ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

Αρχή Ψηφιακής Ασφάλειας

Έκθεση Δραστηριοτήτων 2023

Υποβάλλεται στον Πρόεδρο της Δημοκρατίας σύμφωνα με την πρόνοια του Άρθρου 49 του Ν.89(Ι)/2020, ο οποίος διέπει τη λειτουργία της Αρχής Ψηφιακής Ασφάλειας

Σεπτέμβριος 2024

ΠΕΡΙΕΧΟΜΕΝΑ

ΓΡΑΦΗΜΑΤΑ

ΠΙΝΑΚΕΣ

ΕΙΣΑΓΩΓΗ

ΧΑΙΡΕΤΙΣΜΟΣ ΕΠΙΤΡΟΠΟΥ

Το 2023 ήταν μία χρονιά κατά την οποία δοκιμάστηκαν τόσο η ανθεκτικότητα όσο και η ετοιμότητα της Αρχής Ψηφιακής Ασφάλειας (ΑΨΑ). Αντιμετωπίσαμε πρωτόγνωρες καταστάσεις που ανέδειξαν την ευαίσθητη φύση του τομέα μας, δίνοντας την ευκαιρία στον Κύπριο πολίτη να εκτιμήσει τη σημαντικότητα της κυβερνοασφάλειας. Παρόλο που ο ψηφιακός κόσμος προσφέρει γνώσεις και οικονομικές ευκαιρίες, μπορεί επίσης να χαρακτηριστεί και ως πεδίο μάχης, με πιθανά θύματα την οικονομία μας, τα συστήματα υγείας, τις ηλεκτρονικές επικοινωνίες, τη ναυτιλία, τις μεταφορές και πολλούς άλλους τομείς.

Έχουμε εισέλθει σε μία καινούργια πραγματικότητα, όπου οι κυβερνοεπιθέσεις αποτελούν μέρος της καθημερινότητας και κανείς δεν μπορεί πλέον να νιώθει απόλυτα ασφαλής. Η αντίληψη ότι η κυβερνοασφάλεια είναι πολυτέλεια παύει να υφίσταται, και ο καθένας μας πρέπει να λαμβάνει μέτρα για την αντιμετώπιση των κυβερνοαπειλών. Με τις συνεχείς και ταχείες τεχνολογικές εξελίξεις, η ανάγκη για αποτελεσματικές πρακτικές και πολιτικές ψηφιακής ασφάλειας γίνεται ολοένα και πιο επιτακτική. Μέσα από την ετήσια έκθεση δραστηριοτήτων παρουσιάζεται το έργο μας για την ενίσχυση της ασφάλειας της κυπριακής κοινωνίας.

Κατά το 2023 εστιάσαμε σε πολλαπλές πτυχές της ασφάλειας των δεδομένων και των υποδομών, προωθώντας μια στρατηγική προσέγγιση για την προστασία της ψηφιακής κοινότητας. Τηρώντας τα ιδανικά που μας πρεσβεύουν καταφέραμε να ενισχύσουμε τις σχέσεις μας με τις κρίσιμες υποδομές πληροφοριών της Κυπριακής Δημοκρατίας, αλλά και να επενδύσουμε μαζί σε καίριους πυλώνες, όπως η αλληλοκατανόηση και η συνεργασία για την επίτευξη των στόχων μας. Σε ένα περιβάλλον αυξανόμενης ψηφιοποίησης και εξελισσόμενων απειλών στον κυβερνοχώρο, εκσυγχρονίσαμε τις πρακτικές μας για ρύθμιση και εποπτεία μέσω συστημάτων και εργαλείων όπως είναι η πλατφόρμα έγκαιρων προειδοποιήσεων, το μοντέλο ωριμότητας, η ανάπτυξη εργαλειοθήκης προτύπων/μεθοδολογιών κ.ά.

