Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2024/1774

25.6.2024

ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2024/1774 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 13ης Μαρτίου 2024

για τη συμπλήρωση του κανονισμού (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τα ρυθμιστικά τεχνικά πρότυπα για τον προσδιορισμό των εργαλείων, μεθόδων, διαδικασιών και πολιτικών διαχείρισης κινδύνων ΤΠΕ, καθώς και του απλουστευμένου πλαισίου διαχείρισης κινδύνων ΤΠΕ

(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 15 τέταρτο εδάφιο και το άρθρο 16 παράγραφος 3 τέταρτο εδάφιο,

Εκτιμώντας τα ακόλουθα:

(1) Ο κανονισμός (ΕΕ) 2022/2554 καλύπτει ευρύ φάσμα χρηματοοικονομικών οντοτήτων που διαφέρουν ως προς το μέγεθος, τη δομή, την εσωτερική οργάνωση, καθώς και τη φύση και την πολυπλοκότητα των δραστηριοτήτων τους και συνεπώς έχουν αυξημένα ή μειωμένα στοιχεία πολυπλοκότητας ή κινδύνους. Για να διασφαλιστεί ότι το εν λόγω φάσμα λαμβάνεται δεόντως υπόψη, τυχόν απαιτήσεις όσον αφορά τις πολιτικές, τις διαδικασίες, τα πρωτόκολλα και τα εργαλεία ασφάλειας ΤΠΕ, και όσον αφορά ένα απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ, θα πρέπει να είναι αναλογικές προς το μέγεθος, τη δομή, την εσωτερική οργάνωση, τη φύση και την πολυπλοκότητα των εν λόγω χρηματοοικονομικών οντοτήτων, καθώς και προς τους αντίστοιχους κινδύνους.

(2) Για τον ίδιο λόγο, οι χρηματοοικονομικές οντότητες που υπόκεινται στον κανονισμό (ΕΕ) 2022/2554 θα πρέπει να διαθέτουν ορισμένη ευελιξία ως προς τον τρόπο με τον οποίο συμμορφώνονται με τυχόν απαιτήσεις σχετικά με τις πολιτικές, τις διαδικασίες, τα πρωτόκολλα και τα εργαλεία ασφάλειας ΤΠΕ, καθώς και όσον αφορά τυχόν απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ. Γι' αυτόν τον λόγο, οι χρηματοοικονομικές οντότητες θα πρέπει να μπορούν να χρησιμοποιούν κάθε έγγραφο που ήδη διαθέτουν για να συμμορφώνονται με τυχόν απαιτήσεις τεκμηρίωσης που απορρέουν από τις εν λόγω απαιτήσεις. Συνεπώς, η ανάπτυξη, η τεκμηρίωση και η εφαρμογή συγκεκριμένων πολιτικών ασφάλειας ΤΠΕ θα πρέπει να απαιτούνται μόνο για ορισμένα ουσιώδη στοιχεία, με συνεκτίμηση, μεταξύ άλλων, κορυφαίων πρακτικών και προτύπων του κλάδου. Επιπλέον, για να καλυφθούν ειδικές πτυχές τεχνικής εφαρμογής, είναι αναγκαίο να αναπτυχθούν, να τεκμηριωθούν και να εφαρμοστούν διαδικασίες ασφάλειας ΤΠΕ, μεταξύ άλλων η διαχείριση χωρητικότητας και επιδόσεων, η διαχείριση ευπάθειας και ενημερώσεων κώδικα, η ασφάλεια δεδομένων και συστημάτων και η καταγραφή.

(3) Για να διασφαλιστεί σε βάθος χρόνου η ορθή εφαρμογή των πολιτικών, διαδικασιών, πρωτοκόλλων και εργαλείων ασφάλειας ΤΠΕ που αναφέρονται στον τίτλο II κεφάλαιο I του παρόντος κανονισμού, είναι σημαντικό οι χρηματοοικονομικές οντότητες να αναθέτουν ορθά και να διατηρούν τους ρόλους και τις αρμοδιότητες που σχετίζονται με την ασφάλεια ΤΠΕ, και να καθορίζουν τις συνέπειες της μη συμμόρφωσης με τις πολιτικές ή τις διαδικασίες ασφάλειας ΤΠΕ.

(4) Για να περιοριστεί ο κίνδυνος σύγκρουσης συμφερόντων, οι χρηματοοικονομικές οντότητες θα πρέπει να διασφαλίζουν τον διαχωρισμό των καθηκόντων κατά την ανάθεση ρόλων και αρμοδιοτήτων σχετικά με τις ΤΠΕ.

(5) Για να διασφαλιστεί η ευελιξία και να απλουστευτεί το πλαίσιο ελέγχου των χρηματοοικονομικών οντοτήτων, οι χρηματοοικονομικές οντότητες δεν θα πρέπει να κληθούν να αναπτύξουν ειδικές διατάξεις σχετικά με τις συνέπειες της μη συμμόρφωσης με τις πολιτικές, τις διαδικασίες και τα πρωτόκολλα ασφάλειας ΤΠΕ που αναφέρονται στον τίτλο II κεφάλαιο I του παρόντος κανονισμού, όταν οι εν λόγω διατάξεις προβλέπονται ήδη σε άλλη πολιτική ή διαδικασία.

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

(6) Σε ένα δυναμικό περιβάλλον όπου οι κίνδυνοι ΤΠΕ εξελίσσονται συνεχώς, είναι σημαντικό οι χρηματοοικονομικές οντότητες να αναπτύσσουν δικό τους σύνολο πολιτικών ασφάλειας ΤΠΕ με βάση κορυφαίες πρακτικές και, κατά περίπτωση, πρότυπα όπως ορίζονται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2]).Με αυτόν τον τρόπο, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα μπορούν να παραμένουν ενημερωμένες και προετοιμασμένες σε ένα μεταβαλλόμενο τοπίο.

(7) Για να διασφαλιστεί η ψηφιακή επιχειρησιακή ανθεκτικότητά τους, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα πρέπει, στο πλαίσιο των οικείων πολιτικών, διαδικασιών, πρωτοκόλλων και εργαλείων ασφάλειας ΤΠΕ, να αναπτύσσουν και να εφαρμόζουν πολιτική διαχείρισης πόρων ΤΠΕ, διαδικασίες διαχείρισης χωρητικότητας και επιδόσεων, καθώς και πολιτικές και διαδικασίες για τις λειτουργίες ΤΠΕ. Οι εν λόγω πολιτικές και διαδικασίες είναι απαραίτητες για να διασφαλίζεται η παρακολούθηση της κατάστασης των πόρων ΤΠΕ καθ' όλη τη διάρκεια του κύκλου ζωής τους, ώστε οι εν λόγω πόροι να χρησιμοποιούνται και να διατηρούνται αποτελεσματικά (διαχείριση πόρων ΤΠΕ). Οι εν λόγω πολιτικές και διαδικασίες θα πρέπει επίσης να διασφαλίζουν ότι βελτιστοποιείται η λειτουργία των συστημάτων ΤΠΕ και ότι οι επιδόσεις των συστημάτων ΤΠΕ και της χωρητικότητας ανταποκρίνονται στους καθορισμένους επιχειρηματικούς στόχους και τους στόχους ασφάλειας των πληροφοριών (διαχείριση χωρητικότητας και επιδόσεων). Τέλος, οι εν λόγω πολιτικές και διαδικασίες θα πρέπει να διασφαλίζουν την αποτελεσματική και ομαλή καθημερινή διαχείριση και λειτουργία των συστημάτων ΤΠΕ (λειτουργίες ΤΠΕ), ελαχιστοποιώντας με αυτόν τον τρόπο τον κίνδυνο απώλειας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων. Επομένως, οι εν λόγω πολιτικές και διαδικασίες είναι αναγκαίες για τη διασφάλιση της ασφάλειας των δικτύων, την παροχή επαρκών διασφαλίσεων έναντι εισβολών και κατάχρησης δεδομένων και τη διατήρηση της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων.

(8) Για να διασφαλιστεί η ορθή διαχείριση του κινδύνου των παρωχημένων συστημάτων ΤΠΕ, οι χρηματοοικονομικές οντότητες θα πρέπει να καταγράφουν και να παρακολουθούν τις καταληκτικές ημερομηνίες των υπηρεσιών υποστήριξης από τρίτους σε σχέση με τις ΤΠΕ. Λόγω του δυνητικού αντίκτυπου που μπορεί να έχει η απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων, οι χρηματοοικονομικές οντότητες θα πρέπει να εστιάζονται στους πόρους ή τα συστήματα ΤΠΕ που είναι κρίσιμα για την επιχειρηματική δραστηριότητα κατά την καταγραφή και την παρακολούθηση των εν λόγω καταληκτικών ημερομηνιών.

(9) Οι κρυπτογραφικοί έλεγχοι μπορούν να διασφαλίζουν τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων. Συνεπώς, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα πρέπει να προσδιορίζουν και να εφαρμόζουν τους εν λόγω ελέγχους ακολουθώντας μια προσέγγιση βάσει κινδύνου. Γι' αυτόν τον σκοπό, οι χρηματοοικονομικές οντότητες θα πρέπει να κρυπτογραφούν τα σχετικά δεδομένα σε κατάσταση αποθήκευσης, διαβίβασης ή, κατά περίπτωση, χρήσης, με βάση τα αποτελέσματα μιας διττής διαδικασίας, δηλαδή την κατηγοριοποίηση των δεδομένων και την ολοκληρωμένη αξιολόγηση κινδύνων ΤΠΕ. Δεδομένης της πολυπλοκότητας της κρυπτογράφησης δεδομένων σε κατάσταση χρήσης, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα πρέπει να κρυπτογραφούν τα δεδομένα σε κατάσταση χρήσης μόνον όταν αυτό ενδείκνυται υπό το πρίσμα των αποτελεσμάτων της αξιολόγησης κινδύνων ΤΠΕ. Ωστόσο, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα πρέπει να είναι σε θέση, όταν η κρυπτογράφηση των δεδομένων σε κατάσταση χρήσης δεν είναι εφικτή ή είναι υπερβολικά περίπλοκη, να προστατεύουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των σχετικών δεδομένων μέσω άλλων μέτρων ασφάλειας ΤΠΕ. Δεδομένων των ραγδαίων τεχνολογικών εξελίξεων στον τομέα των τεχνικών κρυπτογράφησης, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα πρέπει να παρακολουθούν τις σχετικές εξελίξεις στην κρυπτανάλυση και να συνεκτιμούν κορυφαίες πρακτικές και πρότυπα. Επομένως, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα πρέπει να ακολουθούν μια ευέλικτη προσέγγιση, βασισμένη στον μετριασμό και την παρακολούθηση των κινδύνων, για την αντιμετώπιση του δυναμικού τοπίου των κρυπτογραφικών απειλών, συμπεριλαμβανομένων των απειλών από κβαντικές εξελίξεις.

(10) Η ασφάλεια των λειτουργιών ΤΠΕ και οι επιχειρησιακές πολιτικές, διαδικασίες, πρωτόκολλα και εργαλεία έχουν ουσιαστική σημασία για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων. Μία βασική πτυχή είναι ο αυστηρός διαχωρισμός των περιβαλλόντων παραγωγής ΤΠΕ από τα περιβάλλοντα όπου συστήματα ΤΠΕ αναπτύσσονται και υποβάλλονται σε δοκιμές ή από άλλα μη παραγωγικά περιβάλλοντα. Ο εν λόγω διαχωρισμός θα πρέπει να χρησιμεύει ως σημαντικό μέτρο ασφάλειας ΤΠΕ έναντι της ακούσιας και μη εξουσιοδοτημένης πρόσβασης, τροποποιήσεων και διαγραφών δεδομένων στο περιβάλλον παραγωγής, οι οποίες θα μπορούσαν να επιφέρουν σημαντικές διαταραχές στις επιχειρηματικές δραστηριότητες των χρηματοοικονομικών οντοτήτων που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού. Ωστόσο, λαμβανομένων υπόψη των υφιστάμενων πρακτικών ανάπτυξης συστημάτων ΤΠΕ, σε εξαιρετικές περιστάσεις, οι χρηματοοικονομικές οντότητες θα πρέπει να μπορούν να διενεργούν δοκιμές σε περιβάλλοντα παραγωγής, υπό την προϋπόθεση ότι αιτιολογούν τις εν λόγω δοκιμές και λαμβάνουν την απαιτούμενη έγκριση.

([2]) Κανονισμός (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Οκτωβρίου 2012, σχετικά με την ευρωπαϊκή τυποποίηση, την τροποποίηση των οδηγιών του Συμβουλίου 89/686/ΕΟΚ και 93/15/ΕΟΚ και των οδηγιών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 94/9/ΕΚ, 94/25/ΕΚ, 95/16/ΕΚ, 97/23/ΕΚ, 98/34/ΕΚ, 2004/22/ΕΚ, 2007/23/ΕΚ, 2009/23/ΕΚ και 2009/105/ΕΚ και την κατάργηση της απόφασης 87/95/ΕΟΚ του Συμβουλίου και της απόφασης αριθ. 1673/2006/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ L 316 της 14.11.2012, σ. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(11) Ο ταχέως εξελισσόμενος χαρακτήρας των τοπίων ΤΠΕ, των ευπαθειών των ΤΠΕ και των κυβερνοαπειλών απαιτεί μια προορατική και ολοκληρωμένη προσέγγιση για τον εντοπισμό, την αξιολόγηση και την αντιμετώπιση των ευπαθειών των ΤΠΕ. Χωρίς μια τέτοια προσέγγιση, οι χρηματοοικονομικές οντότητες, οι πελάτες τους, οι χρήστες ή οι αντισυμβαλλόμενοι ενδέχεται να εκτίθενται σοβαρά σε κινδύνους, γεγονός που θα έθετε σε κίνδυνο την ψηφιακή επιχειρησιακή ανθεκτικότητά τους, την ασφάλεια των δικτύων τους, καθώς και τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων που θα πρέπει να προστατεύουν οι πολιτικές και οι διαδικασίες ασφάλειας ΤΠΕ. Συνεπώς, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα πρέπει να εντοπίζουν και να αποκαθιστούν τις ευπάθειες στο οικείο περιβάλλον ΤΠΕ, και τόσο οι χρηματοοικονομικές οντότητες όσο και οι τρίτοι τους πάροχοι υπηρεσιών ΤΠΕ θα πρέπει να τηρούν ένα συνεκτικό, διαφανές και υπεύθυνο πλαίσιο διαχείρισης ευπαθειών. Για τον ίδιο λόγο, οι χρηματοοικονομικές οντότητες θα πρέπει να παρακολουθούν τις ευπάθειες των ΤΠΕ χρησιμοποιώντας αξιόπιστους πόρους και αυτοματοποιημένα εργαλεία, εξακριβώνοντας ότι οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ διασφαλίζουν την άμεση ανάληψη δράσης για τις ευπάθειες στις παρεχόμενες υπηρεσίες ΤΠΕ.

(12) Η διαχείριση των ενημερώσεων κώδικα θα πρέπει να αποτελεί κρίσιμο μέρος των πολιτικών και διαδικασιών ασφάλειας ΤΠΕ οι οποίες, μέσω των δοκιμών και της ανάπτυξης σε ελεγχόμενο περιβάλλον, αποσκοπούν στην αντιμετώπιση των εντοπιζόμενων ευπαθειών και στην πρόληψη διαταραχών από την εγκατάσταση ενημερώσεων.

(13) Για να διασφαλιστεί η έγκαιρη και διαφανής κοινοποίηση πιθανών απειλών για την ασφάλεια που θα μπορούσαν να επηρεάσουν τη χρηματοοικονομική οντότητα και τα ενδιαφερόμενα μέρη της, οι χρηματοοικονομικές οντότητες θα πρέπει να θεσπίσουν διαδικασίες για την υπεύθυνη γνωστοποίηση των ευπαθειών των ΤΠΕ σε πελάτες, σε αντισυμβαλλομένους και στο κοινό. Κατά τον καθορισμό των εν λόγω διαδικασιών, οι χρηματοοικονομικές οντότητες θα πρέπει να λαμβάνουν υπόψη διάφορους παράγοντες, μεταξύ άλλων τη σοβαρότητα της ευπάθειας, τον δυνητικό αντίκτυπο της εν λόγω ευπάθειας στα ενδιαφερόμενα μέρη και την ετοιμότητα των μέτρων διόρθωσης ή μετριασμού.

(14) Για να καταστεί δυνατή η εκχώρηση δικαιωμάτων πρόσβασης χρηστών, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα πρέπει να θεσπίσουν αυστηρά μέτρα για την εξακρίβωση της μοναδικής ταυτοποίησης των ατόμων και των συστημάτων που θα έχουν πρόσβαση στις πληροφορίες της χρηματοοικονομικής οντότητας. Σε αντίθετη περίπτωση, οι χρηματοοικονομικές οντότητες θα εκτεθούν σε πιθανή μη εξουσιοδοτημένη πρόσβαση, παραβιάσεις δεδομένων και δόλιες δραστηριότητες, θέτοντας συνεπώς σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα ευαίσθητων χρηματοοικονομικών δεδομένων. Ενώ η χρήση γενικών ή κοινών λογαριασμών θα πρέπει κατ' εξαίρεση να επιτρέπεται υπό περιστάσεις που καθορίζονται από τις χρηματοοικονομικές οντότητες, οι χρηματοοικονομικές οντότητες θα πρέπει να διασφαλίζουν ότι τηρείται η λογοδοσία για τις ενέργειες που αναλαμβάνονται μέσω των εν λόγω λογαριασμών. Χωρίς αυτήν τη διασφάλιση, οι δυνητικοί κακόβουλοι χρήστες θα είναι σε θέση να παρεμποδίσουν τη λήψη ερευνητικών και διορθωτικών μέτρων, αφήνοντας τις χρηματοοικονομικές οντότητες ευάλωτες σε κακόβουλες δραστηριότητες που δεν έχουν εντοπιστεί ή σε κυρώσεις μη συμμόρφωσης.

(15) Για τη διαχείριση της ταχείας εξέλιξης σε περιβάλλοντα ΤΠΕ, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα πρέπει να εφαρμόζουν άρτιες πολιτικές και διαδικασίες διαχείρισης έργων ΤΠΕ για τη διατήρηση της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων. Οι εν λόγω πολιτικές και διαδικασίες διαχείρισης έργων ΤΠΕ θα πρέπει να προσδιορίζουν τα στοιχεία που είναι αναγκαία για την επιτυχή διαχείριση έργων ΤΠΕ, συμπεριλαμβανομένων των αλλαγών, της απόκτησης, της συντήρησης και των εξελίξεων των συστημάτων ΤΠΕ της χρηματοοικονομικής οντότητας, ανεξάρτητα από τη μεθοδολογία διαχείρισης έργων ΤΠΕ που έχει επιλέξει η χρηματοοικονομική οντότητα. Στο πλαίσιο των εν λόγω πολιτικών και διαδικασιών, οι χρηματοοικονομικές οντότητες θα πρέπει να υιοθετήσουν πρακτικές και μεθόδους δοκιμών που ανταποκρίνονται στις ανάγκες τους, τηρώντας παράλληλα μια προσέγγιση βάσει κινδύνου και διασφαλίζοντας τη διατήρηση ενός ασφαλούς, αξιόπιστου και ανθεκτικού περιβάλλοντος ΤΠΕ. Για να διασφαλιστεί η ασφαλής υλοποίηση ενός έργου ΤΠΕ, οι χρηματοοικονομικές οντότητες θα πρέπει να διασφαλίζουν ότι το προσωπικό από συγκεκριμένους επιχειρηματικούς τομείς ή ρόλοι που επηρεάζονται ή θίγονται από το εν λόγω έργο ΤΠΕ μπορούν να παρέχουν τις απαραίτητες πληροφορίες και εμπειρογνωσία. Για να διασφαλιστεί η αποτελεσματική εποπτεία, θα πρέπει να υποβάλλονται στο διοικητικό όργανο εκθέσεις για τα έργα ΤΠΕ, ιδίως τα έργα που επηρεάζουν κρίσιμες ή σημαντικές λειτουργίες και για τους σχετικούς κινδύνους τους. Οι χρηματοοικονομικές οντότητες θα πρέπει να προσαρμόζουν τη συχνότητα και λεπτομερή στοιχεία των συστηματικών και υπό εξέλιξη επανεξετάσεων και εκθέσεων στη σημασία και στο μέγεθος των σχετικών έργων ΤΠΕ.

(16) Είναι αναγκαίο να διασφαλιστεί ότι τα πακέτα λογισμικού που αποκτούν και αναπτύσσουν οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού ενσωματώνονται αποτελεσματικά και με ασφάλεια στο υφιστάμενο περιβάλλον ΤΠΕ, σύμφωνα με τους καθιερωμένους επιχειρηματικούς στόχους και τους στόχους ασφάλειας των πληροφοριών. Επομένως, οι χρηματοοικονομικές οντότητες θα πρέπει να αξιολογούν διεξοδικά τα εν λόγω πακέτα λογισμικού. Γι' αυτόν τον σκοπό και για τον εντοπισμό ευπαθειών και πιθανών κενών ασφαλείας τόσο στα πακέτα λογισμικού όσο και στα ευρύτερα συστήματα ΤΠΕ, οι χρηματοοικονομικές οντότητες θα πρέπει να διενεργούν δοκιμές ασφάλειας ΤΠΕ. Για λόγους αξιολόγησης της ακεραιότητας του λογισμικού και για να διασφαλιστεί ότι η χρήση του εν λόγω λογισμικού δεν ενέχει κινδύνους για την ασφάλεια ΤΠΕ, οι χρηματοοικονομικές οντότητες θα πρέπει επίσης να επανεξετάζουν τους πηγαίους κώδικες του λογισμικού που αγοράζεται, συμπεριλαμβανομένου, όπου είναι εφικτό, του ιδιόκτητου λογισμικού που παρέχεται από τρίτους παρόχους υπηρεσιών ΤΠΕ, με χρήση τόσο στατικών όσο και δυναμικών μεθόδων δοκιμών.

(17) Οι αλλαγές, ανεξάρτητα από την κλίμακά τους, φέρουν εγγενείς κινδύνους και ενδέχεται να δημιουργούν σημαντικούς κινδύνους απώλειας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και συνεπώς θα μπορούσαν να οδηγήσουν σε σοβαρές διαταραχές των επιχειρηματικών δραστηριοτήτων. Για την προστασία των χρηματοοικονομικών οντοτήτων από πιθανές ευπάθειες και αδυναμίες ΤΠΕ που θα μπορούσαν να τις εκθέσουν σε σημαντικούς κινδύνους, απαιτείται αυστηρή διαδικασία επαλήθευσης για να επιβεβαιωθεί ότι όλες οι αλλαγές πληρούν τις αναγκαίες απαιτήσεις ασφάλειας ΤΠΕ. Συνεπώς, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα πρέπει, ως βασικό στοιχείο των οικείων πολιτικών και διαδικασιών ασφάλειας ΤΠΕ, να διαθέτουν άρτιες πολιτικές και διαδικασίες διαχείρισης αλλαγών ΤΠΕ. Για να διατηρηθούν η αντικειμενικότητα και η αποτελεσματικότητα της διαδικασίας διαχείρισης αλλαγών ΤΠΕ, να αποφευχθούν οι συγκρούσεις συμφερόντων και να διασφαλιστεί ότι οι αλλαγές ΤΠΕ αξιολογούνται αντικειμενικά, είναι αναγκαίο να διαχωριστούν οι λειτουργίες που ζητούν και εφαρμόζουν τις εν λόγω αλλαγές από τις λειτουργίες που είναι υπεύθυνες για την έγκρισή τους. Για να επιτύχουν αποτελεσματικές μεταβάσεις, ελεγχόμενη εφαρμογή αλλαγών ΤΠΕ και ελάχιστες διαταραχές στη λειτουργία των συστημάτων ΤΠΕ, οι χρηματοοικονομικές οντότητες θα πρέπει να αναθέτουν σαφείς ρόλους και αρμοδιότητες που διασφαλίζουν ότι οι αλλαγές ΤΠΕ σχεδιάζονται και δοκιμάζονται επαρκώς και ότι η ποιότητα είναι διασφαλισμένη. Για να διασφαλιστεί ότι τα συστήματα ΤΠΕ εξακολουθούν να λειτουργούν αποτελεσματικά και να δημιουργηθεί ένα δίχτυ ασφαλείας για τις χρηματοοικονομικές οντότητες, οι χρηματοοικονομικές οντότητες θα πρέπει επίσης να αναπτύξουν και να εφαρμόσουν εφεδρικές διαδικασίες. Οι χρηματοοικονομικές οντότητες θα πρέπει να προσδιορίζουν σαφώς τις εν λόγω εφεδρικές διαδικασίες και να αναθέτουν αρμοδιότητες για τη διασφάλιση ταχείας και αποτελεσματικής απόκρισης σε περίπτωση ανεπιτυχών αλλαγών ΤΠΕ.

