2024/482

7.2.2024

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2024/482 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 31ης Ιανουαρίου 2024

για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την έγκριση του ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων (EUCC)

(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) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) ([1]), και ιδίως το άρθρο 49 παράγραφος 7,

Εκτιμώντας τα ακόλουθα:

(1) Με τον παρόντα κανονισμό προσδιορίζονται οι ρόλοι, οι κανόνες και οι υποχρεώσεις καθώς και η δομή του βασισμένου σε κοινά κριτήρια ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας (EUCC), σύμφωνα με το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας που περιγράφεται στον κανονισμό (ΕΕ) 2019/881. Το EUCC βασίζεται στη συμφωνία αμοιβαίας αναγνώρισης (στο εξής: ΣΑΑ) των πιστοποιητικών ασφάλειας της τεχνολογίας των πληροφοριών της Ομάδας Ανώτερων Υπαλλήλων για την Ασφάλεια των Συστημάτων Πληροφοριών ([2]) (στο εξής: SOG-IS) που χρησιμοποιούν τα κοινά κριτήρια, συμπεριλαμβανομένων των διαδικασιών και των εγγράφων της SOG-IS.

(2) Το σχήμα θα πρέπει να βασίζεται σε θεσπισθέντα διεθνή πρότυπα. Τα κοινά κριτήρια (Common Criteria) είναι διεθνές πρότυπο για την αξιολόγηση της ασφάλειας των πληροφοριών, το οποίο δημοσιεύθηκε, για παράδειγμα, ως ISO/IEC 15408 Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικότητας — Κριτήρια αξιολόγησης για την ασφάλεια της τεχνολογίας πληροφοριών. Βασίζεται σε αξιολόγηση από τρίτους και προβλέπει επτά επίπεδα διασφάλισης της αξιολόγησης (EAL). Τα κοινά κριτήρια συνοδεύονται από την κοινή μεθοδολογία αξιολόγησης (Common Evaluation Methodology), η οποία δημοσιεύθηκε, για παράδειγμα, ως ISO/IEC 18045 — Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικότητας — Κριτήρια αξιολόγησης για την ασφάλεια της τεχνολογίας πληροφοριών — Μεθοδολογία για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών. Οι προδιαγραφές και τα έγγραφα που εφαρμόζουν τις διατάξεις του παρόντος κανονισμού μπορεί να σχετίζονται με δημόσια διαθέσιμο πρότυπο, το οποίο προσομοιάζει το πρότυπο εκείνο που χρησιμοποιείται για την πιστοποίηση δυνάμει του παρόντος κανονισμού, όπως τα κοινά κριτήρια για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών και η κοινή μεθοδολογία για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών.

(3) Το EUCC χρησιμοποιεί τις συνιστώσες 1 έως 5 της προδιαγραφής αξιολόγησης της τρωτότητας (AVA_VAN) των κοινών κριτηρίων. Οι πέντε συνιστώσες παρέχουν όλους τους κύριους καθοριστικούς παράγοντες και τις εξαρτήσεις για την ανάλυση των τρωτών σημείων των προϊόντων ΤΠΕ. Δεδομένου ότι οι συνιστώσες αντιστοιχούν στα επίπεδα διασφάλισης του παρόντος κανονισμού, καθιστούν δυνατή την τεκμηριωμένη επιλογή διασφάλισης, βάσει αξιολογήσεων των απαιτήσεων ασφάλειας και του κινδύνου που σχετίζεται με την προβλεπόμενη χρήση του προϊόντος ΤΠΕ. Ο αιτών πιστοποιητικό EUCC θα πρέπει να παρέχει την τεκμηρίωση που σχετίζεται με την προβλεπόμενη χρήση του προϊόντος ΤΠΕ και την ανάλυση των επιπέδων κινδύνου που σχετίζονται με την εν λόγω χρήση, ώστε ο οργανισμός αξιολόγησης της συμμόρφωσης να μπορεί να αξιολογήσει την καταλληλότητα του επιλεγμένου επιπέδου διασφάλισης. Όταν οι δραστηριότητες αξιολόγησης και πιστοποίησης εκτελούνται από τον ίδιο οργανισμό αξιολόγησης της συμμόρφωσης, ο αιτών θα πρέπει να υποβάλει τις ζητούμενες πληροφορίες μόνον άπαξ.

(4) Ως τεχνικός τομέας νοείται ένα πλαίσιο αναφοράς το οποίο καλύπτει ομάδα προϊόντων ΤΠΕ που έχουν ειδική και παρόμοια λειτουργικότητα ασφάλειας η οποία μετριάζει τις επιθέσεις όταν τα χαρακτηριστικά είναι κοινά σε συγκεκριμένο επίπεδο διασφάλισης. Ο τεχνικός τομέας περιγράφει σε έγγραφα στάθμης της τεχνικής τις ειδικές απαιτήσεις ασφάλειας καθώς και πρόσθετες μεθόδους, τεχνικές και εργαλεία αξιολόγησης που εφαρμόζονται στην πιστοποίηση προϊόντων ΤΠΕ που καλύπτονται από τον εν λόγω τεχνικό τομέα. Επομένως, ο τεχνικός τομέας προάγει επίσης την εναρμόνιση της αξιολόγησης

([1]) ΕΕ L 151 της 7.6.2019, σ. 15.

([2]) Συμφωνία αμοιβαίας αναγνώρισης πιστοποιητικών αξιολόγησης της ασφάλειας της τεχνολογίας πληροφοριών (έκδοση 3.0 του Ιανουαρίου του 2010, διατίθεται στον ιστότοπο sogis.eu), η οποία εγκρίθηκε από την Ομάδα Ανώτερων Υπαλλήλων για την Ασφάλεια των Συστημάτων Πληροφοριών της Ευρωπαϊκής Επιτροπής ως απόκριση στο σημείο 3 της σύστασης 95/144/ΕΚ του Συμβουλίου, της 7ης Απριλίου 1995, για κοινά κριτήρια ασφαλείας της τεχνολογίας πληροφοριών (ΕΕ L 93 της 26.4.1995, σ. 27).

των καλυπτόμενων προϊόντων ΤΠΕ. Επί του παρόντος, δύο τεχνικοί τομείς χρησιμοποιούνται ευρέως για την πιστοποίηση στα επίπεδα AVA_VAN.4 και AVA_VAN.5. Ο πρώτος είναι ο τεχνικός τομέας «Έξυπνες κάρτες και παρεμφερείς διατάξεις», στον οποίο σημαντικό μέρος της απαιτούμενης λειτουργικότητας ασφάλειας εξαρτάται από ειδικά, εξατομικευμένα και συχνά διαχωρίσιμα στοιχεία υλισμικού [π.χ. υλισμικό έξυπνης κάρτας, ολοκληρωμένα κυκλώματα, σύνθετα προϊόντα έξυπνης κάρτας, δομοστοιχεία Trusted Platform Module τα οποία χρησιμοποιούνται στην έμπιστη υπολογιστική (trusted computing) ή κάρτες ψηφιακού ταχογράφου]. Ο δεύτερος είναι ο τεχνικός τομέας «Διατάξεις υλισμικού με θυρίδες ασφαλείας», στον οποίο σημαντικό μέρος της απαιτούμενης λειτουργικότητας ασφάλειας εξαρτάται από υλικό περίβλημα υλισμικού (το οποίο ονομάζεται «θυρίδα ασφαλείας») σχεδιασμένο κατά τρόπο ώστε να είναι ανθεκτικό σε άμεσες επιθέσεις (π.χ. τερματικά πληρωμής, εποχούμενες μονάδες ταχογράφου, έξυπνοι μετρητές, τερματικά ελέγχου πρόσβασης και δομοστοιχεία ασφάλειας λογισμικού).

(5) Όταν υποβάλλει αίτηση πιστοποίησης, ο αιτών θα πρέπει να συνδέει τη συλλογιστική του για την επιλογή επιπέδου διασφάλισης με τους στόχους που περιγράφονται στο άρθρο 51 του κανονισμού (ΕΕ) 2019/881 και με την επιλογή συνιστωσών από τον κατάλογο λειτουργικών απαιτήσεων ασφάλειας και απαιτήσεων κατοχύρωσης της ασφάλειας που περιλαμβάνονται στα κοινά κριτήρια. Οι οργανισμοί πιστοποίησης θα πρέπει να αξιολογούν την καταλληλότητα του επιλεγέντος επιπέδου διασφάλισης και να διασφαλίζουν ότι το επιλεγέν επίπεδο είναι ανάλογο προς το επίπεδο κινδύνου που συνδέεται με την προβλεπόμενη χρήση του προϊόντος ΤΠΕ.

(6) Βάσει των κοινών κριτηρίων, η πιστοποίηση διενεργείται ως προς έναν στόχο ασφάλειας, ο οποίος περιλαμβάνει ορισμό του προβλήματος ασφάλειας του προϊόντος ΤΠΕ καθώς και τους στόχους ασφάλειας που αντιμετωπίζουν το πρόβλημα ασφάλειας. Το πρόβλημα ασφάλειας παρέχει πληροφορίες σχετικά με την προβλεπόμενη χρήση του προϊόντος ΤΠΕ και τους κινδύνους που συνδέονται με την εν λόγω χρήση. Ένα ειδικό σύνολο απαιτήσεων ασφάλειας αποκρίνεται τόσο στο πρόβλημα ασφάλειας όσο και στους στόχους ασφάλειας του προϊόντος ΤΠΕ.

(7) Τα χαρακτηριστικά προστασίας είναι ένα αποτελεσματικό μέσο για τον προκαθορισμό των κοινών κριτηρίων που μπορούν να εφαρμοστούν σε συγκεκριμένη κατηγορία προϊόντων ΤΠΕ και, ως εκ τούτου, είναι επίσης σημαντικό στοιχείο της διαδικασίας πιστοποίησης προϊόντων ΤΠΕ που καλύπτονται από το χαρακτηριστικό προστασίας. Τα χαρακτηριστικά προστασίας χρησιμοποιούνται για την αξιολόγηση μελλοντικών στόχων ασφάλειας οι οποίοι εμπίπτουν στη συγκεκριμένη κατηγορία προϊόντων ΤΠΕ που αφορά το συγκεκριμένο χαρακτηριστικό προστασίας. Τα χαρακτηριστικά προστασίας εξορθολογίζουν και βελτιώνουν περαιτέρω την αποδοτικότητα της διαδικασίας πιστοποίησης του προϊόντος ΤΠΕ και βοηθούν τους χρήστες να προσδιορίζουν ορθά και αποτελεσματικά τη λειτουργικότητα του προϊόντος ΤΠΕ. Επομένως, τα χαρακτηριστικά προστασίας θα πρέπει να θεωρούνται αναπόσπαστο μέρος της διαδικασίας ΤΠΕ που καταλήγει στην πιστοποίηση προϊόντων ΤΠΕ.

(8) Προκειμένου να μπορούν να επιτελέσουν τον ρόλο τους στη διαδικασία ΤΠΕ που στηρίζει την ανάπτυξη και την παράδοση πιστοποιημένου προϊόντος ΤΠΕ, τα ίδια τα χαρακτηριστικά προστασίας θα πρέπει να μπορούν να πιστοποιηθούν ανεξάρτητα από την πιστοποίηση του συγκεκριμένου προϊόντος ΤΠΕ που καλύπτεται από το αντίστοιχο χαρακτηριστικό προστασίας. Ως εκ τούτου, είναι απαραίτητο στα χαρακτηριστικά προστασίας να εφαρμόζεται τουλάχιστον το ίδιο επίπεδο ελέγχου με εκείνο που εφαρμόζεται στους στόχους ασφάλειας, προκειμένου να διασφαλίζεται υψηλό επίπεδο κυβερνοασφάλειας. Τα χαρακτηριστικά προστασίας θα πρέπει να αξιολογούνται και να πιστοποιούνται χωριστά από το σχετικό προϊόν ΤΠΕ και μόνον μέσω της εφαρμογής της κλάσης διασφάλισης των κοινών κριτηρίων και της κοινής μεθοδολογίας αξιολόγησης για χαρακτηριστικά προστασίας (APE) και, όπου συντρέχει περίπτωση, για διαμορφώσεις χαρακτηριστικών προστασίας (ACE). Λόγω του σημαντικού και ευαίσθητου ρόλου των χαρακτηριστικών προστασίας ως σημείου αναφοράς κατά την πιστοποίηση προϊόντων ΤΠΕ, τα χαρακτηριστικά προστασίας θα πρέπει να πιστοποιούνται μόνον από δημόσιους οργανισμούς ή από οργανισμό πιστοποίησης ο οποίος έχει λάβει προηγούμενη έγκριση για το συγκεκριμένο χαρακτηριστικό προστασίας από την εθνική αρχή πιστοποίησης της κυβερνοασφάλειας. Λόγω του σημαντικού ρόλου τους για την πιστοποίηση με «υψηλό» επίπεδο διασφάλισης, ειδικότερα εκτός τεχνικών τομέων, τα χαρακτηριστικά προστασίας θα πρέπει να αναπτύσσονται με τη μορφή εγγράφων στάθμης της τεχνικής τα οποία θα πρέπει να εγκρίνονται από την ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας (στο εξής: ΕΟΠΙΚ).

(9) Τα πιστοποιημένα χαρακτηριστικά προστασίας θα πρέπει να περιλαμβάνονται στην παρακολούθηση της συμμόρφωσης του EUCC από τις εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας. Σε περίπτωση που για συγκεκριμένα πιστοποιημένα χαρακτηριστικά προστασίας διατίθενται η μεθοδολογία, τα εργαλεία και οι δεξιότητες που εφαρμόζονται σε προσεγγίσεις για την αξιολόγηση των προϊόντων ΤΠΕ, οι τεχνικοί τομείς μπορούν να βασίζονται στα εν λόγω συγκεκριμένα χαρακτηριστικά προστασίας.

(10) Προκειμένου να επιτευχθεί υψηλό επίπεδο εμπιστοσύνης και διασφάλισης για τα πιστοποιημένα προϊόντα ΤΠΕ, η αυτοαξιολόγηση δεν θα πρέπει να επιτρέπεται βάσει του παρόντος κανονισμού. Θα πρέπει να επιτρέπεται μόνον αξιολόγηση της συμμόρφωσης από τρίτους και συγκεκριμένα την εγκατάσταση αξιολόγησης της ασφάλειας της τεχνολογίας πληροφοριών και τους οργανισμούς πιστοποίησης.

(11) Η κοινότητα SOG-IS παρείχε κοινές ερμηνείες και προσεγγίσεις για την εφαρμογή στην πιστοποίηση των κοινών κριτηρίων και της κοινής μεθοδολογίας αξιολόγησης, ειδικότερα για το «υψηλό» επίπεδο διασφάλισης που επιδιώκεται στους τεχνικούς τομείς «Έξυπνες κάρτες και παρεμφερείς διατάξεις» και «Διατάξεις υλισμικού με θυρίδες ασφαλείας». Η εκ νέου χρήση τέτοιας συνοδευτικής τεκμηρίωσης στο σχήμα EUCC διασφαλίζει την ομαλή μετάβαση από τα εθνικά εφαρμοζόμενα σχήματα της SOG-IS στο εναρμονισμένο σχήμα EUCC. Ως εκ τούτου, στον παρόντα κανονισμό θα πρέπει να περιληφθούν εναρμονισμένες μεθοδολογίες αξιολόγησης οι οποίες είναι γενικά χρήσιμες για όλες τις δραστηριότητες πιστοποίησης. Επιπλέον, η Επιτροπή θα πρέπει να μπορεί να ζητεί από την ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας να εκδίδει γνώμη, με την οποία θα εγκρίνει και θα συνιστά την εφαρμογή μεθοδολογιών αξιολόγησης που προσδιορίζονται σε έγγραφα στάθμης της τεχνικής για την πιστοποίηση του προϊόντος ΤΠΕ ή του χαρακτηριστικού προστασίας στο πλαίσιο του σχήματος EUCC. Κατά συνέπεια, στο παράρτημα Ι του παρόντος κανονισμού παρατίθενται τα έγγραφα στάθμης της τεχνικής για τις δραστηριότητες αξιολόγησης που εκτελούν οργανισμοί αξιολόγησης της συμμόρφωσης. Επομένως, η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας θα πρέπει να εγκρίνει και να τηρεί έγγραφα στάθμης της τεχνικής. Τα έγγραφα στάθμης της τεχνικής θα πρέπει να χρησιμοποιούνται στην πιστοποίηση. Μόνο σε εξαιρετικές και δεόντως αιτιολογημένες περιπτώσεις μπορεί ένας οργανισμός αξιολόγησης της συμμόρφωσης να μην τα χρησιμοποιήσει, υπό συγκεκριμένες προϋποθέσεις όπως, ειδικότερα, η έγκριση της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας.

(12) Η πιστοποίηση προϊόντων ΤΠΕ σε επίπεδο AVA_VAN 4 ή 5 θα πρέπει να είναι δυνατή μόνον υπό συγκεκριμένες προϋποθέσεις και σε περίπτωση που υπάρχει συγκεκριμένη μεθοδολογία αξιολόγησης. Η συγκεκριμένη μεθοδολογία αξιολόγησης μπορεί να κατοχυρώνεται σε έγγραφα στάθμης της τεχνικής σχετικά με τον τεχνικό τομέα ή σε συγκεκριμένα χαρακτηριστικά προστασίας τα οποία θεσπίζονται ως έγγραφα στάθμης της τεχνικής σχετικά με την οικεία κατηγορία προϊόντος. Μόνο σε εξαιρετικές και δεόντως αιτιολογημένες περιπτώσεις θα πρέπει να είναι δυνατή η πιστοποίηση των εν λόγω επιπέδων διασφάλισης, υπό συγκεκριμένες προϋποθέσεις όπως, ειδικότερα, η έγκριση εκ μέρους της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας, συμπεριλαμβανομένης της εφαρμοστέας μεθοδολογίας αξιολόγησης. Τέτοιες εξαιρετικές και δεόντως αιτιολογημένες περιπτώσεις μπορεί να συντρέχουν όταν η ενωσιακή ή η εθνική νομοθεσία απαιτεί την πιστοποίηση προϊόντος ΤΠΕ σε επίπεδο AVA_VAN 4 ή 5. Ομοίως, σε εξαιρετικές και δεόντως αιτιολογημένες περιπτώσεις, χαρακτηριστικά προστασίας μπορούν να πιστοποιηθούν χωρίς την εφαρμογή των σχετικών εγγράφων στάθμης της τεχνικής, υπό συγκεκριμένες προϋποθέσεις, ειδικότερα την έγκριση της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας, συμπεριλαμβανομένης της εφαρμοστέας μεθοδολογίας αξιολόγησης.

(13) Στόχος των σημάτων και των επισημάνσεων που χρησιμοποιούνται στο πλαίσιο του EUCC είναι να καταδεικνύεται εμφανώς στους χρήστες η αξιοπιστία του πιστοποιημένου προϊόντος ΤΠΕ, ώστε να μπορούν να προβαίνουν σε τεκμηριωμένη επιλογή κατά την αγορά προϊόντων ΤΠΕ. Η χρήση σημάτων και επισημάνσεων θα πρέπει επίσης να υπόκειται στους κανόνες και στις προϋποθέσεις που καθορίζονται στο πρότυπο ISO/IEC 17065 και, κατά περίπτωση, στο πρότυπο ISO/IEC 17030 με την αντίστοιχη καθοδήγηση.

(14) Οι οργανισμοί πιστοποίησης θα πρέπει να αποφασίζουν την περίοδο ισχύος των πιστοποιητικών λαμβάνοντας υπόψη τον κύκλο ζωής του οικείου προϊόντος ΤΠΕ. Η περίοδος ισχύος δεν θα πρέπει να υπερβαίνει τα 5 έτη. Οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας θα πρέπει να καταβάλουν προσπάθειες ώστε να εναρμονίσουν την περίοδο ισχύος στην Ένωση.

(15) Σε περίπτωση περιορισμού του πεδίου ενός υφιστάμενου πιστοποιητικού EUCC το πιστοποιητικό ανακαλείται, θα πρέπει δε να εκδίδεται νέο πιστοποιητικό με το νέο πεδίο ώστε να διασφαλίζεται ότι οι χρήστες είναι σαφώς ενημερωμένοι σχετικά με το ισχύον πεδίο και επίπεδο διασφάλισης του πιστοποιητικού συγκεκριμένου προϊόντος ΤΠΕ.

(16) Η πιστοποίηση χαρακτηριστικών προστασίας διαφέρει από την πιστοποίηση προϊόντων ΤΠΕ, καθώς αφορά μια διαδικασία ΤΠΕ. Δεδομένου ότι το χαρακτηριστικό προστασίας αφορά μια κατηγορία προϊόντων ΤΠΕ, η αξιολόγηση και η πιστοποίησή του δεν μπορούν να πραγματοποιούνται βάσει ενός και μόνον προϊόντος ΤΠΕ. Δεδομένου ότι το χαρακτηριστικό προστασίας ενοποιεί τις γενικές απαιτήσεις ασφάλειας όσον αφορά μια κατηγορία προϊόντων ΤΠΕ και ανεξαρτήτως της δήλωσης του προϊόντος ΤΠΕ από τον πωλητή του, η περίοδος ισχύος πιστοποιητικού EUCC για χαρακτηριστικό προστασίας θα πρέπει, καταρχήν, να είναι τουλάχιστον 5 έτη και μπορεί να εκτείνεται στη διάρκεια ζωής του χαρακτηριστικού προστασίας.

(17) Ως οργανισμός αξιολόγησης της συμμόρφωσης νοείται οργανισμός ο οποίος πραγματοποιεί δραστηριότητες αξιολόγησης της συμμόρφωσης, συμπεριλαμβανομένων βαθμονομήσεων, δοκιμών, πιστοποίησης και επιθεώρησης. Με σκοπό την εξασφάλιση υπηρεσιών υψηλής ποιότητας, στον παρόντα κανονισμό διευκρινίζεται ότι οι δραστηριότητες δοκιμής, αφενός, και οι δραστηριότητες πιστοποίησης και επιθεώρησης, αφετέρου, θα πρέπει να εκτελούνται από οντότητες που λειτουργούν ανεξάρτητα οι μεν από τις δε, και συγκεκριμένα από εγκαταστάσεις αξιολόγησης της ασφάλειας της τεχνολογίας πληροφοριών (στο εξής: ΕΑΑΤΠ) και οργανισμούς πιστοποίησης, αντίστοιχα. Αμφότεροι οι ως άνω οργανισμοί αξιολόγησης της συμμόρφωσης θα πρέπει να είναι διαπιστευμένοι και, σε ορισμένες περιπτώσεις, εξουσιοδοτημένοι.

(18) Ο οργανισμός πιστοποίησης θα πρέπει να λαμβάνει διαπίστευση από τον εθνικό οργανισμό πιστοποίησης σύμφωνα με το πρότυπο ISO/IEC 17065 για το «σημαντικό» και το «υψηλό» επίπεδο διασφάλισης. Επιπλέον της διαπίστευσης σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 σε συνδυασμό με τον κανονισμό (ΕΚ) αριθ. 765/2008, οι οργανισμοί αξιολόγησης της συμμόρφωσης θα πρέπει να πληρούν ειδικές προϋποθέσεις προκειμένου να διασφαλίζεται η τεχνική ικανότητά τους για την αξιολόγηση απαιτήσεων κυβερνοασφάλειας στο πλαίσιο του «υψηλού» επιπέδου διασφάλισης του EUCC, ικανότητα η οποία επιβεβαιώνεται μέσω «εξουσιοδότησης». Για τη στήριξη της διαδικασίας εξουσιοδότησης, θα πρέπει να καταρτιστούν έγγραφα στάθμης της τεχνικής, τα οποία ο ENISA θα δημοσιεύει κατόπιν έγκρισης της ευρωπαϊκής ομάδας πιστοποίησης της κυβερνοασφάλειας.

(19) Η τεχνική ικανότητα μιας ΕΑΑΤΠ θα πρέπει να αξιολογείται μέσω της διαπίστευσης του εργαστηρίου δοκιμών σύμφωνα με το πρότυπο ISO/IEC 17025 και να συμπληρώνεται με την εφαρμογή του προτύπου ISO/IEC 23532-1 για το πλήρες σύνολο των δραστηριοτήτων αξιολόγησης που είναι κρίσιμες για το επίπεδο διασφάλισης και προσδιορίζονται στο πρότυπο ISO/IEC 18045 σε συνδυασμό με το πρότυπο ISO/IEC 15408. Τόσο ο οργανισμός πιστοποίησης όσο και η ΕΑΑΤΠ θα πρέπει να θεσπίζουν και να διατηρούν κατάλληλο σύστημα διαχείρισης ικανοτήτων όσον αφορά το προσωπικό, το οποίο βασίζεται στο πρότυπο ISO/IEC 19896-1 για τα στοιχεία και τα επίπεδα ικανότητας και για την εκτίμηση της ικανότητας. Για το επίπεδο γνώσεων, δεξιοτήτων, πείρας και εκπαίδευσης, οι εφαρμοστέες απαιτήσεις για τους αξιολογητές θα πρέπει να αντλούνται από το πρότυπο ISO/IEC 19896-3. Ισοδύναμες διατάξεις και μέτρα που αφορούν αποκλίσεις από τα εν λόγω συστήματα διαχείρισης ικανοτήτων θα πρέπει να αποδεικνύονται, σύμφωνα με τους στόχους του συστήματος.