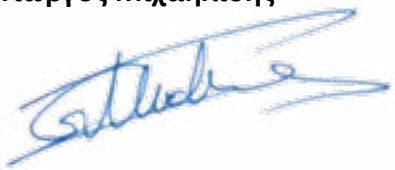
Η φιλοσοφία μας, την οποία επιδιώκουμε να μεταδώσουμε και στην ευρύτερη κοινωνία, είναι να θέτουμε υψηλούς στόχους, να προχωράμε με σταθερά και μεθοδικά βήματα και να επιταχύνουμε την ανάπτυξή μας όταν χρειάζεται. Βάσει αυτής της φιλοσοφίας, το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας, προσφέρει χορηγίες σχετικά με την ενίσχυση της κυβερνοασφάλειας των μικρομεσαίων επιχειρήσεων, διοργανώνει σεμινάρια και εκπαιδεύσεις προς όλη την κοινωνία και οργανώνει συναντήσεις ενημέρωσης και δικτύωσης.

Οι προσπάθειες αυτές αύξησαν τις ανάγκες και τις υποχρεώσεις μας, απαιτώντας περαιτέρω ενίσχυση του προσωπικού σε διάφορους τομείς. Το 2023 η οικογένεια της ΑΨΑ μεγάλωσε, προσθέτοντας στο δυναμικό της εξειδικευμένους επαγγελματίες του κλάδου, οι οποίοι συνέβαλαν στην επίτευξη των στόχων μας. Επιπρόσθετα, το Γραφείο Επιτρόπου Επικοινωνιών μεταστεγάστηκε σε νέα υπερσύγχρονα κτήρια, ενισχύοντας έτσι τις δυνατότητές του στην παροχή υψηλού επιπέδου υπηρεσιών και ενίσχυσης της ψηφιακής ασφάλειας. Επιπλέον, λαμβάνοντας υπόψη τις βασικές ελλείψεις ανθρώπινου δυναμικού στον κλάδο, δημιουργήσαμε την Ακαδημία Τεχνολογίας, Πληροφοριών, Επικοινωνιών και Κυβερνοασφάλειας (ICT) με απώτερο στόχο να καταστεί ένα αυτοσυντηρούμενο Περιφερειακό Κέντρο Εκπαίδευσης στον τομέα του ICT.

Το έργο μας δεν σταματά εδώ. Σε καμία περίπτωση δεν επαναπαυόμαστε και καθημερινά εξελισσόμαστε, επενδύοντας στις δυνατότητές μας και στην ενίσχυση μιας κουλτούρας συνεργασίας. Η κυβερνοασφάλεια αποτελεί μια ισορροπημένη κατανομή της ευθύνης και ενεργής συμμετοχής όλων μας, καθώς και μία αξία που θα πρέπει να ενστερνιζόμαστε όλοι.

Τέλος, σας διαβεβαιώνω ότι η ΑΨΑ μπορεί να ανταποκριθεί με επιτυχία στις απαιτήσεις του παρόντος και στις προκλήσεις του μέλλοντος. Με το ίδιο πείσμα και ζήλο που μας διακατέχει από την πρώτη μέρα λειτουργίας μας, παραμένουμε ενημερωμένοι και σε εγρήγορση, προκειμένου να δημιουργήσουμε ένα ασφαλέστερο μέλλον για όλους. Τα γεγονότα ορόσημα που ακολουθούν, αποτελούν έμπρακτο παράδειγμα της εργασίας αλλά και των δυνατοτήτων της ΑΨΑ.

Γιώργος Μιχαηλίδης



Επίτροπος Επικοινωνιών

ΓΕΓΟΝΟΤΑ ΟΡΟΣΗΜΑ 2023

Η χρονιά που πέρασε αποτέλεσε μια περίοδο σημαντικών εξελίξεων και προκλήσεων για την Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ). Μέσα από στρατηγικές κινήσεις και στοχευμένες δράσεις, καταφέραμε να επιτύχουμε σημαντικά ορόσημα, διαμορφώνοντας έτσι τις βάσεις για περαιτέρω ανάπτυξη και επιτυχίες στο μέλλον.

Μετάβαση στην οδηγία NIS2

Η Οδηγία Network and Information Security Directive 2 (NIS2) πραγματεύεται τα μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας, θέτοντας ακόμα πιο υψηλούς στόχους κυβερνοασφάλειας για τις βασικές και σημαντικές οντότητες κάθε κράτους μέλους της ΕΕ, με γνώμονα τη μεγιστοποίηση της κοινωνικής ανθεκτικότητας μέσω δομημένων προσεγγίσεων κυβερνοασφάλειας σε πολλαπλά επίπεδα. Με σκοπό την εναρμόνιση της Οδηγίας (ΕΕ) 2022/2555 («Οδηγία NIS2») στην εθνική νομοθεσία, η ΑΨΑ ετοίμασε τροποποιητικό νομοσχέδιο σχετικά με την εν λόγω εναρμόνιση. Ταυτόχρονα, με τη νέα οδηγία η ΑΨΑ αναλαμβάνει επιπρόσθετους ρόλους και αρμοδιότητες (βλ. Ενότητα 2.2).

