



IT-Sicherheitsrichtlinien nutzergerecht gestalten und etablieren

Training für empathisches Security Policy Engineering und strategische Sicherheitskommunikation

IT-Sicherheitsrichtlinien stoßen häufig auf Ablehnung, da sie als einschränkend wahrgenommen werden. Das erschwert ihre Anwendung und steigert potenzielle Risiken. Die IT-Abteilung wird dabei oft eher als Hindernis denn als unterstützender Partner gesehen. Unsere Weiterbildung vermittelt, wie Empathisches Policy-Engineering und gezielte Sicherheitskommunikation zu mehr Akzeptanz und praktischer Umsetzbarkeit führen.

Mit Empathie und Strategie zur besseren Akzeptanz

IT-Sicherheitsrichtlinien stoßen in Unternehmen oft auf Widerstand. Mitarbeitende empfinden sie als hinderlich, was zu mangelnder Akzeptanz und unzureichender Umsetzung führt.

Dadurch steigt das Sicherheitsrisiko, während gleichzeitig die Zusammenarbeit zwischen IT-Abteilung und Endnutzenden belastet wird. Die IT wird häufig als Bremser statt als Partner wahrgenommen.

Unsere Weiterbildung zeigt Ihnen praxisnahe Methoden, um diese Herausforderung zu meistern: Empathisches Policy-Engineering und strategische Sicherheitskommunikation für mehr Verständnis, Vertrauen und nachhaltige Sicherheit im gesamten Unternehmen.

Kursdetails auf einen Blick

- Für Mitarbeitende der IT-Abteilung und IT-Sicherheitsverantwortliche
- Offene Schulung oder Inhouse Training
- Dauer: 2 Tage à 5 Stunden
- Format: Online
- Kosten: 1.300,00 Euro (zzgl. MwSt.)

Nutzerzentriert entwickeln und überzeugend kommunizieren

Sie lernen, IT-Sicherheitsrichtlinien zu entwickeln, die nicht nur theoretisch sinnvoll, sondern auch in der Praxis akzeptiert und umgesetzt werden. Dafür vermitteln wir Ihnen bewährte Strategien aus der Forschung und Praxis. Beim Empathischen Policy-Engineering gestalten Sie Richtlinien so, dass sie die Perspektive der Nutzenden berücksichtigen und praktikabel sind.

Mit strategischer Sicherheitskommunikation setzen Sie Techniken ein, um IT-Sicherheit verständlich und überzeugend zu vermitteln – Widerstände werden abgebaut, die Akzeptanz erhöht.

Ein weiterer Schwerpunkt liegt auf Konfliktprävention und Zusammenarbeit. Sie erfahren, wie Sie Spannungen zwischen der IT und anderen Abteilungen reduzieren und eine kooperative Sicherheitskultur etablieren. Durch praxisnahe Übungen und Rollenspiele setzen Sie das Gelernte direkt um und entwickeln ein sicheres Gespür für die wirksame Durchsetzung von Sicherheitsrichtlinien.

Nach dem Seminar können Sie:

- **Gezielte Konfliktlösungsstrategien einsetzen**, um sicheres Verhalten zu fördern und Widerstände abzubauen.
- **Sicherheitsmaßnahmen entwickeln**, die sowohl den Anforderungen der Nutzenden als auch den Sicherheitszielen des Unternehmens entsprechen.
- **Sicherheitsmaßnahmen praktisch und nutzerfreundlich entwerfen**, sodass ihre Akzeptanz steigt und die Umsetzung erleichtert wird.

Alle Details und Anmeldung finden Sie hier:



<https://s.fhg.de/security-policy>



Lernlabor
Cybersicherheit

Kursinhalte

Herausforderungen in der Sicherheitskonformität

- Identifikation typischer Herausforderungen in der Sicherheitskonformität
- Wechselwirkung zwischen Sicherheitsdesign und Nutzerverhalten

Nutzerbedürfnisse verstehen

- Methoden wie Design Thinking und Stakeholder-Analyse zur Erfassung von Nutzerbedürfnissen
- Praktische Übungen und Checklisten zur besseren Umsetzung

Empathisches Policy-Engineering

- Bedeutung von Empathie im Policy-Design verstehen und gezielt anwenden
- Change-Management-Techniken und Innovationsmodelle für nachhaltige Sicherheitsmaßnahmen nutzen
- Best-practice Vorgehensmodell zur Erstellung und Einführung von Sicherheitsrichtlinien
- Interaktive Übungen zur Entwicklung und Bewertung eigener Sicherheitsrichtlinien

Effektive Sicherheitskommunikation

- Die Rolle klarer, überzeugender Kommunikation für sicherheitskonformes Verhalten verstehen
- Verbale und nonverbale Kommunikationstechniken gezielt einsetzen, um Widerstände zu minimieren

Konfliktlösungsstrategien für die IT-Sicherheit

- Verhandlungstechniken erlernen, um Sicherheitsmaßnahmen wirksam durchzusetzen
- Win-Win-Ansätze entwickeln, um als vertrauenswürdiger Partner wahrgenommen zu werden
- Praxisnahe Rollenspiele zur gezielten Anwendung von Kommunikation und Konfliktmanagement

Fachliche Ansprechpartnerin am Fraunhofer IAO

Dr. Mrudula Arunkumar
Tel. +49 711 970-5132
mrudula.arunkumar@iao.fraunhofer.de

Fraunhofer-Institut IAO
Nobelstr. 12
70569 Stuttgart
www.fraunhofer.de