(20) Προκειμένου να λάβει εξουσιοδότηση, η ΕΑΑΤΠ θα πρέπει να αποδεικνύει την ικανότητά της να εξακριβώνει την ανυπαρξία γνωστών τρωτών σημείων, την ορθή και συνεπή εφαρμογή λειτουργικοτήτων ασφάλειας προηγμένης τεχνολογίας για τη συγκεκριμένη τεχνολογία και την ανθεκτικότητα του στοχευμένου προϊόντος ΤΠΕ σε επιδέξιους επιτιθέμενους. Επιπλέον, για εξουσιοδοτήσεις στον τεχνικό τομέα «Έξυπνες κάρτες και παρεμφερείς διατάξεις», η ΕΑΑΤΠ θα πρέπει να αποδεικνύει ότι διαθέτει επίσης τις τεχνικές ικανότητες οι οποίες είναι αναγκαίες για τις δραστηριότητες αξιολόγησης και τα σχετικά καθήκοντα όπως ορίζονται στη συνοδευτική τεκμηρίωση «Ελάχιστες απαιτήσεις ΕΑΑΤΠ για αξιολογήσεις ασφάλειας έξυπνων καρτών και παρεμφερών διατάξεων» ([3]) στο πλαίσιο των κοινών κριτηρίων. Για εξουσιοδοτήσεις στον τεχνικό τομέα «Διατάξεις υλισμικού με θυρίδες ασφαλείας», η ΕΑΑΤΠ θα πρέπει να αποδεικνύει, επιπλέον, ότι πληροί τις ελάχιστες τεχνικές απαιτήσεις οι οποίες είναι αναγκαίες για την εκτέλεση δραστηριοτήτων αξιολόγησης και σχετικών καθηκόντων σε διατάξεις υλισμού με θυρίδες ασφαλείας, κατά τις συστάσεις της ΕΟΠΙΚ. Στο πλαίσιο των ελάχιστων απαιτήσεων, η ΕΑΑΤΠ θα πρέπει να μπορεί να εκτελεί τους διαφόρους τύπους επιθέσεων που περιγράφονται στη συνοδευτική τεκμηρίωση «Εφαρμογή κινδύνου επίθεσης σε διατάξεις υλισμικού με θυρίδες ασφαλείας» στο πλαίσιο των κοινών κριτηρίων. Οι ως άνω ικανότητες θα πρέπει να περιλαμβάνουν τις γνώσεις και τις δεξιότητες του αξιολογητή και τον εξοπλισμό και τις μεθόδους αξιολόγησης που απαιτούνται για τον καθορισμό και την αξιολόγηση των διαφόρων τύπων επιθέσεων.

(21) Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας θα πρέπει να παρακολουθεί τη συμμόρφωση των οργανισμών πιστοποίησης, της ΕΑΤΤΠ και των κατόχων πιστοποιητικών με τις υποχρεώσεις που υπέχουν από τον παρόντα κανονισμό και τον κανονισμό (ΕΕ) 2019/881. Προς τούτο, η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας θα πρέπει να χρησιμοποιεί κάθε κατάλληλη πηγή πληροφοριών, συμπεριλαμβανομένων πληροφοριών που αποκτά από συμμετέχοντες στη διαδικασία πιστοποίησης και από ίδιες έρευνες.

(22) Οι οργανισμοί πιστοποίησης θα πρέπει να συνεργάζονται με τις αρμόδιες αρχές εποπτείας της αγοράς και να λαμβάνουν υπόψη κάθε πληροφορία σχετικά με τρωτά σημεία η οποία μπορεί να έχει σημασία για τα προϊόντα ΤΠΕ για τα οποία έχουν εκδώσει πιστοποιητικά. Οι οργανισμοί πιστοποίησης θα πρέπει να παρακολουθούν τα χαρακτηριστικά προστασίας που έχουν πιστοποιήσει ώστε να εξακριβώνουν κατά πόσον οι απαιτήσεις ασφάλειας που καθορίζονται για μια κατηγορία προϊόντων ΤΠΕ εξακολουθούν να αντικατοπτρίζουν τις πιο πρόσφατες εξελίξεις όσον αφορά τις κυβερνοαπειλές.

(23) Με σκοπό τη στήριξη της παρακολούθησης της συμμόρφωσης, οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας θα πρέπει να συνεργάζονται με τις αρμόδιες αρχές εποπτείας της αγοράς σύμφωνα με το άρθρο 58 του κανονισμού (ΕΕ) 2019/881 και με τον κανονισμό (ΕΕ) 2019/1020 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]). Δυνάμει του άρθρου 4 παράγραφος 3 του κανονισμού 2019/1020, οι οικονομικοί φορείς της Ένωσης υποχρεούνται να ανταλλάσσουν πληροφορίες και να συνεργάζονται με τις αρχές εποπτείας της αγοράς.

([3]) Joint Interpretation Library: Minimum ITSEF Requirements for Security Evaluations of Smart cards and similar devices (Ελάχιστες απαιτήσεις ΕΑΑΤΠ για αξιολογήσεις ασφάλειας έξυπνων καρτών και παρεμφερών διατάξεων), έκδοση 2.1, Φεβρουάριος 2020, διατίθεται στον ιστότοπο sogis.eu.

([4]) Κανονισμός (ΕΕ) 2019/1020 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Ιουνίου 2019, για την εποπτεία της αγοράς και τη συμμόρφωση των προϊόντων και για την κατάργηση της οδηγίας 2004/42/ΕΚ και των κανονισμών (ΕΚ) αριθ. 765/2008 και (ΕΕ) αριθ. 305/2011 (ΕΕ L 169 της 25.6.2019, σ. 1).

(24) Οι οργανισμοί πιστοποίησης θα πρέπει να παρακολουθούν τη συμμόρφωση των κατόχων πιστοποιητικών και τη συμμόρφωση όλων των πιστοποιητικών που εκδίδονται στο πλαίσιο του EUCC. Η παρακολούθηση θα πρέπει να διασφαλίζει ότι όλες οι εκθέσεις παρακολούθησης που υποβάλλει η ΕΑΑΤΠ, και τα συμπεράσματα που περιέχονται σε αυτές, καθώς και τα κριτήρια και οι μέθοδοι αξιολόγησης εφαρμόζονται με συνεπή και ορθό τρόπο σε όλες τις δραστηριότητες πιστοποίησης.

(25) Όταν εντοπίζονται δυνητικά ζητήματα μη συμμόρφωσης τα οποία επηρεάζουν ένα πιστοποιημένο προϊόν ΤΠΕ, είναι σημαντικό να διασφαλίζεται απόκριση αναλογική προς τη δυνητική μη συμμόρφωση. Επομένως, τα πιστοποιητικά μπορεί να ανασταλούν. Η αναστολή θα πρέπει να συνεπάγεται ορισμένους περιορισμούς όσον αφορά την προώθηση και τη χρήση του οικείου προϊόντος ΤΠΕ, αλλά δεν θα πρέπει να θίγει το κύρος του πιστοποιητικού. Η αναστολή θα πρέπει να κοινοποιείται στους αγοραστές των επηρεαζόμενων προϊόντων ΤΠΕ από τον κάτοχο του πιστοποιητικού EUCC, οι δε αρμόδιες αρχές εποπτείας της αγοράς θα πρέπει να ενημερώνονται από την αρμόδια εθνική αρχή πιστοποίησης της κυβερνοασφάλειας. Για την ενημέρωση του κοινού, ο ENISA θα πρέπει να δημοσιεύει πληροφορίες σχετικά με τις αναστολές σε ειδικό ιστότοπο.

(26) Ο κάτοχος πιστοποιητικού EUCC θα πρέπει να εφαρμόζει τις αναγκαίες διαδικασίες διαχείρισης τρωτών σημείων και να διασφαλίζει ότι οι εν λόγω διαδικασίες είναι ενσωματωμένες στην οργάνωσή του. Όταν περιέρχεται σε γνώση του δυνητικό τρωτό σημείο, ο κάτοχος του πιστοποιητικού EUCC θα πρέπει να διενεργεί ανάλυση επιπτώσεων τρωτότητας. Όταν η ανάλυση επιπτώσεων τρωτότητας επιβεβαιώνει ότι το τρωτό σημείο μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης, ο κάτοχος του πιστοποιητικού θα πρέπει να διαβιβάζει έκθεση της αξιολόγησης στον οργανισμό πιστοποίησης ο οποίος θα πρέπει, με τη σειρά του, να ενημερώνει την εθνική αρχή πιστοποίησης της κυβερνοασφάλειας. Η έκθεση θα πρέπει να παρέχει ενημέρωση σχετικά με τις επιπτώσεις του τρωτού σημείου, τις αναγκαίες αλλαγές ή διορθωτικές λύσεις που απαιτούνται, συμπεριλαμβανομένων ενδεχόμενων ευρύτερων συνεπειών του τρωτού σημείου καθώς και διορθωτικών λύσεων για άλλα προϊόντα. Όταν απαιτείται, το πρότυπο EN ISO/IEC 29147 θα πρέπει να συμπληρώνει τη διαδικασία για τη δημοσιοποίηση του τρωτού σημείου.

(27) Για τον σκοπό της πιστοποίησης, οι οργανισμοί αξιολόγησης της συμμόρφωσης και οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας αποκτούν εμπιστευτικά και ευαίσθητα δεδομένα και πληροφορίες που συνιστούν επιχειρηματικό απόρρητο, σε σχέση επίσης με διανοητική ιδιοκτησία ή παρακολούθηση της συμμόρφωσης, οι οποίες απαιτούν κατάλληλη προστασία. Ως εκ τούτου, θα πρέπει να διαθέτουν τις αναγκαίες τεχνικές ικανότητες και γνώσεις και θα πρέπει να θεσπίζουν συστήματα για την προστασία των πληροφοριών. Οι απαιτήσεις και οι προϋποθέσεις για την προστασία των πληροφοριών θα πρέπει να πληρούνται τόσο για τη διαπίστευση όσο και για την εξουσιοδότηση.

(28) Ο ENISA θα πρέπει να παρέχει τον κατάλογο των πιστοποιημένων χαρακτηριστικών προστασίας στον ιστότοπό του για την πιστοποίηση της κυβερνοασφάλειας και να αναφέρει το καθεστώς τους, σύμφωνα με τον κανονισμό (ΕΕ) 2019/881.

(29) Ο παρών κανονισμός καθορίζει προϋποθέσεις για συμφωνίες αμοιβαίας αναγνώρισης με τρίτες χώρες. Τέτοιες συμφωνίες αμοιβαίας αναγνώρισης μπορεί να είναι διμερείς ή πολυμερείς και θα πρέπει να αντικαταστήσουν παρόμοιες υφιστάμενες συμφωνίες. Προκειμένου να διευκολύνουν την ομαλή μετάβαση σε τέτοιες συμφωνίες αμοιβαίας αναγνώρισης, τα κράτη μέλη μπορούν να συνεχίσουν τις υφιστάμενες ρυθμίσεις συνεργασίας με τρίτες χώρες για περιορισμένο χρονικό διάστημα.

(30) Οι οργανισμοί πιστοποίησης που εκδίδουν πιστοποιητικά EUCC σε «υψηλό» επίπεδο διασφάλισης, καθώς και οι σχετικές συνδεδεμένες ΕΑΑΤΠ, θα πρέπει να υποβάλλονται σε αξιολογήσεις από ομοτίμους. Στόχος των αξιολογήσεων από ομοτίμους θα πρέπει να είναι η εξακρίβωση της διαρκούς συμμόρφωσης του καταστατικού και των διαδικασιών του υποβληθέντος σε αξιολόγηση από ομοτίμους οργανισμού πιστοποίησης με τις απαιτήσεις του σχήματος EUCC. Οι συγκεκριμένες αξιολογήσεις από ομοτίμους διαφέρουν από τις αξιολογήσεις από ομοτίμους μεταξύ εθνικών αρχών πιστοποίησης της κυβερνοασφάλειας, οι οποίες προβλέπονται στο άρθρο 59 του κανονισμού (ΕΕ) 2019/881. Οι αξιολογήσεις από ομοτίμους θα πρέπει να εξακριβώνουν ότι οι οργανισμοί πιστοποίησης λειτουργούν με εναρμονισμένο τρόπο και εκδίδουν πιστοποιητικά της ίδιας ποιότητας, θα πρέπει δε να εντοπίζουν κάθε δυνητικό ισχυρό σημείο και αδυναμία στη λειτουργία των οργανισμών πιστοποίησης, μεταξύ άλλων με σκοπό την ανταλλαγή βέλτιστων πρακτικών. Καθώς υπάρχουν διαφορετικά είδη οργανισμών πιστοποίησης, θα πρέπει να επιτρέπονται διαφορετικά είδη αξιολογήσεων από ομοτίμους. Σε πιο σύνθετες περιπτώσεις, όπως όταν οργανισμοί πιστοποίησης εκδίδουν πιστοποιητικά σε διαφορετικά επίπεδα AVA_VAN, μπορούν να χρησιμοποιούνται διαφορετικά είδη αξιολόγησης από ομοτίμους, υπό τον όρο ότι πληρούνται όλες οι προϋποθέσεις.

(31) Η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας θα πρέπει να διαδραματίζει σημαντικό ρόλο στη διατήρηση του σχήματος. Τούτο θα πρέπει να πραγματοποιηθεί, μεταξύ άλλων, μέσω της συνεργασίας με τον ιδιωτικό τομέα, της δημιουργίας ειδικευμένων υποομάδων καθώς και των σχετικών προπαρασκευαστικών εργασιών και της παροχής της βοήθειας που ζητεί η Επιτροπή. Η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας διαδραματίζει σημαντικό ρόλο στην έγκριση εγγράφων στάθμης της τεχνικής. Κατά την έγκριση και την έκδοση εγγράφων στάθμης της τεχνικής, θα πρέπει να λαμβάνονται δεόντως υπόψη τα στοιχεία που αναφέρονται στο άρθρο 54 παράγραφος 1 στοιχείο γ) του κανονισμού

(ΕΕ) 2019/881. Οι τεχνικοί τομείς και τα έγγραφα τεχνολογίας αιχμής θα πρέπει να δημοσιεύονται στο παράρτημα Ι του παρόντος κανονισμού. Τα χαρακτηριστικά προστασίας τα οποία θεσπίστηκαν ως έγγραφα στάθμης της τεχνικής θα πρέπει να δημοσιεύονται στο παράρτημα ΙΙ. Προκειμένου να διασφαλίζεται ο επίκαιρος χαρακτήρας των εν λόγω παραρτημάτων, η Επιτροπή δύναται να τα τροποποιεί, σύμφωνα με τη διαδικασία που καθορίζεται στο άρθρο 66 παράγραφος 2 του κανονισμού (ΕΕ) 2019/881 και λαμβάνοντας υπόψη τη γνώμη της ευρωπαϊκής ομάδας πιστοποίησης της κυβερνοασφάλειας. Στο παράρτημα ΙΙΙ παρατίθενται συνιστώμενα χαρακτηριστικά προστασίας, τα οποία κατά τον χρόνο έναρξης ισχύος του παρόντος κανονισμού δεν είναι έγγραφα στάθμης της τεχνικής. Θα πρέπει να δημοσιοποιηθούν στον ιστότοπο του ENISA που αναφέρεται στο άρθρο 50 παράγραφος 1 του κανονισμού (ΕΕ) 2019/881.

(32) Ο παρών κανονισμός θα πρέπει να αρχίσει να εφαρμόζεται 12 μήνες μετά την έναρξη ισχύος του. Οι απαιτήσεις που προβλέπονται στο κεφάλαιο IV και στο παράρτημα V δεν χρήζουν μεταβατικής περιόδου και θα πρέπει, επομένως, να εφαρμόζονται από την έναρξη ισχύος του παρόντος κανονισμού.

(33) Τα μέτρα που προβλέπονται στον παρόντα κανονισμό είναι συνεπή με τη γνώμη της ευρωπαϊκής επιτροπής πιστοποίηση της κυβερνοασφάλειας που συστάθηκε δυνάμει του άρθρου 66 του κανονισμού (ΕΕ) 2019/881,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

ΚΕΦΑΛΑΙΟ Ι

ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1

Αντικείμενο και πεδίο εφαρμογής

Ο παρών κανονισμός καθορίζει το βασισμένο σε κοινά κριτήρια ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας (EUCC).

Ο παρών κανονισμός εφαρμόζεται σε όλα τα προϊόντα τεχνολογιών των πληροφοριών και των επικοινωνιών (στο εξής: ΤΠΕ), συμπεριλαμβανομένης της τεκμηρίωσής τους, τα οποία υποβάλλονται για πιστοποίηση στο πλαίσιο του EUCC, και σε όλα τα χαρακτηριστικά προστασίας τα οποία υποβάλλονται για πιστοποίηση στο πλαίσιο της διαδικασίας ΤΠΕ που οδηγεί στην πιστοποίηση προϊόντων ΤΠΕ.

Άρθρο 2

Ορισμοί

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

1) «κοινά κριτήρια»: τα κοινά κριτήρια για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών, τα οποία καθορίζονται στο πρότυπο ISO/IEC 15408·

2) «κοινή μεθοδολογία αξιολόγησης»: η κοινή μεθοδολογία για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών, η οποία καθορίζεται στο πρότυπο ISO/IEC 18045·

3) «στόχος αξιολόγησης»: προϊόν ή τμήμα προϊόντος ΤΠΕ, ή χαρακτηριστικό προστασίας στο πλαίσιο διαδικασίας ΤΠΕ, που υποβάλλονται σε αξιολόγηση κυβερνοασφάλειας προκειμένου να λάβουν πιστοποίηση EUCC·

4) «στόχος ασφάλειας»: ισχυρισμός απαιτήσεων ασφάλειας εξαρτώμενων από την υλοποίηση για συγκεκριμένο προϊόν ΤΠΕ·

5) «χαρακτηριστικό προστασίας»: διαδικασία ΤΠΕ η οποία καθορίζει τις απαιτήσεις ασφάλειας για συγκεκριμένη κατηγορία προϊόντων ΤΠΕ που αντιμετωπίζουν ανάγκες ασφάλειας μη εξαρτώμενες από την υλοποίηση, και η οποία μπορεί να χρησιμοποιηθεί για την αξιολόγηση προϊόντων ΤΠΕ που εμπίπτουν στη συγκεκριμένη κατηγορία για τον σκοπό της πιστοποίησής τους·

6) «τεχνική έκθεση αξιολόγησης»: έγγραφο το οποίο εκπονεί ΕΑΑΤΠ, στο οποίο παρουσιάζει τα ευρήματα, τα πορίσματα και τις αιτιολογήσεις που προέκυψαν από την αξιολόγηση προϊόντος ΤΠΕ ή χαρακτηριστικού προστασίας σύμφωνα με τους κανόνες και τις υποχρεώσεις που καθορίζονται στον παρόντα κανονισμό·

7) «ΕΑΑΤΠ»: εγκατάσταση αξιολόγησης της ασφάλειας της τεχνολογίας πληροφοριών, η οποία είναι οργανισμός αξιολόγησης της συμμόρφωσης, όπως ορίζεται στο άρθρο 2 σημείο 13 του κανονισμού (ΕΚ) αριθ. 765/2008, που εκτελεί καθήκοντα αξιολόγησης·

8) «επίπεδο AVA_VAN»: επίπεδο διασφάλισης ανάλυσης τρωτότητας το οποίο καταδεικνύει το επίπεδο των δραστηριοτήτων αξιολόγησης της κυβερνοασφάλειας που εκτελούνται προκειμένου να καθοριστεί το επίπεδο ανθεκτικότητας κατά δυνητικής εκμετάλλευσης ελαττωμάτων ή αδυναμιών του στόχου αξιολόγησης στο λειτουργικό περιβάλλον του όπως καθορίζεται στα κοινά κριτήρια·

9) «πιστοποιητικό EUCC»: πιστοποιητικό κυβερνοασφάλειας το οποίο εκδίδεται στο πλαίσιο του EUCC για προϊόντα ΤΠΕ ή για χαρακτηριστικά προστασίας τα οποία μπορούν να χρησιμοποιηθούν αποκλειστικά και μόνον στη διαδικασία ΤΠΕ της πιστοποίησης προϊόντων ΤΠΕ·

10) «σύνθετο προϊόν»: προϊόν ΤΠΕ το οποίο αξιολογείται μαζί με άλλο υποκείμενο προϊόν ΤΠΕ που έχει ήδη λάβει πιστοποιητικό EUCC και από τη λειτουργικότητα ασφάλειας του οποίου εξαρτάται το σύνθετο προϊόν ΤΠΕ·

11) «εθνική αρχή πιστοποίησης της κυβερνοασφάλειας»: αρχή την οποία ορίζει κράτος μέλος δυνάμει του άρθρου 58 παράγραφος 1 του κανονισμού (ΕΕ) 2019/881·

12) «οργανισμός πιστοποίησης»: οργανισμός αξιολόγησης της συμμόρφωσης όπως ορίζεται στο άρθρο 2 σημείο 13 του κανονισμού (ΕΚ) αριθ. 765/2008, ο οποίος πραγματοποιεί δραστηριότητες πιστοποίησης·

13) «τεχνικός τομέας»: κοινό τεχνικό πλαίσιο που σχετίζεται με συγκεκριμένη τεχνολογία για την εναρμονισμένη πιστοποίηση με ένα σύνολο χαρακτηριστικών απαιτήσεων ασφάλειας·

14) «έγγραφο στάθμης της τεχνικής»: έγγραφο το οποίο προσδιορίζει μεθόδους, τεχνικές και εργαλεία αξιολόγησης που εφαρμόζονται στην πιστοποίηση προϊόντων ΤΠΕ ή στις απαιτήσεις ασφάλειας γενικής κατηγορίας προϊόντων ΤΠΕ ή οποιεσδήποτε άλλες απαιτήσεις αναγκαίες για την πιστοποίηση, με σκοπό την εναρμόνιση της αξιολόγησης, ειδικότερα τεχνικών τομέων ή χαρακτηριστικών προστασίας·

15) «αρχή εποπτείας της αγοράς»: αρχή όπως ορίζεται στο άρθρο 3 σημείο 4 του κανονισμού (ΕΕ) 2019/1020.

Άρθρο 3

Πρότυπα αξιολόγησης

Στις αξιολογήσεις που διενεργούνται στο πλαίσιο του σχήματος EUCC εφαρμόζονται τα ακόλουθα πρότυπα:

α) τα κοινά κριτήρια·

β) η κοινή μεθοδολογία αξιολόγησης.

Άρθρο 4

Επίπεδα διασφάλισης

1. Οι οργανισμοί πιστοποίησης εκδίδουν πιστοποιητικά EUCC σε «σημαντικό» ή «υψηλό» επίπεδο διασφάλισης.

2. Τα πιστοποιητικά EUCC σε «σημαντικό» επίπεδο διασφάλισης αντιστοιχούν σε πιστοποιητικά που καλύπτουν επίπεδο AVA_VAN 1 ή 2.

3. Τα πιστοποιητικά EUCC σε «υψηλό» επίπεδο διασφάλισης αντιστοιχούν σε πιστοποιητικά που καλύπτουν επίπεδα AVA_VAN 3, 4 ή 5.

4. Το επίπεδο διασφάλισης που επιβεβαιώνεται σε πιστοποιητικό EUCC διακρίνει μεταξύ της συμμορφούμενης και της επαυξημένης χρήσης των συνιστωσών διασφάλισης οι οποίες προσδιορίζονται στα κοινά κριτήρια σύμφωνα με το παράρτημα VIII.

5. Οι οργανισμοί αξιολόγησης της συμμόρφωσης εφαρμόζουν τις εν λόγω συνιστώσες διασφάλισης από τις οποίες εξαρτάται το επίπεδο AVA_VAN που επιλέγεται σύμφωνα με τα πρότυπα που αναφέρονται στο άρθρο 3.

Άρθρο 5

Μέθοδοι πιστοποίησης προϊόντων ΤΠΕ

1. Η πιστοποίηση προϊόντος ΤΠΕ διενεργείται ως προς τον στόχο ασφάλειάς του:

α) όπως ορίζεται από τον αιτούντα· ή

β) ο οποίος ενσωματώνει χαρακτηριστικό προστασίας στο πλαίσιο διαδικασίας ΤΠΕ, όταν το προϊόν ΤΠΕ εμπίπτει στην κατηγορία προϊόντων ΤΠΕ που καλύπτεται από το συγκεκριμένο χαρακτηριστικό προστασίας.

2. Τα χαρακτηριστικά προστασίας πιστοποιούνται αποκλειστικά και μόνον για τον σκοπό της πιστοποίησης προϊόντων ΤΠΕ που εμπίπτουν στη συγκεκριμένη κατηγορία προϊόντων ΤΠΕ που καλύπτεται από το χαρακτηριστικό προστασίας.

Άρθρο 6

Αυτοαξιολόγηση της συμμόρφωσης

Αυτοαξιολόγηση της συμμόρφωσης κατά την έννοια του άρθρου 53 του κανονισμού (ΕΕ) 2019/881 δεν επιτρέπεται.

