



2023/0108(COD)

21.9.2023

ΤΡΟΠΟΛΟΓΙΕΣ 17 - 52

Σχέδιο έκθεσης
Josianne Cutajar
(PE752.802v01-00)

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

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

Πρόταση κανονισμού
Αιτιολογική σκέψη 2

Κείμενο που προτείνει η Επιτροπή

(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, αποκτούν ολοένα και μεγαλύτερη σημασία για την πρόληψη και τον μετριασμό των περιστατικών κυβερνοασφάλειας. 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**⁸. 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.

Τροπολογία

(2) Οι διαχειριζόμενες υπηρεσίες ασφάλειας είναι υπηρεσίες που **παρέχονται από παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας σύμφωνα με το άρθρο 6 σημείο 40) της οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου**. **Οι εν λόγω υπηρεσίες**, οι οποίες συνίστανται στην εκτέλεση ή την παροχή βοήθειας για δραστηριότητες που σχετίζονται με τη διαχείριση κινδύνων κυβερνοασφάλειας από τους πελάτες τους, αποκτούν ολοένα και μεγαλύτερη σημασία για την πρόληψη και τον μετριασμό των περιστατικών κυβερνοασφάλειας. Ως εκ τούτου, οι πάροχοι **διαχειριζόμενων υπηρεσιών ασφάλειας** θεωρούνται βασικές ή σημαντικές οντότητες που ανήκουν σε τομέα υψηλής κρισιμότητας σύμφωνα με το **παράρτημα I σημείο 10** της οδηγίας (ΕΕ) 2022/2555. 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.

⁸ 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).

⁸ 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).

Or. en

Τροπολογία 18

Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skytvedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Πρόταση κανονισμού Αιτιολογική σκέψη 2

Κείμενο που προτείνει η Επιτροπή

(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, αποκτούν ολοένα και μεγαλύτερη σημασία για την πρόληψη και τον μετριασμό των περιστατικών κυβερνοασφάλειας. 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 Συμβουλίου⁸. 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

Τροπολογία

(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, **συμπεριλαμβανομένων της πρόληψης, του εντοπισμού, της αντιμετώπισης περιστατικών ή της ανάκαμψης από αυτά**, αποκτούν ολοένα και μεγαλύτερη σημασία για την πρόληψη και τον μετριασμό των περιστατικών κυβερνοασφάλειας. 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 Συμβουλίου⁸. Σύμφωνα με την αιτιολογική σκέψη 86 της εν λόγω οδηγίας, οι πάροχοι υπηρεσίας διαχείρισης της

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.

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.

⁸ 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).

⁸ 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).

Or. en

Τροπολογία 19 **Enĵen Tošenovský**

Πρόταση κανονισμού **Αιτιολογική σκέψη 3**

Κείμενο που προτείνει η Επιτροπή

(3) Οι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας διαδραματίζουν επίσης σημαντικό ρόλο στο αποθεματικό κυβερνοασφάλειας της ΕΕ, η σταδιακή

Τροπολογία

(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 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.**

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 **αξιόπιστων παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας** που αποτελούν το αποθεματικό κυβερνοασφάλειας της ΕΕ, η οποία θα πρέπει, μεταξύ άλλων, να λαμβάνει υπόψη το αν ο ενδιαφερόμενος πάροχος έχει λάβει ευρωπαϊκή ή εθνική πιστοποίηση κυβερνοασφάλειας. **Επιπλέον, μόλις τεθεί σε εφαρμογή ένα ευρωπαϊκό σχήμα πιστοποίησης** της κυβερνοασφάλειας για διαχειριζόμενες υπηρεσίες ασφάλειας, **το οποίο θα αντικαταστήσει επίσης όλα τα σχετικά εθνικά σχήματα πιστοποίησης της κυβερνοασφάλειας, για τη συμπερίληψη των αξιόπιστων παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας στο αποθεματικό κυβερνοασφάλειας της ΕΕ θα πρέπει να εφαρμόζεται υποχρεωτική πιστοποίηση σύμφωνα με το εν λόγω σχήμα πιστοποίησης.**

Or. en

Τροπολογία 20
Johan Nissinen

Πρόταση κανονισμού
Αιτιολογική σκέψη 4

(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.

