Ευρωπαϊκή Επιτροπή

Η ΚΑΤΑΣΤΑΣΗ ΤΗΣ ΕΝΩΣΗΣ

2018

Οικοδόμηση ισχυρής κυβερνοασφάλειας στην Ευρώπη

#SOTEU

12 Σεπτεμβρίου 2018

«Οι κυβερνοεπιθέσεις δεν γνωρίζουν σύνορα, αλλά η ικανότητα απόκρισής μας διαφέρει πολύ από τη μια χώρα στην άλλη, γεγονός που δημιουργεί κενά όπου τα τρωτά σημεία προσελκύουν όλο και περισσότερο τις επιθέσεις. Η ΕΕ χρειάζεται πιο ισχυρές και πιο αποτελεσματικές δομές για να αποκτήσει αυξημένη ανθεκτικότητα έναντι των κυβερνοεπιθέσεων και να τις αντιμετωπίζει. Δεν θέλουμε να είμαστε από τους πλέον αδύναμους κρίκους στην καταπολέμηση αυτής της παγκόσμιας απειλής.»

Ζαν-Κλοντ Γιούνκερ, Ψηφιακή σύνοδος κορυφής του Τάλιν, 29 Σεπτεμβρίου 2017

Το 2017 η Ευρωπαϊκή Επιτροπή και η Ύπατη Εκπρόσωπος πρότειναν μια ευρεία δέσμη μέτρων για την οικοδόμηση ισχυρής κυβερνοασφάλειας στην ΕΕ, ούτως ώστε να εξοπλίσουν την Ευρώπη με τα κατάλληλα εργαλεία για την αντιμετώπιση των διαρκώς μεταβαλλόμενων κυβερνοαπειλών. Οι προσπάθειες αυτές συμπληρώνονται πλέον από πρόταση η οποία βοηθά την ΕΕ να συγκεντρώσει πόρους και εμπειρογνωσία στους τομείς της έρευνας και της καινοτομίας και να αναλάβει ηγετικό ρόλο στην κυβερνοασφάλεια και τις ψηφιακές τεχνολογίες επόμενης γενιάς.

Οι σημερινές κυβερνοαπειλές

+4 000 επιθέσεις με λυτρισμικό (ransomware) καθημερινά το 2016

Το **80 % των ευρωπαϊκών επιχειρήσεων** βίωσε τουλάχιστον ένα περιστατικό κυβερνοασφάλειας κατά τη διάρκεια του τελευταίου έτους.

Τα **περιστατικά ασφάλειας** στο σύνολο των τομέων της οικονομίας **αυξήθηκαν κατά 38 %** —η μεγαλύτερη αύξηση των τελευταίων 12 ετών.

Σε ορισμένα κράτη μέλη, το **50 % όλων των διαπραττόμενων εγκλημάτων** είναι κυβερνοεγκλήματα.

+ 150 χώρες και + 230 000 συστήματα σε ευρύ φάσμα τομέων σε διάφορες χώρες επηρεάστηκαν από την επίθεση «Wannycry» τον Μάιο του 2017, με αποτέλεσμα να υπάρξουν σημαντικές επιπτώσεις σε βασικές υπηρεσίες που συνδέονται με το διαδίκτυο, συμπεριλαμβανομένων των υπηρεσιών νοσοκομειακής περίθαλψης και μεταφοράς με ασθενοφόρα.

Ενίσχυση της ανθεκτικότητας έναντι των κυβερνοεπιθέσεων

Η Επιτροπή υποστηρίζει ήδη την ενίσχυση της ικανότητας της ΕΕ να αποτρέπει τις κυβερνοαπειλές, καθώς και την αύξηση της ανθεκτικότητας και τη βελτίωση της απόκρισής της έναντι αυτών, μεταξύ άλλων μέσω των εξής:

Παροχή στήριξης για την αποτελεσματική εφαρμογή της πρώτης νομοθεσίας της ΕΕ για την κυβερνοασφάλεια (οδηγία για την ασφάλεια συστημάτων δικτύου και πληροφοριών), με τους παρακάτω τρόπους:

ΕΝΙΣΧΥΣΗ ΤΩΝ ΙΚΑΝΟΤΗΤΩΝ

Τα κράτη μέλη πρέπει να βελτιώσουν τις ικανότητές τους στον τομέα της κυβερνοασφάλειας.

ΣΥΝΕΡΓΑΣΙΑ

Αύξηση της συνεργασίας σε επίπεδο ΕΕ

ΠΡΟΛΗΨΗ ΚΙΝΔΥΝΩΝ

Οι παράγοντες σε τομείς καίριας σημασίας (όπως η ενέργεια, οι μεταφορές και η υγεία) είναι υποχρεωμένοι να θέσουν σε εφαρμογή μέτρα για την πρόληψη των κινδύνων και την αντιμετώπιση κυβερνοπεριστατικών.