(18) Όσον αφορά τον εντοπισμό, τη διαχείριση και την αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα πρέπει να θεσπίσουν πολιτική συμβάντων που σχετίζονται με τις ΤΠΕ, η οποία θα περιλαμβάνει τις συνιστώσες μιας διαδικασίας διαχείρισης συμβάντων που σχετίζονται με τις ΤΠΕ. Γι' αυτόν τον σκοπό, οι χρηματοοικονομικές οντότητες θα πρέπει να προσδιορίζουν όλους τους σχετικούς υπεύθυνους επικοινωνίας εντός και εκτός του οργανισμού που μπορούν να διευκολύνουν τον ορθό συντονισμό και την εφαρμογή των διαφόρων σταδίων στο πλαίσιο της εν λόγω διαδικασίας. Για τη βελτιστοποίηση του εντοπισμού και της αντιμετώπισης συμβάντων που σχετίζονται με τις ΤΠΕ και για τον προσδιορισμό των τάσεων μεταξύ των εν λόγω συμβάντων, τα οποία αποτελούν πολύτιμη πηγή πληροφοριών που δίνουν τη δυνατότητα στις χρηματοοικονομικές οντότητες να εντοπίζουν και να αντιμετωπίζουν με αποτελεσματικότητα τα βαθύτερα αίτια και τα προβλήματα, οι χρηματοοικονομικές οντότητες θα πρέπει ιδίως να αναλύουν λεπτομερώς τα συμβάντα που σχετίζονται με τις ΤΠΕ και θεωρούνται σημαντικότερα, μεταξύ άλλων λόγω της τακτικής επανεμφάνισής τους.

(19) Για να διασφαλιστεί ο έγκαιρος και αποτελεσματικός εντοπισμός ασυνήθιστων δραστηριοτήτων, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα πρέπει να συλλέγουν, να παρακολουθούν και να αναλύουν τις διάφορες πηγές πληροφοριών και να κατανέμουν τους σχετικούς ρόλους και αρμοδιότητες. Όσον αφορά τις εσωτερικές πηγές πληροφόρησης, τα αρχεία καταγραφής αποτελούν εξαιρετικά σημαντική πηγή, αλλά οι χρηματοοικονομικές οντότητες δεν θα πρέπει να βασίζονται μόνο στα αρχεία καταγραφής. Αντ' αυτού, οι χρηματοοικονομικές οντότητες θα πρέπει να εξετάζουν τις ευρύτερες πληροφορίες ώστε να περιλαμβάνουν ό,τι αναφέρεται από άλλες εσωτερικές λειτουργίες, καθώς οι εν λόγω λειτουργίες αποτελούν συχνά πολύτιμη πηγή σχετικών πληροφοριών. Για τον ίδιο λόγο, οι χρηματοοικονομικές οντότητες θα πρέπει να αναλύουν και να παρακολουθούν τις πληροφορίες που συλλέγονται από εξωτερικές πηγές, συμπεριλαμβανομένων των πληροφοριών που παρέχονται από τρίτους παρόχους ΤΠΕ σχετικά με τα συμβάντα που επηρεάζουν τα συστήματα και τα δίκτυά τους, καθώς και άλλες πηγές πληροφοριών που οι χρηματοοικονομικές οντότητες θεωρούν συναφείς. Στον βαθμό που οι πληροφορίες αυτές αποτελούν δεδομένα προσωπικού χαρακτήρα, εφαρμόζεται το δίκαιο της Ένωσης για την προστασία των δεδομένων. Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να περιορίζονται σε ό,τι είναι αναγκαίο για τον εντοπισμό συμβάντων.

(20) Για να διευκολυνθεί ο εντοπισμός συμβάντων που σχετίζονται με τις ΤΠΕ, οι χρηματοοικονομικές οντότητες θα πρέπει να διατηρούν αποδεικτικά στοιχεία για τα εν λόγω συμβάντα. Για να διασφαλιστεί, αφενός, ότι τα εν λόγω αποδεικτικά στοιχεία διατηρούνται για επαρκές χρονικό διάστημα και, αφετέρου, για να αποφευχθεί η υπερβολική κανονιστική επιβάρυνση, οι χρηματοοικονομικές οντότητες θα πρέπει να καθορίζουν την περίοδο διατήρησης λαμβάνοντας υπόψη, μεταξύ άλλων, την κρισιμότητα των δεδομένων και τις απαιτήσεις διατήρησης που απορρέουν από το δίκαιο της Ένωσης.

(21) Για να διασφαλιστεί ο έγκαιρος εντοπισμός συμβάντων που σχετίζονται με τις ΤΠΕ, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα πρέπει να θεωρούν ότι δεν είναι εξαντλητικά τα κριτήρια που προσδιορίζονται για την ενεργοποίηση του εντοπισμού και της αντιμετώπισης συμβάντων που σχετίζονται με τις ΤΠΕ. Επιπλέον, ενώ οι χρηματοοικονομικές οντότητες θα πρέπει να εξετάζουν καθένα από τα εν λόγω κριτήρια, οι περιστάσεις που περιγράφονται στα κριτήρια δεν χρειάζεται να συντρέχουν ταυτόχρονα και η σημασία των επηρεαζόμενων υπηρεσιών ΤΠΕ θα πρέπει να λαμβάνεται δεόντως υπόψη για την ενεργοποίηση των διαδικασιών εντοπισμού και αντιμετώπισης συμβάντων που σχετίζονται με τις ΤΠΕ.

(22) Κατά την ανάπτυξη πολιτικής επιχειρησιακής συνέχειας των ΤΠΕ, οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού θα πρέπει να λαμβάνουν υπόψη τις βασικές συνιστώσες της διαχείρισης κινδύνων ΤΠΕ, συμπεριλαμβανομένων των στρατηγικών διαχείρισης συμβάντων που σχετίζονται με τις ΤΠΕ και επικοινωνίας, της διαδικασίας διαχείρισης αλλαγών ΤΠΕ και των κινδύνων που συνδέονται με τρίτους παρόχους υπηρεσιών ΤΠΕ.

(23) Είναι αναγκαίο να καθοριστεί το σύνολο των σεναρίων που θα πρέπει να λαμβάνουν υπόψη οι χρηματοοικονομικές οντότητες που αναφέρονται στον τίτλο ΙΙ του παρόντος κανονισμού τόσο για την εφαρμογή σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ όσο και για τις δοκιμές των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ. Τα σενάρια αυτά θα πρέπει να χρησιμεύουν ως αφετηρία για τις χρηματοοικονομικές οντότητες, ώστε να αναλύουν τόσο τη συνάφεια και την ευλογοφάνεια κάθε σεναρίου όσο και την ανάγκη ανάπτυξης εναλλακτικών σεναρίων. Οι χρηματοοικονομικές οντότητες θα πρέπει να επικεντρώνονται στα σενάρια στα οποία οι επενδύσεις σε μέτρα ανθεκτικότητας θα μπορούσαν να είναι αποδοτικότερες και αποτελεσματικότερες. Πραγματοποιώντας δοκιμές σε σχέση με τη μετάβαση μεταξύ της κύριας υποδομής ΤΠΕ και τυχόν εφεδρικής χωρητικότητας, αντίγραφα ασφαλείας και εφεδρικές εγκαταστάσεις, τα χρηματοοικονομικά ιδρύματα θα πρέπει να αξιολογούν αν η εν λόγω χωρητικότητα, τα αντίγραφα ασφαλείας και οι εν λόγω εγκαταστάσεις λειτουργούν αποτελεσματικά για επαρκές χρονικό διάστημα και να διασφαλίζουν την αποκατάσταση της κανονικής λειτουργίας της κύριας υποδομής ΤΠΕ σύμφωνα με τους στόχους αποκατάστασης.

(24) Είναι αναγκαίο να καθοριστούν απαιτήσεις για τον λειτουργικό κίνδυνο και ειδικότερα απαιτήσεις για τη διαχείριση έργων και αλλαγών ΤΠΕ και τη διαχείριση της επιχειρησιακής συνέχειας των ΤΠΕ με βάση εκείνες που ισχύουν ήδη για τους κεντρικούς αντισυμβαλλομένους, τα κεντρικά αποθετήρια τίτλων και τους τόπους διαπραγμάτευσης δυνάμει, αντίστοιχα, των κανονισμών (ΕΕ) αριθ. 648/2012 ([3]), (ΕΕ) αριθ. 600/2014 ([4]) και (ΕΕ) αριθ. 909/2014 ([5]) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

(25) Σύμφωνα με το άρθρο 6 παράγραφος 5 του κανονισμού (ΕΕ) 2022/2554, οι χρηματοοικονομικές οντότητες πρέπει να επανεξετάζουν το οικείο πλαίσιο διαχείρισης κινδύνων ΤΠΕ και να υποβάλλουν στην αρμόδια αρχή τους έκθεση σχετικά με την εν λόγω επανεξέταση. Για να μπορούν οι αρμόδιες αρχές να επεξεργάζονται εύκολα τις πληροφορίες που περιέχονται στις εν λόγω εκθέσεις και να διασφαλίζεται η επαρκής διαβίβαση των εν λόγω πληροφοριών, οι χρηματοοικονομικές οντότητες θα πρέπει να υποβάλλουν τις εν λόγω εκθέσεις σε ηλεκτρονική μορφή με δυνατότητα αναζήτησης.

(26) Οι απαιτήσεις για τις χρηματοοικονομικές οντότητες που υπόκεινται στο απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 16 του κανονισμού (ΕΕ) 2022/2554 θα πρέπει να επικεντρώνονται στους βασικούς τομείς και στοιχεία που, υπό το πρίσμα της κλίμακας, του κινδύνου, του μεγέθους και της πολυπλοκότητας των εν λόγω χρηματοοικονομικών οντοτήτων, είναι κατ' ελάχιστον αναγκαία για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της γνησιότητας των δεδομένων και των υπηρεσιών των εν λόγω χρηματοοικονομικών οντοτήτων. Στο πλαίσιο αυτό, οι εν λόγω χρηματοοικονομικές οντότητες θα πρέπει να εφαρμόζουν πλαίσιο εσωτερικής διακυβέρνησης και ελέγχου με σαφείς αρμοδιότητες, ώστε να καθίσταται δυνατή η δημιουργία αποτελεσματικού και άρτιου πλαισίου διαχείρισης κινδύνων. Επιπλέον, για να μειωθεί η διοικητική και επιχειρησιακή επιβάρυνση, οι εν λόγω χρηματοοικονομικές οντότητες θα πρέπει να αναπτύξουν και να τεκμηριώσουν μόνο μία πολιτική, δηλαδή μια πολιτική ασφάλειας των πληροφοριών, η οποία προσδιορίζει τις υψηλού επιπέδου αρχές και τους κανόνες που απαιτούνται για την προστασία της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της γνησιότητας των δεδομένων και των υπηρεσιών των εν λόγω χρηματοοικονομικών οντοτήτων.

(27) Οι διατάξεις του παρόντος κανονισμού αφορούν τον τομέα του πλαισίου διαχείρισης κινδύνων ΤΠΕ, περιγράφοντας λεπτομερώς τα ειδικά στοιχεία που ισχύουν για τις χρηματοοικονομικές οντότητες σύμφωνα με το άρθρο 15 του κανονισμού (ΕΕ) 2022/2554 και σχεδιάζοντας το απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ για τις χρηματοοικονομικές οντότητες που ορίζονται στο άρθρο 16 παράγραφος 1 του εν λόγω κανονισμού. Για να διασφαλιστεί η συνοχή μεταξύ του συνήθους και του απλουστευμένου πλαισίου διαχείρισης κινδύνων ΤΠΕ και δεδομένου ότι οι εν λόγω διατάξεις θα πρέπει να τεθούν σε εφαρμογή ταυτόχρονα, είναι σκόπιμο να συμπεριληφθούν οι εν λόγω διατάξεις σε ενιαία νομοθετική πράξη.

(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 διαβούλευση με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA).

([3]) Κανονισμός (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4ης Ιουλίου 2012, για τα εξωχρηματιστηριακά παράγωγα, τους κεντρικούς αντισυμβαλλομένους και τα αρχεία καταγραφής συναλλαγών (ΕΕ L 201 της 27.7.2012, σ. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) 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).

([5]) Κανονισμός (ΕΕ) αριθ. 909/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με τη βελτίωση του διακανονισμού αξιογράφων στην Ευρωπαϊκή Ένωση και τα κεντρικά αποθετήρια τίτλων και για την τροποποίηση των οδηγιών 98/26/ΕΚ και 2014/65/ΕΕ και του κανονισμού (ΕΕ) αριθ. 236/2012 (ΕΕ L 257 της 28.8.2014, σ. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(29) Η μεικτή επιτροπή των Ευρωπαϊκών Εποπτικών Αρχών που αναφέρεται στο άρθρο 54 του κανονισμού (ΕΕ) αριθ. 1093/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]), στο άρθρο 54 του κανονισμού (ΕΕ) αριθ. 1094/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]) και στο άρθρο 54 του κανονισμού (ΕΕ) αριθ. 1095/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([8]) διενήργησε ανοικτές δημόσιες διαβουλεύσεις σχετικά με τα σχέδια ρυθμιστικών τεχνικών προτύπων στα οποία βασίζεται ο παρών κανονισμός, ανέλυσε το δυνητικό κόστος και τα οφέλη των προτεινόμενων προτύπων και ζήτησε συμβουλές από την ομάδα τραπεζικών συμφεροντούχων που συστάθηκε σύμφωνα με το άρθρο 37 του κανονισμού (ΕΕ) αριθ. 1093/2010, την ομάδα συμφεροντούχων ασφαλίσεων και αντασφαλίσεων και την ομάδα συμφεροντούχων ταμείων επαγγελματικών συνταξιοδοτικών παροχών που συστάθηκαν σύμφωνα με το άρθρο 37 του κανονισμού (ΕΕ) αριθ. 1094/2010 και την ομάδα συμφεροντούχων κινητών αξιών και αγορών που συστάθηκε σύμφωνα με το άρθρο 37 του κανονισμού (ΕΕ) αριθ. 1095/2010.

(30) Στον βαθμό που απαιτείται η επεξεργασία δεδομένων προσωπικού χαρακτήρα για τη συμμόρφωση με τις υποχρεώσεις που ορίζονται στην παρούσα πράξη, θα πρέπει να εφαρμόζονται πλήρως οι κανονισμοί (ΕΕ) 2016/679 ([9]) και (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([10]). Για παράδειγμα, θα πρέπει να τηρείται η αρχή της ελαχιστοποίησης των δεδομένων όταν συλλέγονται δεδομένα προσωπικού χαρακτήρα, ώστε να διασφαλίζεται ο κατάλληλος εντοπισμός συμβάντων. Ζητήθηκε επίσης η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων σχετικά με το σχέδιο κειμένου της παρούσας πράξης,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

ΤΙΤΛΟΣ I

ΓΕΝΙΚΗ ΑΡΧΗ

Άρθρο 1

Συνολικό προφίλ κινδύνου και πολυπλοκότητα

Κατά την ανάπτυξη και την εφαρμογή των πολιτικών, διαδικασιών, πρωτοκόλλων και εργαλείων ασφάλειας ΤΠΕ που αναφέρονται στον τίτλο II και του απλουστευμένου πλαισίου διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στον τίτλο III, λαμβάνονται υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας, καθώς και η φύση, η κλίμακα και τα στοιχεία αυξημένης ή μειωμένης πολυπλοκότητας των υπηρεσιών, δραστηριοτήτων και λειτουργιών της, συμπεριλαμβανομένων των στοιχείων που αφορούν:

α) την κρυπτογράφηση και την κρυπτογραφία,

β) την ασφάλεια λειτουργιών ΤΠΕ,

γ) την ασφάλεια δικτύου,

([6]) 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).

([7]) 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).

([8]) 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).

([9]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) 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).

δ) τη διαχείριση έργων και αλλαγών ΤΠΕ,

ε) τον δυνητικό αντίκτυπο των κινδύνων ΤΠΕ στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων, καθώς και των διαταραχών στη συνέχεια και τη διαθεσιμότητα των δραστηριοτήτων της χρηματοοικονομικής οντότητας.

ΤΙΤΛΟΣ ΙΙ

ΠΕΡΑΙΤΕΡΩ ΕΝΑΡΜΟΝΙΣΗ ΤΩΝ ΕΡΓΑΛΕΙΩΝ, ΜΕΘΟΔΩΝ, ΔΙΑΔΙΚΑΣΙΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΩΝ ΤΠΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΑΡΘΡΟ 15 ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ (ΕΕ) 2022/2554

ΚΕΦΑΛΑΙΟ Ι

Πολιτικές, διαδικασίες, πρωτόκολλα και εργαλεία ασφάλειας ΤΠΕ

Τμήμα 1

Άρθρο 2

Γενικά στοιχεία των πολιτικών, διαδικασιών, πρωτοκόλλων και εργαλείων ασφάλειας ΤΠΕ

1. Οι χρηματοοικονομικές οντότητες διασφαλίζουν ότι οι οικείες πολιτικές ασφάλειας ΤΠΕ, η ασφάλεια των πληροφοριών και οι σχετικές διαδικασίες, τα πρωτόκολλα και τα εργαλεία που αναφέρονται στο άρθρο 9 παράγραφος 2 του κανονισμού (ΕΕ) 2022/2554 ενσωματώνονται στο οικείο πλαίσιο διαχείρισης κινδύνων ΤΠΕ. Οι χρηματοοικονομικές οντότητες θεσπίζουν τις πολιτικές, τις διαδικασίες, τα πρωτόκολλα και τα εργαλεία ασφάλειας ΤΠΕ που ορίζονται στο παρόν κεφάλαιο, τα οποία:

α) διασφαλίζουν την ασφάλεια των δικτύων,

β) περιέχουν διασφαλίσεις έναντι εισβολών και κατάχρησης δεδομένων,

γ) διατηρούν τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, μεταξύ άλλων μέσω της χρήσης τεχνικών κρυπτογράφησης,

δ) εξασφαλίζουν την ακριβή και έγκαιρη διαβίβαση δεδομένων χωρίς σημαντικές διαταραχές και αδικαιολόγητες καθυστερήσεις.

2. Οι χρηματοοικονομικές οντότητες διασφαλίζουν ότι οι πολιτικές ασφάλειας ΤΠΕ που αναφέρονται στην παράγραφο 1:

α) ευθυγραμμίζονται με τους στόχους ασφάλειας των πληροφοριών της χρηματοοικονομικής οντότητας που περιλαμβάνονται στη στρατηγική ψηφιακής επιχειρησιακής ανθεκτικότητας που αναφέρεται στο άρθρο 6 παράγραφος 8 του κανονισμού (ΕΕ) 2022/2554·

β) αναφέρουν την ημερομηνία της επίσημης έγκρισης των πολιτικών ασφάλειας ΤΠΕ από το διοικητικό όργανο·

γ) περιέχουν δείκτες και μέτρα έτσι ώστε:

i) να παρακολουθείται η εφαρμογή των πολιτικών, διαδικασιών, πρωτοκόλλων και εργαλείων ασφάλειας ΤΠΕ·

ii) να καταγράφονται οι εξαιρέσεις από την εν λόγω εφαρμογή·

iii) να διασφαλίζεται ότι η ψηφιακή επιχειρησιακή ανθεκτικότητα της χρηματοοικονομικής οντότητας είναι διασφαλισμένη σε περίπτωση εξαιρέσεων, όπως αναφέρεται στο σημείο ii)·

δ) προσδιορίζουν τις αρμοδιότητες του προσωπικού σε όλα τα επίπεδα για τη διασφάλιση της ασφάλειας ΤΠΕ της χρηματοοικονομικής οντότητας·

ε) προσδιορίζουν τις συνέπειες της μη συμμόρφωσης του προσωπικού της χρηματοοικονομικής οντότητας με τις πολιτικές ασφάλειας ΤΠΕ, όταν δεν προβλέπονται σχετικές διατάξεις σε άλλες πολιτικές της χρηματοοικονομικής οντότητας·

στ) απαριθμούν την τεκμηρίωση που πρέπει να τηρείται·

ζ) προσδιορίζουν τις ρυθμίσεις για τον διαχωρισμό των καθηκόντων στο πλαίσιο του μοντέλου των τριών γραμμών άμυνας ή άλλου εσωτερικού μοντέλου διαχείρισης κινδύνων και ελέγχου, κατά περίπτωση, για την αποφυγή συγκρούσεων συμφερόντων·

η) λαμβάνουν υπόψη κορυφαίες πρακτικές και, κατά περίπτωση, πρότυπα όπως ορίζονται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 1025/2012·

θ) προσδιορίζουν τους ρόλους και τις αρμοδιότητες για την ανάπτυξη, την εφαρμογή και τη συντήρηση πολιτικών, διαδικασιών, πρωτοκόλλων και εργαλείων ασφάλειας ΤΠΕ·

ι) επανεξετάζονται σύμφωνα με το άρθρο 6 παράγραφος 5 του κανονισμού (ΕΕ) 2022/2554·

ια) λαμβάνουν υπόψη τις ουσιώδεις αλλαγές που αφορούν τη χρηματοοικονομική οντότητα, συμπεριλαμβανομένων ουσιωδών αλλαγών των δραστηριοτήτων ή των διαδικασιών της χρηματοοικονομικής οντότητας, του τοπίου των κυβερνοαπειλών ή των εφαρμοστέων νομικών υποχρεώσεων.

Τμήμα 2

Άρθρο 3

Διαχείριση κινδύνων ΤΠΕ

Οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν πολιτικές και διαδικασίες διαχείρισης κινδύνων ΤΠΕ που περιλαμβάνουν όλα τα ακόλουθα:

α) ένδειξη της έγκρισης του επιπέδου ανοχής κινδύνου για τους κινδύνους ΤΠΕ που καθορίζεται σύμφωνα με το άρθρο 6 παράγραφος 8 στοιχείο β) του κανονισμού (ΕΕ) 2022/2554·

β) διαδικασία και μεθοδολογία για τη διενέργεια της αξιολόγησης κινδύνων ΤΠΕ, με τις οποίες προσδιορίζονται:

i) ευπάθειες και απειλές που επηρεάζουν ή ενδέχεται να επηρεάσουν τις υποστηριζόμενες επιχειρηματικές λειτουργίες, τα συστήματα ΤΠΕ και τους πόρους ΤΠΕ που υποστηρίζουν τις εν λόγω λειτουργίες·

ii) οι ποσοτικοί ή ποιοτικοί δείκτες για τη μέτρηση των επιπτώσεων και της πιθανότητας εμφάνισης των ευπαθειών και των απειλών που αναφέρονται στο σημείο i)·

γ) τη διαδικασία για τον προσδιορισμό, την εφαρμογή και την τεκμηρίωση των μέτρων αντιμετώπισης κινδύνων ΤΠΕ για τους κινδύνους ΤΠΕ που εντοπίζονται και αξιολογούνται, συμπεριλαμβανομένου του προσδιορισμού των μέτρων αντιμετώπισης κινδύνων ΤΠΕ που είναι αναγκαία για να περιέλθουν οι κίνδυνοι ΤΠΕ στο επίπεδο ανοχής κινδύνου που αναφέρεται στο στοιχείο α)·

δ) όσον αφορά την εναπομένουσα έκθεση σε κινδύνους ΤΠΕ που εξακολουθούν να υφίστανται μετά την εφαρμογή των μέτρων αντιμετώπισης κινδύνων ΤΠΕ που αναφέρονται στο στοιχείο γ):

i) διατάξεις σχετικά με τον προσδιορισμό της εναπομένουσας έκθεσης στους εν λόγω κινδύνους ΤΠΕ·

ii) την ανάθεση ρόλων και αρμοδιοτήτων σχετικά με:

1) την αποδοχή της εναπομένουσας έκθεσης σε κινδύνους ΤΠΕ που υπερβαίνουν το επίπεδο ανοχής κινδύνου της χρηματοοικονομικής οντότητας που αναφέρεται στο στοιχείο α)·

2) τη διαδικασία επανεξέτασης που αναφέρεται στο σημείο iv) του παρόντος στοιχείου δ)·

iii) την κατάρτιση καταλόγου της αποδεκτής εναπομένουσας έκθεσης σε κινδύνους ΤΠΕ, συμπεριλαμβανομένης αιτιολόγησης της αποδοχής της·

iv) διατάξεις σχετικά με την επανεξέταση της αποδεκτής εναπομένουσας έκθεσης σε κινδύνους ΤΠΕ τουλάχιστον μία φορά ετησίως, μεταξύ άλλων για τα εξής:

1) τον προσδιορισμό τυχόν αλλαγών στην εναπομένουσα έκθεση σε κινδύνους ΤΠΕ·

2) την αξιολόγηση των διαθέσιμων μέτρων μετριασμού·

3) την αξιολόγηση του αν οι λόγοι που δικαιολογούν την αποδοχή της εναπομένουσας έκθεσης σε κινδύνους ΤΠΕ εξακολουθούν να υφίστανται και να ισχύουν κατά την ημερομηνία της επανεξέτασης·

ε) διατάξεις σχετικά με την παρακολούθηση:

i) τυχόν αλλαγών στο τοπίο των κινδύνων ΤΠΕ και των κυβερνοαπειλών·

ii) εσωτερικών και εξωτερικών ευπαθειών και απειλών·

iii) των κινδύνων ΤΠΕ της χρηματοοικονομικής οντότητας που καθιστά δυνατό τον άμεσο εντοπισμό των αλλαγών που θα μπορούσαν να επηρεάσουν το οικείο προφίλ κινδύνου ΤΠΕ·

στ) διατάξεις σχετικά με τη διαδικασία που διασφαλίζει ότι λαμβάνονται υπόψη τυχόν αλλαγές στην επιχειρηματική στρατηγική και στη στρατηγική ψηφιακής επιχειρησιακής ανθεκτικότητας της χρηματοοικονομικής οντότητας.

