ΟΡΓΑΝΙΣΜΟΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

ΜΙΑ ΑΞΙΟΠΙΣΤΗ ΕΥΡΩΠΗ, ΑΣΦΑΛΗΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Στρατηγική του ENISA

Ιούνιος 2020

ΜΙΑ ΑΞΙΟΠΙΣΤΗ ΕΥΡΩΠΗ, ΑΣΦΑΛΗΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

ΟΡΓΑΝΙΣΜΟΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

ΠΡΟΛΟΓΟΣ

Για περισσότερα από 15 έτη, ο ENISA —ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια— διαδραματίζει βασικό ρόλο στην ενίσχυση της φιλοδοξίας της ΕΕ να υποστηρίζει την ψηφιακή εμπιστοσύνη και ασφάλεια σε ολόκληρη την Ευρώπη, σε συνεργασία με τα κράτη μέλη, τα θεσμικά όργανα και τους οργανισμούς της ΕΕ. Φέρνοντας κοντά τις κοινότητες, ο ENISA συνέβαλε επιτυχώς στην ενίσχυση της ετοιμότητας και της δυνατότητας ανταπόκρισης της Ευρώπης σε περιστατικά στον κυβερνοχώρο.

Ταυτόχρονα, ο βαθμός ψηφιοποίησης της οικονομίας και της κοινωνίας μας έχει αυξηθεί σημαντικά, όπως αποδείχθηκε κατά τη διάρκεια της κρίσης λόγω της νόσου COVID-19, οπότε η συλλογική και μαζική στροφή σε απομακρυσμένες λύσεις ΤΠ κρίθηκε αναγκαία για τη συνέχιση πολλών δραστηριοτήτων. Η κρίση αυτή υπογράμμισε τον βαθμό στον οποίο οι επιπτθέμενοι στον κυβερνοχώρο εκμεταλλεύονται την εξάρτησή μας από τις συγκεκριμένες τεχνολογίες. Αποκάλυψε επίσης τον τρόπο με τον οποίο το τοπίο των απειλών στον κυβερνοχώρο επεκτάθηκε από στοχευμένες επιθέσεις προς νέες μορφές μαζικών απειλών για εκατομμύρια επιχειρήσεις και πολίτες, συμπεριλαμβανομένου του ολοένα και αυξανόμενου αριθμού περιστατικών επίθεσης με εξελιγμένα λογισμικά εκβίασης (ransomware). Η ταχεία ανάπτυξη ψηφιακών προϊόντων και υπηρεσιών, από το νέφος και τις τηλεδιασκέψεις έως το 5G και την τεχνητή νοημοσύνη, ανέδειξε επίσης την ανάγκη αποκάλυψης και αντιμετώπισης νέων προκλήσεων.

Με τη μόνιμη εντολή του και τα ενισχυμένα καθήκοντα και δυνατότητές του, ο ENISA προορίζεται, περισσότερο από ποτέ, να διαδραματίσει ηγετικό ρόλο στην παροχή συνδρομής στην ΕΕ και τα κράτη μέλη της ώστε να ανταποκριθούν στις εν λόγω προκλήσεις, καθώς ανατέλλει μια νέα εποχή για την κυβερνοασφάλεια στην Ευρώπη.

Για να το επιτύχει αυτό, ο ENISA θα εργαστεί για την πρόβλεψη σχετικών τάσεων, προκειμένου να αντλήσει και να μοιραστεί εμπειρογνωμοσύνη και γνώσεις αιχμής για όλους. Θα υποστηρίξει την Ευρωπαϊκή Επιτροπή και τα κράτη μέλη στην παροχή συνδρομής σε δημόσιους και ιδιωτικούς φορείς καθώς και σε πολίτες με στόχο την πρόληψη και διαχείριση κινδύνων που σχετίζονται με περιστατικά στον κυβερνοχώρο. Με την εφαρμογή του πλαισίου πιστοποίησης της κυβερνοασφάλειας, ο ENISA θα συμβάλλει σε μια μεταστροφή βελτιώνοντας το επίπεδο ασφάλειας των ψηφιακών λύσεων που αναπτύσσονται στην Ευρώπη. Με τον τρόπο αυτό, θα αυξήσει την ικανότητα επιλογής και εμπιστοσύνης για όλους. Ο Οργανισμός θα υποστηρίξει επίσης ενεργά την ευρωπαϊκή επιχειρησιακή κοινότητα για την κυβερνοασφάλεια, μέσω στενής συνεργασίας και προετοιμασίας, με στόχο την από κοινού αντιμετώπιση του επόμενου περιστατικού μεγάλης κλίμακας στον κυβερνοχώρο που θα πλήξει την Ευρώπη.

