Rat der
Europäischen Union

Brüssel, den 16. Januar 2025
(OR. en)

5426/25

CYBER 21
SAN 15

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	15. Januar 2025
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2025) 10 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN Europäischer Aktionsplan für die Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern

Die Delegationen erhalten in der Anlage das Dokument COM(2025) 10 final.

Anl.: COM(2025) 10 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 15.1.2025
COM(2025) 10 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

Europäischer Aktionsplan für die Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern

1. Einleitung

Das Sicherheitsumfeld der EU verändert sich rasch, und wir sind Zeugen einer Eskalation von hybriden Angriffen und Cyberangriffen, die darauf abzielen, unsere Gesellschaft zu destabilisieren, Spaltungen und Störungen herbeizuführen, aber auch Profite durch Cyberkriminalität zu erlangen. Europa muss daher dringend seine Abwehrbereitschaft und Widerstandsfähigkeit gegenüber dieser neuen Realität stärken, und zwar in allen Sektoren und im Einklang mit einem gesamtgesellschaftlichen und ressortübergreifenden Ansatz, wie im Bericht des Sonderberaters der Präsidentin der Europäischen Kommission, Sauli Niinistö, gefordert.

Sichere und resiliente Gesundheitssysteme sind ein Eckpfeiler des Sozialmodells der EU. Krankenhäuser und Gesundheitssysteme stehen jedoch vor wachsenden Bedrohungen, insbesondere durch Ransomware-Banden, die sie aus finanziellen Gründen, wegen des großen Wertes der Patientendaten, einschließlich elektronischer Patientenakten, ins Visier nehmen. Das Gesundheitswesen ist in der Tat in den letzten vier Jahren zu dem am häufigsten angegriffenen Sektor in der EU geworden, auch während der COVID-19-Pandemie, als die Gesundheitsinfrastrukturen zunehmend Ziel von Cyberangriffen wurden. Cyberangriffe auf Krankenhäuser und Gesundheitsdienstleister führen zu direkten Schäden für die Menschen, weil sich medizinische Abläufe verzögern, die Arbeit in den Notaufnahmen stillsteht und im Extremfall sogar Menschen sterben.

Diese Probleme werden durch den laufenden digitalen Wandel im Gesundheitswesen noch verschärft. Digitale Gesundheitsdienste und die Nutzung und Weiterverwendung von Gesundheitsdaten können Versorgungsmodelle ermöglichen, die besser auf die Bedürfnisse und Vorlieben der Menschen und Patienten zugeschnitten sind, indem sie von vornherein dem Auftreten von Krankheiten vorbeugen helfen oder eine frühzeitigere Behandlung ermöglichen. Die Integration digitaler Werkzeuge und Lösungen in klinische Prozesse sowie die Nutzung und Weiterverwendung von Gesundheitsdaten können zu besseren klinischen Entscheidungen führen, zur Automatisierung im Gesundheitswesen beitragen und eine schnellere und bessere Versorgung der Patienten ermöglichen. Digitale Werkzeuge, Datennutzung und Medizinprodukte, die häufig mit dem Internet verbunden und durch künstliche Intelligenz (KI) gesteuert werden, sind unverzichtbar geworden, um Herausforderungen wie den Mangel an Fachkräften im Gesundheitswesen zu bewältigen.

Gleichzeitig erweitern digitale Werkzeuge aber auch die Palette potenzieller Angriffsziele für Cyberkriminelle. Überdies scheuen bestimmte staatliche Akteure nicht davor zurück, Gesundheitseinrichtungen ins Visier zu nehmen, wie der anhaltende Angriffskrieg Russlands gegen die Ukraine zeigt. Der Gesundheitssektor wird so im Rahmen einer umfassenderen hybriden Kampagne zu einem potenziellen Ziel für Cyberangriffe. Cyberangriffe gefährden nicht nur die Sicherheit der Patienten, sondern untergraben auch das Vertrauen der Öffentlichkeit in die Gesundheitsinfrastrukturen und verursachen erhebliche Wiederherstellungskosten. Über die Abwehr von Cyberangriffen hinaus sind resiliente und sichere digitale Infrastrukturen aber auch wichtig für die Umsetzung und vollständige Einführung des europäischen Gesundheitsdatenraums[1] (EHDS).

[1] https://www.consilium.europa.eu/en/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/.

Daher ist es an der Zeit, die Cybersicherheit und Resilienz der europäischen Krankenhäuser und Gesundheitsdienstleister zu steigern und zu stärken, wie Präsidentin von der Leyen in ihren politischen Leitlinien für die Kommission 2024-2029[2] betonte. Mit diesem Aktionsplan wird der Dringlichkeit der Lage und den einzigartigen Bedrohungen, denen der Sektor ausgesetzt ist, Rechnung getragen. Es gibt keine Wunderwaffe zur Bewältigung der Cybersicherheitsprobleme im Gesundheitswesen. Stattdessen werden in diesem Aktionsplan – aufbauend auf dem vorhandenen Fachwissen der europäischen Cybersicherheitsbranche – eine verstärkte Prävention, eine verbesserte Abwehrbereitschaft und ein besser koordiniertes Solidaritätskonzept gefordert. Daher spiegelt der Aktionsplan das Sicherheitskonzept der EU wider, das in der anstehenden europäischen Strategie für die innere Sicherheit weiterentwickelt und formalisiert wird. Darin soll eine umfassende Reaktion zur Bewältigung aller Bedrohungen der inneren Sicherheit festgelegt werden. Der Schwerpunkt wird auf der Fähigkeit liegen, Bedrohungen vorherzusehen, Schaden zu verhindern und die Menschen zu schützen, wobei auf allen Ebenen ein gesamtgesellschaftlicher Ansatz verfolgt wird.

Das Gesundheitswesen umfasst eine Vielzahl von Einrichtungen und Akteuren, darunter Krankenhäuser, Kliniken, Pflegeheime, Rehabilitationszentren und verschiedene Gesundheitsdienstleister. Dazu gehören aber auch die pharmazeutische, medizinische und biotechnologische Industrie, Hersteller von Medizinprodukten und Gesundheitsforschungseinrichtungen. Der Schwerpunkt dieses Aktionsplans liegt in erster Linie auf der Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern, d. h allen natürlichen oder juristischen Personen oder sonstigen Einrichtungen, die im Hoheitsgebiet eines Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringen[3]. Krankenhäuser und Gesundheitsdienstleister sind eng mit anderen Gesundheitseinrichtungen verflochten, und sie sind den Menschen am nächsten. Gleichzeitig sollten bei Maßnahmen zur Erhöhung der Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern auch Risiken für die Lieferkette und das Ökosystem im weiteren Sinne berücksichtigt werden, die beispielsweise von Einrichtungen ausgehen, die Gesundheitsdaten für Zwecke der Forschung und des maschinellen Lernens nutzen oder Medizinprodukte herstellen, insbesondere digitale medizinische Geräte, die mit dem Internet oder anderen Geräten („Internet der Dinge“) verbunden sind.

Die Sicherung der Gesundheitssysteme fällt zwar in erster Linie in die Zuständigkeit der Mitgliedstaaten, jedoch ist das Gesundheitswesen gleichzeitig auch ein kritischer Sektor im Sinne der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der EU (NIS-2-Richtlinie)[4]. Cyberkriminelle und andere Bedrohungsakteure sind grenzüberschreitend tätig, und die Herausforderungen, vor denen Gesundheitseinrichtungen im Bereich der Cybersicherheit stehen, sind in allen Mitgliedstaaten ähnlich. Eine Zusammenarbeit auf europäischer Ebene ist daher wichtig, um bewährte Verfahren auf EU-Ebene und auf nationaler Ebene auszutauschen und zu verbreiten. Deshalb werden im Aktionsplan eine Koordinierung und Maßnahmen auf EU-Ebene vorgeschlagen. Gleichzeitig

[2] https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en.
[3] Artikel 3 Buchstabe g der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32011L0024.
[4] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie), https://eur-lex.europa.eu/eli/dir/2022/2555.

werden die Mitgliedstaaten aufgefordert, selbst tätig zu werden, um die Gesundheitsversorgung und das weitere Gesundheitsökosystem voranzubringen.

Der Schwerpunkt des Aktionsplans liegt auf dem Kapazitätsaufbau im Gesundheitswesen im Hinblick auf die **Prävention** von Cybersicherheitsvorfällen, denn Vorbeugen ist immer besser als Heilen. Zweitens enthält der Aktionsplan Maßnahmen zur Verbesserung des Informationsaustauschs im Bereich der Cybersicherheit und der Fähigkeit zur **Erkennung** von Cyberbedrohungen, um eine schnellere Reaktion zu ermöglichen. Drittens beinhaltet er Maßnahmen für eine bessere **Reaktion** auf Sicherheitsvorfälle und für eine rasche **Wiederherstellung**. Schließlich sieht der Aktionsplan Möglichkeiten vor, um Akteure, von denen Cyberbedrohungen ausgehen, von Angriffen auf die Gesundheitssysteme in Europa **abzuschrecken**.

Die Umsetzung des Aktionsplans wird Hand in Hand mit den Gesundheitsdienstleistern und dem weiteren Gesundheitsökosystem, den Mitgliedstaaten und den Cybersicherheitskreisen erfolgen. Dabei wird es auf ein kooperatives Vorgehen ankommen, um die wirksamsten Maßnahmen genauer festzulegen und zu verfeinern, damit alle kritischen Gesundheitsdienstleister in Europa davon profitieren können. Deshalb wird diese Mitteilung von einer umfassenden Konsultation der Interessenträger, der Branche und der Mitgliedstaaten begleitet. Die internationale Zusammenarbeit ist für die Cybersicherheit wichtig, weil Cyberbedrohungen von Natur aus grenzenlos und vernetzt sind. Vergleichbare Cybersicherheitsbedrohungen bestehen auch in den Erweiterungs- und Nachbarschaftsländern sowie in anderen strategischen Partnerländern der EU. Dadurch kann letztlich auch die Sicherheit kritischer Infrastrukturen in der EU in Gefahr geraten. Es wird somit wichtig sein, die bei der Umsetzung des Aktionsplans gewonnenen Erkenntnisse auch in der Zusammenarbeit der EU sowohl mit Erweiterungsländern als auch mit anderen Partnerländern je nach Bedrohungslage zu berücksichtigen.

2. Das Cybersicherheitsproblem der Krankenhäuser und Gesundheitsdienstleister

Cyberbedrohungen im Gesundheitswesen

Cyberangriffe nehmen weltweit und auch innerhalb der EU zu, wobei die Bedrohungslage immer komplexer und dynamischer wird. Die Fortschritte im Bereich der KI verschaffen kriminellen und böswilligen Akteuren immer leistungsfähigere Werkzeuge, mit denen sie die Präzision und Wirkung ihrer Operationen erhöhen können, und verändern gleichzeitig die Möglichkeiten der Cyberabwehr, indem sie automatisierte Schutzmaßnahmen und Echtzeit-Vorkehrungen gegen Angriffe ermöglichen.

