Ευρωπαϊκό Κοινοβούλιο
2019-2024

Έγγραφο συνόδου

A9-0307/2023

26.10.2023

***I
ΕΚΘΕΣΗ

σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την τροποποίηση του κανονισμού (ΕΕ) 2019/881 όσον αφορά τις διαχειριζόμενες υπηρεσίες ασφάλειας
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας

Εισηγήτρια: Josianne Cutajar

Υπόμνημα για τα χρησιμοποιούμενα σύμβολα

*	Διαδικασία διαβούλευσης
***	Διαδικασία έγκρισης
***I	Συνήθης νομοθετική διαδικασία (πρώτη ανάγνωση)
***II	Συνήθης νομοθετική διαδικασία (δεύτερη ανάγνωση)
***III	Συνήθης νομοθετική διαδικασία (τρίτη ανάγνωση)

(Η ενδεικνυόμενη διαδικασία στηρίζεται στη νομική βάση που προτείνεται στο σχέδιο πράξης)

Τροπολογίες σε σχέδιο πράξης

Τροπολογίες του Κοινοβουλίου σε δύο στήλες

Η διαγραφή κειμένου σημαίνεται με ***πλάγιους έντονους χαρακτήρες*** στην αριστερή στήλη. Η αντικατάσταση κειμένου σημαίνεται με ***πλάγιους έντονους χαρακτήρες*** και στις δύο στήλες. Το νέο κείμενο σημαίνεται με ***πλάγιους έντονους χαρακτήρες*** στη δεξιά στήλη.

Η πρώτη και η δεύτερη γραμμή της επικεφαλίδας κάθε τροπολογίας προσδιορίζουν το σχετικό τμήμα του εξεταζόμενου σχεδίου πράξης. Εάν μία τροπολογία αναφέρεται σε ήδη υφιστάμενη πράξη την οποία το σχέδιο πράξης αποσκοπεί να τροποποιήσει, η επικεφαλίδα περιέχει επιπλέον και μία τρίτη και μία τέταρτη γραμμή που προσδιορίζουν αντίστοιχα την υφιστάμενη πράξη και τη διάταξή της στην οποία αναφέρεται η τροπολογία.

Τροπολογίες του Κοινοβουλίου με μορφή ενοποιημένου κειμένου

Τα νέα τμήματα του κειμένου σημαίνονται με ***πλάγιους έντονους χαρακτήρες***. Τα τμήματα του κειμένου που απαλείφονται σημαίνονται με το σύμβολο ▌ ή με διαγραφή. Η αντικατάσταση κειμένου σημαίνεται με ***πλάγιους έντονους χαρακτήρες*** που υποδηλώνουν το νέο κείμενο και με διαγραφή του κειμένου που αντικαθίσταται.
Κατ' εξαίρεση, δεν σημαίνονται οι τροποποιήσεις αυστηρά τεχνικής φύσης που επιφέρουν οι υπηρεσίες κατά την επεξεργασία του τελικού κειμένου.

ΠΕΡΙΕΧΟΜΕΝΑ

Σελίδα

ΣΧΕΔΙΟ ΝΟΜΟΘΕΤΙΚΟΥ ΨΗΦΙΣΜΑΤΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ

σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την τροποποίηση του κανονισμού (ΕΕ) 2019/881 όσον αφορά τις διαχειριζόμενες υπηρεσίες ασφάλειας

(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

(Συνήθης νομοθετική διαδικασία: πρώτη ανάγνωση)

Το Ευρωπαϊκό Κοινοβούλιο,

– έχοντας υπόψη την πρόταση της Επιτροπής προς το Κοινοβούλιο και το Συμβούλιο (COM(2023)0208),

– έχοντας υπόψη το άρθρο 294 παράγραφος 2 και το άρθρο 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, σύμφωνα με τα οποία του υποβλήθηκε η πρόταση από την Επιτροπή (C9-0137/2023),

– έχοντας υπόψη το άρθρο 294 παράγραφος 3 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης,

– έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής της 13ης Ιουλίου 2023[1],

– έχοντας υπόψη το άρθρο 59 του Κανονισμού του,

– έχοντας υπόψη την επιστολή της Επιτροπής Εσωτερικής Αγοράς και Προστασίας των Καταναλωτών,

– έχοντας υπόψη την έκθεση της Επιτροπής Βιομηχανίας, Έρευνας και Ενέργειας (A9-0307/2023),

1. εγκρίνει τη θέση του σε πρώτη ανάγνωση όπως παρατίθεται κατωτέρω·

2. ζητεί από την Επιτροπή να υποβάλει εκ νέου την πρόταση στο Κοινοβούλιο, αν την αντικαταστήσει με νέο κείμενο, αν της επιφέρει σημαντικές τροποποιήσεις ή αν προτίθεται να της επιφέρει σημαντικές τροποποιήσεις·

3. αναθέτει στην Πρόεδρό του να διαβιβάσει τη θέση του Κοινοβουλίου στο Συμβούλιο, στην Επιτροπή και στα εθνικά κοινοβούλια.

[1] ΕΕ C 349 της 29.9.2023, σ. 167.

Τροπολογία 1

ΤΡΟΠΟΛΟΓΙΕΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ*

στην πρόταση της Επιτροπής

2023/0108 (COD)

Πρόταση

ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

για την τροποποίηση του κανονισμού (ΕΕ) 2019/881 όσον αφορά τις διαχειριζόμενες υπηρεσίες ασφάλειας

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης και ιδίως το άρθρο 114,

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής[1],

Έχοντας υπόψη τη γνώμη της Επιτροπής των Περιφερειών,

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία[2],

---

* Τροπολογίες: το νέο ή το τροποποιημένο κείμενο σημειώνεται με έντονους πλάγιους χαρακτήρες· οι διαγραφές σημειώνονται με το σύμβολο ▌.

1 ***ΕΕ C 349 της 29.9.2023, σ. 167.***

2 ***Θέση του Ευρωπαϊκού Κοινοβουλίου της … (δεν έχει ακόμη δημοσιευτεί στην Επίσημη Εφημερίδα) και απόφαση του Συμβουλίου της … .***

Εκτιμώντας τα ακόλουθα:

(1) Ο κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[3] θεσπίζει ένα πλαίσιο για τη θέσπιση ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας με σκοπό τη διασφάλιση επαρκούς επιπέδου κυβερνοασφάλειας για τα προϊόντα ***τεχνολογίας πληροφοριών και επικοινωνιών (***ΤΠΕ***)***, τις υπηρεσίες ΤΠΕ και τις διαδικασίες ΤΠΕ στην Ένωση, καθώς και με σκοπό την αποφυγή του κατακερματισμού της εσωτερικής αγοράς όσον αφορά τα σχήματα πιστοποίησης της κυβερνοασφάλειας στην Ένωση.

(1α) Προκειμένου να διασφαλιστεί η ανθεκτικότητα της Ένωσης σε κυβερνοεπιθέσεις και να προληφθούν τυχόν τρωτά σημεία στην αγορά της Ένωσης, ο παρών κανονισμός αποσκοπεί στη συμπλήρωση του οριζόντιου κανονιστικού πλαισίου που θεσπίζει ολοκληρωμένες απαιτήσεις κυβερνοασφάλειας για όλα τα προϊόντα με ψηφιακά στοιχεία σύμφωνα με τον κανονισμό (ΕΕ).../... του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[4] (2022/0272 (COD)), θεσπίζοντας βασικές απαιτήσεις για τις υπηρεσίες που τελούν υπό διαχείριση κυβερνοασφάλειας, την εφαρμογή τους και την αξιοπιστία τους.

(2) Οι διαχειριζόμενες υπηρεσίες ασφάλειας, οι οποίες συνίστανται στην εκτέλεση ή την παροχή βοήθειας για δραστηριότητες που σχετίζονται με τη διαχείριση κινδύνων κυβερνοασφάλειας από τους πελάτες τους, ***μεταξύ άλλων στους τομείς του εντοπισμού, της αντιμετώπισης περιστατικών ή της ανάκαμψης από αυτά,*** αποκτούν ολοένα και μεγαλύτερη σημασία για την πρόληψη και τον μετριασμό των περιστατικών κυβερνοασφάλειας. ***Οι δραστηριότητες των παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας συνίστανται σε υπηρεσίες που σχετίζονται με την πρόληψη, τον προσδιορισμό, την προστασία, τον εντοπισμό, την ανάλυση, την ανάσχεση, την αντιμετώπιση και την ανάκαμψη, συμπεριλαμβανομένων, μεταξύ άλλων, της παροχής πληροφοριών σχετικά με κυβερνοαπειλές, της παρακολούθησης απειλών σε πραγματικό χρόνο μέσω προδραστικών τεχνικών,***

---

3 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).

4 Κανονισμός (ΕΕ) .../... του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της ... σχετικά με ... (ΕΕ L, ..., ELI: ...).

συμπεριλαμβανομένων της ασφάλειας βάσει σχεδιασμού, της εκτίμησης κινδύνου, της εκτεταμένης ανίχνευσης, της διόρθωσης και της αντιμετώπισης. Ως εκ τούτου, οι πάροχοι των εν λόγω υπηρεσιών θεωρούνται βασικές ή σημαντικές οντότητες που ανήκουν σε τομέα υψηλής κρισιμότητας σύμφωνα με την οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[5]. Σύμφωνα με την αιτιολογική σκέψη 86 της εν λόγω οδηγίας, οι πάροχοι υπηρεσίας διαχείρισης της ασφάλειας σε τομείς όπως η αντιμετώπιση περιστατικών, οι δοκιμές διείσδυσης, οι έλεγχοι ασφάλειας και η παροχή συμβουλών διαδραματίζουν ιδιαίτερα σημαντικό ρόλο στην παροχή συνδρομής σε οντότητες που καταβάλλουν προσπάθειες για την πρόληψη, τον εντοπισμό και την αντιμετώπιση περιστατικών ή την ανάκαμψη από αυτά. Ωστόσο, οι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας αποτέλεσαν και οι ίδιοι στόχο κυβερνοεπιθέσεων και ενέχουν ιδιαίτερο κίνδυνο λόγω της στενής ενσωμάτωσής τους στις δραστηριότητες των πελατών τους. Συνεπώς, οι βασικές και σημαντικές οντότητες κατά την έννοια της οδηγίας (ΕΕ) 2022/2555 θα πρέπει να επιδεικνύουν αυξημένη επιμέλεια κατά την επιλογή παρόχου διαχειριζόμενης υπηρεσίας ασφάλειας.

(3) Οι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας διαδραματίζουν επίσης σημαντικό ρόλο στο αποθεματικό κυβερνοασφάλειας της ΕΕ, η σταδιακή σύσταση του οποίου υποστηρίζεται από τον κανονισμό (ΕΕ) .../… [για τη θέσπιση μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για τον εντοπισμό, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας]. Το αποθεματικό της ΕΕ για την κυβερνοασφάλεια πρέπει να χρησιμοποιείται για τη στήριξη δράσεων αντίδρασης και άμεσης ανάκαμψης σε περίπτωση σημαντικών και μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας. Ο κανονισμός (ΕΕ).../... [για τη θέσπιση μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για τον εντοπισμό, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας] θεσπίζει διαδικασία επιλογής των παρόχων που αποτελούν το αποθεματικό κυβερνοασφάλειας της ΕΕ, η οποία θα πρέπει, μεταξύ άλλων, να λαμβάνει υπόψη το αν ο ενδιαφερόμενος

[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).

πάροχος έχει λάβει ευρωπαϊκή ή εθνική πιστοποίηση κυβερνοασφάλειας. Οι σχετικές υπηρεσίες που παρέχονται από «αξιόπιστους παρόχους» σύμφωνα με τον κανονισμό (ΕΕ).../... [για τη θέσπιση μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για τον εντοπισμό, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας] αντιστοιχούν στις «διαχειριζόμενες υπηρεσίες ασφάλειας» σύμφωνα με τον παρόντα κανονισμό.