Καθώς ο ENISA αναλαμβάνει τον νέο του ρόλο, η διαφάνεια, η ευελιξία και η αξιοπιστία θα αποτελέσουν βασικούς γνώμονες στις καθημερινές του εργασίες, ενώ θα συνεργάζεται στενότερα με τα κράτη μέλη και την Ευρωπαϊκή Επιτροπή για την ευθυγράμμιση των προσεγγίσεων. Ο ENISA θα προσπαθήσει επίσης να βελτιώσει τον περιβαλλοντικό του αντίκτυπο στο πλαίσιο της συνεχιζόμενης κλιματικής κρίσης, ενώ θα προσφέρει ένα κοινωνικά υπεύθυνο εργασιακό περιβάλλον χωρίς αποκλεισμούς.

Το παρόν έγγραφο στρατηγικής, το οποίο καταρτίστηκε με τη συμμετοχή όλου του προσωπικού του ENISA, των μελών του διοικητικού συμβουλίου και της συμβουλευτικής ομάδας του στο πλαίσιο μιας διαδικασίας συνεργασίας χωρίς αποκλεισμούς, θέτει τους σαφείς στόχους που θα καθοδηγήσουν το έργο του ENISA κατά τα επόμενα έτη για την αντιμετώπιση των πολυάριθμων μελλοντικών προκλήσεων.

Για λογαριασμό του Διοικητικού Συμβουλίου

Jean-Baptiste Demaison
Πρόεδρος του Διοικητικού Συμβουλίου

Krzysztof Silicki
Αντιπρόεδρος του Διοικητικού Συμβουλίου

ΟΡΑΜΑ

Μια αξιόπιστη Ευρώπη, ασφαλής στον κυβερνοχώρο

ΑΠΟΣΤΟΛΗ

Η αποστολή του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) είναι να επιτύχει ένα υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση σε συνεργασία με την ευρύτερη κοινότητα. Αυτό το επιτυγχάνει ενεργώντας ως κέντρο εμπειρογνωμοσύνης στον τομέα της κυβερνοασφάλειας, συλλέγοντας και παρέχοντας ανεξάρτητες, υψηλής ποιότητας τεχνικές συμβουλές και συνδρομή στα κράτη μέλη και τους φορείς της ΕΕ για την κυβερνοασφάλεια. Συνεισφέρει στην ανάπτυξη και την εφαρμογή των ενωσιακών πολιτικών για τον κυβερνοχώρο.

Στόχος μας είναι να ενισχύσουμε την εμπιστοσύνη στη συνδεδεμένη οικονομία, να προωθήσουμε την ανθεκτικότητα και την εμπιστοσύνη στις υποδομές και τις υπηρεσίες της Ένωσης και να διατηρήσουμε την κοινωνία και τους πολίτες μας ψηφιακά ασφαλείς. Φιλοδοξία μας είναι να αποτελούμε έναν ευέλικτο, περιβαλλοντικά και κοινωνικά υπεύθυνο οργανισμό με επίκεντρο τον άνθρωπο.

ΑΞΙΕΣ

Κοινοτική νοοτροπία
Ο ENISA συνεργάζεται με τις κοινότητες, δείχνοντας σεβασμό στις ικανότητες και την τεχνογνωσία τους, ενώ προάγει συνέργειες και την εμπιστοσύνη για την καλύτερη επίτευξη της αποστολής του.

Αριστεία
Ο ENISA επιδιώκει να εφαρμόζει τεχνογνωσία αιχμής στο έργο του, να τηρεί τα υψηλότερα ποιοτικά πρότυπα λειτουργίας και να αξιολογεί την απόδοσή του για τη συνεχή βελτίωσή του μέσω της καινοτομίας και της προνοητικότητας.