Συνεργασία με τα κράτη μέλη στα εξής:

ΟΡΓΑΝΙΣΜΟΣ ΤΗΣ ΕΕ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Ενίσχυση του Οργανισμού της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο ώστε να προσφέρει καλύτερη στήριξη στα κράτη μέλη

ΠΛΑΙΣΙΟ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΗΣ ΕΕ

Ένα πλαίσιο πιστοποίησης σε επίπεδο ΕΕ για να διασφαλίζεται ότι τα προϊόντα και οι υπηρεσίες είναι ασφαλή στον κυβερνοχώρο.

ΣΥΝΤΟΝΙΣΜΕΝΗ ΑΝΤΙΜΕΤΩΠΙΣΗ

Εξασφάλιση ταχείας και συντονισμένης αντίδρασης σε κυβερνοεπιθέσεις μεγάλης κλίμακας

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) βοηθά τις αρχές των κρατών μελών που είναι αρμόδιες για την κυβερνοασφάλεια ώστε να προστατεύουν καλύτερα την ΕΕ από κυβερνοεπιθέσεις.

Συγκέντρωση πόρων και εμπειρογνωσίας στον τομέα της τεχνολογίας για την κυβερνοασφάλεια

Πέραν των ήδη υφιστάμενων πρωτοβουλιών της ΕΕ στον τομέα της κυβερνοασφάλειας, σήμερα η Επιτροπή προτείνει να συμπληρωθούν οι προσπάθειες αυτές με τη δημιουργία ενός δικτύου κέντρων ικανοτήτων και ενός ευρωπαϊκού κέντρου βιομηχανικών, τεχνολογικών και ερευνητικών ικανοτήτων στον τομέα της κυβερνοασφάλειας τα οποία θα αναπτύξουν και θα καθιερώσουν τα εργαλεία και τις τεχνολογίες που χρειαζόμαστε για να μπορούμε να ανταποκρινόμαστε σε μια διαρκώς μεταβαλλόμενη απειλή.

Το ευρωπαϊκό κέντρο, σε συνεργασία με τα κράτη μέλη, θα συντονίζει με τον πλέον στοχευμένο τρόπο τα κονδύλια που προβλέπονται για την κυβερνοασφάλεια στον επόμενο μακροπρόθεσμο προϋπολογισμό της ΕΕ. Αυτό θα συμβάλει στη δημιουργία νέων ευρωπαϊκών ικανοτήτων στον κυβερνοχώρο.

Διαθέτουμε ήδη πλούσια εμπειρογνωσία στην Ευρώπη —σε ολόκληρη την ΕΕ βρίσκονται πάνω από **660 κέντρα ικανοτήτων στον τομέα της κυβερνοασφάλειας**. Η Επιτροπή, για να αξιοποιήσει και να χρησιμοποιήσει αποτελεσματικά την εμπειρογνωσία των κέντρων αυτών, προτείνει έναν μηχανισμό με τους εξής στόχους:

Συγκέντρωση και ανταλλαγή της υπάρχουσας εμπειρογνωσίας, καθώς και διασφάλιση της πρόσβασης σ' αυτήν

Παροχή συνδρομής για την ανάπτυξη ενωσιακών προϊόντων και λύσεων στον τομέα της κυβερνοασφάλειας

Διασφάλιση της μακροπρόθεσμης στρατηγικής συνεργασίας μεταξύ κλάδων, ερευνητικών κοινοτήτων και κυβερνήσεων

Πραγματοποίηση από κοινού επενδύσεων και κοινή χρήση δαπανηρών υποδομών

Ευρωπαϊκό κέντρο ικανοτήτων:

Θα συντονίζει την αξιοποίηση των κονδυλίων που προβλέπονται για την κυβερνοασφάλεια στον επόμενο μακροπρόθεσμο προϋπολογισμό της ΕΕ για την περίοδο 2021-2027 στο πλαίσιο των προγραμμάτων «Ψηφιακή Ευρώπη» και «Ορίζων Ευρώπη». Το κέντρο θα παρέχει στήριξη στο δίκτυο και την κοινότητα με στόχο την προώθηση της έρευνας και της καινοτομίας στον τομέα της **κυβερνοασφάλειας**. Επιπλέον, θα οργανώνει **από κοινού επενδύσεις** από την ΕΕ, τα κράτη μέλη και τον σχετικό κλάδο. Για παράδειγμα, στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη», θα επενδυθεί ποσό ύψους **2 δισ. ευρώ** για την προάσπιση της ψηφιακής οικονομίας, της κοινωνίας και των δημοκρατιών της ΕΕ μέσω της ενίσχυσης του ενωσιακού κλάδου της κυβερνοασφάλειας και της χρηματοδότησης εξοπλισμού και υποδομών κυβερνοασφάλειας προηγμένης τεχνολογίας.

