DEUTSCHE
BUNDESBANK
EUROSYSTEM

Implementierung von TIBER-DE

Dezember 2022

Version 3.0

Inhalt

Abkürzungen

BT	Blue Team
GTL	Generic Threat Landscape
RTP	Red Team Provider
TCT	TIBER Cyber Team
TIP	Threat Intelligence Provider
TKC	TIBER Knowledge Center
TTM	TIBER Test Manager
WT	White Team
WTL	White Team Lead

1 Einleitung und 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 Konzentration der Bereitstellung von IT-Dienstleistungen auf wenige Unternehmen zurückzuführen. Zum anderen stellen jedoch auch professionelle und hochgradig organisierte Angriffe (sogenannte APTs, Advanced Persistent Threats) eine zunehmende Gefahr dar. Um sich vor Angriffen zu schützen ist es sinnvoll, aktuelle Standards der Cybersicherheit (wie beispielsweise den IT-Grundschutz des BSI[1] oder die internationale Norm ISO/IEC 27001[2]) einzuhalten und eine unternehmensweite Sensibilisierung vorzunehmen. Ob dies jedoch den gewünschten Effekt erzielt, ist meist erst im Fall eines realen Angriffs feststellbar. So können Implementierungsfehler oder menschliche Schwächen die getroffenen Sicherheitsvorkehrungen schnell zunichtemachen.

Bedrohungsgeleitete 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)[3] ein einheitliches Rahmenwerk für bedrohungsgeleitete Penetrationstests geschaffen. Das TIBER-EU-Rahmenwerk stellt dabei sehr hohe Anforderungen an den Umfang und Ablauf solcher Tests, um eine hohe Qualität und Realitätsnähe sicherzustellen. TIBER-Tests müssen die Produktivsysteme eines Unternehmens testen. Zudem müssen prinzipiell alle kritischen Funktionen eines Unternehmens im Fokus eines TIBER-Tests enthalten sein. Auch sollen solche externen Dienstleister die Tests durchführen, die nicht Teil des getesteten Unternehmens und die speziell für die Durchführung komplexer Red-Teaming-Tests[4] qualifiziert sind.[5] Motivation für einen TIBER-Test ist es dabei nicht, die erfolgreiche Abwehr eines Angriffs sicherzustellen, sondern Schwachstellen in den eigenen Abwehrmechanismen und -maßnahmen zu identifizieren. Ein erfolgreicher TIBER-Test liefert dem Unternehmen Hinweise darüber, wie Angreifer erfolgreich vorgehen könnten, damit die eigene Cyberresilienz entsprechend verbessert werden kann.

Um diese Tests in standardisierter Form auch dem deutschen Finanzsektor zugänglich zu machen, hat die Bundesbank gemeinsam mit dem BMF im August 2019 beschlossen, das europäische TIBER-EU-Rahmenwerk in Deutschland umzusetzen. Mit der Implementierung von TIBER-DE erhalten die Unternehmen des deutschen Finanzsektors seit dem Jahr 2020 die Möglichkeit, ihre Widerstandsfähigkeit durch anspruchsvolle und zielgerichtete Angriffe auf den Prüfstand zu stellen. Seit dem Start wurde eine Reihe von Tests der Zielgruppe (s. Abschnitt 3) durchgeführt und das vorliegende Dokument auf Basis der gewonnenen Erkenntnisse aktualisiert.

Ein TIBER-DE-Test wird stets von einem Unternehmen selbst unter Einbeziehung entsprechender Dienstleis-

1 Siehe auch: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (letzter Zugriff: 23.11.2022)
2 Siehe auch: https://www.iso.org/isoiec-27001-information-security.html (letzter Zugriff: 23.11.2022).
3 Siehe auch: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html (letzter Zugriff: 23.11.2022).
4 Red-Teaming bezeichnet den Versuch beauftragter professioneller Angreifer, in die Systeme des getesteten Unternehmens einzudringen. Dabei werden jedoch ethische und rechtliche Grenzen nicht überschritten. Red-Teaming gilt als äußerst realitätsnahe Möglichkeit zur Überprüfung der eigenen Abwehrmechanismen.
5 Siehe Services Procurement Guide: https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf (letzter Zugriff: 23.11.2022).

ter durchgeführt und vom bei der Bundesbank angesiedelten nationalen Kompetenzzentrum (dem TIBER Cyber Team, TCT) begleitet und unterstützt.

Zentrale Voraussetzung für einen erfolgreichen TIBER-Test ist die vertrauensvolle Zusammenarbeit des Unternehmens mit den externen Dienstleistern und dem TCT. In einem offenen Austausch sollen nachhaltige Verbesserungen bewirkt werden. Aus diesem Grund ist TIBER-DE für die Unternehmen freiwillig und basiert auf einem kooperativen Ansatz. TIBER-Tests ergänzen somit auf effektive Weise die vielfältigen bisherigen Bemühungen von Unternehmen und ihren Aufsehern, Regulatoren und Überwachern auf diesem Gebiet und leisten einen wichtigen Beitrag zur nachhaltigen Verbesserung der Cyberwiderstandsfähigkeit des deutschen Finanzsektors.

2 Der Aufbau von TIBER-DE

Das TIBER-EU-Rahmenwerk gibt eine Vielzahl an Kernelementen vor, die bei allen TIBER-Tests einzuhalten sind. Das vorliegende Umsetzungsdokument zu TIBER-DE setzt alle diese Kernelemente um, ohne dass diese hier explizit wiederholt werden. Das vorliegende Dokument gestaltet TIBER-DE im Rahmen der durch TIBER-EU vorgegebenen Spielräume aus und legt fest, welche optionalen Elemente übernommen werden.

Die Bundesbank und das BMF haben beschlossen, bei der Umsetzung von TIBER-DE einen freiwilligen, kooperativen Ansatz zu verfolgen. Er stellt keine finanzaufsichtlich angeordnete Maßnahme dar und fördert die selbständige und selbstkritische Auseinandersetzung der Unternehmen mit der Cyberwiderstandsfähigkeit ihrer Systeme. Für die deutsche Implementierung von TIBER-EU wurde daher analog zu den TIBER-Umsetzungen in anderen europäischen Ländern eine Organisationsstruktur gewählt, die die Finanzaufsicht[6] zwar – unbeschadet gesetzlicher Verpflichtungen – an bestimmten Punkten einbezieht (vgl. Abschnitte 5 und 8), darüber hinaus den Unternehmen aber weitgehende Freiheit und Selbständigkeit beim Test und der Verbesserung ihrer eigenen kritischen Funktionen einräumt.

