DEUTSCHE BUNDESBANK
EUROSYSTEM

Implementierung von TIBER-DE

Juli 2025

Version 4.0

INHALTSVERZEICHNIS

1 Hintergrund 3

2 Regelungsgehalt und Anwendungsbereich 4

3 Rolle der Deutschen Bundesbank 6

4 Finanzaufsichtliche Einbindung 7

5 Haftungsausschluss 8

1 HINTERGRUND

Die Bedrohung durch Cyberangriffe hat sich in den letzten Jahren für die Finanzwirtschaft und dort agierende Unternehmen zu einem der relevantesten Risiken entwickelt. Dies ist zum einen auf die zunehmende Vernetzung von Akteuren und die wachsende Bedeutung von einigen Unternehmen bei der Bereitstellung von kritischen IT-Dienstleistungen zurückzuführen. Zum anderen stellen auch professionelle und hochgradig organisierte Angreifer eine zunehmende Gefahr dar. Um sich vor Angriffen zu schützen, ist es sinnvoll, sich an aktuellen Standards der Cybersicherheit (wie beispielsweise dem IT-Grundschutz des BSI[1] oder der internationalen Norm ISO/IEC 27001[2]) zu orientieren und eine unternehmensweite Sensibilisierung vorzunehmen. Inwiefern die praktische Umsetzung dieser Maßnahmen erfolgreich war, kann meist erst im Falle eines realen Angriffs festgestellt werden. So können Implementierungsfehler oder menschliche Schwächen die getroffenen Sicherheitsvorkehrungen schnell zunichtemachen.

Bedrohungsorientierte Penetrationstests adressieren diesen Punkt, indem sie die Vorgehensweisen realer Angreifer imitieren und so eine realitätsnahe Überprüfung der Cyberwiderstandsfähigkeit eines Unternehmens unter kontrollierten Bedingungen ermöglichen. Um diese Tests in standardisierter Form in Europa zu ermöglichen, haben die Notenbanken der EU mit TIBER-EU (Threat Intelligence-based Ethical Red Teaming) ein einheitliches Rahmenwerk für freiwillige bedrohungsgeleitete Penetrationstests geschaffen. Das Rahmenwerk legt die Anforderungen an den Umfang und Ablauf solcher Tests fest und stellt eine hohe Qualität und Realitätsnähe sicher.

---

1 Siehe auch:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (letzter Zugriff: 01.07.2025).
2 Siehe auch: https://www.iso.org/isoiec-27001-information-security.html (letzter Zugriff: 01.07.2025).

2 REGELUNGSGEHALT UND ANWENDUNGSBEREICH

Im August 2019 hat die Deutsche Bundesbank gemeinsam mit dem Bundeministerium der Finanzen beschlossen, das TIBER-EU-Rahmenwerk in Deutschland als TIBER-DE umzusetzen. Mit der Implementierung von TIBER-DE erhalten Unternehmen des deutschen Finanzsektors seit dem Jahr 2020 die Möglichkeit, ihre Cyberwiderstandsfähigkeit durch anspruchsvolle und zielgerichtete Angriffe auf den Prüfstand zu stellen.

TIBER-DE richtet sich in erster Linie an große und kritische Unternehmen des deutschen Finanzsektors, um deren Cyberwiderstandsfähigkeit zu stärken und Ansteckungseffekte im Finanzsektor zu verringern.

Seit der umfassenden Überarbeitung des TIBER-EU-Rahmenwerkes im Januar 2025 ist eine Anpassung oder Spezifizierung einzelner Prozessbestandteile im nationalen Kontext nicht mehr notwendig, der Regelungsgehalt des TIBER-EU-Rahmenwerks findet bei TIBER-DE-Tests direkt und vollumfänglich Anwendung.[3] Die im Rahmen eines TIBER-DE-Tests zu durchlaufenden Prozessschritte sind als Bestandteil des TIBER-EU-Rahmenwerks auf der Webseite der Europäischen Zentralbank[4] veröffentlicht. Hier sind ebenfalls weiterführende Leitfäden zu finden, welche die einzelnen Testbestandteile konkretisieren.

---

3 Laut des TIBER-EU-Rahmenwerkes kann vor der Vorbereitungsphase eines Tests ein Bericht zur nationalen Bedro-hungslage im Finanzsektor (Generic Threat Landscape, GTL) vom TCT bereitgestellt werden. Die GTL kann als Basis für die Erstellung des Berichts zur unternehmensspezifischen Bedrohungslage dienen. Bei TIBER-DE-Tests wird von der Möglichkeit der Bereitstellung der GTL durch das TCT Gebrauch gemacht.
4 https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html (letzter Zugriff: 01.07.2025)

Die Vorgaben des TIBER-EU-Rahmenwerks stehen darüber hinaus im vollen Einklang mit den Regelungen des technischen Regulierungsstandards für bedrohungsorientierte Penetrationstests[5] (Threat-led Penetration Tests, TLPT) nach der Verordnung (EU) 2022/2254 (Digital Operational Resilience Act, DORA)[6]. Somit bildet TIBER-EU die operationelle Grundlage sowohl für die Durchführung verpflichtender bedrohungsorientierter Penetrationstests auf Grundlage von DORA, als auch für die Durchführung freiwilliger TIBER-DE-Tests.

