SWP

SWP-Aktuell

NR. 36 JULI 2026

Cybersicherheit im Gesundheitssektor

Nationale, europäische und globale Resilienz zusammendenken

Michael Bayerlein / Annegret Bendiek / Jonas Hemmelskamp / Maik von der Forst

Der Gesundheitssektor sieht sich weltweit einer zunehmenden Bedrohung durch Cyberangriffe ausgesetzt. Das European Repository of Cyber Incidents (EuRepoC) verzeichnete zwischen 2022 und 2025 insgesamt 351 signifikante Angriffe auf Gesundheitseinrichtungen. Diese Daten liefern erste Erkenntnisse über die Auswirkungen von und das Krisenmanagement nach Cyberangriffen auf das Gesundheitswesen und verdeutlichen, dass solche Angriffe eine Bedrohung für die öffentliche Gesundheit und die nationale Sicherheit darstellen. Die Datenauswertung zeigt, dass es eines Scharniers zwischen nationalen kritischen Sektoren und der europäischen bzw. der internationalen Ebene bedarf. Diese Funktion könnte der Nationale Sicherheitsrat einnehmen. Im Mittelpunkt steht dabei die Erstellung integrierter nationaler und internationaler Lagebilder auf Basis interdisziplinärer Auswertungen. Nur so können Bedrohungen systematisch erfasst, daraus wirksame Maßnahmen abgeleitet und der Gesundheitssektor ganzheitlich abgesichert werden.

Die fortschreitende Digitalisierung von medizinischen Infrastrukturen und deren Versorgungsketten erhöht einerseits die Effizienz und Qualität der Gesundheitsversorgung, führt andererseits jedoch zu einer wesentlichen Ausweitung der Angriffsflächen. Die Bedrohung durch Cyberangriffe im Gesundheitssektor ist nicht nur eine Gefahr für die nationale Sicherheit, sondern beeinträchtigt die medizinische Versorgung weltweit. Cyberangriffe auf den Gesundheitssektor, darunter Krankenhäuser und Unternehmen der Gesundheitswirtschaft, haben sich in den vergangenen Jahren auf der ganzen Welt zu einer gravierenden sicherheitspolitischen und gesellschaftlichen Herausforderung entwickelt. Laut der Open-Source-Datenbank des European Repository of Cyber Incidents ist der Gesundheitsbereich mit weltweit 351 signifikanten Cyberangriffen zwischen 2022 und 2025 einer der am stärksten betroffenen Sektoren.

Im Gesundheitssektor manifestieren sich Cyberangriffe in Form von Ransomware-Attacken, Datendiebstahl oder gezielten Störungen von Krankenhaus-IT-Systemen. Im schlimmsten Fall können diese Angriffe zu erheblichen Beeinträchtigungen der Versorgung von Patient:innen führen. Die Folgen sind potenziell lebensbedrohlich, da Behandlungsabläufe unterbrochen, Diagnosen verzögert oder medizinische Geräte funktionsunfähig werden können. Zudem

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

gefährden Angriffe auf Gesundheitsdaten, etwa auf elektronische Akten, das Vertrauen der Bevölkerung in staatliche Institutionen. Der im Mai 2026 bekannt gewordene Cyberangriff auf den Abrechnungsdienstleister Unimed, bei dem die Daten von über 100.000 Privatpatient:innen deutscher Universitätsklinika entwendet wurden, illustriert dies eindrücklich.

Wie die Grenzen zwischen nationaler, europäischer und internationaler Politik sowie verschiedenen Politikfeldern verschwimmen, zeigte zuletzt der Cyberangriff auf das US-Unternehmen Stryker, das Medizinprodukte herstellt, Mitte März 2026: Eine globale Netzwerkstörung legte das Unternehmen weltweit lahm. Der Angriff unterbrach zeitweise die Lieferung chirurgischer Verbrauchsmaterialien und personalisierter Implantate, wodurch auf der ganzen Welt Operationen verschoben werden mussten. Allein im irischen Cork konnten über 4000 Mitarbeiter vorübergehend ihrer Arbeit nicht mehr nachgehen. Die iranische Hackergruppe Handala erklärte sich verantwortlich für diesen sogenannten Wiper-Angriff, durch den Daten des Unternehmens gelöscht wurden; er sei eine Vergeltungsmaßnahme für einen Raketenangriff vom 28. Februar 2026 gewesen, bei dem eine iranische Schule getroffen und mindestens 175 Menschen getötet worden waren. Dieses Beispiel verdeutlicht, wie schnell einzelne Vorfälle eine internationale Tragweite bekommen können und die Verbindung zu Offline-Konflikten herstellen.

