1. Dezember 2026 · 10:00–15:00 Uhr
Kostenfreie Online-Veranstaltung

AKADEMIE HEIDELBERG

Durchführung interner Red Teamings in Anlehnung an das TIBER-Rahmenwerk

Banken-Aufsicht-Seminar · 5 CPE-Punkte

- **Bedrohungsorientierte Penetrationstests nach TLPT/TIBER und warum Red Teaming nicht nur etwas für »Große« ist**
- **Wie TLPT, TIBER und freiwillige Red Teamings zusammenhängen**
- **Vorbereitung, Durchführung und Nachbereitung von Red Teamings sowie Maßnahmen zur Schließung von Schwachstellen**
- **Nachhaltige Verbesserung der Sicherheitsarchitektur und kontinuierliche Weiterentwicklung der Cyberabwehrfähigkeiten**
- **Praxis-Erfahrungen aus aktuellen TIBER-Tests der Bundesbank**

Referenten

Dr. Ronny Merkel
TIBER-Cyber-Team
Deutsche Bundesbank
Frankfurt/Main

Roman Müller
Teamleiter Red Teaming
Oneconsult Deutschland AG
Berlin

Durchführung interner Red Teamings in Anlehnung an das TIBER-Rahmenwerk

Programm

Dr. Ronny Merkel, Bundesbank · 10:00–12:00

Red Teaming in Zeiten von DORA und TIBER – wie kann das regulatorische Rahmenwerk von LSIs gewinnbringend genutzt werden?

- Wozu brauchen wir Red Teaming?
- Von CBEST bis DORA: Die Geschichte des (regulatorischen) Red Teamings im europäischen Finanzsektor
- TIBER-EU als zentraler Standard zur Umsetzung von europaweit einheitlichem Red Teaming für kritische Finanzunternehmen
- Inside TIBER-EU: Wie läuft ein TIBER-Test ab?
- Lessons learned aus sechs Jahren TIBER-Tests
- Warum Red Teaming nicht nur etwas für »Große« ist: Wie auch LSIs das TIBER-Playbook sinnvoll nutzen können
- Knappe Ressourcen: Wo LSIs beim Red Teaming sparen können
- Ausblick: Die Zukunft des Red Teamings in Europa: Wie geht es mit TIBER und DORA weiter?

Roman Müller, Oneconsult · 13:00–15:00

Proportionale Pentesting-Möglichkeiten für LSIs in der Praxis – Vorbereitung, Durchführung, Nachbereitung und Maßnahmen zum Erkennen und Schließen von Schwachstellen

Der Referent führt die Teilnehmenden anhand eines beispielhaften LSI durch den gesamten Prozess eines typischen Red Teamings. Vom ersten Gedanken, ob und wann ein Red Teaming überhaupt sinnvoll ist, über die konkrete Durchführung bis hin zum strukturierten Umgang mit den Ergebnissen. Jeder Abschnitt wird mit Anekdoten aus realen Engagements, persönlichen Erfahrungen und insbesondere lehrreichen Fehltritten angereichert.

Im Einzelnen werden u. a. die folgenden Themen behandelt:

- Begriffsklärung und Reifegrad: Abgrenzung zwischen Penetration Testing und Red Teaming. Wann ist eine Organisation bereit für den nächsten Schritt und wann ist ein klassischer Penetrationstest die bessere Wahl?
- Scoping und Zieldefinition: Identifikation der kritischen Funktionen, Ableitung relevanter Flags und Festlegung eines realistischen Testumfangs
- Stakeholder-Management: Wie gewinnt man intern die richtigen Unterstützer und wie geht man mit Widerständen aus Fachbereichen und IT-Betrieb um?
- Threat-Intelligence: Vorbereitung, Steuerung und Einordnung der Ergebnisse. Was macht einen guten Threat-Intelligence-Bericht aus, und wie fließen die Erkenntnisse in die Testplanung ein?
- Red-Teaming: Definition von Szenarien, Festlegung von Flags und Spielregeln für die operative Durchführung
- Vorstellung eines beispielhaften Angriffsplans: Der Dozent stellt einen konkreten Angriffsplan vor und erläutert Schritt für Schritt die einzelnen Techniken, die Aufgabenverteilung im Team sowie die Regeln für Kommunikation und Eskalation. Ergänzt durch Erfahrungsberichte und einen Exkurs zu modernen Phishing-Methoden, wie sie in der Praxis tatsächlich zum Einsatz kommen
- Umgang mit Findings: Priorisierung, Maßnahmenplanung und Nachverfolgung
- Typische Findings bei LSIs: Praxisbeispiele zu den häufigsten Schwachstellen, wiederkehrenden Problemen bei Red-Team-Engagements mit kleineren Instituten und die aus Sicht des Dozenten wirksamsten Gegenmaßnahmen
- Praxis-Hinweise und Umsetzungs-Tipps