Παροχή καθοδήγησης προς τους Φορείς Κρίσιμων Υποδομών μέσω ανάπτυξης εργαλειοθήκης

Στα πλαίσια της προστασίας των κρίσιμων υποδομών, αλλά και με γνώμονα την ενίσχυση της κυβερνοασφάλειας στην Κυπριακή Δημοκρατία, η ΑΨΑ ανέπτυξε μία εργαλειοθήκη (toolkit) με πρότυπα και μεθοδολογίες, με σκοπό την καθοδήγηση των Φορέων για συμμόρφωση με τις υποχρεώσεις τους. Η εργαλειοθήκη έχει δημοσιευθεί (https://dsa.cy/activities/toolkit) με στόχο να χρησιμοποιείται όχι μόνο από τους κρίσιμους Φορείς, αλλά και από οποιονδήποτε άλλο οργανισμό θέλει να κτίσει μια σωστά δομημένη προσέγγιση για την κυβερνοασφάλεια (βλ. Ενότητα 6.2.2).

Πλαίσιο αξιολόγησης και ελέγχου κρίσιμων υποδομών μέσω εφαρμογής Μοντέλου Ωριμότητας κυβερνοασφάλειας

Η ΑΨΑ με στόχο την αναγνώριση του επιπέδου ωριμότητας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών σε σχέση με τις απαιτήσεις της νομοθεσίας για τα απαραίτητα μέτρα κυβερνοασφάλειας, έχει ολοκληρώσει την ανάπτυξη του Μοντέλου Ωριμότητας Κυβερνοασφάλειας (Cybersecurity Maturity Model) και προχώρησε με την πιλοτική εφαρμογή του. Το μοντέλο αυτό θα χρησιμοποιηθεί τόσο από τους ίδιους τους Φορείς για να επιμετρούν το επίπεδο ωριμότητας και συμμόρφωσής τους με τις πρόνοιες της νομοθεσίας που αφορά τα μέτρα ασφάλειας, αλλά κυρίως θα αποτελέσει το εργαλείο ελέγχου και αξιολόγησης από μέρους των εξωτερικών ελεγκτών των εποπτευόμενων Φορέων (βλ. Ενότητα 2.3).

Διεθνής εκδήλωση «Interregional CyberDrill for Europe»

Η ΑΨΑ φιλοξένησε την διαπεριφερειακή εκδήλωση «Interregional CyberDrill for Europe». Η εκδήλωση αυτή διοργανώθηκε από το Γραφείο Ανάπτυξης Τηλεπικοινωνιών (BDT) της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU). Η εκδήλωση είχε ως στόχο την ενίσχυση των ικανοτήτων αντιμετώπισης περιστατικών των εμπλεκόμενων ομάδων Αντιμετώπισης Συμβάντων της Ασφάλειας Υπολογιστών (CSIRTs), καθώς και τη διασφάλιση μιας συνεχούς συλλογικής προσπάθειας για τον μετριασμό των απειλών στον κυβερνοχώρο μεταξύ των ομάδων (CSIRTs) της Ευρώπης και της Ασίας-Ειρηνικού (βλ. Ενότητα 8.1.14).

Πλατφόρμα Έγκαιρων Προειδοποιήσεων (EARLY WARNING SYSTEM)

Μέσα στο πλαίσιο της συνεχούς παρακολούθησης για κυβερνοεπιθέσεις και της έγκαιρης ενημέρωσης, το εθνικό CSIRT έχει υλοποιήσει συστήματα και μηχανισμούς, οι οποίοι μπορούν σε πραγματικό χρόνο να ανιχνεύσουν επιθέσεις σε πληθώρα απειλών. Παράλληλα, έχουν εγκατασταθεί αισθητήρες στις κρίσιμες υποδομές της Δημοκρατίας που ελέγχονται από την υποδομή του Κέντρου Επιχειρήσεων Ασφαλείας (Security Operations Centre - SOC) του Εθνικού CSIRT. Στο υπερσύγχρονο κέντρο επιχειρήσεων γίνεται χρήση πολλαπλών οθονών παρέχοντας στους αναλυτές πληροφόρηση από τους αισθητήρες και ένα πλήθος συστημάτων και μηχανισμών ανίχνευσης και ανάλυσης. Αυτή η πληροφόρηση παρέχει

