

Zertifikatslehrgang

BSI IT-Grundschutz-Praktiker

IT-Infrastrukturen besser schützen
IT-Grundschutz-Praktiker-Schulung nach dem BSI-Curriculum

Lehrgangstermine 2025

Neuer Zertifikatslehrgang



IT-Grundschutz

Modul I: 9./10. April 2025 Online

Modul II: 24./25. Juni 2025 in Siegburg bei Bonn

Vorwort

Angriffe auf die IT-Infrastruktur stellen zunehmend **das größte Sicherheitsrisiko für Unternehmen** dar. Aufgrund der stetig ansteigenden Bedrohungslage sind immer mehr wesentliche Geschäftsprozesse gefährdet, wenn es um ein mögliches Eindringen durch Cyberkriminelle geht. Auch die Sicherheitstechnik ist davon verstärkt betroffen. Für eine erfolgreiche Digitalisierung in Unternehmen ist Informationssicherheit daher die grundlegende Voraussetzung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit dem **IT-Grundschutz** eine Vorgehensweise entwickelt, die Unternehmen darin unterstützt, **ihre IT-Infrastruktur sicher zu schützen**. Ziel ist es, durch die Implementation von definierten Maßnahmen ein ausreichendes Schutzniveau in Unternehmen sicherzustellen. Bei Betreibern kritischer Infrastrukturen (KRITIS-Unternehmen) fordert der Gesetzgeber sogar die Einhaltung der entsprechenden Standards explizit ein.

Um diese Expertise für Unternehmen verfügbar zu machen, hat das **BSI** ein **Schulungscurriculum** konzipiert, welches Sicherheitsverantwortliche dazu befähigt, in ihrem Unternehmen entsprechende IT-Sicherheitsmaßnahmen, wie z. B. ein **Informationssicherheitsmanagementsystem (ISMS)** zu implementieren wie auch weiterzuentwickeln.

Die **SIMEDIA Akademie** hat als **anerkannter Schulungsanbieter des BSI** die Schulungen zum BSI-IT-Grundschutz-Praktiker mit in ihr Weiterbildungsprogramm aufgenommen.

In der **IT-Grundschutz-Basisbildung** mit einem Zeitumfang von **24 h** insgesamt lernen Sie die Grundlagen des IT-Grundschutzes kennen. Im Anschluss können Sie Ihr Wissen durch die Teilnahme an einer **Prüfung zum „IT-Grundschutz-Praktiker“** beweisen und erhalten damit eine **qualifizierte Teilnahmebestätigung**.

Zielgruppe:

IT-Sicherheitsbeauftragte, IT-Leiter, IT-Berater, Projektleiter, Datenschutzbeauftragte und andere mit Themen der Informationssicherheit befasste Sicherheitsverantwortliche (z. B. bei der Planung von IT-basierter Sicherheitstechnik)

Tag 1 – 9-17 Uhr:
Modul I
Einführung



9. April 2025 – Online
Beginn: 9:00 Uhr

1. Einführung und Grundlagen der Informationssicherheit und rechtliche Rahmenbedingungen

- Begriffe (Arten und Wichtigkeit von Informationen, Aspekte der Integrität, Verfügbarkeit, Vertraulichkeit usw.)
- Unterschied zwischen IT und OT sowie Security und Safety
- Gesetzliche Grundlagen (BSIG, IT-SiG usw.)

2. Normen und Standards der Informationssicherheit

- Evaluation von relevanten Normen
- Synergieeffekte herausstellen
- integrierte Managementsysteme, VSA, C5, HV-Benchmark
- Überblick, Zweck und Struktur über relevante Normen und Richtlinien z.B. ISO 2700x usw.)
- Cobit, ITIL usw.
- IT-Grundschutz-Kompodium
- Branchenspezifische Sicherheitsstandards und IT-Grundschutz-Profile

3. Einführung IT-Grundschutz

- IT-Grundschutz – Bestandteile
- Sicherheitsprozess
- Rollen, Verantwortung und Aufgaben (Institutionsleitung, Informationssicherheitsbeauftragte, ICS-Informationssicherheitsbeauftragte, Information-Management-Team usw.)
- Sicherheitskonzept
- Leitlinie erstellen

Tag 2 – 9-17 Uhr:

