Grundlagen der IT-Sicherheit

Von Prävention bis Reaktion

Erlernen Sie die Grundlagen der IT-Sicherheit! Das Seminar bietet einen Überblick zu Bedrohungen, Angriffsmethoden und Schutzmaßnahmen. Mit praktischen Übungen wenden Sie das Wissen direkt an und minimieren Risiken – für mehr Sicherheit im Umgang mit digitalen Gefahren, privat und beruflich.

IT-Sicherheit im Alltag: Begriffe verstehen, Risiken erkennen

IT-Sicherheit begegnet uns täglich, doch oft bleiben die Begriffe abstrakt. Was bedeuten sie für mich persönlich und welche Konsequenzen ergeben sich für mein Unternehmen?

Dieses praxisorientierte Seminar vermittelt Ihnen die Grundbegriffe der IT-Sicherheit und bietet einen umfassenden Überblick über Angriffsmethoden, Bedrohungen und passende Schutzmaßnahmen.

Sie lernen nicht nur theoretische Ansätze, sondern setzen das Wissen auch in praktischen Übungen ein, um die erlernten Konzepte direkt anzuwenden.

Mit der fortschreitenden Digitalisierung steigt der Bedarf an grundlegenden Kenntnissen zur IT-Sicherheit, sowohl im privaten als auch beruflichen Umfeld.

Kursdetails auf einen Blick

- für Anwender*innen, Einsteiger*innen
- Offene Schulung oder Inhouse Training
- Dauer: 1 Tag à 8 Stunden
- Format: Online
- Kosten: 600,00 Euro (zzgl. MwSt.)

Praxisnahes Grundlagenwissen für mehr Sicherheit in der digitalen Welt

Schlagzeilen zu Cyberbedrohungen sind allgegenwärtig, doch oft fehlt das Verständnis für die dahinterliegenden Prozesse. Unser Seminar schließt diese Lücke, indem es praxisnah und verständlich erklärt, wie Sie den IT-Sicherheitsanforderungen erfolgreich begegnen können.

Die Teilnehmer:innen erfahren, wie man Schutzziele identifiziert, gängige Angriffsmethoden analysiert und geeignete Schutzmechanismen entwickelt.

Der Mix aus Theorie und praktischen Übungen gewährleistet, dass die vermittelten Inhalte nicht nur nachvollziehbar, sondern auch direkt umsetzbar sind. So können Sie IT-Sicherheitsrisiken effektiv bewerten und entsprechende Maßnahmen ergreifen.

Nach dem Seminar können Sie:

- die **Grundlagen der IT-Sicherheit verstehen und** auf Ihre berufliche und private Umgebung **anwenden**.
- **Angriffsmethoden** identifizieren, deren **Auswirkungen** einschätzen und geeignete **Gegenmaßnahmen einleiten.**
- **Präventive Maßnahmen** umsetzen, um **Risiken frühzeitig** zu **erkennen** und digitale Gefahren zu minimieren.

Kursinhalte

Das Spektrum der behandelten Fragestellungen umfasst:

- **Kennenlernen der Grundbegriffe der IT-Sicherheit:**
  - Einführung in zentrale Konzepte und Terminologien der IT-Sicherheit, wie Vertraulichkeit, Integrität, Authentizität und Nicht-Abstreitbarkeit, sowie ein Überblick über deren Bedeutung im IT-Betrieb.
- **Identifizieren von Sicherheitszielen:**
  - Analyse der grundlegenden Schutzziele der Informationssicherheit und deren Anwendung in unterschiedlichen Szenarien – von der Absicherung einzelner Systeme bis hin zur ganzheitlichen Sicherheitsstrategie in Organisationen.
- **Angriffsmethoden und Bedrohungen:**
  - Überblick über typische Bedrohungsszenarien, Schwachstellen und Angriffsvektoren, z. B. Malware, Phishing, Zero-Day-Exploits oder Insider-Bedrohungen, sowie deren Auswirkungen auf IT-Systeme und Geschäftsprozesse.
- **Gegenmaßnahmen:**
  - Vorstellung technischer und organisatorischer Maßnahmen zur Abwehr von Bedrohungen, z. B. Firewalls, Intrusion Detection/Prevention Systeme, Sicherheitsrichtlinien.
- **Physical Security und Social Engineering:**
  - Betrachtung der Sicherheit von IT-Infrastrukturen (Zutrittskontrollen, Überwachung, Schutz vor Diebstahl) sowie die Gefahren durch menschliche Manipulation, insbesondere durch Social Engineering-Techniken.

Alle Kursdetails und die Anmeldung finden Sie hier:

https://shorturl.at/w6XJH

Lernlabor
Cybersicherheit

Fachlicher Ansprechpartner an der H-BRS

Prof. Dr. Michael Redemacher
Tel. +49 89 2241 865 151
Michael.Rademacher@h-brs.de

Hochschule Bonn-Rhein-Sieg
Grantham-Allee 20
53757 Sankt Augustin
www.fraunhofer.de