Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2025/2392

1.12.2025

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2025/2392 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 28ης Νοεμβρίου 2025

σχετικά με την τεχνική περιγραφή των κατηγοριών σημαντικών και κρίσιμων προϊόντων με ψηφιακά στοιχεία σύμφωνα με τον κανονισμό (ΕΕ) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

(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) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2024, σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 168/2013 και (ΕΕ) 2019/1020 και της οδηγίας (ΕΕ) 2020/1828 (κανονισμός για την κυβερνοανθεκτικότητα) ([1]), και ιδίως το άρθρο 7 παράγραφος 4,

Εκτιμώντας τα ακόλουθα:

(1) Ο κανονισμός (ΕΕ) 2024/2847 καθορίζει κανόνες κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία. Ειδικότερα, το παράρτημα ΙΙΙ του εν λόγω κανονισμού καθορίζει κατηγορίες σημαντικών προϊόντων με ψηφιακά στοιχεία τα οποία, όταν διατίθενται στην αγορά, υπόκεινται σε διαδικασίες αξιολόγησης της συμμόρφωσης αυστηρότερες από εκείνες που ισχύουν για άλλα προϊόντα με ψηφιακά στοιχεία. Το παράρτημα IV του κανονισμού (ΕΕ) 2024/2847 καθορίζει κατηγορίες κρίσιμων προϊόντων με ψηφιακά στοιχεία για τα οποία οι κατασκευαστές θα μπορούσαν να υποχρεωθούν να λάβουν ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας στο πλαίσιο ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2]) ή τα οποία θα υπόκεινται σε υποχρεωτική αξιολόγηση της συμμόρφωσης από τρίτους, όταν διατίθενται στην αγορά.

(2) Σύμφωνα με το άρθρο 7 παράγραφος 1 και το άρθρο 8 παράγραφος 1 του κανονισμού (ΕΕ) 2024/2847, η βασική λειτουργικότητα ενός προϊόντος με ψηφιακά στοιχεία καθορίζει αν το εν λόγω προϊόν με ψηφιακά στοιχεία πληροί την τεχνική περιγραφή μιας κατηγορίας σημαντικών ή κρίσιμων προϊόντων με ψηφιακά στοιχεία και, ως εκ τούτου, τις εφαρμοστέες διαδικασίες αξιολόγησης της συμμόρφωσης.

(3) Κατά την ανάπτυξη ενός προϊόντος με ψηφιακά στοιχεία, και προκειμένου να επιτευχθεί το επιθυμητό σύνολο λειτουργιών του, οι κατασκευαστές ενσωματώνουν συνήθως στα δικά τους προϊόντα με ψηφιακά στοιχεία άλλα κατασκευαστικά στοιχεία τα οποία είναι επίσης προϊόντα με ψηφιακά στοιχεία και τα οποία μπορούν να πληρούν την τεχνική περιγραφή μιας κατηγορίας σημαντικών ή κρίσιμων προϊόντων. Σύμφωνα με τον κανονισμό (ΕΕ) 2024/2847, ένα προϊόν με ψηφιακά στοιχεία υπόκειται στις διαδικασίες αξιολόγησης της συμμόρφωσης που εφαρμόζονται σε σημαντικά ή κρίσιμα προϊόντα με ψηφιακά στοιχεία, αν το εν λόγω προϊόν στο σύνολό του είναι σημαντικό ή κρίσιμο προϊόν, όπως ορίζεται στα παραρτήματα ΙΙΙ και IV του εν λόγω κανονισμού. Για παράδειγμα, η ενσωμάτωση ενός ενσωματωμένου προγράμματος περιήγησης ως στοιχείου μιας εφαρμογής ειδήσεων για χρήση σε έξυπνα τηλέφωνα δεν καθιστά από μόνη της την εφαρμογή ειδήσεων υποκείμενη στη διαδικασία αξιολόγησης της συμμόρφωσης που εφαρμόζεται σε προϊόντα με ψηφιακά στοιχεία που έχουν τη βασική λειτουργία «αυτόνομων και ενσωματωμένων προγραμμάτων περιήγησης». Ωστόσο, σύμφωνα με τον κανονισμό (ΕΕ) 2024/2847, ο κατασκευαστής πρέπει να διασφαλίζει ότι το προϊόν με ψηφιακά στοιχεία πληροί στο σύνολό του τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας. Ως εκ τούτου, ο κατασκευαστής πρέπει να αξιολογήσει την ασφάλεια ολόκληρου του προϊόντος, λαμβάνοντας υπόψη, κατά περίπτωση, την ασφάλεια των κατασκευαστικών στοιχείων ή των λειτουργιών που είναι ενσωματωμένες σε αυτό. Για παράδειγμα, προκειμένου ο κατασκευαστής μιας εφαρμογής ειδήσεων να αποδείξει ότι το προϊόν του με ψηφιακά στοιχεία συμμορφώνεται με τον κανονισμό (ΕΕ) 2024/2847, ο εν λόγω κατασκευαστής πρέπει να αποδείξει ότι η εφαρμογή ειδήσεων στο σύνολό της πληροί τις εφαρμοστέες απαιτήσεις, λαμβάνοντας υπόψη, κατά περίπτωση, την ασφάλεια του προγράμματος περιήγησης που είναι ενσωματωμένο στην εφαρμογή του.

([1]) ΕΕ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) Κανονισμός (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) (ΕΕ L 151 της 7.6.2019, σ. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Το γεγονός ότι ένα προϊόν με ψηφιακά στοιχεία εκτελεί λειτουργίες διαφορετικές ή επιπρόσθετες εκείνων που περιγράφονται λεπτομερώς στις τεχνικές περιγραφές που ορίζονται στον παρόντα κανονισμό δεν σημαίνει αφ' εαυτού ότι το προϊόν με ψηφιακά στοιχεία δεν διαθέτει τη βασική λειτουργικότητα κατηγορίας προϊόντων που ορίζεται στα παραρτήματα III και IV του κανονισμού (ΕΕ) 2024/2847. Για παράδειγμα, τα προϊόντα με ψηφιακά στοιχεία που έχουν τη βασική λειτουργικότητα των «λειτουργικών συστημάτων» περιλαμβάνουν συχνά λογισμικό που εκτελεί βοηθητικές λειτουργίες που δεν περιλαμβάνονται στην τεχνική περιγραφή της εν λόγω κατηγορίας προϊόντων, όπως αριθμομηχανές ή απλά προγράμματα επεξεργασίας γραφικών. Τα προϊόντα με ψηφιακά στοιχεία συχνά ενσωματώνουν επίσης κατασκευαστικά στοιχεία που έχουν τη λειτουργικότητα άλλου σημαντικού ή κρίσιμου προϊόντος με ψηφιακά στοιχεία, όπως είναι ένα λειτουργικό σύστημα που ενσωματώνει λειτουργικότητα προγράμματος περιήγησης ή ένας δρομολογητής που ενσωματώνει λειτουργικότητα τείχους προστασίας. Τούτο, ωστόσο, δεν σημαίνει από μόνο του ότι τα εν λόγω προϊόντα με ψηφιακά στοιχεία δεν έχουν τη βασική λειτουργικότητα των «λειτουργικών συστημάτων» ή των «δρομολογητών, μόντεμ που προορίζονται για τη σύνδεση με το διαδίκτυο και διακοπτών», αντίστοιχα.