Ransomware ist nach wie vor eine große Herausforderung für die Cybersicherheit in der EU und weltweit. In einem Bericht werden ihre weltweiten jährlichen Kosten bis 2031 auf mehr als 250 Mrd. EUR geschätzt[5]. Wenn Ransomware-Kriminelle zuschlagen, verschlüsseln sie nicht nur die Daten ihrer Opfer, um Lösegeld zu erpressen, sondern geben zunehmend auch sensible Informationen weiter, um zusätzlich Druck auszuüben. Eine weitere große Herausforderung sind Schwachstellen in Software und Hardware: nach Angaben der Agentur der Europäischen Union für Cybersicherheit

[5] Cybersecurity Ventures (1. Juni 2024): „Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031“. Abrufbar unter: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

(ENISA)[6] ist das Gesundheitswesen der Sektor, aus dem die meisten Sicherheitsvorfälle im Zusammenhang mit solchen Schwachstellen gemeldet wurden[7]. Andere wachsende Bedrohungen sind verteilte Überlastungsangriffe (DDoS-Angriffe), die darauf ausgelegt sind, ein angegriffenes Zielsystem mit einer Flut von Anfragen zu überlasten und es so für rechtmäßige Nutzer unerreichbar zu machen[8].

Im Gesundheitssektor sind ähnliche Bedrohungstendenzen im Bereich der Cybersicherheit zu beobachten, wobei der Schwerpunkt auf Ransomware-Angriffen liegt. Nach Angaben der ENISA handelte es sich bei 54 % der analysierten Cybersicherheitsvorfälle im Gesundheitssektor im Zeitraum 2021-2023 um Ransomware-Angriffe. 83 % der Angriffe waren finanziell motiviert, was den hohen Wert der Daten aus dem Gesundheitswesen belegt, während 10 % der Angriffe aus ideologischen Gründen erfolgte[9]. Ebenso wurde in einem Bericht der Kommission aus dem Jahr 2024 festgestellt, dass bei 71 % der Angriffe, die sich auf die Patientenversorgung auswirkten (verzögerte Behandlung und Diagnose, eingeschränkte Verfügbarkeit von Notdiensten), Ransomware eingesetzt wurde[10]. Ransomware-Angriffe können sich besonders beeinträchtigend auf die Erbringung von Gesundheitsdienstleistungen auswirken und die Sicherheit der Patienten in Gefahr bringen. Außerdem gehen Ransomware-Angriffe häufig mit Verletzungen der Vertraulichkeit von Patientendaten einher[11], die häufig auch sensible Gesundheitsdaten enthalten, wodurch das Grundrecht der Menschen auf Schutz ihrer personenbezogenen Daten verletzt wird.

Gleichzeitig wird mit der zunehmenden Digitalisierung der Gesundheitsversorgung auch die mögliche Angriffsfläche immer größer. Dem Bericht über den Stand der digitalen Dekade 2024 zufolge können durchschnittlich 79 % der EU-Bürgerinnen und -Bürger in der Primärversorgung online auf ihre elektronischen Patientenakten zugreifen[12]. Elektronische Patientenakten, klinische Informationssysteme, Workflow-Systeme in Krankenhäusern, IT-Systeme für die Erstattung von Behandlungskosten, medizinische Bildgebungssysteme und Medizinprodukte, die zu Diagnose- oder Patientenüberwachungszwecken verwendet werden, sind allesamt Beispiele für digitale Werkzeuge, die einerseits eine wichtige Rolle bei der Steigerung der Effizienz und Leistungsfähigkeit des Gesundheitssektors spielen können, andererseits aber auch potenzielle Ziele von Cybersicherheitsangriffen sind. Bestimmte Gesundheitsversorgungstätigkeiten wie Intensivpflege und radiologische Bildgebung oder bestimmte medizinische Fachgebiete wie Onkologie und Kardiologie,

---

[6] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (Rechtsakt zur Cybersicherheit), http://data.europa.eu/eli/reg/2019/881/oj.

[7] ENISA-Bericht zur Bedrohungslage: Gesundheitssektor (Juli 2023).

[8] ENISA-Bericht zur Bedrohungslage 2024.

[9] ENISA-Bericht zur Bedrohungslage: Gesundheitssektor (Juli 2023). Darin wurden Gesundheitsdienstleister sowie andere Arten von Einrichtungen analysiert, darunter solche, die gesundheitsbezogene Forschung betreiben, aber auch Hersteller bestimmter gesundheitsbezogener Produkte, Gesundheitsbehörden, Krankenversicherungen, stationäre Behandlungseinrichtungen und Sozialdienstleister. Abrufbar unter: https://www.enisa.europa.eu/publications/health-threat-landscape.

[10] Europäische Kommission: Gemeinsame Forschungsstelle (JRC), Reina, V. und Griesinger, C., Cyber security in the health and medicine sector – A study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings, Amt für Veröffentlichungen der Europäischen Union, 2024, https://data.europa.eu/doi/10.2760/693487.

[11] Nach dem ENISA-Bericht zur Bedrohungslage im Gesundheitssektor wurde bei 43 % der untersuchten Ransomware-Vorfälle eine Datenschutzverletzung oder ein Datendiebstahl nachgewiesen.

[12] Bericht über den Stand der digitalen Dekade 2024.

die in hohem Maße von Digitaltechnik abhängen, sind einem besonderen Risiko von Cyberangriffen ausgesetzt. Darüber hinaus können Probleme in den Lieferketten dazu führen, dass Geräte mit unzureichender Cybersicherheit angeschafft werden, wodurch bestehende allgemeine Risiken noch verschärft werden.

So wurden beispielsweise während der COVID-19-Pandemie große Teile des irischen Gesundheitssystems durch einen Ransomware-Angriff lahmgelegt, was dazu führte, dass in 31 der betroffenen 54 Akutkrankenhäuser am Morgen des Vorfalls zumindest einige Dienste ausfallen mussten[13]. Die Gesundheitsdienste mussten auf Papieraufzeichnungen zurückgreifen, was die Tätigkeiten verlangsamte und ihre Effizienz verringerte. Der Angriff erfolgte mit einer Phishing-E-Mail, die einen Schädling im Anhang enthielt[14]. Der Vorfall zeigte, dass sich Cyberangriffe über verschiedene Systeme hinweg ausbreiten können und es daher wichtig ist, die gesamte mögliche Angriffsfläche einer Gesundheitseinrichtung zu schützen. Außerdem verdeutlichte er, wie wichtig es ist, für eine grundlegende Cyberhygiene- und Cybersicherheitskultur in allen Organisationen zu sorgen.

Cybersicherheitsreife der Krankenhäuser und Gesundheitsdienstleister

Das Gesundheitswesen in der EU ist sehr vielfältig und weist in Bezug auf Eigentumsverhältnisse, Struktur und Größe der Krankenhäuser und anderen Gesundheitsdienstleister in den einzelnen Mitgliedstaaten große Unterschiede auf. In einigen Fällen wird die Gesundheitsversorgung zentral auf nationaler Ebene geleitet, in anderen dagegen auf regionaler und lokaler Ebene; Gesundheitsdienstleister können sich sowohl in öffentlicher als auch privater Hand befinden. Darüber hinaus kann es innerhalb ein und desselben Landes Unterschiede geben, wenn z. B. zwischen den Regionen erhebliche sozioökonomische und territoriale Unterschiede bestehen, die ein komplexes Bild ergeben. Daraus können große Probleme für ein derart komplexes Gesundheitswesen erwachsen, etwa bei schweren Gesundheitskrisen infolge übertragbarer Krankheiten wie der COVID-19-Pandemie, aber auch bei anderen Gesundheitsrisiken, z. B. im Zusammenhang mit dem Klimawandel. Schließlich gibt es auch erhebliche Unterschiede und eine Fragmentierung in Bezug auf den Grad der Digitalisierung und die Einführung neuer Technik durch die Gesundheitsdienstleister. Ein Beispiel für diese Komplexität ist, dass ein durch einen Cybersicherheitsvorfall verursachter Ausfall von Diensten zu schweren Schäden und Beeinträchtigungen für Patienten führen kann, und zwar selbst in kleinen Gesundheitseinrichtungen, z. B. in Kliniken oder bei medizinischen Notdiensten, die unverzichtbare Dienste für eine relativ geringe Zahl von Nutzern erbringen.

Nach dem ENISA-Bericht über den Stand der Cybersicherheit in der Union 2024[15] hat die Cybersicherheit des EU-Gesundheitswesens eine mittlere Reife erreicht, wobei es zwischen den Gesundheitseinrichtungen in Europa aber große Unterschiede beim Reifegrad im Bereich der Cybersicherheit gibt. Mängel bestehen in wichtigen Aspekten wie ausreichendes Personal, Kenntnisse der Organisationen über ihre Lieferketten im Bereich der Informations- und

[13] Irish Health Service Executive (2021): ‘Conti cyber attack on the HSE: Independent Post Incident Review’.
[14] Irish Health Service Executive: ‘Cyber-attack and HSE response’. Abrufbar unter: https://www2.hse.ie/services/cyber-attack/what-happened/.
[15] ENISA: Bericht über den Stand der Cybersicherheit in der Union 2024 (September 2024). Abrufbar unter: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

Kommunikationstechnologie (IKT) und Installation aktueller Sicherheitsmerkmale in den Produkten. Der Sektor tut sich mit grundlegenden Maßnahmen der Cyberhygiene und mit grundlegenden Sicherheitsmaßnahmen schwer. Dies wird durch die Tatsache verdeutlicht, dass fast alle befragten Gesundheitseinrichtungen Probleme mit der Durchführung von Bewertungen der Cybersicherheitsrisiken haben und fast die Hälfte von ihnen noch nie eine Risikobewertung durchgeführt hat[16].

Eine weitere große Herausforderung für die Cybersicherheit von Krankenhäusern ist die Schnittstelle zwischen Informationstechnik (IT) und operativer Technik (OT), bei der unterschiedliche Sicherheitsprioritäten in Bezug auf Vertraulichkeit, Verfügbarkeit und Zuverlässigkeit aufeinandertreffen und wo eine Sicherheitsverletzung in einem Bereich Auswirkungen auf den anderen haben kann. Im ENISA-Bericht über den Stand der Cybersicherheit in der Union 2024 wird ferner betont, dass der Gesundheitssektor infolge der großen Vielfalt von Gesundheitseinrichtungen, Geräten und Produkten bei der Gewährleistung der Sicherheit der dort verwendeten IKT-Produkte und -Prozesse unzureichend abschneidet.

Diese Vielfalt stellt in Verbindung mit dem unterschiedlichen Stand des Cyberbewusstseins des Personals und des Managements von Krankenhäusern eine komplexe Herausforderung für die Gewährleistung der Cybersicherheit der Gesundheitssysteme dar. So hatten laut der Eurobarometer-Umfrage 2024 zu Cyberkompetenzen in den vergangenen zwölf Monaten nur 25 % der befragten Unternehmen im Gesundheits-, Bildungs- und Sozialwesen Schulungen oder Sensibilisierungsmaßnahmen zur Cybersicherheit für ihr Personal durchgeführt[17]. Es besteht daher Handlungsbedarf, um eine Kultur des Cybersicherheitsbewusstseins unter den an vorderster Front tätigen Angehörigen der Gesundheitsberufe zu fördern. Weitere Schwachstellen, die die Cybersicherheit von Gesundheitsdienstleistern gefährden, sind Personalrotationen, geteilte Arbeitsplatzrechner, ein schlechtes Authentifizierungsmanagement und die Verwendung von Wechseldatenträgern[18].