Trotz der Bemühungen, gesamtgesellschaftliche Resilienz aufzubauen, fehlt es im Gesundheitssektor Politikebenen übergreifend an zweierlei: einerseits an einer systematischen Einbindung internationaler Akteure in den Informationsaustausch, andererseits an einem hierfür notwendigen Koordinierungsmechanismus. Letzteres bedeutet, es genügt nicht, Sicherheitsvorfälle nur zu melden und in einem Lagebild zu erfassen. Stattdessen braucht es ein strukturiertes, auf internationaler Ebene angesiedeltes Monitoring der Auswirkungen von Cyberangriffen auf das Gesundheitssystem. Nur so können die Informationen bereitgestellt werden, die für das nationale bzw. lokale Krisenmanagement in den Krankenhäusern notwendig sind. Die ausschließliche Fokussierung auf nationale Sicherheit und damit auf nationale und EU-interne Strukturen und Kompetenzen greift folglich zu kurz, weil sie globale Synergien vernachlässigt, die für ein effektives Gesundheitskrisenmanagement essenziell sind.

Europäische und nationale Politikinitiativen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spielt in Deutschland eine zentrale Rolle beim Schutz des Gesundheitswesens vor Cybergefahren. Angesichts der fortschreitenden Digitalisierung und einer steigenden Zahl von Angriffen auf Krankenhäuser, Praxen und Pflegeeinrichtungen bietet das BSI umfassende Unterstützung, Standards und Handlungsempfehlungen. Das BSI hat Gesundheitseinrichtungen in Deutschland dazu aufgefordert, ihre Sicherheitsmaßnahmen und Backup-Systeme zu verstärken. Es arbeitet dabei eng mit der Europäischen Cybersicherheitsbehörde (ENISA) zusammen und sammelt Meldungen über schwerwiegende Cybervorfälle. Betreiber kritischer Infrastrukturen sind nach der Zweiten EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2) verpflichtet, solche Vorfälle zu melden. Geschieht dies, besteht die Chance, dass die Verantwortung zugewiesen (Attribution) und Strafverfahren oder auch diplomatische Reaktionen gegen Angreifer:innen eingeleitet werden können.

Sowohl die EU als auch die Bundesregierung haben in den letzten Jahren den Schutz kritischer Infrastrukturen in den Mittelpunkt vieler Gesetzesinitiativen gestellt:

Die Critical Entities Resilience Directive (CER) und die NIS-2-Richtlinie auf EU-Ebene und die dazugehörigen nationalen Implementierungsgesetze — in Deutschland das KRITIS-Dachgesetz und das nationale IT-Sicherheitsgesetz — zielen darauf ab, die Resilienz kritischer Infrastrukturen ein-

schließlich des Gesundheitssektors zu stärken. CER und NIS-2 verfolgen einen Allgefahrenansatz, wobei CER physische und digitale Bedrohungen in den Blick nimmt; NIS-2 hingegen konzentriert sich auf die Cybersicherheit und erweitert die Meldepflichten zum Beispiel für Gesundheitseinrichtungen, um Cyberangriffe abzuwehren. Hinzu kommt die EU Preparedness Union Strategy, die eine ganzheitliche Krisenvorsorge anstrebt und Früherkennung, Prävention und Reaktion auf Bedrohungen wie Cyberangriffe oder Pandemien umfasst. Der EU-Aktionsplan für die Cybersicherheit im Gesundheitswesen sieht Maßnahmen wie die Einrichtung eines EU-weiten Unterstützungszentrums für Krankenhäuser sowie »Reaktionsplaybooks« vor.