ΚΕΦΑΛΑΙΟ II

ΠΙΣΤΟΠΟΙΗΣΗ ΠΡΟΪΟΝΤΩΝ ΤΠΕ

ΤΜΗΜΑ I

ΕΙΔΙΚΆ ΠΡΌΤΥΠΑ ΚΑΙ ΑΠΑΙΤΉΣΕΙΣ ΓΙΑ ΤΗΝ ΑΞΙΟΛΌΓΗΣΗ

Άρθρο 7

Κριτήρια και μέθοδοι αξιολόγησης για προϊόντα ΤΠΕ

1. Προϊόν ΤΠΕ το οποίο υποβάλλεται για πιστοποίηση αξιολογείται, τουλάχιστον, σύμφωνα με:

α) τα εφαρμοστέα στοιχεία των προτύπων που αναφέρονται στο άρθρο 3·

β) τις κλάσεις απαιτήσεων κατοχύρωσης της ασφάλειας για αξιολόγηση της τρωτότητας και ανεξάρτητες λειτουργικές δοκιμές, όπως προβλέπεται στα πρότυπα αξιολόγησης που αναφέρονται στο άρθρο 3·

γ) το επίπεδο κινδύνου που σχετίζεται με την προβλεπόμενη χρήση των οικείων προϊόντων ΤΠΕ δυνάμει του άρθρου 52 του κανονισμού (ΕΕ) 2019/881 και τις λειτουργίες ασφάλειας των εν λόγω προϊόντων οι οποίες στηρίζουν τους στόχους ασφάλειας που καθορίζονται στο άρθρο 51 του κανονισμού (ΕΕ) 2019/881·

δ) τα εφαρμοστέα έγγραφα στάθμης της τεχνικής που παρατίθενται στο παράρτημα I· και

ε) τα εφαρμοστέα πιστοποιημένα χαρακτηριστικά προστασίας που παρατίθενται στο παράρτημα II.

2. Σε εξαιρετικές και δεόντως αιτιολογημένες περιπτώσεις ο οργανισμός αξιολόγησης της συμμόρφωσης μπορεί να ζητήσει τη μη εφαρμογή του σχετικού εγγράφου στάθμης της τεχνικής. Σε τέτοιες περιπτώσεις, ο οργανισμός αξιολόγησης της συμμόρφωσης ενημερώνει την εθνική αρχή πιστοποίησης της κυβερνοασφάλειας, επισυνάπτοντας στο αίτημά του αιτιολόγηση δεόντως εμπεριστατωμένη. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας αξιολογεί την αιτιολόγηση της εξαίρεσης και, εφόσον είναι

βάσιμη, την εγκρίνει. Εν αναμονή της απόφασης της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας, ο οργανισμός αξιολόγησης της συμμόρφωσης δεν εκδίδει κανένα πιστοποιητικό. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας κοινοποιεί αμελλητί την εγκεκριμένη εξαίρεση στην ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας, η οποία δύναται να εκδώσει γνωμοδότηση. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας λαμβάνει ιδιαιτέρως υπόψη τη γνωμοδότηση της ευρωπαϊκής ομάδας πιστοποίησης της κυβερνοασφάλειας.

3. Η πιστοποίηση προϊόντων ΤΠΕ σε επίπεδο AVA_VAN 4 ή 5 είναι δυνατή μόνον στις ακόλουθες περιπτώσεις:

α) όταν το προϊόν ΤΠΕ καλύπτεται από οποιονδήποτε τεχνικό τομέα που παρατίθεται στο παράρτημα I, το προϊόν ΤΠΑ αξιολογείται σύμφωνα με τα εφαρμοστέα έγγραφα στάθμης της τεχνικής των εν λόγω τεχνικών τομέων,

β) όταν το προϊόν ΤΠΕ εμπίπτει σε κατηγορία προϊόντων ΤΠΕ που καλύπτεται από πιστοποιημένο χαρακτηριστικό προστασίας το οποίο περιλαμβάνει επίπεδο AVA_VAN 4 ή 5 και το οποίο παρατίθεται ως χαρακτηριστικό προστασίας τεχνολογίας αιχμής στο παράρτημα II, το προϊόν ΤΠΕ αξιολογείται σύμφωνα με τη μεθοδολογία αξιολόγησης που προσδιορίζεται για το συγκεκριμένο χαρακτηριστικό προστασίας,

γ) σε περίπτωση που τα στοιχεία α) και β) της παρούσας παραγράφου δεν έχουν εφαρμογή και σε περίπτωση που η συμπερίληψη τεχνικού τομέα στο παράρτημα I ή πιστοποιημένου χαρακτηριστικού προστασίας στο παράρτημα II δεν είναι πιθανή στο εγγύς μέλλον, και μόνον σε εξαιρετικές και δεόντως αιτιολογημένες περιπτώσεις, υπό τους όρους που καθορίζονται στην παράγραφο 4.

4. Σε περίπτωση που οργανισμός αξιολόγησης της συμμόρφωσης εκτιμά ότι συντρέχει εξαιρετική και δεόντως αιτιολογημένη περίπτωση κατά την παράγραφο 3 στοιχείο γ) ανωτέρω, κοινοποιεί τη σκοπούμενη πιστοποίηση στην εθνική αρχή πιστοποίησης της κυβερνοασφάλειας επισυνάπτοντας αιτιολόγηση και προτεινόμενη μεθοδολογία αξιολόγησης. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας αξιολογεί την αιτιολόγηση της εξαίρεσης και, σε περίπτωση που είναι βάσιμη, εγκρίνει ή τροποποιεί τη μεθοδολογία αξιολόγησης που πρέπει να εφαρμόζει ο οργανισμός αξιολόγησης της συμμόρφωσης. Εν αναμονή της απόφασης της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας, ο οργανισμός αξιολόγησης της συμμόρφωσης δεν εκδίδει κανένα πιστοποιητικό. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας αναφέρει αμελλητί τη σκοπούμενη πιστοποίηση στην ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας, η οποία δύναται να εκδώσει γνωμοδότηση. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας λαμβάνει ιδιαιτέρως υπόψη τη γνωμοδότηση της ευρωπαϊκής ομάδας πιστοποίησης της κυβερνοασφάλειας.

5. Σε περίπτωση προϊόντος ΤΠΕ που υποβάλλεται σε αξιολόγηση σύνθετου προϊόντος σύμφωνα με τα σχετικά έγγραφα στάθμης της τεχνικής, η ΕΑΑΤΠ που διενήργησε την αξιολόγηση του υποκείμενου προϊόντος ΤΠΕ γνωστοποιεί τις σχετικές πληροφορίες στην ΕΑΑΤΠ που διενεργεί την αξιολόγηση του σύνθετου προϊόντος ΤΠΕ.

ΤΜΗΜΑ II

ΈΚΔΟΣΗ, ΑΝΑΝΈΩΣΗ ΚΑΙ ΑΝΆΚΛΗΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΏΝ EUCC

Άρθρο 8

Απαραίτητες πληροφορίες για την πιστοποίηση

1. Οι αιτούντες πιστοποίηση στο πλαίσιο του EUCC παρέχουν ή διαθέτουν με άλλον τρόπο στον οργανισμό πιστοποίησης και στην ΕΑΤΤΠ κάθε πληροφορία αναγκαία για τις δραστηριότητες πιστοποίησης.

2. Οι πληροφορίες της παραγράφου 1 περιλαμβάνουν κάθε σχετική τεκμηρίωση σύμφωνα με τις ενότητες με τίτλο «Στοιχεία ενεργειών φορέα ανάπτυξης» (Developer action elements), στον κατάλληλο μορφότυπο όπως προβλέπεται στις ενότητες με τίτλο «Περιεχόμενο και παρουσίαση στοιχείων τεκμηρίωσης» (Content and presentation of evidence elements) των κοινών κριτηρίων και της κοινής μεθοδολογίας αξιολόγησης για το επιλεγμένο επίπεδο διασφάλισης και τις σχετικές απαιτήσεις κατοχύρωσης της ασφάλειας. Η τεκμηρίωση περιλαμβάνει, κατά περίπτωση, στοιχεία σχετικά με το προϊόν ΤΠΕ και τον πηγαίο κώδικά του σύμφωνα με τον παρόντα κανονισμό, με την επιφύλαξη διασφαλίσεων κατά της μη εξουσιοδοτημένης γνωστοποίησης.

3. Οι αιτούντες πιστοποίηση δύνανται να παρέχουν στον οργανισμό πιστοποίησης και στην ΕΑΤΤΠ κατάλληλα αποτελέσματα αξιολόγησης από προγενέστερη πιστοποίηση δυνάμει:

α) του παρόντος κανονισμού·

β) άλλου ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας θεσπισθέντος δυνάμει του άρθρου 49 του κανονισμού (ΕΕ) 2019/881·

γ) εθνικού σχήματος που αναφέρεται στο άρθρο 49 του παρόντος κανονισμού.

4. Σε περίπτωση που τα αποτελέσματα της αξιολόγησης έχουν σημασία για τα καθήκοντά της, η ΕΑΑΤΠ δύναται να χρησιμοποιεί εκ νέου τα αποτελέσματα της αξιολόγησης, εφόσον τα εν λόγω αποτελέσματα πληρούν τις εφαρμοστέες απαιτήσεις και η γνησιότητά τους είναι επιβεβαιωμένη.

5. Όταν ο οργανισμός πιστοποίησης επιτρέπει την πιστοποίηση προϊόντος ως σύνθετου προϊόντος, ο αιτών πιστοποίηση θέτει στη διάθεση του οργανισμού πιστοποίησης και της ΕΑΑΤΠ κάθε αναγκαίο στοιχείο, κατά περίπτωση, σύμφωνα με το έγγραφο στάθμης της τεχνικής.

6. Οι αιτούντες πιστοποίηση παρέχουν επίσης στον οργανισμό πιστοποίησης και στην ΕΑΑΤΠ τις ακόλουθες πληροφορίες:

α) τον σύνδεσμο προς τον ιστότοπό τους που περιέχει τις συμπληρωματικές πληροφορίες σχετικά με την κυβερνοασφάλεια που αναφέρονται στο άρθρο 55 του κανονισμού (ΕΕ) 2019/881·

β) περιγραφή των διαδικασιών τους για τη διαχείριση τρωτών σημείων και τη δημοσιοποίηση τρωτών σημείων.

7. Ο οργανισμός πιστοποίησης, η ΕΑΑΤΠ και ο αιτών διατηρούν κάθε σχετική τεκμηρίωση η οποία αναφέρεται στο παρόν άρθρο για διάστημα 5 ετών μετά τη λήξη ισχύος του πιστοποιητικού.

Άρθρο 9

Προϋποθέσεις έκδοσης πιστοποιητικού EUCC

1. Οι οργανισμοί πιστοποίησης εκδίδουν πιστοποιητικό EUCC, εφόσον πληρούνται όλες οι ακόλουθες προϋποθέσεις:

α) η κατηγορία προϊόντος ΤΠΕ εμπίπτει στο πεδίο της διαπίστευσης, και όπου συντρέχει περίπτωση της εξουσιοδότησης, του οργανισμού πιστοποίησης και της ΕΑΑΤΠ που συμμετέχει στην πιστοποίηση·

β) ο αιτών πιστοποίηση υπέγραψε δήλωση με την οποία αναλαμβάνει όλες τις δεσμεύσεις που απαριθμούνται στην παράγραφο 2·

γ) η ΕΑΑΤΠ ολοκλήρωσε την αξιολόγηση χωρίς ένσταση σύμφωνα με τα πρότυπα, τα κριτήρια και τις μεθόδους αξιολόγησης που αναφέρονται στα άρθρα 3 και 7·

δ) ο οργανισμός πιστοποίησης ολοκλήρωσε την επανεξέταση των αποτελεσμάτων της αξιολόγησης χωρίς ένσταση·

ε) ο οργανισμός πιστοποίησης έλεγξε ότι οι τεχνικές εκθέσεις αξιολόγησης της ΕΑΑΤΠ είναι συνεπείς με την παρασχεθείσα τεκμηρίωση και ότι τα πρότυπα, τα κριτήρια και οι μέθοδοι αξιολόγησης που αναφέρονται στα άρθρα 3 και 7 εφαρμόστηκαν ορθά.

2. Ο αιτών πιστοποίηση αναλαμβάνει τις ακόλουθες δεσμεύσεις:

α) να παρέχει στον οργανισμό πιστοποίησης και στην ΕΑΑΤΠ κάθε αναγκαία πλήρη και ορθή πληροφορία και να παρέχει συμπληρωματικές αναγκαίες πληροφορίες, εφόσον ζητηθούν·

β) να μην προωθεί το προϊόν ΤΠΕ ως πιστοποιημένο βάσει του EUCC πριν από την έκδοση του πιστοποιητικού EUCC·

γ) να προωθεί το προϊόν ΤΠΕ ως πιστοποιημένο σε σχέση μόνον με το πεδίο που καθορίζεται στο πιστοποιητικό EUCC·

δ) να παύσει πάραυτα την προώθηση του προϊόντος ΤΠΕ ως πιστοποιημένου σε περίπτωση αναστολής, ανάκλησης ή λήξης της ισχύος του πιστοποιητικού EUCC·

ε) να διασφαλίζει ότι τα προϊόντα ΤΠΕ που πωλούνται με παραπομπή στο πιστοποιητικό EUCC είναι απολύτως πανομοιότυπα με το προϊόν ΤΠΕ που υποβλήθηκε σε πιστοποίηση·

στ) να τηρεί τους κανόνες χρήσης του σήματος και της επισήμανσης που θεσπίζονται για το πιστοποιητικό EUCC σύμφωνα με το άρθρο 11.

3. Σε περίπτωση προϊόντος ΤΠΕ που υποβάλλεται σε πιστοποίηση σύνθετου προϊόντος σύμφωνα με τα σχετικά έγγραφα στάθμης της τεχνικής, ο οργανισμός πιστοποίησης που διενήργησε την πιστοποίηση του υποκείμενου προϊόντος ΤΠΕ γνωστοποιεί τις σχετικές πληροφορίες στον οργανισμό πιστοποίησης που διενεργεί την πιστοποίηση του σύνθετου προϊόντος ΤΠΕ.

Άρθρο 10

Περιεχόμενο και μορφή πιστοποιητικού EUCC

1. Το πιστοποιητικό EUCC περιέχει τουλάχιστον τις πληροφορίες που παρατίθενται στο παράρτημα VII.

2. Το πεδίο και τα όρια του πιστοποιημένου προϊόντος ΤΠΕ προσδιορίζονται σαφώς στο πιστοποιητικό EUCC ή στην έκθεση πιστοποίησης, επισημαίνεται δε κατά πόσον η πιστοποίηση αφορά το σύνολο του προϊόντος ΤΠΕ ή μόνον τμήματά του.

3. Ο οργανισμός πιστοποίησης παρέχει στον αιτούντα το πιστοποιητικό EUCC τουλάχιστον σε ηλεκτρονική μορφή.

4. Ο οργανισμός πιστοποίησης εκπονεί έκθεση πιστοποίησης σύμφωνα με το παράρτημα V για κάθε πιστοποιητικό EUCC το οποίο εκδίδει. Η έκθεση πιστοποίησης βασίζεται στην τεχνική έκθεση αξιολόγησης που εκπονεί η ΕΑΑΤΠ. Η τεχνική έκθεση αξιολόγησης και η έκθεση πιστοποίησης προσδιορίζουν τα συγκεκριμένα κριτήρια και τις συγκεκριμένες μεθόδους αξιολόγησης που αναφέρονται στο άρθρο 7 και που χρησιμοποιήθηκαν για την αξιολόγηση.

5. Ο οργανισμός πιστοποίησης παρέχει στην εθνική αρχή πιστοποίησης της κυβερνοασφάλειας και στον ENISA κάθε πιστοποιητικό EUCC και κάθε έκθεση πιστοποίησης σε ηλεκτρονική μορφή.

Άρθρο 11

Σήματα και επισημάνσεις

1. Ο κάτοχος πιστοποιητικού δύναται να θέσει σήμα και επισήμανση σε πιστοποιημένο προϊόν ΤΠΕ. Το σήμα και η επισήμανση καταδεικνύουν ότι το προϊόν ΤΠΕ πιστοποιήθηκε σύμφωνα με τον παρόντα κανονισμό. Το σήμα και η επισήμανση τίθενται σύμφωνα με το παρόν άρθρο και το παράρτημα IX.

2. Το σήμα και η επισήμανση τίθενται κατά τρόπο εμφανή, ευανάγνωστο και ανεξίτηλο στο πιστοποιημένο προϊόν ΤΠΕ ή στην πινακίδα με τα στοιχεία του. Όταν η φύση του προϊόντος δεν το επιτρέπει ή δεν το δικαιολογεί, το σήμα και η επισήμανση τοποθετούνται στη συσκευασία του προϊόντος και στα συνοδευτικά έγγραφα. Σε περίπτωση που το πιστοποιημένο προϊόν ΤΠΕ παραδίδεται με τη μορφή λογισμικού, το σήμα και η επισήμανση εμφανίζονται κατά τρόπο εμφανή, ευανάγνωστο και ανεξίτηλο στην τεκμηρίωση που το συνοδεύει ή παρέχεται στους χρήστες εύκολη και άμεση πρόσβαση στην εν λόγω τεκμηρίωση μέσω ιστοτόπου.

3. Το σήμα και η επισήμανση έχουν τη μορφή που παρατίθεται στο παράρτημα IX και περιέχουν τα εξής στοιχεία:

α) το επίπεδο διασφάλισης και το επίπεδο AVA_VAN του πιστοποιημένου προϊόντος ΤΠΕ·

β) τον μοναδικό αναγνωριστικό αριθμό του πιστοποιητικού, ο οποίος περιλαμβάνει τα εξής:

1) την ονομασία του σχήματος·

2) το όνομα και τον αριθμό αναφοράς της διαπίστευσης του οργανισμού πιστοποίησης που εξέδωσε το πιστοποιητικό·

3) το έτος και τον μήνα έκδοσης·

4) τον αναγνωριστικό αριθμό που απέδωσε ο οργανισμός πιστοποίησης που εξέδωσε το πιστοποιητικό.

4. Το σήμα και η επισήμανση συνοδεύονται από κωδικό QR με σύνδεσμο προς ιστότοπο που περιέχει τουλάχιστον τα εξής:

α) τις πληροφορίες σχετικά με την περίοδο ισχύος του πιστοποιητικού·

β) τις απαραίτητες πληροφορίες για την πιστοποίηση οι οποίες καθορίζονται στα παραρτήματα V και VII·

γ) τις πληροφορίες που ο κάτοχος του πιστοποιητικού πρέπει να δημοσιοποιεί σύμφωνα με το άρθρο 55 του κανονισμού (ΕΕ) 2019/881· και

δ) όπου συντρέχει περίπτωση, τις ιστορικές πληροφορίες που σχετίζονται με τη/τις συγκεκριμένη/-ες πιστοποίηση/-εις του προϊόντος ΤΠΕ ώστε να καθίσταται δυνατή η ιχνηλασιμότητα.

Άρθρο 12

Περίοδος ισχύος πιστοποιητικού EUCC

1. Ο οργανισμός πιστοποίησης καθορίζει περίοδο ισχύος για κάθε πιστοποιητικό EUCC που εκδίδει λαμβάνοντας υπόψη τα χαρακτηριστικά του πιστοποιημένου προϊόντος ΤΠΕ.

2. Η περίοδος ισχύος του πιστοποιητικού EUCC δεν υπερβαίνει τα 5 έτη.

3. Κατά παρέκκλιση από την παράγραφο 2, η περίοδος ισχύος μπορεί να υπερβαίνει τα 5 έτη, με την επιφύλαξη προηγούμενης έγκρισης της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας κοινοποιεί αμελλητί την έγκριση που χορήγησε στην ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας.

Άρθρο 13

Επανεξέταση πιστοποιητικού EUCC

1. Κατόπιν αιτήματος του κατόχου του πιστοποιητικού ή για άλλους δεόντως αιτιολογημένους λόγους, ο οργανισμός πιστοποίησης δύναται να αποφασίσει την επανεξέταση του πιστοποιητικού EUCC για προϊόν ΤΠΕ. Η επανεξέταση διενεργείται σύμφωνα με το παράρτημα IV. Ο οργανισμός πιστοποίησης καθορίζει την έκταση της επανεξέτασης. Οσάκις απαιτείται για την επανεξέταση, ο οργανισμός πιστοποίησης ζητεί από την ΕΑΑΤΠ να διενεργήσει εκ νέου αξιολόγηση του πιστοποιημένου προϊόντος ΤΠΕ.

2. Μετά τα αποτελέσματα της επανεξέτασης, και κατά περίπτωση της εκ νέου αξιολόγησης, ο οργανισμός πιστοποίησης:

α) επιβεβαιώνει το πιστοποιητικό EUCC·

β) ανακαλεί το πιστοποιητικό EUCC σύμφωνα με το άρθρο 14·

γ) ανακαλεί το πιστοποιητικό EUCC σύμφωνα με το άρθρο 14 και εκδίδει νέο πιστοποιητικό EUCC με πανομοιότυπο πεδίο και μεγαλύτερη περίοδο ισχύος· ή

δ) ανακαλεί το πιστοποιητικό EUCC σύμφωνα με το άρθρο 14 και εκδίδει νέο πιστοποιητικό EUCC με διαφορετικό πεδίο.

3. Ο οργανισμός πιστοποίησης δύναται να αναστείλει, αμελλητί, το πιστοποιητικό EUCC σύμφωνα με το άρθρο 30, εν αναμονή λήψης διορθωτικών μέτρων από τον κάτοχο του πιστοποιητικού EUCC.

Άρθρο 14

Ανάκληση πιστοποιητικού EUCC

1. Με την επιφύλαξη του άρθρου 58 παράγραφος 8 στοιχείο ε) του κανονισμού (ΕΕ) 2019/881, πιστοποιητικό EUCC ανακαλείται από τον οργανισμό πιστοποίησης που το εξέδωσε.

2. Ο οργανισμός πιστοποίησης που αναφέρεται στην παράγραφο 1 κοινοποιεί στην εθνική αρχή πιστοποίησης της κυβερνοασφάλειας την ανάκληση του πιστοποιητικού. Κοινοποιεί επίσης την εν λόγω ανάκληση στον ENISA προκειμένου να διευκολύνει την άσκηση των καθηκόντων του βάσει του άρθρου 50 του κανονισμού (ΕΕ) 2019/881. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας ενημερώνει άλλες αρμόδιες αρχές εποπτείας της αγοράς.

3. Ο κάτοχος πιστοποιητικού EUCC μπορεί να ζητήσει την ανάκληση του πιστοποιητικού.

ΚΕΦΑΛΑΙΟ III

ΠΙΣΤΟΠΟΙΗΣΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΠΡΟΣΤΑΣΙΑΣ

ΤΜΗΜΑ I

ΕΙΔΙΚΆ ΠΡΌΤΥΠΑ ΚΑΙ ΑΠΑΙΤΉΣΕΙΣ ΓΙΑ ΤΗΝ ΑΞΙΟΛΌΓΗΣΗ

Άρθρο 15

Κριτήρια και μέθοδοι αξιολόγησης

1. Τα χαρακτηριστικά προστασίας αξιολογούνται, τουλάχιστον, σύμφωνα με τα ακόλουθα στοιχεία:

α) τα εφαρμοστέα στοιχεία των προτύπων που αναφέρονται στο άρθρο 3·

β) το επίπεδο κινδύνου που σχετίζεται με την προβλεπόμενη χρήση των οικείων προϊόντων ΤΠΕ δυνάμει του άρθρου 52 του κανονισμού (ΕΕ) 2019/881 και τις λειτουργίες ασφάλειας των εν λόγω προϊόντων οι οποίες στηρίζουν τους στόχους ασφάλειας που καθορίζονται στο άρθρο 51 του ίδιου κανονισμού· και

γ) τα εφαρμοστέα έγγραφα στάθμης της τεχνικής που παρατίθενται στο παράρτημα Ι. Χαρακτηριστικό προστασίας που καλύπτεται από τεχνικό τομέα πιστοποιείται ως προς τις απαιτήσεις που καθορίζονται στον συγκεκριμένο τεχνικό τομέα.

2. Σε εξαιρετικές και δεόντως αιτιολογημένες περιπτώσεις ο οργανισμός αξιολόγησης της συμμόρφωσης μπορεί να πιστοποιήσει χαρακτηριστικό προστασίας χωρίς να εφαρμόσει τα σχετικά έγγραφα στάθμης της τεχνικής. Σε τέτοιες περιπτώσεις, ο οργανισμός αξιολόγησης της συμμόρφωσης ενημερώνει την αρμόδια εθνική αρχή πιστοποίησης της κυβερνοασφάλειας και παρέχει, αφενός, αιτιολόγηση για τη σκοπούμενη πιστοποίηση χωρίς εφαρμογή των σχετικών εγγράφων στάθμης της τεχνικής, αφετέρου δε την προτεινόμενη μεθοδολογία αξιολόγησης. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας αξιολογεί την αιτιολόγηση και, εφόσον είναι βάσιμη, εγκρίνει τη μη εφαρμογή των σχετικών εγγράφων στάθμης της τεχνικής, εγκρίνει δε ή τροποποιεί, κατά περίπτωση, τη μεθοδολογία αξιολόγησης που πρέπει να εφαρμόσει ο οργανισμός αξιολόγησης της συμμόρφωσης. Εν αναμονή της απόφασης της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας, ο οργανισμός αξιολόγησης της συμμόρφωσης δεν εκδίδει κανένα πιστοποιητικό για το χαρακτηριστικό προστασίας. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας κοινοποιεί αμελλητί την εγκριθείσα μη εφαρμογή των σχετικών εγγράφων στάθμης της τεχνικής στην ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας, η οποία δύναται να εκδώσει γνωμοδότηση. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας λαμβάνει ιδιαιτέρως υπόψη τη γνωμοδότηση της ευρωπαϊκής ομάδας πιστοποίησης της κυβερνοασφάλειας.