(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.

Ταυτόχρονα, αυτοί οι πολλαπλοί στόχοι του κανονισμού θα πρέπει να σταθμίζονται σε συνάρτηση με τη δυνητική κανονιστική επιβάρυνση και το κόστος που συνδέεται με την πιστοποίηση, δεδομένου ότι η συμμόρφωση με τις απαιτήσεις πιστοποίησης θα συνεπάγεται πρόσθετες δαπάνες και διοικητικές προσπάθειες, οι οποίες θα μπορούσαν να αποτελέσουν πηγή ανησυχίας για τους μικρότερους παρόχους.

Or. en

Τροπολογία 21

Ville Niinistö

εξ ονόματος της Ομάδας Verts/ALE

Πρόταση κανονισμού

Αιτιολογική σκέψη 4 α (νέα)

(4a) Δεδομένου ότι η αγορά και τα εκπαιδευτικά συστήματα προσφέρουν ποικιλία εκπαιδευτικών πόρων και προγραμμάτων τυπικής κατάρτισης, πρέπει να υπογραμμιστεί ότι οι γνώσεις αποκτώνται επίσης με μη τυπικούς τρόπους και ότι οι δεξιότητες μπορούν να αποδεικνύονται, μεταξύ άλλων, μέσω τίτλων σπουδών και πιστοποίησης. Ειδικότερα στο ταχέως εξελισσόμενο τοπίο των απειλών, τα κράτη μέλη και οι δικαιούχοι των διαχειριζόμενων υπηρεσιών ασφάλειας θα πρέπει να λαμβάνουν υπόψη τους υψηλής ειδίκευσης ερευνητές τρωτών σημείων. Επιπλέον, τα φυσικά και νομικά πρόσωπα που ερευνούν τρωτά σημεία είναι δυνατόν σε ορισμένα κράτη μέλη να εκτεθούν σε ποινική και αστική ευθύνη και γι' αυτόν τον λόγο τα κράτη μέλη ενθαρρύνονται να εκδώσουν κατευθυντήριες γραμμές σχετικά με τη μη δίωξη της έρευνας στον τομέα της ασφάλειας των πληροφοριών και την απαλλαγή από την αστική ευθύνη για τις εν λόγω δραστηριότητες.

Or. en

Αιτιολόγηση

Ο χώρος των επαγγελματιών του τομέα της ασφάλειας παρουσιάζει εν μέρει ανομοιογένεια λόγω των διαφορών ως προς τις μη τυποποιημένες σταδιοδρομίες, την πρόσβαση στην τυπική εκπαίδευση και τους πόρους πιστοποίησης. Ως εκ τούτου, πρέπει να ενθαρρύνουμε την απασχόληση ειδικευμένων ατόμων και να εξασφαλίσουμε ένα θετικό πλαίσιο για δραστηριότητες που έχουν ως αποτέλεσμα τη βελτίωση της κυβερνοασφάλειας.

Τροπολογία 22
Josianne Cutajar

Πρόταση κανονισμού
Αιτιολογική σκέψη 4 α (νέα)

(4a) 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 «Πορεία προς την ψηφιακή δεκαετία»^{8α}, ιδίως όσον αφορά τον στόχο το 75 % των επιχειρήσεων της ΕΕ να αρχίσουν να χρησιμοποιούν υπολογιστικό νέφος/TN/μαζικά δεδομένα, τον στόχο ποσοστό πάνω από το 90 % των ΜΜΕ να κατακτήσει τουλάχιστον ένα βασικό επίπεδο ψηφιακής έντασης και τον στόχο να παρέχονται διαδικτυακά οι βασικές δημόσιες υπηρεσίες.