In dieser Struktur wird das nationale Kompetenzzentrum – das TIBER Cyber Team (TCT) – im Bereich Zahlungsverkehr und Abwicklungssysteme der Bundesbank angesiedelt und so grundsätzlich von der Finanzaufsicht getrennt. Das TCT übernimmt die Betreuung der TIBER-DE-Tests und bestätigt die Einhaltung der Vorgaben nach deren Durchführung. Hauptaufgabe – und Selbstverständnis – des TCTs ist dabei in erster Linie, das Unternehmen und die Dienstleister so zu unterstützen, dass der Nutzen für das Unternehmen möglichst maximiert wird und der gesamte Testprozess reibungslos abläuft.

Der Einbezug der Finanzaufsicht erfolgt unbeschadet gesetzlicher Verpflichtungen grundsätzlich ausschließlich über das TCT. Dieses wendet sich innerhalb der Finanzaufsicht an einen eng begrenzten Personenkreis, der mit TIBER-DE vertraut ist und das nötige Fachwissen mitbringt, um den jeweiligen TIBER-Test fachlich einordnen zu können. Insgesamt ist das TCT in Bezug auf die Durchführung von TIBER-DE-Tests Kontaktstelle für:

- Teilnehmer und potenzielle Teilnehmer
- andere Behörden, die in den TIBER-DE-Testprozess

6 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. Darüber hinaus wird grundsätzlich auch das Referat GIT 1 (Cybersicherheit in der Digitalisierung) der BaFin entsprechend eingebunden.

eingebunden werden (z.B. Sicherheitsbehörden[7])
- andere TIBER-Implementierungen in Europa
- Red Teaming- und Threat Intelligence-Dienstleister (vgl. Abschnitt 4)
- Die Bundesregierung und deren Ministerien sowie sonstige Gremien – wie etwa der Ausschuss für Finanzstabilität (AFS).

Die Weiterentwicklung von TIBER-DE sowie die Festlegung strategischer Zielsetzungen wird durch einen Lenkungsausschuss vorgenommen, der sich aus Vertretern der Bundesbank und der BaFin zusammensetzt. Der Lenkungsausschuss gibt die Schwerpunkte des Arbeitsprogramms des TCTs vor, evaluiert, inwieweit das TCT die ihm gesetzten Ziele erreicht hat und prüft mindestens einmal jährlich, ob Änderungen der TIBER-EU-Rahmenvorgaben, der Bedrohungslage oder des Marktumfeldes eine Anpassung von TIBER-DE erforderlich machen. Der Lenkungsausschuss wird vom TCT über dessen Aktivitäten und wesentliche Erkenntnisse in allgemeiner Form informiert.

Neben dem TCT können Sicherheitsbehörden in den Testprozess eingebunden werden, um die im Rahmen von TIBER-DE gesammelten Informationen zur Bedrohungslage und den Vorgehensweisen der Angreifer – soweit rechtlich möglich und angemessen – auf Plausibilität zu prüfen bzw. gegebenenfalls zu ergänzen. Dies ist vor allem im Rahmen der Erstellung und regelmäßigen Anpassung des Berichts zur nationalen Bedrohungslage sowie im Rahmen des Berichts zur unternehmensspezifischen Bedrohungslage von Bedeutung (siehe Abschnitt 5).

3 Zielgruppe

TIBER-DE richtet sich in erster Linie an kritische Unternehmen des Finanzsektors, um deren Cyberwiderstandsfähigkeit zu stärken und Ansteckungseffekte im Finanzsektor zu verringern. Dabei gehören insbesondere die folgenden Unternehmen zur Zielgruppe:

- große in Deutschland aktive Banken
- große in Deutschland aktive Versicherer
- in Deutschland aktive Finanzmarktinfrastrukturen
- in Deutschland aktive und für den Finanzsektor kritische IT-Dienstleister

Als Orientierungshilfe für Unternehmen kann dabei die Überlegung herangezogen werden, ob sich bei einem Ausfall einzelner Funktionen erhebliche Störungen oder nachhaltige negative Konsequenzen für den Finanzsektor bzw. die Finanzstabilität, die öffentliche Sicherheit oder andere kritische Sektoren ergeben könnten. Die Zielgruppe ist bewusst nicht starr definiert, um fallspezifische Einzelbewertungen zu ermöglichen und die Flexibilität freiwilliger TIBER-DE-Tests nicht einzuschränken. Nur die ganzheitliche Betrachtung eines Unternehmens, dessen interner Struktur und seiner Vernetzung mit externen Dienstleistern kann letztlich Aufschluss darüber geben, ob ein TIBER-Test empfehlenswert ist. Dabei wird das TCT die nach seiner Einschätzung relevanten Unternehmen gezielt ansprechen, um gemeinsam die Möglichkeiten der Durchführung eines TIBER-DE-Tests zu erörtern.

Auch internationale Unternehmen, die nicht nur primär in Deutschland aktiv sind, können sich einem TIBER-DE-Test unterziehen. Unter Umständen bedarf es in einem solchen Fall aber einer Abstimmung mit der zuständigen TIBER-Behörde im Heimatland des Unternehmens.

7 Sicherheitsbehörden im Sinne dieses Dokuments sind z.B. jene, welche im Nationalen Cyber-Abwehrzentrum organisiert sind. Am nationalen Cyber-Abwehrzentrum sind unter anderem folgende Behörden beteiligt: Bundesamt für Sicherheit in der Informationstechnik, Bundesamt für Verfassungsschutz, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bundeskriminalamt, Bundesnachrichtendienst, Bundespolizei, Militärischer Abschirmdienst, Zollkriminalamt.

Gemeinsame TIBER-Tests mit den für TIBER verantwortlichen TCTs anderer Mitgliedsstaaten bzw. der Europäischen Zentralbank können in diesem Fall zum Einsatz kommen, um Doppelarbeiten zu vermeiden.
Die Teilnahme an einem TIBER-Test setzt einen gewissen Reifegrad der Cyberwiderstandsfähigkeit eines Unternehmens voraus. Obwohl größere Mängel in der grundlegenden Sicherheit eines Unternehmens prinzipiell kein Hindernis für die Testdurchführung darstellen, entfaltet sich der volle Nutzen eines TIBER-Tests erst bei einem gewissen Mindestniveau an Cybersicherheit, denn nur dann wurden grobe Mängel bereits behoben und es kann somit eine Fokussierung auf detailliertere und unternehmensspezifische Schwachstellen erfolgen.

Im Ergebnis ist es das Ziel, ein Netzwerk der nationalen, zur Zielgruppe gehörenden Unternehmen zu etablieren, um gemeinsam und mithilfe der Durchführung von TIBER-DE-Tests die Cyberwiderstandsfähigkeit des Finanzsektors nachhaltig und auf kooperativer Basis zu verbessern.

