Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2025/1190

18.6.2025

ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2025/1190 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 13ης Φεβρουαρίου 2025

για τη συμπλήρωση του κανονισμού (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τα ρυθμιστικά τεχνικά πρότυπα για τον καθορισμό των κριτηρίων που χρησιμοποιούνται για τον προσδιορισμό των χρηματοοικονομικών οντοτήτων που υποχρεούνται να διενεργούν δοκιμές παρείσδυσης βάσει απειλών (TLPT), των απαιτήσεων και των προτύπων που διέπουν τη χρήση εσωτερικών δοκιμαστών, των απαιτήσεων σχετικά με το πεδίο εφαρμογής, τη μεθοδολογία των δοκιμών και την προσέγγιση για κάθε φάση των σταδίων δοκιμής, αποτελεσμάτων, ολοκλήρωσης και αποκατάστασης, καθώς και του είδους της εποπτικής και άλλης σχετικής συνεργασίας που απαιτούνται για την εφαρμογή TLPT και για τη διευκόλυνση της αμοιβαίας αναγνώρισης

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 ([1]), και ιδίως το άρθρο 26 παράγραφος 11 τέταρτο εδάφιο,

Εκτιμώντας τα ακόλουθα:

(1) Ο παρών κανονισμός καταρτίστηκε σύμφωνα με το πλαίσιο TIBER-EU και αντικατοπτρίζει τη μεθοδολογία, τη διαδικασία και τη δομή των δοκιμών παρείσδυσης βάσει απειλών (στο εξής: TLPT), όπως περιγράφονται στο TIBER-EU. Οι χρηματοοικονομικές οντότητες που υποβάλλονται σε TLPT μπορούν να αναφέρονται στο πλαίσιο TIBER-EU ή σε μία από τις εθνικές εφαρμογές του και να το/την εφαρμόζουν, στον βαθμό που το εν λόγω πλαίσιο ή η εν λόγω εφαρμογή συνάδει με τις απαιτήσεις που προβλέπονται στα άρθρα 26 και 27 του κανονισμού (ΕΕ) 2022/2554 και στον παρόντα κανονισμό. Ο ορισμός μιας ενιαίας δημόσιας αρχής στον χρηματοοικονομικό τομέα, η οποία θα είναι υπεύθυνη για θέματα σχετικά με τις TLPT σε εθνικό επίπεδο, σύμφωνα με το άρθρο 26 παράγραφος 9 του κανονισμού (ΕΕ) 2022/2554, δεν θα πρέπει να θίγει την αρμοδιότητα των αρμόδιων αρχών στις οποίες έχει ανατεθεί σε επίπεδο Ένωσης η εποπτεία ορισμένων χρηματοοικονομικών οντοτήτων σύμφωνα με το άρθρο 46 του εν λόγω κανονισμού, όπως, για παράδειγμα, της Ευρωπαϊκής Κεντρικής Τράπεζας για σημαντικά πιστωτικά ιδρύματα, οι οποίες πρέπει να θεωρούνται αρμόδιες για θέματα σχετικά με τις TLPT. Όταν μόνο ορισμένα από τα καθήκοντα που σχετίζονται με τις TLPT ανατίθενται σε άλλη εθνική αρχή του χρηματοοικονομικού τομέα σύμφωνα με το άρθρο 26 παράγραφος 10 του κανονισμού (ΕΕ) 2022/2554, η αρμόδια αρχή της χρηματοοικονομικής οντότητας που αναφέρεται στο άρθρο 46 του εν λόγω κανονισμού θα πρέπει να παραμένει αρμόδια για τα μη ανατεθέντα καθήκοντα σχετικά με τις TLPT.

(2) Λαμβανομένης υπόψη της πολυπλοκότητας των TLPT και των σχετικών κινδύνων, η χρήση τους θα πρέπει να περιορίζεται στις χρηματοοικονομικές οντότητες για τις οποίες δικαιολογείται. Ως εκ τούτου, οι αρχές που είναι αρμόδιες για θέματα TLPT (αρχές TLPT, είτε σε ενωσιακό είτε σε εθνικό επίπεδο) θα πρέπει να εξαιρούν από το πεδίο των TLPT τις χρηματοοικονομικές οντότητες οι οποίες δραστηριοποιούνται σε βασικούς υποτομείς χρηματοοικονομικών υπηρεσιών για τους οποίους δεν δικαιολογείται η χρήση TLPT. Αυτό σημαίνει ότι τα πιστωτικά ιδρύματα, τα ιδρύματα πληρωμών και τα ιδρύματα ηλεκτρονικού χρήματος, τα κεντρικά αποθετήρια τίτλων, οι κεντρικοί αντισυμβαλλόμενοι, οι τόποι διαπραγμάτευσης, οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις θα μπορούσαν να απαλλάσσονται από την απαίτηση διενέργειας TLPT, ακόμη και αν πληρούν τα ποσοτικά κριτήρια, υπό το πρίσμα της συνολικής αξιολόγησης του προφίλ κινδύνου και της ωριμότητας από πλευράς ΤΠΕ, των επιπτώσεων στον χρηματοοικονομικό τομέα και σχετικών προβληματισμών για τη χρηματοοικονομική σταθερότητα.

(3) Οι αρχές TLPT θα πρέπει να αξιολογούν, υπό το πρίσμα της συνολικής αξιολόγησης του προφίλ κινδύνου και της ωριμότητας από πλευράς ΤΠΕ, των επιπτώσεων στον χρηματοοικονομικό τομέα και σχετικών προβληματισμών για τη χρηματοοικονομική σταθερότητα, κατά πόσον θα πρέπει να υποβάλλονται σε TLPT τύποι χρηματοοικονομικών οντοτήτων πέραν των πιστωτικών ιδρυμάτων, των ιδρυμάτων πληρωμών, των ιδρυμάτων ηλεκτρονικού χρήματος, των κεντρικών αντισυμβαλλομένων, των κεντρικών αποθετηρίων τίτλων, των τόπων διαπραγμάτευσης, των ασφαλιστικών και αντασφαλιστικών επιχειρήσεων. Η αξιολόγηση του αν οι εν λόγω χρηματοοικονομικές οντότητες πληρούν τα συγκεκριμένα ποιοτικά κριτήρια θα πρέπει να έχει ως στόχο τον προσδιορισμό των χρηματοοικονομικών οντοτήτων για τις οποίες είναι σκόπιμη η διενέργεια TLPT, με τη χρήση διατομεακών και αντικειμενικών δεικτών. Ταυτόχρονα, με βάση την αξιολόγηση

([1]) ΕΕ L 333 της 27.12.2022, σ. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

του αν μια χρηματοοικονομική οντότητα πληροί τα συγκεκριμένα ποιοτικά κριτήρια, οι οντότητες που υποβάλλονται σε TLPT θα πρέπει να περιορίζονται σε εκείνες για τις οποίες δικαιολογούνται οι δοκιμές. Το αν μια χρηματοοικονομική οντότητα πληροί τα συγκεκριμένα ποιοτικά κριτήρια θα πρέπει επίσης να αξιολογείται υπό το πρίσμα της ανάπτυξης νέων αγορών και της αυξανόμενης σημασίας των συμμετεχόντων στις νέες αγορές για τον χρηματοοικονομικό τομέα στο μέλλον, συμπεριλαμβανομένων των παρόχων υπηρεσιών κρυπτοστοιχείων που έχουν λάβει άδεια λειτουργίας σύμφωνα με το άρθρο 59 του κανονισμού (ΕΕ) 2023/1114 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2]).

(4) Οι χρηματοοικονομικές οντότητες ενδέχεται να έχουν τον ίδιο ενδοομιλικό πάροχο υπηρεσιών ΤΠΕ ή να ανήκουν στον ίδιο όμιλο και να βασίζονται στη χρήση κοινών συστημάτων ΤΠΕ. Στην περίπτωση αυτή, είναι σημαντικό οι αρχές TLPT να λαμβάνουν υπόψη τη δομή και τον συστημικό χαρακτήρα ή τη σημασία της εν λόγω χρηματοοικονομικής οντότητας για τον χρηματοοικονομικό τομέα σε εθνικό ή ενωσιακό επίπεδο όταν αξιολογούν αν μια χρηματοοικονομική οντότητα θα πρέπει να υποβάλλεται σε TLPT και αν οι TLPT θα πρέπει να διενεργούνται σε επίπεδο οντότητας ή σε επίπεδο ομίλου (μέσω κοινής TLPT).

(5) Προκειμένου να αντικατοπτρίζεται το πλαίσιο TIBER-EU, η μεθοδολογία των δοκιμών θα πρέπει να προβλέπει τη συμμετοχή των ακόλουθων βασικών συμμετεχόντων: της χρηματοοικονομικής οντότητας, με ομάδα ελέγχου (που αντικατοπτρίζει την «ομάδα ελέγχου» του πλαισίου TIBER-EU) και μπλε ομάδα (που αντικατοπτρίζει την «μπλε ομάδα» του πλαισίου TIBER-EU), και της αρχής TLPT, με τη μορφή κυβερνοομάδας TLPT (που αντικατοπτρίζει τις «κυβερνοομάδες TIBER» του πλαισίου TIBER-EU), ενός παρόχου πληροφοριών για απειλές και δοκιμαστών (όπου οι δοκιμαστές αντικατοπτρίζουν τον «πάροχο κόκκινης ομάδας» του πλαισίου TIBER-EU).

(6) Προκειμένου να διασφαλιστεί ότι οι TLPT αξιοποιούν την πείρα που αναπτύχθηκε στο πλαίσιο της εφαρμογής του TIBER-EU και να μειωθούν οι κίνδυνοι που συνδέονται με τη διενέργεια TLPT, θα πρέπει να διασφαλιστεί ότι οι αρμοδιότητες των κυβερνοομάδων TLPT που θα συσταθούν σε επίπεδο αρχών TLPT αντιστοιχούν όσο το δυνατόν περισσότερο στις αρμοδιότητες των κυβερνοομάδων του πλαισίου TIBER-EU. Ως εκ τούτου, οι κυβερνοομάδες TLPT θα πρέπει να διαθέτουν διαχειριστές δοκιμών οι οποίοι θα είναι υπεύθυνοι για την εποπτεία των επιμέρους TLPT και για τον σχεδιασμό και τον συντονισμό των επιμέρους δοκιμών. Οι κυβερνοομάδες TLPT θα πρέπει να λειτουργούν ως ενιαίο σημείο επαφής για την επικοινωνία σχετικά με τις δοκιμές με εσωτερικούς και εξωτερικούς συμφεροντούχους, για τη συλλογή και την επεξεργασία παρατηρήσεων και διδαγμάτων που αντλήθηκαν από παλαιότερες δοκιμές, καθώς και για τη στήριξη των χρηματοοικονομικών οντοτήτων που υποβάλλονται σε δοκιμές TLPT.

(7) Προκειμένου να αντικατοπτρίζεται η μεθοδολογία του πλαισίου TIBER-EU, οι διαχειριστές των δοκιμών θα πρέπει να διαθέτουν τις απαραίτητες δεξιότητες και ικανότητες για να παρέχουν συμβουλές και να αμφισβητούν τις προτάσεις των δοκιμαστών. Η πείρα από το πλαίσιο TIBER-EU έχει αποδείξει ότι είναι χρήσιμο για κάθε δοκιμή να ορίζεται μια ομάδα τουλάχιστον δύο διαχειριστών δοκιμής. Προκειμένου να αποτυπωθεί το γεγονός ότι η TLPT χρησιμοποιείται για την προώθηση της διδακτικής εμπειρίας και να διασφαλιστεί η εμπιστευτικότητα των δοκιμών, και εκτός εάν αντιμετωπίζουν ζητήματα πόρων ή εμπειρογνωσίας, οι αρχές TLPT ενθαρρύνονται ιδιαίτερα να ελέγχουν ότι, για όσο διάστημα διαρκεί η TLPT, οι διαχειριστές της δοκιμής δεν θα πρέπει να ασκούν εποπτικές δραστηριότητες στην ίδια χρηματοοικονομική οντότητα που υποβάλλεται σε TLPT.

(8) Είναι σημαντικό, για λόγους συνέπειας με το πλαίσιο TIBER-EU, η αρχή TLPT να παρακολουθεί στενά τις δοκιμές σε κάθε στάδιό τους. Λαμβάνοντας υπόψη τη φύση των δοκιμών και τους κινδύνους που συνδέονται με αυτές, η συμμετοχή της αρχής TLPT σε κάθε ξεχωριστό στάδιο των δοκιμών έχει θεμελιώδη σημασία. Ειδικότερα, θα πρέπει να ζητείται η γνώμη της αρχής TLPT, η οποία θα πρέπει να επικυρώνει τις αξιολογήσεις ή τις αποφάσεις των χρηματοοικονομικών οντοτήτων που ενδέχεται, αφενός, να επηρεάσουν την αποτελεσματικότητα της δοκιμής και, αφετέρου, να έχουν αντίκτυπο στους κινδύνους που συνδέονται με τη δοκιμή. Τα βασικά βήματα στα οποία απαιτείται ειδική συμμετοχή της αρχής TLPT περιλαμβάνουν την επικύρωση ορισμένων βασικών εγγράφων τεκμηρίωσης των δοκιμών, καθώς και την επιλογή παρόχων πληροφοριών για απειλές, δοκιμαστών και μέτρων διαχείρισης κινδύνων. Η συμμετοχή των αρχών TLPT, και ειδικότερα όσον αφορά τις επικυρώσεις, δεν θα πρέπει να συνεπάγεται υπερβολική επιβάρυνση των εν λόγω αρχών και, ως εκ τούτου, θα πρέπει να περιορίζεται στα έγγραφα τεκμηρίωσης και στις αποφάσεις που επηρεάζουν άμεσα τη διενέργεια της TLPT. Μέσω της ενεργού συμμετοχής τους σε κάθε στάδιο των δοκιμών, οι αρχές TLPT μπορούν να αξιολογούν αποτελεσματικά τη συμμόρφωση των χρηματοοικονομικών οντοτήτων με τις σχετικές απαιτήσεις, πράγμα που αναμένεται να επιτρέπει στις εν λόγω αρχές να εκδίδουν βεβαιώσεις σύμφωνα με το άρθρο 26 παράγραφος 7 του κανονισμού (ΕΕ) 2022/2554.

([2]) Κανονισμός (ΕΕ) 2023/1114 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 31ης Μαΐου 2023, για τις αγορές κρυπτοστοιχείων και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1093/2010 και (ΕΕ) αριθ. 1095/2010 και των οδηγιών 2013/36/ΕΕ και (ΕΕ) 2019/1937 (ΕΕ L 150 της 9.6.2023, σ. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) Το απόρρητο των TLPT είναι υψίστης σημασίας προκειμένου να διασφαλίζεται ότι οι συνθήκες των δοκιμών είναι ρεαλιστικές. Για τον λόγο αυτό, οι δοκιμές θα πρέπει να είναι συγκεκαλυμμένες και θα πρέπει να λαμβάνονται προφυλάξεις για τη διατήρηση της εμπιστευτικότητας των TLPT, συμπεριλαμβανομένης της επιλογής κωδικών ονομασιών οι οποίες θα πρέπει να σχεδιάζονται κατά τρόπο ώστε να μην είναι δυνατή η ταυτοποίηση της TLPT από τρίτους. Εάν τα μέλη του προσωπικού που είναι υπεύθυνα για την ασφάλεια της χρηματοοικονομικής ομάδας γνωρίζουν για μια προγραμματισμένη ή υπό εξέλιξη TLPT, είναι πιθανό να είναι πιο προσεκτικά και σε μεγαλύτερη εγρήγορση απ' ό,τι κατά τη διάρκεια της συνήθους εργασίας τους, με αποτέλεσμα να αλλοιώνεται το αποτέλεσμα των δοκιμών. Ως εκ τούτου, τα μέλη του προσωπικού της χρηματοοικονομικής οντότητας εκτός της ομάδας ελέγχου θα πρέπει να ενημερώνονται για τυχόν προγραμματισμένες ή υπό εξέλιξη TLPT μόνο όταν συντρέχουν σοβαροί λόγοι και με την επιφύλαξη της προηγούμενης συμφωνίας των διαχειριστών των δοκιμών, μεταξύ άλλων για τη διασφάλιση του απορρήτου της δοκιμής σε περίπτωση που κάποιο μέλος της μπλε ομάδας εντοπίσει τη δοκιμή.

(10) Όπως αποδεικνύεται από την πείρα που αποκτήθηκε στο πλαίσιο TIBER-EU όσον αφορά την «ομάδα ελέγχου», η επιλογή κατάλληλου επικεφαλής της ομάδας ελέγχου είναι απαραίτητη για την ασφαλή διενέργεια των TLPT. Ο επικεφαλής της ομάδας ελέγχου θα πρέπει να έχει την αναγκαία εντολή εντός της χρηματοοικονομικής οντότητας ώστε να καθοδηγεί όλες τις πτυχές των δοκιμών, χωρίς να διακυβεύεται η εμπιστευτικότητά τους. Για τον ίδιο λόγο, τα μέλη της ομάδας ελέγχου θα πρέπει να έχουν βαθιά γνώση της χρηματοοικονομικής οντότητας, του ρόλου και της στρατηγικής θέσης του επικεφαλής της ομάδας ελέγχου, θα πρέπει να διαθέτουν την απαιτούμενη προϋπηρεσία και να έχουν πρόσβαση στο διοικητικό συμβούλιο. Για να μειωθεί ο κίνδυνος υπονόμευσης της TLPT, η ομάδα ελέγχου θα πρέπει να έχει όσο το δυνατόν λιγότερα μέλη.

