CyberHubs

Στρατηγική για τις δεξιότητες κυβερνοασφάλειας

ΕΛΛΑΔΑ

Co-funded by
the European Union

Περίληψη Παραδοτέου D2.3

Στρατηγική για τις δεξιότητες κυβερνοασφάλειας στην Ελλάδα

Στόχος του παραδοτέου είναι να παρουσιάσει μια ολοκληρωμένη στρατηγική για την ανάπτυξη του εργατικού δυναμικού της Ελλάδας στον τομέα της κυβερνοασφάλειας, ώστε να αντιμετωπιστούν οι τρέχουσες και μελλοντικές προκλήσεις στο ψηφιακό τοπίο. Η στρατηγική επιδιώκει τη δημιουργία μιας ανθεκτικής, καταρτισμένης και ενημερωμένης κοινωνίας, ικανής να μετριάζει αποτελεσματικά τους ψηφιακούς κινδύνους.

Η έρευνα (ΣΕΠΕ - Deloitte, 2022) του Συνδέσμου Ελληνικών Επιχειρήσεων Πληροφορικής και Επικοινωνιών (ΣΕΠΕ) για την αξιολόγηση της επάρκειας ειδικών Τεχνολογίας Πληροφοριών και Επικοινωνιών (ΤΠΕ) στην Ελλάδα, επιβεβαίωσε ότι οι περισσότερες επιχειρήσεις έχουν κενές θέσεις για ειδικούς ΤΠΕ. Στο άμεσο μέλλον αναμένεται σημαντική αύξηση της ζήτησης για τις ειδικότητες αυτές. Το εκτιμώμενο κενό ζήτησης-προσφοράς για την περίοδο 2023-2030 είναι μεταξύ 7.000 και 7.500 ατόμων ετησίως. Η μελέτη διαπίστωσε ότι η ασφάλεια στον κυβερνοχώρο είναι μία από τις τρεις πρώτες ειδικότητες με τη μεγαλύτερη ζήτηση σε ολόκληρο τον τομέα των ΤΠΕ.

Στο νομοθετικό σκέλος η Ευρωπαϊκή Ένωση (ΕΕ) αναγνωρίζοντας τις προκλήσεις που αντιμετωπίζουν οι ευρωπαϊκές επιχειρήσεις, εξέδωσε την Πράξη για την Ψηφιακή Επιχειρησιακή Ανθεκτικότητα (DORA) και την Οδηγία για την Ασφάλεια Δικτύων και Πληροφοριών (NIS2), με στόχο τη θωράκιση των λειτουργιών των χρηματοπιστωτικών οντοτήτων και των εταιρειών που παρέχουν υπηρεσίες που σχετίζονται με κρίσιμες υποδομές, αντίστοιχα.

Από την πλευρά της η Ελλάδα σε σύμπλευση με την ΕΕ, έχει αναλάβει σημαντικές πρωτοβουλίες για να ανταποκριθεί στις διεθνείς και κοινοτικές απαιτήσεις, να δημιουργήσει ένα ασφαλές περιβάλλον για τις ψηφιακές τεχνολογίες και να αυξήσει την εμπιστοσύνη των πολιτών και των επιχειρήσεων στις ψηφιακές εφαρμογές και υπηρεσίες. Απόρροια των παραπάνω αποτελεί ο Νόμος 5160/2024 που ενσωματώνει την Οδηγία NIS 2 ενδυναμώνοντας έτσι την Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ), ώστε να ασκήσει αποτελεσματικά τις αρμοδιότητές της ως Εθνική Αρμόδια Αρχή για την εφαρμογή της Οδηγίας, αποκτώντας μεταξύ άλλων διευρυμένες εποπτικές και ελεγκτικές αρμοδιότητες.