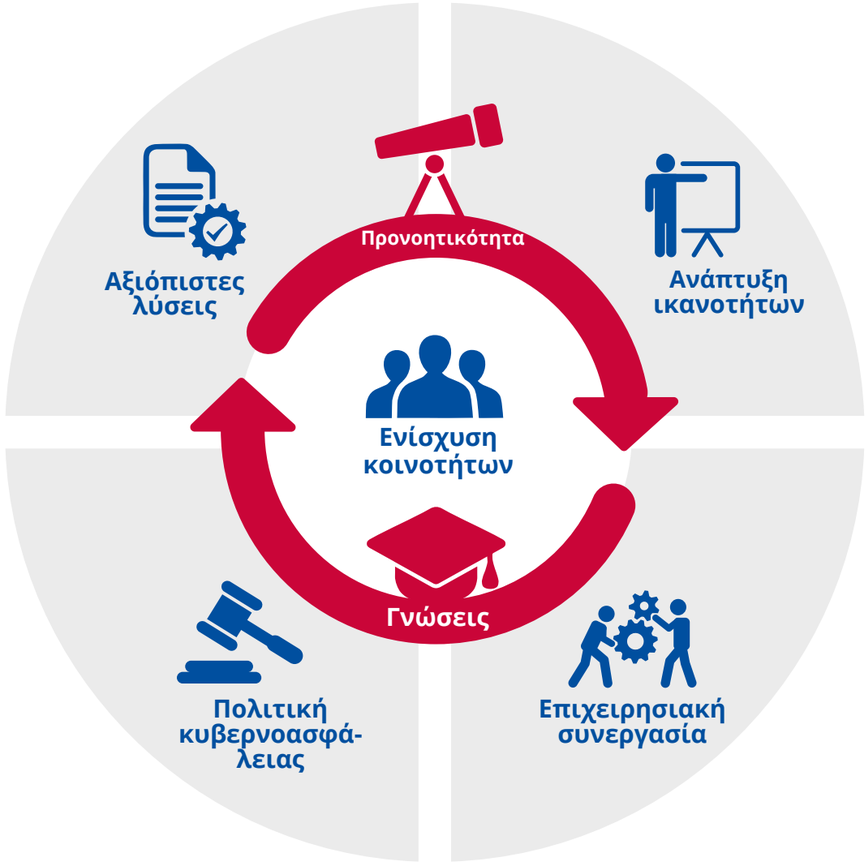
Ακεραιότητα/δεοντολογία
Ο ENISA τηρεί τις αρχές δεοντολογίας και τους σχετικούς κανόνες και υποχρεώσεις της ΕΕ στις υπηρεσίες και το εργασιακό περιβάλλον του διασφαλίζοντας την αμεροληψία και τη συμμετοχή χωρίς αποκλεισμούς.

Σεβασμός
Ο ENISA σέβεται τα θεμελιώδη ευρωπαϊκά δικαιώματα και αξίες που καλύπτουν όλες τις υπηρεσίες και το περιβάλλον εργασίας του, καθώς και τις προσδοκίες των ενδιαφερόμενων μερών του.

Ευθύνη
Ο ENISA αναλαμβάνει ευθύνη διασφαλίζοντας με τον τρόπο αυτό την ενσωμάτωση των κοινωνικών και περιβαλλοντικών διαστάσεων σε πρακτικές και διαδικασίες.

Διαφάνεια
Ο ENISA θεσπίζει διαδικασίες, δομές και μεθόδους που είναι ανοικτές, τεκμηριωμένες και ανεξάρτητες, περιορίζοντας έτσι τη μεροληψία, την ασάφεια, την απάτη και την αδιαφάνεια.