(4) Η πιστοποίηση των διαχειριζόμενων υπηρεσιών ασφάλειας δεν είναι μόνο σημαντική για τη διαδικασία επιλογής για το αποθεματικό κυβερνοασφάλειας της ΕΕ, αλλά αποτελεί επίσης βασικό δείκτη ποιότητας για τους ιδιωτικούς και δημόσιους φορείς που προτίθενται να αγοράσουν τέτοιες υπηρεσίες. Δεδομένης της κρισιμότητας των διαχειριζόμενων υπηρεσιών ασφάλειας και της ευαισθησίας των δεδομένων που επεξεργάζονται, η πιστοποίηση μπορεί να παράσχει στους δυνητικούς πελάτες σημαντική καθοδήγηση και διασφάλιση σχετικά με την αξιοπιστία των εν λόγω υπηρεσιών. Τα ευρωπαϊκά σχήματα πιστοποίησης για τις διαχειριζόμενες υπηρεσίες ασφάλειας συμβάλλουν στην αποφυγή του κατακερματισμού της ενιαίας αγοράς. Ως εκ τούτου, ο παρών κανονισμός αποσκοπεί στην ενίσχυση της λειτουργίας της εσωτερικής αγοράς.

(4α) Τα ευρωπαϊκά συστήματα πιστοποίησης για διαχειριζόμενες υπηρεσίες ασφάλειας θα πρέπει να οδηγήσουν στην αξιοποίηση των εν λόγω υπηρεσιών και στην αύξηση του ανταγωνισμού στον τομέα, λαμβάνοντας υπόψη τις ειδικές ανάγκες τόσο των παρόχων όσο και των δικαιούχων. Ως εκ τούτου, τα εν λόγω συστήματα θα πρέπει να επιτυγχάνουν ισορροπία μεταξύ του στόχου τους και της πιθανής κανονιστικής, διοικητικής και οικονομικής επιβάρυνσης που θα μπορούσαν να αντιμετωπίσουν οι πάροχοι, ιδίως οι πολύ μικρές ή οι μικρές και μεσαίες επιχειρήσεις (ΜΜΕ). Επιπλέον, τα συστήματα θα πρέπει να ενθαρρύνουν τη χρήση πιστοποιημένων διαχειριζόμενων υπηρεσιών ασφάλειας, συμβάλλοντας στην προσβασιμότητά τους, ιδίως για μικρότερους φορείς, όπως οι πολύ μικρές επιχειρήσεις και οι ΜΜΕ, καθώς και οι τοπικές και περιφερειακές αρχές που έχουν περιορισμένες ικανότητες και πόρους, αλλά είναι πιο επιρρεπείς σε παραβιάσεις της κυβερνοασφάλειας με οικονομικές, νομικές και λειτουργικές επιπτώσεις, καθώς και επιπτώσεις στη φήμη τους.

(4β) Το ενωσιακό σύστημα πιστοποίησης για διαχειριζόμενες υπηρεσίες ασφάλειας θα πρέπει να διασφαλίζει τη διαθεσιμότητα ασφαλών και υψηλής ποιότητας υπηρεσιών που εγγυώνται ασφαλή ψηφιακή μετάβαση και συμβάλλουν στην επίτευξη των στόχων που καθορίζονται στο πρόγραμμα πολιτικής «Ψηφιακή δεκαετία», ιδίως όσον αφορά τον στόχο το 75 % των επιχειρήσεων της ΕΕ να αρχίσουν να χρησιμοποιούν υπολογιστικό νέφος, ΤΝ ή μαζικά δεδομένα, τον στόχο ποσοστό πάνω από το 90 % των πολύ μικρών επιχειρήσεων και των ΜΜΕ να κατακτήσει τουλάχιστον ένα βασικό επίπεδο ψηφιακής έντασης και τον στόχο να παρέχονται διαδικτυακά οι βασικές δημόσιες υπηρεσίες.

(4γ) Στο τρέχον ταχέως εξελισσόμενο ψηφιακό και τεχνολογικό τοπίο, η προσφορά εκπαιδευτικών πόρων και επίσημων προγραμμάτων κατάρτισης ποικίλει και οι γνώσεις μπορούν να αποκτηθούν με διάφορους τρόπους, τόσο τυπικούς, για παράδειγμα μέσω πανεπιστημίων ή μαθημάτων, όσο και μη τυπικούς, για παράδειγμα μέσω προγραμμάτων επαγγελματικής κατάρτισης ή μακροχρόνιας εργασιακής πείρας στον σχετικό τομέα.

(5) Εκτός από την ανάπτυξη προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ, οι διαχειριζόμενες υπηρεσίες ασφάλειας περιλαμβάνουν συχνά πρόσθετα χαρακτηριστικά υπηρεσιών που βασίζονται στις ικανότητες, την εμπειρογνωσία και την πείρα του προσωπικού τους. Προκειμένου να διασφαλίζεται πολύ υψηλή ποιότητα των παρεχόμενων διαχειριζόμενων υπηρεσιών ασφάλειας, μέρος των στόχων ασφάλειας θα πρέπει να είναι το πολύ υψηλό επίπεδο των εν λόγω ικανοτήτων, εμπειρογνωσίας και πείρας, καθώς και κατάλληλες εσωτερικές διαδικασίες. Συνεπώς, για να εξασφαλιστεί ότι όλες οι πτυχές μιας διαχειριζόμενης υπηρεσίας ασφάλειας μπορούν να καλυφθούν από ένα ***ειδικό*** σχήμα πιστοποίησης, είναι αναγκαίο να τροποποιηθεί ο κανονισμός (ΕΕ) 2019/881. ***Η ανάπτυξη σχημάτων πιστοποίησης βάσει του παρόντος κανονισμού θα πρέπει να λαμβάνει υπόψη τα αποτελέσματα και τις συστάσεις της αξιολόγησης και επανεξέτασης που προβλέπονται στον παρόντα κανονισμό.***

(5α) Η διαδικασία πιστοποίησης που προβλέπεται εντός του πλαισίου που θεσπίζει ο παρών κανονισμός θα πρέπει να εξορθολογιστεί, ώστε να διασφαλιστούν η διεθνής αναγνώριση και η εναρμόνιση με διεθνή πρότυπα, με σκοπό να διευκολυνθεί η ανάπτυξη μιας αξιόπιστης ενωσιακής αγοράς και παράλληλα να

δημιουργηθούν εταιρικές σχέσεις με ομόφρονες τρίτες χώρες, μεταξύ άλλων υπό το πρίσμα των διατάξεων του κανονισμού (ΕΕ).../... του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[6] (2023/0109(COD)) όσον αφορά την πρόσβαση στην εφεδρεία στον τομέα της κυβερνοασφάλειας σε επίπεδο Ένωσης.

(5β) Προκειμένου να διασφαλιστεί η ανάπτυξη αξιόπιστης ενωσιακής αγοράς για διαχειριζόμενες υπηρεσίες ασφάλειας, οι πάροχοί τους και τα κράτη μέλη θα πρέπει να συνεργάζονται και να συμβάλλουν στη συλλογή δεδομένων σχετικά με την κατάσταση και την εξέλιξη της αγοράς εργασίας στον τομέα της κυβερνοασφάλειας.

(5γ) Μια συντονισμένη προσέγγιση σε επίπεδο Ένωσης με σκοπό την ενίσχυση της ανθεκτικότητας των υποδομών ζωτικής σημασίας βασίζεται στην ανάπτυξη ικανοτήτων των κρατών μελών. Ωστόσο, η Ένωση βρίσκεται αντιμέτωπη με μια έλλειψη ταλέντων, χαρακτηριστικό της οποίας είναι η έλλειψη ειδικευμένων επαγγελματιών, και με ένα ταχέως εξελισσόμενο τοπίο απειλών, όπως αναγνωρίζεται στην ανακοίνωση της Επιτροπής, της 18ης Απριλίου 2023, σχετικά με την ακαδημία κυβερνοδεξιοτήτων. Συνεπώς, προκειμένου να διευκολυνθεί η εμφάνιση βασικών διαχειριζόμενων υπηρεσιών ασφάλειας και να υπάρξει καλύτερη επισκόπηση της σύνθεσης του εργατικού δυναμικού της Ένωσης στον τομέα της κυβερνοασφάλειας, η συνεργασία μεταξύ των κρατών μελών, της Επιτροπής, του ENISA και των ενδιαφερόμενων μερών, συμπεριλαμβανομένου του ιδιωτικού τομέα και της πανεπιστημιακής κοινότητας, θα πρέπει να ενισχυθεί μέσω της ανάπτυξης συμπράξεων δημόσιου και ιδιωτικού τομέα, της στήριξης πρωτοβουλιών έρευνας και καινοτομίας, της ανάπτυξης και αμοιβαίας αναγνώρισης κοινών προτύπων και πιστοποίησης δεξιοτήτων κυβερνοασφάλειας, μεταξύ άλλων μέσω του ευρωπαϊκού πλαισίου δεξιοτήτων κυβερνοασφάλειας. Αυτό θα πρέπει επίσης να διευκολύνει την κινητικότητα των επαγγελματιών της κυβερνοασφάλειας εντός της Ένωσης, καθώς και την ενσωμάτωση των γνώσεων και της κατάρτισης στον τομέα της κυβερνοασφάλειας στα εκπαιδευτικά προγράμματα, διασφαλίζοντας παράλληλα την πρόσβαση των νέων,

---

6 Κανονισμός (ΕΕ) .../... του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της ... σχετικά με ... (ΕΕ L, ..., ELI: ...).

συμπεριλαμβανομένων των ατόμων που ζουν σε μειονεκτούσες περιοχές όπως νησιά, αραιοκατοικημένες, αγροτικές και απομακρυσμένες περιοχές, σε θέσεις μαθητείας και πρακτικής άσκησης. Τα μέτρα αυτά θα πρέπει επίσης να αποσκοπούν στην προσέλκυση περισσότερων γυναικών και κοριτσιών στον τομέα και να συμβάλλουν στην αντιμετώπιση του χάσματος μεταξύ των φύλων στους τομείς των θετικών επιστημών, της τεχνολογίας, της μηχανικής και των μαθηματικών. Ο ιδιωτικός τομέας θα πρέπει επίσης να επιδιώκει την παροχή κατάρτισης στον χώρο εργασίας η οποία να καλύπτει τις δεξιότητες με τη μεγαλύτερη ζήτηση, με τη συμμετοχή της δημόσιας διοίκησης και νεοφυών επιχειρήσεων, καθώς και των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων.

(5δ) Θα πρέπει να εξασφαλιστούν κατάλληλη χρηματοδότηση και πόροι για τους σκοπούς των πρόσθετων καθηκόντων που ανατίθενται στον ENISA με τις τροποποιήσεις του κανονισμού (ΕΕ) 2019/881 που εισάγονται με τον παρόντα κανονισμό.

(5ε) Για τη συμπλήρωση ορισμένων μη ουσιωδών στοιχείων του παρόντος κανονισμού, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων, σύμφωνα με το άρθρο 290 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης για τη δημιουργία ενός ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας. Είναι ιδιαίτερα σημαντικό η Επιτροπή να διεξάγει, κατά τις προπαρασκευαστικές της εργασίες, τις κατάλληλες διαβουλεύσεις, μεταξύ άλλων σε επίπεδο εμπειρογνωμόνων, οι οποίες να πραγματοποιούνται σύμφωνα με τις αρχές που ορίζονται στη διοργανική συμφωνία της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου[7]. Πιο συγκεκριμένα, προκειμένου να διασφαλιστεί η ίση συμμετοχή στην προετοιμασία των κατ' εξουσιοδότηση πράξεων, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο λαμβάνουν όλα τα έγγραφα κατά τον ίδιο χρόνο με τους εμπειρογνώμονες των κρατών μελών, και οι εμπειρογνώμονές τους έχουν συστηματικά πρόσβαση στις

7 ΕΕ L 123 της 12.5.2016, σ. 1.

συνεδριάσεις των ομάδων εμπειρογνωμόνων της Επιτροπής που ασχολούνται με την προετοιμασία κατ' εξουσιοδότηση πράξεων.