Um Cybersicherheitsrisiken im Gesundheitsbereich auf nationaler Ebene effizienter abzuwehren, aber auch mit dem Ziel, das deutsche Gesundheitswesen besser auf Krieg und Katastrophen vorzubereiten, hat die deutsche Gesundheitsministerin ein spezifisches Gesundheitssicherstellungsgesetz angekündigt. Es soll die oben genannten sektorenübergreifenden KRITIS-Gesetze ergänzen. Kernaspekte des geplanten Gesetzes sind die ganzheitliche Stärkung der Resilienz des Gesundheitssektors und eine engere Kooperation mit Sicherheitsbehörden sowie der Bundeswehr. Die Nationale Sicherheitsstrategie und der Aktionsplan Gesamtverteidigung formulieren zudem den Anspruch, die Ziele gesamtgesellschaftliche Resilienz und zivil-militärische Zusammenarbeit miteinander zu verzahnen — jedoch ist nicht klar, wie dies konkret im Gesundheitsbereich und Politikebenen übergreifend umgesetzt werden kann. Resilienzaufbau und Preparedness sind zentrale Herausforderungen, wie sich in der Diskussion zur Reform der Nationalen Sicherheitsstrategie zeigt.

Die Überlegungen zum Schutz der kritischen Infrastruktur Gesundheit werden konzeptionell bereits in Verbindung mit einer verstärkten zivil-militärischen Zusammenarbeit gedacht. Johannes Backus, Generalstabsarzt des Sanitätsdienstes der Bundeswehr und Kommandeur des Kommandos Gesundheitsversorgung, versteht Resilienz in diesem Zusammenhang als Zusammenwirken aller relevanten Einsatz-, Verwaltungs- und Versorgungsakteure sowie als Koordination zwischen Staat und Bevölkerung. Die Umsetzung besagter Überlegungen scheitert allerdings oftmals an Ressortgrenzen und mangelnder Top-down-Organisation durch den Nationalen Sicherheitsrat.

So wichtig nationale Maßnahmen im Rahmen des angestrebten Konzepts der Gesamtverteidigung auch sind, gerät die europäische und internationale Zusammenarbeit beim Schutz der kritischen Infrastruktur Gesundheit oft aus dem Blick. Cyberbedrohungen kennen aber keine nationalen Grenzen und können nur durch eine grenz- und behördenübergreifende Koordinierung unter Einbindung von europäischen und internationalen Partnern effektiv bekämpft werden. Obwohl die EU-Strategie zur Preparedness national umgesetzt werden muss, sollte gerade auf nationaler Ebene im Gesundheitsbereich die europäische und internationale Dimension mitgedacht werden, indem zum Beispiel ein systematischer Informationsaustausch stattfindet.

Stand der Daten auf der Basis von EuRepoC

Cyberangriffe auf den Gesundheitssektor sind nicht nur eine Bedrohung für die nationale Sicherheit, sondern in erster Linie für die (globale) öffentliche Gesundheit. Eine Untersuchung von 351 signifikanten Cyberangriffen auf den Gesundheitssektor zwischen 2022 und 2025 zeigt ein differenziertes Bild: Die Angriffe lassen sich auf Grundlage ihrer Intensität, des Angriffsmusters, der Zuschreibung von Verantwortung (Attribution) und politischer Reaktionen in sechs Angriffskategorien bzw. Cluster (C0 — C5) einteilen, die sich in ihren operativen Konsequenzen für den Betrieb der betroffenen Gesundheitseinrichtung(en) national und international deutlich unterscheiden.

Die mit insgesamt 174 Fällen am häufigsten vertretenen Kategorien C2 und C5 zielen auf Datendiebstahl ab. Während bei Angrif-

fen der Kategorie C5 die Motivation meist unbekannt ist, stehen hinter denen der Kategorie C2 kriminell motivierte Akteure, die Ransomware einsetzen, um Daten zu verschlüsseln und die Einrichtung anschließend zu erpressen. Trotz ihrer Häufigkeit haben diese Vorfälle geringe Auswirkungen auf die operativen Versorgungsprozesse.

Dagegen stehen die insgesamt 137 Angriffe der Kategorien C0, C1 und C4 mit disruptiven Folgen in Verbindung und verursachen mittel- bis langfristige Ausfälle operativer Systeme: von einigen Tagen (45 Fälle) bis zu Wochen (92 Fälle). Diese Störungen im Betrieb halten im Gesundheitssektor länger an als in anderen Sektoren. Angriffe der Kategorie C0 führen zu langfristigen Systemausfällen, ohne dass eine öffentliche Zuweisung von Verantwortung möglich ist. Bei Vorfällen der Kategorien C1 und C4 wird Ransomware eingesetzt, woraufhin eine Erpressung erfolgt (C1) bzw. was eine langfristige Störung auslöst (C4).

Die 40 Angriffe der Kategorie C3 lassen sich beschreiben als Spionage mit niedriger Intensität, wobei wenige einem staatlichen Akteur zugeordnet werden können.

