Online-Vortrag LIVE: Cybersicherheit im Gesundheitswesen

Live-Übertragung: 24. September 2025, 13.30 – 19.00 Uhr
(inkl. 30 Min. Pause)

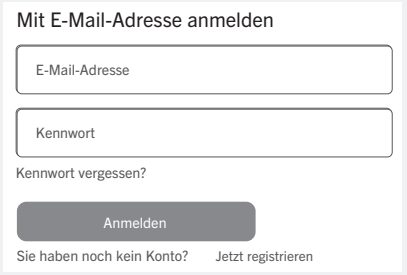
Zeitstunden: 5,0 – mit Bescheinigung nach §15 Abs. 2 FAO

Kostenbeitrag: 275,– € (USt.-befreit)
Ermäßigter Kostenbeitrag für Mitglieder der kooperierenden Rechtsanwaltskammern

Nr.: 22246504

Diese und weitere Fortbildungen aus dem Fachinstitut finden Sie hier

Anmeldung über die neue DAI-Webseite
www.anwaltsinstitut.de
mit vielen neuen Services:



- Zugriff auf alle digitalen Unterlagen zur Fortbildung: Von Arbeitsunterlage bis zur Teilnahmebescheinigung
- Komfortable Umbuchungsmöglichkeiten
- Direkter Zugriff auf alle digitalen Lernangebote
- Speichern interessanter Fortbildungen auf Ihrer persönlichen Merkliste

Die DAI Online-Vorträge LIVE

Bei einem Online-Vortrag LIVE verfolgen Sie die Veranstaltung/Fortbildung zum angegebenen Termin über das eLearning Center. Ein moderierter textbasierter Chat ermöglicht Ihnen die Interaktion mit den Referierenden und anderen Teilnehmenden. Sie benötigen nur einen aktuellen Browser, eine stabile Internetverbindung und Lautsprecher. Die Arbeitsunterlage steht elektronisch zur Verfügung.

Teilnahmebescheinigung nach §15 Abs. 2 FAO

Das DAI stellt die Voraussetzungen zum Nachweis der durchgängigen Teilnahme sowie die Möglichkeit der Interaktion während der Dauer der Fortbildung bereit. Die Online-Vorträge LIVE werden damit wie Präsenzveranstaltungen anerkannt und können für die gesamten 15 Zeitstunden genutzt werden.

Kontakt

Deutsches Anwaltsinstitut e. V.
Gerard-Mortier-Platz 3, 44793 Bochum
Tel. 0234 970640
support@anwaltsinstitut.de
Vereinsregister des Amtsgerichts Bochum: VR-Nr. 961

FAOcomplete – Ihr eLearning-Paket im DAI

Dieses eLearning-Angebot ist Bestandteil von FAOcomplete: Mit diesem eLearning-Paket können Sie sich aus unserem vielfältigen Angebot Ihre komplette FAO-Fortbildung in einem Fachinstitut komfortabel, flexibel und zu einem attraktiven Festpreis zusammenstellen. **Genauere Informationen finden Sie unter www.anwaltsinstitut.de/faocomplete**

DAI-Newsletter – Jetzt anmelden

Einfach QR-Code scannen oder unter www.anwaltsinstitut.de/dainewsletter/

DAI Deutsches Anwaltsinstitut e.V.

Fachinstitut für Informationstechnologierecht

Online-Vortrag LIVE

Cybersicherheit im Gesundheitswesen

24. September 2025
13.30 – 19.00 Uhr
Online

Peter Schüller
Rechtsanwalt (Syndikusrechtsanwalt), Director Legal

FAO complete Fachinstitut Informationstechnologierecht

www.anwaltsinstitut.de

Gemeinnützige Einrichtung der Bundesrechtsanwaltskammer, Bundesnotarkammer, Rechtsanwaltskammern und Notarkammern.