(5ε) Ζητήθηκε η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και διατύπωσε γνώμη στις [ΗΗ/ΜΜ/ΕΕΕΕ][8],

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

---

8 ΕΕ C .../…

Άρθρο 1

Τροποποιήσεις του κανονισμού (ΕΕ) 2019/881

Ο κανονισμός (ΕΕ) 2019/881 τροποποιείται ως εξής:

1) στο άρθρο 1 παράγραφος 1 πρώτο εδάφιο το στοιχείο β) αντικαθίσταται από το ακόλουθο κείμενο:

«β) το πλαίσιο για τη θέσπιση ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας με σκοπό τη διασφάλιση επαρκούς επιπέδου κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας στην Ένωση, καθώς και για τον σκοπό της αποφυγής του κατακερματισμού της εσωτερικής αγοράς όσον αφορά τα σχήματα πιστοποίησης της κυβερνοασφάλειας στην Ένωση.»·

2) Το άρθρο 2 τροποποιείται ως εξής:

α) τα σημεία 9, 10 και 11 αντικαθίστανται από το ακόλουθο κείμενο:

«9) “ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας”: πλήρες σύνολο κανόνων, τεχνικών απαιτήσεων, προτύπων και διαδικασιών που θεσπίζονται σε επίπεδο Ένωσης και που εφαρμόζονται στην πιστοποίηση ή την αξιολόγηση της συμμόρφωσης συγκεκριμένων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας,

«10) “εθνικό σχήμα πιστοποίησης της κυβερνοασφάλειας”: πλήρες σύνολο κανόνων, τεχνικών απαιτήσεων, προτύπων και διαδικασιών που έχουν αναπτυχθεί και εγκριθεί από εθνική δημόσια αρχή και που εφαρμόζονται για την πιστοποίηση ή την αξιολόγηση της συμμόρφωσης των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ και διαχειριζόμενων υπηρεσιών ασφάλειας που εμπίπτουν στο πεδίο εφαρμογής του συγκεκριμένου σχήματος,

11) “ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας”: έγγραφο το οποίο εκδίδεται από τον αρμόδιο οργανισμό και βεβαιώνει ότι ένα συγκεκριμένο προϊόν ΤΠΕ, μια συγκεκριμένη υπηρεσία ΤΠΕ, διαδικασία ΤΠΕ ή διαχειριζόμενη υπηρεσία ασφάλειας έχει αξιολογηθεί ως προς τη

συμμόρφωση με συγκεκριμένες απαιτήσεις ασφαλείας που προβλέπει ένα ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας,»·

β) προστίθεται το ακόλουθο σημείο:

«14α)“διαχειριζόμενη υπηρεσία ασφάλειας”: υπηρεσία ***που παρέχεται σε τρίτο και*** που συνίσταται στην εκτέλεση ή την παροχή βοήθειας ***ή συμβουλών*** για δραστηριότητες που σχετίζονται με τη διαχείριση κινδύνων κυβερνοασφάλειας, ***συμπεριλαμβανομένων του χειρισμού περιστατικών,*** των δοκιμών διείσδυσης, των ελέγχων ασφάλειας και της παροχής συμβουλών,»·

γ) τα σημεία 20, 21 και 22 αντικαθίστανται από το ακόλουθο κείμενο:

«20) “τεχνικές προδιαγραφές”: έγγραφο με το οποίο ορίζονται οι τεχνικές απαιτήσεις που πρέπει να πληρούνται από προϊόν ΤΠΕ, υπηρεσία ΤΠΕ, διαδικασία ΤΠΕ ή διαχειριζόμενη υπηρεσία ασφάλειας· ή οι σχετικές με αυτά διαδικασίες αξιολόγησης της συμμόρφωσης,

21) “επίπεδο διασφάλισης”: η βάση για την εμπιστοσύνη ότι ένα προϊόν ΤΠΕ, μια υπηρεσία ΤΠΕ, μια διαδικασία ΤΠΕ ή μια διαχειριζόμενη υπηρεσία ασφάλειας πληροί τις απαιτήσεις ασφαλείας συγκεκριμένου ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας, το οποίο δείχνει το επίπεδο στο οποίο έχει αξιολογηθεί ένα προϊόν ΤΠΕ, μια υπηρεσία ΤΠΕ, μια διαδικασία ΤΠΕ ή μια διαχειριζόμενη υπηρεσία ασφάλειας αλλά δεν μετρά από μόνο του την ασφάλεια του σχετικού προϊόντος ΤΠΕ, υπηρεσίας ΤΠΕ, διαδικασίας ΤΠΕ ή διαχειριζόμενης υπηρεσίας ασφάλειας,

22) “αυτοαξιολόγηση της συμμόρφωσης”: ενέργεια που πραγματοποιείται από κατασκευαστή ή πάροχο προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας, η οποία αξιολογεί αν τα εν λόγω προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ ή διαχειριζόμενες υπηρεσίες ασφάλειας πληρούν τις απαιτήσεις συγκεκριμένου ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας.»·

3) το άρθρο 4 παράγραφος 6 αντικαθίσταται από το ακόλουθο κείμενο:

«6. Ο ENISA προάγει τη χρήση της ευρωπαϊκής πιστοποίησης της κυβερνοασφάλειας προκειμένου να αποφευχθεί ο κατακερματισμός της εσωτερικής αγοράς. Ο ENISA συμβάλλει στη θέσπιση και τη διατήρηση ενός ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας σύμφωνα με τον τίτλο ΙΙΙ του παρόντος κανονισμού, προκειμένου να αυξηθεί η διαφάνεια της κυβερνοασφάλειας των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας και, επομένως, να ενισχυθεί η εμπιστοσύνη στην ψηφιακή εσωτερική αγορά και η ανταγωνιστικότητά της.»·

4) το άρθρο 8 τροποποιείται ως εξής:

α) η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Ο ENISA υποστηρίζει και προάγει τη χάραξη και την εφαρμογή της πολιτικής της Ένωσης για την πιστοποίηση της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας, όπως καθορίζονται στον τίτλο ΙΙΙ του παρόντος κανονισμού:

α) παρακολουθώντας σε συνεχή βάση τις εξελίξεις σε σχετικούς τομείς προτυποποίησης και συνιστώντας κατάλληλες τεχνικές προδιαγραφές για χρήση στην ανάπτυξη ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας δυνάμει του άρθρου 54 παράγραφος 1 στοιχείο γ) σε περιπτώσεις στις οποίες δεν υπάρχουν διαθέσιμα πρότυπα,

β) επεξεργαζόμενος υποψήφια ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας (στο εξής: υποψήφια σχήματα) για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας σύμφωνα με το άρθρο 49,

γ) αξιολογώντας τα εγκριθέντα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας σύμφωνα με το άρθρο 49 παράγραφος 8,

δ) συμμετέχοντας σε αξιολογήσεις από ομοτίμους δυνάμει του άρθρου 59 παράγραφος 4,

ε) επικουρώντας την Επιτροπή, μέσω της παροχής της γραμματειακής

υποστήριξης στην ΕΟΠΙΚ δυνάμει του άρθρου 62 παράγραφος 5.»·

β) η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. Ο ENISA συντάσσει και δημοσιεύει κατευθυντήριες γραμμές και αναπτύσσει ορθές πρακτικές, όσον αφορά τις απαιτήσεις κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας, σε συνεργασία με τις εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας και με τον κλάδο, με τρόπο επίσημο και δομημένο και με διαφάνεια.»·

γ) η παράγραφος 5 αντικαθίσταται από το ακόλουθο κείμενο:

«5. Ο ENISA διευκολύνει την καθιέρωση και χρήση ευρωπαϊκών και διεθνών προτύπων για τη διαχείριση κινδύνου και την ασφάλεια των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας.»·

5) στο άρθρο 46, οι παράγραφοι 1 και 2 αντικαθίστανται από το ακόλουθο κείμενο:

«1. Το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας θεσπίζεται με στόχο να βελτιωθούν οι συνθήκες για τη λειτουργία της εσωτερικής αγοράς μέσω αναβάθμισης του επιπέδου κυβερνοασφάλειας εντός της Ένωσης και επιτρέποντας εναρμονισμένη προσέγγιση, σε επίπεδο Ένωσης, των ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας, με απώτερο στόχο τη δημιουργία ψηφιακής ενιαίας αγοράς για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας.

2. Το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας προβλέπει μηχανισμό για τη θέσπιση ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας. Βεβαιώνει ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ που έχουν αξιολογηθεί σύμφωνα με τα εν λόγω σχήματα συμμορφώνονται με συγκεκριμένες απαιτήσεις ασφάλειας με σκοπό να διαφυλάσσεται η διαθεσιμότητα, η γνησιότητα, η ακεραιότητα και η εμπιστευτικότητα αποθηκευμένων ή διαβιβαζόμενων ή επεξεργασμένων δεδομένων ή των σχετικών λειτουργιών ή υπηρεσιών που παρέχονται ή είναι προσβάσιμες μέσω των εν λόγω προϊόντων, υπηρεσιών και διαδικασιών σε

όλη τη διάρκεια του κύκλου ζωής τους. Επιπλέον, βεβαιώνει ότι οι διαχειριζόμενες υπηρεσίες ασφάλειας που έχουν αξιολογηθεί σύμφωνα με τα εν λόγω σχήματα συμμορφώνονται με συγκεκριμένες απαιτήσεις ασφάλειας με σκοπό την προστασία της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων, τα οποία είναι προσβάσιμα, υποβάλλονται σε επεξεργασία, αποθηκεύονται ή διαβιβάζονται σε σχέση με την παροχή των εν λόγω υπηρεσιών, και ότι οι εν λόγω υπηρεσίες παρέχονται συνεχώς με την απαιτούμενη επάρκεια, εμπειρογνωσία και πείρα από προσωπικό με πολύ υψηλό επίπεδο σχετικών τεχνικών γνώσεων και επαγγελματικής ακεραιότητας.»·

6) στο άρθρο 47, οι παράγραφοι 2 και 3 αντικαθίστανται από το ακόλουθο κείμενο:

«2. Το κυλιόμενο πρόγραμμα εργασίας της Ένωσης περιλαμβάνει ειδικότερα κατάλογο των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ ή των κατηγοριών τους, καθώς και των διαχειριζόμενων υπηρεσιών ασφάλειας, που μπορούν να έχουν όφελος από τη συμπερίληψή τους στο πεδίο εφαρμογής ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας. ***Στο πλαίσιο αυτό, η Επιτροπή μπορεί να περιλαμβάνει ενδελεχή αξιολόγηση των υφιστάμενων διαδρομών κατάρτισης για τη γεφύρωση των ελλείψεων δεξιοτήτων που έχουν εντοπιστεί, καθώς και κατάλογο προτάσεων για την αντιμετώπιση των αναγκών των ειδικευμένων εργαζομένων και των ειδών δεξιοτήτων.***

3. Η προσθήκη συγκεκριμένων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ ή κατηγοριών τους, ή διαχειριζόμενων υπηρεσιών ασφάλειας, στο κυλιόμενο πρόγραμμα εργασίας της Ένωσης αιτιολογείται βάσει ενός ή περισσότερων από τους ακόλουθους λόγους:

α) της διαθεσιμότητας και της ανάπτυξης των εθνικών σχημάτων πιστοποίησης της κυβερνοασφάλειας που καλύπτουν συγκεκριμένη κατηγορία προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας και ιδίως όσον αφορά τον κίνδυνο κατακερματισμού,

β) του σχετικού δικαίου ή πολιτικής της Ένωσης ή του σχετικού δικαίου ή

πολιτικής κράτους μέλους,

γ) της ζήτησης στην αγορά,

γα) των τεχνολογικών εξελίξεων και της διαθεσιμότητας και ανάπτυξης διεθνών συστημάτων πιστοποίησης της κυβερνοασφάλειας και διεθνών και βιομηχανικών προτύπων.

