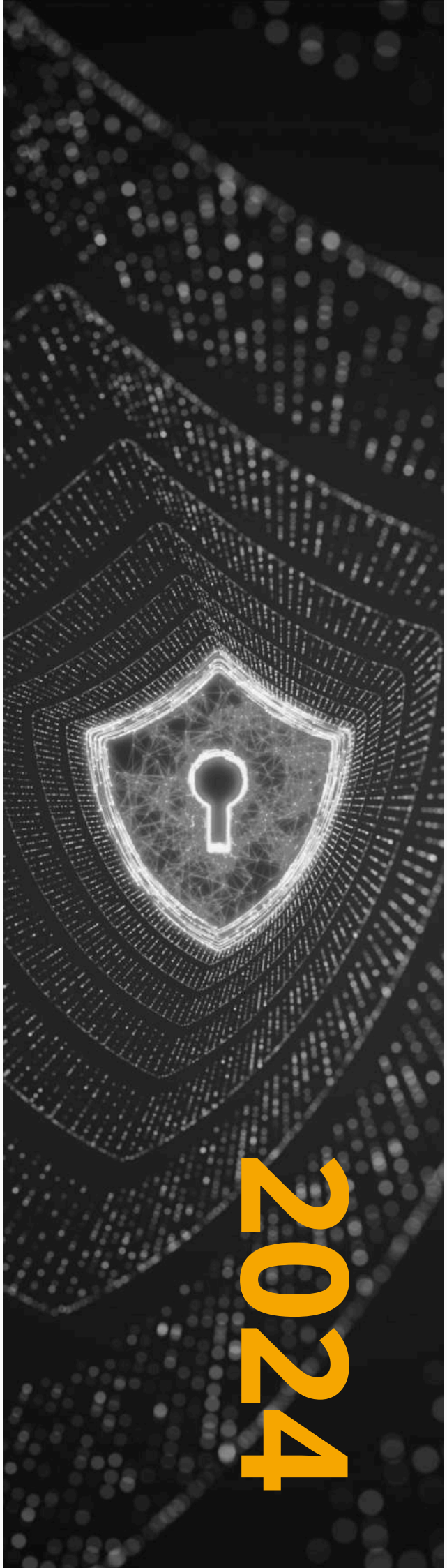


ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

Αρχή Ψηφιακής Ασφάλειας

Έκθεση Δραστηριοτήτων

2024

Το Όραμά μας

Το όραμα της Αρχής Ψηφιακής Ασφάλειας είναι όπως η Κύπρος καταστεί μια από τις πρωτοπόρες χώρες της περιοχής στα θέματα κυβερνοασφάλειας, για την προστασία των κρίσιμων υποδομών πληροφοριών του κράτους, των επιχειρήσεων και της κοινωνίας ευρύτερα, και τη δημιουργία ενός κατάλληλου και ελκυστικού περιβάλλοντος οικονομικής ανάπτυξης και προώθησης των υπηρεσιών στις οποίες η Κύπρος κατέχει υψηλή θέση παγκοσμίως.

dsa.cy

Ακρωνύμια & Συντομογραφίες

Ακρωνύμιο	Πλήρες Όνομα
ΑΨΑ	Αρχή Ψηφιακής Ασφάλειας
Ακαδημία ICT	Ακαδημία Πληροφορικής, Τεχνολογίας και Επικοινωνιών (ICT Academy) του Γραφείου Επιτρόπου Επικοινωνιών
ΕΑΠΚ	Εθνική Αρχή Πιστοποίηση Κυβερνοασφάλειας
ΕΕ	Ευρωπαϊκή Ένωση
Εθνικό CSIRT- CY	Εθνική Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων
ΙδΕΚ	Ίδρυμα Έρευνας και Καινοτομίας
ΚΕΒΕ	Κυπριακό Εμπορικό και Βιομηχανικό Επιμελητήριο
ΜμΕ	Μικρομεσαίες Επιχειρήσεις
MoU	Memorandum of Understanding - Μνημόνιο Συναντίληψης
ΤΠΕ	Τεχνολογία Πληροφοριών και Επικοινωνιών
ΡΣΕ	Ρύθμιση Στρατηγική και Εποπτεία (Τομέας ΑΨΑ)
DEP	Digital Europe Programme – Πρόγραμμα Ψηφιακή Ευρώπη
DiGiNN	Ευρωπαϊκός Κόμβος Ψηφιακής Καινοτομίας Κύπρου - Digital Innovation Hub Cyprus
ECCC	Πανευρωπαϊκός Οργανισμός Αρμοδιότητας Κυβερνοασφάλειας
ECSO	European Cybersecurity Organisation
ENISA	European Network and Information Security Agency - Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια
GB	Governing Board – Διοικητικό Συμβούλιο
HEP	Horizon Europe Programme – Πρόγραμμα Ορίζοντας Ευρώπη
ICT	Information and Communication Technology
NCC-CY	Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας Κύπρου
SOC	Κέντρο Επιχειρήσεων Κυβερνοασφάλειας - Security Operation Center

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΕΧΟΜΕΝΑ

1 ΕΙΣΑΓΩΓΗ
ΧΑΙΡΕΤΙΣΜΟΣ ΕΠΙΤΡΟΠΟΥ

Είναι πλέον κοινώς αποδεκτό ότι η κυβερνοασφάλεια αποτελεί αναπόσπαστο μέρος της καθημερινότητάς μας, καθώς οι κυβερνοεπιθέσεις δεν στοχεύουν μόνο μεγάλους οργανισμούς και κρίσιμες υποδομές, αλλά επηρεάζουν άμεσα τους πολίτες, τις επιχειρήσεις και, κατ' επέκταση, την εθνική οικονομία και ασφάλεια.

Το 2024 υπήρξε χρονιά έντονων εξελίξεων και νέων δεδομένων στον τομέα της ψηφιακής ασφάλειας — ένα έτος γεμάτο προκλήσεις, αλλά και σημαντικές ευκαιρίες. Η δυναμική φύση της τεχνολογίας και η αυξανόμενη πολυπλοκότητα των ψηφιακών απειλών ανέδειξαν την ανάγκη για ευελιξία, προσαρμοστικότητα και συνεχή βελτίωση. Παρά το γεγονός ότι οι νέες μορφές κυβερνοαπειλών δοκίμασαν ξανά την ανθεκτικότητα και την ετοιμότητά μας, παράλληλα μας έδωσαν τη δυνατότητα να μάθουμε, να εξελιχθούμε και να ενισχύσουμε την ψηφιακή μας άμυνα.

Σημαντικό ορόσημο της χρονιάς αποτέλεσε η προετοιμασία για την εφαρμογή της Οδηγίας (ΕΕ) 2022/2555 (NIS2), η οποία διευρύνει το πεδίο εποπτείας κρίσιμων υποδομών, εντάσσοντας νέους τομείς βάσει του βαθμού ψηφιοποίησης, της διασύνδεσής τους και της σημασίας τους για την οικονομία και την κοινωνία. Η Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) διαδραμάτισε κεντρικό ρόλο στην προσπάθεια προσαρμογής της Κύπρου στις νέες απαιτήσεις, διασφαλίζοντας ότι η χώρα παραμένει ανθεκτική απέναντι στις σύγχρονες ψηφιακές προκλήσεις.

Εξίσου σημαντική ήταν η έναρξη της 24ωρης λειτουργίας του Κέντρου Επιχειρήσεων Κυβερνοασφάλειας (SOC – Security Operation Centre), το οποίο ενίσχυσε ουσιαστικά την Εθνική Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (CSIRT-CY). Μέσω της συνεχούς επιτήρησης και παρακολούθησης δεδομένων σε πραγματικό χρόνο, ενισχύθηκε η δυνατότητα πρόληψης αλλά και άμεσης και αποτελεσματικής ανταπόκρισης σε κυβερνοεπιθέσεις.

Επίσης, το 2024 σηματοδότησε τη συμπλήρωση του πρώτου χρόνου λειτουργίας της Ακαδημίας Τεχνολογίας, Πληροφορικής και Επικοινωνιών (ICT Academy). Μέσω της Ακαδημίας, πραγματοποιήθηκαν περισσότερες από 150 εκδηλώσεις με τη συμμετοχή άνω των 4.000 ατόμων. Η λειτουργία της ανταποκρίνεται στην ανάγκη κάλυψης του διαρκώς αυξανόμενου κενού σε ψηφιακές δεξιότητες, προσφέροντας υψηλού επιπέδου εκπαίδευση και κατάρτιση στους τομείς της κυβερνοασφάλειας, των τηλεπικοινωνιών και των αναδυόμενων τεχνολογιών.

Παράλληλα, και αναγνωρίζοντας τις αυξανόμενες ανάγκες, ενισχύσαμε την ΑΨΑ με νέες δομές και εξειδικευμένο ανθρώπινο δυναμικό, ικανό να ανταποκριθεί στις διαρκώς υψηλότερες απαιτήσεις, δίδοντας ταυτόχρονα έμφαση στη συνεχή εκπαίδευση του προσωπικού, ενδυναμώνοντας την αποτελεσματικότητα και την ετοιμότητα της Αρχής.

Αναμφίβολα, οι προκλήσεις του 2024 ανέδειξαν με τον πλέον ξεκάθαρο τρόπο ότι η κυβερνοασφάλεια δεν αποτελεί μια στατική κατάσταση, αλλά μια δυναμική και διαρκή διαδικασία, η οποία απαιτεί συνεχείς επενδύσεις, εκπαίδευση και συνεργασία. Την ίδια στιγμή, οι ευκαιρίες που προέκυψαν μάς έδωσαν την ικανότητα να ενισχύσουμε τις δυνατότητές μας και να προσφέρουμε ουσιαστική υποστήριξη σε κρίσιμες υποδομές, επιχειρήσεις και πολίτες. Τα ορόσημα που αναφέρονται στις επόμενες σελίδες καταδεικνύουν τη σημαντικότητα του έργου της ΑΨΑ κατά το έτος 2024.

Αυτό αποδεικνύεται από τη σημαντική πρόοδο που καταγράψαμε σε διεθνείς αξιολογήσεις, φτάνοντας στη θέση Tier 1 στην οποία συγκαταλέγονται κράτη με ανεπτυγμένες και ώριμες εθνικές στρατηγικές και προσεγγίσεις κυβερνοασφάλειας, του Παγκόσμιου Δείκτη Κυβερνοασφάλειας (GCI) της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU), ενώ στον πρώτο επίσημο EU Cybersecurity Index του ENISA ξεπεράσαμε τον μέσο όρο της ΕΕ κατά 5,19 μονάδες.

Κλείνοντας, θα ήθελα να τονίσω εκ νέου πως οι απειλές δεν περιορίζονται πλέον σε συγκεκριμένους στόχους, αλλά επηρεάζουν ολόκληρη την κοινωνία και την οικονομία. Αυτό καθιστά σαφές ότι η ψηφιακή ασφάλεια δεν είναι απλώς ένα τεχνικό ζήτημα, αλλά συλλογική ευθύνη.

Με αφοσίωση στον στόχο μιας ψηφιακά ανθεκτικής Κύπρου και καθοδηγούμενοι από τις εθνικές μας προτεραιότητες, συνεχίζουμε με αποφασιστικότητα να σχεδιάζουμε και να υλοποιούμε πρωτοβουλίες που ανταποκρίνονται στις ανάγκες εναρμόνισης της Κυπριακής Δημοκρατίας με το νέο Ευρωπαϊκό νομοθετικό πλαίσιο καθώς και προσαρμογής της Κύπρου στις προκλήσεις της σύγχρονης εποχής. Τα πιο κάτω γεγονότα-ορόσημα καταδεικνύουν τη σημαντικότητα του έργου, της αναβάθμισης αλλά και της προόδου της ΑΨΑ κατά το έτος 2024.

ΓΙΩΡΓΟΣ ΜΙΧΑΗΛΙΔΗΣ
ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

2 ΓΕΓΟΝΟΤΑ ΟΡΟΣΗΜΑ 2024

Το 2024 αποτέλεσε μια χρονιά-ορόσημο για την ΑΨΑ και την κυβερνοασφάλεια στην Κύπρο, σηματοδοτώντας μεταξύ άλλων, την προετοιμασία για εφαρμογή της Οδηγίας NIS2, τον 1ο χρόνο λειτουργίας της Ακαδημίας, την εικοσιτετράωρη λειτουργία του SOC καθώς και την ολοκλήρωση των πρώτων δύο χρόνων λειτουργίας του NCC-CY. Οι παρακάτω εξελίξεις αποτυπώνουν τη δυναμική πορεία της ΑΨΑ στην ενίσχυση της ανθεκτικότητας του ψηφιακού οικοσυστήματος.

Οδηγία NIS2

Οι προετοιμασίες της Κύπρου για την υλοποίηση της Οδηγίας NIS2 κορυφώθηκαν κατά το 2024, αφού εντός του έτους ολοκληρώθηκε το τελικό προσχέδιο του σχετικού τροποποιητικού νομοσχεδίου, το οποίο αναμένεται να ψηφιστεί από τη Βουλή των Αντιπροσώπων το 2025 (Βλέπε ενότητα 6.2 για περισσότερες πληροφορίες). Επίσης, άρχισαν και οι διεργασίες για την αξιολόγηση κρισιμότητας των βασικών και σημαντικών οντοτήτων που θα εμπίπτουν στο πεδίο εφαρμογής της νέας Οδηγίας, καθώς και η διαδικασία σχεδίασης της αναβάθμισης του νέου εργαλείου (iDSAMPL2) επικοινωνίας των οντοτήτων με την ΑΨΑ.

Μοντέλο Ωριμότητας Κυβερνοασφάλειας και Εποπτικοί Ελέγχοι

Σημαντική πρόοδος σημειώθηκε επίσης και στο πεδίο της εποπτείας, με την οριστικοποίηση και δημοσίευση του Μοντέλου Ωριμότητας Κυβερνοασφάλειας, το οποίο βοηθά στην αναγνώριση του επιπέδου ωριμότητας των Κρίσιμων Υποδομών της Κυπριακής Δημοκρατίας καθώς και τη δημιουργία Μητρώου Εγκεκριμένων Ελεγκτών, το οποίο οδήγησε στην επιτυχή ολοκλήρωση και δημοσίευση της Απόφασης ΚΔΠ 245/2024, που διέπει ολόκληρη τη διαδικασία ελέγχων κυβερνοασφάλειας των κρίσιμων φορέων στην Κυπριακή Δημοκρατία (Βλέπε ενότητα 6.3 & 6.4 για περισσότερες πληροφορίες).

Λειτουργία του Κέντρου Επιχειρήσεων Κυβερνοασφάλειας (SOC) σε 24/7 Βάση

Ένα από τα σημαντικότερα επιτεύγματα της ΑΨΑ για το 2024 είναι η πλήρης επιχειρησιακή λειτουργία του Security Operations Center (SOC) σε 24ωρη βάση, 7 ημέρες την εβδομάδα. Η συνεχής λειτουργία του SOC ενισχύει την ικανότητα της Αρχής να παρακολουθεί, να εντοπίζει και να ανταποκρίνεται άμεσα σε κυβερνοαπειλές, διασφαλίζοντας την προστασία των κρίσιμων υποδομών της χώρας και ενισχύοντας τη συνολική κυβερνοανθεκτικότητα της Κυπριακής Δημοκρατίας.

Άσκηση Cyber Europe 2024

Η ΑΨΑ συντόνισε τη συμμετοχή της Κύπρου στην 7η Πανευρωπαϊκή Άσκηση Αντιμετώπισης Κρίσεων στον Κυβερνοχώρο «Cyber Europe 2024», η οποία πραγματοποιήθηκε με επιτυχία τον Ιούνιο του 2024 υπό την διοργάνωση του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA). Η άσκηση προώθησε τη συνεργασία μεταξύ διαφόρων οργανισμών, και ανέδειξε επίσης τους αναγκαίους τομείς βελτίωσης. (Βλέπε ενότητα 7.3 για περισσότερες πληροφορίες).

Άσκηση Cyber Cyprus 2024

Επιπρόσθετα, η Αρχή σε συνεργασία με το Υπουργείο Άμυνας και το Υφυπουργείο Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής, με την πλήρη υποστήριξη του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), διοργάνωσε την πρώτη εθνική άσκηση κυβερνοασφάλειας Cyber Cyprus 2024. Η πρωτοβουλία αυτή αποτέλεσε την πρώτη εθνικής εμβέλειας άσκηση επί χάρτου (τύπου tabletop), η οποία επικεντρώθηκε σε σενάριο επίθεσης λυτρισμικού (ransomware) στον τομέα των μεταφορών, δοκιμάζοντας τις ικανότητες απόκρισης κρίσιμων φορέων του δημόσιου και ιδιωτικού τομέα (Βλέπε ενότητα 7.3 για περισσότερες πληροφορίες).

Πρώτος χρόνος λειτουργίας της Ακαδημίας ICT

Η Ακαδημία ICT του Γραφείου Επιτρόπου Επικοινωνιών, στον μόλις πρώτο χρόνο λειτουργίας της, διοργάνωσε πληθώρα εθνικών και διεθνών συνεδρίων, ημερίδων, δημοσιογραφικών διασκέψεων, διαλέξεων, σεμιναρίων, εκπαιδεύσεων, εργαστηρίων και άλλων τελετών, διοργανώνοντας πάνω από 150 εκδηλώσεις με περισσότερους από 4.000 συμμετέχοντες, εγκαθιδρύοντας δυναμικά το ρόλο της ως εθνικό και περιφερειακό φορέα προώθησης της γνώσης και της τεχνολογικής καινοτομίας (βλέπε ενότητα 10 για περισσότερες πληροφορίες).

Ολοκλήρωση του ευρωπαϊκού έργου N4CY για τη σύσταση και τη λειτουργία του NCC-CY

Το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY), ξεκίνησε τις εργασίες του τον Ιανουάριο του 2023 μέσω του Ευρωπαϊκού Έργου N4CY (Development of the National Cybersecurity Coordination Centre of the Republic of CYprus), το οποίο συγχρηματοδοτήθηκε από το πρόγραμμα «Ψηφιακή Ευρώπη» και την Κυπριακή Δημοκρατία. Ο στόχος του έργου, το οποίο είχε συνολική διάρκεια δύο έτη, ήταν η σύσταση, η λειτουργία και η ανάπτυξη του NCC-CY. Μέσω του συγκεκριμένου έργου, η ΑΨΑ υλοποίησε σημαντικές δράσεις όπως η παροχή χορηγιών σε ΜμΕ, η δημιουργία της **κοινότητας κυβερνοασφάλειας**, η ανάπτυξη του **HelpDesk** για την υποστήριξη σε θέματα κυβερνοασφάλειας καθώς και πολυεπίπεδες **δράσεις εκπαίδευσης και ευαισθητοποίησης**. Το έργο N4CY στο οποίο συμμετείχε επίσης ως εταίρος το ΙδΕΚ ολοκληρώθηκε με επιτυχία στις 31 Δεκεμβρίου 2024.

Στα πλαίσια αυτά και σε συνεργασία με το ΙδΕΚ, η ΑΨΑ ολοκλήρωσε **σχέδιο χορηγιών** ύψους ενός εκατομμυρίου ΕΥΡΩ για **στήριξη των μικρομεσαίων επιχειρήσεων** της χώρας. Συνολικά επωφελήθηκαν 19 μικρομεσαίες επιχειρήσεις οι οποίες πιστοποιήθηκαν επίσης και με το πλαίσιο Κυβερνο-υγιεινής του NCC-CY (βλέπε ενότητα 9 για περισσότερες πληροφορίες).

Επιτυχής πρόταση 7.6 εκατομμυρίων Ευρώ για την περαιτέρω ανάπτυξη του NCC-CY

Ένα ακόμη σημαντικό ορόσημο για την ενίσχυση της κυβερνοασφάλειας αποτελεί η εξασφάλιση χρηματοδότησης ύψους 7.676.690 ευρώ μέσω του έργου N4CY2, το οποίο θα ξεκινήσει επίσημα την 1η Ιανουαρίου 2025. Συγχρηματοδοτούμενο από το πρόγραμμα “Ψηφιακή Ευρώπη” και την Κυπριακή Δημοκρατία, το έργο το οποίο εγκρίθηκε κατά το 2024, θέτει τις βάσεις για την περαιτέρω ανάπτυξη του NCC-CY και του οικοσυστήματος κυβερνοασφάλειας στην Κύπρο, μέσω στρατηγικών συνεργασιών, προγραμμάτων στήριξης μικρομεσαίων επιχειρήσεων και δράσεων ευαισθητοποίησης και εκπαίδευσης. Παράλληλα, περιλαμβάνει την ενίσχυση της Κοινότητας Κυβερνοασφάλειας και του Help Desk, το οποίο παρέχει υποστήριξη σε οργανισμούς, ΜμΕ και πολίτες για χρηματοδοτήσεις μέσω των προγραμμάτων DEP και HEP. Το έργο ολοκληρώνεται στις 31/12/2028.

3 ΟΡΑΜΑ, ΣΤΟΧΟΙ ΚΑΙ ΣΤΡΑΤΗΓΙΚΗ

Η Αρχή Ψηφιακής Ασφάλειας αποτελεί τον εθνικό φορέα υπεύθυνο για τον σχεδιασμό, τη ρύθμιση και την υλοποίηση της στρατηγικής κυβερνοασφάλειας της Κυπριακής Δημοκρατίας. Μέσα από ένα ολιστικό μοντέλο διοίκησης και δράσεων, η ΑΨΑ προωθεί ένα ασφαλές και ανθεκτικό ψηφιακό περιβάλλον, με στόχο την προστασία των κρίσιμων υποδομών, την ενδυνάμωση των εθνικών ικανοτήτων και την υποστήριξη της κοινωνίας και των επιχειρήσεων απέναντι στις σύγχρονες κυβερνοαπειλές.

3.1 Το Όραμα της Αρχής Ψηφιακής Ασφάλειας

Το όραμα της ΑΨΑ είναι όπως η Κύπρος καταστεί μια από τις πρωτοπόρες χώρες της περιοχής στα θέματα κυβερνοασφάλειας, για την προστασία των κρίσιμων υποδομών πληροφοριών του κράτους, των επιχειρήσεων και της κοινωνίας ευρύτερα, και τη δημιουργία ενός κατάλληλου και ελκυστικού περιβάλλοντος οικονομικής ανάπτυξης και προώθησης των υπηρεσιών στις οποίες η Κύπρος κατέχει υψηλή θέση παγκοσμίως.

3.2 Οι Στόχοι της Αρχής Ψηφιακής Ασφάλειας

Η Αρχή στοχεύει στη δημιουργία ενός ανθεκτικού και ασφαλούς ψηφιακού περιβάλλοντος μέσα από στοχευμένες δράσεις και στρατηγικές πρωτοβουλίες. Δίνοντας έμφαση στη συνεργασία, τη ρύθμιση, την εκπαίδευση και την ενίσχυση των κρίσιμων φορέων, ενισχύει την κυβερνοασφάλεια σε εθνικό επίπεδο. Παράλληλα, αναπτύσσει μακροπρόθεσμους στόχους που διασφαλίζουν τη συνεχή εξέλιξη και προσαρμογή στις νέες προκλήσεις του ψηφιακού κόσμου, διαμορφώνοντας ένα πλαίσιο που προστατεύει τόσο τις κρίσιμες υποδομές όσο και το σύνολο της κοινωνίας.

Η στρατηγική αυτή αποτυπώνεται μέσα από τους ακόλουθους βασικούς στόχους, οι οποίοι καθορίζουν τις προτεραιότητες και τις δράσεις της Αρχής:

Ανάπτυξη και Ενίσχυση Συνεργασιών με εμπλεκόμενους φορείς – Στόχος μας η δημιουργία ισχυρών και διαρκών σχέσεων με εμπλεκόμενους φορείς, όπως κρατικές υπηρεσίες, επιχειρήσεις και κοινωνία των πολιτών, για την αποτελεσματική αντιμετώπιση των προκλήσεων στην κυβερνοασφάλεια.

Εφαρμογή και ενίσχυση Νομικού, Κανονιστικού και Ρυθμιστικού Πλαισίου – Εφαρμόζουμε και ενισχύουμε το εποπτικό πλαίσιο για την κατάλληλη διαχείριση κινδύνων κυβερνοασφάλειας στις κρίσιμες υποδομές του τόπου, καθώς και την αποτροπή και την αντιμετώπιση κυβερνοαπειλών, με έμφαση στην συμμόρφωση με τους νόμους και τους κανονισμούς.

Ενδυνάμωση της Εθνικής Ικανότητας Κυβερνοασφάλειας – Αναπτύσσουμε και ενδυναμώνουμε τις ικανότητες της χώρας για την προστασία των κρίσιμων υποδομών και των πληροφοριακών συστημάτων.

Ενίσχυση της Ικανότητας των Κρίσιμων Φορέων – Παρέχουμε υποστήριξη προς τις κρίσιμες υποδομές της χώρας για την αναβάθμιση των ικανοτήτων τους στην κυβερνοασφάλεια, ώστε να αντιμετωπίζουν και να αντιδρούν αποτελεσματικά σε κυβερνοαπειλές.

Ασφάλεια για Όλους – Αναλαμβάνουμε πρωτοβουλίες που να συνεισφέρουν τα συμφέροντα όλων των πολιτών, επιχειρήσεων και φορέων.

Ανάπτυξη Ακαδημίας Πληροφορικής, Τεχνολογίας και Επικοινωνιών – Ενισχύουμε την Ακαδημία, όραμα της οποίας είναι να καταστεί ως ένα Περιφερειακό Κέντρο Εκπαίδευσης επαγγελματιών στον τομέα του Information and Communication Technology (ICT).

Μακροπρόθεσμοι Στόχοι - Χτίζοντας το αύριο στην ΑΨΑ – Επενδύουμε και σχεδιάζουμε το μέλλον μέσω του καθορισμού μακροπρόθεσμων στόχων που διασφαλίζουν την εξέλιξη τόσο της Αρχής όσο και της Εθνικής ασφάλειας.

Παροχή Υπηρεσιών Κυβερνοασφάλειας σε Περιφερειακό Επίπεδο - Σκοπός η δημιουργία ενός περιφερειακού κέντρου παροχής υπηρεσιών κυβερνοασφάλειας.

4 ΔΟΜΕΣ

Το Γραφείο Επιτρόπου Επικοινωνιών - ΑΨΑ αποτελεί τον βασικό φορέα διαχείρισης και ενίσχυσης της κυβερνοασφάλειας στην Κυπριακή Δημοκρατία, με δομές που καλύπτουν ρύθμιση, εποπτεία, πρόληψη και αντιμετώπιση κυβερνοαπειλών. Οι βασικές δομές που λειτουργούν υπό την ΑΨΑ είναι πέντε (5) και περιλαμβάνουν τον Τομέα Ρύθμισης, Στρατηγικής και Εποπτείας, το Εθνικό CSIRT-CY (SOC), την Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας (NCCA), το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY) και την Ακαδημία Τεχνολογίας, Πληροφοριών και Επικοινωνιών (ICT Academy).

4.1 Τομέας Ρύθμισης, Στρατηγικής και Εποπτείας

Ο Τομέας Ρύθμισης, Στρατηγικής και Εποπτείας (ΡΣΕ) της ΑΨΑ είναι υπεύθυνος για την υλοποίηση της Οδηγίας NIS στην Κυπριακή Δημοκρατία, περιλαμβανομένου του συντονισμού της υλοποίησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας. Ως κύρια δραστηριότητα, προωθεί την επίτευξη υψηλού επίπεδου ασφάλειας δικτύων και συστημάτων πληροφοριών για διάφορους κρίσιμους φορείς και παροχείς στη χώρα, όπως Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, Φορείς Κρίσιμων Υποδομών Πληροφοριών, Παροχείς Δικτύων ή/και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών και Παροχείς Ψηφιακών Υπηρεσιών.

Ο Τομέας ΡΣΕ προσφέρει μια σειρά από υπηρεσίες, περιλαμβανομένων ρυθμιστικών πλαισίων για μέτρα ασφάλειας και την εποπτεία τους, αξιολογήσεις κρισιμότητας και κινδύνων, διαχείριση κοινοποιήσεων περιστατικών για σκοπούς συμμόρφωσης, και πρωτοβουλίες για ενίσχυση του επιπέδου κυβερνοασφάλειας σε δημόσιο και ιδιωτικό τομέα.

4.2 Εθνικό CSIRT- CY (Εθνική Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων)

Στο πλαίσιο της εφαρμογής της ευρωπαϊκής Οδηγίας NIS για την ασφάλεια δικτύων και πληροφοριακών συστημάτων, το Εθνικό CSIRT-CY αποτελεί κρίσιμο πυλώνα στην αρχιτεκτονική της κυβερνοασφάλειας, τόσο σε εθνικό όσο και σε διεθνές επίπεδο. Η αποστολή του, είναι η διασφάλιση της επιχειρησιακής συνέχειας και της ετοιμότητας απέναντι σε απειλές που ενδέχεται να επηρεάσουν τη λειτουργία ζωτικής σημασίας υποδομών (π.χ., ενέργειας), τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα, καθώς και τη γενικότερη κοινωνικοοικονομική δραστηριότητα της χώρας. Στόχος είναι η προστασία και η ταχεία απόκριση σε περιστατικά κυβαρνοασφάλειας, η ανταλλαγή πληροφοριών και η συνεργασία μεταξύ φορέων, ενισχύοντας τη συνολική ανθεκτικότητα του κυβερνοχώρου.

Η επιχειρησιακή του αποτελεσματικότητα ενισχύεται περαιτέρω μέσω της λειτουργίας του Κέντρου Επιχειρήσεων Κυβερνοασφάλειας (SOC) της ΑΨΑ, το οποίο από το 2024 λειτουργεί σε 24ωρη βάση, διασφαλίζοντας συνεχή επιτήρηση και δυνατότητα έγκυρης προειδοποίησης και άμεσης απόκρισης σε περιστατικά. Το Εθνικό SOC έχει διευρύνει την κάλυψη του με την εγκατάσταση 46 αισθητήρων που παρακολουθούν την κίνηση στο δίκτυο των κρίσιμων υποδομών και ανιχνεύουν για επιθέσεις. Παράλληλα αυτό προσφέρει μια πιο ολοκληρωμένη εικόνα για το πεδίο κυβερνοεπιθέσεων και το είδος των απειλών στην Κύπρο. Η ομάδα SOC έχει χειριστεί περισσότερο από 1100 κρίσιμες ειδοποιήσεις κινδύνου το 2024.