Interessant ist, dass auch Angriffe von eigentlichen Ransomware-Gruppen im Gesundheitssektor weniger auf die Verschlüsselung als auf die Exfiltration von Patient:innendaten (82 Fälle) abzielen (bisweilen sogar nur auf Letzteres). Diese personenbezogenen Daten sind oftmals noch sensibler als entwendete Daten aus anderen Sektoren und können besonders gut zur Erpressung der Einrichtungen benutzt werden. Dieses Ransomware-Modell beinhaltet Double Extortion, das heißt, die Täter stehlen Daten und verschlüsseln die Systeme, um doppelt erpressen zu können — für die Nicht-Offenlegung und für die Entschlüsselung der Daten. Wenn nicht gezahlt wird, werden Daten in der Regel veröffentlicht.

Obwohl die Behörden in diesen Fällen häufig Ermittlungen einleiten, kommt es in der Mehrheit der disruptiven Fälle weder zu einer Schuldzuweisung noch zu politischen oder weitergehenden juristischen Folgen. Problematisch ist dies in Anbetracht der Auswirkungen, die diese Angriffe nicht nur auf Informationssysteme, sondern auch auf die Gesundheit haben können. Angesichts dieser Datenlage greift es zu kurz, Ransomware-Gruppen nur als Sicherheitsbedrohung zu betrachten — disruptive Angriffe auf Gesundheitseinrichtungen mit Folgen für deren operative Prozesse beeinträchtigen systematisch die öffentliche Gesundheit.

Der Blick auf die Mikroebene

Die sechs genannten Angriffskategorien ermöglichen indirekte Rückschlüsse auf die Auswirkungen von Cyberangriffen vor Ort. Zunächst lässt sich feststellen, dass die Angriffsziele im Gesundheitssektor sehr heterogen sind: Sie reichen von Krankenhäusern, Praxen, Apotheken und Medizinprodukteherstellern über Versicherungen, Rettungsdienste und Pharmafirmen bis hin zu Nichtregierungsorganisationen. Je nach betroffener Einrichtung, Methode und Weg (Angriffsvektor) sowie Ausmaß des Angriffs (Anzahl und Typ der betroffenen Systeme und Einrichtungen) sind die Auswirkungen auf die öffentliche Gesundheit sehr unterschiedlich. Die Kritikalität einer Einrichtung für die Gesundheitsversorgung wird anhand von Faktoren wie Größe, Versorgungsauftrag, Standort, Spezialisierung und (nicht) vorhandener Alternativen eingeschätzt.

Will man die identifizierten Cluster (C0 — C5) von Cyberangriffen nach ihrer Auswirkung auf die Gesundheitsversorgung klassifizieren, bietet sich folgende Aufteilung an (aufsteigende Relevanz):

1. Datendiebstahl/-verschlüsselung (z. B. Patient:innendaten, Versicherungsnummern oder Bankdaten),
2. Einschränkungen von IT-Serviceleistungen (z. B. Website, Terminportale oder Kommunikation),
3. Einschränkungen operativer Programme und Dienstleistungen (z. B. Krankenhausinformationssystem, Sterilisation, radiologische oder Laborprogramme, Blutbank).

In Kombination mit dem Wissen über die betroffene(n) Einrichtung(en) und der zeitlichen Komponente lässt sich eine Aussage über die spezifischen Auswirkungen auf die Gesundheitsversorgung treffen. Die

EuRepoC-Daten zeigen, dass Cyberangriffe, die diagnostische (z. B. Labore oder die Radiologie) oder operative Prozesse (z. B. Sterilisation, Aufnahme von Patienten, Dokumentation) beeinträchtigen, schwerwiegende Folgen für die Gesundheitsversorgung haben. Dies geschah 2023 am Universitätsklinikum Luigi Vanvitelli in Italien, wo es zu spürbaren Kapazitätseinschränkungen kam, weil auf manuelle Prozesse umgestellt wurde (C4).