^{8α} Απόφαση (ΕΕ) 2022/2481 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, για τη θέσπιση του προγράμματος πολιτικής 2030 «Ψηφιακή Δεκαετία»

Or. en

Τροπολογία 23

Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan

Πρόταση κανονισμού

Αιτιολογική σκέψη 4 α (νέα)

(4a) Τα ευρωπαϊκά σχήματα πιστοποίησης για διαχειριζόμενες υπηρεσίες ασφάλειας θα πρέπει να διευκολύνουν τη χρήση των εν λόγω υπηρεσιών, ιδίως για μικρότερες οντότητες, συμπεριλαμβανομένων των τοπικών και περιφερειακών αρχών ή των

ΜΜΕ, οι οποίες συχνά δεν διαθέτουν τους οικονομικούς και ανθρώπινους πόρους που απαιτούνται ώστε να παρέχουν οι ίδιες τις υπηρεσίες αυτές, αλλά είναι ευάλωτες σε κυβερνοεπιθέσεις με δυνητικά σοβαρές συνέπειες.

Or. en

Τροπολογία 24 Josianne Cutajar

Πρόταση κανονισμού Αιτιολογική σκέψη 5

Κείμενο που προτείνει η Επιτροπή

(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 εμπειρογνώσια 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, εμπειρογνώσιας και πείρας, καθώς και κατάλληλες εσωτερικές διαδικασίες. Συνεπώς, για να εξασφαλιστεί ότι όλες οι πτυχές μιας διαχειριζόμενης υπηρεσίας ασφάλειας μπορούν να καλυφθούν από ένα σχήμα πιστοποίησης, είναι αναγκαίο να τροποποιηθεί ο κανονισμός (ΕΕ) 2019/881. Ζητήθηκε η γνώμη του Ευρωπαϊκού 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],

Τροπολογία

(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 εμπειρογνώσια 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, εμπειρογνώσιας και πείρας, καθώς και κατάλληλες εσωτερικές διαδικασίες. Συνεπώς, για να εξασφαλιστεί ότι όλες οι πτυχές μιας διαχειριζόμενης υπηρεσίας ασφάλειας μπορούν να καλυφθούν από ένα σχήμα πιστοποίησης, είναι αναγκαίο να τροποποιηθεί ο κανονισμός (ΕΕ) 2019/881. Το **σχήμα πιστοποίησης που θεσπίζεται βάσει του παρόντος κανονισμού θα πρέπει επίσης να λαμβάνει υπόψη τα αποτελέσματα και τις συστάσεις της αξιολόγησης και επανεξέτασης που προβλέπονται στο άρθρο 67 του εν λόγω κανονισμού.** Ζητήθηκε σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου η

Τροπολογία 25

Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skytvedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Πρόταση κανονισμού Αιτιολογική σκέψη 5

Κείμενο που προτείνει η Επιτροπή

(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 σχήμα πιστοποίησης, είναι αναγκαίο να τροποποιηθεί ο κανονισμός (ΕΕ) 2019/881. Ζητήθηκε η γνώμη του Ευρωπαϊκού 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],

Τροπολογία

(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 **και αξιοπιστία** 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 σχήμα πιστοποίησης, είναι αναγκαίο να τροποποιηθεί ο κανονισμός (ΕΕ) 2019/881. Ζητήθηκε σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου η γνώμη του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων, ο οποίος γνωμοδότησε στις [ΗΗ/ΜΜ/ΕΕΕΕ],

Τροπολογία 26
Enĵen Tošenovský

Πρόταση κανονισμού
Αιτιολογική σκέψη 5

Κείμενο που προτείνει η Επιτροπή

(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 σχήμα πιστοποίησης, είναι αναγκαίο να τροποποιηθεί ο κανονισμός (ΕΕ) 2019/881. Ζητήθηκε η γνώμη του Ευρωπαϊκού 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],

Τροπολογία

(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. Ζητήθηκε σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου η γνώμη του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων, ο οποίος γνωμοδότησε στις [ΗΗ/ΜΜ/ΕΕΕΕ],

Or. en

Τροπολογία 27

Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skytvedal, Ivan Štefanec, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan

Πρόταση κανονισμού
Αιτιολογική σκέψη 5 α (νέα)