την απαραίτητη επίγνωση της κατάστασης και της ψηφιακής δραστηριότητας στον κυβερνοχώρο, και επιτρέπει στην ομάδα να εντοπίζει ύποπτες ή ασυνήθιστες συμπεριφορές και να προβαίνει στις απαραίτητες ενέργειες. Με απόφαση του Προέδρου της Δημοκρατίας, έχουν εγκατασταθεί μέχρι στιγμής 33 αισθητήρες εκ των οποίων οι 30 είναι στον δημόσιο τομέα (βλ. Ενότητα 3.6).

Πρόγραμμα Δράσης Στήριξης του ENISA (CYBERSECURITY SUPPORT ACTION)

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). Η ΑΨΑ σε συνεργασία με τον ENISA, προσέφερε αυτές τις υπηρεσίες σε υποδομές στην Κύπρο και κατάφερε να εξαντλήσει όλο τον προϋπολογισμό που είχε διατεθεί σε σχετικό σχέδιο για την Κύπρο. Τριάντα επτά (37) υποδομές από διάφορους τομείς (Ενέργειας, Τηλεπικοινωνιών, Υγείας κ.α.) επωφελήθηκαν από τις υπηρεσίες. (βλ. Ενότητα 7.4)

Συγχρηματοδοτούμενα Ευρωπαϊκά Ερευνητικά Προγράμματα για Κυβερνοασφάλεια

Η εμπλοκή σε ευρωπαϊκά προγράμματα είναι σημαντική γιατί συνεισφέρει στην έρευνα και τεχνολογία, αλλά και στην οικονομία της χώρας και κατ' επέκταση στην ενδυνάμωση του έργου της ΑΨΑ. Εντός του 2023 χρηματοδοτήθηκαν ακόμα δύο Ευρωπαϊκά προγράμματα με την ολική χρηματοδότηση να ανέρχεται στα €4,394,038. Στο πρώτο Ευρωπαϊκό έργο, η ΑΨΑ θα ιδρύσει ένα από τα δύο πρώτα Διασυνοριακά Κέντρα Κυβερνοασφάλειας στην Ευρώπη, μέσω του προγράμματος «ATHENA», με στόχο την ενίσχυση των δυνατοτήτων πρόβλεψης, πρόληψης, ανίχνευσης και απόκρισης των Κρατών Μελών. Το δεύτερο έργο «CY-TRUST», στοχεύει στην αύξηση της Κυβερνοασφάλειας, μέσω της εισαγωγής Τομεακών Επιχειρησιακών Κέντρων Ασφάλειας (Sectorial Security Operations Centres), καλύπτοντας τους τομείς της Ενέργειας, της Ναυτιλίας, των Κυβερνητικών & ΜΜΕ και Μικρομεσαίων Επιχειρήσεων (βλ. Ενότητα 9).

Δημιουργία Κοινότητας Κυβερνοασφάλειας

Κατά το 2023, το Εθνικό Κέντρο Κυβερνοασφάλειας της Κύπρου (NCC-CY) δημιούργησε την Εθνική Κοινότητα Κυβερνοασφάλειας. Η Κοινότητα συγκεντρώνει ενδιαφερόμενα μέρη με εμπειρογνωμοσύνη στους ακόλουθους τομείς: α) Ακαδημαϊκή εμπειρογνωμοσύνη ή εμπειρογνωμοσύνη σε έρευνα ή/και καινοτομία, β) Βιομηχανική ανάπτυξη ή ανάπτυξη προϊόντων, γ) Εξειδίκευση στον τομέα της κατάρτισης/εκπαίδευσης, δ) Εξειδίκευση στην ασφάλεια πληροφοριών ή/και επιχειρήσεις αντιμετώπισης περιστατικών, ε) Εμπειρογνωμοσύνη σε θέματα δεοντολογίας, στ) Εμπειρογνωμοσύνη σε τυπική και τεχνική τυποποίηση και προδιαγραφές.