Κυριότεροι φορείς στον τομέα των δεξιοτήτων κυβερνοασφάλειας στην Ελλάδα είναι:

- ✓ Εθνική Αρχή Κυβερνοασφάλειας
- ✓ Υπουργείο Ψηφιακής Διακυβέρνησης
- ✓ Υπουργείο Παιδείας, Θρησκευμάτων και Αθλητισμού
- ✓ Ακαδημαϊκά και ερευνητικά ιδρύματα
- ✓ Επιχειρήσεις ΤΠΕ
- ✓ ENISA
- ✓ ISACA και ISC2 (Ελληνικό παράρτηματα)

Η ελληνική στρατηγική για τις δεξιότητες στον τομέα της κυβερνοασφάλειας βασίζεται στην αντιμετώπιση των ελλείψεων εργατικού δυναμικού, στην ενίσχυση της εκπαίδευσης και στην προώθηση της συνεργασίας για τη δημιουργία ενός ανθεκτικού τοπίου στον τομέα της κυβερνοασφάλειας. Οραματίζεται την ανάπτυξη ενός εξειδικευμένου εργατικού δυναμικού που θα είναι εξοπλισμένο για να ανταποκριθεί στις απαιτήσεις ενός εξελισσόμενου περιβάλλοντος

κυβερνοαπειλών, ενώ παράλληλα θα υποστηρίζει τον ψηφιακό μετασχηματισμό και την οικονομική ανάπτυξη της χώρας. Οι στρατηγικοί στόχοι θα επιτευχθούν μέσω μιας σειράς πρωτοβουλιών, καθεμία από τις οποίες έχει διαφορετικά χρονοδιαγράμματα (2 έτη, 2-3 έτη, 2-5 έτη και 5+ έτη). Η ολοκλήρωση αυτών των στόχων περιγράφεται στο ακόλουθο σχέδιο δράσης.

1. Ανάπτυξη εξειδικευμένου εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας:
    - Προώθηση της δια βίου μάθησης για την αναβάθμιση των υφιστάμενων επαγγελματιών και την προσαρμογή στις εξελισσόμενες απειλές στον κυβερνοχώρο.
    - Προώθηση της ανάπτυξης προηγμένων δεξιοτήτων μέσω εξειδικευμένων πιστοποιήσεων, μεταπτυχιακών προγραμμάτων και πρακτικής εμπειρίας.
2. Ενίσχυση της συνεργασίας δημόσιου και ιδιωτικού τομέα:
    - Δημιουργία εταιρικών σχέσεων μεταξύ του ακαδημαϊκού, του κυβερνητικού και του ιδιωτικού τομέα για την ενίσχυση των ευκαιριών κατάρτισης, την προώθηση της καινοτομίας και την κοινή χρήση πόρων.
    - Ενθάρρυνση των επενδύσεων του ιδιωτικού τομέα στην κατάρτιση και ανάπτυξη των εργαζομένων για την αύξηση της ικανότητας και της εμπειρογνωμοσύνης του εργατικού δυναμικού.
3. Ενίσχυση της εθνικής ευαισθητοποίησης και κουλτούρας για την ασφάλεια στον κυβερνοχώρο:
    - Καλλιέργεια μιας κουλτούρας ευαισθητοποίησης σε θέματα κυβερνοασφάλειας μέσω στοχευμένων εκστρατειών δημόσιας εκπαίδευσης και προγραμμάτων κατάρτισης.
    - Προώθηση των βέλτιστων πρακτικών κυβερνοασφάλειας σε όλους τους τομείς της κοινωνίας για τη μείωση της ευπάθειας σε κυβερνοαπειλές.
4. Δημιουργία ενός βιώσιμου οικοσυστήματος κυβερνοασφάλειας:
    - Ανάπτυξη ενός πλαισίου για τη συνεχή παρακολούθηση και αξιολόγηση των αναγκών σε δεξιότητες κυβερνοασφάλειας, εξασφαλίζοντας την ευθυγράμμιση με τις απαιτήσεις του κλάδου και τις κανονιστικές απαιτήσεις.
    - Δημιουργία κέντρων αριστείας και παρατηρητηρίων για τη στήριξη του μακροπρόθεσμου σχεδιασμού του εργατικού δυναμικού και της καινοτομίας σε λύσεις κυβερνοασφάλειας.