(5) Από την άλλη πλευρά, ένα προϊόν με ψηφιακά στοιχεία που έχει την ικανότητα να εκτελεί τις λειτουργίες μιας κατηγορίας προϊόντων που ορίζεται στα παραρτήματα III και IV του κανονισμού (ΕΕ) 2024/2847, αλλά του οποίου η βασική λειτουργικότητα είναι διαφορετική από εκείνη της εν λόγω κατηγορίας προϊόντων, δεν πρέπει να θεωρείται ότι πληροί την τεχνική περιγραφή της εν λόγω κατηγορίας προϊόντων. Για παράδειγμα, ένα λογισμικό ενορχήστρωσης, αυτοματοποίησης και απόκρισης ασφαλείας (SOAR) έχει συχνά την ικανότητα να εκτελεί τις λειτουργίες προϊόντων με ψηφιακά στοιχεία στην κατηγορία των «συστημάτων διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM)», δηλαδή να συλλέγει δεδομένα, να τα αναλύει και να τα παρουσιάζει ως αξιοποιήσιμες πληροφορίες για σκοπούς ασφαλείας. Ωστόσο, δεδομένου ότι η βασική λειτουργία του δεν είναι η λειτουργία SIEM, το λογισμικό SOAR δεν πρέπει γενικά να θεωρείται ότι πληροί την τεχνική περιγραφή των «συστημάτων διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM)». Ομοίως, ένα έξυπνο τηλέφωνο ενσωματώνει συνήθως κατασκευαστικά στοιχεία που εκτελούν τις λειτουργίες διαφόρων κατηγοριών προϊόντων που ορίζονται στα παραρτήματα III και IV του κανονισμού (ΕΕ) 2024/2847, π.χ. λειτουργικό σύστημα ή ενσωματωμένο διαχειριστή κωδικών πρόσβασης. Ωστόσο, δεδομένου ότι η βασική λειτουργία ενός έξυπνου τηλεφώνου δεν είναι αυτή ενός λειτουργικού συστήματος ή ενός διαχειριστή κωδικών πρόσβασης, δεν πρέπει γενικά να θεωρείται ότι πληροί την τεχνική περιγραφή των εν λόγω κατηγοριών προϊόντων.

(6) Σύμφωνα με το άρθρο 13 παράγραφοι 2 και 3 του κανονισμού (ΕΕ) 2024/2847, οι κατασκευαστές προϊόντων με ψηφιακά στοιχεία πρέπει να εφαρμόζουν τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στο παράρτημα I μέρος I του κανονισμού (ΕΕ) 2024/2847 κατά τρόπο αναλογικό προς τους κινδύνους του προϊόντος με ψηφιακά στοιχεία, με βάση τον επιδιωκόμενο σκοπό και την ευλόγως προβλέψιμη χρήση, καθώς και τους όρους χρήσης του προϊόντος με ψηφιακά στοιχεία, λαμβανομένου υπόψη του χρονικού διαστήματος κατά το οποίο αναμένεται να χρησιμοποιηθεί το προϊόν. Σύμφωνα με το άρθρο 13 παράγραφοι 2 και 3 του εν λόγω κανονισμού και ανεξάρτητα από το αν το προϊόν με ψηφιακά στοιχεία θεωρείται σημαντικό ή κρίσιμο προϊόν με ψηφιακά στοιχεία, οι κατασκευαστές πρέπει να διενεργούν ολοκληρωμένη εκτίμηση κινδύνων κυβερνοασφάλειας και να αναφέρουν πώς εφαρμόζονται οι ουσιώδεις απαιτήσεις κυβερνοασφάλειας, όπως τεκμηριώνεται από την εκτίμηση κινδύνου, συμπεριλαμβανομένων των δοκιμών και της διασφάλισης τους. Όταν η βασική λειτουργικότητα του προϊόντος τους με ψηφιακά στοιχεία πληροί την τεχνική περιγραφή σημαντικού ή κρίσιμου προϊόντος με ψηφιακά στοιχεία, οι κατασκευαστές πρέπει να αποδεικνύουν τη συμμόρφωση σύμφωνα με τις ειδικές διαδικασίες αξιολόγησης της συμμόρφωσης που θεσπίζονται με το άρθρο 32 παράγραφοι 2, 3, 4 και 5 του κανονισμού (ΕΕ) 2024/2847.

(7) Ο παρών κανονισμός περιλαμβάνει παραδείγματα προϊόντων με ψηφιακά στοιχεία των οποίων η βασική λειτουργικότητα πληροί την τεχνική περιγραφή ορισμένων σημαντικών ή κρίσιμων προϊόντων με ψηφιακά στοιχεία. Τα παραδείγματα αυτά δίδονται μόνο για ενδεικτικούς σκοπούς και δεν αποτελούν εξαντλητικό κατάλογο.

(8) Προκειμένου να παρέχεται ασφάλεια δικαίου στους κατασκευαστές, οι κατηγορίες προϊόντων με ψηφιακά στοιχεία που είναι μικροεπεξεργαστές ανθεκτικοί στην παραποίηση, μικροελεγκτές ανθεκτικοί στην παραποίηση, και έξυπνες κάρτες και παρόμοιες συσκευές, συμπεριλαμβανομένων των ασφαλών στοιχείων, θα πρέπει να διακρίνονται με βάση το επίπεδο αντοχής σε πιθανές εκμεταλλεύσιμες ευπάθειες ή ελαττώματα ή αδυναμίες για το οποίο έχουν σχεδιαστεί. Το επίπεδο AVA_VAN είναι ένας ευρέως χρησιμοποιούμενος και τυποποιημένος τρόπος με τον οποίο εκφράζεται αυτό το επίπεδο αντοχής. Τα επίπεδα AVA_VAN καθορίζονται στα δημοσίως διαθέσιμα πρότυπα των κοινών κριτηρίων και της κοινής μεθοδολογίας αξιολόγησης, στα οποία βασίζονται τα υφιστάμενα πλαίσια πιστοποίησης που έχουν υιοθετηθεί ευρέως στην αγορά, όπως ο εκτελεστικός κανονισμός (ΕΕ) 2024/482 της Επιτροπής ([3]). Ο εκτελεστικός κανονισμός (ΕΕ) 2024/482 θεσπίζει ευρωπαϊκό

([3]) Εκτελεστικός κανονισμός (ΕΕ) 2024/482 της Επιτροπής, 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) (ΕΕ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

σχήμα πιστοποίησης της κυβερνοασφάλειας που μπορεί να χρησιμοποιηθεί για την πιστοποίηση ενός προϊόντος σε συγκεκριμένο επίπεδο διασφάλισης. Με βάση τις παγκόσμιες πρακτικές, ο εκτελεστικός κανονισμός (ΕΕ) 2024/482 προβλέπει τη δυνατότητα έκδοσης πιστοποιητικών με βάση παλαιότερες εκδόσεις των προτύπων έως το τέλος του 2027. Ως εκ τούτου, στο πλαίσιο του κανονισμού (ΕΕ) 2024/2847, είναι σκόπιμο να επιτραπεί να εκφράζονται τα επίπεδα AVA_VAN με αναφορά είτε στην πλέον πρόσφατη έκδοση είτε σε παλαιότερες εκδόσεις των εν λόγω προτύπων.