δ) των εξελίξεων όσον αφορά τις κυβερνοαπειλές,

ε) αιτήματος για την επεξεργασία συγκεκριμένου υποψήφιου ευρωπαϊκού σχήματος πιστοποίησης από την ΕΟΠΙΚ.»,

7) Το άρθρο 49 ***τροποποιείται ως εξής***:

α) η παράγραφος 7 αντικαθίσταται από το ακόλουθο κείμενο:

«7. Η Επιτροπή, με βάση το υποψήφιο σχήμα που προετοιμάζει ο ENISA, ***εξουσιοδοτείται να εκδίδει κατ' εξουσιοδότηση*** πράξεις ***σύμφωνα με το άρθρο 65α, οι οποίες συμπληρώνουν τον παρόντα κανονισμό προβλέποντας*** ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας, το οποίο πληροί τις απαιτήσεις των άρθρων 51, 52 και 54***.»,***

β) προστίθεται η ακόλουθη παράγραφος:

«7α. Πριν από την έκδοση των εν λόγω κατ' εξουσιοδότηση πράξεων, η Επιτροπή, σε συνεργασία με τον ENISA, διενεργεί και δημοσιεύει εκτίμηση επιπτώσεων του προτεινόμενου ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας. Κατά την εκπόνηση της εκτίμησης επιπτώσεων, η Επιτροπή διενεργεί δημόσιες διαβουλεύσεις και συμβουλεύεται την ομάδα συμφεροντούχων για την πιστοποίηση της κυβερνοασφάλειας (SCCG) και την ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας (ECCG).»,

8) το άρθρο 51 τροποποιείται ως εξής:

α) ο τίτλος αντικαθίσταται από το ακόλουθο κείμενο:

«Στόχοι ασφάλειας των ευρωπαϊκών σχημάτων πιστοποίησης της

κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ»

β) η εισαγωγική περίοδος αντικαθίσταται από το ακόλουθο κείμενο:

«Ένα ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ ή διαδικασίες ΤΠΕ σχεδιάζεται με τέτοιο τρόπο ώστε να επιτυγχάνει, κατά περίπτωση, τουλάχιστον τους ακόλουθους στόχους ασφάλειας:»**,**

9) προστίθεται το ακόλουθο άρθρο:

*«*Άρθρο 51α Στόχοι ασφάλειας των ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας για τις διαχειριζόμενες υπηρεσίες ασφάλειας

Ένα ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας για διαχειριζόμενες υπηρεσίες ασφάλειας σχεδιάζεται με τέτοιο τρόπο ώστε να επιτυγχάνει, κατά περίπτωση, τουλάχιστον τους ακόλουθους στόχους ασφάλειας:

α) διασφαλίζει ότι οι διαχειριζόμενες υπηρεσίες ασφάλειας παρέχονται με την απαιτούμενη επάρκεια, εμπειρογνωσία και πείρα, μεταξύ άλλων ότι το προσωπικό που είναι επιφορτισμένο με την παροχή των υπηρεσιών αυτών διαθέτει πολύ υψηλό επίπεδο τεχνικών γνώσεων και ικανοτήτων στον συγκεκριμένο τομέα, επαρκή και κατάλληλη πείρα, καθώς και το υψηλότερο επίπεδο επαγγελματικής ακεραιότητας,

β) διασφαλίζει ότι ο πάροχος εφαρμόζει κατάλληλες εσωτερικές διαδικασίες που εξασφαλίζουν ότι το επίπεδο ποιότητας των παρεχόμενων διαχειριζόμενων υπηρεσιών ασφάλειας είναι πάντοτε πολύ υψηλό,

γ) προστατεύει τα δεδομένα τα οποία είναι προσβάσιμα, αποθηκεύονται, διαβιβάζονται ή αποτελούν με άλλο τρόπο αντικείμενο επεξεργασίας σε σχέση με την παροχή διαχειριζόμενων υπηρεσιών ασφαλείας από τυχαία ή μη εγκεκριμένη πρόσβαση, αποθήκευση, κοινοποίηση, καταστροφή, άλλη επεξεργασία, ή απώλεια ή αλλοίωση ή έλλειψη διαθεσιμότητας,

δ) διασφαλίζει την έγκαιρη αποκατάσταση της διαθεσιμότητας και της πρόσβασης σε δεδομένα, υπηρεσίες και λειτουργίες σε περίπτωση φυσικών ή τεχνικών συμβάντων,

ε) διασφαλίζει ότι εγκεκριμένα άτομα, προγράμματα ή μηχανήματα μπορούν να έχουν πρόσβαση σε δεδομένα, υπηρεσίες ή λειτουργίες που καλύπτονται από το δικαίωμα πρόσβασης που τους παρέχεται,

στ) καταγράφει και παρέχει τη δυνατότητα προσδιορισμού των δεδομένων, των υπηρεσιών ή των λειτουργιών στα οποία υπήρξε πρόσβαση, τα οποία χρησιμοποιήθηκαν ή αποτέλεσαν με άλλο τρόπο αντικείμενο επεξεργασίας καθώς και τις χρονικές στιγμές κατά τις οποίες έλαβαν χώρα τα παραπάνω και από ποιον,

ζ) διασφαλίζει ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ που αναπτύσσονται κατά την παροχή των διαχειριζόμενων υπηρεσιών ασφάλειας είναι εξ ορισμού και εκ σχεδιασμού ασφαλή ***και παρέχονται με επικαιροποιημένο λογισμικό και υλισμικό,*** δεν περιέχουν γνωστά τρωτά σημεία και περιλαμβάνουν τις τελευταίες επικαιροποιήσεις ασφάλειας.»

10) το άρθρο 52 τροποποιείται ως εξής:

α) η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Ένα ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας μπορεί να προσδιορίζει ένα ή περισσότερα από τα ακόλουθα επίπεδα διασφάλισης για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας: “βασικό”, “σημαντικό” ή “υψηλό”. Το επίπεδο διασφάλισης είναι ανάλογο του επιπέδου του κινδύνου ο οποίος συνδέεται με την προβλεπόμενη χρήση του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ, της διαδικασίας ΤΠΕ ή της διαχειριζόμενης υπηρεσίας ασφάλειας από άποψη πιθανότητας και αντικτύπου ενός συμβάντος.»·

β) η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. Οι απαιτήσεις ασφάλειας που αντιστοιχούν σε κάθε επίπεδο διασφάλισης παρέχονται στο σχετικό ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας, συμπεριλαμβανομένων των αντίστοιχων λειτουργιών ασφάλειας και της αντίστοιχης αυστηρότητας και βάθους της αξιολόγησης στην οποία θα υποβληθεί το προϊόν ΤΠΕ, η υπηρεσία ΤΠΕ, η διαδικασία ΤΠΕ ή η διαχειριζόμενη υπηρεσία ασφάλειας.»·

γ) οι παράγραφοι 5, 6 και 7 αντικαθίστανται από το ακόλουθο κείμενο:

«5. Ένα ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας ή μία δήλωση συμμόρφωσης ΕΕ που αναφέρεται σε "βασικό" επίπεδο διασφάλισης παρέχει τη διασφάλιση ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ, οι διαδικασίες ΤΠΕ και οι διαχειριζόμενες υπηρεσίες ασφάλειας για τα οποία εκδόθηκε το εν λόγω πιστοποιητικό ή η εν λόγω δήλωση συμμόρφωσης ΕΕ πληρούν τις αντίστοιχες απαιτήσεις ασφάλειας, συμπεριλαμβανομένων των λειτουργιών ασφάλειας, και ότι έχουν αξιολογηθεί σε επίπεδο με σκοπό την ελαχιστοποίηση των γνωστών βασικών κινδύνων των συμβάντων και των κυβερνοεπιθέσεων. Οι δραστηριότητες αξιολόγησης που πρόκειται να διεξαχθούν περιλαμβάνουν τουλάχιστον επανεξέταση της τεχνικής τεκμηρίωσης. Εφόσον δεν είναι κατάλληλη τέτοια επανεξέταση, διεξάγονται υποκατάστατες δραστηριότητες αξιολόγησης με ισοδύναμο αποτέλεσμα.

6. Ένα ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας που αναφέρεται σε "σημαντικό" επίπεδο διασφάλισης παρέχει τη διασφάλιση ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ, οι διαδικασίες ΤΠΕ και οι διαχειριζόμενες υπηρεσίες ασφάλειας για τα οποία εκδόθηκε το εν λόγω πιστοποιητικό πληρούν τις αντίστοιχες απαιτήσεις ασφάλειας, συμπεριλαμβανομένων των λειτουργιών ασφάλειας, και ότι έχουν αξιολογηθεί σε επίπεδο με σκοπό την ελαχιστοποίηση των γνωστών κινδύνων κυβερνοασφάλειας και του κινδύνου συμβάντων και κυβερνοεπιθέσεων που πραγματοποιούνται από δράστες με περιορισμένες δεξιότητες και πόρους. Οι δραστηριότητες αξιολόγησης που πρόκειται να διεξαχθούν περιλαμβάνουν τουλάχιστον τα ακόλουθα: επανεξέταση για να καταδειχθεί η απουσία δημοσίως γνωστών τρωτών σημείων και δοκιμές για να αποδειχθεί ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ, οι διαδικασίες ΤΠΕ ή οι διαχειριζόμενες υπηρεσίες ασφάλειας εφαρμόζουν ορθά τις απαραίτητες λειτουργίες ασφάλειας. Εφόσον οποιεσδήποτε τέτοιες δραστηριότητες αξιολόγησης δεν είναι κατάλληλες, διεξάγονται υποκατάστατες δραστηριότητες αξιολόγησης με ισοδύναμο αποτέλεσμα.

7. Ένα ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας που αναφέρεται σε "υψηλό" επίπεδο διασφάλισης παρέχει τη διασφάλιση ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ, οι διαδικασίες ΤΠΕ και οι διαχειριζόμενες υπηρεσίες ασφάλειας για τα οποία εκδόθηκε το εν λόγω πιστοποιητικό πληρούν τις αντίστοιχες απαιτήσεις ασφάλειας, συμπεριλαμβανομένων των λειτουργιών ασφάλειας, και ότι έχουν αξιολογηθεί σε επίπεδο με σκοπό την ελαχιστοποίηση του κινδύνου κυβερνοεπιθέσεων προηγμένης τεχνολογίας που πραγματοποιούνται από δράστες με σημαντικές δεξιότητες και πόρους. Οι δραστηριότητες αξιολόγησης που πρόκειται να διεξαχθούν περιλαμβάνουν τουλάχιστον τα ακόλουθα: επανεξέταση για να καταδειχθεί η απουσία δημοσίως γνωστών τρωτών σημείων, δοκιμές για να αποδειχθεί ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ, οι διαδικασίες ΤΠΕ ή οι διαχειριζόμενες υπηρεσίες ασφάλειας εφαρμόζουν ορθά τις απαραίτητες λειτουργίες ασφάλειας με την πλέον προηγμένη τεχνολογία, και αξιολόγηση της αντοχής τους σε ειδικευμένους επιτιθέμενους, με τη χρήση δοκιμών διείσδυσης. Εφόσον οποιεσδήποτε τέτοιες δραστηριότητες αξιολόγησης δεν είναι κατάλληλες, διεξάγονται υποκατάστατες δραστηριότητες αξιολόγησης με ισοδύναμο αποτέλεσμα.»·

11) στο άρθρο 53, οι παράγραφοι 1, 2 και 3 αντικαθίστανται από το ακόλουθο κείμενο:

«1. Ένα ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας μπορεί να επιτρέπει την αυτοαξιολόγηση της συμμόρφωσης υπό την αποκλειστική ευθύνη του κατασκευαστή ή του παρόχου προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας. Η αυτοαξιολόγηση της συμμόρφωσης επιτρέπεται μόνο σχετικά με προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας χαμηλού κινδύνου που αντιστοιχούν σε "βασικό" επίπεδο διασφάλισης.

2. Ο κατασκευαστής ή ο πάροχος προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας μπορεί να εκδώσει δήλωση συμμόρφωσης ΕΕ στην οποία να αναφέρεται ότι έχει καταδειχθεί η εκπλήρωση των απαιτήσεων που ορίζονται στο σχήμα. Με την έκδοση της εν

λόγω δήλωσης, ο κατασκευαστής ή ο πάροχος προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας αναλαμβάνει την ευθύνη για τη συμμόρφωση του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ, της διαδικασίας ΤΠΕ ή της διαχειριζόμενης υπηρεσίας ασφάλειας με τις απαιτήσεις που ορίζονται στο εν λόγω σχήμα.