4 Beteiligte Akteure

Die folgenden Akteure werden an einem TIBER-Test beteiligt (vgl. Abbildung 1):

- Das **TCT** stellt das nationale Kompetenzzentrum einer TIBER-Implementierung dar. In Deutschland ist das TCT bei der Bundesbank angesiedelt (vgl. Abschnitt 2). Es begleitet die von Unternehmen durchgeführten TIBER-Tests während ihres kompletten Verlaufs, unterstützt diese mit dem benötigten Fachwissen, achtet auf die Einhaltung der Rahmenbedingungen von TIBER-Tests, attestiert deren Rahmenwerkskonformität nach Abschluss und stellt die Kommunikationsschnittstelle nach außen dar. Das TCT kann einen Test als nicht TIBER-konform einstufen, wenn dieser nicht im Einklang mit dessen Anforderungen durchgeführt wurde. Bei grenzüberschreitenden TIBER-Tests können die verantwortlichen TCTs anderer Mitgliedstaaten in den Test eingebunden werden. Durch die Einbindung wird die Akzeptanz des TIBER-Tests in diesen Mitgliedsstaaten sichergestellt.

- Der **TIBER Test Manager (TTM)** ist ein Mitglied des TCT, welcher ein spezifisches Unternehmen betreut und die Schnittstelle zu diesem bildet. Der TTM betreut das Unternehmen während der gesamten Laufzeit eines TIBER-Tests und ist prinzipiell in alle Treffen und Absprachen zwischen den beteiligten Akteuren eingebunden. Dies gilt uneingeschränkt auch für regelmäßige Telefonate, wie etwa zur Absprache aktueller Angriffsschritte während der Testphase.

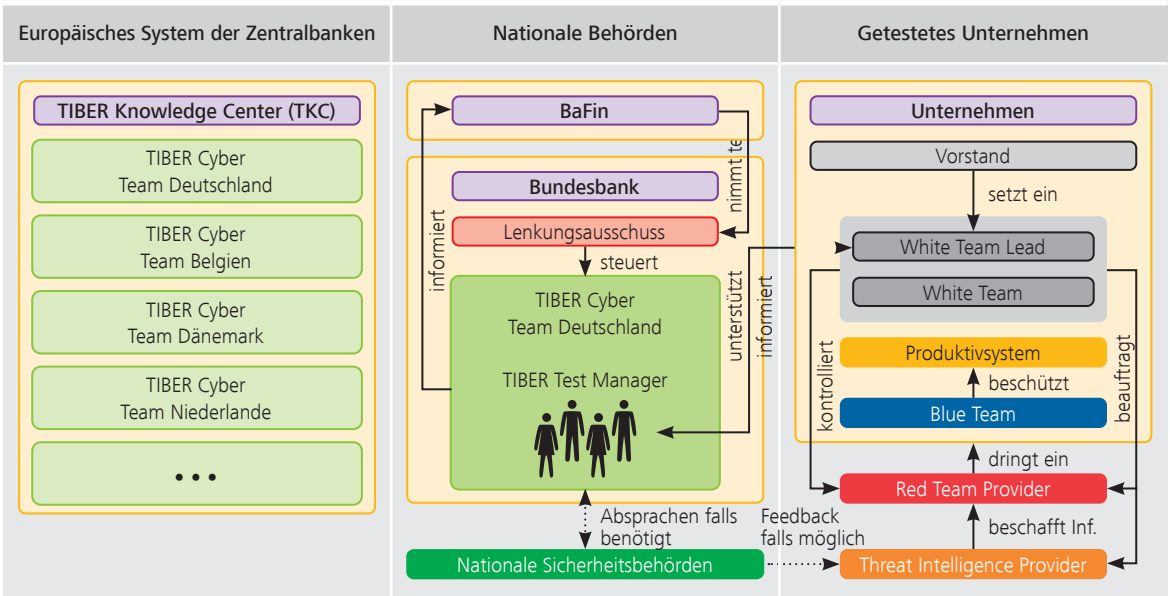
- Das **White Team (WT),** welches durch den **White Team Lead (WTL)** geleitet wird, ist die für die Durchführung eines TIBER-Tests verantwortliche Instanz innerhalb eines Unternehmens. Der WTL wird gemäß Anforderung im Rahmenwerk durch den Unternehmensvorstand eingesetzt und bildet die Schnittstelle zum TTM des TCTs.[8]

- Das **Blue Team (BT)** besteht aus allen Mitarbeitern des Unternehmens, welche nicht Teil des WT sind. In der Praxis wird dieses jedoch i.d.R. durch Mitarbeiter der mit der Unternehmenssicherheit beauftragten Stellen (z.B. Security Operations Center, Computer Emergency Response Team, etc.) repräsentiert. Das BT darf nicht über die Durchführung eines TIBER-Tests informiert sein.

8 Weitere Details zu den Aufgaben des White Teams sind in der White Team Guidance des TIBER-EU-Rahmenwerk festgelegt, welche über die Webseite der EZB einsehbar ist: https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf (letzter Zugriff: 23.11.2022).

- Als externe Dienstleister werden der **Red Team Provider (RTP)** zur Bereitstellung des Red Teams sowie der **Threat Intelligence Provider (TIP)** zur Bereitstellung der Threat Intelligence von den hierzu autorisierten Mitgliedern des White Teams engagiert. Die hierzu autorisierten Mitglieder des White Teams schließen Verträge mit den Dienstleistern ab und beaufsichtigen die korrekte Ausführung des Tests im Unternehmen durch die Dienstleister. Während der TIP Informationen über generelle und unternehmensspezifische Schwachstellen sammelt und diese dem RTP zur Verfügung stellt, führt der RTP die eigentlichen Angriffe durch. Dabei ist es das Ziel, die Abwehrmaßnahmen des Unternehmens zu überwinden und in das Produktivsystem einzudringen. Sofern dies rechtlich und organisatorisch möglich ist, wird angestrebt, die gesammelten Informationen zur Bedrohungslage in Absprache mit dem TCT einem Feedback durch eine oder mehrere nationale Sicherheitsbehörden zu unterziehen.
- Das **TIBER Knowledge Center (TKC)** stellt das europäische Kompetenzzentrum für alle nationalen TIBER-Implementierungen dar. Es setzt sich aus Vertretern der nationalen TCTs derjenigen EU-Mitgliedsstaaten zusammen, in denen das TIBER-EU-Rahmenwerk implementiert wurde. Neben der Weiterentwicklung von TIBER-EU verfolgt das TKC das Ziel, die TCTs aller Mitgliedsstaaten bei ihren TIBER-Implementierungen zu unterstützen. Dazu stellt es relevante Dokumente und Trainings bereit, ermöglicht den Erfahrungsaustausch und die Zusammenarbeit der Länder und stellt die Vergleichbarkeit hinsichtlich der Methoden und Qualität der nationalen Umsetzungen sicher. Es werden jedoch keine konkreten Ergebnisse geteilt oder detaillierte Informationen zu den einzelnen Tests weitergegeben. Das TCT der Bundesbank ist im TKC vertreten und beteiligt sich aktiv an der Sicherstellung einer hohen Qualität von TIBER-Tests.