Για τους σκοπούς της πρώτης παραγράφου στοιχείο γ), η διαδικασία που αναφέρεται στο εν λόγω στοιχείο διασφαλίζει ότι:

α) παρακολουθείται η αποτελεσματικότητα των εφαρμοζόμενων μέτρων αντιμετώπισης κινδύνων ΤΠΕ·

β) αξιολογείται αν έχουν επιτευχθεί τα καθορισμένα επίπεδα ανοχής κινδύνου της χρηματοοικονομικής οντότητας·

γ) αξιολογείται αν η χρηματοοικονομική οντότητα έχει προβεί σε ενέργειες για τη διόρθωση ή τη βελτίωση των εν λόγω μέτρων, όπου είναι αναγκαίο.

Τμήμα 3

Διαχείριση πόρων ΤΠΕ

Άρθρο 4

Πολιτική διαχείρισης πόρων ΤΠΕ

1. Στο πλαίσιο των πολιτικών, των διαδικασιών, των πρωτοκόλλων και των εργαλείων ασφάλειας ΤΠΕ που αναφέρονται στο άρθρο 9 παράγραφος 2 του κανονισμού (ΕΕ) 2022/2554, οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν πολιτική για τη διαχείριση των πόρων ΤΠΕ.

2. Η πολιτική για τη διαχείριση των πόρων ΤΠΕ που αναφέρεται στην παράγραφο 1:

α) καθορίζει την παρακολούθηση και τη διαχείριση του κύκλου ζωής των πόρων ΤΠΕ που προσδιορίζονται και ταξινομούνται σύμφωνα με το άρθρο 8 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554·

β) καθορίζει ότι η χρηματοοικονομική οντότητα τηρεί αρχεία με όλα τα ακόλουθα στοιχεία:

i) το μοναδικό αναγνωριστικό κάθε πόρου ΤΠΕ·

ii) πληροφορίες σχετικά με την τοποθεσία, είτε φυσική είτε λογική, όλων των πόρων ΤΠΕ·

iii) την ταξινόμηση όλων των πόρων ΤΠΕ, όπως αναφέρεται στο άρθρο 8 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2254·

iv) την ταυτότητα των ιδιοκτητών των πόρων ΤΠΕ·

v) τις επιχειρηματικές λειτουργίες ή υπηρεσίες που υποστηρίζονται από τον πόρο ΤΠΕ·

vi) τις απαιτήσεις επιχειρησιακής συνέχειας των ΤΠΕ, συμπεριλαμβανομένων των στόχων για τον χρόνο ανάκαμψης και το σημείο ανάκαμψης·

vii) αν ο πόρος ΤΠΕ μπορεί να είναι ή όντως είναι εκτεθειμένος σε εξωτερικά δίκτυα, συμπεριλαμβανομένου του διαδικτύου·

viii) τις συνδέσεις και τις αλληλεξαρτήσεις μεταξύ των πόρων ΤΠΕ και των επιχειρηματικών λειτουργιών που χρησιμοποιούν κάθε πόρο ΤΠΕ·

ix) κατά περίπτωση, για όλους τους πόρους ΤΠΕ, τις καταληκτικές ημερομηνίες των τακτικών, εκτεταμένων και εξατομικευμένων υπηρεσιών υποστήριξης του τρίτου παρόχου υπηρεσιών ΤΠΕ, μετά τις οποίες οι εν λόγω πόροι ενεργητικού ΤΠΕ δεν υποστηρίζονται πλέον από τον προμηθευτή τους ή από τρίτο πάροχο υπηρεσιών ΤΠΕ·

γ) όσον αφορά τις χρηματοοικονομικές οντότητες πλην των πολύ μικρών επιχειρήσεων, καθορίζει ότι οι εν λόγω χρηματοοικονομικές οντότητες τηρούν αρχεία με τις πληροφορίες που είναι αναγκαίες για τη διενέργεια συγκεκριμένης αξιολόγησης κινδύνων ΤΠΕ σε όλα τα παρωχημένα συστήματα ΤΠΕ που αναφέρονται στο άρθρο 8 παράγραφος 7 του κανονισμού (ΕΕ) 2022/2554.

Άρθρο 5

Διαδικασία διαχείρισης πόρων ΤΠΕ

1. Οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν διαδικασία για τη διαχείριση των πόρων ΤΠΕ.

2. Η διαδικασία για τη διαχείριση των πόρων ΤΠΕ που αναφέρεται στην παράγραφο 1 προσδιορίζει τα κριτήρια για τη διενέργεια της αξιολόγησης κρισιμότητας των πληροφοριακών πόρων και των πόρων ΤΠΕ που υποστηρίζουν επιχειρηματικές λειτουργίες. Η εν λόγω αξιολόγηση λαμβάνει υπόψη:

α) τον κίνδυνο ΤΠΕ που σχετίζεται με τις εν λόγω επιχειρηματικές λειτουργίες και τις εξαρτήσεις τους από τους πληροφοριακούς πόρους ή τους πόρους ΤΠΕ·

β) τον τρόπο με τον οποίο η απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των εν λόγω πληροφοριακών πόρων και πόρων ΤΠΕ θα επηρεάσει τις επιχειρηματικές διαδικασίες και δραστηριότητες των χρηματοοικονομικών οντοτήτων.

Τμήμα 4

Κρυπτογράφηση και κρυπτογραφία

Άρθρο 6

Κρυπτογράφηση και κρυπτογραφικοί έλεγχοι

1. Στο πλαίσιο των πολιτικών, των διαδικασιών, των πρωτοκόλλων και των εργαλείων ασφάλειας ΤΠΕ που αναφέρονται στο άρθρο 9 παράγραφος 2 του κανονισμού (ΕΕ) 2022/2554, οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν πολιτική για την κρυπτογράφηση και τους κρυπτογραφικούς ελέγχους.

2. Οι χρηματοοικονομικές οντότητες σχεδιάζουν την πολιτική κρυπτογράφησης και κρυπτογραφικών ελέγχων που αναφέρεται στην παράγραφο 1 με βάση τα αποτελέσματα εγκεκριμένης κατηγοριοποίησης δεδομένων και αξιολόγησης κινδύνων ΤΠΕ. Η πολιτική αυτή περιλαμβάνει κανόνες για όλα τα ακόλουθα:

α) την κρυπτογράφηση των δεδομένων σε κατάσταση αποθήκευσης και διαβίβασης·

β) την κρυπτογράφηση των δεδομένων σε κατάσταση χρήσης, εφόσον απαιτείται·

γ) την κρυπτογράφηση των συνδέσεων εσωτερικού δικτύου και της κίνησης με εξωτερικούς φορείς·

δ) τη διαχείριση κρυπτογραφικών κλειδιών που αναφέρεται στο άρθρο 7, με καθορισμό κανόνων για την ορθή χρήση, την προστασία και τον κύκλο ζωής των κρυπτογραφικών κλειδιών.

Για τους σκοπούς του στοιχείου β), όταν δεν είναι δυνατή η κρυπτογράφηση των δεδομένων σε κατάσταση χρήσης, οι χρηματοοικονομικές οντότητες επεξεργάζονται τα δεδομένα σε κατάσταση χρήσης σε χωριστό και προστατευόμενο περιβάλλον ή λαμβάνουν ισοδύναμα μέτρα για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας, της γνησιότητας και της διαθεσιμότητας των δεδομένων.

3. Στην πολιτική για την κρυπτογράφηση και τους κρυπτογραφικούς ελέγχους που αναφέρεται στην παράγραφο 1 οι χρηματοοικονομικές οντότητες περιλαμβάνουν κριτήρια για την επιλογή τεχνικών κρυπτογράφησης και πρακτικών χρήσης, λαμβάνοντας υπόψη τις κορυφαίες πρακτικές και τα πρότυπα, όπως ορίζονται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 1025/2012, και την ταξινόμηση των σχετικών πόρων ΤΠΕ που καθορίζεται σύμφωνα με το άρθρο 8 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554. Οι χρηματοοικονομικές οντότητες που δεν είναι σε θέση να τηρούν τις κορυφαίες πρακτικές ή τα πρότυπα ή να χρησιμοποιούν τις πλέον αξιόπιστες τεχνικές θεσπίζουν μέτρα μετριασμού και παρακολούθησης που διασφαλίζουν την ανθεκτικότητα έναντι των κυβερνοαπειλών.

4. Στην πολιτική για την κρυπτογράφηση και τους κρυπτογραφικούς ελέγχους που αναφέρεται στην παράγραφο 1 οι χρηματοοικονομικές οντότητες περιλαμβάνουν διατάξεις για την επικαιροποίηση ή τη μεταβολή, κατά περίπτωση, της κρυπτογραφικής τεχνολογίας με βάση τις εξελίξεις στην κρυπτανάλυση. Με τις εν λόγω επικαιροποιήσεις ή αλλαγές διασφαλίζεται ότι η κρυπτογραφική τεχνολογία παραμένει ανθεκτική έναντι των κυβερνοαπειλών, όπως απαιτείται από το άρθρο 10 παράγραφος 2 στοιχείο α). Οι χρηματοοικονομικές οντότητες που δεν είναι σε θέση να επικαιροποιήσουν ή να αλλάξουν την κρυπτογραφική τεχνολογία θεσπίζουν μέτρα μετριασμού και παρακολούθησης που διασφαλίζουν την ανθεκτικότητα έναντι των κυβερνοαπειλών.

5. Στην πολιτική για την κρυπτογράφηση και τους κρυπτογραφικούς ελέγχους που αναφέρεται στην παράγραφο 1 οι χρηματοοικονομικές οντότητες περιλαμβάνουν απαίτηση για την καταγραφή της θέσπισης μέτρων μετριασμού και παρακολούθησης που θεσπίζονται σύμφωνα με τις παραγράφους 3 και 4 και για την παροχή της σχετικής αιτιολογημένης εξήγησης.

Άρθρο 7

Διαχείριση κρυπτογραφικών κλειδιών

1. Στην πολιτική διαχείρισης κρυπτογραφικών κλειδιών που αναφέρεται στο άρθρο 6 παράγραφος 2 στοιχείο δ) οι χρηματοοικονομικές οντότητες περιλαμβάνουν απαιτήσεις για τη διαχείριση κρυπτογραφικών κλειδιών καθ' όλη τη διάρκεια του κύκλου ζωής τους, συμπεριλαμβανομένης της δημιουργίας, ανανέωσης, αποθήκευσης, υποστήριξης, αρχειοθέτησης, ανάκτησης, διαβίβασης, απόσυρσης, ανάκλησης και καταστροφής των εν λόγω κρυπτογραφικών κλειδιών.

2. Οι χρηματοοικονομικές οντότητες προσδιορίζουν και εφαρμόζουν ελέγχους για την προστασία των κρυπτογραφικών κλειδιών καθ' όλη τη διάρκεια του κύκλου ζωής τους από απώλεια, μη εξουσιοδοτημένη πρόσβαση, γνωστοποίηση και τροποποίηση. Οι χρηματοοικονομικές οντότητες σχεδιάζουν τους εν λόγω ελέγχους με βάση τα αποτελέσματα εγκεκριμένης κατηγοριοποίησης δεδομένων και της αξιολόγησης κινδύνων ΤΠΕ.

3. Οι χρηματοοικονομικές οντότητες αναπτύσσουν και εφαρμόζουν μεθόδους για την αντικατάσταση των κρυπτογραφικών κλειδιών σε περίπτωση απώλειας ή εφόσον τα εν λόγω κλειδιά εκτίθενται σε κίνδυνο ή υφίστανται ζημία.

4. Οι χρηματοοικονομικές οντότητες δημιουργούν και τηρούν μητρώο για όλα τα πιστοποιητικά και τις συσκευές αποθήκευσης πιστοποιητικών τουλάχιστον για τους πόρους ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες. Οι χρηματοοικονομικές οντότητες ενημερώνουν το εν λόγω μητρώο.

5. Οι χρηματοοικονομικές οντότητες διασφαλίζουν την άμεση ανανέωση των πιστοποιητικών πριν από τη λήξη τους.

Τμήμα 5

Ασφάλεια λειτουργιών ΤΠΕ

Άρθρο 8

Πολιτικές και διαδικασίες για τις λειτουργίες ΤΠΕ

1. Στο πλαίσιο των πολιτικών, των διαδικασιών, των πρωτοκόλλων και των εργαλείων ασφάλειας ΤΠΕ που αναφέρονται στο άρθρο 9 παράγραφος 2 του κανονισμού (ΕΕ) 2022/2554, οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν πολιτικές και διαδικασίες για τη διαχείριση των λειτουργιών ΤΠΕ. Οι εν λόγω πολιτικές και διαδικασίες προσδιορίζουν τον τρόπο με τον οποίο οι χρηματοοικονομικές οντότητες λειτουργούν, παρακολουθούν, ελέγχουν και αποκαθιστούν τους οικείους πόρους ΤΠΕ, συμπεριλαμβανομένης της τεκμηρίωσης των λειτουργιών ΤΠΕ.

2. Οι πολιτικές και οι διαδικασίες για τις λειτουργίες ΤΠΕ που αναφέρονται στην παράγραφο 1 περιλαμβάνουν όλα τα ακόλουθα:

α) περιγραφή των πόρων ΤΠΕ, η οποία περιλαμβάνει όλα τα ακόλουθα:

   i) απαιτήσεις σχετικά με την ασφαλή εγκατάσταση, συντήρηση, παραμετροποίηση και απεγκατάσταση συστήματος ΤΠΕ·

   ii) απαιτήσεις σχετικά με τη διαχείριση των πληροφοριακών πόρων που χρησιμοποιούνται από τους πόρους ΤΠΕ, μεταξύ άλλων την επεξεργασία και τον χειρισμό τους, τόσο αυτοματοποιημένα όσο και μη αυτόματα·

   iii) απαιτήσεις σχετικά με τον προσδιορισμό και τον έλεγχο των παρωχημένων συστημάτων ΤΠΕ·

β) ελέγχους και παρακολούθηση των συστημάτων ΤΠΕ, μεταξύ άλλων όλα τα ακόλουθα στοιχεία:

   i) απαιτήσεις δημιουργίας εφεδρικών συστημάτων και αποκατάστασης των συστημάτων ΤΠΕ·

   ii) απαιτήσεις προγραμματισμού, με συνεκτίμηση των αλληλεξαρτήσεων μεταξύ των συστημάτων ΤΠΕ·

   iii) πρωτόκολλα για τη διαδρομή ελέγχου και στοιχεία του αρχείου καταγραφής συστημάτων·

   iv) απαιτήσεις που διασφαλίζουν ότι η διενέργεια εσωτερικού ελέγχου και άλλων δοκιμών ελαχιστοποιεί τις διαταραχές στις επιχειρηματικές δραστηριότητες·

   v) απαιτήσεις σχετικά με τον διαχωρισμό των περιβαλλόντων παραγωγής ΤΠΕ από τα περιβάλλοντα ανάπτυξης και δοκιμών και άλλα μη παραγωγικά περιβάλλοντα·

   vi) απαιτήσεις για τη διεξαγωγή της ανάπτυξης και των δοκιμών σε περιβάλλοντα που διαχωρίζονται από το περιβάλλον παραγωγής·

   vii) απαιτήσεις για τη διεξαγωγή της ανάπτυξης και των δοκιμών σε περιβάλλοντα παραγωγής·

γ) τον χειρισμό σφαλμάτων σε σχέση με τα συστήματα ΤΠΕ, μεταξύ άλλων όλα τα ακόλουθα στοιχεία:

i) διαδικασίες και πρωτόκολλα για τον χειρισμό σφαλμάτων·

ii) επαφές υποστήριξης και παραπομπής, συμπεριλαμβανομένων των εξωτερικών επαφών υποστήριξης σε περίπτωση απρόβλεπτων επιχειρησιακών ή τεχνικών ζητημάτων·

iii) διαδικασίες επανεκκίνησης, κατάργησης και ανάκτησης συστημάτων ΤΠΕ για χρήση σε περίπτωση διαταραχής συστημάτων ΤΠΕ.

Για τους σκοπούς του στοιχείου β) σημείο v), στον διαχωρισμό λαμβάνονται υπόψη όλες οι συνιστώσες του περιβάλλοντος, συμπεριλαμβανομένων λογαριασμών, δεδομένων ή συνδέσεων, όπως απαιτείται από το άρθρο 13 πρώτο εδάφιο στοιχείο α).

Για τους σκοπούς του στοιχείου β) σημείο vii), οι πολιτικές και οι διαδικασίες που αναφέρονται στην παράγραφο 1 προβλέπουν ότι οι περιπτώσεις στις οποίες διενεργούνται δοκιμές σε περιβάλλον παραγωγής προσδιορίζονται σαφώς, αιτιολογούνται, αφορούν περιορισμένο χρονικό διάστημα και εγκρίνονται από τη σχετική υπηρεσία σύμφωνα με το άρθρο 16 παράγραφος 6. Οι χρηματοοικονομικές οντότητες διασφαλίζουν τη διαθεσιμότητα, την εμπιστευτικότητα, την ακεραιότητα και τη γνησιότητα των συστημάτων ΤΠΕ και των δεδομένων παραγωγής κατά τη διάρκεια των δραστηριοτήτων ανάπτυξης και δοκιμών στο περιβάλλον παραγωγής.

Άρθρο 9

Διαχείριση χωρητικότητας και επιδόσεων

1. Στο πλαίσιο των πολιτικών, των διαδικασιών, των πρωτοκόλλων και των εργαλείων ασφάλειας ΤΠΕ που αναφέρονται στο άρθρο 9 παράγραφος 2 του κανονισμού (ΕΕ) 2022/2554, οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν διαδικασίες για τη διαχείριση χωρητικότητας και επιδόσεων για τα ακόλουθα:

α) τον προσδιορισμό των απαιτήσεων χωρητικότητας των οικείων συστημάτων ΤΠΕ·

β) την εφαρμογή βελτιστοποίησης των πόρων·

γ) τις διαδικασίες παρακολούθησης για τη διατήρηση και τη βελτίωση:

i) της διαθεσιμότητας δεδομένων και συστημάτων ΤΠΕ·

ii) της αποδοτικότητας των συστημάτων ΤΠΕ·

iii) της πρόληψης των ελλείψεων χωρητικότητας των συστημάτων ΤΠΕ.

2. Οι διαδικασίες διαχείρισης χωρητικότητας και επιδόσεων που αναφέρονται στην παράγραφο 1 διασφαλίζουν ότι οι χρηματοοικονομικές οντότητες λαμβάνουν μέτρα κατάλληλα για την κάλυψη των ιδιαιτεροτήτων των συστημάτων ΤΠΕ με μακροχρόνιες ή πολύπλοκες διαδικασίες σύναψης συμβάσεων ή έγκρισης ή των συστημάτων ΤΠΕ με υψηλή ένταση πόρων.

Άρθρο 10

Ευπάθεια και διαχείριση ενημερώσεων κώδικα

1. Στο πλαίσιο των πολιτικών, των διαδικασιών, των πρωτοκόλλων και των εργαλείων ασφάλειας ΤΠΕ που αναφέρονται στο άρθρο 9 παράγραφος 2 του κανονισμού (ΕΕ) 2022/2554, οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν διαδικασίες διαχείρισης ευπαθειών.

2. Με τις διαδικασίες διαχείρισης ευπαθειών που αναφέρονται στην παράγραφο 1:

α) εντοπίζονται και επικαιροποιούνται συναφείς και αξιόπιστοι πληροφοριακοί πόροι για την ανάπτυξη και τη διατήρηση ευαισθητοποίησης σχετικά με τις ευπάθειες·

β) διασφαλίζονται οι επιδόσεις της αυτοματοποιημένης σάρωσης και των αυτοματοποιημένων αξιολογήσεων ευπαθειών των πόρων ΤΠΕ, στο πλαίσιο των οποίων η συχνότητα και το αντικείμενο των εν λόγω δραστηριοτήτων είναι ανάλογα με την ταξινόμηση που καθορίζεται σύμφωνα με το άρθρο 8 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 και το συνολικό προφίλ κινδύνου του πόρου ΤΠΕ·

γ) εξακριβώνεται αν:

i) οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ χειρίζονται τις ευπάθειες που σχετίζονται με τις υπηρεσίες ΤΠΕ που παρέχονται στη χρηματοοικονομική οντότητα·

ii) οι εν λόγω πάροχοι υπηρεσιών αναφέρουν εγκαίρως στη χρηματοοικονομική οντότητα τουλάχιστον τις κρίσιμες ευπάθειες και στατιστικά στοιχεία και τάσεις·

δ) παρακολουθείται η χρήση:

i) βιβλιοθηκών τρίτων, συμπεριλαμβανομένων βιβλιοθηκών ανοικτού κώδικα, τις οποίες χρησιμοποιούν υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες·

ii) υπηρεσιών ΤΠΕ που αναπτύσσονται από την ίδια τη χρηματοοικονομική οντότητα ή είναι ειδικά προσαρμοσμένες ή ανεπτυγμένες για τη χρηματοοικονομική οντότητα από τρίτο πάροχο υπηρεσιών ΤΠΕ·

ε) θεσπίζονται διαδικασίες για την υπεύθυνη γνωστοποίηση ευπαθειών σε πελάτες, σε αντισυμβαλλομένους και στο κοινό·

στ) δίνεται προτεραιότητα στην ανάπτυξη ενημερώσεων κώδικα και άλλων μέτρων μετριασμού για την αντιμετώπιση των εντοπιζόμενων ευπαθειών·

ζ) παρακολουθείται και επαληθεύεται η αποκατάσταση των ευπαθειών·

η) απαιτούνται η καταγραφή τυχόν εντοπιζόμενων ευπαθειών που επηρεάζουν τα συστήματα ΤΠΕ και η παρακολούθηση της επίλυσής τους.

Για τους σκοπούς του στοιχείου β), οι χρηματοοικονομικές οντότητες διενεργούν την αυτοματοποιημένη σάρωση και τις αυτοματοποιημένες αξιολογήσεις ευπαθειών των πόρων ΤΠΕ για τους πόρους ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες τουλάχιστον σε εβδομαδιαία βάση.

Για τους σκοπούς του στοιχείου γ), οι χρηματοοικονομικές οντότητες ζητούν από τους τρίτους παρόχους υπηρεσιών ΤΠΕ να διερευνήσουν τις σχετικές ευπάθειες, να προσδιορίσουν τα βαθύτερα αίτια και να εφαρμόσουν κατάλληλα μέτρα μετριασμού.

Για τους σκοπούς του στοιχείου δ), οι χρηματοοικονομικές οντότητες, κατά περίπτωση σε συνεργασία με τον τρίτο πάροχο υπηρεσιών ΤΠΕ, παρακολουθούν την έκδοση και τις πιθανές επικαιροποιήσεις των βιβλιοθηκών τρίτων. Σε περίπτωση έτοιμων προς χρήση (ετοιμοπαράδοτων) πόρων ΤΠΕ ή συνιστωσών πόρων ΤΠΕ που αποκτώνται και χρησιμοποιούνται στη λειτουργία υπηρεσιών ΤΠΕ που δεν υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες, οι χρηματοοικονομικές οντότητες παρακολουθούν τη χρήση, στο μέτρο του δυνατού, βιβλιοθηκών τρίτων, συμπεριλαμβανομένων βιβλιοθηκών ανοικτού κώδικα.