Angriffe hingegen, die rein auf den Diebstahl von Patient:innendaten abzielen, werden häufig mit Informations- bzw. Vertrauensverlust assoziiert. 2025 wurden zum Beispiel bei der britischen HCRG Care Group, die Gesundheitsdienstleistungen anbietet, sensible Daten entwendet und teilweise ins Darknet gestellt (C2), 2023 die Daten von über einer Million Patient:innen des Medizinprodukteherstellers Zoll gestohlen (C1). Auch wenn Angriffe mit dem Ziel Datendiebstahl theoretisch keine direkten Auswirkungen auf die operative Gesundheitsversorgung haben, können auch sie die Versorgung indirekt beeinträchtigen, nämlich wenn die ergriffenen Schutzmaßnahmen eine Trennung vom Netz oder das Herunterfahren bestimmter Dienste erfordern. Dazu kam es 2025 beim Unternehmen SimonMed, das 200 Radiologen an 170 Standorten in 11 US-Bundesstaaten beschäftigt (C2).

Bekannte kriminelle Bedrohungsakteure wie BianLian, Medusa, BlackCat oder LockBit, die offen als Täter auftreten, übernehmen häufig die Verantwortung für solche Ransomware-Angriffe, um die betroffenen Einrichtungen zu erpressen. Beispielsweise wurde 2023 der Dienstleister TransForm Shared Service Organization durch das DAIXIN-Team angegriffen, was sich indirekt auf die Patientenversorgung und die Terminplanung in fünf Krankenhäusern in der kanadischen Provinz Ontario auswirkte (C1). 2024 musste das pharmazeutische Unternehmen Octapharma aus der Schweiz im Zuge eines Angriffs durch die Blacksuit-Gruppe über 150 Plasmaspendezentren in den USA temporär schließen (C2). Obwohl Angreifer wie LockBit von sich selbst behaupten, dass sie sich explizit nicht gegen den Gesundheitssektor richten, zeichnen die Daten ein anderes Bild. Die häufigsten Angriffsziele sind neben Krankenhäusern vor allem größere Praxen und Dienstleister wie Versicherungen oder Medizinprodukteunternehmen. Selbst Nichtregierungsorganisationen werden zur Zielscheibe, wie der Fall Omni Family Health (C1) zeigt.

Krankenhäuser können manchmal recht schnell auf Angriffe reagieren, indem sie analoge Notfallprozesse in Kraft setzen, wie Beispiele 2024 im Krankenhaus Lindenbrunn in Coppenbrügge (C4) und 2025 im Stell Hospital in Frankreich (C4) belegen. Zugleich gehen auch damit Einschränkungen einher, wodurch während eines Angriffs Termine oder geplante Eingriffe verschoben werden müssen, wie bei einem Angriff auf die Krankenhäuser in Lippstadt, Erwitte und Geseke 2024 (C4). Ob dies reine Vorsichtsmaßnahmen waren, lässt sich den öffentlich zugänglichen Berichten nicht entnehmen. Als Heiligabend 2023 drei Krankenhäuser der Katholischen Hospitalvereinigung Ostwestfalen gGmbH von der Notfallversorgung abgemeldet (C4) und 2024 bei den Wertachkliniken Bobingen und Schwabmünchen (C4) Operationen verschoben wurden, geschah dies hingegen vorsorglich. Klar ist: Mehr Transparenz über die Gefahrenlage ermöglicht ein stärker abgestimmtes Krisen- bzw. Notfallmanagement.

Wenn Krankenhäuser infolge eines Cyberangriffs von der Notfallversorgung abgemeldet werden, müssen Rettungswagen unter Umständen umgeleitet werden, so 2023 bei einem Angriff auf das amerikanische Unternehmen Ardent, das über 30 Krankenhäuser betreibt und zeitweise 10 Notaufnahmen abmelden musste (C4), oder 2024, als in Mailand zwei Krankenhäuser nicht mehr von Rettungswagen angefahren wurden (C4). In ländlichen Gegenden muss in solchen Fällen mit deutlich längeren Transportzeiten gerechnet werden, was in der Konsequenz zu Patientenschäden führen kann.

Als besonders schwerwiegend sind Angriffe, die zentrale Systeme in einem Krankenhausnetzwerk oder einem Konzern der Gesundheitsversorgung betreffen. Die dadurch ausgelösten Kaskadeneffekte

können die Systeme mehr als einer Institution kompromittieren. Ein Beispiel hierfür ist der Angriff auf das Hipocrate-Informationssystem in Rumänien 2024, der zur Folge hatte, dass 25 Krankenhäuser analog weiterarbeiten mussten und weitere 75 Einrichtungen sich vorsorglich von der Plattform abkoppelten (C4). Auch die Beeinträchtigung von Zulieferern, Rettungsdiensten oder Apotheken kann erhebliche Auswirkungen auf die Versorgung haben. Dies zeigen der Ausfall einer Rettungsleitstelle in Bozen 2025 (C0) und zwei russische Apothekenketten, die 2025 etwa 1000 Filialen vorübergehend schlossen (C0).