(11) Υπάρχουν εγγενή στοιχεία των κινδύνων που σχετίζονται με τη διενέργεια TLPT, καθώς οι κρίσιμες λειτουργίες δοκιμάζονται σε περιβάλλον παραγωγής, με πιθανότητα πρόκλησης συμβάντων άρνησης υπηρεσίας, απροσδόκητων βλαβών του συστήματος, ζημιών σε κρίσιμα συστήματα παραγωγής ή απώλειας, τροποποίησης ή δημοσιοποίησης δεδομένων. Οι κίνδυνοι αυτοί αναδεικνύουν την ανάγκη λήψης ισχυρών μέτρων διαχείρισης κινδύνων. Προκειμένου να διασφαλιστεί ότι η TLPT διεξάγεται με ελεγχόμενο τρόπο καθ' όλη τη διάρκεια των δοκιμών, είναι πολύ σημαντικό οι χρηματοοικονομικές οντότητες να γνωρίζουν σε κάθε σημείο τους ιδιαίτερους κινδύνους που προκύπτουν σε μια TLPT και να μετριάζονται οι κίνδυνοι αυτοί. Στο πλαίσιο αυτό, με την επιφύλαξη των εσωτερικών διαδικασιών της χρηματοοικονομικής οντότητας και της ευθύνης και των εξουσιοδοτήσεων που έχουν ήδη παρασχεθεί στον επικεφαλής της ομάδας ελέγχου, μπορεί να είναι σκόπιμη η παροχή πληροφοριών σχετικά με τα μέτρα διαχείρισης κινδύνου TLPT ή, σε ειδικές περιπτώσεις, η έγκριση των εν λόγω μέτρων διαχείρισης κινδύνου από το ίδιο το διοικητικό όργανο της χρηματοοικονομικής οντότητας. Για να είναι σε θέση να παρέχουν αποτελεσματικές και τις πλέον εξειδικευμένες επαγγελματικές υπηρεσίες και να περιορίζουν τους εν λόγω κινδύνους, οι δοκιμαστές και οι πάροχοι πληροφοριών για απειλές (από κοινού: πάροχοι TLPT) είναι επίσης σημαντικό να διαθέτουν το υψηλότερο επίπεδο δεξιοτήτων, εμπειρογνωσίας και κατάλληλη πείρα στον τομέα των πληροφοριών για απειλές και των TLPT στον κλάδο των χρηματοοικονομικών υπηρεσιών.

(12) Οι συμβατικές δοκιμές παρείσδυσης παρέχουν συχνά λεπτομερή και χρήσιμη αξιολόγηση των τεχνικών ευπαθειών και των ευπαθειών παραμετροποίησης ενός μόνο συστήματος ή περιβάλλοντος μεμονωμένα, αλλά, σε αντίθεση με τη δοκιμή κόκκινης ομάδας βάσει στοιχείων, δεν αξιολογούν ολόκληρο το σενάριο μιας στοχευμένης επίθεσης κατά της οντότητας στο σύνολό της, συμπεριλαμβανομένων όλων των ανθρώπων, των διαδικασιών και των τεχνολογιών της συνολικά. Ως εκ τούτου, κατά τη διαδικασία επιλογής των παρόχων TLPT, οι χρηματοοικονομικές οντότητες θα πρέπει να βεβαιώνονται ότι οι εν λόγω πάροχοι διαθέτουν τις απαιτούμενες δεξιότητες να διενεργούν δοκιμές κόκκινης ομάδας βάσει στοιχείων και όχι μόνο δοκιμές παρείσδυσης. Επομένως, είναι αναγκαίο να θεσπιστούν αναλυτικά κριτήρια για τους δοκιμαστές, εσωτερικούς και εξωτερικούς, και για τους παρόχους πληροφοριών για απειλές, οι οποίοι είναι πάντα εξωτερικοί. Όταν οι πάροχοι TLPT ανήκουν στην ίδια εταιρεία, το προσωπικό που αναλαμβάνει μια TLPT θα πρέπει να διαχωρίζεται επαρκώς.

(13) Ενδέχεται να συντρέχουν εξαιρετικές περιστάσεις κατά τις οποίες οι χρηματοοικονομικές οντότητες δεν είναι σε θέση να συνάπτουν συμβάσεις με παρόχους TLPT που πληρούν τα αναλυτικά κριτήρια. Ως εκ τούτου, οι χρηματοοικονομικές οντότητες, αφού αποδείξουν τη μη διαθεσιμότητα τέτοιου είδους παρόχων πληροφοριών για απειλές, θα πρέπει να έχουν τη δυνατότητα να εμπλέκουν πρόσωπα που δεν πληρούν όλα τα αναλυτικά κριτήρια, υπό την προϋπόθεση ότι μετριάζουν δεόντως τυχόν πρόσθετους κινδύνους που προκύπτουν και ότι η αρχή TLPT αξιολογεί όλα αυτά τα κριτήρια.

(14) Όταν σε μια TLPT συμμετέχουν περισσότερες από μία χρηματοοικονομικές οντότητες και αρχές TLPT, θα πρέπει να προσδιορίζονται οι ρόλοι όλων των μερών στη διαδικασία TLPT για τη διενέργεια της πλέον αποδοτικής και ασφαλούς δοκιμής. Για τους σκοπούς των ομαδικών δοκιμών, είναι αναγκαία η θέσπιση ειδικών απαιτήσεων προκειμένου να προσδιορίζεται ο ρόλος της ορισθείσας χρηματοοικονομικής οντότητας, δηλαδή ότι θα πρέπει να είναι υπεύθυνη για την παροχή όλων των αναγκαίων εγγράφων τεκμηρίωσης στην επικεφαλής αρχή TLPT και για την παρακολούθηση της διαδικασίας των δοκιμών. Η ορισθείσα χρηματοοικονομική οντότητα θα πρέπει επίσης να είναι υπεύθυνη για τις κοινές πτυχές της αξιολόγησης της διαχείρισης κινδύνων. Παρά τον ρόλο της ορισθείσας χρηματοοικονομικής οντότητας, οι υποχρεώσεις κάθε χρηματοοικονομικής οντότητας που συμμετέχει στη διαδικασία ομαδικών TLPT δεν θα πρέπει να επηρεάζονται κατά τη διάρκεια της ομαδικής δοκιμής. Η ίδια αρχή θα πρέπει να ισχύει και για τις κοινές TLPT.

(15) Όπως αποδεικνύεται από την πείρα που έχει αποκομιστεί από την εφαρμογή του πλαισίου TIBER-EU, η διεξαγωγή διά ζώσης ή εικονικών συνεδριάσεων με τη συμμετοχή όλων των συμφεροντούχων (χρηματοοικονομικές οντότητες, αρχές, δοκιμαστές και πάροχοι πληροφοριών για απειλές) είναι ο αποτελεσματικότερος τρόπος να διασφαλιστεί η κατάλληλη διενέργεια των δοκιμών. Ως εκ τούτου, θα πρέπει να πραγματοποιούνται διά ζώσης και εικονικές συνεδριάσεις σε διάφορα στάδια της διαδικασίας, και ειδικότερα κατά το προπαρασκευαστικό στάδιο και κατά την έναρξη της TLPT για την οριστικοποίηση του πεδίου της, κατά το στάδιο των δοκιμών για την οριστικοποίηση της έκθεσης πληροφοριών για απειλές και του σχεδίου δοκιμής κόκκινης ομάδας και για τις εβδομαδιαίες ενημερώσεις, καθώς και κατά το στάδιο της ολοκλήρωσης για την αναπαραγωγή των δράσεων των δοκιμαστών και της μπλε ομάδας, τις δράσεις μωβ ομάδας και την ανταλλαγή παρατηρήσεων σχετικά με την TLPT.

(16) Προκειμένου να διασφαλιστεί η ομαλή διεξαγωγή των TLPT, η αρχή TLPT θα πρέπει να παρουσιάζει σαφώς στη χρηματοοικονομική οντότητα τις προσδοκίες της όσον αφορά τις δοκιμές. Στο πλαίσιο αυτό, οι διαχειριστές των δοκιμών θα πρέπει να διασφαλίζουν την κατάλληλη ροή πληροφοριών με την ομάδα ελέγχου εντός της χρηματοοικονομικής οντότητας και με τους παρόχους TLPT.

(17) Η χρηματοοικονομική οντότητα θα πρέπει να επιλέγει τις κρίσιμες ή σημαντικές λειτουργίες που θα εμπίπτουν στο πεδίο της TLPT. Κατά την επιλογή των εν λόγω λειτουργιών, η χρηματοοικονομική οντότητα θα πρέπει να βασίζεται σε διάφορα κριτήρια που αφορούν τη σημασία κάθε λειτουργίας για την ίδια τη χρηματοοικονομική οντότητα και για τον χρηματοοικονομικό τομέα, σε ενωσιακό και εθνικό επίπεδο, όχι μόνο από οικονομική άποψη, αλλά λαμβάνοντας επίσης υπόψη τον συμβολικό ή πολιτικό χαρακτήρα της λειτουργίας. Προκειμένου να διευκολυνθεί η ομαλή μετάβαση στο στάδιο της συλλογής πληροφοριών για απειλές, η ομάδα ελέγχου θα πρέπει να παρέχει στους δοκιμαστές και στον πάροχο πληροφοριών για απειλές που δεν συμμετέχουν στη διαδικασία οριοθέτησης του πεδίου λεπτομερείς πληροφορίες σχετικά με τη συμφωνηθείσα οριοθέτηση του πεδίου.

(18) Για να παράσχει στους δοκιμαστές τις πληροφορίες που απαιτούνται για την προσομοίωση μιας πραγματικής και ρεαλιστικής επίθεσης στα εν χρήση συστήματα της χρηματοοικονομικής οντότητας που στηρίζουν τις κρίσιμες ή σημαντικές λειτουργίες της, ο πάροχος πληροφοριών για απειλές θα πρέπει να συλλέγει στοιχεία ή πληροφορίες που καλύπτουν τουλάχιστον δύο βασικούς τομείς ενδιαφέροντος: τους στόχους, προσδιορίζοντας πιθανές επιφάνειες εκτεθειμένες σε επιθέσεις σε ολόκληρη τη χρηματοοικονομική οντότητα, και τις απειλές, προσδιορίζοντας σχετικούς παράγοντες απειλής και πιθανά σενάρια απειλής. Προκειμένου να διασφαλίζεται ότι ο πάροχος πληροφοριών για απειλές λαμβάνει υπόψη τις σχετικές απειλές για τη χρηματοοικονομική οντότητα, οι δοκιμαστές, η ομάδα ελέγχου και οι διαχειριστές δοκιμής θα πρέπει να παρέχουν τις παρατηρήσεις τους για το σχέδιο έκθεσης πληροφοριών για απειλές. Ο πάροχος πληροφοριών για απειλές μπορεί να χρησιμοποιήσει ένα γενικό τοπίο απειλών, αν υπάρχει, που παρέχεται από την αρχή TLPT για τον χρηματοοικονομικό τομέα ενός κράτους μέλους ως βάση αναφοράς για το εθνικό τοπίο απειλών. Με βάση την εφαρμογή του πλαισίου TIBER-EU, η διαδικασία συλλογής πληροφοριών για απειλές διαρκεί συνήθως περίπου 4 εβδομάδες.

(19) Για να μπορούν οι δοκιμαστές να αποκτήσουν γνώσεις και να ελέγξουν περαιτέρω το έγγραφο προσδιορισμού του πεδίου και τη στοχευμένη έκθεση πληροφοριών για απειλές προκειμένου να οριστικοποιήσουν το σχέδιο δοκιμών κόκκινης ομάδας, είναι σημαντικό, πριν από το στάδιο δοκιμών κόκκινης ομάδας της TLPT, οι δοκιμαστές να λαμβάνουν από τον πάροχο πληροφοριών για απειλές αναλυτικές εξηγήσεις σχετικά με τη στοχευμένη έκθεση πληροφοριών για απειλές και την ανάλυση πιθανών σεναρίων απειλής.

(20) Για να μπορούν οι δοκιμαστές να διενεργούν ρεαλιστικές και ολοκληρωμένες δοκιμές στις οποίες εκτελούνται όλες οι φάσεις επιθέσεων και επιτυγχάνονται οι ενδείκτες, θα πρέπει να αφιερώνεται επαρκής χρόνος στο ενεργό στάδιο δοκιμών κόκκινης ομάδας. Με βάση την πείρα που αποκτήθηκε από το πλαίσιο TIBER-EU, ο χρόνος που διατίθεται θα πρέπει να είναι τουλάχιστον 12 εβδομάδες και θα πρέπει να καθορίζεται λαμβάνοντας υπόψη τον αριθμό των εμπλεκόμενων μερών, το πεδίο της TLPT, τους πόρους της εμπλεκόμενης χρηματοοικονομικής οντότητας ή οντοτήτων, τυχόν εξωτερικές απαιτήσεις και τη διαθεσιμότητα των υποστηρικτικών πληροφοριών που παρέχει η χρηματοοικονομική οντότητα.

(21) Κατά τη διάρκεια του ενεργού σταδίου δοκιμών κόκκινης ομάδας, οι δοκιμαστές θα πρέπει να αναπτύξουν μια σειρά τακτικών, τεχνικών και διαδικασιών για να δοκιμάσουν επαρκώς τα συστήματα παραγωγής της χρηματοοικονομικής οντότητας. Οι τακτικές, τεχνικές και διαδικασίες θα πρέπει να περιλαμβάνουν, κατά περίπτωση, την αναγνώριση (δηλαδή συλλογή όσο το δυνατόν περισσότερων πληροφοριών σχετικά με έναν στόχο), τη χρήση τους ως όπλου (δηλαδή ανάλυση πληροφοριών σχετικά με την υποδομή, τις εγκαταστάσεις και τους εργαζομένους και προετοιμασία των επιχειρήσεων που αφορούν ειδικά τον στόχο), την εκτέλεση (δηλαδή την ενεργό έναρξη της πλήρους επιχείρησης κατά του στόχου), την εκμετάλλευση (δηλαδή όπου στόχος των δοκιμαστών είναι να παραβιάσουν τους διακομιστές, τα δίκτυα της χρηματοοικονομικής οντότητας και να εκμεταλλευτούν το προσωπικό της μέσω κοινωνικής μηχανικής), τον έλεγχο και την κυκλοφορία (δηλαδή απόπειρες μετάβασης από τα παραβιασμένα συστήματα σε ακόμη πιο ευάλωτα ή υψηλής αξίας), και δράσεις κατά του στόχου (δηλαδή απόκτηση περαιτέρω πρόσβασης σε παραβιασμένα συστήματα και απόκτηση πρόσβασης στις προσυμφωνηθείσες πληροφορίες και τα δεδομένα στόχου, όπως συμφωνήθηκαν προηγουμένως στο σχέδιο δοκιμής κόκκινης ομάδας).

(22) Κατά τη διενέργεια μιας TLPT, οι δοκιμαστές θα πρέπει να ενεργούν λαμβάνοντας υπόψη τον διαθέσιμο χρόνο για την πραγματοποίηση της επίθεσης, τους πόρους και τα δεοντολογικά και νομικά όρια. Σε περίπτωση που οι δοκιμαστές δεν είναι σε θέση να προχωρήσουν στο προγραμματισμένο επόμενο στάδιο της επίθεσης, θα πρέπει να παρέχεται περιστασιακή βοήθεια από την ομάδα ελέγχου, με τη σύμφωνη γνώμη της αρχής TLPT, με τη μορφή «πλεονεκτημάτων». Τα πλεονεκτήματα μπορούν να κατηγοριοποιηθούν γενικά σε πληροφοριακά πλεονεκτήματα και πλεονεκτήματα πρόσβασης και ενδέχεται να συνίστανται στην παροχή πρόσβασης σε συστήματα ΤΠΕ ή εσωτερικά δίκτυα για τη συνέχιση της δοκιμής και την εστίαση στα επόμενα στάδια της επίθεσης.

(23) Κατά τη διάρκεια του ενεργού σταδίου δοκιμών κόκκινης ομάδας, εφόσον απαιτείται προκειμένου να καταστεί δυνατή η συνέχιση της TLPT ως έσχατη λύση σε εξαιρετικές περιστάσεις και αφού εξαντληθούν όλες οι εναλλακτικές επιλογές, θα πρέπει να χρησιμοποιείται συνεργατική δραστηριότητα δοκιμών στην οποία θα συμμετέχουν τόσο οι δοκιμαστές όσο και η μπλε ομάδα. Στο πλαίσιο της εν λόγω περιορισμένης άσκησης δράσεων μωβ ομάδας, μπορούν να χρησιμοποιηθούν οι ακόλουθες μέθοδοι: «σύλληψη και ελευθέρωση», όπου οι δοκιμαστές επιχειρούν να συνεχίσουν τα σενάρια, να εντοπιστούν και στη συνέχεια να επαναλάβουν τις δοκιμές, «πολεμικά παιχνίδια», τα οποία επιτρέπουν πιο σύνθετα σενάρια για τη δοκιμή της λήψης στρατηγικών αποφάσεων, ή «συνεργατική εξακρίβωση της δυνατότητας υλοποίησης» που επιτρέπει στους δοκιμαστές και στα μέλη της μπλε ομάδας να επικυρώνουν από κοινού συγκεκριμένα μέτρα, εργαλεία ή τεχνικές ασφάλειας σε ελεγχόμενο και συνεργατικό περιβάλλον.

