



## Κυβερνοασφάλεια: ενίσχυση των ικανοτήτων της ΕΕ για αποτελεσματική επιχειρησιακή συνεργασία, αλληλεγγύη και ανθεκτικότητα

Strasbourg, 18 Απριλίου 2023

Η Επιτροπή εξέδωσε σήμερα πρόταση για την **πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο** με σκοπό την ενίσχυση των ικανοτήτων της ΕΕ στον τομέα της κυβερνοασφάλειας. Θα στηρίξει τον εντοπισμό απειλών και περιστατικών κυβερνοασφάλειας στην ΕΕ και την ευαισθητοποίηση σχετικά με αυτά, θα αυξήσει την ετοιμότητα των κρίσιμων οντοτήτων και θα ενισχύσει επίσης την αλληλεγγύη, τη συντονισμένη διαχείριση κρίσεων και τις ικανότητες αντίδρασης σε όλα τα κράτη μέλη. Η πράξη για την αλληλεγγύη στον κυβερνοχώρο καθορίζει τις ικανότητες που χρειάζεται η ΕΕ προκειμένου να καταστεί η Ευρώπη πιο ανθεκτική και να αντιδρά αποτελεσματικότερα στις κυβερνοαπειλές, ενισχύοντας παράλληλα τον υφιστάμενο μηχανισμό συνεργασίας. Η πράξη αυτή θα συμβάλει στη δημιουργία ενός ασφαλούς και προστατευμένου ψηφιακού περιβάλλοντος για τους πολίτες και τις επιχειρήσεις και στην προστασία κρίσιμων οντοτήτων και βασικών υπηρεσιών, όπως τα νοσοκομεία και οι υπηρεσίες κοινής ωφελείας.

Η Επιτροπή παρουσίασε επίσης μια **Ακαδημία Δεξιοτήτων για την Κυβερνοασφάλεια** στο πλαίσιο του [Ευρωπαϊκού Έτους Δεξιοτήτων 2023](#), προκειμένου να εξασφαλίσει μια πιο συντονισμένη προσέγγιση για την κάλυψη της έλλειψης ταλέντων στον τομέα της κυβερνοασφάλειας, πράγμα που αποτελεί προϋπόθεση για την ενίσχυση της ανθεκτικότητας της Ευρώπης. Η Ακαδημία αυτή θα φέρει υπό τη σκέπη της διάφορες υφιστάμενες πρωτοβουλίες που αποσκοπούν στην προώθηση των δεξιοτήτων κυβερνοασφάλειας και θα τις καταστήσει διαθέσιμες σε διαδικτυακή πλατφόρμα, καθιστώντας τις έτσι περισσότερο ορατές και αυξάνοντας τον αριθμό των ειδικευμένων επαγγελματιών στον τομέα της κυβερνοασφάλειας στην ΕΕ.

Στο πλαίσιο της [Ευρωπαϊκής Ένωσης Ασφάλειας](#), η ΕΕ έχει δεσμευτεί ότι θα διασφαλίσει επαρκή προστασία για τους πολίτες και τις επιχειρήσεις της Ευρώπης, τόσο εντός όσο και εκτός διαδικτύου, και ότι θα προωθήσει έναν ανοικτό, ασφαλή και σταθερό κυβερνοχώρο. Ωστόσο, το αυξανόμενο μέγεθος, η συχνότητα και ο αντίκτυπος των περιστατικών κυβερνοασφάλειας συνιστούν μείζονα απειλή τόσο για τη λειτουργία των συστημάτων δικτύου και πληροφοριών όσο και για την ευρωπαϊκή ενιαία αγορά. Η στρατιωτική επίθεση της Ρωσίας κατά της Ουκρανίας έχει επιδεινώσει περαιτέρω την απειλή αυτή, σε συνδυασμό με την πληθώρα υποστηριζόμενων από κράτη εγκληματικών παραγόντων και ακτιβιστών χάκερ που εμπλέκονται στις τρέχουσες γεωπολιτικές εντάσεις.

