
Managerin
juditschmidt@kpmg.com
KPMG AG Wirtschaftsprüfungsgesellschaft

Ronald Koß
Partner
rkoss@kpmg.com
KPMG AG Wirtschaftsprüfungsgesellschaft