(24) Η TLPT θα πρέπει να χρησιμοποιείται ως διδακτική εμπειρία για την ενίσχυση της ψηφιακής επιχειρησιακής ανθεκτικότητας των χρηματοοικονομικών οντοτήτων. Στο πλαίσιο αυτό, η μπλε ομάδα και οι δοκιμαστές θα πρέπει να αναπαράγουν την επίθεση και να επανεξετάζουν τις ενέργειες που ανέλαβαν για την άντληση διδαγμάτων από τις δοκιμές σε συνεργασία με τους δοκιμαστές. Για τον σκοπό αυτό και για να καταστεί δυνατή η κατάλληλη προετοιμασία, η έκθεση δοκιμής της κόκκινης ομάδας και η έκθεση δοκιμής της μπλε ομάδας θα πρέπει να διατίθενται σε όλα τα μέρη που συμμετέχουν στις δραστηριότητες αναπαραγωγής, πριν από τη διεξαγωγή τυχόν δραστηριοτήτων αναπαραγωγής. Επιπλέον, κατά το στάδιο ολοκλήρωσης θα πρέπει να πραγματοποιείται μια άσκηση δράσεων μωβ ομάδας για τη μεγιστοποίηση της διδακτικής εμπειρίας. Οι μέθοδοι που μπορούν να χρησιμοποιηθούν για την άσκηση δράσεων μωβ ομάδας κατά το στάδιο ολοκλήρωσης θα πρέπει να περιλαμβάνουν συζητήσεις για εναλλακτικά σενάρια επιθέσεων, τη διερεύνηση εναλλακτικών σεναρίων σε εν χρήση συστήματα ή την εκ νέου διερεύνηση των προγραμματισμένων σεναρίων σε εν χρήση συστήματα τα οποία οι δοκιμαστές δεν ήταν σε θέση να ολοκληρώσουν ή να εκτελέσουν κατά το στάδιο των δοκιμών.

(25) Για την περαιτέρω διευκόλυνση της διδακτικής εμπειρίας όλων των μερών που συμμετέχουν στις TLPT, προς όφελος μελλοντικών δοκιμών, και για την προώθηση της ψηφιακής επιχειρησιακής ανθεκτικότητας των χρηματοοικονομικών οντοτήτων, τα ενδιαφερόμενα μέρη θα πρέπει να παρέχουν αμοιβαία παρατηρήσεις σχετικά με τη συνολική διαδικασία, και ειδικότερα να προσδιορίζουν ποιες δραστηριότητες εξελίχθηκαν ικανοποιητικά ή θα μπορούσαν να βελτιωθούν, καθώς και ποιες πτυχές της διαδικασίας TLPT λειτούργησαν ικανοποιητικά ή θα μπορούσαν να βελτιωθούν.

(26) Οι αρμόδιες αρχές που αναφέρονται στο άρθρο 46 του κανονισμού (ΕΕ) 2022/2554 και οι αρχές TLPT, όταν είναι διαφορετικές, θα πρέπει να συνεργάζονται για την ενσωμάτωση προηγμένων δοκιμών μέσω TLPT στις υφιστάμενες εποπτικές διαδικασίες. Στο πλαίσιο αυτό και προκειμένου να επιτευχθεί η κοινή ορθή κατανόηση των πορισμάτων της TLPT και του τρόπου ερμηνείας τους, είναι σκόπιμο να καθιερωθεί στενή συνεργασία μεταξύ των διαχειριστών της δοκιμής που συμμετείχαν στην TLPT και των αρμόδιων εποπτικών αρχών, ιδίως όσον αφορά τη συνοπτική έκθεση της δοκιμής και τα σχέδια αποκατάστασης.

(27) Το άρθρο 26 παράγραφος 8 πρώτο εδάφιο του κανονισμού (ΕΕ) 2022/2554 απαιτεί από τις χρηματοοικονομικές οντότητες να συνάπτουν σύμβαση με εξωτερικούς δοκιμαστές ανά τρεις δοκιμές. Όταν οι χρηματοοικονομικές οντότητες περιλαμβάνουν στην ομάδα των δοκιμαστών εσωτερικούς και εξωτερικούς δοκιμαστές, θα πρέπει να θεωρείται ότι η TLPT διενεργήθηκε με εσωτερικούς δοκιμαστές για τους σκοπούς του εν λόγω άρθρου.

(28) Ο παρών κανονισμός βασίζεται στα σχέδια ρυθμιστικών τεχνικών προτύπων που υπέβαλαν στην Επιτροπή η Ευρωπαϊκή Αρχή Τραπεζών, η Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων και η Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών (Ευρωπαϊκές Εποπτικές Αρχές), σε συμφωνία με την Ευρωπαϊκή Κεντρική Τράπεζα.

(29) Οι Ευρωπαϊκές Εποπτικές Αρχές διενήργησαν ανοικτές δημόσιες διαβουλεύσεις σχετικά με τα σχέδια ρυθμιστικών τεχνικών προτύπων στα οποία βασίζεται ο παρών κανονισμός, ανέλυσαν τα ενδεχόμενα συναφή κόστη και τις ωφέλειες και ζήτησαν τις συμβουλές της ομάδας τραπεζικών συμφεροντούχων η οποία έχει συσταθεί σύμφωνα με το άρθρο 37 του κανονισμού (ΕΕ) αριθ. 1093/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3]), της ομάδας συμφεροντούχων ασφαλίσεων και αντασφαλίσεων και της ομάδας συμφεροντούχων ταμείων επαγγελματικών συνταξιοδοτικών παροχών, οι οποίες έχουν συσταθεί σύμφωνα με το άρθρο 37 του κανονισμού (ΕΕ) αριθ. 1094/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]), και της ομάδας συμφεροντούχων κινητών αξιών και αγορών η οποία έχει συσταθεί σύμφωνα με το άρθρο 37 του κανονισμού (ΕΕ) αριθ. 1095/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([5]).

(30) Σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]), ζητήθηκε η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος γνωμοδότησε στις 20 Αυγούστου 2024,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

Ορισμοί

Για τους σκοπούς του παρόντος κανονισμού, ισχύουν οι ακόλουθοι ορισμοί:

1) «ομάδα ελέγχου»: η ομάδα που απαρτίζεται από το προσωπικό της ελεγχόμενης χρηματοοικονομικής οντότητας και, κατά περίπτωση, λαμβανομένου υπόψη του πεδίου της TLPT, το προσωπικό των τρίτων παρόχων υπηρεσιών της και κάθε άλλου μέρους, το οποίο διαχειρίζεται τη δοκιμή·

2) «επικεφαλής της ομάδας ελέγχου»: το μέλος του προσωπικού της χρηματοοικονομικής οντότητας που είναι υπεύθυνο για τη διεξαγωγή όλων των δραστηριοτήτων σε σχέση με την TLPT για τη χρηματοοικονομική οντότητα στο πλαίσιο μια δεδομένης δοκιμής·

3) «μπλε ομάδα»: το προσωπικό της χρηματοοικονομικής οντότητας και, κατά περίπτωση, το προσωπικό τρίτων παρόχων υπηρεσιών της χρηματοοικονομικής οντότητας και κάθε άλλου μέρους που θεωρείται συναφές σε σχέση με το πεδίο της TLPT, το οποίο υπερασπίζεται τη χρήση συστημάτων δικτύου και πληροφοριών μιας χρηματοοικονομικής οντότητας διατηρώντας την οικεία κατάσταση κυβερνοασφάλειας έναντι προσομοιωμένων ή πραγματικών επιθέσεων και το οποίο δεν γνωρίζει για την TLPT·

4) «καθήκοντα μπλε ομάδας»: καθήκοντα τα οποία εκτελούνται συνήθως από τη μπλε ομάδα, όπως το κέντρο επιχειρήσεων ασφάλειας (SOC), οι υπηρεσίες υποδομής ΤΠΕ, οι υπηρεσίες υποστήριξης, οι υπηρεσίες διαχείρισης συμβάντων σε επιχειρησιακό επίπεδο·

5) «κόκκινη ομάδα»: οι δοκιμαστές, εσωτερικοί ή εξωτερικοί, με τους οποίους έχουν συναφθεί συμβάσεις για τη διενέργεια TLPT ή τους έχει ανατεθεί μια TLPT·

6) «δράσεις μωβ ομάδας»: συνεργατική δραστηριότητα δοκιμών στην οποία συμμετέχουν τόσο οι δοκιμαστές όσο και η μπλε ομάδα·

([3]) Κανονισμός (ΕΕ) αριθ. 1093/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, σχετικά με τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Τραπεζών), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/78/ΕΚ της Επιτροπής (ΕΕ L 331 της 15.12.2010, σ. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Κανονισμός (ΕΕ) αριθ. 1094/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, για τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/79/ΕΚ της Επιτροπής (ΕΕ L 331 της 15.12.2010, σ. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Κανονισμός (ΕΕ) αριθ. 1095/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, σχετικά με τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/77/ΕΚ (ΕΕ L 331 της 15.12.2010, σ. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

7) «αρχή TLPT»: οποιαδήποτε από τις ακόλουθες:

α) η ενιαία δημόσια αρχή στον χρηματοοικονομικό τομέα που ορίζεται σύμφωνα με το άρθρο 26 παράγραφος 9 του κανονισμού (ΕΕ) 2022/2554,

β) η αρχή στον χρηματοοικονομικό τομέα στην οποία έχει ανατεθεί η άσκηση ορισμένων ή όλων των καθηκόντων σε σχέση με την εκτέλεση TLPT, σύμφωνα με το άρθρο 26 παράγραφος 10 του κανονισμού (ΕΕ) 2022/2554,

γ) οποιαδήποτε από τις αρμόδιες αρχές που αναφέρονται στο άρθρο 46 του κανονισμού (ΕΕ) 2022/2554·

8) «κυβερνοομάδα TLPT» ή «TCT»: το προσωπικό των αρχών TLPT το οποίο είναι υπεύθυνο για θέματα σχετικά με τις TLPT·

9) «διαχειριστές δοκιμής»: το προσωπικό που έχει οριστεί να διευθύνει τις δραστηριότητες της αρχής TLPT για συγκεκριμένη TLPT με σκοπό την παρακολούθηση της συμμόρφωσης με τον παρόντα κανονισμό·

10) «πάροχος πληροφοριών για απειλές»: οι εμπειρογνώμονες που προσλαμβάνονται από τη χρηματοοικονομική οντότητα για κάθε TLPT και είναι εξωτερικοί σε σχέση με τη χρηματοοικονομική οντότητα και τους ενδοομιλικούς παρόχους υπηρεσιών ΤΠΕ, εάν υπάρχουν, οι οποίοι συλλέγουν και αναλύουν στοχευμένες πληροφορίες για απειλές που αφορούν τις χρηματοοικονομικές οντότητες που εμπίπτουν στο πεδίο συγκεκριμένης άσκησης TLPT και αναπτύσσουν αντίστοιχα συναφή και ρεαλιστικά σενάρια απειλών·

11) «πάροχοι TLPT»: δοκιμαστές και πάροχοι πληροφοριών για απειλές·

12) «πλεονέκτημα»: η βοήθεια ή οι πληροφορίες που παρέχει η ομάδα ελέγχου στους δοκιμαστές ώστε να μπορούν να συνεχίσουν την εκτέλεση μιας διαδρομής επίθεσης όταν δεν είναι σε θέση να προχωρήσουν μόνοι τους και όταν δεν υπάρχει άλλη εύλογη εναλλακτική λύση, μεταξύ άλλων λόγω ανεπάρκειας χρόνου ή πόρων σε μια δεδομένη TLPT·

13) «διαδρομή επίθεσης»: η διαδρομή που ακολουθούν οι δοκιμαστές κατά τη διάρκεια του ενεργού σταδίου δοκιμών κόκκινης ομάδας της TLPT για την επίτευξη των ενδεικτών που έχουν καθοριστεί για την εν λόγω TLPT·

14) «ενδείκτες»: βασικοί στόχοι των συστημάτων ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες μιας χρηματοοικονομικής οντότητας τους οποίους οι δοκιμαστές προσπαθούν να επιτύχουν μέσω της δοκιμής·

15) «ευαίσθητες πληροφορίες»: πληροφορίες που μπορούν εύκολα να αξιοποιηθούν για την πραγματοποίηση επιθέσεων κατά των συστημάτων ΤΠΕ της χρηματοοικονομικής οντότητας, διανοητική ιδιοκτησία, εμπιστευτικά επιχειρηματικά δεδομένα ή δεδομένα προσωπικού χαρακτήρα, που μπορούν να βλάψουν άμεσα ή έμμεσα τη χρηματοοικονομική οντότητα και το οικοσύστημά της σε περίπτωση που φτάσουν στα χέρια κακόβουλων παραγόντων·

16) «ομάδα»: όλες οι χρηματοοικονομικές οντότητες που συμμετέχουν σε ομαδικές TLPT σύμφωνα με το άρθρο 26 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2554·

17) «κράτος μέλος υποδοχής»: το κράτος μέλος υποδοχής σύμφωνα με το ενωσιακό τομεακό δίκαιο που εφαρμόζεται σε κάθε χρηματοοικονομική οντότητα·

18) «κοινές TLPT»: TLPT, πλην των ομαδικών TLPT, όπως αναφέρονται στο άρθρο 26 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2554, στις οποίες συμμετέχουν περισσότερες από μία χρηματοοικονομικές οντότητες που χρησιμοποιούν τον ίδιο ενδοομιλικό πάροχο υπηρεσιών ΤΠΕ ή ανήκουν στον ίδιο όμιλο και χρησιμοποιούν από κοινού τα συστήματα ΤΠΕ.

Άρθρο 2

Προσδιορισμός των χρηματοοικονομικών οντοτήτων που υποχρεούνται να διενεργούν TLPT

1. Οι αρχές TLPT αξιολογούν αν κάποια χρηματοοικονομική οντότητα υποχρεούται να διενεργεί TLPT, λαμβάνοντας υπόψη τις επιπτώσεις των εν λόγω χρηματοοικονομικών οντοτήτων, τον συστημικό χαρακτήρα τους και το οικείο προφίλ κινδύνου ΤΠΕ, με βάση όλα τα ακόλουθα κριτήρια:

α) παράγοντες που σχετίζονται με τις επιπτώσεις και τον συστημικό χαρακτήρα:

i) το μέγεθος της χρηματοοικονομικής οντότητας, που προσδιορίζεται με βάση το αν η χρηματοοικονομική οντότητα παρέχει χρηματοοικονομικές υπηρεσίες σε ένα ή περισσότερα κράτη μέλη και συγκρίνοντας τις δραστηριότητες της χρηματοοικονομικής οντότητας με τις δραστηριότητες άλλων χρηματοοικονομικών οντοτήτων που παρέχουν παρόμοιες υπηρεσίες·

ii) την έκταση και τη φύση της διασυνδεσιμότητας της χρηματοοικονομικής οντότητας με άλλες χρηματοοικονομικές οντότητες στον χρηματοοικονομικό τομέα σε ένα ή περισσότερα κράτη μέλη·

iii) την κρισιμότητα ή τη σημασία των υπηρεσιών που παρέχει η χρηματοοικονομική οντότητα στον χρηματοοικονομικό τομέα·

iv) τη δυνατότητα υποκατάστασης των υπηρεσιών που παρέχει η χρηματοοικονομική οντότητα·

v) την πολυπλοκότητα του επιχειρηματικού μοντέλου της χρηματοοικονομικής οντότητας και των σχετικών υπηρεσιών και διαδικασιών·

vi) αν η χρηματοοικονομική οντότητα ανήκει σε όμιλο συστημικού χαρακτήρα σε ενωσιακό ή εθνικό επίπεδο στον χρηματοοικονομικό τομέα και χρησιμοποιεί συστήματα ΤΠΕ από κοινού με άλλες οντότητες·

β) παράγοντες που σχετίζονται με κινδύνους ΤΠΕ:

i) το προφίλ κινδύνου της χρηματοοικονομικής οντότητας·

ii) το τοπίο των απειλών της χρηματοοικονομικής οντότητας·

iii) τον βαθμό εξάρτησης κρίσιμων ή σημαντικών λειτουργιών ή υποστηρικτικών λειτουργιών της χρηματοοικονομικής οντότητας από συστήματα και διαδικασίες ΤΠΕ·

iv) την πολυπλοκότητα της αρχιτεκτονικής ΤΠΕ της χρηματοοικονομικής οντότητας·

v) τις υπηρεσίες και τις λειτουργίες ΤΠΕ που στηρίζονται από τρίτους παρόχους υπηρεσιών ΤΠΕ, καθώς και το πλήθος και το είδος των συμβατικών ρυθμίσεων με τρίτους παρόχους υπηρεσιών ΤΠΕ ή ενδοομιλικούς παρόχους υπηρεσιών ΤΠΕ·

vi) τα αποτελέσματα τυχόν εποπτικών ελέγχων που αφορούν την αξιολόγηση του επιπέδου ωριμότητας της χρηματοοικονομικής οντότητας από πλευράς ΤΠΕ·

vii) την ωριμότητα των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ και των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ·

viii) την ωριμότητα των επιχειρησιακών μέτρων ασφάλειας ΤΠΕ στους τομείς του εντοπισμού και του μετριασμού, συμπεριλαμβανομένης της ικανότητας:

1) παρακολούθησης σε μόνιμη βάση των υποδομών ΤΠΕ της χρηματοοικονομικής οντότητας,

2) ανίχνευσης συμβάντων που σχετίζονται με τις ΤΠΕ σε πραγματικό χρόνο,

3) ανάλυσης των συμβάντων που αναφέρονται στο σημείο 2,

4) έγκαιρης και αποτελεσματικής ανταπόκρισης στα συμβάντα που αναφέρονται στο σημείο 2·

ix) αν η χρηματοοικονομική οντότητα ανήκει σε όμιλο που δραστηριοποιείται στον χρηματοοικονομικό τομέα σε ενωσιακό ή εθνικό επίπεδο και χρησιμοποιεί συστήματα ΤΠΕ από κοινού με άλλες οντότητες.