Με βάση ένα [ισχυρό στρατηγικό, πολιτικό και νομοθετικό πλαίσιο](#) που έχει ήδη θεσπιστεί, η προτεινόμενη πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο και η Ακαδημία Δεξιοτήτων για την Κυβερνοασφάλεια θα συμβάλουν περαιτέρω στην ενίσχυση του εντοπισμού κυβερνοαπειλών, της ανθεκτικότητας και της ετοιμότητας σε όλα τα επίπεδα του οικοσυστήματος κυβερνοασφάλειας της ΕΕ.

### Πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο

Η πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο θα ενισχύσει την αλληλεγγύη σε επίπεδο Ένωσης με σκοπό τη βελτίωση του **εντοπισμού**, της **ετοιμότητας** και της **αντιμετώπισης** σημαντικών ή μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας, με τη δημιουργία μιας ευρωπαϊκής ασπίδας κυβερνοασφάλειας και ενός ευρέως μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο.

Για τον ταχύ και αποτελεσματικό εντοπισμό σημαντικών κυβερνοαπειλών, η Επιτροπή προτείνει τη δημιουργία μιας **ευρωπαϊκής κυβερνοασπίδας η οποία είναι μια πανευρωπαϊκή υποδομή που συνίσταται σε εθνικά και διασυνοριακά κέντρα επιχειρήσεων ασφάλειας (Security Operations Centres, SOC) σε ολόκληρη την ΕΕ**. Πρόκειται για οντότητες επιφορτισμένες με τον εντοπισμό και την ανάληψη δράσης για την αντιμετώπιση απειλών στον κυβερνοχώρο. Θα χρησιμοποιούν τεχνολογίες αιχμής, όπως η τεχνητή νοημοσύνη (TN) και η προηγμένη ανάλυση δεδομένων, για τον εντοπισμό και την έγκαιρη αποστολή προειδοποιήσεων σχετικά με κυβερνοαπειλές και περιστατικά σε διασυνοριακό επίπεδο. Με τη σειρά τους, οι αρχές και οι σχετικές οντότητες θα είναι σε θέση να αντιδρούν αποτελεσματικότερα και αποδοτικότερα σε μείζονα περιστατικά.

Τα κέντρα αυτά θα μπορούσαν να τεθούν σε λειτουργία έως τις αρχές του 2024. Κατά την προπαρασκευαστική φάση της ευρωπαϊκής κυβερνοασπίδας, τον Απρίλιο του 2023 η Επιτροπή επέλεξε,

στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη», [τρεις κοινοπραξίες διασυνοριακών κέντρων επιχειρήσεων ασφάλειας \(SOC\)](#), στις οποίες συμμετείχαν δημόσιοι φορείς από 17 κράτη μέλη και την Ισλανδία.

Η πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο προβλέπει επίσης τη δημιουργία ενός **μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο** για την αύξηση της ετοιμότητας και την ενίσχυση των ικανοτήτων αντιμετώπισης περιστατικών στην ΕΕ. Θα στηρίζει τα ακόλουθα:

- **Δράσεις ετοιμότητας**, συμπεριλαμβανομένων δοκιμασιών οντοτήτων σε τομείς εξαιρετικά κρίσιμης σημασίας (υγειονομική περίθαλψη, μεταφορές, ενέργεια κ.λπ.) για τον εντοπισμό πιθανών τρωτών σημείων, βάσει κοινών σεναρίων κινδύνου και κοινών μεθοδολογιών.
- **Δημιουργία μιας νέας εφεδρείας της ΕΕ για την κυβερνοασφάλεια** αποτελούμενης από υπηρεσίες αντιμετώπισης περιστατικών που θα προσφέρουν αξιόπιστοι πάροχοι, με τους οποίους θα υπογράφονται συμβάσεις εκ των προτέρων και θα είναι επομένως έτοιμοι να επέμβουν, κατόπιν αιτήματος κράτους μέλους ή θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, σε περίπτωση σημαντικού ή μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας.
- **Παροχή χρηματοδοτικής στήριξης για αμοιβαία συνδρομή**, σε περιπτώσεις κατά τις οποίες ένα κράτος μέλος θα μπορούσε να προσφέρει στήριξη σε άλλο κράτος μέλος.

