Sichere medizinische IT in Gesundheitseinrichtungen

Seminar zu Cybersicherheitsstrategien für medizinische IT-Systeme

Dieses Seminar vermittelt praxisnah, wie Sie medizinische IT-Systeme vor Cyberangriffen schützen. Sie lernen, Schwachstellen zu erkennen, Sicherheitsziele zu definieren und typische Angreifer-Modelle zu beurteilen.

Cybersicherheit im Gesundheitswesen – Schutz vor Angriffen auf Systeme und Patientendaten

Cyberangriffe auf medizinische Einrichtungen nehmen zu und können schwerwiegende Folgen haben, wie die Veröffentlichung sensibler Patientendaten oder die Beeinträchtigung der medizinischen Versorgung, was eine Gefahr für Leib und Leben darstellt.

Daher fordern Regularien wie die EU-Medizinprodukteverordnung (MDR) oder die B3S-Richtlinie explizite Maßnahmen zur Cybersicherheit. Diese Schulung adressiert diese Herausforderungen, indem sie Bedrohungen der medizinischen IT-Infrastruktur, insbesondere von DICOM-, HL7- und FHIR-Systemen, analysiert.

Die Teilnehmer:innen erfahren, wie Angreifer gezielte Attacken auf medizinische Geräte und Systeme durchführen und wie Betreiber sich wirksam dagegen schützen können.

Kursdetails auf einen Blick

- Für **Medizintechniker*innen, IT-Administrator*innen, IT-Sicherheitsbeauftragte**
- **offene Schulung** oder **Inhouse Training**
- Dauer: **2 Tage à 7 Stunden**
- Format: **Präsenz**
- Kosten: 1.320,00 Euro (zzgl. MwSt.)

Sicherheit für medizinische IT-Systeme

Ein zentraler Bestandteil des Seminars ist die Vermittlung grundlegender Sicherheitsziele für medizinische Systeme, wie Verfügbarkeit, Vertraulichkeit und Integrität. Anhand realer Praxisbeispiele lernen die Teilnehmenden, typische Schwachstellen in medizinischen IT-Systemen zu erkennen und deren Auswirkungen auf den laufenden Betrieb zu verstehen.

Dabei werden aktuelle Fälle analysiert, in denen Angreifer gezielt Zugang zu Patientendaten erhielten, und es wird nachvollziehbar aufgezeigt, wie diese Schwachstellen entstanden sind – etwa durch fehlerhafte Konfigurationen, unzureichende Netzwerksegmentierung oder veraltete Softwarestände. Darauf aufbauend werden Techniken, Best Practices und konkrete Konfigurationsmöglichkeiten vermittelt, um zentrale Dienste wie DICOM-Server, PACS-Systeme oder Schnittstellen zu Medizingeräten wirksam abzusichern.

In praxisorientierten Übungen identifizieren die Teilnehmenden gefährdete Geräte und Systeme im Netzwerk, bewerten deren Risiko und lernen, geeignete Schutzmaßnahmen zu ergreifen. So werden sie befähigt, medizinische IT-Infrastrukturen nachhaltig zu härten und die Sicherheit sensibler Patientendaten im Klinik- und Praxisalltag zu gewährleisten.

Nach dem Seminar können Sie:

- **Sicherheitsziele** für medizinische Systeme definieren.
- typische Angreifer-Fähigkeiten und -Modelle beurteilen.
- **die Sicherheit** von medizinischen Systemen anhand ihrer Spezifikation und Konfiguration grob einschätzen.

Alle Kursdetails und die Anmeldung finden Sie hier:

https://s.fhg.de/Cybersecurity-Healthcare

Kursinhalte

Das Spektrum der behandelten Themen umfasst:

Tag 1
- Block 1: Motivation und echte Praxisbeispiele von Sicherheitsproblemen im Gesundheitswesen
- Hands-On 1: offene DICOM-Server im Internet finden
- Block 2: Einführung in die Cybersicherheit im Gesundheitswesen
- Block 3: Open Source Intelligence (OSINT) – Was finden Angreifer über mein Unternehmen/Einrichtung heraus?
- Hands-On 2: Überprüfen des eigenen Unternehmens mit Hilfe von OSINT-Methode

Tag 2
- Block 4: Cyber-Resilienz im Gesundheitswesen
- Block 5: Sichere und unsichere Medizinkommunikation
- Block 6: Intrusion Detection und Incident Response im Medizinsektor
- Block 7: DICOM, HL7 und FHIR Security in der Praxis
- Hands-On 3: Sichere DICOM-Konfiguration

Vor der Veranstaltung:

Nach Anmeldeschluss erhalten Sie Zugang zu unserem Online Lernportal. Hier stehen Ihnen zwei Web Based Trainings (WBT) zu den Themen Netzwerksicherheit und Regulatorik bereit, die wir Sie bitten vorab zu bearbeiten.

Fachlicher Ansprechpartner am Fraunhofer SIT

Nico Brüggemann
Tel. +49 6151869521
nico.brueggemann@sit.fraunhofer.de

Fraunhofer SIT
Rheinstraße 75
64295 Darmstadt

Lernlabor
Cybersicherheit