Για τους σκοπούς του στοιχείου α) σημείο i), η αρχή TLPT εξετάζει, όπου είναι δυνατόν:

α) το μερίδιο αγοράς της χρηματοοικονομικής οντότητας σε ενωσιακό και εθνικό επίπεδο·

β) το φάσμα των δραστηριοτήτων που προσφέρει η χρηματοοικονομική οντότητα·

γ) το μερίδιο αγοράς των υπηρεσιών που παρέχονται από τη χρηματοοικονομική οντότητα ή των δραστηριοτήτων που αναλαμβάνονται σε ενωσιακό και εθνικό επίπεδο.

Για τους σκοπούς του στοιχείου α) σημείο v), η αρχή TLPT εξετάζει, όπου είναι δυνατόν:

α) αν η χρηματοοικονομική οντότητα εφαρμόζει περισσότερα από ένα επιχειρηματικά μοντέλα·

β) τη διασυνδεσιμότητα των διαφόρων επιχειρηματικών διαδικασιών και των συναφών υπηρεσιών.

2. Οι αρχές TLPT απαιτούν από όλες τις ακόλουθες χρηματοοικονομικές οντότητες να διενεργούν TLPT, εκτός εάν από την αξιολόγηση που αναφέρεται στην παράγραφο 1 όσον αφορά μια χρηματοοικονομική οντότητα προκύπτει ότι οι επιπτώσεις της, οι προβληματισμοί σχετικά με τη χρηματοπιστωτική σταθερότητα που αφορούν την εν λόγω χρηματοοικονομική οντότητα ή το οικείο προφίλ κινδύνου ΤΠΕ δεν δικαιολογούν τη διενέργεια TLPT:

α) πιστωτικά ιδρύματα που πληρούν οποιαδήποτε από τις ακόλουθες προϋποθέσεις:

i) έχουν προσδιοριστεί ως παγκόσμια συστημικώς σημαντικά ιδρύματα (G-SII) σύμφωνα με το άρθρο 131 της οδηγίας 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7])·

ii) έχουν προσδιοριστεί ως άλλα συστημικά σημαντικά ιδρύματα (O-SII), σύμφωνα με το άρθρο 131 της οδηγίας 2013/36/ΕΕ·

iii) ανήκουν σε G-SII ή O-SII·

([7]) Οδηγία 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με την πρόσβαση στη δραστηριότητα των πιστωτικών ιδρυμάτων και την προληπτική εποπτεία των πιστωτικών ιδρυμάτων, την τροποποίηση της οδηγίας 2002/87/ΕΚ και την κατάργηση των οδηγιών 2006/48/ΕΚ και 2006/49/ΕΚ (ΕΕ L 176 της 27.6.2013, σ. 338, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

β) ιδρύματα πληρωμών που υπερέβησαν σε καθένα από τα 2 ημερολογιακά έτη που προηγήθηκαν της αξιολόγησης από την αρχή TLPT το συνολικό ποσό πράξεων πληρωμής ύψους 150 δισεκατ. EUR, όπως ορίζονται στο άρθρο 4 σημείο 5 της οδηγίας (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([8])·

γ) ιδρύματα ηλεκτρονικού χρήματος που υπερέβησαν σε καθένα από τα 2 ημερολογιακά έτη που προηγήθηκαν της αξιολόγησης από την αρχή TLPT είτε το συνολικό ποσό πράξεων πληρωμής ύψους 150 δισεκατ. EUR, όπως ορίζονται στο άρθρο 4 σημείο 5 της οδηγίας (ΕΕ) 2015/2366 είτε το συνολικό ποσό ηλεκτρονικού χρήματος σε κυκλοφορία ύψους 40 δισεκατ. EUR·

δ) κεντρικά αποθετήρια τίτλων·

ε) κεντρικούς αντισυμβαλλομένους·

στ) τόπους διαπραγμάτευσης με σύστημα ηλεκτρονικών συναλλαγών που πληρούν οποιοδήποτε από τα ακόλουθα κριτήρια:

i) ο τόπος διαπραγμάτευσης έχει το μεγαλύτερο μερίδιο αγοράς όσον αφορά τον κύκλο εργασιών σε εθνικό επίπεδο για καθένα από τα 2 ημερολογιακά έτη που προηγήθηκαν της αξιολόγησης από την αρχή TLPT σε οποιοδήποτε από τα ακόλουθα:

1) κινητές αξίες όπως ορίζονται στο άρθρο 4 παράγραφος 1 σημείο 44 στοιχείο α) της οδηγίας 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([9])·

2) κινητές αξίες όπως ορίζονται στο άρθρο 4 παράγραφος 1 σημείο 44 στοιχείο β) της οδηγίας 2014/65/ΕΕ·

3) παράγωγα όπως ορίζονται στο άρθρο 2 παράγραφος 1 σημείο 29 του κανονισμού (ΕΕ) αριθ. 600/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([10])·

4) δομημένα χρηματοπιστωτικά προϊόντα όπως ορίζονται στο άρθρο 2 παράγραφος 1 σημείο 28 του κανονισμού (ΕΕ) αριθ. 600/2014·

5) δικαιώματα εκπομπής όπως αναφέρονται στο παράρτημα Ι τμήμα Γ σημείο 11 της οδηγίας 2014/65/ΕΕ·

ii) ο τόπος διαπραγμάτευσης έχει μερίδιο αγοράς όσον αφορά τον κύκλο εργασιών σε ενωσιακό επίπεδο που υπερβαίνει το 5 % για καθένα από τα 2 ημερολογιακά έτη που προηγήθηκαν της αξιολόγησης από την αρχή TLPT σε οποιοδήποτε από τα ακόλουθα:

1) μετοχές εταιρειών και άλλους τίτλους ισοδύναμους με μετοχές εταιρειών, προσωπικών εταιρειών και άλλων οντοτήτων, καθώς και αποθετήρια έγγραφα μετοχών·

2) ομόλογα ή άλλες μορφές τιτλοποιημένου χρέους, καθώς και αποθετήρια έγγραφα τέτοιων κινητών αξιών·

3) παράγωγα όπως ορίζονται στο άρθρο 2 παράγραφος 1 σημείο 29 του κανονισμού (ΕΕ) αριθ. 600/2014·

4) δομημένα χρηματοπιστωτικά προϊόντα όπως ορίζονται στο άρθρο 2 παράγραφος 1 σημείο 28 του κανονισμού (ΕΕ) αριθ. 600/2014·

5) δικαιώματα εκπομπής όπως αναφέρονται στο παράρτημα Ι τμήμα Γ σημείο 11 της οδηγίας 2014/65/ΕΕ·

([8]) Οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2015, σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 2002/65/ΕΚ, 2009/110/ΕΚ και 2013/36/ΕΕ και του κανονισμού (ΕΕ) αριθ. 1093/2010 και την κατάργηση της οδηγίας 2007/64/ΕΚ (ΕΕ L 337 της 23.12.2015, σ. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) Οδηγία 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και την τροποποίηση της οδηγίας 2002/92/ΕΚ και της οδηγίας 2011/61/ΕΕ (ΕΕ L 173 της 12.6.2014, σ. 349, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) Κανονισμός (ΕΕ) αριθ. 600/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 (ΕΕ L 173 της 12.6.2014, σ. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

ζ) ασφαλιστικές και αντασφαλιστικές επιχειρήσεις που πληρούν όλα τα ακόλουθα κριτήρια:

i) έχουν ακαθάριστο εγγεγραμμένο ασφάλιστρο πάνω από 1 500 000 000 EUR·

ii) έχουν τεχνικές προβλέψεις πάνω από 10 000 000 000 EUR·

iii) ασφαλιστικές επιχειρήσεις που ασκούν μόνο δραστηριότητες ασφάλισης ζωής ή ασκούν δραστηριότητες ασφάλισης ζωής και ζημιών και διαθέτουν συνολικά στοιχεία ενεργητικού που υπερβαίνουν το 3,5 % του αθροίσματος των συνολικών στοιχείων ενεργητικού που αποτιμώνται σύμφωνα με το άρθρο 75 της οδηγίας 2009/138/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [11], των ασφαλιστικών και αντασφαλιστικών επιχειρήσεων που είναι εγκατεστημένες στο κράτος μέλος.

Για τους σκοπούς του στοιχείου στ) σημείο ii), όταν ο τόπος διαπραγμάτευσης ανήκει σε όμιλο που χρησιμοποιεί από κοινού συστήματα ΤΠΕ ή τον ίδιο ενδοομιλικό πάροχο υπηρεσιών ΤΠΕ, λαμβάνεται υπόψη ο κύκλος εργασιών των συμβάσεων κινητών αξιών και παραγώγων σε όλους τους τόπους διαπραγμάτευσης που ανήκουν στον ίδιο όμιλο και είναι εγκατεστημένοι στην Ένωση.

Για τους σκοπούς του στοιχείου ζ), οι αρχές TLPT προσδιορίζουν ένα υποσύνολο όλων των ασφαλιστικών και αντασφαλιστικών επιχειρήσεων, εφαρμόζοντας τα κριτήρια που ορίζονται στο στοιχείο ζ) σημεία i), ii) και iii). Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις που περιλαμβάνονται στο εν λόγω υποσύνολο υποχρεούνται να διενεργούν TLPT όταν πληρούν επίσης οποιοδήποτε από τα ακόλουθα κριτήρια:

α) το ακαθάριστο εγγεγραμμένο ασφάλιστρο υπερβαίνει τα 3 000 000 000 EUR·

β) οι τεχνικές προβλέψεις υπερβαίνουν τα 30 000 000 000 EUR·

γ) τα συνολικά στοιχεία ενεργητικού υπερβαίνουν το 10 % του αθροίσματος των συνολικών στοιχείων ενεργητικού που αποτιμώνται σύμφωνα με το άρθρο 75 της οδηγίας 2009/138/ΕΚ των ασφαλιστικών και αντασφαλιστικών επιχειρήσεων που είναι εγκατεστημένες στο κράτος μέλος.

3. Όταν περισσότερες από μία χρηματοοικονομικές οντότητες που ανήκουν στον ίδιο όμιλο και χρησιμοποιούν από κοινού συστήματα ΤΠΕ ή όταν περισσότερες από μία χρηματοοικονομικές οντότητες που χρησιμοποιούν τον ίδιο ενδοομιλικό πάροχο υπηρεσιών ΤΠΕ πληρούν τα κριτήρια που ορίζονται στην παράγραφο 2, οι αρχές TLPT των εν λόγω χρηματοοικονομικών οντοτήτων αποφασίζουν, σύμφωνα με το άρθρο 16 παράγραφος 2, αν η απαίτηση διενέργειας TLPT σε ατομική βάση έχει σημασία για τις εν λόγω χρηματοοικονομικές οντότητες.

Όταν η αρχή TLPT της μητρικής επιχείρησης ομίλου χρηματοοικονομικών οντοτήτων που αναφέρεται στο πρώτο εδάφιο διαφέρει από τις αρχές TLPT των χρηματοοικονομικών οντοτήτων του ομίλου, οι αρχές TLPT των χρηματοοικονομικών οντοτήτων που ανήκουν στον εν λόγω όμιλο ζητούν τη γνώμη της εν λόγω αρχής σχετικά με το αν είναι σκόπιμο να διενεργηθεί TLPT σε ατομική βάση.

Άρθρο 3

TCT και διαχειριστές δοκιμών TLPT

1. Η αρχή TLPT αναθέτει την ευθύνη για τον συντονισμό των δραστηριοτήτων σχετικά με τις TLPT σε μια TCT. Η TCT απαρτίζεται από διαχειριστές δοκιμών στους οποίους ανατίθεται η εποπτεία μιας επιμέρους TLPT.

2. Για κάθε δοκιμή, η αρχή TLPT ορίζει έναν διαχειριστή δοκιμής και τουλάχιστον έναν αναπληρωτή.

3. Οι διαχειριστές δοκιμής παρακολουθούν και διασφαλίζουν τη συμμόρφωση με τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό.

[11] Οδηγία 2009/138/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009, σχετικά με την ανάληψη και την άσκηση δραστηριοτήτων ασφάλισης και αντασφάλισης (Φερεγγυότητα II) (ΕΕ L 335 της 17.12.2009, σ. 1, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. Ο διαχειριστής δοκιμής κοινοποιεί τα στοιχεία επικοινωνίας της TCT στη χρηματοοικονομική οντότητα μέσω της κοινοποίησης που αναφέρεται στο άρθρο 9 παράγραφος 1.

5. Η αρχή TLPT συμμετέχει σε όλα τα στάδια της TLPT.

Άρθρο 4

Οργανωτικές ρυθμίσεις για τις χρηματοοικονομικές οντότητες

1. Οι χρηματοοικονομικές οντότητες ορίζουν επικεφαλής της ομάδας ελέγχου, ο οποίος είναι υπεύθυνος για την καθημερινή διαχείριση της TLPT και τις αποφάσεις και τις ενέργειες της ομάδας ελέγχου.

2. Οι χρηματοοικονομικές οντότητες θεσπίζουν οργανωτικά και διαδικαστικά μέτρα προκειμένου να διασφαλίσουν ότι:

α) η πρόσβαση σε πληροφορίες που αφορούν οποιαδήποτε προγραμματισμένη ή υπό εξέλιξη TLPT περιορίζεται, με βάση την αρχής της ανάγκης γνώσης, στην ομάδα ελέγχου, στο διοικητικό όργανο, στους δοκιμαστές, στον πάροχο πληροφοριών για απειλές και στην αρχή TLPT·

β) η ομάδα ελέγχου διαβουλεύεται με τους διαχειριστές δοκιμής πριν από τη συμμετοχή οποιουδήποτε μέλους της μπλε ομάδας σε TLPT·

γ) η ομάδα ελέγχου ενημερώνεται για κάθε εντοπισμό της TLPT από μέλη του προσωπικού της χρηματοοικονομικής οντότητας ή των τρίτων παρόχων υπηρεσιών της· σε περίπτωση παραπομπής της επακόλουθης αντιμετώπισης συμβάντος στο κατάλληλο επίπεδο, όπου απαιτείται, η ομάδα ελέγχου αναλαμβάνει την εν λόγω παραπομπή στο κατάλληλο επίπεδο·

δ) εφαρμόζονται ρυθμίσεις σχετικά με το απόρρητο της TLPT, οι οποίες ισχύουν για το προσωπικό της χρηματοοικονομικής οντότητας, το προσωπικό των οικείων τρίτων παρόχων υπηρεσιών ΤΠΕ, τους δοκιμαστές και τον πάροχο πληροφοριών για απειλές·

ε) η ομάδα ελέγχου παρέχει στους διαχειριστές δοκιμής κάθε πληροφορία σε σχέση με την TLPT, κατόπιν αιτήματος·

στ) όπου είναι δυνατόν, τα μέρη που συμμετέχουν στην TLPT αναφέρονται σε αυτή μόνο με κωδική ονομασία.

Άρθρο 5

Διαχείριση κινδύνων για TLPT

1. Κατά το προπαρασκευαστικό στάδιο που αναφέρεται στο άρθρο 9, η ομάδα ελέγχου αξιολογεί τους κινδύνους που συνδέονται με τις δοκιμές συστημάτων παραγωγής κρίσιμων ή σημαντικών λειτουργιών της χρηματοοικονομικής οντότητας, συμπεριλαμβανομένων των πιθανών επιπτώσεων:

α) στον χρηματοοικονομικό τομέα·

β) στη χρηματοπιστωτική σταθερότητα σε ενωσιακό ή εθνικό επίπεδο.

Η ομάδα ελέγχου επανεξετάζει τις εν λόγω επιπτώσεις καθ' όλη τη διάρκεια των δοκιμών.

2. Για τους σκοπούς της αξιολόγησης και της διαχείρισης κινδύνων, η ομάδα ελέγχου λαμβάνει υπόψη τουλάχιστον τα ακόλουθα είδη κινδύνων που σχετίζονται με:

α) τη χορήγηση πρόσβασης στον πάροχο πληροφοριών για απειλές και στους εξωτερικούς δοκιμαστές, κατά περίπτωση, σε ευαίσθητες πληροφορίες σχετικά με τη χρηματοοικονομική οντότητα·

β) την έλλειψη συμμόρφωσης της TLPT με τον κανονισμό (ΕΕ) 2022/2554 και με τον παρόντα κανονισμό, όταν η εν λόγω έλλειψη συμμόρφωσης έχει ως αποτέλεσμα την έλλειψη της βεβαίωσης που αναφέρεται στο άρθρο 26 παράγραφος 7 του κανονισμού (ΕΕ) 2022/2554, μεταξύ άλλων όταν η εν λόγω έλλειψη συμμόρφωσης οφείλεται σε παραβιάσεις της εμπιστευτικότητας της TLPT ή σε έλλειψη δεοντολογικής συμπεριφοράς·

γ) την παραπομπή κρίσεων και συμβάντων στο κατάλληλο επίπεδο·

δ) το ενεργό στάδιο κόκκινης ομάδας, συμπεριλαμβανομένων των κινδύνων που σχετίζονται με τη διακοπή κρίσιμων δραστηριοτήτων και την αλλοίωση δεδομένων λόγω των δραστηριοτήτων των δοκιμαστών, και τις πιθανές επιπτώσεις του σε τρίτους·

ε) τη δραστηριότητα της μπλε ομάδας, συμπεριλαμβανομένων των κινδύνων που σχετίζονται με τη διακοπή κρίσιμων δραστηριοτήτων και την αλλοίωση δεδομένων λόγω των δραστηριοτήτων της μπλε ομάδας, και τις πιθανές επιπτώσεις της σε τρίτους·

στ) την ελλιπή αποκατάσταση των συστημάτων που επηρεάζονται από την TLPT.

Άρθρο 6

Διαχείριση κινδύνων για ομαδικές ή κοινές TLPT

1. Στην περίπτωση κοινής TLPT ή ομαδικής TLPT, η ομάδα ελέγχου κάθε χρηματοοικονομικής οντότητας διενεργεί δική της αξιολόγηση κινδύνων και θεσπίζει δικά της μέτρα διαχείρισης κινδύνων.