ΣΤΡΑΤΗΓΙΚΟΙ ΣΤΟΧΟΙ



ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ 1

Στρατηγικός στόχος

ΕΝΙΣΧΥΜΕΝΕΣ ΚΑΙ ΕΝΕΡΓΕΣ ΚΟΙΝΟΤΗΤΕΣ ΣΕ ΟΛΟΚΛΗΡΟ ΤΟ ΟΙΚΟΣΥΣΤΗΜΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Πλαίσιο

Η κυβερνοασφάλεια αποτελεί κοινή ευθύνη. Η Ευρώπη επιδιώκει τη δημιουργία ενός διατομεακού πλαισίου συνεργασίας χωρίς αποκλεισμούς. Ο ENISA διαδραματίζει βασικό ρόλο στην ενίσχυση της ενεργού συνεργασίας μεταξύ των ενδιαφερόμενων φορέων στον τομέα της κυβερνοασφάλειας στα κράτη μέλη και στα θεσμικά όργανα και οργανισμούς της ΕΕ. Επιδιώκει να διασφαλίσει τη συμπληρωματικότητα των κοινών προσπαθειών, προσθέτοντας αξία για τους ενδιαφερόμενους φορείς, διερευνώντας συνέργειες και χρησιμοποιώντας αποτελεσματικά περιορισμένη εμπειρογνωμοσύνη και πόρους στον τομέα της κυβερνοασφάλειας. Οι κοινότητες θα πρέπει να ενισχυθούν ώστε να κλιμακώσουν το μοντέλο κυβερνοασφάλειας.

Τι θέλουμε να επιτύχουμε

- Ένα πανευρωπαϊκό, υπερσύγχρονο σύνολο γνώσεων σχετικά με τις έννοιες και τις πρακτικές της κυβερνοασφάλειας, το οποίο θεμελιώνει τη συνεργασία μεταξύ των βασικών παραγόντων στην κυβερνοασφάλεια, προωθεί τα διδάγματα που αποκομίζονται, την εμπειρογνωμοσύνη της ΕΕ και δημιουργεί νέες συνέργειες.
- Ένα ενισχυμένο οικοσύστημα στον κυβερνοχώρο που περιλαμβάνει τις αρχές των κρατών μελών, τα θεσμικά όργανα και τους οργανισμούς της ΕΕ, τις ενώσεις, τα ερευνητικά κέντρα και τα πανεπιστήμια, τη βιομηχανία, τους ιδιωτικούς φορείς και τους πολίτες, που όλοι τους διαδραματίζουν τον ρόλο τους για να καταστήσουν την Ευρώπη ασφαλή στον κυβερνοχώρο.

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ 2

Στρατηγικός στόχος

“

Η ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΩΣ ΑΝΑΠΟΣΠΑΣΤΟ ΤΜΗΜΑ ΤΩΝ ΠΟΛΙΤΙΚΩΝ ΤΗΣ ΕΕ

Πλαίσιο

Η κυβερνοασφάλεια αποτελεί τον ακρογωνιαίο λίθο του ψηφιακού μετασχηματισμού και είναι αναγκαία για όλους τους τομείς, επομένως θα πρέπει να εξεταστεί σε ένα ευρύ φάσμα τομέων και πρωτοβουλιών πολιτικής. Η κυβερνοασφάλεια δεν θα πρέπει να περιορίζεται σε μια εξειδικευμένη κοινότητα τεχνικών εμπειρογνωμόνων στον κυβερνοχώρο. Η κυβερνοασφάλεια θα πρέπει επομένως να ενσωματωθεί σε όλους τους τομείς πολιτικής της ΕΕ. Η αποφυγή του κατακερματισμού και η ανάγκη συνεκτικής προσέγγισης λαμβάνοντας υπόψη τις ιδιαιτερότητες του κάθε τομέα είναι καθοριστικής σημασίας.

Τι θέλουμε να επιτύχουμε

- Προληπτική συμβουλευτική και υποστήριξη σε όλους τους σχετικούς παράγοντες σε επίπεδο ΕΕ, θέτοντας τη διάσταση της κυβερνοασφάλειας στον κύκλο ζωής της χάραξης πολιτικής μέσω βιώσιμων και στοχευμένων τεχνικών κατευθυντήριων γραμμών.
- Θέσπιση πλαισίων διαχείρισης κινδύνων για την κυβερνοασφάλεια σε όλους τους τομείς και τήρησή τους σε ολόκληρο τον κύκλο ζωής της πολιτικής για την κυβερνοασφάλεια.