3. Ο κατασκευαστής ή ο πάροχος προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας καθιστά τη δήλωση συμμόρφωσης ΕΕ, την τεχνική τεκμηρίωση και όλες τις άλλες σχετικές πληροφορίες που αφορούν τη συμμόρφωση των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ ή των διαχειριζόμενων υπηρεσιών ασφάλειας με το σχήμα διαθέσιμα στην εθνική αρχή πιστοποίησης της κυβερνοασφάλειας που αναφέρεται στο άρθρο 58 για περίοδο που καθορίζεται στο αντίστοιχο ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας. Αντίγραφο της δήλωσης συμμόρφωσης ΕΕ υποβάλλεται στην εθνική αρχή πιστοποίησης της κυβερνοασφάλειας και στον ENISA.»·

12) στο άρθρο 54, η παράγραφος 1 τροποποιείται ως εξής:

α) το στοιχείο α) αντικαθίσταται από το ακόλουθο κείμενο:

«α) το αντικείμενο και το πεδίο εφαρμογής του ευρωπαϊκού σχήματος πιστοποίησης, συμπεριλαμβανομένων του τύπου ή των κατηγοριών των καλυπτόμενων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ και διαχειριζόμενων υπηρεσιών ασφάλειας,»·

β) το στοιχείο ι) αντικαθίσταται από το ακόλουθο κείμενο:

«ι) τους κανόνες παρακολούθησης της συμμόρφωσης των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας με τις απαιτήσεις των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας ή των δηλώσεων συμμόρφωσης ΕΕ, συμπεριλαμβανομένων των μηχανισμών για την κατάδειξη της συνεχούς συμμόρφωσης με τις συγκεκριμένες απαιτήσεις της κυβερνοασφάλειας,»·

γ) το στοιχείο ιβ) αντικαθίσταται από το ακόλουθο κείμενο:

«ιβ) τους κανόνες σχετικά με τις συνέπειες όσον αφορά προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας που έχουν πιστοποιηθεί ή για τα οποία έχει εκδοθεί δήλωση συμμόρφωσης ΕΕ τα οποία όμως δεν συμμορφώνονται προς τις απαιτήσεις του σχήματος,»·

δ) το στοιχείο ιε) αντικαθίσταται από το ακόλουθο κείμενο:

«ιε) τον προσδιορισμό εθνικών ή διεθνών σχημάτων πιστοποίησης της κυβερνοασφάλειας που καλύπτουν τον ίδιο τύπο ή τις ίδιες κατηγορίες προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ και διαχειριζόμενων υπηρεσιών ασφάλειας απαιτήσεις ασφάλειας, κριτήρια και μεθόδους αξιολόγησης και επίπεδα διασφάλισης,»·

ε) το στοιχείο ιζ) αντικαθίσταται από το ακόλουθο κείμενο:

«ιζ) την περίοδο διαθεσιμότητας της δήλωσης συμμόρφωσης ΕΕ, την τεχνική τεκμηρίωση και όλες τις άλλες σχετικές πληροφορίες που πρέπει να καταστούν διαθέσιμες από τον κατασκευαστή ή τον πάροχο προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας,»·

13) το άρθρο 56 τροποποιείται ως εξής:

α) η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ, οι διαδικασίες ΤΠΕ και οι διαχειριζόμενες υπηρεσίες ασφάλειας που έχουν πιστοποιηθεί στο πλαίσιο ενός ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας που εγκρίνεται δυνάμει του άρθρου 49 τεκμαίρονται ότι πληρούν τις απαιτήσεις ενός τέτοιου σχήματος.»·

β) η παράγραφος 3 τροποποιείται ως εξής:

i) το πρώτο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«Η Επιτροπή αξιολογεί τακτικά την απόδοση και τη χρήση των εγκριθέντων ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας, καθώς και αν συγκεκριμένα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας πρόκειται να καταστούν

υποχρεωτικά μέσω συναφούς ενωσιακού δικαίου προκειμένου να διασφαλίζεται επαρκές επίπεδο κυβερνοασφάλειας των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας στην Ένωση και να βελτιωθεί η λειτουργία της εσωτερικής αγοράς. Η πρώτη τέτοια αξιολόγηση διενεργείται έως τις 31 Δεκεμβρίου 2023 και οι ακόλουθες αξιολογήσεις διενεργούνται τουλάχιστον ανά διετία εν συνεχεία. Η Επιτροπή, βασιζόμενη στα αποτελέσματα της εν λόγω αξιολόγησης, προσδιορίζει τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ, τις διαδικασίες ΤΠΕ και τις διαχειριζόμενες υπηρεσίες ασφάλειας που καλύπτονται από ήδη υφιστάμενο σχήμα πιστοποίησης και τα οποία πρέπει να καλυφθούν από υποχρεωτικό σχήμα πιστοποίησης.»·

ii) το τρίτο εδάφιο τροποποιείται ως εξής:

αα) το στοιχείο α) αντικαθίσταται από το ακόλουθο κείμενο:

«α) λαμβάνει υπόψη τον αντίκτυπο των μέτρων στους κατασκευαστές ή τους παρόχους των εν λόγω προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας και στους χρήστες από άποψη κόστους των εν λόγω μέτρων και τα κοινωνικά ή οικονομικά οφέλη που προκύπτουν από το αναμενόμενο βελτιωμένο επίπεδο ασφάλειας για τα στοχευόμενα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ, τις διαδικασίες ΤΠΕ ή τις διαχειριζόμενες υπηρεσίες ασφάλειας,»·

ββ) το στοιχείο δ) αντικαθίσταται από το ακόλουθο κείμενο:

«δ) λαμβάνει υπόψη τις προθεσμίες εφαρμογής, τα μεταβατικά μέτρα και χρονικά διαστήματα, ιδίως όσον αφορά τις πιθανές συνέπειες του μέτρου για τους κατασκευαστές ή παρόχους προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας, συμπεριλαμβανομένων των ***συγκεκριμένων συμφερόντων και αναγκών των πολύ μικρών, των μικρών και των***

***μεσαίων επιχειρήσεων*,»·**

iii) προστίθεται το ακόλουθο εδάφιο:

«Όσον αφορά το τρίτο εδάφιο στοιχείο δ) του παρόντος άρθρου, η Επιτροπή εξασφαλίζει κατάλληλη χρηματοδοτική στήριξη στο κανονιστικό πλαίσιο των υφιστάμενων προγραμμάτων της Ένωσης, ιδίως προκειμένου να μειωθεί η οικονομική επιβάρυνση των πολύ μικρών επιχειρήσεων και των ΜΜΕ, συμπεριλαμβανομένων των νεοφυών επιχειρήσεων που δραστηριοποιούνται στον τομέα των διαχειριζόμενων υπηρεσιών ασφάλειας.»·

γ) οι παράγραφοι 7 και 8 αντικαθίστανται από το ακόλουθο κείμενο:

«7. Το φυσικό ή νομικό πρόσωπο που υποβάλλει τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ, τις διαδικασίες ΤΠΕ ή τις διαχειριζόμενες υπηρεσίες ασφάλειας προς πιστοποίηση θέτει στη διάθεση της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας που αναφέρεται στο άρθρο 58, σε περίπτωση που η εν λόγω αρχή είναι ο οργανισμός που εκδίδει το ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας, ή του οργανισμού αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 60 όλες τις πληροφορίες που απαιτούνται για τη διενέργεια της πιστοποίησης.

8. Ο κάτοχος ευρωπαϊκού πιστοποιητικού κυβερνοασφάλειας ενημερώνει την αρχή ή τον οργανισμό που αναφέρεται στην παράγραφο 7 για τυχόν τρωτά σημεία ή παρατυπίες που εντοπίστηκαν σε μεταγενέστερο στάδιο σχετικά με την ασφάλεια του πιστοποιημένου προϊόντος ΤΠΕ, υπηρεσίας ΤΠΕ, διαδικασίας ΤΠΕ ή διαχειριζόμενης υπηρεσίας ασφάλειας και μπορεί να έχουν αντίκτυπο στη συμμόρφωσή του με τις απαιτήσεις σχετικά με την πιστοποίηση. Η εν λόγω αρχή ή οργανισμός διαβιβάζει τις εν λόγω πληροφορίες χωρίς αδικαιολόγητη καθυστέρηση στην ενδιαφερόμενη εθνική αρχή πιστοποίησης της κυβερνοασφάλειας.»

14) στο άρθρο 57, οι παράγραφοι 1 και 2 αντικαθίστανται από το ακόλουθο κείμενο:

«1. Με την επιφύλαξη της παραγράφου 3 του παρόντος άρθρου, τα εθνικά σχήματα πιστοποίησης της κυβερνοασφάλειας και οι σχετικές διαδικασίες για τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ, τις διαδικασίες ΤΠΕ και τις

διαχειριζόμενες υπηρεσίες ασφάλειας που καλύπτονται από ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας παύουν να παράγουν αποτελέσματα από την ημερομηνία που ορίζεται στην ***κατ' εξουσιοδότηση*** πράξη που εκδίδεται σύμφωνα με το άρθρο 49 παράγραφος 7. Τα εθνικά σχήματα πιστοποίησης της κυβερνοασφάλειας και οι σχετικές διαδικασίες για τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ, τις διαδικασίες ΤΠΕ και τις διαχειριζόμενες υπηρεσίες ασφάλειας που δεν καλύπτονται από ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας εξακολουθούν να παράγουν αποτελέσματα.

2. Τα κράτη μέλη δεν θεσπίζουν νέα εθνικά σχήματα πιστοποίησης της κυβερνοασφάλειας για τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ, τις διαδικασίες ΤΠΕ και τις διαχειριζόμενες υπηρεσίες ασφάλειας που καλύπτονται ήδη από ισχύον ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας.»·

15) το άρθρο 58 τροποποιείται ως εξής:

α) η παράγραφος 7 τροποποιείται ως εξής:

i) τα στοιχεία α) και β) αντικαθίστανται από το ακόλουθο κείμενο:

«α) εποπτεύουν και μεριμνούν για την εφαρμογή των κανόνων που περιλαμβάνονται στα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας σύμφωνα με το άρθρο 54 παράγραφος 1 στοιχείο ι) για την παρακολούθηση της συμμόρφωσης των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας προς τις απαιτήσεις των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας που έχουν εκδοθεί στα αντίστοιχα εδάφη τους, σε συνεργασία με άλλες αρμόδιες αρχές εποπτείας της αγοράς,

β) παρακολουθούν τη συμμόρφωση με τις υποχρεώσεις των κατασκευαστών ή των παρόχων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας που είναι εγκατεστημένοι στα αντίστοιχα εδάφη τους και που διενεργούν αυτοαξιολόγηση συμμόρφωσης και επιβάλλουν την εφαρμογή των εν λόγω υποχρεώσεων και παρακολουθούν ιδίως τη συμμόρφωση με τις υποχρεώσεις των εν λόγω κατασκευαστών ή

παρόχων που προβλέπονται στο άρθρο 53 παράγραφοι 2 και 3 και στο αντίστοιχο ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας και επιβάλλουν την εφαρμογή των εν λόγω υποχρεώσεων,»·

ii) το στοιχείο η) αντικαθίσταται από το ακόλουθο κείμενο:

«η) συνεργάζονται με άλλες εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας ή άλλες δημόσιες αρχές, μεταξύ άλλων ανταλλάσσοντας πληροφορίες σχετικά με την πιθανή μη συμμόρφωση προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ και διαχειριζόμενων υπηρεσιών ασφάλειας με τις απαιτήσεις του παρόντος κανονισμού ή με τις απαιτήσεις συγκεκριμένων ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας, και»·

β) η παράγραφος 9 αντικαθίσταται από το ακόλουθο κείμενο:

«9. Οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας συνεργάζονται μεταξύ τους και με την Επιτροπή, ιδίως ανταλλάσσοντας πληροφορίες, εμπειρίες και ορθές πρακτικές όσον αφορά την πιστοποίηση της κυβερνοασφάλειας και τα τεχνικά ζητήματα που αφορούν την κυβερνοασφάλεια των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας.»·

16) στο άρθρο 59 παράγραφος 3, τα στοιχεία β) και γ) αντικαθίστανται από το ακόλουθο κείμενο:

«β) τις διαδικασίες για την εποπτεία και την επιβολή των κανόνων παρακολούθησης της συμμόρφωσης των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας με ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας δυνάμει του άρθρου 58 παράγραφος 7 στοιχείο α),

γ) τις διαδικασίες για την παρακολούθηση και την τήρηση των υποχρεώσεων των κατασκευαστών ή των παρόχων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας δυνάμει του άρθρου 58 παράγραφος 7 στοιχείο β),»

16α) προστίθεται το ακόλουθο άρθρο:

«Άρθρο 65α

Άσκηση των ανατιθέμενων αρμοδιοτήτων

1. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις υπό τους όρους του παρόντος άρθρου.