Referent

Peter Schüller, Rechtsanwalt (Syndikusrechtsanwalt), Director Legal

Inhalt

Gesundheitseinrichtungen sind mittlerweile ein beliebtes Ziel von Cyberattacken. Die Bedrohungslage ist eindeutig. Cybercrime ist ein Wirtschaftszweig im Darknet, der schon heute hunderte Millionen schwer ist. In die IT-Systeme eingeschleuste Schadsoftware verschlüsselt Daten und legt das System lahm. Zur Entschlüsselung werden Lösegeldforderungen gestellt (engl. Ransom). Bei den Angriffen handelt es sich nicht mehr nur um Aktionen der zu Kultfiguren hochstilisierten Hacker. Es sind schlicht Cyberkriminelle, die sich im Darknet zu Gruppen zusammenschließen und „Produkte" wie Ransomware-as-a-Service allen Interessierten anbieten, die Teil des Netzwerks werden wollen. Diese Affiliates, wie sie sich selbst nennen, gehen arbeitsteilig vor. Die Bandbreite reicht von harmlosen Telefonanrufen bis hin zu Phishing E-Mails und Brute Force Angriffen auf die Sicherheitsarchitektur der IT-Netzwerke. Sind Angriffspunkte und Werkzeuge erschaffen, wird der Angriff durchgeführt. Das Phänomen ist freilich nicht neu. Wer erinnert sich nicht an das Loveletter-Virus (auch als Love Bug bekannt) aus dem Jahr 2000. Und auch Anna Kournikova hatte 2001 bekanntlich nicht vor, ein Foto von sich mit der Welt zu teilen. Doch die Qualität der Cyberangriffe hat sich geändert. Waren es früher tatsächlich noch Hacker, die auf Sicherheitslücken hinweisen wollten, geht es heute schlicht um Erpressung.

Das Gesundheitswesen ist gezwungen, mit dieser Bedrohungslage umzugehen. Digitale Gesundheitsanwendungen, Videosprechstunden, eRezept, telemedizinische Ver- und Nachsorge und nicht zuletzt der Wunsch der Patienten, auf ihre Behandlungs- und Gesundheitsdaten in einer elektronischen Gesundheitsakte zugreifen zu können, stellt die Leistungserbringer im Gesundheitswesen vor neue Herausforderungen. Die Digitalisierung im Gesundheitswesen bringt fortlaufend neue Anforderungen an die Cybersicherheit (früher auch IT-Sicherheit), den Datenschutz und die Datensicherheit mit sich. Der Einsatz ausreichend resilienter Software ist dabei nur ein Puzzleteil. Es bedarf der Schaffung eines Information Security Management System (ISMS), um auf den Ernstfall vorbereitet zu sein. Denn es droht nicht weniger als der Ausfall der Patientenversorgung im Falle eines Cyberangriffs. Denn die Strukturen sind derart vernetzt, dass der Angriff auf einen Rechner einen Dominoeffekt durch die gesamte Versorgungskette zur Folge haben kann.

Die anwaltliche Beratungspraxis muss sich mit dieser Querschnittsmaterie befassen, um die Mandatsbearbeitung sowohl auf Leistungserbringer- als auch auf Patientenseite optimal gewährleisten zu können. Die Veranstaltung gibt einen kompakten Überblick über die cyberrechtlichen Bestimmungen im Gesundheitswesen, die heutzutage von allen Leistungserbringern im Gesundheitswesen zu beachten sind, um negative Rechtsfolgen zu vermeiden.

Eine instruktive Arbeitsunterlage rundet die Veranstaltung ab.

Arbeitsprogramm

1. **Die Bedrohungslage**
2. **Rechtsgrundlagen der Cybersicherheit im Gesundheitswesen**
   a) Einführung
   b) Europäisches und deutsches Verfassungsrecht
   c) Nationales Recht
3. **Technische Grundlagen der Cybersicherheit**
   a) Begriff
   b) Anforderungen
   c) Maßnahmen
   d) Standards
4. **Cybersicherheit im Krankenhaus**
   a) KRITIS Betreiber
   b) Organisatorische und technische Vorkehrungen (OTV)
   c) Branchenspezifische Sicherheitsstandards (B3S)
5. **Cybersicherheit bei Medizinprodukten**
   a) KRITIS Betreiber
   b) Medizinprodukterecht
   c) Produkthaftung
6. **Telematikinfrastruktur**
   a) Grundlagen
   b) Rolle und Aufgabe der gematik
   c) Anwendungen der gematik
   d) Funktionsfähigkeit und Sicherheit
7. **Ambulante Gesundheitsversorgung**
   a) IT-Sicherheitsrichtlinien
   b) DSGVO
   c) Digital-Gesetz
   d) Doctolib
   e) Privatärztliche Verrechnungsstellen
   f) Praxishomepage
8. **Digitale Gesundheitsanwendungen**
   a) Anwendungsbereiche
   b) Zulassung
   c) Cybersicherheitsanforderungen
9. **Telemedizin**
   a) Definition und Bedeutung
   b) Cybersicherheitsanforderungen
10. **Compliance**
    a) Verantwortung
    b) Gesetzliche Pflichten
    c) Rechtsfolgen
    d) Compliance-Management-Systeme
    e) Internal Investigations
11. **Patientenschäden durch Cyberangriffe**
    a) Facharztstandard
    b) Aufklärungspflicht
    c) Mithaftung Dritter
12. **Ambulante Gesundheitsversorgung**
    a) Leistungsart
    b) Vertragsart
    c) Gesetzliche und untergesetzliche Anforderungen
    d) Grenzüberschreitende Zusammenarbeit