Για τους σκοπούς του στοιχείου στ), οι χρηματοοικονομικές οντότητες λαμβάνουν υπόψη την κρισιμότητα της ευπάθειας, την ταξινόμηση που καθορίζεται σύμφωνα με το άρθρο 8 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 και το προφίλ κινδύνου των πόρων ΤΠΕ που επηρεάζονται από τις εντοπιζόμενες ευπάθειες.

3. Στο πλαίσιο των πολιτικών, των διαδικασιών, των πρωτοκόλλων και των εργαλείων ασφάλειας ΤΠΕ που αναφέρονται στο άρθρο 9 παράγραφος 2 του κανονισμού (ΕΕ) 2022/2554, οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν διαδικασίες διαχείρισης ενημερώσεων κώδικα.

4. Με τις διαδικασίες διαχείρισης ενημερώσεων κώδικα που αναφέρονται στην παράγραφο 3:

α) εντοπίζονται και αξιολογούνται, στο μέτρο του δυνατού, οι διαθέσιμες ενημερώσεις κώδικα και επικαιροποιήσεις λογισμικού και υλισμικού με τη χρήση αυτοματοποιημένων εργαλείων·

β) προσδιορίζονται διαδικασίες έκτακτης ανάγκης για την ενημέρωση κώδικα και την επικαιροποίηση πόρων ΤΠΕ·

γ) υποβάλλονται σε δοκιμές και υλοποιούνται οι ενημερώσεις κώδικα και οι επικαιροποιήσεις λογισμικού και υλισμικού που αναφέρονται στο άρθρο 8 παράγραφος 2 στοιχείο β) σημεία v), vi) και vii)·

δ) ορίζονται προθεσμίες για την εγκατάσταση των ενημερώσεων κώδικα και επικαιροποιήσεων λογισμικού και υλισμικού, καθώς και διαδικασίες παραπομπής συμβάντων σε περίπτωση που οι εν λόγω προθεσμίες δεν μπορούν να τηρηθούν.

Άρθρο 11

Ασφάλεια δεδομένων και συστημάτων

1. Στο πλαίσιο των πολιτικών, των διαδικασιών, των πρωτοκόλλων και των εργαλείων ασφάλειας ΤΠΕ που αναφέρονται στο άρθρο 9 παράγραφος 2 του κανονισμού (ΕΕ) 2022/2554, οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν διαδικασία ασφάλειας δεδομένων και συστημάτων.

2. Στη διαδικασία ασφάλειας δεδομένων και συστημάτων που αναφέρεται στην παράγραφο 1 περιλαμβάνονται όλα τα ακόλουθα στοιχεία που σχετίζονται με την ασφάλεια των δεδομένων και των συστημάτων ΤΠΕ, με βάση την ταξινόμηση που καθορίζεται σύμφωνα με το άρθρο 8 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554:

α) οι περιορισμοί πρόσβασης που αναφέρονται στο άρθρο 21 του παρόντος κανονισμού, οι οποίοι στηρίζουν τις απαιτήσεις προστασίας για κάθε επίπεδο ταξινόμησης·

β) ο προσδιορισμός βάσης αναφοράς ασφαλούς διαμόρφωσης όσον αφορά τους πόρους ΤΠΕ, η οποία ελαχιστοποιεί την έκθεση των εν λόγω πόρων ΤΠΕ σε κυβερνοαπειλές, καθώς και μέτρων για την τακτική επαλήθευση της αποτελεσματικής εφαρμογής των εν λόγω βάσεων αναφοράς·

γ) ο προσδιορισμός μέτρων ασφαλείας ώστε να διασφαλίζεται ότι μόνον εγκεκριμένο λογισμικό είναι εγκατεστημένο σε συστήματα ΤΠΕ και συσκευές τελικού σημείου·

δ) ο προσδιορισμός μέτρων ασφαλείας κατά κακόβουλων κωδικών·

ε) ο προσδιορισμός μέτρων ασφαλείας ώστε να διασφαλίζεται ότι για τη διαβίβαση και την αποθήκευση δεδομένων της χρηματοοικονομικής οντότητας χρησιμοποιούνται μόνον εγκεκριμένα μέσα αποθήκευσης δεδομένων, συστήματα και συσκευές τελικού σημείου·

στ) οι ακόλουθες απαιτήσεις για την εξασφάλιση της χρήσης φορητών συσκευών τελικού σημείου και ιδιωτικών μη φορητών συσκευών τελικού σημείου:

i) η απαίτηση χρήσης διαχειριστικής λύσης για την εξ αποστάσεως διαχείριση των συσκευών τελικού σημείου και την εξ αποστάσεως διαγραφή των δεδομένων της χρηματοοικονομικής οντότητας·

ii) η απαίτηση χρήσης μηχανισμών ασφαλείας που δεν μπορούν να τροποποιηθούν, να καταργηθούν ή να παρακαμφθούν από μέλη του προσωπικού ή τρίτους παρόχους υπηρεσιών ΤΠΕ με μη επιτρεπτό τρόπο·

iii) η απαίτηση χρήσης αφαιρούμενων συσκευών αποθήκευσης δεδομένων μόνον όταν η εναπομένουσα έκθεση σε κινδύνους ΤΠΕ παραμένει εντός του επιπέδου ανοχής κινδύνου της χρηματοοικονομικής οντότητας που αναφέρεται στο άρθρο 3 πρώτο εδάφιο στοιχείο α)·

ζ) η διαδικασία για την ασφαλή διαγραφή δεδομένων, τα οποία υπάρχουν στις εγκαταστάσεις της χρηματοοικονομικής οντότητας ή αποθηκεύονται εξωτερικά, και τα οποία η χρηματοοικονομική οντότητα δεν χρειάζεται πλέον να συλλέγει ή να αποθηκεύει·

η) η διαδικασία για την ασφαλή απόρριψη ή τον παροπλισμό συσκευών αποθήκευσης δεδομένων που βρίσκονται στις εγκαταστάσεις της χρηματοοικονομικής οντότητας ή αποθηκεύονται εξωτερικά και περιέχουν εμπιστευτικές πληροφορίες·

θ) ο προσδιορισμός και η εφαρμογή μέτρων ασφαλείας για την πρόληψη της απώλειας και της διαρροής δεδομένων σε σχέση με τα συστήματα και τις συσκευές τελικού σημείου·

ι) η εφαρμογή μέτρων ασφαλείας για να διασφαλίζεται ότι η τηλεργασία και η χρήση ιδιωτικών συσκευών τελικού σημείου δεν επηρεάζουν αρνητικά την ασφάλεια ΤΠΕ της χρηματοοικονομικής οντότητας·

ια) για πόρους ή υπηρεσίες ΤΠΕ που διαχειρίζεται τρίτος πάροχος υπηρεσιών ΤΠΕ, ο προσδιορισμός και η εφαρμογή απαιτήσεων για τη διατήρηση της ψηφιακής επιχειρησιακής ανθεκτικότητας, σύμφωνα με τα αποτελέσματα της κατηγοριοποίησης δεδομένων και της αξιολόγησης κινδύνων ΤΠΕ.

Για τους σκοπούς του στοιχείου β), η βάση αναφοράς ασφαλούς διαμόρφωσης που αναφέρεται στο εν λόγω σημείο λαμβάνει υπόψη κορυφαίες πρακτικές και κατάλληλες τεχνικές που προβλέπονται στα πρότυπα που ορίζονται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 1025/2012.

Για τους σκοπούς του στοιχείου ια), οι χρηματοοικονομικές οντότητες λαμβάνουν υπόψη τα ακόλουθα:

α) την εφαρμογή των ρυθμίσεων που συνιστά ο προμηθευτής σχετικά με τα στοιχεία που διαχειρίζεται η χρηματοοικονομική οντότητα·

β) σαφή κατανομή των ρόλων και των αρμοδιοτήτων για την ασφάλεια των πληροφοριών μεταξύ της χρηματοοικονομικής οντότητας και του τρίτου παρόχου υπηρεσιών ΤΠΕ, σύμφωνα με την αρχή της πλήρους ευθύνης της χρηματοοικονομικής οντότητας επί του οικείου τρίτου παρόχου υπηρεσιών ΤΠΕ που αναφέρεται στο άρθρο 28 παράγραφος 1 στοιχείο α) του κανονισμού (ΕΕ) 2022/2554, και, για τις χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 28 παράγραφος 2 του εν λόγω κανονισμού, σύμφωνα με την πολιτική της χρηματοοικονομικής οντότητας σχετικά με τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες·

γ) την ανάγκη διασφάλισης και διατήρησης επαρκών ικανοτήτων στο πλαίσιο της χρηματοοικονομικής οντότητας σε σχέση με τη διαχείριση και την ασφάλεια της χρησιμοποιούμενης υπηρεσίας·

δ) τεχνικά και οργανωτικά μέτρα για την ελαχιστοποίηση των κινδύνων που σχετίζονται με την υποδομή που χρησιμοποιείται από τον τρίτο πάροχο υπηρεσιών ΤΠΕ για τις οικείες υπηρεσίες ΤΠΕ, λαμβανομένων υπόψη των κορυφαίων πρακτικών και των προτύπων, όπως ορίζονται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 1025/2012.

Άρθρο 12

Καταγραφή

1. Οι χρηματοοικονομικές οντότητες, στο πλαίσιο των διασφαλίσεων έναντι εισβολών και κατάχρησης δεδομένων, αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν διαδικασίες, πρωτόκολλα και εργαλεία καταγραφής.

2. Οι διαδικασίες, τα πρωτόκολλα και τα εργαλεία καταγραφής που αναφέρονται στην παράγραφο 1 περιλαμβάνουν όλα τα ακόλουθα:

α) τον προσδιορισμό των συμβάντων που πρέπει να καταγράφονται, την περίοδο διατήρησης των αρχείων καταγραφής και τα μέτρα για την ασφάλεια και τον χειρισμό των δεδομένων των αρχείων καταγραφής, με συνεκτίμηση του σκοπού για τον οποίο δημιουργούνται τα αρχεία καταγραφής·

β) την ευθυγράμμιση του βαθμού λεπτομέρειας των αρχείων καταγραφής με τον σκοπό και τη χρήση τους, ώστε να καθίσταται δυνατός ο αποτελεσματικός εντοπισμός ασυνήθιστων δραστηριοτήτων, όπως αναφέρεται στο άρθρο 24·

γ) την απαίτηση καταγραφής συμβάντων που σχετίζονται με όλα τα ακόλουθα:

i) τον έλεγχο λογικής και φυσικής πρόσβασης, όπως αναφέρεται στο άρθρο 21, και τη διαχείριση ταυτότητας·

ii) τη διαχείριση της χωρητικότητας·

iii) τη διαχείριση αλλαγών·

iv) τις λειτουργίες ΤΠΕ, συμπεριλαμβανομένων των δραστηριοτήτων των συστημάτων ΤΠΕ·

v) τις δραστηριότητες κίνησης στο δίκτυο, συμπεριλαμβανομένων των επιδόσεων του δικτύου ΤΠΕ·

δ) μέτρα για την προστασία των συστημάτων καταγραφής και των πληροφοριών των αρχείων καταγραφής από παραποίηση, διαγραφή και μη εξουσιοδοτημένη πρόσβαση σε κατάσταση αποθήκευσης, διαβίβασης και, κατά περίπτωση, χρήσης·

ε) μέτρα για τον εντοπισμό αστοχίας των συστημάτων καταγραφής·

στ) με την επιφύλαξη τυχόν εφαρμοστέων ρυθμιστικών απαιτήσεων βάσει του ενωσιακού ή του εθνικού δικαίου, τον συγχρονισμό των ρολογιών κάθε συστήματος ΤΠΕ της χρηματοοικονομικής οντότητας με βάση τεκμηριωμένη αξιόπιστη πηγή χρόνου αναφοράς.

Για τους σκοπούς του στοιχείου α), οι χρηματοοικονομικές οντότητες καθορίζουν την περίοδο διατήρησης, λαμβάνοντας υπόψη τους επιχειρηματικούς στόχους και τους στόχους ασφάλειας των πληροφοριών, τον λόγο καταχώρισης του συμβάντος στα αρχεία καταγραφής και τα αποτελέσματα της αξιολόγησης κινδύνων ΤΠΕ.

Τμήμα 6

Ασφάλεια δικτύου

Άρθρο 13

Διαχείριση ασφάλειας δικτύου

Οι χρηματοοικονομικές οντότητες, στο πλαίσιο των διασφαλίσεων που εγγυώνται την ασφάλεια των δικτύων έναντι εισβολών και κατάχρησης δεδομένων, αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν πολιτικές, διαδικασίες, πρωτόκολλα και εργαλεία για τη διαχείριση της ασφάλειας δικτύου, μεταξύ άλλων όλα τα ακόλουθα:

α) τον διαχωρισμό και την κατάτμηση των συστημάτων και δικτύων ΤΠΕ, λαμβάνοντας υπόψη:

i) την κρισιμότητα ή τη σημασία της λειτουργίας την οποία υποστηρίζουν τα εν λόγω συστήματα και δίκτυα ΤΠΕ·

ii) την ταξινόμηση που καθορίζεται σύμφωνα με το άρθρο 8 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554·

iii) το συνολικό προφίλ κινδύνου των πόρων ΤΠΕ οι οποίοι χρησιμοποιούν τα εν λόγω συστήματα και δίκτυα ΤΠΕ·

β) την τεκμηρίωση όλων των συνδέσεων δικτύου και των ροών δεδομένων της χρηματοοικονομικής οντότητας·

γ) τη χρήση χωριστού και ειδικού δικτύου για τη διαχείριση των πόρων ΤΠΕ·

δ) τον προσδιορισμό και την εφαρμογή ελέγχων πρόσβασης στο δίκτυο για την πρόληψη και τον εντοπισμό συνδέσεων στο δίκτυο της χρηματοοικονομικής οντότητας από οποιαδήποτε μη εγκεκριμένη συσκευή ή σύστημα, ή τελικό σημείο που δεν πληροί τις απαιτήσεις ασφαλείας της χρηματοοικονομικής οντότητας·

ε) την κρυπτογράφηση συνδέσεων δικτύου που διέρχονται μέσω εταιρικών δικτύων, δημόσιων δικτύων, εγχώριων δικτύων, δικτύων τρίτων και ασύρματων δικτύων, για τα χρησιμοποιούμενα πρωτόκολλα επικοινωνίας, με συνεκτίμηση των αποτελεσμάτων της εγκεκριμένης κατηγοριοποίησης δεδομένων, των αποτελεσμάτων της αξιολόγησης κινδύνων ΤΠΕ και της κρυπτογράφησης των συνδέσεων δικτύου που αναφέρονται στο άρθρο 6 παράγραφος 2·

στ) τον σχεδιασμό δικτύων σύμφωνα με τις απαιτήσεις ασφάλειας ΤΠΕ που έχει θεσπίσει η χρηματοοικονομική οντότητα, με συνεκτίμηση κορυφαίων πρακτικών για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας του δικτύου·

ζ) τη διασφάλιση της κίνησης στο δίκτυο μεταξύ των εσωτερικών δικτύων και του διαδικτύου και άλλων εξωτερικών συνδέσεων·

η) τον προσδιορισμό των ρόλων και των αρμοδιοτήτων και των βημάτων για τον καθορισμό, την εφαρμογή, την έγκριση, την αλλαγή και την επανεξέταση των κανόνων του τείχους προστασίας και των φίλτρων σύνδεσης·

θ) τη διενέργεια επανεξετάσεων της αρχιτεκτονικής δικτύου και του σχεδιασμού ασφάλειας δικτύου μία φορά ετησίως και περιοδικά για τις πολύ μικρές επιχειρήσεις, για τον εντοπισμό πιθανών ευπαθειών·

ι) τα μέτρα για την προσωρινή απομόνωση, κατά περίπτωση, των υποδικτύων και των στοιχείων και συσκευών δικτύου·

ια) την εφαρμογή βάσης αναφοράς ασφαλούς διαμόρφωσης όλων των στοιχείων του δικτύου και τη θωράκιση του δικτύου και των συσκευών δικτύου σύμφωνα με τυχόν οδηγίες του προμηθευτή, κατά περίπτωση, με πρότυπα, όπως ορίζονται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 1025/2012, και με κορυφαίες πρακτικές·

ιβ) τις διαδικασίες περιορισμού, κλειδώματος και τερματισμού λειτουργίας συστημάτων και των απομακρυσμένων περιόδων λειτουργίας μετά από συγκεκριμένη περίοδο αδράνειας·

ιγ) όσον αφορά τις συμφωνίες υπηρεσιών δικτύου:

i) τον προσδιορισμό και την εξειδίκευση των μέτρων ασφάλειας ΤΠΕ και πληροφοριών, των επιπέδων υπηρεσιών και των απαιτήσεων διαχείρισης όλων των υπηρεσιών δικτύου·

ii) αν οι εν λόγω υπηρεσίες παρέχονται από ενδοομιλικό πάροχο υπηρεσιών ΤΠΕ ή από τρίτους παρόχους υπηρεσιών ΤΠΕ.

Για τους σκοπούς του στοιχείου η), οι χρηματοοικονομικές οντότητες διενεργούν την επανεξέταση των κανόνων του τείχους προστασίας και των φίλτρων σύνδεσης σε τακτική βάση σύμφωνα με την ταξινόμηση που καθορίζεται σύμφωνα με το άρθρο 8 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 και το συνολικό προφίλ κινδύνου των σχετικών συστημάτων ΤΠΕ. Για τα συστήματα ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες, οι χρηματοοικονομικές οντότητες επαληθεύουν την επάρκεια των υφιστάμενων κανόνων του τείχους προστασίας και των φίλτρων σύνδεσης τουλάχιστον κάθε 6 μήνες.

Άρθρο 14

Διασφάλιση των πληροφοριών σε κατάσταση διαβίβασης

1. Στο πλαίσιο των διασφαλίσεων για τη διατήρηση της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων, οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν πολιτικές, διαδικασίες, πρωτόκολλα και εργαλεία για την προστασία των πληροφοριών σε κατάσταση διαβίβασης. Ειδικότερα, οι χρηματοοικονομικές οντότητες διασφαλίζουν όλα τα ακόλουθα:

α) τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων κατά τη μετάδοση στο δίκτυο, καθώς και τη θέσπιση διαδικασιών για την αξιολόγηση της συμμόρφωσης με τις εν λόγω απαιτήσεις·

β) την πρόληψη και τον εντοπισμό των διαρροών δεδομένων και την ασφαλή διαβίβαση πληροφοριών μεταξύ της χρηματοοικονομικής οντότητας και εξωτερικών μερών·

γ) την εφαρμογή, την τεκμηρίωση και την τακτική επανεξέταση των απαιτήσεων σχετικά με τις συμφωνίες εμπιστευτικότητας ή μη γνωστοποίησης που αντικατοπτρίζουν τις ανάγκες της χρηματοοικονομικής οντότητας για την προστασία των πληροφοριών για το προσωπικό τόσο της ίδιας όσο και τρίτων.

2. Οι χρηματοοικονομικές οντότητες σχεδιάζουν τις πολιτικές, τις διαδικασίες, τα πρωτόκολλα και τα εργαλεία για την προστασία των πληροφοριών σε κατάσταση διαβίβασης που αναφέρονται στην παράγραφο 1 με βάση τα αποτελέσματα της εγκεκριμένης κατηγοριοποίησης δεδομένων και της αξιολόγησης κινδύνων ΤΠΕ.

Τμήμα 7

Διαχείριση έργων και αλλαγών ΤΠΕ

Άρθρο 15

Διαχείριση έργων ΤΠΕ

1. Στο πλαίσιο των διασφαλίσεων για τη διατήρηση της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων, οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν πολιτική διαχείρισης έργων ΤΠΕ.

2. Η πολιτική διαχείρισης έργων ΤΠΕ που αναφέρεται στην παράγραφο 1 προσδιορίζει τα στοιχεία που διασφαλίζουν την αποτελεσματική διαχείριση των έργων ΤΠΕ που σχετίζονται με την αγορά, τη συντήρηση και, κατά περίπτωση, την ανάπτυξη των συστημάτων ΤΠΕ της χρηματοοικονομικής οντότητας.

3. Στην πολιτική διαχείρισης έργων ΤΠΕ που αναφέρεται στην παράγραφο 1 περιλαμβάνονται όλα τα ακόλουθα:

α) οι στόχοι των έργων ΤΠΕ,

β) η διακυβέρνηση των έργων ΤΠΕ, συμπεριλαμβανομένων των ρόλων και των αρμοδιοτήτων,

γ) ο σχεδιασμός, το χρονοδιάγραμμα και τα στάδια των έργων ΤΠΕ,

δ)η αξιολόγηση κινδύνων έργων ΤΠΕ,

ε) σχετικά ορόσημα,

στ) οι απαιτήσεις διαχείρισης αλλαγών,

ζ) οι δοκιμές όλων των απαιτήσεων, συμπεριλαμβανομένων των απαιτήσεων ασφαλείας, και η αντίστοιχη διαδικασία έγκρισης κατά την εγκατάσταση συστήματος ΤΠΕ στο περιβάλλον παραγωγής.

4. Με την πολιτική διαχείρισης έργων ΤΠΕ που αναφέρεται στην παράγραφο 1 διασφαλίζεται η ασφαλής υλοποίηση των έργων ΤΠΕ μέσω της παροχής των αναγκαίων πληροφοριών και εμπειρογνωσίας από τον επιχειρηματικό τομέα ή τις λειτουργίες που επηρεάζονται από το έργο ΤΠΕ.

5. Σύμφωνα με την αξιολόγηση κινδύνων έργων ΤΠΕ που αναφέρεται στην παράγραφο 3 στοιχείο δ), η πολιτική διαχείρισης έργων ΤΠΕ που αναφέρεται στην παράγραφο 1 προβλέπει ότι η εκπόνηση και η πρόοδος των έργων ΤΠΕ που επηρεάζουν κρίσιμες ή σημαντικές λειτουργίες της χρηματοοικονομικής οντότητας και οι συναφείς κίνδυνοί τους αναφέρονται στο διοικητικό όργανο ως εξής:

α) μεμονωμένα ή συγκεντρωτικά, ανάλογα με τη σημασία και το μέγεθος των έργων ΤΠΕ·

β) περιοδικά και, κατά περίπτωση, ανάλογα με τα συμβάντα.

Άρθρο 16

Απόκτηση, ανάπτυξη και συντήρηση συστημάτων ΤΠΕ

1. Στο πλαίσιο των διασφαλίσεων για τη διατήρηση της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων, οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν πολιτική που διέπει την απόκτηση, την ανάπτυξη και τη συντήρηση συστημάτων ΤΠΕ. Η πολιτική αυτή:

α) προσδιορίζει πρακτικές ασφαλείας και μεθοδολογίες που σχετίζονται με την απόκτηση, την ανάπτυξη και τη συντήρηση συστημάτων ΤΠΕ·

β) απαιτεί τον προσδιορισμό:

i) τεχνικών προδιαγραφών και τεχνικών προδιαγραφών των ΤΠΕ, όπως ορίζονται στο άρθρο 2 σημεία 4) και 5) του κανονισμού (ΕΕ) αριθ. 1025/2012·

ii) απαιτήσεων σχετικά με την απόκτηση, την ανάπτυξη και τη συντήρηση συστημάτων ΤΠΕ, με ιδιαίτερη έμφαση στις απαιτήσεις ασφάλειας ΤΠΕ και στην έγκρισή τους από τη σχετική επιχειρηματική λειτουργία και τον ιδιοκτήτη πόρων ΤΠΕ σύμφωνα με τις ρυθμίσεις εσωτερικής διακυβέρνησης της χρηματοοικονομικής οντότητας·

γ) προσδιορίζει μέτρα για τον μετριασμό του κινδύνου ακούσιας τροποποίησης ή εσκεμμένης χειραγώγησης των συστημάτων ΤΠΕ κατά την ανάπτυξη, τη συντήρηση και την εγκατάσταση των εν λόγω συστημάτων ΤΠΕ στο περιβάλλον παραγωγής.

2. Οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν διαδικασία απόκτησης, ανάπτυξης και συντήρησης συστημάτων ΤΠΕ για τις δοκιμές και την έγκριση όλων των συστημάτων ΤΠΕ πριν από τη χρήση τους και μετά τη συντήρησή τους, σύμφωνα με το άρθρο 8 παράγραφος 2 στοιχείο β) σημεία v), vi) και vii). Το επίπεδο των δοκιμών είναι ανάλογο προς την κρισιμότητα των σχετικών επιχειρηματικών διαδικασιών και πόρων ΤΠΕ. Οι δοκιμές σχεδιάζονται έτσι ώστε να επαληθεύεται ότι τα νέα συστήματα ΤΠΕ είναι κατάλληλα να λειτουργούν όπως προβλέπεται, συμπεριλαμβανομένης της ποιότητας του λογισμικού που αναπτύσσεται εσωτερικά.

Οι κεντρικοί αντισυμβαλλόμενοι, πέραν των απαιτήσεων που ορίζονται στο πρώτο εδάφιο, περιλαμβάνουν, κατά περίπτωση, στον σχεδιασμό και στη διεξαγωγή των δοκιμών που αναφέρονται στο πρώτο εδάφιο:

α) εκκαθαριστικά μέλη και πελάτες,

β) διαλειτουργικούς κεντρικούς αντισυμβαλλομένους,

γ) άλλα ενδιαφερόμενα μέρη.

Τα κεντρικά αποθετήρια τίτλων, πέραν των απαιτήσεων που ορίζονται στο πρώτο εδάφιο, περιλαμβάνουν, κατά περίπτωση, στον σχεδιασμό και στη διεξαγωγή των δοκιμών που αναφέρονται στο πρώτο εδάφιο:

α) χρήστες,

β) παρόχους κρίσιμων υπηρεσιών κοινής ωφέλειας και κρίσιμων υπηρεσιών,

γ) άλλα κεντρικά αποθετήρια τίτλων,

δ) άλλες υποδομές αγορών,

ε) κάθε άλλο ίδρυμα με το οποίο τα κεντρικά αποθετήρια τίτλων έχουν εντοπίσει αλληλεξαρτήσεις στην οικεία πολιτική επιχειρησιακής συνέχειας.

3. Η διαδικασία που αναφέρεται στην παράγραφο 2 περιλαμβάνει τις επιδόσεις των επανεξετάσεων πηγαίου κώδικα που καλύπτουν τόσο τις στατικές όσο και τις δυναμικές δοκιμές. Οι εν λόγω δοκιμές περιλαμβάνουν δοκιμές ασφαλείας για τα συστήματα και τις εφαρμογές που είναι εκτεθειμένα στο διαδίκτυο σύμφωνα με το άρθρο 8 παράγραφος 2 στοιχείο β) σημεία v), vi) και vii). Οι χρηματοοικονομικές οντότητες:

α) εντοπίζουν και αναλύουν τις ευπάθειες και τις ανωμαλίες του πηγαίου κώδικα·

β) εγκρίνουν σχέδιο δράσης για την αντιμετώπιση των εν λόγω ευπαθειών και ανωμαλιών·

γ) παρακολουθούν την εφαρμογή του εν λόγω σχεδίου δράσης.

4. Η διαδικασία που αναφέρεται στην παράγραφο 2 περιλαμβάνει δοκιμές ασφαλείας των πακέτων λογισμικού το αργότερο κατά τη φάση της ενοποίησης, σύμφωνα με το άρθρο 8 παράγραφος 2 στοιχείο β) σημεία v), vi) και vii).

5. Η διαδικασία που αναφέρεται στην παράγραφο 2 προβλέπει ότι:

α) τα μη παραγωγικά περιβάλλοντα αποθηκεύουν μόνον ανωνυμοποιημένα, ψευδωνυμοποιημένα ή τυχαιοποιημένα δεδομένα παραγωγής·

β) οι χρηματοοικονομικές οντότητες πρέπει να προστατεύουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων σε μη παραγωγικά περιβάλλοντα.

6. Κατά παρέκκλιση από την παράγραφο 5, η διαδικασία που αναφέρεται στην παράγραφο 2 μπορεί να προβλέπει ότι τα δεδομένα παραγωγής αποθηκεύονται μόνο για συγκεκριμένες περιπτώσεις δοκιμών, για περιορισμένο χρονικό διάστημα και μετά την έγκριση από τη σχετική λειτουργία και την αναφορά των περιπτώσεων αυτών στη λειτουργία διαχείρισης κινδύνων ΤΠΕ.

7. Η διαδικασία που αναφέρεται στην παράγραφο 2 περιλαμβάνει την εφαρμογή ελέγχων για την προστασία της ακεραιότητας του πηγαίου κώδικα των συστημάτων ΤΠΕ που αναπτύσσονται εντός της επιχείρησης ή από τρίτο πάροχο υπηρεσιών ΤΠΕ και παραδίδονται στη χρηματοοικονομική οντότητα από τρίτο πάροχο υπηρεσιών ΤΠΕ.

8. Η διαδικασία που αναφέρεται στην παράγραφο 2 προβλέπει ότι το ιδιόκτητο λογισμικό και, όπου είναι εφικτό, ο πηγαίος κώδικας που παρέχεται από τρίτους παρόχους υπηρεσιών ΤΠΕ ή προέρχεται από έργα ανοικτού κώδικα πρέπει να αναλύονται και να υποβάλλονται σε δοκιμές σύμφωνα με την παράγραφο 3 πριν από την εγκατάστασή τους στο περιβάλλον παραγωγής.

9. Οι παράγραφοι 1 έως 8 του παρόντος άρθρου εφαρμόζονται επίσης σε συστήματα ΤΠΕ που αναπτύσσονται ή τελούν υπό τη διαχείριση χρηστών εκτός της λειτουργίας ΤΠΕ, με τη χρήση προσέγγισης βάσει κινδύνου.

Άρθρο 17

Διαχείριση αλλαγών ΤΠΕ

1. Στο πλαίσιο των διασφαλίσεων για τη διατήρηση της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων, οι χρηματοοικονομικές οντότητες περιλαμβάνουν στις διαδικασίες διαχείρισης αλλαγών ΤΠΕ που αναφέρονται στο άρθρο 9 παράγραφος 4 στοιχείο ε) του κανονισμού (ΕΕ) 2022/2554, σε σχέση με όλες τις αλλαγές σε λογισμικό, υλισμικό, στοιχεία, συστήματα ή παραμέτρους ασφάλειας υλικολογισμικού, όλα τα ακόλουθα στοιχεία:

α) επαλήθευση της τήρησης των απαιτήσεων ασφάλειας ΤΠΕ·

β) μηχανισμούς για τη διασφάλιση της ανεξαρτησίας των λειτουργιών που εγκρίνουν αλλαγές και των λειτουργιών που είναι υπεύθυνες για την υποβολή αιτήματος για τις εν λόγω αλλαγές και την εφαρμογή τους·

γ) σαφή περιγραφή των ρόλων και των αρμοδιοτήτων ώστε να διασφαλίζεται ότι:

i) προσδιορίζονται και προγραμματίζονται αλλαγές·

ii) σχεδιάζεται κατάλληλη μετάβαση·

iii) οι αλλαγές υποβάλλονται σε δοκιμές και οριστικοποιούνται με ελεγχόμενο τρόπο·

iv) υπάρχει αποτελεσματική διασφάλιση της ποιότητας·

δ) την τεκμηρίωση και την κοινοποίηση λεπτομερών στοιχείων της αλλαγής, συμπεριλαμβανομένων:

i) του σκοπού και του πεδίου εφαρμογής της αλλαγής·

ii) του χρονοδιαγράμματος για την εφαρμογή της αλλαγής·

iii) των αναμενόμενων αποτελεσμάτων·

ε) τον προσδιορισμό των εφεδρικών διαδικασιών και των αρμοδιοτήτων, συμπεριλαμβανομένων των διαδικασιών και των αρμοδιοτήτων για τη ματαίωση αλλαγών ή την ανάκαμψη της λειτουργίας από αλλαγές που δεν εφαρμόστηκαν επιτυχώς·

στ) διαδικασίες, πρωτόκολλα και εργαλεία για τη διαχείριση αλλαγών έκτακτης ανάγκης που παρέχουν επαρκείς διασφαλίσεις·

ζ) διαδικασίες για την τεκμηρίωση, την επαναξιολόγηση, την εκτίμηση και την έγκριση αλλαγών έκτακτης ανάγκης μετά την εφαρμογή τους, συμπεριλαμβανομένων των εναλλακτικών λύσεων και των ενημερώσεων κώδικα·

η) τον προσδιορισμό των πιθανών επιπτώσεων αλλαγής στα υφιστάμενα μέτρα ασφάλειας ΤΠΕ και την αξιολόγηση του αν η αλλαγή αυτή απαιτεί τη θέσπιση πρόσθετων μέτρων ασφάλειας ΤΠΕ.

2. Αφού πραγματοποιήσουν σημαντικές αλλαγές στα οικεία συστήματα ΤΠΕ, οι κεντρικοί αντισυμβαλλόμενοι και τα κεντρικά αποθετήρια τίτλων υποβάλλουν τα οικεία συστήματα ΤΠΕ σε αυστηρές δοκιμές μέσω της προσομοίωσης ακραίων συνθηκών.

Οι κεντρικοί αντισυμβαλλόμενοι περιλαμβάνουν, κατά περίπτωση, στον σχεδιασμό και στη διεξαγωγή των δοκιμών που αναφέρονται στο πρώτο εδάφιο:

α) εκκαθαριστικά μέλη και πελάτες,

β) διαλειτουργικούς κεντρικούς αντισυμβαλλομένους,

γ) άλλα ενδιαφερόμενα μέρη.

Τα κεντρικά αποθετήρια τίτλων περιλαμβάνουν, κατά περίπτωση, στον σχεδιασμό και στη διεξαγωγή των δοκιμών που αναφέρονται στο πρώτο εδάφιο:

α) χρήστες,

β) παρόχους κρίσιμων υπηρεσιών κοινής ωφέλειας και κρίσιμων υπηρεσιών,

γ) άλλα κεντρικά αποθετήρια τίτλων,

δ) άλλες υποδομές αγορών,

ε) κάθε άλλο ίδρυμα με το οποίο τα κεντρικά αποθετήρια τίτλων έχουν εντοπίσει αλληλεξαρτήσεις στην οικεία πολιτική επιχειρησιακής συνέχειας των ΤΠΕ.

Τμήμα 8

Άρθρο 18

Υλική και περιβαλλοντική ασφάλεια

1. Στο πλαίσιο των διασφαλίσεων για τη διατήρηση της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων, οι χρηματοοικονομικές οντότητες προσδιορίζουν, τεκμηριώνουν και εφαρμόζουν πολιτική υλικής και περιβαλλοντικής ασφάλειας. Οι χρηματοοικονομικές οντότητες σχεδιάζουν την εν λόγω πολιτική υπό το πρίσμα του τοπίου των κυβερνοαπειλών, σύμφωνα με την ταξινόμηση που καθορίζεται σύμφωνα με το άρθρο 8 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554, και υπό το πρίσμα του συνολικού προφίλ κινδύνου των πόρων ΤΠΕ και των προσβάσιμων πληροφοριακών πόρων.

2. Η πολιτική υλικής και περιβαλλοντικής ασφάλειας που αναφέρεται στην παράγραφο 1 περιλαμβάνει όλα τα ακόλουθα:

α) παραπομπή στο τμήμα της πολιτικής για τον έλεγχο της διαχείρισης δικαιωμάτων πρόσβασης που αναφέρονται στο άρθρο 21 πρώτο εδάφιο στοιχείο ζ)·

β) μέτρα για την προστασία από επιθέσεις, ατυχήματα και περιβαλλοντικές απειλές και κινδύνους των εγκαταστάσεων, των κέντρων δεδομένων της χρηματοοικονομικής οντότητας και των ευαίσθητων οριοθετημένων χώρων που προσδιορίζει η χρηματοοικονομική οντότητα, όπου βρίσκονται πόροι ΤΠΕ και πληροφοριακοί πόροι·

γ) μέτρα για τη διασφάλιση των πόρων ΤΠΕ, τόσο εντός όσο και εκτός των εγκαταστάσεων της χρηματοοικονομικής οντότητας, με συνεκτίμηση των αποτελεσμάτων της αξιολόγησης κινδύνων ΤΠΕ που συνδέονται με τους σχετικούς πόρους ΤΠΕ·

δ) μέτρα για τη διασφάλιση της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των πόρων ΤΠΕ, των πληροφοριακών πόρων και των συσκευών ελέγχου φυσικής πρόσβασης της χρηματοοικονομικής οντότητας μέσω της κατάλληλης συντήρησης·

ε) μέτρα για τη διατήρηση της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων, συμπεριλαμβανομένης:

i) πολιτικής καθαρού γραφείου για τα έγγραφα·

ii) πολιτικής καθαρής οθόνης για τις εγκαταστάσεις επεξεργασίας πληροφοριών.

Για τους σκοπούς του στοιχείου β), τα μέτρα για την προστασία από περιβαλλοντικές απειλές και κινδύνους είναι ανάλογα με τη σημασία των εγκαταστάσεων, των κέντρων δεδομένων, των ευαίσθητων οριοθετημένων χώρων, και με την κρισιμότητα των λειτουργιών ή των συστημάτων ΤΠΕ που βρίσκονται εκεί.

Για τους σκοπούς του στοιχείου γ), η πολιτική υλικής και περιβαλλοντικής ασφάλειας που αναφέρεται στην παράγραφο 1 περιλαμβάνει μέτρα για την παροχή κατάλληλης προστασίας σε πόρους ΤΠΕ χωρίς επίβλεψη.

ΚΕΦΑΛΑΙΟ ΙΙ

Πολιτική ανθρώπινων πόρων και έλεγχος πρόσβασης

Άρθρο 19

Πολιτική ανθρώπινων πόρων

Στην πολιτική τους για τους ανθρώπινους πόρους ή σε άλλες σχετικές πολιτικές, οι χρηματοοικονομικές οντότητες περιλαμβάνουν όλα τα ακόλουθα στοιχεία που σχετίζονται με την ασφάλεια ΤΠΕ:

α) τον προσδιορισμό και την ανάθεση τυχόν ειδικών αρμοδιοτήτων για την ασφάλεια ΤΠΕ·

β) απαιτήσεις προκειμένου το προσωπικό της χρηματοοικονομικής οντότητας και των τρίτων παρόχων υπηρεσιών ΤΠΕ που χρησιμοποιούν ή έχουν πρόσβαση σε πόρους ΤΠΕ της χρηματοοικονομικής οντότητας:

i) να ενημερώνεται για τις πολιτικές, τις διαδικασίες και τα πρωτόκολλα ασφάλειας ΤΠΕ της χρηματοοικονομικής οντότητας και να τα τηρεί·

ii) να γνωρίζει τους διαύλους αναφοράς που εφαρμόζει η χρηματοοικονομική οντότητα για τον εντοπισμό ασυνήθιστων δραστηριοτήτων, συμπεριλαμβανομένων, κατά περίπτωση, των διαύλων αναφοράς που έχουν θεσπιστεί σύμφωνα με την οδηγία (ΕΕ) 2019/1937 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([11])·

iii) να επιστρέψει στη χρηματοοικονομική οντότητα, μετά τη λήξη της απασχόλησής του, όλους τους πόρους ΤΠΕ και τους ενσώματους πληροφοριακούς πόρους που βρίσκονται στην κατοχή του και ανήκουν στη χρηματοοικονομική οντότητα.

Άρθρο 20

Διαχείριση ταυτότητας

1. Στο πλαίσιο ελέγχου της διαχείρισης δικαιωμάτων πρόσβασης, οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν πολιτικές και διαδικασίες διαχείρισης ταυτότητας που διασφαλίζουν τη μοναδική ταυτοποίηση και επαλήθευση ταυτότητας των φυσικών προσώπων και των συστημάτων που έχουν πρόσβαση στις πληροφορίες των χρηματοοικονομικών οντοτήτων, ώστε να καθίσταται δυνατή η εκχώρηση δικαιωμάτων πρόσβασης χρήστη σύμφωνα με το άρθρο 21.

2. Οι πολιτικές και οι διαδικασίες διαχείρισης ταυτότητας που αναφέρονται στην παράγραφο 1 περιλαμβάνουν όλα τα ακόλουθα:

α) με την επιφύλαξη του άρθρου 21 πρώτο εδάφιο στοιχείο γ), σε κάθε μέλος του προσωπικού της χρηματοοικονομικής οντότητας ή του προσωπικού των τρίτων παρόχων υπηρεσιών ΤΠΕ που έχει πρόσβαση στους πληροφοριακούς πόρους και στους πόρους ΤΠΕ της χρηματοοικονομικής οντότητας αποδίδεται μοναδική ταυτότητα που αντιστοιχεί σε μοναδικό λογαριασμό χρήστη·

β) διαδικασία διαχείρισης κύκλου ζωής ταυτοτήτων και λογαριασμών στο πλαίσιο διαχείρισης της δημιουργίας, της αλλαγής, της επανεξέτασης και επικαιροποίησης, της προσωρινής απενεργοποίησης και της κατάργησης όλων των λογαριασμών.

Για τους σκοπούς του στοιχείου α), οι χρηματοοικονομικές οντότητες τηρούν αρχεία όλων των χορηγήσεων ταυτότητας. Τα εν λόγω αρχεία τηρούνται μετά από αναδιοργάνωση της χρηματοοικονομικής οντότητας ή μετά τη λήξη της συμβατικής σχέσης, με την επιφύλαξη των απαιτήσεων διατήρησης που ορίζονται στο εφαρμοστέο ενωσιακό και εθνικό δίκαιο.

Για τους σκοπούς του στοιχείου β), οι χρηματοοικονομικές οντότητες αναπτύσσουν, όποτε είναι εφικτό και σκόπιμο, αυτοματοποιημένες λύσεις για τη διαδικασία διαχείρισης κύκλου ζωής ταυτοτήτων.

Άρθρο 21

Έλεγχος πρόσβασης

Στο πλαίσιο του ελέγχου της διαχείρισης δικαιωμάτων πρόσβασης, οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν πολιτική που περιλαμβάνει όλα τα ακόλουθα:

α) την εκχώρηση δικαιωμάτων πρόσβασης σε πόρους ΤΠΕ με βάση τις αρχές της ανάγκης γνώσης, της ανάγκης χρήσης και των ελάχιστων προνομίων, μεταξύ άλλων για την εξ αποστάσεως πρόσβαση και την πρόσβαση έκτακτης ανάγκης·

β) τον διαχωρισμό των καθηκόντων που έχουν σχεδιαστεί για την πρόληψη της αδικαιολόγητης πρόσβασης σε κρίσιμα δεδομένα ή για την αποτροπή της κατανομής συνδυασμών δικαιωμάτων πρόσβασης που ενδέχεται να χρησιμοποιηθούν για την παράκαμψη ελέγχων·

γ) διάταξη σχετικά με τη λογοδοσία χρήστη, περιορίζοντας στο μέτρο του δυνατού τη χρήση γενικών και κοινών λογαριασμών χρήστη και διασφαλίζοντας ότι ανά πάσα στιγμή μπορεί να εξακριβωθεί η ταυτότητα των χρηστών σε σχέση με τις ενέργειες που εκτελούνται στα συστήματα ΤΠΕ·

([11]) Οδηγία (ΕΕ) 2019/1937 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2019, σχετικά με την προστασία των προσώπων που αναφέρουν παραβιάσεις του δικαίου της Ένωσης (ΕΕ L 305 της 26.11.2019, σ. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

δ) διάταξη σχετικά με τους περιορισμούς της πρόσβασης σε πόρους ΤΠΕ, καθορίζοντας δικλείδες ασφαλείας και εργαλεία για την πρόληψη της μη εξουσιοδοτημένης πρόσβασης·

ε) διαδικασίες διαχείρισης λογαριασμών για τη χορήγηση, την αλλαγή ή την ανάκληση δικαιωμάτων πρόσβασης για λογαριασμούς χρήστη και γενικούς λογαριασμούς, μεταξύ άλλων γενικούς λογαριασμούς διαχειριστή, συμπεριλαμβανομένης διάταξης για όλα τα ακόλουθα:

i) την ανάθεση ρόλων και αρμοδιοτήτων για τη χορήγηση, την επανεξέταση και την ανάκληση δικαιωμάτων πρόσβασης·

ii) την εκχώρηση προνομιακής πρόσβασης, πρόσβασης έκτακτης ανάγκης και διαχειριστή με βάση την ανάγκη χρήσης ή ad hoc για όλα τα συστήματα ΤΠΕ·

iii) την ανάκληση δικαιωμάτων πρόσβασης χωρίς αδικαιολόγητη καθυστέρηση μετά τη λήξη της απασχόλησης ή όταν η πρόσβαση δεν είναι πλέον απαραίτητη·

iv) την επικαιροποίηση δικαιωμάτων πρόσβασης όταν απαιτούνται αλλαγές και τουλάχιστον μία φορά ετησίως για όλα τα συστήματα ΤΠΕ, εκτός από τα συστήματα ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες και τουλάχιστον κάθε 6 μήνες για συστήματα ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες·

στ) μεθόδους επαλήθευσης ταυτότητας, συμπεριλαμβανομένων όλων των ακόλουθων στοιχείων:

i) της χρήσης μεθόδων επαλήθευσης ταυτότητας ανάλογων με την ταξινόμηση που καθορίζεται σύμφωνα με το άρθρο 8 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 και με το συνολικό προφίλ κινδύνου των πόρων ΤΠΕ και με συνεκτίμηση κορυφαίων πρακτικών·

ii) της χρήσης μεθόδων ισχυρής αυθεντικοποίησης σύμφωνα με κορυφαίες πρακτικές και τεχνικές για την εξ αποστάσεως πρόσβαση στο δίκτυο της χρηματοοικονομικής οντότητας, για προνομιακή πρόσβαση, για πρόσβαση στους πόρους ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες ή πόρους ΤΠΕ που είναι προσβάσιμοι από το κοινό·

ζ) μέτρα για δικλείδες ασφαλείας φυσικής πρόσβασης που περιλαμβάνουν:

i) την ταυτοποίηση και καταγραφή των φυσικών προσώπων που είναι εξουσιοδοτημένα να έχουν πρόσβαση σε εγκαταστάσεις, κέντρα δεδομένων και ευαίσθητους οριοθετημένους χώρους που προσδιορίζει η χρηματοοικονομική οντότητα, όπου βρίσκονται πόροι ΤΠΕ και πληροφοριακοί πόροι·

ii) τη χορήγηση δικαιωμάτων φυσικής πρόσβασης σε κρίσιμους πόρους ΤΠΕ μόνο σε εξουσιοδοτημένα πρόσωπα, σύμφωνα με τις αρχές της ανάγκης γνώσης και των ελάχιστων προνομίων, και σε ad hoc βάση·

iii) την παρακολούθηση της φυσικής πρόσβασης σε εγκαταστάσεις, κέντρα δεδομένων και ευαίσθητους οριοθετημένους χώρους που προσδιορίζει η χρηματοοικονομική οντότητα, όπου βρίσκονται πόροι ΤΠΕ και πληροφοριακοί πόροι·

iv) την επανεξέταση των δικαιωμάτων φυσικής πρόσβασης προκειμένου να διασφαλιστεί η άμεση ανάκληση περιττών δικαιωμάτων πρόσβασης.

Για τους σκοπούς του στοιχείου ε) σημείο i), οι χρηματοοικονομικές οντότητες καθορίζουν την περίοδο διατήρησης, λαμβάνοντας υπόψη τους επιχειρηματικούς στόχους και τους στόχους ασφάλειας των πληροφοριών, τους λόγους καταχώρισης του συμβάντος στα αρχεία καταγραφής και τα αποτελέσματα της αξιολόγησης κινδύνων ΤΠΕ.

Για τους σκοπούς του στοιχείου ε) σημείο ii), οι χρηματοοικονομικές οντότητες χρησιμοποιούν, όπου είναι δυνατόν, ειδικούς λογαριασμούς για την εκτέλεση διοικητικών καθηκόντων στα συστήματα ΤΠΕ. Όπου είναι εφικτό και σκόπιμο, οι χρηματοοικονομικές οντότητες εφαρμόζουν αυτοματοποιημένες λύσεις για τη διαχείριση προνομιακής πρόσβασης.

Για τους σκοπούς του στοιχείου ζ) σημείο i), η ταυτοποίηση και η καταγραφή είναι ανάλογες προς τη σημασία των εγκαταστάσεων, των κέντρων δεδομένων, των ευαίσθητων οριοθετημένων χώρων και με την κρισιμότητα των λειτουργιών ή των συστημάτων ΤΠΕ που βρίσκονται εκεί.

Για τους σκοπούς του στοιχείου ζ) σημείο iii), η παρακολούθηση είναι ανάλογη με την ταξινόμηση που καθορίζεται σύμφωνα με το άρθρο 8 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 και την κρισιμότητα του χώρου στον οποίο πραγματοποιείται πρόσβαση.

