ΕΙΔΙΚΉ ΈΚΘΕΣΗ 19/2026 **EL**

Εντοπισμός και αντιμετώπιση περιστατικών κυβερνοασφάλειας

Το πλαίσιο συνεργασίας της ΕΕ σημειώνει πρόοδο, είναι όμως εν μέρει μόνο αποτελεσματικό εξαιτίας καθυστερήσεων στην υλοποίηση και της περιορισμένης ανταλλαγής πληροφοριών

CURIA RATIONUM
ΕΥΡΩΠΑΪΚΟ ΕΛΕΓΚΤΙΚΟ ΣΥΝΕΔΡΙΟ

Περιεχόμενα

Σημείο

Παραρτήματα

Παράρτημα I – Σχετικά με τον έλεγχο

Παράρτημα II – Το τοπίο της κυβερνοασφάλειας της ΕΕ

Παράρτημα III – Επιλεγμένες δράσεις κυβερνοασφάλειας

Παράρτημα IV – Αξιολόγηση από το ΕΕΣ των χρηματοδοτούμενων από την ΕΕ έργων κυβερνοασφάλειας

Συντομογραφίες

Γλωσσάριο

Απαντήσεις της Επιτροπής

Απαντήσεις του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Θέματα Κυβερνοασφάλειας (ECCC)

Απαντήσεις του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA)

Χρονογραμμή

Κλιμάκιο ελέγχου

01

Κύρια μηνύματα

Το θέμα και η σημασία του

01 Οι κίνδυνοι κυβερνοεπιθέσεων αυξάνονται όσο περισσότερο ψηφιοποιούνται η οικονομία μας και η καθημερινότητά μας. Η κυβερνοασφάλεια ορίζεται ως «οι δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων»[1] και απαιτεί μια ολιστική προσέγγιση για την πρόληψη, τον εντοπισμό, την αντιμετώπιση και την ανάκαμψη από κυβερνοαπειλές.

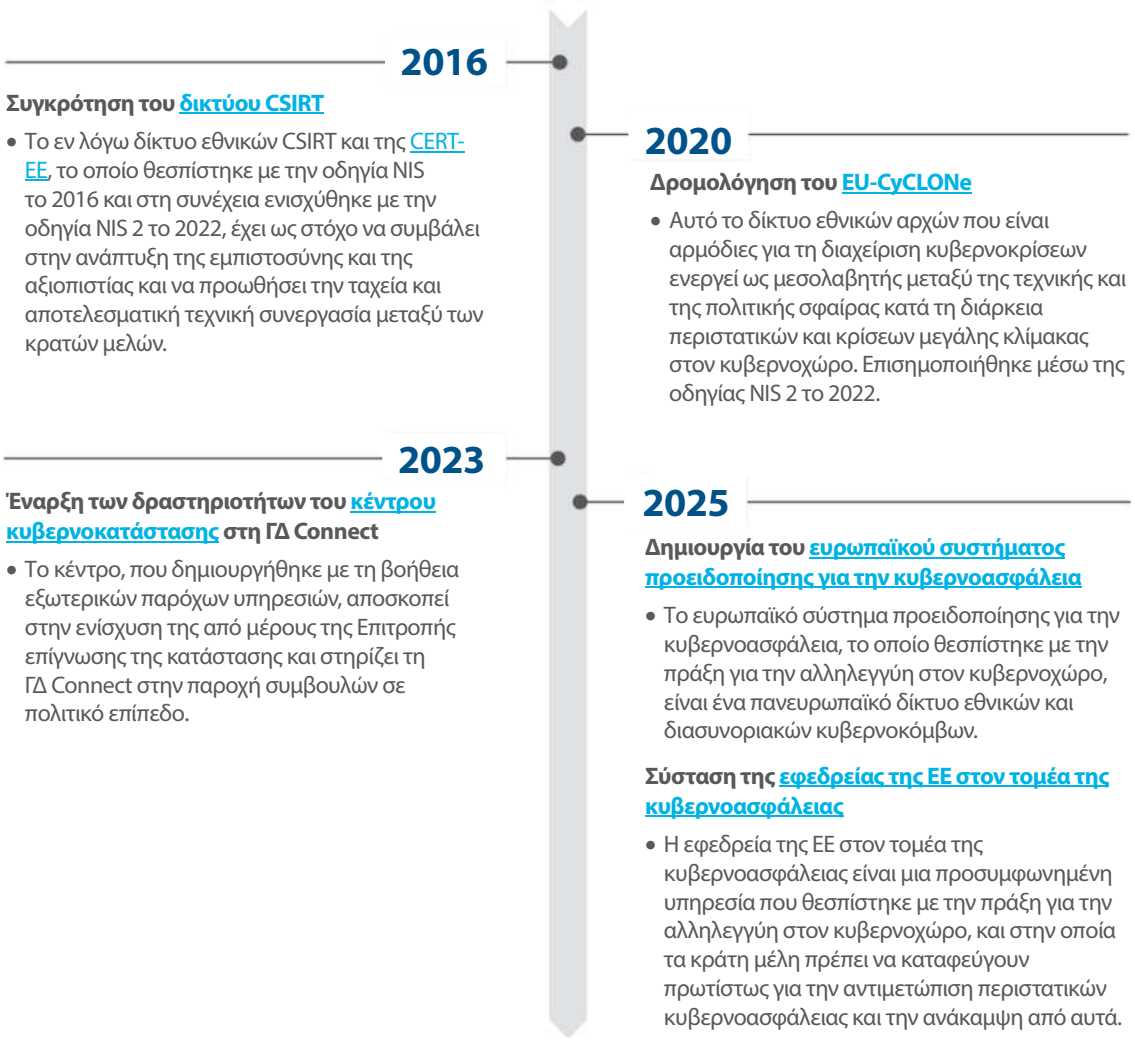
02 Στον τομέα της κυβερνοασφάλειας της ΕΕ που δεν άπτεται του στρατιωτικού κλάδου, συμμετέχουν πολυάριθμες δημόσιες και ιδιωτικές οντότητες σε περιφερειακό, εθνικό και ενωσιακό επίπεδο. Η κυβερνοασφάλεια αποτελεί επίσης βασική συνιστώσα της εθνικής ασφάλειας και άμυνας.

[1] Κανονισμός (ΕΕ) 2019/881 («Πράξη για την κυβερνοασφάλεια»).

03 Τα κράτη μέλη φέρουν την πρωταρχική ευθύνη για την πρόληψη περιστατικών και κρίσεων κυβερνοασφάλειας που τα επηρεάζουν, για την προετοιμασία έναντι τέτοιου ενδεχομένου, καθώς και για την αντιμετώπισή τους. Δεδομένου ότι τα περιστατικά αυτά μπορούν να επηρεάσουν την ομαλή λειτουργία της εσωτερικής αγοράς, ο ρόλος της ΕΕ είναι επίσης σημαντικός σε περίπτωση σημαντικού περιστατικού ή κρίσης. Τα τελευταία χρόνια, η ΕΕ έχει ενισχύσει το εξελισσόμενο κανονιστικό της πλαίσιο για την κυβερνοασφάλεια[2] και έχει καθιερώσει δίκτυα και μηχανισμούς, όπως φαίνεται στο ***γράφημα 1*** κατωτέρω και στο ***παράρτημα II***.

[2] Παραδείγματος χάριν, η Επιτροπή πρότεινε τη δέσμη μέτρων Omnibus για τον ψηφιακό τομέα τον Νοέμβριο του 2025 και την αναθεωρημένη πράξη της ΕΕ για την κυβερνοασφάλεια τον Ιανουάριο του 2026.

Γράφημα 1 | Δίκτυα και μηχανισμοί της ΕΕ για την κυβερνοασφάλεια, από το 2016 έως το 2025



CSIRT: ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές
ΓΔ Connect: Γενική Διεύθυνση Επικοινωνιακών Δικτύων, Περιεχομένου και Τεχνολογιών
EU-CyCLONe: Ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για τις κρίσεις στον κυβερνοχώρο
Οδηγία NIS: Οδηγία (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση
Οδηγία NIS 2: Οδηγία (ΕΕ) 2022/2555 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση

Πηγή: ΕΕΣ.

04 Στο πλαίσιο του τρέχοντος πολυετούς δημοσιονομικού πλαισίου 2021-2027, η κύρια πηγή χρηματοδότησης για την κυβερνοασφάλεια είναι το πρόγραμμα «Ψηφιακή Ευρώπη» (DIGITAL). Διαθέτει συνολικό προϋπολογισμό ύψους 8,1 δισεκατομμυρίων ευρώ, εκ των οποίων 1,4 δισεκατομμύρια διατίθενται για την ενίσχυση της κυβερνοασφάλειας.

05 Στόχος του ελέγχου μας ήταν να αξιολογηθεί αν οι δράσεις της ΕΕ διευκολύνουν αποτελεσματικά τον εντοπισμό και την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας. Ελέγξαμε αν αυτό ίσχυε στις εξής περιπτώσεις:

- δίκτυα και μηχανισμούς σε επίπεδο ΕΕ [δηλαδή το δίκτυο ομάδων αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (δίκτυο CSIRT), το ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (EU-CyCLONe), το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια, το κέντρο κυβερνοκατάστασης και η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας]·
- δράσεις που χρηματοδοτούνται στο πλαίσιο του προγράμματος DIGITAL.

06 Αναμένουμε ότι τα ευρήματά μας θα συμβάλουν στην ενίσχυση της κυβερνοανθεκτικότητας της ΕΕ, βελτιώνοντας την αποτελεσματικότητα και την αποδοτικότητα των δικτύων και των μηχανισμών της ΕΕ, καθώς και τον τρόπο επιλογής και παρακολούθησης των χρηματοδοτούμενων από την ΕΕ δράσεων.

07 Ο έλεγχος κάλυψε την περίοδο από το 2022 έως το 2025. Βασίζεται σε εξέταση και ανάλυση σχετικών εγγράφων, σε επισκέψεις ελέγχου σε τρία κράτη μέλη, την Ιρλανδία, την Ελλάδα και την Ιταλία, καθώς και σε γραπτά ερωτηματολόγια και συνεντεύξεις με συμφεροντούχους. Περαιτέρω γενικές πληροφορίες και λεπτομέρειες σχετικά με την εμβέλεια και την προσέγγιση του ελέγχου παρατίθενται στο ***παράρτημα I***.

Τα ευρήματα και οι συστάσεις μας

08 Συνολικά, καταλήγουμε στο συμπέρασμα ότι οι δράσεις της ΕΕ διευκολύνουν μόνον εν μέρει τον εντοπισμό και την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας. Ενώ έχει τεθεί σταδιακά σε εφαρμογή ένα πλαίσιο συνεργασίας, οι εργασίες συνεχίζονται καθώς δεν είναι ακόμη πλήρως λειτουργικό. Η περιορισμένη ανταλλαγή πληροφοριών, οι αδυναμίες στην αναφορά στοιχείων και οι αξιοσημείωτες καθυστερήσεις στην εφαρμογή παρεμποδίζουν την πλήρη αξιοποίηση των δυνατοτήτων των δικτύων και μηχανισμών της ΕΕ. Τα έργα που χρηματοδοτούνται από το πρόγραμμα DIGITAL επιδιώκουν σχετικούς στόχους, αλλά αρκετά αντιμετωπίζουν επιχειρησιακές προκλήσεις και καθυστερήσεις, ενώ υπάρχουν αδυναμίες στο συνολικό πλαίσιο παρακολούθησης των επιδόσεων.

09 Το ισχύον πλαίσιο των δικτύων και των μηχανισμών της ΕΕ για τη διευκόλυνση του εντοπισμού και της αντιμετώπισης σημαντικών περιστατικών κυβερνοασφάλειας αναπτύχθηκε σταδιακά. Το 2025 το Συμβούλιο ενέκρινε το σχέδιο στρατηγικής για τον κυβερνοχώρο, το οποίο καθορίζει το πλαίσιο της ΕΕ για τη διαχείριση κυβερνοκρίσεων. Διαπιστώσαμε ότι το εν λόγω σχέδιο αποσαφηνίζει σε μεγάλο βαθμό τους ρόλους και τις αρμοδιότητες όσον αφορά τη διαχείριση κυβερνοκρίσεων στην ΕΕ. Ωστόσο, οι διαδικαστικές ρυθμίσεις σχετικά με τον τρόπο με τον οποίο θα πρέπει να συνεργάζονται το δίκτυο CSIRT (που δημιουργήθηκε το 2016) και το EU-CyCLONe (που τέθηκε επίσημα σε λειτουργία το 2023) δεν έχουν ακόμη επισημοποιηθεί (σημεία ***24***-***30***).

10 Διαπιστώσαμε ότι η ανταλλαγή πληροφοριών μέσω αυτών των δικτύων είναι περιορισμένη. Αυτό οφείλεται κυρίως σε καθυστερήσεις στη μεταφορά της οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση (οδηγία NIS 2) στα εθνικά δίκαια, σε δυσκολίες στον προσδιορισμό του κατά πόσον ένα περιστατικό έχει διασυνοριακό αντίκτυπο και στην εθνική νομοθεσία για την ασφάλεια που εμποδίζει την ανταλλαγή πληροφοριών. Η προστιθέμενη αξία των δικτύων μειώνεται σημαντικά εάν τα κράτη μέλη δεν είναι πρόθυμα να ανταλλάσσουν έγκαιρες και αξιοποιήσιμες πληροφορίες (σημεία ***31***-***44***).

Σύσταση 1

Ενίσχυση της ανταλλαγής πληροφοριών μεταξύ των κρατών μελών

Για τη βελτίωση του εντοπισμού και της αντιμετώπισης περιστατικών κυβερνοασφάλειας, η Επιτροπή, σε συνεργασία με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), πρέπει:

α) να προτείνει, στην ομάδα συνεργασίας για την ασφάλεια δικτύων και πληροφοριών, να διενεργήσει λεπτομερή ανάλυση των περιορισμών εθνικής ασφάλειας που παρεμποδίζουν την ανταλλαγή πληροφοριών και επηρεάζουν την κυβερνοανθεκτικότητα της ΕΕ, και να βρει νομικές και τεχνικές λύσεις για να ενισχυθεί η ανταλλαγή πληροφοριών, τηρουμένων παράλληλα των ορίων που επιβάλλει η εθνική ασφάλεια·

β) με την επιφύλαξη των αποφάσεων των συννομοθετών, να διασφαλίσει, σε συνεργασία με τα κράτη μέλη, ότι το ενιαίο σημείο εισόδου για την αναφορά περιστατικών που προτείνεται στη δέσμη μέτρων Omnibus για τον ψηφιακό τομέα είναι ικανό να εντοπίζει πιθανά διασυνοριακά περιστατικά·

γ) να επεξεργαστεί λύσεις προκειμένου να καταστεί δυνατή η αναφορά συμβάντων στον ENISA σε πραγματικό χρόνο.

Ημερομηνία-στόχος: 2027 για τα α) και β), 2028 για το γ)

11 Το 2022 η Επιτροπή δημιούργησε το λεγόμενο «κέντρο κυβερνοκατάστασης» για να αυξήσει την από μέρους της επίγνωση της κατάστασης, με σκοπό τη στήριξη των θεσμικών αρμοδιοτήτων της για τη διαχείριση κρίσεων. Η λειτουργία του κέντρου υποστηρίζεται σε μεγάλο βαθμό από σύμβαση που συνάπτεται με εξωτερικούς παρόχους υπηρεσιών. Διαπιστώσαμε ότι το έργο που επιτελείται από εξωτερικούς παρόχους υπηρεσιών επικαλύπτει εν μέρει την υφιστάμενη ικανότητα του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) όσον αφορά την επίγνωση της κατάστασης και την παρακολούθηση των απειλών. Θεωρούμε ότι με τον τρόπο με τον οποίο συστάθηκε το κέντρο κυβερνοκατάστασης δεν αξιοποιήθηκαν επαρκώς οι δυνατότητες εξορθολογισμού που θα προσέφερε η χρήση των πληροφοριών που είχαν ήδη στη διάθεσή τους η Επιτροπή και ο ENISA. Επιπλέον, η απουσία ολοκληρωμένου, λεπτομερούς σχεδίου για το μέλλον μετά τη λήξη της σύμβασης καθιστά επισφαλή τη λειτουργία του κέντρου κυβερνοκατάστασης μετά το 2026 (σημεία ***45***-***51***).

Σύσταση 2

Εξορθολογισμός των ικανοτήτων επίγνωσης της κατάστασης στον τομέα της κυβερνοασφάλειας στην ΕΕ και βελτιστοποίηση της διάδοσης των πληροφοριών

Για μεγαλύτερη αποδοτικότητα, η Επιτροπή πρέπει, σε συνεργασία με τον ENISA, να αξιολογήσει τη σκοπιμότητα της από κοινού απόκτησης και ανάλυσης πληροφοριών για την επίγνωση της κατάστασης. Θα πρέπει επίσης να καθιστά τις πληροφορίες αυτές και τις σχετικές εκθέσεις για τις κυβερνοαπειλές διαθέσιμες σε όλες τις αρμόδιες υπηρεσίες και οργανισμούς της ΕΕ.

Ημερομηνία-στόχος: 2027

12 Η πράξη του 2024 για την αλληλεγγύη στον κυβερνοχώρο θεσπίζει την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, η οποία αποσκοπεί στη στήριξη των κρατών μελών για την αντιμετώπιση σοβαρών περιστατικών κυβερνοασφάλειας και την ανάκαμψη από αυτά. Την εφεδρεία αυτή απαρτίζουν επιλεγμένοι πάροχοι υπηρεσιών για κάθε κράτος μέλος, οι οποίοι μπορούν να αποκρίνονται σε περιστατικά σε εικοσιτετράωρη βάση. Μολονότι η προσέγγιση αυτή συμβάλλει στην αντιμετώπιση των ειδικών απαιτήσεων των κρατών μελών και στην οικοδόμηση εμπιστοσύνης, ο διαθέσιμος προϋπολογισμός κατανέμεται ισομερώς μεταξύ τους και δεν λαμβάνει υπόψη τις ειδικές ανάγκες κάθε κράτους μέλους (σημεία ***52***-***57***).

13 Θεωρούμε ότι η χρήση από πριν συμβεβλημένων παρόχων καθιστά δυνατή την ταχεία ανάπτυξη υπηρεσιών αντιμετώπισης περιστατικών. Μολονότι η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας αποσκοπεί πρωτίστως στη στήριξη της αντιμετώπισης και της ανάκαμψης, όταν δεν χρησιμοποιείται για την αντιμετώπιση περιστατικών, μπορεί να εξυπηρετεί σκοπούς ετοιμότητας. Με την ευέλικτη αυτή προσέγγιση αποτρέπεται το ενδεχόμενο προπληρωμένες υπηρεσίες να παραμείνουν σε αχρησία. Ωστόσο, η εφεδρεία κινδυνεύει να χρησιμοποιηθεί κυρίως για σκοπούς ετοιμότητας και όχι αντιμετώπισης, σε αντίθεση με τον επιδιωκόμενο σκοπό της (σημεία ***58***-***61***).

14 Το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια είναι ένα δίκτυο εθνικών και διασυνοριακών κυβερνοκόμβων που αποσκοπούν στη βελτίωση του εντοπισμού, της ανάλυσης και της αντιμετώπισης κυβερνοαπειλών. Διαπιστώσαμε ότι, κατά τον χρόνο του ελέγχου, λόγω αξιοσημείωτων καθυστερήσεων στην προμήθεια εργαλείων και υπηρεσιών, οι δύο κόμβοι (ATHENA και ENSOC) δεν είχαν ξεκινήσει ακόμη να λειτουργούν και ότι το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια δεν λειτουργούσε ακόμη (σημεία ***62***-***70***).

15 Ένας από τους βασικούς στόχους του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια είναι η ενθάρρυνση της ουσιαστικής ανταλλαγής πληροφοριών μεταξύ ομάδων κρατών μελών. Μολονότι αυτό έχει τη δυνατότητα να επιλύσει ορισμένα από τα προβλήματα στην ανταλλαγή πληροφοριών, είναι επίσης πολύ δύσκολο να ενσωματωθούν οι κυβερνοκόμβοι στο ήδη πολύπλοκο τοπίο της κυβερνοασφάλειας. Διαπιστώσαμε ότι οι συμφωνίες συνεργασίας, η κοινή ταξινόμηση και τα πρότυπα διαλειτουργικότητας που απαιτούνται για την πλήρη λειτουργία του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια δεν είχαν ακόμη τεθεί σε εφαρμογή (σημεία ***71***-***74***).

Σύσταση 3

Ενσωμάτωση του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια στο τοπίο της κυβερνοασφάλειας της ΕΕ

Η Επιτροπή πρέπει, από κοινού με τον ENISA και τα κράτη μέλη, να διασφαλίσει την εφαρμογή ρυθμίσεων συνεργασίας και προτύπων διαλειτουργικότητας για τη διευκόλυνση της ανταλλαγής πληροφοριών μεταξύ των διασυνοριακών κόμβων που συμμετέχουν στο ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια, το δίκτυο CSIRT και το EU-CyCLONe.

Ημερομηνία-στόχος: 2028

16 Το 2018 η Επιτροπή πρότεινε τη δημιουργία του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Θέματα Κυβερνοασφάλειας (ECCC) για τη διαχείριση της συνιστώσας κυβερνοασφάλειας του προγράμματος DIGITAL, αρχής γενομένης από το 2021. Ο κανονισμός ECCC απαιτούσε τη δημιουργία μιας κοινότητας ικανοτήτων στον τομέα της κυβερνοασφάλειας, η οποία θα απαρτίζεται από εκπροσώπους της βιομηχανίας, ακαδημαϊκών και ερευνητικών οργανισμών. Στη συνέχεια, επιλεγμένα μέλη από την κοινότητα ικανοτήτων στον τομέα της κυβερνοασφάλειας θα συγκροτούσαν στρατηγική συμβουλευτική ομάδα (SAG) (σημεία ***75*** και ***76***).

17 Διαπιστώσαμε καθυστερήσεις τόσο όσον αφορά την επίτευξη της οικονομικής αυτονομίας του ECCC όσο και σχετικά με τη συγκρότηση της κοινότητας ικανοτήτων στον τομέα της κυβερνοασφάλειας και της SAG, κάτι που σήμαινε ότι η κοινότητα ικανοτήτων στον τομέα της κυβερνοασφάλειας και η SAG δεν ήταν σε θέση να συμβάλλουν στη διαμόρφωση των προγραμμάτων εργασίας του DIGITAL. Θεωρούμε ότι εν προκειμένω χάθηκε μια ευκαιρία (σημεία ***77***-***81***).

18 Διαπιστώσαμε ότι όλα τα έργα που εξετάσαμε επιδίωκαν συναφείς στόχους που συμβάλλουν στην επίτευξη των στόχων της κυβερνοασφάλειας του DIGITAL. Ωστόσο, εντοπίσαμε περιπτώσεις στις οποίες η ποιότητα ή τα αποτελέσματα που επιτεύχθηκαν δεν ήταν ικανοποιητικά, κυρίως εξαιτίας καθυστερήσεων στην υλοποίηση (σημεία ***82***-***87***).

19 Ο κανονισμός DIGITAL προβλέπει ότι, για λόγους ασφάλειας, η χρηματοδότηση για την κυβερνοασφάλεια μπορεί να περιορίζεται σε οντότητες που είναι εγκατεστημένες στα κράτη μέλη και ελέγχονται πολίτες της ΕΕ. Η κεντρική υπηρεσία επικύρωσης στον Ευρωπαϊκό Εκτελεστικό Οργανισμό Έρευνας διενεργεί την εν λόγω αξιολόγηση του ιδιοκτησιακού καθεστώτος και του ελέγχου για λογαριασμό του ECCC (σημεία ***88***-***91***).