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ 3

Στρατηγικός στόχος

“

ΑΠΟΤΕΛΕΣΜΑΤΙΚΗ ΣΥΝΕΡΓΑΣΙΑ ΜΕΤΑΞΥ ΕΠΙΧΕΙΡΗΣΙΑΚΩΝ ΠΑΡΑΓΟΝΤΩΝ ΕΝΤΟΣ ΤΗΣ ΕΝΩΣΗΣ ΣΕ ΠΕΡΙΠΤΩΣΗ ΜΑΖΙΚΩΝ ΠΕΡΙΣΤΑΤΙΚΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Πλαίσιο

Τα οφέλη της ευρωπαϊκής ψηφιακής οικονομίας και της κοινωνίας μπορούν να επιτευχθούν πλήρως μόνο υπό την προϋπόθεση της κυβερνοασφάλειας. Οι επιθέσεις στον κυβερνοχώρο δεν γνωρίζουν σύνορα. Όλα τα στρώματα της κοινωνίας μπορούν να επηρεαστούν και η Ένωση θα πρέπει να είναι έτοιμη να ανταποκριθεί σε μαζικές (μεγάλης κλίμακας και διασυνοριακές) κυβερνοεπιθέσεις και κρίσεις στον κυβερνοχώρο. Οι διασυνοριακές αλληλεξαρτήσεις υπογράμμισαν την ανάγκη αποτελεσματικής συνεργασίας μεταξύ των κρατών μελών και των θεσμικών οργάνων της ΕΕ για ταχύτερη αντίδραση και κατάλληλο συντονισμό των προσπαθειών σε όλα τα επίπεδα (στρατηγικό, επιχειρησιακό, τεχνικό και επικοινωνιακό).

Τι θέλουμε να επιτύχουμε

- Συνεχής διασυνοριακή υποστήριξη και υποστήριξη όλων των επιπέδων της συνεργασίας μεταξύ των κρατών μελών, καθώς και με τα θεσμικά όργανα της ΕΕ. Ιδίως ενόψει πιθανών περιστατικών και κρίσεων μεγάλης κλίμακας, υποστήριξη της κλιμάκωσης της τεχνικής, επιχειρησιακής, πολιτικής και στρατηγικής συνεργασίας μεταξύ βασικών επιχειρησιακών παραγόντων ώστε να καθίσταται δυνατή η έγκαιρη ανταπόκριση, η ανταλλαγή πληροφοριών, η επίγνωση της κατάστασης και η επικοινωνία για τις κρίσεις σε ολόκληρη την Ένωση.
- Πλήρης και άμεσος τεχνικός χειρισμός, κατόπιν αιτήματος των κρατών μελών, για τη διευκόλυνση τεχνικών και επιχειρησιακών αναγκών σε περίπτωση διαχείρισης συμβάντων και περιστατικών.

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ 4

Στρατηγικός στόχος

ΠΡΩΤΟΠΟΡΙΑΚΕΣ ΔΕΞΙΟΤΗΤΕΣ ΚΑΙ ΙΚΑΝΟΤΗΤΕΣ ΣΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΕ ΟΛΟΚΛΗΡΗ ΤΗΝ ΕΝΩΣΗ

Πλαίσιο

Η συχνότητα και η πολυπλοκότητα των επιθέσεων στον κυβερνοχώρο αυξάνεται με ταχείς ρυθμούς, ενώ ταυτόχρονα η χρήση υποδομών και τεχνολογιών ΤΠΕ από άτομα, οργανισμούς και βιομηχανίες αυξάνεται ραγδαία. Η ζήτηση για γνώσεις και ικανότητες στον τομέα της κυβερνοασφάλειας ξεπερνά την προσφορά. Η ΕΕ θα πρέπει να επενδύσει στην οικοδόμηση ικανοτήτων και ταλέντων στον τομέα της κυβερνοασφάλειας σε όλα τα επίπεδα, από τον μη ειδικό έως τον επαγγελματία υψηλής εξειδίκευσης. Οι επενδύσεις θα πρέπει να εστιάζουν όχι μόνο στην αύξηση της ικανότητας στον τομέα της κυβερνοασφάλειας στα κράτη μέλη, αλλά και στη διασφάλιση ότι οι διάφορες επιχειρησιακές κοινότητες διαθέτουν τις κατάλληλες ικανότητες αντιμετώπισης του τοπίου των απειλών στον κυβερνοχώρο.