In vielen Fällen werden IT und OT zumindest teilweise an Dienstleister ausgelagert. Die Eurobarometer-Umfrage von 2024 ergab, dass der Anteil der Unternehmen, die zumindest einige Aspekte ihrer Cybersicherheit auslagern, im Gesundheits-, Bildungs- und Sozialwesen mit 57 % der befragten Unternehmen am höchsten ist[19]. Ebenso gibt es einen deutlichen Trend zur Umstellung auf Cloud-Computing, der zurückzuführen ist auf den Bedarf an skalierbarer Datenspeicherung und -verwaltung, Kosteneffizienz, verbesserter Zusammenarbeit und Unterstützung fortgeschrittener Technologien wie der KI und des Internets der medizinischen Dinge. Im Jahr 2022 nutzten 58 % der Gesundheitseinrichtungen eine Cloud-gestützte Plattform für digitale Gesundheitsdienste[20]. Dieser

[16] ENISA-Bericht zur Bedrohungslage: Gesundheitssektor (Juli 2023). Abrufbar unter: https://www.enisa.europa.eu/publications/health-threat-landscape.
[17] Flash-Eurobarometer 547 zu Cyber-Kompetenzen (Mai 2024). Abrufbar unter: https://europa.eu/eurobarometer/surveys/detail/3176.
[18] Panacea – People-centric cybersecurity in healthcare (2021): White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres.
[19] Flash-Eurobarometer 547 zu Cyber-Kompetenzen (Mai 2024). Abrufbar unter: https://europa.eu/eurobarometer/surveys/detail/3176.
[20] ENISA: Bericht über NIS-Investitionen 2022 (November 2022). Abrufbar unter: https://www.enisa.europa.eu/publications/nis-investments-2022.

Wandel kann zwar erhebliche Effizienzgewinne bringen, birgt aber auch Risiken, die fundierte Entscheidungen über die Auftragsvergabe und eine sichere Konfiguration erforderlich machen.

Über allen diesen Herausforderungen steht die übergeordnete Frage des Kapazitätsaufbaus und der Finanzierung. Die Finanzierung der Cybersicherheit im Gesundheitswesen ist bislang ungenügend und bleibt ein allgemeines Problem in der gesamten EU[21]. Zudem sind diese Finanzierungsprobleme vor dem Hintergrund alternder Bevölkerungen zu sehen, die in den kommenden Jahrzehnten in den europäischen Gesundheitssystemen einen weitverbreiteten Haushaltsdruck erzeugen dürften.

Die anhaltende Nutzung veralteter Werkzeuge und Systeme, begrenzte Ressourcen zur Prävention oder Bewältigung von Sicherheitsvorfällen und Lücken in der Cybersicherheitsreife sind häufig auf Finanzierungslücken zurückzuführen. Krankenhäuser stehen vor der ständigen Herausforderung, eine moderne, sichere und digitale Infrastruktur mit anderen notwendigen Investitionen zur Verbesserung der Patientenversorgung in Einklang zu bringen, etwa für die Einstellung von Ärzten und anderen Angehörigen der Gesundheitsberufe, die Einführung neuartiger Diagnose- und Behandlungsmethoden und die Anschaffung neuer Geräte. Nach ENISA-Angaben[22] rangiert der Gesundheitssektor beim Anteil der Ausgaben für Informationssicherheit an den gesamten IT-Ausgaben nur an siebter Stelle von 12 untersuchten Sektoren, wobei der Median im Gesundheitswesen 8,3 % beträgt.

3. Europäisches Unterstützungszentrum für Cybersicherheit für Krankenhäuser und Gesundheitsdienstleister

Der EU-Rahmen für die Cybersicherheit bietet eine breite Palette von Instrumenten, die eingesetzt werden sollten, um Krankenhäuser und Gesundheitsdienstleister sicherer und resilienter zu machen. Zur Bewältigung der zahlreichen genannten Herausforderungen muss ein einheitliches, strategisches Konzept auf EU-Ebene entwickelt werden, das die erforderlichen Ressourcen, Fachkenntnisse und Instrumente zusammenführt, um den Cyberbedrohungen wirksam entgegenzutreten. Ein umfassender Überblick sowie eine bessere Planung und Koordinierung sind wichtig, damit Gesundheitsdienstleistern in der gesamten EU dabei geholfen werden kann, sich selbst besser zu verteidigen. Dazu ist die ENISA im Rahmen ihres Auftrags[23], die kritischen Infrastrukturen der EU zu schützen und zu unterstützen, am besten in der Lage, innerhalb ihrer Organisation ein spezielles **Europäisches Unterstützungszentrum für Cybersicherheit für Krankenhäuser und Gesundheitsdienstleister**[24] einzurichten.

Das Unterstützungszentrum sollte schrittweise **einen umfassenden Dienstleistungskatalog aufstellen, der den Bedürfnissen von Krankenhäusern und Gesundheitsdienstleistern entspricht** und die ganze Palette der verfügbaren Dienste für Abwehrbereitschaft, Prävention, Erkennung und Reaktion enthält. In

[21] Die Organisation und Durchführung der Gesundheitsdienste und der medizinischen Versorgung fällt nach Artikel 168 des Vertrags über die Arbeitsweise der Europäischen Union in die Zuständigkeit der Mitgliedstaaten, und die Finanzierung der Gesundheitssysteme unterscheidet sich von einem Mitgliedstaat zum anderen.
[22] ENISA: Bericht über NIS-Investitionen 2022 (November 2022). Abrufbar unter: https://www.enisa.europa.eu/publications/nis-investments-2022.
[23] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).
[24] In dieser Mitteilung wird synonym dafür der Begriff „Unterstützungszentrum“ verwendet.

Zusammenarbeit mit den Behörden der Mitgliedstaaten und ausgehend von den Erfahrungen der Krankenhäuser und Gesundheitsdienstleister sollte das Unterstützungszentrum ein benutzerfreundliches und leicht zugängliches Verzeichnis aller auf europäischer, nationaler und regionaler Ebene verfügbaren Instrumente aufstellen. Bei der Wahrnehmung seiner Tätigkeiten sollte es für eine geeignete Koordinierung mit den Mitgliedstaaten sorgen und bei Bedarf die Festlegung von Prioritäten und die Durchführung von Maßnahmen in Echtzeit unterstützen.

Als wichtigen Baustein für die Aufstellung des Dienstleistungskatalogs des Unterstützungszentrums wird die Kommission die Einleitung von Pilotprojekten in der gesamten EU vorschlagen. Diese Projekte sollen bewährte Verfahren für die Bewertung der Cyberhygiene und der Sicherheitsrisiken entwickeln und sich mit der nötigen fortlaufenden Überwachung der Cybersicherheit, mit Bedrohungsanalysen und der Reaktion auf Sicherheitsvorfälle mithilfe modernster Cybersicherheitslösungen befassen. Die Ergebnisse dieser Pilotprojekte, die aus dem Programm Digitales Europa finanziert und vom Europäischen Kompetenzzentrum für Cybersicherheit (ECCC) durchgeführt werden sollen, werden sodann in weitere Maßnahmen auf EU-Ebene und in die Arbeit des Unterstützungszentrums einfließen.

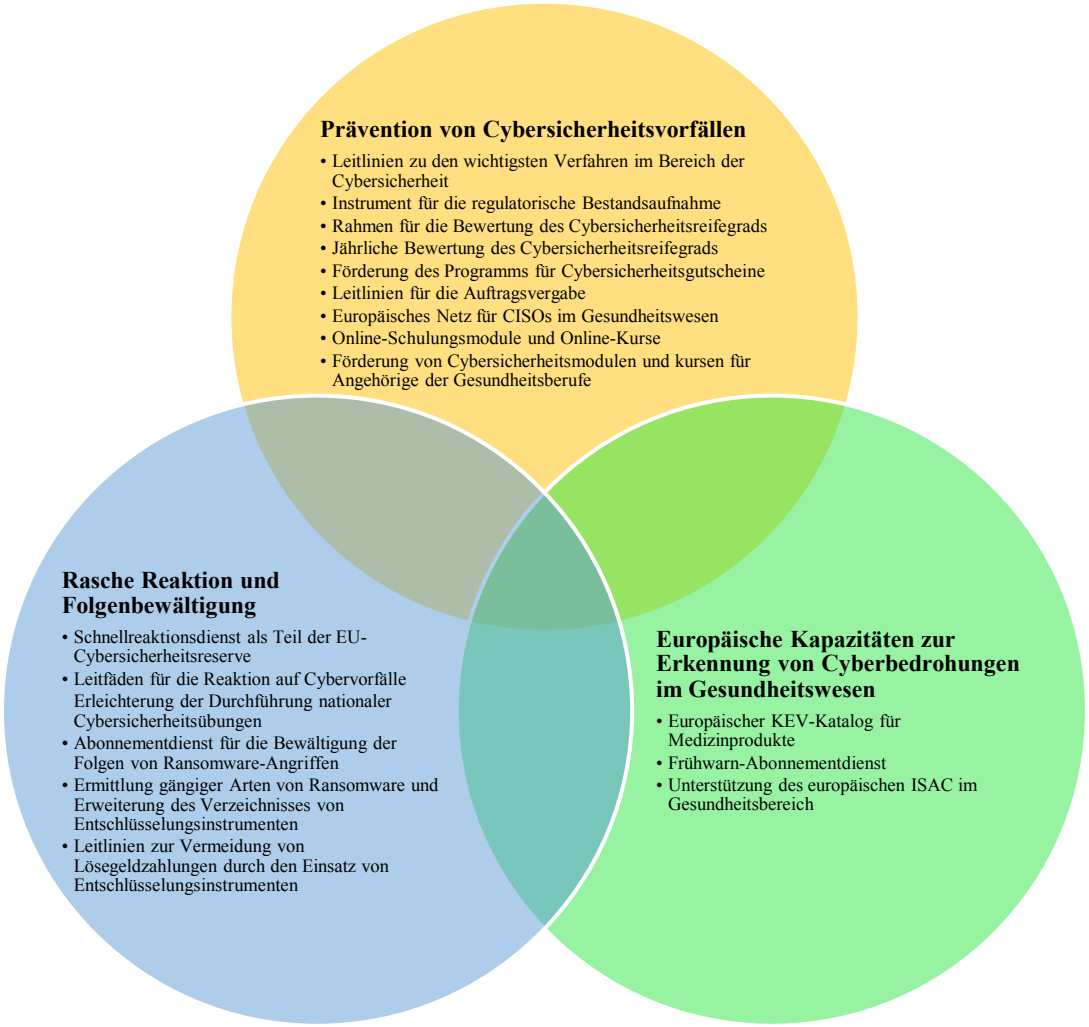

Abbildung 1: Konzepte für den Dienstleistungskatalog des Unterstützungszentrums für Krankenhäuser und Gesundheitsdienstleister

3.1. Prävention von Cybersicherheitsvorfällen

Einfache Maßnahmen zur Verringerung der Wahrscheinlichkeit von Sicherheitsvorfällen

Grundlegende Cybersicherheitsmaßnahmen wie die Sicherstellung, dass die Systeme stets auf dem neuesten Stand gehalten werden, die Verwaltung von Sicherungskopien und die Umsetzung der Multifaktor-Authentifizierung können Organisationen vor schätzungsweise bis zu 98 % solcher Angriffe schützen[25]. Viele der wirksamsten Maßnahmen für die Cyberhygiene und das Risikomanagement sind relativ einfach zu treffen, sodass mit wenig Aufwand schon eine deutliche Verbesserung der Cybersicherheit erreicht werden kann. Eine der Hauptaufgaben des Unterstützungszentrums sollte daher darin bestehen, **klare und gezielte Leitlinien zu entwickeln, um die wichtigsten Cybersicherheitsverfahren herauszustellen und den Gesundheitsdienstleistern bei der Umsetzung zu helfen**. Diese Unterstützung darf nicht auf große Krankenhäuser beschränkt bleiben, sondern muss auch eine maßgeschneiderte Beratung kleinerer Einrichtungen umfassen, wie z. B. von örtlichen Arztpraxen und Spezialkliniken, die sich oft keine besonderen Cybersicherheitsteams leisten können, aber genauso anfällig für Angriffe sind. Darüber hinaus ist die regionale Bedeutung bestimmter Gesundheitseinrichtungen für die Patientenversorgung, beispielsweise in dünn besiedelten Gebieten, zu berücksichtigen. Gesundheitsforschungseinrichtungen, die große Mengen an sensiblen personenbezogenen Daten verarbeiten, würden ebenfalls von Leitlinien für grundlegende Cybersicherheitsmaßnahmen zur Verbesserung ihrer Resilienz profitieren.