(9) Τα μέτρα που προβλέπονται στον παρόντα κανονισμό είναι σύμφωνα με τη γνώμη της επιτροπής που έχει συσταθεί βάσει του άρθρου 62 παράγραφος 1 του κανονισμού (ΕΕ) 2024/2847,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

Ορισμοί

Για τους σκοπούς του παρόντος κανονισμού ισχύουν οι ακόλουθοι ορισμοί:

1) «κοινά κριτήρια»: τα κοινά κριτήρια για την αξιολόγηση της ασφάλειας της τεχνολογίας των πληροφοριών, όπως ορίζονται στο άρθρο 2 παράγραφος 1 του εκτελεστικού κανονισμού (ΕΕ) 2024/482 ή όπως καθορίζονται στα πρότυπα που αναφέρονται στο άρθρο 3 παράγραφος 2 στοιχεία α) και β) του εν λόγω εκτελεστικού κανονισμού·

2) «κοινή μεθοδολογία αξιολόγησης»: η κοινή μεθοδολογία για την αξιολόγηση της ασφάλειας της τεχνολογίας των πληροφοριών, όπως ορίζεται στο άρθρο 2 παράγραφος 2 του εκτελεστικού κανονισμού (ΕΕ) 2024/482 ή όπως ορίζεται στα πρότυπα που αναφέρονται στο άρθρο 3 παράγραφος 2 στοιχεία γ) και δ) του εν λόγω εκτελεστικού κανονισμού.

Άρθρο 2

1. Η τεχνική περιγραφή των κατηγοριών προϊόντων με ψηφιακά στοιχεία των κλάσεων I και II που απαριθμούνται στο παράρτημα III του κανονισμού (ΕΕ) 2024/2847 καθορίζεται στο παράρτημα I του παρόντος κανονισμού.

2. Η τεχνική περιγραφή των κατηγοριών προϊόντων με ψηφιακά στοιχεία που απαριθμούνται στο παράρτημα IV του κανονισμού (ΕΕ) 2024/2847 καθορίζεται στο παράρτημα II του παρόντος κανονισμού.

Άρθρο 3

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

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

Βρυξέλλες, 28 Νοεμβρίου 2025.

Για την Επιτροπή
Η Πρόεδρος
Ursula VON DER LEYEN

ΠΑΡΑΡΤΗΜΑ I

ΣΗΜΑΝΤΙΚΑ ΠΡΟΪΟΝΤΑ ΜΕ ΨΗΦΙΑΚΑ ΣΤΟΙΧΕΙΑ

Κλάση I

Κατηγορία προϊόντων	Τεχνική περιγραφή
1. Λογισμικό και υλισμικό συστημάτων διαχείρισης ταυτότητας και διαχείρισης προνομιακής πρόσβασης, συμπεριλαμβανομένων συσκευών ανάγνωσης επαλήθευσης ταυτότητας και ελέγχου πρόσβασης, μεταξύ των οποίων συσκευές ανάγνωσης βιομετρικών δεδομένων	Τα συστήματα διαχείρισης ταυτότητας είναι προϊόντα με ψηφιακά στοιχεία που παρέχουν μηχανισμούς επαλήθευσης ταυτότητας ή εξουσιοδότησης και που μπορούν επίσης να παρέχουν μηχανισμούς για τη διαχείριση του κύκλου ζωής των διαπιστευτηρίων ταυτότητας φυσικών προσώπων, νομικών προσώπων, συσκευών ή συστημάτων, π.χ. καταχώριση ταυτότητας, καθώς και παροχή, συντήρηση και διαγραφή ταυτότητας από το μητρώο. Τα συστήματα αυτά περιλαμβάνουν συστήματα διαχείρισης πρόσβασης που ελέγχουν την πρόσβαση φυσικών προσώπων, νομικών προσώπων, συσκευών ή συστημάτων σε ψηφιακούς πόρους ή φυσικές τοποθεσίες. Το λογισμικό διαχείρισης προνομιακής πρόσβασης είναι ένα σύστημα διαχείρισης πρόσβασης που ελέγχει και παρακολουθεί τα δικαιώματα πρόσβασης σε συστήματα πληροφορικής ή λειτουργικής τεχνολογίας και σε ευαίσθητες πληροφορίες εντός ενός οργανισμού, συμπεριλαμβανομένων συστημάτων που επιβάλλουν πολιτικές ελέγχου διαφοροποιημένης πρόσβασης για προνομιούχους χρήστες. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, συσκευές επαλήθευσης ταυτότητας και ελέγχου πρόσβασης, συσκευές ανάγνωσης βιομετρικών δεδομένων, λογισμικό ενιαίας σύνδεσης, λογισμικό συνενωμένης διαχείρισης ταυτότητας, λογισμικό κωδικού πρόσβασης μίας χρήσης, συσκευές επαλήθευσης ταυτότητας υλισμικού, όπως γεννήτριες αριθμών ταυτοποίησης συναλλαγής (TAN), λογισμικό επαλήθευσης ταυτότητας και λογισμικό πολυπαραγοντικής επαλήθευσης ταυτότητας.
2. Αυτόνομα και ενσωματωμένα προγράμματα περιήγησης	Προϊόντα λογισμικού με ψηφιακά στοιχεία που επιτρέπουν στους τελικούς χρήστες να έχουν πρόσβαση, να παράγουν και να αλληλεπιδρούν με διαδικτυακό περιεχόμενο και υπηρεσίες που φιλοξενούνται σε διακομιστές που είναι συνδεδεμένοι με δίκτυα όπως το διαδίκτυο. Περιλαμβάνουν συνήθως μια μηχανή προγράμματος περιήγησης για την ερμηνεία και την εμφάνιση περιεχομένου γραμμένου σε γλώσσα σήμανσης (π.χ. HTML), την υποστήριξη διαδικτυακών πρωτοκόλλων (π.χ. HTTP, HTTPS), την ικανότητα εκτέλεσης σεναρίων και διαχείρισης εισροών χρήστη, καθώς και την αποθήκευση προσωρινών ή μόνιμων δεδομένων από ιστοτόπους (cookies). Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, αυτοτελείς εφαρμογές που πληρούν τις λειτουργίες των προγραμμάτων περιήγησης, ενσωματωμένα προγράμματα περιήγησης που προορίζονται για ενσωμάτωση σε άλλο σύστημα ή εφαρμογή, καθώς και προγράμματα περιήγησης με ενσωμάτωση παράγοντα TN.
3. Διαχειριστές κωδικών πρόσβασης	Προϊόντα με ψηφιακά στοιχεία που αποθηκεύουν κωδικούς πρόσβασης, τοπικά σε συσκευή ή σε απομακρυσμένο διακομιστή, συμπεριλαμβανομένων δραστηριοτήτων όπως η δημιουργία κωδικών πρόσβασης, καθώς και η κοινοχρησία κωδικών πρόσβασης και η ενσωμάτωση σε τοπικές εφαρμογές ή εφαρμογές τρίτων για τη χρήση κωδικών πρόσβασης. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, τοπικούς διαχειριστές κωδικών πρόσβασης, διαχειριστές κωδικών πρόσβασης που παρέχονται ως επεκτάσεις προγραμμάτων περιήγησης, διαχειριστές κωδικών πρόσβασης επιχειρήσεων, καθώς και διαχειριστές κωδικών πρόσβασης βάσει υλισμικού.