Δίκτυο εθνικών κέντρων συντονισμού:

Κάθε κράτος μέλος θα ορίσει ως επικεφαλής του δικτύου ένα εθνικό κέντρο συντονισμού, το οποίο θα ασχολείται ενεργά με την ανάπτυξη νέων ικανοτήτων και ευρύτερων δεξιοτήτων στον τομέα της κυβερνοασφάλειας. Το δίκτυο θα συμβάλλει στον εντοπισμό και τη στήριξη των πλέον συναφών έργων σε σχέση με την κυβερνοασφάλεια στα κράτη μέλη.

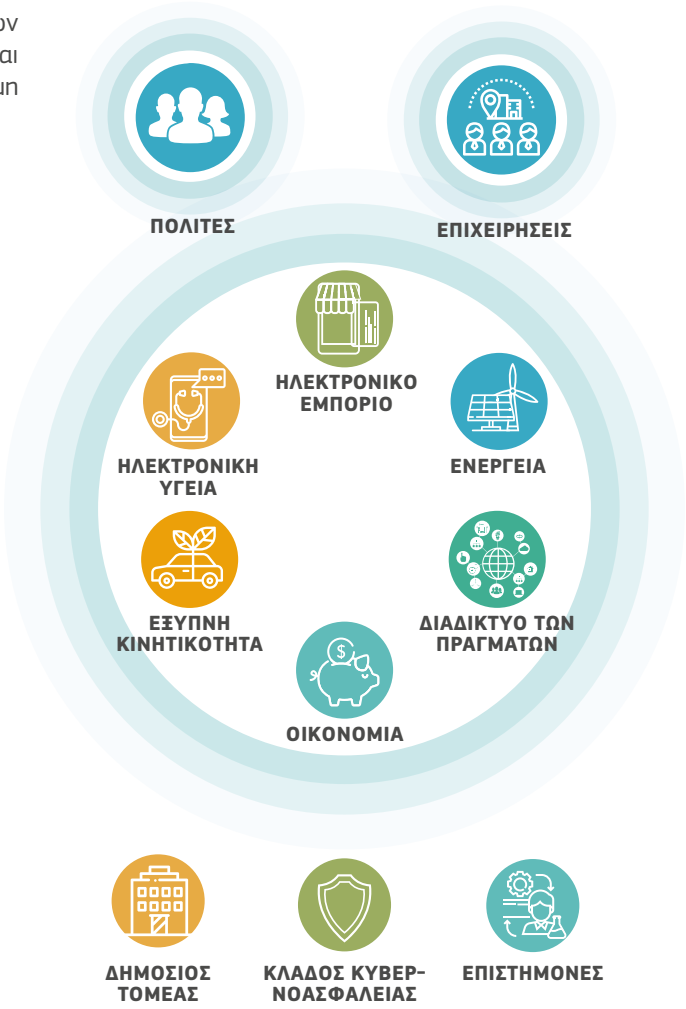
Κοινότητα ικανοτήτων:

Μια μεγάλη, ανοικτή και πολυσχιδής ομάδα ενδιαφερόμενων μερών στον τομέα της κυβερνοασφάλειας από τον κλάδο της έρευνας και τον ιδιωτικό και τον δημόσιο τομέα, συμπεριλαμβανομένων τόσο μη στρατιωτικών όσο και αμυντικών αρχών·

Τι θα βελτιωθεί;

- καλύτερος συντονισμός των εργασιών·
- πρόσβαση σε εμπειρογνωσία·
- πρόσβαση σε εγκαταστάσεις δοκιμών και πειραματισμού·
- αξιολόγηση των προϊόντων όσον αφορά την κυβερνοασφάλεια·
- πρόσβαση σε καινοτόμα προϊόντα και λύσεις στον τομέα της κυβερνοασφάλειας·
- στήριξη για την προώθηση προϊόντων και υπηρεσιών στην αγορά·
- αυξημένη προβολή σε δυνητικούς επενδυτές και επιχειρηματικούς εταίρους·
- εξοικονόμηση κόστους μέσω επενδύσεων από κοινού με άλλα κράτη μέλη·
- ικανότητα της ΕΕ να προστατεύει την οικονομία και τη δημοκρατία της με αυτόνομο τρόπο·
- η ΕΕ θα καταστεί πρωτοπόρος στον τομέα της κυβερνοασφάλειας.

Ποιος θα ωφεληθεί;



Υπηρεσία Εκδόσεων

Print ISBN 978-92-79-92480-4 doi:10.2775/734641 NA-04-18-693-EL-C
PDF ISBN 978-92-79-92474-3 doi:10.2775/35696 NA-04-18-693-EL-N