Το Εθνικό CSIRT-CY παρέχει μεταξύ άλλων τις ακόλουθες υπηρεσίες πρόληψης και ανταπόκρισης:

- Συστήματα έγκαιρης προειδοποίησης βάσει ανίχνευσης ύποπτων δραστηριοτήτων σε πραγματικό χρόνο.
- Έγκαιρες ειδοποιήσεις ασφαλείας προς τους διαχειριστές συστημάτων των υποδομών, συνοδευόμενες από αναλυτικές οδηγίες για μέτρα μετριασμού, παραμετροποιήσεις και εναλλακτικές λύσεις αντιμετώπισης.
- Άμεση εφαρμογή πολιτικής διαχείρισης περιστατικών κυβερνοασφάλειας όταν ένα συμβάν εντοπιστεί ή βρίσκεται σε εξέλιξη εντός του οργανισμού.
- Παροχή υπηρεσιών διαχείρισης και ανάλυσης ψηφιακών τεκμηρίων μετά από σοβαρά περιστατικά ασφάλειας, στο πλαίσιο δικανικής έρευνας.

4.3 Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας (National Cybersecurity Certification Authority - NCCA)

Η ΑΨΑ έχει οριστεί από το Υπουργικό Συμβούλιο ως η Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας (ΕΑΠΚ) βάσει των απαιτήσεων του Κανονισμού (ΕΕ) 2019/881 που αφορά την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας, πληροφοριών και επικοινωνιών (ΤΠΕ). Η ΕΑΠΚ, ως εποπτική αρχή, μεριμνά για την εφαρμογή των κανόνων που περιλαμβάνονται στα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας των προϊόντων, υπηρεσιών και διαδικασιών ΤΠΕ, τόσο εντός αλλά και εκτός ΕΕ. Συγκεκριμένα, η ΕΑΠΚ εποπτεύει τους Οργανισμούς Αξιολόγησης Συμμόρφωσης (Conformity Assessment Bodies – CABs), οι οποίοι αποτελούνται από τους φορείς αξιολόγησης (Conformity Bodies - CBs) και τα τεχνικά εργαστήρια (ITSEFs) που διενεργούν τις τεχνικές αξιολογήσεις. Επιπρόσθετα, χειρίζεται τυχόν παράπονα που σχετίζονται με τους Οργανισμούς Αξιολόγησης Συμμόρφωσης, τα πιστοποιημένα προϊόντα, υπηρεσίες και διαδικασίες, τους κατασκευαστές και παρόχους υπηρεσιών. Είναι επίσης υπεύθυνη για την εξουσιοδότηση των Οργανισμών Αξιολόγησης Συμμόρφωσης, για την πιστοποίηση προϊόντων και υπηρεσιών στο «υψηλό» επίπεδο διασφάλισης, βάσει των Ευρωπαϊκών Σχημάτων Πιστοποίησης Κυβερνοασφάλειας (βλέπε ενότητα 12 για περισσότερες πληροφορίες). Παράλληλα, η ΕΑΠΚ αναμένεται να ασκεί και καθήκοντα αρμόδιας αρχής για τον Κανονισμό (ΕΕ) 2024/2847 «Cyber Resilience Act» (CRA), ο οποίος εισάγει οριζόντιες απαιτήσεις κυβερνοασφάλειας για όλα τα προϊόντα με ψηφιακά στοιχεία καθ' όλο τον κύκλο ζωής τους .Ο Κανονισμός «Cyber Resilience Act» τέθηκε σε ισχύ στις 10 Δεκεμβρίου 2024.

4.4 Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY)

Με τη θέσπιση του Ευρωπαϊκού Κανονισμού 2021/887 του Ευρωπαϊκού Κοινοβουλίου και του Ευρωπαϊκού Συμβουλίου της 20ης Μαΐου 2021, ιδρύθηκε το European Cybersecurity Competence Center - ECCC για Βιομηχανικά, Τεχνολογικά και Ερευνητικά θέματα Κυβερνοασφάλειας και το Δίκτυο, το οποίο αποτελείται από τα NCCs των κρατών μελών της ΕΕ και της Ευρωπαϊκής Ζώνης Ελεύθερων Συναλλαγών (ΕΖΕΣ/EFTA).

Την 21η Δεκεμβρίου 2021, με απόφαση του Υπουργικού Συμβουλίου η ΑΨΑ, οντότητα του ευρύτερου δημόσιου τομέα, ορίστηκε ως το NCC-CY στην Κυπριακή Δημοκρατία, καθιστώντας την Κύπρο μια από τις πρώτες 5 χώρες που ίδρυσαν και στελέχωσαν το NCC τους.

Το NCC-CY συστάθηκε μέσω του Ευρωπαϊκού Προγράμματος N4CY, το οποίο συγχρηματοδοτήθηκε από το πρόγραμμα Ψηφιακή Ευρώπη και την Κυπριακή Δημοκρατία, με στόχο την ενίσχυση της κυβερνοασφάλειας στη χώρα. Στο πλαίσιο αυτό, έχει δρομολογήσει πολυδιάστατες δράσεις, μεταξύ των οποίων περιλαμβάνεται η παροχή σχεδίου χορηγιών προς τρίτους, σε συνεργασία με το Ίδρυμα Έρευνας και Καινοτομίας - ΙΔΕΚ. Παράλληλα, δημιούργησε και ενισχύει συνεχώς την Κυπριακή Κοινότητα Κυβερνοασφάλειας, στην οποία συμμετέχουν οντότητες από τον ιδιωτικό και δημόσιο τομέα, τη βιομηχανία και την ακαδημαϊκή κοινότητα. Στόχος της κοινότητας είναι η συνεργασία, η ανταλλαγή γνώσης και η προώθηση ερευνητικών και εκπαιδευτικών προγραμμάτων. Μια ακόμα σημαντική πρωτοβουλία του NCC-CY είναι η ανάπτυξη πιστοποιήσεων όπως παραδείγματος χάριν το Πλαίσιο Κυβερνο-Υγιεινής, το οποίο λειτουργεί ως σύστημα πιστοποίησης και εφαρμογής βασικών μέτρων ασφάλειας για Μικρομεσαίες Επιχειρήσεις - ΜμΕ βοηθώντας να ανταποκριθούν στις προκλήσεις της ψηφιακής εποχής, ενώ παρέχει και υποστήριξη μέσω του Help Desk του σε οργανισμούς, μικρομεσαίες επιχειρήσεις και πολίτες για συμμετοχή σε προγράμματα DEP & HEP.

4.5 Ακαδημία Πληροφορικής, Τεχνολογίας και Επικοινωνιών

Ιδρυμένη τον Δεκέμβριο του 2023 και πιστοποιημένη από την Αρχή Ανάπτυξης Ανθρώπινου Δυναμικού, η Ακαδημία ICT αποτελεί πρότυπη Δομή Επαγγελματικής Κατάρτισης. Μέσω της Ακαδημίας εκπαιδεύονται επαγγελματίες στον τομέα της τεχνολογίας, προωθώντας την καινοτομία και την ανάπτυξη. Η εκπαίδευση που προσφέρεται συνδυάζει θεωρητική γνώση και πρακτική εφαρμογή, προετοιμάζοντας τους συμμετέχοντες να αντιμετωπίσουν τις τεχνολογικές προκλήσεις του μέλλοντος και να εισέλθουν δυναμικά στην αγορά εργασίας. Η Ακαδημία επενδύει στην έρευνα και την καινοτομία, διαμορφώνοντας ισχυρές συνεργασίες με τη βιομηχανία και ενισχύοντας έτσι τη σύνδεση της εκπαίδευσης με τις πραγματικές ανάγκες της αγοράς.

4.6 Στελέχωση και άλλες οριζόντιες δομές

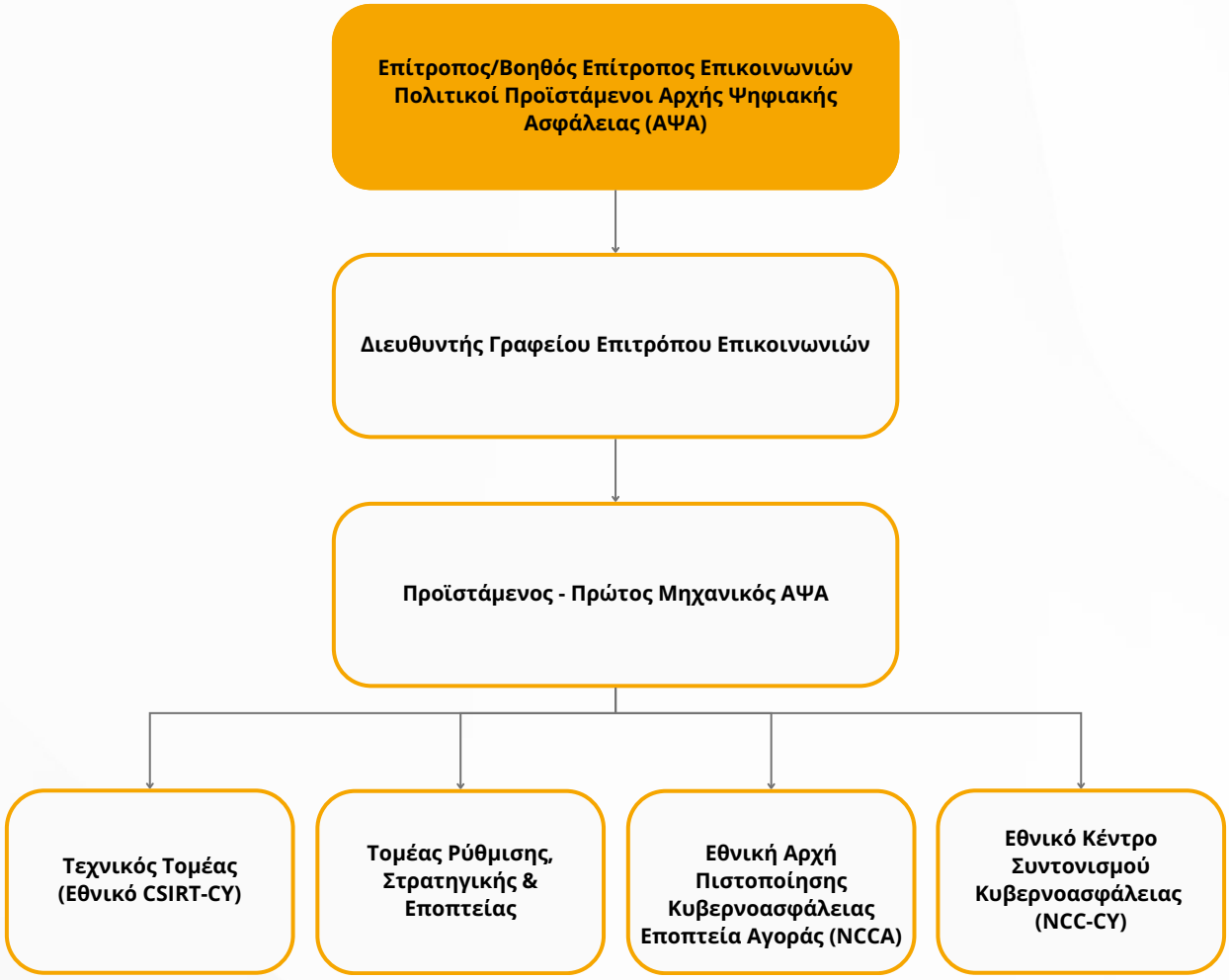
Τα μόνιμα στελέχη της ΑΨΑ για το έτος 2024 περιλαμβάνουν τον Προϊστάμενο, Νομικούς Λειτουργούς, Ανώτερους Μηχανικούς Ψηφιακής Ασφάλειας και Μηχανικούς Ψηφιακής Ασφάλειας.

Για να μπορέσει να καλύψει τις ανάγκες, κατά τη διάρκεια του 2024, η Αρχή απασχολούσε επιπλέον συνεργάτες παροχής υπηρεσιών, για την υποστήριξη της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας, του Εθνικού Κέντρου Συντονισμού Κυβερνοασφάλειας, της Ακαδημίας Πληροφορικής, Τεχνολογίας και Επικοινωνιών, καθώς και άλλων οριζόντιων δομών όπως αυτών της Γραμματειακής Υποστήριξης, του τμήματος Πληροφορικής, του Λογιστηρίου, του τμήματος Προσφορών καθώς και αυτών που απασχολούνταν στις δομές που αφορούν τη διαχείριση Έργων και Ευρωπαϊκών Προγραμμάτων.

Το 2024, λειτούργησε επίσης πλήρως, το σύστημα 24ωρης βάρδιας του Εθνικού CSIRT, για την αντιμετώπιση περιστατικών (Duty Officers) καθώς και για την παρακολούθηση των αισθητήρων που είναι τοποθετημένοι στις κρίσιμες υποδομές της Δημοκρατίας (Σύστημα Έγκαιρης Προειδοποίησης - Early Warning System).

Στο μεσοδιάστημα η ΑΨΑ προωθεί πρόταση για τη δημιουργία ενός σημαντικού αριθμού επιπλέον μόνιμων θέσεων εργασίας τα επόμενα χρόνια, με στόχο την κάλυψη των αναγκών της που αποσκοπούν στη συνεχιζόμενη ενίσχυση και βελτίωση των επιπέδων κυβερνοασφάλειας στην Κυπριακή Δημοκρατία.

Η οργανωτική δομή της ΑΨΑ για το 2024 απεικονίζεται στο παρακάτω γράφημα.



5 ΑΝΑΠΤΥΞΗ ΚΑΙ ΕΝΙΣΧΥΣΗ ΣΥΝΕΡΓΑΣΙΩΝ ΜΕ ΕΜΠΛΕΚΟΜΕΝΟΥΣ ΦΟΡΕΙΣ

Η Αρχή Ψηφιακής Ασφάλειας δίνει ιδιαίτερη έμφαση στη συνεργασία με εθνικούς, ευρωπαϊκούς και διεθνείς φορείς, αναγνωρίζοντας ότι η κυβερνοασφάλεια αποτελεί συλλογική ευθύνη και απαιτεί συντονισμένες δράσεις. Στο πλαίσιο αυτό, το 2024 χαρακτηρίστηκε από ενεργή εμπλοκή σε διεθνείς οργανισμούς μέσω της συμμετοχής της Αρχής σε συναντήσεις και συνεδρίες, καθώς και από τη σύναψη ή/και την ενίσχυση συνεργασιών με κρατικούς, ευρωπαϊκούς και άλλους διεθνείς οργανισμούς.

5.1 Συνεργασία με Κρατικούς Αρμόδιους Φορείς

Η συνεργασία με κρατικούς αρμόδιους φορείς, είναι ζωτικής σημασίας για την ΑΨΑ και αποσκοπεί μεταξύ άλλων, στην ανταλλαγή κρίσιμων πληροφοριών, την αντιμετώπιση κυβερνοαπειλών και την εφαρμογή βέλτιστων πρακτικών στον τομέα της ψηφιακής προστασίας της χώρας.

Ίδρυμα Έρευνας και Καινοτομίας (ΙΔΕΚ)

Μέσω της ήδη αγαστής συνεργασίας, η ΑΨΑ και το ΙΔΕΚ εργάζονται από κοινού με στόχο την ενίσχυση της έρευνας, της καινοτομίας και γενικότερα της ανάπτυξης του τομέα της κυβερνοασφάλειας. Κατά το 2024 διαχειρίστηκαν από κοινού το πρώτο πιλοτικό σχέδιο χορηγιών για την ενίσχυση της κυβερνοασφάλειας στις κυπριακές ΜμΕ, με προϋπολογισμό 1.000.000 ευρώ. Το πρόγραμμα, το οποίο υλοποιήθηκε στο πλαίσιο του έργου N4CY και συγχρηματοδοτήθηκε από την Κυπριακή Δημοκρατία και το πρόγραμμα «Ψηφιακή Ευρώπη» της ΕΕ, ολοκληρώθηκε επιτυχώς στις 31 Ιανουαρίου 2024 (Βλέπε ενότητα 9.3 για περισσότερες πληροφορίες).

Ανοικτό Πανεπιστήμιο Κύπρου

Επιπλέον, η Αρχή Ψηφιακής Ασφάλειας διατηρεί στενή συνεργασία με το Ανοικτό Πανεπιστήμιο Κύπρου, με στόχο την προώθηση της κυβερνοασφάλειας μέσω τεχνολογικών και εκπαιδευτικών πρωτοβουλιών. Κατά το έτος 2024, η συνεργασία επικεντρώθηκε στην από κοινού ανάπτυξη και εφαρμογή προηγμένων μηχανισμών ανίχνευσης και απόκρισης σε κυβερνοαπειλές. Ενδεικτικά παραδείγματα αποτελούν η ανάπτυξη και επιχειρησιακή ενσωμάτωση συστημάτων ανίχνευσης δικτυακών εισβολών (NIDS), καθώς και η αξιοποίηση λύσεων Endpoint Detection & Response (EDR). Παράλληλα, υλοποιήθηκαν στοχευμένα προγράμματα κατάρτισης και ασκήσεις προσομοίωσης μέσω πλατφορμών τύπου Cyber Range, με σκοπό την ενίσχυση της κυβερνοανθεκτικότητας. Η εν λόγω συνεργασία διευρύνθηκε περαιτέρω με τη συντονισμένη συμμετοχή σε ευρωπαϊκά ερευνητικά έργα, όπως τα «ATHENA», «CY-TRUST» και «SecawarenessTruss», συμβάλλοντας καθοριστικά στην ανάπτυξη καινοτόμων, επιστημονικά τεκμηριωμένων λύσεων στον τομέα της κυβερνοασφάλειας.

Πανεπιστήμιο Κύπρου

Παράλληλα, στο πλαίσιο της συνεργασίας της Αρχής με το Πανεπιστήμιο Κύπρου, έγινε ο σχεδιασμός, η υλοποίηση και η συντήρηση της πλατφόρμας CY-MAP Analyzer. Αυτή η τεχνολογική λύση εκτελεί παθητική σάρωση του προσβάσιμου εθνικού διαδικτυακού χώρου της Κυπριακής Δημοκρατίας για την ανίχνευση ευπαθειών, εντοπίζει μολυσμένα συστήματα, και εποπτεύει τα πρωτόκολλα επικοινωνίας και την ασφάλειά τους. Η εν λόγω συνεργασία ευθυγραμμίζεται και ενισχύει τη Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας.

Κυπριακός Οργανισμός Προώθησης Ποιότητας (ΚΟΠΠ)

Επίσης, η ΑΨΑ ως ΕΑΠΚ εδραιώνει στενές συνεργασίες με κρατικούς φορείς, προκειμένου να διασφαλιστεί η ομογενοποίηση και η εφαρμογή των κανονισμών και οδηγιών που αφορούν την πιστοποίηση της κυβερνοασφάλειας. Στο πλαίσιο αυτό συμπεριλαμβάνεται η υποστήριξη και η συνεργασία με τον Κυπριακό Οργανισμό Προώθησης Ποιότητας, ως ο Εθνικός Οργανισμός Διαπίστευσης, για την παρακολούθηση και την εποπτεία των δραστηριοτήτων των οργανισμών αξιολόγησης της συμμόρφωσης.

Κυπριακός Οργανισμός Τυποποίησης (CYS)

Το ήδη υπάρχον μνημόνιο Συνεργασίας μεταξύ της ΑΨΑ και του Κυπριακού Οργανισμού Τυποποίησης (CYS) αφορά τη δημιουργία μοντέλου αξιολόγησης ωριμότητας δυνατοτήτων και πλαισίου ελέγχου (Capability Maturity Assessment and Audit Framework). Κατά το έτος 2024, πραγματοποιήθηκε το έργο υλοποίησης του Μοντέλου Ωριμότητας Κυβερνοασφάλειας (CMAAF) και η Δημιουργία Πλαισίου Ελεγκτών, το οποίο οδήγησε στην επιτυχή ολοκλήρωση και δημοσίευση της Απόφασης ΚΔΠ 245/2024 (για περισσότερες πληροφορίες βλέπε ενότητα 6.3 & 6.4).

Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Το Μνημόνιο Συνεργασίας μεταξύ του Γραφείου Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΕΠΔΠΧ) και του Γραφείου Επιτρόπου Επικοινωνιών (ΕΕ) έχει ως σκοπό τον καθορισμό πλαισίου διαδικασίας, υιοθέτησης και εφαρμογής κατάλληλων μηχανισμών για την αποδοτικότερη και αποτελεσματικότερη συνεργασία των δύο Επιτρόπων (ΕΕ και ΕΠΔΠΧ) κατά την παραλαβή ή/και λήψη ή/και διεκπεραίωση:

- Περιπτώσεων γνωστοποίησης παραβίασης προσωπικών δεδομένων από τους παροχείς δημόσια διαθέσιμων Υπηρεσιών Ηλεκτρονικών Επικοινωνιών κατ' εφαρμογή του Νόμου 112(I)/2004[1], και
- Περιπτώσεων συμβάντων από φορείς εκμετάλλευσης βασικών υπηρεσιών, φορείς κρίσιμων υποδομών και παροχείς ψηφιακών υπηρεσιών που οδηγούν σε παραβιάσεις προσωπικών δεδομένων, κατ' εφαρμογή του Νόμου 89(I)/2020[2].

Εντός του 2024 υπήρξαν συνέργειες όπως συχνή ανταλλαγή πληροφοριών, στα πλαίσια της εφαρμογής του περί της Γνωστοποίησης Παραβιάσεων Προσωπικών Δεδομένων από τους παροχείς δημόσια διαθέσιμων υπηρεσιών Ηλεκτρονικών Επικοινωνιών Διάταγμα, Κ.Δ.Π. 190/2015 και του περί Ασφάλειας Δικτύων Συστημάτων και Πληροφοριών Νόμου 89(I)/2020.

Εθνική Αρχή Στοιχημάτων

Επιπρόσθετα το 2024, και με βάση τα όσα καθορίζονται σε σχετικό Μνημόνιο Συνεργασίας με την Εθνική Αρχή Στοιχημάτων, έγιναν συντονισμένες ενέργειες για τη διασύνδεση της Αρχής με το Εθνικό SOC, για την καλύτερη προστασία και αντιμετώπιση κυβερνοεπιθέσεων. Επίσης, η εν λόγω συνεργασία περιλαμβάνει τις απαραίτητες ενέργειες για τη συντήρηση και εύρυθμη λειτουργία του δικτύου, ενισχύοντας έτσι την αποτελεσματικότητα του μηχανισμού έγκαιρης ανίχνευσης και απόκρισης σε περιστατικά κυβερνοασφάλειας.

Αστυνομία Κύπρου

Η Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) διατήρησε και κατά το 2024 θεσμοθετημένη και τακτική συνεργασία με την Αστυνομία, με στόχο την ανταλλαγή κρίσιμων πληροφοριών που αφορούν κυβερνοεπιθέσεις και λοιπές απειλές στον κυβερνοχώρο. Η συνεργασία αυτή συμβάλλει στην άμεση ενημέρωση, στην αμοιβαία υποστήριξη και στη συντονισμένη διαχείριση περιστατικών που ενδέχεται να επηρεάσουν την ασφάλεια των ψηφιακών υποδομών της χώρας.

Συγκεκριμένα, στο πλαίσιο της εθνικής άσκησης «CYBER CYPRUS 2024», η οποία διοργανώθηκε από την Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) υπό την καθοδήγηση του ευρωπαϊκού οργανισμού ENISA, η συμμετοχή της Υποδιεύθυνσης Ηλεκτρονικού Εγκλήματος (ΥΗΕ) της Αστυνομίας Κύπρου, σε συνεργασία με την ΑΨΑ, υπήρξε καθοριστικής σημασίας για την επιτυχή υλοποίηση του σεναρίου. Η ενεργή εμπλοκή της ΥΗΕ σε κρίσιμες φάσεις της άσκησης ανέδειξε σημεία βελτίωσης στις διαδικασίες επικοινωνίας μεταξύ των εμπλεκομένων φορέων, προσφέροντας ουσιαστική ευκαιρία για την αναθεώρηση και βελτίωση των επιχειρησιακών διαδικασιών. Η επιτυχία της συνεργασίας αυτής εντοπίζεται κυρίως στην εξάλειψη μη αποδοτικών μηχανισμών, στη βελτίωση της διαλειτουργικότητας και στην ενίσχυση της μεταξύ τους επικοινωνίας, γεγονός που συνέβαλε στην ταχύτερη απόκριση και αποτελεσματικότερη διαχείριση πληροφοριών σε περιόδους κρίσης, ενισχύοντας τη συνολική ετοιμότητα και ανθεκτικότητα του εθνικού μηχανισμού κυβερνοασφάλειας.

Υφυπουργείο Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής

Κατά το 2024, συνεχίστηκε επίσης η στενή συνεργασία της ΑΨΑ με το Υφυπουργείο Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής (ΥΕΚΨΠ), εστιάζοντας στην ανταλλαγή τεχνικής πληροφόρησης και στην ανάπτυξη κοινών μηχανισμών διαχείρισης κυβερνοπεριστατικών. Η συνεργασία αυτή ενισχύει την ανθεκτικότητα της χώρας έναντι ψηφιακών απειλών και προωθεί την υλοποίηση εθνικών στρατηγικών για την κυβερνοασφάλει, χαράζοντας παράλληλα την πολιτική του κράτους.

Εθνική Φρουρά

Παράλληλα, η ΑΨΑ διατήρησε και ενίσχυσε κατά το 2024 τη στρατηγικής σημασίας συνεργασία της με την Εθνική Φρουρά, συμμετέχοντας σε ασκήσεις κυβερνοασφάλειας τύπου Cyber Range και Cyber Drills. Επιπλέον, μέσω κοινών εξειδικευμένων προγραμμάτων εκπαίδευσης, ενισχύθηκε περαιτέρω η επιχειρησιακή ετοιμότητα και η διαλειτουργικότητα των εμπλεκόμενων φορέων στον τομέα της άμυνας του κυβερνοχώρου.

5.2 Ενίσχυση της συνεργασίας μεταξύ διεθνών – Ευρωπαϊκών ενδιαφερόμενων μερών

Η διεθνής συνεργασία στον τομέα της κυβερνοασφάλειας αποτελεί ακρογωνιαίο λίθο για την προστασία των κρίσιμων υποδομών, των επιχειρήσεων και γενικότερα της κοινωνίας. Η Αρχή Ψηφιακής Ασφάλειας, μέσω της διασύνδεσής της με διεθνείς και ευρωπαϊκούς οργανισμούς, συμβάλλει στην ενδυνάμωση της κυβερνοάμυνας, αξιοποιώντας εξειδικευμένη τεχνογνωσία και τεχνολογικές καινοτομίες. Παράλληλα, η ανταλλαγή πληροφοριών και η συμμετοχή σε διεθνή δίκτυα κυβερνοασφάλειας επιταχύνει την ανάπτυξη προηγμένων εργαλείων προστασίας και τη διαμόρφωση αποτελεσματικών ρυθμιστικών πλαισίων.

Κατά το έτος 2024, η ΑΨΑ διατήρησε ενεργό και ουσιαστικό ρόλο σε μια σειρά ευρωπαϊκών θεσμικών οργάνων και ομάδων συνεργασίας, συμβάλλοντας καθοριστικά στη χάραξη πολιτικής, την ανταλλαγή τεχνογνωσίας και την ενίσχυση της ψηφιακής ασφάλειας σε ευρωπαϊκό επίπεδο.

Στο πλαίσιο της συμμετοχής της στο **NIS Cooperation Group**, η Αρχή έλαβε μέρος τόσο στις ολομέλειες όσο και στις επιμέρους θεματικές ομάδες εργασίας. Η συμβολή της ήταν συνεχής και τεκμηριωμένη στις ομάδες που επικεντρώνονται στη διαχείριση κινδύνων και ευπαθειών, την αναφορά περιστατικών, την εποπτεία, τις εκλογικές διαδικασίες, την ενεργειακή ασφάλεια, τις αξιολογήσεις ομοτίμων (peer reviews) και τις εθνικές στρατηγικές κυβερνοασφάλειας (National Cybersecurity Strategies - NCSs). Επιπλέον, υπήρξε δραστήρια παρουσία στις ομάδες για τις υποδομές και παρόχους ψηφιακών υπηρεσιών, την κυβερνοασφάλεια των δικτύων 5G και τηλεπικοινωνιών, τον τομέα της υγείας, της αεροπλοΐας, καθώς και την ασφάλεια της εφοδιαστικής αλυσίδας.

Εκπροσωπώντας την Κύπρο, η ΑΨΑ συμμετείχε ενεργά και στο Management Board του ENISA, λαμβάνοντας μέρος σε όλες τις συνεδριάσεις που πραγματοποιήθηκαν κατά το 2024. Η Αρχή διατηρεί επίσης τον ρόλο του Εθνικού Συνδέσμου (NLO) με τον ENISA, με συμμετοχή σε δράσεις και συντονισμό σε εθνικό επίπεδο για την υλοποίηση των στρατηγικών του ENISA.

Παράλληλα, η Αρχή συνέχισε τη συστηματική της παρουσία στο **ECASEC**, το φόρουμ αρμόδιων εθνικών αρχών για την ασφάλεια των ηλεκτρονικών επικοινωνιών, προάγοντας την ευθυγράμμιση των εθνικών πρακτικών με το ευρωπαϊκό πλαίσιο.

Στον τομέα της διαχείρισης κρίσεων, η Αρχή Ψηφιακής Ασφάλειας συμμετείχε ενεργά στο **CyCLONe**, το δίκτυο συνδέσμων για την αντιμετώπιση κυβερνοκρίσεων, συνδράμοντας στην ανάπτυξη κοινών διαδικασιών απόκρισης και επικοινωνίας σε επίπεδο Ευρωπαϊκής Ένωσης. Συμμετείχε επίσης στις ομάδες εργασίας για ασκήσεις (**WG Exercises**), συμβάλλοντας στον σχεδιασμό και την υλοποίηση πανευρωπαϊκών ασκήσεων ετοιμότητας.