2. Η ομάδα ελέγχου της ορισθείσας χρηματοοικονομικής οντότητας που αναφέρεται στο άρθρο 16 παράγραφος 3 στοιχείο β) του παρόντος κανονισμού ή η χρηματοοικονομική οντότητα που ορίζεται σύμφωνα με το άρθρο 26 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2554 αξιολογεί τους κινδύνους που σχετίζονται με τη συμμετοχή πολλαπλών χρηματοοικονομικών οντοτήτων στην TLPT. Οι ομάδες ελέγχου των εμπλεκόμενων χρηματοοικονομικών οντοτήτων συνεργάζονται με την ομάδα ελέγχου της ορισθείσας χρηματοοικονομικής οντότητας για τον εντοπισμό πιθανών κοινών κινδύνων.

Άρθρο 7

Επιλογή παρόχων TLPT

1. Η ομάδα ελέγχου λαμβάνει μέτρα για τη διαχείριση των κινδύνων που σχετίζονται με την TLPT και διασφαλίζει ειδικότερα ότι, για κάθε TLPT:

α) ο πάροχος πληροφοριών για απειλές και οι εξωτερικοί δοκιμαστές παρέχουν στην ομάδα ελέγχου λεπτομερές βιογραφικό σημείωμα και αντίγραφα των πιστοποιήσεων που, σύμφωνα με τα αναγνωρισμένα πρότυπα της αγοράς, ενδείκνυνται για την εκτέλεση των δραστηριοτήτων τους·

β) ο πάροχος πληροφοριών για απειλές και οι εξωτερικοί δοκιμαστές καλύπτονται δεόντως και πλήρως από σχετική ασφάλιση επαγγελματικής ευθύνης, μεταξύ άλλων έναντι κινδύνων παραπτωμάτων και αμέλειας·

γ) ο πάροχος πληροφοριών για απειλές παρέχει τουλάχιστον τρεις συστάσεις από προηγούμενες αναθέσεις στο πλαίσιο δοκιμών παρείσδυσης και δοκιμών κόκκινης ομάδας·

δ) οι εξωτερικοί δοκιμαστές παρέχουν τουλάχιστον πέντε συστάσεις από προηγούμενες αναθέσεις που σχετίζονται με δοκιμές παρείσδυσης και δοκιμές κόκκινης ομάδας·

ε) τα μέλη του προσωπικού του παρόχου πληροφοριών για απειλές στα οποία έχει ανατεθεί η TLPT:

i) περιλαμβάνουν τουλάχιστον έναν διαχειριστή με τουλάχιστον 5ετή πείρα στον τομέα των πληροφοριών για απειλές και τουλάχιστον ένα επιπλέον μέλος με τουλάχιστον 2ετή πείρα στον τομέα των πληροφοριών για απειλές·

ii) διαθέτουν ευρύ φάσμα και κατάλληλο επίπεδο επαγγελματικών γνώσεων και δεξιοτήτων, συμπεριλαμβανομένων:

1) τακτικών, τεχνικών και διαδικασιών συλλογής πληροφοριών·

2) γεωπολιτικών, τεχνικών και τομεακών γνώσεων·

3) επαρκών δεξιοτήτων επικοινωνίας για τη σαφή παρουσίαση και υποβολή εκθέσεων σχετικά με το αποτέλεσμα της ανάθεσης.

iii) έχουν συμμετάσχει συνδυαστικά σε τουλάχιστον τρεις προηγούμενες αναθέσεις στον τομέα των πληροφοριών για απειλές στο πλαίσιο δοκιμών παρείσδυσης και δοκιμών κόκκινης ομάδας·

iv) δεν εκτελούν ταυτόχρονα καθήκοντα μπλε ομάδας ή άλλες υπηρεσίες που ενδέχεται να προκαλέσουν σύγκρουση συμφερόντων όσον αφορά τη χρηματοοικονομική οντότητα, τον τρίτο πάροχο υπηρεσιών ΤΠΕ ή τον ενδοομιλικό πάροχο υπηρεσιών ΤΠΕ που συμμετέχει σε TLPT η οποία τους έχει ανατεθεί·

v) διαχωρίζονται από το προσωπικό του ίδιου παρόχου TLPT που παρέχει εξωτερικούς δοκιμαστές για την ίδια TLPT και δεν υποβάλλουν αναφορά σε αυτό·

στ) όσον αφορά τους εξωτερικούς δοκιμαστές, η κόκκινη ομάδα στην οποία έχει ανατεθεί η TLPT:

i) απαρτίζεται από τουλάχιστον έναν διαχειριστή, με τουλάχιστον 5ετή πείρα σε δοκιμές παρείσδυσης και δοκιμές κόκκινης ομάδας, καθώς και τουλάχιστον δύο επιπλέον δοκιμαστές, καθένας από τους οποίους διαθέτει τουλάχιστον 2ετή πείρα σε δοκιμές παρείσδυσης και δοκιμές κόκκινης ομάδας·

ii) διαθέτει ευρύ φάσμα και κατάλληλο επίπεδο επαγγελματικών γνώσεων και δεξιοτήτων, συμπεριλαμβανομένων γνώσεων σχετικά με την επιχειρηματική δραστηριότητα της χρηματοοικονομικής οντότητας, την αναγνώριση, τη διαχείριση κινδύνων, την αξιοποίηση της ανάπτυξης, τη φυσική παρείσδυση, την κοινωνική μηχανική, την ανάλυση ευπαθειών, καθώς και επαρκείς δεξιότητες επικοινωνίας για τη σαφή παρουσίαση και υποβολή εκθέσεων σχετικά με το αποτέλεσμα της ανάθεσης·

iii) έχει συμμετάσχει συνδυαστικά σε τουλάχιστον πέντε προηγούμενες αναθέσεις που σχετίζονται με δοκιμές παρείσδυσης και δοκιμές κόκκινης ομάδας·

iv) δεν απασχολείται ούτε παρέχει υπηρεσίες σε πάροχο πληροφοριών για απειλές που εκτελεί ταυτόχρονα καθήκοντα μπλε ομάδας είτε για χρηματοοικονομική οντότητα, είτε για τρίτο πάροχο υπηρεσιών ΤΠΕ είτε για ενδοομιλικό πάροχο υπηρεσιών ΤΠΕ που συμμετέχει στην TLPT·

v) διαχωρίζεται από το προσωπικό του ίδιου παρόχου TLPT που παρέχει ταυτόχρονα υπηρεσίες πληροφοριών για απειλές για την ίδια TLPT.

ζ) οι δοκιμαστές και ο πάροχος πληροφοριών για απειλές εκτελούν διαδικασίες αποκατάστασης με την ολοκλήρωση των δοκιμών, συμπεριλαμβανομένης της ασφαλούς διαγραφής πληροφοριών που σχετίζονται με κωδικούς πρόσβασης, διαπιστευτήρια και άλλα μυστικά κλειδιά που παραβιάστηκαν κατά τη διάρκεια της TLPT, της ασφαλούς κοινοποίησης στις χρηματοοικονομικές οντότητες των λογαριασμών που παραβιάστηκαν, της ασφαλούς συλλογής, αποθήκευσης, διαχείρισης και διαγραφής άλλων δεδομένων που συλλέχθηκαν κατά τη διάρκεια των δοκιμών·

η) οι δοκιμαστές, επιπλέον των διαδικασιών αποκατάστασης με την ολοκλήρωση των δοκιμών που αναφέρονται στο στοιχείο ζ), διενεργούν τις ακόλουθες διαδικασίες αποκατάστασης:

i) απενεργοποίηση εντολών και ελέγχου·

ii) διακόπτες τερματισμού του πεδίου εφαρμογής και της ημερομηνίας·

iii) αφαίρεση κερκόπορτων και άλλων κακόβουλων λογισμικών·

iv) κοινοποίηση πιθανής παραβίασης·

v) διαδικασίες για μελλοντική αποκατάσταση εφεδρικών αντιγράφων που μπορεί να αφορούν κακόβουλο λογισμικό ή εργαλεία που εγκαταστάθηκαν κατά τη διάρκεια της δοκιμής·

vi) παρακολούθηση των δραστηριοτήτων της μπλε ομάδας και ενημέρωση της ομάδας ελέγχου σχετικά με τυχόν εντοπισμούς·

θ) οι δοκιμαστές και ο πάροχος πληροφοριών για απειλές δεν εκτελούν ούτε συμμετέχουν σε καμία από τις ακόλουθες δραστηριότητες:

i) μη εξουσιοδοτημένη καταστροφή εξοπλισμού της χρηματοοικονομικής οντότητας και των οικείων τρίτων παρόχων υπηρεσιών ΤΠΕ, εάν υπάρχουν·

ii) μη ελεγχόμενη τροποποίηση πληροφοριών και πόρων ΤΠΕ της χρηματοοικονομικής οντότητας και των οικείων τρίτων παρόχων υπηρεσιών ΤΠΕ, εάν υπάρχουν·

iii) εκούσια παραβίαση της συνέχειας κρίσιμων ή σημαντικών λειτουργιών της χρηματοοικονομικής οντότητας·

iv) μη εξουσιοδοτημένη συμπερίληψη συστημάτων εκτός πεδίου των δοκιμών·

v) μη εξουσιοδοτημένη γνωστοποίηση των αποτελεσμάτων των δοκιμών.

2. Η ομάδα ελέγχου τηρεί αρχείο των εγγράφων τεκμηρίωσης που παρέχουν οι δοκιμαστές και οι πάροχοι πληροφοριών για απειλές προκειμένου να αποδείξουν τη συμμόρφωση με την παράγραφο 1 στοιχεία α) έως στ).

Σε εξαιρετικές περιστάσεις, οι χρηματοοικονομικές οντότητες μπορούν να συνάπτουν συμβάσεις με εξωτερικούς δοκιμαστές και παρόχους πληροφοριών για απειλές οι οποίοι δεν πληρούν μία ή περισσότερες από τις απαιτήσεις που ορίζονται στην παράγραφο 1 στοιχεία α) έως στ), υπό την προϋπόθεση ότι οι εν λόγω χρηματοοικονομικές οντότητες λαμβάνουν κατάλληλα μέτρα για τον μετριασμό των κινδύνων που σχετίζονται με την έλλειψη συμμόρφωσης με τα εν λόγω σημεία και καταγράφουν τα εν λόγω μέτρα.

Άρθρο 8

Ιδιαίτερα χαρακτηριστικά ομαδικών ή κοινών TLPT

1. Εκτός εάν αποφασίσει διαφορετικά η επικεφαλής αρχή TLPT, όταν σε μια ομαδική ή κοινή TLPT συμμετέχουν περισσότερες από μία χρηματοοικονομικές οντότητες, οι οποίες προσδιορίζονται σύμφωνα με το άρθρο 16 παράγραφος 2 ή 4, κάθε χρηματοοικονομική οντότητα ακολουθεί καθένα από τα βήματα που ορίζονται στα άρθρα 9 έως 15.

2. Εκτός εάν προβλέπεται διαφορετικά στον παρόντα κανονισμό, όταν σε μια ομαδική ή κοινή TLPT συμμετέχουν περισσότερες αρχές TLPT, όπως αναφέρεται στο άρθρο 16 παράγραφος 3 ή 5, οι αναφορές των άρθρων 9 έως 15 στην «αρχή TLPT» νοούνται ως αναφορές στην επικεφαλής αρχή TLPT για την εν λόγω ομαδική ή κοινή TLPT.

Άρθρο 9

Προπαρασκευαστικό στάδιο

1. Μια χρηματοοικονομική οντότητα που προσδιορίζεται σύμφωνα με το άρθρο 26 παράγραφος 8 τρίτο εδάφιο του κανονισμού (ΕΕ) 2022/2554 κινεί διαδικασία TLPT κατόπιν κοινοποίησης από την αρχή TLPT ότι πρόκειται να διενεργηθεί TLPT.

2. Εντός 3 μηνών από την παραλαβή της κοινοποίησης που αναφέρεται στην παράγραφο 1, η χρηματοοικονομική οντότητα υποβάλλει στους διαχειριστές δοκιμής όλες τις ακόλουθες πληροφορίες για την έναρξη της TLPT:

α) καταστατικό χάρτη έργου που περιλαμβάνει σχέδιο έργου υψηλού επιπέδου και περιέχει τις πληροφορίες που ορίζονται στο παράρτημα I·

β) τα στοιχεία επικοινωνίας του επικεφαλής της ομάδας ελέγχου·

γ) πληροφορίες σχετικά με την προβλεπόμενη χρήση εσωτερικών ή εξωτερικών δοκιμαστών ή και των δύο, κατά περίπτωση, όπως περιγράφεται λεπτομερώς στο άρθρο 15·

δ) πληροφορίες σχετικά με τους διαύλους επικοινωνίας που θα χρησιμοποιηθούν κατά τη διενέργεια της TLPT·

ε) την κωδική ονομασία της TLPT.

3. Όταν οι πληροφορίες που αναφέρονται στην παράγραφο 2 στοιχεία α) έως ε) είναι πλήρεις και διασφαλίζουν την καταλληλότητα και την αποτελεσματική διεξαγωγή της TLPT, η αρχή TLPT επικυρώνει τις πληροφορίες έναρξης TLPT της χρηματοοικονομικής οντότητας και ενημερώνει σχετικά τη χρηματοοικονομική οντότητα.

4. Μετά την επικύρωση των πληροφοριών έναρξης TLPT από την αρχή TLPT, η χρηματοοικονομική οντότητα συγκροτεί ομάδα ελέγχου για την υποστήριξη του επικεφαλής της ομάδας ελέγχου στα ακόλουθα καθήκοντά του:

α) προσδιορισμό διαύλων και διαδικασιών επικοινωνίας εντός της ομάδας ελέγχου, με τους δοκιμαστές και τους παρόχους πληροφοριών για απειλές σε όλα τα θέματα που σχετίζονται με την TLPT·

β) ενημέρωση του διοικητικού οργάνου της χρηματοοικονομικής οντότητας σχετικά με την πρόοδο της TLPT και τους συναφείς κινδύνους·

γ) λήψη αποφάσεων βάσει εμπειρογνωσίας καθ' όλη τη διάρκεια της TLPT·

δ) εκτέλεση της TLPT σύμφωνα με τον παρόντα κανονισμό·

ε) επιλογή του παρόχου πληροφοριών για απειλές για την TLPT·

στ) επιλογή των εξωτερικών δοκιμαστών, των εσωτερικών δοκιμαστών ή και των δύο·

ζ) προετοιμασία του εγγράφου προσδιορισμού του πεδίου.

5. Όταν η αρχή TLPT θεωρεί ότι η αρχική σύνθεση της ομάδας ελέγχου και τυχόν επακόλουθες μεταβολές αυτής επαρκούν για την εκτέλεση των καθηκόντων που αναφέρονται στην παράγραφο 4, η αρχή TLPT επικυρώνει την ομάδα ελέγχου και ενημερώνει σχετικά τον επικεφαλής της ομάδας ελέγχου.

6. Εντός 6 μηνών από την παραλαβή της κοινοποίησης από την αρχή TLPT που αναφέρεται στην παράγραφο 1, η χρηματοοικονομική οντότητα υποβάλλει στους διαχειριστές δοκιμής έγγραφο προσδιορισμού του πεδίου που περιέχει όλες τις πληροφορίες που ορίζονται στο παράρτημα II. Το διοικητικό όργανο της χρηματοοικονομικής οντότητας εγκρίνει το έγγραφο προσδιορισμού του πεδίου.

7. Οι χρηματοοικονομικές οντότητες εξετάζουν τα ακόλουθα κριτήρια για τη συμπερίληψη κρίσιμων ή σημαντικών λειτουργιών στο πεδίο της TLPT:

α) την κρισιμότητα ή τη σημασία της λειτουργίας και τις πιθανές επιπτώσεις της στον χρηματοοικονομικό τομέα και στη χρηματοπιστωτική σταθερότητα σε ενωσιακό και εθνικό επίπεδο·

β) τη σημασία της λειτουργίας για τις καθημερινές επιχειρηματικές δραστηριότητες της χρηματοοικονομικής οντότητας·

γ) την ανταλλαξιμότητα της λειτουργίας·

δ) τη διασυνδεσιμότητα με άλλες λειτουργίες·

ε) τη γεωγραφική θέση της λειτουργίας·

στ) την τομεακή εξάρτηση άλλων οντοτήτων από τη λειτουργία·

ζ) εφόσον είναι διαθέσιμες, πληροφορίες για απειλές σχετικά με τη λειτουργία.

8. Η ομάδα ελέγχου κοινοποιεί τις πληροφορίες έναρξης TLPT και το έγγραφο προσδιορισμού του πεδίου στους δοκιμαστές και στους παρόχους πληροφοριών για απειλές μετά τη σύναψη σύμβασης με αυτούς. Η ομάδα ελέγχου ενημερώνει τους δοκιμαστές και τους παρόχους πληροφοριών για απειλές σχετικά με τη διαδικασία δοκιμών που πρέπει να ακολουθηθεί.

9. Η χρηματοοικονομική οντότητα διασφαλίζει ότι η σύναψη σύμβασης ή η ανάθεση σε δοκιμαστές και παρόχους πληροφοριών για απειλές ολοκληρώνεται πριν από την έναρξη του σταδίου των δοκιμών.

10. Πριν από την έναρξη του σταδίου των δοκιμών, η ομάδα ελέγχου διαβουλεύεται με τους διαχειριστές δοκιμής σχετικά με την αξιολόγηση κινδύνων TLPT και τα μέτρα διαχείρισης κινδύνων. Η ομάδα ελέγχου επανεξετάζει την αξιολόγηση κινδύνων ή τα μέτρα διαχείρισης κινδύνων εάν η αρχή TLPT σχηματίσει τη γνώμη ότι δεν αντιμετωπίζουν επαρκώς τους κινδύνους της TLPT.