ΤΜΗΜΑ II

ΈΚΔΟΣΗ, ΑΝΑΝΈΩΣΗ ΚΑΙ ΑΝΆΚΛΗΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΏΝ EUCC ΓΙΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΆ ΠΡΟΣΤΑΣΊΑΣ

Άρθρο 16

Απαραίτητες πληροφορίες για την πιστοποίηση χαρακτηριστικών προστασίας

Οι αιτούντες πιστοποίηση χαρακτηριστικού προστασίας στο πλαίσιο του EUCC παρέχουν ή διαθέτουν με άλλον τρόπο στον οργανισμό πιστοποίησης και στην ΕΑΤΤΠ κάθε πληροφορία αναγκαία για τις δραστηριότητες πιστοποίησης. Το άρθρο 8 παράγραφοι 2, 3, 4 και 7 εφαρμόζεται τηρουμένων των αναλογιών.

Άρθρο 17

Έκδοση πιστοποιητικών EUCC για χαρακτηριστικά προστασίας

1. Οι αιτούντες πιστοποίηση παρέχουν στον οργανισμό πιστοποίησης και στην ΕΑΑΤΠ κάθε αναγκαία πλήρη και ορθή πληροφορία.

2. Τα άρθρα 9 και 10 εφαρμόζονται τηρουμένων των αναλογιών.

3. Η ΕΑΑΤΠ αξιολογεί αν το χαρακτηριστικό προστασίας είναι πλήρες, συνεπές, τεχνικά άρτιο και αποτελεσματικό για την προβλεπόμενη χρήση και τους στόχους ασφάλειας της κατηγορίας του προϊόντος ΤΠΕ που καλύπτεται από το συγκεκριμένο χαρακτηριστικό προστασίας.

4. Τα χαρακτηριστικά προστασίας πιστοποιούνται αποκλειστικά και μόνο από:

α) εθνική αρχή πιστοποίησης της κυβερνοασφάλειας ή άλλο δημόσιο οργανισμό διαπιστευμένο ως οργανισμό πιστοποίησης· ή

β) οργανισμό πιστοποίησης, με την προηγούμενη έγκριση της εθνικής αρχής πιστοποίηση της κυβερνοασφάλειας για κάθε επιμέρους χαρακτηριστικό προστασίας.

Άρθρο 18

Περίοδος ισχύος πιστοποιητικού EUCC για χαρακτηριστικά προστασίας

1. Ο οργανισμός πιστοποίησης καθορίζει περίοδο ισχύος για κάθε πιστοποιητικό EUCC.

2. Η περίοδος ισχύος μπορεί να εκτείνεται στη διάρκεια ζωής των οικείου χαρακτηριστικού προστασίας.

Άρθρο 19

Επανεξέταση πιστοποιητικού EUCC για χαρακτηριστικά προστασίας

1. Κατόπιν αιτήματος του κατόχου του πιστοποιητικού ή για άλλους δεόντως αιτιολογημένους λόγους, ο οργανισμός πιστοποίησης δύναται να αποφασίσει την επανεξέταση πιστοποιητικού EUCC για χαρακτηριστικό προστασίας. Η επανεξέταση διενεργείται εφαρμόζοντας τις προϋποθέσεις που καθορίζονται στο άρθρο 15. Ο οργανισμός πιστοποίησης καθορίζει την έκταση της επανεξέτασης. Οσάκις απαιτείται για την επανεξέταση, ο οργανισμός πιστοποίησης ζητεί από την ΕΑΑΤΠ να διενεργήσει εκ νέου αξιολόγηση του πιστοποιημένου χαρακτηριστικού προστασίας.

2. Μετά τα αποτελέσματα της επανεξέτασης, και κατά περίπτωση της εκ νέου αξιολόγησης, ο οργανισμός πιστοποίησης προβαίνει σε μια από τις ακόλουθες ενέργειες:

α) επιβεβαιώνει το πιστοποιητικό EUCC·

β) ανακαλεί το πιστοποιητικό EUCC σύμφωνα με το άρθρο 20·

γ) ανακαλεί το πιστοποιητικό EUCC σύμφωνα με το άρθρο 20 και εκδίδει νέο πιστοποιητικό EUCC με πανομοιότυπο πεδίο και μεγαλύτερη περίοδο ισχύος·

δ) ανακαλεί το πιστοποιητικό EUCC σύμφωνα με το άρθρο 20 και εκδίδει νέο πιστοποιητικό EUCC με διαφορετικό πεδίο.

Άρθρο 20

Ανάκληση πιστοποιητικού EUCC για χαρακτηριστικό προστασίας

1. Με την επιφύλαξη του άρθρου 58 παράγραφος 8 στοιχείο ε) του κανονισμού (ΕΕ) 2019/881, πιστοποιητικό EUCC για χαρακτηριστικό προστασίας ανακαλείται από τον οργανισμό πιστοποίησης που το εξέδωσε. Το άρθρο 14 εφαρμόζεται τηρουμένων των αναλογιών.

2. Πιστοποιητικό για χαρακτηριστικό προστασίας το οποίο εκδόθηκε σύμφωνα με το άρθρο 17 παράγραφος 4 στοιχείο β) ανακαλείται από την εθνική αρχή πιστοποίησης της κυβερνοασφάλειας η οποία ενέκρινε το εν λόγω πιστοποιητικό.

ΚΕΦΑΛΑΙΟ IV

ΟΡΓΑΝΙΣΜΟΙ ΑΞΙΟΛΟΓΗΣΗΣ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ

Άρθρο 21

Πρόσθετες ή ειδικές απαιτήσεις για οργανισμό πιστοποίησης

1. Οι οργανισμοί πιστοποίησης εξουσιοδοτούνται από την εθνική αρχή πιστοποίησης της κυβερνοασφάλειας να εκδίδουν πιστοποιητικά EUCC σε «υψηλό» επίπεδο διασφάλισης στην περίπτωση που, επιπλέον της πλήρωσης των απαιτήσεων που καθορίζονται στο άρθρο 60 παράγραφος 1 και στο παράρτημα του κανονισμού (ΕΕ) 2019/881 σχετικά με τη διαπίστευση οργανισμών αξιολόγησης της συμμόρφωσης, οι εν λόγω οργανισμοί καταδεικνύουν ότι:

α) διαθέτουν την εμπειρογνωσία και τις ικανότητες που απαιτούνται για τη λήψη απόφασης πιστοποίησης σε «υψηλό» επίπεδο διασφάλισης·

β) διενεργούν τις δραστηριότητες πιστοποίησης σε συνεργασία με ΕΑΑΤΠ εξουσιοδοτημένη σύμφωνα με το άρθρο 22· και

γ) διαθέτουν τις απαιτούμενες ικανότητες και λαμβάνουν κατάλληλα τεχνικά και λειτουργικά μέτρα για την αποτελεσματική προστασία εμπιστευτικών και ευαίσθητων πληροφοριών για «υψηλό» επίπεδο διασφάλισης, επιπλέον των απαιτήσεων που καθορίζονται στο άρθρο 43.

2. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας αξιολογεί αν ο οργανισμός πιστοποίησης πληροί όλες τις απαιτήσεις που καθορίζονται στην παράγραφο 1. Η εν λόγω αξιολόγηση περιλαμβάνει τουλάχιστον δομημένες συνεντεύξεις και επανεξέταση τουλάχιστον μίας πιλοτικής πιστοποίησης την οποία ο οργανισμός πιστοποίησης διενήργησε σύμφωνα με τον παρόντα κανονισμό.

Στην αξιολόγησή της, η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας μπορεί να χρησιμοποιήσει εκ νέου κάθε κατάλληλο αποδεικτικό στοιχείο από προγενέστερη εξουσιοδότηση ή παρόμοιες δραστηριότητες το οποίο χορηγήθηκε δυνάμει:

α) του παρόντος κανονισμού·

β) άλλου ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας θεσπισθέντος δυνάμει του άρθρου 49 του κανονισμού (ΕΕ) 2019/881·

γ) εθνικού σχήματος που αναφέρεται στο άρθρο 49 του παρόντος κανονισμού.

3. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας εκπονεί έκθεση εξουσιοδότησης η οποία υποβάλλεται σε αξιολόγηση από ομοτίμους σύμφωνα με το άρθρο 59 παράγραφος 3 στοιχείο δ) του κανονισμού (ΕΕ) 2019/881.

4. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας προσδιορίζει τις κατηγορίες προϊόντων ΤΠΕ και τα χαρακτηριστικά προστασίας στα οποία εκτείνεται η εξουσιοδότηση. Η εξουσιοδότηση ισχύει για διάστημα το οποίο δεν υπερβαίνει την περίοδο ισχύος της διαπίστευσης. Μπορεί να ανανεωθεί κατόπιν αιτήματος, εφόσον ο οργανισμός πιστοποίησης εξακολουθεί να πληροί τις απαιτήσεις που καθορίζονται στο παρόν άρθρο. Για την ανανέωση της εξουσιοδότησης δεν απαιτείται η διενέργεια πιλοτικών αξιολογήσεων.

5. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας ανακαλεί την εξουσιοδότηση του οργανισμού πιστοποίησης εάν δεν πληροί πλέον τις προϋποθέσεις που καθορίζονται στο παρόν άρθρο. Μετά την ανάκληση της εξουσιοδότησης, ο οργανισμός πιστοποίησης παύει πάραυτα να προβάλλεται ως εξουσιοδοτημένος οργανισμός πιστοποίησης.

Άρθρο 22

Πρόσθετες ή ειδικές απαιτήσεις για ΕΑΑΤΠ

1. Μια ΕΑΑΤΠ εξουσιοδοτείται από την εθνική αρχή πιστοποίησης της κυβερνοασφάλειας να διενεργεί την αξιολόγηση προϊόντων ΤΠΕ τα οποία υπόκεινται σε πιστοποίηση βάσει του «υψηλού» επιπέδου διασφάλισης, όταν, επιπλέον της πλήρωσης των απαιτήσεων που καθορίζονται στο άρθρο 60 παράγραφος 1 και στο παράρτημα του κανονισμού (ΕΕ) 2019/881 σχετικά με τη διαπίστευση οργανισμών αξιολόγησης της συμμόρφωσης, η ΕΑΑΤΠ καταδεικνύει ότι πληροί όλες τις ακόλουθες προϋποθέσεις:

α) διαθέτει την αναγκαία εμπειρογνωσία για την εκτέλεση των δραστηριοτήτων αξιολόγησης με σκοπό τον καθορισμό της ανθεκτικότητας σε κυβερνοεπιθέσεις προηγμένης τεχνολογίας που πραγματοποιούνται από παράγοντες με σημαντικές δεξιότητες και σημαντικούς πόρους·

β) για τους τεχνικούς τομείς και τα χαρακτηριστικά προστασίας, τα οποία περιλαμβάνονται στη διαδικασία ΤΠΕ για τα συγκεκριμένα προϊόντα ΤΠΕ, διαθέτει:

1) την εμπειρογνωσία για την εκτέλεση των συγκεκριμένων δραστηριοτήτων αξιολόγησης που είναι αναγκαίες για τον μεθοδικό καθορισμό της ανθεκτικότητας στόχου αξιολόγησης σε επιδέξιους επιτιθέμενους στο λειτουργικό περιβάλλον του υποθέτοντας «μέτριο» ή «υψηλό» κίνδυνο επίθεσης όπως καθορίζεται στα πρότυπα που αναφέρονται στο άρθρο 3·

2) τις τεχνικές ικανότητες οι οποίες προσδιορίζονται στα έγγραφα στάθμης της τεχνικής που παρατίθενται στο παράρτημα Ι·

γ) διαθέτει τις απαιτούμενες ικανότητες και λαμβάνει κατάλληλα τεχνικά και λειτουργικά μέτρα για την αποτελεσματική προστασία εμπιστευτικών και ευαίσθητων πληροφοριών για «υψηλό» επίπεδο διασφάλισης, επιπλέον των απαιτήσεων που καθορίζονται στο άρθρο 43.

2. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας αξιολογεί αν η ΕΑΑΤΠ πληροί όλες τις απαιτήσεις που καθορίζονται στην παράγραφο 1. Η εν λόγω αξιολόγηση περιλαμβάνει τουλάχιστον δομημένες συνεντεύξεις και επανεξέταση τουλάχιστον μίας πιλοτικής αξιολόγησης την οποία η ΕΑΑΤΠ διενήργησε σύμφωνα με τον παρόντα κανονισμό.

3. Στην αξιολόγησή της, η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας μπορεί να χρησιμοποιήσει εκ νέου κάθε κατάλληλο αποδεικτικό στοιχείο από προγενέστερη εξουσιοδότηση ή παρόμοιες δραστηριότητες το οποίο χορηγήθηκε δυνάμει:

α) του παρόντος κανονισμού·

β) άλλου ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας θεσπισθέντος δυνάμει του άρθρου 49 του κανονισμού (ΕΕ) 2019/881·

γ) εθνικού σχήματος που αναφέρεται στο άρθρο 49 του παρόντος κανονισμού.

4. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας εκπονεί έκθεση εξουσιοδότησης η οποία υποβάλλεται σε αξιολόγηση από ομοτίμους σύμφωνα με το άρθρο 59 παράγραφος 3 στοιχείο δ) του κανονισμού (ΕΕ) 2019/881.

5. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας προσδιορίζει τις κατηγορίες προϊόντων ΤΠΕ και τα χαρακτηριστικά προστασίας στα οποία εκτείνεται η εξουσιοδότηση. Η εξουσιοδότηση ισχύει για διάστημα το οποίο δεν υπερβαίνει την περίοδο ισχύος της διαπίστευσης. Μπορεί να ανανεωθεί κατόπιν αιτήματος, εφόσον η ΕΑΑΤΠ εξακολουθεί να πληροί τις απαιτήσεις που καθορίζονται στο παρόν άρθρο. Για την ανανέωση της εξουσιοδότησης δεν θα πρέπει να απαιτείται η διενέργεια πιλοτικών αξιολογήσεων.

6. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας ανακαλεί την εξουσιοδότηση της ΕΑΑΤΠ εάν δεν πληροί πλέον τις προϋποθέσεις που καθορίζονται στο παρόν άρθρο. Μετά την ανάκληση της εξουσιοδότησης, η ΕΑΑΤΠ παύει να προβάλλεται ως εξουσιοδοτημένη ΕΑΑΤΠ.

Άρθρο 23

Κοινοποίηση οργανισμών πιστοποίησης

1. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας κοινοποιεί στην Επιτροπή τους οργανισμούς πιστοποίησης οι οποίοι είναι αρμόδιοι, στην επικράτειά της, για την πιστοποίηση σε «σημαντικό» επίπεδο διασφάλισης βάσει της διαπίστευσής τους.

2. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας κοινοποιεί στην Επιτροπή τους οργανισμούς πιστοποίησης οι οποίοι είναι αρμόδιοι, στην επικράτειά της, για την πιστοποίηση σε «υψηλό» επίπεδο διασφάλισης βάσει της διαπίστευσής τους και της απόφασης εξουσιοδότησης.

3. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας παρέχει τουλάχιστον τις ακόλουθες πληροφορίες όταν κοινοποιεί στην Επιτροπή τους οργανισμούς πιστοποίησης:

α) το/τα επίπεδο/-α διασφάλισης για το/τα οποίο/-α ο οργανισμός πιστοποίησης είναι αρμόδιος να εκδίδει πιστοποιητικά EUCC·

β) τις ακόλουθες πληροφορίες σχετικά με τη διαπίστευση:

1) ημερομηνία της διαπίστευσης·

2) όνομα και διεύθυνση του οργανισμού πιστοποίησης·

3) χώρα καταχώρισης του οργανισμού πιστοποίησης·

4) αριθμό αναφοράς της διαπίστευσης·

5) πεδίο και περίοδο ισχύος της διαπίστευσης·

6) διεύθυνση, τοποθεσία και σύνδεσμο προς τον σχετικό ιστότοπο του εθνικού οργανισμού διαπίστευσης· και

γ) τις ακόλουθες πληροφορίες σχετικά με την εξουσιοδότηση για «υψηλό» επίπεδο:

1) ημερομηνία εξουσιοδότησης·

2) αριθμό αναφοράς της εξουσιοδότησης·

3) περίοδο ισχύος της εξουσιοδότησης·

4) πεδίο της εξουσιοδότησης συμπεριλαμβανομένου του υψηλότερου επιπέδου AVA_VAN και, κατά περίπτωση, του καλυπτόμενου τεχνικού τομέα.

4. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας διαβιβάζει αντίγραφο της κοινοποίησης που αναφέρεται στις παραγράφους 1 και 2 στον ENISA για τη δημοσίευση επακριβών πληροφοριών στον ιστότοπο για την πιστοποίηση της κυβερνοασφάλειας σχετικά με την επιλεξιμότητα οργανισμών πιστοποίησης.

5. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας εξετάζει αμελλητί κάθε πληροφορία σχετικά με τη μεταβολή του καθεστώτος της διαπίστευσης που παρέχεται από τον εθνικό οργανισμό διαπίστευσης. Σε περίπτωση ανάκλησης της διαπίστευσης ή της εξουσιοδότησης, η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας ενημερώνει σχετικά την Επιτροπή και δύναται να υποβάλει στην Επιτροπή αίτημα σύμφωνα με το άρθρο 61 παράγραφος 4 του κανονισμού (ΕΕ) 2019/881.

Άρθρο 24

Κοινοποίηση ΕΑΑΤΠ

Οι υποχρεώσεις κοινοποίησης των εθνικών αρχών πιστοποίησης της κυβερνοασφάλειας που καθορίζονται στο άρθρο 23 ισχύουν επίσης για την ΕΑΑΤΠ. Η κοινοποίηση περιλαμβάνει τη διεύθυνση της ΕΑΑΤΠ, την έγκυρη διαπίστευση και, κατά περίπτωση, την έγκυρη εξουσιοδότηση της συγκεκριμένης ΕΑΑΤΠ.

ΚΕΦΑΛΑΙΟ V

ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΑΙ ΜΗ ΣΥΜΜΟΡΦΩΣΗ

ΤΜΗΜΑ I

ΠΑρακολούθηση τησ συμμόρφωσησ

Άρθρο 25

Δραστηριότητες παρακολούθησης της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας

1. Με την επιφύλαξη του άρθρου 58 παράγραφος 7 του κανονισμού (ΕΕ) 2019/881, η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας παρακολουθεί τη συμμόρφωση:

α) του οργανισμού πιστοποίησης και της ΕΑΑΤΠ με τις υποχρεώσεις που υπέχουν από τον παρόντα κανονισμό και τον κανονισμό (ΕΕ) 2019/881·

β) των κατόχων πιστοποιητικού EUCC με τις υποχρεώσεις που υπέχουν από τον παρόντα κανονισμό και τον κανονισμό (ΕΕ) 2019/881·

γ) των πιστοποιημένων προϊόντων ΤΠΕ με τις απαιτήσεις που καθορίζονται στο EUCC·

δ) της διασφάλισης που δηλώνεται στο πιστοποιητικό EUCC για την αντιμετώπιση των εξελισσόμενων κυβερνοαπειλών.

2. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας ασκεί τις δραστηριότητες παρακολούθησης ειδικότερα βάσει:

α) των πληροφοριών που προέρχονται από οργανισμούς πιστοποίησης, εθνικούς οργανισμούς διαπίστευσης και αρμόδιες αρχές εποπτείας της αγοράς·

β) των πληροφοριών που προκύπτουν από τους ελέγχους και τις έρευνες που διεξάγει η ίδια ή άλλη αρχή·

γ) της δειγματοληψίας που διενεργείται σύμφωνα με την παράγραφο 3·

δ) των καταγγελιών που λαμβάνει.

3. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας λαμβάνει σε ετήσια βάση, σε συνεργασία με άλλες αρχές εποπτείας της αγοράς, δείγμα τουλάχιστον 4 % των πιστοποιητικών EUCC όπως καθορίζεται σε εκτίμηση κινδύνου. Κατόπιν αιτήματος και ενεργώντας για λογαριασμό της αρμόδιας εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας, οι οργανισμοί πιστοποίησης και, εφόσον απαιτείται, η ΕΑΑΤΠ συνδράμουν την εν λόγω αρχή στην παρακολούθηση της συμμόρφωσης.

4. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας επιλέγει το δείγμα πιστοποιημένων προϊόντων ΤΠΕ προς έλεγχο εφαρμόζοντας αντικειμενικά κριτήρια, όπως τα ακόλουθα:

α) κατηγορία προϊόντος·

β) επίπεδα διασφάλισης των προϊόντων·

γ) κάτοχος πιστοποιητικού·

δ) οργανισμός πιστοποίησης και, κατά περίπτωση, υπεργολάβος ΕΑΑΤΠ·

ε) κάθε άλλη πληροφορία που περιέρχεται σε γνώση της αρχής.

5. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας ενημερώνει τους κατόχους του πιστοποιητικού EUCC σχετικά με τα επιλεγμένα πιστοποιητικά ΤΠΕ και τα κριτήρια επιλογής.

6. Ο οργανισμός πιστοποίησης που πιστοποίησε το προϊόν ΤΠΕ του δείγματος διενεργεί, κατόπιν αιτήματος της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας, με τη βοήθεια της αντίστοιχης ΕΑΑΤΠ, πρόσθετη επανεξέταση σύμφωνα με τη διαδικασία που καθορίζεται στο τμήμα IV.2 του παραρτήματος IV και ενημερώνει την εθνική αρχή πιστοποίησης της κυβερνοασφάλειας για τα αποτελέσματα.

7. Εάν η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας έχει επαρκείς λόγους να πιστεύει ότι πιστοποιημένο προϊόν ΤΠΕ δεν συμμορφώνεται πλέον με τον παρόντα κανονισμό ή με τον κανονισμό (ΕΕ) 2019/881, μπορεί να διενεργεί έρευνες ή να κάνει χρήση κάθε άλλης εξουσίας παρακολούθησης η οποία προβλέπεται στο άρθρο 58 παράγραφος 8 του κανονισμού (ΕΕ) 2019/881.

8. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας ενημερώνει τον οργανισμό πιστοποίησης και την οικεία ΕΑΑΤΠ σχετικά με τρέχουσες έρευνες οι οποίες αφορούν επιλεγμένα προϊόντα ΤΠΕ.

9. Εάν η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας διαπιστώσει ότι τρέχουσα έρευνα αφορά προϊόντα ΤΠΕ τα οποία πιστοποιήθηκαν από οργανισμούς πιστοποίησης εγκατεστημένους σε άλλα κράτη μέλη, ενημερώνει σχετικά τις εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας των αντίστοιχων κρατών μελών προκειμένου να συνεργαστούν στις έρευνες, εφόσον συντρέχει περίπτωση. Η εν λόγω εθνική αρχή πιστοποίησης της κυβερνοασφάλειας ενημερώνει επίσης την ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας για τις διασυνοριακές έρευνες και τα επακόλουθα αποτελέσματα.

Άρθρο 26

Δραστηριότητες παρακολούθησης του οργανισμού πιστοποίησης

1. Ο οργανισμός πιστοποίησης παρακολουθεί:

α) τη συμμόρφωση των κατόχων πιστοποιητικού με τις υποχρεώσεις που υπέχουν από τον παρόντα κανονισμό και τον κανονισμό (ΕΕ) 2019/881 σε σχέση με το πιστοποιητικό EUCC που εξέδωσε ο οργανισμός πιστοποίησης·

β) τη συμμόρφωση των προϊόντων ΤΠΕ που πιστοποίησε με τις αντίστοιχες απαιτήσεις ασφάλειας·

γ) τη διασφάλιση που δηλώνεται στα πιστοποιημένα χαρακτηριστικά προστασίας.

2. Ο οργανισμός πιστοποίησης ασκεί τις δραστηριότητες παρακολούθησης βάσει:

α) των πληροφοριών που παρέχονται βάσει των δεσμεύσεων του αιτούντος πιστοποίηση που αναφέρονται στο άρθρο 9 παράγραφος 2·

β) των πληροφοριών που προκύπτουν από δραστηριότητες άλλων αρμόδιων αρχών εποπτείας της αγοράς·

γ) των καταγγελιών που λαμβάνει·

δ) πληροφοριών σχετικά με τρωτά σημεία που μπορεί να επηρεάσουν τα προϊόντα ΤΠΕ που έχει πιστοποιήσει.

3. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας δύναται να καταρτίσει κανόνες για περιοδικό διάλογο μεταξύ οργανισμών πιστοποίησης και κατόχων πιστοποιητικών EUCC με σκοπό τον έλεγχο και την υποβολή εκθέσεων σχετικά με τη συμμόρφωση με τις δεσμεύσεις που αναλαμβάνονται δυνάμει του άρθρου 9 παράγραφος 2, με την επιφύλαξη δραστηριοτήτων που αφορούν άλλες αρμόδιες αρχές εποπτείας της αγοράς.