Τι θέλουμε να επιτύχουμε

- Ευθυγραμμισμένες ικανότητες, επαγγελματική εμπειρία και εκπαιδευτικές δομές στον τομέα της κυβερνοασφάλειας, για την κάλυψη των συνεχώς αυξανόμενων αναγκών για γνώσεις και ικανότητες στον τομέα της κυβερνοασφάλειας στην ΕΕ.
- Ένα αυξημένο βασικό επίπεδο εγρήγορσης και ικανοτήτων στον τομέα του κυβερνοχώρου σε ολόκληρη την ΕΕ, με παράλληλη ενσωμάτωση του κυβερνοχώρου σε νέους κλάδους.
- Καλά σχεδιασμένες και δοκιμασμένες δυνατότητες με την κατάλληλη ικανότητα αντιμετώπισης του εξελισσόμενου περιβάλλοντος απειλών σε ολόκληρη την ΕΕ.

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ 5

Στρατηγικός στόχος

“

ΥΨΗΛΟ ΕΠΙΠΕΔΟ ΕΜΠΙΣΤΟΣΥΝΗΣ ΣΕ ΑΣΦΑΛΕΙΣ ΨΗΦΙΑΚΕΣ ΛΥΣΕΙΣ

Πλαίσιο

Τα ψηφιακά προϊόντα και υπηρεσίες αποφέρουν οφέλη, αλλά ενέχουν και κινδύνους, οι οποίοι θα πρέπει να εντοπιστούν και να μετριαστούν. Κατά τη διαδικασία αξιολόγησης της ασφάλειας των ψηφιακών λύσεων και διασφάλισης της αξιοπιστίας τους, είναι απαραίτητο να υιοθετείται μια κοινή προσέγγιση, με στόχο την επίτευξη ισορροπίας μεταξύ των αναγκών της κοινωνίας, της αγοράς, της οικονομίας και της κυβερνοασφάλειας. Η σύσταση μιας ουδέτερης οντότητας που ενεργεί με διαφανή τρόπο θα αυξήσει την εμπιστοσύνη των πελατών στις ψηφιακές λύσεις και στο ευρύτερο ψηφιακό περιβάλλον.

Τι θέλουμε να επιτύχουμε

- Ένα ασφαλές ψηφιακό περιβάλλον στον κυβερνοχώρο σε ολόκληρη την ΕΕ, όπου οι πολίτες μπορούν να εμπιστεύονται προϊόντα, υπηρεσίες και διαδικασίες ΤΠΕ μέσω της ανάπτυξης συστημάτων πιστοποίησης σε βασικούς τεχνολογικούς τομείς.

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ 6

Στρατηγικός στόχος

“

ΠΡΟΒΛΕΨΗ ΑΝΑΔΥΟΜΕΝΩΝ ΚΑΙ ΜΕΛΛΟΝΤΙΚΩΝ ΠΡΟΚΛΗΣΕΩΝ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Πλαίσιο

Πολυάριθμες νέες τεχνολογίες, που βρίσκονται ακόμη σε πρώιμο στάδιο ή πλησιάζουν το στάδιο της γενικευμένης υιοθέτησης, θα επωφεληθούν από τη χρήση μεθόδων πρόβλεψης. Μέσω μιας δομημένης διαδικασίας που θα επιτρέπει τον διάλογο μεταξύ των ενδιαφερόμενων φορέων, οι υπεύθυνοι λήψης αποφάσεων και χάραξης πολιτικής θα είναι σε θέση να καθορίζουν στρατηγικές έγκαιρου μετριασμού που βελτιώνουν την ανθεκτικότητα της ΕΕ στις απειλές για την κυβερνοασφάλεια, και να βρίσκουν λύσεις για την αντιμετώπιση αναδυόμενων προκλήσεων.

Τι θέλουμε να επιτύχουμε

- Κατανόηση των αναδυόμενων τάσεων και μοτίβων με τη χρήση προβλέψεων και μελλοντικών σεναρίων που συμβάλλουν στον μετριασμό των προκλήσεων που αντιμετωπίζουν οι ενδιαφερόμενοι φορείς στον κυβερνοχώρο.
- Έγκαιρη εκτίμηση των προκλήσεων και των κινδύνων από την υιοθέτηση και προσαρμογή στις αναδυόμενες μελλοντικές επιλογές, παράλληλα με τη συνεργασία με τους ενδιαφερόμενους φορείς για κατάλληλες στρατηγικές μετριασμού.