Επιπλέον, η ΑΨΑ υποστήριξε με τεκμηριωμένες παρεμβάσεις την ανάπτυξη του **EU Cybersecurity Index**, ενισχύοντας τη διαφάνεια και τη συγκρισιμότητα των εθνικών επιδόσεων στον τομέα της κυβερνοασφάλειας.

Στο πλαίσιο των δράσεων ευαισθητοποίησης, η Αρχή συμμετείχε δυναμικά και στις σχετικές επιτροπές που ασχολούνται με τον **Ευρωπαϊκό Μήνα Κυβερνοασφάλειας (ECSM)**, οργανώνοντας και προωθώντας με τη σειρά της εκστρατείες ενημέρωσης της κοινωνίας σε εθνικό επίπεδο.

Επιπρόσθετα, η Αρχή διατήρησε παρουσία και στο **European Security and Defence College (ESDC)**, ενισχύοντας τη συνεργασία μεταξύ φορέων ασφάλειας και άμυνας στον ψηφιακό τομέα μέσω εκπαιδευτικών και ενημερωτικών δραστηριοτήτων.

Η ΑΨΑ είναι επίσης μέλος του Governing Board του **ECCC** το οποίο εδρεύει στο Βουκουρέστι και στοχεύει στην ενίσχυση των δυνατοτήτων και της ανταγωνιστικότητας της Ευρώπης στον τομέα της κυβερνοασφάλειας. Συνεργαζόμενο με το **Δίκτυο Εθνικών Κέντρων Συντονισμού (NCCs)** σε κάθε χώρα Κράτος Μέλος, στοχεύει στη δημιουργία μιας ισχυρής Κοινότητας Κυβερνοασφάλειας, αποτελώντας το νέο ευρωπαϊκό πλαίσιο στήριξης της καινοτομίας και της βιομηχανικής πολιτικής. Στα πλαίσια αυτά, η ΑΨΑ συμμετείχε ενεργά και στις 3 επίσημες συνεδριάσεις του **Governing Board (GB)** του ECCC που πραγματοποιήθηκαν κατά το 2024, καθώς και στις 7 ομάδες εργασίας (Working Groups) του Κέντρου.

Μέσω της ενεργής συμμετοχής σε 7 ομάδες εργασίας του ECCC, η Αρχή μπόρεσε να συμβάλει στην ανάπτυξη της στρατηγικής ατζέντας του **European Cybersecurity Competence Centre** και να καταθέσει πολυάριθμες προτάσεις σχετικά με τα θέματα που άπτονται των αρμοδιοτήτων του.

Παράλληλα, πραγματοποιήθηκαν πέραν των 15 συναντήσεων με άλλα **Εθνικά Κέντρα Συντονισμού Κυβερνοασφάλειας** που αποσκοπούσαν στην προώθηση εθνικών και ευρωπαϊκών πρωτοβουλιών.

Την αφοσίωση της ΑΨΑ προς τη στήριξη και την ενίσχυση του ECCC αντικατοπτρίζουν επίσης οι συμμετοχές της Αρχής σε δύο ημερίδες ενημέρωσης (info days) για νέες προσκλήσεις χρηματοδότησης του προγράμματος "Ψηφιακή Ευρώπη" σε Βουκουρέστι και Βρυξέλλες αντίστοιχα.

Κατά το 2024 ξεκίνησε επίσης η διαδικασία διαβούλευσης για την κατάρτιση μνημονίου συνεργασίας μεταξύ της Αρχής Ψηφιακής Ασφάλειας και της αντίστοιχης ρυθμιστικής Αρχής της Αλβανίας **(NSCA)**. Σκοπός της πρωτοβουλίας είναι η ενίσχυση της διακρατικής συνεργασίας στους τομείς της κυβερνοασφάλειας, της ανταλλαγής τεχνογνωσίας και βέλτιστων πρακτικών, καθώς και της ταχείας ανταπόκρισης σε διασυνοριακά περιστατικά ασφάλειας στον κυβερνοχώρο. Μέσω του μνημονίου, επιδιώκεται η θέσπιση ενός πλαισίου αμοιβαίας υποστήριξης και επικοινωνίας, το οποίο θα συμβάλει στην προστασία κρίσιμων ψηφιακών υποδομών και στη διαμόρφωση κοινών προτύπων ασφάλειας. Η διαβούλευση περιλαμβάνει τεχνικές, νομικές και διοικητικές πτυχές, με στόχο την επίτευξη ενός ολοκληρωμένου και λειτουργικού συμφωνητικού πλαισίου.

Εντός του έτους 2024 συνεχίστηκαν οι συνεργασίες κάτω από τα Μνημόνια Συνεργασίας που διαχειρίζεται η ΑΨΑ εκ μέρους της Κυπριακής Δημοκρατίας, με τρίτες χώρες (π.χ. Πολωνία, Ηνωμένα Αραβικά Εμιράτα, Σερβία, Ρουμανία, Μάλτα), οι διερευνητικές επαφές για ανάπτυξη συνεργασιών με χώρες εντός και εκτός της Ευρωπαϊκής Ένωσης, καθώς και την ανταλλαγή πληροφοριών και αλληλοβοήθειας, όπου εφαρμόζεται.

Συμπληρωματικά των πιο πάνω, η ΑΨΑ συμμετείχε ενεργά σε διεθνείς και πανευρωπαϊκές εκδηλώσεις με στόχο την ενημέρωση, την ευαισθητοποίηση, την ανταλλαγή γνώσεων και την ενθάρρυνση συμμετοχής σε ευρωπαϊκά έργα του τομέα της κυβερνοασφάλειας (βλέπε ενότητα 9.2 για περισσότερες πληροφορίες).

Συμμετοχή σε Ομάδες Εργασίας (WGs) του ECCC

Η Αρχή Ψηφιακής Ασφάλειας είναι επίσης ενεργό μέλος στις επτά ακόλουθες ομάδες εργασίας του ECCC: WG1: Evolution and Security Clearance questions, WG2: NCC Network Governance and Community animation, WG3: NCC Network functioning , WG4: Strategic Agenda ,WG5: Cyber Skills (Awareness), WG6: Collaboration with Ukraine, και WG7: SOCs. Κατά το 2024, η ΑΨΑ έλαβε μέρος σε δεκαεννέα (19) σχετικές συναντήσεις με επίκεντρο τις πιο πάνω θεματικές.

Συμμετοχή σε WGs του ECSO

Εξίσου σημαντική είναι η συμμετοχή της ΑΨΑ και σε 2 ομάδες εργασίας του ECSO (European Cybersecurity Organisation) και συγκεκριμένα στο 1) WG2 - Trusted Supply Chains και 2) WG5 - Skills & Human Factors – Road2Cyber. Ο ECSO είναι ένας μη κερδοσκοπικός οργανισμός που ενισχύει το οικοσύστημα κυβερνοασφάλειας της Ευρώπης, προωθώντας τη συνεργασία μεταξύ του δημόσιου και ιδιωτικού τομέα για την ενίσχυση της ψηφιακής ανθεκτικότητας.

ECCG (European Cybersecurity Certification Group)

Η Αρχή επιδιώκει και προωθεί επίσης την ενεργή συνεργασία με άλλες Εθνικές Αρχές Πιστοποίησης Κυβερνοασφάλειας τόσο των Κρατών Μελών της ΕΕ όσο και τρίτων χωρών, και ενισχύει την εκπροσώπηση της Κύπρου μέσω της συμμετοχής της σε ευρωπαϊκές επιτροπές και ανάλογες ομάδες εργασίας. Η συμμετοχή της ΑΨΑ στο ECCG, συμβάλλει στον καθορισμό πολιτικών πιστοποίησης και τεχνικών οδηγιών, ενώ μέσω της στενής συνεργασίας με εμπειρογνώμονες και ρυθμιστικούς φορείς, προάγει την ανταλλαγή βέλτιστων πρακτικών, διασφαλίζοντας την αποτελεσματικότητα και την επικαιρότητα των διαδικασιών πιστοποίησης.

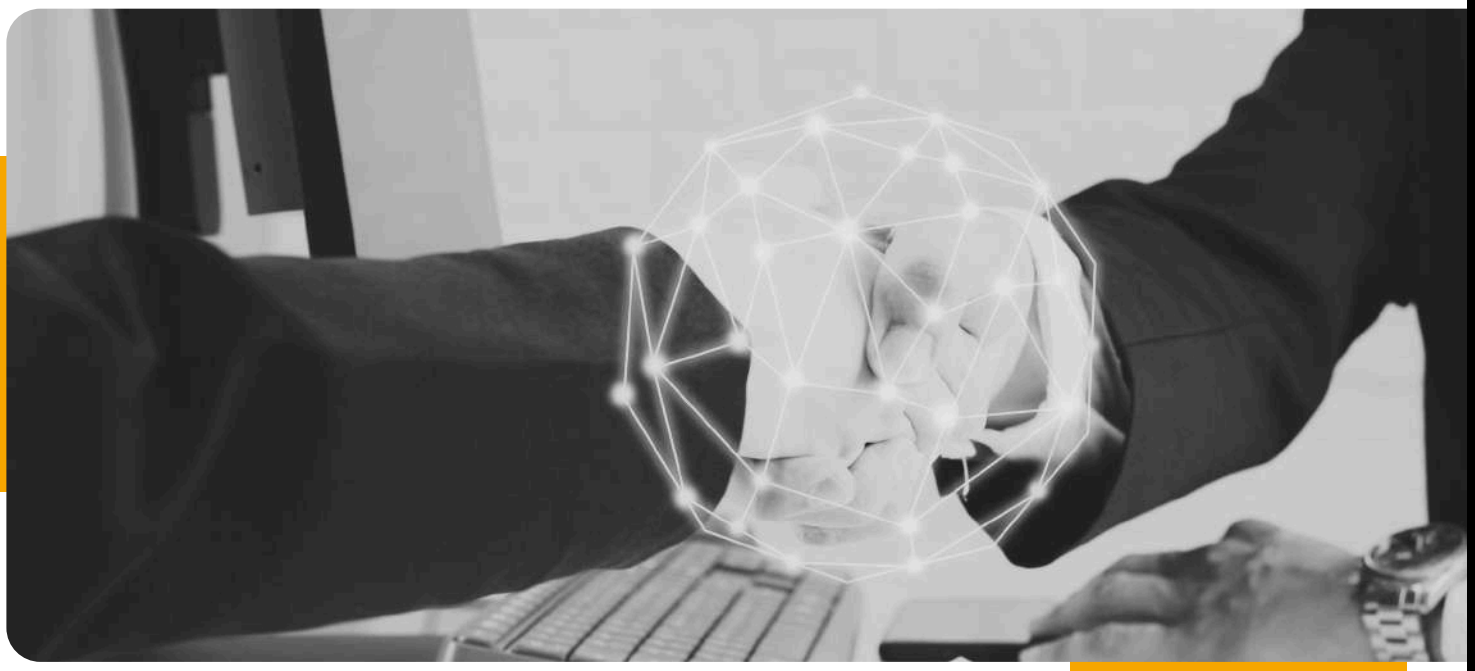
ENISA - Working Groups

Συνεχίζοντας, η ΑΨΑ ως ΕΑΠΚ συμμετέχει στις ομάδες εργασίας του ENISA οι οποίες υποστηρίζουν την προετοιμασία και την ανάπτυξη υποψήφιων σχημάτων πιστοποίησης κυβερνοασφάλειας. Η Αρχή διαδραματίζει σημαντικό ρόλο στις ομάδες εργασίας αφού συνεισφέρει τεχνική εμπειρογνωμοσύνη στη σύνταξη των σχημάτων, όπως επίσης και στην αξιολόγηση και επικύρωσή τους. Απώτερος στόχος είναι η διασφάλιση και εφαρμογή εναρμονισμένων σχημάτων μεταξύ των κρατών μελών.

5.3 Συνεργασία με κρίσιμες υποδομές

Αναντίλεκτα, η συνεργασία της Αρχής Ψηφιακής Ασφάλειας με τις κρίσιμες υποδομές αποτελεί πρωταρχικό πυλώνα για τη διασφάλιση της ανθεκτικότητας και της λειτουργικότητας ζωτικών τομέων της χώρας. Τομείς όπως η ενέργεια, οι μεταφορές, η υγεία και οι τηλεπικοινωνίες, είναι θεμελιώδεις για την εύρυθμη λειτουργία του κράτους και επομένως αποτελούν πρωταρχικούς στόχους κυβερνοαπειλών. Μέσω της στενής συνεργασίας, ενισχύεται η δυνατότητα πρόληψης και αντιμετώπισης κυβερνοεπιθέσεων, ενώ προωθείται η ανταλλαγή πληροφοριών και η εφαρμογή κοινών πρακτικών ασφαλείας.

Στα πλαίσια της συνεχόμενης βελτίωσης της επικοινωνίας της ΑΨΑ με τις κρίσιμες υποδομές, κατά το 2024 ορίστηκαν σύνδεσμοι επικοινωνίας (account managers) εκ μέρους του Τομέα Ρύθμισης, Στρατηγικής και Εποπτείας για όλα τα θέματα που σχετίζονται με αυτήν. Σκοπός της ανάθεσης ήταν η διασφάλιση της καλύτερης δυνατής συνεργασίας και υποστήριξης εκ μέρους της Αρχής προς τους κρίσιμους φορείς για τη βελτίωση των επιπέδων κυβερνοασφάλειας τους και την ανθεκτικότητα των κρίσιμων υποδομών της Κυπριακής Δημοκρατίας. Ο θεσμός των account managers θεωρείται επιτυχημένος, αφού οι κρίσιμοι φορείς πολλές φορές κάνουν χρήση του θεσμού και επικοινωνούν ώστε να μένουν ενημερωμένοι για σημαντικά θέματα. Η ΑΨΑ έχει ως διαχρονικό στόχο τη συνεχή ενίσχυση των επιπέδων εμπιστοσύνης μεταξύ αυτής και των εποπτευόμενων φορέων.



Η Αρχή Ψηφιακής Ασφάλειας επίσης, στα πλαίσια των αρμοδιοτήτων της και του ευρύτερου στόχου της ενδυνάμωσης των σχέσεων με τις Κρίσιμες Υποδομές, πραγματοποίησε αρκετές συναφείς δράσεις όπως σεμινάρια ευαισθητοποίησης, εκπαιδεύσεις, συνέδρια και ημερίδες καθώς επίσης και ενημερωτικούς οδηγούς (βλέπε ενότητα 8.4 για περισσότερες πληροφορίες).

5.4 Συνεργασία με ιδιωτικό τομέα

Η συνεργασία με τον ιδιωτικό τομέα και τις μικρομεσαίες επιχειρήσεις (ΜμΕ) είναι εξίσου σημαντική, αφού οι ΜμΕ αποτελούν τη ραχοκοκαλιά της οικονομίας. Αντιλαμβανόμενοι ότι συχνά διαθέτουν περιορισμένους πόρους και τεχνογνωσία για να αντιμετωπίσουν κυβερνοαπειλές, η ΑΨΑ κατά το 2024 ανέλαβε διάφορες πρωτοβουλίες για τη στήριξη τους.

Στις 17 Οκτωβρίου 2024 η ΑΨΑ υπέγραψε Μνημόνιο Συνεργασίας με το **DiGiNN**, μια στρατηγική σύμπραξη κορυφαίων κυπριακών οργανισμών στους τομείς της τεχνολογίας, έρευνας και επιχειρηματικότητας.Το DiGiNN - Ευρωπαϊκός Κόμβος Ψηφιακής Καινοτομίας Κύπρου - Digital Innovation Hub Cyprus ενώνει την ακαδημαϊκή και επιχειρηματική κοινότητα της Κύπρου για την προώθηση του ψηφιακού μετασχηματισμού, υποστηρίζοντας επιχειρήσεις και οργανισμούς σε όλη τη διαδικασία ψηφιακής ανάπτυξης. Παρέχει πρόσβαση σε εξειδικευμένους εμπειρογνώμονες, προηγμένες υποδομές, επενδυτικές ευκαιρίες και ένα ισχυρό δίκτυο καινοτομίας, διευκολύνοντας τη μετάβαση στην ψηφιακή εποχή. Το MoU στοχεύει στη συνδιοργάνωση εκδηλώσεων, την ανταλλαγή τεχνογνωσίας και την ενίσχυση συνεργειών. Κατά το 2024, οι δύο φορείς πραγματοποίησαν διαδικτυακές συναντήσεις για τη διαμόρφωση κοινού σχεδίου δράσης, εστιάζοντας στην υποστήριξη ΜΜΕ και νεοφυών επιχειρήσεων, την προώθηση των δραστηριοτήτων τους, την ενίσχυση της ψηφιοποίησης και την ανάπτυξη τοπικών ικανοτήτων κυβερνοασφάλειας. Ως αποτέλεσμα της πιο πάνω πρωτοβουλίας κατά το 2024 διοργανώθηκαν δύο κοινές δράσεις (βλέπε ενότητα 9 για περισσότερες πληροφορίες).

Συνεχίζοντας, και στα πλαίσια της συνεργασίας που αναπτύχθηκε κατά το 2023 με την υπογραφή σχετικού Μνημονίου Συνεργασίας - MoU, ενδυναμώθηκαν και ενισχύθηκαν οι κοινές δράσεις με το **ΚΕΒΕ** και κατά το 2024 που αποσκοπούσαν στη στήριξη των επιχειρήσεων, την ενδυνάμωση της ανταγωνιστικότητας τους και τη βελτίωση του επιχειρηματικού τους περιβάλλοντος. Η συνεργασία με το ΚΕΒΕ αποτελεί ένα σημαντικό βήμα προς τη δημιουργία ενός ισχυρού και βιώσιμου επιχειρηματικού περιβάλλοντος, συμβάλλοντας έτσι στην οικονομική ανάπτυξη και την ενίσχυση της επιχειρηματικότητας στην Κύπρο (βλέπε ενότητα 9.1 για περισσότερες πληροφορίες).

Ιδιαίτερα αξιοσημείωτη είναι επίσης η δραστηριοποίηση της **Κοινότητας Κυβερνοασφάλειας**. Δημιουργημένη από την ΑΨΑ ως το καθορισμένο NCC-CY, συγκεντρώνει φορείς από τον ιδιωτικό και δημόσιο τομέα, τη βιομηχανία, την ακαδημαϊκή κοινότητα και την έρευνα, προωθώντας τη συνεργασία και την ανταλλαγή γνώσεων στον τομέα της κυβερνοασφάλειας. Για σκοπούς αποτελεσματικότερης λειτουργίας της Κοινότητας, το 2024 δημιουργήθηκε η πλατφόρμα διαχείρισης των μελών της, συνδέοντας την κοινότητα με την ευρωπαϊκή πλατφόρμα Atlas, διευκολύνοντας παράλληλα την ανταλλαγή πληροφοριών και ενισχύοντας τη δικτύωση μεταξύ τους. Η αποστολή μηνιαίων ενημερωτικών δελτίων καθώς και η διοργάνωση εκδηλώσεων και εκπαιδεύσεων, είναι μερικές από τις δράσεις ενίσχυσης και ενδυνάμωσης της κοινότητας. Συγκεκριμένα κατά το 2024 διεξήχθη η εναρκτήρια εκδήλωση της κοινότητας, πραγματοποιήθηκαν ημερίδες και εκπαιδεύσεις με εξειδικευμένους ομιλητές από το εξωτερικό, ενώ τα μέλη της κοινότητας είχαν την ευκαιρία να συμμετάσχουν σε άλλες εκδηλώσεις της ΑΨΑ ως κεντρικοί ομιλητές ή/και εκπαιδευτές. Με αυτό τον τρόπο η ΑΨΑ προσπαθεί να διασφαλίσει ότι τα μέλη της κοινότητας της παραμένουν ενημερωμένα και έχουν πρόσβαση σε διάφορες ευκαιρίες ανάπτυξης και δικτύωσης, που προκύπτουν τόσο σε εθνικό όσο και πανευρωπαϊκό επίπεδο.

Κλείνοντας, και αντιλαμβανόμενοι πλήρως τη σημαντικότητα του τομέα των αερομεταφορών, συνεχίστηκε η στενή συνεργασία μεταξύ της ΑΨΑ και της **Hermes Airports Ltd**. Αξίζει να σημειωθεί ότι οι δύο Οργανισμοί έχουν ήδη καθορίσει το πλαίσιο της συνεργασίας τους μέσω σχετικού συμφωνητικού συνεργασίας που υπογράφτηκε κατά τα προηγούμενα έτη.

6 ΕΦΑΡΜΟΓΗ & ΕΝΙΣΧΥΣΗ ΝΟΜΙΚΟΥ, ΚΑΝΟΝΙΣΤΙΚΟΥ ΚΑΙ ΡΥΘΜΙΣΤΙΚΟΥ ΠΛΑΙΣΙΟΥ

Στο πλαίσιο της αποστολής της Αρχής Ψηφιακής Ασφάλειας για την ενίσχυση της εθνικής ανθεκτικότητας στον κυβερνοχώρο, το 2024 δόθηκε ιδιαίτερη έμφαση στην εφαρμογή, επικαιροποίηση και ενίσχυση του νομοθετικού και ρυθμιστικού πλαισίου κυβερνοασφάλειας. Οι δράσεις που αναλήφθηκαν κάλυψαν τόσο την εφαρμογή του υφιστάμενου νομικού πλαισίου όσο και την προσαρμογή του στις απαιτήσεις της νέας Οδηγίας NIS2, με στόχο την ενίσχυση της ετοιμότητας και της συμμόρφωσης των εμπλεκόμενων φορέων.

6.1 Νόμος ΑΨΑ - Ν. 89 (Ι)/2020 Περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών

Σύμφωνα με τον περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμο του 2020 (Ν. 89(Ι)/2020), η ΑΨΑ ορίστηκε ως η αρμόδια εθνική αρχή στην Κυπριακή Δημοκρατία για την ασφάλεια δικτύων και συστημάτων πληροφοριών και ως υπεύθυνη για το συντονισμό και υλοποίηση της εθνικής στρατηγικής κυβερνοασφάλειας.

Ο Νόμος 89(Ι)/2020, ο οποίος εναρμονίστηκε με την Οδηγία (ΕΕ) 2016/1148[3], προάγει τη διατήρηση της ακεραιότητας και ασφάλειας των πληροφοριών και την επίτευξη ενός υψηλού επιπέδου ασφάλειας δικτύων και συστημάτων πληροφοριών στην Κυπριακή Δημοκρατία. Περαιτέρω, ο Νόμος 89(Ι)/2020 καθορίζει τις υποχρεώσεις των φορέων που εμπίπτουν στο πεδίο εφαρμογής του για την ενίσχυση του επιπέδου ασφάλειας των δικτύων και συστημάτων πληροφοριών τους και προάγει τη συνεργασία σε εθνικό και διεθνές επίπεδο για σκοπούς ενίσχυσης της κυβερνοασφάλειας στην Κυπριακή Δημοκρατία.

6.2 Οδηγία NIS & NIS2 και τροποποίηση Νόμου

Στις 27 Δεκεμβρίου 2022, δημοσιεύθηκε στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης η Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS2).

Η Οδηγία (ΕΕ) 2016/1148 (Οδηγία NIS) αποτέλεσε την πρώτη νομοθετική πράξη της Ευρωπαϊκής Ένωσης σχετικά με την ασφάλεια δικτύων και συστημάτων πληροφοριών, εντούτοις ο εκσυγχρονισμός της ήταν επιβεβλημένος για να συμβαδίζει με την αυξημένη ψηφιοποίηση και το εξελισσόμενο τοπίο απειλών στον κυβερνοχώρο.

Η Οδηγία NIS2, με την επέκταση του πεδίου εφαρμογής των κανόνων κυβερνοασφάλειας σε νέους τομείς και οντότητες, ενισχύει σημαντικά την ανθεκτικότητα και τις ικανότητες αντιμετώπισης συμβάντων των δημόσιων και ιδιωτικών οντοτήτων, των αρμόδιων αρχών και της Ευρωπαϊκής Ένωσης.

Εντός του 2024, η Αρχή προχώρησε στην προώθηση σχετικού ολοκληρωμένου τροποποιητικού νομοσχεδίου στη Νομική Υπηρεσία για νομοτεχνικό έλεγχο και αναμένεται εντός του 2025 να προωθηθεί στο Υπουργικό Συμβούλιο για έγκριση και ακολούθως στη Βουλή των Αντιπροσώπων για την ψήφιση.

Το τροποποιητικό νομοσχέδιο καθορίζει, μεταξύ άλλων, τροποποιήσεις στα άρθρα του βασικού νόμου, Νόμου 89(Ι)/2020, ως ακολούθως:

- το πεδίο εφαρμογής προβλέπει ρυθμίσεις σε περιπτώσεις όπου υπάρχουν τομεακές νομικές πράξεις της Ένωσης (lex specialis),
- τον προσδιορισμό των βασικών και σημαντικών οντοτήτων,
- τον καθορισμό και την εφαρμογή της Εθνικής Στρατηγικής Κυβερνοασφαλείας,
- την κατάρτιση εθνικού πλαισίου διαχείρισης κυβερνοκρίσεων,
- τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που πρέπει να λαμβάνονται από τις βασικές και σημαντικές οντότητες,
- την ευθύνη της ανώτατης διοίκησης σχετικά με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας,
- την υποχρέωση κοινοποίησης περιστατικών στην Αρχή από βασικές και σημαντικές οντότητες,
- τα μέτρα εποπτείας και επιβολής που δύναται να επιβάλλονται από την Αρχή σε βασικές ή σημαντικές οντότητες σε σχέση με τις υποχρεώσεις τους ως αυτές προβλέπονται στο νομοσχέδιο,
- τις περιπτώσεις εθελούσιας κοινοποίησης περιστατικών, κυβερνοαπειλών και παρ' ολίγον περιστατικών και από οντότητες που δεν εμπίπτουν στο πεδίο εφαρμογής του νόμου, και
- την επιβολή διοικητικών προστίμων σε βασικές και σημαντικές οντότητες.

6.3 Εθνικό Πλαίσιο Κυβερνοασφάλειας και Δραστηριότητες – Μοντέλο Ωριμότητας

Το 2024, η ΑΨΑ προχώρησε επίσης σε σημαντικά βήματα για την εφαρμογή του Εθνικού Πλαισίου Κυβερνοασφάλειας, εστιάζοντας στη θεσμοθέτηση του Μοντέλου Ωριμότητας Κυβερνοασφάλειας και στη δημιουργία του Μητρώου Ελεγκτών. Οι δράσεις αυτές ενισχύουν τη συμμόρφωση των φορέων κρίσιμων υποδομών με τις εθνικές απαιτήσεις ασφαλείας και προάγουν μια συστηματική προσέγγιση αξιολόγησης της κυβερνοανθεκτικότητάς τους.

Εντός του 2024, η ΑΨΑ δημοσίευσε την περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Έλεγχοι Ωριμότητας Κυβερνοασφάλειας) Απόφαση του 2024 (Κ.Δ.Π. 245/2024). Βάσει της Απόφασης καθιερώνεται το Μοντέλο Ωριμότητας της Κυβερνοασφάλειας που έχει αναπτυχθεί από την Αρχή Ψηφιακής Ασφάλειας ως η διαδικασία ελέγχου. Το μοντέλο αυτό βασίζεται στις απαιτήσεις της απόφασης Κ.Δ.Π. 389/2020, καθώς και άλλες διεθνείς βέλτιστες πρακτικές και πρότυπα. Πιο συγκεκριμένα το Μοντέλο περιλαμβάνει εξειδίκευση και αποσαφήνιση των απαιτήσεων του Παραρτήματος ΙΙΙ της περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών) Απόφασης Κ.Δ.Π. 389/2020, αντιστοιχισμένο σε διακριτά επίπεδα ωριμότητας για κάθε μέτρο ασφάλειας. Το μοντέλο καλύπτει όλο το φάσμα των απαιτήσεων ασφάλειας στο πλαίσιο των τριών πυλώνων, δηλαδή στους πυλώνες της προετοιμασίας (Prepare), προστασίας και εντοπισμού (Protect and Detect) και ανταπόκρισης (Respond). Το Μοντέλο Ωριμότητας περιέχει πέντε διακριτά επίπεδα ωριμότητας κυβερνοασφάλειας, με το επίπεδο 3 να είναι το στάδιο το οποίο ένας Φορέας συμμορφώνεται με τις ελάχιστες απαιτήσεις της Απόφασης Κ.Δ.Π 389/2020.

Επιπρόσθετα, η Αρχή ανακοίνωσε την έναρξη λειτουργίας του Μητρώου Ελεγκτών Κυβερνοασφάλειας το οποίο δημιουργήθηκε στα πλαίσιο της Απόφασης Κ.Δ.Π. 245/2024. Το Μητρώο το οποίο είναι δημόσια διαθέσιμο περιλαμβάνει τους εγγεγραμμένους ελεγκτές που δικαιούνται βάσει της Απόφασης Κ.Δ.Π 245/2024 να διενεργούν ελέγχους ωριμότητας κυβερνοασφάλειας σε Φορείς Κρίσιμων Υποδομών.

6.4 Εποπτεία Μέτρων Ασφάλειας σε Κρίσιμους Φορείς

Κατά το 2024, η Αρχή Ψηφιακής Ασφάλειας σύμφωνα με την περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Έλεγχοι Ωριμότητας Κυβερνοασφάλειας) Απόφαση Κ.Δ.Π. 245/2024, κατάρτησε πρόγραμμα και ξεκίνησε τη διενέργεια ελέγχων συμμόρφωσης των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και των Φορέων Κρίσιμων Υποδομών Πληροφοριών, για την περίοδο 2024-2025. Το πεδίο εφαρμογής του ελέγχου συμμόρφωσης περιλαμβάνει όλα τα μέτρα ασφάλειας της περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών) Απόφαση Κ.Δ.Π. 389/2020.

