NIS-2-Richtlinie im Gesundheitswesen rechtskonform umsetzen

Cyber-Resilienz für Gesundheitseinrichtungen – Anforderungen verstehen und praxisnah umsetzen

Beginn:
08.04.2027 - 09:00 Uhr

Ende:
08.04.2027 - 16:30 Uhr

Dauer:
1,0 Tag

Flex: Ostfildern oder Online

Veranstaltungsnr.: **36328.00.002**

Leitung

Dr. Thomas Liedtke

Präsenz oder Online
EUR 590,00
(MwSt.-frei)
Mitgliederpreis
EUR 531,00
(MwSt.-frei)

BESCHREIBUNG

Das Gesundheitswesen gehört zu den attraktivsten Angriffszielen für Cyberkriminelle. Ransomware-Angriffe auf Krankenhäuser, Angriffe auf Labor- und Medizintechnik oder Ausfälle klinischer Informationssysteme können nicht nur wirtschaftliche Schäden verursachen, sondern unmittelbar die Patientenversorgung gefährden.

Mit der NIS-2-Richtlinie steigen die Anforderungen an Cybersecurity, Risikomanagement und die Verantwortung der Leitungsebene erheblich. Gleichzeitig bestehen enge Wechselwirkungen mit weiteren regulatorischen Vorgaben wie der CER-Richtlinie, der DSGVO, dem KRITIS-Dachgesetz (soweit relevant), den Anforderungen des BSI sowie – je nach Einrichtung – der Medizinprodukteverordnung (MDR) und dem Cyber Resilience Act (CRA).

In diesem Seminar erfahren Sie, welche Anforderungen konkret für Einrichtungen des Gesundheitswesens gelten und wie Sie diese praxisnah, risikoorientiert und auditfähig umsetzen.

Ziel der Weiterbildung

- beurteilen, ob Ihre Einrichtung unter die NIS-2-Anforderungen fällt,
- die regulatorischen Anforderungen für Gesundheitseinrichtungen einordnen,
- Risiken für Patientenversorgung und IT systematisch bewerten,
- geeignete technische und organisatorische Maßnahmen auswählen,
- Meldepflichten bei Sicherheitsvorfällen korrekt erfüllen,
- Verantwortlichkeiten zwischen Geschäftsführung, IT und Informationssicherheit klar definieren,
- Schnittstellen zu DSGVO, MDR, CRA und ISO 27001 verstehen.

Methoden und Lern-Fokus (Vortrag, Workshop, Übungen, Fallstudien, Rollen-/Planspiele, Gruppenarbeit, Transferaufgaben, Wissenstest, etc.):

- Vortrag, Workshop, Übungen
- Fallstudien wie z.B.
  - Ransomware-Angriff auf ein Krankenhaus – Incident Response und Meldepflichten.
  - Angriff über einen externen Medizintechnik-Dienstleister – Lieferkettenrisiken und Drittparteienmanagement.
  - Einsatz einer KI zur radiologischen Bildauswertung – Zusammenspiel von NIS2, AI Act, MDR und CRA.

PROGRAMM

1. Einführung

Die Bedrohungslage im Gesundheitswesen

- aktuelle Cyberangriffe auf Krankenhäuser
- Ransomware
- Ausfall medizinischer IT
- Auswirkungen auf die Patientenversorgung

Warum steht das Gesundheitswesen besonders im Fokus?

2. NIS2 im Gesundheitswesen

- Ziele der Richtlinie
- Wer ist betroffen?
- Krankenhäuser
- Universitätskliniken
- MVZ (Medizinisches Versorgungszentrum)
- Labore
- Pflegeeinrichtungen
- Gesundheitsdienstleister
- digitale Gesundheitsdienste

Besonderheiten gegenüber anderen Branchen

3. Anforderungen an Gesundheitseinrichtungen

- Risikomanagement
- Informationssicherheitsmanagement
- Business Continuity Management
- Notfallmanagement
- Lieferketten
- Cloud-Dienste
- medizinische Geräte
- Netzwerksegmentierung
- Multi-Faktor-Authentifizierung

Praxisbeispiele

4. Incident Management

Sicherheitsvorfälle richtig behandeln

- Erkennung
- Bewertung
- Meldepflichten
- Kommunikation
- Wiederherstellung

Übung

Ransomware im Krankenhaus

5. Risikoanalyse

Praxisworkshop im Kontext des Gesundheitswesens

- Beispielszenarien
- Bedrohungen
- Schwachstellen
- Auswirkungen
- Maßnahmen

6. Schnittstellen zu weiteren Regularien

- DSGVO
- B3S Gesundheit
- ISO 27001
- BSI IT-Grundschutz
- MDR
- CRA
- AI Act
- CER

Wann gilt was?