Modul I

Vorgehensweise, Kompendium, Umsetzung,



10. April 2025 – Online

Beginn: 9:00 Uhr

4. IT-Grundschutz-Vorgehensweise (Überblick)

- Leitfragen zur IT-Grundschutz-Absicherung
- Basis-Anforderungen
- Standard-Anforderungen
- Anforderungen für den erhöhten Schutzbedarf
- Wahl der Vorgehensweise am Praxisbeispiel

5. Kompendium (Überblick)

- Aufbau und Anwendung des Kompendiums
- ISMS
- Prozess-Bausteine
- System-Bausteine
- Umsetzungshinweise
- Erstellung eines Bausteins

6. Umsetzung der IT-Grundschutz-Vorgehensweise

- Netzplan erstellen
- Geschäftsprozess und zugehörige Anwendungen sowie IT-Systeme, Räume erfassen
- Schutzbedarfskategorien, Vorgehen und Vererbung
- Modellierung gemäß IT-Grundschutz (Vorgehen, Dokumentation, Anforderungen anpassen)

7. IT-Grundschutz-Check

- Was wird geprüft?
- Vorbereitung und Durchführung
- IT-Grundschutz-Check dokumentieren
- Entscheidungskriterien
- Beispiel für die Dokumentation
- Beispiel für die Durchführung

Tag 3 – 9-17 Uhr:
Modul II
Analyse, Planung,
Zertifizierung



24. Juni 2025 – Siegburg bei Bonn
Beginn: 9:00 Uhr

8. Risikoanalyse

- Die elementaren Gefährdungen sowie andere Gefährdungsübersichten
- Vorgehen bei der Risikobewertung und Risikobehandlung
- Beispiel für die Risikobewertung

9. Umsetzungsplanung

- Maßnahmenplan entwickeln und dokumentieren, Aufwand schätzen, Umsetzungsreihenfolge und Verantwortlichkeit bestimmen, begleitende Maßnahmen planen
- Aufwände schätzen

10. Aufrechterhaltung und kontinuierliche Verbesserung

- Leitfragen für die Überprüfung
- Überprüfungsverfahren
- Kennzahlen
- Reifegradmodelle
- Beispiel für Anwendung kontinuierlicher Verbesserungsprozess (KVP)

11. Zertifizierung und Erwerb des IT-Grundschutz-Zertifikats auf Basis von ISO-27001

- Bewährte Methoden der Szenarienbildung
- Arten von Audits z.B. Prozess und Produkt Audit
- Grundsätze der Auditierung 1st, 2nd, 3rdParty Auditoren
- Modell der Akkreditierung und Zertifizierung
- Ablauf des BSI-Zertifizierungsprozesses

12. IT-Grundschutz-Profile

- Aufbau eines IT-Grundschutz-Profils
- Nutzung/Erstellung eines IT-Grundschutz-Profils
- Anwendung bzw. Nutzungsmöglichkeit veröffentlichter Profile

Tag 4 – 9-17 Uhr:
Modul II
Audit, BCM,
Abschlussprüfung



25. Juni 2025 – Siegburg bei Bonn
Beginn: 9:00 Uhr

13. Vorbereitung auf ein Audit

- Planung und Vorbereitung auf ein Audit (Rollen und Verantwortlichkeiten, Unabhängigkeit, Auditplan, Checklisten, Kombination von Audits, Synergieeffekte) Audit-prep/defens
- Auditprozess-Aktivitäten (Zusammenstellung eines Teams, Dokumente vorbereiten, Planung des Vor-Ort-Audits, Umgang mit Nichtkonformitäten)
- Berichtswesen (Inhalt und Aufbau eines Berichtes, Genehmigung und Verteilung, Aufbewahrung und Vertraulichkeit)
- Folgemaßnahmen (Vor-Audit, Wiederholungsaudit, Überwachung, Korrekturmaßnahmen)
- Qualifikation von Auditoren (Berufserfahrung, Schulung, persönliche Eigenschaften, Aufrechterhaltung der Qualifikation)

14. Sicherheitsvorfallbehandlung Management

15. BCM-Prozess

- Überblick über den BSI-Standard 200-4
- Überblick über den BCM-Prozess, in Anlehnung an das IT-Grundschutz-Kompendium, insbesondere Notfallmanagement.