An TIBER-DE beteiligte Akteure Abbildung 1



An TIBER-DE beteiligte Akteure: TIBER Knowledge Center (TKC), TIBER Cyber Team (TCT), TIBER Test Manager (TTM), White Team (WT), White Team Lead (WTL), Blue Team (BT), Red Team Provider (RTP), Threat Intelligence Provider (TIP), ggf. nationale Sicherheitsbehörden.

Quelle: Deutsche Bundesbank

5 Der Ablauf eines TIBER-DE-Tests

Für die Durchführung von TIBER-DE-Tests wird durch das TCT ein Bericht zur nationalen Bedrohungslage[9] bereitgestellt, welcher allen sich testenden Unternehmen als Ausgangsbasis zur Verfügung steht. Ein solcher Bericht beschreibt die generelle, unternehmensunabhängige Bedrohungssituation des nationalen Finanzsektors und sollte regelmäßig aktualisiert werden.

Ein TIBER-DE-Test ist in drei Phasen eingeteilt:[10]

- Die **Vorbereitungsphase** umfasst die Schritte Initiierung, Kick-Off, Bestimmung des Testumfangs und Beschaffung (siehe Abbildung 2). In dieser Phase werden die folgenden Tätigkeiten durchgeführt:

  – Die Durchführung eines TIBER-DE-Tests wird formal vom Unternehmen und vom TCT beschlossen. Das für den Test zuständige White Team inklusive des White Team Leads wird vom Unternehmen in Absprache mit dem TCT bestimmt. Das White Team legt ein Pseudonym für den TIBER-DE-Test fest. Aufgrund der sensiblen Natur der auszutauschenden Testinformationen ist dieses Pseudonym anstelle des Klarnamens des Unternehmens in allen TIBER-bezogenen Kommunikationsprozessen zu verwenden.

  – Im Rahmen eines Initiierungstreffens[11] informiert der TTM das WT über den TIBER-DE-Testprozess, die beteiligten Akteure und ihre Verantwortlichkeiten, Sicherheitsprotokolle und sichere Kommunikationskanäle sowie Modalitäten der weiteren Testplanung und -durchführung.

  Die Finanzaufsicht wird über die beabsichtigte Durchführung des TIBER-DE-Tests durch das TCT informiert. Notwendige Maßnahmen zum Risikomanagement inklusive notwendiger Risikomanagementkontrollen und -prozesse werden durch das WT etabliert, um eine kontrollierte und sichere Testdurchführung zu ermöglichen (s. auch Abschnitt 6).

  – Im Rahmen eines Kickoff-Treffens[12] werden alle relevanten Akteure (soweit bereits festgelegt) über den Testablauf informiert, tauschen ihre gegenseitigen Erwartungen aus und legen das weitere Vorgehen fest. Grundlage der Diskussion bildet dabei der durch das WT vorbereitete Projektplan[13], welcher die generelle Zeitplanung inklusive zu organisierender Treffen und zu erstellender Dokumente beinhaltet und bei Bedarf angepasst wird. An dem Kickoff-Treffen kann auf Wunsch auch die Finanzaufsicht teilnehmen.

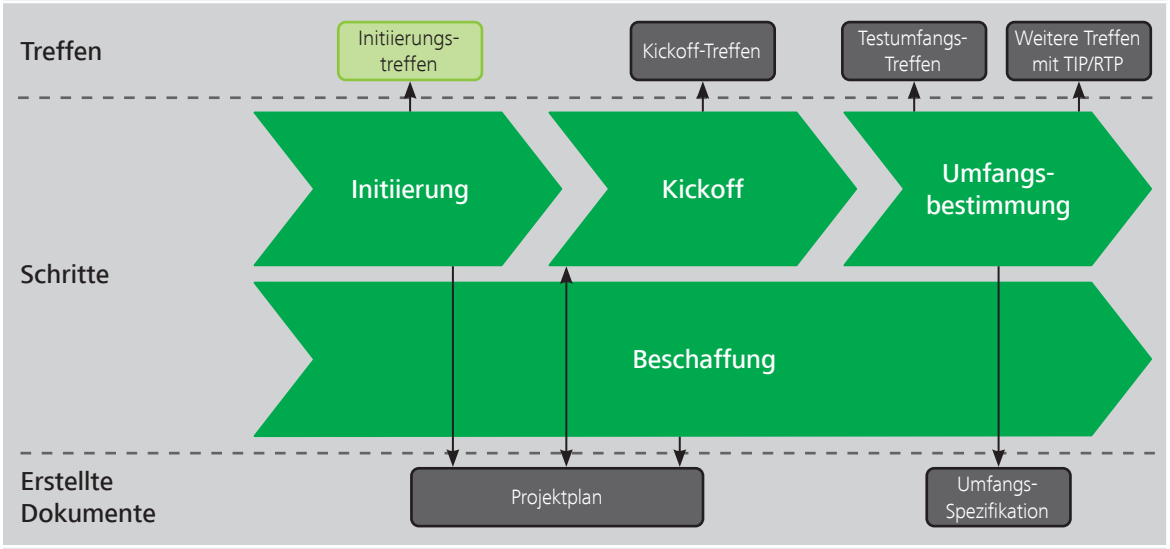
  – Der Umfang des Tests wird festgelegt. Dabei muss der Testumfang alle kritischen Funktionen des Unternehmens beinhalten und in einer Umfangsspezifikation[14] schriftlich festgehalten werden. Im Rahmen eines Testumfangstreffens[15] wird die Umfangsspezifikation dem TCT, WT, RTP und TIP (falls Ausschreibung und Vergabe bereits abgeschlossen sind) vorgestellt und nach deren Rückmeldung finalisiert sowie vom Unternehmensvorstand und dem TCT genehmigt. Die Umfangsspezifikation wird der zuständigen Finanzaufsicht vor dem Testumfangstreffen zur Kenntnisnahme vorgelegt. Etwaige Anmerkungen können so über das TCT während des Testumfangstreffens

9 Entspricht dem GTL-Report des TIBER-EU-Rahmenwerks.
10 Eine Übersicht über alle im Rahmen der drei Phasen durchzuführenden Treffen bzw. zu erstellenden Dokumente einschließlich der jeweiligen Verantwortlichen und involvierten Akteure befindet sich in Annex 1 und 2 (Abschnitt 10).
11 Entspricht dem Pre-launch meeting des TIBER-EU-Rahmenwerks.
12 Entspricht dem Launch Meeting des TIBER-EU-Rahmenwerks.
13 Entspricht dem Project Plan des TIBER-EU-Rahmenwerks.
14 Entspricht dem Scope Specification Document des TIBER-EU-Rahmenwerks.
15 Entspricht dem Scoping Meeting des TIBER-EU-Rahmenwerks.

eingebracht werden. Die Finanzaufsicht wird nach diesem Schritt unbeschadet gesetzlicher Verpflichtungen grundsätzlich erst wieder im Rahmen der Übersendung des Abschlussberichts eingebunden.