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ 7

Στρατηγικός στόχος

ΑΠΟΤΕΛΕΣΜΑΤΙΚΗ ΚΑΙ ΑΠΟΔΟΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΓΝΩΣΕΩΝ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΗΝ ΕΥΡΩΠΗ

Πλαίσιο

Κινητήριος δύναμη της κυβερνοασφάλειας είναι οι πληροφορίες και οι γνώσεις. Προκειμένου οι επαγγελματίες της κυβερνοασφάλειας να είναι σε θέση να επιτύχουν αποτελεσματικά τους στόχους που έχουμε θέσει, να εργάζονται σε ένα συνεχώς μεταβαλλόμενο περιβάλλον —όσον αφορά τις ψηφιακές εξελίξεις καθώς και σε σχέση με τους παράγοντες— για να αντιμετωπίζουν τις προκλήσεις της εποχής μας, χρειαζόμαστε μια συνεχή διαδικασία συλλογής, οργάνωσης, σύνοψης, ανάλυσης, γνωστοποίησης και διατήρησης των πληροφοριών και των γνώσεων σχετικά με την κυβερνοασφάλεια. Όλες οι φάσεις είναι απαραίτητες για να διασφαλίζεται ότι οι πληροφορίες και οι γνώσεις κοινοποιούνται και επεκτείνονται στο οικοσύστημα της ΕΕ στον τομέα της κυβερνοασφάλειας.

Τι θέλουμε να επιτύχουμε

- Από κοινού διαχείριση πληροφοριών και γνώσεων για το οικοσύστημα της κυβερνοασφάλειας της ΕΕ σε προσιτή, προσαρμοσμένη, έγκαιρη και εφαρμόσιμη μορφή, με κατάλληλη μεθοδολογία, υποδομές και εργαλεία, συνδυασμένες μεθόδους διασφάλισης ποιότητας για την επίτευξη της συνεχούς βελτίωσης των υπηρεσιών.

ΠΛΗΡΟΦΟΡΙΕΣ ΓΙΑ ΤΟΝ ENISA

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ο ENISA, είναι ο οργανισμός της Ένωσης με αποστολή την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ευρώπη. Ο Ευρωπαϊκός Οργανισμός για την Κυβερνοασφάλεια Έχοντας, που ιδρύθηκε το 2004 και ενισχύθηκε από την Πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο, συμβάλλει στη χάραξη της πολιτικής της ΕΕ στον τομέα του κυβερνοχώρου, ενισχύει την αξιοπιστία των προϊόντων, υπηρεσιών και διαδικασιών ΤΠΕ με συστήματα πιστοποίησης της κυβερνοασφάλειας, συνεργάζεται με κράτη μέλη και φορείς της ΕΕ και βοηθά την Ευρώπη να προετοιμαστεί για τις μελλοντικές προκλήσεις στον κυβερνοχώρο. Μέσω της ανταλλαγής γνώσεων, της ανάπτυξης ικανοτήτων και της αύξησης της εγρήγορσης, ο Οργανισμός συνεργάζεται με τους βασικούς ενδιαφερόμενους φορείς για την ενίσχυση της εμπιστοσύνης στη συνδεδεμένη οικονομία, την υποστήριξη της ανθεκτικότητας των υποδομών της Ένωσης και, τελικά, τη διατήρηση της ψηφιακής ασφάλειας για την κοινωνία και τους πολίτες της Ευρώπης. Περισσότερες πληροφορίες για τον ENISA και το έργο του διατίθενται στη διεύθυνση www.enisa.europa.eu

TP-02-20-759-EL-N

ENISA
Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια

Γραφείο Αθηνών
Βασιλίσσης Σοφίας 1
151 24 Μαρούσι, Αττική, Ελλάδα

Γραφείο Ηρακλείου
Νικολάου Πλαστήρα 95
700 13 Βασιλικά Βουτών, Ηράκλειο, Κρήτη

enisa.europa.eu