Κατηγορία προϊόντων	Τεχνική περιγραφή
4. Λογισμικό που αναζητεί, αφαιρεί ή θέτει σε καραντίνα κακόβουλο λογισμικό	Προϊόντα λογισμικού με ψηφιακά στοιχεία, τα οποία συνήθως αναφέρονται ως αντιιικό λογισμικό (antivirus) ή μέσο αντιμετώπισης κακόβουλου λογισμικού (antimalware), τα οποία εντοπίζουν ή αναζητούν κακόβουλο λογισμικό ή κώδικα σε συσκευές ή αφαιρούν ή θέτουν σε καραντίνα το εν λόγω λογισμικό ή τον εν λόγω κώδικα, προκειμένου να διατηρηθεί η ακεραιότητα, η εμπιστευτικότητα ή η διαθεσιμότητα των εν λόγω συσκευών. Στο πλαίσιο αυτής της κατηγορίας προϊόντων, ως κακόβουλο λογισμικό νοείται το λογισμικό που περιέχει κακόβουλα χαρακτηριστικά ή ικανότητες που μπορούν να προκαλέσουν άμεση ή έμμεση βλάβη στον χρήστη και/ή στο σύστημα υπολογιστών, π.χ. ιούς, λογισμικά σκουλήκια, λυτρισμικό, κατασκοπευτικό λογισμικό και δούρειους ίππους. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, λογισμικό που ανιχνεύει ή αναζητεί κακόβουλο λογισμικό σε πραγματικό χρόνο ή χειροκίνητα, ανίχνευση rootkit και δίσκους διάσωσης με τη βασική λειτουργία της αναζήτησης, αφαίρεσης ή θέσης σε καραντίνα κακόβουλου λογισμικού.
5. Προϊόντα με ψηφιακά στοιχεία με τη λειτουργία εικονικού ιδιωτικού δικτύου (VPN)	Προϊόντα με ψηφιακά στοιχεία που δημιουργούν κρυπτογραφημένη λογική σήραγγα η οποία δημιουργείται από τους πόρους του συστήματος ενός φυσικού ή εικονικού δικτύου. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, προγράμματα-πελάτες εικονικού ιδιωτικού δικτύου, διακομιστές εικονικού ιδιωτικού δικτύου και πύλες εικονικού ιδιωτικού δικτύου.
6. Συστήματα διαχείρισης δικτύου	Προϊόντα με ψηφιακά στοιχεία που διαχειρίζονται συνδεδεμένα στοιχεία δικτύου, π.χ. διακομιστές, δρομολογητές, διακόπτες, σταθμούς εργασίας, εκτυπωτές ή κινητές συσκευές, παρακολουθώντας τα και ελέγχοντας τις λειτουργίες και τη διαμόρφωση του δικτύου τους. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, διατερματικά συστήματα διαχείρισης και ειδικά συστήματα διαχείρισης διαμόρφωσης, π.χ. ελεγκτές για δικτύωση βάσει λογισμικού.
7. Συστήματα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM)	Προϊόντα με ψηφιακά στοιχεία που συλλέγουν δεδομένα από πολλαπλές πηγές, τα αναλύουν, τα συσχετίζουν και τα παρουσιάζουν ως αξιοποιήσιμες πληροφορίες για σκοπούς που σχετίζονται με την ασφάλεια, όπως είναι ο εντοπισμός απειλών και συμβάντων, η εγκληματολογική ανάλυση ή οι σκοποί συμμόρφωσης.
8. Συστήματα διαχείρισης εκκίνησης	Προϊόντα λογισμικού με ψηφιακά στοιχεία που διαχειρίζονται τη διαδικασία αρχικής εκκίνησης συστήματος μετά την ενεργοποίηση/επανεκκίνηση με την αρχικοποίηση υλισμικού, τη φόρτωση ή τη μεταφορά ελέγχου στο περιβάλλον ή τους πόρους του λειτουργικού συστήματος και την επιλογή τρόπου εκκίνησης. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, υλικολογισμικό UEFI, φορτωτές εκκίνησης ενός ή πολλαπλών σταδίων.
9. Λογισμικό έκδοσης υποδομών δημόσιου κλειδιού και ψηφιακών πιστοποιητικών	Προϊόντα με ψηφιακά στοιχεία που χρησιμοποιούνται στο πλαίσιο υποδομής δημόσιου κλειδιού (PKI) και τα οποία διαχειρίζονται την επικύρωση, τη δημιουργία, την έκδοση, τη διανομή, την κατάσταση δημοσίευσης, την ανανέωση ή την ανάκληση ψηφιακών πιστοποιητικών ή την παραγωγή, αποθήκευση, μεσεγγύηση, ανταλλαγή, καταστροφή ή εναλλαγή κρυπτογραφικών κλειδιών που συνδέονται με τα εν λόγω ψηφιακά πιστοποιητικά. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, τα συστήματα διαχείρισης κλειδιών, τα συστήματα διαχείρισης ψηφιακών πιστοποιητικών, τους αποκριτές ηλεκτρονικού πρωτοκόλλου κατάστασης πιστοποιητικού και τις λύσεις PKI «όλα σε ένα».