Στόχος των ελέγχων είναι η ώθηση της προσπάθειας για σταδιακή ενίσχυση της ασφάλειας και της ανθεκτικότητας των υποδομών και των υπηρεσιών των Φορέων, η αντιμετώπιση περιστατικών παραβίασης ασφάλειας και η διασφάλιση της επιχειρησιακής συνέχειας των δικτύων, των συστημάτων πληροφοριών και των υπηρεσιών τους σε περίπτωση καταστροφικής βλάβης ή σε περίπτωση ανωτέρας βίας.

Εντός του 2024, η ΑΨΑ προχώρησε στην υλοποίηση αριθμού επιπρόσθετων δράσεων εποπτείας προς τους κρίσιμους φορείς ως ακολούθως:

- Παρακολούθηση της υποβολής των προβλεπόμενων εγγράφων με βάση τις απαιτήσεις των άρθρων 13 και 21 της Απόφασης Κ.Δ.Π 389/2020 (μεταξύ άλλων, έγγραφα διαχείρισης κινδύνων, διακυβέρνησης και σχεδιασμού επιχειρησιακής συνέχειας).
- Διεκπεραίωση συναντήσεων προόδου σε έξι (6) κρίσιμους Φορείς, για να διαπιστωθεί το επίπεδο εφαρμογής των προνοιών της Απόφασης Κ.Δ. Π 389/2020, και ειδικά, τον έλεγχο υλοποίησης και εφαρμογής των μέτρων ασφαλείας για αντιμετώπιση των υψηλότερων σε κρισιμότητα κινδύνων που εντοπίζονται από τους φορείς.
- Διεκπεραίωση 2 πιλοτικών ελέγχων συμμόρφωσης με τη χρήση του Μοντέλου Ωριμότητας Κυβερνοασφάλειας όπως αυτό δημοσιεύθηκε στην Απόφαση Κ.Δ.Π 245/2024 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Έλεγχοι Ωριμότητας Κυβερνοασφάλειας)

Πέραν των ελέγχων δράσεων, διενεργήθηκαν επιτόπιες έρευνες σε φορείς κρίσιμων υποδομών μετά από περιστατικά κυβερνοασφάλειας με στόχο τη διερεύνηση, την αξιολόγηση της συμμόρφωσης με τις απαιτήσεις της Κ.Δ.Π 389/2020, την αποτίμηση των κινδύνων και την παροχή κατευθυντήριων γραμμών προς ενίσχυση της ασφάλειας των υποδομών των συγκεκριμένων φορέων.

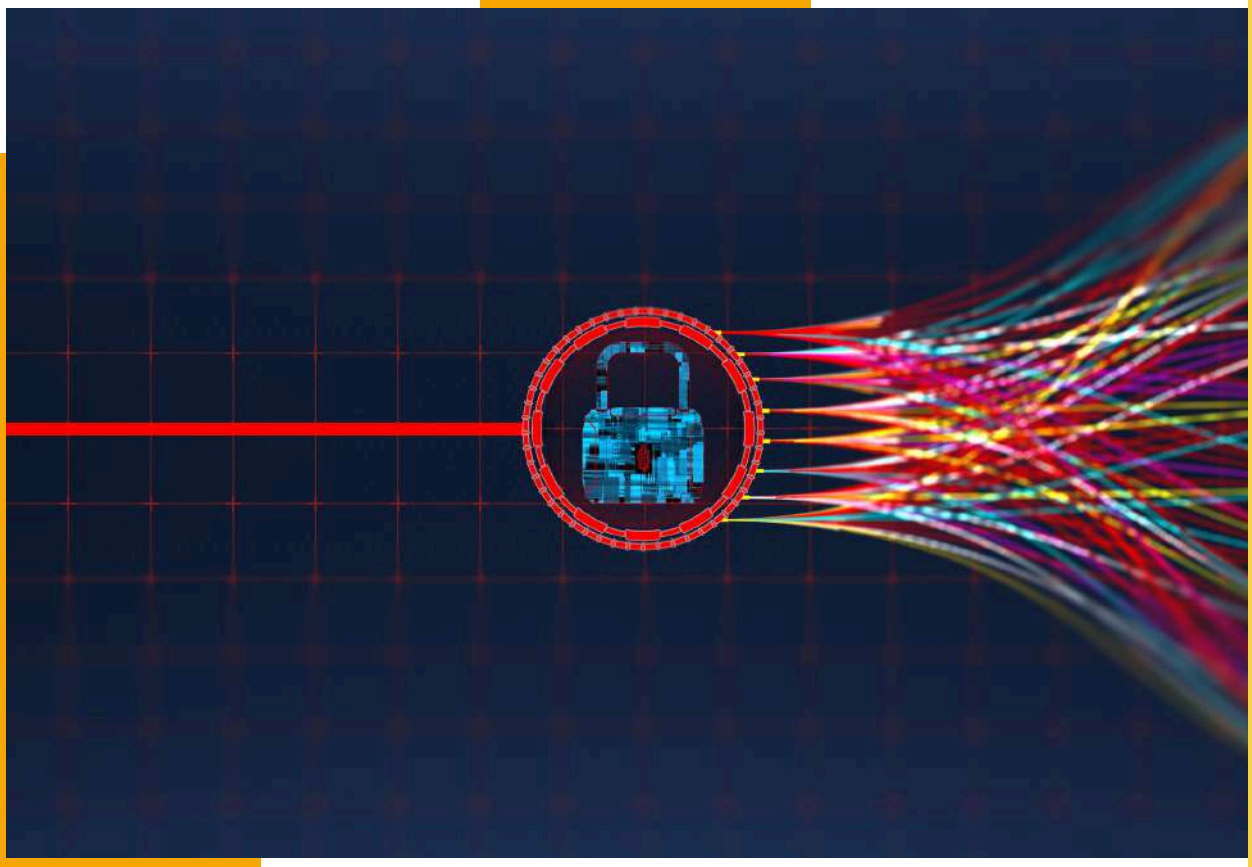
Επιπρόσθετα, μετά από επιτόπιες έρευνες και ακροάσεις σε άλλους φορείς κρίσιμων υποδομών, εκδόθηκε απόφαση σχετικά με τα περιστατικά για τη λήψη απαραίτητων διορθωτικών μέτρων, με στόχο την ενίσχυση της ασφάλειας, της ανθεκτικότητας και της συμμόρφωσης με τις απαιτήσεις της Κ.Δ.Π 389/2020 και άλλα θέματα φυσικής ασφάλειας. Υπάρχει πλάνο για διενέργεια μελλοντικών επιθεωρήσεων για την επαλήθευση της συμμόρφωσης των φορέων αυτών.

6.5 Κοινοποίηση Περιστατικών Παραβίασης Ψηφιακής Ασφάλειας

Η έγκαιρη και ορθή κοινοποίηση περιστατικών ψηφιακής ασφάλειας αποτελεί κρίσιμο εργαλείο για την ενίσχυση της εθνικής κυβερνοανθεκτικότητας.

Η Απόφαση ΚΔΠ 39/2022, σχετικά με τις κοινοποιήσεις περιστατικών ασφάλειας, εφαρμόζεται υποχρεωτικά από όλους τους εποπτευόμενους φορείς της ΑΨΑ. Η εν λόγω Απόφαση θέτει τα κριτήρια, τα κατώτατα όρια και τις συνθήκες βάσει των οποίων ένα περιστατικό ασφάλειας κρίνεται ως να έχει σοβαρό ή/και σημαντικό αντίκτυπο στην παροχή των υπηρεσιών των προαναφερθέντων φορέων. Συνεπώς, ενεργοποιείται η υποχρέωση των φορέων για υποβολή κοινοποιήσεων περιστατικών στην ΑΨΑ, εστιάζοντας σε περιστατικά που σχετίζονται με την απώλεια ή αλλοίωση των βασικών χαρακτηριστικών ασφάλειας των υπηρεσιών τους, δηλαδή την εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και αυθεντικότητα. Επιπλέον, η Απόφαση ρυθμίζει τη διαδικασία υποβολής των κοινοποιήσεων, καθορίζοντας το περιεχόμενο, τον τρόπο και τις προθεσμίες που οφείλουν να τηρούν οι Φορείς και οι Παροχείς.

Κατά το 2024, υποβλήθηκαν στην Αρχή δέκα (10) επίσημες κοινοποιήσεις περιστατικών, συμπεριλαμβανομένου τόσο των υποχρεωτικών, αλλά και εθελοντικών κοινοποιήσεων, οι οποίες έτυχαν διαχείρισης κατά περίπτωση.



6.6 Νέο Μοντέλο Τελών ΑΨΑ

Στο πλαίσιο εφαρμογής του Νόμου για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (Ν.89(Ι)/2020) και της Οδηγίας (ΕΕ) 2022/2555, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας στην ΕΕ και τη σημαντική διεύρυνση του αριθμού των επηρεαζόμενων Φορέων, η Αρχή Ψηφιακής Ασφάλειας αποφάσισε τη μελέτη και ανάπτυξη ενός αναθεωρημένου οικονομικού μοντέλου για τον αυτοματοποιημένο υπολογισμό των τελών χρηματοδότησης, τα οποία θα καταβάλουν οι φορείς που θα οριστούν σύμφωνα με τον Νόμο 89(Ι)/2020, όπως θα τροποποιηθεί για να εναρμονιστεί με την Οδηγία NIS2.

Τα τέλη χρηματοδότησης, που αποτελούν τη βασική πηγή εισοδημάτων της ΑΨΑ, υπολογίζονται βάσει οικονομικού μοντέλου που εγκρίνεται με σχετικούς Κανονισμούς της Βουλής των Αντιπροσώπων. Το 2024 ξεκίνησε η αναθεώρηση της δευτερογενούς νομοθεσίας και του οικονομικού μοντέλου ώστε οι ισχύοντες Κανονισμοί να αντικατασταθούν με νεότερους, λαμβάνοντας υπόψη τις αλλαγές που επιφέρει η εφαρμογή του NIS2 και τις αλλαγές που πρέπει να επέλθουν για τον εκσυγχρονισμό των υφιστάμενων διαδικασιών και τη δικαιότερη κατανομή των τελών. Προς αυτό το σκοπό ανατέθηκε στο Πανεπιστήμιο Κύπρου η διεξαγωγή ειδικής μελέτης και η ανάπτυξη νέου μοντέλου. Το μοντέλο θα οριστικοποιηθεί στο πλαίσιο αξιολόγησης από ομάδα εργασίας στην οποία συμμετέχουν το Υφυπουργείο Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής (ΥΕΚΨΠ) και το Υπουργείο Οικονομικών (ΥΠΟΙΚ), και εντός του 2025 αναμένεται όπως οι Κανονισμοί προωθηθούν στο Υπουργικό Συμβούλιο και τη Βουλή των Αντιπροσώπων για έγκριση και ψήφιση.

7 ΕΝΔΥΝΑΜΩΣΗ ΤΗΣ ΕΘΝΙΚΗΣ ΙΚΑΝΟΤΗΤΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Καθ' όλη τη διάρκεια του 2024, η ΑΨΑ πραγματοποίησε με επιτυχία σημαντικές δραστηριότητες κατάρτισης για το προσωπικό της, στοχεύοντας στην ενίσχυση των δεξιοτήτων και των ικανοτήτων των μελών της. Οι πρωτοβουλίες αυτές επικεντρώθηκαν τόσο στην ανάπτυξη δεξιοτήτων κυβερνοασφάλειας, μέσα από την εκπαίδευση σε σύγχρονες τεχνικές και βέλτιστες πρακτικές για την πρόληψη και την αντιμετώπιση κυβερνοαπειλών, όσο και στη βελτίωση των ικανοτήτων διαχείρισης έργων της Ευρωπαϊκής Ένωσης, μέσω εξειδικευμένων σεμιναρίων που παρείχαν πολύτιμες γνώσεις για τη διαχείριση χρηματοδοτούμενων προγραμμάτων. Οι δράσεις αυτές επιβεβαιώνουν τη δέσμευση της ΑΨΑ για συνεχή εκπαίδευση και ανάπτυξη του προσωπικού της, με στόχο τη διατήρηση υψηλών προτύπων στον τομέα της κυβερνοασφάλειας και της αποτελεσματικής διαχείρισης ευρωπαϊκών έργων.

7.1 Εκπαιδεύσεις Προσωπικού

Εντός του 2024, τα μέλη του προσωπικού της Αρχής Ψηφιακής Ασφάλειας συμμετείχαν σε εξειδικευμένες εκπαιδεύσεις προσαρμοσμένες στις ειδικότητές τους.

Συγκεκριμένα πραγματοποιήθηκε εκπαίδευση σε τεχνικό επίπεδο η οποία επικεντρώθηκε στην απόκτηση πρακτικών γνώσεων για την **προστασία πληροφοριακών συστημάτων.** Μέσα από πρακτικά εργαστήρια, οι αναλυτές ανέπτυξαν την ικανότητα να εκτελούν βασικούς ελέγχους ασφαλείας, να εντοπίζουν ύποπτη δραστηριότητα και να συμβάλλουν στην ενίσχυση της ασφάλειας των υποδομών ενός οργανισμού σε καθημερινό επίπεδο.

Επιπρόσθετα έγινε εκπαίδευση που αφορούσε την **ψηφιακή εγκληματολογία,** καλύπτοντας θεωρία, νομοθεσίες, διαδικασίες και βέλτιστες πρακτικές βασισμένες σε διεθνή πρότυπα. Επιπρόσθετα δόθηκε η ευκαιρία στους αναλυτές να εφαρμόσουν σε σχετικά εργαστήρια τα όσα έμαθαν και να αποκτήσουν πρακτική εμπειρία για το θέμα εξειδίκευσής τους.

Πραγματοποιήθηκε επίσης εκπαίδευση στη **διαχείριση περιστατικών** η οποία κάλυψε ολόκληρη τη διαδικασία χειρισμού και απόκρισης συμβάντων, τις τακτικές διαδικασίες και τεχνικές που απαιτούνται για τον αποτελεσματικό Σχεδιασμό, Καταγραφή, Διαλογή, Ειδοποίηση και Συγκράτηση δεδομένων καθώς και δραστηριότητες μετά το συμβάν. Αυτές περιλαμβάνουν εξάλειψη, συγκέντρωση αποδεικτικών στοιχείων και εγκληματολογική ανάλυση, που οδηγούν σε πιθανή δίωξη ή αντίμετρα για να διασφαλιστεί ότι το περιστατικό δεν θα επαναληφθεί.

Αντιλαμβανόμενοι και τη σημαντικότητα του **ethical hacking**, πραγματοποιήθηκε εκπαίδευση για την κατανόηση και την αποτελεσματική αντιμετώπιση των σύγχρονων απειλών στον κυβερνοχώρο. Η ομάδα ανέπτυξε την απαραίτητη τεχνογνωσία και δεξιότητες ώστε να υιοθετεί τη νοοτροπία του χάκερ, με στόχο την έγκαιρη αναγνώριση και αποτροπή κακόβουλων ενεργειών. Μέσα από αυτή τη διαδικασία, ενισχύθηκε ουσιαστικά η ικανότητά της να προστατεύει αποτελεσματικά κρίσιμα συστήματα και υποδομές από πραγματικές κυβερνοεπιθέσεις, καθώς και να αξιολογούν την ασφάλεια των συστημάτων ενός οργανισμού.

Εξίσου σημαντική εκπαίδευση ήταν αυτή που αφορούσε το **ISO 27001 Lead Implementer**. Παρακολουθώντας το συγκεκριμένο σεμινάριο, μέλη του προσωπικού απέκτησαν εξειδικευμένες γνώσεις και δεξιότητες στην εφαρμογή ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) σύμφωνα με τις απαιτήσεις του διεθνώς αναγνωρισμένου προτύπου.

Συμπληρωματικά πραγματοποιήθηκε και η εκπαίδευση **ISO 27001 Lead Auditor** που αφορά την αξιολόγηση ενός συστήματος ασφάλειας πληροφοριών και των παραδοτέων κάποιου Οργανισμού/Φορέα με στόχο τον εντοπισμό θεμάτων προς εξασφάλιση συμμόρφωσης με το συγκεκριμένο πρότυπο. Επίσης προσέφερε την εκμάθηση βασικών δεξιοτήτων και γνώσεων σχετικά με τον κύκλο ζωής ενός ελέγχου από το σχεδιασμό, τη διεξαγωγή και τη διαχείριση ελέγχων, συμπεριλαμβανομένης της αξιολόγησης και του μετριασμού των κινδύνων καθώς και την ετοιμασία παραδοτέων ενός ελέγχου.

Ιδιαίτερα σημαντική κρίνεται επίσης και η εκπαίδευση που πραγματοποιήθηκε κατά το 2024 για τους **Ελεγκτές Ωριμότητας Κυβερνοασφάλειας.** Οι συμμετέχοντες απέκτησαν γνώσεις και δεξιότητες ώστε να μπορούν να διενεργούν ελέγχους κυβερνοασφάλειας με τη χρήση του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) της Αρχής Ψηφιακής Ασφάλειας.

Επιπρόσθετα των πιο πάνω, τα μέλη του προσωπικού είχαν την ευκαιρία να παρακολουθήσουν το σεμινάριο **Privacy and Data Protection: Recent ECtHR and CJEU Case Law - ERA Academy of Law** το οποίο πραγματοποιήκε από το Academy of European Law (ERA). Η συγκεκριμένη δράση παρείχε ενημέρωση σχετικά με πρόσφατη νομολογία που αναπτύχθηκε από το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων (ΕΔΔΑ) και από το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) για θέματα της νομοθεσίας περί απορρήτου και προστασίας δεδομένων.

Από τις ετήσιες εκπαιδεύσεις δε θα μπορούσε να λείπει αυτή που αφορά το **Γενικό Κανονισμό για την Προστασία Δεδομένων (ΕΕ) 2016/679 – ΓΕΠΔΠΧΗ**. Το συγκεκριμένο σεμινάριο διοργανώθηκε από το Γραφείο της Επιτρόπου για την Προστασία των Δεδομένων Προσωπικού Χαρακτήρα και παρείχε πληροφορίες και διευκρινίσεις στα θέματα και προκλήσεις που αντιμετωπίζουν οι Υπεύθυνοι Προστασίας Δεδομένων στο δημόσιο τομέα.

Τέλος, πραγματοποιήθηκαν και άλλες οριζόντιες εκπαιδεύσεις σε θεματολογίες όπως η διαχείριση έργων, σεμινάρια για πιστοποιήσεις υπηρεσιών και προϊόντων, γενικές ενημερώσεις του τομέα τη κυβερνοασφάλειας και η ορθολογιστική διαχείριση Ευρωπαϊκών Προγραμμάτων.

7.2 Ενίσχυση δυνατοτήτων αρχιτεκτονικής SOC

Η συνεχής εξέλιξη των κυβερνοαπειλών και η ανάγκη για υψηλό επίπεδο κυβερνοασφάλειας καθιστούν επιτακτική την αναβάθμιση και ενίσχυση της αρχιτεκτονικής του Κέντρου Επιχειρήσεων Κυβερνοασφάλειας (SOC).

Στο πλαίσιο του έργου SENTINEL, πραγματοποιήθηκαν σημαντικές μετατροπές στην υποδομή του SOC, με στόχο την αύξηση της διαθεσιμότητας, της αποδοτικότητας και της ασφάλειας των παρεχόμενων υπηρεσιών ανίχνευσης και αντίδρασης σε κυβερνοσυμβάντα. Η νέα ενισχυμένη αρχιτεκτονική του Κέντρου, παρέχει τη δυνατότητα να ανταποκρίνεται σε συμβάντα με ταχύτερο και αποδοτικότερο τρόπο, να υποστηρίζει περισσότερες πηγές δεδομένων (logs, alerts, telemetry) σε πραγματικό χρόνο, και να εφαρμόζει προηγμένες μεθόδους ανίχνευσης (threat detection) με τη χρήση αναβαθμισμένων εργαλείων SIEM, SOAR, EDR και NDR. Οι τεχνικές παρεμβάσεις που πραγματοποιήθηκαν καλύπτουν τόσο τη δικτυακή υποδομή όσο και την υπολογιστική ισχύ. Η προσέγγιση αυτή εναρμονίζεται με τις σύγχρονες βέλτιστες πρακτικές στον τομέα της κυβερνοασφάλειας και ενισχύει τη συνολική στρατηγική άμυνας έναντι των ψηφιακών απειλών.

7.3 Διοργάνωση και συμμετοχή Εθνικών και Διεθνών Ασκήσεων

Η συμμετοχή της ΑΨΑ σε εθνικές και διεθνείς κυβερνοασκήσεις αποτελεί βασικό εργαλείο για τη διασφάλιση της επιχειρησιακής ετοιμότητας και την ενίσχυση της συνεργασίας μεταξύ κρίσιμων φορέων. Κατά το 2024, η Αρχή είχε ενεργό ρόλο τόσο στον συντονισμό μεγάλων Πανευρωπαϊκών Ασκήσεων όσο και στη διοργάνωση Εθνικών Ασκήσεων.

Κατά το 2024 η ΑΨΑ συμμετείχε και συντόνισε σε εθνικό επίπεδο την 7η Πανευρωπαϊκή Άσκηση Αντιμετώπισης Κρίσεων στον Κυβερνοχώρο **Cyber Europe 2024**, η οποία πραγματοποιήθηκε με επιτυχία τον Ιούνιο του 2024 υπό τη διοργάνωση του Οργανισμού της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια (ENISA). Η διήμερη αυτή άσκηση, αποτελεί μια από τις μεγαλύτερες κυβερνοασκήσεις στην Ευρώπη, προσομοίωσε ένα εκτεταμένο σενάριο κυβερνοεπιθέσεων που επηρέαζε κρίσιμες υποδομές στον ενεργειακό τομέα, στους παρόχους υπηρεσιών κέντρων δεδομένων και στη δημόσια διοίκηση. Στόχος της άσκησης ήταν η αξιολόγηση της τεχνικής και επιχειρησιακής ετοιμότητας των συμμετεχόντων, καθώς και η ενίσχυση της διακρατικής συνεργασίας για την αντιμετώπιση κυβερνοαπειλών μεγάλης κλίμακας. Η πολυπρόσωπη και πολυεπίπεδη συμμετοχή προσέφερε μια πολύτιμη ευκαιρία για την αξιολόγηση των διαδικασιών αντιμετώπισης περιστατικών, τη δοκιμή και βελτίωση της ετοιμότητας, τη βελτίωση της διαλειτουργικότητας μεταξύ δημόσιου και ιδιωτικού τομέα, την ενίσχυση της συντονισμένης απόκρισης, και την οικοδόμηση εμπιστοσύνης μεταξύ των φορέων κυβερνοασφάλειας, προάγοντας την ανταλλαγή πληροφοριών και βέλτιστων πρακτικών, την εκπαίδευση και ανάπτυξη δεξιοτήτων των συμμετεχόντων και την ενίσχυση της ανθεκτικότητας των εθνικών υποδομών.

Επίσης, τον Σεπτέμβριο του 2024 διοργανώθηκε από την ΑΨΑ σε συνεργασία με το Υπουργείο Άμυνας και το Υφυπουργείο Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής, με την πλήρη υποστήριξη του Οργανισμού της ΕΕ για την Κυβερνοασφάλεια (ENISA) η πρώτη εθνική άσκηση κυβερνοασφάλειας **Cyber Cyprus 2024**. Αποτελώντας την πρώτη εθνικής εμβέλειας άσκηση τύπου tabletop, επικεντρώθηκε σε σενάριο επίθεσης ransomware στον τομέα των μεταφορών, δοκιμάζοντας τις ικανότητες απόκρισης κρίσιμων φορέων του δημόσιου και ιδιωτικού τομέα. Μέσα από ρεαλιστικά περιστατικά, οι συμμετέχοντες κλήθηκαν να λάβουν αποφάσεις στρατηγικής σημασίας και να διαχειριστούν επικοινωνία και συνεργασίες υπό πίεση. Τα βασικά ευρήματα της άσκησης ανέδειξαν την ανάγκη για συνεχή εκπαίδευση, την ύπαρξη κενών σε εσωτερικές διαδικασίες (SOPs), καθώς και την έλλειψη ενός ενιαίου Εθνικού Σχεδίου Διαχείρισης Κυβερνοκρίσεων που να καλύπτει όλα τα βασικά είδη σεναρίων. Η άσκηση Cyber Cyprus 2024 αποτέλεσε αφετηρία για την ενίσχυση της διατομεακής συνεργασίας και την ανάπτυξη συστάσεων, όπως η δημιουργία εθνικού μηχανισμού συντονισμού και η εδραίωση σταθερού πλαισίου διαχείρισης κυβερνοαπειλών. Τα αποτελέσματα της άσκησης τροφοδοτούν τον εθνικό σχεδιασμό και ενισχύουν τη θωράκιση της χώρας απέναντι στις εξελισσόμενες ψηφιακές προκλήσεις.

7.4 Ωριμότητα Κυβερνοασφάλειας στην ΚΔ

Η Κυπριακή Δημοκρατία είναι βαθιά προσηλωμένη και έχει δεσμευτεί να βελτιώνει και να ενισχύει συνεχώς την ασφάλεια στον κυβερνοχώρο μέσω συντονισμένων πρωτοβουλιών, στοχευμένων επενδύσεων και ενεργού συμμετοχής σε διεθνείς συμπράξεις. Ως μέρος των δραστηριοτήτων αυτών, η ΑΨΑ συμμετέχει ενεργά σε διάφορες αξιολογήσεις ωριμότητας, για να προσμετρά τους τομείς όπου μπορεί να βελτιώνεται περισσότερο και για να ενισχύσει ευρύτερα τα επίπεδα κυβερνοασφάλειας στην Κυπριακή Δημοκρατία.

Τα αποτελέσματα του ITU Global Cybersecurity Index 2024 - GCIv5 αντικατοπτρίζουν πλήρως την πρόοδο της Κύπρου στον Παγκόσμιο Δείκτη Κυβερνοασφάλειας (GCI) της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU). Στην τελευταία έκδοση του GCI v5, **η Κύπρος πέτυχε υψηλότερη κατάταξη, καταλαμβάνοντας πλέον θέση Tier 1, όπου συγκαταλέγονται κράτη με ανεπτυγμένες και ώριμες εθνικές στρατηγικές και προσεγγίσεις κυβερνοασφάλειας**. Η πρόοδος αυτή είναι αποτέλεσμα των συνδυασμένων προσπαθειών και του συντονισμού της Αρχής Ψηφιακής Ασφάλειας, μαζί με διάφορες αρμόδιες αρχές της χώρας. Με την εφαρμογή σύγχρονων στρατηγικών και την ενίσχυση του θεσμικού πλαισίου, η Κύπρος βελτίωσε τις επιδόσεις της σε τομείς όπως τα νομικά και τεχνικά μέτρα, ανάπτυξη ικανοτήτων καθώς και σε θεματικές όπως η Ευρωπαϊκή και διεθνής συνεργασία. Η αναγνώριση αυτή υπογραμμίζει τη συνεχή αφοσίωση της ΑΨΑ στην ενίσχυση του εθνικού πλαισίου κυβερνοασφάλειας, προς όφελος τόσο της οικονομίας όσο και της κοινωνίας, συμβάλλοντας σε ένα πιο ασφαλές και ανθεκτικό ψηφιακό περιβάλλον για όλους.

Επίσης κατά το έτος 2024, η Κύπρος στο σύνθετο δείκτη του πρώτου επίσημου EU Cybersecurity Index που συντάσσει ο ENISA και αξιολογεί το επίπεδο κυβερνοασφάλειας των κρατών μελών της ΕΕ, **παρουσίασε συνολική βαθμολογία υψηλότερη από τον μέσο όρο της Ευρωπαϊκής Ένωσης, με σημαντική βελτίωση σε σχέση με την αντίστοιχη επίδοση της στο πιλοτικό EU Cybersecurity Index 2023.** Η βελτίωση αυτή παρατηρείται και στις τέσσερις διαστάσεις του σύνθετού δείκτη. Συγκεκριμένα, στη διάσταση Capacity καταγράφηκε η μεγαλύτερη αύξηση, ενώ σημαντική πρόοδος σημειώθηκε επίσης στις διαστάσεις Policy, Operations και Market/Industry. Τα αποτελέσματα υποδεικνύουν σταθερή πρόοδο και ενίσχυση της συνολικής επίδοσης της χώρας σε θέματα κυβερνοασφάλειας.

Καταληκτικά και στο πλαίσιο ενίσχυσης της κυβερνοασφάλειας και της συμμόρφωσης με την Ευρωπαϊκή Οδηγία NIS2 (Οδηγία (ΕΕ) 2022/2555), η Αρχή Ψηφιακής Ασφάλειας αναπτύσσει μια ηλεκτρονική πλατφόρμα που αποσκοπεί σε ένα ολοκληρωμένο **Σύστημα Διαχείρισης Βασικών και Σημαντικών Οντοτήτων**. Εντός του 2024, αναπτύχθηκαν οι λεπτομερείς προδιαγραφές για τον πυρήνα και τα συστατικά μέρη (modules) του συστήματος αυτού, και προκηρύχθηκε η σχετική προσφορά με Ευρωπαϊκό διαγωνισμό με το έργο να αναμένεται να ολοκληρωθεί κατά το 2025. Το σύστημα αυτό θα αποτελέσει ένα σύγχρονο και αποτελεσματικό εργαλείο εποπτείας, διευκολύνοντας τη διαχείριση των οντοτήτων που εμπίπτουν στις υποχρεώσεις της Οδηγίας. Μέσω της αυτοματοποίησης των διαδικασιών συμμόρφωσης, της παρακολούθησης δράσεων και της ταχύτερης ανταπόκρισης σε περιστατικά κυβερνοασφάλειας, το νέο σύστημα θα ενισχύσει τη δυνατότητα της Αρχής να διασφαλίζει την ορθή εφαρμογή των κανονιστικών απαιτήσεων. Επιπλέον, θα παρέχει ένα κεντρικό σημείο διαχείρισης και διαμοιρασμού πληροφοριών, επιτρέποντας τόσο στους Λειτουργούς της Αρχής όσο και στους χρήστες των Φορέων να λειτουργούν με μεγαλύτερη αποδοτικότητα και διαφάνεια. Μέσω της υλοποίησης αυτής, αναμένεται να επιτευχθεί σημαντική βελτίωση στην εποπτεία και την επιχειρησιακή ετοιμότητα, συμβάλλοντας συνολικά στην ενίσχυση της ανθεκτικότητας των κρίσιμων και σημαντικών υποδομών της χώρας έναντι κυβερνοαπειλών.

