

Grundlagen der IT-Sicherheit – Cyberangriffe erkennen

Praxisnahes Wissen zu Bedrohungen, Schutzmaßnahmen und gesetzlichen Vorgaben

Beginn: 14.04.2026 - 16:00 Uhr	 Live-Online	Veranstaltungsnr.: 36312.00.001	Live-Online
Ende: 27.04.2026 - 18:00 Uhr		Leitung <u>Sergej Schneider</u>	EUR 1.280,00 (MwSt.-frei)
Dauer: 2,0 Tage		ENTEAS GmbH <u>Alle Referent:innen</u>	Mitgliederpreis ⓘ EUR 1.152,00 (MwSt.-frei)

in Zusammenarbeit mit:



BESCHREIBUNG



*****Beachten Sie, das Seminar ist Teil des Zertifikatkurses mit optionaler Prüfung "Administrator für IT-Systeme" – www.tae.de/60175.*******

Cyberangriffe auf Unternehmen, Behörden und Institutionen nehmen weltweit drastisch zu. IT-Sicherheit ist heute kein optionales Thema mehr – sie ist ein entscheidender Faktor für den Schutz sensibler Unternehmensdaten, die Sicherstellung von Geschäftsprozessen und den Erhalt von Vertrauen und Reputation. Angesichts rasanter Digitalisierung, steigender Cyberkriminalität und verschärfter Regulatorik ist es für Unternehmen, IT-Fachkräfte und Organisationen jeder Größe unerlässlich, grundlegende Kenntnisse im Bereich IT-Sicherheit zu besitzen – um Risiken rechtzeitig zu erkennen und gezielt gegenzusteuern.

Unser Seminar bietet praxisnahes Basiswissen zu aktuellen Bedrohungen, typischen Angriffsmethoden und wirksamen Schutzmaßnahmen. Es vermittelt ein klares Verständnis für die Bedeutung von Datenschutz, Informationssicherheit und gesetzlichen Anforderungen wie der DSGVO, ISO 27001 und der NIS2-Richtlinie.

Ziel der Weiterbildung

Das Seminar schafft ein fundiertes Verständnis für IT-Sicherheitsrisiken und grundlegende Schutzmaßnahmen. Die Teilnehmenden erwerben die Fähigkeit, Gefahren frühzeitig zu erkennen, einfache Sicherheitsmaßnahmen anzuwenden und sicherheitsrelevante Fragestellungen kompetent einzuordnen.

Durch die Kombination aus Theorie, realitätsnahen Beispielen und praktischen Übungen erhalten die Teilnehmenden eine solide Basis für weiterführende Schulungen oder den eigenständigen Ausbau ihrer IT-Sicherheitskompetenz.

IMMER TOP!

Unser Qualitätsversprechen



Seit über 65 Jahren gehört die Technische Akademie Esslingen (TAE) mit Sitz in Ostfildern – nahe der Landeshauptstadt Stuttgart – zu Deutschlands größten Weiterbildungs-Anbietern für berufliche und berufsvorbereitende Qualifizierung im technischen Umfeld. Unser Ziel ist Ihr Erfolg. Egal ob Seminar, Zertifikatslehrgang oder Fachtagung, unsere Veranstaltungen sind stets abgestimmt auf die Bedürfnisse von Ingenieuren sowie Fach- und Führungskräften aus technisch geprägten Unternehmen. Dabei können Sie sich stets zu 100 Prozent auf die Qualität unserer Angebote verlassen. Warum das so ist?

PROGRAMM

*****Beachten Sie die Termine und Uhrzeiten des Seminars*****

Di., 14.04.2026, 16:00 - 18:00 Uhr
Do., 16.04.2026, 16:00 - 18:00 Uhr
Mo., 20.04.2026, 16:00 - 18:00 Uhr
Di., 21.04.2026, 16:00 - 18:00 Uhr
Do., 23.04.2026, 16:00 - 18:00 Uhr
Mo., 27.04.2026, 16:00 - 18:00 Uhr

Tag 1 – Sicherheitsgrundlagen

- Einführung in die allgemeinen Kerngrundlagen der IT-Sicherheit
- Datenschutz, Datensicherheit und IT-Security
- Grundlagen zur Informationssicherheit (DSGVO, ISO, NIS, etc.)
- Diskussion zu aktuellen Sicherheitsstandards und gesetzlichen Anforderungen

Methodik: Vortrag, Fallstudien, Gruppendiskussionen

Tag 2 – Angriffsszenarien: Social Engineering

- Einführung in Social Engineering
- Psychologische Manipulation und gängige Methoden
- Phishing, Pretexting, Baiting und Tailgating
- Selbststudium: Identifikation von Social Engineering Angriffen anhand von Fallbeispielen

Methodik: Präsentationen, Analyse realer Fälle, Rollenspiele

Tag 3 – Angriffsszenarien: Malware

- Arten von Malware: Viren, Würmer, Trojaner, Ransomware
- Mechanismen der Verbreitung und Infektion
- Analyse von Schadsoftware (Demonstrationen in einer sicheren Umgebung)
- Selbststudium: Erarbeitung von Präventionsstrategien gegen Malware