20 Στην περίπτωση χρηματοδοτικής στήριξης προς τρίτους, η αξιολόγηση του ιδιοκτησιακού καθεστώτος και του ελέγχου αποτελεί ευθύνη των δικαιούχων του έργου, με βάση τη δική τους προσέγγιση και μεθοδολογία. Διαπιστώσαμε ότι το ECCC δεν επικυρώνει τη μεθοδολογία τους ούτε διενεργεί ελέγχους για να διασφαλίσει ότι επιλεγμένα τρίτα μέρη είναι εγκατεστημένα στην ΕΕ και ελέγχονται από κράτη μέλη ή πολίτες της ΕΕ. Θεωρούμε ότι υπάρχει σημαντικός κίνδυνος οι δικαιούχοι να μην έχουν την ικανότητα να διενεργούν σωστά τους εν λόγω ελέγχους. Ο κίνδυνος αυτός δεν έχει μετριαστεί επαρκώς και θα μπορούσε να οδηγήσει στην έκθεση ευαίσθητων υποδομών, επιχειρησιακών δεδομένων και κρίσιμων για την ασφάλεια τεχνολογιών (σημεία ***92***-***96***).

Σύσταση 4

Εξασφάλιση της διενέργειας διεξοδικής αξιολόγησης του ιδιοκτησιακού καθεστώτος και του ελέγχου των οντοτήτων που λαμβάνουν χρηματοδότηση από την ΕΕ στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη»

Το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Θέματα Κυβερνοασφάλειας πρέπει:

α) να αποκομίσει εύλογη βεβαιότητα ότι οι δικαιούχοι που είναι υπεύθυνοι για την παροχή χρηματοδοτικής στήριξης σε τρίτους διαθέτουν την απαιτούμενη διοικητική και τεχνική ικανότητα για τη διενέργεια επαρκών αξιολογήσεων ιδιοκτησιακού καθεστώτος και ελέγχου, με βάση την υφιστάμενη μεθοδολογία που έχουν στη διάθεσή τους οι δικαιούχοι που υλοποιούν δράσεις χρηματοδοτικής στήριξης σε τρίτους·

β) να ελέγξει, βάσει δείγματος, κατά πόσον η ενωσιακή χρηματοδότηση έχει χορηγηθεί αποκλειστικά σε επιλέξιμες οντότητες.

Ημερομηνία-στόχος: 2026 για το α) και 2027 για το β)

21 Οι δικαιούχοι που διαχειρίζονται έργα χρηματοδοτούμενα από την ΕΕ πρέπει να αναφέρουν στοιχεία σχετικά με την πρόοδο και τα αποτελέσματά τους στο ECCC, χρησιμοποιώντας ορόσημα και παραδοτέα. Αμφότερα είναι καίριας σημασίας για την παρακολούθηση των έργων, και πρέπει να καθορίζονται με τον κατάλληλο τρόπο. Διαπιστώσαμε ότι σχεδόν κανένα από τα έργα του δείγματός μας δεν είχε ακολουθήσει τις οδηγίες σχετικά με τον τρόπο κατάρτισης των ορόσημων και των παραδοτέων και ότι πολλά από αυτά δεν ήταν καν χρήσιμα για την παρακολούθηση της προόδου (σημεία ***97***-***99***).

22 Διαπιστώσαμε ότι πολλοί από τους δείκτες επιδόσεων που χρησιμοποιούν οι δικαιούχοι δεν είναι συναφείς ή μετρήσιμοι και στερούνται τιμής-στόχου ή τιμής βάσης. Επιπλέον, η αναφορά στοιχείων σχετικά με τους εν λόγω δείκτες ήταν ανεπαρκής και, ως εκ τούτου, δεν μπορεί να χρησιμεύει για την αξιολόγηση των επιδόσεων των έργων (σημεία ***100***-***102***).

23 Για την παρακολούθηση των επιτευγμάτων του προγράμματος DIGITAL στο σύνολό του, όλα τα έργα πρέπει να αναφέρουν στοιχεία σχετικά με ειδικούς δείκτες του προγράμματος που τροφοδοτούν τις ετήσιες δηλώσεις επιδόσεων προγράμματος της Επιτροπής. Το ECCC είναι υπεύθυνο για τη συλλογή και την επαλήθευση των δεδομένων που αναφέρονται σε σχέση με τους εν λόγω δείκτες. Εντοπίσαμε αρκετά προβλήματα στον τρόπο συλλογής των δεδομένων αλλά και στη συνολική ποιότητά τους. Δεν εντοπίσαμε τεκμήρια από τα οποία να προκύπτει ότι το ECCC επαλήθευε την ακρίβεια των αναφερόμενων δεδομένων. Βάσει των δειγματοληπτικών ελέγχων μας, θεωρούμε ότι τα αναφερόμενα δεδομένα δεν αντικατοπτρίζουν με ακρίβεια τα αποτελέσματα που επιτυγχάνονται (σημεία ***103-106***).

Σύσταση 5

Ενίσχυση του πλαισίου παρακολούθησης των επιδόσεων της συνιστώσας κυβερνοασφάλειας του προγράμματος «Ψηφιακή Ευρώπη»

Για να καταστεί δυνατή η επαρκής παρακολούθηση της προόδου και των επιδόσεων, το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Θέματα Κυβερνοασφάλειας πρέπει:

a) να διασφαλίζει, πριν από την υπογραφή της εκάστοτε επιχορήγησης, ότι όλα τα έργα έχουν καθορισμένα ορόσημα, παραδοτέα και δείκτες επιδόσεων που συμμορφώνονται με τις οδηγίες που παρέχονται στο έντυπο της αίτησης·

b) να σχεδιάσει και να εφαρμόσει ένα άρτιο σύστημα για τη συλλογή, την ιχνηλασιμότητα, την επαλήθευση και τη συσσωμάτωση των δεδομένων για τους δείκτες επιδόσεων της συνιστώσας κυβερνοασφάλειας του προγράμματος «Ψηφιακή Ευρώπη», ώστε να διασφαλίζεται ότι οι δείκτες αντικατοπτρίζουν με ακρίβεια τα αποτελέσματα που επιτυγχάνονται.

Ημερομηνία-στόχος: 2027

02

Οι παρατηρήσεις μας αναλυτικότερα

Αν και τα δίκτυα και οι μηχανισμοί της ΕΕ για την κυβερνοασφάλεια στηρίζουν δράσεις συνεργασίας και απόκρισης, η περιορισμένη ανταλλαγή πληροφοριών και η ελλιπής υλοποίηση αποδυναμώνουν την αποτελεσματικότητά τους

Τα δίκτυα της ΕΕ διευκολύνουν τη συνεργασία των κρατών μελών, ωστόσο η περιορισμένη ανταλλαγή πληροφοριών μειώνει την προστιθέμενη αξία τους

24 Το ισχύον ενωσιακό πλαίσιο δικτύων και μηχανισμών για τη διευκόλυνση του εντοπισμού και της αντιμετώπισης σημαντικών περιστατικών κυβερνοασφάλειας αναπτύχθηκε σταδιακά, αρχής γενομένης από τη θέσπιση της οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση[3] (οδηγία NIS), η οποία τέθηκε σε ισχύ τον Αύγουστο του 2016. Στο ***παράρτημα II*** παρουσιάζουμε σχηματικά το τρέχον τοπίο της ΕΕ.

[3] Οδηγία (ΕΕ) 2016/1148.

Τα δίκτυα της ΕΕ καθιστούν δυνατή τη συνεργασία των κρατών μελών σε τεχνικό και επιχειρησιακό επίπεδο

25 Με την οδηγία NIS δημιουργήθηκε το δίκτυο CSIRT, στο οποίο συμμετέχουν η CERT-ΕΕ (Υπηρεσία Κυβερνοασφάλειας για τα Θεσμικά και Λοιπά Όργανα και Οργανισμούς της Ένωσης) και οι CSIRT που ορίζονται από τα κράτη μέλη. Το δίκτυο αυτό αποσκοπεί στην οικοδόμηση εμπιστοσύνης μεταξύ των εθνικών CSIRT και στην προώθηση της ταχείας και αποτελεσματικής επιχειρησιακής συνεργασίας μεταξύ των κρατών μελών.

26 Το EU-CyCLONe συγκροτήθηκε το 2020 ως άτυπο δίκτυο συνεργασίας των εθνικών αρχών που είναι αρμόδιες για τη διαχείριση κυβερνοκρίσεων. Χρησιμεύει ως γέφυρα μεταξύ του τεχνικού επιπέδου στο οποίο λειτουργεί το δίκτυο CSIRT και του πολιτικού επιπέδου του Συμβουλίου της Ευρωπαϊκής Ένωσης και των ολοκληρωμένων ρυθμίσεών του για την πολιτική αντιμετώπιση κρίσεων. Με την έναρξη ισχύος της οδηγίας NIS 2 το 2023 επισημοποιήθηκε ο ρόλος του EU-CyCLONe, το οποίο και έλαβε σαφή εντολή.

27 Αξιολογήσαμε κατά πόσον οι ρόλοι και οι αρμοδιότητες των εν λόγω δικτύων σε επίπεδο ΕΕ είναι σαφώς καθορισμένοι και κατά πόσον καθιστούν δυνατή τη συνεργασία των κρατών μελών.

28 Ο ENISA ενεργεί ως γραμματεία του δικτύου CSIRT και του EU-CyCLONe και τους παρέχει πόρους, εμπειρογνωσία, υποδομές και τα εργαλεία ΤΠ που χρειάζονται για να συνεργαστούν και να επικοινωνούν με ασφάλεια με σκοπό την ανταλλαγή πληροφοριών. Στην έρευνα που διενήργησε σχετικά με τον βαθμό ικανοποίησης των συμφεροντούχων[4] στις αρχές του 2025, ο ENISA έλαβε καλές βαθμολογίες όσον αφορά τις επιδόσεις του ως γραμματείας των εν λόγω δικτύων. Αυτή η θετική αναπληροφόρηση επιβεβαιώθηκε και κατά τις επισκέψεις ελέγχου μας, στο πλαίσιο των οποίων οι εθνικές αρχές κυβερνοασφάλειας εξέφρασαν την εκτίμησή τους.

[4] ENISA, Ενοποιημένη ετήσια έκθεση δραστηριοτήτων για το 2024, σ. 33 και 36.

29 Το 2025, το Συμβούλιο ενέκρινε το σχέδιο στρατηγικής για τον κυβερνοχώρο, το οποίο καθορίζει τους ρόλους και τις αρμοδιότητες των βασικών παραγόντων (συμπεριλαμβανομένου του δικτύου CSIRT και του EU-CyCLONe) και των μηχανισμών που εμπλέκονται στα διάφορα στάδια περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας ή κυβερνοκρίσεων. Διαπιστώσαμε ότι το σχέδιο στρατηγικής για τον κυβερνοχώρο αποσαφηνίζει σε μεγάλο βαθμό τους ρόλους και τις αρμοδιότητες σε σχέση με τη διαχείριση κυβερνοκρίσεων στην ΕΕ και λαμβάνει υπόψη τις αλλαγές που έχει υποστεί το τοπίο της κυβερνοασφάλειας από το πρώτο σχέδιο στρατηγικής το 2017. Καθορίζει τρία επίπεδα συνεργασίας: ένα τεχνικό, ένα επιχειρησιακό και ένα τρίτο πολιτικό. Περιγράφει λεπτομερώς τα νέα δίκτυα και τις δομές που έχουν δημιουργηθεί από το 2017, όπως το EU-CyCLONe, οι ενωσιακές ομάδες ταχείας αντίδρασης σε υβριδικές ενέργειες και το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια, και εξετάζει τον τρόπο με τον οποίο η διαχείριση κυβερνοκρίσεων θα πρέπει να ενσωματωθεί στο ευρύτερο πλαίσιο της ΕΕ για την αντιμετώπιση κρίσεων.

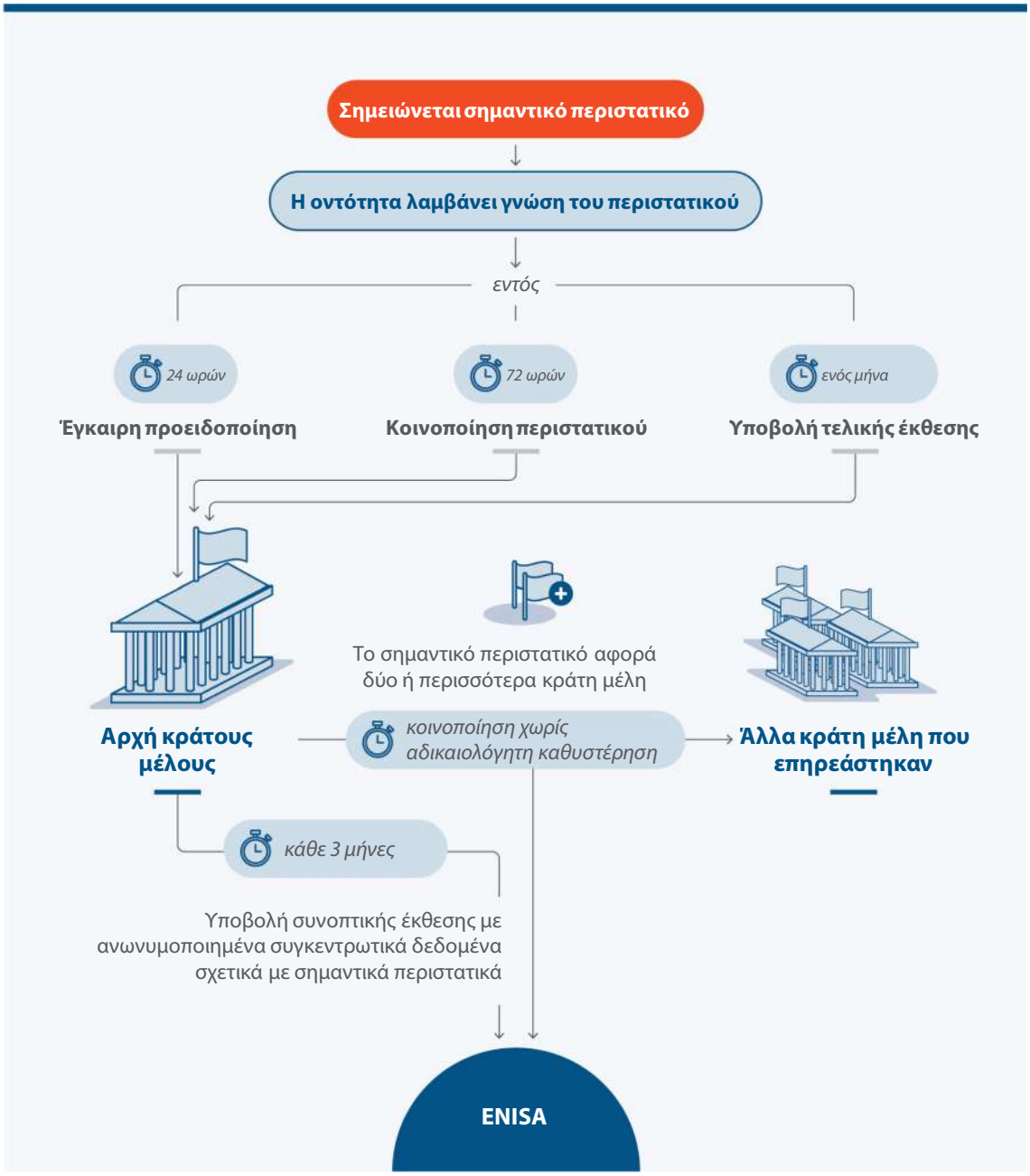
30 Εντούτοις, παρά την επίσημη σύσταση του δικτύου CSIRT το 2016 και του EU-CyCLONe το 2023, τα δύο δίκτυα δεν έχουν ακόμη επισημοποιήσει τους διαδικαστικούς όρους που θα ρυθμίζουν τη μεταξύ τους συνεργασία. Επίσης, δεν έχουν συμφωνήσει βάσει ποιων κριτηρίων το δίκτυο CSIRT θα ενημερώνει το EU-CyCLONe ότι ένα παρατηρούμενο περιστατικό κυβερνοασφάλειας συνιστά δυνητικό ή εν εξελίξει περιστατικό κυβερνοασφάλειας μεγάλης κλίμακας. Τα δύο δίκτυα πρέπει επίσης να συμφωνήσουν σε μια κοινή ταξινομία όσον αφορά τα επίπεδα σοβαρότητας των περιστατικών και βασικές έννοιες, όπως η «απειλή», ο «παράγοντας απειλής», το «περιστατικό» ή ο «αντίκτυπος», η οποία είναι απαραίτητη προϋπόθεση για την αυτοματοποίηση της ανταλλαγής πληροφοριών. Επί του παρόντος, υπάρχει περιθώριο για διαφορετικές ερμηνείες ως προς το πότε ένα περιστατικό μπορεί να χαρακτηριστεί σημαντικό ή μεγάλης κλίμακας. Οι αρχές κυβερνοασφάλειας και των τριών κρατών μελών που επισκεφθήκαμε ανέφεραν την έλλειψη κοινής ταξινομίας.

Η περιορισμένη ανταλλαγή πληροφοριών και αναφορά στοιχείων αποδυναμώνει σημαντικά την προστιθέμενη αξία αυτών των δικτύων

31 Τα γεωγραφικά σύνορα δεν αποτρέπουν την εμφάνιση και την εξάπλωση περιστατικών κυβερνοασφάλειας και κυβερνοεπιθέσεων. Η ανταλλαγή πληροφοριών μεταξύ των κρατών μελών σχετικά, παραδείγματος χάριν, με τις τακτικές και τις τεχνικές που χρησιμοποιούν οι παράγοντες απειλής, καθώς και σχετικά με τις ψηφιακές ενδείξεις παραβίασης ενός συστήματος δικτύου ή πληροφοριών («δείκτες παραβίασης»), μπορεί να ενισχύσει σημαντικά την κυβερνοασφάλεια.

32 Διαπιστώσαμε ότι η ανταλλαγή πληροφοριών ήταν περιορισμένη, κάτι που μείωνε σημαντικά την προστιθέμενη αξία των εν λόγω δικτύων. Οι περιορισμοί που παρατηρήσαμε αφορούν κυρίως καθυστερήσεις στη μεταφορά της οδηγίας NIS 2 στα εθνικά δίκαια, ζητήματα σχετικά με τον προσδιορισμό του κατά πόσον ένα περιστατικό έχει διασυνοριακό αντίκτυπο, την εγχώρια νομοθεσία για την εθνική ασφάλεια που περιορίζει την ανταλλαγή πληροφοριών, καθώς και την έλλειψη εμπιστοσύνης.
Η οδηγία NIS 2 θεσπίζει διάφορες απαιτήσεις αναφοράς στοιχείων για τις οντότητες που εμπίπτουν στο πεδίο εφαρμογής της και για τις αρχές των κρατών μελών, όπως φαίνεται στο ***γράφημα 2***.

Γράφημα 2 | Χρονοδιάγραμμα αναφοράς περιστατικών βάσει της οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την ΕΕ (οδηγία NIS 2)



Πηγή: ΕΕΣ, βάσει του ENISA.

33 Τα κράτη μέλη είχαν προθεσμία μέχρι τον Οκτώβριο του 2024 για να μεταφέρουν την οδηγία NIS 2 στο εθνικό τους δίκαιο, αλλά μόνο δύο την τήρησαν. Οι καθυστερήσεις στη μεταφορά έχουν σημαντικές επιπτώσεις στην ανταλλαγή πληροφοριών, καθώς, για όσο διάστημα διαρκεί η καθυστέρηση, οι οντότητες που υπάγονται στην οδηγία NIS 2 δεν δεσμεύονται νομικά να αναφέρουν σχετικά περιστατικά. Η Επιτροπή εκτίμησε[5] ότι 15 500 οντότητες υπάγονταν στην οδηγία NIS, ενώ περισσότερες από 110 000 εμπίπτουν στο πεδίο εφαρμογής της οδηγίας NIS 2. Παραδείγματος χάριν, η δημόσια διοίκηση, που, σύμφωνα με την έκθεση του ENISA για το τοπίο των απειλών του 2025, είναι στην ΕΕ ο τομέας που βρίσκεται περισσότερο από κάθε άλλον στο στόχαστρο, δεν είχε υποχρέωση να αναφέρει περιστατικά βάσει της οδηγίας NIS.

34 Η αναφορά δεδομένων για περιστατικά στον ENISA κάθε τρεις μήνες (δηλαδή πολύ μετά την πιθανή επέλευση ενός περιστατικού) περιορίζει την προστιθέμενη αξία τους. Τα δεδομένα αυτά χρησιμεύουν κυρίως για στατιστικούς σκοπούς και για την αναφορά ιστορικών τάσεων, αλλά όχι για τη βελτίωση του εντοπισμού και της απόκρισης. Ο ENISA παρέχει στα κράτη μέλη ένα διαδικτυακό εργαλείο για να υποβάλλουν τις αναφορές τους. Το υπόδειγμα αναφοράς περιέχει ένα ελάχιστο σύνολο δεδομένων που πρέπει να διαβιβάζονται, όπως το είδος του περιστατικού και ο πληττόμενος τομέας. Επιπλέον, ο ENISA προτείνει στα κράτη μέλη να παρέχουν πρόσθετες πληροφορίες που θα διευκολύνουν τη διεξοδικότερη ανάλυση των δεδομένων, όπως τη σύνδεση περιστατικών με συγκεκριμένα τρωτά σημεία. Ωστόσο, δεν αποφασίζουν όλα τα κράτη μέλη να υποβάλλουν τέτοιες πληροφορίες, γεγονός που μειώνει σημαντικά την ποιότητα και την προστιθέμενη αξία των συλλεγόμενων δεδομένων.

35 Ο ENISA, στην έκθεσή του του 2024 σχετικά με την κατάσταση της κυβερνοασφάλειας στην ΕΕ, δήλωσε ότι είναι πιθανόν οι αναφορές περιστατικών να υπολείπονται της πραγματικότητας, καθώς φαίνεται ότι τα περιστατικά που αναφέρθηκαν ήταν λίγα στον αριθμό. Το διάστημα 2018-2021, τα κράτη μέλη ανέφεραν ετησίως στον ENISA από 100 έως 500 περιστατικά. Ο αριθμός αυξάνεται σταδιακά και, το 2024, ανήλθε σε 1 276[6].

---

[5] Ευρωπαϊκή Επιτροπή, Έκθεση εκτίμησης επιπτώσεων, 2020.

[6] Στοιχεία CIRAS για το 2024.

36 Στην έκθεσή του για το τοπίο των απειλών του 2025, η οποία καλύπτει την περίοδο από τον Ιούνιο του 2024 έως τον Ιούνιο του 2025, ο ENISA εντόπισε περίπου 4 800 περιστατικά κυβερνοασφάλειας[7] μέσω πληροφοριών ανοικτής πηγής, όπως ειδησεογραφικά άρθρα. Δεν ήταν όλα τους περιστατικά που θα έπρεπε να είχαν αναφερθεί βάσει της οδηγίας NIS 2, καθώς το φάσμα περιστατικών για το οποίο ο οργανισμός συλλέγει δεδομένα είναι ευρύτερο. Αντιθέτως, πολλά σημαντικά περιστατικά δεν αναφέρονται στις πληροφορίες ανοικτής πηγής. Δεδομένου ότι τα δεδομένα που αναφέρουν τα κράτη μέλη είναι ανωνυμοποιημένα, ο ENISA δεν μπορεί να συσχετίσει τα περιστατικά που εντοπίζει με εκείνα που αναφέρουν τα κράτη μέλη. Ως εκ τούτου, δεν είναι δυνατόν να προσδιοριστεί με ακρίβεια η έκταση του φαινομένου υπο-αναφοράς περιστατικών. Σε κάθε περίπτωση, θεωρούμε ότι η διαφορά μεταξύ του πλήθους των περιστατικών που αναφέρουν τα κράτη μέλη και εκείνων που αναφέρονται στην έκθεση για το τοπίο των απειλών υποδηλώνει ότι δεν αναφέρονται όλα τα σημαντικά περιστατικά που λαμβάνουν χώρα.

