PRÄSENZ

SICHERHEITS-ALPTRAUM IOT?

ABSICHERUNG VON IOT-SYSTEMEN

Die Herausforderung: Vielfältige Sicherheitslücken machen IoT zum leichten Angriffsziel. Die Problemfaktoren: Anbindung zum Internet, geringfügige Absicherung und wenig Rechenleistung. Neben all dem eröffnen sie aber in der Regel Zugang zu persönlichen Daten und vertraulichen Informationen von Unternehmen. Dieses Seminar stattet Sie mit notwendigem Wissen zu Sicherheitslücken im IoT-Bereich aus. Welche möglichen Sicherheitsrisiken gibt es in der Kommunikationsarchitektur? Lernen Sie anhand von realen Beispielen, wie Sie Ihr System schützen können.

Inhalte des Seminars

Überblick zum Angriffsziel IoT
– Sicherheitslücken bei IoT
– Vorführungen zum Google Hacking

Vertiefte Analyse der IoT-Architektur
– Risiken und Bedrohungen
– Schutzmaßnahmen

Embedded Systems & IoT
– TPM (Trusted Platform Module) und Trusting Computing
– Sicherheitsmechanismen innerhalb des Linux Kernel

Demonstration und Hands-on
– Schwachstellenscanner im direkten Einsatz
– Pentesting für IoT

Ihr Nutzen

» Nach dem Seminar können Sie nicht nur für IoT-Geräte, sondern auch für das gesamte Unternehmensnetz Bedrohungen abwehren.
» Sie wissen, wie man Sicherheitslücken aufspürt, abschätzt und beseitigt.
» Sie lernen, von außen erreichbare IoT-Geräte im Unternehmen zu identifizieren und abzusichern.

INFORMATIONEN IM ÜBERBLICK

Grundlegende IT-Kenntnisse, Grundlegende IT-Sicherheitskenntnisse von Vorteil

Software Architekten*innen und Entwickler*innen in IoT, Admins, Betreiber*innen

1 Tag Präsenz

600,–

Garching bei München, inhouse

Veranstaltet durch

Fraunhofer AISEC

Referent:

Sascha Wessel, Abteilungsleiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/absicherung-iot-systeme