8 ΕΝΙΣΧΥΣΗ ΙΚΑΝΟΤΗΤΑΣ ΚΡΙΣΙΜΩΝ ΦΟΡΕΩΝ

Η ενίσχυση της κυβερνοανθεκτικότητας των κρίσιμων υποδομών αποτελεί στρατηγική προτεραιότητα της ΑΨΑ. Κατά το 2024, υλοποιήθηκαν στοχευμένες δράσεις που περιλάμβαναν την ανάπτυξη εργαλείων υποστήριξης, την αξιοποίηση ευρωπαϊκών προγραμμάτων, την οργάνωση εξειδικευμένων εκπαιδεύσεων, καθώς και τη διοργάνωση ενημερωτικών ημερίδων και συνεδρίων. Μέσα από αυτές τις πρωτοβουλίες, ενισχύθηκε σημαντικά η ετοιμότητα και η συμμόρφωση των εμπλεκόμενων φορέων με τις απαιτήσεις του ρυθμιστικού πλαισίου, συμβάλλοντας στη δημιουργία ενός ασφαλούς ψηφιακού περιβάλλοντος.

8.1 Εργαλειοθήκη (Toolkit) Κ.Δ.Π. 389/2020

Στα πλαίσια των αρμοδιοτήτων της αλλά πρωτίστως με γνώμονα την ενίσχυση της κυβερνοασφάλειας στην Κυπριακή Δημοκρατία, η ΑΨΑ εντός του 2024, προχώρησε με αναθεώρηση (2η Έκδοση) της εργαλειοθήκης κυβερνοασφάλειας με πολιτικές συμβατές με τις Αποφάσεις Κ.Δ.Π 389/2020 (Μέτρα Ασφάλειας) και Κ.Δ.Π 245/2024 (Μοντέλο Ωριμότητας Κυβερνοασφάλειας).

Η εργαλειοθήκη περιλαμβάνει, μεταξύ άλλων, βελτιωμένες πολιτικές και διαδικασίες για την υποστήριξη της συμμόρφωσης με τις Αποφάσεις Κ.Δ.Π. 389/2020 και Κ.Δ.Π. 245/2024, τυποποιημένα πλαίσια για τη διαχείριση κινδύνων, το χειρισμό περιστατικών, τη διακυβέρνηση και τη Στρατηγική, καθώς και Σχέδια ανάκτησης μετά από καταστροφή (DR) και Επιχειρησιακής Συνέχειας (BC), τα οποία αποσκοπούν στην καθοδήγηση των Φορέων για την αποτελεσματική αντιμετώπιση και ανάκαμψη από περιστατικά στον κυβερνοχώρο.

Μέσω της εργαλειοθήκης, η ΑΨΑ επιδιώκει να ενισχύσει την ευαισθητοποίηση και την ετοιμότητα των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών στον τομέα της κυβερνοασφάλειας, κυρίως με την υιοθέτηση της Οδηγίας NIS2 η οποία αναμένεται να μπει σε εφαρμογή εντός του 2025 καθώς και άλλες νέες επιχειρήσεις/οργανισμούς που δύναται να εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας NIS2 και έχουν ως στόχο τη βελτίωση της κυβερνοασφάλειας και της ανθεκτικότητας στον κυβερνοχώρο.

8.2 Πρόγραμμα Ενίσχυσης μέσω ENISA Support Action

Επιπρόσθετα και κατά το 2022, η Ευρωπαϊκή Επιτροπή ανέθεσε στον Ευρωπαϊκό Οργανισμό για την κυβερνοασφάλεια (ENISA) πόρους 15 εκατομμυρίων ευρώ, για τη δημιουργία και την εφαρμογή της Δράσης Υποστήριξης της Κυβερνοασφάλειας. Στόχος του προγράμματος είναι η παροχή υπηρεσιών κυβερνοασφάλειας για την υποστήριξη των κρατών μελών για την ενίσχυση της ετοιμότητάς τους (εκ των προτέρων) και των ικανοτήτων απόκρισης (εκ των υστέρων). Αυτές οι υπηρεσίες ενισχύουν τις προσπάθειες, τόσο σε εθνικό όσο και σε επίπεδο ΕΕ, για περαιτέρω βελτίωση των ικανοτήτων πρόληψης και ανίχνευσης, ενίσχυση της επίγνωσης της κατάστασης και αντιμετώπισης μεγάλης κλίμακας περιστατικών ή κρίσεων κυβερνοασφάλειας.

Το 2024, η ΑΨΑ κατάφερε να υλοποιήσει δράσεις αξιοποιώντας το σύνολο του διαθέσιμου προϋπολογισμού που έχει διατεθεί για την Κύπρο, μέσα από το σχέδιο ENISA support Action. Η ΑΨΑ υλοποίησε 4 δοκιμές διείσδυσης (penetration testing), διάθεση εκατόν έξι (106) άδειες χρήσης (licenses) μέσω της πλατφόρμας Cyber Ranges, παρέχοντας προηγμένη εκπαίδευση στις κρίσιμες υποδομές, εβδομαδιαία παρακολούθηση κινδύνων (Risk Monitoring) των κρίσιμων υποδομών εφαρμόζοντας τη λύση Scorecard Solution ενώ με πόρους του συγκεκριμένου προγράμματος διοργανώθηκε η Εθνική Άσκηση Κυβερνοασφάλειας (βλέπε ενότητα 7.3 για περισσότερες πληροφορίες).

8.3 AR in A BOX – ENISA (Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια)

Το AR-in-a-BOX είναι μια ολοκληρωμένη λύση για δραστηριότητες ευαισθητοποίησης σε θέματα κυβερνοασφάλειας, σχεδιασμένη για να καλύπτει τις ανάγκες δημόσιων φορέων καθώς και ιδιωτικών εταιρειών. Παρέχει θεωρητικές και πρακτικές γνώσεις σχετικά με τον τρόπο σχεδιασμού και υλοποίησης αποτελεσματικών προγραμμάτων ευαισθητοποίησης στον κυβερνοχώρο, με στόχο την ανάπτυξη κουλτούρας όσον αφορά την κυβερνοασφάλεια.

Η ΑΨΑ τον Απρίλιο του 2024 διοργάνωσε Ημερίδα Ενημέρωσης σε συνεργασία με τον ENISA με θέμα «Awareness Raising in a Box (AR-in-a-Box)», με τη συμμετοχή πέραν των 60 ενδιαφερόμενων. Στα πλαίσια της διοργάνωσης, ο ENISA πραγματοποίησε επίσης πιλοτική εφαρμογή της συγκεκριμένης λύσης σε τρεις Φορείς της ΑΨΑ. Τα αποτελέσματα της εφαρμογής του πιλοτικού προγράμματος το οποίο διήρκεσε τρεις (3) μήνες ήταν αρκετά ενθαρρυντικά και μέσω αυτών βοήθησε τους συγκεκριμένους οργανισμούς να εξασφαλίσουν προϋπολογισμό για να μπορέσουν να τρέξουν με μεγαλύτερη ευκολία τη συγκεκριμένη λύση στην υπηρεσία τους.

8.4 Εκπαιδεύσεις και ενημερώσεις προς Κρίσιμες Υποδομές

Προχωρώντας, η Αρχή υλοποίησε ένα ευρύ φάσμα εκπαιδευτικών και ενημερωτικών δράσεων με στόχο την ενίσχυση της ετοιμότητας και της συμμόρφωσης των φορέων κρίσιμων υποδομών. Μέσα από συνέδρια, ημερίδες και εργαστήρια, προωθήθηκε η κατανόηση των σύγχρονων προκλήσεων στον τομέα της κυβερνοασφάλειας και ενισχύθηκε η τεχνική και οργανωτική ετοιμότητα των συμμετεχόντων, με έμφαση στη διαχείριση κινδύνων, την τυποποίηση, την τεχνητή νοημοσύνη και την εφαρμογή της Οδηγίας NIS2.

Συγκεκριμένα, κατά τον Απρίλιο του 2024 πραγματοποιήθηκε με μεγάλη επιτυχία το συνέδριο **«Cyber Security in Telecommunications»**, το οποίο συνδιοργανώθηκε από την ΑΨΑ, το Cyprus Computer Society και το British High Commission. Το συνέδριο κάλυψε μεγάλο εύρος σημαντικών θεμάτων για την ασφάλεια στον τομέα των ηλεκτρονικών επικοινωνιών, ο οποίος αποτελεί νευραλγικό τομέα της οικονομίας - και από μόνος του αλλά και ως η βάση για το συνδεδεμένο κόσμο στον οποίο ζούμε σήμερα. Όλοι οι κρίσιμοι τομείς της οικονομίας στηρίζονται πλέον σε πολύ μεγάλο βαθμό στις υπηρεσίες ηλεκτρονικών επικοινωνιών - και για αυτό είναι πιο σημαντικό από ποτέ όπως τα δίκτυα και οι υπηρεσίες να θωρακίζονται έναντι των υφιστάμενων και αναδυόμενων απειλών που εμφανίζονται στον κυβερνοχώρο.

Συνεχίζοντας, τον Ιούνιο του 2024, πραγματοποιήθηκε ενημερωτική ημερίδα με θέμα «Έλεγχοι Συμμόρφωσης βάσει του Μοντέλου Ωριμότητας Κυβερνοασφάλειας (**Cybersecurity Maturity Model**) στην Ακαδημία Τεχνολογίας, Πληροφορικής και Επικοινωνιών (ICT Academy) του Επιτρόπου Επικοινωνιών. Στην ημερίδα παρευρέθηκαν γύρω στα 120 άτομα από Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, Φορείς Κρίσιμων Υποδομών Πληροφοριών, Παροχείς Υπηρεσιών και/ή Δικτύων Ηλεκτρονικών Επικοινωνιών και Παροχείς Ψηφιακών Υπηρεσιών, τόσο από το δημόσιο όσο και από τον ιδιωτικό τομέα. Οι συμμετέχοντες είχαν την ευκαιρία να ενημερωθούν για τη δημιουργία και χρήση του νέου Μοντέλου Ωριμότητας Κυβερνοασφάλειας (Cybersecurity Maturity Model) που έχει αναπτύξει η Αρχή, καθώς και τον τρόπο που θα διενεργούνται οι σχετικοί έλεγχοι μέσω εγκεκριμένων ελεγκτών κυβερνοασφάλειας.

Κατά τον Οκτώβριο, και στα πλαίσια του μήνα Κυβερνοασφάλειας και της ενίσχυσης της προστασίας των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ) και Φορέων Κρίσιμων Υποδομών Πληροφοριών (ΦΚΥΠ), η Αρχή διοργάνωσε διήμερο (2) εργαστήριο με θέμα: **«Μεθοδολογία Διαχείρισης Κινδύνων Ασφάλειας Πληροφοριών»** το οποίο πραγματοποιήθηκε στην Ακαδημία Τεχνολογίας, Πληροφορικής και Επικοινωνιών (ICT Academy) του Γραφείου του Επιτρόπου Επικοινωνιών. Το εργαστήριο ήταν διαδραστικό και προσαρμοσμένο για να παρέχει τη θεμελιώδη θεωρία και ταυτόχρονα τη δοκιμή των γνώσεων σε προκαθορισμένα σενάρια που άπτονται της Μεθοδολογίας της Διαχείρισης Κινδύνων Ασφάλειας Πληροφοριών.

Τον ίδιο μήνα, η ΑΨΑ σε συνεργασία με τον Κυπριακό Οργανισμό Τυποποίησης (CYS) διοργάνωσε επίσης ενημερωτική ημερίδα, με θέμα «**Cybersecurity in the AI ERA**». Η ημερίδα εστίασε στις προκλήσεις και τα νέα δεδομένα στον τομέα της κυβερνοασφάλειας που αναδεικνύονται με την ανάπτυξη της Τεχνητής Νοημοσύνης, προσφέροντας πολύτιμες γνώσεις για τις εξελίξεις και τις απαιτήσεις στον τομέα της τυποποίησης.

Επιπρόσθετα η Αρχή Ψηφιακής Ασφάλειας **σε συνεργασία με το Υπουργείο Άμυνας (ΥΠΑΜ)** και το Ανοικτό Πανεπιστήμιο, διοργάνωσε επίσης τον Οκτώβριο επιμορφωτική Ημερίδα Κυβερνοασφάλειας στην οποία συμμετείχε στρατιωτικό προσωπικό της Εθνικής Φρουράς και του Υπουργείου Άμυνας. Η Ημερίδα πραγματοποιήθηκε στην Ακαδημία Τεχνολογίας, Πληροφορικής και Επικοινωνιών (ICT Academy) του Γραφείου του Επιτρόπου Επικοινωνιών και αποσκοπούσε στην ενημέρωση του προσωπικού για τις ενδεχόμενες απειλές που προέρχονται από τη χρήση του Διαδικτύου σε πραγματική κατάσταση, προκειμένου να λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία τόσο των πληροφοριών που διαχειρίζεται, όσο και των προσωπικών τους δεδομένων.

Στα πλαίσια πάντοτε των αρμοδιοτήτων της, η Αρχή Ψηφιακής Ασφάλειας δημοσίευσε επίσης **συνοπτικό Οδηγό της Οδηγίας (ΕΕ) 2022/2555 (Οδηγία NIS2)** που αποσκοπεί στην καθοδήγηση των οντοτήτων που θα εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας, αλλά και ενημέρωσης του κοινού ευρύτερα. Η Οδηγία NIS2 η οποία τέθηκε σε εφαρμογή στις 18 Οκτωβρίου 2024, έχει ως στόχο να αντιμετωπίσει τις ελλείψεις που εντοπίστηκαν από την εφαρμογή της Οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS), να την προσαρμόσει στις τρέχουσες ανάγκες και να την καταστήσει ανθεκτική στις μελλοντικές εξελίξεις. Ο συνοπτικός Οδηγός περιλαμβάνει πολλές σημαντικές πληροφορίες όπως πχ τους τομείς που εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας NIS2, τη διαδικασία κοινοποίησης περιστατικών, τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας, την εποπτεία των βασικών και σημαντικών οντοτήτων, την εφαρμογή της Οδηγίας NIS2 και τις προβλεπόμενες κυρώσεις καθώς και τις ευθύνες της Διοίκησης.

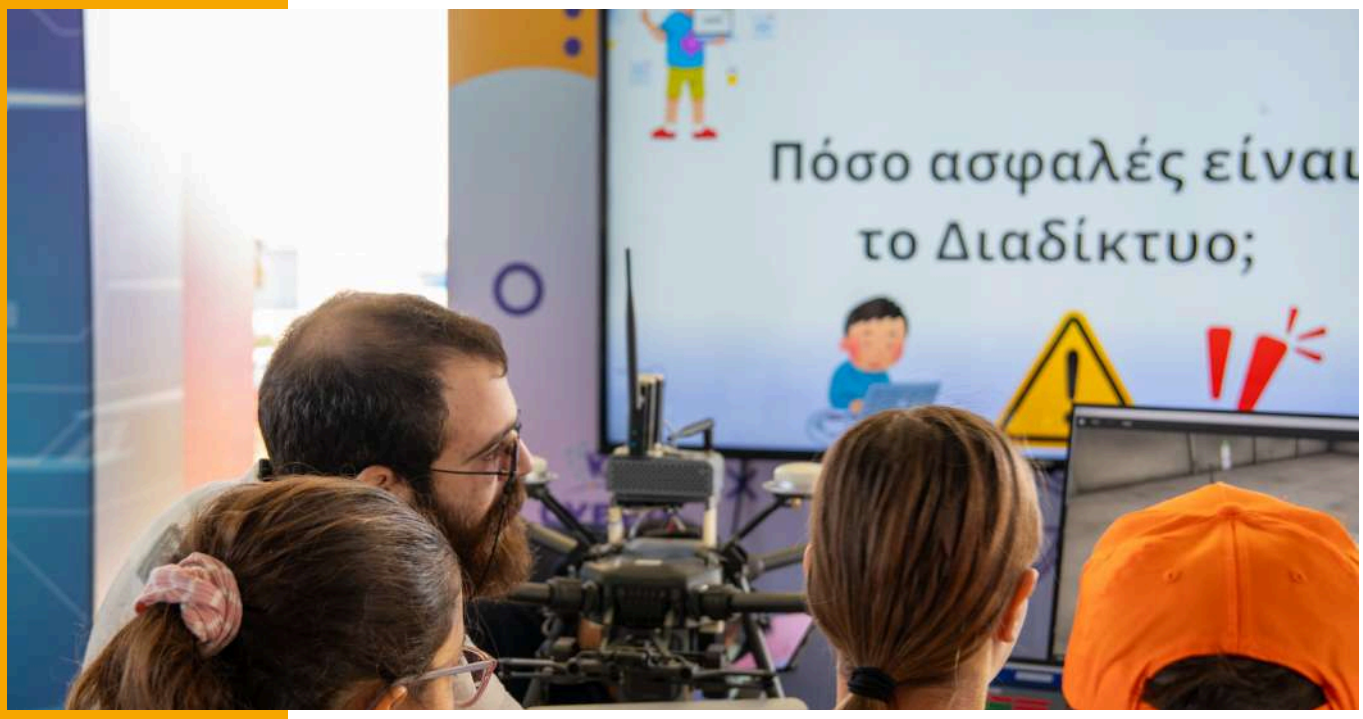
Καταληκτικά επιπρόσθετα για την ενίσχυση της κυβερνοασφάλειας στον τομέα της ναυτιλίας, διοργανώθηκε σε συνεργασία με το Υπουργείο Εξωτερικών, το Υφυπουργείο Ναυτιλίας, την Αμερικάνικη Πρεσβεία, τα Sandia National Laboratories των ΗΠΑ και το Ανοικτό Πανεπιστήμιο Κύπρου, το δεύτερο εργαστήριο κυβερνοασφάλειας με τίτλο **"Preventing Cyber Aggression in the Maritime Domain"** (βλέπε ενότητα 12.2 για περισσότερες πληροφορίες).

9 ΑΣΦΑΛΕΙΑ ΓΙΑ ΟΛΟΥΣ

Η ΑΨΑ στο πλαίσιο της αποστολής της για την ενίσχυση της ψηφιακής ασφάλειας στην Κύπρο, έχει αναλάβει πρωτοβουλίες ευαισθητοποίησης, συνδιοργανώνοντας συνέδρια, εκδηλώσεις και εκπαιδευτικά προγράμματα για όλη την κοινωνία. Πέραν των πιο κάτω δράσεων, η ΑΨΑ είναι ενεργή και στα μέσα κοινωνικής δικτύωσης (Facebook, LinkedIn, X), αναρτώντας υλικό που αποσκοπεί, μεταξύ άλλων, στην ευαισθητοποίηση και την ενημέρωση της κοινωνίας για τη σημαντικότητα της κυβερνοασφάλειας. Στόχος αυτών των δράσεων είναι η ενημέρωση, η ανάπτυξη δεξιοτήτων και η ενίσχυση της ανθεκτικότητας έναντι κυβερνοαπειλών.

9.1 Διοργάνωση Εκδηλώσεων Ευαισθητοποίησης

Η ευαισθητοποίηση γύρω από την κυβερνοασφάλεια είναι απαραίτητη για την προστασία όλων, από παιδιά και γονείς, άτομα μεγαλύτερης ηλικίας μέχρι και μικρομεσαίες επιχειρήσεις (ΜμΕ). Αντιλαμβανόμενη ότι, με την κατάλληλη ενημέρωση, κάθε μέλος της κοινωνίας μπορεί να συμβάλει στη δημιουργία ενός πιο ασφαλούς ψηφιακού περιβάλλοντος, η ΑΨΑ ανέλαβε πολυδιάστατη δράση κατά το 2024.



Επενδύοντας στην ευαισθητοποίηση των παιδιών, η ΑΨΑ προχώρησε σε **έκδοση εικονογραφημένης ιστορίας** για παιδιά από 5 -12 ετών στοχεύοντας στην επεξήγηση με εύληπτο τρόπο τη σημασία της κυβερνοασφάλειας, αλλά και γενικότερα το ρόλο και τις αρμοδιότητες της ΑΨΑ. Η ηρωίδα του βιβλίου είναι ένα δυναμικό κορίτσι, η Φοίβη (μια από της Αμαζόνες και συμβολίζει κάποιον που αφιερώνεται σε έναν σκοπό), που αγαπάει πολύ την τεχνολογία και χάρη σε αυτήν, οι μικροί αναγνώστες ξεναγούνται στην Αρχή Ψηφιακής Ασφάλειας. Μέσα από τη μυθοπλασία, τα παιδιά μαθαίνουν για τους τομείς της ΑΨΑ, τη σπουδαιότητα της κυβερνοασφάλειας και γενικότερα τη σημασία της προστασίας όλων των πολιτών είτε χρησιμοποιούν την τεχνολογία είτε όχι.

Επιπρόσθετα και αποσκοπώντας εκ νέου στην ευαισθητοποίηση των παιδιών, η Αρχή Ψηφιακής Ασφάλειας συμμετείχε στην **3η Διεθνής Έκθεση Βιβλίου Λεμεσού (Limassol Book Fair)** η οποία πραγματοποιήθηκε το Νοέμβριο του 2024 στη Λεμεσό. Η παρουσία της ΑΨΑ περιλάμβανε μεταξύ άλλων ενημερωτικό περίπτερο στην Παιδική και Νεανική σκηνή με ενημερωτικά φυλλάδια και διαφημιστικά δωράκια, παιχνίδια με γρίφους, εκπαιδευτικά σενάρια μέσω της τεχνολογίας μικτής πραγματικότητας (Mixed Reality) καθώς επίσης και την παρουσίαση του βιβλίου «Η Φοίβη στην Αρχή Ψηφιακής Ασφάλειας».

Εστιάζοντας στους επαγγελματίες του κλάδου, στις 4 Ιουνίου 2024, πραγματοποιήθηκε η **τελετή έναρξης του Ευρωπαϊκού Έργου N4CY** στο ICT Academy του Επιτρόπου Επικοινωνιών, με στόχο την ανάπτυξη του NCC-CY. Κατά την εκδήλωση, η οποία προσέλκυσε πέραν των 100 ενδιαφερομένων, ο Επίτροπος Επικοινωνιών, κ. Γιώργος Μιχαηλίδης, ανέδειξε τη στρατηγική σημασία του NCC-CY, εστιάζοντας στη δημιουργία της κοινότητας κυβερνοασφάλειας, την ετοιμασία σχεδίων χορηγιών και την υλοποίηση δράσεων εκπαίδευσης και ευαισθητοποίησης. Ο Υφυπουργός Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής, κ. Νικόδημος Δαμιανού, υπογράμμισε τη δέσμευση της πολιτείας για την ενίσχυση της κυβερνοασφάλειας και την αξιοποίηση των υπηρεσιών του Κέντρου από όλους τους ενδιαφερόμενους φορείς ενώ ο Εκτελεστικός Διευθυντής του Πανευρωπαϊκού Οργανισμού Κυβερνοασφάλειας, κ. Luca Tagliaretti, παρουσίασε το όραμα του Οργανισμού για την ενίσχυση της ευρωπαϊκής ακεραιότητας στον τομέα.

Αντιλαμβανόμενοι επίσης τη σημαντικότητα της εκπαίδευσης στην επιχειρηματικήςκοινότητα του τόπου, και μετά την επιτυχία των προηγούμενων κοινών δράσεων με το ΚΕΒΕ (Κυπριακού Εμπορικού και Βιομηχανικού Επιμελετηρίου) συνδιοργανώθηκε από κοινού με την ΑΨΑ το **δεύτερο Cybersecurity Weekend**, το οποίο πραγματοποιήθηκε τον Απρίλιου του 2024, στη Λάρνακα. Στο Cybersecurity Weekend συμμετείχαν συνολικά 20 άτομα από 10 εταιρείες, με εκπροσώπους τόσο από τη διοίκηση όσο και από τις τεχνικές ομάδες. Κατά τη διάρκεια του Cybersecurity Weekend οι συμμετέχοντες έλαβαν ολοκληρωμένες ενημερώσεις για διάφορα θέματα ασφάλειας στον κυβερνοχώρο από εμπειρογνώμονες ενώ παράλληλα ενημερώθηκαν σχετικά με το ρόλο της ΑΨΑ και για τις τελευταίες εξελίξεις του τομέα. Επιπλέον, πραγματοποιήθηκαν κατ' ιδίαν προσωπικές συναντήσεις (Business to Business - B2B) με επαγγελματίες του τομέα (μέλη της κοινότητας κυβερνοασφάλειας) παρέχοντας στους οργανισμούς την ευκαιρία για ανάπτυξη συνεργασιών. Το Νοέμβριο του ίδιου έτους, διοργανώθηκε το **τρίτο Cybersecurity Weekend** στην Αγία Νάπα σε συνεργασία και πάλι με το Επιμελητήριο, με επίκεντρο τον τομέα της υγείας. Στόχος του Cybersecurity Weekend ήταν η ενημέρωση και ευαισθητοποίηση των επιχειρήσεων σχετικά με τη νέα οδηγία NIS2. Για την επίτευξη αυτού του στόχου, η εκδήλωση περιελάβανε ενημερωτικές παρουσιάσεις, εκπαιδευτικές δραστηριότητες και B2B συναντήσεις με εξειδικευμένες εταιρείες κυβερνοασφάλειας, μέλη της κοινότητας κυβερνοασφάλειας του NCC-CY.

Επιπρόσθετα η Αρχή διοργάνωσε **ημερίδα για την Ευρωπαϊκή Πιστοποίηση Κυβερνοασφάλειας** συγκεντρώνοντας ομιλητές και επαγγελματίες τόσο από την Ευρωπαϊκή Επιτροπή και τον ENISA όσο και από τον ιδιωτικό τομέα με εμπειρία στα θέματα πιστοποίησης κυβερνοασφάλειας. Απώτερος στόχος της ημερίδας ήταν η ενημέρωση των συμμετεχόντων για τον Κανονισμό Πιστοποίησης Κυβερνοασφάλειας, τα καθήκοντα της ΑΨΑ ως Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας και γενικότερα ο ρόλος των διαφόρων εμπλεκόμενων μερών προωθώντας παράλληλα και τη συνεργασία στον τομέα των πιστοποιήσεων.

Στο πλαίσιο των προσπαθειών που καταβάλλει η ΑΨΑ για την προώθηση της κυβερνοασφάλειας ευρύτερα στην κοινωνία, συμμετείχε στο **Reflect Festival** που πραγματοποιήθηκε τον Μάιο στη Λεμεσό. Το Reflect Festival είναι η μεγαλύτερη εκδήλωση στον κλάδο της τεχνολογίας και της καινοτομίας στην Κύπρο, με τη συμμετοχή πέραν των 10.000 ενδιαφερομένων και μία από τις ταχύτερα αναπτυσσόμενες εκδηλώσεις στην περιοχή της Μεσογείου.

Η ΑΨΑ συμμετείχε με περίπτερο, αναδεικνύοντας τις δράσεις και την αποστολή της. Στόχος ήταν η προσέλκυση μελών στην κοινότητα κυβερνοασφάλειας και η ενημέρωση των ενδιαφερόμενων για τις μελλοντικές χρηματοδοτήσεις και τα οφέλη από τη συμμετοχή στα προγράμματα Digital Europe Program (DEP) και Horizon Europe Program (HEP).

Αξιοσημείωτη είναι επίσης η διοργάνωση από την ΑΨΑ του **1ου Cybersecurity for ALL Festival**, το οποίο πραγματοποιήθηκε στις 18 & 19 Οκτωβρίου στο Nicosia Mall και αποσκοπούσε στην ευαισθητοποίηση και ενημέρωση του κοινού για την ασφαλή χρήση του διαδικτύου και την αξία της κυβερνοασφάλειας. Κατά τη διάρκεια του Φεστιβάλ, πέραν των 4000 επισκεπτών είχαν την ευκαιρία να ενημερωθούν και να εξοικειωθούν με τον κόσμο της κυβερνοασφάλειας μέσω διαφόρων δράσεων και δραστηριοτήτων που ανέδειξαν τη σημασία της κυβερνοασφάλειας. Οι κύριοι στόχοι της εκδήλωσης περιλάμβαναν την ενημέρωση των παιδιών για τους κινδύνους του διαδικτύου και την ασφαλή χρήση του, την ενθάρρυνση των νέων να εξετάσουν την κυβερνοασφάλεια ως επαγγελματική επιλογή και η παροχή χρήσιμων συμβουλών στους γονείς για την προστασία των παιδιών τους στο διαδίκτυο. Εκπρόσωποι από σημαντικούς φορείς και οργανισμούς συμμετείχαν με περίπτερα στο Φεστιβάλ, μεταξύ των οποίων το Πανεπιστήμιο Κύπρου, η Αστυνομία Κύπρου - Υποδιεύθυνση Ηλεκτρονικού Εγκλήματος, το Cyprus Computer Society, το Κέντρο Ασφαλούς Διαδικτύου Κύπρου – Παιδαγωγικό Ινστιτούτο Κύπρου, η Εθνική Επιτροπή Περιβάλλον και Υγεία του Παιδιού και το Τεχνολογικό Πανεπιστήμιο Κύπρου.