37 Μια ακόμη ένδειξη υπο-αναφοράς είναι το πλήθος των κοινοποιήσεων σχετικά με σημαντικά διασυνοριακά περιστατικά που λαμβάνουν τα λοιπά πληττόμενα κράτη μέλη και ο ENISA. Παρόμοια απαίτηση προβλεπόταν στο πλαίσιο της οδηγίας NIS, αλλά κρίθηκε αναποτελεσματική, καθώς η Επιτροπή κατέληξε[8] το 2020 στο συμπέρασμα ότι, παρά την ισχύουσα υποχρέωση, σπανίως αποστέλλονταν κοινοποιήσεις και απέδωσε το φαινόμενο αυτό στην έλλειψη σαφών διαδικασιών για την ανταλλαγή πληροφοριών και στην απουσία κοινών στόχων που να δίνουν σχετικά κίνητρα.

38 Η υποχρέωση ενημέρωσης των άλλων κρατών μελών είναι ζωτικής σημασίας για την πρόληψη των δευτερογενών επιπτώσεων των περιστατικών, καθώς σε αντίθετη περίπτωση πλήττεται η κυβερνοασφάλεια της ΕΕ. Το 2025 αναφέρθηκαν μόλις 14 σημαντικά διασυνοριακά περιστατικά, από επτά κράτη μέλη. Τα κράτη μέλη υπέβαλαν δύο αναφορές περιστατικών το 2024, καμία το 2023, ενώ τρεις με πιθανό διασυνοριακό αντίκτυπο το 2022. Αυτό δείχνει ότι τα ποσοστά αναφοράς σημαντικών διασυνοριακών περιστατικών είναι πολύ χαμηλά και δεν αντικατοπτρίζουν την πραγματική έκταση των επιθέσεων αυτού του είδους. Συγκριτικά, στην έκθεσή του του 2024 για το τοπίο των απειλών, ο ENISA εντόπισε 322 περιστατικά που στόχευαν ειδικά δύο ή περισσότερα κράτη μέλη. Το περιστατικό στην αεροδιαστημική εταιρεία Collins Aerospace (βλέπε ***πλαίσιο 1***) αποτελεί ενδεικτικό παράδειγμα παράλειψης αναφοράς από τα κράτη μέλη περιστατικού παρά τον σημαντικό διασυνοριακό αντίκτυπό του.

---

[7] ENISA, Έκθεση για το τοπίο των απειλών του 2025.

[8] Ευρωπαϊκή Επιτροπή, Έκθεση εκτίμησης επιπτώσεων, 2020.

Πλαίσιο 1

Περιστατικό κυβερνοασφάλειας που διατάραξε τη λειτουργία των αεροδρομίων

Τον Σεπτέμβριο του 2025, η Collins Aerospace, σημαντικός πάροχος τεχνολογίας στον τομέα των αερομεταφορών, δέχθηκε σημαντική επίθεση λυτρισμικού που είχε ως στόχο το λογισμικό επεξεργασίας των επιβατών της. Η επίθεση ανάγκασε μεγάλα ευρωπαϊκά αεροδρόμια να καταφύγουν σε μη αυτοματοποιημένες διαδικασίες, με αποτέλεσμα να προκληθούν εκτεταμένες καθυστερήσεις και ματαιώσεις πτήσεων. Η διαταραχή ήταν σοβαρότερη στο αεροδρόμιο Heathrow του Λονδίνου, στο αεροδρόμιο των Βρυξελλών, στο αεροδρόμιο Brandenburg του Βερολίνου και στο αεροδρόμιο του Δουβλίνου.

Σύμφωνα με την οδηγία NIS 2, ένα περιστατικό θεωρείται «σημαντικό» εάν, μεταξύ άλλων, προκαλεί σοβαρή λειτουργική διατάραξη των υπηρεσιών ή οικονομική ζημία στην πληγείσα οντότητα. Ωστόσο, κανένα κράτος μέλος δεν χειρίστηκε το περιστατικό ούτε ως σημαντικό ούτε ως διασυνοριακό περιστατικό μεγάλης κλίμακας. Ως εκ τούτου, κανένα από τα επηρεαζόμενα κράτη μέλη δεν κοινοποίησε επισήμως στον ENISA ή στα άλλα κράτη μέλη το περιστατικό. Το δίκτυο CSIRT δεν ενημέρωσε σχετικώς το EU-CyCLONe, το οποίο και δεν ήταν επομένως σε θέση να υποστηρίξει τη συντονισμένη διαχείριση του περιστατικού.

Πηγή: Ανάλυση του ΕΕΣ βάσει των συνομιλιών με εκπροσώπους του ENISA.

39 Ένας άλλος λόγος για την περιορισμένη αναφορά διασυνοριακών περιστατικών είναι ότι εναπόκειται στην αρχή κάθε κράτους μέλους να αποφασίσει αν ένα αναφερθέν περιστατικό έχει διασυνοριακό αντίκτυπο, όπως και το να προσδιορίσει τα υπόλοιπα πληττόμενα κράτη μέλη. Υπάρχει το ενδεχόμενο, ανάλογα με τις πληροφορίες που έχει στη διάθεσή της η αναφέρουσα οντότητα ή η αρχή του κράτους μέλους, να μην έχει επίγνωση του διασυνοριακού χαρακτήρα ορισμένων επιθέσεων. Επί του παρόντος, δεν υπάρχει πλατφόρμα σε επίπεδο ΕΕ που να δέχεται αναφορές περιστατικών σε πραγματικό χρόνο από όλα τα κράτη μέλη και η οποία θα μπορούσε να συσχετίσει πληροφορίες σχετικά με τομείς ή δείκτες παραβίασης για τον εντοπισμό διασυνοριακών περιστατικών. Ως εκ τούτου, υπάρχει σημαντικός κίνδυνος κάποια διασυνοριακά περιστατικά να μην εντοπίζονται και να μην αναφέρονται ως τέτοια.

40 Από το 2016 και μετά, κανένα κράτος μέλος δεν έχει χαρακτηρίσει περιστατικό κυβερνοασφάλειας ως «μεγάλης κλίμακας». Κατ' αρχήν, στον εν λόγω ορισμό εμπίπτει κάθε περιστατικό που επηρεάζει σημαντικά τουλάχιστον δύο κράτη μέλη. Ωστόσο, ακόμη και περιστατικά κυβερνοασφάλειας που έχουν προκαλέσει παγκόσμιες διακοπές λειτουργίας και σημαντικές ζημίες, όπως αυτά που παρουσιάζονται στο ***γράφημα 3***, δεν θεωρούνται μεγάλης κλίμακας. Ως εκ τούτου, η διαδικασία κλιμάκωσης του EU-CyCLONe δεν έχει ενεργοποιηθεί ποτέ πλήρως εξαιτίας κάποιου περιστατικού μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας.

Γράφημα 3 | Παραδείγματα μειζόνων περιστατικών κυβερνοασφάλειας

Πηγή: ΕΕΣ, με προσαρμοσμένα στοιχεία από Cloudflare, ENISA, Ευρωπόλ, Wired, IBM, CrowdStrike.

41 Πέρα από την υποχρέωση αναφοράς στοιχείων που επιβάλλεται σε οντότητες και κράτη μέλη, το δίκτυο CSIRT δημιουργήθηκε με σκοπό να διευκολυνθεί η ανταλλαγή πληροφοριών. Η εμπιστοσύνη μεταξύ των κρατών μελών βρίσκεται στον πυρήνα των εργασιών του δικτύου CSIRT, όπου οι πληροφορίες ανταλλάσσονται σε εθελοντική βάση. Το δίκτυο χάνει πολλή από την προστιθέμενη αξία του, εάν τα κράτη μέλη δεν είναι πρόθυμα να ανταλλάσσουν έγκαιρες και αξιοποιήσιμες πληροφορίες.

42 Η ανταλλαγή πληροφοριών σε επίπεδο ΕΕ περιορίζεται από τη νομοθεσία κάθε κράτους μέλους για την εθνική ασφάλεια. Εάν ένα κράτος μέλος θεωρήσει ότι οι πληροφορίες που σχετίζονται με κυβερνοεπίθεση εναντίον κάποιας κρίσιμης σημασίας οντότητας είναι διαβαθμισμένες ή ότι η αναφορά συγκεκριμένου περιστατικού θα ήταν επιζήμια για την εθνική του ασφάλεια, δεν είναι υποχρεωμένο να προβεί σε κοινοποίηση. Κατά τη διάρκεια των επισκέψεών μας στα κράτη μέλη, εκπρόσωποι του δικτύου CSIRT και του EU-CyCLONe δήλωσαν ότι η ανταλλαγή πληροφοριών μπορεί να πραγματοποιηθεί μόνο εντός των ορίων της νομοθεσίας για την εθνική ασφάλεια. Δεν έχει διενεργηθεί σε επίπεδο ΕΕ ανάλυση των εθνικών νομικών πλαισίων των κρατών μελών και του αντικτύπου τους στην ανταλλαγή πληροφοριών.

43 Το 2016 το δίκτυο CSIRT απαρτιζόταν από 28 εθνικές CSIRT, με δύο εκπροσώπους ανά κράτος μέλος. Η απουσία οποιασδήποτε ανταλλαγής πληροφοριών αποτελεί ζήτημα που δεν παύει να απασχολεί και, μάλιστα, στην αξιολόγηση της οδηγίας NIS η Επιτροπή αναγνώρισε ότι τα κράτη μέλη δεν ανταλλάσσουν συστηματικά πληροφορίες μεταξύ τους, γεγονός που επηρεάζει ιδιαίτερα την αποτελεσματικότητα των μέτρων κυβερνοασφάλειας και τον βαθμό συλλογικής επίγνωσης της κατάστασης σε επίπεδο ΕΕ. Κατ' εφαρμογή της οδηγίας NIS 2, πολλά κράτη μέλη έχουν ορίσει τομεακές CSIRT επιπλέον των εθνικών CSIRT και, ως εκ τούτου, το δίκτυο έχει επεκταθεί σημαντικά. Κατά τον χρόνο του ελέγχου, απαρτιζόταν από 42 CSIRT και περισσότερους από 700 μεμονωμένους συμμετέχοντες. Δυσχεραίνεται έτσι ακόμη περισσότερο η οικοδόμηση εμπιστοσύνης, καθώς η διατήρηση στενών δεσμών μεταξύ όλων των μελών δεν είναι απλή υπόθεση.

44 Το δίκτυο CSIRT έχει επίγνωση του προβλήματος σχετικά με την ανταλλαγή πληροφοριών και επεξεργάζεται διάφορες δράσεις που θα βοηθούσαν στην ενίσχυση της εμπιστοσύνης σε ένα δίκτυο που ολοένα διευρύνεται. Η δημιουργία μικρότερων ομάδων κρατών μελών που σχηματίζουν διασυνοριακούς κόμβους, όπως περιγράφεται λεπτομερώς στα σημεία ***62***-***74***, αποτελεί εναλλακτική προσέγγιση έναντι ενός πανευρωπαϊκού δικτύου, που μπορεί να συμβάλει στην αντιμετώπιση αυτής της πρόκλησης.

Οι υπηρεσίες βάσει σύμβασης του κέντρου κυβερνοκατάστασης επικαλύπτουν εν μέρει τις υφιστάμενες ικανότητες και η μελλοντική λειτουργία του είναι μετέωρη

45 Σύμφωνα με την οδηγία NIS 2, σε περιπτώσεις όπου ένα δυνητικό ή εν εξελίξει μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας έχει ή ενδέχεται να έχει σημαντικό αντίκτυπο, στο EU-CyCLONe συμμετέχει και η Επιτροπή[9]. Αυτός ο νέος ρόλος, όπως και η εξέλιξη του τοπίου των απειλών, οδήγησαν την Επιτροπή στη σύσταση ειδικής ομάδας για τον συντονισμό του κυβερνοχώρου εντός της ΓΔ Connect το 2022. Η εν λόγω ειδική ομάδα περιλαμβάνει ένα κέντρο κυβερνοκατάστασης, το οποίο αναμένεται να βοηθήσει την Επιτροπή να βελτιώσει την από μέρους της επίγνωση της κατάστασης, με σκοπό τη στήριξη των θεσμικών αρμοδιοτήτων της για τη διαχείριση κρίσεων. Αναμένεται επίσης να βοηθήσει τη ΓΔ Connect να παρέχει συμβουλές σε πολιτικό επίπεδο.

46 Για την οργάνωση του κέντρου κυβερνοκατάστασης, η Επιτροπή υποστηρίζεται σε μεγάλο βαθμό από εξωτερικούς παρόχους υπηρεσιών με τους οποίους συνήφθησαν συμβάσεις τον Δεκέμβριο του 2022 αξίας σχεδόν 18 εκατομμυρίων ευρώ για μία τετραετία. Αξιολογήσαμε τη σύσταση του κέντρου, τις εκροές του και τα σχέδια της Επιτροπής για τη μελλοντική λειτουργία του.

47 Στο πλαίσιο των παρεχόμενων υπηρεσιών, οι ανάδοχοι έχουν δημιουργήσει έναν πίνακα πληροφοριών που βασίζεται σε εμπορικές ροές πληροφοριών για κυβερνοαπειλές, με σκοπό την παρουσίαση και την ανταλλαγή πληροφοριών σχετικά με απειλές. Καταρτίζουν επίσης διάφορες αναφορές πληροφοριών για κυβερνοαπειλές, συμπεριλαμβανομένων ημερήσιων και εβδομαδιαίων, καθώς και θεματικές αναφορές για χώρες ή συγκεκριμένους τομείς της οικονομίας. Το φυσικό κέντρο κυβερνοκατάστασης, το οποίο αποτελείται από αίθουσα εξοπλισμένη με σταθμούς εργασίας συνδεδεμένους εξ αποστάσεως με τον πίνακα πληροφοριών που φιλοξενείται από τους αναδόχους, έχει εγκατασταθεί σε ένα από τα κτίρια της Επιτροπής. Κατά τον χρόνο του ελέγχου, με το κέντρο κυβερνοκατάστασης ασχολούνταν λίγοι υπάλληλοι της Επιτροπής. Η υποστήριξή του ήταν κυρίως έργο πολλών αναλυτών από τους αναδόχους, καθώς και ειδικών του ENISA.

[9] Άρθρο 16, παράγραφος 2, της οδηγίας NIS 2.

48 Διαπιστώσαμε ότι το έργο που επιτελούν οι εξωτερικοί πάροχοι υπηρεσιών για το κέντρο κυβερνοκατάστασης επικαλύπτει εν μέρει την υφιστάμενη ικανότητα του ENISA. ο οποίος διαθέτει μόνιμη ικανότητα επίγνωσης της κατάστασης και παρακολούθησης των απειλών. Δημοσιεύει τακτικά αναφορές σχετικά με κυβερνοαπειλές, συμπεριλαμβανομένων συνοπτικών αναφορών σχετικά με συγκεκριμένα περιστατικά, καθώς και εβδομαδιαίες αναφορές που παρέχουν επισκόπηση των απειλών. Οι αναφορές βασίζονται σε πληροφορίες ανοικτής πηγής και είναι παρόμοιες με εκείνες που καταρτίζουν οι ανάδοχοι. Επιπλέον, ο ENISA εκπονεί ή συνεισφέρει σε ενημερωτικά σημειώματα υψηλού επιπέδου που απευθύνονται στους υπευθύνους χάραξης πολιτικής εν μέσω κάποιας κρίσης, τα οποία είναι εφάμιλλης αξίας με αυτά που παράγει το κέντρο κυβερνοκατάστασης.

49 Επιπλέον, τα δεδομένα που χρησιμοποιεί το κέντρο κυβερνοκατάστασης για την κατάρτιση των εν λόγω αναφορών βασίζονται σε εμπορικές ροές πληροφοριών για κυβερνοαπειλές και είναι παρόμοια με τα δεδομένα που χρησιμοποιούνται από άλλες υπηρεσίες της Επιτροπής, όπως η Γενική Διεύθυνση Ψηφιακών Υπηρεσιών και η CERT-EE. Θεωρούμε ότι με τον τρόπο με τον οποίο συστάθηκε το κέντρο κυβερνοκατάστασης δεν αξιοποιήθηκαν επαρκώς οι δυνατότητες εξορθολογισμού που θα προσέφερε η χρήση των πληροφοριών που είχαν ήδη στη διάθεσή τους η Επιτροπή και ο ENISA.

50 Η σύμβαση λήγει τον Δεκέμβριο του 2026 και, στη συνέχεια, οι ανάδοχοι θα σταματήσουν να παρέχουν τις υπηρεσίες τους για το κέντρο κυβερνοκατάστασης. Οι υπηρεσίες αυτές περιλαμβάνουν την ενημέρωση του πίνακα πληροφοριών με τα διαθέσιμα δεδομένα, την κατάρτιση των αναφορών σχετικά με τις απειλές και τη στελέχωση της πλειονότητας του κέντρου. Ο πίνακας πληροφοριών θα περιέλθει στην Επιτροπή, αλλά θα χάσει την προστιθέμενη αξία του εάν δεν επικαιροποιείται συνεχώς με πληροφορίες για κυβερνοαπειλές.

51 Κατά τον χρόνο του ελέγχου, η Επιτροπή δεν είχε στα σκαριά κάποιο σχέδιο σχετικά με την υποστήριξη από τους εξωτερικούς παρόχους υπηρεσιών για τη λειτουργία του κέντρου κυβερνοκατάστασης μετά τη λήξη της σύμβασης. Θεωρούμε ότι η απουσία ολοκληρωμένου, λεπτομερούς σχεδίου για το μέλλον μετά τη λήξη της σύμβασης καθιστά επισφαλή τη λειτουργία του κέντρου κυβερνοκατάστασης μετά το 2026.

Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας διευκολύνει την ταχεία ανάπτυξη υπηρεσιών αντιμετώπισης περιστατικών

52 Το 2022, αμέσως μετά τη στρατιωτική επίθεση της Ρωσίας κατά της Ουκρανίας και αναγνωρίζοντας ότι οι κυβερνοεπιθέσεις μεγάλης κλίμακας έχουν αρχίσει να παίρνουν μεγαλύτερες διαστάσεις, η Επιτροπή χορήγησε στον ENISA έκτακτη χρηματοδότηση ύψους 15 εκατομμυρίων ευρώ για την πιλοτική εφαρμογή της δράσης για τη στήριξη της κυβερνοασφάλειας, η οποία δρομολογήθηκε το 2023. Την ίδια χρονιά η Επιτροπή χορήγησε πρόσθετη χρηματοδότηση (περίπου 20 εκατ. ευρώ) για την παράταση του προγράμματος μέχρι το τέλος του 2026.

53 Η Επιτροπή πρότεινε επίσης την πράξη για την αλληλεγγύη στον κυβερνοχώρο, η οποία εγκρίθηκε τον Δεκέμβριο του 2024, με σκοπό την προετοιμασία για την αντιμετώπιση περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας. Η πράξη θεσπίζει εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, η οποία περιλαμβάνει υπηρεσίες αντιμετώπισης περιστατικών που παρέχονται από αξιόπιστους παρόχους. Άρχισε να λειτουργεί σταδιακά το 2025, με προϋπολογισμό 36 εκατομμύρια ευρώ για την περίοδο 2025-2027.

54 Αξιολογήσαμε τον τρόπο οργάνωσης του προγράμματος δράσης για τη στήριξη της κυβερνοασφάλειας, καθώς αποτελεί τη βάση για την εφεδρεία της ΕΕ στον συγκεκριμένο τομέα. Ελέγξαμε επίσης κατά πόσον τα διδάγματα που αντλήθηκαν από το 2022 λήφθηκαν υπόψη κατά τον σχεδιασμό της συγκεκριμένης εφεδρείας.

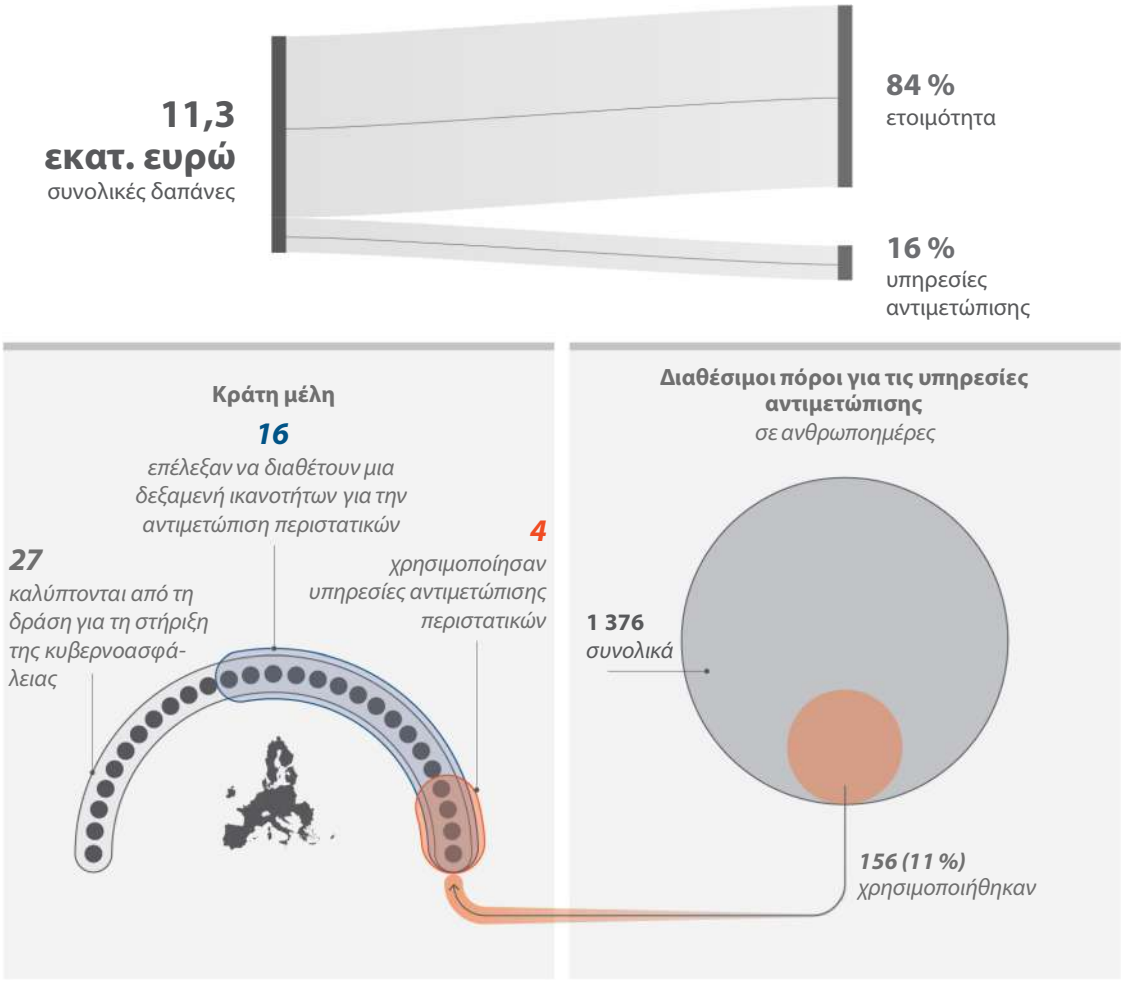
55 Ο ENISA σχεδίασε τη δράση για τη στήριξη της κυβερνοασφάλειας ως μηχανισμό παροχής υπηρεσιών με σκοπό την υποστήριξη της ετοιμότητας και της απόκρισης των κρατών μελών σε μεγάλης κλίμακας περιστατικά ή κρίσεις κυβερνοασφάλειας. Όλες οι υπηρεσίες ανατίθενται εκ των προτέρων από τον ENISA, γεγονός που σημαίνει ότι οι πάροχοι υπηρεσιών είναι έτοιμοι να αναλάβουν δράση με το που τους το ζητήσει κάποιο κράτος μέλος. Αυτό οφείλεται επίσης στην οργάνωση του ENISA, καθώς υπάρχει πάντα ένας υπάλληλος σε επιφυλακή σε εικοσιτετράωρη βάση για να ανταποκριθεί στα αιτήματα των κρατών μελών.

