Rat der
Europäischen Union

Brüssel, den 17. Februar 2025
(OR. en)

6302/25
ADD 1

EF 34
ECOFIN 162
DELACT 10

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	14. Februar 2025
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	C(2025) 885 final
Betr.:	ANHÄNGE der DELEGIERTEN VERORDNUNG (EU) …/… DER KOMMISSION 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 Penetrationstests 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 Ergebnisse, 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 gegenseitigen Anerkennung dieser Tests erforderlich ist

Die Delegationen erhalten in der Anlage das Dokument C(2025) 885 final.

Anl.: C(2025) 885 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 13.2.2025
C(2025) 885 final

ANNEXES 1 to 8

ANHÄNGE

der

DELEGIERTEN VERORDNUNG (EU) …/… DER KOMMISSION

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 Penetrationstests 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 Ergebnisse, 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 gegenseitigen Anerkennung dieser Tests erforderlich ist

ANHANG I
Inhalt der Projektcharta (Artikel 9 Absatz 2 Buchstabe a)

Information	**Erforderliche Angaben**
Für den Projektplan verantwortliche Person, d. h. Leiter des Kontrollteams	Name Kontaktdaten
Tester	☐ intern ☐ extern ☐ beides
Gemäß Artikel 9 Absatz 2 Buchstabe d und Artikel 9 Absatz 4 Buchstabe a gewählte Kommunikationskanäle, einschließlich: a) Verwendung von E-Mail-Verschlüsselung b) Verwendung von Online-Datenräumen c) Verwendung von Instant Messaging	
Codename des TLPT	
Etwaige kritische oder wichtige Funktionen, die das Finanzunternehmen in anderen Mitgliedstaaten ausübt	1. Auflistung kritischer oder wichtiger Funktionen, die in einem anderen Mitgliedstaat ausgeübt werden 2. für jede kritische oder wichtige Funktion Angabe des Mitgliedstaats bzw. der Mitgliedstaaten, in dem (denen) sie ausgeübt werden
Etwaige kritische oder wichtige Funktionen, die von IKT-Drittdienstleistern unterstützt werden	3. Auflistung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern unterstützt werden 4. für jede Funktion Angabe des IKT-Drittdienstleisters
Voraussichtliche Fristen für den Abschluss	
1) der Vorbereitungsphase gemäß Artikel 9	JJJJ-MM-TT
2) der Testphase gemäß den Artikeln 10 und 11	JJJJ-MM-TT
3) der Abschlussphase gemäß Artikel 12	JJJJ-MM-TT

4) der Erstellung des Plans mit Abhilfemaßnahmen gemäß Artikel 13	JJJJ-MM-TT

ANHANG II
Inhalt des Scoping-Dokuments (Artikel 9 Absatz 6)

1. Das Scoping-Dokument enthält eine Auflistung aller kritischen oder wichtigen Funktionen, die das Finanzunternehmen ermittelt hat.

2. Für jede ermittelte kritische oder wichtige Funktion sind folgende Angaben zu machen:

   a) Wenn die kritische oder wichtige Funktion nicht in den Anwendungsbereich des TLPT fällt, Erläuterung der Gründe, aus denen sie nicht einbezogen wurde

   b) Wenn die kritische oder wichtige Funktion in den Anwendungsbereich des TLPT fällt:

      i) Angabe der Gründe für die Einbeziehung

      ii) Das (die) identifizierte(n) IKT-System(e) zur Unterstützung dieser kritischen oder wichtigen Funktion

      iii) für jedes ermittelte IKT-System:

         1. Angabe, ob es ausgelagert ist, und falls ja, Name des IKT-Drittdienstleisters

         2. Rechtsräume, in denen das IKT-System verwendet wird

         3. Übergeordnete Beschreibung der vorläufigen Flags, aus der hervorgeht, welcher Sicherheitsaspekt (Vertraulichkeit, Integrität, Authentizität oder Verfügbarkeit) von dem einzelnen Flag erfasst ist

ANHANG III

Inhalt des spezifischen Bedrohungsanalyseberichts (Artikel 10 Absatz 5)

Der spezifische Bedrohungsanalysebericht enthält Informationen zu allen folgenden Punkten:

1. Gesamtumfang der Bedrohungsuntersuchungen, die mindestens Folgendes einbeziehen:
   a) kritische oder wichtige Funktionen, die in den Anwendungsbereich fallen
   b) ihr geografischer Standort
   c) verwendete EU-Amtssprache
   d) relevante IKT-Drittdienstleister
   e) Zeitraum, in dem die Untersuchungen durchgeführt wurden
2. Gesamtbewertung, welche konkreten verwertbaren Informationen über das Finanzunternehmen zu finden sind, unter anderem:
   a) Benutzernamen und Passwörter der Mitarbeiter
   b) Look-Alike-Domains, die mit offiziellen Domains des Finanzunternehmens verwechselt werden können
   c) Technische Auskundschaftung: (für Exploits) anfällige Software, Systeme und Technologien
   d) von Mitarbeitern im Internet veröffentlichte Informationen über das Finanzunternehmen, die für die Zwecke eines Angriffs verwendet werden könnten
   e) Informationen, die im Dark Web verkauft werden
   f) sonstige einschlägige Informationen, die im Internet oder in öffentlichen Netzwerken verfügbar sind
   g) gegebenenfalls Informationen über Möglichkeiten des physischen Zugangs, z. B. zu den Räumlichkeiten des Finanzunternehmens
3. Bedrohungsanalysen unter Berücksichtigung der allgemeinen Bedrohungslage und der besonderen Situation des Finanzunternehmens, darunter mindestens:
   a) das geopolitische Umfeld
   b) das wirtschaftliche Umfeld
   c) technologische und sonstige Trends im Zusammenhang mit den Tätigkeiten im Finanzdienstleistungssektor
4. Bedrohungsprofile der böswilligen Akteure (bestimmte Einzelperson/Gruppe oder allgemeine Gruppe), die das Finanzunternehmen angreifen könnten, einschließlich der Systeme des Finanzunternehmens, die von böswilligen Akteuren am wahrscheinlichsten kompromittiert oder angegriffen werden, der möglichen Motivation, Absicht und Gründe für den möglichen zielgerichteten Angriff und der möglichen Vorgehensweise der Angreifer.
5. Bedrohungsszenarien: mindestens drei End-to-End-Bedrohungsszenarien für die gemäß Nummer 4 ermittelten Bedrohungsprofile, die die höchsten Werte für die Schwere der Bedrohung aufweisen. Die Bedrohungsszenarien beschreiben den End-to-End-Angriffspfad und umfassen mindestens:

(a) ein Szenario, das u. a. eine Kompromittierung der Dienstverfügbarkeit umfasst

(b) ein Szenario, das u. a. eine Kompromittierung der Datenintegrität umfasst

(c) ein Szenario, das u. a. die Kompromittierung der Vertraulichkeit von Informationen umfasst

6. Gegebenenfalls eine Beschreibung des in Artikel 10 Absatz 4 genannten nicht bedrohungsorientierten Szenarios

ANHANG IV
Inhalt des Red-Team-Testplans (Artikel 11 Absatz 1)

Der Red-Team-Testplan enthält Informationen zu allen folgenden Punkten:

a) Kommunikationskanäle und -verfahren

b) für den Angriff zulässige und nicht zulässige Taktiken, Techniken und Verfahren, einschließlich ethischer Grenzen für Social Engineering

c) von den Testern zu ergreifende Risikomanagementmaßnahmen

d) Beschreibung jedes Szenarios, einschließlich

   i) des simulierten Angreifers

   ii) seiner Absicht, Motivation und Ziele

   iii) der Funktionen und der unterstützenden IKT-Systeme, gegen die sich der Angriff richtet

   iv) der Aspekte der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität, auf die der Angriff ausgerichtet ist

   v) Flags

e) detaillierte Beschreibung jedes voraussichtlichen Angriffspfads, einschließlich der Voraussetzungen und etwaigen Hilfestellungen durch das Kontrollteam, mit Angabe der zeitlichen Vorgaben für deren Aktivierung und potenziellen Verwendung

f) Planung der Red-Teaming-Aktivitäten, einschließlich der Zeitplanung für die Durchführung jedes Szenarios, mindestens aufgeschlüsselt nach den drei Phasen, die ein Tester während der Testphase absolviert, d. h. Eindringen in die IKT-Systeme des Finanzunternehmens, Bewegung durch die IKT-Systeme und letztlich Erreichen des Angriffsziels und Rückzug aus den IKT-Systemen (In-, Through- und Out-Phase)

g) Besonderheiten der Infrastruktur der Finanzunternehmen, die bei den Tests zu berücksichtigen sind

h) gegebenenfalls zusätzliche Informationen oder sonstige Ressourcen, die die Tester für die Ausführung der Szenarien benötigen

ANHANG V
Inhalt des Red-Team-Testberichts (Artikel 12 Absatz 2)