Συνεχίζοντας, και μετά από πρωτοβουλία της Αρχής, με τη στήριξη του Υπουργείου Παιδείας, Αθλητισμού και Νεολαίας, η Κύπρος συμμετείχε στη **διεθνή εκπαιδευτική κατασκήνωση CyberWizards"**, η οποία διοργανώθηκε από το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας της Εσθονίας, το διάστημα 29 Ιουλίου έως 03 Αυγούστου 2024. Η δράση αυτή πραγματοποιήθηκε στα πλαίσια της ανάπτυξης συνεργασιών μεταξύ των Εθνικών Κέντρων Συντονισμού Κυβερνοασφάλειας (NCCs) αλλά και γενικότερα της πολιτικής του Οργανισμού μας για ανάπτυξη δράσεων ευαισθητοποίησης στον μαθητικό κόσμο. Η κατασκήνωση είχε ως στόχο την εκπαίδευση και ευαισθητοποίηση μαθητριών 13-16 ετών στον τομέα της κυβερνοασφάλειας. Με την υποστήριξη του ECCC, προσέφερε ένα ολοκληρωμένο εκπαιδευτικό πακέτο γνώσεων και δραστηριοτήτων στους συμμετέχοντες, με επίκεντρο την ασφάλεια στον κυβερνοχώρο, επιτρέποντας στους συμμετέχοντες να αποκτήσουν νέες γνώσεις και δεξιότητες σε θέματα όπως η ανάκτηση πληροφοριών, η αντιμετώπιση επιθέσεων στον κυβερνοχώρο, η προστασία του διαδικτύου και η χρήση λειτουργικών συστημάτων.

Εν κατακλείδι η ΑΨΑ, ετοίμασε και διένειμε πολυδιάστατο εκπαιδευτικό υλικό σε επιχειρήσεις, γονείς, δασκάλους και άτομα 65+ ετών με χρήσιμες συμβουλές, διαμορφωμένο ειδικά για να καλύπτει τις ανάγκες της κάθε ομάδας ξεχωριστά, τόσο σχεδιαστικά όσο και σε επίπεδο περιεχομένου.

9.2 Συμμετοχή της ΑΨΑ σε διεθνείς εκδηλώσεις

1ο Παγκόσμιο Συνέδριο Κυβερνοασφάλειας

Ενδεικτικά, στις 28 Μαρτίου 2024, η ΑΨΑ συμμετείχε στο 1ο Παγκόσμιο Συνέδριο Κυβερνοασφάλειας στη Λευκωσία. Το συνέδριο, συγκέντρωσε περισσότερους από 200 συμμετέχοντες και εστίασε στις προκλήσεις της κυβερνοασφάλειας στην εποχή της τεχνητής νοημοσύνης. Ο Επίτροπος Επικοινωνιών, κ. Γιώργος Μιχαηλίδης, και ο Προϊστάμενος της ΑΨΑ, κ. Διαμαντής Ζαφειριάδης, ως κεντρικοί ομιλητές τόνισαν τη σημασία του πολυδιάστατου ρόλου της ΑΨΑ.

Cyprus International Businesses Forum 2024

Επίσης στις 25 Ιουνίου 2024, διοργανώθηκε το «Διεθνές Επιχειρηματικό Φόρουμ Κύπρου» στη Λεμεσό, με τον Επίτροπο Επικοινωνιών, κ. Γιώργο Μιχαηλίδη να αναπτύσσει στην ομιλία του τις προτεραιότητες και πρωτοβουλίες της ΑΨΑ. Επίσης ο κ. Μιχαηλίδης συμμετείχε σε συζήτηση πάνελ για την κυβερνοασφάλεια στο επιχειρηματικό περιβάλλον, ενώ το Φόρουμ σε γενικότερα πλαίσια κάλυψε θεματικές όπως οι σχετικές ευρωπαϊκές νομοθεσίες, η τεχνητή νοημοσύνη, η κυβερνοασφάλεια και η διαχείριση ταλέντων.

2ο Πολωνό-Κυπριακό Φόρουμ Κυβερνοασφάλειας

Στα πλαίσια της προσπάθειας που καταβάλλεται για ανάπτυξη σχέσεων και συνεργειών με άλλες χώρες, η ΑΨΑ στήριξε και συμμετείχε στο φόρουμ Κύπρου - Πολωνίας: "POLCYBER 2024", που επικεντρώθηκε στον τομέα της κυβερνοασφάλειας. Η εκδήλωση πραγματοποιήθηκε τον Ιούνιο του 2024 στο ΚΕΒΕ και οι παρευρισκόμενοι είχαν την ευκαιρία να ενημερωθούν μεταξύ άλλων και για τις δράσεις και τις αρμοδιότητες του NCC-CY.

4ο Συνέδριο Κυβερνοασφάλειας

Τον Σεπτέμβριο του 2024, πραγματοποιήθηκε το 4ο Συνέδριο Κυβερνοασφάλειας, το οποίο τελέστηκε υπό την αιγίδα της ΑΨΑ, με τίτλο «Προστατεύοντας το Ψηφιακό σας Φρούριο». Το συνέδριο επικεντρώθηκε στη διαχείριση κυβερνοαπειλών με τον κ. Ζαφειριάδη να αναπτύσσει το θέμα «Κρίσιμες Υποδομές και Οδηγία NIS2», ενώ παράλληλα η ΑΨΑ διένειμε ενημερωτικό υλικό στον ειδικά διαμορφωμένο εκθεσιακό της χώρο.

9η Κοινή Συνάντηση Τομέων Αγροδιατροφής & Ψηφιοποίησης (EEN)

Όπως είναι εύκολα αντιληπτό, η ανάπτυξη συνεργασιών με άλλους ευρωπαϊκούς θεσμούς είναι εξαιρετικά σημαντικός πυλώνας στην επίτευξη των στόχων της ΑΨΑ. Σε αυτά τα πλαίσια, τον Οκτώβριο του 2024 η ΑΨΑ συμμετείχε στην 9η Κοινή Συνάντηση των Τομέων Αγροδιατροφής & Ψηφιοποίησης του Enterprise Europe Network (EEN), η οποία πραγματοποιήθηκε στην Κύπρο, προβάλλοντας τη σημαντικότητα της ανάπτυξης ουσιαστικών συνεργασιών μεταξύ των NCCs και των EENs. Στη συνάντηση συμμετείχαν πέραν των 120 εκπροσώπων των EEN από όλες τις ευρωπαϊκές χώρες.

Cybertech Europe 2024

Η Αρχή συμμετείχε στο συνέδριο Cybertech Europe 2024, το οποίο πραγματοποιήθηκε στη Ρώμη, με τον Επίτροπο Επικοινωνιών κ. Γιώργο Μιχαηλίδη να λαμβάνει μέρος ως κεντρικός ομιλητής στην ενότητα "Cyber and the European Angle", τον Οκτώβριο του 2024. Κατά την παρέμβασή του, αναδείχθηκε η ευρωπαϊκή διάσταση των πολιτικών και πρωτοβουλιών στον τομέα της κυβερνοασφάλειας. Το συνέδριο αποτέλεσε σημείο αναφοράς για τις τελευταίες εξελίξεις στο συνεχώς μεταβαλλόμενο τοπίο της κυβερνοασφάλειας, συγκεντρώνοντας ηγετικές προσωπικότητες, καινοτόμους και επαγγελματίες από όλη την Ευρώπη και τον κόσμο.

Διεθνής Ένωση Τηλεπικοινωνιών (ITU) - "Global Symposium for Regulators 2024"

Η Αρχή συμμετείχε στο Παγκόσμιο Συμπόσιο Ρυθμιστικών Αρχών 2024 ("Global Symposium for Regulators 2024" – GSR-24) της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU), με τον Βοηθό Επίτροπο Επικοινωνιών και Πρόεδρο της "Ευρωπαϊκής και Μεσογειακής Ομάδας Ρυθμιστών Τηλεπικοινωνιών" (EMERG) κ. Πέτρο Γαλίδη να παραχωρεί συνέντευξη στον Maximillian Jacobson-Gonzalez, Senior Communications Officer της ITU. Κατά τη διάρκεια της συνέντευξης, ο κ. Γαλίδης αναφέρθηκε στα βασικά συμπεράσματα της συνεδρίας "Mastering Digital Transformation" (Session 4), την οποία συντόνισε εκπροσωπώντας την Προεδρία του EMERG για το 2024. Επίσης, ανέδειξε τον ρόλο και τις προτεραιότητες του EMERG, καθώς και τη σημασία της περιφερειακής συνεργασίας για την επίτευξη καθολικής, ουσιαστικής και σχετικής συνδεσιμότητας, ως καταλύτη για την επιτάχυνση του Ψηφιακού Μετασχηματισμού.

6ο Cybersecurity Forum

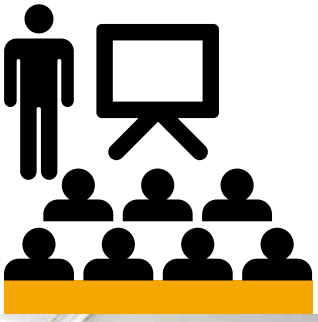
Η Αρχή συμμετείχε στο 6ο Cybersecurity Forum, το οποίο πραγματοποιήθηκε τον Σεπτέμβριο στο Karpacz της Πολωνίας, στο πλαίσιο του 33ου Οικονομικού Φόρουμ. Το Forum επικεντρώθηκε σε στρατηγικά ζητήματα κυβερνοασφάλειας, προωθώντας τον διάλογο και την ανταλλαγή καλών πρακτικών μεταξύ φορέων από την Ευρώπη και διεθνώς. Κατά τη διάρκεια του συνεδρίου, παρουσιάστηκαν καινοτόμα ευρωπαϊκά έργα, δράσεις χρηματοδότησης τρίτων, και νέες προτάσεις στο πλαίσιο των προγραμμάτων DEP και HEP, ενώ παράλληλα συζητήθηκαν η συνεργασία με τον ερευνητικό και δημόσιο τομέα, η πιστοποίηση και η ενίσχυση των ΜμΕ.

Bucharest Cybersecurity Conference (BCC2024)

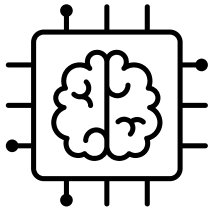
Η Αρχή συμμετείχε στο συνέδριο Bucharest Cybersecurity Conference (BCC2024), που πραγματοποιήθηκε τον Οκτώβριο στο Βουκουρέστι, με τη διοργάνωση της Ρουμανικής Διεύθυνσης Κυβερνοασφάλειας (DNSC) και τη συνεργασία του NCC-Romania, του ENISA και του ECCC. Ο Επίτροπος Επικοινωνιών συμμετείχε ως ομιλητής, συμβάλλοντας στον ευρωπαϊκό διάλογο για την κυβερνοασφάλεια. Το συνέδριο συγκέντρωσε υψηλόβαθμους εκπροσώπους από την Ευρώπη και διεθνώς, εστιάζοντας στην εφαρμογή της ευρωπαϊκής πολιτικής για την κυβερνοασφάλεια, όπως η Οδηγία NIS2 και οι Κανονισμοί Cyber Resilience Act και Cyber Solidarity Act. Συζητήθηκαν επίσης ζητήματα τεχνητής νοημοσύνης, ασφάλειας κρίσιμων υποδομών και διεθνούς συνεργασίας, ενώ η τρίτη ημέρα ήταν αφιερωμένη στο συνέδριο “Cybersecurity Resilience & Market 2024” της ENISA και του ECCC.

9.3 Διοργάνωση Εκπαιδεύσεων

Καθώς η ενίσχυση της γνώσης και της ευαισθητοποίησης γύρω από θέματα κυβερνοασφάλειας παραμένει στρατηγικός στόχος της ΑΨΑ, το 2024, η Αρχή διοργάνωσε στοχευμένα εκπαιδευτικά σεμινάρια για μαθητές, γονείς και επαγγελματίες, αξιοποιώντας διαδραστικές μεθόδους, ενώ υποστήριξε και εξειδικευμένες θεματικές εκδηλώσεις, όπως η σχέση Τεχνητής Νοημοσύνης και κυβερνοασφάλειας, προάγοντας τη διάχυση της γνώσης σε μεγάλο φάσμα της κοινωνίας.



Συγκεκριμένα η Αρχή μέσω του **Ευρωπαϊκού έργου CYberSafety IV** πραγματοποιεί διαδραστικά εκπαιδευτικά σεμινάρια σε μαθητές, γονείς, εκπαιδευτικούς και σε άτομα που εργάζονται με παιδιά με στόχο να προάγει την καλύτερη και ασφαλέστερη και υπεύθυνη χρήση του Διαδικτύου. Κατά το έτος 2024, η ΑΨΑ επισκέφθηκε δεκαοκτώ (18) διαφορετικά σχολεία, πραγματοποιώντας εικοσιτέσσερα (24) ξεχωριστά σεμινάρια μετά το πέρας των οποίων, οι μαθητές είχαν τη δυνατότητα να διαγωνιστούν σε ένα παιχνίδι γνώσεων κυβερνοασφάλειας μέσω της εξειδικευμένης πλατφόρμας Kahoot.



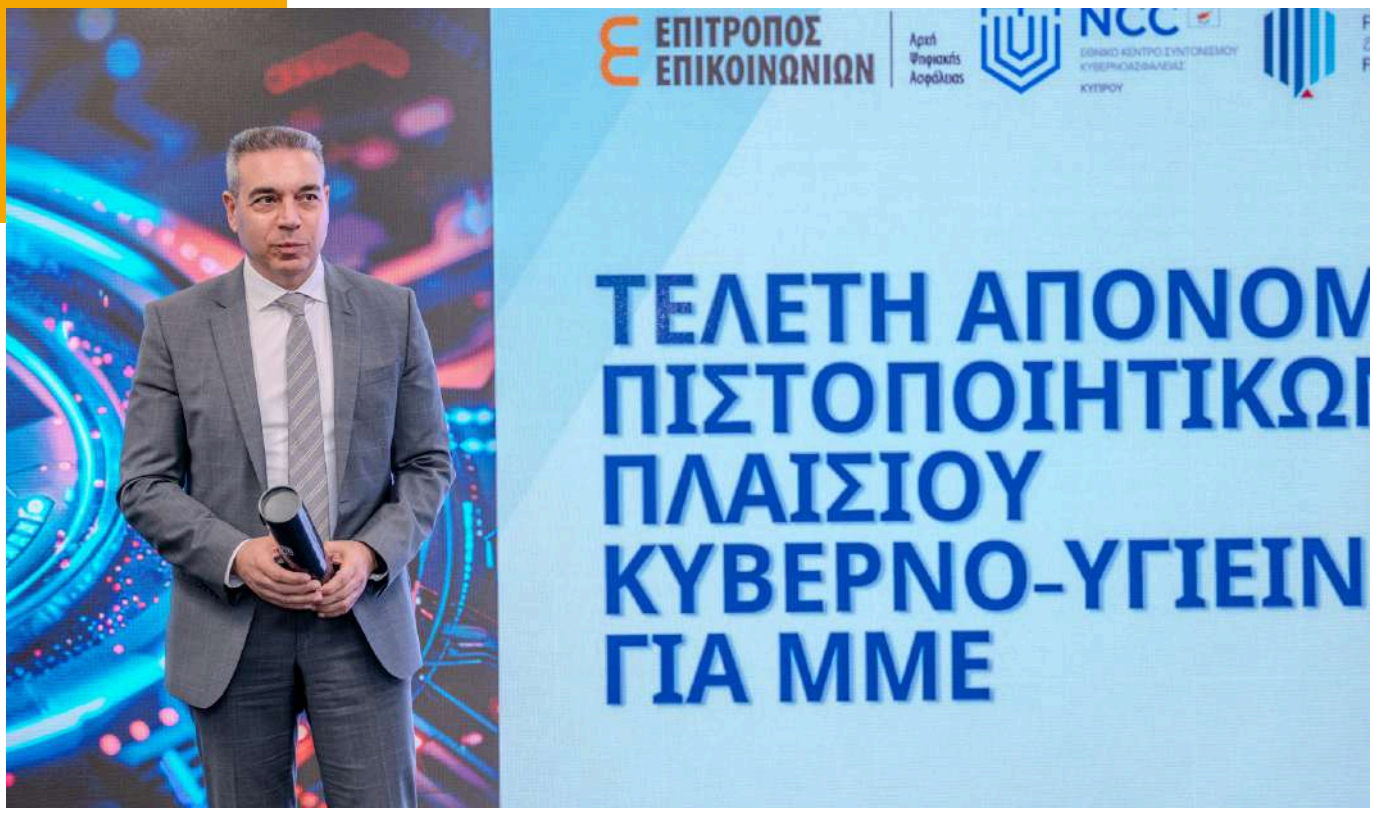
Προχωρώντας σε εξειδικευμένες θεματικές, η ΑΨΑ υποστήριξε κατά τον Ιούνιο το σεμινάριο **«AI & Cybersecurity: Facts and the Future Landscape»**, που διοργανώθηκε από το DiGiNN στη Λευκωσία. Σε αυτό συμμετείχαν πάνω από 80 άτομα από τον δημόσιο και ιδιωτικό τομέα, με στόχο την ανάλυση των κυβερνοαπειλών που σχετίζονται με την Τεχνητή Νοημοσύνη.

9.4 Σχέδια χορηγιών προς τρίτους

Στο πλαίσιο της προσπάθειας που καταβάλλει η ΑΨΑ για ενίσχυση της κυβερνοασφάλειας στις ΜμΕ, ολοκληρώθηκε σε συνεργασία με το ΙδΕΚ κατά το 2024 το σχέδιο χορηγιών «Ενίσχυση Κυβερνοασφάλειας στις Κυπριακές ΜμΕ 2023», με προϋπολογισμό 1.000.000 ευρώ.

Η πρόσκληση συγχρηματοδοτήθηκε από την Κυπριακή Δημοκρατία και το Πρόγραμμα «Ψηφιακή Ευρώπη» της ΕΕ, στο πλαίσιο του έργου «N4CY-Development of the National Cybersecurity Coordination Centre of the Republic of Cyprus». Ως συνέχεια της πρωτοβουλίας αυτής, στις 20 Νοεμβρίου 2024, στο πλαίσιο του συνεδρίου «Αναπτύσσοντας δεξιότητες στον τομέα της Κυβερνοασφάλειας», πραγματοποιήθηκε η τελετή απονομής των πιστοποιητικών στις δεκαεννέα (19) εταιρείες που ολοκλήρωσαν επιτυχώς τις πιστοποιήσεις τους σύμφωνα με το Πλαίσιο Κυβερνο-Υγιεινής για ΜμΕ του NCC-CY και έλαβαν χρηματοδότηση μέσω του σχεδίου.

Το Πλαίσιο κυβερνο-υγιεινής για ΜμΕ, είναι ένα σύστημα πιστοποίησης που περιλαμβάνει έντεκα (11) βασικά μέτρα ελέγχου. Αυτά τα μέτρα έχουν σχεδιαστεί για να ενισχύσουν την κυβερνοασφάλεια των ΜμΕ, καλύπτοντας τομείς όπως η διαχείριση πρόσβασης, η ασφάλεια δικτύου, η ενημέρωση λογισμικού, η προστασία από κακόβουλο λογισμικό, η διαχείριση ταυτότητας, η ασφάλεια εφαρμογών, η διαχείριση περιστατικών, η συντήρηση αντιγράφων ασφαλείας, η ασφάλεια κατά την ανάπτυξη συστημάτων, η κρυπτογράφηση και η διαχείριση προμηθευτών.



10 ΑΚΑΔΗΜΙΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

Η Ακαδημία ICT αποτελεί τον κεντρικό εκπαιδευτικό βραχίονα του Γραφείου Επιτρόπου Επικοινωνιών, προσφέροντας εξειδικευμένα προγράμματα κατάρτισης, εκδηλώσεις ευαισθητοποίησης και άλλες καινοτόμες δράσεις. Η ενσωμάτωση νέων τεχνολογιών και η υιοθέτηση ψηφιακών εργαλείων αναβάθμισαν τη λειτουργία της Ακαδημίας, καθιστώντας την βασικό πυλώνα γνώσης και εκπαίδευσης στην Κύπρο.

10.1 Δράσεις ανάπτυξης της Ακαδημίας

Κατά το 2024 υλοποιήθηκε μεγάλος αριθμός εκδηλώσεων και εκπαιδεύσεων, με την ανάληψη καινοτόμων πρωτοβουλιών ιδιαίτερα κατά τον πανευρωπαϊκό μήνα κυβερνοασφάλειας καθώς επίσης και για την ανάπτυξη του μουσείου του Γραφείου του Επιτρόπου Επικοινωνιών.

150

ΣΥΝΟΛΙΚΕΣ ΕΚΔΗΛΩΣΕΙΣ

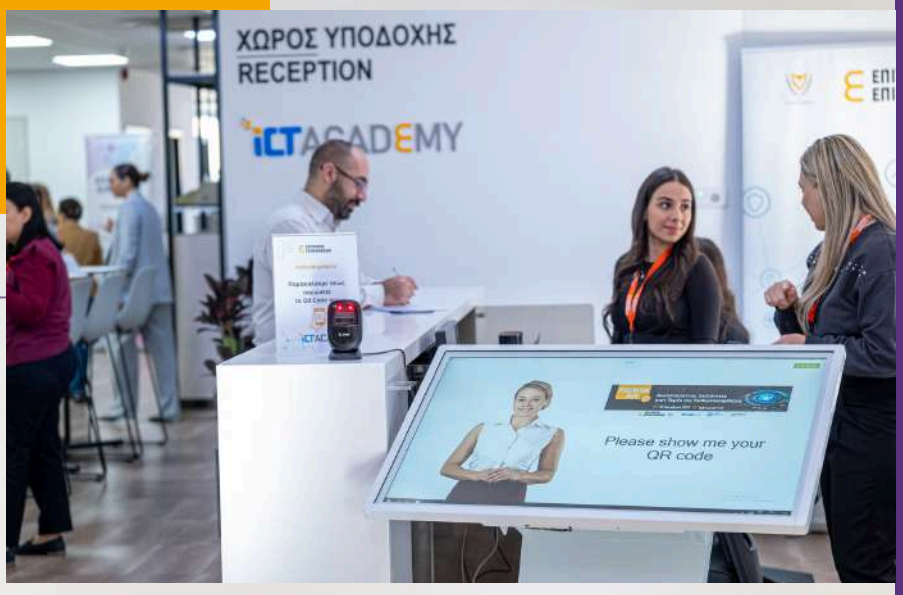
4.000

ΣΥΝΟΛΙΚΟΣ ΑΡΙΘΜΟΣ ΣΥΜΜΕΤΕΧΟΝΤΩΝ

Σηματοδοτώντας τον 1ο χρόνο λειτουργίας του ICT, το 2024 υπήρξε μια εξαιρετικά δυναμική χρονιά καθώς ολοκληρώθηκαν 150 εκδηλώσεις που προσέλκυσαν περισσότερους από 4000 συμμετέχοντες από την Κύπρο και το εξωτερικό.

Ιδιαίτερα σημαντική ήταν η συμμετοχή της ΑΨΑ στην ετήσια εκστρατεία του **Ευρωπαϊκού Μήνα Κυβερνοασφάλειας (ECSM)**, ενισχύοντας την ευαισθητοποίηση για την ασφάλεια στο διαδίκτυο. Σε αυτό το πλαίσιο, διοργανώθηκαν εκδηλώσεις όπως η ημερίδα **«Boosting SMEs Cybersecurity Resilience»**, το συνέδριο **«European Cybersecurity Certification Day»** και το συνέδριο **«Cybersecurity in the AI Era»**. Επιπλέον, πραγματοποιήθηκε η Εναρκτήρια Εκδήλωση της Κοινότητας Κυβερνοασφάλειας, του NCC-CY, η οποία σηματοδότησε την επίσημη έναρξη της καθώς και το **3ο Cybersecurity Weekend** σε συνεργασία με το ΚΕΒΕ το οποίο αποσκοπούσε στην ενημέρωση του τομέα της υγείας για τη νέα Ευρωπαϊκή Οδηγία NIS2. Επίσης, στο πλαίσιο της **Διεθνούς Έκθεσης Βιβλίου** στη Λεμεσό, παρουσιάστηκε το παιδικό παραμύθι της ΑΨΑ **«Η Φοίβη στην Αρχή Ψηφιακής Ασφάλειας»**, ως ένα ακόμη εργαλείο εκπαίδευσης και ευαισθητοποίησης των παιδιών για την ασφαλή πλοήγηση στο διαδίκτυο, που συγγράφηκε και εκτυπώθηκε κατά το 2024. Οι δράσεις κορυφώθηκαν με το πρωτοποριακό **«Cybersecurity for ALL Festival»**, που προσέλκυσε πάνω από 4000 επισκέπτες, απευθυνόμενο στο ευρύ κοινό και ειδικότερα στις οικογένειες και τα παιδιά. Περισσότερες λεπτομέρειες για αυτές τις δράσεις αναφέρονται σε προηγούμενες ενότητες.

Η ΑΨΑ επενδύει επίσης συνεχώς στη βελτίωση των εγκαταστάσεων και των υπηρεσιών της Ακαδημίας. Το 2024, ολοκληρώθηκαν εκτεταμένες αναβαθμίσεις, όπως η δημιουργία νέου λογότυπου, η ανάπτυξη της ιστοσελίδας **ictacademy.cy**, η εφαρμογή εξειδικευμένης πλατφόρμας διαχείρισης εκδηλώσεων και η εισαγωγή αυτοματοποιημένου συστήματος προσέλευσης. Παράλληλα, εγκαταστάθηκαν νέες ψηφιακές οθόνες ενημέρωσης, βελτιώθηκαν οι δικτυακές υποδομές και προστέθηκε προηγμένος τεχνικός εξοπλισμός, ενισχύοντας την εμπειρία των συμμετεχόντων.



Συμπληρωματικά, και σε ειδικά διαμορφωμένο εκθεσιακό χώρο εντός της Ακαδημίας, δημιουργήθηκε κατά το 2024 μουσείο, που αναδεικνύει την ιστορία και την εξέλιξη των επικοινωνιών και των ταχυδρομείων. Οι επισκέπτες μπορούν να ανακαλύψουν σπάνια εκθέματα, όπως παλιούς υπολογιστές, κινητά τηλέφωνα και άλλα ιστορικά αντικείμενα, αποκτώντας μια ολοκληρωμένη εικόνα της τεχνολογικής εξέλιξης στην Κύπρο. Ο χώρος συνδυάζει την παράδοση με τις σύγχρονες τεχνολογικές καινοτομίες, προσφέροντας μια βιωματική εμπειρία στους επισκέπτες.

11 ΜΑΚΡΟΠΡΟΘΕΣΜΟΙ ΣΤΟΧΟΙ *ΧΤΙΖΟΝΤΑΣ ΤΟ ΑΥΡΙΟ ΣΤΗΝ ΑΨΑ*

Η ΑΨΑ, προσηλωμένη στη συνεχή εξέλιξη και ενίσχυση του τομέα της κυβερνοασφάλειας, χαράζει μια στρατηγική πορεία ανάπτυξης με έμφαση στην έρευνα και την καινοτομία. Μέσω των μακροπρόθεσμων στόχων της, επιδιώκει να ενισχύσει τη θέση της Κύπρου ως ένα ισχυρό κόμβο κυβερνοασφάλειας και να εδραιώσει το οικοσύστημα των εμπλεκόμενων φορέων, τόσο σε εθνικό όσο και σε διεθνές επίπεδο.

11.1 Έρευνα, Καινοτομία και Συμμετοχή σε Ευρωπαϊκά Συγχρηματοδοτούμενα Προγράμματα

Η Αρχή επενδύει συστηματικά στην έρευνα και την καινοτομία ως βασικούς μοχλούς ενίσχυσης της κυβερνοανθεκτικότητας της χώρας και διατήρησης της τεχνολογικής ετοιμότητας σε εθνικό και ευρωπαϊκό επίπεδο. Το 2024, μέσω της ενεργού συμμετοχής της σε συγχρηματοδοτούμενα έργα, ενίσχυσε τη συνεργασία, υποστήριξε την ανάπτυξη Κέντρων Επιχειρήσεων Κυβερνοασφάλειας και αξιοποίησε ευρωπαϊκούς μηχανισμούς για την ενίσχυση εθνικών δομών και υποδομών, συμμετέχοντας ενεργά τόσο ως συντονιστής όσο και ως εταίρος.

Συμμετοχή σε Ευρωπαϊκά Συγχρηματοδοτούμενα Προγράμματα ως Συντονιστές

Ευρωπαϊκό Έργο N4CY2

Κατά το έτος 2024 η ΑΨΑ κατέθεσε επιτυχώς πρόταση μέσω του προγράμματος «Ψηφιακή Ευρώπη», για ενίσχυση των δράσεων του NCC-CY με συνολικό προϋπολογισμό 7.676.690 ευρώ μέσω του προγράμματος N4CY2. Το ευρωπαϊκό έργο N4CY2, το οποίο αποτελεί συνέχεια του επιτυχημένου προγράμματος N4CY θα ξεκινήσει επίσημα την 1η Ιανουαρίου 2025 και θα θέσει τις βάσεις για περαιτέρω ανάπτυξη και ενίσχυση του τομέα της κυβερνοασφάλειας σε εθνικό και ευρωπαϊκό επίπεδο. Οι στόχοι του N4CY2 περιλαμβάνουν την ανάπτυξη του οικοσυστήματος κυβερνοασφάλειας στην Κύπρο μέσω της προώθησης και ενίσχυσης συνεργασιών με εθνικούς και διεθνείς εταίρους, την παροχή σχεδίων χορηγιών προς τρίτους, την ευαισθητοποίηση και εκπαίδευση μέσω της διοργάνωσης δράσεων και προγραμμάτων που θα ενισχύσουν την ανθεκτικότητα της κοινωνίας απέναντι στις σύγχρονες κυβερνοαπειλές, καθώς και την υλοποίηση πρωτοποριακών δράσεων που θα συμβάλλουν στη δημιουργία ενός ασφαλούς ψηφιακού περιβάλλοντος σε εθνικό και ευρωπαϊκό επίπεδο. Επιπλέον, το έργο N4CY2 περιλαμβάνει την περαιτέρω ανάπτυξη της Κοινότητας Κυβερνοασφάλειας καθώς επίσης και την ενίσχυση τουΓραφείου Υποστήριξης (Help Desk), το οποίο ήδη παρέχει υποστήριξη και καθοδήγηση σε οργανισμούς, μικρομεσαίες επιχειρήσεις και πολίτες για τα προγράμματα DEP και HEP.