56 Ο ENISA επέλεξε να κατανείμει ισομερώς τον διαθέσιμο προϋπολογισμό μεταξύ των κρατών μελών. Στην πράξη, ο οργανισμός προκήρυξε ανοικτό διαγωνισμό που υποδιαιρέθηκε σε 27 παρτίδες, μία ανά κράτος μέλος, για την επιλογή έως και τριών ιδιωτικών παρόχων υπηρεσιών ασφάλειας για την παροχή υπηρεσιών μέχρι τα τέλη του 2026. Επιπλέον, προέβη στην επιλογή ορισμένων παρόχων στο πλαίσιο πανευρωπαϊκής παρτίδας για την παροχή υπηρεσιών σε επιλέξιμες τρίτες χώρες, καθώς και σε θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ, ή για την υποστήριξη της αντιμετώπισης διασυνοριακών περιστατικών.

57 Η προσέγγιση αυτή επέτρεψε στον ENISA να συνεκτιμήσει τις ειδικές απαιτήσεις κάθε χώρας, όπως τη γλώσσα, τις εθνικές διαπιστεύσεις ασφαλείας ή την εδραιωμένη παρουσία στα κράτη μέλη. Από την άλλη πλευρά, δεδομένου ότι οι πάροχοι δεν επιλέχθηκαν υπό την προϋπόθεση να παρέχουν υπηρεσίες σε ολόκληρη την ΕΕ, ένα σημαντικό μειονέκτημα της προσέγγισης αυτής είναι ότι, εάν ένα κράτος μέλος δεν χρησιμοποιεί τις προσυμφωνημένες υπηρεσίες, ο προϋπολογισμός που έχει δεσμευθεί για τέτοιες υπηρεσίες για ένα συγκεκριμένο κράτος μέλος δεν μπορεί να αξιοποιηθεί για την παροχή βοήθειας σε κάποιο άλλο.

58 Όσον αφορά τη δράση για τη στήριξη της κυβερνοασφάλειας, τα κράτη μέλη μπορούσαν να επιλέξουν μεταξύ υπηρεσιών ετοιμότητας ή απόκρισης ή συνδυασμού και των δύο. Τα κράτη μέλη επέλεξαν πρωτίστως να χρησιμοποιήσουν τη διαθέσιμη χρηματοδότηση για να βελτιώσουν την ετοιμότητά τους (84 % των δαπανών το 2023). Εκείνα που επέλεξαν να διαθέτουν μια δεξαμενή ικανοτήτων για την αντιμετώπιση περιστατικών (συνήψαν δηλαδή προκαθορισμένη συμφωνία με πάροχο που διασφαλίζει ότι το κράτος μέλος μπορεί να έχει πρόσβαση στις υπηρεσίες του παρόχου κατόπιν αιτήματος με σκοπό την ταχεία αντιμετώπιση ενός περιστατικού κυβερνοασφάλειας) τη χρησιμοποίησαν με φειδώ, όπως φαίνεται στο ***γράφημα 4***. Στα τρία κράτη μέλη που επισκεφθήκαμε, οι αρχές εξέφρασαν την εκτίμησή τους για την από μέρους του ENISA διαχείριση της δράσης για τη στήριξη της κυβερνοασφάλειας.

Γράφημα 4 | Δράση για τη στήριξη της κυβερνοασφάλειας του ENISA μέχρι το 2023



Πηγή: ΕΕΣ, βάσει στοιχείων του ENISA.

59 Για την περίοδο 2024-2026, μόνο εννέα κράτη μέλη ζήτησαν να διαθέτουν μια δεξαμενή ικανοτήτων για την αντιμετώπιση περιστατικών. Στο πλαίσιο των συνομιλιών μας με εκπροσώπους του ENISA και των αρχών τριών κρατών μελών επιβεβαιώσαμε την έντονη προτίμησή τους για δραστηριότητες ετοιμότητας.

60 Μολονότι η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας αποσκοπεί πρωτίστως στην υποστήριξη της αντιμετώπισης και της ανάκαμψης όσον αφορά μείζονα περιστατικά κυβερνοασφάλειας, υπάρχει η δυνατότητα οι προδεσμευμένες υπηρεσίες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας που δεν χρησιμοποιούνται για την αντιμετώπιση περιστατικών να μετατραπούν σε υπηρεσίες ετοιμότητας. Με την ευέλικτη αυτή προσέγγιση αποτρέπεται το ενδεχόμενο προπληρωμένες υπηρεσίες να παραμείνουν σε αχρησία.

61 Θεωρούμε ότι το μοντέλο που επιλέχθηκε για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας βασίζεται στα διδάγματα που αντλήθηκαν από το πρόγραμμα δράσης για τη στήριξη της κυβερνοασφάλειας. Ωστόσο, τα δεδομένα που αποτυπώνουν τη χρήση του προγράμματος δράσης για τη στήριξη της κυβερνοασφάλειας καταδεικνύουν τον κίνδυνο η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας να χρησιμοποιείται πρωτίστως για σκοπούς ετοιμότητας και όχι απόκρισης, σε αντίθεση με τον δεδηλωμένο στην πράξη για την αλληλεγγύη στον κυβερνοχώρο σκοπό.

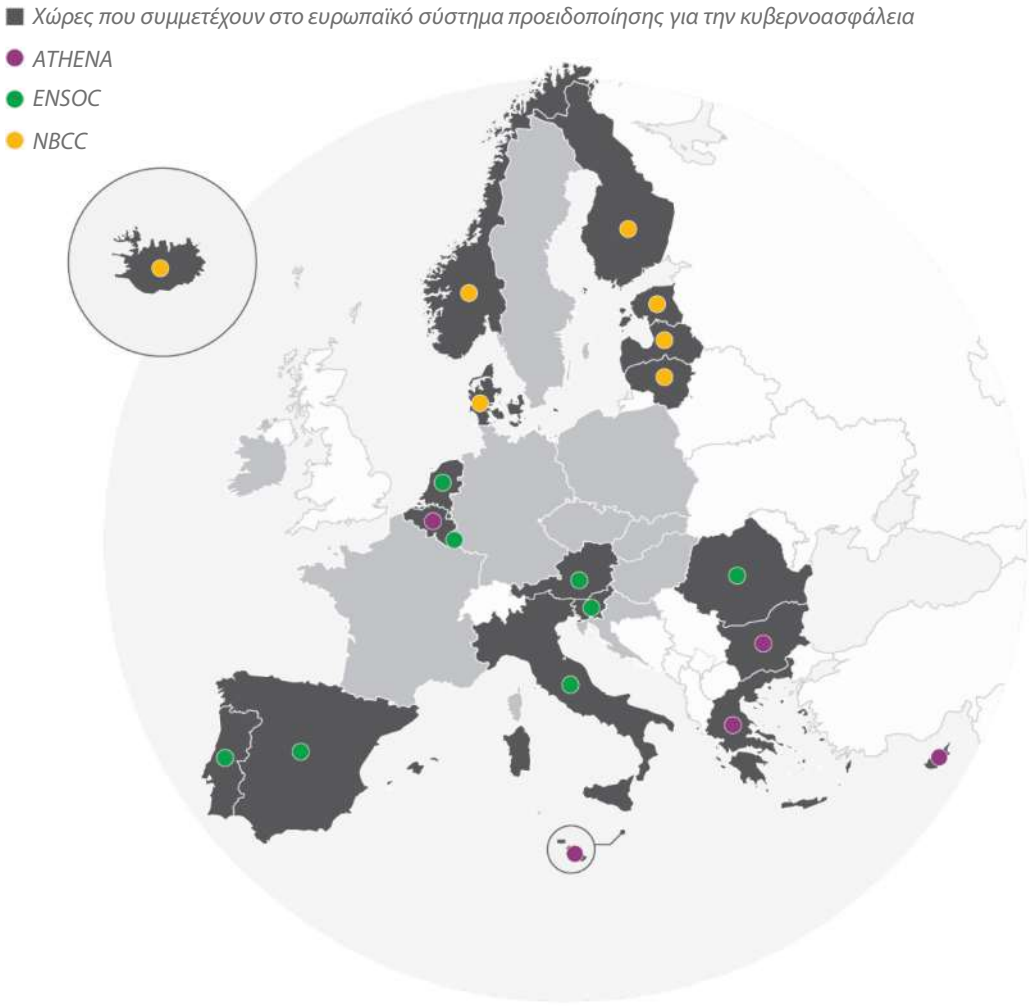
Το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια αποσκοπεί στη βελτίωση των ικανοτήτων ανίχνευσης απειλών, ωστόσο δεν είναι σε λειτουργία

62 Ένας από τους βασικούς στόχους του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια είναι η ενθάρρυνση της ουσιαστικής ανταλλαγής πληροφοριών προκειμένου να ενισχυθεί η ικανότητα ανίχνευσης και ανάλυσης κυβερνοαπειλών και απόκρισης σε αυτές. Η συμμετοχή στο σύστημα προειδοποίησης είναι προαιρετική, αλλά τα κράτη μέλη που επιλέγουν να προσχωρήσουν σε διασυνοριακό κυβερνοκόμβο πρέπει να δεσμευθούν να ανταλλάσσουν σχετικές πληροφορίες με τα άλλα μέλη. Μέσω της συνεργασίας σε ομάδες, εντός ενός αξιόπιστου και ασφαλούς περιβάλλοντος, τα κράτη μέλη έχουν πιθανότητες να αποφύγουν ορισμένα από τα προβλήματα που σχετίζονται με την ανταλλαγή πληροφοριών και τα οποία αναλύονται στα σημεία ***31***-***44***.

63 Κατά τον χρόνο του ελέγχου, 13 κράτη μέλη είχαν επιλέξει να συμμετάσχουν στο ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια, δημιουργώντας δύο διασυνοριακούς κόμβους: τον ATHENA και τον ENSOC. Ένας τρίτος διασυνοριακός κυβερνοκόμβος, ο NBCC, είχε λάβει χρηματοδότηση για να συσταθεί εντός του 2026, με το δίκτυο να αριθμεί συνολικά 20 χώρες μέλη (18 κράτη μέλη και η Ισλανδία και η Νορβηγία[10]), όπως φαίνεται στο ***γράφημα 5***.

[10] Συνδεδεμένες τρίτες χώρες σύμφωνα με το άρθρο 10, παράγραφος 1, στοιχείο α), του κανονισμού (ΕΕ) 2021/694.

Γράφημα 5 | Χώρες που συμμετέχουν στο ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια



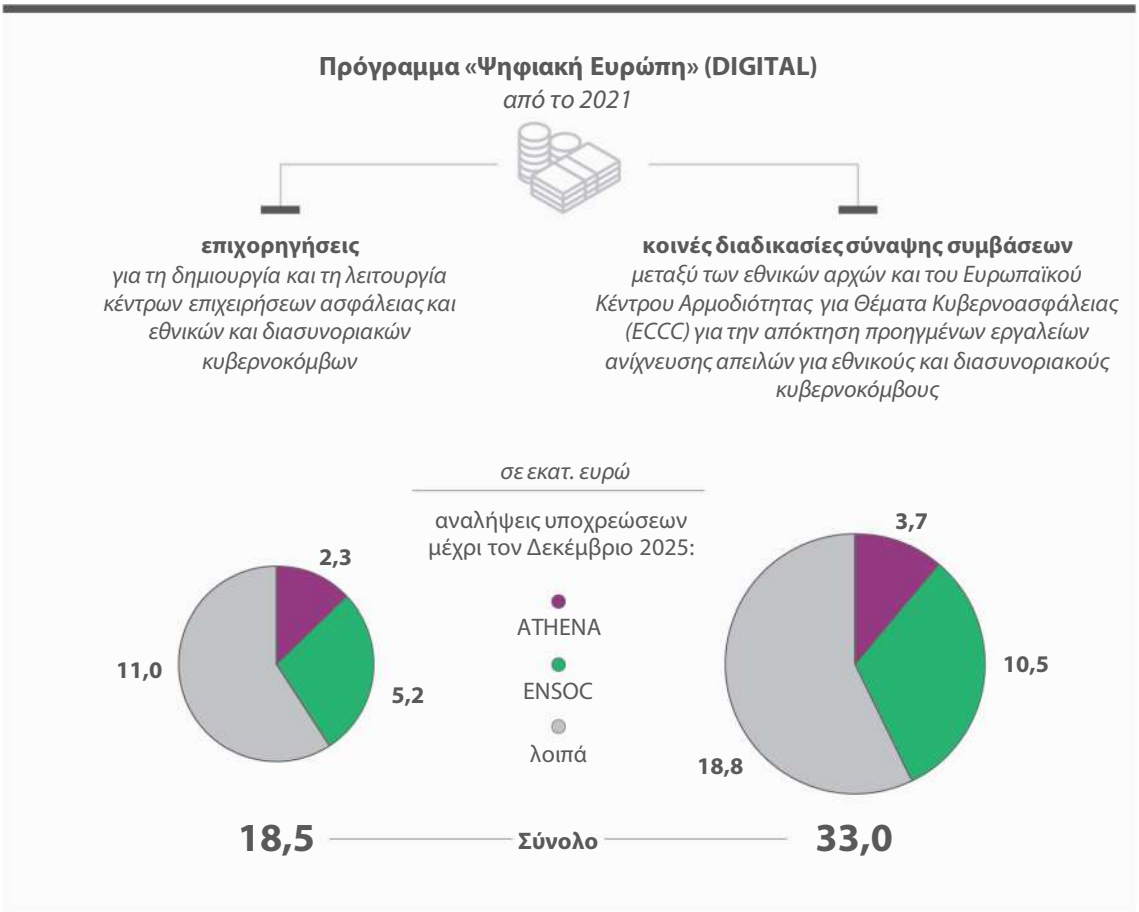
Πηγή: ΕΕΣ.

64 Αξιολογήσαμε τον τρόπο με τον οποίο δημιουργήθηκαν οι δύο πρώτοι διασυνοριακοί κυβερνοκόμβοι, καθώς και την πρόοδό τους προς την επίτευξη των στόχων του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια. Εξετάσαμε επίσης πώς εντάσσονται οι διασυνοριακοί κόμβοι που δημιουργήθηκαν στο ευρύτερο τοπίο της κυβερνοασφάλειας και πώς αλληλεπιδρούν με τα υφιστάμενα δίκτυα και δομές.

Μέχρι στιγμής δεν έχουν επιτευχθεί απτά αποτελέσματα, λόγω αξιοσημείωτων καθυστερήσεων στις διαδικασίες σύναψης συμβάσεων

65 Η χρηματοδότηση για τη στήριξη της δημιουργίας εθνικών και διασυνοριακών κυβερνοκόμβων διατίθεται μέσω του προγράμματος DIGITAL από το 2021. Η εν λόγω χρηματοδότηση διοχετεύεται μέσω μιας πολύπλοκης διαδικασίας με δύο παράλληλες ροές: παραδοσιακές επιχορηγήσεις για τη στήριξη της δημιουργίας και της λειτουργίας των κόμβων, καθώς και κοινή διαδικασία σύναψης συμβάσεων για την απόκτηση προηγμένων εργαλείων ανίχνευσης απειλών, όπως φαίνεται στο ***γράφημα 6***. Έπειτα από σχετική πρόσκληση υποβολής προτάσεων που προκηρύχθηκε τον Νοέμβριο του 2022, οι κόμβοι ATHENA και ENSOC ξεκίνησαν τις εργασίες τους τον Ιανουάριο του 2024.

Γράφημα 6 | Χρηματοδότηση κυβερνοκόμβων από το πρόγραμμα «Ψηφιακή Ευρώπη»



Πηγή: ΕΕΣ, βάσει στοιχείων του ECCC.

66 Οι κλειστές διαδικασίες σύναψης συμβάσεων δύο φάσεων[11] διοργανώθηκαν από τα μέλη του ATHENA και του ENSOC, καθώς και από τη ΓΔ Connect (πρώτη φάση) και το νεοσυσταθέν ECCC (δεύτερη φάση). Η προσέγγιση των δύο φάσεων αποσκοπεί στον περιορισμό της κυκλοφορίας ευαίσθητων πληροφοριών, καθώς οι λεπτομερείς τεχνικές προδιαγραφές κοινοποιούνται μόνο στους υποψηφίους που έχουν περάσει την πρώτη φάση.

67 Η πρώτη φάση ξεκίνησε τον Μάιο του 2024 για τον ENSOC και τον Ιούλιο του 2024 για τον κόμβο ATHENA. Οι ενδιαφερόμενες εταιρείες είχαν προθεσμία ενός μήνα για να υποβάλουν προσφορά. Ωστόσο, οι επιτυχόντες υποψήφιοι ενημερώθηκαν μόλις τον Απρίλιο του 2025, σχεδόν ένα έτος μετά την έναρξη της διαδικασίας.

68 Επιπλέον, καμία από διαδικασίες σύναψης συμβάσεων, ούτε για τον ENSOC ούτε για τον ATHENA, μπορούσε να προχωρήσει στη δεύτερη φάση εκείνη την περίοδο, καθώς τα μέλη των κόμβων και το ECCC δεν ήταν σε θέση να παράσχουν στις προεπιλεγείσες εταιρείες τις τεχνικές προδιαγραφές που ήταν απαραίτητες για την υποβολή προσφοράς, δεδομένου ότι βρίσκονταν ακόμη στο στάδιο της οριστικοποίησης.

69 Η δεύτερη φάση των διαδικασιών σύναψης συμβάσεων ξεκίνησε μόλις τον Αύγουστο του 2025 για ορισμένα τμήματα του ENSOC και είχε προγραμματιστεί για τις αρχές του 2026 για τον ATHENA. Κατά τον χρόνο του ελέγχου, 18 μήνες μετά την έναρξη της διαδικασίας σύναψης συμβάσεων, δεν είχε υπογραφεί σύμβαση για καμία από τις παρτίδες. Θεωρούμε ότι η έλλειψη κατάλληλης προετοιμασίας και η πολυπλοκότητα των διαδικασιών σύναψης συμβάσεων λειτούργησαν εις βάρος της έγκαιρης ολοκλήρωσής τους.

70 Συνεπώς, διαπιστώσαμε ότι οι διασυνοριακοί κόμβοι δεν βρίσκονται σε καλό δρόμο για την επίτευξη των στόχων τους. Χωρίς τα απαραίτητα εργαλεία για την ανίχνευση απειλών και την ανταλλαγή πληροφοριών, η λειτουργία τους έχει ανασταλεί, ενώ το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια δεν λειτουργεί ακόμη, με αποτέλεσμα να καθυστερεί η αποτελεσματική ανάπτυξη προηγμένων ικανοτήτων για την ανίχνευση και πρόληψη απειλών και περιστατικών στον κυβερνοχώρο. Έχουν υπογραφεί τροποποιήσεις για την παράταση της διάρκειας της συμφωνίας επιχορήγησης, ώστε να ληφθούν υπόψη οι καθυστερήσεις που έχουν σημειωθεί μέχρι στιγμής στις διαδικασίες σύναψης συμβάσεων (15 μήνες για τον ATHENA και 18 μήνες για τον ENSOC).

[11] Πρόσκληση υποβολής προσφορών για τον ENSOC και πρόσκληση υποβολής προσφορών για τον ATHENA.

Οι διασυνοριακοί κυβερνοκόμβοι δημιουργούν πρόσθετους διαύλους επικοινωνίας που επιτείνουν ακόμη περισσότερο την πολυπλοκότητα

71 Μία από τις βασικές εργασίες των διασυνοριακών κυβερνοκόμβων είναι η ανταλλαγή χρήσιμων πληροφοριών για την ενίσχυση της ανίχνευσης και αντιμετώπισης απειλών. Πρόκειται, μεταξύ άλλων, για πληροφορίες σχετικά με κυβερνοαπειλές, τρωτά σημεία, δείκτες παραβίασης και παράγοντες απειλής. Οι εργασίες των διασυνοριακών κυβερνοκόμβων αλληλεπικαλύπτονται εν μέρει με τις εργασίες των εθνικών CSIRT και του δικτύου CSIRT, ιδίως όσον αφορά την ανταλλαγή πληροφοριών σχετικά με κυβερνοαπειλές και τρωτά σημεία. Δεν υπάρχει διακριτό όριο μεταξύ των ρόλων των διασυνοριακών κυβερνοκόμβων και των CSIRT. Σύμφωνα με το σχέδιο στρατηγικής για τον κυβερνοχώρο του 2025 (σημείο ***29***), οι διασυνοριακοί κυβερνοκόμβοι προορίζονται να λειτουργούν τόσο σε τεχνικό (όπως οι εθνικές CSIRT και το δίκτυο CSIRT) όσο και σε επιχειρησιακό επίπεδο (όπως το EU-CyCLONe).

72 Σύμφωνα με την πράξη για την αλληλεγγύη στον κυβερνοχώρο, οι διασυνοριακοί κυβερνοκόμβοι υποχρεούνται να υπογράφουν συμφωνίες συνεργασίας μεταξύ τους για τη διευκόλυνση της ανταλλαγής πληροφοριών. Ο ENISA έπρεπε να είχε εκδώσει κατευθυντήριες γραμμές σχετικά με τη διαλειτουργικότητα μεταξύ διασυνοριακών κυβερνοκόμβων μέχρι τον Φεβρουάριο του 2026, κατ' απαίτηση της πράξης για την αλληλεγγύη στον κυβερνοχώρο. Εν τω μεταξύ, τον Δεκέμβριο του 2025, το ECCC χορήγησε επιχορήγηση σε κοινοπραξία (στην οποία συμμετέχουν ορισμένα μέλη του ENSOC και του ATHENA) για τον καθορισμό τεχνικού πλαισίου διαλειτουργικότητας μεταξύ των διασυνοριακών κυβερνοκόμβων. Βέβαια, οι κατευθυντήριες γραμμές και το πλαίσιο αναμένεται να ολοκληρωθούν αφού τεθούν σε λειτουργία οι διασυνοριακοί κυβερνοκόμβοι. Όπως επισημάναμε στη γνώμη μας του 2023 σχετικά με την πρόταση της πράξης για την αλληλεγγύη στον κυβερνοχώρο[12], αν δεν επιτευχθεί γρήγορα μια συμφωνία, υπάρχει κίνδυνος να αναπτυχθούν συστήματα που είναι ασύμβατα μεταξύ τους, με αποτέλεσμα να αυξηθεί το κόστος.

[12] Γνώμη 02/2023 σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας, σημείο 26.

73 Οι διασυνοριακοί κυβερνοκόμβοι υποχρεούνται επίσης να ανταλλάσσουν σχετικές πληροφορίες για περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας με το EU-CyCLONe και το δίκτυο CSIRT χωρίς αδικαιολόγητη καθυστέρηση. Σε επίπεδο κρατών μελών, η δημιουργία εθνικών κυβερνοκόμβων και η συμμετοχή σε διασυνοριακούς κυβερνοκόμβους προσφέρουν πρόσθετα επίπεδα επικοινωνίας. Επίσης, ο συντονισμός με τρίτες χώρες[13], οι οποίες δεν είναι μέλη του δικτύου CSIRT ή του EU-CyCLONe, περιπλέκει περισσότερο την κατάσταση.