Κατηγορία προϊόντων	Τεχνική περιγραφή
10. Φυσικές και εικονικές διεπαφές δικτύου	Οι φυσικές διεπαφές δικτύου είναι προϊόντα με ψηφιακά στοιχεία τα οποία συνδέουν απευθείας μια συσκευή με ένα δίκτυο μέσω διεπαφής προγραμματισμού εφαρμογών (API) η οποία παρέχεται από τους οδηγούς διεπαφής, που συνήθως λειτουργούν στο επίπεδο ζεύξης δεδομένων, και διαθέτουν προσαρμογείς υλισμικού σε μέσα μετάδοσης με αντίστοιχο υλικολογισμικό, που συνήθως λειτουργούν στο φυσικό επίπεδο και στο επίπεδο ζεύξης δεδομένων. Οι εικονικές διεπαφές δικτύου είναι προϊόντα με ψηφιακά στοιχεία που συνδέουν άμεσα ή έμμεσα μια συσκευή με ένα δίκτυο μέσω API που αντιστοιχεί στη διεπαφή των οδηγών φυσικών διεπαφών δικτύου, που συνήθως λειτουργούν στο επίπεδο ζεύξης δεδομένων. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, ενσύρματες και ασύρματες κάρτες διεπαφής δικτύου, ελεγκτές και προσαρμογείς, π.χ. για Wi-Fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee ή Fieldbus, καθώς και αμιγώς εικονικά αυτόνομα προϊόντα, π.χ. κάρτες εικονικής διεπαφής δικτύου, διεπαφές δικτύου υπό μορφή περιέκτη και διεπαφές VPN.
11. Λειτουργικά συστήματα	Προϊόντα λογισμικού με ψηφιακά στοιχεία που παρέχουν αφαιρετική διεπαφή του υποκείμενου υλισμικού και ελέγχουν την εκτέλεση του λογισμικού και τα οποία μπορούν να παρέχουν υπηρεσίες όπως είναι η διαχείριση και διαμόρφωση υπολογιστικών πόρων, ο προγραμματισμός, ο έλεγχος εισροών-εκροών, η διαχείριση δεδομένων, ενώ παρέχουν διεπαφή μέσω της οποίας οι εφαρμογές αλληλεπιδρούν με πόρους και περιφερειακά του συστήματος. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, λειτουργικά συστήματα σε πραγματικό χρόνο, λειτουργικά συστήματα γενικής χρήσης και λειτουργικά συστήματα ειδικής χρήσης.
12. Δρομολογητές, μόντεμ που προορίζονται για σύνδεση στο διαδίκτυο, και διακόπτες	Οι δρομολογητές είναι προϊόντα με ψηφιακά στοιχεία που καθορίζουν και ελέγχουν τη ροή δεδομένων μεταξύ διαφορετικών δικτύων επιλέγοντας διαδρομές με τη χρήση μηχανισμών και αλγορίθμων πρωτοκόλλου δρομολόγησης, οι οποίοι συνήθως λειτουργούν στο επίπεδο δικτύου. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, ενσύρματους και ασύρματους δρομολογητές, εικονικούς δρομολογητές και δρομολογητές με ή χωρίς μόντεμ.
	Τα μόντεμ που προορίζονται για τη σύνδεση με το διαδίκτυο είναι προϊόντα υλισμικού με ψηφιακά στοιχεία που χρησιμοποιούν ψηφιακές τεχνικές διαμόρφωσης και αποδιαμόρφωσης για τη μετατροπή αναλογικών σημάτων σε ψηφιακά σήματα και αντιστρόφως για επικοινωνίες βάσει IP. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, μόντεμ οπτικών ινών, μόντεμ ψηφιακής συνδρομητικής γραμμής (DSL), καλωδιακά μόντεμ (DOCSIS), δορυφορικά μόντεμ και κυψελοειδή μόντεμ.
	Οι διακόπτες είναι προϊόντα με ψηφιακά στοιχεία που παρέχουν συνδεσιμότητα μεταξύ δικτυωμένων συσκευών μέσω μηχανισμών προώθησης πακέτων και διαθέτουν επίπεδο διαχείρισης, το οποίο συνήθως εφαρμόζεται στο επίπεδο ζεύξης δεδομένων ή στο επίπεδο δικτύου. Στην κατηγορία αυτή περιλαμβάνονται, μεταξύ άλλων, οι διαχειριζόμενοι διακόπτες, οι έξυπνοι διακόπτες, οι διακόπτες πολλαπλών επιπέδων, οι εικονικοί διακόπτες ασφαλείας, οι προγραμματιζόμενοι διακόπτες για δικτύωση βάσει λογισμικού και οι γέφυρες, π.χ. τα σημεία ασύρματης πρόσβασης.

Κατηγορία προϊόντων	Τεχνική περιγραφή
13. Μικροεπεξεργαστές με λειτουργίες σχετικές με την ασφάλεια	Προϊόντα με ψηφιακά στοιχεία που είναι ολοκληρωμένα κυκλώματα τα οποία εκτελούν λειτουργίες κεντρικής επεξεργασίας που βασίζονται σε εξωτερική μνήμη και περιφερειακά, συμπεριλαμβανομένου του μικροκώδικα και άλλου υλικολογισμικού χαμηλού επιπέδου. Επιπλέον, παρέχουν λειτουργίες σχετικές με την ασφάλεια, π.χ. κρυπτογράφηση, επαλήθευση ταυτότητας, ασφαλή αποθήκευση κλειδιών, παραγωγή τυχαίων αριθμών, αξιόπιστο περιβάλλον εκτέλεσης ή άλλους μηχανισμούς προστασίας βάσει υλισμικού, που αποσκοπούν στην ασφάλεια άλλων προϊόντων, δικτύων ή υπηρεσιών πέραν του ίδιου του μικροεπεξεργαστή, όπως είναι η ασφαλής αλυσίδα εκκίνησης, η εικονικοποίηση ή οι ασφαλείς διεπαφές επικοινωνίας.
14. Μικροελεγκτές με λειτουργίες σχετικές με την ασφάλεια	Προϊόντα με ψηφιακά στοιχεία τα οποία είναι ολοκληρωμένα κυκλώματα και εκτελούν κεντρικές λειτουργίες επεξεργασίας που ενσωματώνουν μνήμη η οποία επιτρέπει τον προγραμματισμό του μικροελεγκτή και συνήθως και άλλα περιφερειακά, συμπεριλαμβανομένου του μικροκώδικα και άλλου υλικολογισμικού χαμηλού επιπέδου. Επιπλέον, παρέχουν λειτουργίες σχετικές με την ασφάλεια, π.χ. κρυπτογράφηση, επαλήθευση ταυτότητας, ασφαλή αποθήκευση κλειδιών, παραγωγή τυχαίων αριθμών, αξιόπιστο περιβάλλον εκτέλεσης ή άλλους μηχανισμούς προστασίας βάσει υλισμικού, που αποσκοπούν στην ασφάλεια άλλων προϊόντων, δικτύων ή υπηρεσιών πέραν του ίδιου του μικροελεγκτή, όπως είναι η ασφαλής αλυσίδα εκκίνησης, η εικονικοποίηση ή οι ασφαλείς διεπαφές επικοινωνίας.
15. Ολοκληρωμένα κυκλώματα ειδικών εφαρμογών (ASIC) και συστοιχίες επιτόπια προγραμματιζόμενων πυλών (FPGA) με λειτουργίες σχετικές με την ασφάλεια	Τα ολοκληρωμένα κυκλώματα ειδικών εφαρμογών (ASIC) με λειτουργίες σχετικές με την ασφάλεια είναι προϊόντα με ψηφιακά στοιχεία τα οποία είναι ολοκληρωμένα κυκλώματα, πλήρως ή εν μέρει σχεδιασμένα για την εκτέλεση συγκεκριμένης λειτουργίας ή την υλοποίηση συγκεκριμένης εφαρμογής, συμπεριλαμβανομένου του μικροκώδικα και άλλου υλικολογισμικού χαμηλού επιπέδου. Επιπλέον, παρέχουν λειτουργίες σχετικές με την ασφάλεια, π.χ. κρυπτογράφηση, επαλήθευση ταυτότητας, ασφαλή αποθήκευση κλειδιών, παραγωγή τυχαίων αριθμών, αξιόπιστο περιβάλλον εκτέλεσης ή άλλους μηχανισμούς προστασίας βάσει υλισμικού, που αποσκοπούν στην ασφάλεια άλλων προϊόντων, δικτύων ή υπηρεσιών πέραν των ίδιων των ASIC, όπως είναι η ασφαλής αλυσίδα εκκίνησης, η εικονικοποίηση ή οι ασφαλείς διεπαφές επικοινωνίας.
	Οι συστοιχίες επιτόπια προγραμματιζόμενων πυλών (FPGA) με λειτουργίες σχετικές με την ασφάλεια είναι προϊόντα με ψηφιακά στοιχεία που είναι ολοκληρωμένα κυκλώματα τα οποία χαρακτηρίζονται από μήτρα διαμορφώσιμων λογικών συστοιχιών που έχουν σχεδιαστεί για να είναι επαναπρογραμματιζόμενα μετά την κατασκευή για την εκτέλεση συγκεκριμένης λειτουργίας ή την υλοποίηση συγκεκριμένης εφαρμογής, συμπεριλαμβανομένου του μικροκώδικα και άλλου υλικολογισμικού χαμηλού επιπέδου. Επιπλέον, παρέχουν λειτουργίες σχετικές με την ασφάλεια, π.χ. κρυπτογράφηση, επαλήθευση ταυτότητας, ασφαλή αποθήκευση κλειδιών, παραγωγή τυχαίων αριθμών, αξιόπιστο περιβάλλον εκτέλεσης ή άλλους μηχανισμούς προστασίας βάσει υλισμικού, που αποσκοπούν στην ασφάλεια άλλων προϊόντων, δικτύων ή υπηρεσιών πέραν των ίδιων των FPGA, όπως είναι η ασφαλής αλυσίδα εκκίνησης, η εικονικοποίηση ή οι ασφαλείς διεπαφές επικοινωνίας.
16. Εικονικοί βοηθοί γενικής χρήσης για έξυπνες κατοικίες	Προϊόντα με ψηφιακά στοιχεία που επικοινωνούν στο δημόσιο διαδίκτυο, είτε απευθείας είτε μέσω άλλου εξοπλισμού, τα οποία επεξεργάζονται απαιτήσεις, καθήκοντα ή ερωτήσεις που βασίζονται σε υποδείξεις σε φυσική γλώσσα, π.χ. ηχητικές ή γραπτές, και τα οποία, με βάση τις εν λόγω απαιτήσεις, καθήκοντα ή ερωτήσεις, παρέχουν πρόσβαση σε άλλες υπηρεσίες ή ελέγχουν τις λειτουργίες των συνδεδεμένων συσκευών σε οικιακές εγκαταστάσεις. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, έξυπνους ομιλητές με ενσωματωμένο εικονικό βοηθό και αυτόνομους εικονικούς βοηθούς που πληρούν αυτή την περιγραφή.