2. Η εξουσία έκδοσης των κατ' εξουσιοδότηση πράξεων κατά το άρθρο 49 παράγραφος 7 ανατίθεται στην Επιτροπή για περίοδο πέντε ετών από την ... [ημερομηνία έναρξης ισχύος του τροποποιημένου κανονισμού]. Η Επιτροπή συντάσσει έκθεση σχετικά με τις εξουσίες που της έχουν ανατεθεί το αργότερο εννέα μήνες πριν από τη λήξη της πενταετούς περιόδου. Η εξουσιοδότηση ανανεώνεται σιωπηρά για περιόδους ίδιας διάρκειας, εκτός αν το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο προβάλλει αντιρρήσεις το αργότερο τρεις μήνες πριν από τη λήξη της κάθε περιόδου.

3. Το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο μπορεί ανά πάσα στιγμή να ανακαλέσει την εξουσιοδότηση που αναφέρεται στο άρθρο 49 παράγραφος 7. Η απόφαση ανάκλησης περατώνει την εξουσιοδότηση που προσδιορίζεται στην εν λόγω απόφαση. Αρχίζει να ισχύει την επομένη της δημοσίευσης της απόφασης στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης ή σε μεταγενέστερη ημερομηνία που ορίζεται σε αυτή. Δεν θίγει το κύρος των κατ' εξουσιοδότηση πράξεων που ισχύουν ήδη.

4. Πριν από την έκδοση μιας κατ' εξουσιοδότηση πράξης, η Επιτροπή διεξάγει διαβουλεύσεις με εμπειρογνώμονες που ορίζουν τα κράτη μέλη σύμφωνα με τις αρχές της διοργανικής συμφωνίας της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου.

5. Μόλις εκδώσει μια κατ' εξουσιοδότηση πράξη, η Επιτροπή την κοινοποιεί ταυτόχρονα στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.

6. Κάθε κατ' εξουσιοδότηση πράξη που εκδίδεται δυνάμει του άρθρου 49 παράγραφος 7 αρχίζει να ισχύει μόνον εφόσον δεν διατυπωθούν αντιρρήσεις είτε από το Ευρωπαϊκό Κοινοβούλιο είτε από το Συμβούλιο εντός προθεσμίας δύο μηνών από την κοινοποίηση της πράξης στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ή εάν, πριν από τη λήξη της εν λόγω

προθεσμίας, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ενημερώσουν αμφότερα την Επιτροπή ότι δεν θα διατυπώσουν αντιρρήσεις. Η προθεσμία αυτή παρατείνεται κατά [δύο μήνες] κατόπιν πρωτοβουλίας του Ευρωπαϊκού Κοινοβουλίου ή του Συμβουλίου.·»

17) Το άρθρο 67 αντικαθίσταται από το ακόλουθο κείμενο:

«Άρθρο 67

Αξιολόγηση και επανεξέταση

1. Έως τις 28 Ιουνίου 2024 και στη συνέχεια ανά τριετία, η Επιτροπή εξετάζει τον αντίκτυπο, την αποτελεσματικότητα και την απόδοση του ENISA και των εργασιακών πρακτικών του, τη δυνατότητα για ενδεχόμενη τροποποίηση της εντολής του ENISA, και τις δημοσιονομικές επιπτώσεις οποιασδήποτε τέτοιας τροποποίησης. Στην αξιολόγηση λαμβάνονται υπόψη οι αντιδράσεις που έχουν παρασχεθεί στον ENISA σε σχέση με τις δραστηριότητές του. Σε περίπτωση που η Επιτροπή κρίνει ότι οι στόχοι, η εντολή και τα καθήκοντα που του έχουν ανατεθεί δεν δικαιολογούν πλέον τη συνέχιση της λειτουργίας του ENISA, η Επιτροπή μπορεί να εισηγηθεί την τροποποίηση του παρόντος κανονισμού ως προς τις διατάξεις που αφορούν τον ENISA.

2. Η αξιολόγηση εξετάζει τον αντίκτυπο, την αποτελεσματικότητα και την απόδοση των διατάξεων του τίτλου ΙΙΙ του παρόντος κανονισμού σε σχέση με τους στόχους αφενός της διασφάλισης επαρκούς επιπέδου κυβερνοασφάλειας των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ, των διαδικασιών ΤΠΕ και των διαχειριζόμενων υπηρεσιών ασφάλειας στην Ένωση και αφετέρου της βελτίωσης της λειτουργίας της εσωτερικής αγοράς,

3. Η αξιολόγηση εξετάζει επίσης:

α) την αποδοτικότητα και την αποτελεσματικότητα των διαδικασιών που οδηγούν στη διαβούλευση, την προετοιμασία και την έγκριση ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας, καθώς και τρόπους βελτίωσης και επιτάχυνσης των εν λόγω διαδικασιών·

β) κατά πόσον είναι απαραίτητες βασικές απαιτήσεις κυβερνοασφάλειας για την πρόσβαση στην εσωτερική αγορά, ώστε να αποφευχθεί η είσοδος προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ και διαχειριζόμενων υπηρεσιών ασφάλειας που δεν πληρούν τις βασικές απαιτήσεις κυβερνοασφάλειας στην αγορά της Ένωσης.

4. Έως τις 28 Ιουνίου 2024 και στη συνέχεια ανά τριετία, η Επιτροπή διαβιβάζει την έκθεση αξιολόγησης μαζί με τα συμπεράσματά της στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και το διοικητικό συμβούλιο. Τα συμπεράσματα της εν λόγω έκθεσης δημοσιοποιούνται.»

Άρθρο 2

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.

(τόπος), (ημερομηνία)

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Η Πρόεδρος	*Ο Πρόεδρος*

ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ

Η εισηγήτρια υποστηρίζει την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την τροποποίηση του κανονισμού (ΕΕ) 2019/8811 όσον αφορά τις διαχειριζόμενες υπηρεσίες ασφάλειας, κατανοώντας την ανάγκη για επικαιροποίηση και ενίσχυση των ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας μέσω της δυνατότητας να καλύπτουν σημαντικές και αναπτυσσόμενες υπηρεσίες του κλάδου. Λαμβάνοντας υπόψη ότι μεμονωμένα κράτη μέλη έχουν ήδη αρχίσει να θεσπίζουν σχήματα πιστοποίησης για διαχειριζόμενες υπηρεσίες ασφάλειας, η εισηγήτρια θεωρεί ότι η παρούσα τροποποίηση της πράξης για την κυβερνοασφάλεια έχει κρίσιμη σημασία για την πρόληψη σημαντικών αποκλίσεων στα εθνικά σχήματα οι οποίες θα μπορούσαν να συνεπάγονται κατακερματισμό της αγοράς, εις βάρος των οικονομικών και των στρατηγικών συμφερόντων της Ένωσης.

Στο πλαίσιο αυτό, επισημαίνεται ότι στόχος της παρούσας πρότασης είναι να συμπληρώσει την πράξη για την αλληλεγγύη στον κυβερνοχώρο. Ειδικότερα, η συγκεκριμένη επέκταση των ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας θα δώσει στις διαχειριζόμενες υπηρεσίες ασφάλειας —οι οποίες είναι το αντίστοιχο των «αξιόπιστων παρόχων» της πράξης για την αλληλεγγύη στον κυβερνοχώρο— τη δυνατότητα να διαδραματίσουν σημαντικό ρόλο στη μελλοντική εφεδρεία στον τομέα της κυβερνοασφάλειας σε επίπεδο Ένωσης. Ως εκ τούτου, η παρούσα πρόταση έχει επίσης μεγάλη σημασία για την προώθηση της ευρύτερης ικανότητας κυβερνοασφάλειας της Ένωσης, η οποία είναι απαραίτητη για την καταπολέμηση πιθανών απειλών σε μια διαρκώς μεταβαλλόμενη γεωπολιτική πραγματικότητα.

Εντός των ορίων της πρότασης της Επιτροπής, στόχος της εισηγήτριας είναι να ενοποιήσει και να προσδώσει περαιτέρω σαφήνεια στην παρούσα στοχευμένη τροποποίηση της πράξης για την κυβερνοασφάλεια. Ο στόχος αυτός αντικατοπτρίζεται στις αλλαγές που επιφέρει η εισηγήτρια στον ορισμό των διαχειριζόμενων υπηρεσιών ασφάλειας, με τις οποίες διευκρινίζεται ότι οι υπηρεσίες «ανατίθενται εξωτερικά», ενώ ταυτόχρονα αναλύεται περαιτέρω τι μπορεί να συμπεριληφθεί στον ορισμό. Οι τροπολογίες που κατατέθηκαν σχετικά με την αναγνώριση των διεθνών προτύπων κυβερνοασφάλειας αποσκοπούν στο να ενισχυθεί η εμπιστοσύνη και παράλληλα να αναπτυχθούν ολοκληρωμένοι κανόνες της ΕΕ.

Το παρόν σχέδιο έκθεσης δίνει μεγαλύτερη έμφαση στην αντιμετώπιση του χάσματος δεξιοτήτων και στη στήριξη των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων. Όσον αφορά το χάσμα δεξιοτήτων, οι κατατεθείσες τροπολογίες βασίζονται στην ήδη διαφαινόμενη ανάγκη για δεξιότητες στο σύστημα πιστοποίησης στον κυβερνοχώρο όσον αφορά «την απαιτούμενη επάρκεια, εμπειρογνωσία και πείρα από προσωπικό με πολύ υψηλό επίπεδο σχετικών τεχνικών γνώσεων και επαγγελματικής ακεραιότητας». Κατά την άποψη της εισηγήτριας, τα ευρωπαϊκά σχήματα πιστοποίησης, εκτός από το να προωθούν τη συνεργασία μεταξύ όλων των συμμετεχόντων φορέων, καθώς και μεταξύ των κρατών μελών, του ιδιωτικού τομέα, της πανεπιστημιακής κοινότητας και των ερευνητικών ιδρυμάτων, πρέπει να λειτουργήσουν καταλυτικά για τη χάραξη ενός νέου χάρτη πορείας για την κατάρτιση και την ενδυνάμωση του εργατικού δυναμικού, συλλέγοντας περισσότερα δεδομένα σχετικά με τις αναγκαίες δεξιότητες και συμβάλλοντας στην αντιμετώπιση του χάσματος μεταξύ των φύλων στους τομείς των θετικών επιστημών, της τεχνολογίας, της μηχανικής και των μαθηματικών.

Ταυτόχρονα, οι πολύ μικρές, οι μικρές και οι μεσαίες επιχειρήσεις, οι οποίες αποτελούν τη ραχοκοκαλιά της ευρωπαϊκής οικονομίας και ασφαλώς διαδραματίζουν θετικό ρόλο στον κλάδο της κυβερνοασφάλειας, θα πρέπει να λάβουν κατάλληλη χρηματοδοτική στήριξη στο κανονιστικό πλαίσιο των υφιστάμενων προγραμμάτων της Ένωσης για τη μείωση τυχόν δυσανάλογης οικονομικής επιβάρυνσής τους.