Solcherart Vulnerabilitäten werden in Zukunft zunehmen. Bezogen auf Deutschland liegt das daran, dass die Zentrumsmedizin unter anderem im Zuge des Krankenhausversorgungsverbesserungsgesetzes mit einer Zentralisierung von Informationssystemen einhergeht. Außerdem ist damit zu rechnen, dass die Wiederherstellung von Systemen nach einem Cyberangriff mit längerfristigen Leistungseinschränkungen verbunden ist. Dadurch wiederum entsteht eine Mehrbelastung alternativer Versorger im Nahbereich. Gravierende Auswirkungen hätten solche durch Cyberangriffe bedingten Leistungseinschränkungen, wenn eine sogenannte Doppellage (twin threats) vorliegt, also zum Beispiel während eines militärischen Konflikts oder eines Extremwetterereignisses wie Hitze.

Auf Basis der getroffenen Clustereinteilung der EuRepoC-Daten und anhand der skizzierten Folgen von Cyberangriffen für die Gesundheitsversorgung wird deutlich: Auch wenn sich das Angriffsmuster ähnelt, haben die Angriffe unterschiedlich disruptive Auswirkungen. Insgesamt wirken sich Angriffe, die den Clustern 3 oder 5 zugeordnet werden, weniger stark auf die Gesundheitsversorgung aus als diejenigen der Cluster 0,1 und 4; die des Clusters 2 liegen in der Mitte. Jedoch können auch Angriffe innerhalb eines Clusters sehr unterschiedlich verlaufen, sodass bisher jeweils eine Einzelfallbetrachtung erforderlich ist.

Mögliche Rolle der WHO auf der Makroebene

Die auf der Mikroebene identifizierten Cluster und Wirkungsketten haben regelmäßig eine internationale Dimension. Der Angriff auf Stryker legte Produktionsstandorte in Cork, Tuttlingen und Mühlheim gleichzeitig still, der Vorfall bei Octapharma zwang über 150 Plasmaspendezentren zur temporären Schließung, und der Ausfall des Hipocrate-Informationssystems betraf mehr als einhundert Einrichtungen. Cyberangriffe auf das Gesundheitswesen wirken damit entlang von Versorgungsketten, die nationale und sektorale Grenzen überschreiten. Zur systematischen Erfassung bedarf es einer Institution mit globaler Perspektive und klinischer Fachexpertise, die die Auswirkungen einzelner Cyberangriffe auf die Gesundheitsversorgung in einer Gesamtschau ermitteln kann.

Die zentrale Instanz zur Koordinierung globaler Gesundheitsbemühungen und der Bewertung gesundheitlicher Risiken ist die Weltgesundheitsorganisation (WHO). Mit dem Surveillance System for Attacks on Health Care (SSA) verfügt sie bereits über ein institutionell geeignetes Modell, dessen aktuelles Mandat jedoch auf kinetische (physische) Angriffe in humanitären Notlagen begrenzt ist. Eine Ausweitung des SSA-Mandats auf den Cyberbereich würde eine kritische Lücke schließen, da die bestehenden sicherheitsorientierten Register die spezifischen und mitunter grenzüberschreitenden Auswirkungen von Cyberangriffen auf die Gesundheitsversorgung nicht erfassen können — ihnen fehlt die nötige Fachexpertise: EuRepoC liefert belastbare Informationen zu Angriffsvektor, Attribution und technischer Intensität, macht aber keine Angaben zur Auswirkung auf die Gesundheitsversorgung. Die Emergency Events Database (EM-DAT) und die Global Terrorism Database (GTD) bilden weder digitale Angriffsformen noch die fachspezifische Kritikalität von Gesundheitseinrichtungen ab.

Das seit 2017 von der WHO betriebene SSA registriert zwar auch Angriffe, die zu

einer Behinderung der Gesundheitsversorgung führen (»obstruction to health care delivery«), beschränkt sich bislang jedoch auf kinetische Angriffe und nur solche in komplexen humanitären Notlagen (»complex humanitarian emergencies«). Allein das Krisenregister der Deutschen Arbeitsgemeinschaft Krankenhaus-Einsatzplanung (DAKEP) umfasst Sonderlagen einschließlich IT-Vorfällen in Krankenhäusern, berücksichtigt aber nur Deutschland, Österreich, die Schweiz und Luxemburg; überdies erfolgt die Meldung durch die Einrichtung selbst und meistens erst im Nachhinein.