Άρθρο 27

Δραστηριότητες παρακολούθησης του κατόχου του πιστοποιητικού

1. Για την παρακολούθηση της συμμόρφωσης του πιστοποιημένου προϊόντος ΤΠΕ με τις απαιτήσεις ασφάλειας που το αφορούν, ο κάτοχος πιστοποιητικού EUCC εκτελεί τα ακόλουθα καθήκοντα:

α) παρακολουθεί τις πληροφορίες σχετικά με τρωτά σημεία οι οποίες αφορούν το πιστοποιημένο προϊόν ΤΠΕ, συμπεριλαμβανομένων γνωστών εξαρτήσεων, με δικά του μέσα, αλλά επίσης λαμβάνοντας υπόψη:

   1) δημοσίευση ή υπόμνημα που αφορά πληροφορίες σχετικά με τρωτά σημασία από χρήστη ή ερευνητή ασφάλειας που αναφέρεται στο άρθρο 55 παράγραφος 1 στοιχείο γ) του κανονισμού (ΕΕ) 2019/881·

   2) υπόμνημα από οποιαδήποτε άλλη πηγή·

β) παρακολουθεί τη διασφάλιση που δηλώνεται στο πιστοποιητικό EUCC.

2. Ο κάτοχος πιστοποιητικού EUCC συνεργάζεται με τον οργανισμό πιστοποίησης, την ΕΑΑΤΠ και, κατά περίπτωση, την εθνική αρχή πιστοποίησης της κυβερνοασφάλειας για τη στήριξη των δραστηριοτήτων παρακολούθησης που εκτελούν.

ΤΜΗΜΑ ΙΙ

Συμμόρφωση

Άρθρο 28

Συνέπειες μη συμμόρφωσης πιστοποιημένου προϊόντος ΤΠΕ ή χαρακτηριστικού προστασίας

1. Εάν πιστοποιημένο προϊόν ΤΠΕ ή χαρακτηριστικό προστασίας δεν συμμορφώνεται με τις απαιτήσεις που καθορίζονται στον παρόντα κανονισμό και στον κανονισμό (ΕΕ) 2019/881, ο οργανισμός πιστοποίησης ενημερώνει τον κάτοχο του πιστοποιητικού EUCC σχετικά με την εντοπισθείσα μη συμμόρφωση και ζητεί τη λήψη διορθωτικών μέτρων.

2. Όταν περίπτωση μη συμμόρφωσης με τις διατάξεις του παρόντος κανονισμού μπορεί να επηρεάζει τη συμμόρφωση με άλλη σχετική ενωσιακή νομοθεσία, η οποία προβλέπει τη δυνατότητα να καταδεικνύεται η τεκμαιρόμενη συμμόρφωση με τις απαιτήσεις της συγκεκριμένης νομικής πράξης κάνοντας χρήση του πιστοποιητικού EUCC, ο οργανισμός πιστοποίησης ενημερώνει αμελλητί την εθνική αρχή πιστοποίησης της κυβερνοασφάλειας. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας ενημερώνει αμελλητί την αρχή εποπτείας της αγοράς που είναι υπεύθυνη για την εν λόγω άλλη σχετική ρύθμιση της ενωσιακής νομοθεσίας σχετικά με την εντοπισθείσα περίπτωση μη συμμόρφωσης.

3. Μόλις λάβει τις πληροφορίες που αναφέρονται στην παράγραφο 1, ο κάτοχος του πιστοποιητικού EUCC προτείνει στον οργανισμό πιστοποίησης, εντός της προθεσμίας που τάσσει ο οργανισμός πιστοποίησης, η οποία δεν υπερβαίνει τις 30 ημέρες, τα αναγκαία διορθωτικά μέτρα για την αντιμετώπιση της μη συμμόρφωσης.

4. Ο οργανισμός πιστοποίησης δύναται να αναστείλει αμελλητί το πιστοποιητικό EUCC σύμφωνα με το άρθρο 30 σε έκτακτες περιπτώσεις ή σε περίπτωση που ο κάτοχος του πιστοποιητικού EUCC δεν συνεργάζεται δεόντως με τον οργανισμό πιστοποίησης.

5. Ο οργανισμός πιστοποίησης διενεργεί επανεξέταση σύμφωνα με τα άρθρα 13 και 19 και εκτιμά κατά πόσον τα διορθωτικά μέτρα αντιμετωπίζουν την έλλειψη συμμόρφωσης.

6. Σε περίπτωση που ο κάτοχος του πιστοποιητικού EUCC δεν προτείνει κατάλληλα διορθωτικά μέτρα εντός της προθεσμίας που αναφέρεται στην παράγραφο 3, το πιστοποιητικό αναστέλλεται σύμφωνα με το άρθρο 30 ή ανακαλείται σύμφωνα με τα άρθρα 14 ή 20.

7. Το παρόν άρθρο δεν εφαρμόζεται σε περιπτώσεις τρωτών σημείων που επηρεάζουν πιστοποιημένο προϊόν ΤΠΕ, τα οποία αντιμετωπίζονται σύμφωνα με τα οριζόμενα στο κεφάλαιο VI.

Άρθρο 29

Συνέπειες μη συμμόρφωσης του κατόχου του πιστοποιητικού

1. Όταν ο οργανισμός πιστοποίησης διαπιστώνει ότι:

α) ο κάτοχος του πιστοποιητικού EUCC ή ο αιτών πιστοποίηση δεν συμμορφώνεται με τις δεσμεύσεις και τις υποχρεώσεις του οι οποίες καθορίζονται στο άρθρο 9 παράγραφος 2, το άρθρο 17 παράγραφος 2) και τα άρθρα 27 και 41· ή

β) ο κάτοχος του πιστοποιητικού EUCC δεν συμμορφώνεται με το άρθρο 56 παράγραφος 8 του κανονισμού (ΕΕ) 2019/881 ή το κεφάλαιο VI του παρόντος κανονισμού·

τάσσει προθεσμία, η οποία δεν υπερβαίνει τις 30 ημέρες, εντός της οποίας ο κάτοχος του πιστοποιητικού EUCC λαμβάνει διορθωτικά μέτρα.

2. Σε περίπτωση που ο κάτοχος του πιστοποιητικού EUCC δεν προτείνει κατάλληλα διορθωτικά μέτρα εντός της προθεσμίας που αναφέρεται στην παράγραφο 1, το πιστοποιητικό αναστέλλεται σύμφωνα με το άρθρο 30 ή ανακαλείται σύμφωνα με τα άρθρα 14 και 20.

3. Συνεχιζόμενη ή επαναλαμβανόμενη παράβαση, από τον κάτοχο του πιστοποιητικού EUCC, των υποχρεώσεων που αναφέρονται στην παράγραφο 1 ενεργοποιεί την ανάκληση του πιστοποιητικού EUCC σύμφωνα με το άρθρο 14 ή το άρθρο 20.

4. Ο οργανισμός πιστοποίησης ενημερώνει την εθνική αρχή πιστοποίησης της κυβερνοασφάλειας για τις διαπιστώσεις που αναφέρονται στην παράγραφο 1. Εάν η περίπτωση μη συμμόρφωσης επηρεάζει τη συμμόρφωση με άλλη σχετική ενωσιακή νομοθεσία, η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας ενημερώνει πάραυτα την αρχή εποπτείας της αγοράς που είναι υπεύθυνη για την εν λόγω άλλη σχετική ενωσιακή νομοθεσία σχετικά με την εντοπισθείσα περίπτωση μη συμμόρφωσης.

Άρθρο 30

Αναστολή του πιστοποιητικού EUCC

1. Όταν στον παρόντα κανονισμό γίνεται αναφορά σε αναστολή πιστοποιητικού EUCC, ο οργανισμός πιστοποίησης αναστέλλει το οικείο πιστοποιητικό EUCC για χρονικό διάστημα σύστοιχο με τις περιστάσεις που ενεργοποίησαν την αναστολή, το οποίο δεν υπερβαίνει τις 42 ημέρες. Η περίοδος αναστολής αρχίζει την επομένη της ημέρας της απόφασης του οργανισμού πιστοποίησης. Η αναστολή δεν θίγει το κύρος του πιστοποιητικού.

2. Ο οργανισμός πιστοποίησης κοινοποιεί αμελλητί την αναστολή στον κάτοχο του πιστοποιητικού και στην εθνική αρχή πιστοποίησης της κυβερνοασφάλειας παραθέτοντας τους λόγους της αναστολής, τα μέτρα που ζητεί να ληφθούν και τη διάρκεια της περιόδου αναστολής.

3. Οι κάτοχοι πιστοποίησης ενημερώνουν τους αγοραστές των οικείων προϊόντων ΤΠΕ σχετικά με την αναστολή και τους λόγους αναστολής που παρέθεσε ο οργανισμός πιστοποίησης, πλην των τμημάτων της αιτιολογίας η κοινοποίηση των οποίων θα συνιστούσε κίνδυνο ασφάλειας ή των τμημάτων που περιέχουν ευαίσθητες πληροφορίες. Ο κάτοχος του πιστοποιητικού δημοσιοποιεί επίσης τις πληροφορίες αυτές.

4. Εάν άλλη σχετική ενωσιακή νομοθεσία προβλέπει τεκμήριο συμμόρφωσης βασισμένο σε πιστοποιητικά που εκδίδονται σύμφωνα με τις διατάξεις του παρόντος κανονισμού, η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας ενημερώνει την αρχή εποπτείας της αγοράς που είναι υπεύθυνη για την εν λόγω άλλη σχετική ενωσιακή νομοθεσία σχετικά με την αναστολή.

5. Η αναστολή πιστοποιητικού κοινοποιείται στον ENISA σύμφωνα με το άρθρο 42 παράγραφος 3.

6. Σε δεόντως αιτιολογημένες περιπτώσεις, η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας δύναται να επιτρέψει παράταση της περιόδου αναστολής πιστοποιητικού EUCC. Η συνολική περίοδος αναστολής δεν μπορεί να υπερβαίνει το 1 έτος.

Άρθρο 31

Συνέπειες μη συμμόρφωσης του οργανισμού αξιολόγησης της συμμόρφωσης

1. Σε περίπτωση μη συμμόρφωσης οργανισμού πιστοποίησης με τις υποχρεώσεις που υπέχει, ή του οικείου οργανισμού πιστοποίησης σε περίπτωση εντοπισμού μη συμμόρφωσης της ΕΑΑΤΠ, η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας προβαίνει αμελλητί στις εξής ενέργειες:

α) προσδιορίζει, με τη βοήθεια της οικείας ΕΑΑΤΠ, τα δυνητικώς επηρεαζόμενα πιστοποιητικά EUCC·

β) κατά περίπτωση, ζητεί την πραγματοποίηση δραστηριοτήτων αξιολόγησης σε ένα ή περισσότερα προϊόντα ΤΠΕ ή χαρακτηριστικά προστασίας, είτε από την ΕΑΑΤΠ που διενήργησε την αξιολόγηση είτε από οποιαδήποτε άλλη διαπιστευμένη και, κατά περίπτωση, εξουσιοδοτημένη ΕΑΑΤΠ που μπορεί να είναι σε καλύτερη θέση, από τεχνική άποψη, να συμβάλει στον ως άνω προσδιορισμό·

γ) αναλύει τις επιπτώσεις της έλλειψης συμμόρφωσης·

δ) ενημερώνει τον κάτοχο του πιστοποιητικού EUCC ο οποίος θίγεται από τη μη συμμόρφωσης.

2. Βάσει των μέτρων που αναφέρονται στην παράγραφο 1, ο οργανισμός πιστοποίησης λαμβάνει οποιαδήποτε από τις ακόλουθες αποφάσεις σε σχέση με κάθε επηρεαζόμενο πιστοποιητικό EUCC:

α) διατηρεί το πιστοποιητικό EUCC αμετάβλητο·

β) ανακαλεί το πιστοποιητικό EUCC σύμφωνα με το άρθρο 14 ή το άρθρο 20 και, κατά περίπτωση, εκδίδει νέο πιστοποιητικό EUCC.

3. Βάσει των μέτρων που αναφέρονται στην παράγραφο 1, η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας:

α) εάν συντρέχει περίπτωση, αναφέρει τη μη συμμόρφωση του οργανισμού πιστοποίησης ή της σχετικής ΕΑΑΤΠ στον εθνικό οργανισμό διαπίστευσης·

β) κατά περίπτωση, αξιολογεί τις δυνητικές επιπτώσεις στην εξουσιοδότηση.

ΚΕΦΑΛΑΙΟ VI

ΔΙΑΧΕΙΡΙΣΗ ΚΑΙ ΔΗΜΟΣΙΟΠΟΙΗΣΗ ΤΡΩΤΩΝ ΣΗΜΕΙΩΝ

Άρθρο 32

Πεδίο της διαχείρισης τρωτών σημείων

Το παρόν κεφάλαιο εφαρμόζεται σε προϊόντα ΤΠΕ για τα οποία εκδόθηκε πιστοποιητικό EUCC.

ΤΜΗΜΑ I

Διαχείριση τρωτών σημείων

Άρθρο 33

Διαδικασίες διαχείρισης τρωτών σημείων

1. Ο κάτοχος πιστοποιητικού EUCC θεσπίζει και διατηρεί κάθε αναγκαία διαδικασία διαχείρισης τρωτών σημείων σύμφωνα με τους κανόνες οι οποίοι θεσπίζονται στο παρόν τμήμα και οι οποίοι, όπου συντρέχει περίπτωση, συμπληρώνονται με διαδικασίες που καθορίζονται στο πρότυπο EN ISO/IEC 30111.

2. Ο κάτοχος πιστοποιητικού EUCC διατηρεί και δημοσιεύει κατάλληλες μεθόδους απόκτησης πληροφοριών σχετικά με τρωτά σημεία που αφορούν τα προϊόντα του από εξωτερικές πηγές, συμπεριλαμβανομένων χρηστών, οργανισμών πιστοποίησης και ερευνητών ασφάλειας.

3. Όταν ο κάτοχος πιστοποιητικού EUCC εντοπίζει ή λαμβάνει πληροφορίες σχετικά με δυνητικό τρωτό σημείο το οποίο επηρεάζει πιστοποιημένο προϊόν ΤΠΕ, καταχωρίζει τις πληροφορίες και διενεργεί ανάλυση επιπτώσεων τρωτότητας.

4. Όταν ένα δυνητικό τρωτό σημείο έχει αντίκτυπο σε σύνθετο προϊόν, ο κάτοχος του πιστοποιητικού EUCC ενημερώνει τον κάτοχο εξαρτώμενων πιστοποιητικών EUCC σχετικά με το δυνητικό τρωτό σημείο.

5. Ανταποκρινόμενος σε εύλογο αίτημα του οργανισμού πιστοποίησης που εξέδωσε το πιστοποιητικό, ο κάτοχος πιστοποιητικού EUCC διαβιβάζει κάθε σχετική πληροφορία για δυνητικά τρωτά σημεία στον εν λόγω οργανισμό πιστοποίησης.

Άρθρο 34

Ανάλυση επιπτώσεων τρωτότητας

1. Η ανάλυση επιπτώσεων τρωτότητας παραπέμπει στον στόχο αξιολόγησης και στις δηλώσεις διασφάλισης που περιέχονται στο πιστοποιητικό. Η ανάλυση επιπτώσεων τρωτότητας διενεργείται εντός κατάλληλου χρονοδιαγράμματος λαμβανομένων υπόψη της δυνατότητας εκμετάλλευσης και του κρίσιμου χαρακτήρα του δυνητικού τρωτού σημείου του πιστοποιημένου προϊόντος ΤΠΕ.

2. Κατά περίπτωση, διενεργείται υπολογισμός του κινδύνου επίθεσης σύμφωνα με τη σχετική μεθοδολογία που περιλαμβάνεται στα πρότυπα που αναφέρονται στο άρθρο 3 και στα σχετικά έγγραφα στάθμης της τεχνικής που παρατίθενται στο παράρτημα I, προκειμένου να εξακριβωθεί η δυνατότητα εκμετάλλευσης του τρωτού σημείου. Το επίπεδο AVA_VAN του πιστοποιητικού EUCC λαμβάνεται υπόψη.

Άρθρο 35

Έκθεση ανάλυσης επιπτώσεων τρωτότητας

1. Ο κάτοχος προσκομίζει έκθεση ανάλυσης επιπτώσεων τρωτότητας σε περίπτωση που η ανάλυση επιπτώσεων καταδεικνύει ότι το τρωτό σημείο έχει πιθανώς επιπτώσεις στη συμμόρφωση του προϊόντος ΤΠΕ με το πιστοποιητικό του.

2. Η έκθεση ανάλυσης επιπτώσεων τρωτότητας περιέχει αξιολόγηση των ακόλουθων στοιχείων:

α) των επιπτώσεων των τρωτών σημείων στο πιστοποιημένο προϊόν ΤΠΕ·

β) ενδεχόμενων κινδύνων που συνδέονται με την εγγύτητα ή το ενδεχόμενο κυβερνοεπίθεσης·

γ) της δυνατότητας διόρθωσης του τρωτού σημείου·

δ) εάν το τρωτό σημείο μπορεί να διορθωθεί, ενδεχόμενων τρόπων αντιμετώπισης του τρωτού σημείου.

3. Όπου συντρέχει περίπτωση, η έκθεση ανάλυσης επιπτώσεων τρωτότητας περιέχει στοιχεία σχετικά με τους ενδεχόμενους τρόπους εκμετάλλευσης του τρωτού σημείου. Οι πληροφορίες σχετικά με ενδεχόμενους τρόπους εκμετάλλευσης του τρωτού σημείου αντιμετωπίζονται σύμφωνα με κατάλληλα μέτρα ασφάλειας προκειμένου να προστατευτεί ο εμπιστευτικός χαρακτήρας τους και να διασφαλιστεί, εφόσον απαιτείται, η περιορισμένη διανομή τους.

4. Ο κάτοχος πιστοποιητικού EUCC διαβιβάζει αμελλητί έκθεση ανάλυσης επιπτώσεων τρωτότητας στον οργανισμό πιστοποίησης ή στην εθνική αρχή πιστοποίησης της κυβερνοασφάλειας σύμφωνα με το άρθρο 56 παράγραφος 8 του κανονισμού (ΕΕ) 2019/881.

5. Σε περίπτωση που στην έκθεση ανάλυσης επιπτώσεων τρωτότητας διαπιστώνεται ότι το τρωτό σημείο δεν έχει μόνιμο χαρακτήρα, κατά την έννοια των προτύπων που αναφέρονται στο άρθρο 3, και ότι μπορεί να διορθωθεί, εφαρμόζεται το άρθρο 36.

6. Σε περίπτωση που στην έκθεση ανάλυσης επιπτώσεων τρωτότητας διαπιστώνεται ότι το τρωτό σημείο δεν έχει μόνιμο χαρακτήρα και ότι δεν μπορεί να διορθωθεί, το πιστοποιητικό EUCC ανακαλείται σύμφωνα με το άρθρο 14.

7. Ο κάτοχος του πιστοποιητικού EUCC παρακολουθεί κάθε εναπομένον τρωτό σημείο προκειμένου να διασφαλίσει ότι δεν είναι δυνατή η εκμετάλλευσή του σε περίπτωση μεταβολών στο λειτουργικό περιβάλλον.

Άρθρο 36

Διόρθωση τρωτών σημείων

Ο κάτοχος πιστοποιητικού EUCC υποβάλλει στον οργανισμό πιστοποίησης πρόταση για κατάλληλα διορθωτικά μέτρα. Ο οργανισμός πιστοποίησης επανεξετάζει το πιστοποιητικό σύμφωνα με το άρθρο 13. Το αντικείμενο της επανεξέτασης καθορίζεται με την προτεινόμενη διόρθωση του τρωτού σημείου.

ΤΜΗΜΑ ΙΙ

Δημοσιοποίηση τρωτών σημείων

Άρθρο 37

Ανταλλαγή πληροφοριών με την εθνική αρχή πιστοποίησης της κυβερνοασφάλειας

1. Οι πληροφορίες που παρέχει ο οργανισμός πιστοποίησης στην εθνική αρχή πιστοποίησης της κυβερνοασφάλειας περιλαμβάνουν κάθε στοιχείο το οποίο είναι απαραίτητο ώστε η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας να κατανοήσει τις επιπτώσεις του τρωτού σημείου, τις αλλαγές που πρέπει να πραγματοποιηθούν στο προϊόν ΤΠΕ και, εφόσον υπάρχει, κάθε πληροφορία προερχόμενη από τον οργανισμό πιστοποίησης σχετικά με τις ευρύτερες συνέπειες του τρωτού σημείου για άλλα πιστοποιημένα προϊόντα ΤΠΕ.

2. Οι πληροφορίες που παρέχονται σύμφωνα με την παράγραφο 1 δεν περιέχουν στοιχεία σχετικά με τους τρόπους εκμετάλλευσης του τρωτού σημείου. Η παρούσα διάταξη δεν θίγει τις ερευνητικές εξουσίες της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας.

Άρθρο 38

Συνεργασία με άλλες εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας

1. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας γνωστοποιεί τις σχετικές πληροφορίες που παραλαμβάνει σύμφωνα με το άρθρο 37 σε άλλες εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας και στον ENISA.

2. Άλλες εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας μπορεί να αποφασίσουν να αναλύσουν περαιτέρω το τρωτό σημείο ή, κατόπιν ενημέρωσης του κατόχου του πιστοποιητικού EUCC, να ζητήσουν από τους αρμόδιους οργανισμούς πιστοποίησης να αξιολογήσουν αν το τρωτό σημείο ενδέχεται να επηρεάζει άλλα πιστοποιημένα προϊόντα ΤΠΕ.

Άρθρο 39

Δημοσίευση του τρωτού σημείου

Με την ανάκληση ενός πιστοποιητικού, ο κάτοχος του πιστοποιητικού EUCC γνωστοποιεί και καταχωρίζει κάθε δημόσια γνωστό και διορθωμένο τρωτό σημείο του προϊόντος ΤΠΕ στην ευρωπαϊκή βάση δεδομένων τρωτών σημείων, η οποία δημιουργήθηκε

σύμφωνα με το άρθρο 12 της οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([5]), ή σε άλλα επιγραμμικά αποθετήρια, τα οποία αναφέρονται στο άρθρο 55 παράγραφος 1 στοιχείο δ) του κανονισμού (ΕΕ) 2019/881.

ΚΕΦΑΛΑΙΟ VII

ΤΗΡΗΣΗ, ΓΝΩΣΤΟΠΟΙΗΣΗ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

Άρθρο 40

Τήρηση αρχείων από οργανισμούς πιστοποίησης και ΕΑΑΤΠ

1. Οι ΕΑΑΤΠ και οι οργανισμοί πιστοποίησης τηρούν σύστημα αρχειοθέτησης, το οποίο περιέχει όλα τα έγγραφα που καταρτίζονται σε σχέση με κάθε αξιολόγηση και πιστοποίηση που διενεργούν.

2. Οι οργανισμοί πιστοποίησης και οι ΕΑΑΤΠ αποθηκεύουν τα αρχεία με ασφαλή τρόπο και τηρούν τα εν λόγω αρχεία για το διάστημα που είναι αναγκαίο για τους σκοπούς του παρόντος κανονισμού και για τουλάχιστον 5 έτη μετά την ανάκληση του σχετικού πιστοποιητικού EUCC. Όταν ο οργανισμός πιστοποίησης εκδίδει νέο πιστοποιητικό EUCC σύμφωνα με το άρθρο 13 παράγραφος 2 στοιχείο γ), διατηρεί την τεκμηρίωση του ανακληθέντος πιστοποιητικού EUCC μαζί με το νέο πιστοποιητικό EUCC και για το ίδιο χρονικό διάστημα.

Άρθρο 41

Πληροφορίες που διατίθενται από τον κάτοχο πιστοποιητικού

1. Οι πληροφορίες που αναφέρονται στο άρθρο 55 του κανονισμού (ΕΕ) 2019/881 διατίθενται σε γλώσσα εύκολα προσβάσιμη στους χρήστες.

2. Ο κάτοχος πιστοποιητικού EUCC αποθηκεύει με ασφάλεια, για το διάστημα που είναι αναγκαίο για τους σκοπούς του παρόντος κανονισμού και για τουλάχιστον 5 έτη μετά την ανάκληση του σχετικού πιστοποιητικού EUCC, τις ακόλουθες πληροφορίες:

α) αρχεία των πληροφοριών που παρασχέθηκαν στον οργανισμό πιστοποίησης και στην ΕΑΑΤΠ κατά τη διάρκεια της διαδικασίας πιστοποίησης·

β) δείγμα του πιστοποιημένου προϊόντος ΤΠΕ.

3. Όταν ο οργανισμός πιστοποίησης εκδίδει νέο πιστοποιητικό EUCC σύμφωνα με το άρθρο 13 παράγραφος 2 στοιχείο γ), ο κάτοχος διατηρεί την τεκμηρίωση του ανακληθέντος πιστοποιητικού EUCC μαζί με το νέο πιστοποιητικό EUCC και για το ίδιο χρονικό διάστημα.