Gesundheitseinrichtungen unterliegen auch einer Reihe EU-rechtlicher Verpflichtungen in Bezug auf ihre Cybersicherheit[26]. Diese Verpflichtungen sind zwar von entscheidender Bedeutung, um eine hohes

[25] Microsoft Digital Defense Report 2022. Abrufbar unter: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[26] Wie die NIS-2-Richtlinie; Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyberresilienz-Verordnung), https://eur-lex.europa.eu/eli/reg/2024/2847/ojhttps://eur-lex.europa.eu/eli/reg/2024/2847/oj/deu; Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, https://eur-lex.europa.eu/eli/reg/2017/745/ojhttps://eur-lex.europa.eu/eli/reg/2017/745/oj (Medizinprodukte-Verordnung), https://eur-lex.europa.eu/eli/reg/2017/745/oj/, die Medizinprodukte-Verordnung; Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika (In-vitro-Diagnostika-Verordnung), https://eur-lex.europa.eu/eli/reg/2017/746/ojhttps://eur-lex.europa.eu/eli/reg/2017/746/oj; Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr (Datenschutz-Grundverordnung), https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679; Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Verordnung über künstliche Intelligenz), https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R1689; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten, COM(2022) 197 final, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:52022PC0197. Die Verhandlungen endeten im Frühjahr 2024 mit einer politischen Einigung. Nach der Fertigstellung des Textes dürfte die Veröffentlichung im Amtsblatt voraussichtlich im Frühjahr 2025 erfolgen.

gemeinsames Grundniveau der Cybersicherheit und Datensicherheit zu gewährleisten, gleichzeitig muss aber unbedingt sichergestellt werden, dass die Regulierung nicht unnötig schwierig und aufwendig in der Anwendung ist. Eine allzu strenge Betonung der Einhaltung der Vorschriften sollte dem Ziel, eine starke Cybersicherheitskultur zu fördern, nicht zuwiderlaufen. **Ein leicht zugängliches Instrument für die regulatorische Bestandsaufnahme kann helfen, den Verwaltungsaufwand für Unternehmen, die mehreren Rechtsrahmen unterliegen, so gering wie möglich zu halten**. Neben der Ausarbeitung von Leitlinien und Instrumentarien sollte das Unterstützungszentrum eng mit der Kommission und den Mitgliedstaaten zusammenarbeiten, um ein solches Bestandsaufnahmeinstrument so bald wie möglich zu entwickeln und zu verbreiten. Das Unterstützungszentrum würde daher eine wichtige Rolle dabei spielen, die Cybersicherheitsvorschriften leicht verständlich und umsetzbar zu machen, indem es z. B. Umsetzungsleitlinien[27] bereitstellt und nötigenfalls die einschlägige Normung fördert.

Ein weiteres Instrument zur Erleichterung der einfachen Umsetzung guter Cyberhygienepraktiken sind die künftigen **europäischen Brieftaschen für die digitale Identität**. Die Verringerung der Abhängigkeit von schwachen Identifizierungsmechanismen wie Passwörtern ist entscheidend, um die Risiken des unbefugten Zugangs zu Gesundheitsdaten zu mindern. Hierbei kommt es darauf an, die Umstellung auf sichere Anmeldelösungen, die auf einer zuverlässigen Identifizierung beruhen, zu vollziehen. Die europäische Brieftasche für die digitale Identität bietet eine harmonisierte, EU-weite Möglichkeit für die elektronische Identifizierung von Angehörigen der Gesundheitsberufe und wird ab Ende 2026 eine solide und einheitliche Lösung zur Verfügung stellen. Alle Online-Gesundheitsinformationssysteme, die eine starke Nutzerauthentifizierung umsetzen müssen, werden verpflichtet sein, ab Ende 2027 die Brieftasche für Identifizierungszwecke zu akzeptieren[28].

Abwehrbereitschaft und gezielte Unterstützung

Tests der Abwehrbereitschaft, die Maßnahmen wie Penetrationstests umfassen, sind ein Eckpfeiler einer wirksamen Cybersicherheit, und die Kommission hat der ENISA bereits Mittel für Pilotinitiativen zur Abwehrbereitschaft zugewiesen. Dies verdeutlicht, dass das Gesundheitswesen zu den Sektoren gehört, in denen der Bedarf an Tests und weiteren Bewertungen zur Ermittlung von Lücken bei der Cybersicherheitsreife am größten ist. Mit dem Inkrafttreten der Cybersolidaritätsverordnung werden diese Bemühungen unter Federführung des ECCC erheblich ausgeweitet. Um diesem Erfordernis Rechnung zu tragen, wird die Kommission in Absprache mit der NIS-Kooperationsgruppe, EU-CyCLONe[29] und der ENISA prüfen, ob das Gesundheitswesen ein Sektor ist, für den im Rahmen der Cybersolidaritätsverordnung Unterstützung für **koordinierte Tests der Abwehrbereitschaft** gewährt werden kann. Darüber hinaus sollte das Unterstützungszentrum einen **maßgeschneiderten Rahmen für die Bewertung der Cybersicherheitsreife speziell für die Gesundheitsversorgung** entwickeln. Eine solche Bewertung des Reifegrads würde den Einrichtungen verwertbare Einblicke in ihre Schwachstellen geben und es ihnen ermöglichen, ihre Cybersicherheitsbereitschaft gegenüber Patienten und Interessenträgern nachzuweisen und so Vertrauen in ihre Dienste aufzubauen. Auf aggregierter Ebene

[27] Für Ausarbeitung von Leitlinien für die Auslegung der Datenschutz-Grundverordnung (DSGVO) ist der Europäische Datenschutzausschuss (EDSA) zuständig. Bei der Ausarbeitung von Leitlinien durch die ENISA sind die Befugnisse des EDSA uneingeschränkt zu beachten.
[28] Artikel 5f Absätze 1 und 2 der Verordnung (EU) Nr. 910/2014.
[29] Netzwerk der Verbindungsorganisationen für Cyberkrisen (*Cyber Crisis Liaison Organisation Network*, EU-CyCLONe).

sollte das Unterstützungszentrum eine **jährliche Bewertung der Cybersicherheitsreife im Gesundheitswesen** durchführen, die einen klaren Überblick über die Cybersicherheit des Gesundheitswesens sowohl auf nationaler als auch auf EU-Ebene geben würde.

Das Gesundheitswesen ist bei Cybersicherheitsdiensten in hohem Maße auf externe Auftragnehmer angewiesen[30], was die Notwendigkeit einer gezielten Unterstützung zur Stärkung der Resilienz unterstreicht. Aufbauend auf erfolgreichen Initiativen wie den EU-Innovationsgutscheinen **sollten die Mitgliedstaaten gezielte Maßnahmen wie Cybersicherheitsgutscheine für kleinste, kleine und mittlere Krankenhäuser und Gesundheitsdienstleister in Erwägung ziehen**. Mithilfe solcher Gutscheine könnte die Einführung spezifischer Cybersicherheitsmaßnahmen unterstützt werden. Die Gutscheine sollten vorrangig aufgrund der Ergebnisse von Tests der Abwehrbereitschaft und von Reifebewertungen vergeben werden.

Das lokale Wissen und die Gegebenheiten vor Ort sind für die wirksame Einführung von Gutscheinen oder anderen Unterstützungsprogrammen von entscheidender Bedeutung, um die Relevanz und Zugänglichkeit zu gewährleisten. Mit EU-Mitteln wie z. B. aus dem Europäischen Fonds für regionale Entwicklung werden bereits Initiativen in den Bereichen Cybersicherheit und digitales Gesundheitswesen unterstützt; daher könnten sie auch zur Entwicklung von Systemen gezielter Cybersicherheitsgutscheine für Gesundheitsdienstleister herangezogen werden. Im Zuge dieser Bemühungen würde das Unterstützungszentrum mit den Mitgliedstaaten und den regionalen Programmplanungsbehörden zusammenarbeiten, um die Entwicklung solcher regionaler Gutscheinprogramme zu unterstützen, und zwar ausgehend von den Lehren aus bestehenden nationalen Projekten sowie aus den im Rahmen des Programms Digitales Europa finanzierten Maßnahmen, damit eine praktische und wirkungsvolle Umsetzung gewährleistet wird.

Darüber hinaus tragen die Horizont-Programme seit 2014 maßgeblich zur Finanzierung einer Reihe von Forschungsinitiativen bei, deren Schwerpunkt auf der Stärkung der Resilienz von Gesundheitseinrichtungen wie Krankenhäusern gegenüber Cyberbedrohungen und der Minderung der Risiken im Zusammenhang mit dem Missbrauch neuer Technologien liegt. Zu den Ergebnissen zählen eine Reihe spezialisierter Instrumente, Rahmen und Systeme wie Risikobewertungsinstrumente, Plattformen für den Schutz der Privatsphäre, kryptografische Lösungen, Schulungsprogramme zur Sensibilisierung für Cybersicherheit und Systeme zur Erkennung von Bedrohungen in Echtzeit. Insbesondere wurden diese Lösungen durch reale Pilotimplementierungen im Gesundheitswesen gründlich validiert, um ihre Wirksamkeit und praktische Anwendbarkeit beim Schutz vor Cyberbedrohungen sicherzustellen.

Sicherung der Lieferketten in der Gesundheitsversorgung

Eine zentrale Herausforderung für Gesundheitseinrichtungen ist die Verwaltung komplexer IKT-Lieferketten, die eine Reihe von Produkten wie vernetzte Medizinprodukte, Systeme für elektronische Patientenakten und Bürohardware umfassen. Krankenhäuser und Gesundheitsdienstleister benötigen für ihren Betrieb zuverlässige und sichere IKT-Systeme und -Dienste. Als Beitrag zur Bewältigung der

[30] Siehe den ENISA-Bericht über NIS-Investitionen 2023 (November 2023), in dem die große Bedeutung der externen Unterstützung bei der Prüfung und Einhaltung der Cybersicherheit hervorgehoben wird. Abrufbar unter: https://www.enisa.europa.eu/publications/nis-investments-2023.

Herausforderungen im Bereich der Cybersicherheit im Gesundheitswesen sollte die NIS-Kooperationsgruppe eine **koordinierte Sicherheitsrisikobewertung durchführen, in der sowohl technische als auch strategische Risiken im Zusammenhang mit den Lieferketten für Medizinprodukte bewertet und Abhilfemaßnahmen vorgeschlagen werden**[31]. Gegebenenfalls sollte die NIS-Kooperationsgruppe dabei mit der Koordinierungsgruppe Medizinprodukte zusammenarbeiten.