Το σχέδιο δράσης οργανώνεται σύμφωνα με τους στρατηγικούς στόχους, με κάθε πρωτοβουλία να διαρθρώνεται σε υψηλό επίπεδο. Η προσέγγιση αυτή διατηρεί την ευθυγράμμιση με τους γενικούς στόχους της στρατηγικής, ενώ πιο συγκεκριμένες λεπτομέρειες θα αναπτυχθούν στην έκθεση του Πακέτου Εργασίας WP3. Ο ακόλουθος πίνακας παρουσιάζει συνοπτικά μια γενική επισκόπηση των προτεινόμενων πρωτοβουλιών.

Αρ. Πρωτοβουλίας	Όνομα πρωτοβουλίας	Στόχος	Τομέας εστίασης
1	Δημόσια έργα κυβερνοασφάλειας	Ενίσχυση του πλαισίου κυβερνοασφάλειας της Ελλάδας με την αντιμετώπιση των υφιστάμενων προκλήσεων, τη δημιουργία νέων ευκαιριών απασχόλησης στον τομέα της κυβερνοασφάλειας και τη στήριξη του ψηφιακού μετασχηματισμού της χώρας.	Δημόσιος τομέας
2	Συνεργασία με άλλες χώρες	Η συνεργασία με τρίτες χώρες θα μας βοηθήσει να ανταλλάξουμε ιδέες, απόψεις, τεχνολογίες ώστε να μπορέσουμε να ενσωματώσουμε πρακτικές και να υιοθετήσουμε στρατηγικές για την εύρεση των κατάλληλων ατόμων σε ρόλους που έχουν υψηλή ζήτηση στην αγορά εργασίας.	Συνεργασία
3	Ανάπτυξη ενός τυποποιημένου προγράμματος σπουδών για την ασφάλεια στον κυβερνοχώρο	Ενίσχυση του κυβερνογραφικού αλφαβητισμού μεταξύ του γενικού πληθυσμού και των μη επαγγελματιών του τομέα της πληροφορικής, ώστε να δημιουργηθεί ένα βασικό επίπεδο ευαισθητοποίησης στον τομέα της κυβερνοασφάλειας.	Εκπαίδευση και κατάρτιση
4	Εκστρατεία ευαισθητοποίησης και εκπαίδευσης του κοινού για την κυβερνοασφάλεια	Ενίσχυση του κυβερνογραφικού αλφαβητισμού μεταξύ του γενικού πληθυσμού και των μη επαγγελματιών του τομέα της πληροφορικής, ώστε να δημιουργηθεί ένα βασικό επίπεδο ευαισθητοποίησης στον τομέα της κυβερνοασφάλειας.	
5	Επέκταση των ευέλικτων προγραμμάτων μάθησης και πιστοποίησης	Αύξηση της προσβασιμότητας στην εκπαίδευση στον τομέα της κυβερνοασφάλειας μέσω διαδικτυακών μαθημάτων, πιστοποιήσεων και ευέλικτων επιλογών μάθησης. Παροχή υποτροφιών (καλύπτοντας τα δίδακτρα ή προσφέροντας εγγυήσεις απασχόλησης) σε μεταπτυχιακούς και διδακτορικούς φοιτητές από τον ιδιωτικό τομέα, με δέσμευση για απασχόληση μετά την αποφοίτηση.	
6	Πρόγραμμα πρακτικής άσκησης και μαθητείας δημόσιου και ιδιωτικού τομέα	Γεφύρωση του χάσματος δεξιοτήτων με την παροχή πρακτικής εμπειρίας στον τομέα της ασφάλειας στον κυβερνοχώρο μέσω συνεργατικών προγραμμάτων πρακτικής άσκησης.	Συμπράξεις με τη βιομηχανία
7	Στοχευμένη χρηματοδότηση έρευνας και ανάπτυξης	Στοχευμένη χρηματοδότηση από την ΕΕ και το δημόσιο για την έρευνα και την τεχνολογική ανάπτυξη.	Έρευνα και ανάπτυξη

8	Εθνική πλατφόρμα πληροφοριών για τις απειλές στον κυβερνοχώρο	Δημιουργία μιας κεντρικής πλατφόρμας ανταλλαγής πληροφοριών σχετικά με απειλές για να καταστεί δυνατή η συνεργασία σε πραγματικό χρόνο μεταξύ του δημόσιου και του ιδιωτικού τομέα.	