4. Κατόπιν αιτήματος του οργανισμού πιστοποίησης ή της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας, ο κάτοχος πιστοποιητικού EUCC καθιστά διαθέσιμα τα αρχεία και τα αντίγραφα που αναφέρονται στην παράγραφο 2.

Άρθρο 42

Πληροφορίες οι οποίες πρέπει να διατίθενται από τον ENISA

1. Ο ENISA δημοσιεύει στον ιστότοπο που αναφέρεται στο άρθρο 50 παράγραφος 1 του κανονισμού (ΕΕ) 2019/881 τις ακόλουθες πληροφορίες:

α) όλα τα πιστοποιητικά EUCC·

β) τις πληροφορίες σχετικά με το καθεστώς πιστοποιητικού EUCC, και ειδικότερα αν είναι σε ισχύ, αν έχει ανασταλεί, αν έχει ανακληθεί ή αν έχει λήξει·

γ) εκθέσεις πιστοποίησης οι οποίες αντιστοιχούν σε κάθε πιστοποιητικό EUCC·

([5]) Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) (ΕΕ L 333 της 27.12.2022, σ. 80).

δ) κατάλογο διαπιστευμένων οργανισμών αξιολόγησης της συμμόρφωσης·

ε) κατάλογο εξουσιοδοτημένων οργανισμών αξιολόγησης της συμμόρφωσης·

στ) τα έγγραφα στάθμης της τεχνικής που παρατίθενται στο παράρτημα Ι·

ζ) τις γνώμες της ευρωπαϊκής ομάδας πιστοποίησης της κυβερνοασφάλειας που αναφέρονται στο άρθρο 62 παράγραφος 4 στοιχείο γ) του κανονισμού (ΕΕ) 2019/881·

η) εκθέσεις αξιολόγησης από ομοτίμους οι οποίες εκδίδονται σύμφωνα με το άρθρο 47.

2. Οι πληροφορίες που αναφέρονται στην παράγραφο 1 διατίθενται τουλάχιστον στην αγγλική γλώσσα.

3. Οι οργανισμοί πιστοποίησης και, κατά περίπτωση, οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας ενημερώνουν αμελλητί τον ENISA σχετικά με τις αποφάσεις τους οι οποίες επηρεάζουν το περιεχόμενο ή το καθεστώς πιστοποιητικού EUCC που αναφέρεται στην παράγραφο 1 στοιχείο β).

4. Ο ENISA διασφαλίζει ότι στις πληροφορίες που δημοσιεύονται σύμφωνα με την παράγραφο 1 στοιχεία α), β) και γ) προσδιορίζονται σαφώς οι εκδόσεις πιστοποιημένου προϊόντος ΤΠΕ οι οποίες καλύπτονται από πιστοποιητικό EUCC.

Άρθρο 43

Προστασία πληροφοριών

Οι οργανισμοί αξιολόγησης της συμμόρφωσης, οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας, η ΕΟΠΙΚ, ο ENISA, η Επιτροπή και κάθε άλλο μέρος μεριμνούν για την ασφάλεια και την προστασία των επιχειρηματικών απορρήτων και άλλων εμπιστευτικών πληροφοριών, συμπεριλαμβανομένου του εμπορικού απορρήτου, καθώς και για την προστασία δικαιωμάτων διανοητικής ιδιοκτησίας, λαμβάνουν δε τα αναγκαία και κατάλληλα τεχνικά και οργανωτικά μέτρα.

ΚΕΦΑΛΑΙΟ VIII

ΣΥΜΦΩΝΙΕΣ ΑΜΟΙΒΑΙΑΣ ΑΝΑΓΝΩΡΙΣΗΣ ΜΕ ΤΡΙΤΕΣ ΧΩΡΕΣ

Άρθρο 44

Προϋποθέσεις

1. Τρίτες χώρες οι οποίες είναι διατεθειμένες να πιστοποιήσουν τα προϊόντα τους σύμφωνα με τον παρόντα κανονισμό και οι οποίες επιθυμούν να αναγνωριστεί η εν λόγω πιστοποίηση από την Ένωση συνάπτουν με την Ένωση συμφωνία αμοιβαίας αναγνώρισης.

2. Η συμφωνία αμοιβαίας αναγνώρισης καλύπτει τα εφαρμοστέα επίπεδα διασφάλισης για πιστοποιημένα προϊόντα ΤΠΕ και, εφόσον συντρέχει περίπτωση, για χαρακτηριστικά προστασίας.

3. Οι συμφωνίες αμοιβαίας αναγνώρισης που αναφέρονται στην παράγραφο 1 μπορούν να συνάπτονται μόνον με τρίτες χώρες που πληρούν τις ακόλουθες προϋποθέσεις:

α) διαθέτουν μια αρχή η οποία:

1) είναι δημόσιος οργανισμός, ανεξάρτητος από τις οντότητες τις οποίες εποπτεύει και παρακολουθεί όσον αφορά την οργανωτική και νομική δομή, την οικονομική χρηματοδότηση και τη λήψη αποφάσεων·

2) διαθέτει κατάλληλες εξουσίες παρακολούθησης και εποπτείας για τη διενέργεια ερευνών και είναι εξουσιοδοτημένη να λαμβάνει κατάλληλα διορθωτικά μέτρα για τη διασφάλιση συμμόρφωσης·

3) διαθέτει αποτελεσματικό, αναλογικό και αποτρεπτικό σύστημα επιβολής κυρώσεων για τη διασφάλιση συμμόρφωσης·

4) συμφωνεί να συνεργάζεται με την ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και τον ENISA για την ανταλλαγή βέλτιστων πρακτικών και σχετικών εξελίξεων στον τομέα της πιστοποίησης της κυβερνοασφάλειας και να καταβάλλει προσπάθειες για την ομοιόμορφη ερμηνεία των επί του παρόντος εφαρμοστέων κριτηρίων και μεθόδων αξιολόγησης, μεταξύ άλλων, μέσω της εφαρμογής εναρμονισμένης τεκμηρίωσης η οποία είναι ισοδύναμη με τα έγγραφα στάθμης της τεχνικής που παρατίθενται στο παράρτημα Ι·

β) διαθέτουν ανεξάρτητο οργανισμό διαπίστευσης ο οποίος πραγματοποιεί διαπιστεύσεις κάνοντας χρήση προτύπων ισοδύναμων με εκείνα που αναφέρονται στον κανονισμό (ΕΚ) αριθ. 765/2008·

γ) δεσμεύονται ότι οι διεργασίες και διαδικασίες αξιολόγησης και πιστοποίησης θα εκτελούνται με τον δέοντα επαγγελματισμό, λαμβάνοντας υπόψη τη συμμόρφωση με τα διεθνή πρότυπα που αναφέρονται στον παρόντα κανονισμό, και ειδικότερα στο άρθρο 3·

δ) έχουν την ικανότητα να αναφέρουν τρωτά σημεία που δεν έχουν εντοπισθεί προηγουμένως και διαθέτουν παγιωμένη και κατάλληλη διαδικασία διαχείρισης και γνωστοποίησης τρωτών σημείων·

ε) διαθέτουν παγιωμένες διαδικασίες για την αποτελεσματική υποβολή και τον χειρισμό καταγγελιών και την παροχή αποτελεσματικών μέσων έννομης προστασίας στους καταγγέλλοντες·

στ) θεσπίζουν μηχανισμό συνεργασίας με άλλους οργανισμούς της Ένωσης και των κρατών μελών στον τομέα της πιστοποίησης της κυβερνοασφάλειας στο πλαίσιο του παρόντος κανονισμού, ο οποίος περιλαμβάνει ανταλλαγή πληροφοριών σχετικά με ενδεχόμενη μη συμμόρφωση πιστοποιητικών, παρακολούθηση των σχετικών εξελίξεων στον τομέα της πιστοποίησης και διασφάλιση κοινής προσέγγισης για τη διατήρηση και την επανεξέταση της πιστοποίησης.

4. Επιπλέον των προϋποθέσεων που καθορίζονται στην παράγραφο 3, συμφωνία αμοιβαίας αναγνώρισης που αναφέρεται στην παράγραφο 1 η οποία καλύπτει «υψηλό» επίπεδο διασφάλισης μπορεί να συναφθεί με τρίτες χώρες μόνον εάν πληρούνται επίσης οι ακόλουθες προϋποθέσεις:

α) η τρίτη χώρα διαθέτει ανεξάρτητη και δημόσια αρχή πιστοποίησης της κυβερνοασφάλειας η οποία εκτελεί ή αναθέτει δραστηριότητες αξιολόγησης αναγκαίες για την πιστοποίηση σε «υψηλό» επίπεδο διασφάλισης οι οποίες είναι ισοδύναμες με τις απαιτήσεις και τις διαδικασίες που καθορίζονται για τις εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας στον παρόντα κανονισμό και στον κανονισμό (ΕΕ) 2019/881·

β) η συμφωνία αμοιβαίας αναγνώρισης θεσπίζει κοινό μηχανισμό ισοδύναμο με την αξιολόγηση από ομοτίμους για την πιστοποίηση EUCC με σκοπό τη βελτίωση της ανταλλαγής πρακτικών και την από κοινού επίλυση ζητημάτων στον τομέα της αξιολόγησης και της πιστοποίησης.

ΚΕΦΑΛΑΙΟ IX

ΑΞΙΟΛΟΓΗΣΗ ΟΡΓΑΝΙΣΜΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ ΑΠΟ ΟΜΟΤΙΜΟΥΣ

Άρθρο 45

Διαδικασία αξιολόγησης από ομοτίμους

1. Οργανισμός πιστοποίησης ο οποίος εκδίδει πιστοποιητικά EUCC σε «υψηλό» επίπεδο διασφάλισης υποβάλλεται σε αξιολόγηση από ομοτίμους σε τακτική βάση και τουλάχιστον κάθε 5 έτη. Οι διάφοροι τύποι αξιολόγησης από ομοτίμους απαριθμούνται στο παράρτημα VI.

2. Η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας καταρτίζει και διατηρεί πρόγραμμα αξιολογήσεων από ομοτίμους ώστε να διασφαλίζεται η τήρηση της ως άνω περιοδικότητας. Πλην δεόντως αιτιολογημένων περιπτώσεων, οι αξιολογήσεις από ομοτίμους διενεργούνται επιτόπου.

3. Η αξιολόγηση από ομοτίμους μπορεί να βασίζεται σε τεκμηρίωση που συλλέχθηκε στο πλαίσιο προγενέστερων αξιολογήσεων από ομοτίμους ή παρόμοιων διαδικασιών του οργανισμού πιστοποίησης που αξιολογείται από ομοτίμους ή της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας, εφόσον:

α) τα αποτελέσματα δεν είναι παλαιότερα των 5 ετών·

β) τα αποτελέσματα συνοδεύονται από περιγραφή των διαδικασιών αξιολόγησης που ομοτίμους που θεσπίστηκαν για το συγκεκριμένο σχήμα όταν αφορούν αξιολόγηση από ομοτίμους η οποία διενεργήθηκε υπό διαφορετικό σχήμα πιστοποίησης·

γ) στην έκθεση αξιολόγησης από ομοτίμους που αναφέρεται στο άρθρο 47 προσδιορίζονται τα αποτελέσματα τα οποία χρησιμοποιούνται εκ νέου με ή χωρίς περαιτέρω αξιολόγηση.

4. Όταν η αξιολόγηση από ομοτίμους καλύπτει τεχνικό τομέα, αξιολογείται επίσης η οικεία ΕΑΑΤΠ.

5. Ο οργανισμός πιστοποίησης που αξιολογείται από ομοτίμους και, εφόσον απαιτείται, η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας διασφαλίζουν ότι κάθε σχετική πληροφορία τίθεται στη διάθεση της ομάδας αξιολόγησης από ομοτίμους.

6. Η αξιολόγηση από ομοτίμους διενεργείται από ομάδα αξιολόγησης από ομοτίμους η οποία συστήνεται σύμφωνα με τα προβλεπόμενα στο παράρτημα VI.

Άρθρο 46

Στάδια της αξιολόγησης από ομοτίμους

1. Κατά το προπαρασκευαστικό στάδιο, τα μέλη της ομάδας αξιολόγησης από ομοτίμους επανεξετάζουν την τεκμηρίωση του οργανισμού πιστοποίησης, η οποία καλύπτει τις πολιτικές και τις διαδικασίες του, συμπεριλαμβανομένης της χρήσης εγγράφων στάθμης της τεχνικής.

2. Κατά το στάδιο της επιτόπιας επίσκεψης, η ομάδα αξιολόγησης από ομοτίμους αξιολογεί την τεχνική ικανότητα του οργανισμού και, κατά περίπτωση, την ικανότητα ΕΑΑΤΠ η οποία διενήργησε τουλάχιστον μία αξιολόγηση προϊόντος ΤΠΕ που καλύπτεται από αξιολόγηση από ομοτίμους.

3. Η διάρκεια του σταδίου της επιτόπιας επίσκεψης μπορεί να παραταθεί ή να μειωθεί ανάλογα με παράγοντες όπως η δυνατότητα εκ νέου χρησιμοποίησης υφιστάμενης τεκμηρίωσης και αποτελεσμάτων αξιολόγησης από ομοτίμους ή ο αριθμός ΕΑΑΤΠ και τεχνικών τομέων για τους οποίους ο οργανισμός πιστοποίησης εκδίδει πιστοποιητικά.

4. Κατά περίπτωση, η ομάδα αξιολόγησης από ομοτίμους εξακριβώνει την τεχνική ικανότητα κάθε ΕΑΑΤΠ επισκεπτόμενη το/τα τεχνικό/-α εργαστήριο/-ά της και πραγματοποιώντας συνεντεύξεις με τους αξιολογητές της σχετικά με τον τεχνικό τομέα και τις σχετικές ειδικές μεθόδους κυβερνοεπίθεσης.

5. Στο στάδιο υποβολής έκθεσης, η ομάδα αξιολόγησης από ομοτίμους καταγράφει τα ευρήματά της σε έκθεση αξιολόγησης από ομοτίμους, η οποία περιλαμβάνει τα πορίσματα και, κατά περίπτωση, κατάλογο των περιπτώσεων μη συμμόρφωσης που παρατηρήθηκαν, καθεμία εκ των οποίων βαθμολογείται σύμφωνα με το επίπεδο κρισιμότητά της.

6. Η έκθεση αξιολόγησης από ομοτίμους πρέπει να συζητείται πρώτα με τον οργανισμό πιστοποίησης που υποβάλλεται στην αξιολόγηση από ομοτίμους. Μετά τις εν λόγω συζητήσεις, ο υποβληθείς σε αξιολόγηση από ομοτίμους οργανισμός πιστοποίησης καταρτίζει χρονοδιάγραμμα των μέτρων που πρέπει να ληφθούν για την αντιμετώπιση των ζητημάτων που περιγράφονται στα πορίσματα.

Άρθρο 47

Έκθεση αξιολόγησης από ομοτίμους

1. Η ομάδα αξιολόγησης από ομοτίμους παρέχει στον οργανισμό πιστοποίησης που υποβάλλεται σε αξιολόγηση από ομοτίμους σχέδιο της έκθεσης αξιολόγησης από ομοτίμους.

2. Ο οργανισμός πιστοποίησης που υποβάλλεται σε αξιολόγηση από ομοτίμους υποβάλλει στην ομάδα αξιολόγησης από ομοτίμους σχόλια σχετικά με τα ευρήματα και κατάλογο δεσμεύσεων για την αντιμετώπιση των ελλείψεων που προσδιορίζονται στο σχέδιο έκθεσης αξιολόγησης από ομοτίμους.

3. Η ομάδα αξιολόγησης από ομοτίμους υποβάλλει στην ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας τελική έκθεση αξιολόγησης από ομοτίμους, η οποία περιλαμβάνει επίσης τα σχόλια και τις δεσμεύσεις του οργανισμού πιστοποίησης που υποβλήθηκε σε αξιολόγηση από ομοτίμους. Η ομάδα αξιολόγησης από ομοτίμους περιλαμβάνει επίσης στην έκθεση τη θέση της επί των σχολίων και τη γνώμη της για το κατά πόσον οι δεσμεύσεις επαρκούν για την αντιμετώπιση των ελλείψεων που προσδιορίστηκαν.

4. Εάν στην έκθεση αξιολόγησης από ομοτίμους προσδιορίζονται περιπτώσεις μη συμμόρφωσης, η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας δύναται να τάξει κατάλληλη προθεσμία στον οργανισμό πιστοποίησης που υποβάλλεται σε αξιολόγηση από ομοτίμους προκειμένου να αντιμετωπίσει τις εν λόγω περιπτώσεις μη συμμόρφωσης.

5. Η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας εκδίδει γνώμη σχετικά με την έκθεση αξιολόγησης από ομοτίμους:

α) εάν στην έκθεση αξιολόγησης από ομοτίμους δεν προσδιορίζονται περιπτώσεις μη συμμόρφωσης ή εάν ο οργανισμός πιστοποίησης που υποβάλλεται σε αξιολόγηση από ομοτίμους αντιμετώπισε κατάλληλα τις περιπτώσεις μη συμμόρφωσης, η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας δύναται να εκδώσει θετική γνώμη και όλα τα σχετικά έγγραφα δημοσιεύονται στον ιστότοπο του ENISA για την πιστοποίηση·

β) σε περίπτωση που ο οργανισμός πιστοποίησης που υποβάλλεται σε αξιολόγηση από ομοτίμους δεν αντιμετώπισε κατάλληλα τις περιπτώσεις μη συμμόρφωσης εντός της ταχθείσας προθεσμίας, η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας δύναται να εκδώσει αρνητική γνώμη η οποία δημοσιεύεται στον ιστότοπο του ENISA για την πιστοποίηση, συμπεριλαμβανομένων της έκθεσης αξιολόγησης από ομοτίμους και όλων των σχετικών εγγράφων.

6. Κάθε ευαίσθητη, προσωπική ή ιδιόκτητη πληροφορία απαλείφεται από τα έγγραφα πριν από τη δημοσίευσή τους.

ΚΕΦΑΛΑΙΟ X

ΔΙΑΤΗΡΗΣΗ ΤΟΥ ΣΧΗΜΑΤΟΣ

Άρθρο 48

Διατήρηση του EUCC

1. Η Επιτροπή δύναται να ζητήσει από την ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας να εκδώσει γνώμη με σκοπό τη διατήρηση του EUCC και την πραγματοποίηση των αναγκαίων προπαρασκευαστικών εργασιών.

2. Η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας μπορεί να εκδίδει γνώμη για την έγκριση εγγράφων στάθμης της τεχνικής.

3. Ο ENISA δημοσιεύει τα έγγραφα στάθμης της τεχνικής τα οποία έχει εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας.

ΚΕΦΑΛΑΙΟ XI

ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 49

Εθνικά σχήματα τα οποία καλύπτονται από το EUCC

1. Σύμφωνα με το άρθρο 57 παράγραφος 1 του κανονισμού (ΕΕ) 2019/881 και με την επιφύλαξη του άρθρου 57 παράγραφος 3 του ίδιου κανονισμού, κάθε εθνικό σχήμα πιστοποίησης της κυβερνοασφάλειας και σχετική διαδικασία για προϊόντα ΤΠΕ και διαδικασίες ΤΠΕ που καλύπτονται από το EUCC παύει να παράγει αποτελέσματα 12 μήνες από την έναρξη ισχύος του παρόντος κανονισμού.

2. Κατά παρέκκλιση από το άρθρο 50, διαδικασία πιστοποίησης μπορεί να κινηθεί στο πλαίσιο εθνικού σχήματος πιστοποίησης της κυβερνοασφάλειας εντός 12 μηνών από την έναρξη ισχύος του παρόντος κανονισμού, εφόσον η διαδικασία πιστοποίησης ολοκληρωθεί το αργότερο εντός 24 μηνών από την έναρξη ισχύος του παρόντος κανονισμού.

3. Τα πιστοποιητικά που εκδίδονται στο πλαίσιο εθνικών σχημάτων πιστοποίησης της κυβερνοασφάλειας μπορεί να υπόκεινται σε επανεξέταση. Τα νέα πιστοποιητικά τα οποία αντικαθιστούν τα πιστοποιητικά που επανεξετάστηκαν εκδίδονται σύμφωνα με τον παρόντα κανονισμό.

Άρθρο 50

Έναρξη ισχύος

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

Εφαρμόζεται από τις 27 Φεβρουαρίου 2025.

Το κεφάλαιο IV και το παράρτημα V εφαρμόζονται από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού.

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

Βρυξέλλες, 31 Ιανουαρίου 2024.

Για την Επιτροπή
Η Πρόεδρος
Ursula VON DER LEYEN

ΠΑΡΑΡΤΗΜΑ Ι

Τεχνικοί τομείς και έγγραφα στάθμης της τεχνικής

1. Τεχνικοί τομείς σε επίπεδο AVA_VAN 4 ή 5:

   α) έγγραφα σχετικά με την εναρμονισμένη αξιολόγηση του τεχνικού τομέα «έξυπνες κάρτες και παρεμφερείς διατάξεις» και ιδίως τα ακόλουθα έγγραφα στην αντίστοιχη έκδοσή τους που ίσχυε την [ημερομηνία έναρξης ισχύος]:

      1) «Minimum ITSEF requirements for security evaluations of smart cards and similar devices», εγκεκριμένο αρχικά από την ΕΟΠΙΚ στις 20 Οκτωβρίου 2023·

      2) «Minimum Site Security Requirements», εγκεκριμένο αρχικά από την ΕΟΠΙΚ στις 20 Οκτωβρίου 2023·

      3) «Application of Common Criteria to integrated circuits», εγκεκριμένο αρχικά από την ΕΟΠΙΚ στις 20 Οκτωβρίου 2023·

      4) «Security Architecture requirements (ADV_ARC) for smart cards and similar devices», εγκεκριμένο αρχικά από την ΕΟΠΙΚ στις 20 Οκτωβρίου 2023·

      5) «Certification of "open" smart card products», εγκεκριμένο αρχικά από την ΕΟΠΙΚ στις 20 Οκτωβρίου 2023·

      6) «Composite product evaluation for smart cards and similar devices», εγκεκριμένο αρχικά από την ΕΟΠΙΚ στις 20 Οκτωβρίου 2023·

      7) «Application of Attack Potential to Smartcards», εγκεκριμένο αρχικά από την ΕΟΠΙΚ στις 20 Οκτωβρίου 2023·

   β) έγγραφα σχετικά με την εναρμονισμένη αξιολόγηση του τεχνικού τομέα «διατάξεις υλισμικού με θυρίδες ασφαλείας» και ιδίως τα ακόλουθα έγγραφα στην αντίστοιχη έκδοσή τους που ίσχυε την [ημερομηνία έναρξης ισχύος]:

      1) «Minimum ITSEF requirements for security evaluations of hardware devices with security boxes», εγκεκριμένο αρχικά από την ΕΟΠΙΚ στις 20 Οκτωβρίου 2023·

      2) «Minimum Site Security Requirements», εγκεκριμένο αρχικά από την ΕΟΠΙΚ στις 20 Οκτωβρίου 2023·

      3) «Application of Attack Potential to hardware devices with security boxes», εγκεκριμένο αρχικά από την ΕΟΠΙΚ στις 20 Οκτωβρίου 2023.

2. Έγγραφα στάθμης της τεχνικής στην αντίστοιχη έκδοσή τους που ίσχυε την [ημερομηνία έναρξης ισχύος]:

   α) έγγραφο σχετικό με την εναρμονισμένη διαπίστευση των οργανισμών αξιολόγησης της συμμόρφωσης: «Accreditation of ITSEFs for the EUCC», εγκεκριμένο αρχικά από την ΕΟΠΙΚ στις 20 Οκτωβρίου 2023.