74 Υπάρχει ανάγκη για σαφείς συμφωνίες συνεργασίας για την επίτευξη συμφωνίας σχετικά με μια κοινή ταξινομία και τον τρόπο ανταλλαγής πληροφοριών, καθώς και για τη διασφάλιση της διαλειτουργικότητας. Τα διδάγματα που αντλήθηκαν από το δίκτυο CSIRT δείχνουν ότι πρόκειται για μια σημαντική πρόκληση. Διαπιστώσαμε ότι, κατά τον χρόνο του ελέγχου, δεν είχαν συμφωνηθεί διαδικαστικές ρυθμίσεις σχετικά με τη συνεργασία και την ανταλλαγή πληροφοριών. Θεωρούμε ότι η δημιουργία εθνικών και διασυνοριακών κυβερνοκόμβων θα μπορούσε να προαγάγει την αποτελεσματικότερη ανταλλαγή πληροφοριών. Ωστόσο, η ενσωμάτωση των διασυνοριακών κόμβων στο ήδη πολύπλοκο τοπίο της κυβερνοασφάλειας θα είναι ένα δύσκολο εγχείρημα και απαιτεί πρόσθετους διαύλους επικοινωνίας και ρυθμίσεις συνεργασίας.

[13] Ισλανδία και Νορβηγία.

Τα χρηματοδοτούμενα από την ΕΕ έργα στο πλαίσιο του προγράμματος DIGITAL αποσκοπούν στην ενίσχυση της κυβερνοασφάλειας, αλλά αντιμετωπίζουν προκλήσεις όσον αφορά την υλοποίηση και την αναφορά στοιχείων

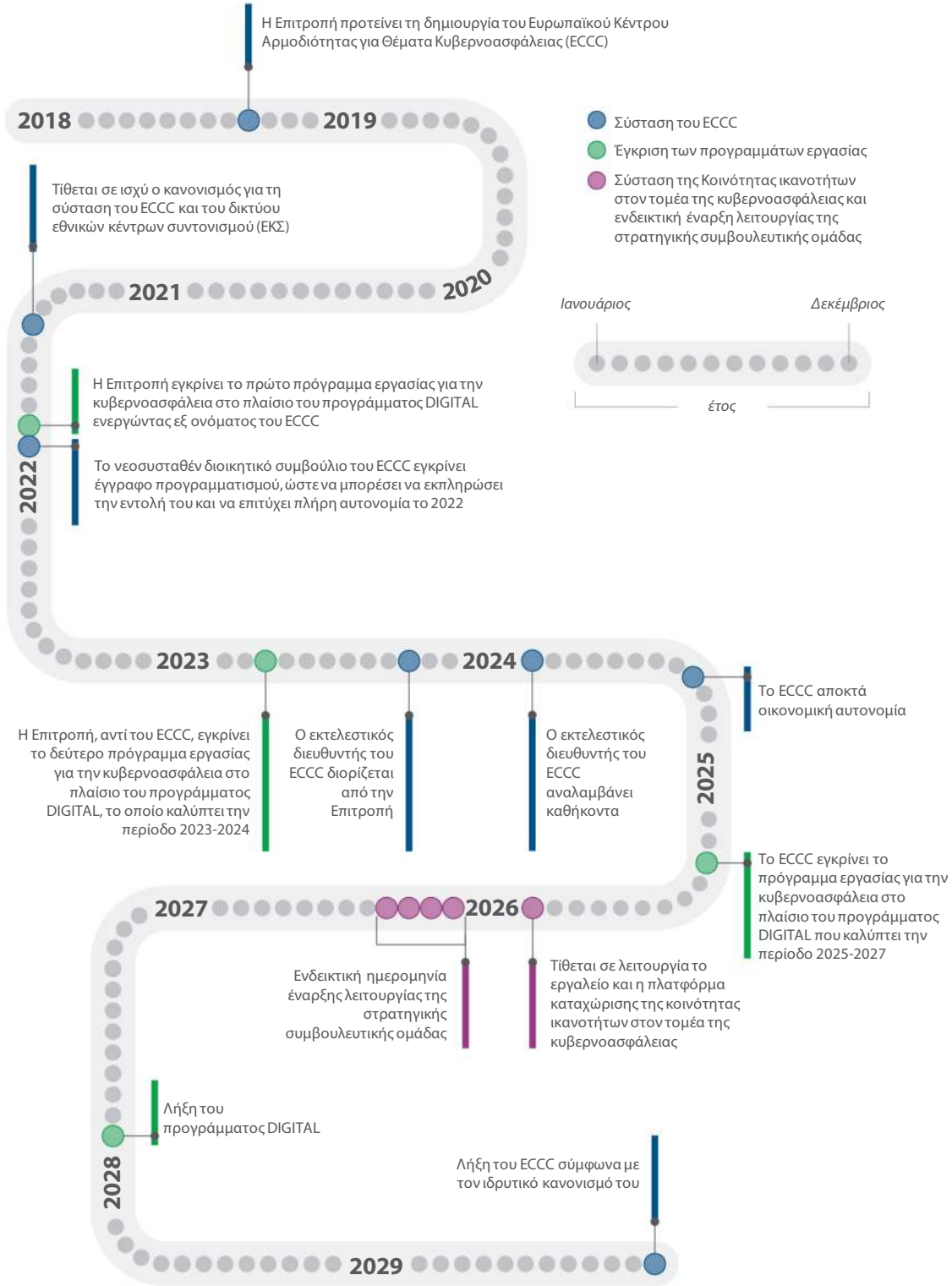
Καθυστερήσεις στη σύστασή της εμπόδισαν την κοινότητα ικανοτήτων στον τομέα της κυβερνοασφάλειας να διαμορφώσει το πρόγραμμα DIGITAL σύμφωνα με τις ανάγκες της

75 Για τη διαχείριση της συνιστώσας κυβερνοασφάλειας του προγράμματος DIGITAL, το 2018 η Επιτροπή πρότεινε τη δημιουργία του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Θέματα Κυβερνοασφάλειας (ECCC). Ο κανονισμός ECCC προέβλεπε την υποστήριξη του ECCC από ένα δίκτυο 29 εθνικών κέντρων συντονισμού (ΕΚΣ), ένα για κάθε κράτος μέλος και για την Ισλανδία και τη Νορβηγία. Προέβλεπε επίσης τη δημιουργία της κοινότητας ικανοτήτων στον τομέα της κυβερνοασφάλειας (εφεξής η «Κοινότητα»), η οποία θα αποτελείται από εκπροσώπους της βιομηχανίας, ακαδημαϊκών και ερευνητικών οργανισμών, καθώς και άλλων σχετικών ενώσεων της κοινωνίας των πολιτών.

76 Είκοσι μέλη κατ' ανώτατο όριο της Κοινότητας θα συμμετέχουν στη στρατηγική συμβουλευτική ομάδα (SAG), η οποία αποτελεί μία από τις τρεις συνιστώσες της δομής του ECCC. Ένα από τα βασικά καθήκοντα της SAG είναι η διοργάνωση δημόσιων διαβουλεύσεων για την τροφοδότηση του θεματολογίου του ECCC και των προγραμμάτων εργασίας του DIGITAL.

77 Αξιολογήσαμε κατά πόσον το πρόγραμμα DIGITAL και τα προγράμματα εργασίας του εγκρίθηκαν βάσει εμπεριστατωμένης ανάλυσης των αναγκών, καθώς και τον τρόπο με τον οποίο το ECCC, το δίκτυο των ΕΚΣ, η Κοινότητα και η SAG κατάφεραν να συμβάλουν στη διαμόρφωση των προγραμμάτων εργασίας. Στην πράξη, το ECCC, το δίκτυο των ΕΚΣ, η Κοινότητα και η SAG συστάθηκαν σταδιακά επί σειρά ετών (βλέπε ***γράφημα 7***).

Γράφημα 7 | Χρονογραμμή της σύστασης του ευρωπαϊκού κέντρου ικανοτήτων στον τομέα της κυβερνοασφάλειας, του δικτύου εθνικών κέντρων συντονισμού, της Κοινότητας και της στρατηγικής συμβουλευτικής ομάδας



Πηγή: ΕΕΣ.

78 Δεδομένου ότι το ECCC άρχισε να λειτουργεί πλήρως μόλις τον Σεπτέμβριο του 2024, για τις περιόδους 2021-2022 και 2023-2024 η Επιτροπή ήταν αυτή που ενέκρινε, εξ ονόματος του ECCC, τα προγράμματα εργασίας. Η Κοινότητα δεν μπόρεσε να συνεισφέρει στα δύο αυτά προγράμματα εργασίας.

79 Εν τω μεταξύ, τα κράτη μέλη άρχισαν να δημιουργούν τα εθνικά κέντρα συντονισμού, τα οποία λειτουργούν ως σημεία επαφής σε εθνικό επίπεδο για την Κοινότητα. Η σύσταση και η λειτουργία τους συγχρηματοδοτήθηκαν από το πρόγραμμα DIGITAL, με ενωσιακή χρηματοδότηση άνω των 90 εκατομμυρίων ευρώ να έχει χορηγηθεί μέχρι τον χρόνο του ελέγχου, συμπεριλαμβανομένων περίπου 44 εκατομμυρίων ευρώ που θα διανεμηθούν περαιτέρω μέσω της χρηματοδοτικής στήριξης προς τρίτους. Για τη στήριξη των ΕΚΣ, έχουν εγγραφεί στον προϋπολογισμό επιπλέον 38 εκατομμύρια ευρώ μέχρι το 2027.

80 Διαπιστώσαμε ότι, τον Δεκέμβριο του 2025, τέσσερα χρόνια μετά τη σύσταση του ECCC και του δικτύου ΕΚΣ, η Κοινότητα δεν είχε ακόμη συσταθεί και ούτε είχε ακόμη οριστεί η σύνθεση της SAG. Το ECCC ενέκρινε το τελευταίο πρόγραμμα εργασίας για την κυβερνοασφάλεια στο πλαίσιο του προγράμματος DIGITAL στις 14 Μαρτίου 2025, που καλύπτει την περίοδο 2025-2027. Ενώ το ECCC κατάρτισε και ενέκρινε το πρόγραμμα εργασίας του μετά από εκτενείς διαβουλεύσεις με τα κράτη μέλη και το δίκτυο των ΕΚΣ, δεν μπόρεσε να επωφεληθεί από τη συνεισφορά και τις συμβουλές της Κοινότητας ή της SAG. Πρόκειται για μια συνθήκη που έρχεται σε αντίθεση με τις διατάξεις του ιδρυτικού κανονισμού της και θεωρούμε ότι πρόκειται για χαμένη ευκαιρία.

81 Το πρόγραμμα DIGITAL πρόκειται να λήξει το 2027 και, εφόσον δεν παραταθεί η εντολή του, το ECCC αναμένεται να ολοκληρώσει τις εργασίες του το 2029. Ως εκ τούτου, ενδέχεται η υποστήριξη του δικτύου των ΕΚΣ, της Κοινότητας και της SAG, όταν αυτά τεθούν σε λειτουργία, να είναι χρήσιμη μόνο για σύντομο χρονικό διάστημα.

Τα χρηματοδοτούμενα από την ΕΕ έργα επιδιώκουν συναφείς στόχους, αλλά πολλά αντιμετωπίζουν επιχειρησιακά προβλήματα

82 Επιλέξαμε δείγμα 11 έργων που σχετίζονται με τον εντοπισμό και την αντιμετώπιση περιστατικών κυβερνοασφάλειας και χρηματοδοτήθηκαν στο πλαίσιο του προγράμματος DIGITAL κατά την περίοδο 2022-2025 (βλέπε ***γράφημα 5*** στα ***παραρτήματα I*** και ***III***). Αξιολογήσαμε κατά πόσον:

- οι στόχοι των έργων συμβάδιζαν με τα αναμενόμενα αποτελέσματα όπως αυτά είχαν διατυπωθεί στις προσκλήσεις υποβολής προτάσεων και με εκείνα του προγράμματος DIGITAL συνολικά·
- τα έργα έχουν επιτύχει μέχρι στιγμής τις προβλεπόμενες εκροές και τα προβλεπόμενα αποτελέσματά τους·
- οι εκροές των έργων παραδόθηκαν εγκαίρως.

Το αποτέλεσμα της αξιολόγησης αυτής παρουσιάζεται στο ***παράρτημα IV***.

Ορισμένα έργα έχουν να επιδείξουν κάποια πρώτα αποτελέσματα, αλλά πολλά αντιμετωπίζουν προκλήσεις και καθυστερήσεις στη λειτουργία τους

83 Διαπιστώσαμε ότι όλα τα έργα επιδιώκουν στόχους που συμβάλλουν στην επίτευξη των στόχων κυβερνοασφάλειας του προγράμματος DIGITAL[14] και ότι ανταποκρίνονται στους περισσότερους από τους στόχους των προσκλήσεων υποβολής προτάσεων[15].

84 Από τα 11 έργα του δείγματός μας, δύο βρίσκονταν σε πρώιμο στάδιο υλοποίησης και, ως εκ τούτου, δεν μπορέσαμε να καταλήξουμε σε συμπέρασμα σχετικά με τις επιδόσεις τους. Από τα υπόλοιπα, αξιολογήσαμε τέσσερα ως ικανοποιητικά όσον αφορά την επίτευξη των προβλεπόμενων εκροών και αποτελεσμάτων τους. Θεωρήσαμε ότι δύο έργα παρουσιάζουν ορισμένες αδυναμίες και αξιολογήσαμε τρία ως μη ικανοποιητικά (βλέπε ***παράρτημα IV***).

---

[14] Άρθρο 6 του κανονισμού (ΕΕ) 2021/694 για τη θέσπιση του προγράμματος Ψηφιακή Ευρώπη.

[15] Προσκλήσεις υποβολής προτάσεων: Ανάπτυξη ικανοτήτων των κέντρων επιχειρήσεων ασφάλειας· ανάπτυξη του δικτύου εθνικών κέντρων συντονισμού με τα κράτη μέλη· στήριξη της ετοιμότητας και αμοιβαία συνδρομή· και καινοτόμες εφαρμογές της ΤΝ και άλλων τεχνολογιών γενικής εφαρμογής για κέντρα επιχειρήσεων ασφάλειας.

85 Το πρόγραμμα DIGITAL αποσκοπεί ρητά στην αύξηση του επιπέδου κυβερνοασφάλειας των μικρών και μεσαίων επιχειρήσεων (ΜΜΕ). Στο πλαίσιο αυτό, αρκετά έργα προσφέρουν συγκεκριμένες λύσεις για τις ΜΜΕ (βλέπε ***πλαίσιο 2***).

Πλαίσιο 2

Παραδείγματα έργων που αποφέρουν απτά αποτελέσματα στις ΜΜΕ

Το έργο GR-SME-SOC (έργο αριθ. 6 στο ***παράρτημα III***) αποσκοπεί στην παροχή εργαλείων και υπηρεσιών κυβερνοασφάλειας στις ΜΜΕ στην Ελλάδα, με τη δημιουργία ενός κέντρου επιχειρήσεων ασφάλειας (SOC) προσαρμοσμένου στις ανάγκες τους. Το έργο ξεκίνησε τον Ιανουάριο του 2024 και υλοποιείται από κοινοπραξία πέντε ελληνικών οργανισμών. Το σχέδιο είναι να προσφερθούν δωρεάν υπηρεσίες κυβερνοασφάλειας σε 120 ΜΜΕ για ένα έτος και, στη συνέχεια, οι υπηρεσίες να διατεθούν στο εμπόριο. Το έργο προσφέρει στις ΜΜΕ προηγμένες υπηρεσίες, όπως παρακολούθηση σε πραγματικό χρόνο, ανίχνευση απειλών με βάση την ΤΝ και ταχεία αντιμετώπιση περιστατικών.

Με το έργο NCC-IE (έργο αριθ. 3 στο ***παράρτημα III***), ο συντονιστής του έργου παρείχε επιχορηγήσεις ύψους περίπου 1,8 εκατομμυρίων ευρώ σε περισσότερες από 50 ιρλανδικές ΜΜΕ για τη βελτίωση της κυβερνοασφάλειάς τους. Το καθεστώς επιχορηγήσεων ωφέλησε εταιρείες με 2 έως περίπου 200 εργαζομένους, συμπεριλαμβανομένων οικογενειακών επιχειρήσεων, νεοφυών επιχειρήσεων και παγκόσμιων εξαγωγέων σε διάφορους τομείς. Οι επιχορηγήσεις προορίζονταν αποκλειστικά για εταιρείες που είχαν προηγουμένως υποβληθεί σε έλεγχο κυβερνοασφάλειας υπό τη διαχείριση της κρατικής υπηρεσίας Enterprise Ireland. Η επιχορήγηση κάλυπτε το 80 % των δαπανών (έως 60 000 ευρώ) για την υλοποίηση των συστάσεων που είχαν διατυπωθεί στο πλαίσιο του ως άνω ελέγχου.

Πηγή: ΕΕΣ.

86 Πολλά έργα του δείγματός μας πασχίζουν να τηρήσουν τις προθεσμίες ή αντιμετωπίζουν επιχειρησιακές προκλήσεις (βλέπε ***παράρτημα IV***). Διαπιστώσαμε ότι τέσσερα έργα αντιμετωπίζουν σημαντικές καθυστερήσεις. Μεταξύ αυτών οι κόμβοι ENSOC και ATHENA, όπως περιγράφεται λεπτομερώς στα σημεία ***65***-***70***. Στο ***πλαίσιο 3*** παρουσιάζουμε και άλλα παραδείγματα.

Πλαίσιο 3

Παραδείγματα έργων που αντιμετωπίζουν επιχειρησιακές προκλήσεις και καθυστερήσεις

Στην Ιρλανδία, η αρχή διαχείρισης της τοπικής αυτοδιοίκησης (LGMA) είναι ο μοναδικός δικαιούχος της επιχορήγησης για το έργο ILG-SOC (έργο αριθ. 8 στο ***παράρτημα III***). Στόχος του έργου είναι η δημιουργία ενός επιτελικού κέντρου επιχειρήσεων ασφάλειας για 31 τοπικές αρχές, το οποίο θα χρησιμοποιεί προηγμένα εργαλεία ανίχνευσης και αντιμετώπισης απειλών. Το έργο ξεκίνησε τον Οκτώβριο του 2023, με διάρκεια τριών ετών. Στο πλαίσιο της ενδιάμεσης επανεξέτασης, όλα τα παραδοτέα απορρίφθηκαν. Το έργο περιλαμβάνει διάφορες διαδικασίες σύναψης συμβάσεων που απέτυχαν ή καθυστέρησαν. Η διάρκεια του έργου θα παραταθεί (χωρίς πρόσθετη χρηματοδότηση), γεγονός που θα μπορούσε να δώσει στο έργο αρκετό χρονικό περιθώριο για να ολοκληρωθεί επιτυχώς.

Στην Ελλάδα, το έργο EL-SOC (έργο αριθ. 5 στο ***παράρτημα III***) αποσκοπεί στη δημιουργία ενός ενοποιημένου SOC («Ενοποιημένο Κέντρο Αναφοράς Κυβερνοασφάλειας») σε εθνικό επίπεδο, το οποίο θα συγκεντρώνει πληροφορίες από τα τομεακά SOC. Με τον τρόπο αυτό θα παρέχεται ολοκληρωμένη επισκόπηση της κατάστασης στον τομέα της κυβερνοασφάλειας σε πραγματικό χρόνο. Το έργο θα λειτουργεί μεταξύ Ιανουαρίου 2024 και Δεκεμβρίου 2026. Η προγραμματισμένη προμήθεια υλισμικού και υπηρεσιών καθυστέρησε λόγω προβλημάτων στην οριστικοποίηση και τη δημοσίευση των τεχνικών προδιαγραφών στο πλαίσιο της πρόσκλησης υποβολής προσφορών. Ο συντονιστής του έργου απέδωσε την καθυστέρηση, μεταξύ άλλων, σε ζητήματα που σχετίζονται με την εξασφάλιση εθνικής συγχρηματοδότησης και στην περιορισμένη διαθεσιμότητα προσωπικού στον τομέα των δημόσιων συμβάσεων.

Πηγή: ΕΕΣ.

87 Δύο άλλα έργα του δείγματός μας αντιμετωπίζουν μέτριες καθυστερήσεις, ενώ τρία παρήγαγαν τις εκροές τους εγκαίρως. Τέλος, δύο έργα βρίσκονται σε πρώιμο στάδιο υλοποίησης και, ως εκ τούτου, δεν μπορούμε να καταλήξουμε σε συμπέρασμα.

Οι περιορισμοί ασφάλειας έχουν προκαλέσει επιχειρησιακά κωλύματα, ενώ σημαντικοί κίνδυνοι ανακύπτουν από τη διενέργεια ελέγχων από τους δικαιούχους

88 Ο κανονισμός DIGITAL προβλέπει ότι, για λόγους ασφάλειας, η χρηματοδότηση για την κυβερνοασφάλεια μπορεί να περιορίζεται σε οντότητες που είναι εγκατεστημένες στην ΕΕ και ελέγχονται από κράτη μέλη ή πολίτες της ΕΕ. Ο περιορισμός αυτός αποσκοπεί στον μετριασμό του κινδύνου παρείσφρησης κρατών εκτός της ΕΕ ή άσκησης από αυτά επιρροής και στην αποτροπή της ανταλλαγής ευαίσθητων πληροφοριών ασφάλειας με αρχές τρίτων χωρών.

89 Η υποχρέωση ιδιοκτησιακού καθεστώτος και ελέγχου εντός της ΕΕ ισχύει όχι μόνο για τους δικαιούχους επιχορηγήσεων, αλλά και για τους υπεργολάβους τους και τυχόν αποδέκτες χρηματοδοτικής στήριξης προς τρίτους (FSTP). Με εξαίρεση την τελευταία κατηγορία (βλέπε σημεία ***92-96***), η αξιολόγηση διενεργείται από την κεντρική υπηρεσία επικύρωσης του Ευρωπαϊκού Εκτελεστικού Οργανισμού Έρευνας. Ωστόσο, η τελική απόφαση σχετικά με την επιλεξιμότητα για συμμετοχή σε κλειστές διαδικασίες εξακολουθεί να εναπόκειται στη χορηγούσα αρχή, δηλαδή στη ΓΔ Connect ή στο ECCC.

90 Κατά τη διάρκεια των ελεγκτικών εργασιών μας, οι δικαιούχοι ανέφεραν επανειλημμένα τις πρακτικές προκλήσεις που θέτουν οι αξιολογήσεις ιδιοκτησιακού καθεστώτος και ελέγχου. Η αξιολόγηση της ύπαρξης ιδιοκτησιακού καθεστώτος και ελέγχου εντός της ΕΕ μπορεί να είναι μια πολύπλοκη και χρονοβόρα διαδικασία. Απαιτείται ανάλυση της πλήρους ιδιοκτησιακής δομής και της αλυσίδας ελέγχου κάθε οργανισμού, συμπεριλαμβανομένων όλων των επιπέδων ιδιοκτησίας μέχρι τους τελικούς ιδιοκτήτες. Η κεντρική υπηρεσία επικύρωσης απαιτεί από κάθε οντότητα να παρέχει εκτενή τεκμηρίωση σχετικά με την ιδιοκτησιακή δομή και τα ειδικά δικαιώματά της, την εταιρική διακυβέρνηση και τυχόν εμπορικούς, οικονομικούς ή άλλους δεσμούς που επιτρέπουν την απόκτηση του ελέγχου.