Die Cyberresilienzverordnung bildet einen neuen, umfassenden Rahmen, mit dem Cybersicherheitsanforderungen für die Planung, Konzeption und Entwicklung sowie für die Behandlung und Meldung aktiv ausgenutzter Schwachstellen und die Bereitstellung entsprechender Sicherheits-Patches in Bezug auf fast alle Hardware- und Softwareprodukte auf allen Stufen der Wertschöpfungskette festgelegt werden[32]. Medizinprodukte sind eine Produktart, die in einem der empfindlichsten Bereiche unserer Gesellschaft verwendet wird. Die Cybersicherheitsanforderungen an diese Produkte ergeben sich aus den bereits bestehenden Verordnungen über Medizinprodukte und In-vitro-Diagnostika[33]. Bei der laufenden Bewertung dieser Verordnungen wird das Potenzial für mehr Kohärenz und Synergien zwischen diesen Rahmen untersucht, um eine Vereinfachung und den neuesten Stand der Cybersicherheit zu gewährleisten.

Darüber hinaus sollten die Ergebnisse der Risikobewertung den Gesundheitseinrichtungen bei der Überprüfung ihrer Verfahren im Bereich der Cybersicherheit in der Lieferkette gemäß der NIS-2-Richtlinie helfen und könnten in die Entwicklung neuer **Vergabeleitlinien**[34] einfließen. Diese Leitlinien, die von der ENISA mithilfe ihres Unterstützungszentrums entwickelt würden, sollten die jüngsten Trends widerspiegeln, wie z. B. die Verlagerung der Speicherung von Patientendaten in die Cloud, einschließlich der Notwendigkeit einer sicheren Migration elektronischer Gesundheitsdaten in Cloud-Umgebungen. Darüber hinaus sollten die neuen Leitlinien den Einrichtungen praktische Instrumente an die Hand geben, damit sie ihre Lieferketten nachvollziehen können, was auch Anbieter verwalteter Sicherheitsdienste, Bescheinigungsberichte oder Risikobewertungen Dritter einschließt.

Im Cloud-Bereich sind weitere Maßnahmen erforderlich, um die einzigartigen Herausforderungen des Umgangs mit sensiblen Gesundheitsdaten, einschließlich erhöhter Sicherheit, Privatsphäre und operativer Risiken, zu bewältigen. Um die Sicherheitsvorkehrungen zu stärken, empfehlen Sachverständige für Cloud-Dienste die Einbettung der Sicherheit durch Voreinstellungen und Technikgestaltung („*Security by Default and by Design*“). Dabei wird einer sicheren Infrastruktur, einem proaktiven Schwachstellenmanagement und einer Mischung aus staatlichen und privaten Cloud-Lösungen Vorrang eingeräumt. Eine kontinuierliche Überwachung und anbieterspezifische Bescheinigungen – wie z. B. Zertifizierungen von Sicherheitsanbietern und Prüfungen der Konformität

[31] Nach Artikel 22 der NIS-2-Richtlinie.
[32] In einem ersten Schritt müssen ab dem 1. August 2025 breit gefasste Kategorien von Funkanlagen, die nicht in den Anwendungsbereich der Verordnung über Medizinprodukte und der Verordnung über In-vitro-Diagnostika fallen, die grundlegenden Anforderungen der Funkanlagenrichtlinie in Bezug auf die Cybersicherheit erfüllen, wenn sie im Binnenmarkt in Verkehr gebracht werden. In einer zweiten Phase wird die Cyberresilienzverordnung ab dem 11. Dezember 2027 Anwendung finden.
[33] Im Dezember 2019 veröffentlichte die Kooperationsgruppe Medizinprodukte Leitlinien zur Cybersicherheit von Medizinprodukten, mit denen die Hersteller bei der Erfüllung der Anforderungen aus Anhang I der beiden Verordnungen unterstützt werden, https://ec.europa.eu/docsroom/documents/41863.
[34] Aufbauend auf den ENISA-Vergabeleitlinien für Cybersicherheit in Krankenhäusern 2020 (Februar 2020). Abrufbar unter: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

mit nationalen und internationalen Normen – sind ebenfalls unerlässlich, um solide Sicherheitspraktiken zu gewährleisten.

Bei Diensten wie *Infrastructure-as-a-Service* (IaaS), *Platform-as-a-Service* (PaaS) und *Software-as-a-Service* (SaaS) obliegt die Umsetzung der Sicherheitsvorkehrungen häufig dem Kunden. Viele Gesundheitseinrichtungen verfügen jedoch nicht über die Ressourcen, um diese Anforderungen selbst zu erfüllen. Zu diesem Zweck **sollten Cloud-Diensteanbieter angehalten werden, grundlegende Sicherheitsmaßnahmen von vornherein als Standardmerkmal umzusetzen**. Diese Maßnahmen würden das Risiko von Fehlkonfigurationen verringern, einen einheitlichen Schutz in allen vom Kunden selbst verwalteten Umgebungen aufrechterhalten und den Nutzern eine größere Sicherheit bieten. Die Festlegung eines Standard-Sicherheitsszenarios würde darauf abzielen, einen soliden Schutz mit Praktikabilität in Einklang zu bringen und die Nutzbarkeit für ein breites Spektrum von Gesundheitseinrichtungen zu gewährleisten. Diese Bemühungen würden eine enge Zusammenarbeit zwischen Cloud-Anbietern und dem Gesundheitswesen erfordern, um bewährte Verfahren der Branche zur Entwicklung wirksamer und skalierbarer Lösungen zu nutzen.

Schulungen und Kompetenzentwicklung

Arbeitskräfte mit nachgefragten Kompetenzen sind wichtig für ein langfristiges nachhaltiges Wachstum und für die Wettbewerbsfähigkeit in Europa sowie für hochwertige Dienstleistungen, einschließlich Gesundheitsdienstleistungen. Der Mangel an qualifizierten Cybersicherheitsfachkräften stellt in ganz Europa eine große Herausforderung dar, wobei schätzungsweise 299 000 Fachkräfte fehlen, um den Bedarf auf dem Arbeitsmarkt in der EU zu decken[35]. Laut der Eurobarometer-Umfrage von 2024 zu Cyber-Kompetenzen[36] sehen 81 % der Unternehmen Schwierigkeiten bei der Einstellung von Cybersicherheitspersonal als ein wesentliches Risiko mit Blick auf potenzielle Cyberangriffe. In den Bereichen Bildung, Gesundheit und Sozialwesen werden 66 % der Aufgaben im Bereich der Cybersicherheit mit Beschäftigten besetzt, die von Stellen außerhalb der Cybersicherheit wechseln, was den dringenden Bedarf an Umschulung und Weiterbildung unterstreicht.

Um dieser Herausforderung zu begegnen, sollte das Unterstützungszentrum mit dem künftigen Konsortium für eine europäische Digitalinfrastruktur (*European Digital Infrastructure Consortium*, EDIC) für Cybersicherheitskompetenzen zusammenarbeiten, das in der Mitteilung der Kommission über die Akademie für Cybersicherheitskompetenzen vorgesehen ist[37]. Die Arbeit sollte den Austausch zwischen Cybersicherheitsfachkräften im Gesundheitswesen, wie z. B. leitenden Beauftragten für Informationssicherheit (*Chief Information Security Officers*, CISOs), erleichtern. Eine mögliche Maßnahme wäre die Schaffung eines **europäischen Netzes für CISOs im Gesundheitswesen**, beginnend mit einem Pool von Sachverständigen für den Austausch und die Entwicklung bewährter Verfahren, von Strategien zur Bindung von Talenten und von Lösungen, um Cybersicherheitsfachkräfte für den Gesundheitssektor zu gewinnen. Darüber hinaus sollten im Rahmen der Akademie für

[35] The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study | Plattform für digitale Kompetenzen und Arbeitsplätze.
[36] Flash-Eurobarometer 547 zu Cyber-Kompetenzen.
[37] Mitteilung der Kommission an das Europäische Parlament und den Rat: Schließung der Fachkräftelücke im Cybersicherheitsbereich zur Förderung der Wettbewerbsfähigkeit, des Wachstums und der Resilienz in der EU („Akademie für Cybersicherheitskompetenzen"), COM(2023) 207 final.

Cybersicherheitskompetenzen Ressourcen entwickelt werden, um den Personalbestand im Bereich der Cybersicherheit im Gesundheitswesen mit Unterstützung von Industrie und Wissenschaft zu auszubauen. In diesem Zusammenhang sollten die Interessenträger aus der Branche angehalten werden, Unterstützung für die Verbesserung von Schulungen im Bereich der Cybersicherheit zu leisten.

Cybersicherheitsvorfälle im Gesundheitswesen sind nach wie vor in hohem Maße auf menschliches Versagen zurückzuführen. Das verdeutlicht, dass eine umfassende Schulung der Mitarbeitenden und eine Schärfung des Cyberbewusstseins dringend erforderlich sind. Angesichts der häufigen Nutzung digitaler Werkzeuge durch Angehörige der Gesundheitsberufe ist es unabdingbar, ihnen das nötige Wissen über sichere Verfahrensweisen zu vermitteln. Gezielte Schulungs- und Sensibilisierungskampagnen können die Risiken erheblich verringern. Zu diesem Zweck sollte das Unterstützungszentrum mit Angehörigen der Gesundheitsberufe und Anbietern von Gesundheitsdienstleistungen sowie mit Anbietern der allgemeinen und beruflichen Bildung, der Industrie, dem EDIC für Cybersicherheitskompetenzen und den Behörden der Mitgliedstaaten zusammenarbeiten, um **umfassende, leicht zugängliche Online-Schulungsmodule und -Kurse** zu erstellen und zu verbreiten.

Die Einbeziehung von digitalen Kompetenzen und Cybersicherheitsmodulen in die Lehrpläne ist für den Aufbau eines soliden Fundaments für die Cybersicherheit im Gesundheitswesen unverzichtbar. Solche Module sollten sektorspezifische Fragen wie Patientendatenschutz und Schwachstellen bei der Sicherheit von Medizinprodukten behandeln. Bei der Entwicklung dieser Ressourcen sollten frühere Maßnahmen wie das im Rahmen des Programms Erasmus+ finanzierte Projekt BeWell[38] und das im Rahmen von Horizont 2020 finanzierte Projekt PANACEA[39] berücksichtigt werden.

3.2. Europäische Kapazitäten zur Erkennung von Cyberbedrohungen im Gesundheitswesen

Eine wirksame Erkennung von Cyberbedrohungen ist die Voraussetzung für eine rasche Reaktion auf Sicherheitsvorfälle. Bedrohungsakteure können Techniken einsetzen, die die Erkennung eines erfolgreichen Eindringens erschweren, wodurch ein längerer unbefugter Zugriff auf ein System möglich wird[40]. Daher können bessere Kapazitäten zur Erkennung von Bedrohungen dazu beitragen, Cyberangriffe aufzuhalten. Bei dem Ransomware-Angriff auf den finnischen Psychotherapie-Anbieter Vastaamo, bei dem der Täter Patienten erpresste, deren vertrauliche Patientenakten gestohlen worden waren, kam es beispielsweise schon 2018 zu einem ersten Eindringen, das dem Anbieter aber erst 2020 bekannt wurde[41].