Abschlussprüfung

Referenten



Berens, Holger

Ass. iur. Holger Berens berät seit mehr als 35 Jahren internationale Unternehmen, KRITIS und Kommunen in allen Bereichen des Compliance-, Sicherheitsmanagements, Krisen- und Notfallmanagement. Er ist Managing Partner der Concepture Gruppe und verantwortet den Bereich Informationssicherheit, Compliance und BCM. Er ist Vorstandsvorsitzender des Bundesverbandes für den Schutz Kritischer Infrastrukturen (BSKI). Darüber hinaus war er bis zur Emeritierung im Jahr 2022 Leiter des Studiengangs Compliance and Corporate Security (LL. M.) an der Rheinischen Fachhochschule (RFH) in Köln und Leiter des Kompetenzzentrums für Internationale Sicherheit (KIS) an der RFH.



Prof. Dr. Berens, Johannes

Partner der concepture GmbH und Consultant für Fragestellungen des maschinellen Lernens und Sicherheitsmanagementsysteme. Seit 2016 entwickelte er an der Bergischen Universität Wuppertal in mehreren BMBF geförderten Forschungsprojekt eine KI zur Prognose drohender Studienabbrüche. Zwischen 2008 und 2015 gründete und leitete er an der Rheinischen Fachhochschule Köln gGmbH vier Außenstellen. Dort ist er bis heute Studiengangsleiter für die Masterstudiengänge „Generell Management“ und „International BusinessAdministration“.

Anmeldebedingungen

Veranstaltungsort

Die Veranstaltungen finden in Siegburg bei Bonn statt: Kranz Parkhotel GmbH, Mühlenstraße 32-44, 53721 Siegburg, Telefon: 02241 / 547 - 0, info@kranzparkhotel.de
Es steht ein begrenztes Zimmerkontingent **bis 4 Wochen** vor Veranstaltungsbeginn zur Verfügung. Bitte nehmen Sie die Reservierung unter Berufung auf Ihre Teilnahme an der Veranstaltung selbst vor. Stichwort: SIMEDIA.

Kosten

Die Teilnahmegebühr für die jeweils zweitägigen Module betragen € 1.195,-, für den viertägigen Zertifikatslehrgang € 2.390,- und ist nach Rechnungserhalt vor Beginn der Veranstaltung zu entrichten. Der Preis versteht sich zuzüglich Mehrwertsteuer. Darin enthalten sind eine digitale Dokumentation, Mittagessen, Erfrischungen und Pausenverpflegung sowie das gemeinsame Abendessen zwischen zwei gebuchten Veranstaltungstagen.

Anmeldung

Ihre Anmeldung und Zahlung richten Sie bitte an die SIMEDIA Akademie GmbH, Alte Heerstraße 1, 53121 Bonn. Nach Eingang Ihrer Anmeldung, die Sie telefonisch +49 228 9629370, per E-Mail anmeldung@simedia.de oder über das Internet unter www.simedia.de vornehmen können, erhalten Sie die Anmeldebestätigung und detaillierte Informationen zur gebuchten Veranstaltung sowie das Hotel. Die SIMEDIA Akademie behält sich vor, Anmeldungen ohne Angabe von Gründen abzulehnen.

Stornierung/Rücktritt

Wenn Sie bereits verbindlich zu einer Veranstaltung angemeldet sind, aber nicht teilnehmen können, stehen Ihnen folgende Möglichkeiten zur Verfügung:

Bis unmittelbar vor Beginn einer Veranstaltung können Sie einen Kollegen (Ersatzperson) benennen. Dafür entstehen Ihnen keine weiteren Kosten.

Bis 4 Wochen vor der Veranstaltung können Sie die Teilnahme kostenlos stornieren. Der Rücktritt muss immer schriftlich (per E-Mail) erfolgen.

- Erfolgt der Rücktritt zwischen 30 und 8 Tagen vor Veranstaltungsbeginn, werden wir 50% der Teilnahmegebühr berechnen.
- Erfolgt der Rücktritt nach weniger als 8 Tagen vor der Veranstaltung, ist die volle Teilnahmegebühr zu entrichten.

Erscheint der Teilnehmer nicht, ohne abgesagt zu haben, sind wir berechtigt, die volle Veranstaltungsgebühr in Rechnung zu stellen. Sollte die Veranstaltung seitens SIMEDIA Akademie GmbH abgesagt werden, so besteht ein Anspruch auf volle Rückerstattung der Teilnahmegebühr; Ansprüche darüber hinaus bestehen nicht.