



## IT-Sicherheit 2.0

### Seminar

Datum	Zeit	Ort
22. April 2020	14:15 - 18:00 Uhr	_Raum Lovelace, Halle 2.2

Die Bedrohung der IT-Sicherheit bei fortschreitender Digitalisierung ist nicht zu leugnen und eine Realität, die fast täglich in den Medien berichtet wird. Deshalb ist es für alle Beteiligten wichtig, dass nicht nur Kliniken, sondern auch die Hersteller die IT-Sicherheit ihrer (Medizin-)Produkte gewährleisten.

Herr Gruetz aus dem Klinikum Wolfsburg berichtet über die Anforderungen an Medical Devices aus dem Blickwinkel der Informationssicherheit und erörtert ausgehend vom Branchenspezifischen Sicherheitsstandard wesentliche Fragen aus der Betreibersicht.

Herr Prof. Dr. Pohl stellt in seinem Vortrag „Digital Security in medical devices“ die Herstellersicht dar:

- Anforderungen der MDR und IVDR an Geräte, Software, Firmware und Microcode
- Relevante internationale Normen
- Standards zur Entwicklung sicherer Hardware und Software, Best Practice
- Entwicklungsbegleitender Prüf- und Security Testing Process mit Darstellung der 5 Prüfmethode: Risikoanalyse/Security Requirements, Threat Modeling des Design, Static Source Code Analysis, Fuzzing, Penetration Testing
- Erfahrungen mit dem Prozess und Aufwands- und Erfolgsbewertung
- Beispiele für derart abgesicherte Systeme

und stellt im anschließenden Workshop die fünf Prüfmethode an konkreten Beispielen vor.

[Jetzt hier Ihr Seminticket buchen!](#)

## Schlagworte

[Technik und Interoperabilität](#) [Seminar IT](#) [Sicherheit](#) [Bedrohung](#) [Digitalisierung](#) [Informationssicherheit](#) [Sicherheitsstandards](#) [Betreiber](#) [MDR](#) [Normen](#) [Threat Modeling](#) [Fuzzing](#)

## Akteure

### Speaker:



[Rüdiger Gruetz](#), IT-Sicherheitsbeauftragter, Stabstelle IT-Sicherheit, Klinikum Wolfsburg



[Prof. Dr. Hartmut Pohl](#), Geschäftsführender Gesellschafter, softScheck GmbH

**Vorsitz:**



[Cornelia Vosseler](#), Vizepräsidentin, Berufsverband Medizin-Informatiker (BVMI) e. V.