Κατηγορία προϊόντων	Τεχνική περιγραφή
17. Προϊόντα έξυπνης κατοικίας με λειτουργίες ασφαλείας, μεταξύ των οποίων έξυπνες κλειδαριές θυρών, κάμερες ασφαλείας, συστήματα ενδοεπικοινωνίας για βρέφη και συστήματα συναγερμού	Προϊόντα με ψηφιακά στοιχεία που προστατεύουν τη φυσική ασφάλεια των καταναλωτών σε οικιακό περιβάλλον και τα οποία μπορούν να ελέγχονται ή να υπόκεινται σε διαχείριση εξ αποστάσεως από άλλα συστήματα, καθώς και υλισμικό και λογισμικό που ελέγχουν κεντρικά τα εν λόγω προϊόντα. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, έξυπνες διατάξεις ασφάλισης θυρών, συστήματα παρακολούθησης βρεφών, συστήματα συναγερμού και οικιακές κάμερες ασφαλείας.
18. Παιχνίδια συνδεδεμένα με το διαδίκτυο που καλύπτονται από την οδηγία 2009/48/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([1]), τα οποία διαθέτουν κοινωνικά διαδραστικά χαρακτηριστικά (π.χ. ομιλία ή βιντεοσκόπηση) ή διαθέτουν χαρακτηριστικά εντοπισμού θέσης	Τα συνδεδεμένα με το διαδίκτυο παιχνίδια που έχουν κοινωνικά διαδραστικά χαρακτηριστικά είναι προϊόντα με ψηφιακά στοιχεία που καλύπτονται από την οδηγία 2009/48/ΕΚ, τα οποία επικοινωνούν στο δημόσιο διαδίκτυο, είτε απευθείας είτε μέσω οποιουδήποτε άλλου εξοπλισμού, και τα οποία διαθέτουν ενσωματωμένες τεχνολογίες που επιτρέπουν την εισερχόμενη και εξερχόμενη επικοινωνία, π.χ. πληκτρολόγιο, μικρόφωνο, ηχείο ή κάμερα.
	Τα συνδεδεμένα με το διαδίκτυο παιχνίδια με χαρακτηριστικά εντοπισμού θέσης είναι προϊόντα με ψηφιακά στοιχεία που καλύπτονται από την οδηγία 2009/48/ΕΚ, τα οποία επικοινωνούν στο δημόσιο διαδίκτυο, είτε απευθείας είτε μέσω οποιουδήποτε άλλου εξοπλισμού, και τα οποία διαθέτουν τεχνολογίες που επιτρέπουν την παρακολούθηση ή τη συναγωγή συμπερασμάτων σχετικά με τη γεωγραφική θέση του παιχνιδιού ή του χρήστη του. Όταν το παιχνίδι απλώς ανιχνεύει την εγγύτητα του χρήστη ή άλλων παιχνιδιών με τη χρήση τεχνολογιών ανίχνευσης, το παιχνίδι δεν πρέπει να θεωρείται ότι διαθέτει χαρακτηριστικά εντοπισμού θέσης.
19. Ατομικά φορετά προϊόντα που φοριούνται ή τοποθετούνται στο ανθρώπινο σώμα με σκοπό την παρακολούθηση της υγείας (π.χ. με καταγραφή δεδομένων) και στα οποία δεν εφαρμόζεται ο κανονισμός (ΕΕ) 2017/745 ([2]) ή (ΕΕ) 2017/746 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3]), ή ατομικά φορετά προϊόντα που προορίζονται για χρήση από και για παιδιά	Τα ατομικά φορετά προϊόντα που φοριούνται ή τοποθετούνται στο ανθρώπινο σώμα με σκοπό την παρακολούθηση της υγείας είναι προϊόντα με ψηφιακά στοιχεία που φοριούνται στο σώμα απευθείας ή μέσω ενδυμάτων ή εξαρτημάτων και τα οποία μπορούν, τακτικά ή συνεχώς, να καταγράφουν και να επεξεργάζονται περαιτέρω πληροφορίες, συμπεριλαμβανομένων μετρικών του σώματος, συναφών με την υγεία του χρήστη, εξαιρουμένων των προϊόντων που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού (ΕΕ) 2017/745 ή του κανονισμού (ΕΕ) 2017/746. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, συσκευές παρακολούθησης της φυσικής κατάστασης, έξυπνα ρολόγια, έξυπνα κοσμήματα, έξυπνα ενδύματα και αθλητικά ενδύματα που πληρούν την παρούσα περιγραφή.
	Τα ατομικά φορετά προϊόντα που προορίζονται για χρήση από και για παιδιά είναι προϊόντα με ψηφιακά στοιχεία που μπορούν να φοριούνται ή να τοποθετούνται στο σώμα, απευθείας ή μέσω ενδυμάτων ή εξαρτημάτων, ατόμων ηλικίας κάτω των 14 ετών. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, φορετά προϊόντα για την ασφάλεια των παιδιών.