– Im Zuge der Beschaffung werden TIP und RTP vom Unternehmen ausgewählt und das Unternehmen schließt mit ihnen Verträge (Beschaffung; dabei darf prinzipiell ein Anbieter beide Teams stellen, die Teams müssen sich jedoch aus unterschiedlichen Personen zusammensetzen). Beide Teams sind vom WTL umfassend über den Projektplan und den Testumfang zu unterrichten. Dies kann zum einen bereits im Rahmen des Testumfangstreffens, zum anderen in weiteren Treffen des WTs mit dem TIP und dem RTP erfolgen.

Vorbereitungsphase eines TIBER-DE-Tests Abbildung 2



Verantwortlichkeiten eingefärbt: WTL (grau), TTM (hellgrün).
Quelle: Deutsche Bundesbank

- Die **Testphase** umfasst die Schritte Sammlung von Informationen zur Bedrohungslage und Durchführung des Red Team Tests (siehe Abbildung 3). In dieser Phase werden die folgenden Tätigkeiten durchgeführt:

  – Erstellung eines Berichts zur unternehmensspezifischen Bedrohungslage[16] durch den TIP, welcher basierend auf dem bereitgestellten Bericht zur nationalen Bedrohungslage weitere unternehmensspezifische Bedrohungen, Schwachstellen und Angriffsszenarien beinhaltet. Wegen der im Vergleich zu realen Angriffen stark reduzierten Zeit zur Informationssammlung ist eine Anreicherung des Berichts durch unternehmensinterne relevante Informationen explizit vorgesehen (z.B. Überblick über vorhandene Systeme zur Unterstützung kritischer Funktionen, Risikoregister, identifizierte Schwachstellen, Beispiele kürzlich aufgetretener Angriffe). Der TIP berichtet dem

16 Entspricht dem Targeted Threat Intelligence Report des TIBER-EU-Rahmenwerks.

WTL und dem TTM regelmäßig über den Fortschritt der Informationssammlung.

– Diskussion des durch den TIP erstellten Berichtsentwurfs zur unternehmensspezifischen Bedrohungslage sowie Vorstellung, Diskussion und Auswahl möglicher Angriffsszenarien im Rahmen eines Szenario-Workshops[17].

– Weiterentwicklung des Berichts zur unternehmensspezifischen Bedrohungslage (falls gewünscht unter Einbeziehung relevanter nationaler Sicherheitsbehörden) durch den TIP.

– Erstellung eines Testplans durch den RTP[18], welcher auf dem Bericht zur unternehmensspezifischen Bedrohungslage basiert und die zu testenden Angriffsszenarien auf die kritischen Funktionen des Unternehmens ausformuliert.

  Dabei ist es ausdrücklich erlaubt, neben den im Bericht zur unternehmensspezifischen Bedrohungslage beschriebenen, bedrohungsgeleiteten Angriffsszenarien auch weitere, als relevant eingestufte Szenarien in den Testplan einzubeziehen bzw. eine modulare Kombination verschiedener Angriffsschritte vorzunehmen. Unter einem solchen sog. „Szenario X" ist ein Szenario zu verstehen, in dem das Red Team nicht einen konkreten Threat Actor imitieren muss, sondern von der bedrohungsgeleiteten Natur eines TIBER-DE-Tests abweichen kann. So können auch alternative bzw. explorative Szenarien einbezogen werden.

– Diskussion des durch den RTP erstellten Testplans im Rahmen eines Testplan-Workshops. Finalisierung des Berichts zur unternehmensspezifischen Bedrohungslage und des Testplans im Anschluss an den Testplan-Workshop.

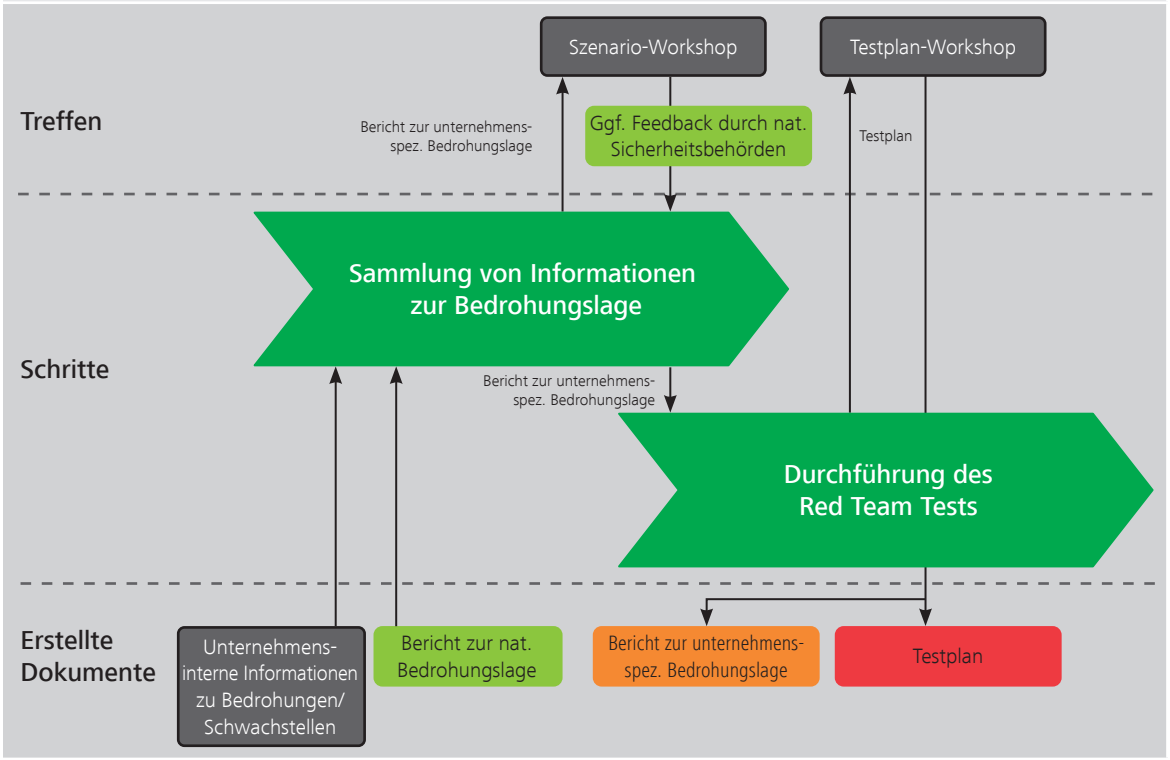
– Durchführung des Red Teamings durch den RTP anhand der spezifizierten Angriffsszenarien. Dabei können auf Basis zwischenzeitlich gewonnener Erkenntnisse und in Absprache mit dem TTM kurzfristige Anpassungen des Testplans vorgenommen oder Hilfestellungen (sog. Leg-ups) gegeben werden. Der RTP berichtet dem WTL und dem TTM in regelmäßigen Updates über den Fortschritt des Red Teamings.