ΚΕΦΑΛΑΙΟ III

Εντοπισμός και αντιμετώπιση συμβάντων που σχετίζονται με τις ΤΠΕ

Άρθρο 22

Πολιτική διαχείρισης συμβάντων που σχετίζονται με τις ΤΠΕ

Στο πλαίσιο των μηχανισμών για τον εντοπισμό ασυνήθιστων δραστηριοτήτων, συμπεριλαμβανομένων ζητημάτων που αφορούν τις επιδόσεις του δικτύου ΤΠΕ και συμβάντων που σχετίζονται με τις ΤΠΕ, οι χρηματοοικονομικές οντότητες αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν πολιτική συμβάντων που σχετίζονται με τις ΤΠΕ, μέσω της οποίας:

α) τεκμηριώνουν τη διαδικασία διαχείρισης συμβάντων που σχετίζονται με τις ΤΠΕ, η οποία αναφέρεται στο άρθρο 17 του κανονισμού (ΕΕ) 2022/2554·

β) καταρτίζουν κατάλογο των σχετικών επαφών με εσωτερικές λειτουργίες και εξωτερικά ενδιαφερόμενα μέρη που συμμετέχουν άμεσα στην ασφάλεια των λειτουργιών ΤΠΕ, μεταξύ άλλων όσον αφορά:

i) τον εντοπισμό και την παρακολούθηση κυβερνοαπειλών·

ii) τον εντοπισμό ασυνήθιστων δραστηριοτήτων·

iii) τη διαχείριση ευπαθειών·

γ) θεσπίζουν, εφαρμόζουν και θέτουν σε λειτουργία τεχνικούς, οργανωτικούς και επιχειρησιακούς μηχανισμούς για την υποστήριξη της διαδικασίας διαχείρισης συμβάντων που σχετίζονται με τις ΤΠΕ, συμπεριλαμβανομένων μηχανισμών που επιτρέπουν τον έγκαιρο εντοπισμό ασυνήθιστων δραστηριοτήτων και συμπεριφορών σύμφωνα με το άρθρο 23 του παρόντος κανονισμού·

δ) διατηρούν όλα τα αποδεικτικά στοιχεία για τα συμβάντα που σχετίζονται με τις ΤΠΕ για χρονικό διάστημα που δεν υπερβαίνει το αναγκαίο για τους σκοπούς για τους οποίους συλλέγονται τα δεδομένα, ανάλογα με την κρισιμότητα των επηρεαζόμενων επιχειρηματικών λειτουργιών, των υποστηρικτικών διαδικασιών, των πόρων ΤΠΕ και των πληροφοριακών πόρων, σύμφωνα με το άρθρο 15 του κατ' εξουσιοδότηση κανονισμού (ΕΕ) 2024/1772 της Επιτροπής ([12]) και με οποιαδήποτε ισχύουσα απαίτηση διατήρησης σύμφωνα με το ενωσιακό δίκαιο·

ε) θεσπίζουν και εφαρμόζουν μηχανισμούς για την ανάλυση σημαντικών ή επαναλαμβανόμενων συμβάντων που σχετίζονται με τις ΤΠΕ και πρακτικών όσον αφορά τον αριθμό και την εμφάνιση συμβάντων που σχετίζονται με τις ΤΠΕ.

Για τους σκοπούς του στοιχείου δ), οι χρηματοοικονομικές οντότητες διατηρούν τα αποδεικτικά στοιχεία που αναφέρονται στο εν λόγω στοιχείο με ασφαλή τρόπο.

Άρθρο 23

Εντοπισμός ασυνήθιστων δραστηριοτήτων και κριτήρια για τον εντοπισμό και την αντιμετώπιση συμβάντων που σχετίζονται με τις ΤΠΕ

1. Οι χρηματοοικονομικές οντότητες καθορίζουν σαφείς ρόλους και αρμοδιότητες για τον αποτελεσματικό εντοπισμό και την αντιμετώπιση συμβάντων που σχετίζονται με τις ΤΠΕ και ασυνήθιστων δραστηριοτήτων.

2. Ο μηχανισμός για τον άμεσο εντοπισμό ασυνήθιστων δραστηριοτήτων, συμπεριλαμβανομένων ζητημάτων που αφορούν τις επιδόσεις του δικτύου ΤΠΕ και συμβάντων που σχετίζονται με τις ΤΠΕ, όπως αναφέρεται στο άρθρο 10 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554, δίνει τη δυνατότητα στις χρηματοοικονομικές οντότητες:

α) να συλλέγουν, να παρακολουθούν και να αναλύουν όλα τα ακόλουθα:

i) εσωτερικούς και εξωτερικούς παράγοντες, συμπεριλαμβανομένων τουλάχιστον των αρχείων καταγραφής που συλλέγονται σύμφωνα με το άρθρο 12 του παρόντος κανονισμού, των πληροφοριών από επιχειρηματικές λειτουργίες και λειτουργίες ΤΠΕ, καθώς και τυχόν προβλημάτων που αναφέρουν οι χρήστες της χρηματοοικονομικής οντότητας·

ii) δυνητικές εσωτερικές και εξωτερικές κυβερνοαπειλές, λαμβανομένων υπόψη σεναρίων που χρησιμοποιούνται συνήθως από παράγοντες απειλής και σεναρίων που βασίζονται σε δραστηριότητες συλλογής πληροφοριών για απειλές·

([12]) Κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2024/1772 της Επιτροπής, της 13ης Μαρτίου 2024, για τη συμπλήρωση του κανονισμού (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τα ρυθμιστικά τεχνικά πρότυπα για τον προσδιορισμό των κριτηρίων ταξινόμησης συμβάντων που σχετίζονται με τις ΤΠΕ και κυβερνοαπειλών, τον καθορισμό κατώτατων ορίων σημαντικότητας και τον προσδιορισμό των λεπτομερειών των αναφορών μειζόνων συμβάντων (ΕΕ L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii) την κοινοποίηση συμβάντων που σχετίζονται με τις ΤΠΕ από τρίτο πάροχο υπηρεσιών ΤΠΕ της χρηματοοικονομικής οντότητας, τα οποία εντοπίζονται στα συστήματα και τα δίκτυα ΤΠΕ του τρίτου παρόχου υπηρεσιών ΤΠΕ και ενδέχεται να επηρεάσουν τη χρηματοοικονομική οντότητα·

β) να εντοπίζουν ασυνήθιστες δραστηριότητες και συμπεριφορά και να εφαρμόζουν εργαλεία που δημιουργούν προειδοποιήσεις για ασυνήθιστες δραστηριότητες και συμπεριφορά, τουλάχιστον για τους πόρους ΤΠΕ και τους πληροφοριακούς πόρους που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες·

γ) να δίνουν προτεραιότητα στις προειδοποιήσεις που αναφέρονται στο στοιχείο β), ώστε να καθίσταται δυνατή η διαχείριση των εντοπισθέντων συμβάντων που σχετίζονται με τις ΤΠΕ εντός του προβλεπόμενου χρόνου επίλυσης, όπως καθορίζεται από τις χρηματοοικονομικές οντότητες, τόσο κατά τη διάρκεια όσο και εκτός του ωραρίου εργασίας·

δ) να καταγράφουν, να αναλύουν και να αξιολογούν κάθε σχετική πληροφορία για όλες τις ασυνήθιστες δραστηριότητες και συμπεριφορές, με αυτόματο ή μη αυτόματο τρόπο.

Για τους σκοπούς του στοιχείου β), τα εργαλεία που αναφέρονται στο εν λόγω στοιχείο περιλαμβάνουν τα εργαλεία που παρέχουν αυτοματοποιημένες προειδοποιήσεις βάσει προκαθορισμένων κανόνων για τον εντοπισμό ανωμαλιών που επηρεάζουν την πληρότητα και την ακεραιότητα των πηγών δεδομένων ή τη συλλογή αρχείων καταγραφής.

3. Οι χρηματοοικονομικές οντότητες προστατεύουν κάθε καταγραφή των ασυνήθιστων δραστηριοτήτων από παραποίηση και μη εξουσιοδοτημένη πρόσβαση σε κατάσταση αποθήκευσης, διαβίβασης και, κατά περίπτωση, χρήσης.

4. Οι χρηματοοικονομικές οντότητες καταγράφουν όλες τις σχετικές πληροφορίες για κάθε εντοπισθείσα ασυνήθιστη δραστηριότητα που καθιστούν δυνατό:

α) τον προσδιορισμό της ημερομηνίας και της ώρας εμφάνισης της ασυνήθιστης δραστηριότητας·

β) τον προσδιορισμό της ημερομηνίας και της ώρας εντοπισμού της ασυνήθιστης δραστηριότητας·

γ) τον προσδιορισμό του τύπου της ασυνήθιστης δραστηριότητας.

5. Οι χρηματοοικονομικές οντότητες λαμβάνουν υπόψη όλα τα ακόλουθα κριτήρια για την ενεργοποίηση των διαδικασιών εντοπισμού και αντιμετώπισης συμβάντων που σχετίζονται με τις ΤΠΕ, οι οποίες αναφέρονται στο άρθρο 10 παράγραφος 2 του κανονισμού (ΕΕ) 2022/2554:

α) ενδείξεις ότι ενδέχεται να έχει διαπραχθεί κακόβουλη δραστηριότητα σε σύστημα ή δίκτυο ΤΠΕ ή ότι το εν λόγω σύστημα ή δίκτυο ΤΠΕ ενδέχεται να έχει τεθεί σε κίνδυνο·

β) απώλειες δεδομένων που εντοπίζονται σε σχέση με τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων·

γ) δυσμενείς επιπτώσεις που εντοπίζονται στις συναλλαγές και τις δραστηριότητες της χρηματοοικονομικής οντότητας·

δ) μη διαθεσιμότητα συστημάτων και δικτύου ΤΠΕ.

6. Για τους σκοπούς της παραγράφου 5, οι χρηματοοικονομικές οντότητες λαμβάνουν επίσης υπόψη την κρισιμότητα των επηρεαζόμενων υπηρεσιών.

ΚΕΦΑΛΑΙΟ IV

Διαχείριση της επιχειρησιακής συνέχειας των ΤΠΕ

Άρθρο 24

Συνιστώσες της πολιτικής επιχειρησιακής συνέχειας των ΤΠΕ

1. Στην πολιτική επιχειρησιακής συνέχειας των ΤΠΕ που αναφέρεται στο άρθρο 11 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554, οι χρηματοοικονομικές οντότητες περιλαμβάνουν όλα τα ακόλουθα:

α) περιγραφή:

i) των στόχων της πολιτικής επιχειρησιακής συνέχειας των ΤΠΕ, συμπεριλαμβανομένης της διασύνδεσης των ΤΠΕ και της συνολικής επιχειρησιακής συνέχειας, και λαμβάνοντας υπόψη τα αποτελέσματα της ανάλυσης επιχειρηματικών επιπτώσεων (ΑΕΕ) που αναφέρεται στο άρθρο 11 παράγραφος 5 του κανονισμού (ΕΕ) 2022/2554·

ii) του πεδίου εφαρμογής των ρυθμίσεων, των σχεδίων, των διαδικασιών και των μηχανισμών επιχειρησιακής συνέχειας των ΤΠΕ, συμπεριλαμβανομένων των περιορισμών και των εξαιρέσεων·

iii) του χρονοδιαγράμματος που πρέπει να καλύπτεται από τις ρυθμίσεις, τα σχέδια, τις διαδικασίες και τους μηχανισμούς επιχειρησιακής συνέχειας των ΤΠΕ·

iv) των κριτηρίων για την ενεργοποίηση και την απενεργοποίηση των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ, των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ και των σχεδίων επικοινωνίας σε καταστάσεις κρίσης·

β) διατάξεις σχετικά με:

i) τη διακυβέρνηση και την οργάνωση για την εφαρμογή της πολιτικής επιχειρησιακής συνέχειας των ΤΠΕ, συμπεριλαμβανομένων των ρόλων, των αρμοδιοτήτων και των διαδικασιών παραπομπής συμβάντων που διασφαλίζουν τη διαθεσιμότητα επαρκών πόρων·

ii) την ευθυγράμμιση μεταξύ των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ και των σχεδίων συνολικής επιχειρησιακής συνέχειας, όσον αφορά τουλάχιστον όλα τα ακόλουθα:

1) σενάρια πιθανών αστοχιών, συμπεριλαμβανομένων των σεναρίων που αναφέρονται στο άρθρο 26 παράγραφος 2 του παρόντος κανονισμού·

2) στόχους αποκατάστασης, διευκρινίζοντας ότι η χρηματοοικονομική οντότητα είναι σε θέση να αποκαταστήσει τις εργασίες των κρίσιμων ή σημαντικών λειτουργιών της μετά από διαταραχές σύμφωνα με τους στόχους ως προς τον χρόνο και το σημείο αποκατάστασης·

iii) την ανάπτυξη σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ για σοβαρές διαταραχές της επιχειρηματικής δραστηριότητας στο πλαίσιο των εν λόγω σχεδίων, και την ιεράρχηση των δράσεων επιχειρησιακής συνέχειας των ΤΠΕ με τη χρήση προσέγγισης βάσει κινδύνου·

iv) την ανάπτυξη, τις δοκιμές και την επανεξέταση σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ, σύμφωνα με τα άρθρα 25 και 26 του παρόντος κανονισμού·

v) την επανεξέταση της αποτελεσματικότητας των εφαρμοζόμενων ρυθμίσεων, σχεδίων, διαδικασιών και μηχανισμών επιχειρησιακής συνέχειας των ΤΠΕ, σύμφωνα με το άρθρο 26 του παρόντος κανονισμού·

vi) την ευθυγράμμιση της πολιτικής επιχειρησιακής συνέχειας των ΤΠΕ με:

1) την πολιτική επικοινωνίας που αναφέρεται στο άρθρο 14 παράγραφος 2 του κανονισμού (ΕΕ) 2022/2554·

2) τις δράσεις επικοινωνίας και διαχείρισης κρίσεων που αναφέρονται στο άρθρο 11 παράγραφος 2 στοιχείο ε) του κανονισμού (ΕΕ) 2022/2554.

2. Παράλληλα με τις απαιτήσεις που αναφέρονται στην παράγραφο 1, οι κεντρικοί αντισυμβαλλόμενοι διασφαλίζουν ότι η οικεία πολιτική επιχειρησιακής συνέχειας των ΤΠΕ:

α) περιέχει μέγιστο χρόνο αποκατάστασης για τις κρίσιμες λειτουργίες τους που δεν υπερβαίνει τις 2 ώρες·

β) λαμβάνει υπόψη τις εξωτερικές συνδέσεις και αλληλεξαρτήσεις στο πλαίσιο των χρηματοοικονομικών υποδομών, συμπεριλαμβανομένων των τόπων διαπραγμάτευσης που εκκαθαρίζονται από τον κεντρικό αντισυμβαλλόμενο, των συστημάτων διακανονισμού τίτλων και πληρωμών, και των πιστωτικών ιδρυμάτων που χρησιμοποιούνται από τον κεντρικό αντισυμβαλλόμενο ή από συνδεδεμένο κεντρικό αντισυμβαλλόμενο·

γ) ορίζει την εφαρμογή ρυθμίσεων για:

i) να διασφαλίζεται η συνέχεια των κρίσιμων ή σημαντικών λειτουργιών του κεντρικού αντισυμβαλλομένου βάσει σεναρίων καταστροφής·

ii) να διατηρείται δευτερεύων τόπος επεξεργασίας ικανός να διασφαλίζει τη συνέχεια των κρίσιμων ή σημαντικών λειτουργιών του κεντρικού αντισυμβαλλομένου, που είναι πανομοιότυπος με τον κύριο τόπο·

iii) να διατηρείται ή να υπάρχει άμεση πρόσβαση σε δευτερεύοντα επιχειρησιακό χώρο, ώστε το προσωπικό να μπορεί να διασφαλίζει τη συνέχεια της υπηρεσίας, εάν δεν είναι διαθέσιμη η κύρια τοποθεσία της επιχείρησης·

iv) να εξετάζεται η ανάγκη επιπρόσθετων τόπων επεξεργασίας, ιδίως όταν η ποικιλομορφία των προφίλ κινδύνου του κύριου και του δευτερεύοντος τόπου δεν ενισχύει επαρκώς την εμπιστοσύνη ότι οι στόχοι επιχειρησιακής συνέχειας του κεντρικού αντισυμβαλλομένου πληρούνται σε όλα τα σενάρια.

Για τους σκοπούς του στοιχείου α), οι κεντρικοί αντισυμβαλλόμενοι ολοκληρώνουν τις διαδικασίες και τις πληρωμές στο τέλος της ημέρας κατά την απαιτούμενη ώρα και ημέρα υπό οποιεσδήποτε περιστάσεις.

Για τους σκοπούς του στοιχείου γ) σημείο i), οι ρυθμίσεις που αναφέρονται στο εν λόγω στοιχείο αφορούν τη διαθεσιμότητα επαρκών ανθρώπινων πόρων, τον μέγιστο χρόνο διακοπής των κρίσιμων λειτουργιών, την εναλλακτική σύνδεση ή εφεδρεία και την ανάκτηση σε δευτερεύοντα τόπο.

Για τους σκοπούς του στοιχείου γ) σημείο ii), ο δευτερεύων τόπος επεξεργασίας που αναφέρεται στο εν λόγω στοιχείο έχει γεωγραφικό προφίλ κινδύνου διαφορετικό από εκείνο του κύριου τόπου.

3. Παράλληλα με τις απαιτήσεις που αναφέρονται στην παράγραφο 1, τα κεντρικά αποθετήρια τίτλων διασφαλίζουν ότι η οικεία πολιτική επιχειρησιακής συνέχειας των ΤΠΕ:

α) λαμβάνει υπόψη τυχόν συνδέσεις και αλληλεξαρτήσεις με χρήστες, παρόχους κρίσιμων υπηρεσιών κοινής ωφέλειας και κρίσιμων υπηρεσιών, άλλα κεντρικά αποθετήρια τίτλων και άλλες υποδομές αγορών·

β) απαιτεί οι οικείες ρυθμίσεις επιχειρησιακής συνέχειας των ΤΠΕ να διασφαλίζουν ότι ο στόχος του χρόνου αποκατάστασης για τις κρίσιμες ή σημαντικές λειτουργίες τους δεν υπερβαίνει τις 2 ώρες.

4. Παράλληλα με τις απαιτήσεις που αναφέρονται στην παράγραφο 1, οι τόποι διαπραγμάτευσης διασφαλίζουν ότι η οικεία πολιτική επιχειρησιακής συνέχειας των ΤΠΕ διασφαλίζει ότι:

α) οι συναλλαγές μπορούν να συνεχιστούν εντός 2 ωρών ή περίπου σε δύο ώρες από συμβάν δυσλειτουργίας·

β) ο μέγιστος όγκος δεδομένων που μπορεί να απολεσθούν από οποιαδήποτε υπηρεσία ΤΠ του τόπου διαπραγμάτευσης μετά από οποιοδήποτε συμβάν δυσλειτουργίας είναι σχεδόν μηδενικός.

Άρθρο 25

Δοκιμές των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ

1. Κατά την υλοποίηση δοκιμών των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ σύμφωνα με το άρθρο 11 παράγραφος 6 του κανονισμού (ΕΕ) 2022/2554, οι χρηματοοικονομικές οντότητες λαμβάνουν υπόψη την ανάλυση επιχειρηματικών επιπτώσεων (ΑΕΕ) της χρηματοοικονομικής οντότητας και την αξιολόγηση κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 3 παράγραφος 1 στοιχείο β) του παρόντος κανονισμού.

2. Οι χρηματοοικονομικές οντότητες αξιολογούν, μέσω της δοκιμής των οικείων σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ που αναφέρονται στην παράγραφο 1, αν είναι σε θέση να διασφαλίσουν τη συνέχεια των κρίσιμων ή σημαντικών λειτουργιών τους. Οι δοκιμές αυτές:

α) εκτελούνται με βάση σενάρια δοκιμών που προσομοιώνουν πιθανές διαταραχές, συμπεριλαμβανομένης επαρκούς δέσμης σοβαρών αλλά ευλογοφανών σεναρίων·

β) περιέχουν τις δοκιμές των υπηρεσιών ΤΠΕ που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ, κατά περίπτωση·

γ) όσον αφορά τις χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, όπως αναφέρονται στο άρθρο 11 παράγραφος 6 δεύτερο εδάφιο του κανονισμού (ΕΕ) 2022/2554, περιέχουν σενάρια μετάβασης από την κύρια υποδομή ΤΠΕ στην εφεδρική χωρητικότητα, αντίγραφα ασφαλείας και εφεδρικές εγκαταστάσεις·

δ) σχεδιάζονται έτσι ώστε να αμφισβητούνται οι παραδοχές στις οποίες βασίζονται τα σχέδια επιχειρησιακής συνέχειας, συμπεριλαμβανομένων των ρυθμίσεων διακυβέρνησης και των σχεδίων επικοινωνίας σε καταστάσεις κρίσης·

ε) περιέχουν διαδικασίες για την επαλήθευση της ικανότητας του προσωπικού των χρηματοοικονομικών οντοτήτων, των τρίτων παρόχων υπηρεσιών ΤΠΕ, των συστημάτων ΤΠΕ και των υπηρεσιών ΤΠΕ να ανταποκρίνονται επαρκώς στα σενάρια που λαμβάνονται δεόντως υπόψη σύμφωνα με το άρθρο 26 παράγραφος 2.

Για τους σκοπούς του στοιχείου α), οι χρηματοοικονομικές οντότητες περιλαμβάνουν πάντα στις δοκιμές τα σενάρια που εξετάζονται για την ανάπτυξη των σχεδίων επιχειρησιακής συνέχειας.

Για τους σκοπούς του στοιχείου β), οι χρηματοοικονομικές οντότητες λαμβάνουν δεόντως υπόψη σενάρια που συνδέονται με αφερεγγυότητα ή αθέτηση υποχρεώσεων των τρίτων παρόχων υπηρεσιών ΤΠΕ ή συνδέονται με πολιτικούς κινδύνους στις δικαιοδοσίες των τρίτων παρόχων υπηρεσιών ΤΠΕ, κατά περίπτωση.

Για τους σκοπούς του στοιχείου γ), οι δοκιμές επαληθεύουν αν τουλάχιστον κρίσιμες ή σημαντικές λειτουργίες μπορούν να λειτουργήσουν με τον δέοντα τρόπο για επαρκές χρονικό διάστημα και αν μπορεί να αποκατασταθεί η κανονική λειτουργία.

3. Παράλληλα με τις απαιτήσεις που αναφέρονται στην παράγραφο 2, οι κεντρικοί αντισυμβαλλόμενοι περιλαμβάνουν στις δοκιμές των οικείων σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ που αναφέρονται στην παράγραφο 1:

α) εκκαθαριστικά μέλη,

β) εξωτερικούς παρόχους,

γ) σχετικά ιδρύματα στη χρηματοοικονομική υποδομή με τα οποία οι κεντρικοί αντισυμβαλλόμενοι έχουν εντοπίσει αλληλεξαρτήσεις στις πολιτικές τους για επιχειρησιακή συνέχεια.

4. Παράλληλα με τις απαιτήσεις που αναφέρονται στην παράγραφο 2, τα κεντρικά αποθετήρια τίτλων περιλαμβάνουν στις δοκιμές των οικείων σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ που αναφέρονται στην παράγραφο 1, κατά περίπτωση:

α) χρήστες των κεντρικών αποθετηρίων τίτλων,

β) παρόχους κρίσιμων υπηρεσιών κοινής ωφέλειας και κρίσιμων υπηρεσιών,

γ) άλλα κεντρικά αποθετήρια τίτλων,

δ) άλλες υποδομές αγορών,

ε) κάθε άλλο ίδρυμα με το οποίο τα κεντρικά αποθετήρια τίτλων έχουν εντοπίσει αλληλεξαρτήσεις στην οικεία πολιτική επιχειρησιακής συνέχειας.

5. Οι χρηματοοικονομικές οντότητες τεκμηριώνουν τα αποτελέσματα των δοκιμών που αναφέρονται στην παράγραφο 1. Τυχόν ελλείψεις που εντοπίζονται και προκύπτουν από τις εν λόγω δοκιμές αναλύονται, αντιμετωπίζονται και αναφέρονται στο διοικητικό όργανο.