Επιπλέον, ο προτεινόμενος κανονισμός θεσπίζει τον **μηχανισμό επανεξέτασης περιστατικών κυβερνοασφάλειας** με σκοπό να ενισχυθεί η ανθεκτικότητα της Ένωσης μέσω της επανεξέτασης και της αξιολόγησης σημαντικών ή μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας μετά την εκδήλωσή τους, της άντλησης διδαγμάτων και, κατά περίπτωση, της έκδοσης συστάσεων για τη βελτίωση της κατάστασης στην ΕΕ όσον αφορά την κυβερνοασφάλεια.

Ο συνολικός προϋπολογισμός για όλες τις δράσεις που καλύπτει η πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο ανέρχεται σε **1,1 δισ. ευρώ, εκ των οποίων τα 2/3 περίπου** θα χρηματοδοτηθούν από την ΕΕ μέσω του προγράμματος «Ψηφιακή Ευρώπη».

## **Ακαδημία Δεξιοτήτων της ΕΕ για την Κυβερνοασφάλεια**

Η **Ακαδημία Δεξιοτήτων της ΕΕ για την Κυβερνοασφάλεια** θα φέρει υπό τη σκέπη της ιδιωτικές και δημόσιες πρωτοβουλίες που αποσκοπούν στην ενίσχυση των δεξιοτήτων κυβερνοασφάλειας σε ευρωπαϊκό και εθνικό επίπεδο, καθιστώντας τις περισσότερο ορατές και συμβάλλοντας στην κάλυψη της έλλειψης ταλέντων των επαγγελματιών στον τομέα της κυβερνοασφάλειας.

Η Ακαδημία θα φιλοξενηθεί αρχικά διαδικτυακά στην [πλατφόρμα της Επιτροπής για τις ψηφιακές δεξιότητες και θέσεις εργασίας](#). Οι πολίτες που ενδιαφέρονται να ακολουθήσουν σταδιοδρομία στον τομέα της κυβερνοασφάλειας θα είναι σε θέση να βρίσκουν ευκαιρίες κατάρτισης και πιστοποίησης από ολόκληρη την ΕΕ σε έναν ενιαίο ιστότοπο. Οι ενδιαφερόμενοι φορείς θα έχουν επίσης τη δυνατότητα να αναλαμβάνουν δεσμεύσεις για τη στήριξη της βελτίωσης των δεξιοτήτων κυβερνοασφάλειας στην ΕΕ δρομολογώντας ειδικές δράσεις, όπως η παροχή κατάρτισης και πιστοποιήσεων στον τομέα της κυβερνοασφάλειας.

Η Ακαδημία θα εξελιχθεί ώστε να περιλαμβάνει έναν κοινό χώρο για την πανεπιστημιακή κοινότητα, τους παρόχους κατάρτισης και τον κλάδο, βοηθώντας τους να συντονίζουν εκπαιδευτικά προγράμματα, προγράμματα κατάρτισης και χρηματοδότηση και να παρακολουθούν την εξέλιξη της αγοράς εργασίας στον τομέα της κυβερνοασφάλειας.

## **Συστήματα πιστοποίησης για διαχειριζόμενες υπηρεσίες ασφάλειας**

Η Επιτροπή πρότεινε επίσης σήμερα **στοχευμένη τροποποίηση της πράξης για την κυβερνοασφάλεια**, με σκοπό να καταστεί δυνατή στο μέλλον η έγκριση ευρωπαϊκών συστημάτων πιστοποίησης για τις «διαχειριζόμενες υπηρεσίες ασφάλειας». Πρόκειται για εξαιρετικά κρίσιμες και ευαίσθητες υπηρεσίες που προσφέρονται από παρόχους υπηρεσιών κυβερνοασφάλειας, όπως η αντιμετώπιση περιστατικών, οι δοκιμές διείσδυσης, οι έλεγχοι ασφάλειας και η παροχή συμβουλών, με σκοπό την παροχή βοήθειας σε εταιρείες και άλλους οργανισμούς για την πρόληψη, τον εντοπισμό και την αντιμετώπιση κυβερνοπεριστατικών ή την ανάκαμψη από τις επιπτώσεις τους.

