



## TRENDS UND ENTWICKLUNG DER MODERNEN KRYPTOGRAPHIE

# POST-QUANTEN-SICHERHEIT

**Die Herausforderung: Quantencomputer brechen viele der heute gängigen Verfahren der IT-Sicherheit.** Die IT-Sicherheit adressiert heutzutage Aufgabenstellungen, die von einem gewöhnlichen Computer nicht oder nur mit unverhältnismäßig großem Aufwand gelöst werden können. Wie kann IT-Sicherheit jedoch zukunftsfest gestaltet werden? Der Kurs bietet einen Einstieg in die Technologie der Quantencomputer. Lernen Sie, wie Sie Gefahren besser abschätzen und wie sich quantenresistente Verfahren entwickeln lassen.

### Inhalte des Seminars

#### Funktionsweise eines Quantencomputers

#### Quantengatter und einfache Quanten-Algorithmen mit Hands-on-Simulationen

#### Die Auswirkungen der Algorithmen von Shor und Grover auf die moderne Kryptographie

#### Einführung in Post-Quanten-Kryptographie, praxisnahe Übungen zu dem Thema

#### Die laufende Standardisierung der NIST

### Ihr Nutzen

- » Nach dem Seminar können Sie die Funktionsweise eines Quantencomputers nachvollziehen.
- » Sie können Quantengatter und einfache Quanten-Algorithmen programmieren.
- » Sie wissen, wie man die Auswirkungen der Algorithmen von Shor und Grover auf die moderne Kryptographie abschätzt.
- » Sie können Post-Quanten-Kryptographie anwenden.

### INFORMATIONEN IM ÜBERBLICK

 Grundlegende Kenntnisse in IT-Sicherheit und Kryptographie von Vorteil, aber nicht zwingend

 Administratoren\*innen, die schon heute ihre IT-Infrastruktur postquantensicher machen wollen, Anwendende von IT-Sicherheit, die verstehen wollen, wie sich die IT-Sicherheit in den nächsten Jahren entwickelt, Fachkräfte und Spezialisten\*innen aus der Hochsicherheitsindustrie

 2 Tage Präsenz oder online

 1200,-

 Weiden in der Oberpfalz

Veranstaltet durch

 **Fraunhofer**  
AISEC

Referent:



Daniel Loebenberger  
Professor für  
Cybersicherheit an  
der Ostbayerischen  
Hochschule Amberg Weiden  
und Leiter der Forschungs-  
gruppe Secure Infrastruc-  
ture am Fraunhofer AISEC



Weitere Infos und  
aktuelle Termine  
buchen unter:

[www.cybersicherheit.fraunhofer.de/post-quanten-sicherheit](http://www.cybersicherheit.fraunhofer.de/post-quanten-sicherheit)