(5a) Δεδομένου ότι τα ευρωπαϊκά σχήματα κυβερνοασφάλειας θα πρέπει να πιστοποιούν ότι οι διαχειριζόμενες υπηρεσίες ασφάλειας παρέχονται από προσωπικό υψηλής ειδίκευσης που είναι σε θέση να παρέχει αξιόπιστα τις υπηρεσίες αυτές και να διασφαλίζει τα υψηλότερα πρότυπα κυβερνοασφάλειας, είναι επιτακτική ανάγκη να υπάρχει επαρκής διαθεσιμότητα προσωπικού υψηλής ειδίκευσης στην Ένωση. 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 18 Απριλίου 2023, σχετικά με την Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας. Είναι σημαντικό να καλυφθεί αυτή η έλλειψη ταλέντων με την ενίσχυση της συνεργασίας και του συντονισμού μεταξύ των διαφόρων ενδιαφερόμενων μερών, συμπεριλαμβανομένων του ιδιωτικού τομέα, της πανεπιστημιακής κοινότητας, των κρατών μελών, της Επιτροπής και του Οργανισμού της ΕΕ για την κυβερνοασφάλεια (ENISA), ώστε να επεκταθούν και να δημιουργηθούν συνέργειες για επενδύσεις στην εκπαίδευση και την κατάρτιση, την ανάπτυξη συμπράξεων δημόσιου και ιδιωτικού τομέα, τη στήριξη πρωτοβουλιών έρευνας και καινοτομίας, την ανάπτυξη και την αμοιβαία αναγνώριση κοινών προτύπων και την πιστοποίηση των δεξιοτήτων κυβερνοασφάλειας, μεταξύ άλλων μέσω του ευρωπαϊκού πλαισίου δεξιοτήτων κυβερνοασφάλειας. Αυτό αναμένεται επίσης να διευκολύνει την κινητικότητα των επαγγελματιών στον τομέα της κυβερνοασφάλειας εντός της Ένωσης.

Or. en

Τροπολογία 28
Johan Nissinen

Πρόταση κανονισμού
Αιτιολογική σκέψη 5 α (νέα)

Κείμενο που προτείνει η Επιτροπή

Τροπολογία

(5α) Δεδομένου ότι τα σχήματα πιστοποίησης θα αυξήσουν την πολυπλοκότητα ενός ήδη πολύπλοκου ρυθμιστικού πλαισίου, είναι πολύ σημαντικό να αποφευχθούν πιθανές επικαλύψεις ή συγκρούσεις με τους υφιστάμενους κανονισμούς και τα πρότυπα κυβερνοασφάλειας. Επισημαίνει περαιτέρω την ανάγκη προσεκτικής εξέτασης και αναλογικότητας κατά την εφαρμογή του κανονισμού, προκειμένου να μειωθούν οι αρνητικές επιπτώσεις στην ελευθερία της αγοράς και την καινοτομία.

Or. en

Τροπολογία 29
Josianne Cutajar

Πρόταση κανονισμού
Αιτιολογική σκέψη 5 α (νέα)

Κείμενο που προτείνει η Επιτροπή

Τροπολογία

(5α) Θα πρέπει να εξεταστεί το ενδεχόμενο κατάλληλης χρηματοδότησης και πόρων που θα συνοδεύουν τα πρόσθετα καθήκοντα που ανατίθενται στον ENISA με την παρούσα πράξη.

Or. en

Τροπολογία 30
Enĵen Tošenovský

Πρόταση κανονισμού

Άρθρο 1 – παράγραφος 1 – σημείο 2 – στοιχείο α – εισαγωγικό μέρος

Κείμενο που προτείνει η Επιτροπή

Τροπολογία

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

α) τα σημεία 7, 9, 10 και 11 αντικαθίστανται από το ακόλουθο κείμενο:

Or. en

Τροπολογία 31

Enĵen Toĥenovský

Πρόταση κανονισμού

Άρθρο 1 – παράγραφος 1 – σημείο 2 – στοιχείο α

Κανονισμός (ΕΕ) 2019/881

Άρθρο 2 – σημείο 7

Κείμενο που προτείνει η Επιτροπή

Τροπολογία

7) “χειρισμός συμβάντων”: ο χειρισμός συμβάντων όπως ορίζεται στο άρθρο 6 σημείο 8) της οδηγίας (ΕΕ) 2022/2555,

Or. en

Τροπολογία 32

Enĵen Toĥenovský

Πρόταση κανονισμού

Άρθρο 1 – παράγραφος 1 – σημείο 2 – στοιχείο β – εισαγωγικό μέρος

Κείμενο που προτείνει η Επιτροπή

Τροπολογία

β) προστίθεται το ακόλουθο σημείο:

β) προστίθενται τα ακόλουθα **σημεία**:

Or. en

Τροπολογία 33

Enĵen Toĥenovský

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 1 – σημείο 2 – στοιχείο β
Κανονισμός (ΕΕ) 2019/881
Άρθρο 2 – σημείο 7α

Κείμενο που προτείνει η Επιτροπή

Τροπολογία

7α) “κίνδυνος”: ο κίνδυνος όπως ορίζεται στο άρθρο 6 σημείο 9) της οδηγίας (ΕΕ) 2022/2555,

Or. en

Τροπολογία 34
Enĵen Toĥenovský

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 1 – σημείο 2 – στοιχείο β
Κανονισμός (ΕΕ) 2019/881
Άρθρο 2 – σημείο 14α

Κείμενο που προτείνει η Επιτροπή

Τροπολογία

14α) “διαχειριζόμενη υπηρεσία ασφάλειας”: **υπηρεσία που συνίσταται στην εκτέλεση ή την παροχή βοήθειας για δραστηριότητες που σχετίζονται με τη διαχείριση κινδύνων κυβερνοασφάλειας, συμπεριλαμβανομένης της αντιμετώπισης περιστατικών, των δοκιμών διείσδυσης, των ελέγχων ασφάλειας και της παροχής συμβουλών**

14α) “διαχειριζόμενη υπηρεσία ασφάλειας”: η **διαχειριζόμενη υπηρεσία ασφάλειας κατά την έννοια του άρθρου 6 σημείο 40) της οδηγίας (ΕΕ) 2022/2555**.

Or. en

Τροπολογία 35
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 1 – σημείο 2 – στοιχείο β
Κανονισμός (ΕΕ) 2019/881
Άρθρο 2 – σημείο 14α

Κείμενο που προτείνει η Επιτροπή

Τροπολογία

14α) “διαχειριζόμενη υπηρεσία ασφάλειας”: υπηρεσία που συνίσταται στην εκτέλεση ή την παροχή βοήθειας για δραστηριότητες που σχετίζονται με τη διαχείριση κινδύνων κυβερνοασφάλειας, συμπεριλαμβανομένης της αντιμετώπισης περιστατικών, *των δοκιμών διείσδυσης, των ελέγχων ασφάλειας και της παροχής συμβουλών*

14α) “διαχειριζόμενη υπηρεσία ασφάλειας”: *διαχειριζόμενη* υπηρεσία που συνίσταται στην εκτέλεση ή την παροχή βοήθειας για δραστηριότητες που σχετίζονται με τη διαχείριση κινδύνων κυβερνοασφάλειας, συμπεριλαμβανομένων της *πρόληψης, του εντοπισμού*, της αντιμετώπισης περιστατικών *ή της ανάκαμψης* από αυτά,

Or. en

Τροπολογία 36
Enĵen Tošenovský

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 1 – σημείο 2 – στοιχείο β
Κανονισμός (ΕΕ) 2019/881
Άρθρο 2 – σημείο 14α α

Κείμενο που προτείνει η Επιτροπή

Τροπολογία

14α α) “πάροχος διαχειριζόμενων υπηρεσιών ασφάλειας”: *ο πάροχος διαχειριζόμενων υπηρεσιών ασφάλειας όπως ορίζεται στο άρθρο 6 σημείο 40) της οδηγίας (ΕΕ) 2022/2555,*

Or. en

Τροπολογία 37
Ville Niinistö
εξ ονόματος της Ομάδας Verts/ALE

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 1 – σημείο 6
Κανονισμός (ΕΕ) 2019/881
Άρθρο 47 – παράγραφος 2

Κείμενο που προτείνει η Επιτροπή

Τροπολογία

2. Το κυλιόμενο πρόγραμμα εργασίας

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.