Κύριος στόχος της Κοινότητας είναι η ενίσχυση, η ανταλλαγή και η διάδοση της εμπειρογνωμοσύνης της σε θέματα κυβερνοασφάλειας, τόσο σε εθνικό όσο και ευρωπαϊκό επίπεδο. (βλ. Ενότητα 5.2)

Σχέδιο Χορηγιών «Ενίσχυση Κυβερνοασφάλειας στις Κυπριακές Μικρομεσαίες Επιχειρήσεις (ΜμΕ) 2023 (NCC-CY-Enterprises/1223) & Δημιουργία Πλαισίου Κυβερνουγιεινής»

Το NCC-CY σε συνεργασία με το Ίδρυμα Έρευνας και Καινοτομίας (ΙδΕΚ) εξήγγειλε το πρώτο πιλοτικό σχέδιο χορηγιών προς ΜμΕ, με συνολικό προϋπολογισμό ενός (1) εκατομμυρίου ευρώ. Στόχος του σχεδίου ήταν η ενίσχυση των επιπέδων κυβερνοασφάλειας των μικρομεσαίων επιχειρήσεων του τόπου. (βλ.Ενότητα 5.3) . Επιπρόσθετα, το NCC-CY, αποσκοπώντας στην υγιή και ομαλή ανάπτυξη και εξέλιξη των Μικρομεσαίων Επιχειρήσεων (ΜμΕ), ανέπτυξε το «Πλαίσιο Κυβερνο-υγιεινής για ΜμΕ», ενός οδηγού για την εφαρμογή βασικών μέτρων από τις επιχειρήσεις με σκοπό την αύξηση του επιπέδου ασφαλείας τους (βλ. Ενότητα 5.4). Το συγκεκριμένο πλαίσιο είναι αναπόσπαστο κομμάτι του Σχεδίου Χορηγιών, ωστόσο μπορεί να χρησιμοποιηθεί και ως βέλτιστη πρακτική από ΜμΕ ανεξαρτήτως κλάδου οικονομικής δραστηριότητας.

Ακαδημία Τεχνολογίας Πληροφοριών, Επικοινωνιών & Κυβερνοασφάλειας (ICT)

Στα πλαίσια της στρατηγικής της ΑΨΑ δημιουργήθηκε η Ακαδημία Τεχνολογίας, Πληροφοριών, Επικοινωνιών και Κυβερνοασφάλειας (ICT), που έχει ως στόχο να καταστεί ένα αυτοσυντηρούμενο Περιφερειακό Κέντρο Εκπαίδευσης στον τομέα του ICT (βλ. Ενότητα 5.6). Σκοπός είναι να βοηθήσει στη στελέχωση θέσεων στην αγορά εργασίας μέσω της επανειδίκευσης και της αναβάθμισης των δεξιοτήτων των επαγγελματιών, όπως επίσης και στην εκπαίδευση / ενημέρωση του συνόλου της κοινωνίας, συμπεριλαμβανομένων μαθητών, γονέων, δασκάλων και ατόμων πέραν των 65 ετών. Στα ίδια πλαίσια, η ΑΨΑ στοχεύει στη διοργάνωση εγχώριων και διεθνών σεμιναρίων και συνεδρίων, καθώς επίσης και εκδηλώσεων δικτύωσης.

Ενίσχυση Ανθρώπινου Δυναμικού ΑΨΑ

Λόγω του αυξανόμενου όγκου κυβερνοεπιθέσεων και παράλληλα της ανάγκης για αναβαθμισμένη ανταπόκριση στα περιστατικά για την υποστήριξη των κρίσιμων υποδομών της Δημοκρατίας, η ΑΨΑ ολοκλήρωσε τις διαδικασίες για τη στελέχωση του Τομέα Ρύθμισης, Στρατηγικής και Εποπτείας και του Εθνικού CSIRT-CY. Κατά το 2023, προσλήφθηκαν δύο (2) Ανώτεροι Μηχανικοί και δεκαοκτώ (18) Μηχανικοί Ψηφιακής Ασφάλειας (βλ. Ενότητα 1.4).