Η πιστοποίηση είναι καίριας σημασίας και μπορεί να διαδραματίσει σημαντικό ρόλο στο πλαίσιο της εφεδρείας της ΕΕ για την κυβερνοασφάλεια και της [οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση](#) (οδηγία NIS 2), διευκολύνοντας επίσης τη διασυνοριακή παροχή των εν λόγω υπηρεσιών.

## **Επόμενα βήματα**

Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο θα εξετάσουν τώρα τον **προτεινόμενο κανονισμό σχετικά με την πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο**, καθώς και τη **στοχευμένη τροποποίηση της πράξης για την κυβερνοασφάλεια**.

Το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Θέματα Κυβερνοασφάλειας θα οργανώνει την κοινή προμήθεια εργαλείων και υποδομών με τα επιλεγμένα **διασυνοριακά κέντρα επιχειρήσεων ασφάλειας** για την ανάπτυξη ικανοτήτων κυβερνοανίχνευσης.

Ο Οργανισμός της ΕΕ για την Κυβερνοασφάλεια (ENISA) και το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Θέματα Κυβερνοασφάλειας θα συνεχίσουν να εργάζονται για τις δεξιότητες στον τομέα της κυβερνοασφάλειας, συμβάλλοντας στην υλοποίηση της **Ακαδημίας Δεξιοτήτων για την Κυβερνοασφάλεια**, σύμφωνα με τις αντίστοιχες εντολές τους και σε στενή συνεργασία με την Επιτροπή και τα κράτη μέλη.

Η Επιτροπή προτείνει να λάβει η Ακαδημία τη μορφή μιας κοινοπραξίας ευρωπαϊκής ψηφιακής υποδομής (European digital infrastructure consortium, EDIC), ενός νέου νομικού πλαισίου για την υλοποίηση πολυκρατικών έργων. Η δυνατότητα αυτή θα συζητηθεί τώρα με τα κράτη μέλη.

Επιπλέον, πρέπει να διασφαλίζεται η απαραίτητη υψηλής ποιότητας κατάρτιση των επαγγελματιών του κλάδου. Στο πλαίσιο αυτό, ο ENISA θα αναπτύξει ένα πιλοτικό έργο με το οποίο θα διερευνηθεί η δημιουργία ενός ευρωπαϊκού συστήματος πιστοποίησης δεξιοτήτων κυβερνοασφάλειας.

## Ιστορικό

Με την προτεινόμενη πράξη της ΕΕ για την κυβερνοασφάλεια, η Επιτροπή ανταποκρίνεται στην [έκκληση των κρατών μελών](#) για ενίσχυση της κυβερνοανθεκτικότητας της ΕΕ και υλοποιεί τη δέσμευσή της που εκφράζεται στην πρόσφατη [κοινή ανακοίνωση για την άμυνα στον κυβερνοχώρο](#) για την προετοιμασία μιας πρωτοβουλίας της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο.

Η πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο και η Ακαδημία Δεξιοτήτων για την Κυβερνοασφάλεια βασίζονται στη [στρατηγική της ΕΕ για την κυβερνοασφάλεια](#), καθώς και στο νομοθετικό πλαίσιο της ΕΕ για την ενίσχυση της συλλογικής ανθεκτικότητας της ΕΕ έναντι των αυξανόμενων απειλών για την κυβερνοασφάλεια. Αυτό περιλαμβάνει την [οδηγία σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση](#) (NIS 2) και την [πράξη για την κυβερνοασφάλεια](#).