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. **Πρέπει να συμπεριληφθούν μέτρα στήριξης για την εκτίμηση των αναγκών για ειδικευμένους εργαζόμενους, των τύπων δεξιοτήτων και των υφιστάμενων διαδρομών κατάρτισης, σε συνδυασμό με μέτρα για την κάλυψη τυχόν ελλείψεων που εντοπίζονται.**

Or. en

Αιτιολόγηση

Η διαδικασία για τον προσδιορισμό των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ ή των κατηγοριών τους, καθώς και των διαχειριζόμενων υπηρεσιών ασφάλειας πρέπει να συνοδεύεται από αξιολόγηση δεξιοτήτων και μέτρα για την κάλυψη των ελλείψεων.

Τροπολογία 38

Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard

Πρόταση κανονισμού

Άρθρο 1 – παράγραφος 1 – σημείο 6

Κανονισμός (ΕΕ) 2019/881

Άρθρο 47 – παράγραφος 3 – στοιχείο α

Κείμενο που προτείνει η Επιτροπή

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,

Τροπολογία

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

Or. en

Αιτιολόγηση

Το κυλιόμενο πρόγραμμα εργασίας της Ένωσης δεν θα πρέπει να αξιολογεί μόνο την ανάπτυξη εθνικών σχημάτων, αλλά και τα πρότυπα του κλάδου και τα διεθνή πρότυπα.

Τροπολογία 39

Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Πρόταση κανονισμού

Άρθρο 1 – παράγραφος 1 – σημείο 7

Κανονισμός (ΕΕ) 2019/881

Άρθρο 49 – παράγραφος 7

Κείμενο που προτείνει η Επιτροπή

Τροπολογία

7) στο άρθρο 49 η παράγραφος 7 αντικαθίσταται από το ακόλουθο κείμενο:

διαγράφεται

7. Η Επιτροπή, με βάση το υποψήφιο σχήμα που προετοιμάζει ο ENISA, μπορεί να εκδίδει εκτελεστικές πράξεις οι οποίες προβλέπουν σε σχέση με ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας που πληρούν τις απαιτήσεις των άρθρων 51, 52 και 54. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 66 παράγραφος 2.

Or. en

Τροπολογία 40

Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Πρόταση κανονισμού

Άρθρο 1 – παράγραφος 1 – σημείο 7

Κανονισμός (ΕΕ) 2019/881

Άρθρο 49 – παράγραφος 7

7. Η Επιτροπή, με βάση το υποψήφιο σχήμα που προετοιμάζει ο ENISA, μπορεί να εκδίδει **εκτελεστικές** πράξεις οι οποίες προβλέπουν σε σχέση με ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ, διαδικασίες ΤΠΕ και διαχειριζόμενες υπηρεσίες ασφάλειας που πληρούν τις απαιτήσεις των άρθρων 51, 52 και 54. **Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 66 παράγραφος 2.**

7. Η Επιτροπή, με βάση το υποψήφιο σχήμα που προετοιμάζει ο ENISA, μπορεί να εκδίδει **κατ' εξουσιοδότηση** πράξεις οι οποίες προβλέπουν 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.

(Η τροπολογία αφορά το σύνολο του κειμένου. Η έγκρισή της απαιτεί αντίστοιχες προσαρμογές σε όλο το κείμενο.)

Or. en

Αιτιολόγηση

Since the adoption of the Cyber Security Act, no certification schemes have been adopted, nor has the Union Rolling Work Programme (URWP), which reflects wider stakeholder involvement, been formalized. Instead, some proposals, such as the EUCS, have introduced wide-ranging requirements that are not risk-based, hinder innovation and competitiveness, are highly political and therefore outside of ENISA's mandate in the CSA, and have not been properly consulted with relevant stakeholders or tested through impact assessments. It is therefore suggested that the adoption of a scheme is done through delegated act, and preceded by a impact assessment involving SCCG and ECCG consultations to improve the transparency of schemes and the effectiveness of the certification framework in general.

Τροπολογία 41

Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Πρόταση κανονισμού

Άρθρο 1 – παράγραφος 1 – σημείο 7

Κανονισμός (ΕΕ) 2019/881

Άρθρο 49 – παράγραφος 7 α (νέα)

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 διαβουλεύσεις με την ομάδα συμφεροντούχων για την πιστοποίηση της κυβερνοασφάλειας (SCCG) και την ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας (ECCG).