Methodik: Vortrag, praktische Analyse von Malware-Funktionen, Gruppenübungen

Tag 4 – Angriffsszenarien: Angriffsarten & Hacking-Methoden

- Überblick über gängige Angriffstechniken (Brute-Force, Man-in-the-Middle, DDoS)
- Netzwerkangriffe und Schwachstellenanalyse
- Selbststudium: Identifikation von Sicherheitslücken in einem vorgegebenen Szenario

Methodik: Demonstrationen und interaktive Übungen mit sicheren Testumgebungen

Tag 5 – Schutzmaßnahmen: Verschlüsselung & Sicherheitsmechanismen

- Grundlagen der Verschlüsselung (symmetrische/asymmetrische Verfahren, Hash-Werte)
- Einführung in Steganographie
- Verwendung von digitalen Zertifikaten und Signaturen
- Selbststudium: Durchführung einer eigenen Verschlüsselung mit vorgegebenen Tools

Methodik: Theoretische Einführung mit praktischer Anwendung (z. B. Hash-Werte generieren, Verschlüsselungstools ausprobieren)

Tag 6 – Schutzmaßnahmen: Risikomanagement & Sicherheitsstrategien

- Einführung in das IT-Risikomanagement
- Methoden zur Erkennung und Bewertung von Risiken
- Kennwortsicherheit und sicherheitsfördernde Systeme

Methodik: Gruppenarbeiten zur Risikobewertung, Passwort-Sicherheitsanalysen, Diskussion zu Sicherheitsstrategien

TEILNEHMER:INNENKREIS

Das Seminar richtet sich an:

- **System- und Netzwerkadministratoren**, die ihre Security-Grundlagen stärken möchten
- **Softwareentwickler**, die sichere Anwendungen konzipieren und umsetzen wollen
- **IT-Support-Mitarbeitende**, die Bedrohungen schnell erkennen und richtig reagieren müssen
- **Quereinsteiger und Berufsumsteiger**, die sich im Bereich IT-Security weiterbilden möchten
- **Verantwortliche für Datenschutz und IT-Compliance**
- **Führungskräfte in IT-nahen Bereichen**, die ein Verständnis für Sicherheitsanforderungen benötigen

REFERENT:INNEN



Sven Bechtloff

Herr Bechtloff ist ein erfahrener IT-Spezialist mit über 20 Jahren Praxis in der Planung, Implementierung und Betreuung anspruchsvoller IT-Infrastrukturen. Zusätzlich verfügt er über umfangreiche Erfahrung in der Ausbildung und Weiterentwicklung von IT-Fachkräften.

Sein technisches Know-how erstreckt sich über Microsoft- und Netzwerkinfrastrukturen, Automatisierung mit PowerShell und Ansible, Virtualisierung mit Hyper-V und Kubernetes, Azure-Cloud-Services sowie IT-Sicherheit.

Er verantwortet die technische Konzeption und Umsetzung geschäftskritischer Systeme – sowohl in lokalen Rechenzentren als auch in Cloud-Umgebungen. Neben seiner Projektstätigkeit ist er als IT-Trainer aktiv und engagiert sich ehrenamtlich als IHK-Prüfer für Fachinformatiker.

Zertifizierungen (Auswahl):

Microsoft Certified Solutions Associate (MCSA)

Microsoft Certified Solutions Expert – Cloud & Infrastructure (MCSE)

CompTIA Network+, Security+, Linux+

Certified Ethical Hacker (CEH v10)

Ausbildereignungsschein (AdA, IHK)

Weitere Veranstaltungen

[Administrator für IT-Systeme](#)



Sergej Schneider

Geschäftsführender Gesellschafter, ENTEAS GmbH, Stuttgart

Weitere Veranstaltungen

[Administrator für IT-Systeme](#)

VERANSTALTUNGORT

ONLINE

GEBÜHREN UND FÖRDERMÖGLICHKEITEN

Die Teilnahme beinhaltet ausführliche Unterlagen.

Preis:

Die Teilnahmegebühr beträgt:

1.280,00 € (MwSt.-frei)

Fördermöglichkeiten:

Bei einem Großteil unserer Veranstaltungen profitieren Sie von bis zu 70 % Zuschuss aus der [ESF-Fachkursförderung](#).

Bisher sind diese Mittel für den vorliegenden Kurs nicht bewilligt. Dies kann verschiedene Gründe haben. Wir empfehlen Ihnen daher, Kontakt mit unserer [Anmeldung](#) aufzunehmen. Diese gibt Ihnen gerne Auskunft über die Förderfähigkeit der Veranstaltung.

Weitere Bundesland-spezifische Fördermöglichkeiten finden Sie [hier](#).

Inhouse Durchführung:

Sie möchten diese Veranstaltung firmenintern bei Ihnen vor Ort durchführen? Dann fragen Sie jetzt ein individuelles [Inhouse-Training](#) an.