Ευρωπαϊκό Έργο europeAn THreat intelligence, rEspoNse and prepAredness platform (ATHENA)

Το έργο ATHENA, άρχισε τον Ιανουάριο του 2024 και αποτελεί μια στρατηγικής σημασίας πρωτοβουλία, η οποία αποσκοπεί στην ανάπτυξη μιας από τις δύο πρώτες ενιαίες ευρωπαϊκές πλατφόρμες πληροφόρησης, αντίδρασης και επιχειρησιακής ετοιμότητας για την αντιμετώπιση απειλών στον κυβερνοχώρο, σύμφωνα με την πράξη αλληλεγγύης στον κυβερνοχώρο (Cyber Solidarity ACT) της Ευρωπαϊκής Ένωσης. Η πρόταση ATHENA έχει υιοθετήσει ένα προσχέδιο Κέντρων Επιχειρήσεων Κυβερνοασφάλειας για διασυνοριακή συνεργασία και συντονισμό, με σκοπό τη δημιουργία ενός συμπλέγματος συντονισμένης απόκρισης για τα κράτη μέλη της ΕΕ και άλλες επιλέξιμες οντότητες. Η ΑΨΑ κατέχει το ρόλο του συντονιστή ενώ συμμετέχουν επίσης οι Εθνικές Αρχές κυβερνοασφάλειας της Ελλάδας, της Βουλγαρίας και της Μάλτας. Κατά το έτος 2024, ολοκληρώθηκε με επιτυχία το σχέδιο αρχιτεκτονικής για την υλοποίηση του διασυνοριακού Κέντρου Επιχειρήσεων Κυβερνοασφάλειας, σε επίπεδο κεντρικής υποδομής (που αποτελεί τον βασικό κορμό της αρχιτεκτονικής) καθώς και στις επιμέρους εγκαταστάσεις των εμπλεκόμενων φορέων. Το έργο θα διαρκέσει 36 μήνες και ο συνολικός προϋπολογισμός για το κόστος λειτουργίας και ανάπτυξης, υλικό, και υπηρεσίες ανέρχεται σε 10.457.086,79€.

Ευρωπαϊκό Έργο CY TRUST

Το CY-TRUST, άρχισε τον Νοέμβριο του 2023 και ο στόχος του είναι η ενίσχυση της ικανότητας της Κυπριακής Δημοκρατίας να προστατεύει τις υποδομές και τους πολίτες της από κυβερνοαπειλές, μέσω της δημιουργίας Τομεακών Κέντρων Επιχειρήσεων Κυβερνοασφάλειας (Τομεακά SOCs), που θα καλύπτουν 4 τομείς (συμπεριλαμβανομένων της Ενέργειας, της Ναυτιλίας, των Κυβερνητικών υποδομών και των ΜμΕ). Το έργο αυτό θα ακολουθήσει και θα υιοθετήσει το προτεινόμενο Σχέδιο Κέντρων Επιχειρήσεων Κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης για διασυνοριακό συντονισμό και συνεργασία, συνδυάζοντας ικανότητες για κοινή αντίληψη κατάστασης, συντονισμένη διαχείριση περιστατικών, και κοινή προετοιμασία. Επιπλέον, με έμφαση στην υιοθέτηση ευρωπαϊκών και διεθνών προτύπων, τα Τομεακά SOCs του CY-TRUST θα διευκολύνουν την καθιέρωση του απαιτούμενου επιπέδου διαλειτουργικότητας, συνεργασίας και συντονισμού σε όλα τα επίπεδα άμυνας, εργαλείων, διαδικασιών και ανθρωπίνου δυναμικού. Το 2024, ολοκληρώθηκε με επιτυχία το σχέδιο αρχιτεκτονικής για τα Τομεακά SOCs, εναρμονιζόμενο με τις απαιτήσεις των τεσσάρων τομέων (Ενέργεια, Ναυτιλία, Κυβέρνηση και ΜμΕ), και θέτοντας τις βάσεις για την επόμενη φάση της υλοποίησης του έργου. Το έργο θα διαρκέσει 36 μήνες και ο συνολικός προϋπολογισμός για το κόστος λειτουργίας και ανάπτυξης, υλικό, και υπηρεσίες ανέρχεται σε €3,864,583.20 ευρώ.

Συμμετοχή σε Ευρωπαϊκά Συγχρηματοδοτούμενα Προγράμματα ως Εταίροι

Αρ.	Έργο	Στόχοι	Συνολικός Προϋπολογισμός
1	Synapse HORIZON-CL3-2022-CS-01 Διάρκεια Έργου: 01/11/2023 - 31/10/2026	Μια Ολοκληρωμένη Πλατφόρμα Διαχείρισης Κινδύνου και Ανθεκτικότητας Κυβερνοασφάλειας, με Ολιστική Επίγνωση Κατάστασης, Ικανότητες Αντιμετώπισης Περιστατικών και Προετοιμασίας	Συνολικός προϋπολογισμός έργου: €7,629,500. Εγκεκριμένος Προϋπολογισμός ΑΨΑ: €261,250 Η χρηματοδότηση καλύπτεται πλήρως (100%) από την Ευρωπαϊκή Ένωση
2	PHOENIIX HORIZON-CL3-2021-CS-01 Διάρκεια Έργου: 01/07/2022 - 30/06/2026	Ένα Ευρωπαϊκό πλαίσιο Κυβερνοανθεκτικότητας με Ορχήστρωση και Αυτοματοποίηση Υποβοηθούμενη από Τεχνητή Νοημοσύνη για τη Συνεχή Επιχειρησιακή Λειτουργία, Αντιμετώπιση Περιστατικών και Ανταλλαγή Πληροφοριών	Συνολικός προϋπολογισμός έργου: €4,825,000 Εγκεκριμένος Προϋπολογισμός ΑΨΑ: €141,125 Η χρηματοδότηση καλύπτεται πλήρως (100%) από την Ευρωπαϊκή Ένωση
3	5G TACTIC DIGITAL-ECCC-2022-CYBER-03 Διάρκεια Έργου: 01/12/2023 - 30/11/2026	5G Υπηρεσίες Αξιόπιστων και Ασφαλών Δικτύων	Συνολικός προϋπολογισμός έργου: €5.211.185 Εγκεκριμένος Προϋπολογισμός ΑΨΑ: €172,270 Συγχρηματοδοτούμενο έργο με ποσοστό κάλυψης 50%.
4	CYBER SYNCHRONY DIGITAL-ECCC-2023-DEPLOY-CYBER-04 Διάρκεια Έργου: 01/06/2024 - 31/05/2027	Στοχεύει ένα ολιστικό πλαίσιο που συνδυάζει πρωτοποριακές τεχνολογίες για την ανάπτυξη μιας ενιαίας και ανθεκτικής υποδομής κυβερνοασφάλειας.	Συνολικός Προϋπολογισμός έργου: €6.998.153 Εγκεκριμένος Προϋπολογισμός ΑΨΑ: €167,391 Συγχρηματοδοτούμενο έργο με ποσοστό κάλυψης 50%.
5	2020-EU-IA-0219 **CEF Telecom** (2014-2020) Διάρκεια Έργου: 01/08/2021 - 31/07/2024	Κοινή Πλατφόρμα Επιχειρήσεων Κυβερνοασφάλειας (JCOP)	Συνολικός Προϋπολογισμός έργου: €1.700.227 Εγκεκριμένος Προϋπολογισμός ΑΨΑ: €200,625 Συγχρηματοδοτούμενο έργο με ποσοστό κάλυψης 75%.

Αρ.	Έργο	Στόχοι	Συνολικός Προϋπολογισμός
6	DIGITAL-2021-QCI-01 Διάρκεια Έργου:01/01/2023 - 31/08/2025	Κυπριακή Υποδομή Κβαντικών Επικοινωνιών	Συνολικός Προϋπολογισμός έργου €7.512.843 Εγκεκριμένος Προϋπολογισμός ΑΨΑ: €75,852 Συγχρηματοδοτούμενο έργο με ποσοστό κάλυψης 100%.
7	DIGITAL-2023-DEPLOY-04 Διάρκεια Έργου: 01/10/2024 - 31/03/2026	Κυπριακό Κέντρο Ασφαλούς Διαδικτύου	Συνολικός Προϋπολογισμός έργου €977.370 Εγκεκριμένος Προϋπολογισμός ΑΨΑ: €33,919 Συγχρηματοδοτούμενο έργο με ποσοστό κάλυψης 50%.
8	DIGITAL-ECCC-2023-CYBER-04 Διάρκεια Έργου: 01/09/2024 - 31/08/2027	Ανάπτυξη του Εθνικού Κέντρου Συντονισμού Κυβερνοασφάλειας της Δημοκρατίας της Κύπρου Ενοποίηση και Αναβάθμιση των Δυνατοτήτων Πιστοποίησης σε όλη την Ευρώπη	Συνολικός Προϋπολογισμός έργου €3.169.019 Εγκεκριμένος Προϋπολογισμός ΑΨΑ: €153,887 Συγχρηματοδοτούμενο έργο με ποσοστό κάλυψης 50%.
9	DIGITAL-ECCC-2022-CYBER-03 Διάρκεια Έργου: 01/01/2024 - 31/12/2026	Εστιάζει στη δημιουργία μιας προσαρμοσμένης ομοσπονδιακής πλατφόρμας εύρους κυβερνοασφάλειας. Η πλατφόρμα θα προσφέρει καινοτόμα εκπαιδευτικά προγράμματα σε οργανισμούς κρίσιμων υποδομών για την ανάπτυξη εξειδικευμένου εργατικού δυναμικού στην άμυνα του κυβερνοχώρου και τη συνεργατική αντιμετώπιση.	Συνολικός προϋπολογισμός του έργου: €3.537.827 Εγκεκριμένος Προϋπολογισμός ΑΨΑ: €502.986 Συγχρηματοδοτούμενο έργο με ποσοστό κάλυψης 50%.
10	DIGITAL-ECCC-2024-DEPLOY-CYBER-06 Διάρκεια Έργου: 10/12/2024 - 31/05/2026	Εστιάζει στην υποστήριξη της εφαρμογής του Cyber Resilience Act μέσω της ανάπτυξης καινοτόμων εργαλείων συμμόρφωσης και αξιολόγησης κινδύνων.	Συνολικός Προϋπολογισμός έργου €3.442.597 Εγκεκριμένος Προϋπολογισμός ΑΨΑ: €184,768 Συγχρηματοδοτούμενο έργο με ποσοστό κάλυψης 50%.

22

Ευρωπαϊκά Έργα από τη σύσταση της ΑΨΑ

€73.1 εκατ.

Συνολικός προϋπολογισμός έργων

€31.3 εκατ.

Συνολικός προϋπολογισμός για τις κυπριακές οντότητες

Αρχή Ψηφιακής Ασφάλειας

€11.99 εκατ.

Συνολικός προϋπολογισμός για την ΑΨΑ

Σχεδιάζοντας το μέλλον και αντιλαμβανόμενη επίσης την αναγκαιότητα για υιοθέτηση σύγχρονων πρακτικών μάθησης, η ΑΨΑ προγραμματίζει επίσης την ενσωμάτωση στην Ακαδημία ICT, καινοτόμων-διαδραστικών τεχνολογιών, όπως η εικονική πραγματικότητα (VR) καθώς και την ανάπτυξη εκπαιδευτικών πλατφόρμων. Επιπλέον, δρομολογούνται πρωτοβουλίες για τη φιλοξενία διεθνών εκδηλώσεων και επιτροπών, ενισχύοντας περαιτέρω τη θέση της Ακαδημίας ICT ως κέντρο αριστείας στην εκπαίδευση και την τεχνολογία σε περιφερειακό επίπεδο.

11.2 Προώθηση Επαγγέλματος

Περεταίρω, η καλλιέργεια και ανάδειξη του επαγγέλματος της κυβερνοασφάλειας αποτελεί ουσιαστική προτεραιότητα για την ΑΨΑ, η οποία επενδύει στη δημιουργία ευκαιριών για νέους επαγγελματίες και στην ενίσχυση της συμμετοχής όλων στον κλάδο. Το 2024, αναπτύχθηκαν στοχευμένες πρωτοβουλίες συνεργασίας με πανεπιστημιακά ιδρύματα και ευρωπαϊκά δίκτυα, με στόχο την προώθηση της καινοτομίας, της ισότητας και της διασύνδεσης της ακαδημαϊκής κοινότητας με την αγορά εργασίας.

Προς αυτή την κατεύθυνση, η συνεργασία με ακαδημαϊκά ιδρύματα αποτελεί βασικό πυλώνα για τον σχεδιασμό του μέλλοντος καθώς και για την προώθηση της καινοτομίας και της αριστείας. Στα πλαίσια αυτά κατά το 2024 η ΑΨΑ σύστησε την **Επιτροπή Πανεπιστημίων**, στην οποία συμμετέχουν όλα τα πανεπιστήμια της Κύπρου τόσο του ιδιωτικού όσο και του δημόσιου τομέα. Τον Ιανουάριο και τον Μάιο του 2024 πραγματοποιήθηκαν δύο διαδικτυακές συναντήσεις με σκοπό τη διερεύνηση κοινών πρωτοβουλιών και δραστηριοτήτων, εστιάζοντας στην ενίσχυση της συνεργασίας μεταξύ της ΑΨΑ και των ακαδημαϊκών ιδρυμάτων. Οι βασικοί άξονες συζήτησης περιλάμβαναν τη συνδιοργάνωση θερινών σχολείων, τη συμμετοχή των πανεπιστημίων σε εκδηλώσεις της ΑΨΑ ως ομιλητές ή εκπαιδευτές, καθώς και την ανάπτυξη κοινών δράσεων ευαισθητοποίησης και προώθησης του επαγγέλματος.

Ιδιαίτερα ενεργή είναι και η εμπλοκή της Αρχής στις προσπάθειες που καταβάλλονται για μεγαλύτερη εκπροσώπηση των γυναικών στον τομέα της Κυβερνοασφάλειας. Για αυτό το λόγο και με τη στήριξη της ΑΨΑ, ιδρύθηκε κατά το 2024 το **Women4Cyber Cyprus**. Το Women4Cyber ιδρύθηκε το 2019 στο πλαίσιο του Ευρωπαϊκού Οργανισμού για την Κυβερνοασφάλεια (ECSO), με στόχο την αντιμετώπιση της ανισότητας των φύλων στον τομέα της κυβερνοασφάλειας, καθώς και την κάλυψη της αυξανόμενης ζήτησης για εξειδικευμένους επαγγελματίες στον κυβερνοχώρο στην Ευρώπη, εκπροσωπώντας μια κοινότητα 30 παραρτημάτων και σχεδόν 70.000 υποστηρικτών από όλη την Ευρώπη — συμπεριλαμβανομένης πλέον και της Κύπρου.

12 ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΕ ΠΕΡΙΦΕΡΕΙΑΚΟ ΕΠΙΠΕΔΟ

Αποστολή της ΑΨΑ ως Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας είναι να προωθήσει το θεσμό της πιστοποίησης για προϊόντα, υπηρεσίες και διαδικασίες στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών, μέσω της ανάπτυξης των γνώσεων και δεξιοτήτων με όραμα να καταστεί η Κύπρος περιφερειακό κέντρο πιστοποιήσεων.

12.1 Πιστοποιήσεις Προϊόντων και Υπηρεσιών

Αποστολή της ΑΨΑ ως Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας είναι να προωθήσει το θεσμό της πιστοποίησης για προϊόντα, υπηρεσίες και διαδικασίες στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών, μέσω της ανάπτυξης των γνώσεων και δεξιοτήτων, με όραμα να καταστεί η Κύπρος περιφερειακό κέντρο πιστοποιήσεων.

Κατά τη διάρκεια του 2024, η ΑΨΑ παρείχε στοχευμένη υποστήριξη και καθοδήγηση στον Εθνικό Οργανισμό Διαπίστευσης, με στόχο την ενίσχυση των διαδικασιών διαπίστευσης για την εφαρμογή των επιπρόσθετων απαιτήσεων των ευρωπαϊκών σχημάτων πιστοποίησης. Παράλληλα, οργάνωσε εξειδικευμένες εκπαιδεύσεις τόσο για το προσωπικό όσο και για ενδιαφερόμενα μέρη, με στόχο τη συλλογική κατανόηση των σχημάτων και προετοιμασία για την υλοποίηση του πρώτου πιλοτικού έργου πιστοποίησης στην Κύπρο.

Προς την υλοποίηση του οράματος αυτού η ΑΨΑ προχώρησε και στην ανάπτυξη σχέσεων με οργανισμούς εντός και εκτός Ευρωπαϊκής Ένωσης με στόχο την ανταλλαγή τεχνογνωσίας, την ευθυγράμμισή της με βέλτιστες πρακτικές, και στην ενίσχυση της αναγνωρισιμότητας της Κύπρου ως αξιόπιστου εταίρου σε θέματα πιστοποίησης και κυβερνοασφάλειας.

12.2 Κέντρο Αριστείας για τη Ναυτιλία

Η Αρχή, στα πλαίσια ενίσχυσης της κυβερνοαμυνας των κρίσιμων υποδομών του Κράτους, έχει αναγνωρίσει ότι ένας από τους πιο σημαντικούς τομείς είναι αυτός της ναυτιλίας. Μία ενδεχόμενη κυβερνοεπίθεση σε αυτόν τον κλάδο μπορεί να έχει σοβαρές επιπτώσεις στην οικονομία τους Κράτους, στην ασφάλεια των πλοίων και των επιβατών τους, καθώςκαι στην ευημερία των Κύπριων πολιτών, αφού ενδέχεται να υπάρχουν καθυστερήσεις στην παράδοση βασικών αγαθών.

Προς την ενίσχυση του τομέα, πέραν της εφαρμογής της Οδηγία NIS και της ανανεωμένης NIS2- οι οποίες αποτελούν πολύτιμα εργαλεία για τη βελτίωση της κυβερνοασφάλειας στον ναυτιλιακό τομέα- η Αρχή έχει συμμετάσχει ενεργά στην ενίσχυση της ανθεκτικότητας του κλάδου μέσω ευρωπαϊκών έργων και διεθνών συνεργασιών.

Χαρακτηριστικά παραδείγματα αποτελούν τα συγχρηματοδοτούμενα από την Ευρωπαϊκή Ένωση έργα. Ένα από αυτά είναι το CY-TRUST, που στοχεύει στη δημιουργία Τομεακών Κέντρων Επιχειρήσεων Ασφάλειας (SOCs), συμπεριλαμβανομένου ενός για τον ναυτιλιακό τομέα, με έμφαση στην Επίγνωση Κατάστασης, την Αντιμετώπιση Περιστατικών και την Ετοιμότητα. Επιπλέον, το SecAwarenessTruss, που επικεντρώνεται στην ενίσχυση της εκπαίδευσης στην κυβερνοασφάλεια για κρίσιμες υποδομές μέσω ρεαλιστικών περιβαλλόντων προσομοίωσης (cyber ranges).

Επιπρόσθετα, η Αρχή εντός του έτους πραγματοποίησε μια σειρά από εποικοδομητικές συναντήσεις με σημαντικούς φορείς του ναυτιλιακού τομέα, συμπεριλαμβανομένων εκπροσώπων εταιρειών, ρυθμιστικών αρχών και τεχνολογικών παρόχων. Μέσω αυτών των συναντήσεων επιδιώχθηκε η κατανόηση των ειδικών προκλήσεων που αντιμετωπίζει ο τομέας, κάτι που οδήγησε στη διερεύνηση του ενδεχόμενου δημιουργίας ενός περιφερειακού κέντρου κυβερνοασφάλεια (Maritime Cybersecurity Centre of Excellence), ειδικά σχεδιασμένο για τη ναυτιλία. Η ιδέα αυτή βασίστηκε και στα αποτελέσματα μελέτης που διενεργήθηκε το 2022, σε συνεργασία των Sandia National Laboratories, του Ανοικτού Πανεπιστημίου Κύπρου και της Αρχής Ψηφιακής Ασφάλειας, η οποία πρότεινε την οικοδόμηση ενός πλαισίου διακυβέρνησης του κυβερνοχώρου της ναυτιλίας και των αντίστοιχων μηχανισμών εφαρμογής.

Το περιφερειακό κέντρο κυβερνοασφάλειας θα καλύπτει τέσσερις βασικούς πυλώνες, «Ανταλλαγής Πληροφοριών για Απειλές» (Threat Intelligence), «Εκπαίδευσης» (Training Center), «Οδηγίες, Πολιτικές και Ρυθμιστικό Πλαίσιο» (Guidance, Policies and Regulatory Framework) καθώς και τον πυλώνα «Κέντρο Έρευνας και Καινοτομίας» (Research and Innovation Center). Ο στόχος του κέντρου αυτού είναι να επικεντρωθεί στην εφαρμογή μηχανισμών ψηφιοποίησης και τεχνολογικών εξελίξεων, καθώς και στην εκπαίδευση, την ευαισθητοποίηση, την καινοτομία και την ανάπτυξη πολιτικών και οδηγιών, σύμφωνα με τους ισχύοντες κανονισμούς. Ένα τέτοιο κέντρο θα μπορούσε να λειτουργήσει ως ο πυρήνας μιας ολοκληρωμένης προσέγγισης στην κυβερνοασφάλεια, συμβάλλοντας στην ενίσχυση της ανθεκτικότητας της ναυτιλίας, στην προστασία των κρίσιμων υποδομών και στην προώθηση της ασφαλούς ναυσιπλοΐας.

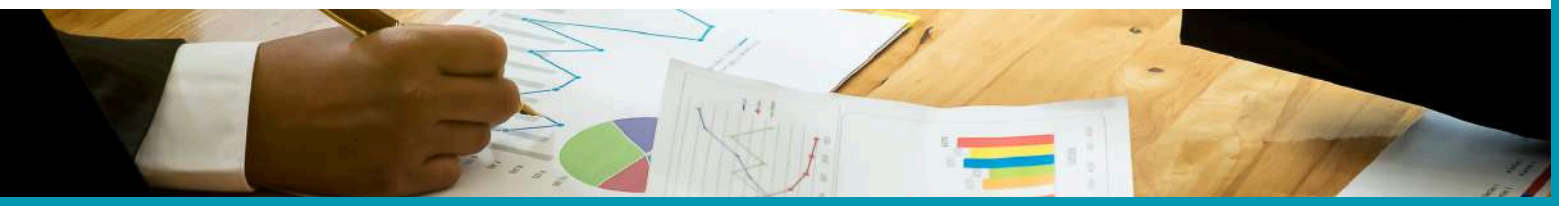
Ως σημαντικό ορόσημο εντός του έτους, ήταν και η διοργάνωση του εργαστήριου κυβερνοασφάλειας με τίτλο «Preventing Cyber Aggression in the Maritime Domain», στις 4 και 5 Νοεμβρίου. Το εργαστήριο αυτό πραγματοποιήθηκεσε συνεργασία με το Υπουργείο Εξωτερικών, το Υφυπουργείο Ναυτιλίας, την Αμερικάνικη Πρεσβεία, τα Sandia National Laboratories των ΗΠΑ και το Ανοικτό Πανεπιστήμιο Κύπρου. Προσέλκυσε έντονο ενδιαφέρον από ιδιωτικούς αλλά και δημόσιους φορείς, με συνολικό αριθμό συμμετεχόντων 65. Κατά τη διάρκεια των δύο ημερών, οι συμμετέχοντες απέκτησαν πολύτιμες γνώσεις σχετικά με τις τελευταίες κυβερνοεπιθέσεις στον τομέα της ναυτιλίας και έμαθαν πώς να αξιοποιούν εργαλεία ανοιχτού κώδικα (open-source) μέσω μιας πρακτικής άσκησης.

13 ΣΤΑΤΙΣΤΙΚΑ ΚΑΙ ΕΡΕΥΝΕΣ

13.1 Στατιστικά και έρευνες παρατηρητηρίου

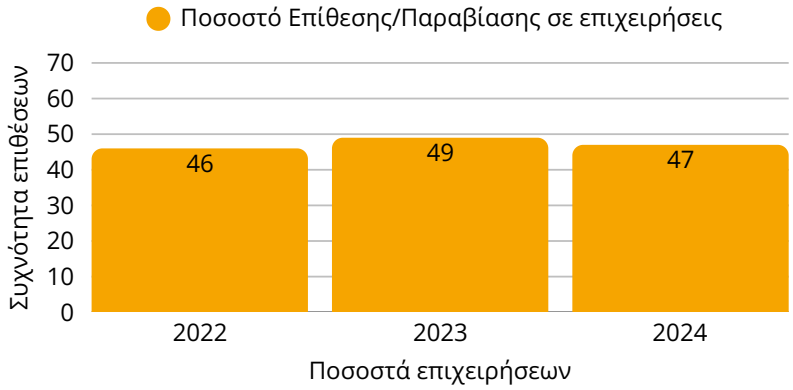
Η Αρχή συγκεντρώνει και αξιολογεί δεδομένα και πληροφορίες σχετικά με την κυβερνοασφάλεια και την ψηφιακή ασφάλεια, με στόχο την εξαγωγή χρήσιμων συμπερασμάτων. Τα συμπεράσματα αυτά αξιοποιούνται για την υλοποίηση δράσεων εντός του πλαισίου των αρμοδιοτήτων της, όπως η διοργάνωση εκπαιδευτικών σεμιναρίων που ενισχύουν τις γνώσεις και τις δεξιότητες σε θέματα κυβερνοασφάλειας, καθώς και η διεξαγωγή εκστρατειών ενημέρωσης και ευαισθητοποίησης, τόσο για τους πολίτες όσο και για τις επιχειρήσεις.

Στο πλαίσιο αυτό, το 2024 η ΑΨΑ πραγματοποίησε δύο Παγκύπριες έρευνες με στόχο τη συλλογή στοιχείων και πληροφοριών για την κυβερνοασφάλεια στην κυπριακή επικράτεια[4]. Οι έρευνες του παρατηρητηρίου επικεντρώθηκαν στην αξιολόγηση θεμάτων που αφορούσαν τον τρόπο χειρισμού θεμάτων κυβερνοασφάλειας ή/και ψηφιακής ασφάλειας, αποτίμησης της σημαντικότητας που αποδίδεται στα θέματα αυτά, τον τρόπο αντιμετώπισης περιστατικών κυβερνοεπιθέσεων, αλλά και τις συνέπειες από τέτοια περιστατικά. Η πρώτη έρευνα απευθυνόταν σε επιχειρήσεις ενώ η δεύτερη σε πολίτες. Οι 2 έρευνες διεξήχθησαν παράλληλα, κατά τους μήνες Σεπτέμβριο-Οκτώβριο 2024, με δείγμα 1001 πολιτών και 450 επιχειρήσεων από διάφορους τομείς της βιομηχανίας, του εμπορίου και των υπηρεσιών.



Τα κυριότερα αποτελέσματα της έρευνας που αφορά τις επιχειρήσεις:

1 Σχεδόν οι μισές επιχειρήσεις (47% 2024, 49% το 2023 και 46% το 2022) δέχθηκαν κάποια επίθεση/παραβίαση τους τελευταίους 12 μήνες (Γράφημα 1) με μέσο όρο 1 επίθεση κάθε 10 μέρες σημειώνοντας μείωση σε σύγκριση με το προηγούμενο έτος, όπου σημειωνόταν μία επίθεση κάθε εβδομάδα (ή κάθε 9 ημέρες το 2022).



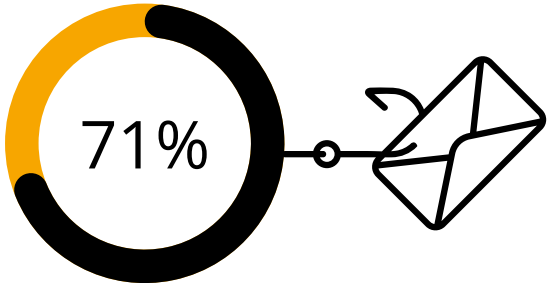
€12,000

Μέσο κόστος ζημίας

1/10

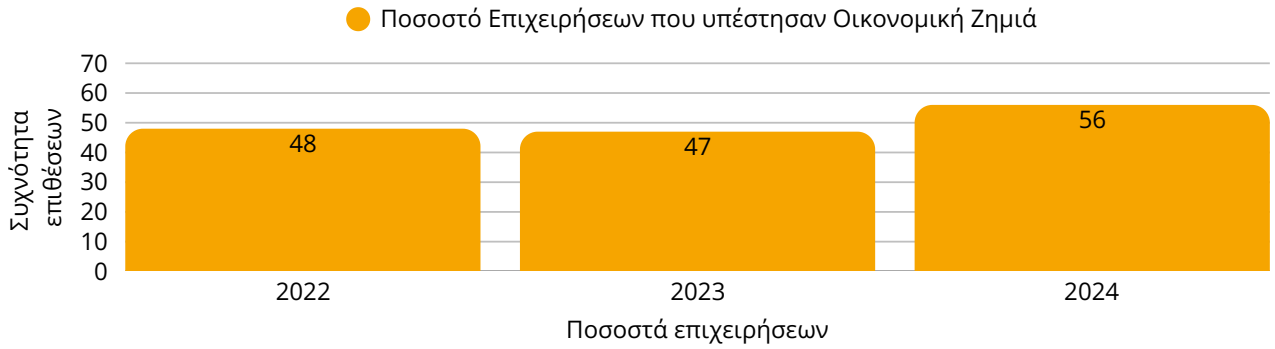
1 επίθεση κάθε 10 μέρες

Η πιο συχνή μορφή επίθεσης που δέχονται οι επιχειρήσεις είναι το phishing δηλαδή απατηλά μηνύματα μέσω ηλεκτρονικού ταχυδρομείου. Αν και αυτό το ποσοστό μειώθηκε κατά 3 ποσοστιαίες μονάδες σε σχέση με το 2023, εμφανίζει αύξηση 6 ποσοστιαίων μονάδων συγκριτικά με το 2022.