91 Σε τρία χρηματοδοτούμενα από την ΕΕ έργα του δείγματός μας, τουλάχιστον ένας δικαιούχος κοινοπραξίας αποκλείστηκε στη συνέχεια, καθώς κρίθηκε ότι ήταν υπό την ιδιοκτησία ή τον έλεγχο τρίτης χώρας. Το γεγονός ότι αποκλείστηκαν μέλη της κοινοπραξίας καταδεικνύει ότι η έννοια της ύπαρξης ιδιοκτησιακού καθεστώτος και ελέγχου εντός της ΕΕ δεν είναι πλήρως κατανοητή από όλους τους συμμετέχοντες στο πρόγραμμα DIGITAL. Συνολικά, με βάση τα δεδομένα της κεντρικής υπηρεσίας επικύρωσης, το 7 % του συνόλου των αιτούντων επιχορηγήσεις του προγράμματος DIGITAL σε σχέση με την κυβερνοασφάλεια ή υπεργολάβων απέτυχαν στην εν λόγω αξιολόγηση κατά την περίοδο 2022-2025. Η υποβολή αίτησης από μη επιλέξιμους συμμετέχοντες στο πλαίσιο πρόσκλησης υποβολής προτάσεων προξενεί καθυστερήσεις, όπως φαίνεται στο ***πλαίσιο 4***.

Πλαίσιο 4

Ενδεικτική περίπτωση στην οποία οι δικαιούχοι αποκλείστηκαν μετά την αποτυχία τους στους ελέγχους ασφαλείας

Δύο από τα μέλη της κοινοπραξίας του έργου NG-SOC (έργο αριθ. 7 στο ***παράρτημα III***) δεν κατάφεραν να περάσουν επιτυχώς την αξιολόγηση ιδιοκτησιακού καθεστώτος και ελέγχου. Το αποτέλεσμα ανακοινώθηκε περίπου έναν μήνα πριν από τη λήξη της προθεσμίας για την υπογραφή της συμφωνίας επιχορήγησης.
Ο συντονιστής του έργου χρειάστηκε να συμφωνήσει να αναλάβει τις εργασίες που είχαν προηγουμένως ανατεθεί στα δύο αποκλεισθέντα μέλη, καθώς δεν υπήρχε χρόνος για την εξεύρεση νέου εταίρου. Ένα από τα αποκλεισθέντα μέλη ανήκε σε συγκεκριμένο κλάδο στον οποίο επρόκειτο να εφαρμοστεί πιλοτικά η λύση που είχε αναπτυχθεί. Ως εκ τούτου, σημαντικό μέρος του έργου, το οποίο αφορούσε τη δοκιμή των λύσεων στην πράξη, δεν θα μπορούσε να προχωρήσει σύμφωνα με τον προγραμματισμό. Η κατάσταση αυτή διορθώθηκε αργότερα με την τροποποίηση της συμφωνίας επιχορήγησης ώστε να συμπεριληφθούν νέα μέλη.

Πηγή: ΕΕΣ.

92 Δύο από τα έργα που εξετάσαμε (NCC-IE και CYberSynchrony) παρέχουν χρηματοδοτική στήριξη προς τρίτους (FSTP). Ο εν λόγω μηχανισμός χρηματοδότησης επιτρέπει στους δικαιούχους επιχορηγήσεων να χρησιμοποιούν μέρος της επιχορήγησης για τη χρηματοδότηση άλλων οντοτήτων μέσω ανοικτών προσκλήσεων υποβολής προτάσεων. Η χρηματοδοτική στήριξη προς τρίτους μπορεί να διευκολύνει την πρόσβαση σε ενωσιακή χρηματοδότηση. Στην περίπτωση αυτή, οι δικαιούχοι φέρουν την αποκλειστική ευθύνη για τη διεξαγωγή των αξιολογήσεων ιδιοκτησιακού καθεστώτος και ελέγχου, και δεν εμπλέκεται η κεντρική υπηρεσία επικύρωσης.

93 Το 2021 η Επιτροπή δημοσίευσε γενικές κατευθυντήριες γραμμές για το κοινό που απευθύνονταν σε όσους υπέβαλαν αίτηση σε κλειστές διαδικασίες, οι οποίες επικαιροποιήθηκαν το 2026. Μολονότι η χρηματοδοτική στήριξη προς τρίτους εφαρμόζεται από το 2021 για τις προσκλήσεις υποβολής προτάσεων στο πλαίσιο του προγράμματος DIGITAL, ούτε η Επιτροπή ούτε το ECCC έχουν παράσχει λεπτομερή μεθοδολογία στους δικαιούχους σχετικά με τον τρόπο με τον οποίο θα πρέπει να διενεργούν την αξιολόγηση του ιδιοκτησιακού καθεστώτος και του ελέγχου στο πλαίσιο της ευρύτερης αξιολόγησης των τρίτων στους οποίους παρέχουν τη χρηματοδοτική αυτή στήριξη. Τον Ιούλιο του 2025 το ECCC κοινοποίησε μη υποχρεωτική καθοδήγηση, παρέχοντας στο δίκτυο των ΕΚΣ δομημένη προσέγγιση όσον αφορά τις αξιολογήσεις ιδιοκτησιακού καθεστώτος και ελέγχου. Το έγγραφο καθοδήγησης περιέχει γενικές αρχές και μέτρα που θα μπορούσαν να ληφθούν. Ωστόσο, δεν προσδιορίζει τον τρόπο με τον οποίο θα πρέπει να διενεργούνται οι αξιολογήσεις αυτές, καθιστώντας έτσι τους δικαιούχους υπεύθυνους για την ανάπτυξη της δικής τους προσέγγισης.

94 Διαπιστώσαμε ότι το ECCC δεν επικυρώνει τη μεθοδολογία που υιοθετούν οι δικαιούχοι ούτε διενεργεί δειγματοληπτικούς ελέγχους για να διασφαλίσει ότι η μεθοδολογία είναι αρκετά αξιόπιστη και ότι οι επιλεγμένοι αποδέκτες χρηματοδοτικής στήριξης είναι πράγματι εγκατεστημένοι στην ΕΕ και ελέγχονται από κράτη μέλη ή πολίτες της ΕΕ.

95 Στην ετήσια έκθεσή μας για το 2024, διαπιστώσαμε ότι οι δικαιούχοι στους οποίους η Επιτροπή έχει αναθέσει τη διαχείριση της χρηματοδοτικής στήριξης προς τρίτους (στον τομέα της έρευνας) δεν υποχρεούνταν να αποδεικνύουν την αποτελεσματικότητα των δικλίδων που εφαρμόζουν, προκειμένου να διασφαλίζουν την κανονικότητα των δαπανών της ΕΕ. Ομοίως, το ECCC δεν αξιολογεί τη διοικητική και τεχνική ικανότητα των δικαιούχων να διαχειρίζονται ορθά τις αξιολογήσεις του ιδιοκτησιακού καθεστώτος και του ελέγχου. Όπως περιγράφεται λεπτομερώς στο σημείο ***90***, η αξιολόγηση αυτή μπορεί να είναι πολύπλοκη και διενεργείται σε επίπεδο ΕΕ από ειδική υπηρεσία με εξειδικευμένη εμπειρογνωσία.

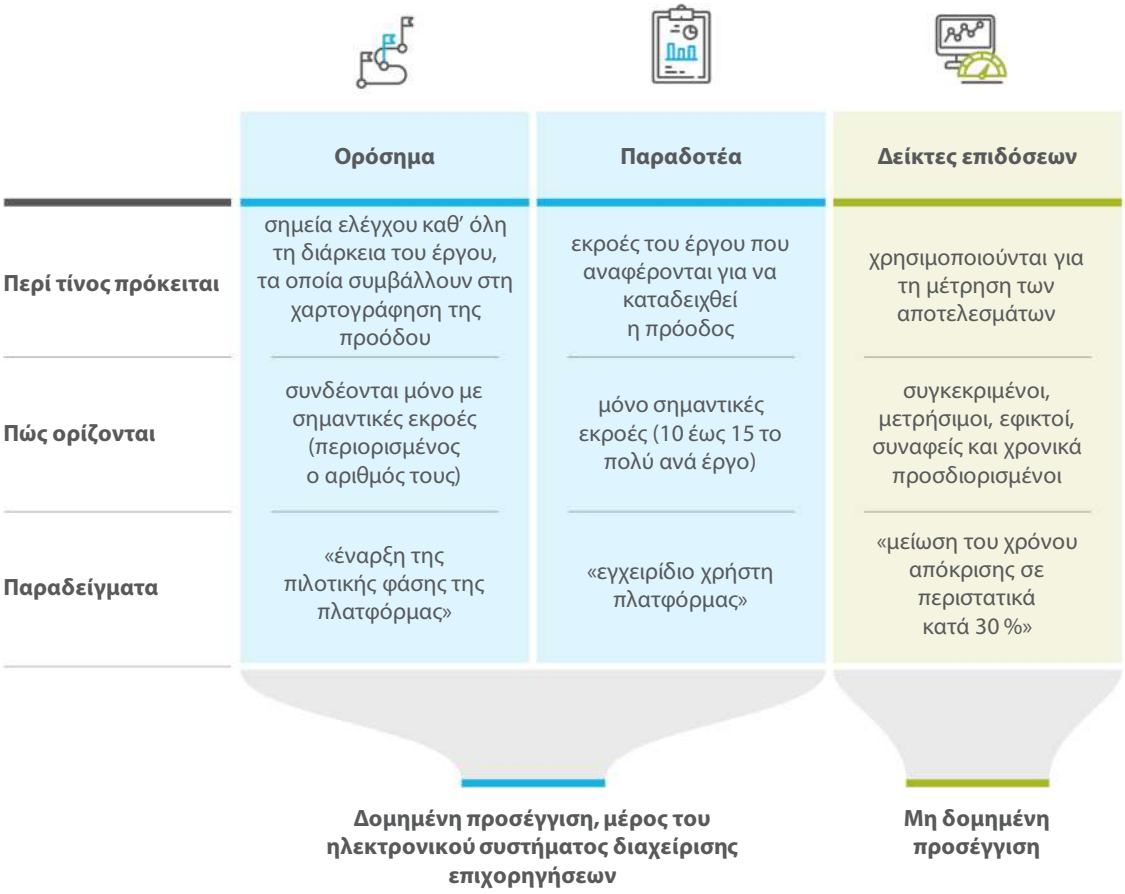
96 Στο πλαίσιο αυτό, θεωρούμε ότι υπάρχει σημαντικός κίνδυνος οι δικαιούχοι, οι οποίοι είναι υπεύθυνοι για τη διενέργεια των ελέγχων του ιδιοκτησιακού καθεστώτος και του ελέγχου, να μην έχουν την ικανότητα σωστής εκτέλεσής τους. Δεδομένης της φύσης των χρηματοδοτούμενων δραστηριοτήτων, η αδυναμία αυτή θα μπορούσε να εκθέσει σε κίνδυνο ευαίσθητες υποδομές, επιχειρησιακά δεδομένα και κρίσιμες για την ασφάλεια τεχνολογίες.

Τα περισσότερα έργα που χρηματοδοτούνται από την ΕΕ έχουν ανεπαρκή πλαίσια επιδόσεων και τα σχετικά με τις επιδόσεις στον τομέα της κυβερνοασφάλειας δεδομένα του προγράμματος DIGITAL δεν είναι ακριβή

Τα περισσότερα έργα που χρηματοδοτούνται από την ΕΕ έχουν ανεπαρκή πλαίσια επιδόσεων

97 Οι δικαιούχοι που διαχειρίζονται έργα χρηματοδοτούμενα από την ΕΕ πρέπει να αναφέρουν στο ECCC στοιχεία σχετικά με την πρόοδο και τα αποτελέσματά τους, χρησιμοποιώντας ορόσημα, παραδοτέα και δείκτες, όπως παρουσιάζεται στο ***γράφημα 8***. Εξετάσαμε κατά πόσον τα ορόσημα και τα παραδοτέα που καθορίστηκαν για κάθε έργο καθιστούν δυνατή την παρακολούθηση των έργων. Αξιολογήσαμε επίσης κατά πόσον οι δείκτες επιδόσεων του έργου είναι συναφείς και μετρήσιμοι και έχουν τιμή βάσης και τιμή-στόχο.

Γράφημα 8 | Ορόσημα, παραδοτέα και δείκτες επιδόσεων σε έργα του προγράμματος DIGITAL



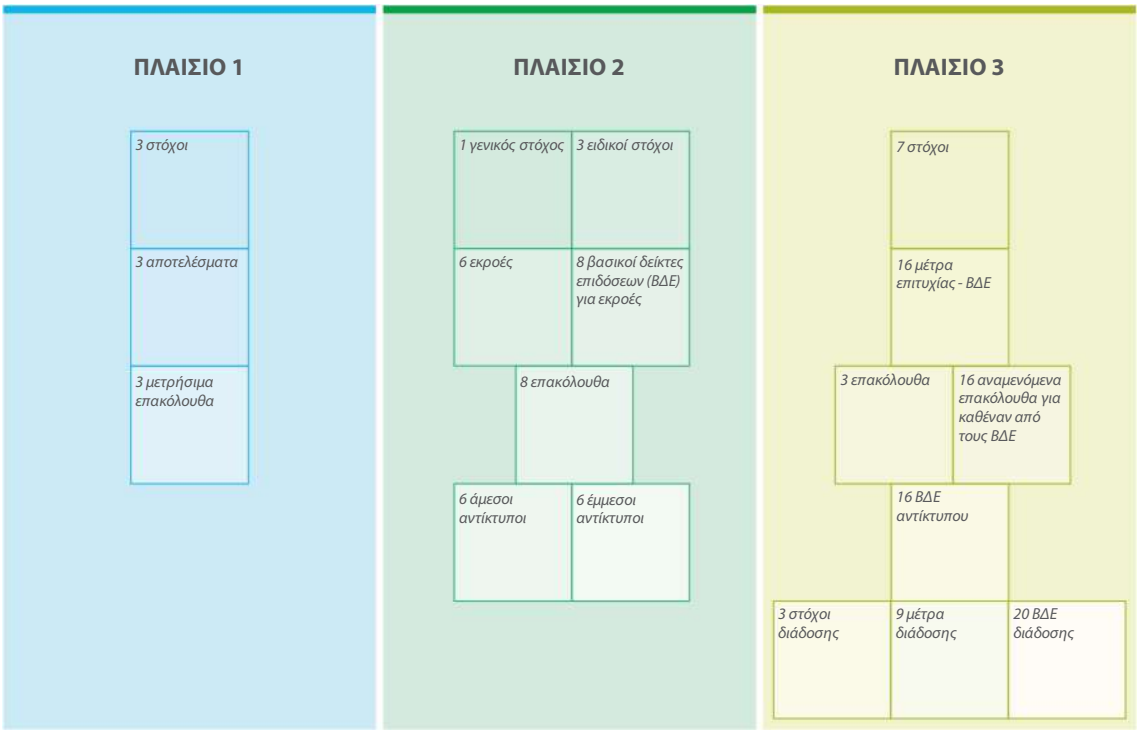
Πηγή: ΕΕΣ, βάσει του εντύπου της αίτησης επιχορήγησης.

98 Στην πρόταση έργου τους, οι δικαιούχοι πρέπει να καθορίσουν μια σειρά ορόσημων και παραδοτέων, ακολουθώντας μια δομημένη προσέγγιση που καθορίζεται στις οδηγίες προς τους αιτούντες. Όλα τα ορόσημα και τα παραδοτέα απαριθμούνται στο ηλεκτρονικό σύστημα διαχείρισης επιχορηγήσεων χάριν καλύτερης παρακολούθησής τους. Συνήθως, το ECCC εξετάζει κάθε έργο δύο φορές: μια πρώτη φορά στα μισά της υλοποίησής του και μια δεύτερη μετά την ολοκλήρωσή του. Κατά τη διάρκεια των εξετάσεων αυτών, εξωτερικοί εμπειρογνώμονες επαληθεύουν την επίτευξη των ορόσημων και των παραδοτέων και το ECCC τα επικυρώνει. Τα ορόσημα και τα παραδοτέα είναι επομένως καίριας σημασίας για την παρακολούθηση των έργων και πρέπει να καθορίζονται με τον κατάλληλο τρόπο.

99 Διαπιστώσαμε ότι σχεδόν κανένα από τα έργα του δείγματός μας δεν τήρησε τις οδηγίες σχετικά με τον αριθμό των ορόσημων και των παραδοτέων: ο αριθμός των ορόσημων ανά έργο κυμαίνεται από 8 έως 39, ενώ ο αριθμός των παραδοτέων από 8 έως 45. Πολλά από τα ορόσημα και τα παραδοτέα δεν τηρούν τις οδηγίες σχετικά με τον τρόπο καθορισμού τους και, ως εκ τούτου, δεν είναι χρήσιμα για την παρακολούθηση της προόδου (παραδείγματος χάριν, «συνάντηση για την έναρξη της κατάρτισης πρόσκλησης υποβολής ερευνητικών προτάσεων» ή «επίσημα πρακτικά συνάντησης στο πλαίσιο έργου»).
Για τρία έργα, η επιτροπή αξιολόγησης είχε εντοπίσει τα ζητήματα αυτά πριν από την υπογραφή της επιχορήγησης. Σε δύο περιπτώσεις, οι δικαιούχοι πρότειναν μόνο ήσσονος σημασίας αλλαγές (π.χ. στις καταληκτικές ημερομηνίες) χωρίς να αντιμετωπίσουν τα βασικά ζητήματα, ενώ στην τρίτη περίπτωση δεν έγινε καμία αλλαγή. Για έξι ακόμη έργα του δείγματός μας, από την ανάλυσή μας προκύπτει ότι τα ορόσημα ή τα παραδοτέα δεν συμβαδίζουν με τις οδηγίες και δεν είναι πάντοτε κατάλληλα. Θεωρούμε ότι ο ακατάλληλος καθορισμός παραδοτέων ή ορόσημων ή ο υπερβολικά μεγάλος αριθμός αυτών δυσχεραίνει την παρακολούθηση της προόδου.

100 Σε αντίθεση με τα ορόσημα και τα παραδοτέα, οι δείκτες επιδόσεων δεν ακολουθούν δομημένη προσέγγιση και δεν ενοποιούνται σε πίνακα στο σύστημα διαχείρισης επιχορηγήσεων, αλλά είναι διάσπαρτοι σε διάφορα τμήματα της πρότασης. Η προσέγγιση αυτή είχε ως αποτέλεσμα να προταθεί πληθώρα πλαισίων επιδόσεων από τους δικαιούχους. Ενώ ορισμένοι έχουν θέσει αποκλειστικά στόχους έργων που συνδέονται με δείκτες επιδόσεων, άλλοι έχουν δημιουργήσει πολύ πιο σύνθετα πλαίσια επιδόσεων. Στο ***γράφημα 9*** παρουσιάζουμε ορισμένα παραδείγματα.

Γράφημα 9 | Παράδειγμα της ποικιλίας των πλαισίων επιδόσεων που σχεδιάστηκαν για τα έργα



Πηγή: ΕΕΣ.

101 Από την ανάλυσή μας καταλήγουμε στο ότι πολλοί από τους δείκτες επιδόσεων που χρησιμοποιούν οι δικαιούχοι δεν είναι συναφείς ή μετρήσιμοι και στερούνται τιμής-στόχου ή τιμής βάσης (βλέπε ***πλαίσιο 5***). Επιπλέον, επτά έργα έχουν καθορίσει 20 τουλάχιστον δείκτες, ενώ ένα έργο έχει 52. Το αποτέλεσμα της αξιολόγησης αυτής παρουσιάζεται στο ***παράρτημα IV***.

Πλαίσιο 5

Παραδείγματα ακατάλληλων δεικτών επιδόσεων

Μη μετρήσιμοι:

- «Δείκτης παραβίασης και άλλες παρεχόμενες υπηρεσίες ενισχύουν τις ικανότητες κυβερνοασφάλειας των ΜΜΕ»
- «Παροχή εργαλείων και μεθόδων αντιμετώπισης περιστατικών που επιτρέπουν την ενοποίηση με τους διαύλους επικοινωνίας του EU-CyCLONe»

Δεν παρέχεται τιμή βάσης ή τιμή-στόχος:

- «Βελτίωση της ετοιμότητας του προσωπικού κατά ≥ 20 %»
- «Μείωση κατά ≥ 20 % των προσπαθειών που απαιτούνται για την ευθυγράμμιση και τη συμμόρφωση με τις σχετικές πρωτοβουλίες της ΕΕ για την κυβερνοασφάλεια»

Δεν σχετίζονται με τις επιδόσεις:

- «Τελική έκθεση σχετικά με το έργο στο τέλος της φάσης χρηματοδότησης»
- «Αριθμός ασκουμένων που θα συμμετάσχουν σε όλες τις συνεδρίες κατάρτισης»

Πηγή: ΕΕΣ, βάσει της τεκμηρίωσης του έργου.

102 Συνολικά, θεωρούμε ότι η μεγάλη ποικιλία των πλαισίων επιδόσεων, ο ακατάλληλος καθορισμός των δεικτών και ο υπερβολικός αριθμός τους περιπλέκουν σημαντικά την παρακολούθηση των επιδόσεων. Ως εκ τούτου, δεν είναι δυνατή η ορθή αξιολόγηση των επιδόσεων των έργων. Η κατάσταση περιπλέκεται περαιτέρω από το γεγονός ότι το υπόδειγμα αναφοράς στοιχείων δεν περιέχει ειδική ενότητα σχετικά με τους δείκτες επιδόσεων των έργων και, ως εκ τούτου, τα περισσότερα έργα του δείγματός μας δεν ανέφεραν σχετικά στοιχεία.

Τα δεδομένα σχετικά με τις επιδόσεις της συνιστώσας κυβερνοασφάλειας του προγράμματος DIGITAL δεν είναι ακριβή

103 Για την παρακολούθηση των επιτευγμάτων του προγράμματος DIGITAL, ο σχετικός κανονισμός προβλέπει δείκτες προγράμματος σχετικά με τους οποίους πρέπει να αναφέρουν στοιχεία όλα τα έργα, όπως περιγράφεται λεπτομερώς στο ***πλαίσιο 6***.

Πλαίσιο 6

Δείκτες του προγράμματος DIGITAL για την κυβερνοασφάλεια

1.α Ο αριθμός υποδομών ή εργαλείων κυβερνοασφάλειας, ή και των δύο, που αποκτώνται με κοινές συμβάσεις, μεταξύ άλλων στο πλαίσιο του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια

1.β Ο αριθμός υποδομών ή εργαλείων κυβερνοασφάλειας, ή και τα δύο, που τέθηκαν σε λειτουργία

2. Ο αριθμός χρηστών και κοινοτήτων χρηστών που αποκτούν πρόσβαση σε ευρωπαϊκά μέσα κυβερνοασφάλειας

3. Ο αριθμός των δράσεων που στηρίζουν την ετοιμότητα και την αντιμετώπιση περιστατικών κυβερνοασφάλειας στο πλαίσιο του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια

Πηγή: Παράρτημα II του κανονισμού (ΕΕ) 2021/694 για τη θέσπιση του προγράμματος Ψηφιακή Ευρώπη· πλαίσιο παρακολούθησης και αξιολόγησης του προγράμματος «Ψηφιακή Ευρώπη» (SWD(2024) 37).

104 Αξιολογήσαμε κατά πόσον τα έργα του δείγματός μας είχαν αναφέρει στοιχεία σχετικά με τους εν λόγω δείκτες και εξετάσαμε τον τρόπο με τον οποίο το ECCC συλλέγει και επαληθεύει τα εν λόγω στοιχεία.