Άρθρο 26

Σχέδια αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ

1. Κατά την κατάρτιση των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ που αναφέρονται στο άρθρο 11 παράγραφος 3 του κανονισμού (ΕΕ) 2022/2554, οι χρηματοοικονομικές οντότητες λαμβάνουν υπόψη τα αποτελέσματα της ανάλυσης επιχειρηματικών επιπτώσεων (ΑΕΕ) της χρηματοοικονομικής οντότητας. Τα εν λόγω σχέδια αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ:

α) προσδιορίζουν τις συνθήκες που οδηγούν στην ενεργοποίηση ή απενεργοποίησή τους, καθώς και τυχόν εξαιρέσεις από την εν λόγω ενεργοποίηση ή απενεργοποίηση·

β) περιγράφουν τα μέτρα που πρέπει να ληφθούν για τη διασφάλιση της διαθεσιμότητας, της ακεραιότητας, της συνέχειας και της αποκατάστασης τουλάχιστον των συστημάτων και υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες της χρηματοοικονομικής οντότητας·

γ) σχεδιάζονται έτσι ώστε να ανταποκρίνονται στους στόχους αποκατάστασης των λειτουργιών των χρηματοοικονομικών οντοτήτων·

δ) τεκμηριώνονται και τίθενται στη διάθεση του προσωπικού που συμμετέχει στην εκτέλεση των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ και είναι άμεσα προσβάσιμα σε περίπτωση έκτακτης ανάγκης·

ε) προβλέπουν τόσο βραχυπρόθεσμες όσο και μακροπρόθεσμες επιλογές ανάκαμψης, συμπεριλαμβανομένης της μερικής ανάκαμψης της λειτουργίας των συστημάτων·

στ) καθορίζουν τους στόχους των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ και τις προϋποθέσεις για την επιτυχή εκτέλεσή τους.

Για τους σκοπούς του στοιχείου δ), οι χρηματοοικονομικές οντότητες προσδιορίζουν σαφώς τους ρόλους και τις αρμοδιότητες.

2. Τα σχέδια αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ που αναφέρονται στην παράγραφο 1 προσδιορίζουν σχετικά σενάρια, συμπεριλαμβανομένων σεναρίων σοβαρών διαταραχών της επιχειρηματικής δραστηριότητας και αυξημένης πιθανότητας επέλευσης διαταραχής. Στα εν λόγω σχέδια αναπτύσσονται σενάρια με βάση τις τρέχουσες πληροφορίες για τις απειλές και τα διδάγματα που αντλήθηκαν από προηγούμενα περιστατικά διαταραχών της επιχειρηματικής δραστηριότητας. Οι χρηματοοικονομικές οντότητες λαμβάνουν δεόντως υπόψη όλα τα ακόλουθα σενάρια:

α) κυβερνοεπιθέσεις και μετάβαση μεταξύ της κύριας υποδομής ΤΠΕ και της εφεδρικής χωρητικότητας, αντιγράφων ασφαλείας και εφεδρικών εγκαταστάσεων·

β) σενάρια στα οποία η ποιότητα της παροχής μιας κρίσιμης ή σημαντικής λειτουργίας επιδεινώνεται σε μη αποδεκτό επίπεδο ή αποτυγχάνει, και τον δυνητικό αντίκτυπο της αφερεγγυότητας ή άλλης αθέτησης υποχρεώσεων οποιουδήποτε σχετικού τρίτου παρόχου υπηρεσιών ΤΠΕ·

γ) μερική ή ολική βλάβη εγκαταστάσεων, συμπεριλαμβανομένων γραφείων και επαγγελματικών χώρων, καθώς και κέντρων δεδομένων·

δ) σημαντική αστοχία των πόρων ΤΠΕ ή της υποδομής επικοινωνίας·

ε) τη μη διαθεσιμότητα κρίσιμου αριθμού προσωπικού ή μελών του προσωπικού που είναι επιφορτισμένα με τη διασφάλιση της συνέχειας των λειτουργιών·

στ) επιπτώσεις της κλιματικής αλλαγής και συμβάντων σχετικών με την υποβάθμιση του περιβάλλοντος, φυσικών καταστροφών, πανδημιών και σωματικών επιθέσεων, συμπεριλαμβανομένων των εισβολών και των τρομοκρατικών επιθέσεων·

ζ) επιθέσεις προσώπων που κατέχουν εμπιστευτικές πληροφορίες·

η) πολιτική και κοινωνική αστάθεια, μεταξύ άλλων, κατά περίπτωση, στη δικαιοδοσία του τρίτου παρόχου υπηρεσιών ΤΠΕ και στην τοποθεσία όπου αποθηκεύονται και υποβάλλονται σε επεξεργασία τα δεδομένα·

θ) εκτεταμένες διακοπές ρεύματος.

3. Όταν τα κύρια μέτρα ανάκαμψης ενδέχεται να μην είναι εφικτά σε βραχυπρόθεσμο ορίζοντα λόγω κόστους, κινδύνων, υλικοτεχνικής υποστήριξης ή απρόβλεπτων περιστάσεων, εξετάζονται εναλλακτικές επιλογές μέσω των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ που αναφέρονται στην παράγραφο 1.

4. Στο πλαίσιο των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ που αναφέρονται στην παράγραφο 1, οι χρηματοοικονομικές οντότητες εξετάζουν και εφαρμόζουν μέτρα συνέχειας για τον μετριασμό της αθέτησης υποχρεώσεων των τρίτων παρόχων υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες της χρηματοοικονομικής οντότητας.

ΚΕΦΑΛΑΙΟ V

Έκθεση σχετικά με την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ

Άρθρο 27

Μορφή και περιεχόμενο της έκθεσης σχετικά με την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ

1. Οι χρηματοοικονομικές οντότητες υποβάλλουν την έκθεση σχετικά με την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6 παράγραφος 5 του κανονισμού (ΕΕ) 2022/2554 σε ηλεκτρονική μορφή με δυνατότητα αναζήτησης.

2. Οι χρηματοοικονομικές οντότητες περιλαμβάνουν όλες τις ακόλουθες πληροφορίες στην έκθεση που αναφέρεται στην παράγραφο 1:

α) ένα εισαγωγικό τμήμα το οποίο:

i) προσδιορίζει σαφώς τη χρηματοοικονομική οντότητα που αποτελεί το αντικείμενο της έκθεσης και περιγράφει τη δομή του ομίλου της, κατά περίπτωση·

ii) περιγράφει το πλαίσιο της έκθεσης όσον αφορά τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της χρηματοοικονομικής οντότητας, την οργάνωσή της, τις προσδιορισμένες κρίσιμες λειτουργίες, τη στρατηγική, μείζονα υπό εξέλιξη έργα ή δραστηριότητες, τις σχέσεις και την εξάρτησή της από ενδοεπιχειρησιακές και ανατεθείσες υπηρεσίες και συστήματα ΤΠΕ ή τις επιπτώσεις που θα είχε η ολική απώλεια ή σοβαρή υποβάθμιση των εν λόγω συστημάτων σε κρίσιμες ή σημαντικές λειτουργίες και στην αποτελεσματικότητα της αγοράς·

iii) συνοψίζει τις σημαντικές αλλαγές στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ από την προηγούμενη έκθεση που υποβλήθηκε·

iv) παρέχει συνοπτική παρουσίαση του τρέχοντος και του βραχυπρόθεσμου προφίλ κινδύνου ΤΠΕ, του τοπίου των απειλών, της εκτιμώμενης αποτελεσματικότητας των δικλείδων ασφαλείας και των πολιτικών ασφάλειας της χρηματοοικονομικής οντότητας·

β) την ημερομηνία έγκρισης της έκθεσης από το διοικητικό όργανο της χρηματοοικονομικής οντότητας·

γ) περιγραφή του λόγου επανεξέτασης του πλαισίου διαχείρισης κινδύνων ΤΠΕ σύμφωνα με το άρθρο 6 παράγραφος 5 του κανονισμού (ΕΕ) 2022/2554·

δ) τις ημερομηνίες έναρξης και λήξης της περιόδου επανεξέτασης·

ε) αναφορά της λειτουργίας που είναι υπεύθυνη για την επανεξέταση·

στ) περιγραφή των σημαντικών αλλαγών και βελτιώσεων στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ από την προηγούμενη επανεξέταση·

ζ) σύνοψη των πορισμάτων της επανεξέτασης και λεπτομερή ανάλυση και αξιολόγηση της σοβαρότητας των αδυναμιών, των ελλείψεων και των κενών στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ κατά τη διάρκεια της περιόδου επανεξέτασης·

η) περιγραφή των μέτρων για την αντιμετώπιση των αδυναμιών, των ελλείψεων και των κενών που εντοπίστηκαν, μεταξύ άλλων όλα τα ακόλουθα:

i) σύνοψη των μέτρων που ελήφθησαν για την αποκατάσταση των αδυναμιών, των ελλείψεων και των κενών που εντοπίστηκαν·

ii) αναμενόμενη ημερομηνία εφαρμογής των μέτρων και ημερομηνίες που σχετίζονται με τον εσωτερικό έλεγχο της εφαρμογής, συμπεριλαμβανομένων πληροφοριών σχετικά με την πρόοδο της εφαρμογής των εν λόγω μέτρων κατά την ημερομηνία σύνταξης της έκθεσης, με επεξήγηση, κατά περίπτωση, του ενδεχόμενου κινδύνου μη τήρησης των προθεσμιών·

iii) εργαλεία που πρέπει να χρησιμοποιούνται και προσδιορισμό της λειτουργίας που είναι υπεύθυνη για την εκτέλεση των μέτρων, με λεπτομερή περιγραφή του αν τα εργαλεία και οι λειτουργίες είναι εσωτερικά ή εξωτερικά·

iv) περιγραφή των επιπτώσεων που έχουν στους δημοσιονομικούς, ανθρώπινους και υλικούς πόρους της χρηματοοικονομικής οντότητας οι αλλαγές που προβλέπονται στα μέτρα, συμπεριλαμβανομένων των πόρων που προορίζονται για την εφαρμογή τυχόν διορθωτικών μέτρων·

v) πληροφορίες σχετικά με τη διαδικασία ενημέρωσης της αρμόδιας αρχής, κατά περίπτωση·

vi) όταν οι αδυναμίες, οι ελλείψεις ή τα κενά που εντοπίζονται δεν υπόκεινται σε διορθωτικά μέτρα, λεπτομερή επεξήγηση των κριτηρίων που χρησιμοποιούνται για την ανάλυση των επιπτώσεων των εν λόγω αδυναμιών, ελλείψεων ή κενών, για την αξιολόγηση της σχετικής εναπομένουσας έκθεσης σε κινδύνους ΤΠΕ, καθώς και των κριτηρίων που χρησιμοποιούνται για την αποδοχή της σχετικής εναπομένουσας έκθεσης σε κινδύνους·

θ) πληροφορίες σχετικά με τις προγραμματισμένες περαιτέρω εξελίξεις του πλαισίου διαχείρισης κινδύνων ΤΠΕ·

ι) συμπεράσματα που προκύπτουν από την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ·

ια) πληροφορίες σχετικά με προηγούμενες επισκοπήσεις, μεταξύ άλλων:

i) κατάλογο προηγούμενων επανεξετάσεων μέχρι σήμερα·

ii) κατά περίπτωση, κατάσταση εφαρμογής των διορθωτικών μέτρων που προσδιορίζονται στην τελευταία έκθεση·

iii) όταν τα προτεινόμενα διορθωτικά μέτρα σε προηγούμενες επανεξετάσεις έχουν αποδειχθεί αναποτελεσματικά ή έχουν δημιουργήσει απρόβλεπτες προκλήσεις, περιγραφή του τρόπου με τον οποίο τα εν λόγω διορθωτικά μέτρα θα μπορούσαν να βελτιωθούν ή των εν λόγω απροσδόκητων προκλήσεων·

ιβ) πηγές πληροφοριών που χρησιμοποιήθηκαν για την κατάρτιση της έκθεσης, μεταξύ άλλων όλα τα ακόλουθα στοιχεία:

i) για χρηματοοικονομικές οντότητες πλην των πολύ μικρών επιχειρήσεων που αναφέρονται στο άρθρο 6 παράγραφος 6 του κανονισμού (ΕΕ) 2022/2554, τα αποτελέσματα των εσωτερικών ελέγχων·

ii) τα αποτελέσματα των αξιολογήσεων συμμόρφωσης·

iii) τα αποτελέσματα δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας και, κατά περίπτωση, τα αποτελέσματα προηγμένων δοκιμών —βασιζόμενα σε δοκιμές παρείσδυσης βάσει απειλών (TLPT)— εργαλείων, συστημάτων και διαδικασιών ΤΠΕ·

iv) εξωτερικές πηγές.

Για τους σκοπούς του στοιχείου γ), όταν η επανεξέταση ξεκινά μετά από εποπτικές οδηγίες ή συμπεράσματα που προέκυψαν από σχετικές δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας ή διαδικασίες ελέγχου, η έκθεση περιέχει ρητές αναφορές στις εν λόγω οδηγίες ή στα συμπεράσματα, οι οποίες επιτρέπουν τον προσδιορισμό του λόγου έναρξης της επανεξέτασης. Όταν η επανεξέταση ξεκινά μετά από συμβάντα που σχετίζονται με τις ΤΠΕ, η έκθεση περιέχει τον κατάλογο όλων των συμβάντων που σχετίζονται με τις ΤΠΕ με ανάλυση των βαθύτερων αιτίων του συμβάντος.

Για τους σκοπούς του στοιχείου στ), η περιγραφή περιλαμβάνει ανάλυση των επιπτώσεων των αλλαγών στη στρατηγική ψηφιακής επιχειρησιακής ανθεκτικότητας της χρηματοοικονομικής οντότητας, στο πλαίσιο εσωτερικού ελέγχου ΤΠΕ της χρηματοοικονομικής οντότητας και στη διακυβέρνηση διαχείρισης κινδύνων ΤΠΕ της χρηματοοικονομικής οντότητας.

ΤΙΤΛΟΣ III

ΑΠΛΟΥΣΤΕΥΜΕΝΟ ΠΛΑΙΣΙΟ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΩΝ ΤΠΕ ΓΙΑ ΤΙΣ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΕΣ ΟΝΤΟΤΗΤΕΣ ΠΟΥ ΑΝΑΦΕΡΟΝΤΑΙ ΣΤΟ ΑΡΘΡΟ 16 ΠΑΡΑΓΡΑΦΟΣ 1 ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ (ΕΕ) 2022/2554

ΚΕΦΑΛΑΙΟ I

Απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ

Άρθρο 28

Διακυβέρνηση και οργάνωση

1. Οι χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 διαθέτουν πλαίσιο εσωτερικής διακυβέρνησης και ελέγχου που διασφαλίζει την αποτελεσματική και συνετή διαχείριση των κινδύνων ΤΠΕ για την επίτευξη υψηλού επιπέδου ψηφιακής επιχειρησιακής ανθεκτικότητας.

2. Οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1, εντός του οικείου απλουστευμένου πλαισίου διαχείρισης κινδύνων ΤΠΕ, διασφαλίζουν ότι το διοικητικό τους όργανο:

α) φέρει τη συνολική ευθύνη να διασφαλίζει ότι το απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ καθιστά δυνατή την επίτευξη της επιχειρηματικής στρατηγικής της χρηματοοικονομικής οντότητας σύμφωνα με τη διάθεση ανάληψης κινδύνου της εν λόγω χρηματοοικονομικής οντότητας, και διασφαλίζει ότι οι κίνδυνοι ΤΠΕ λαμβάνονται υπόψη σε αυτό το πλαίσιο·

β) καθορίζει σαφείς ρόλους και αρμοδιότητες για όλα τα καθήκοντα που σχετίζονται με τις ΤΠΕ·

γ) καθορίζει στόχους για την ασφάλεια των πληροφοριών και απαιτήσεις ΤΠΕ·

δ) εγκρίνει, επιβλέπει και περιοδικά επανεξετάζει:

i) την ταξινόμηση των πληροφοριακών πόρων της χρηματοοικονομικής οντότητας, όπως αναφέρεται στο άρθρο 30 παράγραφος 1 του παρόντος κανονισμού, τον κατάλογο των κυριότερων εντοπισθέντων κινδύνων και την ανάλυση των επιχειρηματικών επιπτώσεων και τις σχετικές πολιτικές·

ii) τα σχέδια επιχειρησιακής συνέχειας της χρηματοοικονομικής οντότητας και τα μέτρα αντιμετώπισης και ανάκαμψης που αναφέρονται στο άρθρο 16 παράγραφος 1 στοιχείο στ) του κανονισμού (ΕΕ) 2022/2554·

ε) κατανέμει και επανεξετάζει τουλάχιστον μία φορά ετησίως τον προϋπολογισμό που είναι απαραίτητος για την εκπλήρωση των αναγκών ψηφιακής επιχειρησιακής ανθεκτικότητας της χρηματοοικονομικής οντότητας όσον αφορά όλα τα είδη πόρων, συμπεριλαμβανομένων των σχετικών προγραμμάτων ευαισθητοποίησης σε θέματα ασφάλειας των ΤΠΕ, της κατάρτισης για την ψηφιακή επιχειρησιακή ανθεκτικότητα και των δεξιοτήτων ΤΠΕ για όλους·

στ) προσδιορίζει και εφαρμόζει τις πολιτικές και τα μέτρα που περιλαμβάνονται στα κεφάλαια I, II και III του παρόντος τίτλου για τον εντοπισμό, την αξιολόγηση και τη διαχείριση των κινδύνων ΤΠΕ στους οποίους είναι εκτεθειμένη η χρηματοοικονομική οντότητα·

ζ) προσδιορίζει και εφαρμόζει διαδικασίες, πρωτόκολλα ΤΠΕ και εργαλεία που είναι απαραίτητα για την προστασία όλων των πληροφοριακών πόρων και των πόρων ΤΠΕ·

η) διασφαλίζει ότι το προσωπικό της χρηματοοικονομικής οντότητας ενημερώνεται και διαθέτει επαρκείς γνώσεις και δεξιότητες, ώστε να κατανοεί και να αξιολογεί τους κινδύνους ΤΠΕ και τις επιπτώσεις τους στις δραστηριότητες της χρηματοοικονομικής οντότητας, ανάλογα με τον υπό διαχείριση κίνδυνο ΤΠΕ·

θ) θεσπίζει τις ρυθμίσεις υποβολής εκθέσεων, μεταξύ άλλων τη συχνότητα, τη μορφή και το περιεχόμενο των εκθέσεων προς το διοικητικό όργανο σχετικά με την ασφάλεια των πληροφοριών και την ψηφιακή επιχειρησιακή ανθεκτικότητα.

3. Οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1 μπορούν, σύμφωνα με το ενωσιακό και το εθνικό τομεακό δίκαιο, να αναθέτουν τα καθήκοντα επαλήθευσης της συμμόρφωσης με τις απαιτήσεις διαχείρισης κινδύνων ΤΠΕ σε ενδοομιλικούς ή τρίτους παρόχους υπηρεσιών ΤΠΕ. Σε περίπτωση τέτοιας εξωτερικής ανάθεσης, οι χρηματοοικονομικές οντότητες παραμένουν εξολοκλήρου υπεύθυνες για την επαλήθευση της συμμόρφωσης με τις απαιτήσεις διαχείρισης κινδύνων ΤΠΕ.

4. Οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1 διασφαλίζουν τον κατάλληλο διαχωρισμό και την ανεξαρτησία των λειτουργιών ελέγχου και των λειτουργιών εσωτερικής επιθεώρησης.

5. Οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1 διασφαλίζουν ότι το απλουστευμένο τους πλαίσιο διαχείρισης κινδύνων ΤΠΕ υπόκειται σε εσωτερική επιθεώρηση από ελεγκτές, σύμφωνα με το πρόγραμμα ελέγχου των χρηματοοικονομικών οντοτήτων. Οι ελεγκτές διαθέτουν επαρκείς γνώσεις, δεξιότητες και εμπειρογνωσία όσον αφορά τους κινδύνους ΤΠΕ και είναι ανεξάρτητοι. Η συχνότητα και η εστίαση των ελέγχων ΤΠΕ είναι ανάλογες προς τους κινδύνους ΤΠΕ που αντιμετωπίζει η χρηματοοικονομική οντότητα.

6. Με βάση το αποτέλεσμα της επιθεώρησης που αναφέρεται στην παράγραφο 5, οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1 διασφαλίζουν την έγκαιρη επαλήθευση και αποκατάσταση κρίσιμων ευρημάτων ελέγχου ΤΠΕ.

Άρθρο 29

Πολιτική και μέτρα για την ασφάλεια των πληροφοριών

1. Οι χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν πολιτική ασφάλειας των πληροφοριών που υπάγεται στο απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ. Στην εν λόγω πολιτική ασφάλειας των πληροφοριών προσδιορίζονται οι αρχές και οι κανόνες υψηλού επιπέδου για την προστασία της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της γνησιότητας των δεδομένων και των υπηρεσιών που παρέχουν οι εν λόγω χρηματοοικονομικές οντότητες.

2. Με βάση την πολιτική τους για την ασφάλεια των πληροφοριών που αναφέρεται στην παράγραφο 1, οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1 θεσπίζουν και εφαρμόζουν μέτρα ασφάλειας ΤΠΕ για τον μετριασμό της έκθεσής τους σε κινδύνους ΤΠΕ, συμπεριλαμβανομένων των μέτρων μετριασμού που εφαρμόζονται από τρίτους παρόχους υπηρεσιών ΤΠΕ.

Τα μέτρα ασφάλειας ΤΠΕ περιλαμβάνουν όλα τα μέτρα που αναφέρονται στα άρθρα 30 έως 38.

Άρθρο 30

Ταξινόμηση πληροφοριακών πόρων και πόρων ΤΠΕ

1. Εντός του απλουστευμένου πλαισίου διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 16 παράγραφος 1 στοιχείο α) του κανονισμού (ΕΕ) 2022/2554, οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1 του εν λόγω άρθρου προσδιορίζουν, ταξινομούν και τεκμηριώνουν όλες τις κρίσιμες ή σημαντικές λειτουργίες, τους πληροφοριακούς πόρους και τους πόρους ΤΠΕ που τις υποστηρίζουν και τις αλληλεξαρτήσεις τους. Οι χρηματοοικονομικές οντότητες επανεξετάζουν τον εν λόγω προσδιορισμό και ταξινόμηση, ανάλογα με τις ανάγκες.

2. Οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1 προσδιορίζουν όλες τις κρίσιμες ή σημαντικές λειτουργίες που υποστηρίζονται από τρίτους παρόχους υπηρεσιών ΤΠΕ.

Άρθρο 31

Διαχείριση κινδύνων ΤΠΕ

1. Οι χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 περιλαμβάνουν στο απλουστευμένο τους πλαίσιο διαχείρισης κινδύνων ΤΠΕ όλα τα ακόλουθα:

α) καθορισμό των επιπέδων ανοχής κινδύνου για τους κινδύνους ΤΠΕ, σύμφωνα με τη διάθεση ανάληψης κινδύνου της χρηματοοικονομικής οντότητας·

β) τον προσδιορισμό και την αξιολόγηση των κινδύνων ΤΠΕ στους οποίους είναι εκτεθειμένη η χρηματοοικονομική οντότητα·

γ) την εξειδίκευση στρατηγικών μετριασμού τουλάχιστον για τους κινδύνους ΤΠΕ που δεν εμπίπτουν στα επίπεδα ανοχής κινδύνου της χρηματοοικονομικής οντότητας·

δ) την παρακολούθηση της αποτελεσματικότητας των στρατηγικών μετριασμού που αναφέρονται στο στοιχείο γ)·

ε) τον προσδιορισμό και την αξιολόγηση τυχόν κινδύνων ΤΠΕ και ασφάλειας πληροφοριών οι οποίοι προκύπτουν από οποιαδήποτε σημαντική αλλαγή σε συστήματα ΤΠΕ ή σε υπηρεσίες, διεργασίες ή διαδικασίες ΤΠΕ, καθώς και από τα αποτελέσματα δοκιμών ασφάλειας ΤΠΕ και μετά από κάθε μείζον συμβάν που σχετίζεται με τις ΤΠΕ.

2. Οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1 διενεργούν και τεκμηριώνουν την αξιολόγηση κινδύνων ΤΠΕ περιοδικά, ανάλογα με το προφίλ κινδύνου ΤΠΕ των χρηματοοικονομικών οντοτήτων.

3. Οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1 παρακολουθούν συνεχώς τις απειλές και τις ευπάθειες που σχετίζονται με τις κρίσιμες ή σημαντικές λειτουργίες τους, καθώς και τους πληροφοριακούς πόρους και τους πόρους ΤΠΕ, και επανεξετάζουν τακτικά τα σενάρια κινδύνου που επηρεάζουν τις εν λόγω κρίσιμες ή σημαντικές λειτουργίες.

4. Οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1 καθορίζουν όρια προειδοποίησης και κριτήρια για την ενεργοποίηση και τη δρομολόγηση διαδικασιών αντιμετώπισης συμβάντων που σχετίζονται με τις ΤΠΕ.

Άρθρο 32

Υλική και περιβαλλοντική ασφάλεια

1. Οι χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 προσδιορίζουν και εφαρμόζουν μέτρα υλικής ασφάλειας που σχεδιάζονται με βάση το τοπίο των απειλών και σύμφωνα με την ταξινόμηση που αναφέρεται στο άρθρο 30 παράγραφος 1 του παρόντος κανονισμού, το συνολικό προφίλ κινδύνου των πόρων ΤΠΕ και τους προσβάσιμους πληροφοριακούς πόρους.

2. Τα μέτρα που αναφέρονται στην παράγραφο 1 προστατεύουν τις εγκαταστάσεις των χρηματοοικονομικών οντοτήτων και, κατά περίπτωση, των κέντρων δεδομένων των χρηματοοικονομικών οντοτήτων όπου βρίσκονται οι πόροι ΤΠΕ και οι πληροφοριακοί πόροι από μη εξουσιοδοτημένη πρόσβαση, επιθέσεις και ατυχήματα, καθώς και από περιβαλλοντικές απειλές και κινδύνους.

3. Η προστασία από περιβαλλοντικές απειλές και κινδύνους είναι ανάλογη προς τη σημασία των σχετικών εγκαταστάσεων και, κατά περίπτωση, των κέντρων δεδομένων, καθώς και προς την κρισιμότητα των λειτουργιών ή των συστημάτων ΤΠΕ που βρίσκονται εκεί.

ΚΕΦΑΛΑΙΟ ΙΙ

Περαιτέρω στοιχεία συστημάτων, πρωτοκόλλων και εργαλείων για την ελαχιστοποίηση των επιπτώσεων των κινδύνων ΤΠΕ

Άρθρο 33

Έλεγχος πρόσβασης

Οι χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν διαδικασίες για τον έλεγχο της λογικής και φυσικής πρόσβασης και επιβάλλουν, παρακολουθούν και επανεξετάζουν περιοδικά τις εν λόγω διαδικασίες. Οι διαδικασίες αυτές περιλαμβάνουν τα ακόλουθα στοιχεία ελέγχου της λογικής και φυσικής πρόσβασης:

α) διαχείριση των δικαιωμάτων πρόσβασης σε πληροφοριακούς πόρους, πόρους ΤΠΕ και στις υποστηριζόμενες λειτουργίες τους, καθώς και σε κρίσιμες τοποθεσίες λειτουργίας της χρηματοοικονομικής οντότητας, με βάση την ανάγκη γνώσης, την ανάγκη χρήσης και τα ελάχιστα προνόμια, συμπεριλαμβανομένης της εξ αποστάσεως πρόσβασης και της πρόσβασης έκτακτης ανάγκης·

β) λογοδοσία χρήστη, η οποία διασφαλίζει ότι μπορούν να ταυτοποιούνται οι χρήστες για τις ενέργειες που εκτελούνται στα συστήματα ΤΠΕ·

γ) διαδικασίες διαχείρισης λογαριασμών για τη χορήγηση, την αλλαγή ή την ανάκληση δικαιωμάτων πρόσβασης για λογαριασμούς χρήστη και γενικούς λογαριασμούς, συμπεριλαμβανομένων γενικών λογαριασμών διαχειριστή·

δ) μεθόδους επαλήθευσης ταυτότητας που είναι ανάλογες προς την ταξινόμηση που αναφέρεται στο άρθρο 30 παράγραφος 1 και προς το συνολικό προφίλ κινδύνου των πόρων ΤΠΕ, και οι οποίες βασίζονται σε κορυφαίες πρακτικές·

ε) περιοδική επανεξέταση των δικαιωμάτων πρόσβασης και ανάκληση αυτών όταν δεν είναι πλέον αναγκαία.

Για τους σκοπούς του στοιχείου γ), η χρηματοοικονομική οντότητα εκχωρεί προνομιακή πρόσβαση, πρόσβαση έκτακτης ανάγκης και διαχειριστή με βάση την ανάγκη χρήσης ή ad hoc για όλα τα συστήματα ΤΠΕ και προχωρά σε καταγραφή σύμφωνα με το άρθρο 34 πρώτο εδάφιο στοιχείο στ).

Για τους σκοπούς του στοιχείου δ), οι χρηματοοικονομικές οντότητες χρησιμοποιούν μεθόδους ισχυρής αυθεντικοποίησης που βασίζονται σε κορυφαίες πρακτικές για την εξ αποστάσεως πρόσβαση στο δίκτυο των χρηματοοικονομικών οντοτήτων, για προνομιακή πρόσβαση και για την πρόσβαση σε πόρους ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες που είναι δημόσια διαθέσιμες.

Άρθρο 34

Ασφάλεια λειτουργιών ΤΠΕ

Οι χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554, στο πλαίσιο των συστημάτων, των πρωτοκόλλων και των εργαλείων τους, και για όλους τους πόρους ΤΠΕ:

α) παρακολουθούν και διαχειρίζονται τον κύκλο ζωής όλων των πόρων ΤΠΕ·

β) παρακολουθούν αν οι πόροι ΤΠΕ υποστηρίζονται από τρίτους παρόχους υπηρεσιών ΤΠΕ στις χρηματοοικονομικές οντότητες, κατά περίπτωση·

γ) προσδιορίζουν τις απαιτήσεις χωρητικότητας των οικείων πόρων ΤΠΕ και μέτρα για τη διατήρηση και τη βελτίωση της διαθεσιμότητας και της αποτελεσματικότητας των συστημάτων ΤΠΕ και την πρόληψη ελλείψεων χωρητικότητας ΤΠΕ πριν από την υλοποίησή τους·

δ) διενεργούν αυτοματοποιημένη σάρωση και αυτοματοποιημένες αξιολογήσεις ευπαθειών των πόρων ΤΠΕ ανάλογα με την ταξινόμησή τους, όπως αναφέρεται στο άρθρο 30 παράγραφος 1, και με το συνολικό προφίλ κινδύνου του πόρου ΤΠΕ, και αναπτύσσουν ενημερώσεις κώδικα για την αντιμετώπιση των εντοπιζόμενων ευπαθειών·

ε) διαχειρίζονται τους κινδύνους που σχετίζονται με ανεπίκαιρους, μη υποστηριζόμενους ή παρωχημένους πόρους ΤΠΕ·

στ) καταγράφουν τα συμβάντα που σχετίζονται με τον έλεγχο λογικής και φυσικής πρόσβασης, τις λειτουργίες ΤΠΕ, συμπεριλαμβανομένων των δραστηριοτήτων κίνησης συστημάτων και δικτύων, και τη διαχείριση αλλαγών ΤΠΕ·

ζ) προσδιορίζουν και εφαρμόζουν μέτρα για την παρακολούθηση και την ανάλυση πληροφοριών σχετικά με ασυνήθιστες δραστηριότητες και συμπεριφορά για κρίσιμες ή σημαντικές λειτουργίες ΤΠΕ·

η) εφαρμόζουν μέτρα για την παρακολούθηση συναφών και επικαιροποιημένων πληροφοριών σχετικά με τις κυβερνοαπειλές·

θ) εφαρμόζουν μέτρα για τον εντοπισμό πιθανών διαρροών πληροφοριών, κακόβουλων κωδικών και άλλων απειλών για την ασφάλεια, καθώς και δημοσίως γνωστών ευπαθειών του λογισμικού και του υλισμικού, και ελέγχουν αν υπάρχουν αντίστοιχες νέες ενημερώσεις ασφαλείας.

Για τους σκοπούς του στοιχείου στ), οι χρηματοοικονομικές οντότητες ευθυγραμμίζουν τον βαθμό λεπτομέρειας των αρχείων καταγραφής με τον σκοπό τους και τη χρήση του πόρου ΤΠΕ που παράγει τα εν λόγω αρχεία καταγραφής.

Άρθρο 35

Ασφάλεια δεδομένων, συστημάτων και δικτύων

Οι χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554, στο πλαίσιο των συστημάτων, των πρωτοκόλλων και των εργαλείων τους, αναπτύσσουν και εφαρμόζουν διασφαλίσεις που εγγυώνται την ασφάλεια των δικτύων από εισβολές και κατάχρηση δεδομένων και που διατηρούν τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων. Ειδικότερα, οι χρηματοοικονομικές οντότητες, λαμβάνοντας υπόψη την ταξινόμηση που αναφέρεται στο άρθρο 30 παράγραφος 1 του παρόντος κανονισμού, καθορίζουν όλα τα ακόλουθα:

α) τον προσδιορισμό και την εφαρμογή μέτρων για την προστασία των δεδομένων σε κατάσταση χρήσης, διαβίβασης και αποθήκευσης·

β) τον προσδιορισμό και την εφαρμογή μέτρων ασφαλείας σχετικά με τη χρήση λογισμικού, μέσων αποθήκευσης δεδομένων, συστημάτων και συσκευών τελικού σημείου που διαβιβάζουν και αποθηκεύουν τα δεδομένα της χρηματοοικονομικής οντότητας·

γ) τον προσδιορισμό και την εφαρμογή μέτρων για την πρόληψη και τον εντοπισμό μη εγκεκριμένων συνδέσεων στο δίκτυο της χρηματοοικονομικής οντότητας, καθώς και για τη διασφάλιση της κίνησης δικτύου μεταξύ των εσωτερικών δικτύων της χρηματοοικονομικής οντότητας και του διαδικτύου και άλλων εξωτερικών συνδέσεων·

δ) τον προσδιορισμό και την εφαρμογή μέτρων που διασφαλίζουν τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων κατά τη διάρκεια των διαβιβάσεων δικτύου·

ε) τη διαδικασία για την ασφαλή διαγραφή δεδομένων που υπάρχουν στις εγκαταστάσεις ή αποθηκεύονται εξωτερικά και που η χρηματοοικονομική οντότητα δεν χρειάζεται πλέον να συλλέγει ή να αποθηκεύει·

στ) τη διαδικασία για την ασφαλή απόρριψη ή τον παροπλισμό συσκευών αποθήκευσης δεδομένων σε εγκαταστάσεις ή συσκευών αποθήκευσης δεδομένων που αποθηκεύονται εξωτερικά, οι οποίες περιέχουν εμπιστευτικές πληροφορίες·

ζ) τον προσδιορισμό και την εφαρμογή μέτρων για να διασφαλίζεται ότι η τηλεργασία και η χρήση ιδιωτικών συσκευών τελικού σημείου δεν επηρεάζουν αρνητικά την ικανότητα της χρηματοοικονομικής οντότητας να εκτελεί τις κρίσιμες δραστηριότητές της επαρκώς, έγκαιρα και με ασφάλεια.

Άρθρο 36

Δοκιμές ασφάλειας ΤΠΕ

1. Οι χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 καταρτίζουν και εφαρμόζουν σχέδιο δοκιμών ασφάλειας ΤΠΕ για την επικύρωση της αποτελεσματικότητας των οικείων μέτρων ασφάλειας ΤΠΕ που αναπτύσσουν σύμφωνα με τα άρθρα 33, 34 και 35, καθώς και τα άρθρα 37 και 38 του παρόντος κανονισμού. Οι χρηματοοικονομικές οντότητες διασφαλίζουν ότι το εν λόγω σχέδιο λαμβάνει υπόψη τις απειλές και τις ευπάθειες που προσδιορίζονται εντός του απλουστευμένου πλαισίου διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 31 του παρόντος κανονισμού.

2. Οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1 επανεξετάζουν, αξιολογούν και δοκιμάζουν τα μέτρα ασφάλειας ΤΠΕ, λαμβάνοντας υπόψη το συνολικό προφίλ κινδύνου των πόρων ΤΠΕ της χρηματοοικονομικής οντότητας.

3. Οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1 παρακολουθούν και αξιολογούν τα αποτελέσματα των δοκιμών ασφαλείας και επικαιροποιούν ανάλογα τα οικεία μέτρα ασφαλείας χωρίς αδικαιολόγητη καθυστέρηση στην περίπτωση συστημάτων ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες.

Άρθρο 37

Απόκτηση, ανάπτυξη και συντήρηση συστημάτων ΤΠΕ

Οι χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 σχεδιάζουν και εφαρμόζουν, κατά περίπτωση, διαδικασία που διέπει την απόκτηση, την ανάπτυξη και τη συντήρηση συστημάτων ΤΠΕ ακολουθώντας προσέγγιση βάσει κινδύνου. Με τη διαδικασία αυτή:

α) διασφαλίζεται ότι, πριν από οποιαδήποτε απόκτηση ή ανάπτυξη συστημάτων ΤΠΕ, οι λειτουργικές και μη λειτουργικές απαιτήσεις, συμπεριλαμβανομένων των απαιτήσεων ασφάλειας των πληροφοριών, καθορίζονται σαφώς και εγκρίνονται από την οικεία επιχειρηματική λειτουργία·

β) διασφαλίζονται οι δοκιμές και η έγκριση των συστημάτων ΤΠΕ πριν από την πρώτη χρήση τους και πριν από την εισαγωγή αλλαγών στο περιβάλλον παραγωγής·

γ) προσδιορίζονται μέτρα για τον μετριασμό του κινδύνου ακούσιας τροποποίησης ή εσκεμμένης χειραγώγησης των συστημάτων ΤΠΕ κατά την ανάπτυξη και την εφαρμογή στο περιβάλλον παραγωγής.

Άρθρο 38

Διαχείριση έργων και αλλαγών ΤΠΕ

1. Οι χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν διαδικασία διαχείρισης έργων ΤΠΕ και καθορίζουν τους ρόλους και τις αρμοδιότητες για την υλοποίησή της. Η εν λόγω διαδικασία καλύπτει όλα τα στάδια των έργων ΤΠΕ από την έναρξή τους έως το κλείσιμό τους.

2. Οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1 αναπτύσσουν, τεκμηριώνουν και εφαρμόζουν διαδικασία διαχείρισης αλλαγών ΤΠΕ για να διασφαλίζουν ότι όλες οι αλλαγές στα συστήματα ΤΠΕ καταγράφονται, δοκιμάζονται, αξιολογούνται, εγκρίνονται, εφαρμόζονται και επαληθεύονται με ελεγχόμενο τρόπο και με επαρκείς διασφαλίσεις για τη διατήρηση της ψηφιακής επιχειρησιακής ανθεκτικότητας της χρηματοοικονομικής οντότητας.

ΚΕΦΑΛΑΙΟ III

Διαχείριση της επιχειρησιακής συνέχειας των ΤΠΕ

Άρθρο 39

Συνιστώσες του σχεδίου επιχειρησιακής συνέχειας των ΤΠΕ

1. Οι χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 καταρτίζουν τα οικεία σχέδια επιχειρησιακής συνέχειας των ΤΠΕ λαμβάνοντας υπόψη τα αποτελέσματα της ανάλυσης της έκθεσής τους σε σοβαρές διαταραχές της επιχειρηματικής δραστηριότητας και των δυνητικών επιπτώσεων των εν λόγω διαταραχών, καθώς και τα σενάρια στα οποία ενδέχεται να εκτεθούν οι πόροι ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες, συμπεριλαμβανομένου ενός σεναρίου κυβερνοεπίθεσης.

2. Τα σχέδια επιχειρησιακής συνέχειας των ΤΠΕ που αναφέρονται στην παράγραφο 1:

α) έχουν εγκριθεί από το διοικητικό όργανο της χρηματοοικονομικής οντότητας·

β) είναι τεκμηριωμένα και εύκολα προσβάσιμα σε περίπτωση έκτακτης ανάγκης ή κρίσης·

γ) κατανέμουν επαρκείς πόρους για την εκτέλεσή τους·

δ) καθορίζουν τα προγραμματισμένα επίπεδα ανάκαμψης και τα χρονοδιαγράμματα για την ανάκαμψη και την επανέναρξη των λειτουργιών και των βασικών εσωτερικών και εξωτερικών εξαρτήσεων, συμπεριλαμβανομένων των τρίτων παρόχων υπηρεσιών ΤΠΕ·

ε) προσδιορίζουν τις προϋποθέσεις που ενδέχεται να οδηγήσουν στην ενεργοποίηση των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ και τις δράσεις που πρέπει να αναληφθούν για τη διασφάλιση της διαθεσιμότητας, της συνέχειας και της ανάκαμψης της λειτουργίας των πόρων ΤΠΕ των χρηματοοικονομικών οντοτήτων που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες·

στ) προσδιορίζουν τα μέτρα αποκατάστασης και ανάκαμψης για κρίσιμες ή σημαντικές επιχειρηματικές λειτουργίες, υποστηρικτικές διαδικασίες, πληροφοριακούς πόρους και τις αλληλεξαρτήσεις τους, ώστε να αποφεύγονται δυσμενείς επιπτώσεις στη λειτουργία των χρηματοοικονομικών οντοτήτων·

ζ) προσδιορίζουν διαδικασίες και μέτρα δημιουργίας εφεδρικών συστημάτων στα οποία προσδιορίζεται το εύρος των δεδομένων που υπόκεινται σε εφεδρικά συστήματα, και την ελάχιστη συχνότητα δημιουργίας αντιγράφων ασφαλείας, βάσει της κρισιμότητας της λειτουργίας που χρησιμοποιεί τα εν λόγω δεδομένα·

η) εξετάζουν εναλλακτικές επιλογές στο πλαίσιο των οποίων η ανάκαμψη ενδέχεται να μην είναι εφικτή βραχυπρόθεσμα λόγω κόστους, κινδύνων, υλικοτεχνικής υποστήριξης ή απρόβλεπτων περιστάσεων·

θ) προσδιορίζουν τις ρυθμίσεις εσωτερικής και εξωτερικής επικοινωνίας, συμπεριλαμβανομένων των σχεδίων παραπομπής συμβάντων·

ι) επικαιροποιούνται σύμφωνα με τα διδάγματα που αντλήθηκαν από περιστατικά, δοκιμές, νέους κινδύνους και απειλές που εντοπίστηκαν, μεταβληθέντες στόχους αποκατάστασης, σημαντικές αλλαγές στην οργάνωση της χρηματοοικονομικής οντότητας και στους πόρους ΤΠΕ που υποστηρίζουν κρίσιμες ή επιχειρηματικές λειτουργίες.

Για τους σκοπούς του στοιχείου στ), τα μέτρα που αναφέρονται στο εν λόγω στοιχείο προβλέπουν τον μετριασμό της αθέτησης υποχρεώσεων κρίσιμων τρίτων παρόχων.

Άρθρο 40

Δοκιμές των σχεδίων επιχειρησιακής συνέχειας

1. Οι χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 δοκιμάζουν τα οικεία σχέδια επιχειρησιακής συνέχειας που αναφέρονται στο άρθρο 39 του παρόντος κανονισμού, συμπεριλαμβανομένων των σεναρίων που αναφέρονται στο εν λόγω άρθρο, τουλάχιστον μία φορά ετησίως για τις διαδικασίες δημιουργίας εφεδρικών συστημάτων και αποκατάστασης, ή σε κάθε σημαντική αλλαγή του σχεδίου επιχειρησιακής συνέχειας.

2. Οι δοκιμές των σχεδίων επιχειρησιακής συνέχειας που αναφέρονται στην παράγραφο 1 αποδεικνύουν ότι οι χρηματοοικονομικές οντότητες που αναφέρονται στην εν λόγω παράγραφο είναι σε θέση να διατηρήσουν τη βιωσιμότητα των επιχειρήσεών τους έως ότου αποκατασταθούν οι κρίσιμες δραστηριότητες και εντοπίζουν τυχόν ελλείψεις στα εν λόγω σχέδια.

3. Οι χρηματοοικονομικές οντότητες που αναφέρονται στην παράγραφο 1 τεκμηριώνουν τα αποτελέσματα των δοκιμών των σχεδίων επιχειρησιακής συνέχειας και τυχόν ελλείψεις που εντοπίζονται και προκύπτουν από τις εν λόγω δοκιμές αναλύονται, αντιμετωπίζονται και αναφέρονται στο διοικητικό όργανο.

ΚΕΦΑΛΑΙΟ IV

Έκθεση σχετικά με την επανεξέταση του απλουστευμένου πλαισίου διαχείρισης κινδύνων ΤΠΕ

Άρθρο 41

Μορφή και περιεχόμενο της έκθεσης σχετικά με την επανεξέταση του απλουστευμένου πλαισίου διαχείρισης κινδύνων ΤΠΕ

1. Οι χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 16 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 υποβάλλουν την έκθεση σχετικά με την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 2 του εν λόγω άρθρου σε ηλεκτρονική μορφή με δυνατότητα αναζήτησης.

2. Η έκθεση που αναφέρεται στην παράγραφο 1 περιέχει όλες τις ακόλουθες πληροφορίες:

α) ένα εισαγωγικό τμήμα το οποίο παρέχει:

i) περιγραφή του πλαισίου της έκθεσης όσον αφορά τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της χρηματοοικονομικής οντότητας, την οργάνωσή της, τις προσδιορισμένες κρίσιμες λειτουργίες, τη στρατηγική, μείζονα υπό εξέλιξη έργα ή δραστηριότητες, τις σχέσεις και την εξάρτηση της χρηματοοικονομικής οντότητας από ενδοεπιχειρησιακές και ανατεθείσες υπηρεσίες και συστήματα ΤΠΕ ή τις επιπτώσεις που θα είχε η ολική απώλεια ή σοβαρή υποβάθμιση των εν λόγω συστημάτων σε κρίσιμες ή σημαντικές λειτουργίες και στην αποτελεσματικότητα της αγοράς·

ii) συνοπτική παρουσίαση των υφιστάμενων και των βραχυπρόθεσμων κινδύνων ΤΠΕ που έχουν εντοπιστεί, του τοπίου των απειλών, της εκτιμώμενης αποτελεσματικότητας των δικλείδων ασφαλείας της και των πολιτικών ασφάλειας της χρηματοοικονομικής οντότητας·

iii) πληροφορίες σχετικά με τον αναφερόμενο τομέα·

iv) σύνοψη των σημαντικών αλλαγών στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ από την προηγούμενη έκθεση·

v) σύνοψη και περιγραφή των επιπτώσεων των σημαντικών αλλαγών στο απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ από την προηγούμενη έκθεση·

β) κατά περίπτωση, την ημερομηνία έγκρισης της έκθεσης από το διοικητικό όργανο της χρηματοοικονομικής οντότητας·

γ) περιγραφή των λόγων της επανεξέτασης, η οποία περιλαμβάνει:

i) όταν η έναρξη της επανεξέτασης προκύπτει κατόπιν εποπτικών οδηγιών, αποδεικτικά στοιχεία των εν λόγω οδηγιών·

ii) όταν η επανεξέταση έχει ξεκινήσει μετά την εμφάνιση συμβάντων που σχετίζονται με τις ΤΠΕ, τον κατάλογο όλων των συμβάντων που σχετίζονται με τις ΤΠΕ με ανάλυση των βαθύτερων αιτίων του σχετικού συμβάντος·

δ) τις ημερομηνίες έναρξης και λήξης της περιόδου επανεξέτασης·

ε) το πρόσωπο που είναι υπεύθυνο για την επανεξέταση·

στ) σύνοψη των πορισμάτων και αυτοαξιολόγηση της σοβαρότητας των αδυναμιών, των ελλείψεων και των κενών που εντοπίστηκαν στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ για την περίοδο επανεξέτασης, συμπεριλαμβανομένης λεπτομερούς ανάλυσής τους·

ζ) τα μέτρα αποκατάστασης που προσδιορίστηκαν για την αντιμετώπιση αδυναμιών, ελλείψεων και κενών στο απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ, καθώς και την αναμενόμενη ημερομηνία εφαρμογής των εν λόγω μέτρων, συμπεριλαμβανομένης της παρακολούθησης των αδυναμιών, των ελλείψεων και των κενών που εντοπίστηκαν σε προηγούμενες εκθέσεις, όταν οι εν λόγω αδυναμίες, ελλείψεις και κενά δεν έχουν ακόμη αποκατασταθεί·

η) συνολικά συμπεράσματα σχετικά με την επανεξέταση του απλουστευμένου πλαισίου διαχείρισης κινδύνων ΤΠΕ, συμπεριλαμβανομένων τυχόν περαιτέρω προγραμματισμένων εξελίξεων.

ΤΙΤΛΟΣ IV

ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 42

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 Μαρτίου 2024.

Για την Επιτροπή
Η Πρόεδρος
Ursula VON DER LEYEN