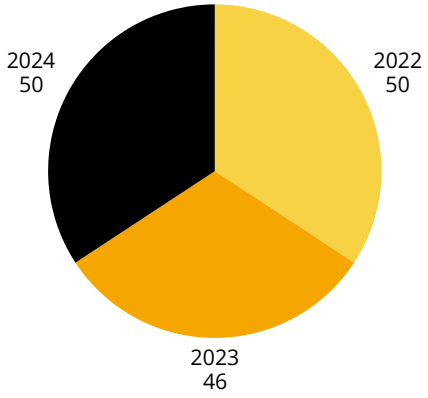
Το phishing παραμένει η πιο πρόσφατη μορφή κυβερνοεπίθεσης για τις επιχειρήσεις, αγγίζοντας το 71%

2 Από τις επιχειρήσεις που δέχθηκαν επίθεση, για περισσότερες από τις μισές (56%) υπέστησαν οικονομικές ζημιές, με το μέσο κόστος να ανέρχεται στις 12.000 ευρώ (Γράφημα 2). Αν και το ποσοστό των επιχειρήσεων που επηρεάστηκαν οικονομικά αυξήθηκε σε σύγκριση με τις δύο προηγούμενες χρονιές (47% το 2023 και 48% το 2022), το μέσο ποσό της ζημίας μειώθηκε κατά 15.000 ευρώ σε σχέση με το 2023 και κατά 10.000 ευρώ σε σχέση με το 2022.



3 **1 στις 4 επιχειρήσεις έχει να ανανεώσει τις πολιτικές της για την κυβερνοασφάλεια πάνω από ένα χρόνο.**

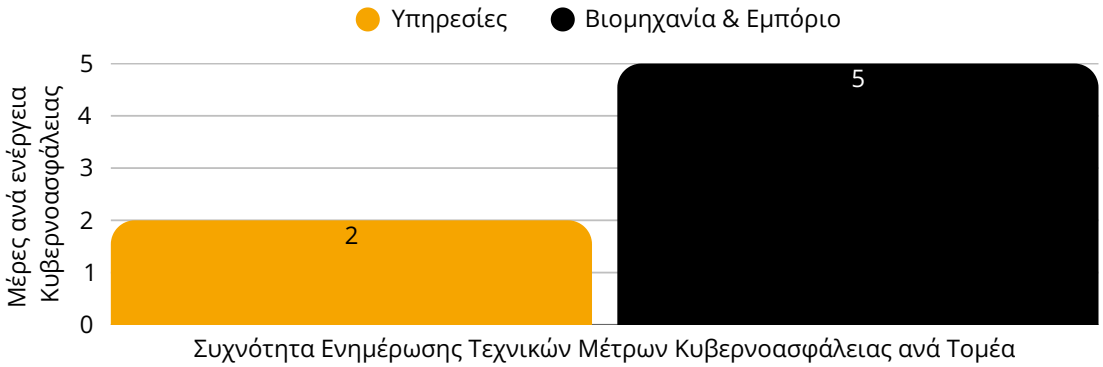
4 Υπάρχει άγνοια των επιχειρήσεων για σεμινάρια που προσφέρονται με θέματα την κυβερνοασφάλεια αφού οι μισές επιχειρήσεις (50% 2024, 46% το 2023 και 50% το 2022) δεν γνωρίζουν για αυτά ενώ μόλις 13% (17% το 2023 και το 2022) συμμετείχε σε αυτά. Αξίζει να αναφερθεί πως όσες επιχειρήσεις συμμετείχαν σε κάποιο σεμινάριο, ευαισθητοποιήθηκαν και προέβησαν σε ενέργειες και δράσεις για την ενίσχυση των μέτρων ασφαλείας που λαμβάνουν.



Ποσοστό άγνοιας επιχειρήσεων για σεμινάρια στον τομέα της κυβερνοασφάλειας

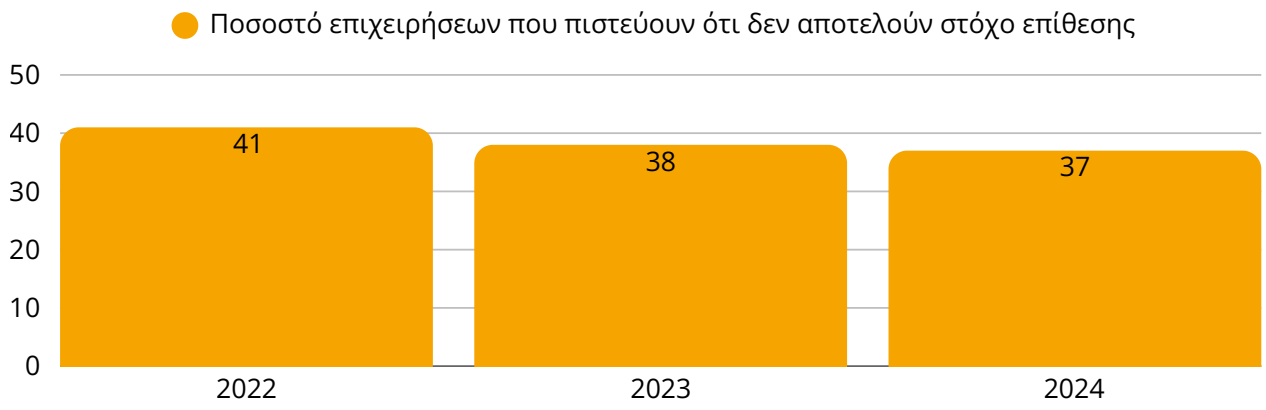
Ποσοστό συμμετοχής επιχειρήσεων σε σεμινάρια κυβερνοασφάλειας

5 Οι επιχειρήσεις του τομέα των υπηρεσιών προχωρούν σε εφαρμογή ή ενημέρωση τεχνικών μέτρων κυβερνοασφάλειας δύο φορές την εβδομάδα, σε αντίθεση με τις επιχειρήσεις της βιομηχανίας και του εμπορίου, οι οποίες πραγματοποιούν αντίστοιχες ενέργειες κάθε πέντε ημέρες.



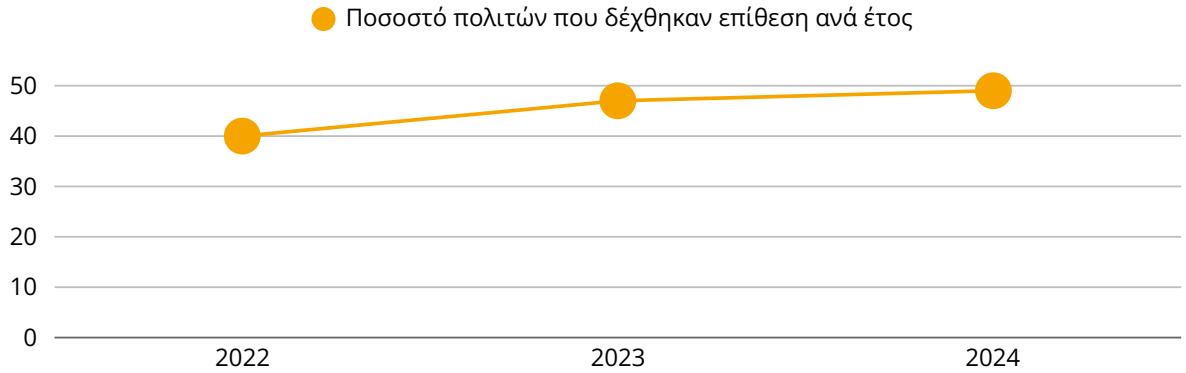
Συχνότητα Ενημέρωσης Τεχνικών Μέτρων Κυβερνοασφάλειας ανά Τομέα

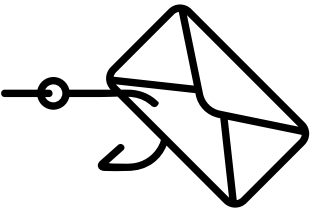
6 Μεταξύ των επιχειρήσεων που δεν δέχθηκαν κάποια επίθεση, το 37% θεωρούν ότι αυτό δεν συνέβη επειδή η εταιρία τους δεν αποτελεί «στόχο», παρόλο που το ποσοστό αυτό παρουσιάζει μικρή μείωση σε σχέση με τις 2 προηγούμενες έρευνες (38% το 2023 και 41% το 2022), εξακολουθεί να προκαλεί ανησυχία αφού οποιαδήποτε επιχείρηση μπορεί να αποτελέσει στόχο και θα πρέπει να λαμβάνει τα κατάλληλα μέτρα προστασίας.



Τα κυριότερα αποτελέσματα της έρευνας που αφορά τους πολίτες ήταν τα ακόλουθα:

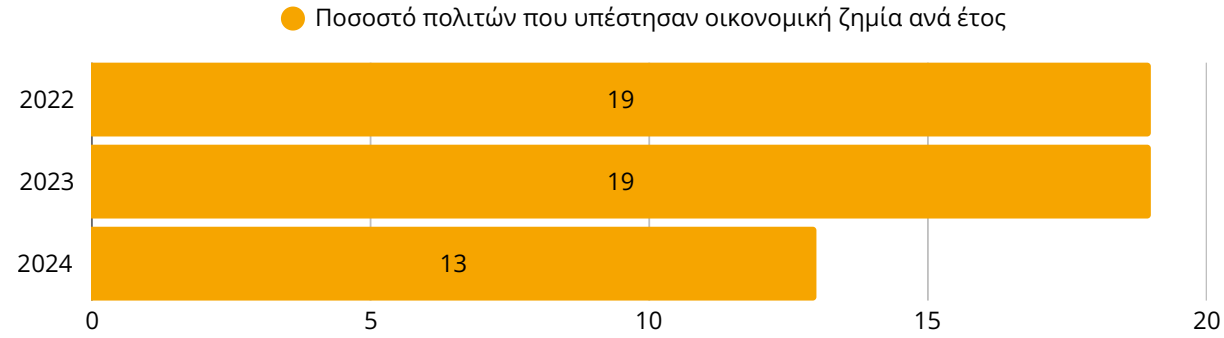
1 Το ποσοστό των πολιτών που δέχθηκαν επίθεση τους τελευταίους 12 μήνες ανήλθε στο 49% παρουσιάζοντας αύξηση σε σχέση με τα προηγούμενα 2 χρόνια (40% το 2022 και 47% το 2023). Ο μέσος όρος των παραβιάσεων ή επιθέσεων ανά πολίτη ανέρχεται σε 28,5 ετησίως, καταγράφοντας αύξηση 10% σε σχέση με το 2023 και 36% σε σχέση με το 2022.





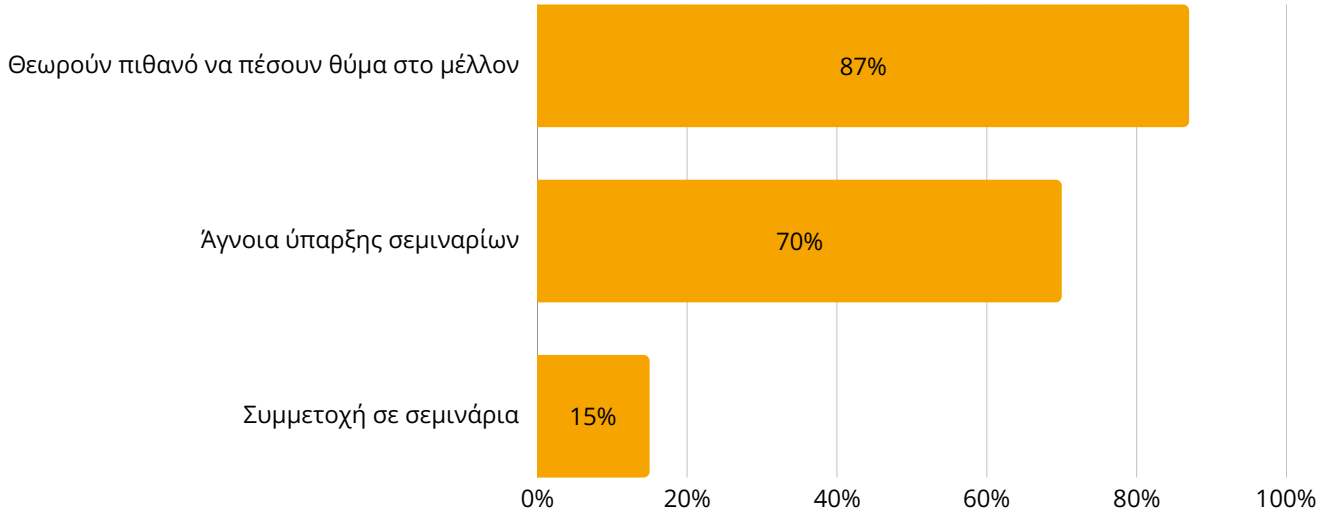
Η πιο συχνή επίθεση που δέχονται οι πολίτες είναι το phishing δηλαδή απατηλά μηνύματα μέσω ηλεκτρονικού ταχυδρομείου με 39% παρουσιάζοντας αύξηση 3 ποσοστιαίων μονάδων σε σχέση με πέρσι και 9 ποσοστιαίων μονάδες σε σχέση με το 2022.

2 Από τους πολίτες που δέχθηκαν επίθεση, το 13% (έναντι 19% το 2022 και το 2023) υπέστη οικονομική ζημία, με το μέσο κόστος να ανέρχεται στα 62 ευρώ. Αξιοσημείωτο είναι το γεγονός πως παρόλο που ο μέσος όρος επιθέσεων αυξήθηκε από 25,9 σε 28,5 παρατηρείται μείωση του κόστους κυβερνοεπιθέσεων (- €79 σε σχέση με το 2023 και - €256) γεγονός που πιθανόν να οφείλεται στην αυξημένη ικανότητα των πολιτών (+7%) να αναγνωρίζουν τα απατηλά μηνύματα. Ενδιαφέρον παρουσιάζει επίσης το γεγονός ότι η ηλικιακή ομάδα 18-34 ετών κατέγραψε το υψηλότερο οικονομικό κόστος, παρά το ότι δεν δέχεται τις περισσότερες επιθέσεις, ενώ η ηλικιακή ομάδα 45-54 ετών εμφάνισε το χαμηλότερο κόστος, παρόλο που καταγράφει το υψηλότερο ποσοστό πολιτών που θεωρούν πιθανή μια μελλοντική επίθεση.



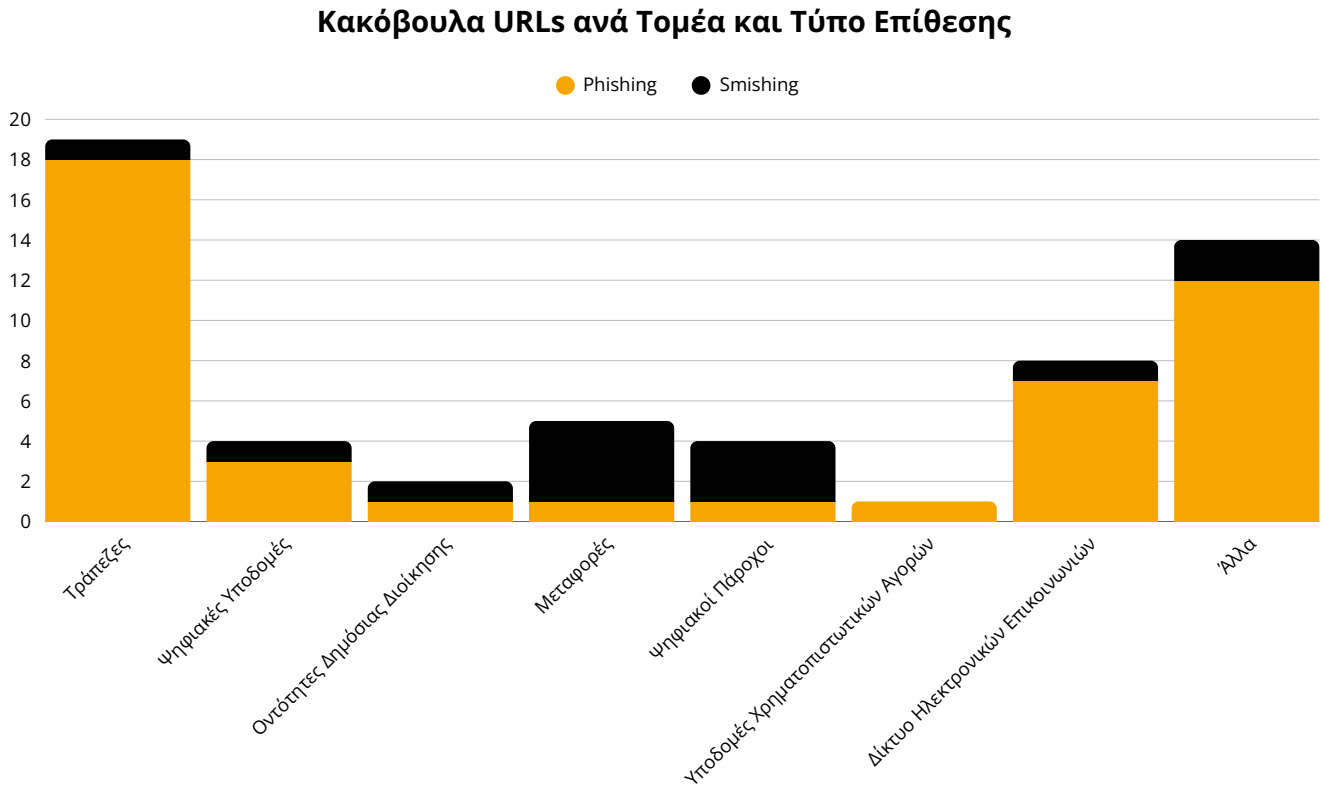
3 Μεταξύ των πολιτών που δεν υπήρξαν θύματα επίθεσης ή παραβίασης τον τελευταίο χρόνο, το 87% δεν αποκλείει το ενδεχόμενο να πέσει θύμα κακόβουλης επίθεσης στο μέλλον. Το ποσοστό αυτό είναι μειωμένο κατά 2% σε σχέση με το 2023.

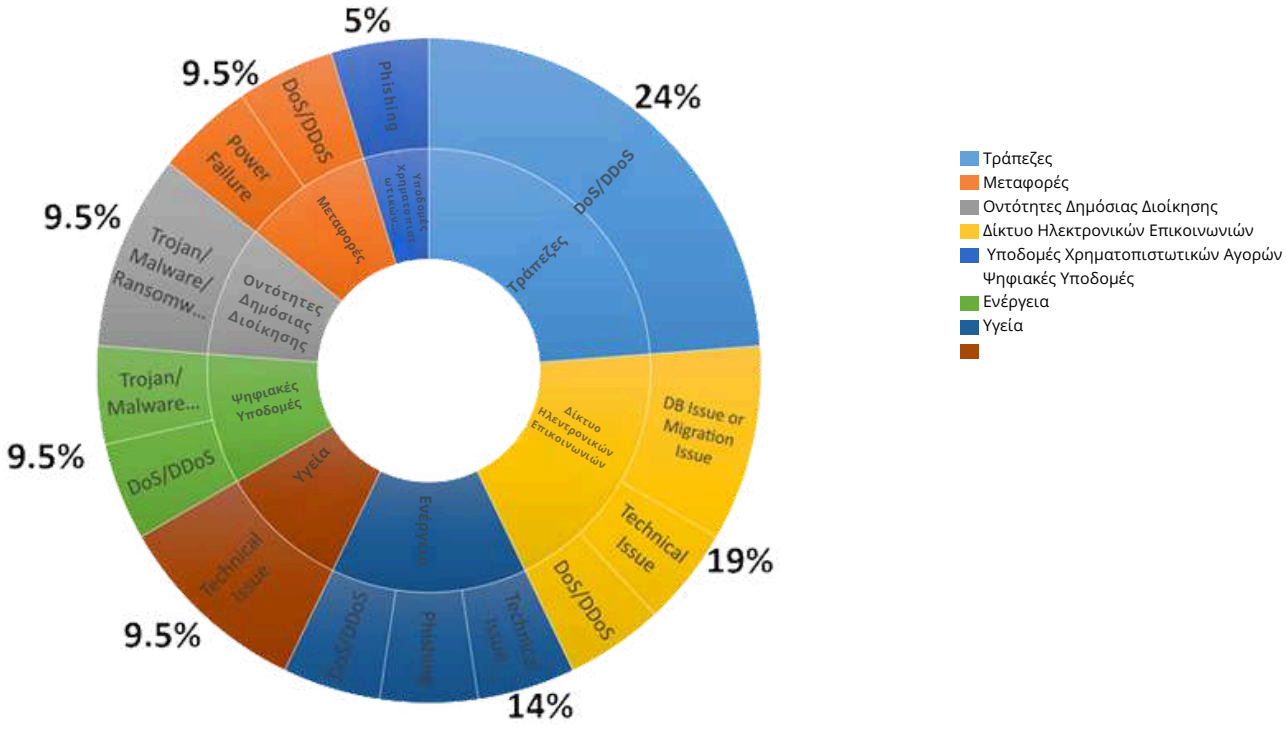
4 Υπάρχει άγνοια των πολιτών για προσφερόμενα σεμινάρια για θέματα που αφορούν την κυβερνοασφάλεια αφού το 70% δήλωσε άγνοια για την ύπαρξή τους, ενώ μόνο το 15% έχει συμμετάσχει σε κάποια από αυτά, ποσοστά όμως που παρουσιάζουν αύξηση σε σχέση με τις 2 προηγούμενες χρονιές. Μέσα από την έρευνα διαφάνηκε πως έπειτα από την παρακολούθηση σεμιναρίων οι πιο σημαντικές αλλαγές που έκαναν ήταν η χρήση ισχυρών κωδικών, η συχνή αλλαγή κωδικών και η αποφυγή ύποπτων ιστοσελίδων.



Οι έρευνες αυτές αποτελούν την τρίτη διαδοχική χαρτογράφηση της εικόνας σε θέματα κυβερνοασφάλειας στις επιχειρήσεις και στους πολίτες στην κυπριακή επικράτεια. Η χαρτογράφηση θα συνεχιστεί σε ετήσια βάση προσαρμοζόμενη στις εξελίξεις και τις μεταβαλλόμενες ανάγκες πληροφόρησης.

13.2 Στατιστικά Εθνικής Ομάδας Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (CSIRT)





485

Κακόβουλα URLs αναφέρθηκαν το 2024

14 ΟΙΚΟΝΟΜΙΚΑ

14.1 Μη Ελεγμένες Οικονομικές Καταστάσεις για το έτος 2024

Οι οικονομικές καταστάσεις της ΑΨΑ για το έτος που έληξε την 31η Δεκεμβρίου 2024 ετοιμάστηκαν όπως προβλέπεται από το άρθρο 48 (2) του Ν. 89(Ι)/2020. Οι βασικότερες πληροφορίες για την καταγραφή δαπανών και εσόδων, που περιέχονται στις προκαταρτικές μη ελεγμένες οικονομικές καταστάσεις για το έτος που έληξε στις 31 Δεκεμβρίου 2024, απεικονίζονται στο Γράφημα 2 και περιλαμβάνουν:

Μη Ελεγμένη Κατάσταση Συνολικών Εισοδημάτων 2024

ΕΣΟΔΑ	**2024 €**	**2023 €**
Έσοδα από τέλη	9,998,421	4,879,598
Έσοδα από συγχρηματοδοτούμενα προγράμματα	1,074,237	4,777,430
Τόκοι-έσοδα χρηματοδότησης	22,685	-
Εκτέλεση έργων για άλλα τμήματα / Υπουργεία	161,207	296,093
	11,256,550	**9,953,121**

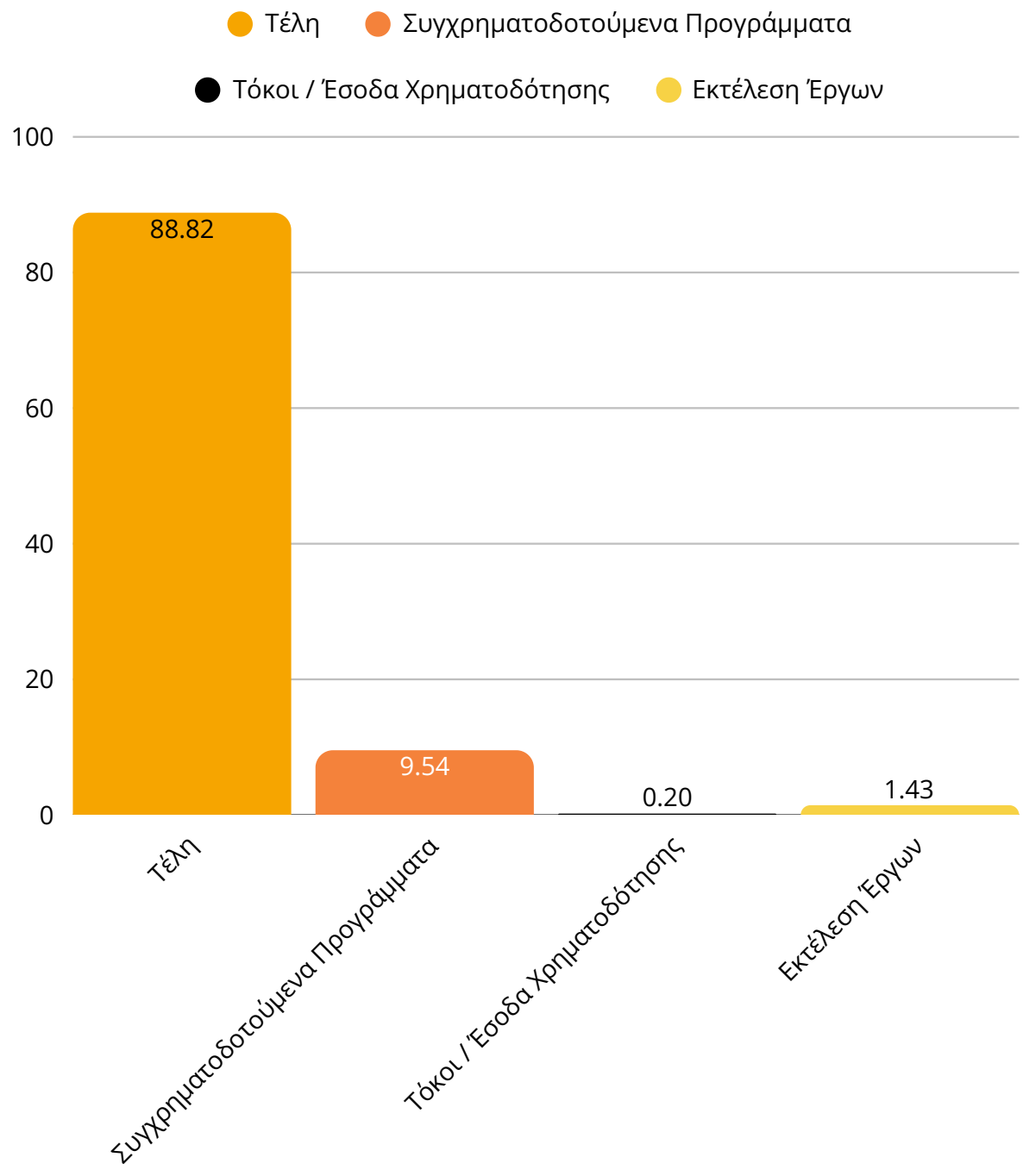
Έσοδα	**2024 €**	**2023 €**
Κόστος προσωπικού Έξοδα Χρηματοδότησης (Τόκοι)	1,208,119	609,981
Λειτουργικά έξοδα γραφείου	2,127,463	2,206,837
Μίσθωση υπηρεσιών	3,973,092	3,214,571
Αποσβέσεις εξοπλισμού και εγκαταστάσεων	519,183	526,481
Αποσβέσεις άϋλου ενεργητικού	95,458	106,352
	7,942,800	**6,664,222**
Πλεόνασμα έτους από συνήθεις εργασίες	**3,313,750**	**3,288,899**
Συνολικά εισοδήματα για το έτος	**3,313,750**	**3,288,899**

**Σημείωση: Τα στοιχεία αφορούν προκαταρτικές μη ελεγμένες οικονομικές καταστάσεις και δύναται να αναπροσαρμοστούν.*

Μη Ελεγμένη Κατάσταση Χρηματοοικονομικής Θέσης στις 31 Δεκεμβρίου 2024

ΠΕΡΙΟΥΣΙΑΚΑ ΣΤΟΙΧΕΙΑ	2024 €	2023 €
Μη Κυκλοφορούντα περιουσιακά στοιχεία		
Εγκαταστάσεις και εξοπλισμός	1,649,916	2,189,361
Άϋλα στοιχεία ενεργητικού	75,644	366,138
Σύνολο μη κυκλοφορούντων περιουσιακών στοιχείων	**1,725,560**	**2,555,499**
Κυκλοφορούντα περιουσιακά στοιχεία		
Χρεώστες και προπληρωμές	14,301,443	8,064,863
Μετρητά στην τράπεζα και στο ταμείο	10,427,511	12,821,515
Σύνολο κυκλοφορούντων περιουσιακών στοιχείων	**24,728,954**	**20,886,378**
Σύνολο Περιουσιακών Στοιχείων	**26,454,514**	**23,441,877**
Ιδια Κεφάλαια και Υποχρεώσεις		
Ίδια κεφάλαια		
Αποθεματικά	11,059,525	8,913,225
Σύνολο ιδίων κεφαλαίων	**11,059,525**	**8,913,225**
Τρέχουσες υποχρεώσεις		
Πιστωτές και οφειλόμενα έξοδα	1,439,378	2,540,959
Προεισπραχθέντα τέλη	12,179,311	9,911,393
Κρατική χορηγία	1,776,300	2,076,300
Ολικό τρεχουσών υποχρεώσεων	**15,394,989**	**14,528,652**
Ολικό ίδιων Κεφαλαίων και Υποχρεώσεων	**26,454,514**	**23,441,877**

Γράφημα 1: Κατανομή Εσόδων για το έτος 2024 (%)



Γράφημα 2: Κατανομή Δαπανών για το έτος 2024 (%)