105 Όλα τα έργα πρέπει να αναφέρουν στοιχεία σχετικά με τους δείκτες του προγράμματος DIGITAL πριν από την ενδιάμεση και την τελική επανεξέτασή τους στο σύστημα διαχείρισης επιχορηγήσεων. Διαπιστώσαμε ότι, από τα επτά έργα που βρίσκονταν στα μέσα του χρονοδιαγράμματος κατά τη διάρκεια του ελέγχου μας και τα οποία, ως εκ τούτου, θα έπρεπε να είχαν αναφέρει στοιχεία σχετικά με τους εν λόγω δείκτες, τρία μόνο το είχαν κάνει. Από τα τρία αυτά έργα, δύο δεν είχαν αναφέρει ακριβείς πληροφορίες: το ένα είχε αναφέρει εσφαλμένο δείκτη, ενώ το άλλο ανέφερε τιμές-στόχο αντί για επιτευχθέντα αποτελέσματα.

106 Κάθε χρόνο, η Επιτροπή αναφέρει τους δείκτες αυτούς στις δηλώσεις επιδόσεων προγράμματος. Μπορούν έτσι οι συμφεροντούχοι να αξιολογήσουν κατά πόσο το πρόγραμμα επιτυγχάνει τους στόχους του. Σύμφωνα με τις δηλώσεις επιδόσεων προγράμματος του 2024, οι δείκτες του προγράμματος DIGITAL για την κυβερνοασφάλεια βρίσκονται σε καλό δρόμο. Το ECCC μάς εξήγησε ότι χρησιμοποίησε μια σειρά ερωτηματολογίων που εστάλησαν στους δικαιούχους των έργων για την κατάρτιση των εν λόγω δεικτών, αντί να βασιστεί στο σύστημα διαχείρισης των επιχορηγήσεων. Εξετάσαμε τα αναλυτικά δεδομένα που παρείχε το ECCC και εντοπίσαμε πολλά προβλήματα όσον αφορά τον τρόπο συλλογής των δεδομένων και τη συνολική ποιότητά τους. Διαπιστώσαμε ότι τα δεδομένα που συλλέχθηκαν δεν αντιστοιχούν στις τιμές που παρουσιάζονται στη δήλωση επιδόσεων του προγράμματος και, ως εκ τούτου, δεν είναι σαφής ο τρόπος υπολογισμού των αναφερόμενων τιμών. Δεν εντοπίσαμε στοιχεία που να αποδεικνύουν ότι η ακρίβεια των αναφερόμενων δεδομένων επαληθεύτηκε από το ECCC. Βάσει των ελέγχων που διενεργήσαμε στα έργα του δείγματός μας, και δεδομένου ότι οι περισσότερες τιμές είναι ελλιπείς ή ανακριβείς, θεωρούμε ότι τα αναφερόμενα δεδομένα δεν αντικατοπτρίζουν κατάλληλα τα επιτευχθέντα αποτελέσματα.

Η παρούσα έκθεση εγκρίθηκε από το Τμήμα III, του οποίου προεδρεύει ο George Marius Hyzler, Μέλος του Ελεγκτικού Συνεδρίου, στο Λουξεμβούργο, κατά τη συνεδρίασή του της 16ης Ιουνίου 2026.

Για το Ελεγκτικό Συνέδριο

Tony Murphy
Πρόεδρος

Παραρτήματα

Παράρτημα I – Σχετικά με τον έλεγχο

01 Η κυβερνοασφάλεια ορίζεται ως «οι δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων»[1]. Ως κυβερνοαπειλή ορίζεται «κάθε πιθανή περίσταση, πιθανό συμβάν ή πιθανή ενέργεια που θα μπορούσε να καταστρέψει, να διαταράξει ή να επιδράσει κατ' άλλον τρόπο δυσμενώς στα συστήματα δικτύου και πληροφοριών, στους χρήστες των εν λόγω συστημάτων και σε άλλα πρόσωπα»[2]. Η κυβερνοασφάλεια απαιτεί μια ολιστική προσέγγιση, η οποία θα συνίσταται σε μια σειρά αλληλένδετων δραστηριοτήτων για την πρόληψη, τον εντοπισμό, την αντιμετώπιση κυβερνοαπειλών και την ανάκαμψη από αυτές, όπως φαίνεται στο ***γράφημα 1*** κατωτέρω.

[1] Κανονισμός (ΕΕ) 2019/881 («Πράξη για την κυβερνοασφάλεια»).

[2] Άρθρο 2 της Πράξης για την κυβερνοασφάλεια.

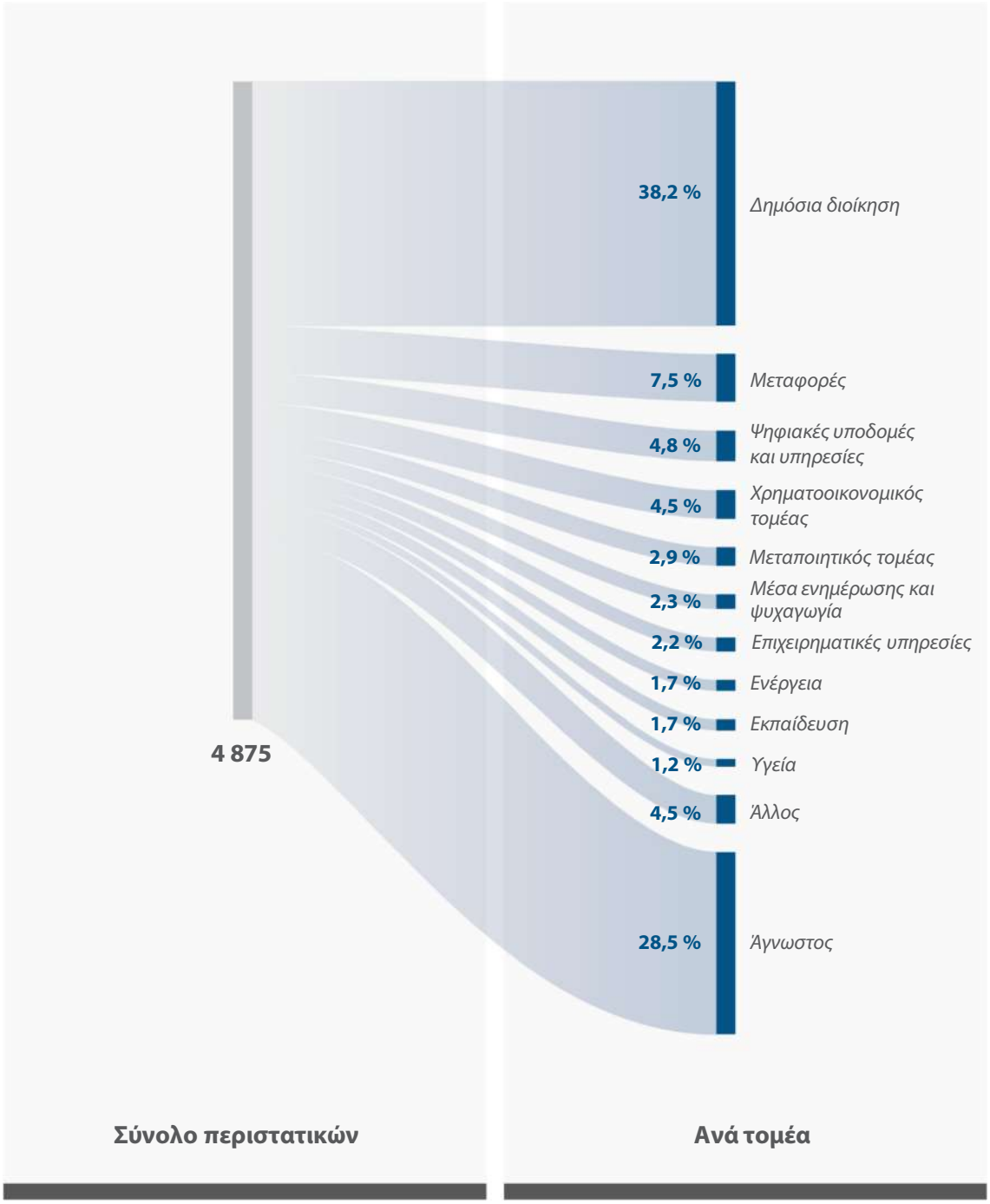
Γράφημα 1 | Παραδείγματα δραστηριοτήτων κυβερνοασφάλειας

Πηγή: ΕΕΣ, βάσει της αιτιολογικής σκέψης 78 της οδηγίας (ΕΕ) 2022/2555 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση (οδηγία NIS 2).

02 Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) θεωρεί ότι το επίπεδο των κυβερνοαπειλών είναι σημαντικό, επισημαίνοντας παράλληλα ότι το τοπίο των απειλών για την κυβερνοασφάλεια έχει καταστεί και εξακολουθεί να είναι σημαντικά πιο περίπλοκο[3]. Οι απειλές αυτές υπογραμμίζουν τη ζωτική σημασία της κυβερνοασφάλειας στις ολοένα και περισσότερο ψηφιακές οικονομίες και κοινωνίες. Στην έκθεσή του για το τοπίο των απειλών του 2025, ο ENISA προσδιόρισε το λυτρισμικό ως την πλέον κρίσιμη απειλή στην ΕΕ. Στο ***γράφημα 2*** παρουσιάζονται οι τομείς που βρίσκονται στο στόχαστρο.

[3] ENISA, Έκθεση σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση το 2024.

Γράφημα 2 | Τομείς που αποτελούν στόχο κυβερνοεπιθέσεων



Πηγή: ΕΕΣ, βάσει του ENISA.

Σημαντικά και μεγάλης κλίμακας περιστατικά κυβερνοασφάλειας

03 Τα περιστατικά κυβερνοασφάλειας, στα οποία περιλαμβάνονται κυβερνοαπειλές και ακούσια συμβάντα (όπως αυτά που αναφέρονται στο ***γράφημα 3*** και στο σημείο ***40***), «μπορούν να παρεμποδίσουν την παροχή δημόσιων υπηρεσιών [και] την άσκηση οικονομικών δραστηριοτήτων, […] να προκαλέσουν σημαντικές οικονομικές ζημίες, να υπονομεύσουν την εμπιστοσύνη των χρηστών, να προκαλέσουν σημαντική ζημία στην οικονομία και τα δημοκρατικά συστήματα της Ένωσης, και μπορούν ακόμη και να έχουν συνέπειες που απειλούν την υγεία ή τη ζωή»[4]. Ένα περιστατικό κυβερνοασφάλειας θεωρείται[5]:

- **σημαντικό**, εάν έχει προκαλέσει ή θα μπορούσε να προκαλέσει σοβαρή λειτουργική διατάραξη των υπηρεσιών ή οικονομική ζημία για την οικεία οντότητα, ή εάν έχει επηρεάσει ή θα μπορούσε να επηρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία·
- **μεγάλης κλίμακας**, εάν έχει προκαλέσει διατάραξη που υπερβαίνει την ικανότητα ενός κράτους μέλους να ανταποκριθεί σε αυτήν ή το οποίο έχει σημαντικό αντίκτυπο σε τουλάχιστον δύο κράτη μέλη.

04 Ένα μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας μπορεί να κλιμακωθεί σε μια μεγάλων διαστάσεων **κυβερνοκρίση στην ΕΕ**, εάν εμποδίζει την ορθή λειτουργία της εσωτερικής αγοράς ή ενέχει σοβαρούς κινδύνους για τη δημόσια ασφάλεια και την προστασία οντοτήτων ή πολιτών σε διάφορα κράτη μέλη ή στην ΕΕ στο σύνολό της[6].

---

[4] Αιτιολογική σκέψη 2 του κανονισμού (ΕΕ) 2025/38 (πράξη για την αλληλεγγύη στον κυβερνοχώρο).

[5] Άρθρα 6 και 23 της οδηγίας NIS 2, τα οποία αναλύονται περαιτέρω στον εκτελεστικό κανονισμό (ΕΕ) 2024/2690 της Επιτροπής για σειρά παρόχων στον τομέα των ψηφιακών υποδομών.

[6] Αιτιολογική σκέψη 69 της οδηγίας NIS 2

Πλαίσιο πολιτικής της ΕΕ

05 Το «οικοσύστημα» του κυβερνοχώρου της ΕΕ είναι περίπλοκο και πολυεπίπεδο και εκτείνεται σε μια σειρά τομέων εσωτερικής πολιτικής, όπως οι τομείς της δικαιοσύνης και των εσωτερικών υποθέσεων, της ψηφιακής ενιαίας αγοράς και των πολιτικών για την έρευνα[7]. Στον τομέα της εξωτερικής πολιτικής, η κυβερνοασφάλεια είναι ζήτημα που απασχολεί τη διπλωματία, και αποτελεί όλο και περισσότερο μέρος της αναδυόμενης πολιτικής της ΕΕ στον τομέα της άμυνας[8].

06 Τα τελευταία χρόνια, η ΕΕ έχει ενισχύσει το κανονιστικό της πλαίσιο σχετικά με την κυβερνοασφάλεια. Στο ***γράφημα 3*** παρακάτω παρατίθενται τα πλέον σημαντικά νομοθετικά κείμενα και μέσα πολιτικής σε επίπεδο ΕΕ. Σύμφωνα με την εμβέλεια του ελέγχου μας (βλέπε σημεία ***13***-***14***), επικεντρωθήκαμε σε μέσα που αφορούν τον εντοπισμό και την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας.

---

[7] Ενημερωτικό έγγραφο του ΕΕΣ σχετικά με τις προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια, σ. 12.

[8] Παραδείγματος χάριν, η στάση της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο (2022), το πλαίσιο για συντονισμένη αντίδραση της ΕΕ σε υβριδικές εκστρατείες (2022), η πολιτική της ΕΕ για την κυβερνοάμυνα (2023) και η αναθεωρημένη εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο (2023).

Γράφημα 3 | Σχετική νομοθεσία και μέσα πολιτικής της ΕΕ

Πηγή: ΕΕΣ.

Ρόλοι και αρμοδιότητες

07 Στον τομέα της κυβερνοασφάλειας της ΕΕ συμμετέχουν πολυάριθμες ιδιωτικές και δημόσιες οντότητες σε περιφερειακό, εθνικό και ενωσιακό επίπεδο, που δεν άπτονται του στρατιωτικού κλάδου, περιλαμβανομένων των οργάνων επιβολής του νόμου. Η κυβερνοασφάλεια αποτελεί επίσης βασική συνιστώσα της εθνικής ασφάλειας και άμυνας[9]. Στο ***παράρτημα II*** παρουσιάζουμε σχηματικά το τρέχον τοπίο της ΕΕ.

08 Τα κράτη μέλη φέρουν την πρωταρχική ευθύνη για την πρόληψη, την ετοιμότητα και την αντιμετώπιση περιστατικών και κρίσεων κυβερνοασφάλειας που τα επηρεάζουν. Σύμφωνα με το άρθρο 4, παράγραφος 2, της Συνθήκης για την Ευρωπαϊκή Ένωση, η εθνική ασφάλεια παραμένει στην αποκλειστική σφαίρα ευθύνης κάθε κράτους μέλους. Δεδομένου ότι τα περιστατικά κυβερνοασφάλειας μπορούν να διαταράξουν και να προκαλέσουν ζημίες σε υποδομές πληροφοριών ζωτικής σημασίας, στις οποίες βασίζεται η ομαλή λειτουργία της εσωτερικής αγοράς, ο ρόλος της ΕΕ είναι επίσης καθοριστικός σε περίπτωση σημαντικού περιστατικού ή κρίσης[10]. Οι βασικές οντότητες σε επίπεδο ΕΕ παρουσιάζονται στο ***γράφημα 4*** κατωτέρω.

[9] Γνώμη 02/2023 σχετικά με την προτεινόμενη πράξη για την αλληλεγγύη στον κυβερνοχώρο.

[10] Σχέδιο στρατηγικής της ΕΕ για τη διαχείριση κυβερνοκρίσεων.

Γράφημα 4 | Οντότητες σε επίπεδο ΕΕ με ρόλο-κλειδί στην κυβερνοασφάλεια

Πηγή: ΕΕΣ.

Ενωσιακή χρηματοδότηση

09 Στο πλαίσιο του τρέχοντος πολυετούς δημοσιονομικού πλαισίου 2021-2027, η κύρια πηγή χρηματοδότησης για την κυβερνοασφάλεια είναι το πρόγραμμα «Ψηφιακή Ευρώπη» (DIGITAL). Το πρόγραμμα αυτό, το οποίο δρομολογήθηκε το 2021, είναι το πρώτο πρόγραμμα της ΕΕ που αποσκοπεί ειδικά στην προώθηση του ψηφιακού μετασχηματισμού της ΕΕ και διαθέτει συνολικό προϋπολογισμό ύψους 8,1 δισεκατομμυρίων ευρώ[11].

10 Το πρόγραμμα DIGITAL χρηματοδοτεί δράσεις κυβερνοασφάλειας στο πλαίσιο του ειδικού στόχου 3 – «Κυβερνοασφάλεια και εμπιστοσύνη». Ειδικότερα, προβλέπεται προϋπολογισμός ύψους 1,4 δισεκατομμυρίων ευρώ προκειμένου:

- να ενισχυθεί ο συντονισμός της κυβερνοασφάλειας μεταξύ των εργαλείων και των υποδομών δεδομένων των κρατών μελών·
- να υποστηριχθεί η ευρεία ανάπτυξη λύσεων για την κυβερνοασφάλεια σε όλους τους τομείς της οικονομίας.

11 Το μεγαλύτερο μέρος της χρηματοδότησης του προγράμματος DIGITAL για την κυβερνοασφάλεια παρέχεται μέσω προσκλήσεων υποβολής προτάσεων. Μεταξύ Νοεμβρίου 2021 και Δεκεμβρίου 2025, προκηρύχθηκαν 12 προσκλήσεις και η διαθέσιμη στο πλαίσιό τους ενωσιακή χρηματοδότηση ανήλθε σε 825 εκατομμύρια ευρώ. Προγραμματίζονται νέες προσκλήσεις υποβολής προτάσεων για το 2026 και το 2027, για τη χορήγηση επιπλέον 212 εκατομμυρίων ευρώ σε επιχορηγήσεις.

12 Ένα ακόμη σημαντικό πρόγραμμα της ΕΕ για τη στήριξη της κυβερνοασφάλειας είναι το «Ορίζων Ευρώπη». Τα έργα κυβερνοασφάλειας χρηματοδοτούνται κυρίως στο πλαίσιο της ομάδας 3 «Πολιτική προστασία για την κοινωνία» και βρίσκονται συνήθως σε πρώιμο στάδιο ωριμότητας λόγω της εστίασης του προγράμματος «Ορίζων Ευρώπη» στην έρευνα και την καινοτομία. Ο μηχανισμός ανάκαμψης και ανθεκτικότητας παρέχει επίσης χρηματοδότηση για μέτρα κυβερνοασφάλειας.

[11] Πρόγραμμα «Ψηφιακή Ευρώπη».

Εμβέλεια και προσέγγιση του ελέγχου

13 Η αύξηση των κυβερνοαπειλών και ο δυνητικός αντίκτυπός τους ανέδειξαν την ανάγκη ενίσχυσης της συλλογικής μας κυβερνοανθεκτικότητας. Στόχος του ελέγχου μας ήταν να αξιολογηθεί αν οι δράσεις της ΕΕ διευκολύνουν αποτελεσματικά τον εντοπισμό και την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας. Συγκεκριμένα, ελέγξαμε αν αυτό ίσχυε στις εξής περιπτώσεις:

- δίκτυα και μηχανισμούς σε επίπεδο ΕΕ (συγκεκριμένα, το δίκτυο CSIRT, το EU-CyCLONe, το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια, το κέντρο κυβερνοκατάστασης και η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας)·
- δράσεις που χρηματοδοτούνται στο πλαίσιο του προγράμματος DIGITAL.

Δεν καλύψαμε τη συνεργασία στον τομέα της επιβολής του νόμου σε επίπεδο ΕΕ, ούτε τις δράσεις κυβερνοαποτροπής που αναλήφθηκαν σε επίπεδο ΕΕ μέσω διπλωματικών μέτρων ή αμυντικών δραστηριοτήτων.

14 Ο έλεγχος κάλυψε την περίοδο από το 2022 έως το 2025. Βασίζεται σε εξέταση και ανάλυση σχετικών εγγράφων, σε επισκέψεις ελέγχου σε τρία κράτη μέλη, την Ιρλανδία, την Ελλάδα και την Ιταλία, καθώς και σε γραπτά ερωτηματολόγια και συνεντεύξεις με συμφεροντούχους. Στο ***γράφημα 5*** παρουσιάζεται η προσέγγιση που ακολουθήσαμε προκειμένου να συγκεντρώσουμε τεκμήρια για τη θεμελίωση των παρατηρήσεών μας.

Γράφημα 5 | Ελεγκτικές εργασίες που πραγματοποιήσαμε

Εξετάσαμε

- Το **νομικό πλαίσιο** που εφαρμόζεται για τον εντοπισμό και την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας
- Τους **ρόλους και τις αρμοδιότητες** των δικτύων και των δομών που συγκροτούνται σε επίπεδο ΕΕ

Αναλύσαμε

- Έγγραφα σχετικά με τη λειτουργία του **δικτύου CSIRT** και του **EU-CyCLONe**
- Τεκμηρίωση σχετικά με το **πλαίσιο προγραμματισμού και παρακολούθησης των επιδόσεων του προγράμματος DIGITAL**
- Τεκμηρίωση σχετικά με **13 επιλεγμένες χρηματοδοτούμενες από την ΕΕ δράσεις** (11 επιχορηγήσεις και 2 συμβάσεις – βλέπε λεπτομερή κατάλογο στο παράρτημα III)

* Επιλέξαμε χρηματοδοτούμενες από την ΕΕ δράσεις σε τρεις χώρες (Ιρλανδία, Ελλάδα και Ιταλία) όπου η σχετική χρηματοδότηση στο πλαίσιο του προγράμματος DIGITAL ήταν υψηλότερη. Οι 11 επιχορηγήσεις επελέγησαν από κατάλογο 137 χρηματοδοτούμενων από την ΕΕ έργων που σχετίζονται με την ανίχνευση και την αντιμετώπιση απειλών, με σκοπό την κάλυψη ενός ευρέος φάσματος έργων.