Der Red-Team-Testbericht enthält mindestens Informationen zu allen folgenden Punkten:

a) Informationen über den durchgeführten Angriff, einschließlich Angaben zu

   i) den angegriffenen kritischen oder wichtigen Funktionen und ermittelten IKT-Systemen, -Prozessen und -Technologien, die die kritische oder wichtige Funktion unterstützen, wie im Red-Team-Testplan festgelegt

   ii) Zusammenfassung jedes Szenarios

   iii) erreichte und nicht erreichte Flags

   iv) erfolgreich und nicht erfolgreich verfolgte Angriffspfade

   v) erfolgreich und nicht erfolgreich angewandte Taktiken, Techniken und Verfahren

   vi) etwaige Abweichungen vom Red-Team-Testplan

   vii) etwaige Hilfestellungen

b) Alle Aktivitäten, von denen die Tester wissen, dass sie vom Blue Team durchgeführt wurden, um den Angriff zu rekonstruieren und seine Auswirkungen abzumildern

c) Festgestellte Schwachstellen und andere Probleme, einschließlich:

   i) Beschreibung der Schwachstelle und anderer Probleme, einschließlich ihrer Kritikalität

   ii) Ursachenanalyse erfolgreicher Angriffe

   iii) Empfehlungen für Abhilfemaßnahmen mit Priorisierung

ANHANG VI
Inhalt des Blue-Team-Testberichts (Artikel 12 Absatz 4)

Der Blue-Team-Testbericht enthält mindestens Informationen zu allen folgenden Punkten:

1. Für jeden von den Testern im Red-Team-Testbericht beschriebenen Angriffsschritt:
   a) Auflistung der entdeckten Angriffshandlungen
   b) Protokolleinträge für diese entdeckten Handlungen
2. Bewertung der Ergebnisse und Empfehlungen der Tester
3. Vom Blue Team gesammelte Beweise für den Angriff durch die Tester
4. Blue-Team-Ursachenanalyse erfolgreicher Angriffe durch die Tester
5. Auflistung der gewonnenen Erkenntnisse und ermittelten Verbesserungspotenziale
6. Auflistung der Themen, die beim Purple-Teaming behandelt werden sollen

ANLAGE VII

Inhalt des Berichts mit einer Zusammenfassung der maßgeblichen Ergebnisse des TLPT gemäß Artikel 26 Absatz 6 der Verordnung (EU) 2022/2554

Der zusammenfassende Testbericht muss mindestens Angaben zu allen folgenden Punkten enthalten:

a) beteiligte Parteien

b) Projektplan

c) validierter Umfang, einschließlich der Gründe für die Einbeziehung oder den Ausschluss kritischer oder wichtiger Funktionen und ermittelter IKT-Systeme, -Prozesse und -Technologien, die die vom TLPT erfassten kritischen oder wichtigen Funktionen unterstützen

d) gewählte Szenarien und etwaige erhebliche Abweichungen vom spezifischen Bedrohungsanalysebericht

e) verfolgte Angriffspfade und angewandte Taktiken, Techniken und Verfahren

f) erreichte und nicht erreichte Flags

g) etwaige Abweichungen vom Red-Team-Testplan

h) etwaige vom Blue Team aufgedeckte Handlungen

i) Purple-Teaming in der Testphase, sofern durchgeführt, und zugrunde liegende Voraussetzungen

j) etwaige Hilfestellungen

k) ergriffene Risikomanagementmaßnahmen

l) festgestellte Schwachstellen und andere Probleme, einschließlich ihrer Kritikalität

m) Ursachenanalyse erfolgreicher Angriffe

n) umfassender Plan mit Abhilfemaßnahmen, in dem Schwachstellen und andere festgestellte Probleme, ihre Ursachen und die Priorität der Behebung zueinander in Beziehung gesetzt werden

o) Erkenntnisgewinn aus den Rückmeldungen

ANHANG VIII
Inhalt der Bescheinigung über den TLPT gemäß Artikel 26 Absatz 7 der Verordnung (EU) 2022/2554

Die Bescheinigung enthält mindestens alle folgenden Angaben:

a) Zum durchgeführten TLPT:

   i) Beginn und Ende des TLPT

   ii) die kritischen oder wichtigen Funktionen, die Gegenstand des Tests waren

   iii) gegebenenfalls Informationen über kritische oder wichtige Funktionen, die Gegenstand des Tests waren und für die der TLPT nicht durchgeführt wurde

   iv) etwaige andere Finanzunternehmen, die an dem TLPT beteiligt waren

   v) etwaige IKT-Drittdienstleister, die an dem TLPT beteiligt waren

   vi) zu den Testern:

      1. Angabe, ob interne Tester eingesetzt wurden

      2. Angabe, ob das Finanzunternehmen von Artikel 5 Absatz 3 Unterabsatz 2 Gebrauch gemacht hat

   vii) Dauer der aktiven Red-Team-Testphase in Kalendertagen

b) Wenn mehrere TLPT-Behörden an dem TLPT beteiligt waren: Nennung der anderen TLPT-Behörden und Angabe, in welcher Eigenschaft sie daran beteiligt waren

c) Aufstellung der Dokumente, die von der TLPT-Behörde für die Ausstellung der Bescheinigung geprüft wurden