Werden Cyberangriffe und ihre Folgen für die Gesundheitsversorgung nicht systematisch erfasst und bewertet, bleiben Wirkungsmuster im Cyberraum anekdotisch und Schutzstandards können nicht evidenzbasiert entwickelt werden. Des Weiteren bleibt die politische Rechenschaftspflicht von Staaten, von deren Gebiet Cyberangriffe ausgehen (die also Bedrohungsakteure steuern oder zumindest tolerieren), schwach. Angriffe global zu erfassen und zu benennen sowie ihre Folgen für die Gesundheitsversorgung zu beurteilen, ist somit nicht nur eine analytische, sondern gleichermaßen eine versorgungs- und sicherheitspolitische Notwendigkeit.

Die WHO könnte die existierende Lücke schließen, da sie gesundheitliche Fachexpertise und globale Reichweite vereint. Die Auswirkungen von Cyberangriffen auf den Gesundheitssektor in einer Gesamtschau auf globaler Ebene zu bewerten, ist besonders relevant, denn Konzentrationsrisiken, Kaskadeneffekte und Doppellagen, die auf der Mikroebene sichtbar geworden sind (S. 4ff), entfalten ihre Wirkung grenzüberschreitend. Die WHO besitzt mit ihrem über die Regionalbüros etablierten Netzwerk die Reichweite, die diese transnationale Wirkungslogik erfordert, und mit ihrer Arbeit zum Schutz von Gesundheitseinrichtungen die Legitimität, die für ein Cyber-Monitoring-Mandat unverzichtbar sind. Dass die WHO Cyberangriffe auf kritische Gesundheitsinfrastruktur mittlerweile explizit als Angriffe auf Gesundheitseinrichtungen klassifiziert, unterstreicht diesen Ansatz.

Mit dem SSA verfügt die WHO über eine erprobte Plattform für genau diese Aufgabe des Monitorings der Auswirkungen von Cyberangriffen auf das Gesundheitssystem. Das SSA verfolgt drei eng verknüpfte Zwecke: Es macht gezielte Angriffe auf die Gesundheitsversorgung global sichtbar; es schafft eine Datengrundlage für evidenzbasierte Prävention und Schutzstandards; es etabliert Rechenschaftspflicht, indem Angriffe auf Gesundheitseinrichtungen als solche benannt und dokumentiert werden. Diese drei Funktionen sind für Cyberangriffe ebenso relevant wie für kinetische und sind unabhängig von bewaffneten Konflikten bedeutsam.

Resolution WHA 65.20 der Weltgesundheitsversammlung, die das Mandat des SSA beschreibt, nutzt zudem einen weiten Angriffsbegriff, indem sie nur von »attacks« spricht. Nach humanitärem Völkerrecht schließen Angriffe auf Gesundheitsinfrastruktur grundsätzlich auch digitale Angriffe ein, denn ein Cyberangriff, der ein Krankenhaus funktionsunfähig macht, unterscheidet sich in seiner Wirkung nicht grundlegend von einem physischen Angriff. Die konzeptionelle Anschlussfähigkeit ist damit gegeben. Das Mandat selbst bleibt indes auf Angriffe in komplexen humanitären Notlagen beschränkt. Eine Erweiterung des SSA um ein Cybermodul, das nicht an diese Voraussetzung gebunden ist, ist der naheliegende nächste Schritt zur Beseitigung der identifizierten Lücke.

Handlungsempfehlungen

Cyberangriffe auf die Gesundheitsinfrastruktur sind eine systemische Bedrohung für die öffentliche Gesundheit und die nationale Sicherheit. Die Angriffe sind disruptiv und die entwendeten Daten sensibel. Die Fälle Stryker, Octapharma und Hipocrate belegen, dass ihre Wirkung entlang komplexer Versorgungsketten verläuft. Cyberrisiken für die öffentliche Gesundheit

sind analog zu systemischen Risiken im Finanzsektor zu betrachten.