## Για περισσότερες πληροφορίες

[Ερωτήσεις και Απαντήσεις](#) – Κυβερνοασφάλεια: ενίσχυση των ικανοτήτων της ΕΕ για αποτελεσματική επιχειρησιακή συνεργασία, αλληλεγγύη και ανθεκτικότητα

[Ενημερωτικό δελτίο](#) – Πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο

[Ενημερωτικό δελτίο](#) – Ακαδημία Δεξιοτήτων για την Κυβερνοασφάλεια

[Πρόταση κανονισμού](#) σχετικά με την πράξη για την αλληλεγγύη στον κυβερνοχώρο

[Ανακοίνωση της Επιτροπής](#) σχετικά με την Ακαδημία Δεξιοτήτων για την Κυβερνοασφάλεια

[Πρόταση κανονισμού](#) σχετικά με την τροποποίηση για τις «διαχειριζόμενες υπηρεσίες ασφάλειας»

[Ενημερωτικό δελτίο](#) – η στρατηγική της ΕΕ για την κυβερνοασφάλεια

[Θεματική σελίδα](#) σχετικά με την πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο

[Ακαδημία Δεξιοτήτων της ΕΕ για την Κυβερνοασφάλεια – Πλατφόρμα ψηφιακών δεξιοτήτων και θέσεων εργασίας](#)

IP/23/2243

Quotes:

Με τη δέσμη μέτρων για την κυβερνοασφάλεια που παρουσιάσαμε σήμερα, δείχνουμε πώς, ενεργώντας με πνεύμα αλληλεγγύης, μπορούμε να οικοδομήσουμε τις υποδομές, τις δεξιότητες και τις ικανότητες που χρειαζόμαστε για να αντιμετωπίσουμε την εντεινόμενη κοινή απειλή για την κυβερνοασφάλειά μας.  
κ. Μαργκρέτε Βέστεϊγιερ, εκτελεστική αντιπρόεδρος για μια Ευρώπη Έτοιμη για την Ψηφιακή Εποχή - 18/04/2023

Η πράξη της ΕΕ για την αλληλεγγύη στον κυβερνοχώρο και η Ακαδημία Δεξιοτήτων για την Κυβερνοασφάλεια είναι τα δύο νέα συγκεκριμένα μέσα που διαθέτουμε για την αντιμετώπιση των επιχειρησιακών αναγκών της ΕΕ στον τομέα της κυβερνοασφάλειας: η πράξη προτείνει συγκεκριμένα μέτρα που θα δώσουν στην ΕΕ τη δυνατότητα να αντιδρά σε απειλές και επιθέσεις, ενώ η Ακαδημία αποσκοπεί στην ενίσχυση της βάσης δεξιοτήτων μας, ώστε να διαθέτουμε τα στελέχη που χρειαζόμαστε για τον σκοπό αυτό.  
κ. Μαργαρίτης Σχοινάς, αντιπρόεδρος για την Προώθηση του Ευρωπαϊκού Τρόπου Ζωής μας - 18/04/2023

Υποβάλαμε σήμερα την πρόταση για μια ευρωπαϊκή κυβερνοασπίδα. Για τον αποτελεσματικό εντοπισμό, την αντιμετώπιση και την ανάκαμψη από απειλές κυβερνοασφάλειας μεγάλης κλίμακας, υπάρχει επιτακτική ανάγκη να πραγματοποιήσουμε επείγοντως σημαντικές επενδύσεις στις ικανότητες κυβερνοασφάλειας. Η πράξη για την αλληλεγγύη στον κυβερνοχώρο αποτελεί κρίσιμο ορόσημο στην πορεία μας προς την επίτευξη του στόχου αυτού.  
κ. Τιερί Μπρετόν, επίτροπος Εσωτερικής Αγοράς - 18/04/2023

Αρμόδιοι επικοινωνίας:

[Johannes BÄHRKE](#) (+32 2 295 86 15)

[Marietta GRAMMENOU](#) (+32 2 298 35 83)

Ερωτήσεις του κοινού: [Europe Direct](#) τηλεφωνικά [00 800 67 89 10 11](#) ή με [ηλεκτρονικό μήνυμα](#)

Related media

 [Cybersecurity](#)