Πίνακας: Προτεινόμενες πρωτοβουλίες του σχεδίου δράσης

Γίνεται αντιληπτό ότι το τοπίο της κυβερνοασφάλειας εξελίσσεται με ταχείς ρυθμούς και οι πρωτοβουλίες του CyberHub πρέπει να προσαρμόζονται στις αλλαγές της τεχνολογίας, στις απαιτήσεις του κλάδου και στις αναδυόμενες απειλές. Για να ανταποκριθεί σε αυτές τις αλλαγές, η επιτροπή εποπτείας του CyberHub θα διεξάγει ετήσιες αναθεωρήσεις για να αξιολογήσει τη συνεχή συνάφεια των δραστηριοτήτων και των βασικών δεικτών απόδοσης του σχεδίου δράσης.

Σε περίπτωση σημαντικών αλλαγών - όπως αλλαγές στους τύπους απειλών στον κυβερνοχώρο, νέες τεχνολογικές εξελίξεις ή επικαιροποιήσεις κανονισμών - τόσο οι πρωτοβουλίες όσο και οι δείκτες απόδοσης μπορεί να αναθεωρηθούν ώστε να αντικατοπτρίζουν το νέο πλαίσιο.

Εάν μια πρωτοβουλία ή δραστηριότητα αποτύχει να επιτύχει τους δείκτες απόδοσης για δύο διαδοχικές περιόδους αναθεώρησης, η επιτροπή θα ξεκινήσει αξιολόγηση για να καθορίσει εάν απαιτούνται προσαρμογές. Αυτό μπορεί να περιλαμβάνει τη βελτίωση του περιεχομένου του προγράμματος, την πραγματική τοποθέτηση πόρων ή την αλλαγή των χρονοδιαγραμμάτων για τη βελτίωση της αποτελεσματικότητας. Η ανατροφοδότηση από τους συμμετέχοντες και τους ενδιαφερόμενους θα διαδραματίσει κρίσιμο ρόλο στην καθοδήγηση αυτών των προσαρμογών.

Η ελληνική στρατηγική για τις δεξιότητες κυβερνοασφάλειας δεν αφορά μόνο την αντιμετώπιση άμεσων αναγκών - είναι ένα μελλοντικό σχέδιο για την εθνική ανθεκτικότητα και ανάπτυξη. Επενδύοντας σε δεξιότητες, εκπαίδευση και συνεργασίες, η Ελλάδα τοποθετείται ως ηγέτης στο ευρωπαϊκό τοπίο της κυβερνοασφάλειας. Η επιτυχία αυτής της στρατηγικής δεν θα διασφαλίσει μόνο τις κρίσιμες υποδομές και τα ψηφιακά περιουσιακά στοιχεία, αλλά θα συμβάλει επίσης στην οικονομική ανάπτυξη, την κοινωνική εμπιστοσύνη στα ψηφιακά συστήματα και την παγκόσμια ανταγωνιστικότητα της χώρας.

Με ισχυρά θεμέλια, σαφείς στόχους και δέσμευση στη συνεργασία, η Ελλάδα είναι καλά εξοπλισμένη για να αντιμετωπίσει τις προκλήσεις ενός ολοένα και πιο διασυνδεδεμένου και πολύπλοκου ψηφιακού μέλλοντος. Η παρούσα στρατηγική αντανακλά ένα συλλογικό όραμα για ένα ασφαλές, καινοτόμο και ανθεκτικό έθνος, διασφαλίζοντας ότι η Ελλάδα θα παραμείνει στην πρώτη γραμμή των παγκόσμιων προσπαθειών για την καταπολέμηση των απειλών στον κυβερνοχώρο.

Το πλήρες κείμενο της **Στρατηγικής για τις δεξιότητες κυβερνοασφάλειας** στην Ελλάδα μπορείτε να το βρείτε στο: cyberhubs.eu

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.