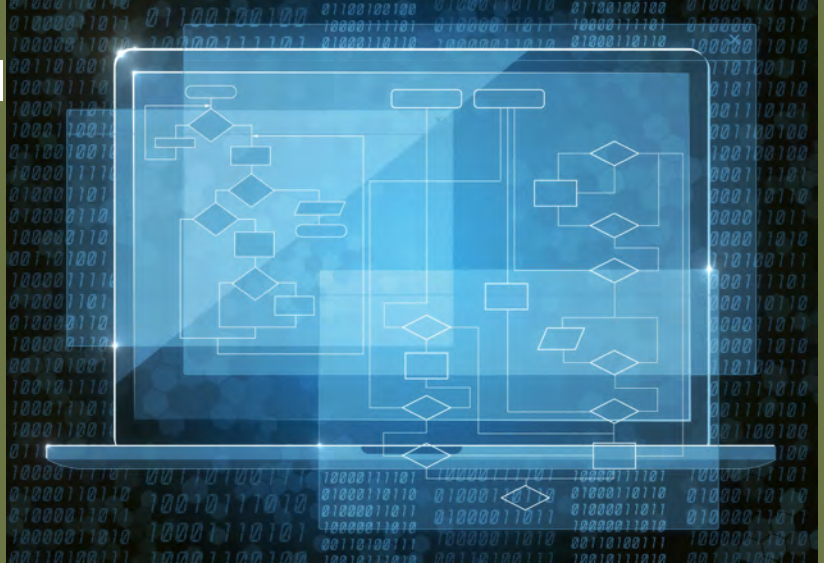
PRÄSENZ



BEDROHUNG MODELLIEREN – RISIKO PRIORISIEREN

SOFTWAREHÄRTUNG: SOFTWARE GEGEN SCHWACHSTELLEN SICHERN – ADVANCED

Die Herausforderung: Sicherheit frühzeitig und effizient implementieren. Weil Sicherheit gegenüber Funktionalität bei der Softwareentwicklung häufig als nachrangig gilt, entstehen Sicherheitslücken in der Software, und Hacker haben leichtes Spiel. Dieses Seminar zeigt am Beispiel eines Java-Webshops, wie die Vorgehensweise der sicheren Softwareentwicklung funktioniert. Anhand zu erwartender Angriffspfade werden effektive Gegenmaßnahmen erarbeitet und die typischen Stolperfallen des Codes gehärtet. Schützen Sie Ihr System!

Inhalte des Seminars

Tag 1

- Kryptographie und Netzwerksicherheit: Anwendungsfälle, Bedrohungen, Maßnahmen
- Plattformen: Web, Apps, native Programme
- Sicherer Code 1: Grundmuster, Architektur und Struktur, codespezifische Sicherheitslücken in Java

Tag 2

- Sicherer Code 2: codespezifische Sicherheitslücken, Review-Prozess
- Security Testing: Vorgehensweise, Pentest, Code Audit, Beispiele: Web, Apps, native Programme
- Organisatorische Sicherheit: Repositories, Deployment

Ihr Nutzen

» Am roten Faden eines Webshops implementieren Sie grundlegende kryptographische Verfahren und lernen effektive Sicherheitsmaßnahmen kennen.

» Sie verstehen, die Tücken einiger weitverbreiteter Codemuster, können sie kompensieren und den finalen Code testen.

» Sie lernen die technischen und organisatorischen Eckpunkte einer sicheren verteilten Entwicklungsumgebung und des Deployments kennen.

INFORMATIONEN IM ÜBERBLICK

Sehr gute Programmierkenntnisse (Java)

Softwareentwickler*innen

2 Tage Präsenz

1200,–

Berlin

Veranstaltet durch

Fraunhofer FOKUS

Referent:

Manuel Raddatz, wiss. Mitarbeiter Techn. Hochschule Brandenburg

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/softwarehaertung