Bundesministerium
für Gesundheit

Bundesministerium für Gesundheit, 11055 Berlin

Mauerstraße 29
10117 Berlin

Postanschrift:
11055 Berlin

Referat 512

sofortprogramm-cybersicherheit@bmg.bund.de

www.bundesgesundheitsministerium.de

Launch der Webseite „cybersicherheit-gesundheitswesen.de“

Aufruf zur Mitwirkung!

Betreff: Self-Assessments „Cybersicherheit im Gesundheitswesen“

Sehr geehrte Damen und Herren,

Cyberangriffe treffen auch Krankenhäuser, Praxen und weitere Einrichtungen des Gesundheitswesens. Die fortschreitende Digitalisierung im Gesundheitswesen führt zu einer immer stärkeren Vernetzung von Systemen und Einrichtungen und damit auch zu wachsenden Risiken für die digitale Infrastruktur. In den letzten Jahren nahmen Angriffe auf die digitalen Infrastrukturen von Gesundheitseinrichtungen stetig zu.

Gleichzeitig besteht bei vielen Gesundheitseinrichtungen weiterhin Nachholbedarf hinsichtlich des IT-Sicherheitsniveaus. Um den bestehenden Bedrohungen wirksam zu begegnen, ist es daher wichtig, eine sichere und resiliente Infrastruktur zu schaffen und adäquate Maßnahmen zur Cybersicherheit zu implementieren. Die Sicherheit digitaler Systeme ist dabei nicht nur eine technische Frage, sondern zugleich eine Frage der Patientensicherheit, des Vertrauens in die digitale Gesundheitsversorgung und der Handlungsfähigkeit von Einrichtungen im Falle eines IT-Sicherheitsvorfalls.

Zusätzlicher Handlungsdruck ergibt sich aus den regulatorischen Anforderungen der NIS-2-Richtlinie. Mit ihrer Umsetzung in nationales Recht wird der Kreis der regulierten Organisationen im Gesundheitswesen erheblich erweitert: Während bislang nur wenige hundert Einrichtungen entsprechenden Anforderungen unterlagen, sind künftig mehrere tausend Gesundheitseinrichtungen verpflichtet, deutlich umfassendere Anforderungen an die IT-Sicherheit zu erfüllen.

Für die betroffenen Organisationen bedeutet dies insbesondere die Notwendigkeit, ein umfassendes Risikomanagement im Bereich der IT-Sicherheit zu etablieren. Dies umfasst regelmäßige und systematische Risikoanalysen, klare organisatorische Prozesse zur Bewältigung von Sicherheitsvorfällen samt definierter Meldeketten bei erheblichen IT-Störungen sowie praxiserprobte Notfall- und Wiederanlauf-pläne zur Aufrechterhaltung des laufenden Betriebs im

Hinweis zu unseren Datenschutzinformationen:
Informationen zur Verarbeitung personenbezogener Daten sind in der Datenschutzerklärung des BMG zu finden: www.bundesgesundheitsministerium.de „Stichwort: Datenschutz“ (Bundesgesundheitsministerium Datenschutz). Sollten Sie keinen Internetzugang haben, kann die Information auf dem Postweg zugesandt werden.

Ernstfall. Darüber hinaus erfordert die Richtlinie eine konsequente Überprüfung und Absicherung von IT-Dienstleistern, externen Schnittstellen und der gesamten Lieferkette. Die NIS-2-Vorgaben stärken zudem die Verantwortung der Leitungsebene für die Umsetzung und Überwachung der Cybersicherheitsmaßnahmen.

Vor diesem Hintergrund wird das „Sofortprogramm Cybersicherheit“ vom Bundesministerium für Gesundheit (BMG) aufgesetzt. Das Programm richtet sich ausschließlich an Einrichtungen entlang des akut-stationären Versorgungspfads. Dazu gehören zum einen Krankenhäuser und zum anderen große Medizinische Versorgungszentren, Labore und radiologische Praxen sowie Einrichtungen zur Versorgung mit Medikamenten, Blut und Blutplasma. Wichtig ist: Nur Einrichtungen werden förderfähig sein, die den NIS-2-Vorgaben unterliegen.

Die Webseite „cybersicherheit-gesundheitswesen.de“ informiert über das Sofortprogramm Cybersicherheit und stellt den Einrichtungen entlang des akut-stationären Versorgungspfades mit dem dazugehörigen Assessment-Tool ein kostenloses Instrument zur Verfügung, um das eigene Cybersicherheits-niveau systematisch einzuschätzen und mögliche Handlungsbedarfe zu identifizieren. Das Assessment-Tool ist als strukturierter Online-Fragenkatalog mit 39 Fragen gestaltet und ermöglicht eine systematische und gleichzeitig aufwandsarme Betrachtung aller Anforderungsbereiche der NIS-2-Richtlinie.

Das Tool greift die gesetzlichen Schwerpunkte der NIS-2-Richtlinie auf und dient allen Einrichtungen als praxisnaher Einstieg in einen kontinuierlichen Verbesserungsprozess der eigenen Cybersicherheit. Der Fragenkatalog ist hierfür in 13 versorgungsrelevante Themencluster unterteilt. Dazu gehören unter anderem die Handlungsfelder „Bewältigung von Sicherheitsvorfällen“, „Risikomanagement“, die „Absicherung der Lieferkette und externer Dienstleister“, „organisatorische und personelle Sicherheit“ sowie „technische Schutzvorkehrungen“. Die Verantwortlichen der Gesundheitseinrichtungen können anhand des Fragenkatalogs schrittweise die eigenen Sicherheitsstandards evaluieren.

Die Verwendung des Assessment-Tools ist vollständig anonym und ohne Rückschluss auf die jeweilige Einrichtung möglich. Es unterstützt Gesundheitseinrichtungen dabei, den eigenen Stand der Cybersicherheit zu bestimmen und konkrete Handlungsbedarfe zu identifizieren. Zugleich leisten die teilnehmenden NIS-2 relevanten Einrichtungen einen wichtigen Beitrag dazu, die Bedarfe der Versorgungspraxis bei der weiteren Ausgestaltung des Sofortprogramms Cybersicherheit zu berücksichtigen. Das Self-Assessment ersetzt nicht die eigenverantwortliche Prüfung der Einrichtung, ob sie in den Anwendungs-bereich des BSIG fällt und der Registrierungspflicht nach § 33 BSIG unterliegt. Ein

Anspruch auf Förderung im Rahmen des Sofortprogramms Cybersicherheit wird durch die Teilnahme nicht begründet.

Der offizielle Start des Tools ist für den **28. September 2026** vorgesehen. Alle Informationen finden Sie ab diesem Tag unter cybersicherheit-gesundheitswesen.de.

Disclaimer

Die Webseite und das Assessment-Tool werden im Auftrag des Bundesministeriums für Gesundheit (BMG) durch Projektpartner betrieben. Die Erhebung und datenschutzkonforme Auswertung etwaiger Daten zu Bedarfen von Gesundheitseinrichtungen erfolgen eigenständig durch die Projektpartner. Dem BMG werden zu keinem Zeitpunkt einrichtungsbezogene Einzelergebnisse zur Verfügung gestellt; das Ministerium erhält lediglich aggregierte, anonymisierte Gesamtberichte.