Ein effizienter Informationsaustausch und eine effiziente Zusammenarbeit sind unentbehrlich, um die Erkennung von Bedrohungen und die Lageerfassung in der gesamten EU zu verbessern. Computer-Notfallteams (*Computer Security Incident Response Teams*, CSIRTs) spielen eine entscheidende Rolle bei der Entgegennahme von Meldungen über Sicherheitsvorfälle, Beinahe-Vorfälle und potenzielle

[38] BeWell – Blueprint alliance for a future health workforce strategy on digital and green skills. Abrufbar unter: https://bewell-project.eu/.
[39] PANACEA – Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for data and people. Abrufbar unter: https://cordis.europa.eu/project/id/826293.
[40] ENISA Health Threat Landscape 2023.
[41] Beschluss 1150/161/2021 des finnischen Datenschutzbeauftragten.

Bedrohungen und stellen Leitlinien für Risikominderungsmaßnahmen auf nationaler Ebene bereit. **Die Mitgliedstaaten werden jedoch nachdrücklich aufgefordert, auch alle Meldungen von Krankenhäusern und Gesundheitsdienstleistern über Cybersicherheitsvorfälle an das Unterstützungszentrum der ENISA weiterzuleiten, um eine EU-weite Lageerfassung zu ermöglichen.** Im Idealfall sollte dies mit einer aussagekräftigen Beschreibung der verschiedenen relevanten Dimensionen der Sicherheitsvorfälle einhergehen, einschließlich bekannter ursächlicher Schwachstellen und Auswirkungen auf Gesundheitsdienste sowie unerwünschter Folgen in Bezug auf Patienten. Darüber hinaus werden die Hersteller von Medizinprodukten und In-vitro-Diagnostika aufgefordert, aktiv ausgenutzte Schwachstellen oder schwerwiegende Cybervorfälle, die sich auf die Sicherheit ihrer Geräte auswirken, sowie potenziell andere Schwachstellen, Sicherheitsvorfälle, Beinahe-Vorfälle oder Cyberbedrohungen, die sich auf das Risikoprofil dieser Geräte auswirken können, über die von der ENISA im Rahmen der Cyberresilienzverordnung einzurichtende und verwaltete zentrale Meldeplattform freiwillig zu melden.

Soweit die in den Berichten enthaltenen Informationen nicht mehr sensibel sind, könnte das Unterstützungszentrum einen von der ENISA finanzierten europäischen Katalog bekannter ausgenutzter Schwachstellen (*Known Exploited Vulnerabilities*, KEV) für Medizinprodukte, elektronische Patientendatensysteme und Anbieter von IKT-Geräten und Software im Gesundheitswesen erstellen. Um erheblichen Herausforderungen bei der Erkennung von Bedrohungen zu begegnen, sollte das Unterstützungszentrum **einen EU-weiten Frühwarn-Abonnementdienst für das Gesundheitswesen einführen, der echtzeitnahe Warnmeldungen ausgibt**. Dieser Dienst würde sich auf verarbeitete Daten von CSIRTs, Gesundheitseinrichtungen und Herstellern, auf frei zugängliches Wissen (*Open Source Intelligence*, OSINT) und auf Daten anderer einschlägiger Akteure wie Cyber-Hubs, Informationsaustausch- und -analysezentren (*Information Sharing and Analysis Centres*, ISACs) und Strafverfolgungsbehörden stützen. Eine verstärkte Zusammenarbeit zwischen der ENISA und der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) – beispielsweise in Bezug auf cyberkriminelle Handlungsmuster im Gesundheitswesen – würde das Lagebewusstsein weiter verbessern helfen.

Die ISACs dienen als zentrale Ressourcen für Erkenntnisse über Cyberbedrohungen, fördern den wechselseitigen Informationsaustausch zwischen dem öffentlichen und dem privaten Sektor und fördern die Vertrauensbildung. Das Unterstützungszentrum sollte dem **europäischen ISAC im Gesundheitsbereich** vermehrt mit Instrumenten und Informationsaustausch, sektorspezifischen Lageerfassungsberichten sowie Förderung einer vertrauenswürdigen Gemeinschaft für taktische und strategische Zusammenarbeit zur Seite stehen. Die Mitgliedstaaten sollten die Entwicklung nationaler ISACs im Gesundheitsbereich fördern[42]. Die ISACs sollten ferner dazu angehalten werden, Gesundheitsdienstleister und Hersteller zusammenzubringen, um zu einem gemeinsamen Verständnis der Bedrohungen der Cybersicherheit, auch in der Lieferkette, zu gelangen und einen Dialog über die

[42] So verfügt Finnland beispielsweise über ein nationales ISAC für den Sozial- und Gesundheitssektor. Siehe finnisches nationales Cybersicherheitszentrum: „ISAC information sharing groups“, abrufbar unter: https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

sichere Gestaltung von Produkten zu erleichtern, der den Realitäten der Einführung vor Ort wirklich Rechnung trägt.

3.3. Rasche Reaktion und Folgenbewältigung

Angesichts der hohen Sensibilität von Patientendaten und der potenziell verheerenden Auswirkungen von Cyberangriffen auf Gesundheitsdienste ist eine rasche und wirksame Reaktion auf Cybersicherheitsvorfälle unerlässlich, um die Sicherheit der Patienten zu gewährleisten. Wenn ein Krankenhaus oder ein Gesundheitsdienstleister mit einem Cyberangriff konfrontiert ist, ist die erste Anlaufstelle das zuständige nationale CSIRT[43]. Das CSIRT ist dafür zuständig, zeitnah – idealerweise innerhalb von 24 Stunden – Unterstützung bei der Bewältigung erheblicher Sicherheitsvorfälle zu leisten. Wenn jedoch ein Sicherheitsvorfall die Kapazität des CSIRT übersteigt, sollte EU-Unterstützung zur Verfügung stehen, um eine rasche und wirksame Reaktion zu gewährleisten.

Die mit der Cybersolidaritätsverordnung eingerichtete EU-Cybersicherheitsreserve bietet Dienste von privaten Anbietern vertrauenswürdiger Sicherheitsdienste für die Reaktion auf Sicherheitsvorfälle, um bei schwerwiegenden Cybersicherheitsvorfällen oder Cybersicherheitsvorfällen großen Ausmaßes und bei anfänglichen Wiederherstellungsbemühungen zu helfen. Diese Reserve soll die Bemühungen der CSIRTs der Mitgliedstaaten ergänzen und es ihnen ermöglichen, in Fällen, die kritische Sektoren wie das Gesundheitswesen betreffen, zusätzliche Unterstützung zu beantragen. Um dieses System zu verbessern, **sollten die Kommission und die ENISA sicherstellen, dass die Reserve einen Schnellreaktionsdienst speziell für das Gesundheitswesen umfasst**. Ergänzend zu anderen bestehenden Rahmen würde dieser Dienst Sachverständige entsenden, um schwerwiegende Cybersicherheitsvorfälle oder Cybersicherheitsvorfälle großen Ausmaßes im Gesundheitswesen unverzüglich zu bewältigen, wenn die nationale Unterstützung nicht ausreicht.

Um die Reaktion und Folgenbewältigung zu verbessern, sollte das Unterstützungszentrum in Zusammenarbeit mit der NIS-Kooperationsgruppe, dem CSIRTs-Netzwerk und gegebenenfalls Europol **maßgeschneiderte Leitfäden für die Reaktion auf Cybervorfälle im Gesundheitswesen** ausarbeiten. Diese Leitfäden würden sowohl CSIRTs als auch Gesundheitseinrichtungen bei der Reaktion auf spezifische Cybersicherheitsbedrohungen, einschließlich Ransomware-Angriffe, als Richtschnur dienen. Angesichts der Bedeutung einer wirksamen Zusammenarbeit zwischen CSIRTs und Strafverfolgungsbehörden bei der Reaktion auf und Untersuchung von Cybersicherheitsvorfällen krimineller Art sollten die Leitfäden unter anderem klare Anleitungen für das Melden solcher Sicherheitsvorfälle an die Strafverfolgungsbehörden enthalten. Darüber hinaus könnte das Unterstützungszentrum **auf der Grundlage der Erfahrungen aus Übungen wie „Cyber Europe 2022" (ENISA) eine breite Einführung nationaler Cybersicherheitsübungen erleichtern, um die Leitfäden zu testen und die Protokolle für die Reaktion auf Sicherheitsvorfälle zu verbessern**.

Als Grundlage für die Politikgestaltung und zur Bewertung der Wirksamkeit von Maßnahmen gegen Ransomware-Angriffe müssen weitere Daten erhoben werden. Zu diesem Zweck sollten die

[43] Gemäß Artikel 23 Absatz 1 der NIS-2-Richtlinie müssen wesentliche und wichtige Einrichtungen dem zuständigen CSIRT oder gegebenenfalls der zuständigen Behörde schwerwiegende Sicherheitsvorfälle melden.

Mitgliedstaaten Einrichtungen, die der NIS-2-Richtlinie unterliegen, einschließlich Gesundheitseinrichtungen, auffordern, zusammen mit anderen Informationen, die sie bei der Meldung erheblicher Cybersicherheitsvorfälle bereitstellen, auch geleistete und beabsichtigte Lösegeldzahlungen anzugeben. Solche Meldungen erleichtern die wirksame Untersuchung von Ransomware-Vorfällen, einschließlich der Nachverfolgung von Zahlungen auf Plattformen für den Austausch von Kryptowährungen, um die Empfänger der Zahlungen zu ermitteln.

Die Geschwindigkeit der Folgenbewältigung ist ein entscheidender Faktor für die Aufrechterhaltung der Resilienz und des Vertrauens der Öffentlichkeit, insbesondere im Gesundheitswesen, wo Ausfallzeiten die Patientenversorgung empfindlich stören können. Für eine wirksame Bewältigung der Folgen von Ransomware-Angriffen müssen die Gesundheitsdienstleister über sichere, aktuelle und separat aufbewahrte Sicherungskopien verfügen, die rasch wiederhergestellt werden können. Als Teil seines Dienstleistungskatalogs könnte das Unterstützungszentrum einen **Abonnementdienst für die Bewältigung der Folgen eines Ransomware-Angriffs anbieten, der Krankenhäusern und Gesundheitsdienstleistern dabei hilft, im Voraus Pläne für die Folgenbewältigung auszuarbeiten**. Die ENISA und Europol sollten zusammenarbeiten, um zu ermitteln, welche Art von Ransomware-Angriffen am häufigsten gegen Gesundheitseinrichtungen gerichtet ist, und das **Verzeichnis von Entschlüsselungsinstrumenten** im Rahmen des Projekts „No More Ransom“[44] **ausbauen**. Darüber hinaus sollten sie leicht zugängliche Leitlinien entwickeln und fördern, um Gesundheitsdienstleistern dabei zu helfen, Lösegeldzahlungen durch den Einsatz von Entschlüsselungsinstrumenten zu vermeiden.

Die **Internationale Initiative zur Bekämpfung von Ransomware**[45] ist ein wichtiges Forum für den Austausch über bestimmte Ransomware-Vorfälle sowie für den Aufbau der Kapazitäten der Mitgliedstaaten zur Stärkung ihrer Cybersicherheitsrahmen und ihrer Ermittlungskapazitäten gegen Ransomware-Akteure. Die Kommission wird gemeinsam mit der Hohen Vertreterin die Zusammenarbeit im Rahmen der Initiative zur Bekämpfung von Ransomware, auch gegen Bedrohungen durch Ransomware im Gesundheitswesen, weiter voranbringen. Ferner wird die Kommission eine Zusammenarbeit in der **G7-Arbeitsgruppe „Cybersicherheit“** anstreben, um die Cybersicherheit im Gesundheitswesen zu stärken. Insbesondere könnte die Arbeitsgruppe Möglichkeiten zur Unterstützung des Gesundheitswesens gegenüber bestimmten Bedrohungen wie Ransomware prüfen und dabei auf Überlegungen wie der Gemeinsamen Erklärung zu Ransomware-Angriffen auf Einrichtungen der Gesundheitsversorgung vom 8. November 2024 aufbauen, die im Rahmen des Sicherheitsrats der Vereinten Nationen vorgelegt wurde[46].