11. Η ομάδα ελέγχου αξιολογεί τη συμμόρφωση των παρόχων πληροφοριών για απειλές και των δοκιμαστών που εξετάζονται για συμμετοχή στην TLPT με τις απαιτήσεις που ορίζονται στο άρθρο 27 του κανονισμού (ΕΕ) 2022/2554 και με το άρθρο 7 παράγραφος 1 του παρόντος κανονισμού, και τεκμηριώνει το αποτέλεσμα της εν λόγω αξιολόγησης. Η ομάδα ελέγχου επιλέγει τους παρόχους πληροφοριών για απειλές σύμφωνα με την εν λόγω αξιολόγηση και τις πρακτικές διαχείρισης κινδύνων που εφαρμόζει. Πριν από τη σύναψη σύμβασης με τους επιλεγμένους παρόχους πληροφοριών για απειλές και τους εξωτερικούς δοκιμαστές, η ομάδα ελέγχου παρέχει στους διαχειριστές δοκιμής στοιχεία που αποδεικνύουν τη συμμόρφωση των εν λόγω παρόχων πληροφοριών για απειλές και των εν λόγω δοκιμαστών με τις απαιτήσεις που ορίζονται στο άρθρο 27 του κανονισμού (ΕΕ) 2022/2554 και με το άρθρο 7 παράγραφος 1 του παρόντος κανονισμού. Η ομάδα ελέγχου δεν προβαίνει στη σύναψη συμβάσεων με τους επιλεγμένους παρόχους πληροφοριών για απειλές και τους εξωτερικούς δοκιμαστές όταν η αρχή TLPT σχηματίσει τη γνώμη ότι οι επιλεγμένοι πάροχοι πληροφοριών για απειλές και οι εξωτερικοί δοκιμαστές δεν συμμορφώνονται με τις απαιτήσεις που ορίζονται στο άρθρο 27 του κανονισμού (ΕΕ) 2022/2554 ή με τις απαιτήσεις που ορίζονται στο άρθρο 7 παράγραφος 1 του παρόντος κανονισμού ή με πρόσθετες απαιτήσεις που απορρέουν από νομοθεσίες για την εθνική ασφάλεια σύμφωνα με το ενωσιακό δίκαιο, ή όταν η χρηματοοικονομική οντότητα δεν συμμορφώνεται με το άρθρο 7 παράγραφος 2 πρώτο εδάφιο του παρόντος κανονισμού, ή όταν δεν πληρούνται οι περιστάσεις που αναφέρονται στο άρθρο 7 παράγραφος 2 δεύτερο εδάφιο του παρόντος κανονισμού.

12. Όταν το έγγραφο προσδιορισμού του πεδίου είναι πλήρες και διασφαλίζει την εκτέλεση κατάλληλης και αποτελεσματικής TLPT, η αρχή TLPT εγκρίνει το εν λόγω έγγραφο και ενημερώνει σχετικά τον επικεφαλής της ομάδας ελέγχου.

Άρθρο 10

Στάδιο δοκιμών: πληροφορίες για απειλές

1. Μετά την έγκριση του εγγράφου προσδιορισμού του πεδίου από την αρχή TLPT, ο πάροχος πληροφοριών για απειλές αναλύει γενικές και ειδικές ανά τομέα πληροφορίες για απειλές που αφορούν τη χρηματοοικονομική οντότητα. Όταν η αρχή TLPT παρέχει ένα γενικό τοπίο απειλών για τον χρηματοοικονομικό τομέα ενός κράτους μέλους, ο πάροχος πληροφοριών για απειλές μπορεί να χρησιμοποιήσει το εν λόγω τοπίο ως βάση αναφοράς για το εθνικό τοπίο απειλών. Ο πάροχος πληροφοριών για απειλές εντοπίζει κυβερνοαπειλές και υφιστάμενες ή πιθανές ευπάθειες που αφορούν τη χρηματοοικονομική οντότητα. Επιπλέον, ο πάροχος πληροφοριών για απειλές συλλέγει πληροφορίες και αναλύει συγκεκριμένες, αξιοποιήσιμες και συναφείς πληροφορίες για τους στόχους και τις απειλές που αφορούν τη χρηματοοικονομική οντότητα, μεταξύ άλλων μέσω διαβούλευσης με την ομάδα ελέγχου και τους διαχειριστές δοκιμής.

2. Ο πάροχος πληροφοριών για απειλές παρουσιάζει τις σχετικές απειλές και τις στοχευμένες πληροφορίες για απειλές και προτείνει τα απαιτούμενα σενάρια στην ομάδα ελέγχου, στους δοκιμαστές και στους διαχειριστές δοκιμής. Τα προτεινόμενα σενάρια διαφέρουν σε σχέση με τους εντοπισθέντες παράγοντες απειλής και τις συναφείς τακτικές, τεχνικές και διαδικασίες και στοχεύουν κάθε κρίσιμη ή σημαντική λειτουργία που εμπίπτει στο πεδίο της TLPT.

3. Ο επικεφαλής της ομάδας ελέγχου επιλέγει τουλάχιστον τρία σενάρια για τη διενέργεια της TLPT με βάση όλα τα ακόλουθα στοιχεία:

α) τη σύσταση του παρόχου πληροφοριών για απειλές και τον χαρακτήρα κάθε σεναρίου βάσει απειλών·

β) τα στοιχεία που παρέχουν οι διαχειριστές δοκιμής·

γ) τη σκοπιμότητα των προτεινόμενων σεναρίων εκτέλεσης, με βάση την κρίση των δοκιμαστών ως εμπειρογνωμόνων·

δ) το μέγεθος, την πολυπλοκότητα και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της.

4. Μόνο ένα από τα επιλεγμένα σενάρια μπορεί να μη βασίζεται σε απειλές και μπορεί να βασίζεται σε μια μελλοντοστρεφή και δυνητικά πλασματική απειλή με υψηλή προγνωστική, προληπτική, καιροσκοπική ή προβαλλόμενη στο μέλλον αξία, δεδομένων των αναμενόμενων εξελίξεων του τοπίου των απειλών που αφορούν τη χρηματοοικονομική οντότητα.

Όσον αφορά τις ομαδικές TLPT, με την επιφύλαξη των σεναρίων που στοχεύουν άμεσα στις κρίσιμες ή σημαντικές λειτουργίες των χρηματοοικονομικών οντοτήτων που συμμετέχουν στις δοκιμές, τουλάχιστον ένα σενάριο περιλαμβάνει τα σχετικά υποκείμενα συστήματα, διαδικασίες και τεχνολογίες ΤΠΕ του τρίτου παρόχου υπηρεσιών ΤΠΕ που υποστηρίζουν τις κρίσιμες ή σημαντικές λειτουργίες των χρηματοοικονομικών οντοτήτων που εμπίπτουν στο πεδίο των δοκιμών.

Όταν η δοκιμή είναι κοινή TLPT στην οποία συμμετέχει ενδοομιλικός πάροχος υπηρεσιών ΤΠΕ, με την επιφύλαξη των σεναρίων που στοχεύουν άμεσα στις κρίσιμες ή σημαντικές λειτουργίες των χρηματοοικονομικών οντοτήτων που συμμετέχουν στη δοκιμή, τουλάχιστον ένα σενάριο περιλαμβάνει τα σχετικά υποκείμενα συστήματα, διαδικασίες και τεχνολογίες ΤΠΕ του ενδοομιλικού παρόχου υπηρεσιών ΤΠΕ που υποστηρίζουν τις κρίσιμες ή σημαντικές λειτουργίες των χρηματοοικονομικών οντοτήτων που εμπίπτουν στο πεδίο των δοκιμών.

5. Ο πάροχος πληροφοριών για απειλές παρέχει στην ομάδα ελέγχου τη στοχευμένη έκθεση πληροφοριών για απειλές, συμπεριλαμβανομένων των σεναρίων που επιλέχθηκαν σύμφωνα με τις παραγράφους 3 και 4. Η έκθεση πληροφοριών για απειλές περιέχει τις πληροφορίες που ορίζονται στο παράρτημα III.

6. Η ομάδα ελέγχου υποβάλλει τη στοχευμένη έκθεση πληροφοριών για απειλές στον διαχειριστή δοκιμών προς έγκριση. Όταν η στοχευμένη έκθεση πληροφοριών για απειλές είναι πλήρης και διασφαλίζει την εκτέλεση αποτελεσματικής TLPT, η αρχή TLPT εγκρίνει την εν λόγω στοχευμένη έκθεση πληροφοριών για απειλές και ενημερώνει σχετικά τον επικεφαλής της ομάδας ελέγχου.

Άρθρο 11

Στάδιο δοκιμών: δοκιμή κόκκινης ομάδας

1. Μετά την έγκριση της στοχευμένης έκθεσης πληροφοριών για απειλές από την αρχή TLPT, οι δοκιμαστές καταρτίζουν το σχέδιο δοκιμής κόκκινης ομάδας που περιέχει τις πληροφορίες που ορίζονται στο παράρτημα IV. Οι δοκιμαστές χρησιμοποιούν το έγγραφο προσδιορισμού του πεδίου και τη στοχευμένη έκθεση πληροφοριών για απειλές ως βάση για την υλοποίηση των σεναρίων επιθέσεων.

2. Οι δοκιμαστές διαβουλεύονται με την ομάδα ελέγχου, τον πάροχο πληροφοριών για απειλές και τους διαχειριστές δοκιμής σχετικά με το σχέδιο δοκιμής κόκκινης ομάδας, συμπεριλαμβανομένων των ρυθμίσεων επικοινωνίας, διαδικασίας και διαχείρισης έργου, της προετοιμασίας και των περιπτώσεων χρήσης για την ενεργοποίηση πλεονεκτημάτων, καθώς και των συμφωνιών υποβολής εκθέσεων στην ομάδα ελέγχου και στους διαχειριστές δοκιμής.

3. Όταν το σχέδιο δοκιμής κόκκινης ομάδας είναι πλήρες και διασφαλίζει την εκτέλεση αποτελεσματικής TLPT, η ομάδα ελέγχου και η αρχή TLPT εγκρίνουν το σχέδιο δοκιμής κόκκινης ομάδας και η TLPT ενημερώνει σχετικά τον επικεφαλής της ομάδας ελέγχου.

4. Μετά την έγκριση του σχεδίου δοκιμής κόκκινης ομάδας σύμφωνα με την παράγραφο 3, οι δοκιμαστές διενεργούν την TLPT κατά τη διάρκεια του ενεργού σταδίου δοκιμής κόκκινης ομάδας.

5. Η διάρκεια του ενεργού σταδίου δοκιμών κόκκινης ομάδα είναι αναλογική προς το πεδίο της TLPT, προς την κλίμακα, τη δραστηριότητα, την πολυπλοκότητα και τον αριθμό των χρηματοοικονομικών οντοτήτων και των τρίτων ή ενδοομιλικών παρόχων υπηρεσιών ΤΠΕ που συμμετέχουν στην TLPT και, σε κάθε περίπτωση, διαρκεί τουλάχιστον 12 εβδομάδες. Τα σενάρια επιθέσεων μπορούν να εκτελούνται διαδοχικά ή ταυτόχρονα. Η ομάδα ελέγχου, ο πάροχος πληροφοριών για απειλές, οι δοκιμαστές και οι διαχειριστές δοκιμής συμφωνούν την ολοκλήρωση του ενεργού σταδίου δοκιμής κόκκινης ομάδας.

6. Με την επιφύλαξη της διασφάλισης ότι το σχέδιο δοκιμής κόκκινης ομάδας παραμένει πλήρες και επιτρέπει την εκτέλεση αποτελεσματικής TLPT, ο επικεφαλής της ομάδας ελέγχου και οι διαχειριστές δοκιμής εγκρίνουν τυχόν αλλαγές του σχεδίου δοκιμής κόκκινης ομάδας μετά την έγκρισή του, συμπεριλαμβανομένου του χρονοδιαγράμματος, του πεδίου, των στοχευμένων συστημάτων ή των ενδεικτών.

7. Κατά τη διάρκεια του ενεργού σταδίου δοκιμών κόκκινης ομάδας, οι δοκιμαστές αναφέρουν τουλάχιστον σε εβδομαδιαία βάση στην ομάδα ελέγχου και στους διαχειριστές δοκιμής την πρόοδο που έχει σημειωθεί στην TLPT, και ο πάροχος πληροφοριών για απειλές παραμένει διαθέσιμος για διαβούλευση και πρόσθετες πληροφορίες για απειλές, όταν ζητηθεί από την ομάδα ελέγχου.

8. Η ομάδα ελέγχου παρέχει εγκαίρως τα πλεονεκτήματα που έχουν σχεδιαστεί με βάση το σχέδιο δοκιμής κόκκινης ομάδας. Μπορούν να προστίθενται ή να προσαρμόζονται πλεονεκτήματα κατόπιν έγκρισης της ομάδας ελέγχου και των διαχειριστών δοκιμής.

9. Σε περίπτωση που οι δραστηριότητες δοκιμών εντοπιστούν από οποιοδήποτε μέλος του προσωπικού της χρηματοοικονομικής οντότητας ή των οικείων τρίτων παρόχων υπηρεσιών ΤΠΕ ή του ενδοομιλικού παρόχου υπηρεσιών ΤΠΕ, κατά περίπτωση, η ομάδα ελέγχου, σε διαβούλευση με τους δοκιμαστές και με την επιφύλαξη της παραγράφου 10, προτείνει και υποβάλλει προς επικύρωση στους διαχειριστές δοκιμής μέτρα που επιτρέπουν τη συνέχιση της TLPT, διασφαλίζοντας παράλληλα τον απόρρητο χαρακτήρα της TLPT.

10. Σε εξαιρετικές περιστάσεις οι οποίες συνεπάγονται κινδύνους επιπτώσεων στα δεδομένα, ζημία σε περιουσιακά στοιχεία και διαταραχή κρίσιμων ή σημαντικών λειτουργιών, υπηρεσιών ή δραστηριοτήτων της ίδιας της χρηματοοικονομικής οντότητας, των οικείων τρίτων παρόχων υπηρεσιών ΤΠΕ ή των ενδοομιλικών παρόχων υπηρεσιών ΤΠΕ, ή διαταραχές στους αντισυμβαλλομένους της ή στον χρηματοοικονομικό τομέα, ο επικεφαλής της ομάδας ελέγχου μπορεί να αναστείλει την TLPT ή, ως έσχατη λύση, όταν η συνέχιση της TLPT δεν είναι δυνατή με άλλον τρόπο και με την επιφύλαξη προηγούμενης επικύρωσης από την αρχή TLPT, να συνεχίσει την TLPT με τη χρήση περιορισμένης άσκησης δράσεων μωβ ομάδας. Η διάρκεια της περιορισμένης άσκησης δράσεων μωβ ομάδας προσμετράται για τον σκοπό της ελάχιστης διάρκειας των 12 εβδομάδων του ενεργού σταδίου δοκιμών κόκκινης ομάδας που αναφέρεται στην παράγραφο 5.

Άρθρο 12

Στάδιο ολοκλήρωσης

1. Μετά την ολοκλήρωση του ενεργού σταδίου δοκιμών κόκκινης ομάδας, ο επικεφαλής της ομάδας ελέγχου ενημερώνει τη μπλε ομάδα ότι πραγματοποιήθηκε TLPT.

2. Εντός 4 εβδομάδων από την ολοκλήρωση του ενεργού σταδίου δοκιμών κόκκινης ομάδας, οι δοκιμαστές υποβάλλουν στην ομάδα ελέγχου έκθεση δοκιμής κόκκινης ομάδας, η οποία περιέχει τις πληροφορίες που ορίζονται στο παράρτημα V.

3. Η ομάδα ελέγχου διαβιβάζει την έκθεση δοκιμής κόκκινης ομάδας στη μπλε ομάδα και στους διαχειριστές δοκιμής χωρίς αδικαιολόγητη καθυστέρηση.

Κατόπιν αιτήματος των διαχειριστών δοκιμής, η έκθεση που αναφέρεται στο πρώτο εδάφιο δεν περιέχει ευαίσθητες πληροφορίες.

4. Μόλις παραλάβει την έκθεση δοκιμής κόκκινης ομάδας και το αργότερο 10 εβδομάδες μετά την ολοκλήρωση του ενεργού σταδίου δοκιμών κόκκινης ομάδας, η μπλε ομάδα υποβάλλει στην ομάδα ελέγχου έκθεση δοκιμής της μπλε ομάδας, η οποία περιέχει τις πληροφορίες που ορίζονται στο παράρτημα VI. Η ομάδα ελέγχου διαβιβάζει την έκθεση δοκιμής μπλε ομάδας στους δοκιμαστές και στους διαχειριστές δοκιμής χωρίς αδικαιολόγητη καθυστέρηση.

Κατόπιν αιτήματος των διαχειριστών δοκιμής, η έκθεση που αναφέρεται στο πρώτο εδάφιο δεν περιέχει ευαίσθητες πληροφορίες.

5. Το αργότερο 10 εβδομάδες μετά την ολοκλήρωση του ενεργού σταδίου δοκιμών κόκκινης ομάδας, η μπλε ομάδα και οι δοκιμαστές αναπαράγουν τις δράσεις επίθεσης και άμυνας που πραγματοποιήθηκαν κατά τη διάρκεια της TLPT. Η ομάδα ελέγχου διεξάγει επίσης άσκηση δράσεων μωβ ομάδας για θέματα που εντόπισαν από κοινού η μπλε ομάδα και οι δοκιμαστές, με βάση τις ευπάθειες που εντοπίστηκαν κατά τη διάρκεια της δοκιμής και, κατά περίπτωση, για θέματα που δεν ήταν δυνατόν να δοκιμαστούν κατά τη διάρκεια του ενεργού σταδίου δοκιμών κόκκινης ομάδας.