5 Delegierte Verordnung (EU) 2025/1190 der Kommission vom 13. Februar 2025 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Kriterien für die Bestimmung der Finanzunternehmen, die zur Durchführung von bedrohungsorientierten Penetrations-tests verpflichtet sind, der Anforderungen und Standards für den Einsatz interner Tester, der Anforderungen hinsichtlich des Testumfangs, der Testmethodik und des Testkonzepts für jede einzelne Phase des Testverfahrens sowie der Ergeb-nisse, des Abschlusses und der Behebungsphasen der Tests sowie der Art der aufsichtlichen und sonstigen relevanten Zusammenarbeit, die für die Umsetzung von bedrohungsorientierten Penetrationstests und die Erleichterung der gegen-seitigen Anerkennung dieser Tests erforderlich ist.
6 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011.

3 ROLLE DER DEUTSCHEN BUNDESBANK

Das TIBER Cyber Team (TCT) ist als nationales Kompetenzzentrum der TIBER-DE-Implementierung im Bereich Zahlungsverkehr und Abwicklungssysteme der Deutschen Bundesbank angesiedelt. Das TCT übernimmt die operative Betreuung für sowohl:

- freiwillig über das TCT anberaumte TIBER-DE-Tests, als auch

- durch die BaFin, die EZB[7] oder eine andere Behörde[8] angeordnete TLPTs nach der DORA-Verordnung.

Dabei stellt das TCT sicher, dass alle Tests einheitlich nach den Vorgaben des TIBER-EU-Rahmenwerks durchgeführt werden. Das TCT ist weiterhin an grenzüberschreitenden Tests gemeinsam mit den TCTs anderer Länder beteiligt.

Kontakt: tiber@bundesbank.de; tlpt@bundesbank.de

7 Sofern diese Anordnung durch die EZB in Deutschland ansässige Unternehmen betrifft und sich die EZB die Testdurchführung nicht explizit selbst vorbehält.
8 In Deutschland beispielsweise die Börsenaufsichtsbehörden der Bundesländer.

4 FINANZAUFSICHTLICHE EINBINDUNG

Für unter DORA verpflichtend durchzuführende TLPT wird die zuständige Finanzaufsicht[9] unbeschadet gesetzlicher Verpflichtungen grundsätzlich an fest vorgegebenen Punkten in den TLPT eingebunden. Sie identifiziert die verpflichtend einem Test zu unterziehenden Unternehmen[10], validiert den Testumfang und erhält den Abschlussbericht sowie den Behebungsplan. Der Austausch zwischen dem Unternehmen und den zuständigen Finanzaufsehern sowie die Weiterleitung zu teilender Dokumente erfolgt, insofern nicht anders vereinbart oder gesetzlich geregelt, grundsätzlich über das TCT.

Im Rahmen eines freiwillig durchgeführten TIBER-DE-Tests erfolgt die Einbindung der Finanzaufsicht sowie die Weitergabe von Dokumenten entsprechend der individuell getroffenen Vereinbarungen.

9 In diesem Dokument umschreibt der Begriff Finanzaufsicht die für die Beaufsichtigung der getesteten Unternehmen jeweils zuständigen Stellen in der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), der Deutschen Bundesbank, der EZB und/oder anderen Aufsichtsbehörden.
10 Entsprechend der europäischen DORA-Regulierung.

5 HAFTUNGSAUSSCHLUSS

Das vorliegende Dokument setzt das TIBER-EU-Rahmenwerk in Deutschland um. Die im vorliegenden Dokument enthaltenen Ausführungen dienen ausschließlich dem Zweck der Information. Sie stellen keine rechtliche oder sonstige fachliche Bewertung dar. Das Unternehmen bleibt für die eigenständige rechtliche und fachliche Bewertung angestrebter Testvorhaben verantwortlich. Die Bundesbank haftet nicht für eventuelle Schäden, welche aus der Nutzung des Dokuments oder im Rahmen der von Unternehmen durchgeführten TIBER-DE-Tests oder TLPT nach DORA entstehen.

Deutsche Bundesbank
Postfach 10 06 02
60006 Frankfurt am Main

Internet
https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/serviceangebot/tiber-de/
E-Mail tiber@bundesbank.de, tlpt@bundesbank.de