7. Roadmap zur Umsetzung

Die ersten 100 Tage

Prioritäten

Quick Wins

- Governance
- Verantwortlichkeiten
- Risikoanalyse
- Maßnahmenplan
- Awareness
- Dokumentation

TEILNEHMER·INNENKREIS

TEILNEHMER:INNENKREIS

Geschäftsführer von Krankenhäusern, Klinikmanagement, Informationssicherheitsbeauftragte, CISO, IT-Leiter, Datenschutzbeauftragte, Qualitätsmanagement, Compliance-Beauftragte, Betreiber medizinischer IT, Hersteller digitaler Gesundheitslösungen und Unternehmen aus der MedTech

REFERENT:INNEN

Dr. Thomas Liedtke

Dr. Thomas Liedtke ist
- seit vielen Jahren beratend tätig für funktionale Sicherheit, Informations- und Produktsecurity. Er ist Mitglied der deutschen DIN-AK-Spiegelgruppe, welche für die Definition ISO/SAE 21434, ISO/PAS 5112 und weitere Cybersecuritystandards verantwortlich ist
- Mitglied des intacs Advisory Boards und Leiter der SPICE Cybersecurity Arbeitsgruppe Leiter der ZVEI Arbeitsgruppe Datensicherheit im Automobil
- Leadauditor für CSMS; ISMS; TISAX
- Berater für die Implementierung der Cybersecurity in Unternehmen Publikationen
- Informationssicherheit: Möglichkeiten und Grenzen; SpringerLink publisher: link.springer.com/book/10.1007/978-3-662-63917-7
- The New Cybersecurity Challenges and Demands for Automotive Organisations and Projects – an Insight View link.springer.com/chapter/10.1007/978-3-031-42307-9_21

Weitere Veranstaltungen

Cyber-Sicherheit für kritische Infrastrukturen: NIS2 & CER verstehen und umsetzen

Einführung in die Kryptographie: Methoden und praktische Anwendungen

Sicherheitsgerichtete Systeme entwickeln

Cyber Resilience Act (CRA) erfolgreich umsetzen

VERANSTALTUNGSORT UND HOTEL

Technische Akademie Esslingen
An der Akademie 5
73760 Ostfildern

Anfahrt

Die TAE befindet sich im Südwesten Deutschlands im Bundesland Baden-Württemberg – in unmittelbarer Nähe zur Landeshauptstadt Stuttgart. Unser Schulungszentrum verfügt über eine hervorragende Anbindung und ist mit allen Verkehrsmitteln gut und schnell zu erreichen.

Hotelübernachtung benötigt?

Über den nachfolgenden Link finden Sie nahegelegene Hotels in direkter Umgebung zu TAE-Konditionen:

Hotelbuchung

GEBÜHREN UND FÖRDERMÖGLICHKEITEN

Die Teilnahme beinhaltet Verpflegung (vor Ort) sowie ausführliche Unterlagen.

Preis:
Die Teilnahmegebühr beträgt:
590,00 € (MwSt.-frei) vor Ort
590,00 € (MwSt.-frei) pro Teilnehmer live online

Fördermöglichkeiten:
Für den aktuellen Veranstaltungstermin steht Ihnen die ESF-Fachkursförderung leider nicht zur Verfügung.

Für alle weiteren Termine erkundigen Sie sich bitte vorab bei unserer Anmeldung.

Andere Bundesland-spezifische Fördermöglichkeiten finden Sie hier.

Inhouse Durchführung:
Sie möchten diese Veranstaltung firmenintern bei Ihnen vor Ort durchführen? Dann fragen Sie jetzt ein individuelles Inhouse-Training an.

IMMER TOP!

Unser Qualitätsversprechen

Seit über 65 Jahren gehört die Technische Akademie Esslingen (TAE) mit Sitz in Ostfildern – nahe der Landeshauptstadt Stuttgart – zu Deutschlands größten Weiterbildungs-Anbietern für berufliche und berufsvorbereitende Qualifizierung im technischen Umfeld. Unser Ziel ist Ihr Erfolg. Egal ob Seminar, Zertifikatslehrgang oder Fachtagung, unsere Veranstaltungen sind stets abgestimmt auf die Bedürfnisse von Ingenieuren sowie Fach- und Führungskräften aus technisch geprägten Unternehmen. Dabei können Sie sich stets zu 100 Prozent auf die Qualität unserer Angebote verlassen. Warum das so ist?