Or. en

Αιτιολόγηση

Since the adoption of the Cyber Security Act, no certification schemes have been adopted, nor has the Union Rolling Work Programme (URWP), which reflects wider stakeholder involvement, been formalized. Instead, some proposals, such as the EUCS, have introduced wide-ranging requirements that are not risk-based, hinder innovation and competitiveness, are highly political and therefore outside of ENISA's mandate in the CSA, and have not been properly consulted with relevant stakeholders or tested through impact assessments. It is therefore suggested that the adoption of a scheme is done through delegated act, and preceded by a impact assessment involving SCCG and ECCG consultations to improve the transparency of schemes and the effectiveness of the certification framework in general.

Τροπολογία 42

Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skytvedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Πρόταση κανονισμού

Άρθρο 1 – παράγραφος 1 – σημείο 7 α (νέο)

Κανονισμός (ΕΕ) 2019/881

Άρθρο 49 – παράγραφος 7 α (νέα)

7α) προστίθεται η ακόλουθη παράγραφος:

«7α. Η Επιτροπή, με βάση το υποψήφιο σχήμα που προετοιμάζει ο ENISA, μπορεί να εκδίδει κατ' εξουσιοδότηση πράξεις οι οποίες προβλέπουν ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας για διαχειριζόμενες υπηρεσίες ασφάλειας το οποίο πληροί τις απαιτήσεις των άρθρων 51, 52 και 54. Οι εν λόγω κατ' εξουσιοδότηση πράξεις εκδίδονται σύμφωνα με τη διαδικασία που αναφέρεται στο άρθρο 66α.»

Or. en

Τροπολογία 43

Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Πρόταση κανονισμού

Άρθρο 1 – παράγραφος 1 – σημείο 9

Κανονισμός (ΕΕ) 2019/881

Άρθρο 51α – παράγραφος 1 – στοιχείο β

Κείμενο που προτείνει η Επιτροπή

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

Τροπολογία

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

Or. en

Τροπολογία 44

Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Πρόταση κανονισμού

Άρθρο 1 – παράγραφος 1 – σημείο 9

Κανονισμός (ΕΕ) 2019/881

Άρθρο 51α – παράγραφος 1 – στοιχείο ζ

Κείμενο που προτείνει η Επιτροπή

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

Τροπολογία

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

Or. en

Τροπολογία 45 **Enĵen Tošenovský**

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 1 – σημείο 9
Κανονισμός (ΕΕ) 2019/881
Άρθρο 51α – παράγραφος 1 – στοιχείο ζ

Κείμενο που προτείνει η Επιτροπή

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

Τροπολογία

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, δεν περιέχουν γνωστά τρωτά σημεία και περιλαμβάνουν τις τελευταίες επικαιροποιήσεις ασφάλειας.»

Or. en

Τροπολογία 46 **Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skytvedal, Ivan Štefanec, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan**

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 1 – σημείο 13 – στοιχείο β – σημείο ii – στοιχείο α α

Κείμενο που προτείνει η Επιτροπή

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·

Τροπολογία

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, ***συμπεριλαμβανομένων των ΜΜΕ. Η Επιτροπή διασφαλίζει ότι οι ΜΜΕ έχουν πρόσβαση σε κατάλληλη χρηματοδοτική στήριξη για την εφαρμογή των μέτρων μέσω υφιστάμενων προγραμμάτων της Ένωσης,»***

Or. en

Τροπολογία 47

Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Πρόταση κανονισμού

Άρθρο 1 – παράγραφος 1 – σημείο 14

Κανονισμός (ΕΕ) 2019/881

Άρθρο 57 – παράγραφος 1

Κείμενο που προτείνει η Επιτροπή

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

Τροπολογία

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 **εκτελεστική 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.

την ημερομηνία που ορίζεται στην **κατ' εξουσιοδότηση πράξη**. 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.

(Η τροπολογία αφορά το σύνολο του κειμένου. Η έγκρισή της απαιτεί αντίστοιχες προσαρμογές σε όλο το κείμενο.)

Or. en

Αιτιολόγηση

Αυτό αντικατοπτρίζει την τροπολογία στο άρθρο 49.