– Eine zeitliche Überschneidung der Tätigkeiten des TIP und des RTP ist möglich, d.h. die durch den TIP gelieferten Schwachstelleninformationen können auch während der Planung und Durchführung der Angriffe weiter angereichert und präzisiert werden.

  Durch die frühzeitige Beteiligung des RTP bei der Erstellung der Angriffsszenarien im Rahmen des Berichts zur unternehmensspezifischen Bedrohungslage können bspw. die durch den TIP gesammelten Informationen zielgerichteter aufbereitet werden. Zudem kann die Verfügbarkeit des TIP während des Red Teamings den bedrohungsgeleiteten Charakter der Angriffsszenarien auch bei nötigen Anpassungen sicherstellen.

17 Entspricht dem Threat Intelligence/Scenario Workshop des TIBER-EU-Rahmenwerks.
18 Entspricht dem Red Teaming Test Plan des TIBER-EU-Rahmenwerks.

Testphase eines TIBER-DE-Tests (ca. 18 Wochen, davon ca. 6 Wochen Threat Intelligence und ca. 12 Wochen Red Teaming) Abbildung 3



Verantwortlichkeiten eingefärbt: WTL (grau), TTM (hellgrün), TIP (orange), RTP (rot).
Quelle: Deutsche Bundesbank

- Die **Abschlussphase** umfasst die Schritte Erstellung der Testberichte, Replay, Purple Teaming und Feedback, Behebungsplan und Abschlussbericht (einschließlich Evaluationsworkshop) sowie Attestierung und Ergebnisweitergabe (siehe Abbildung 4). In dieser Phase werden die folgenden Tätigkeiten durchgeführt:

  – Der RTP verfasst einen Testbericht (RT-Testbericht[19]), welcher das konkrete Vorgehen bei der Durchführung der Angriffe sowie deren Ergebnisse und weitere Beobachtungen beschreibt. Der Bericht sollte ebenfalls detaillierte Informationen zu Möglichkeiten der Verbesserung der Abwehrmechanismen beinhalten (z.B. bzgl. physischer oder technischer Sicherheitsvorkehrungen, Unternehmensrichtlinien und -abläufen, Sensibilisierung und Ausbildung der Mitarbeiter, etc.)

  – Alle relevanten Stellen im Unternehmen werden zu Beginn der Abschlussphase über den Test informiert (Blue Team Briefing).

  – Das BT verfasst basierend auf dem RT-Testbericht einen eigenen Testbericht (BT-Testbericht[20]) über die ergriffenen Gegenmaßnahmen des Unternehmens.

  – RT-Testbericht und BT-Testbericht werden dem TTM zur Einsichtnahme zur Verfügung gestellt.[21]

19 Entspricht dem Red Team Test Report des TIBER-EU-Rahmenwerks.
20 Entspricht dem Blue Team Report des TIBER-EU-Rahmenwerks.
21 Aufgrund des hohen Vertraulichkeitsniveaus dieser Unterlagen werden RT-Testbericht und BT-Testbericht nicht vom TCT gespeichert oder anderweitig aufbewahrt.

– Im Rahmen eines Replay-Workshops[22] werden die durchgeführten Angriffe vorgestellt und aus den Perspektiven des RTP und des BT analysiert. Zudem werden ebenfalls alternative Angriffs- und Abwehrmöglichkeiten in Form eines Purple-Teaming-Elements diskutiert, bei dem der RTP und das BT gemeinsam abweichende Angriffsverläufe und entsprechende Verteidigungsmaßnahmen erörtern (z.B. als „Tabletop Exercise"). Das Blue Team kann somit einen Einblick erlangen, wo das Red Team zu welchem Zeitpunkt war und wo/wie es dieses hätte entdecken/aufhalten können.

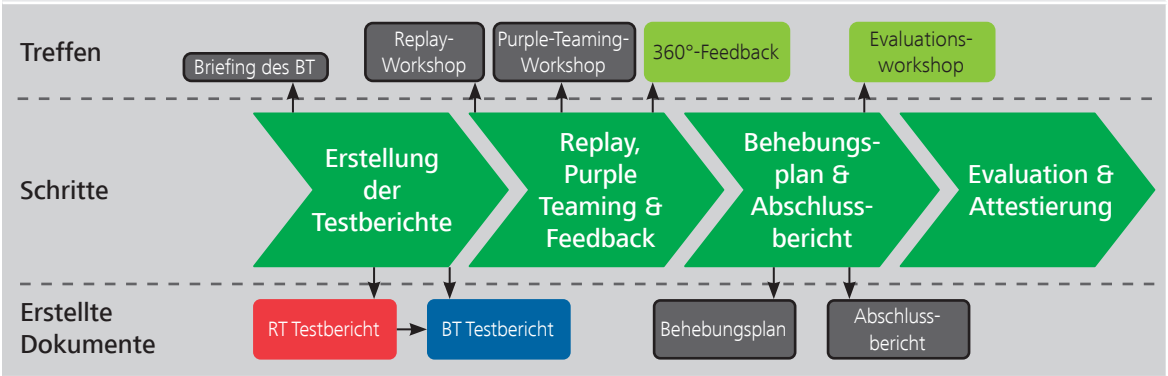
– Im Rahmen eines 360°-Feedback-Workshops[23] geben sich die am Test beteiligten Akteure (TCT, WT, RTP und TIP) Rückmeldung bezüglich ihrer Erfahrungen mit der praktischen Durchführung des TIBER-DE-Tests.

– Das Unternehmen erstellt basierend auf den Testergebnissen einen Maßnahmen-/Behebungsplan[24] auf angemessenem Abstraktionsniveau, welcher die angestrebten Maßnahmen und einen Zeitplan zur Behebung der Schwachstellen aufführt, jedoch keine technischen Details zu diesen enthält. Der Plan ist Bestandteil eines ebenfalls vom Unternehmen zu erstellenden Abschlussberichts[25], welcher den Test und die daraus gewonnenen Erkenntnisse zusammenfasst.

– Die TCT-Leitung organisiert in der Regel einen ergänzenden Evaluationsworkshop zwischen dem Unternehmen und den Mitgliedern des Lenkungsausschusses von TIBER-DE (vgl. Abschnitt 2). Damit soll die Effizienz von TIBER-DE gewährleistet, Anhaltspunkte für eine Verbesserung der TCT-Aktivitäten gewonnen und eine fortlaufende Weiterentwicklung von TIBER-DE sichergestellt werden.

– Die rahmenwerkskonforme Durchführung des TIBER-DE-Tests wird durch das TCT attestiert. Das Unternehmen sendet den Abschlussbericht inklusive des Maßnahmen-/Behebungsplans an das TCT, welches diesen an die zuständige Stelle der Finanzaufsicht weiterleitet (vgl. Abschnitt 8).