ΠΑΡΑΡΤΗΜΑ ΙΙ

Χαρακτηριστικά προστασίας πιστοποιημένα σε επίπεδο AVA_VAN 4 ή 5

1. Για την κατηγορία εγκεκριμένων διατάξεων εξ αποστάσεως δημιουργίας υπογραφών και σφραγίδων:

1) EN 419241-2:2019 — Αξιόπιστα συστήματα υποστήριξης της υπογραφής εξυπηρετητή — Μέρος 2: Χαρακτηριστικό προστασίας για QSCD για την υπογραφή εξυπηρετητή·

2) EN 419221-5:2018 — Κρυπτογραφικά δομοστοιχεία για παρόχους υπηρεσιών εμπιστοσύνης — μέρος 5: Κρυπτογραφικό δομοστοιχείο για υπηρεσίες εμπιστοσύνης

2. Χαρακτηριστικά προστασίας τα οποία θεσπίστηκαν ως έγγραφα στάθμης της τεχνικής:

[ΚΕΝΟ]

ΠΑΡΑΡΤΗΜΑ III

Συνιστώμενα χαρακτηριστικά προστασίας (που απεικονίζουν τους τεχνικούς τομείς από το παράρτημα I)

Χαρακτηριστικά προστασίας που χρησιμοποιούνται για την πιστοποίηση προϊόντων ΤΠΕ που εμπίπτουν στην κατωτέρω αναφερόμενη κατηγορία προϊόντων ΤΠΕ:

α) για την κατηγορία των μηχαναγνώσιμων ταξιδιωτικών εγγράφων:

1) PP Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01·

2) PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control, BSI-CC-PP-0056-2009·

3) PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012-MA-02·

4) PP for a Machine Readable Travel Document with "ICAO Application" Basic Access Control, BSI-CC-PP-0055-2009·

β) για την κατηγορία των ασφαλών διατάξεων δημιουργίας υπογραφής:

1) EN 419211-1:2014 — Χαρακτηριστικά προστασίας για ασφαλή διάταξη δημιουργίας υπογραφής — μέρος 1: Συνοπτική παρουσίαση

2) EN 419211-2:2013 — Χαρακτηριστικά προστασίας για ασφαλή διάταξη δημιουργίας υπογραφής — μέρος 2: Διάταξη με δημιουργία κλειδιού·

3) EN 419211-3:2013 — Χαρακτηριστικά προστασίας για ασφαλή διάταξη δημιουργίας υπογραφής — μέρος 3: Διάταξη με εισαγωγή κλειδιού·

4) EN 419211-4:2013 — Χαρακτηριστικά προστασίας για ασφαλή διάταξη δημιουργίας υπογραφής — μέρος 4: Επέκταση για διάταξη με δημιουργία κλειδιού και αξιόπιστο δίαυλο για την εφαρμογή δημιουργίας πιστοποιητικού

5) EN 419211-5:2013 — Χαρακτηριστικά προστασίας για ασφαλή διάταξη δημιουργίας υπογραφής — μέρος 5: Επέκταση για διάταξη με δημιουργία κλειδιού και αξιόπιστο δίαυλο για την εφαρμογή δημιουργίας υπογραφής·

6) EN 419211-6:2014 — Χαρακτηριστικά προστασίας για ασφαλή διάταξη δημιουργίας υπογραφής — μέρος 6: Επέκταση για διάταξη με εισαγωγή κλειδιού και αξιόπιστο δίαυλο για την εφαρμογή δημιουργίας υπογραφής·

γ) για την κατηγορία των ψηφιακών ταχογράφων:

1) Ψηφιακός ταχογράφος — Κάρτα ταχογράφου, όπως αναφέρεται στον εκτελεστικό κανονισμό (ΕΕ) 2016/799 της Επιτροπής, της 18ης Μαρτίου 2016, σχετικά με την εφαρμογή του κανονισμού (ΕΕ) αριθ. 165/2014 (παράρτημα 1Γ)·

2) Ψηφιακός ταχογράφος — Μονάδα επί οχήματος, όπως αναφέρεται στο παράρτημα I Β του κανονισμού (ΕΚ) αριθ. 1360/2002 της Επιτροπής, η οποία προορίζεται για εγκατάσταση σε οχήματα οδικών μεταφορών·

3) Ψηφιακός ταχογράφος — Εξωτερικός μηχανισμός GNSS (EGF PP), όπως αναφέρεται στο παράρτημα 1Γ του εκτελεστικού κανονισμού (ΕΕ) 2016/799 της Επιτροπής, της 18ης Μαρτίου 2016, σχετικά με την εφαρμογή του κανονισμού (ΕΕ) αριθ. 165/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου·

4) Ψηφιακός ταχογράφος — Αισθητήρας κίνησης (MS PP), όπως αναφέρεται στο παράρτημα 1Γ του εκτελεστικού κανονισμού (ΕΕ) 2016/799 της Επιτροπής, της 18ης Μαρτίου 2016, σχετικά με την εφαρμογή του κανονισμού (ΕΕ) αριθ. 165/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου·

δ) για την κατηγορία ασφαλών ολοκληρωμένων κυκλωμάτων, έξυπνων καρτών και συναφών διατάξεων:

1) Security IC Platform PP, BSI-CC-PP-0084-2014·

2) Java Card System - Open Configuration, V3.0.5 BSI-CC-PP-0099-2017·

3) Java Card System - Closed Configuration, BSI-CC-PP-0101-2017·

4) PP for a PC Client Specific Trusted Platform Module Family 2.0 Level 0 Revision 1.16, ANSSI-CC-PP-2015/07·

5) Universal SIM card, PU-2009-RT-79, ANSSI-CC-PP-2010/04·

6) Embedded UICC (eUICC) for Machine-to-Machine Devices, BSI-CC-PP-0089-2015·

ε) για την κατηγορία των σημείων αλληλεπίδρασης (με σκοπό τις πληρωμές) και των τερματικών σημείου πώλησης:

1) Σημείο αλληλεπίδρασης «POI-CHIP-ONLY», ANSSI-CC-PP-2015/01·

2) Σημείο αλληλεπίδρασης «POI-CHIP-ONLY and Open Protocol Package», ANSSI-CC-PP-2015/02·

3) Σημείο αλληλεπίδρασης «POI-COMPREHENSIVE», ANSSI-CC-PP-2015/03·

4) Σημείο αλληλεπίδρασης «POI-COMPREHENSIVE and Open Protocol Package», ANSSI-CC-PP-2015/04·

5) Σημείο αλληλεπίδρασης «POI-PED-ONLY», ANSSI-CC-PP-2015/05·

6) Σημείο αλληλεπίδρασης «POI-PED-ONLY and Open Protocol Package», ANSSI-CC-PP-2015/06·

στ) για την κατηγορία διατάξεων υλισμικού με θυρίδες ασφαλείας:

1) Cryptographic Module for CSP Signing Operations with Backup - PP CMCSOB, PP HSM CMCSOB 14167-2, ANSSI-CC-PP-2015/08·

2) Cryptographic Module for CSP key generation services - PP CMCKG, PP HSM CMCKG 14167-3, ANSSI-CC-PP-2015/09·

3) Cryptographic Module for CSP Signing Operations without Backup - PP CMCSO, PP HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10.

ΠΑΡΑΡΤΗΜΑ IV

Συνεχεια διασφαλισησ και επανεξεταση Πιστοποιητικων

IV.1 **Συνέχεια διασφάλισης: πεδίο**

1. Οι ακόλουθες απαιτήσεις για τη συνέχεια της διασφάλισης εφαρμόζονται στις δραστηριότητες διατήρησης που αφορούν τα ακόλουθα:

   α) επαναξιολόγηση του κατά πόσον ένα αμετάβλητο πιστοποιημένο προϊόν ΤΠΕ εξακολουθεί να πληροί τις απαιτήσεις ασφάλειας που το αφορούν·

   β) αξιολόγηση των συνεπειών των αλλαγών πιστοποιημένου προϊόντος ΤΠΕ στην πιστοποίησή του·

   γ) εάν περιλαμβάνεται στην πιστοποίηση, εφαρμογή διορθώσεων σύμφωνα με αξιολογημένη διαδικασία διαχείρισης διορθώσεων·

   δ) εάν περιλαμβάνεται, επανεξέταση της διαχείρισης του κύκλου ζωής ή των διαδικασιών παραγωγής του κατόχου του πιστοποιητικού.

2. Ο κάτοχος πιστοποιητικού EUCC μπορεί να ζητήσει την επανεξέταση του πιστοποιητικού στις ακόλουθες περιπτώσεις:

   α) το πιστοποιητικό EUCC λήγει εντός εννέα μηνών·

   β) υπήρξε αλλαγή είτε στο πιστοποιημένο προϊόν ΤΠΕ είτε σε άλλον παράγοντα, η οποία θα μπορούσε να έχει επιπτώσεις στη λειτουργικότητα ασφαλείας του·

   γ) ο κάτοχος του πιστοποιητικού ζητεί να διενεργηθεί εκ νέου η αξιολόγηση τρωτότητας προκειμένου να επαναβεβαιωθεί η διασφάλιση του πιστοποιητικού EUCC η οποία σχετίζεται με την ανθεκτικότητα του προϊόντος ΤΠΕ σε σύγχρονες κυβερνοεπιθέσεις.

IV.2 **Επαναξιολόγηση**

1. Σε περίπτωση που υπάρχει ανάγκη εκτίμησης των επιπτώσεων των αλλαγών στο περιβάλλον απειλής ενός αμετάβλητου πιστοποιημένου προϊόντος ΤΠΕ, υποβάλλεται στον οργανισμό πιστοποίησης αίτημα επαναξιολόγησης.

2. Η επαναξιολόγηση διενεργείται από την ίδια ΕΑΑΤΠ που συμμετείχε στην προηγούμενη αξιολόγηση κάνοντας εκ νέου χρήση όλων των αποτελεσμάτων της που εξακολουθούν να ισχύουν. Η αξιολόγηση επικεντρώνεται στις δραστηριότητες διασφάλισης οι οποίες επηρεάζονται δυνητικώς από τις μεταβολές στις κυβερνοαπειλές που αφορούν πιστοποιημένο προϊόν ΤΠΕ, ειδικότερα τη σχετική οικογένεια AVA_VAN και, επιπλέον, την οικογένεια κύκλου ζωής διασφάλισης (ALC), οπότε συλλέγεται εκ νέου επαρκής τεκμηρίωση σχετικά με τη διατήρηση του περιβάλλοντος ανάπτυξης.

3. Η ΕΑΑΤΠ περιγράφει τις αλλαγές και αναφέρει λεπτομερώς τα αποτελέσματα της επαναξιολόγησης με επικαιροποίηση της προηγούμενης τεχνικής έκθεσης αξιολόγησης.

4. Ο οργανισμός πιστοποίησης επανεξετάζει την επικαιροποιημένη τεχνική έκθεση αξιολόγησης και εκπονεί έκθεση επαναξιολόγησης. Στη συνέχεια το καθεστώς του αρχικού πιστοποιητικού τροποποιείται σύμφωνα με το άρθρο 13.

5. Η έκθεση επαναξιολόγησης και το επικαιροποιημένο πιστοποιητικό υποβάλλονται στην εθνική αρχή πιστοποίησης της κυβερνοασφάλειας και στον ENISA για δημοσίευση στον οικείο ιστότοπο πιστοποίησης της κυβερνοασφάλειας.

IV.3 **Αλλαγές σε πιστοποιημένο προϊόν ΤΠΕ**

1. Σε περίπτωση που ένα πιστοποιημένο προϊόν ΤΠΕ έχει υποστεί αλλαγές, ο κάτοχος του πιστοποιητικού που επιθυμεί να διατηρήσει το πιστοποιητικό υποβάλλει στον οργανισμό πιστοποίησης έκθεση ανάλυσης επιπτώσεων.

2. Η έκθεση ανάλυσης επιπτώσεων περιέχει τα ακόλουθα στοιχεία:

   α) εισαγωγή, στην οποία παρατίθενται οι απαραίτητες πληροφορίες για τον προσδιορισμό της έκθεσης ανάλυσης επιπτώσεων και του στόχου αξιολόγησης που μεταβάλλονται·

β) περιγραφή των αλλαγών του προϊόντος·

γ) προσδιορισμό της επηρεαζόμενης τεκμηρίωσης του φορέα ανάπτυξης·

δ) περιγραφή των τροποποιήσεων της τεκμηρίωσης του φορέα ανάπτυξης·

ε) τα ευρήματα και τα συμπεράσματα σχετικά με τις επιπτώσεις κάθε αλλαγής στη διασφάλιση.

3. Ο οργανισμός πιστοποίησης εξετάζει τις αλλαγές που περιγράφονται στην έκθεση ανάλυσης επιπτώσεων προκειμένου να επικυρώσει τις επιπτώσεις τους στη διασφάλιση του πιστοποιημένου στόχου αξιολόγησης, όπως προτείνεται στα συμπεράσματα της έκθεσης ανάλυσης επιπτώσεων.

4. Μετά την εξέταση, ο οργανισμός πιστοποίησης προσδιορίζει την κλίμακα της αλλαγής ως ήσσονος σημασίας ή μείζονος σημασίας ανάλογα με τις επιπτώσεις της.

5. Σε περίπτωση που οι αλλαγές έχουν επιβεβαιωθεί από τον οργανισμό πιστοποίησης ως ήσσονος σημασίας, εκδίδεται νέο πιστοποιητικό για το τροποποιημένο προϊόν ΤΠΕ και εκπονείται έκθεση διατήρησης για την αρχική έκθεση πιστοποίησης, υπό τους ακόλουθους όρους:

α) η έκθεση διατήρησης αποτελεί υποσύνολο της έκθεσης ανάλυσης επιπτώσεων και περιέχει τις ακόλουθες ενότητες:

1) εισαγωγή·

2) περιγραφή αλλαγών·

3) επηρεαζόμενη τεκμηρίωση φορέα ανάπτυξης·

β) η ημερομηνία λήξης ισχύος του νέου πιστοποιητικού δεν βαίνει πέραν της ημερομηνίας λήξης ισχύος του αρχικού πιστοποιητικού.

6. Το νέο πιστοποιητικό, συμπεριλαμβανομένης της έκθεσης διατήρησης, υποβάλλεται στον ENISA για δημοσίευση στον οικείο ιστότοπο πιστοποίησης της κυβερνοασφάλειας.

7. Σε περίπτωση που ο οργανισμός πιστοποίησης επιβεβαίωσε ότι οι αλλαγές είναι μείζονος σημασίας, διενεργείται εκ νέου αξιολόγηση στο πλαίσιο της προηγούμενης αξιολόγησης και με την εκ νέου χρήση τυχόν αποτελεσμάτων της προηγούμενης αξιολόγησης που εξακολουθούν να ισχύουν.

8. Μετά την ολοκλήρωση της αξιολόγησης του μεταβληθέντος στόχου αξιολόγησης, η ΕΑΑΤΠ εκπονεί νέα τεχνική έκθεση αξιολόγησης. Ο οργανισμός πιστοποίησης επανεξετάζει την επικαιροποιημένη τεχνική έκθεση αξιολόγησης και, κατά περίπτωση, καταρτίζει νέο πιστοποιητικό με νέα έκθεση πιστοποίησης.

9. Το νέο πιστοποιητικό και η νέα έκθεση πιστοποίησης υποβάλλονται στον ENISA για δημοσίευση.

IV.4 **Διαχείριση διορθώσεων**

1. Η διαδικασία διαχείρισης διορθώσεων παρέχει μια δομημένη διαδικασία για την επικαιροποίηση πιστοποιημένου προϊόντος ΤΠΕ. Η διαδικασία διαχείρισης διορθώσεων, συμπεριλαμβανομένου του μηχανισμού ο οποίος εφαρμόζεται στο προϊόν ΤΠΕ από τον αιτούντα πιστοποίηση, μπορεί να χρησιμοποιηθεί μετά την πιστοποίηση του προϊόντος ΤΠΕ υπό την ευθύνη του οργανισμού αξιολόγησης της συμμόρφωσης.

2. Ο αιτών πιστοποίηση μπορεί να συμπεριλάβει στην πιστοποίηση του προϊόντος ΤΠΕ μηχανισμό διορθώσεων, στο πλαίσιο πιστοποιημένης διαδικασίας διαχείρισης που εφαρμόζεται στο προϊόν ΤΠΕ, εφόσον πληρούται μία από τις ακόλουθες προϋποθέσεις:

α) οι λειτουργικότητες που επηρεάζονται από τη διόρθωση βρίσκονται εκτός του στόχου αξιολόγησης του πιστοποιημένου προϊόντος ΤΠΕ·

β) η διόρθωση αφορά προκαθορισμένη ήσσονος σημασίας αλλαγή στο πιστοποιημένο προϊόν ΤΠΕ·

γ) η διόρθωση αφορά επιβεβαιωμένο τρωτό σημείο με κρίσιμες συνέπειες στην ασφάλεια του πιστοποιημένου προϊόντος ΤΠΕ.

3. Εάν η διόρθωση αφορά μείζονος σημασίας αλλαγή στον στόχο αξιολόγησης του πιστοποιημένου προϊόντος ΤΠΕ σε σχέση με τρωτό σημείο που δεν είχε εντοπιστεί παλαιότερα, το οποίο δεν έχει κρίσιμες συνέπειες στην ασφάλεια του προϊόντος ΤΠΕ, εφαρμόζονται οι διατάξεις του άρθρου 13.

4. Η διαδικασία διαχείρισης διορθώσεων προϊόντος ΤΠΕ θα περιλαμβάνει τα ακόλουθα στοιχεία:

   α) τη διαδικασία ανάπτυξης και θέσης σε κυκλοφορία της διόρθωσης για το προϊόν ΤΠΕ·

   β) τον τεχνικό μηχανισμό και τις λειτουργίες για την εφαρμογή της διόρθωσης στο προϊόν ΤΠΕ·

   γ) ένα σύνολο δραστηριοτήτων αξιολόγησης όσον αφορά την αποτελεσματικότητα και την αποδοτικότητα του τεχνικού μηχανισμού.

5. Κατά την πιστοποίηση του προϊόντος ΤΠΕ:

   α) ο αιτών πιστοποίηση του προϊόντος ΤΠΕ παρέχει περιγραφή της διαδικασίας διαχείρισης διορθώσεων·

   β) η ΕΑΑΤΠ εξακριβώνει τα ακόλουθα στοιχεία:

      1) ο φορέας ανάπτυξης εφάρμοσε τους μηχανισμούς διορθώσεων στο προϊόν ΤΠΕ σύμφωνα με τη διαδικασία διαχείρισης διορθώσεων που υποβλήθηκε σε πιστοποίηση·

      2) τα όρια του στόχου αξιολόγησης διαχωρίζονται κατά τρόπο ώστε οι αλλαγές που πραγματοποιούνται στις χωριστές διαδικασίες να μην επηρεάζουν την ασφάλεια του στόχου αξιολόγησης·

      3) ο τεχνικός μηχανισμός διορθώσεων λειτουργεί σύμφωνα με τις διατάξεις του παρόντος τμήματος και τους ισχυρισμούς του αιτούντος·

   γ) ο οργανισμός πιστοποίησης περιλαμβάνει στην έκθεση πιστοποίησης το αποτέλεσμα της διαδικασίας διαχείρισης διορθώσεων που υποβλήθηκε σε αξιολόγηση.

6. Ο κάτοχος του πιστοποιητικού δύναται να εφαρμόσει στο οικείο πιστοποιημένο προϊόν ΤΠΕ τη διόρθωση που κατασκευάστηκε σύμφωνα με την πιστοποιημένη διαδικασία διαχείρισης διορθώσεων και προβαίνει στις ακόλουθες ενέργειες εντός 5 εργάσιμων ημερών στις ακόλουθες περιπτώσεις:

   α) στην περίπτωση που αναφέρεται στο σημείο 2 στοιχείο α), αναφέρει την οικεία διόρθωση στον οργανισμό πιστοποίησης ο οποίος δεν αλλάζει το αντίστοιχο πιστοποιητικό EUCC·

   β) στην περίπτωση που αναφέρεται στο σημείο 2 στοιχείο β), υποβάλλει την οικεία διόρθωση στην ΕΑΑΤΠ για επανεξέταση. Η ΕΑΑΤΠ ενημερώνει τον οργανισμό πιστοποίησης μετά την παραλαβή της διόρθωσης, οπότε ο οργανισμός πιστοποίησης προβαίνει στην κατάλληλη ενέργεια σχετικά με την έκδοση νέας έκδοσης του αντίστοιχου πιστοποιητικού EUCC και την επικαιροποίηση της έκθεσης πιστοποίησης·

   γ) στην περίπτωση που αναφέρεται στο σημείο 2 στοιχείο γ), υποβάλλει την οικεία διόρθωση στην ΕΑΑΤΠ για την αναγκαία επαναξιολόγηση, αλλά μπορεί να εφαρμόσει συγχρόνως τη διόρθωση. Η ΕΑΑΤΠ ενημερώνει τον οργανισμό πιστοποίησης, ο οποίος ξεκινά τις σχετικές δραστηριότητες πιστοποίησης.

ΠΑΡΑΡΤΗΜΑ V

ΠΕΡΙΕΧΟΜΕΝΟ ΕΚΘΕΣΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ

V.1 **Έκθεση πιστοποίησης**

1. Βάσει των τεχνικών εκθέσεων αξιολόγησης που παρέχει η ΕΑΑΤΠ, ο οργανισμός πιστοποίησης εκπονεί έκθεση πιστοποίησης η οποία δημοσιεύεται με το αντίστοιχο πιστοποιητικό EUCC.

2. Η έκθεση πιστοποίησης αποτελεί πηγή λεπτομερών και πρακτικών πληροφοριών σχετικά με το προϊόν ΤΠΕ, ή την κατηγορία προϊόντων ΤΠΕ, και σχετικά με την ασφαλή ανάπτυξη του προϊόντος ΤΠΕ και, επομένως, περιλαμβάνει κάθε δημόσια διαθέσιμη και γνωστοποιήσιμη πληροφορία η οποία έχει σημασία για τους χρήστες και τα ενδιαφερόμενα μέρη. Η έκθεση πιστοποίησης μπορεί να παραπέμπει σε δημόσια διαθέσιμες και γνωστοποιήσιμες πληροφορίες.

3. Η έκθεση πιστοποίησης περιέχει τουλάχιστον τις ακόλουθες ενότητες:

   α) συνοπτική παρουσίαση·

   β) προσδιορισμό του προϊόντος ΤΠΕ ή της κατηγορίας προϊόντων ΤΠΕ για χαρακτηριστικά προστασίας·

   γ) υπηρεσίες ασφάλειας·

   δ) παραδοχές και αποσαφήνιση πεδίου·

   ε) πληροφορίες αρχιτεκτονικής·

   στ) συμπληρωματικές πληροφορίες για την κυβερνοασφάλεια, κατά περίπτωση·

   ζ) δοκιμή του προϊόντος ΤΠΕ, εφόσον διενεργήθηκε·

   η) κατά περίπτωση, προσδιορισμό των διαδικασιών διαχείρισης του κύκλου ζωής και των εγκαταστάσεων παραγωγής του κατόχου του πιστοποιητικού·

   θ) αποτελέσματα της αξιολόγησης και πληροφορίες σχετικά με το πιστοποιητικό·

   ι) συνοπτική περιγραφή του στόχου ασφάλειας του προϊόντος ΤΠΕ που υποβάλλεται για πιστοποίηση·

   ια) όταν υπάρχει, το σήμα ή την επισήμανση που σχετίζεται με το σχήμα·

   ιβ) βιβλιογραφία.

4. Η συνοπτική παρουσίαση είναι η σύνοψη της συνολικής έκθεσης πιστοποίησης. Παρέχει σαφή και συνοπτική επισκόπηση των αποτελεσμάτων της αξιολόγησης και περιλαμβάνει τις ακόλουθες πληροφορίες:

   α) όνομα του αξιολογούμενου προϊόντος ΤΠΕ, απαρίθμηση των συνιστωσών του προϊόντος που περιλαμβάνονται στην αξιολόγηση και έκδοση του προϊόντος ΤΠΕ·

   β) όνομα της ΕΑΑΤΠ που διενήργησε την αξιολόγηση και, εφόσον συντρέχει περίπτωση, τον κατάλογο των υπεργολάβων·

   γ) ημερομηνία ολοκλήρωσης της αξιολόγησης·

   δ) παραπομπή στην τεχνική έκθεση αξιολόγησης που εκπόνησε η ΕΑΑΤΠ·

   ε) συνοπτική περιγραφή των αποτελεσμάτων της έκθεσης πιστοποίησης, και ειδικότερα:

      1) την έκδοση και, κατά περίπτωση, τη δημοσίευση των κοινών κριτηρίων που εφαρμόστηκαν στην αξιολόγηση·

      2) τη δέσμη απαιτήσεων κατοχύρωσης της ασφάλειας και τις συνιστώσες κατοχύρωσης της ασφάλειας των κοινών κριτηρίων, συμπεριλαμβανομένου του επιπέδου AVA_VAN που εφαρμόστηκε κατά την αξιολόγηση και του αντίστοιχου επιπέδου διασφάλισης που καθορίζεται στο άρθρο 52 του κανονισμού (ΕΕ) 2019/881 στο οποίο παραπέμπει το πιστοποιητικό EUCC·

      3) τη λειτουργικότητα ασφάλειας του αξιολογούμενου προϊόντος ΤΠΕ·

      4) σύνοψη των απειλών που αντιμετωπίζονται και των πολιτικών οργανωτικής ασφάλειας που λαμβάνονται υπόψη με το αξιολογούμενο προϊόν ΤΠΕ·

5) ειδικές απαιτήσεις διαμόρφωσης·

6) παραδοχές σχετικά με το λειτουργικό περιβάλλον·

7) όπου συντρέχει περίπτωση, ύπαρξη εγκεκριμένης διαδικασίας διαχείρισης διορθώσεων σύμφωνα με το τμήμα IV.4 του παραρτήματος II·

8) δήλωση/-εις αποποίησης ευθύνης.

5. Το αξιολογούμενο προϊόν ΤΠΕ προσδιορίζεται σαφώς, μεταξύ άλλων, με τις ακόλουθες πληροφορίες:

α) όνομα του αξιολογούμενου προϊόντος ΤΠΕ·

β) απαρίθμηση των συνιστωσών του προϊόντος που περιλαμβάνονται στην αξιολόγηση·

γ) τον αριθμό έκδοσης των συνιστωσών του προϊόντος ΤΠΕ·

δ) προσδιορισμό πρόσθετων απαιτήσεων του λειτουργικού περιβάλλοντος του πιστοποιημένου προϊόντος ΤΠΕ·

ε) όνομα και στοιχεία επικοινωνίας του κατόχου του πιστοποιητικού EUCC·

στ) όπου συντρέχει περίπτωση, διαδικασία διαχείρισης διορθώσεων η οποία περιλαμβάνεται στο πιστοποιητικό·

ζ) σύνδεσμο προς τον ιστότοπο του κατόχου του πιστοποιητικού EUCC, όπου παρέχονται συμπληρωματικές πληροφορίες σχετικά με την κυβερνοασφάλεια για το πιστοποιημένο προϊόν ΤΠΕ σύμφωνα με το άρθρο 55 του κανονισμού (ΕΕ) 2019/881.