Gute Gründe für Ihre Teilnahme:

- Sie verstehen die regulatorischen Anforderungen an bedrohungsorientierte Penetrationstests nach TLPT/TIBER
- Sie bekommen ein Verständnis dafür, diese Anforderungen in abgespeckter Form auch für sich nutzbar zu machen, z. B. im Rahmen von internen Red Teamings
- Sie diskutieren offene Fragen für Ihren Bereich oder Ihr Institut mit anderen Teilnehmenden und erhalten wertvolle Praxistipps im Erfahrungsaustausch mit anderen Expert*innen und Praktiker*innen

Seminarziel

Die aktuelle Cyber-Bedrohungslage zeigt, dass kleine Institute (LSIs) oder deren Dienstleister zunehmend ins Visier von Angreifern geraten – oft gerade wegen vermeintlich geringerer Sicherheitsreife. Ein Verzicht auf strukturierte Sicherheitsüberprüfungen ist daher keine Option – unabhängig von der Größe.

Andererseits fehlen oft Ressourcen, Budgets und spezialisierte Expertise für komplexe und umfassende Testformate. Dies führt in der Praxis nicht selten zu Unsicherheit: Wie viel Testing reicht aus? Welche Maßnahmen sind angemessen, ohne unverhältnismäßig zu sein? Und wie lassen sich realistische Bedrohungsszenarien sinnvoll in kleinere Organisationen übertragen?

Aber auch LSIs und kleinere Dienstleister können freiwillig durch proportionale Red Teamings Schwachstellen identifizieren, beseitigen und dadurch die IT-Sicherheit deutlich erhöhen.

Das Seminar vermittelt praxisnah, wie durch gezielte, risikoorientierte Red Teamings und technische Sicherheitsanalysen die Cyber-Resilienz effektiv verbessert werden kann – auch ohne TLPT-Verpflichtung. Die Teilnehmenden lernen, geeignete Testformate auszuwählen und identifizierte Schwachstellen systematisch zu beheben.

Zielgruppe

Aus der Praxis für die Praxis!
Wir wenden uns insbesondere an die Mitarbeitenden der Bereiche

- IT, Interne Revision, IT-Revision, IT-Organisation und Pentesting
- Informationssicherheit (ISB) und Informationsrisikomanagement
- IT-Sicherheitsmanagement, IT-Architektur und IT-Notfallbeauftragte
- IT-Compliance und IT-Governance, IT-Grundsatz und Regulatorik

sowie andere interessierte Fachbereiche bzw. Vorstandsmitglieder/ Geschäftsleiter*innen, externe Prüfer*innen sowie Bankdienstleister.

Unsere Referenten

Dr. Ronny Merkel
TIBER-Cyber-Team, Deutsche Bundesbank*, Frankfurt/Main

Dr. Ronny Merkel ist Cybersecurity-Experte bei der Deutsche Bundesbank und Leiter des nationalen Kompetenzzentrums für ethische Hackingübungen im Finanzsektor (TIBER Cyber Team). In dieser Rolle begleitet und koordiniert er bedrohungsorientierte Penetrationstests im Finanzsektor und wirkt an der Erstellung und kontinuierlichen Verbesserung der zugehörigen Regulatorik mit. An der Erstellung der technischen Regulierungsstandards zu DORA TLPT sowie der Novellierung des TIBER-EU Rahmenwerks war er maßgeblich beteiligt. Sein fachlicher Fokus liegt auf Red Teaming, Cyber-Resilienz sowie der praktischen Anwendung regulatorischer Vorgaben wie der DORA. Ronny Merkel verfügt über umfassende Erfahrung in der Analyse komplexer Bedrohungsszenarien und unterstützt Finanzinstitute dabei, ihre Sicherheitsfähigkeiten realitätsnah zu testen und weiterzuentwickeln.

