



01.07.2026  
online

[jetzt anmelden](#)

# IT-Sicherheit aus Sicht der Angreifer: Sensibilisierung mit Hacking-Tools, Phishing und KI

Einführung IT-Sicherheit | Tools von Kali Linux | Phishing | WLAN-Sicherheit | Social Engineering | KI-Sicherheit



Christoph Tukiendorf

Penetration Tester, Red Teamer & Gründer  
SPECTER

In diesem praxisorientierten Seminar erhalten Sie einen kompakten und praxisnahen Einblick in die aktuelle Bedrohungslage der IT-Sicherheit. Von Phishing und Social Engineering bis hin zu Angriffen auf WLAN-Netzwerke oder die Manipulation durch künstliche Intelligenz – Sie lernen, wie Cyberangriffe entstehen, wie Angreifer vorgehen und welche Schutzmaßnahmen wirklich greifen.

Anhand von Live-Demonstrationen wird gezeigt, wie gängige Tools aus Kali Linux – etwa NMAP, OSINT oder Metasploit – zur Schwachstellenanalyse eingesetzt werden können und welche Risiken dabei für eigene Systeme bestehen. Zudem erfahren Sie, wie Phishing-Mails erkannt, Netzwerke abgesichert und KI-basierte Angriffe wie Deep Fakes enttarnt werden.

Das Seminar vermittelt praxisnah, wie Sie Sicherheitslücken identifizieren und Risiken minimieren können. Mit klaren Handlungsempfehlungen und anschaulichen Beispielen bietet es wertvolles Wissen, um Systeme und Daten effektiv zu schützen.



## Inhaltsübersicht

- Einführung in die IT-Sicherheit
- Aktuelle Zahlen und Fakten
- Tools von Kali Linux und Live Demo
- Phishing
- Schutzmaßnahmen
- Phishing Links und Live Demo
- WLAN-Sicherheit
- Absicherung von Netzwerken
- Social Engineering
- Techniken und Schutzmaßnahmen
- KI-Sicherheit
- Empfehlungen zum sicheren Umgang von KI-Systemen



**08:45**

### **Login**

**09:00**

### **Begrüßung und Vorstellung**

- Gemeinsame Vorstellungsrunde
- Erwartungen und Zielsetzung

**09:15**

### **Einführung IT-Sicherheit**

- Einordnung der Bedrohungslage
- Aktuelle Zahlen und Fakten

**09:45**

### **Tools von Kali Linux**

- Einführung und Überblick
- Tools, um Schwachstellen zu erkennen
- (Live Demo, z.B. OSINT, NMAP, Metasploit)

**10:45**

### **Kaffeepause**

**11:00**

### **Phishing**

- Identifikation von Phishing
- Schutzmaßnahmen
- Phishing Links (Live Demo)

**12:30**

### **Mittagspause**



**13:30**

### **WLAN-Sicherheit**

- Absicherung von Netzwerken
- Zugriff von Angreifern auf WLAN-Netzwerke (Live Demo)

**15:00**

### **Kaffeepause**

**15:15**

### **Social Engineering**

- Was ist Social Engineering?
- Techniken von Social Engineering
- Schutzmaßnahmen

**16:00**

### **KI-Sicherheit**

- Wie können Angreifer KI ausnutzen (Deep Fakes, etc.)?
- Empfehlungen zum sicheren Umgang von KI-Systemen

**17:00**

### **Ende des Seminars**



## Christoph Tukiendorf

Christoph Tukiendorf ist Penetration Tester und Red Teamer. Mit seiner Firma Specter hat er sich auf Sicherheitsanalysen mit dem Schwerpunkt physische Sicherheit spezialisiert. Bereits während seines Studiums entwickelte er Konzepte, die seine heutige Arbeit prägen: die Verbindung von Cyber Security mit der gezielten Überprüfung der physischen Sicherheit. Seitdem unterstützt er Unternehmen bei der Identifikation und Ausnutzung von Schwachstellen sowohl in IT-Systemen als auch bei physischen Sicherheitsmaßnahmen. Christoph gibt regelmäßig Schulungen und Trainings zu den Themen Cyber Security, Cyber Security Awareness und Penetration Testing.

## Zielgruppe – An wen richtet sich dieses Seminar?

Dieses Seminar richtet sich an IT-Verantwortliche, Datenschutz- und Informationssicherheitsbeauftragte sowie Fachabteilungsleiterinnen und -leiter in öffentlichen Einrichtungen, die aktiv an der Sicherung ihrer Organisation gegen Cyberbedrohungen arbeiten möchten.

Auch Mitarbeitende aus anderen Bereichen, die ein grundlegendes Verständnis für die Funktionsweise von Cyberangriffen und geeignete Schutzmaßnahmen gewinnen möchten, sind angesprochen.