4. Nationale Maßnahmen

Die Wirksamkeit dieses Aktionsplans zur Verbesserung der Cybersicherheit im Gesundheitswesen hängt von der aktiven Mitarbeit und dem Engagement der Mitgliedstaaten ab. Zur erfolgreichen Umsetzung des Aktionsplans könnten die Mitgliedstaaten **nationale Unterstützungszentren für Cybersicherheit für Krankenhäuser und Gesundheitsdienstleister** benennen. Diese Zentren würden als

[44] https://www.nomoreransom.org/de/index.html.
[45] https://www.counter-ransomware.org/.
[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/.

Hauptanlaufstellen für das Gesundheitswesen auf nationaler Ebene fungieren und eng mit dem ENISA-Unterstützungszentrum zusammenarbeiten. Soweit möglich und relevant, sollten die Mitgliedstaaten bestehende Stellen wie nationale CSIRTs im Gesundheitsbereich oder einschlägige Behörden als nationale Unterstützungszentren für Cybersicherheit benennen.

Die Mitgliedstaaten werden außerdem angehalten, **nationale Aktionspläne mit Schwerpunkt auf der Cybersicherheit im Gesundheitswesen** aufzustellen. In diesen Plänen würden die spezifischen Cybersicherheitsrisiken, denen die Gesundheitssysteme ausgesetzt sind, und die zu ihrer Bewältigung ergriffenen nationalen Maßnahmen dargelegt und gleichzeitig sichergestellt, dass Ressourcen und Verfahren auf europäischer Ebene wirksam genutzt werden. Das ENISA-Unterstützungszentrum kann bei der Ausarbeitung dieser Pläne helfen, wobei es bereits bestehende nationale Pläne berücksichtigt und die Bemühungen koordiniert, damit die Ressourcen und Strategien der einzelnen Mitgliedstaaten einander ergänzen.

Ein weiterer Schwerpunkt für die Mitgliedstaaten ist die Erleichterung der gemeinsamen Nutzung von Ressourcen unter den Gesundheitsdienstleistern, was durch eine **gemeinsame Auftragsvergabe oder Ressourcenbündelung** auf nationaler, regionaler oder sogar europäischer Ebene erreicht werden könnte. Dieser Ansatz würde die finanzielle Belastung einzelner Einrichtungen verringern und gleichzeitig ihre Verhandlungsposition gegenüber Anbietern von Cybersicherheitsdiensten stärken.

So wurde im Zuge des französischen CaRE-Programms[47] eine Reihe von Maßnahmen auf nationaler und regionaler Ebene eingeführt, um Herausforderungen bei der Ressourcenbeschaffung zu bewältigen: Ein Cyberkatalog bietet einen Überblick über Cyberlösungen und -pakete, die Krankenhäusern über die nationale Cybersicherheitsagentur, die Agentur für das digitale Gesundheitswesen, regionale Agenturen, nationale Beschaffungsorganisationen zur Verfügung gestellt werden, sowie über kommerzielle Lösungen. Dies wird durch zusätzliche Mittel für regionale Agenturen ergänzt, um gemeinsame Ressourcen anbieten zu können.

Die Mitgliedstaaten sollten sich auch mit den unzureichenden Investitionen in die Cybersicherheit im Gesundheitswesen befassen. Um eine angemessene Finanzierung zu gewährleisten, sollten sie **unverbindliche Benchmarks festlegen und die speziell auf die Cybersicherheit ausgerichteten Finanzierungsziele verfolgen**, wobei diese Investitionen die grundlegende Patientenversorgung nicht beeinträchtigen dürfen. Diese Finanzierungsziele sollten auch darauf abzielen, bei allen digitalen Investitionen in diesem Sektor Sicherheitserwägungen zu berücksichtigen. Die Mitgliedstaaten können bewährte Verfahren und Hinweise zu diesen Zielen über Plattformen wie das Netzwerk für elektronische Gesundheitsdienste[48] austauschen.

[47] Französische Agentur für das digitale Gesundheitswesen: Cybersécurité acceleration et Résilience des Établissements (CaRE). Abrufbar unter: https://esante.gouv.fr/strategie-nationale/cybersecurite.

[48] Das Netzwerk für elektronische Gesundheitsdienste ist ein gemäß Artikel 14 der Richtlinie 2011/24/EU eingerichtetes freiwilliges Netz, mit dem die von den Mitgliedstaaten benannten, für elektronische Gesundheitsdienste zuständigen nationalen Behörden miteinander vernetzt werden.

5. Zusammenarbeit zwischen öffentlichen und privaten Stellen

Die Zusammenarbeit zwischen öffentlichen und privaten Stellen und die Konsultation von Gesundheitsdienstleistern, anderen Einrichtungen des Gesundheitswesens sowie einschlägigen Akteuren der Cybersicherheitsbranche sind für die erfolgreiche Umsetzung des Aktionsplans unverzichtbar. Um einen weiteren Beitrag zur Arbeit des Unterstützungszentrums zu leisten, **wird die Kommission mit Unterstützung der ENISA ein gemeinsames Beratungsgremium für Cybersicherheit im Gesundheitswesen einrichten**, dem hochrangige Vertreter beider Bereiche (Gesundheitsversorgung und Cybersicherheit) angehören und das die Kommission und das Unterstützungszentrum in Bezug auf wirksame Maßnahmen beraten und die Weiterentwicklung öffentlich-privater Partnerschaften in diesem Bereich erörtern kann. Das Beratungsgremium wird auf den bestehenden Bemühungen um öffentlich-private Partnerschaften, einschließlich des europäischen ISAC im Gesundheitsbereich, aufbauen.

Darüber hinaus wird die Kommission für den Bereich der Cybersicherheit einen **Handlungsaufruf** an Unternehmen, Stiftungen, Bildungseinrichtungen und Interessenträger der Branche richten, damit diese Beteiligten **Zusagen für Maßnahmen zur Bewältigung der Herausforderungen im Gesundheitswesen** machen. Aufbauend auf den Erfahrungen der Akademie für Cybersicherheitskompetenzen könnten solche Zusagen beispielsweise im Rahmen der Akademie erfolgen und die Bereitstellung von Schulungen und Materialien für Cybersicherheitsfachkräfte mit Schwerpunkt auf dem Gesundheitswesen umfassen[49]. Andere Zusagen könnten auch Sensibilisierungsmaßnahmen oder die kostenlose oder kostengünstige Bereitstellung verwalteter Sicherheitsdienste für besonders schutzbedürftige Einrichtungen betreffen, um deren Abwehrbereitschaft und Cybersicherheitsresilienz zu erhöhen. Darüber hinaus könnten die Zusagen darin bestehen, Informationen über Cyberbedrohungen an das ENISA-Unterstützungszentrum weiterzugeben. Das Unterstützungszentrum sollte einen Überblick über die im Rahmen des Handlungsaufrufs eingegangenen Zusagen führen, um deren Kohärenz und Komplementarität zu gewährleisten.

6. Abschreckung von Akteuren, von denen Cyberbedrohungen ausgehen

Die innere und auswärtige Cybersicherheitspolitik der EU sollte das Ziel verfolgen, Akteure, von denen Cyberbedrohungen ausgehen, von Angriffen auf die europäischen Gesundheitssysteme abzuhalten. Cyberangriffe auf Gesundheitseinrichtungen sind eine besonders inakzeptable Art böswilliger Cyberaktivitäten, weil sie die Sicherheit der Patienten und das Leben der Menschen gefährden können. Daher sollte die EU die volle Macht ihrer Abschreckungskapazitäten im Bereich der Cybersicherheit und der Strafverfolgung einsetzen, um das allgemeine Geschäftsmodell von Bedrohungsakteuren, die auf den Gesundheitssektor abzielen, auszubremsen und ihnen die Profitquelle zu entziehen. Dazu würde die Förderung grenzüberschreitender Ermittlungen durch einen verstärkten Austausch von Beeinträchtigungsindikatoren und anderen einschlägigen Daten genauso gehören wie eine stärkere Konzentration auf wichtige Täter und bedeutende kriminelle Mittler wie Anbieter von Bulletproof-Hosting oder Mischdiensten für Kryptowährungen.

Das **Instrumentarium für die Cyberdiplomatie** bietet einen Rahmen für die Prävention von Cyberangriffen gegen die EU, die Mitgliedstaaten und ihre Partner, aber auch die Abschreckung davon

[49] Cyber Skills Academy: Get Involved | Plattform für digitale Kompetenzen und Arbeitsplätze.

und die Reaktion darauf. Die Hohe Vertreterin wird den bestehenden Rahmen für Cybersanktionen weiterhin nutzen, um auf Bedrohungen für Gesundheitssysteme zu reagieren.

Kriminelle Akteure für ihr Handeln zur Rechenschaft zu ziehen, ist eine wichtige Abschreckungsmaßnahme. Daher sollten die Mitgliedstaaten sicherstellen, dass die Strafverfolgung vollständig in ihre nationalen Aktionspläne integriert wird. Insbesondere sollten sie die Bestimmungen der Richtlinie über Angriffe auf Informationssysteme[50] und des Budapester Übereinkommens des Europarats über Computerkriminalität[51] in vollem Umfang nutzen, um von Angriffen abzuschrecken, Straftäter vor Gericht zu stellen und kriminelle Infrastrukturen, die Angriffe erleichtern, zu zerschlagen. Durch die erfolgreiche Umsetzung dieser Instrumente sollte sichergestellt werden, dass verbrecherische und böswillige Handlungen gegen die Gesundheitsversorgung bestraft werden.

7. Umsetzung und Überwachung des Aktionsplans

In diesem Aktionsplan ist eine Reihe von Aufgaben für ein Unterstützungszentrum vorgesehen, das innerhalb der ENISA eingerichtet werden soll. Dadurch wird eine ganzheitliche und kohärente Umsetzung des Aktionsplans sichergestellt und gleichzeitig die Schaffung neuer Stellen vermieden, was zu Überschneidungen führen und Gemeinkosten verursachen kann. Die Kommission beabsichtigt, für eine angemessene Mittelausstattung des Unterstützungszentrums zu sorgen.

Sobald das Unterstützungszentrum einsatzbereit ist, sollte die ENISA in Absprache mit der Kommission dem Verwaltungsrat der ENISA sowie den einschlägigen Netzen der Mitgliedstaaten, insbesondere der NIS-Kooperationsgruppe, dem CSIRTs-Netzwerk, dem Netzwerk für elektronische Gesundheitsdienste und gegebenenfalls dem Ausschuss für den europäischen Raum für Gesundheitsdaten, regelmäßig aktuelle Informationen über die Arbeit des Unterstützungszentrums übermitteln. Darüber hinaus sollte sich die ENISA kontinuierlich mit dem öffentlich-privaten Beratungsgremium für Cybersicherheit im Gesundheitswesen über die Durchführung der vom Unterstützungszentrum bereitgestellten Maßnahmen austauschen.