21.9.2023

ΕΠΙΣΤΟΛΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΕΣΩΤΕΡΙΚΗΣ ΑΓΟΡΑΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΚΑΤΑΝΑΛΩΤΩΝ

Κύριο Cristian-Silviu Buşoi
Πρόεδρο
Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας
ΒΡΥΞΕΛΛΕΣ

Θέμα: Γνωμοδότηση σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την τροποποίηση του κανονισμού (ΕΕ) 2019/881 όσον αφορά τις διαχειριζόμενες υπηρεσίες ασφάλειας (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Κύριε πρόεδρε,

Στο πλαίσιο της διεξαγόμενης διαδικασίας, η Επιτροπή Εσωτερικής Αγοράς και Προστασίας των Καταναλωτών ανέλαβε να υποβάλει γνωμοδότηση στην επιτροπή σας. Κατά τη συνεδρίασή της στις 23 Μαΐου 2023, αποφάσισε να διαβιβάσει την παρούσα γνωμοδότηση υπό μορφή επιστολής. Εξέτασε το ζήτημα κατά τη συνεδρίασή της στις 19 Σεπτεμβρίου 2023 και ενέκρινε τη γνωμοδότηση κατά την εν λόγω συνεδρίαση.

Κατά την εν λόγω συνεδρίαση[1], η επιτροπή αποφάσισε να καλέσει την Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας (ITRE), που είναι αρμόδια επί της ουσίας, να συμπεριλάβει στη νομοθετική της έκθεση τις ακόλουθες προτάσεις.

Με εξαιρετική εκτίμηση,

Anna Cavazzini

[1] Ήταν παρόντες κατά την τελική ψηφοφορία οι βουλευτές: Anna Cavazzini (πρόεδρος), Andrus Ansip (αντιπρόεδρος), Krzysztof Hetman (αντιπρόεδρος), Alex Agius Saliba, João Albuquerque, Pablo Arias Echeverría, Laura Ballarín Cereza, Alessandra Basso, Brando Benifei, Biljana Borzan, Vlad Marius Botoş, Deirdre Clune, Dita Charanzová, David Cormand, Carlo Fidanza, Malte Gallée, Sandro Gozi, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Marcel Kolaja, Andrey Kovatchev, Jean-Lin Lacapelle, Morten Løkkegaard, Beata Mazurek, Leszek Miller, Anne Sophie Pelletier, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein, Tom Vandenkendelaere, Kim Van Sparrentak.

ΠΡΟΤΑΣΕΙΣ

Η Επιτροπή Εσωτερικής Αγοράς και Προστασίας των Καταναλωτών καλεί την Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας, που είναι αρμόδια επί της ουσίας, να λάβει υπόψη της τις ακόλουθες προτάσεις:

Α. λαμβάνοντας υπόψη ότι η Επιτροπή δημοσίευσε, στις 18 Απριλίου 2023, νομοθετική πρόταση σχετικά με τις διαχειριζόμενες υπηρεσίες ασφάλειας[2], η οποία συνεπάγεται στοχευμένες τροποποιήσεις της πράξης της ΕΕ για την κυβερνοασφάλεια·

Β. λαμβάνοντας υπόψη ότι, όσον αφορά τη νομοθετική πρόταση για την πράξη της ΕΕ για την κυβερνοασφάλεια (2017/0225(COD))[3], η Επιτροπή Εσωτερικής Αγοράς και Προστασίας των Καταναλωτών (IMCO) υπέβαλε γνωμοδότηση, σύμφωνα με το πρώην άρθρο 54 του Κανονισμού, στην αρμόδια Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας (ITRE) με συντρέχουσες αρμοδιότητες όσον αφορά το πλαίσιο πιστοποίησης της κυβερνοασφάλειας, δεδομένης της σαφούς αρμοδιότητας της επιτροπής IMCO σε σχέση με τα συστήματα πιστοποίησης και, εν γένει, την τυποποίηση, την εποπτεία της αγοράς και την υλοποίηση της ψηφιακής ενιαίας αγοράς·

Γ. λαμβάνοντας υπόψη ότι η πράξη της ΕΕ για την κυβερνοασφάλεια[4] αποσκοπεί στην επίτευξη 1) υψηλού επιπέδου κυβερνοασφάλειας, κυβερνοανθεκτικότητας και εμπιστοσύνης στην ΕΕ μέσω του καθορισμού των στόχων, των καθηκόντων και των οργανωτικών θεμάτων για έναν ενισχυμένο και μετονομασμένο Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), με νέα μόνιμη εντολή, και 2) ενός πλαισίου για εθελοντικά ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας για προϊόντα, υπηρεσίες και διαδικασίες τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ)·

Δ. λαμβάνοντας υπόψη ότι οι προτεινόμενες στοχευμένες τροποποιήσεις αποσκοπούν στη συμπερίληψη των διαχειριζόμενων υπηρεσιών ασφάλειας στο πεδίο εφαρμογής της πράξης της ΕΕ για την κυβερνοασφάλεια και στην προσθήκη ορισμού για τις εν λόγω υπηρεσίες ο οποίος να ευθυγραμμίζεται στενά με τον ορισμό της οδηγίας NIS 2[5]· λαμβάνοντας υπόψη ότι οι τροποποιήσεις θα δώσουν στην Επιτροπή τη δυνατότητα, μέσω εκτελεστικών πράξεων, να εγκρίνει ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας για διαχειριζόμενες υπηρεσίες ασφάλειας, επιπλέον των προϊόντων, υπηρεσιών και διαδικασιών ΤΠΕ, που καλύπτονται ήδη από την πράξη της ΕΕ για την κυβερνοασφάλεια·

Ε. λαμβάνοντας υπόψη ότι οι διαχειριζόμενες υπηρεσίες ασφάλειας διαδραματίζουν ολοένα σημαντικότερο ρόλο στην πρόληψη και τον μετριασμό των περιστατικών στον τομέα της κυβερνοασφάλειας·

1. αναγνωρίζει ότι, στις 23 Μαΐου 2022[6], το Συμβούλιο ζήτησε να αυξηθεί το συνολικό επίπεδο κυβερνοασφάλειας στην ΕΕ, με τη διευκόλυνση της εμφάνισης και της

[2] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:52023PC0208
[3] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2017/0225(OLP)
[4] ΕΕ L 151 της 7.6.2019, σ. 15.
[5] ΕΕ L 333/810 της 27.12.2022.
[6] 9364/22

ανάπτυξης αξιόπιστων παρόχων υπηρεσιών κυβερνοασφάλειας· θεωρεί ότι, μεταξύ άλλων, ο πόλεμος στην Ουκρανία, το τρέχον γεωπολιτικό πλαίσιο και οι συνεχείς απειλές από καθεστώτα τρίτων χωρών, καθώς και μια συνεχώς αναπτυσσόμενη αγορά ψηφιακών τεχνολογιών και ο ψηφιακός μετασχηματισμός των διαδικασιών εν γένει, έχουν οδηγήσει στην ανάγκη για υψηλότερο επίπεδο κυβερνοασφάλειας στην ΕΕ και τα κράτη μέλη της· συνιστά στην Επιτροπή να λάβει προδραστικά μέτρα για τη στήριξη της ανάπτυξης αξιόπιστων παρόχων υπηρεσιών κυβερνοασφάλειας, όπως χρηματοδότηση για έρευνα και ανάπτυξη, προγράμματα κατάρτισης για την ανάπτυξη δεξιοτήτων κυβερνοασφάλειας, και κίνητρα για τις επιχειρήσεις ώστε να επενδύσουν στην κυβερνοασφάλεια· προτείνει να ενισχύσει η ΕΕ τη συνεργασία της με το NATO και άλλους διεθνείς εταίρους για την αντιμετώπιση κυβερνοαπειλών από καθεστώτα τρίτων χωρών, συμπεριλαμβανομένων της ανταλλαγής πληροφοριών σχετικά με απειλές, κοινών ασκήσεων και συντονισμένων αντιδράσεων σε κυβερνοεπιθέσεις·

2. τονίζει ότι η πιστοποίηση των διαχειριζόμενων υπηρεσιών ασφάλειας, με βάση αμερόληπτους κανόνες και κατ' αντιστοιχία προς τα ευρωπαϊκά και διεθνή πρότυπα, είναι απαραίτητη για την οικοδόμηση και τη διασφάλιση της εμπιστοσύνης στην ποιότητα των εν λόγω υπηρεσιών, ιδίως με στόχο την επίτευξη υψηλού επιπέδου προστασίας των καταναλωτών· σημειώνει ότι ορισμένα κράτη μέλη έχουν ήδη εγκρίνει συστήματα πιστοποίησης για διαχειριζόμενες υπηρεσίες ασφάλειας και ότι, επομένως, είναι σημαντικό να αποφευχθούν ο κατακερματισμός της εσωτερικής αγοράς και οι ασυνέπειες, που ενδέχεται να επηρεάσουν τον κλάδο και τις επιχειρήσεις κυβερνοασφάλειας, και να καταστεί δυνατή μια εναρμονισμένη προσέγγιση μέσω της δημιουργίας ενός ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας για τις εν λόγω υπηρεσίες· ζητεί το πλαίσιο πιστοποίησης της κυβερνοασφάλειας να ενσωματώσει τις βέλτιστες πρακτικές από τα υφιστάμενα εθνικά συστήματα πιστοποίησης και να αναπτυχθεί σε διαβούλευση με τους βασικούς ενδιαφερόμενους φορείς του κλάδου της κυβερνοασφάλειας·

3. τονίζει ότι οι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας σε τομείς όπως η αντιμετώπιση περιστατικών, οι δοκιμές διείσδυσης, οι έλεγχοι ασφάλειας και η παροχή συμβουλών, διαδραματίζουν σημαντικό ρόλο στην παροχή συνδρομής σε οντότητες που καταβάλλουν προσπάθειες για την πρόληψη, τον εντοπισμό και την αντιμετώπιση κυβερνοπεριστατικών ή την ανάκαμψη από αυτά· θεωρεί ότι, καθώς όλο και περισσότερες εταιρείες δυσκολεύονται να διατηρήσουν διάφορα σύνθετα συστήματα λογισμικού και διασυνδεδεμένα εταιρικά δίκτυα, βασίζονται κατ' ανάγκη σε παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας και, κατά συνέπεια, οι εν λόγω πάροχοι θα πρέπει να θεωρούνται ουσιώδες στοιχείο του οικοσυστήματος κυβερνοασφάλειας της ΕΕ· σημειώνει, ωστόσο, ότι οι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας έχουν αποτελέσει και οι ίδιοι στόχο κυβερνοεπιθέσεων και ενδέχεται να ενέχουν ιδιαίτερο κίνδυνο λόγω της στενής ενσωμάτωσής τους στις δραστηριότητες των πελατών τους·

4. υπενθυμίζει τη σημασία της οδηγίας NIS 2, που εγκρίθηκε πρόσφατα, όσον αφορά τη διασφάλιση υψηλότερου επιπέδου κυβερνοανθεκτικότητας σε ολόκληρη την Ένωση· ζητεί την ταχεία έγκριση και εφαρμογή εκτελεστικών πράξεων δυνάμει της εν λόγω οδηγίας, προκειμένου να διασφαλιστεί ότι οι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας συμμορφώνονται με τις απαιτήσεις της οδηγίας όσον αφορά τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας·

5. συνιστά οι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας να υποχρεούνται να τηρούν τα σχετικά πρότυπα κυβερνοασφάλειας και να υποβάλλονται σε τακτικές αξιολογήσεις, ώστε να διασφαλίζεται ότι τα συστήματά τους είναι ασφαλή για την προστασία όχι μόνο των ίδιων των παρόχων αλλά και των οντοτήτων που αυτοί εξυπηρετούν· θεωρεί ότι στις εν λόγω αξιολογήσεις θα πρέπει να αξιολογείται η συμμόρφωση των παρόχων με το πλαίσιο πιστοποίησης της κυβερνοασφάλειας σε επίπεδο ΕΕ και η ικανότητά τους να προστατεύουν τόσο τα συστήματά τους όσο και εκείνα των πελατών τους από κυβερνοαπειλές·