Abschlussphase eines TIBER-DE-Tests Abbildung 4



Verantwortlichkeiten eingefärbt: WTL (grau), TTM (hellgrün), RTP (rot), BT (blau).
Quelle: Deutsche Bundesbank

22 Entspricht dem Replay Workshop des TIBER-EU-Rahmenwerks.
23 Entspricht dem 360-Degree Feedback Meeting des TIBER-EU-Rahmenwerks.
24 Entspricht dem Remediation Plan des TIBER-EU-Rahmenwerks.
25 Entspricht dem Test Summary Report des TIBER-EU-Rahmenwerks.

6 Risiken eines TIBER-DE-Tests

Wegen ihrer Durchführung auf den Produktivsystemen sowie der hohen Flexibilität in der Vorgehensweise bieten TIBER-DE-Tests die Möglichkeit einer realitätsnahen Analyse der Cyberwiderstandsfähigkeit eines Unternehmens. Dies bringt jedoch auch Risiken bezüglich der Vertraulichkeit, Integrität oder Verfügbarkeit der Daten bzw. Systeme mit sich. So besteht beispielsweise die Möglichkeit, dass bei unsachgemäßer Durchführung der Tests Systeme beschädigt werden oder ausfallen sowie Daten gelöscht oder unzulässig verbreitet werden könnten. Die einen Test durchführenden Unternehmen sollten daher zunächst eine detaillierte Analyse der Risiken durchführen, die bei der Testdurchführung schlagend werden könnten und dann angemessene Maßnahmen zur Minimierung solcher Risiken vor, während und nach der Testdurchführung ergreifen. Die Bundesbank begleitet im Rahmen ihrer Tätigkeit als nationales Kompetenzzentrum (TCT) alle TIBER-DE-Tests, übernimmt jedoch keine Haftung für eventuelle Schäden, die im Rahmen der von Unternehmen durchgeführten TIBER-DE-Tests entstehen. Das WT ist verantwortlich für die Durchführung des TIBER-DE-Tests, die daraus resultierenden Risiken und deren Minimierung. Es muss sicherstellen, dass Risiken zu jedem Zeitpunkt angemessen identifiziert, analysiert und kontrolliert werden. Einige Beispiele für mögliche diesbezügliche Maßnahmen sind:

- Erstellung detaillierter Risikoanalysen und entsprechender Risiko-Minimierungsmaßnahmen während aller Phasen eines TIBER-DE-Tests;
- Festlegung und ausschließliche Verwendung eines Pseudonyms für das getestete Unternehmen anstelle des Klarnamens;
- Sicherstellung angemessener Regelungen zur Haftung im Schadensfall (inkl. möglicher Versicherungen) in den Verträgen mit sämtlichen einbezogenen externen Anbietern (z.B. TIP und RTP);
- Ausreichende Seniorität (Vorstandsebene) mindestens eines Mitglieds des WT[26], um die Entscheidungsfähigkeit des WT und eine direkte Kommunikation mit dem Vorstand sicherzustellen;
- Klare Befugnis und Beauftragung des WT, im Fall eines erhöhten Schadensrisikos die Tests zu unterbrechen, um in Absprache mit den Anbietern und dem TTM das weitere Vorgehen festzulegen;
- Klare Definition von Umfang, Grenzen, der Erreichbarkeit der Dienstleister und zeitlichem Ablauf der Tests in den Verträgen mit sämtlichen einbezogenen externen Dienstleistern (z.B. TIP und RTP);
- Auswahl externer Anbieter (z.B. TIP und RTP) entsprechend der Vorgaben der TIBER-EU Services Procurement Guidelines[27] und in Rücksprache mit dem TTM;
- Klare Eskalationswege sowie Benennung entsprechender Ansprechpartner für den Notfall sowohl zwischen Unternehmen und externen Anbietern als auch innerhalb des Unternehmens und gegenüber dem TTM;
- Abgrenzung von Handlungen, die RTP und TIP im Rahmen des TIBER-DE-Tests erlaubt sein sollen, d.h. die das Unternehmen gestattet (i. S. e. tatbestandsausschließenden Einverständnisses bzw. Rechtfertigung straf- und zivilrechtlicher Verletzungshandlungen) von Handlungen, die nicht vorgenommen werden sollen. Dies kann insbesondere im Wege der Auflistung von Handlungen geschehen, die ausdrücklich erlaubt sein sollen (white list) oder durch Nennung solcher Handlungen, die in jedem Fall unterbleiben sollen (black list);
- Stufenweiser Aufbau des Tests zur regelmäßigen Kontrolle, wie weit der RTP in die Systeme eingedrungen ist;
- Enger Einbezug des TTM bei allen risikorelevanten Entscheidungen während des Tests.

26 Siehe auch TIBER-EU White Team Guidance: https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf (letzter Zugriff: 23.11.2022).
27 Die TIBER-EU Services Procurement Guidelines können auf der Webseite der EZB eingesehen werden: https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf (letzter Zugriff: 23.11.2022).

7 Vorgegebene und freiwillige Elemente

Das TIBER-EU-Rahmenwerk legt den Großteil der durchzuführenden Elemente fest, lässt jedoch auch Ausgestaltungsspielräume für die nationalen Implementierungen bzw. die Unternehmen.[28] Über die vom TIBER-EU-Rahmenwerk vorgesehenen Kernelemente hinaus sind in der deutschen TIBER-Umsetzung folgende Aspekte vorgegeben (vorgegebene Elemente):

- Im Rahmen von TIBER-DE-Tests ist die Kenntnisnahme der Umfangsspezifikation als auch eine optionale Teilnahme am Kickoff-Treffen durch die zuständige Finanzaufsicht vorgesehen, um transparent über die Durchführung und den Umfang des Tests zu informieren. Danach wird die entsprechende Finanzaufsicht unbeschadet gesetzlicher Verpflichtungen grundsätzlich erst wieder nach dem Abschluss des Tests im Rahmen der Vorlage eines zusammenfassenden Abschlussberichts inkl. eines Maßnahmen-/Behebungsplans (vgl. Abschnitt 8) einbezogen.

- Das TIBER-EU-Rahmenwerk sieht die Möglichkeit vor, einen Bericht zur nationalen Bedrohungslage im Finanzsektor (Generic Threat Landscape, GTL) zu erstellen, welcher allen einen TIBER-DE-Test durchführenden Unternehmen zur Verfügung steht und als Basis für die Erstellung des Berichts zur unternehmensspezifischen Bedrohungslage des TIP dient. Im Rahmen der TIBER-DE-Implementierung wird ein solcher Bericht bereitgestellt und in regelmäßigen Abständen aktualisiert. Nach Möglichkeit soll der Bericht mit den nationalen Sicherheitsbehörden diskutiert werden, um seine Zuverlässigkeit zu erhöhen.