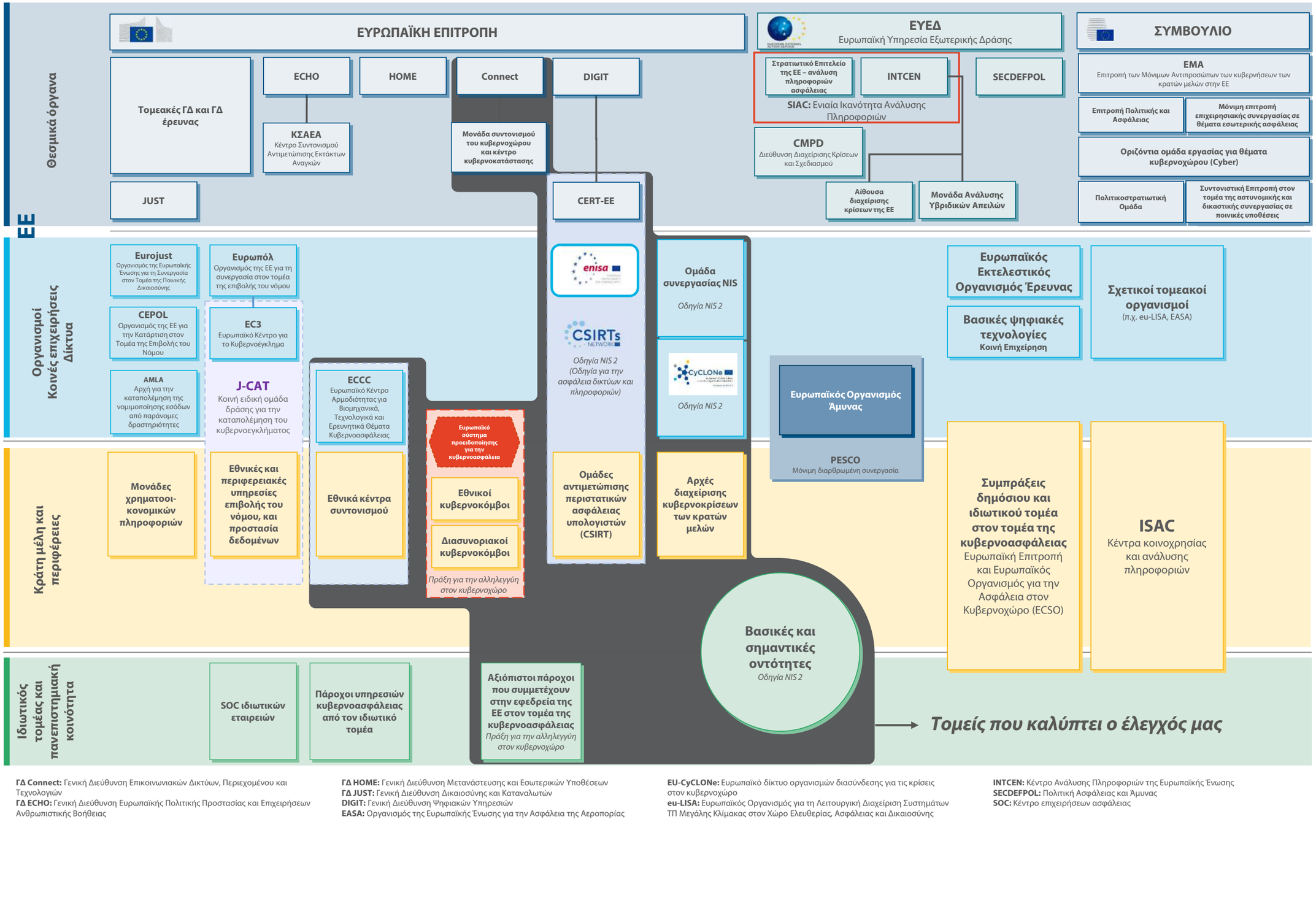
Συνομιλήσαμε με

- Δικαιούχους των **11 επιχορηγήσεων του δείγματος που χρηματοδοτήθηκαν από την ΕΕ**
- Εκπροσώπους των εθνικών αρχών κυβερνοασφάλειας σε **τρία κράτη μέλη** (Ιρλανδία, Ελλάδα και Ιταλία)
- Εκπροσώπους της Ευρωπαϊκής Επιτροπής (**ΓΔ Connect**), του **ENISA** και του **ECCC**

Πηγή: ΕΕΣ.

15 Προσδοκία μας είναι ότι με τα ευρήματά μας θα συμβάλουμε στη βελτίωση της αποτελεσματικότητας και της αποδοτικότητας σε σχέση με τον εντοπισμό και την αντιμετώπιση από την ΕΕ σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας, καθώς και στη βελτίωση του τρόπου επιλογής και παρακολούθησης των χρηματοδοτούμενων από την ΕΕ δράσεων. Η ελεγκτική μεθοδολογία που εφαρμόζουμε είναι σύμφωνη με τα διεθνή πρότυπα ελέγχου που εκδίδει ο Διεθνής Οργανισμός των Ανώτατων Οργάνων Ελέγχου (INTOSAI).

Παράρτημα II – Το τοπίο της κυβερνοασφάλειας της ΕΕ



ΓΔ Connect: Γενική Διεύθυνση Επικοινωνιακών Δικτύων, Περιεχομένου και Τεχνολογιών
ΓΔ ECHO: Γενική Διεύθυνση Ευρωπαϊκής Πολιτικής Προστασίας και Επιχειρήσεων Ανθρωπιστικής Βοήθειας

ΓΔ HOME: Γενική Διεύθυνση Μετανάστευσης και Εσωτερικών Υποθέσεων
ΓΔ JUST: Γενική Διεύθυνση Δικαιοσύνης και Καταναλωτών
DIGIT: Γενική Διεύθυνση Ψηφιακών Υπηρεσιών
EASA: Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια της Αεροπορίας

EU-CyCLONe: Ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για τις κρίσεις στον κυβερνοχώρο
eu-LISA: Ευρωπαϊκός Οργανισμός για τη Λειτουργική Διαχείριση Συστημάτων ΤΠ Μεγάλης Κλίμακας στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης

INTCEN: Κέντρο Ανάλυσης Πληροφοριών της Ευρωπαϊκής Ένωσης
SECDEFPOL: Πολιτική Ασφάλειας και Άμυνας
SOC: Κέντρο επιχειρήσεων ασφάλειας

Παράρτημα III – Επιλεγμένες δράσεις κυβερνοασφάλειας

Κωδικός	Τίτλος	Χώρες	Ημερομηνία έναρξης	Ημερομηνία λήξης	Συνολικό κόστος (σε εκατ. ευρώ) και συνεισφορά της ΕΕ (σε %)	Σύνδεσμος προς τη Δικτυακή πύλη χρηματοδότησης και προσκλήσεων υποβολής προσφορών της ΕΕ
Επιχορηγήσεις για διασυνοριακούς κυβερνοκόμβους που αποτελούν μέρος του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια						
1	**Δημιουργία διασυνοριακών SOC (ATHENA)**	Βουλγαρία, Ελλάδα, Κύπρος, Μάλτα	1.1.2024	31.3.2028	4,7 (50 %)	
2	**ENSOC-ΔΙΑΣΥΝΟΡΙΑΚΗ ΠΛΑΤΦΟΡΜΑ (ENSOC)**	Ισπανία, Ιταλία, Λουξεμβούργο, Κάτω Χώρες, Αυστρία, Πορτογαλία, Ρουμανία	1.1.2024	30.6.2028	10,4 (50 %)	
Επιχορηγήσεις για την ανάπτυξη του δικτύου εθνικών κέντρων συντονισμού (ΕΚΣ) στα κράτη μέλη						
3	**Ανάπτυξη και εφαρμογή του Εθνικού Κέντρου Συντονισμού και Ανάπτυξης της Κυβερνοασφάλειας για την Ιρλανδία (NCC-IE)**	Ιρλανδία	2.10.2023	1.10.2026	4,2 (47 %)	
4	**Ιταλικό Εθνικό Κέντρο Συντονισμού (NCC-IT)**	Ιταλία	1.11.2023	31.10.2025	2,0 (50 %)	

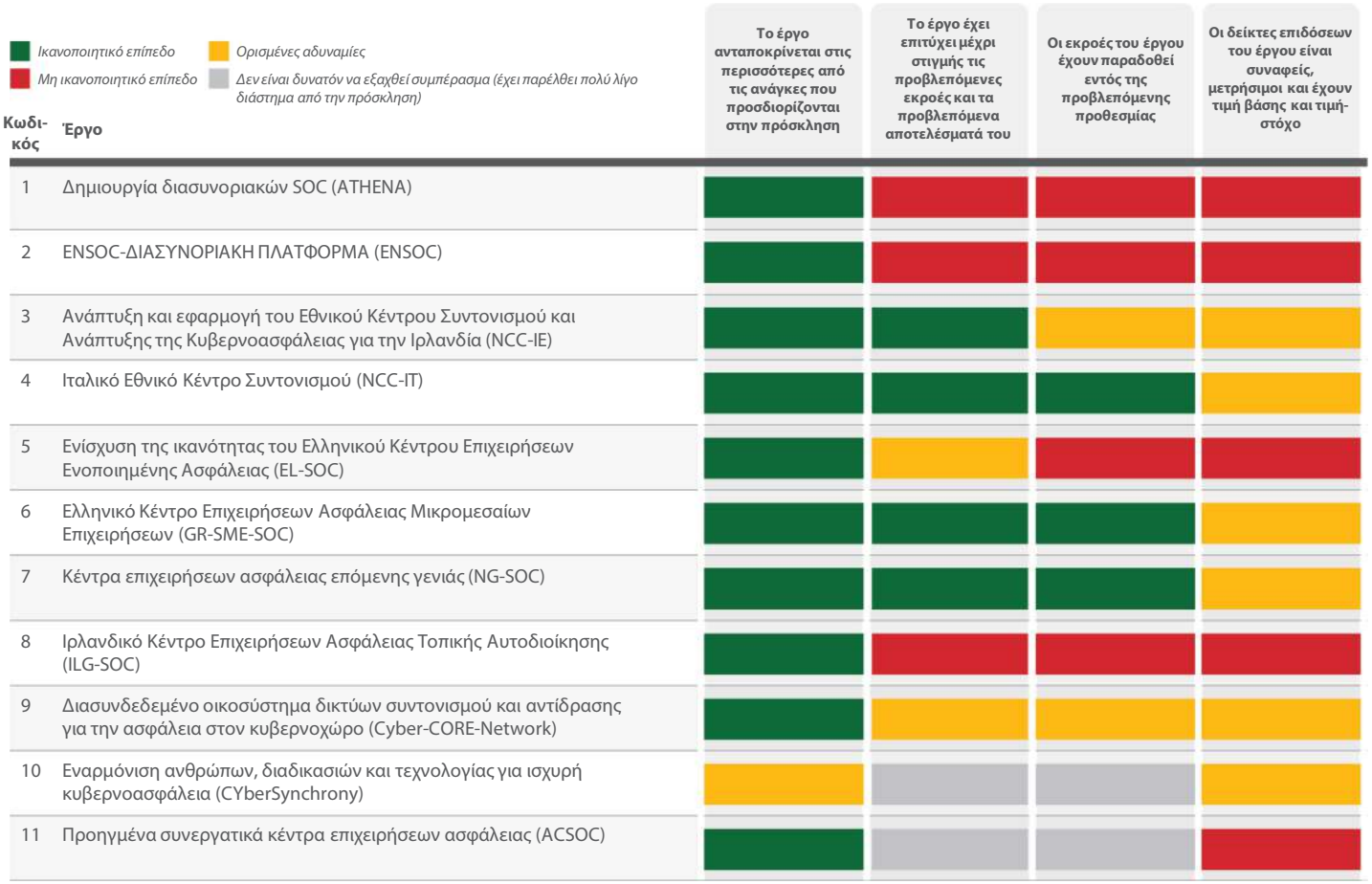
Κωδικός	Τίτλος	Χώρες	Ημερομηνία έναρξης	Ημερομηνία λήξης	Συνολικό κόστος (σε εκατ. ευρώ) και συνεισφορά της ΕΕ (σε %)	Σύνδεσμος προς τη Δικτυακή πύλη χρηματοδότησης και προσκλήσεων υποβολής προσφορών της ΕΕ
Επιχορηγήσεις για την ανάπτυξη των ικανοτήτων των κέντρων επιχειρήσεων ασφάλειας (SOC), την προώθηση καινοτόμων εφαρμογών ΤΝ και άλλων τεχνολογιών γενικής εφαρμογής για τα SOC και την παροχή στήριξης ετοιμότητας και αμοιβαίας συνδρομής						
5	**Ενίσχυση της ικανότητας του Ελληνικού Ενοποιημένου Κέντρου Επιχειρήσεων Ασφάλειας (EL-SOC)**	Ελλάδα, Κύπρος	1.1.2024	31.12.2026	9,7 (50 %)	
6	**Ελληνικό Κέντρο Επιχειρήσεων Ασφάλειας Μικρομεσαίων Επιχειρήσεων (GR-SME-SOC)**	Ελλάδα	1.1.2024	31.12.2026	12,1 (50 %)	
7	**Κέντρα επιχειρήσεων ασφάλειας επόμενης γενιάς (NG-SOC)**	Ελλάδα, Ισπανία, Κύπρος, Λουξεμβούργο, Σλοβενία, Νορβηγία	1.1.2024	31.12.2026	4,8 (50 %)	
8	**Ιρλανδικό Κέντρο Επιχειρήσεων Ασφάλειας Τοπικής Αυτοδιοίκησης (ILG-SOC)**	Ιρλανδία	1.10.2023	30.9.2026	8,3 (50 %)	
9	**Διασυνδεδεμένο οικοσύστημα δικτύων συντονισμού και αντίδρασης για την ασφάλεια στον κυβερνοχώρο (Cyber-CORE-Network)**	Ιρλανδία	1.1.2024	31.12.2026	3,6 (50 %)	
10	**Εναρμόνιση ανθρώπων, διαδικασιών και τεχνολογίας για ισχυρή κυβερνοασφάλεια (CYberSynchrony)**	Βέλγιο, Ελλάδα, Ιταλία, Κύπρος, Κάτω Χώρες	1.6.2024	31.5.2027	7,0 (100 %)	
11	**Προηγμένα συνεργατικά κέντρα επιχειρήσεων ασφάλειας (ACSOC)**	Ελλάδα, Ιταλία, Ρουμανία	1.1.2025	31.12.2027	3,0 (50 %)	

Κωδικός	Τίτλος	Χώρες	Ημερομηνία έναρξης	Ημερομηνία λήξης	Συνολικό κόστος (σε εκατ. ευρώ) και συνεισφορά της ΕΕ (σε %)	Σύνδεσμος προς τη Δικτυακή πύλη χρηματοδότησης και προσκλήσεων υποβολής προσφορών της ΕΕ
Σύμβαση-πλαίσιο για τη δράση για τη στήριξη της κυβερνοασφάλειας του ENISA						
12	**Στήριξη του ENISA για την παροχή υπηρεσιών στο πλαίσιο της δράσης για τη στήριξη της κυβερνοασφάλειας (28 παρτίδες)**	27 παρτίδες για κάθε κράτος μέλος 1 πανευρωπαϊκή παρτίδα	1.12.2022[1]	31.12.2025	28,3 (100 %)	
Σύμβαση παροχής υπηρεσιών για το κέντρο κυβερνοκατάστασης της ΓΔ Connect						
13	**Ειδική υπηρεσία για την υποστήριξη του κέντρου κυβερνοκατάστασης και κυβερνοανάλυσης για την Ευρωπαϊκή Επιτροπή**	-	30.12.2022	30.12.2026	18,0 (100 %)	

Πηγή: ΕΕΣ.

[1] Υπεγράφησαν πολλαπλές συμβάσεις καθ' όλη τη διάρκεια του Δεκεμβρίου 2022.

Παράρτημα IV – Αξιολόγηση από το ΕΕΣ των χρηματοδοτούμενων από την ΕΕ έργων κυβερνοασφάλειας



Συντομογραφίες

Συντομογραφία	Ορισμός/Επεξήγηση
CSIRT	Ομάδα αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές (Computer Security Incident Response Team)
DIGITAL	Πρόγραμμα «Ψηφιακή Ευρώπη»
ECCC	Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας
ENISA	Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια
EU-CyCLONe	Ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για τις κρίσεις στον κυβερνοχώρο
FSTP	Χρηματοδοτική στήριξη προς τρίτους (Financial support to third parties)
SAG	Στρατηγική συμβουλευτική ομάδα (Strategic Advisory Group)
SOC	Κέντρο επιχειρήσεων ασφάλειας (Security operations centre)
ΓΔ Connect	Γενική Διεύθυνση Επικοινωνιακών Δικτύων, Περιεχομένου και Τεχνολογιών
ΕΚΣ	Εθνικό κέντρο συντονισμού
ΜΜΕ	Μικρές και μεσαίες επιχειρήσεις

Γλωσσάριο

Όρος	Ορισμός/Επεξήγηση
Κέντρο επιχειρήσεων ασφάλειας	Οργανωτική μονάδα που είναι επιφορτισμένη με την πρόληψη των απειλών και των περιστατικών στον κυβερνοχώρο και συγκεντρώνει σχετικές πληροφορίες.
Κυβερνοαπειλή	Δυνητική χρήση του κυβερνοχώρου με σκοπό την υπονόμευση της διαθεσιμότητας, γνησιότητας, ακεραιότητας ή εμπιστευτικότητας δεδομένων ή πληροφοριακών συστημάτων.
Κυβερνοκόμβος	Κεντρική πλατφόρμα που συγκεντρώνει διάφορες υπηρεσίες, εργαλεία και επαγγελματίες ΤΠ για την ενίσχυση της παρακολούθησης, του εντοπισμού και της ανάλυσης κυβερνοαπειλών, την πρόληψη περιστατικών κυβερνοασφάλειας και την υποστήριξη της παραγωγής πληροφοριών σχετικά με κυβερνοαπειλές.
Λυτρισμικό	Κακόβουλο λογισμικό που εμποδίζει την πρόσβαση των θυμάτων σε σύστημα πληροφορικής ή κρυπτογραφεί αρχεία ώστε να τα κάνει μη αναγνώσιμα, αναγκάζοντας συνήθως το θύμα να καταβάλει λύτρα για την αποκατάσταση της πρόσβασης.
Παράγοντας απειλής	Άτομο ή ομάδα που εκ προθέσεως προκαλεί βλάβη, διαταράσσει υπηρεσίες ή κλέβει δεδομένα εκμεταλλευόμενο/-η τρωτά σημεία σε συστήματα, δίκτυα και συσκευές ΤΠ.
Περιστατικό κυβερνοασφάλειας	Γεγονός που υπονομεύει τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα ή την εμπιστευτικότητα δεδομένων ή πληροφοριακών συστημάτων.
Περιστατικό κυβερνοασφάλειας μεγάλης κλίμακας	Περιστατικό κυβερνοασφάλειας που είτε δεν μπορεί να αντιμετωπιστεί από μεμονωμένο κράτος μέλος λόγω του μεγέθους της διατάραξης που αυτό προκαλεί είτε έχει σημαντικές επιπτώσεις σε τουλάχιστον δύο κράτη μέλη.
Σημαντικό περιστατικό κυβερνοασφάλειας	Περιστατικό κυβερνοασφάλειας που έχει προκαλέσει ή ενδέχεται να προκαλέσει σοβαρές διαταραχές ή οικονομική ζημία σε έναν οργανισμό, ή σοβαρές ζημίες σε άλλες οντότητες ή μεμονωμένα άτομα.
Ταξινομία	Στο πλαίσιο της κυβερνοασφάλειας, ένα σύστημα ταξινόμησης που χρησιμοποιείται για την οργάνωση, την κατηγοριοποίηση και τη διάρθρωση των γνώσεων σχετικά με βασικές έννοιες, όπως απειλές και περιστατικά.

Απαντήσεις της Επιτροπής

https://www.eca.europa.eu/el/publications/SR-2026-19.

Απαντήσεις του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Θέματα Κυβερνοασφάλειας (ECCC)

https://www.eca.europa.eu/el/publications/SR-2026-19.

Απαντήσεις του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA)

https://www.eca.europa.eu/el/publications/SR-2026-19.

Χρονογραμμή

https://www.eca.europa.eu/el/publications/SR-2026-19.

Κλιμάκιο ελέγχου

Στις ειδικές εκθέσεις του ΕΕΣ παρουσιάζονται τα αποτελέσματα των ελέγχων που διενεργεί το κλιμάκιο επί πολιτικών και προγραμμάτων της ΕΕ ή επί διαχειριστικών θεμάτων που αφορούν συγκεκριμένους τομείς του προϋπολογισμού. Το ΕΕΣ επιλέγει και σχεδιάζει τα εν λόγω ελεγκτικά έργα κατά τρόπο ώστε αυτά να αποφέρουν τον μέγιστο αντίκτυπο, λαμβανομένων υπόψη των κινδύνων για τις επιδόσεις ή για τη συμμόρφωση, του επιπέδου των σχετικών εσόδων ή δαπανών, των επικείμενων εξελίξεων και του πολιτικού και δημόσιου συμφέροντος.

Ο εν προκειμένω έλεγχος επιδόσεων διενεργήθηκε από το Τμήμα Ελέγχου III (Εξωτερικές δράσεις, ασφάλεια και δικαιοσύνη), του οποίου προεδρεύει ο George-Marius Hyzler, Μέλος του ΕΕΣ. Επικεφαλής του ελέγχου ήταν ο George-Marius Hyzler, Μέλος του ΕΕΣ, συνεπικουρούμενος από τον Romuald Kayibanda, προϊστάμενο του ιδιαίτερου γραφείου του, και την Annette Farrugia, σύμβουλο στο ιδιαίτερο γραφείο του, τον Cyril Messein, διοικητικό στέλεχος, τον Frédéric Soblet, υπεύθυνο έργου, τον Jurgen Manjé, ελεγκτή και τη Flavia Di Marco, ελέγκτρια. Γλωσσική υποστήριξη παρείχε η Zoe Amador Martínez. Η Dunja Weibel παρείχε υποστήριξη στη δημιουργία των γραφικών.

Από αριστερά: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

ΔΙΚΑΙΩΜΑΤΑ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

HTML	ISBN 978-92-849-7857-1	ISSN 1977-5660	doi:10.2865/3537662	QJ-01-26-032-EL-Q
PDF	ISBN 978-92-849-7858-8	ISSN 1977-5660	doi:10.2865/1107406	QJ-01-26-032-EL-N

Παραπομπή στην παρούσα έκθεση να γίνεται ως εξής:

Ευρωπαϊκό Ελεγκτικό Συνέδριο, ειδική έκθεση 19/2026, με τίτλο «Εντοπισμός και αντιμετώπιση περιστατικών κυβερνοασφάλειας – Το πλαίσιο συνεργασίας της ΕΕ σημειώνει πρόοδο, είναι όμως εν μέρει μόνο αποτελεσματικό εξαιτίας καθυστερήσεων στην υλοποίηση και της περιορισμένης ανταλλαγής πληροφοριών», Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης, 2026.

Τα τελευταία χρόνια, η ΕΕ έχει ενισχύσει το κανονιστικό της πλαίσιο για την κυβερνοασφάλεια και έχει καθιερώσει δίκτυα και μηχανισμούς για την αντιμετώπιση περιστατικών κυβερνοασφάλειας. Επίσης, η ΕΕ χρηματοδοτεί έργα κυβερνοασφάλειας μέσω του προγράμματος «Ψηφιακή Ευρώπη».

Καταλήγουμε στο συμπέρασμα ότι οι δράσεις της ΕΕ διευκολύνουν μόνον εν μέρει τον εντοπισμό και την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας. Ενώ τίθεται βαθμηδόν σε εφαρμογή ένα πλαίσιο συνεργασίας, οι εργασίες συνεχίζονται καθώς δεν έχει ακόμη αναπτυχθεί πλήρως. Η περιορισμένη ανταλλαγή πληροφοριών, οι αδυναμίες στην αναφορά στοιχείων και οι αξιοσημείωτες καθυστερήσεις στην εφαρμογή παρεμποδίζουν την πλήρη αξιοποίηση των δυνατοτήτων των δικτύων και μηχανισμών της ΕΕ. Τα έργα επιδιώκουν σχετικούς στόχους, αλλά αρκετά αντιμετωπίζουν επιχειρησιακές προκλήσεις και καθυστερήσεις. Επιπλέον, υπάρχουν αδυναμίες στο συνολικό πλαίσιο παρακολούθησης των επιδόσεων. Διατυπώνουμε συστάσεις για την αντιμετώπιση αυτών των αδυναμιών.

Ειδική έκθεση του ΕΕΣ υποβαλλόμενη δυνάμει του άρθρου 287, παράγραφος 4, δεύτερο εδάφιο, ΣΛΕΕ.

ΕΥΡΩΠΑΪΚΟ ΕΛΕΓΚΤΙΚΟ ΣΥΝΕΔΡΙΟ

Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης

ΕΥΡΩΠΑΪΚΟ ΕΛΕΓΚΤΙΚΟ ΣΥΝΕΔΡΙΟ
12, rue Alcide De Gasperi
1615 Luxembourg
ΛΟΥΞΕΜΒΟΥΡΓΟ

Τηλ. +352 4398-1

Πληροφορίες: eca.europa.eu/el/contact
Ιστότοπος: eca.europa.eu
Μέσα κοινωνικής δικτύωσης: @EUauditors