([1]) Οδηγία 2009/48/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Ιουνίου 2009, σχετικά με την ασφάλεια των παιχνιδιών (ΕΕ L 170 της 30.6.2009, σ. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Κανονισμός (ΕΕ) 2017/745 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Απριλίου 2017, για τα ιατροτεχνολογικά προϊόντα, για την τροποποίηση της οδηγίας 2001/83/ΕΚ, του κανονισμού (ΕΚ) αριθ. 178/2002 και του κανονισμού (ΕΚ) αριθ. 1223/2009 και για την κατάργηση των οδηγιών του Συμβουλίου 90/385/ΕΟΚ και 93/42/ΕΟΚ (ΕΕ L 117 της 5.5.2017, σ. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Κανονισμός (ΕΕ) 2017/746 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Απριλίου 2017, για τα in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα και για την κατάργηση της οδηγίας 98/79/ΕΚ και της απόφασης 2010/227/ΕΕ της Επιτροπής (ΕΕ L 117 της 5.5.2017, σ. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Κλάση II

Κατηγορία προϊόντων	Τεχνική περιγραφή
1. Επόπτες (hypervisors) και συστήματα χρόνου λειτουργίας που υποστηρίζουν εικονική εκτέλεση λειτουργικών συστημάτων και παρόμοια περιβάλλοντα	Οι επόπτες είναι προϊόντα λογισμικού με ψηφιακά στοιχεία που εκτρέπουν και/ή κατανέμουν υπολογιστικούς πόρους και καθιστούν δυνατή την εκτέλεση, τη διαχείριση και την ενορχήστρωση εικονικών μηχανών που είναι λογικά διαχωρισμένες μεταξύ τους και/ή από το υλισμικό. Οι επόπτες μπορούν να λειτουργούν απευθείας σε υλισμικό («επόπτες γυμνού μετάλλου»), πάνω από το λειτουργικό σύστημα ή εντός άλλου εικονικού μηχανήματος (ένθετη εικονικοποίηση). Στο πλαίσιο αυτής της κατηγορίας προϊόντων, η εικονική μηχανή είναι ένας λογικός διαχωρισμός υπολογιστικού περιβάλλοντος που καθορίζεται από λογισμικό, ο οποίος περιλαμβάνει εικονικοποιημένο σύνολο πόρων υλισμικού (π.χ. CPU, μνήμη, αποθήκευση, διεπαφές δικτύου) και κατά κανόνα φιλοξενεί το δικό της λειτουργικό σύστημα. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, τους επόπτες τύπου 1 (γυμνού μετάλλου), τους επόπτες τύπου 2 (που φιλοξενούνται σε λειτουργικό σύστημα) και τους υβριδικούς επόπτες.
	Τα συστήματα χρόνου λειτουργίας είναι προϊόντα λογισμικού με ψηφιακά στοιχεία τα οποία διαχειρίζονται την εκτέλεση και τον κύκλο ζωής των περιεκτών που λειτουργούν ως απομονωμένες διαδικασίες σε ένα λειτουργικό σύστημα ενιαίου ξενιστή, κατανέμοντας πόρους και επιτρέποντας τη διαχείριση και την ενορχήστρωση μεμονωμένων περιεκτών. Στο πλαίσιο αυτής της κατηγορίας προϊόντων, ο περιέκτης είναι ένα περιβάλλον εκτέλεσης βασισμένο σε λογισμικό που περικλείει ένα ή περισσότερα στοιχεία λογισμικού και τα παρελκόμενά τους σε ένα ενιαίο πακέτο, το οποίο του επιτρέπει να λειτουργεί ανεξάρτητα και με συνέπεια.
2. Τείχη προστασίας, συστήματα ανίχνευσης και πρόληψης εισβολών	Τα τείχη προστασίας είναι προϊόντα με ψηφιακά στοιχεία που προστατεύουν ένα συνδεδεμένο δίκτυο ή σύστημα από μη εξουσιοδοτημένη πρόσβαση μέσω της παρακολούθησης και του περιορισμού των δεδομένων κίνησης των επικοινωνιών προς και από το εν λόγω δίκτυο. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, τείχη προστασίας δικτύου και τείχη προστασίας από εφαρμογές, όπως τείχη προστασίας ή φίλτρα διαδικτυακών εφαρμογών και πύλες κατά των ανεπιθύμητων μηνυμάτων.
	Τα συστήματα ανίχνευσης εισβολών είναι προϊόντα με ψηφιακά στοιχεία που παρακολουθούν την κυκλοφορία μετά την είσοδό της στο περιβάλλον δικτύου για ύποπτη δραστηριότητα και εντοπίζουν ότι έχει επιχειρηθεί, εκδηλωθεί ή ολοκληρωθεί εισβολή σε συνδεδεμένο δίκτυο ή σύστημα. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, συστήματα ανίχνευσης εισβολών βάσει δικτύου και συστήματα ανίχνευσης εισβολών που βασίζονται σε ξενιστή.
	Τα συστήματα πρόληψης εισβολών είναι προϊόντα με ψηφιακά στοιχεία που αποτελούνται από ένα σύστημα ανίχνευσης εισβολών που ανταποκρίνεται ενεργά σε εισβολή σε συνδεδεμένο δίκτυο ή σύστημα. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, συστήματα πρόληψης εισβολών που βασίζονται σε δίκτυο και συστήματα πρόληψης εισβολών που βασίζονται σε ξενιστή.