Roman Müller
Teamleiter Red Teaming, Oneconsult Deutschland AG*, München

Roman Müller ist Red Teamer und Teamleiter mit langjähriger Erfahrung in der Durchführung von Penetrationstests und Red-Team-Engagements. Sein fachlicher Schwerpunkt liegt auf TLPT- und Red Teaming-Projekten für Kunden aus der Finanz- und Versicherungsbranche. Er war bisher an der Durchführung von vier TIBER-EU-Projekten sowie mehreren Red-Team-Assessments bei LSI-Instituten zentral beteiligt und kennt die besonderen Herausforderungen, denen sich auch kleine und mittlere Institute in der Praxis stellen müssen.

** Die Referenten geben ausschließlich ihre persönliche Auffassung und nicht die eines bestimmten Instituts, der Bundesbank, der BaFin oder einer anderen Aufsichtsbehörde wieder. Die Referenten nehmen auch keine offizielle aufsichtliche Auslegung regulatorischer Sachverhalte vor.*

DORA-konformes IKT-Risikomanagement
14./15. Oktober 2026, Online-Veranstaltung

Steuerung & Begleitung von IT-Projekten
15. Oktober 2026, Online-Veranstaltung

Neue DORA- & Aufsichts-Anforderungen an (IKT-)Notfallmanagement & BCM
21. Oktober 2026, Online-Veranstaltung

Fachtagung IKT-Aufsicht
3./4. November 2026, Online-Veranstaltung

Berechtigungsmanagement im Fokus der Aufsicht
10. November 2026, Online-Veranstaltung

DORA Spezial für Compliance & Governance
17. November 2026, Online-Veranstaltung

Zertifikats-Lehrgang Auslagerungsmanagement (Neue MaRisk) und IKT-Dienstleistersteuerung (DORA)
18. bis 20. November 2026, Online-Veranstaltung

Zertifizierter KI-Governance-Officer (CAIGO)
7. bis 9. Dezember 2026, Online-Veranstaltung

▶ Diese und weitere Seminar-Angebote finden Sie bei uns online unter *www.akademie-heidelberg.de/online-seminare*

Zusätzliche Informationen

Fragen zu diesen Schulungen oder unserem gesamten Seminar-Programm beantworte ich Ihnen sehr gerne.

Björn Wehling
Telefon 06221/65033-44
b.wehling@akademie-heidelberg.de

Anmeldeformular

Durchführung interner Red Teamings in Anlehnung an das TIBER-Rahmenwerk

Name

Vorname

Position

Firma

Straße / Nr.

PLZ / Ort

Telefon

E-Mail

Name der Assistenz

Datum / Unterschrift

Senden Sie Ihre Anmeldung bitte an: **anmeldung@akademie-heidelberg.de**

Termin und Seminarzeiten

Dienstag, 1. Dezember 2026
10:00–15:00 Uhr
Online-Zugang ab 9:45 Uhr

Seminar-Nr. 26 12 BA224 W

Teilnahmegebühr

Die Teilnahme ist kostenfrei.
Die Anmeldung berechtigt zur Teilnahme am Online-Seminar sowie zum Erhalt der Präsentation als PDF-Datei.

Allgemeine Geschäftsbedingungen

Es gelten unsere Allgemeinen Geschäftsbedingungen (Stand: 01.01.2010), die wir Ihnen auf Wunsch gerne zusenden. Diese können Sie jederzeit auch auf unserer Website einsehen: www.akademie-heidelberg.de/agb

Zum Ablauf

- Vor dem Seminartag erhalten Sie von uns eine E-Mail mit einem Link, über den Sie sich direkt in die Online-Veranstaltung einwählen können.
- Für Ihre Teilnahme ist es nicht notwendig, ein Programm herunterzuladen. Sie können am Seminar direkt per *Zoom* im Browser teilnehmen.
- Über Ihr Mikrofon und Ihre Kamera können Sie jederzeit Fragen stellen und mit den Referierenden und weiteren Teilnehmenden diskutieren. Alternativ steht auch ein Chat zur Verfügung.

AH Akademie für Fortbildung Heidelberg GmbH
Maaßstraße 32/1 · 69123 Heidelberg
Telefon 06221/65033-0
info@akademie-heidelberg.de
www.akademie-heidelberg.de

09_26 / 26 12 BA224