Die regelmäßigen Berichte der ENISA, wie der Bericht über den Stand der Cybersicherheit in der Union, der eine aggregierte Bewertung des Reifegrads der Cybersicherheitskapazitäten und -ressourcen in der gesamten EU, auch im Gesundheitswesen, enthält, sollten als Gelegenheit dienen, einschlägige Daten zu veröffentlichen und so die Überwachung der Umsetzung des Aktionsplans zu fördern. Darüber hinaus kann der EU-Cybersicherheitsindex der ENISA[52] quantitative und qualitative Daten liefern, die als Faktenbasis für die Bewertung der Kritikalität und Ausgereiftheit des Gesundheitswesens dienen.

[50] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, https://eur-lex.europa.eu/eli/dir/2013/40/oj/deu.

[51] Übereinkommen über Computerkriminalität (Budapester Übereinkommen, ETS Nr. 185) und die dazugehörigen Protokolle, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[52] ENISA, EU Cybersecurity Index, Framework and Methodological Note (2024). Abrufbar unter: https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

8. Nächste Schritte

Mit dieser Mitteilung wird eine ehrgeizige Agenda für eine größere Cybersicherheit im Gesundheitswesen in der EU festgelegt. Mit der vorgeschlagenen Einrichtung des Unterstützungszentrums für Cybersicherheit für Krankenhäuser und Gesundheitsdienstleister im Herzen der ENISA wird im Aktionsplan ein Weg für die Schaffung eines kohärenten und gemeinsamen europäischen Ansatzes zur Bewältigung der Herausforderungen der Cybersicherheit in diesem Sektor aufgezeigt.

Diese Mitteilung sollte als Beginn eines Prozesses zur Verbesserung der Cybersicherheit im Gesundheitswesen verstanden werden. Die Annahme des Aktionsplans wird daher mit der Einleitung umfassender Konsultationen der Interessenträger und der Fortsetzung des Austauschs mit den Mitgliedstaaten und einschlägigen Netzen einhergehen, um Erkenntnisse zu gewinnen. Auf der Grundlage der Ergebnisse der Konsultationen beabsichtigt die Kommission, im vierten Quartal 2025 Empfehlungen zur weiteren Präzisierung des Aktionsplans vorzulegen.

Die Kommission fordert die Mitgliedstaaten und alle Interessenträger auf, gemeinsam auf die Verwirklichung der Ziele des Aktionsplans hinzuarbeiten.

ANHANG – Überblick über die vorgeschlagenen Maßnahmen

Die Kommission wird

ENISA-Unterstützungszentrum für Cybersicherheit für Krankenhäuser und Gesundheitsdienstleister	
angemessene Ressourcen für das Unterstützungszentrum für Cybersicherheit sicherstellen mit dem ECCC zusammenarbeiten, um Pilotprojekte zur Entwicklung bewährter Verfahren für die Bewertung der Cyberhygiene und der Sicherheitsrisiken einzuleiten und der Notwendigkeit einer kontinuierlichen Überwachung der Cybersicherheit, aber auch den Erkenntnissen über Bedrohungen und die Reaktion auf Sicherheitsvorfälle mithilfe modernster Cybersicherheitslösungen und der Aufstellung des Dienstleistungskatalogs des europäischen Unterstützungszentrums für Cybersicherheit Rechnung zu tragen	2025
Prävention von Cybersicherheitsvorfällen	
in Absprache mit der NIS-Kooperationsgruppe, EU-CyCLONe und der ENISA prüfen, ob das Gesundheitswesen ein Sektor ist, für den im Rahmen der Cybersolidaritätsverordnung Unterstützung für koordinierte Tests der Abwehrbereitschaft gewährt werden kann	1. Quartal 2025
Rasche Reaktion und Folgenbewältigung	
gemeinsam mit der ENISA sicherstellen, dass die EU-Cybersicherheitsreserve einen Schnellreaktionsdienst speziell für das Gesundheitswesen umfasst	4. Quartal 2025
Zusammenarbeit zwischen öffentlichen und privaten Stellen	
mit Unterstützung der ENISA ein gemeinsames Beratungsgremium für Cybersicherheit im Gesundheitswesen einrichten	1. Quartal 2025
im Bereich der Cybersicherheit einen Handlungsaufruf an Unternehmen, Stiftungen, Bildungseinrichtungen und Interessenträger der Branche richten, damit diese Beteiligten Zusagen für Maßnahmen zur Bewältigung der Herausforderungen im Gesundheitswesen machen	2. Quartal 2025
Abschreckung von Akteuren, von denen Cyberbedrohungen ausgehen	
gemeinsam mit der Hohen Vertreterin den Einsatz von Werkzeugen des Instrumentariums für die Cyberdiplomatie prüfen, um böswillige Aktivitäten gegen Gesundheitssysteme zu verhindern, davon abzuhalten und abzuschrecken sowie um darauf zu reagieren	2025
gemeinsam mit der Hohen Vertreterin die internationale Zusammenarbeit gegen Ransomware-Akteure fördern, insbesondere im Rahmen der Internationalen Initiative zur Bekämpfung von Ransomware	2025-2026

eine Zusammenarbeit in der G7-Arbeitsgruppe „Cybersicherheit“ anstreben, um die Cybersicherheit im Gesundheitswesen zu stärken	2025-2026
Nächste Schritte	
umfassende Konsultationen der Interessenträger einleiten	1. Quartal 2025
Empfehlungen zur weiteren Präzisierung des Aktionsplans abgeben	4. Quartal 2025

Die ENISA wird

EU-Unterstützungszentrum für Cybersicherheit für Krankenhäuser und Gesundheitsdienstleister	
die Arbeiten zur Einrichtung eines EU-Unterstützungszentrums für Cybersicherheit für Krankenhäuser und Gesundheitsdienstleister aufnehmen	2. Quartal 2025
einen umfassenden Katalog von Dienstleistungen aufstellen, die vom Unterstützungszentrum für Cybersicherheit bereitzustellen sind	Ab dem 4. Quartal 2025
Prävention von Cybersicherheitsvorfällen	
Leitlinien herausgeben, in denen die wichtigsten Verfahren im Bereich der Cybersicherheit hervorgehoben werden, und Gesundheitsdienstleister bei deren Umsetzung unterstützen	3. Quartal 2025
in enger Zusammenarbeit mit der Kommission und den Mitgliedstaaten ein Instrument für die regulatorische Bestandsaufnahme entwickeln	1. Quartal 2025
einen Rahmen für die Bewertung des Cybersicherheitsreifegrads speziell für das Gesundheitswesen entwickeln	3. Quartal 2025
eine jährliche Bewertung des Cybersicherheitsreifegrads durchführen	2025-2026
mit den Mitgliedstaaten und regionalen Programmbehörden bei der Erstellung von Modellprogrammen für Cybersicherheitsgutscheine zusammenarbeiten	2025-2026
neue Leitlinien für die Auftragsvergabe im Bereich der Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern entwickeln	3. Quartal 2025
ein europäisches Netz für CISOs im Gesundheitswesen schaffen	1. Quartal 2026
Schulungsmodule und -kurse für Angehörige der Gesundheitsberufe ausarbeiten und fördern	1. Quartal 2026

Europäische Kapazitäten zur Erkennung von Cyberbedrohungen im Gesundheitswesen	
einen europäischen KEV-Katalog für Medizinprodukte, Systeme für elektronische Patientenakten und Anbieter von IKT-Geräten und Software für das Gesundheitswesen aufbauen	4. Quartal 2025
einen EU-weiten Frühwarn-Abonnementdienst für das Gesundheitswesen einführen	Ab 2026
das europäische ISAC im Gesundheitsbereich durch Instrumente und Informationsweitergabe unterstützen	2025-2026
Rasche Reaktion und Folgenbewältigung	
gemeinsam mit der Kommission sicherstellen, dass die EU-Cybersicherheitsreserve einen Schnellreaktionsdienst speziell für das Gesundheitswesen umfasst	4. Quartal 2025
in Zusammenarbeit mit dem CSIRTs-Netzwerk auf das Gesundheitswesen zugeschnittene Leitfäden für die Reaktion auf Cybervorfälle entwickeln	3. Quartal 2025
eine breit angelegte Einführung nationaler Cybersicherheitsübungen erleichtern, um die Leitfäden zu testen und die Protokolle für die Reaktion auf Sicherheitsvorfälle zu verbessern	Ab dem 4. Quartal 2025
einen Abonnementdienst für die Bewältigung der Folgen von Ransomware-Angriffen bereitstellen	Ab 2026
gemeinsam mit Europol ermitteln, welche Art von Ransomware-Angriffen am häufigsten gegen Gesundheitseinrichtungen gerichtet ist, und das Verzeichnis von Entschlüsselungstools im Rahmen des Projekts „No More Ransom“ ausbauen	4. Quartal 2025
gemeinsam mit Europol leicht zugängliche Leitlinien entwickeln, um Gesundheitsdienstleistern bei der Vermeidung von Lösegeldzahlungen zu helfen	3. Quartal 2025
Nationale Maßnahmen	
die Mitgliedstaaten bei der Ausarbeitung nationaler Aktionspläne unterstützen	2025
die Bemühungen koordinieren, damit die Ressourcen und Strategien der einzelnen Mitgliedstaaten einander ergänzen	2025-2026
Umsetzung und Überwachung des Aktionsplans	
in Abstimmung mit der Kommission die einschlägigen Netze der Mitgliedstaaten regelmäßig in Bezug auf die Arbeit des Unterstützungszentrums für Cybersicherheit auf dem neusten Stand halten	2025-2026
einen ständigen Austausch mit dem Beratungsgremium für Cybersicherheit im Gesundheitswesen pflegen	2025-2026

Die Mitgliedstaaten werden

Europäische Kapazitäten zur Erkennung von Cyberbedrohungen im Gesundheitswesen	
Meldungen von Krankenhäusern und Gesundheitsdienstleistern über Sicherheitsvorfälle im NIS-2-Rahmen regelmäßig an das europäische Unterstützungszentrum für Cybersicherheit weitergeben	Ab dem 4. Quartal 2025
die Entwicklung nationaler ISACs im Gesundheitsbereich fördern	2025-2026
Prävention von Cybersicherheitsvorfällen	
innerhalb der NIS-Kooperationsgruppe eine koordinierte Sicherheitsrisikobewertung durchführen, bei der sowohl technische als auch strategische Risiken im Zusammenhang mit Lieferketten für Medizinprodukte bewertet werden	4. Quartal 2025
Rasche Reaktion und Folgenbewältigung	
nationale Cybersicherheitsübungen einführen, um die Leitfäden zu testen und die Protokolle für die Reaktion auf Sicherheitsvorfälle zu verbessern	Ab 2026
Nationale Maßnahmen	
nationale Unterstützungszentren für Cybersicherheit für Krankenhäuser und Gesundheitsdienstleister benennen	2. Quartal 2025
nationale Aktionspläne mit Schwerpunkt auf der Cybersicherheit im Gesundheitswesen ausarbeiten	4. Quartal 2025
die gemeinsame Nutzung von Ressourcen unter den Gesundheitsdienstleistern erleichtern	2025-2026
unverbindliche Benchmarks festlegen und speziell auf die Cybersicherheit ausgerichtete Finanzierungsziele verfolgen	4. Quartal 2025
Gesundheitseinrichtungen und andere Stellen, die der NIS-2-Richtlinie unterliegen, dazu auffordern, ihre etwaige Absicht zur Zahlung von Lösegeld zu melden	4. Quartal 2025