6. εκφράζει την ικανοποίησή του για τη νομοθετική πρόταση σχετικά με τις διαχειριζόμενες υπηρεσίες ασφάλειας, η οποία αποσκοπεί στη βελτίωση της ποιότητας των διαχειριζόμενων υπηρεσιών ασφάλειας και στην ενίσχυση της συγκρισιμότητάς τους προς όφελος της ορθής λειτουργίας της εσωτερικής αγοράς και της υλοποίησης της ψηφιακής ενιαίας αγοράς· τονίζει ότι η πιστοποίηση των διαχειριζόμενων υπηρεσιών ασφάλειας δεν είναι μόνο σημαντική για τη διαδικασία επιλογής για το αποθεματικό κυβερνοασφάλειας της ΕΕ, αλλά αποτελεί επίσης ουσιαστικό δείκτη ποιότητας για τους ιδιωτικούς και δημόσιους φορείς που προτίθενται να αγοράσουν τέτοιες υπηρεσίες·

7. σημειώνει ότι η πρόταση ενισχύει τον ρόλο του ENISA, ο οποίος θα πρέπει να στηρίζει και να προωθεί την ανάπτυξη και την εφαρμογή της πολιτικής της Ένωσης για την πιστοποίηση της κυβερνοασφάλειας προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ και διαχειριζόμενων υπηρεσιών ασφάλειας, με τακτική παρακολούθηση των εξελίξεων σε σχετικούς τομείς τυποποίησης και την υποβολή προτάσεων για τεχνικές προδιαγραφές, στις περιπτώσεις όπου δεν υπάρχουν διαθέσιμα πρότυπα· προτείνει να δοθούν στον ENISA πρόσθετοι πόροι και εξουσίες για την άσκηση του διευρυμένου ρόλου του, συμπεριλαμβανομένης χρηματοδότησης για έρευνα και ανάπτυξη, καθώς και σαφής εντολή συντονισμού με τους εθνικούς οργανισμούς κυβερνοασφάλειας και τους ενδιαφερόμενους φορείς του κλάδου· υπογραμμίζει τον ουσιαστικό ρόλο που έχουν οι ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT) για την επίτευξη προβλέψιμου και ασφαλούς ψηφιακού χώρου για τις επιχειρήσεις και τους πολίτες·

8. καλεί την Επιτροπή και τον ENISA να στηρίξουν και να διασφαλίσουν τη συνεπή εφαρμογή του ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας με βάση αμερόληπτους κανόνες και κατ' αντιστοιχία προς τα ευρωπαϊκά και διεθνή πρότυπα για την αυτοαξιολόγηση της συμμόρφωσης από τον κατασκευαστή ή τον πάροχο προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ, διαδικασιών ΤΠΕ ή διαχειριζόμενων υπηρεσιών ασφάλειας, σύμφωνα με την πράξη της ΕΕ για την κυβερνοασφάλεια· πιστεύει ότι η εφαρμογή θα πρέπει να συμβάλλει στην αντιστάθμιση του κόστους της διαπίστευσης και να ενθαρρύνει περισσότερους κατασκευαστές ή παρόχους να συμμετάσχουν στο σύστημα·

9. τονίζει ότι κάθε σύστημα πιστοποίησης θα πρέπει να σχεδιαστεί κατά τρόπο που να δίνει κίνητρο και να ενθαρρύνει όλους τους εμπλεκόμενους φορείς ενός τομέα να αναπτύξουν και να υιοθετήσουν τακτικά επικαιροποιούμενα πρότυπα ασφαλείας, τεχνικές προδιαγραφές και βασικές αρχές για ασφάλεια εκ σχεδιασμού και ιδιωτικότητα εκ σχεδιασμού, σε όλα τα στάδια του κύκλου ζωής του προϊόντος ή της υπηρεσίας· επισημαίνει ότι, κατά την ανάπτυξη των εν λόγω αρχών, πρέπει να λαμβάνονται υπόψη

συστηματικότερα οι παρατηρήσεις εκ μέρους φορέων της κοινωνίας των πολιτών, ανεξάρτητων ερευνητών στον τομέα της ασφάλειας και σχετικών ενδιαφερόμενων μερών· θεωρεί ότι τα συστήματα πιστοποίησης θα πρέπει να συνάδουν με άλλα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας που έχουν εγκριθεί σύμφωνα με την πράξη της ΕΕ για την κυβερνοασφάλεια και θα πρέπει να αποφεύγουν τη δυσανάλογη επιβάρυνση των παρόχων· συνιστά τα συστήματα πιστοποίησης να περιλαμβάνουν σαφείς και λεπτομερείς κατευθυντήριες γραμμές σχετικά με τον τρόπο εφαρμογής των αρχών της ασφάλειας εκ σχεδιασμού και της ιδιωτικότητας εκ σχεδιασμού, και οι εν λόγω κατευθυντήριες γραμμές να είναι σύμφωνες με τις διατάξεις για τον καθορισμού του πλαισίου για τα ευρωπαϊκά συστήματα κυβερνοασφάλειας στην πράξη της ΕΕ για την κυβερνοασφάλεια· προτείνει, όπου είναι αναγκαίο και αναλογικό, τα συστήματα πιστοποίησης να αποτελούνται από έναν μηχανισμό συνεχούς βελτίωσης, όπως τακτικές επανεξετάσεις και επικαιροποιήσεις των προτύπων ασφάλειας και των τεχνικών κανόνων· θεωρεί ότι ο μηχανισμός θα πρέπει να λαμβάνει υπόψη τις τελευταίες εξελίξεις όσον αφορά τις απειλές για την κυβερνοασφάλεια και τις τεχνολογίες κυβερνοασφάλειας· προτείνει κάθε σύστημα πιστοποίησης να περιλαμβάνει μέτρα για την προώθηση της διαφάνειας και της λογοδοσίας, όπως δημοσιοποίηση των αποτελεσμάτων της πιστοποίησης και κυρώσεις σε περίπτωση μη συμμόρφωσης·

10. ζητεί να θεσπιστεί εθελοντικό σήμα εμπιστοσύνης της ΕΕ για πιστοποιημένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας· επισημαίνει, στο πλαίσιο αυτό, ότι το σήμα θα μπορούσε να συμβάλλει στην ευαισθητοποίηση σχετικά με την κυβερνοασφάλεια σε ολόκληρη την εσωτερική αγορά και να δίνει ανταγωνιστικό πλεονέκτημα στις εταιρείες με καλά διαπιστευτήρια κυβερνοασφάλειας· προτείνει το σήμα εμπιστοσύνης της ΕΕ να σχεδιαστεί έτσι ώστε να είναι εύκολα αναγνωρίσιμο και κατανοητό από τους καταναλωτές και τις επιχειρήσεις·

11. συνιστά στην Επιτροπή και στον ENISA να θεσπίσουν ειδικό πρόγραμμα έρευνας και ανάπτυξης για την κυβερνοασφάλεια· συνιστά στην Επιτροπή και τον ENISA να θεσπίσουν ένα πλαίσιο αξιολόγησης κινδύνων κυβερνοασφάλειας για τις επιχειρήσεις, το οποίο θα περιέχει κατευθυντήριες γραμμές σχετικά με τον τρόπο εντοπισμού, αξιολόγησης και μετριασμού των κινδύνων κυβερνοασφάλειας, με δυνατότητα προσαρμογής σε διάφορους τομείς και μεγέθη εταιρειών· προτείνει η Επιτροπή και ο ENISA να προσφέρουν βοήθεια και στήριξη στα κράτη μέλη για τη δημιουργία ενός μηχανισμού αναφοράς περιστατικών κυβερνοασφάλειας για τους καταναλωτές και τις επιχειρήσεις, ώστε να διευκολυνθεί η συλλογή δεδομένων σχετικά με περιστατικά κυβερνοασφάλειας, τα οποία θα μπορούσαν να χρησιμοποιούνται για τη βελτίωση των πολιτικών και των πρακτικών κυβερνοασφάλειας.

ΔΙΑΔΙΚΑΣΙΑ ΤΗΣ ΑΡΜΟΔΙΑΣ ΕΠΙ ΤΗΣ ΟΥΣΙΑΣ ΕΠΙΤΡΟΠΗΣ

Τίτλος	Τροποποίηση του κανονισμού (ΕΕ) 2019/881 όσον αφορά τις διαχειριζόμενες υπηρεσίες ασφάλειας
Έγγραφα αναφοράς	COM(2023)0208 – C9-0137/2023 – 2023/0108(COD)
Ημερομηνία υποβολής στο ΕΚ	19.4.2023
Επιτροπή αρμόδια επί της ουσίας Ημερομ. αναγγελίας στην Ολομέλεια	ITRE 1.6.2023
Γνωμοδοτικές επιτροπές Ημερομ. αναγγελίας στην Ολομέλεια	IMCO LIBE 1.6.2023 1.6.2023
Αποφάσισε να μη γνωμοδοτήσει Ημερομηνία της απόφασης	LIBE 30.5.2023
Εισηγητές Ημερομηνία ορισμού	Josianne Cutajar 2.5.2023
Εξέταση στην επιτροπή	19.7.2023 19.9.2023
Ημερομηνία έγκρισης	25.10.2023
Αποτέλεσμα της τελικής ψηφοφορίας	+: 57 –: 0 0: 2
Βουλευτές παρόντες κατά την τελική ψηφοφορία	Matteo Adinolfi, Nicola Beer, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Michael Bloss, Paolo Borchia, Marc Botenga, Markus Buchheit, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Beatrice Covassi, Ciarán Cuffe, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Christian Ehler, Lina Gálvez Muñoz, Jens Geier, Bart Groothuis, Christophe Grudler, Henrike Hahn, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Thierry Mariani, Marina Mesure, Dan Nica, Niklas Nienass, Ville Niinistö, Johan Nissinen, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Clara Ponsatí Obiols, Manuela Ripa, Sara Skyttedal, Riho Terras, Patrizia Toia, Henna Virkkunen, Pernille Weiss, Carlos Zorrinho
Αναπληρωτές παρόντες κατά την τελική ψηφοφορία	Pascal Arimont, Tiziana Beghin, Franc Bogovič, Damien Carême, Martina Dlabajová, Francesca Donato, Matthias Ecke, Nicolás González Casares, Ladislav Ilčić, Luděk Niedermayer, Emma Wiesner
Αναπληρωτές (άρθρο 209 παράγραφος 7 του Κανονισμού) παρόντες κατά την τελική ψηφοφορία	Asim Ademov, Aušra Maldeikienė, Irène Tolleret
Ημερομηνία κατάθεσης	26.10.2023

ΤΕΛΙΚΗ ΨΗΦΟΦΟΡΙΑ ΜΕ ΟΝΟΜΑΣΤΙΚΗ ΚΛΗΣΗ ΣΤΗΝ ΑΡΜΟΔΙΑ ΕΠΙ ΤΗΣ ΟΥΣΙΑΣ ΕΠΙΤΡΟΠΗ

57	+
ECR	Ladislav Ilčić
ID	Matteo Adinolfi, Paolo Borchia, Marie Dauchy, Thierry Mariani
NI	Tiziana Beghin, Francesca Donato, Clara Ponsatí Obiols
PPE	Asim Ademov, Pascal Arimont, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Franc Bogovič, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Aušra Maldeikienė, Luděk Niedermayer, Markus Pieper, Sara Skyttedal, Riho Terras, Henna Virkkunen, Pernille Weiss
Renew	Nicola Beer, Nicola Danti, Martina Dlabajová, Bart Groothuis, Christophe Grudler, Mauri Pekkarinen, Morten Petersen, Irène Tolleret, Emma Wiesner
S&D	Beatrice Covassi, Josianne Cutajar, Matthias Ecke, Lina Gálvez Muñoz, Jens Geier, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Dan Nica, Tsvetelina Penkova, Patrizia Toia, Carlos Zorrinho
The Left	Marc Botenga, Marina Mesure
Verts/ALE	Michael Bloss, Damien Carême, Ciarán Cuffe, Henrike Hahn, Niklas Nienass, Ville Niinistö, Manuela Ripa

0	-

2	0
ECR	Johan Nissinen
ID	Markus Buchheit

Υπόμνημα των χρησιμοποιούμενων συμβόλων:
+ : υπέρ
- : κατά
0 : αποχή