- Die Analyse der Tests aus Sicht eines Purple Teams (Purple Team = Red Team + Blue Team; vgl. Abschnitt 5) ist aufgrund des damit verbundenen Lerneffekts im Rahmen eines TIBER-DE-Tests vorgegeben.

Darüber hinaus steht es jedem Unternehmen frei, bei einem TIBER-DE-Test folgende optionale Elemente des TIBER-EU-Rahmenwerkes zu adressieren (freiwillige Elemente):

- Dem Unternehmen steht es frei, über seine kritischen Funktionen hinaus weitere im Rahmen eines TIBER-DE-Tests zu untersuchende Prozesse zu spezifizieren.

- Der kontinuierliche Einbezug des TIP über den Beginn der Angriffe durch den RTP hinaus kann unter bestimmten Umständen sinnvoll sein und steht dem Unternehmen frei.

- Der Einbezug physischer Testmethoden (z.B. physische Zugangsverschaffung zum Netzwerk, Platzierung eines Geräts der Angreifer im Unternehmen) ist generell erwünscht und wird befürwortet, insofern dies vom Unternehmen ausdrücklich erlaubt wird und nicht im Widerspruch zur aktuellen Rechtslage oder den Sicherheitsanforderungen des Unternehmens steht.

- Bei der Durchführung des Replay-Workshops steht es dem Unternehmen frei, welche externen, über den RTP und den TTM hinausgehenden Beteiligten einbezogen werden sollen.

28 Die Vorgaben des TIBER-EU-Rahmenwerks sind im Rahmendokument der EZB festgelegt: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf (letzter Zugriff: 23.11.2022).

8 Ergebnisse und finanzaufsichtliche Verwendung

Die detaillierten Ergebnisse des TIBER-DE-Tests und Details über die gefundenen Schwachstellen verbleiben ausschließlich beim getesteten Unternehmen. Aus Gründen der Sicherheit dürfen solche sensiblen Informationen nicht weitergegeben oder offengelegt werden. Weiterhin darf keine zentrale Stelle geschaffen werden, die hoch sicherheitsrelevante Informationen von möglicherweise systemrelevanten Akteuren des deutschen Finanzsystems ansammelt (Konzentrationsrisiko). Aus diesem Grund ist in TIBER-DE unbeschadet gesetzlicher Verpflichtungen keine automatische Weiterleitung der detaillierten Testergebnisse vorgesehen. Auch das TCT wird keine solchen Details speichern oder aufbewahren.

Die zuständige Finanzaufsicht wird unbeschadet gesetzlicher Verpflichtungen grundsätzlich an fest vorgegebenen Punkten in den TIBER-DE-Test eingebunden. Wie oben ausgeführt, muss die Finanzaufsicht über die Durchführung eines TIBER-DE-Tests informiert werden, nimmt auf Wunsch am Kickoff-Meeting teil und erhält Kenntnis über die Umfangsspezifikation des Tests. Darüber hinaus muss das Unternehmen nach Abschluss des Tests einen zusammenfassenden Abschlussbericht inkl. eines Maßnahmen-/Behebungsplans an das TCT senden, welches diesen an die Finanzaufsicht weiterleitet (vgl. Abschnitt 5). Der Bericht soll dabei konkrete Verbesserungen mit Zeitplanung auf einem angemessenen Abstraktionsniveau sowie generelle Erfahrungen aus dem TIBER-DE-Test beinhalten. Der Austausch zwischen dem Unternehmen und den zuständigen Finanzaufsehern erfolgt im Rahmen von TIBER-DE-Tests unbeschadet gesetzlicher Verpflichtungen ausschließlich über das TCT und etablierte Kontaktpunkte der Finanzaufsicht, die mit dem TIBER-DE-Rahmenwerk vertraut sind und die Ergebnisse dementsprechend einschätzen können.

9 Haftungsausschluss

Das vorliegende Dokument beschreibt die Umsetzung des TIBER-EU-Rahmenwerks in Deutschland (TIBER-DE) und setzt dessen Kernelemente 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 entstehen.

10 Annex

Annex 1: Im Laufe eines TIBER-DE-Tests durchzuführende Treffen mit Ausrichtungsverantwortlichem und verpflichtend teilnehmenden Akteuren. Der TTM ist dabei grundsätzlich in alle Treffen und Absprachen zwischen den beteiligten Akteuren eingebunden. Über die hier aufgeführten Treffen hinaus sind regelmäßige Treffen oder Telefonate zu Informations- und Abstimmungszwecken zu organisieren.

	Treffen	Ausrichtungs-verantwortlicher	Verpflichtende (freiwillige) Teilnahme
Vorbereitungsphase	Initiierungstreffen	TTM	WTL (WT), TTM
	Kickoff-Treffen	WTL	WTL (WT), TTM, (TIP), (RTP), (Finanzaufsicht)
	Testumfangs-Treffen	WTL	WTL (WT), TTM, (TIP), (RTP)
Testphase	Szenario-Workshop	WTL	WTL (WT), TTM, TIP, RTP
	Testplan-Workshop	WTL	WTL (WT), TTM, TIP, RTP
	Weitere Treffen mit TIP/RTP nach Bedarf	WTL	WTL (WT), (TTM), TIP, RTP
Abschlussphase	Replay-Workshop	WTL	WTL (WT), TTM, RTP, BT, (TIP)
	Purple-Teaming-Workshop	WTL	WTL (WT), TTM, RTP, BT, (TIP)
	360°-Feedback-Workshop	TTM	WTL (WT), TTM, RTP, BT, TIP
	Evaluationsworkshop	TCT-Leitung	TCT-Leitung, Lenkungsausschuss, WTL, (WT), (TIP), (RTP)

Annex 2: Im Laufe eines TIBER-DE-Tests zu erstellende Dokumente mit Erstellungsverantwortlichem und verpflichtend abzustimmenden Akteuren

	Erstelltes Dokument	Erstellungs-/Bereitstellungs-verantwortlicher	Verpflichtend (freiwillig) abzustimmen mit
Vorbereitungsphase	Projektplan	WTL	TTM, (TIP), (RTP)
	Umfangsspezifikation	WTL	Unternehmensvorstand, TTM, TIP, RTP, Finanzaufsicht
Testphase	Unternehmensinterne Informationen zu Bedrohungen/ Schwachstellen (als Beitrag zum Bericht zur unternehmensspezifischen Bedrohungslage)	WTL	TTM
	Bericht zur unternehmensspezifischen Bedrohungslage	TIP	WTL, TTM, RTP, (nat. Sicherheitsbehörden)
	Testplan	RTP	WTL, TTM, TIP
Abschlussphase	RT-Testbericht	RTP	WTL, TTM
	BT-Testbericht	BT	WTL, TTM
	Behebungsplan	WTL	TTM
	Abschlussbericht	WTL	TTM
	TIBER-DE-Attestierung	TTM	TIP, RTP, Unternehmensvorstand

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