Δημιουργία Γραφείου Διαχείρισης Έργων

Η δημιουργία του Γραφείου Διαχείρισης Έργων (Project Management Office – PMO) αποτέλεσε ένα σημαντικό βήμα για την ΑΨΑ. Το PMO έχει εφαρμόσει μια ισχυρή μεθοδολογία διαχείρισης έργων, έχει αναπτύξει βασικές πολιτικές και διαδικασίες, έχει εκπαιδεύσει το προσωπικό και εισήγαγε προηγμένα εργαλεία διαχείρισης έργων. Τα επιτεύγματα αυτά έχουν βελτιώσει τόσο την αποτελεσματικότητα και την επιτυχία των έργων μας, αλλά έχουν συμβάλει και στην συνολική ανάπτυξη και επιτυχία της Αρχής.

1. ΔΙΟΙΚΗΣΗ

Με βάση τον περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμο του 2020, Ν. 89(Ι)/2020, η Αρχή Ψηφιακής Ασφάλειας υπάγεται διοικητικά στον Επίτροπο Επικοινωνιών και τον Βοηθό Επίτροπο Επικοινωνιών.

1.1 Το Όραμα της Αρχής Ψηφιακής Ασφάλειας

Το Όραμα της ΑΨΑ είναι όπως η Κύπρος καταστεί μια από τις πρωτοπόρες χώρες της περιοχής, σε 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.

1.2 Οι Στόχοι της Αρχής Ψηφιακής Ασφάλειας

Η ΑΨΑ προσβλέπει στην προστασία των κρίσιμων υποδομών πληροφοριών του κράτους και τη σωστή λειτουργία των τεχνολογιών επικοινωνιών και πληροφορικής του τόπου με τα απαιτούμενα επίπεδα ασφάλειας προς όφελος του κάθε χρήστη, των πολιτών, της οικονομίας και της χώρας ευρύτερα, έχοντας ως βασικούς στόχους:

- τη θεσμοθέτηση και εφαρμογή διαφανούς νομοθετικού και ρυθμιστικού πλαισίου σε συνεργασία με όλες τις αρμόδιες υπηρεσίες του κράτους, αλλά και όλους τους εμπλεκόμενους φορείς,
- την ανάπτυξη εμπιστοσύνης μεταξύ όλων των εμπλεκομένων φορέων για τη διασφάλιση σωστής και αποτελεσματικής συνεργασίας,
- τη διαμόρφωση τεχνικών και οργανωτικών μέτρων και διαδικασιών (σε σχέση με την προετοιμασία, την προστασία, τον εντοπισμό και την ανταπόκριση σε συμβάντα), με σκοπό την αύξηση της ασφάλειας των φυσικών χώρων, των μηχανογραφικών και επικοινωνιακών εγκαταστάσεων, του εξοπλισμού και των λογισμικών στον απαιτούμενο βαθμό,
- την ανάπτυξη των απαραίτητων ικανοτήτων σε οργανισμούς και σε επιχειρήσεις, καθώς και τις υπηρεσίες του κράτους επί των θεμάτων κυβερνοασφάλειας,
- τη δημιουργία ή προσαρμογή των απαραίτητων δομών και μηχανισμών από όλους τους εμπλεκόμενους φορείς, ώστε να διασφαλιστούν οι απαιτήσεις και οι δυνατότητες άμεσης ανταπόκρισης σε συμβάντα και κρίσεις στον κυβερνοχώρο,
- την αποδοτική συνεργασία με αρμόδιους φορείς του δημόσιου και ιδιωτικού τομέα, τόσο σε εθνικό όσο και σε διεθνές επίπεδο,
- την προώθηση της έρευνας και καινοτομίας, ώστε το κράτος να είναι σε θέση να αντιμετωπίσει σε ικανοποιητικό βαθμό τις ταχύτατα εξελισσόμενες κυβερνοαπειλές, και κατ' επέκταση να αναπτύξει την κυβερνοασφάλεια εντός της Κυπριακής Δημοκρατίας.
- την προώθηση εκπαίδευσης και ενημέρωσης για την κυβερνοασφάλεια, έτσι ώστε να αναπτυχθεί σταδιακά η νοοτροπία και κατ' επέκταση η αλλαγή της κουλτούρας σε θέματα κυβερνοασφάλειας.