Τροπολογία 48

Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skytvedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Πρόταση κανονισμού

Άρθρο 1 – παράγραφος 1 – σημείο 16 α (νέο)

Κανονισμός (ΕΕ) 2019/881

Άρθρο 66 α (νέο)

Κείμενο που προτείνει η Επιτροπή

Τροπολογία

16α) προστίθεται το ακόλουθο άρθρο:

Άρθρο 66 α (νέο)

Άσκηση της εξουσιοδότησης

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

2. Η προβλεπόμενη στο άρθρο 49 παράγραφος 7α εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων ανατίθεται στην Επιτροπή για περίοδο 5 ετών από την ... [ημερομηνία έναρξης ισχύος της βασικής νομοθετικής πράξης ή από οποιαδήποτε

άλλη ημερομηνία ορίζουν οι συννομοθέτες]. Η Επιτροπή υποβάλλει έκθεση σχετικά με τις εξουσίες που της έχουν ανατεθεί το αργότερο εννέα μήνες πριν από τη λήξη της περιόδου των πέντε ετών. Η εξουσιοδότηση ανανεώνεται σιωπηρά για περιόδους ίδιας διάρκειας, εκτός αν το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο προβάλλουν αντιρρήσεις το αργότερο εντός τριών μηνών πριν από τη λήξη της κάθε περιόδου.

3. Η εξουσιοδότηση που προβλέπεται στο άρθρο 49 παράγραφος 7α μπορεί να ανακληθεί ανά πάσα στιγμή από το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο. 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 7α 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 εν λόγω προθεσμία παρατείνεται κατά [δύο μήνες] με πρωτοβουλία του Ευρωπαϊκού Κοινοβουλίου ή του Συμβουλίου.

Or. en

Τροπολογία 49
Enĵen Toĥenovský

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 1 – σημείο 17 – εισαγωγικό μέρος
Κανονισμός (ΕΕ) 2019/881
Άρθρο 67

Κείμενο που προτείνει η Επιτροπή

17) στο άρθρο 67, οι παράγραφοι 2 και 3 αντικαθίστανται από το ακόλουθο κείμενο:

Τροπολογία

17) στο άρθρο 67, οι παράγραφοι **1, 2, 3 και 4** αντικαθίστανται από το ακόλουθο κείμενο:

Or. en

Τροπολογία 50
Enĵen Toĥenovský

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 1 – σημείο 17
Κανονισμός (ΕΕ) 2019/881
Άρθρο 67 – παράγραφος 1

Κείμενο που προτείνει η Επιτροπή

Τροπολογία

1 Έως τις 28 Ιουνίου 2024 και στη συνέχεια ανά τετραετία, η Επιτροπή αξιολογεί 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 καθήκοντά 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.

Or. en

Τροπολογία 51
Enĵen Toĥenovský

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 1 – σημείο 17
Κανονισμός (ΕΕ) 2019/881
Άρθρο 67 – παράγραφος 2

Κείμενο που προτείνει η Επιτροπή

2. Η αξιολόγηση εξετάζει επίσης τον αντίκτυπο, την αποτελεσματικότητα και την απόδοση των διατάξεων του τίτλου III 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.

Τροπολογία

2. Η αξιολόγηση εξετάζει επίσης τον αντίκτυπο, την αποτελεσματικότητα και την απόδοση των διατάξεων του τίτλου III 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,
συμπεριλαμβανομένης της αξιολόγησης της διαδικασίας και των χρονοδιαγραμμάτων που οδηγούν στην κατάρτιση και την έγκριση των πρώτων ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας, καθώς και του τρόπου με τον οποίο η εν λόγω διαδικασία θα μπορούσε να βελτιωθεί και να επιταχυνθεί για τα επακόλουθα σχήματα πιστοποίησης.

Or. en

Τροπολογία 52
Enĵen Toĥenovský

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 1 – σημείο 17
Κανονισμός (ΕΕ) 2019/881
Άρθρο 67 – παράγραφος 4

Κείμενο που προτείνει η Επιτροπή

Τροπολογία

4. Έως τις 28 Ιουνίου 2024 και στη συνέχεια ανά τετραετία, 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. Η έκθεση συνοδεύεται, εφόσον είναι αναγκαίο, από νομοθετική πρόταση.

Or. en