Κατηγορία προϊόντων	Τεχνική περιγραφή
3. Μικροεπεξεργαστές ανθεκτικοί στην παραποίηση	Προϊόντα με ψηφιακά στοιχεία που είναι μικροεπεξεργαστές με λειτουργίες σχετικές με την ασφάλεια που αναφέρονται στον πίνακα «Κλάση Ι» σημείο 13 του παρόντος παραρτήματος, συμπεριλαμβανομένων αποδεικτικών στοιχείων παραποίησης, αντοχής ή απόκρισης σε παραποίηση, και τα οποία έχουν επιπλέον σχεδιαστεί για να παρέχουν προστασία επιπέδου AVA_VAN 2 ή 3, όπως ορίζεται στα κοινά κριτήρια και στην κοινή μεθοδολογία αξιολόγησης.
4. Μικροελεγκτές ανθεκτικοί στην παραποίηση	Προϊόντα με ψηφιακά στοιχεία που είναι μικροελεγκτές με λειτουργίες σχετικές με την ασφάλεια που αναφέρονται στον πίνακα «Κλάση Ι» σημείο 14 του παρόντος παραρτήματος, συμπεριλαμβανομένων των αποδεικτικών στοιχείων παραποίησης, αντοχής ή απόκρισης σε παραποίηση, και τα οποία έχουν επιπλέον σχεδιαστεί για να παρέχουν προστασία επιπέδου AVA_VAN 2 ή 3, όπως ορίζεται στα κοινά κριτήρια και στην κοινή μεθοδολογία αξιολόγησης.

ΠΑΡΑΡΤΗΜΑ II

ΚΡΙΣΙΜΑ ΠΡΟΪΟΝΤΑ ΜΕ ΨΗΦΙΑΚΑ ΣΤΟΙΧΕΙΑ

Κατηγορία προϊόντων	Τεχνική περιγραφή
1. Συσκευές υλισμικού με θυρίδες ασφαλείας	Προϊόντα υλισμικού με ψηφιακά στοιχεία τα οποία αποθηκεύουν, επεξεργάζονται ή διαχειρίζονται με ασφάλεια ευαίσθητα δεδομένα ή εκτελούν κρυπτογραφικές λειτουργίες και τα οποία αποτελούνται από πολλαπλά διακριτά κατασκευαστικά στοιχεία, ενσωματώνοντας υλικό περίβλημα υλισμικού που παρέχει αποδεικτικά στοιχεία παραποίησης, αντοχή ή απόκριση σε παραποίηση ως αντίμετρα έναντι φυσικών επιθέσεων. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, τα φυσικά τερματικά πληρωμών, τις μονάδες ασφαλείας υλισμικού που παράγουν και διαχειρίζονται κρυπτογραφικά στοιχεία και τους ταχογράφους που πληρούν την ανωτέρω περιγραφή.
2. Πύλες έξυπνων μετρητών στο πλαίσιο έξυπνων συστημάτων μέτρησης, όπως ορίζονται στο άρθρο 2 σημείο 23) της οδηγίας (ΕΕ) 2019/944 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([1]) και άλλες συσκευές για προηγμένους σκοπούς ασφάλειας, συμπεριλαμβανομένης της ασφαλούς κρυπτοεπεξεργασίας	Οι πύλες έξυπνων μετρητών είναι προϊόντα με ψηφιακά στοιχεία που ελέγχουν την επικοινωνία μεταξύ κατασκευαστικών στοιχείων έξυπνων συστημάτων μέτρησης ή συνδεδεμένων με αυτά, όπως ορίζονται στο άρθρο 2 σημείο 23) της οδηγίας (ΕΕ) 2019/944, και εξουσιοδοτημένων τρίτων μερών, όπως είναι οι πάροχοι υπηρεσιών κοινής ωφελείας. Οι πύλες έξυπνων μετρητών συλλέγουν, επεξεργάζονται και αποθηκεύουν δεδομένα μετρητών ή δεδομένα προσωπικού χαρακτήρα, προστατεύουν τις ροές δεδομένων και πληροφοριών υποστηρίζοντας συγκεκριμένες κρυπτογραφικές ανάγκες, όπως η κρυπτογράφηση και η αποκρυπτογράφηση δεδομένων, ενσωματώνουν λειτουργίες τείχους προστασίας και παρέχουν τα μέσα για τον έλεγχο άλλων συσκευών. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, έξυπνες πύλες μέτρησης που σχετίζονται με έξυπνα συστήματα μέτρησης ηλεκτρικής ενέργειας, όπως ορίζονται στο άρθρο 2 σημείο 23) της οδηγίας (ΕΕ) 2019/944. Μπορεί επίσης να περιλαμβάνει έξυπνες πύλες μέτρησης που χρησιμοποιούνται σε άλλα έξυπνα συστήματα μέτρησης που μετρούν την κατανάλωση άλλων πηγών ενέργειας, όπως το αέριο ή η θερμότητα, υπό την προϋπόθεση ότι η πύλη πληροί αυτή την περιγραφή.
3. Έξυπνες κάρτες ή παρόμοιες συσκευές, συμπεριλαμβανομένων των ασφαλών στοιχείων	Τα ασφαλή στοιχεία είναι μικροελεγκτές ή μικροεπεξεργαστές με λειτουργίες σχετικές με την ασφάλεια, συμπεριλαμβανομένων των αποδεικτικών στοιχείων παραποίησης, αντοχής ή απόκρισης σε παραποίηση. Συνήθως αποθηκεύουν, επεξεργάζονται ή διαχειρίζονται κρυπτογραφικές λειτουργίες ή ευαίσθητα δεδομένα, όπως διαπιστευτήρια ταυτότητας ή διαπιστευτήρια πληρωμών. Τα ασφαλή στοιχεία έχουν σχεδιαστεί έτσι ώστε να παρέχουν προστασία επιπέδου τουλάχιστον AVA_VAN.4, όπως ορίζεται στα κοινά κριτήρια ή στην κοινή μεθοδολογία αξιολόγησης. Μπορεί να είναι ξεχωριστά συστατικά στοιχεία από πυρίτιο ή να ενσωματώνονται σε συστήματα σε μικροκύκλωμα (SoC). Τα ασφαλή στοιχεία μπορούν να ενσωματώνουν περιβάλλον εφαρμογής ή λειτουργικό σύστημα και μπορούν να περιλαμβάνουν μία ή περισσότερες εφαρμογές. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, τις μονάδες αξιόπιστης πλατφόρμας (TPM) και την ενσωματωμένη καθολική κάρτα ολοκληρωμένου κυκλώματος (UICC).
	Οι έξυπνες κάρτες ή οι παρόμοιες συσκευές είναι ασφαλή στοιχεία ενσωματωμένα σε φέρον υλικό, όπως πλαστικό ή ξύλο, σε σχήμα κάρτας, ή ασφαλή στοιχεία ενσωματωμένα σε φέροντα υλικά με άλλα σχήματα. Η κατηγορία αυτή περιλαμβάνει, μεταξύ άλλων, τα έγγραφα ταυτότητας και τα ταξιδιωτικά έγγραφα, τις αναγνωρισμένες κάρτες υπογραφής, τις αντικαταστάσιμες UICC, τις φυσικές κάρτες πληρωμής, τις φυσικές κάρτες πρόσβασης, τις ψηφιακές κάρτες ταχογράφου ή τα βραχιόλια πληρωμής με ενσωματωμένα ασφαλή στοιχεία πληρωμών.

([1]) Οδηγία (ΕΕ) 2019/944 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Ιουνίου 2019, σχετικά με τους κοινούς κανόνες για την εσωτερική αγορά ηλεκτρικής ενέργειας και την τροποποίηση της οδηγίας 2012/27/ΕΕ (ΕΕ L 158 της 14.6.2019, σ. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).