6. Μετά την ολοκλήρωση των ασκήσεων αναπαραγωγής και των δράσεων μωβ ομάδας, η ομάδα ελέγχου, η μπλε ομάδα, οι δοκιμαστές και οι πάροχοι πληροφοριών για απειλές ανταλλάσσουν παρατηρήσεις σχετικά με τη διαδικασία TLPT. Οι διαχειριστές δοκιμής μπορούν να διατυπώνουν παρατηρήσεις.

7. Μόλις η αρχή TLPT κοινοποιήσει στον επικεφαλής της ομάδας ελέγχου ότι, σύμφωνα με αξιολόγησή της, η έκθεση δοκιμής της μπλε ομάδας και η έκθεση δοκιμής της κόκκινης ομάδας περιέχουν τις πληροφορίες που ορίζονται στα παραρτήματα V και VI, η χρηματοοικονομική οντότητα υποβάλλει, εντός 8 εβδομάδων, την περίληψη των σχετικών ευρημάτων της TLPT στην αρχή TLPT, όπως αναφέρεται στο άρθρο 26 παράγραφος 6 του κανονισμού (ΕΕ) 2022/2554, η οποία περιέχει τα στοιχεία που παρατίθενται στο παράρτημα VII, προς έγκριση.

Κατόπιν αιτήματος της αρχής TLPT, η έκθεση που αναφέρεται στο πρώτο εδάφιο δεν περιέχει ευαίσθητες πληροφορίες.

Άρθρο 13

Σχέδιο αποκατάστασης

1. Εντός 8 εβδομάδων από την ενημέρωση που αναφέρεται στο άρθρο 12 παράγραφος 7 του παρόντος κανονισμού, η χρηματοοικονομική οντότητα παρέχει τα σχέδια αποκατάστασης και τα έγγραφα τεκμηρίωσης που αναφέρονται στο άρθρο 26 παράγραφος 6 του κανονισμού (ΕΕ) 2022/2554 στην αρχή TLPT και, εάν είναι διαφορετική, στην αρμόδια αρχή της χρηματοοικονομικής οντότητας.

2. Το σχέδιο αποκατάστασης που αναφέρεται στην παράγραφο 1 περιλαμβάνει, για κάθε εύρημα που προέκυψε στο πλαίσιο της TLPT:

α) περιγραφή των ελλείψεων που εντοπίστηκαν·

β) περιγραφή των προτεινόμενων μέτρων αποκατάστασης και της ιεράρχησης και αναμενόμενης ολοκλήρωσής τους, συμπεριλαμβανομένων, κατά περίπτωση, των μέτρων για τη βελτίωση των ικανοτήτων προσδιορισμού, προστασίας, εντοπισμού και αντιμετώπισης·

γ) ανάλυση βαθύτερων αιτίων·

δ) το προσωπικό ή τις λειτουργίες της χρηματοοικονομικής οντότητας που ευθύνονται για την εφαρμογή των προτεινόμενων μέτρων αποκατάστασης ή βελτιώσεων·

ε) τους κινδύνους που συνδέονται με τη μη εφαρμογή των μέτρων που αναφέρονται στο στοιχείο β) και, κατά περίπτωση, τους κινδύνους που συνδέονται με την εφαρμογή των εν λόγω μέτρων.

Άρθρο 14

Βεβαίωση

1. Η βεβαίωση που αναφέρεται στο άρθρο 26 παράγραφος 7 του κανονισμού (ΕΕ) 2022/2554 περιέχει τις πληροφορίες που ορίζονται στο παράρτημα VIII.

2. Όταν σε μια TLPT συμμετείχαν πολλές αρχές TLPT, η επικεφαλής αρχή TLPT παρέχει τη βεβαίωση που αναφέρεται στο άρθρο 26 παράγραφος 7 του κανονισμού (ΕΕ) 2022/2554 στις ελεγχθείσες χρηματοοικονομικές οντότητες.

Άρθρο 15

Χρήση εσωτερικών δοκιμαστών

1. Οι χρηματοοικονομικές οντότητες θεσπίζουν όλες τις ακόλουθες ρυθμίσεις για τη χρήση εσωτερικών δοκιμαστών:

α) θέσπιση και εφαρμογή πολιτικής για τη διαχείριση των εσωτερικών δοκιμαστών σε μια TLPT·

β) μέτρα που διασφαλίζουν ότι η χρήση εσωτερικών δοκιμαστών για τη διενέργεια μιας TLPT δεν επηρεάζει αρνητικά τις γενικές αμυντικές ικανότητες ή τις ικανότητες ανθεκτικότητας της χρηματοοικονομικής οντότητας όσον αφορά συμβάντα που σχετίζονται με τις ΤΠΕ ούτε επηρεάζει σημαντικά τη διαθεσιμότητα πόρων που διατίθενται για καθήκοντα που σχετίζονται με τις ΤΠΕ κατά τη διενέργεια μιας TLPT·

γ) μέτρα που διασφαλίζουν ότι οι εσωτερικοί δοκιμαστές διαθέτουν επαρκείς πόρους και ικανότητες για τη διενέργεια μιας TLPT.

Η πολιτική που αναφέρεται στο στοιχείο α):

α) περιέχει κριτήρια για την αξιολόγηση της καταλληλότητας, των ικανοτήτων, των πιθανών συγκρούσεων συμφερόντων των εσωτερικών δοκιμαστών και προσδιορίζει τις διαχειριστικές αρμοδιότητες στη διαδικασία δοκιμών·

β) είναι τεκμηριωμένη και επανεξετάζεται περιοδικά·

γ) προβλέπει ότι η εσωτερική ομάδα δοκιμών περιλαμβάνει επικεφαλής των δοκιμών και τουλάχιστον δύο επιπλέον μέλη·

δ) απαιτεί όλα τα μέλη της ομάδας δοκιμών να έχουν απασχοληθεί στη χρηματοοικονομική οντότητα ή σε ενδοομιλικό πάροχο υπηρεσιών ΤΠΕ κατά τους προηγούμενους 12 μήνες·

ε) συμπεριλαμβάνει διατάξεις για την κατάρτιση των εσωτερικών δοκιμαστών σχετικά με τον τρόπο διενέργειας δοκιμών παρείσδυσης και δοκιμών κόκκινης ομάδας.

2. Όταν μια αρχή TLPT εγκρίνει τη χρήση εσωτερικών δοκιμαστών σύμφωνα με το άρθρο 27 παράγραφος 2 στοιχείο α) του κανονισμού (ΕΕ) 2022/2554, η αρχή TLPT λαμβάνει υπόψη τις απαιτήσεις που ορίζονται στο άρθρο 7 παράγραφος 1 του παρόντος κανονισμού.

3. Όταν χρησιμοποιεί εσωτερικούς δοκιμαστές, η χρηματοοικονομική οντότητα διασφαλίζει ότι η εν λόγω χρήση αναφέρεται στα ακόλουθα έγγραφα:

α) τις πληροφορίες έναρξης της δοκιμής που αναφέρονται στο άρθρο 9·

β) την έκθεση δοκιμής κόκκινης ομάδας που αναφέρεται στο άρθρο 12 παράγραφος 2·

γ) την περίληψη των σχετικών ευρημάτων της TLPT, όπως αναφέρεται στο άρθρο 26 παράγραφος 6 του κανονισμού (ΕΕ) 2022/2554.

4. Οι δοκιμαστές που απασχολούνται σε ενδοομιλικό πάροχο υπηρεσιών ΤΠΕ θεωρούνται εσωτερικοί δοκιμαστές της χρηματοοικονομικής οντότητας.

Άρθρο 16

Συνεργασία και αμοιβαία αναγνώριση

1. Για τους σκοπούς της διενέργειας TLPT σε σχέση με χρηματοοικονομική οντότητα που παρέχει υπηρεσίες σε περισσότερα του ενός κράτη μέλη, μεταξύ άλλων μέσω υποκαταστήματος, η οικεία αρχή TLPT:

α) καθορίζει ποιες αρχές TLPT των κρατών μελών υποδοχής συμμετέχουν, λαμβάνοντας υπόψη αν μία ή περισσότερες κρίσιμες ή σημαντικές λειτουργίες λειτουργούν ή χρησιμοποιούνται από κοινού στα κράτη μέλη υποδοχής·

β) ενημερώνει τις αρχές TLPT που προσδιορίζονται σύμφωνα με το στοιχείο α) σχετικά με την απόφαση διενέργειας TLPT στη χρηματοοικονομική οντότητα·

γ) εκτός εάν συμφωνηθεί διαφορετικά από τις αρχές TLPT, η αρχή TLPT της χρηματοοικονομικής οντότητας συντονίζει την TLPT.

Οι αρχές TLPT των κρατών μελών υποδοχής μπορούν, εντός 20 εργάσιμων ημερών από την παραλαβή των πληροφοριών σχετικά με τη μελλοντική διενέργεια TLPT, είτε να εκδηλώσουν το ενδιαφέρον τους να παρακολουθήσουν την TLPT ως παρατηρητές είτε να ορίσουν διαχειριστή δοκιμών να συμμετάσχει στην TLPT. Η επικεφαλής αρχή TLPT παρέχει σε όλες τις αρχές TLPT που ενεργούν ως παρατηρητές στην TLPT το έγγραφο προσδιορισμού του πεδίου, τη συνοπτική έκθεση της δοκιμής, το σχέδιο αποκατάστασης και τη βεβαίωση.

Η επικεφαλής αρχή TLPT συντονίζει όλες τις συμμετέχουσες αρχές TLPT καθ' όλη τη διάρκεια της δοκιμής και λαμβάνει όλες τις αναγκαίες αποφάσεις για την ορθή και αποτελεσματική διεξαγωγή της TLPT. Η επικεφαλής αρχή TLPT μπορεί να ορίσει μέγιστο αριθμό συμμετεχουσών αρχών TLPT, όταν διαφορετικά θα μπορούσε να διακυβευθεί η αποτελεσματική διενέργεια της TLPT.

2. Όταν μια χρηματοοικονομική οντότητα χρησιμοποιεί τον ίδιο ενδοομιλικό πάροχο υπηρεσιών ΤΠΕ με χρηματοοικονομικές οντότητες εγκατεστημένες σε άλλα κράτη μέλη ή ανήκει σε όμιλο και χρησιμοποιεί συστήματα ΤΠΕ από κοινού με χρηματοοικονομικές οντότητες του ίδιου ομίλου που είναι εγκατεστημένες σε άλλα κράτη μέλη, η αρχή TLPT της χρηματοοικονομικής οντότητας επικοινωνεί με τις αρχές TLPT των άλλων χρηματοοικονομικών οντοτήτων που χρησιμοποιούν τον ίδιο ενδοομιλικό πάροχο υπηρεσιών ΤΠΕ ή χρησιμοποιούν από κοινού συστήματα ΤΠΕ ως μέλη του ομίλου και αξιολογεί μαζί τους τη σκοπιμότητα και την καταλληλότητα της διεξαγωγής κοινής TLPT ως προς αυτές. Μια κοινή TLPT προτιμάται έναντι μεμονωμένης TLPT όταν μπορεί να επιφέρει μείωση του κόστους και των πόρων για τις χρηματοοικονομικές οντότητες και για τις αρχές TLPT, υπό την προϋπόθεση ότι δεν θίγεται η ορθότητα και η αποτελεσματικότητα των δοκιμών.

3. Για τους σκοπούς της διενέργειας κοινής TLPT:

α) οι αρχές TLPT των χρηματοοικονομικών οντοτήτων συμφωνούν ποια χρηματοοικονομική οντότητα θα οριστεί για τη διενέργεια της TLPT, λαμβάνοντας υπόψη τη δομή του ομίλου και την αποτελεσματικότητα της δοκιμής·

β) η αρχή TLPT της χρηματοοικονομικής οντότητας που ορίζεται σύμφωνα με το στοιχείο α) συντονίζει την TLPT, εκτός εάν συμφωνηθεί διαφορετικά από τις αρχές TLPT των χρηματοοικονομικών οντοτήτων που συμμετέχουν στην κοινή TLPT·

γ) οι αρχές TLPT των χρηματοοικονομικών οντοτήτων πέραν της ορισθείσας χρηματοοικονομικής οντότητας που θα συντονίσει την κοινή TLPT μπορούν είτε να εκδηλώσουν το ενδιαφέρον τους να παρακολουθήσουν την TLPT ως παρατηρητές είτε να ορίσουν διαχειριστή δοκιμών για την εν λόγω TLPT.

Η επικεφαλής αρχή TLPT συντονίζει όλες τις αρχές TLPT που συμμετέχουν στην κοινή TLPT και λαμβάνει όλες τις αναγκαίες αποφάσεις για την ορθή και αποτελεσματική διεξαγωγή της κοινής TLPT.

4. Όταν μια χρηματοοικονομική οντότητα προτίθεται να διενεργήσει ομαδικές TLPT, όπως αναφέρεται στο άρθρο 26 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2554, με πιθανή συμμετοχή χρηματοοικονομικών οντοτήτων εγκατεστημένων σε άλλα κράτη μέλη, η οικεία αρχή TLPT επικοινωνεί με τις αρχές TLPT των άλλων χρηματοοικονομικών οντοτήτων και αξιολογεί μαζί τους τη σκοπιμότητα και την καταλληλότητα της διενέργειας ομαδικής TLPT ως προς αυτές σύμφωνα με το άρθρο 26 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2554.

5. Για τους σκοπούς της διεξαγωγής ομαδικής TLPT όπως αναφέρεται στο άρθρο 26 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2554:

α) οι αρχές TLPT των χρηματοοικονομικών οντοτήτων συμφωνούν ποια χρηματοοικονομική οντότητα θα οριστεί να διενεργήσει την ομαδική TLPT, λαμβάνοντας υπόψη τις υπηρεσίες ΤΠΕ που παρέχονται από τον τρίτο πάροχο υπηρεσιών ΤΠΕ στις χρηματοοικονομικές οντότητες και την αποτελεσματικότητα της δοκιμής·

β) η αρχή TLPT της χρηματοοικονομικής οντότητας που ορίζεται σύμφωνα με το στοιχείο α) συντονίζει την TLPT, εκτός εάν συμφωνηθεί διαφορετικά από τις αρχές TLPT των χρηματοοικονομικών οντοτήτων που συμμετέχουν στην ομαδική TLPT·

γ) οι αρχές TLPT των χρηματοοικονομικών οντοτήτων πέραν της ορισθείσας χρηματοοικονομικής οντότητας που θα συντονίσει την ομαδική TLPT μπορούν είτε να εκδηλώσουν το ενδιαφέρον τους να παρακολουθήσουν την TLPT ως παρατηρητές είτε να ορίσουν διαχειριστή δοκιμών για την εν λόγω TLPT.

Η επικεφαλής αρχή TLPT συντονίζει όλες τις αρχές TLPT που συμμετέχουν στην ομαδική TLPT και λαμβάνει όλες τις αναγκαίες αποφάσεις για την ορθή και αποτελεσματική διεξαγωγή της ομαδικής TLPT.

6. Όταν, σε σχέση με χρηματοοικονομική οντότητα που υποχρεούται να διενεργεί TLPT, η οικεία αρχή TLPT διαφέρει από την αρμόδια αρχή της, όπως αναφέρεται στο άρθρο 46 του κανονισμού (ΕΕ) 2022/2554, οι εν λόγω αρχές ανταλλάσσουν κάθε σχετική πληροφορία σχετικά με όλα τα θέματα που σχετίζονται με την TLPT για τους σκοπούς της διενέργειας της TLPT ή για την εκτέλεση των καθηκόντων τους σύμφωνα με τον εν λόγω κανονισμό.

Άρθρο 17

Έναρξη ισχύος

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Βρυξέλλες, 13 Φεβρουαρίου 2025.

Για την Επιτροπή
Η Πρόεδρος
Ursula VON DER LEYEN

ΠΑΡΑΡΤΗΜΑ I

Περιεχόμενο του καταστατικού χάρτη του έργου [άρθρο 9 παράγραφος 2 στοιχείο α)]

Στοιχείο	Απαιτούμενες πληροφορίες
Υπεύθυνος για το σχέδιο έργου, δηλαδή ο επικεφαλής της ομάδας ελέγχου	Ονοματεπώνυμο Στοιχεία επικοινωνίας
Δοκιμαστές	☐ εσωτερικοί ☐ εξωτερικοί ☐ και τα δύο
Δίαυλοι επικοινωνίας που επιλέγονται σύμφωνα με το άρθρο 9 παράγραφος 2 στοιχείο δ) και το άρθρο 9 παράγραφος 4 στοιχείο α), μεταξύ άλλων: α) κρυπτογράφηση ηλεκτρονικού ταχυδρομείου που θα χρησιμοποιηθεί β) διαδικτυακές αίθουσες δεδομένων που θα χρησιμοποιηθεί γ) υπηρεσία στιγμιαίων μηνυμάτων που θα χρησιμοποιηθεί	
Κωδική ονομασία για την TLPT	
Εάν υπάρχουν, κρίσιμες ή σημαντικές λειτουργίες της χρηματοοικονομικής οντότητας σε άλλα κράτη μέλη	1. κατάλογος των κρίσιμων ή σημαντικών λειτουργιών που εκτελούνται σε άλλο κράτος μέλος 2. για κάθε κρίσιμη ή σημαντική λειτουργία, αναφορά του κράτους μέλους ή των κρατών μελών όπου εκτελείται
Εάν υπάρχουν, κρίσιμες ή σημαντικές λειτουργίες οι οποίες υποστηρίζονται από τρίτους παρόχους υπηρεσιών ΤΠΕ	3. κατάλογος των κρίσιμων ή σημαντικών λειτουργιών που υποστηρίζονται από τρίτους παρόχους υπηρεσιών ΤΠΕ 4. για κάθε λειτουργία, προσδιορισμός του τρίτου παρόχου υπηρεσιών ΤΠΕ
Αναμενόμενες προθεσμίες για την ολοκλήρωση του:	
1) προπαρασκευαστικού σταδίου σύμφωνα με το άρθρο 9	εεεε-μμ-ηη
2) σταδίου των δοκιμών σύμφωνα με τα άρθρα 10 και 11	εεεε-μμ-ηη
3) σταδίου ολοκλήρωσης σύμφωνα με το άρθρο 12	εεεε-μμ-ηη
4) σχεδίου αποκατάστασης σύμφωνα με το άρθρο 13	εεεε-μμ-ηη

ΠΑΡΑΡΤΗΜΑ ΙΙ

Περιεχόμενο του εγγράφου προσδιορισμού του πεδίου (άρθρο 9 παράγραφος 6)

1. Το έγγραφο προσδιορισμού του πεδίου περιλαμβάνει κατάλογο όλων των κρίσιμων ή σημαντικών λειτουργιών που προσδιορίζονται από τη χρηματοοικονομική οντότητα.