Angesichts der Gefährdungslage im Gesundheitsbereich sollte die Bundesregierung Cybersicherheit im Gesundheitssektor als Thema im Nationalen Sicherheitsrat behandeln. Dieser könnte ein Zentrum von Stabsstellen für die 18 kritischen Infrastrukturen einrichten, um stärker als Scharnier zwischen lokaler, europäischer und internationaler Politikebene zu fungieren. Die spezifische sektorale Vulnerabilität wäre der Ausgangspunkt der Lagebilder und Analysen. Anders als das BSI, das primär Meldungen entgegennimmt und technische Mindeststandards setzt, oder das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das operative Krisenvorsorge koordiniert, läge die Funktion dieser Stabsstellen in der analytischen Interpretation und fachlichen Bewertung systemischer Risiken.

Als flankierende Maßnahme könnte die WHO durch die Weltgesundheitsversammlung mandatiert werden, offizielle Meldedaten und öffentlich zugängliche Vorfallsdaten mit ihrer Fachexpertise im Gesundheitsbereich in einem speziellen Monitoring zu vereinen. Zum Beispiel könnte das SSA der WHO um ein Cybermodul erweitert werden. BSI, ENISA und die Europäische Kommission könnten ihre Erfahrungen mit interoperablen und gestaffelten Meldesystemen (DORA aus dem EU-Finanzsektor, NIS-2) teilen, um diese Erfahrungen für die Cybersicherheit im Gesundheitssektor nutzbar zu machen. Expertise zu methodischen Fragen könnten wissenschaftliche, interdisziplinäre Open-Source-Projekte wie EuRepoC liefern.

Ein strukturiertes Monitoring der gesundheitlichen Auswirkungen von Cyberangriffen könnte aggregiert das Ausmaß der Folgen messen, die Cyberangriffe auf die öffentliche Gesundheit haben. Dabei würden nationale Einrichtungen in ihrer jeweiligen Regulation weiterhin als Meldehubs dienen, die WHO übernähme die weitere Auswertung. Ein Vorbild für das Vorgehen bei der Erfassung kann das System der Internationalen Atomenergiebehörde (IAEA) sein, das auf der vertraulichen und anonymisierten Weiterleitung von Vorfallsdaten basiert. In diesem Sinne wäre auch eine tiefergehende Analyse der konkreten und systemischen Auswirkungen auf die Gesundheitsversorgung denkbar, ohne dass Sicherheits- oder Reputationskosten für die meldenden Staaten und Einrichtungen entstünden. Gleichzeitig erhielten die Institutionen und Regierungen als meldende Instanzen einen Vorteil, weil so eine Bewertung von national, europäisch und international gemeldeten Vorfällen ermöglicht wird, die erst eine Einschätzung der Kritikalität des eigenen Gesundheitssektors erlaubt.

Im Finanzsektor gibt es bereits ähnliche Meldeprozesse, die über viele Jahre eingeübt sind. Als Blaupause für die Auswertung von Vorfällen durch die WHO kann die Arbeitsweise der Deutschen Bundesbank dienen. Diese analysiert als Facheinrichtung, inwiefern Cyberangriffe ein systemisches Risiko für die Stabilität des Finanzsystems darstellen. Dafür kann sie einerseits auf Meldedaten zurückgreifen, andererseits aber auch auf öffentlich verfügbare Vorfallsdaten, wie sie EuRepoC bereithält; dies ermöglicht einen breiten Überblick über die globale Cybersicherheitslage.

Lagebilder im Bereich kritischer Infrastrukturen — und insbesondere im Gesundheitssektor — sollten künftig fachlich wie technisch systematisiert bzw. interoperabel werden, um nationale, europäische und internationale Krisenreaktionen effektiver zu gestalten. Die Stärkung der Resilienz im Gesundheitssektor erfordert bei Cyberangriffen, dass nationale, europäische und internationale Schutzmaßnahmen zusammengedacht werden.

Dr. Michael Bayerlein ist Senior Policy Analyst im Global Health Policy Lab (GHPL). Dr. habil. Annegret Bendiek ist Senior Fellow in der Forschungsgruppe EU / Europa und Principal Investigator im Projekt »European Repository of Cyber Incidents«. Jonas Hemmelskamp ist Datenwissenschaftler im Projekt »European Repository of Cyber Incidents«, Universität Heidelberg. Dr. med. Maik von der Forst ist Stellvertretender Leiter der Stabsstelle Krisen- und Katastrophenmanagement, Universitätsklinikum Heidelberg.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1611-6364
ISSN (Online) 2747-5018
DOI: 10.18449/2026A36