6. Οι πληροφορίες που περιλαμβάνονται στο παρόν τμήμα είναι όσο το δυνατόν πιο ακριβείς ώστε να διασφαλίζεται πλήρης και ακριβής αναπαράσταση του προϊόντος ΤΠΕ η οποία μπορεί να χρησιμοποιηθεί εκ νέου σε μελλοντικές αξιολογήσεις.

7. Το τμήμα για την πολιτική ασφάλειας περιλαμβάνει περιγραφή της πολιτικής ασφάλειας του προϊόντος ΤΠΕ και των πολιτικών ή των κανόνων που πρέπει να επιβάλλει ή με τους οποίους πρέπει να συμμορφώνεται το αξιολογούμενο προϊόν ΤΠΕ. Περιλαμβάνει παραπομπή στις ακόλουθες πολιτικές, τις οποίες και περιγράφει:

α) την πολιτική του κατόχου του πιστοποιητικού για τον χειρισμό τρωτών σημείων·

β) την πολιτική του κατόχου του πιστοποιητικού για τη συνέχεια της διασφάλισης.

8. Κατά περίπτωση, η πολιτική μπορεί να περιλαμβάνει τις προϋποθέσεις που αφορούν τη χρήση διαδικασίας διαχείρισης διορθώσεων κατά την περίοδο ισχύος του πιστοποιητικού.

9. Το τμήμα για τις παραδοχές και την αποσαφήνιση του πεδίου περιέχει εξαντλητικές πληροφορίες σχετικά με τις περιστάσεις και τους στόχους που σχετίζονται με την προβλεπόμενη χρήση του προϊόντος όπως αναφέρεται στο άρθρο 7 παράγραφος 1 στοιχείο γ). Οι πληροφορίες περιλαμβάνουν τα εξής στοιχεία:

α) παραδοχές σχετικά με τη χρήση και την ανάπτυξη του προϊόντος ΤΠΕ με τη μορφή ελάχιστων απαιτήσεων, όπως πλήρωση απαιτήσεων σχετικά με κατάλληλη εγκατάσταση και διαμόρφωση καθώς και υλισμικό·

β) παραδοχές σχετικά με το περιβάλλον για τη σύμφωνη προς τις απαιτήσεις λειτουργία του προϊόντος ΤΠΕ.

10. Οι πληροφορίες που απαριθμούνται στο σημείο 9 είναι όσο το δυνατόν πιο κατανοητές για τους χρήστες του πιστοποιημένου προϊόντος ΤΠΕ ώστε να μπορούν να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με τους κινδύνους που συνδέονται με τη χρήση του.

11. Το τμήμα για τις πληροφορίες αρχιτεκτονικής περιλαμβάνει υψηλού επιπέδου περιγραφή του προϊόντος ΤΠΕ και των κύριων συνιστωσών του σύμφωνα με τον σχεδιασμό υποσυστημάτων ADV_TDS των κοινών κριτηρίων.

12. Παρέχεται πλήρης κατάλογος των συμπληρωματικών πληροφοριών σχετικά με την κυβερνοασφάλεια για το προϊόν ΤΠΕ σύμφωνα με το άρθρο 55 του κανονισμού (ΕΕ) 2019/881. Κάθε σχετικό έγγραφο επισημαίνεται με τον αριθμό της έκδοσής του.

13. Το τμήμα για τη δοκιμή του προϊόντος ΤΠΕ περιλαμβάνει τις ακόλουθες πληροφορίες:

α) επωνυμία και πρόσωπο επικοινωνίας της αρχής ή του οργανισμού που εξέδωσε το πιστοποιητικό, συμπεριλαμβανομένης της αρμόδιας εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας·

β) επωνυμία της ΕΑΑΤΠ που διενήργησε την αξιολόγηση, εάν η αξιολόγηση δεν διενεργήθηκε από τον οργανισμό πιστοποίησης·

γ) προσδιορισμό των συνιστωσών διασφάλισης που χρησιμοποιήθηκαν από τα πρότυπα που αναφέρονται στο άρθρο 3·

δ) έκδοση του εγγράφου στάθμης της τεχνικής και περαιτέρω κριτήρια αξιολόγησης της ασφάλειας που χρησιμοποιήθηκαν στην αξιολόγηση·

ε) πλήρεις και ακριβείς ρυθμίσεις και διαμόρφωση του προϊόντος ΤΠΕ κατά την αξιολόγηση, συμπεριλαμβανομένων λειτουργικών σημειώσεων και παρατηρήσεων, εφόσον υπάρχουν·

στ) κάθε χαρακτηριστικό προστασίας το οποίο έχει χρησιμοποιηθεί, συμπεριλαμβανομένων των ακόλουθων πληροφοριών:

1) δημιουργός του χαρακτηριστικού προστασίας·

2) όνομα και αναγνωριστικό του χαρακτηριστικού προστασίας·

3) αναγνωριστικό του πιστοποιητικού του χαρακτηριστικού προστασίας·

4) επωνυμία και στοιχεία επικοινωνίας του οργανισμού πιστοποίησης και της ΕΑΑΤΠ που συμμετείχαν στην αξιολόγηση του χαρακτηριστικού προστασίας·

5) δέσμη/-ες απαιτήσεων κατοχύρωσης της ασφάλειας που απαιτούνται για προϊόν που συμμορφώνεται με το χαρακτηριστικό προστασίας.

14. Το τμήμα των αποτελεσμάτων της αξιολόγησης και των πληροφοριών σχετικά με το πιστοποιητικό περιλαμβάνει τα ακόλουθα στοιχεία:

α) επιβεβαίωση του επιτευχθέντος επιπέδου διασφάλισης όπως αναφέρεται στο άρθρο 4 του παρόντος κανονισμού και στο άρθρο 52 του κανονισμού (ΕΕ) 2019/881·

β) απαιτήσεις διασφάλισης, από τα πρότυπα που αναφέρονται στο άρθρο 3, τις οποίες το προϊόν ΤΠΕ ή το χαρακτηριστικό προστασίας πληροί πραγματικά, συμπεριλαμβανομένου του επιπέδου AVA_VAN·

γ) λεπτομερή περιγραφή των απαιτήσεων διασφάλισης καθώς και στοιχεία σχετικά με την πλήρωση κάθε απαίτησης από το προϊόν·

δ) ημερομηνία έκδοσης και περίοδο ισχύος του πιστοποιητικού·

ε) μοναδικό αναγνωριστικό του πιστοποιητικού.

15. Ο στόχος ασφάλειας περιλαμβάνεται στην έκθεση πιστοποίησης ή αναφέρεται και συνοψίζεται στην έκθεση πιστοποίησης και περιέχεται στην έκθεση πιστοποίησης που τον αφορά για σκοπούς δημοσίευσης.

16. Εμπιστευτικά στοιχεία μπορεί να απαλείφονται από τον στόχο ασφάλειας σύμφωνα με το τμήμα VI.2.

17. Το σήμα ή η επισήμανση που συνδέεται με το EUCC μπορεί να περιλαμβάνεται στην έκθεση πιστοποίησης σύμφωνα με τους κανόνες και τις διαδικασίες που καθορίζονται στο άρθρο 11.

18. Το τμήμα της βιβλιογραφίας περιλαμβάνει παραπομπές σε όλα τα έγγραφα που χρησιμοποιήθηκαν για τη σύνταξη της έκθεσης πιστοποίησης. Οι πληροφορίες αυτές περιλαμβάνουν τουλάχιστον τα ακόλουθα στοιχεία:

α) τα κριτήρια αξιολόγησης της ασφάλειας, τα έγγραφα στάθμης της τεχνικής και άλλες σχετικές προδιαγραφές οι οποίες χρησιμοποιήθηκαν με μνεία της έκδοσής τους·

β) την τεχνική έκθεση αξιολόγησης·

γ) την τεχνική έκθεση αξιολόγησης για τη σύνθετη αξιολόγηση, εφόσον συντρέχει περίπτωση·

δ) τεκμηρίωση για το τεχνικό πλαίσιο αναφοράς·

ε) τεκμηρίωση του φορέα ανάπτυξης η οποία χρησιμοποιήθηκε κατά την αξιολόγηση.

19. Προκειμένου να διασφαλίζεται η δυνατότητα αναπαραγωγής της αξιολόγησης, κάθε έγγραφο στο οποίο γίνεται παραπομπή πρέπει να προσδιορίζεται με μοναδικό τρόπο, με την ορθή ημερομηνία δημοσίευσης και τον ορθό αριθμό έκδοσης.

V.2 **Απαλοιφή εμπιστευτικών στοιχείων από στόχο ασφάλειας για σκοπούς δημοσίευσης**

1. Από τον στόχο ασφάλειας που περιλαμβάνεται, ή στον οποίο γίνεται παραπομπή, στην έκθεση πιστοποίησης δυνάμει του σημείου 1 του τμήματος VI.1 μπορούν να απαλειφθούν οι ιδιοταγείς τεχνικές πληροφορίες, οι οποίες μπορεί επίσης να διατυπωθούν με άλλον τρόπο.

2. Ο στόχος ασφάλειας που προκύπτει μετά την απαλοιφή εμπιστευτικών στοιχείων είναι η πραγματική αναπαράσταση της πλήρους αρχικής έκδοσής του. Τούτο σημαίνει ότι, μετά την απαλοιφή εμπιστευτικών στοιχείων, δεν είναι δυνατόν να παραλείπονται από τον στόχο ασφάλειας πληροφορίες οι οποίες είναι αναγκαίες για να γίνουν κατανοητές οι ιδιότητες ασφάλειας του στόχου αξιολόγησης και το πεδίο της αξιολόγησης.

3. Το περιεχόμενο του στόχου ασφάλειας μετά την απαλοιφή εμπιστευτικών στοιχείων συμμορφώνεται προς τις ακόλουθες ελάχιστες απαιτήσεις:

   α) από την εισαγωγή δεν απαλείφονται εμπιστευτικά στοιχεία, καθώς η εισαγωγή δεν περιλαμβάνει γενικά ιδιοταγείς πληροφορίες·

   β) ο στόχος ασφάλειας μετά την απαλοιφή εμπιστευτικών στοιχείων πρέπει να διαθέτει μοναδικό αναγνωριστικό διαφορετικό από εκείνο της πλήρους αρχικής έκδοσής του·

   γ) η περιγραφή του στόχου αξιολόγησης μπορεί να μειωθεί, καθώς μπορεί να περιλαμβάνει ιδιοταγείς και αναλυτικές πληροφορίες σχετικά με τον σχεδιασμό του στόχου αξιολόγησης οι οποίες δεν θα πρέπει να δημοσιευθούν·

   δ) η περιγραφή του περιβάλλοντος ασφάλειας του στόχου αξιολόγησης (παραδοχές, απειλές, πολιτικές οργανωτικής ασφάλειας) δεν μειώνονται, στο μέτρο που οι πληροφορίες αυτές είναι αναγκαίες για να γίνει κατανοητό το πεδίο της αξιολόγησης·

   ε) οι στόχοι ασφάλειας δεν μειώνονται καθώς κάθε πληροφορία πρέπει να δημοσιοποιείται προκειμένου να γίνει κατανοητή η πρόθεση του στόχου ασφάλειας και του στόχου αξιολόγησης·

   στ) όλες οι απαιτήσεις ασφάλειας δημοσιοποιούνται. Σημειώσεις εφαρμογής μπορεί να παρέχουν πληροφορίες σχετικά με τον τρόπο χρησιμοποίησης των λειτουργικών απαιτήσεων των κοινών κριτηρίων που αναφέρονται στο άρθρο 3 για την κατανόηση του στόχου ασφάλειας·

   ζ) ο συνοπτικός προσδιορισμός του στόχου αξιολόγησης περιλαμβάνει κάθε λειτουργία ασφάλειας του στόχου αξιολόγησης, αλλά πρόσθετες ιδιοταγείς πληροφορίες μπορούν να απαλειφθούν·

   η) περιλαμβάνονται παραπομπές σε χαρακτηριστικά προστασίας που εφαρμόζονται στον στόχο αξιολόγησης·

   θ) από τη συλλογιστική μπορούν να απαλειφθούν ιδιοταγείς πληροφορίες.

4. Ακόμη και αν ο στόχος ασφάλειας μετά την απαλοιφή εμπιστευτικών στοιχείων δεν αξιολογηθεί τυπικά σύμφωνα με τα πρότυπα αξιολόγησης που αναφέρονται στο άρθρο 3, ο οργανισμός πιστοποίησης διασφαλίζει ότι συμμορφώνεται με τον πλήρη και αξιολογημένο στόχο ασφάλειας, στη δε έκθεση πιστοποίησης γίνεται παραπομπή τόσο στον πλήρη στόχο ασφάλειας όσο και στον στόχο ασφάλειας μετά την απαλοιφή εμπιστευτικών στοιχείων.

ΠΑΡΑΡΤΗΜΑ VI

ΠΕΔΙΟ ΚΑΙ ΣΥΝΘΕΣΗ ΤΗΣ ΟΜΑΔΑΣ ΑΞΙΟΛΟΓΗΣΕΩΝ ΑΠΟ ΟΜΟΤΙΜΟΥΣ

VI.1 **Πεδίο της αξιολόγησης από ομοτίμους**

1. Καλύπτονται οι ακόλουθοι τύποι αξιολογήσεων από ομοτίμους:

   α) τύπος 1: ο οργανισμός πιστοποίησης εκτελεί δραστηριότητες πιστοποίησης σε επίπεδο AVA_VAN.3·

   β) τύπος 2: ο οργανισμός πιστοποίησης εκτελεί δραστηριότητες πιστοποίησης οι οποίες σχετίζονται με τεχνικό τομέα που παρατίθεται στα έγγραφα στάθμης της τεχνικής του παραρτήματος Ι·

   γ) τύπος 3: ο οργανισμός πιστοποίησης εκτελεί δραστηριότητες πιστοποίησης άνω του επιπέδου AVA_VAN.3 κάνοντας χρήση χαρακτηριστικού προστασίας που παρατίθεται στα έγγραφα στάθμης της τεχνικής του παραρτήματος Ι.

2. Ο οργανισμός πιστοποίησης που υποβάλλεται σε αξιολόγηση από ομοτίμους υποβάλλει τον κατάλογο πιστοποιημένων προϊόντων ΤΠΕ που μπορεί να είναι υποψήφια για επανεξέταση από την ομάδα αξιολογήσεων από ομοτίμους, σύμφωνα με τους ακόλουθους κανόνες:

   α) τα υποψήφια προϊόντα καλύπτουν το τεχνικό πεδίο της εξουσιοδότησης του οργανισμού πιστοποίησης, από το οποίο θα αναλυθούν τουλάχιστον δύο διαφορετικές αξιολογήσεις προϊόντων σε «υψηλό» επίπεδο διασφάλισης μέσω της αξιολόγησης από ομοτίμους καθώς και ένα χαρακτηριστικό προστασίας, εάν ο οργανισμός πιστοποίησης εξέδωσε πιστοποιητικό «υψηλού» επιπέδου διασφάλισης·

   β) για αξιολόγηση από ομοτίμους τύπου 2, ο οργανισμός πιστοποίησης υποβάλλει τουλάχιστον ένα προϊόν ανά τεχνικό τομέα και ανά ενδιαφερόμενη ΕΑΑΤΠ·

   γ) για αξιολόγηση από ομοτίμους τύπου 3, τουλάχιστον ένα υποψήφιο προϊόν αξιολογείται σύμφωνα με εφαρμοστέα και σχετικά χαρακτηριστικά προστασίας.

VI.2 **Ομάδα αξιολόγησης από ομοτίμους**

1. Η ομάδα αξιολόγησης απαρτίζεται από τουλάχιστον δύο εμπειρογνώμονες οι οποίοι επιλέγονται καθένας από διαφορετικό οργανισμό πιστοποίησης, από διαφορετικά κράτη μέλη, ο οποίος εκδίδει πιστοποιητικά «υψηλού» επιπέδου διασφάλισης. Οι εμπειρογνώμονες θα πρέπει να καταδεικνύουν τη σχετική εμπειρογνωσία στα πρότυπα που αναφέρονται στο άρθρο 3 και στα έγγραφα στάθμης της τεχνικής που εμπίπτουν στο πεδίο της αξιολόγησης από ομοτίμους.

2. Σε περίπτωση ανάθεσης της έκδοσης πιστοποιητικού ή προηγούμενης έγκρισης πιστοποιητικών όπως αναφέρεται στο άρθρο 56 παράγραφος 6 του κανονισμού (ΕΕ) 2019/881, εμπειρογνώμονας της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας που σχετίζεται με τον οικείο οργανισμό πιστοποίησης μπορεί να συμμετέχει επιπλέον στην ομάδα εμπειρογνωμόνων που επιλέγεται σύμφωνα με το σημείο 1 του παρόντος τμήματος.

3. Για αξιολόγηση από ομοτίμους τύπου 2, τα μέλη της ομάδας επιλέγονται από οργανισμούς πιστοποίησης εξουσιοδοτημένους για τον οικείο τεχνικό τομέα.

4. Κάθε μέλος της ομάδας αξιολόγησης έχει πείρα τουλάχιστον δύο ετών στην εκτέλεση δραστηριοτήτων πιστοποίησης σε οργανισμό πιστοποίησης.

5. Για αξιολόγηση από ομοτίμους τύπου 2 ή 3, κάθε μέλος της ομάδας αξιολόγησης έχει πείρα τουλάχιστον δύο ετών στην εκτέλεση δραστηριοτήτων πιστοποίησης στον σχετικό τεχνικό τομέα ή χαρακτηριστικό προστασίας και αποδεδειγμένη εμπειρογνωσία και συμμετοχή στην εξουσιοδότηση ΕΑΑΤΠ.

6. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας η οποία παρακολουθεί και εποπτεύει τον αξιολογούμενο από ομοτίμους οργανισμό πιστοποίησης, καθώς και τουλάχιστον μία εθνική αρχή πιστοποίησης της κυβερνοασφάλειας, ο οργανισμός πιστοποίησης της οποίας δεν υπόκειται στην αξιολόγηση από ομοτίμους, συμμετέχουν στην αξιολόγηση από ομοτίμους ως παρατηρητές. Ο ENISA δύναται επίσης να συμμετέχει στην αξιολόγηση από ομοτίμους ως παρατηρητής.

7. Ο αξιολογούμενος από ομοτίμους οργανισμός πιστοποίησης ενημερώνεται για τη σύνθεση της ομάδας ομοτίμων. Σε αιτιολογημένες περιπτώσεις, μπορεί να αμφισβητήσει τη σύνθεση της ομάδας αξιολόγησης και να ζητήσει την επανεξέτασή της.

ΠΑΡΑΡΤΗΜΑ VII

Περιεχόμενο πιστοποιητικού EUCC

Το πιστοποιητικό EUCC περιέχει τουλάχιστον:

α) μοναδικό αναγνωριστικό το οποίο θεσπίζεται από τον οργανισμό πιστοποίησης που εκδίδει το πιστοποιητικό·

β) πληροφορίες σχετικά με το πιστοποιημένο προϊόν ΤΠΕ ή το χαρακτηριστικό προστασίας και τον κάτοχο του πιστοποιητικού, συμπεριλαμβανομένων των εξής:

1) επωνυμία του προϊόντος ΤΠΕ ή του χαρακτηριστικού προστασίας και, κατά περίπτωση, του στόχου αξιολόγησης·

2) τύπος προϊόντος ΤΠΕ ή του χαρακτηριστικού προστασίας και, κατά περίπτωση, του στόχου αξιολόγησης·

3) έκδοση του προϊόντος ΤΠΕ ή του χαρακτηριστικού προστασίας·

4) όνομα, διεύθυνση και στοιχεία επικοινωνίας του κατόχου του πιστοποιητικού·

5) σύνδεσμος προς τον ιστότοπο του κατόχου του πιστοποιητικού ο οποίος περιέχει τις συμπληρωματικές πληροφορίες σχετικά με την κυβερνοασφάλεια που αναφέρονται στο άρθρο 55 του κανονισμού (ΕΕ) 2019/881·

γ) πληροφορίες σχετικά με την αξιολόγηση και την πιστοποίηση του προϊόντος ΤΠΕ ή του χαρακτηριστικού προστασίας, συμπεριλαμβανομένων των εξής:

1) όνομα, διεύθυνση και στοιχεία επικοινωνίας του οργανισμού πιστοποίησης που εξέδωσε το πιστοποιητικό·

2) σε περίπτωση που η αξιολόγηση δεν διενεργήθηκε από τον οργανισμό πιστοποίησης, επωνυμία της ΕΑΑΤΠ που διενήργησε την αξιολόγηση·

3) επωνυμία της αρμόδιας εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας·

4) παραπομπή στον παρόντα κανονισμό·

5) παραπομπή στην έκθεση πιστοποίησης που σχετίζεται με το πιστοποιητικό που αναφέρεται στο παράρτημα ΙΙΙ·

6) το εφαρμοστέο επίπεδο διασφάλισης σύμφωνα με το άρθρο 4·

7) παραπομπή στην έκδοση των προτύπων που χρησιμοποιήθηκαν για την αξιολόγηση, τα οποία αναφέρονται στο άρθρο 3·

8) προσδιορισμός του επιπέδου διασφάλισης ή της δέσμης απαιτήσεων κατοχύρωσης της ασφάλειας που προσδιορίζονται στα πρότυπα που αναφέρονται στο άρθρο 3 και σύμφωνα με το παράρτημα VI, συμπεριλαμβανομένων των συνιστωσών διασφάλισης που χρησιμοποιήθηκαν και του καλυπτόμενου επιπέδου AVA_VAN·

9) όπου συντρέχει περίπτωση, παραπομπή σε ένα ή περισσότερα χαρακτηριστικά προστασίας με τα οποία συμμορφώνεται το προϊόν ΤΠΕ ή το χαρακτηριστικό προστασίας·

10) ημερομηνία έκδοσης·

11) περίοδος ισχύος του πιστοποιητικού·

δ) το σήμα και η επισήμανση που σχετίζονται με το πιστοποιητικό σύμφωνα με το άρθρο 11.

ΠΑΡΑΡΤΗΜΑ VIII

Δήλωση δέσμης απαιτήσεων κατοχύρωσης της ασφάλειας

1. Αντίθετα προς τους ορισμούς που περιέχονται στα κοινά κριτήρια, η επαύξηση:

α) δεν υποδηλώνεται με το σύμβολο «+»·

β) περιγράφεται αναλυτικά με κατάλογο όλων των σχετικών συνιστωσών·

γ) περιγράφεται λεπτομερώς στην έκθεση πιστοποίησης.

2. Το επίπεδο διασφάλισης που επιβεβαιώνεται σε πιστοποιητικό EUCC μπορεί να συμπληρώνεται με το επίπεδο διασφάλισης της αξιολόγησης όπως προσδιορίζεται στο άρθρο 3 του παρόντος κανονισμού.

3. Εάν το επίπεδο διασφάλισης που επιβεβαιώνεται σε πιστοποιητικό EUCC δεν παραπέμπει σε επαύξηση, το πιστοποιητικό EUCC αναφέρει μια από τις ακόλουθες δέσμες απαιτήσεων κατοχύρωσης της ασφάλειας:

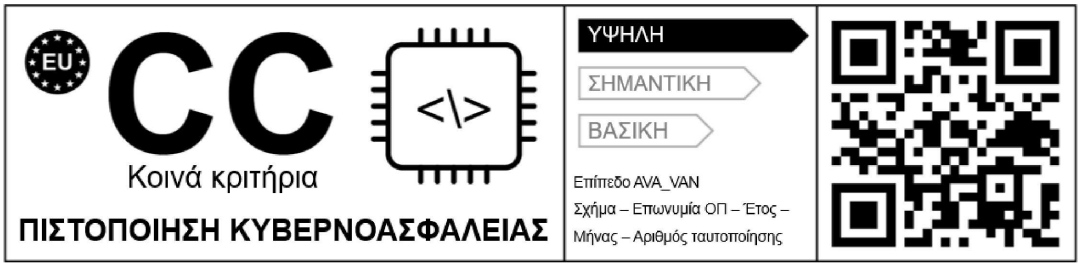
α) «τη συγκεκριμένη δέσμη απαιτήσεων κατοχύρωσης της ασφάλειας»·

β) «τη δέσμη απαιτήσεων κατοχύρωσης της ασφάλειας που είναι σύμφωνη με χαρακτηριστικό προστασίας» σε περίπτωση παραπομπής σε χαρακτηριστικό προστασίας χωρίς επίπεδο διασφάλισης της αξιολόγησης.

ΠΑΡΑΡΤΗΜΑ IX

Σήματα και επισημάνσεις

1. Η μορφή του σήματος και της επισήμανσης:



2. Εάν το σήμα και η επισήμανση σμικρυνθούν ή μεγεθυνθούν, πρέπει να τηρούνται οι αναλογίες του σχεδίου ανωτέρω.

3. Όταν τοποθετούνται επί του προϊόντος ΤΠΕ, το σήμα και η επισήμανση έχουν ύψος τουλάχιστον 5 χιλιοστών.