2. Για κάθε κρίσιμη ή σημαντική λειτουργία που προσδιορίζεται, περιλαμβάνονται οι ακόλουθες πληροφορίες:

   α) όταν η κρίσιμη ή σημαντική λειτουργία δεν περιλαμβάνεται στο πεδίο της TLPT, επεξήγηση των λόγων για τους οποίους δεν περιλαμβάνεται·

   β) όταν η κρίσιμη ή σημαντική λειτουργία περιλαμβάνεται στο πεδίο της TLPT:

      i) επεξήγηση των λόγων για τη συμπερίληψή της·

      ii) το/τα προσδιορισμένο/-α σύστημα/-τα ΤΠΕ που υποστηρίζει/-ουν την εν λόγω κρίσιμη ή σημαντική λειτουργία·

      iii) για κάθε σύστημα ΤΠΕ που προσδιορίζεται:

         1. αν έχει ανατεθεί σε τρίτους και, εάν ναι, όνομα του τρίτου παρόχου υπηρεσιών ΤΠΕ·

         2. δικαιοδοσίες στις οποίες χρησιμοποιείται το σύστημα ΤΠΕ·

         3. υψηλού επιπέδου περιγραφή του προκαταρκτικού ενδείκτη ή των προκαταρκτικών ενδεικτών, στην οποία αναφέρεται ποια πτυχή ασφάλειας της εμπιστευτικότητας, της ακεραιότητας, της γνησιότητας ή της διαθεσιμότητας καλύπτεται από κάθε ενδείκτη.

ΠΑΡΑΡΤΗΜΑ III

Περιεχόμενο της στοχευμένης έκθεσης πληροφοριών για απειλές (άρθρο 10 παράγραφος 5)

Η στοχευμένη έκθεση πληροφοριών για απειλές περιέχει πληροφορίες σχετικά με όλα τα ακόλουθα:

1. Το συνολικό πεδίο εφαρμογής της έρευνας στον τομέα των πληροφοριών, το οποίο περιλαμβάνει τουλάχιστον τα ακόλουθα:
   α) κρίσιμες ή σημαντικές λειτουργίες που εμπίπτουν στο πεδίο εφαρμογής·
   β) τη γεωγραφική τους θέση·
   γ) επίσημη γλώσσα της ΕΕ που χρησιμοποιείται·
   δ) σχετικούς τρίτους παρόχους υπηρεσιών ΤΠΕ·
   ε) χρονική περίοδο κατά την οποία πραγματοποιήθηκε η έρευνα.
2. Τη συνολική αξιολόγηση των συγκεκριμένων αξιοποιήσιμων πληροφοριών που μπορεί να βρει κανείς σχετικά με τη χρηματοοικονομική οντότητα, στις οποίες περιλαμβάνονται:
   α) τα ονόματα χρήστη και οι κωδικοί πρόσβασης των εργαζομένων·
   β) οι παρόμοιοι τομείς διαδικτύου που μπορεί να εκληφθούν λανθασμένα ως επίσημοι τομείς της χρηματοοικονομικής οντότητας·
   γ) τεχνική αναγνώριση: ευάλωτο ή εκμεταλλεύσιμο λογισμικό, συστήματα και τεχνολογίες·
   δ) πληροφορίες που αναρτώνται από εργαζομένους στο διαδίκτυο, σχετικά με τη χρηματοοικονομική οντότητα, οι οποίες θα μπορούσαν να χρησιμοποιηθούν για τους σκοπούς επίθεσης·
   ε) πληροφορίες προς πώληση στο σκοτεινό διαδίκτυο·
   στ) κάθε άλλη σχετική πληροφορία που είναι διαθέσιμη στο διαδίκτυο ή σε δημόσια δίκτυα·
   ζ) κατά περίπτωση, πληροφορίες φυσικής στόχευσης, συμπεριλαμβανομένων των τρόπων πρόσβασης στις εγκαταστάσεις της χρηματοοικονομικής οντότητας.
3. Ανάλυση πληροφοριών για απειλές, στην οποία λαμβάνονται υπόψη το γενικό τοπίο απειλών και η ιδιαίτερη κατάσταση της χρηματοοικονομικής οντότητας, η οποία περιλαμβάνει τουλάχιστον:
   α) το γεωπολιτικό περιβάλλον·
   β) το οικονομικό περιβάλλον·
   γ) τεχνολογικές τάσεις και οποιεσδήποτε άλλες τάσεις που σχετίζονται με τις δραστηριότητες στον τομέα των χρηματοοικονομικών υπηρεσιών.
4. Προφίλ απειλής των κακόβουλων παραγόντων (συγκεκριμένο άτομο / συγκεκριμένη ομάδα ή γενική κατηγορία) οι οποίοι ενδέχεται να στοχεύσουν τη χρηματοοικονομική οντότητα, συμπεριλαμβανομένων των συστημάτων της χρηματοοικονομικής οντότητας τα οποία είναι πιθανότερο να παραβιάσουν ή να στοχεύσουν οι κακόβουλοι παράγοντες, των πιθανών κινήτρων, της πρόθεσης και του σκεπτικού της πιθανής στόχευσης και του πιθανού τρόπου λειτουργίας των δραστών.
5. Σενάρια απειλής: τουλάχιστον τρία ολοκληρωμένα σενάρια απειλής για τα προφίλ απειλής που προσδιορίζονται σύμφωνα με το σημείο 4 τα οποία παρουσιάζουν τις υψηλότερες βαθμολογίες σοβαρότητας απειλής. Τα σενάρια απειλής περιγράφουν την ολοκληρωμένη διαδρομή επίθεσης και περιλαμβάνουν τουλάχιστον:
   α) ένα σενάριο που περιλαμβάνει, μεταξύ άλλων, παραβίαση της διαθεσιμότητας υπηρεσιών·
   β) ένα σενάριο που περιλαμβάνει, μεταξύ άλλων, παραβίαση της ακεραιότητας των δεδομένων·
   γ) ένα σενάριο που περιλαμβάνει, μεταξύ άλλων, παραβίαση της εμπιστευτικότητας των πληροφοριών.
6. Κατά περίπτωση, περιγραφή του σεναρίου που δεν βασίζεται σε απειλή, όπως αναφέρεται στο άρθρο 10 παράγραφος 4.

ΠΑΡΑΡΤΗΜΑ IV

Περιεχόμενο του σχεδίου δοκιμής κόκκινης ομάδας (άρθρο 11 παράγραφος 1)

Το σχέδιο δοκιμής κόκκινης ομάδας περιέχει πληροφορίες σχετικά με όλα τα ακόλουθα:

α) τους διαύλους και τις διαδικασίες επικοινωνίας·

β) τις τακτικές, τις τεχνικές και τις διαδικασίες που επιτρέπεται και δεν επιτρέπεται να χρησιμοποιηθούν στην επίθεση, συμπεριλαμβανομένων των δεοντολογικών ορίων για την κοινωνική μηχανική·

γ) τα μέτρα διαχείρισης κινδύνων που πρέπει να τηρούν οι δοκιμαστές·

δ) περιγραφή κάθε σεναρίου, η οποία περιλαμβάνει:

i) τον προσομοιούμενο παράγοντα απειλής·

ii) την πρόθεση, τα κίνητρα και τους στόχους του·

iii) τη λειτουργία ή τις λειτουργίες που στοχεύει και το σύστημα ή τα συστήματα ΤΠΕ που την/τις υποστηρίζουν·

iv) τις πτυχές εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας και γνησιότητας που στοχεύει·

v) τους ενδείκτες·

ε) λεπτομερή περιγραφή κάθε αναμενόμενης διαδρομής επίθεσης, συμπεριλαμβανομένων των προϋποθέσεων και των πιθανών πλεονεκτημάτων που θα πρέπει να παράσχει η ομάδα ελέγχου, καθώς και των προθεσμιών για την παροχή τους και την πιθανή χρήση τους·

στ) τον προγραμματισμό των δραστηριοτήτων κόκκινης ομάδας, συμπεριλαμβανομένου του χρονοδιαγράμματος για την εκτέλεση κάθε σεναρίου, με ελάχιστο διαχωρισμό στις τρεις φάσεις που πραγματοποιεί ο δοκιμαστής κατά τη διάρκεια του σταδίου της δοκιμής, δηλαδή την είσοδο στα συστήματα ΤΠΕ των χρηματοοικονομικών οντοτήτων, την κυκλοφορία εντός των συστημάτων ΤΠΕ και, τελικά, την εκτέλεση δράσεων κατά των στόχων και την έξοδό του από τα συστήματα ΤΠΕ (φάσεις εισόδου, διέλευσης και εξόδου)·

ζ) ιδιαιτερότητες της υποδομής των χρηματοοικονομικών οντοτήτων που πρέπει να λαμβάνονται υπόψη κατά τη διάρκεια των δοκιμών·

η) εάν υπάρχουν, πρόσθετες πληροφορίες ή άλλους πόρους που θα χρειαστούν οι δοκιμαστές για την εκτέλεση των σεναρίων.

ΠΑΡΑΡΤΗΜΑ V

Περιεχόμενο της έκθεσης δοκιμής κόκκινης ομάδας (άρθρο 12 παράγραφος 2)

Η έκθεση δοκιμής κόκκινης ομάδας περιέχει πληροφορίες τουλάχιστον σχετικά με όλα τα ακόλουθα:

α) πληροφορίες σχετικά με την πραγματοποιηθείσα επίθεση, στις οποίες περιλαμβάνονται:

i) οι στοχευμένες κρίσιμες ή σημαντικές λειτουργίες και τα προσδιορισμένα συστήματα, διαδικασίες και τεχνολογίες ΤΠΕ που υποστηρίζουν την κρίσιμη ή σημαντική λειτουργία, όπως προσδιορίζονται στο σχέδιο δοκιμής κόκκινης ομάδας·

ii) περίληψη κάθε σεναρίου·

iii) ενδείκτες που επιτεύχθηκαν και δεν επιτεύχθηκαν·

iv) διαδρομές επίθεσης που ακολουθήθηκαν επιτυχώς και ανεπιτυχώς·

v) τακτικές, τεχνικές και διαδικασίες που χρησιμοποιήθηκαν επιτυχώς και ανεπιτυχώς·

vi) τυχόν αποκλίσεις από το σχέδιο δοκιμής κόκκινης ομάδας·

vii) τυχόν πλεονεκτήματα που δόθηκαν·

β) όλες οι ενέργειες τις οποίες οι δοκιμαστές γνωρίζουν ότι πραγματοποίησε η μπλε ομάδα για την αναπαράσταση της επίθεσης και τον μετριασμό των επιπτώσεών της·

γ) ευπάθειες που ανακαλύφθηκαν και άλλα ευρήματα, όπου περιλαμβάνονται:

i) περιγραφή των ευπαθειών και άλλων ευρημάτων, συμπεριλαμβανομένης της κρισιμότητάς τους·

ii) ανάλυση των βαθύτερων αιτίων των επιτυχημένων επιθέσεων·

iii) συστάσεις για την αποκατάσταση, στις οποίες επισημαίνονται και οι προτεραιότητες αποκατάστασης.

ΠΑΡΑΡΤΗΜΑ VI

Περιεχόμενο της έκθεσης δοκιμής μπλε ομάδας (άρθρο 12 παράγραφος 4)

Η έκθεση δοκιμής μπλε ομάδας περιέχει πληροφορίες τουλάχιστον σχετικά με όλα τα ακόλουθα:

1. για κάθε στάδιο της επίθεσης που περιγράφεται από τους δοκιμαστές στην έκθεση δοκιμής κόκκινης ομάδας:
   α) κατάλογο των ενεργειών της επίθεσης που εντοπίστηκαν·
   β) εγγραφές στο αρχείο καταγραφής που αντιστοιχούν στις εν λόγω ενέργειες που εντοπίστηκαν·
2. αξιολόγηση των ευρημάτων και συστάσεις των δοκιμαστών·
3. αποδεικτικά στοιχεία της επίθεσης από τους δοκιμαστές που συνέλεξε η μπλε ομάδα·
4. ανάλυση από τη μπλε ομάδα των βαθύτερων αιτίων όσον αφορά τις επιτυχημένες επιθέσεις των δοκιμαστών·
5. κατάλογο των διδαγμάτων που αντλήθηκαν και δυνατότητες βελτίωσης που προσδιορίστηκαν·
6. κατάλογο των θεμάτων που πρέπει να εξεταστούν στο πλαίσιο των δράσεων μωβ ομάδας.

ΠΑΡΑΡΤΗΜΑ VII

Στοιχεία της περίληψης των σχετικών ευρημάτων της TLPT, όπως αναφέρεται στο άρθρο 26 παράγραφος 6 του κανονισμού (ΕΕ) 2022/2554

Η περίληψη των δοκιμών περιέχει πληροφορίες τουλάχιστον σχετικά με όλα τα ακόλουθα:

α) τα μέρη που συμμετείχαν·

β) το σχέδιο έργου·

γ) το επικυρωμένο πεδίο εφαρμογής, συμπεριλαμβανομένου του σκεπτικού στο οποίο βασίζεται η συμπερίληψη ή ο αποκλεισμός κρίσιμων ή σημαντικών λειτουργιών και των προσδιορισμένων συστημάτων, διαδικασιών και τεχνολογιών ΤΠΕ που υποστηρίζουν τις κρίσιμες ή σημαντικές λειτουργίες που καλύπτονται από την TLPT·

δ) επιλεγμένα σενάρια και κάθε σημαντική απόκλιση από τη στοχευμένη έκθεση πληροφοριών για απειλές·

ε) εκτελεσθείσες διαδρομές επίθεσης και χρησιμοποιηθείσες τακτικές, τεχνικές και διαδικασίες·

στ) ενδείκτες που καλύφθηκαν και ενδείκτες που δεν καλύφθηκαν·

ζ) τυχόν αποκλίσεις από το σχέδιο δοκιμής κόκκινης ομάδας·

η) τυχόν εντοπισμούς της μπλε ομάδας·

θ) δράσεις μωβ ομάδας κατά το στάδιο της δοκιμής, εάν διενεργήθηκαν, και τις σχετικές συνθήκες·

ι) τυχόν πλεονεκτήματα που χρησιμοποιήθηκαν·

ια) μέτρα διαχείρισης κινδύνων που ελήφθησαν·

ιβ) ευπάθειες που προσδιορίστηκαν και άλλα ευρήματα, συμπεριλαμβανομένης της κρισιμότητάς τους·

ιγ) ανάλυση των βαθύτερων αιτίων των επιτυχημένων επιθέσεων·

ιδ) υψηλού επιπέδου σχέδιο αποκατάστασης, το οποίο συνδέει τις ευπάθειες και άλλα ευρήματα, τα βαθύτερα αίτιά τους και την προτεραιότητα αποκατάστασης·

ιε) διδάγματα που αντλήθηκαν από τις παρατηρήσεις που ελήφθησαν.

ΠΑΡΑΡΤΗΜΑ VIII

Στοιχεία της βεβαίωσης της TLPT, όπως αναφέρεται στο άρθρο 26 παράγραφος 7 του κανονισμού (ΕΕ) 2022/2554

Στη βεβαίωση περιλαμβάνονται τουλάχιστον όλες οι ακόλουθες πληροφορίες:

α) όσον αφορά την TLPT που εκτελέστηκε:

i) η ημερομηνία έναρξης και λήξης της TLPT·

ii) οι κρίσιμες ή σημαντικές λειτουργίες που εμπίπτουν στο πεδίο της δοκιμής·

iii) κατά περίπτωση, πληροφορίες σχετικά με κρίσιμες ή σημαντικές λειτουργίες που εμπίπτουν στο πεδίο της δοκιμής οι οποίες δεν καλύφθηκαν από την TLPT·

iv) κατά περίπτωση, άλλες χρηματοοικονομικές οντότητες που συμμετείχαν στην TLPT·

v) κατά περίπτωση, οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που συμμετείχαν στην TLPT·

vi) όσον αφορά τους δοκιμαστές:

1. αν χρησιμοποιήθηκαν εσωτερικοί δοκιμαστές·

2. αν η χρηματοοικονομική οντότητα έκανε χρήση του άρθρου 5 παράγραφος 3 δεύτερο εδάφιο·

vii) η διάρκεια, σε ημερολογιακές ημέρες, του ενεργού σταδίου δοκιμών κόκκινης ομάδας·

β) εάν στην TLPT ενεπλάκησαν περισσότερες από μια αρχές TLPT, οι άλλες αρχές TLPT και η ιδιότητά τους·

γ) κατάλογος των εγγράφων που εξετάστηκαν από την αρχή TLPT για τους σκοπούς της βεβαίωσης.