Egal, ob Sie bereits Vorkenntnisse mitbringen oder sich erstmals mit dem Thema befassen – dieses Seminar bietet wertvolle Einblicke und praxisnahe Ansätze für alle, die die Informationssicherheit in ihrer Organisation stärken wollen.

Die Inhalte des Seminars sind relevant für öffentliche Institutionen und öffentliche Unternehmen wie:

Städte, Landkreise, Kommunen und Verbandsgemeinden, Ministerien auf Bundes- und Landesebene, nachgeordnete Behörden und Betriebe von Bund und Ländern, Unternehmen der öffentlichen Hand und Betriebe gewerblicher Art (BgA), gemeinnützige und kirchliche Einrichtungen, Religions- und Weltanschauungsgemeinschaften, Universitäten, Universitätskliniken, Fachhochschulen sowie Forschungseinrichtungen, Verbände und Verbandsgemeinschaften, Kammern, Landesförderbanken, Staatskanzleien sowie Einrichtungen und Organisationen, die unter das Vergaberecht fallen.



## Termine:

**01.07.2026**

**online**

### **TEILNAHMEGEBÜHR:**

Online-Teilnahme: 535,- Euro zzgl. MwSt.

Details zur Anmeldung unter [www.fortbildungskampagne.de/anmeldung](http://www.fortbildungskampagne.de/anmeldung)

### **DIE TEILNAHMEGEBÜHR BEINHALTET:**

- Schulungsunterlagen (digital)
- Teilnahmezertifikat

### **ANMELDUNG:**

Bitte verwenden Sie zur Anmeldung unser Online-Anmeldeformular unter: [www.fortbildungskampagne.de/anmeldung](http://www.fortbildungskampagne.de/anmeldung)

### **KONTAKT FÜR RESERVIERUNGEN UND BUCHUNGEN:**

Haben Sie Fragen zum Seminar oder zu Reservierungen und Buchungen?

Schreiben Sie uns einfach eine Email oder rufen Sie uns unter der folgenden Rufnummer an:

Email: [team@fortbildungskampagne.de](mailto:team@fortbildungskampagne.de) | Telefon: +49 (0) 30 89 56 27 16

### **TEILNAHME- UND STORNIERUNGSKONDITION (AUSZUG):**

Die verbindliche Anmeldung erfolgt über unser Online-Anmeldeformular und wird durch Zusendung einer Anmeldebestätigung sowie der Rechnung bestätigt. Stornierungen sind bis vier Wochen vor Veranstaltungsbeginn kostenfrei, bereits gezahlte Beträge werden erstattet. Bei kurzfristiger Stornierung oder beispielsweise krankheitsbedingter Abwesenheit ist die Benennung eines Ersatzteilnehmers jederzeit möglich. Sofern sich kein Ersatzteilnehmer findet, kann nach Absprache ein Gutschein ausgestellt werden, der zur Teilnahme an einem Nachfolgetermin oder einem ähnlichen Seminar berechtigt. Bitte beachten Sie unsere AGB, die unter dem folgenden Link aufgerufen werden können:

[www.fortbildungskampagne.de/agb](http://www.fortbildungskampagne.de/agb)

### **DATENSCHUTZHINWEISE:**

Wir weisen darauf hin, dass Sie die Verwendung Ihrer Daten gemäß unserer Datenschutzbestimmungen durch eine Nachricht an [datenschutz@fortbildungskampagne.de](mailto:datenschutz@fortbildungskampagne.de) selbstverständlich jederzeit widerrufen können. Bitte beachten Sie unsere Datenschutzbestimmungen, die unter dem folgenden Link aufgerufen werden können:

[www.fortbildungskampagne.de/privacy](http://www.fortbildungskampagne.de/privacy)

### **HINWEISE ZUM DATENSCHUTZ BEI ONLINE-TEILNAHME:**

Details zur technischen Umsetzung der Online-Teilnahme erhalten Sie im Anschluss an Ihre Anmeldung. Ein wirksamer Auftragsverarbeitungsvertrag mit dem technischen Dienstleister liegt vor. Durch die Fortbildungskampagne als Veranstalter erfolgt während der Online-Teilnahme keine Speicherung von schriftlichen, akustischen oder visuellen Daten der Teilnehmenden. Eine temporäre Protokollierung des Chat-Verlaufes einer Online-Veranstaltung wird binnen zwei Arbeitstagen nach der Veranstaltung gelöscht. Bitte beachten Sie, dass Sie im Rahmen Ihrer Online-Teilnahme möglicherweise unfreiwillig Daten und Informationen übertragen, etwa durch weitere Personen in Ihrem Raum. Eine mögliche Übertragung derartiger Informationen liegt in Ihrem Verantwortungsbereich.