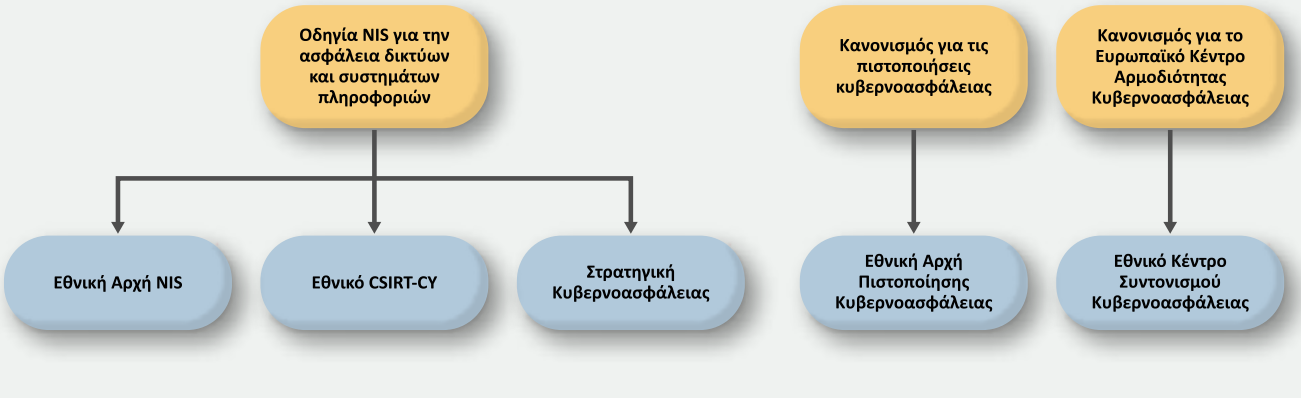
1.3 Οι Ρόλοι και οι αρμοδιότητες της Αρχής Ψηφιακής Ασφάλειας

1.3.1 Ευρωπαϊκό Πλαίσιο Κυβερνοασφάλειας και Ρόλοι ΑΨΑ

Η Ευρωπαϊκή Ένωση έχει προχωρήσει σημαντικά στον τομέα της κυβερνοασφάλειας τα τελευταία χρόνια, εκδίδοντας αριθμό νομοθεσιών[1] (σε μορφή Κανονισμών ή/και Οδηγιών), που καλύπτουν, σε Ευρωπαϊκό επίπεδο, τους γενικούς στόχους και τους ρόλους των Ευρωπαϊκών οργάνων στα θέματα κυβερνοασφάλειας, καθώς και των ρόλων και ελάχιστων δραστηριοτήτων / αρμοδιοτήτων που

αναμένεται να καλύπτουν τα κράτη μέλη. Η Κυπριακή Δημοκρατία ακολουθεί κεντρικοποιημένη προσέγγιση στη διαχείριση των θεμάτων κυβερνοασφάλειας και έτσι η ΑΨΑ έχει αναλάβει τους ακόλουθους ρόλους, όπως φαίνεται στο Γράφημα 1 πιο κάτω:

Γράφημα 1: Ευρωπαϊκές Νομοθεσίες και Ρόλοι ΑΨΑ



Οι πιο πάνω ρόλοι περιγράφονται σε συντομία στις ενότητες 1.3.2, 1.3.3, 1.3.4 και 1.3.5 με αναφορά στα τμήματα της ΑΨΑ. Οι λεπτομερείς δραστηριότητες της ΑΨΑ, σχετικά με τον κάθε ρόλο, ακολουθούν στις ενότητες 2, 3, 4 και 5.

1.3.2 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, προωθώντας 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 (βλ. ενότητα 2 για λεπτομέρειες των δραστηριοτήτων του Τομέα κατά το έτος 2023). Επίσης, στόχος του τομέα είναι ο συντονισμός της υλοποίησης της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας (βλ. Ενότητα 6).

[1] *https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016L1148 - Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση*
https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32019R0881 - Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)
https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32021R0887 - Κανονισμός (ΕΕ) 2021/887 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2021, για τη σύσταση του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού

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

Το Εθνικό CSIRT-CY αποτελεί τον τεχνικό και επιχειρησιακό βραχίονα της ΑΨΑ στα θέματα πρόληψης και διαχείρισης συμβάντων κυβερνοασφάλειας στις κρίσιμες υποδομές πληροφοριών της Κυπριακής Δημοκρατίας. Στόχος του Εθνικού CSIRT-CY είναι η πρόληψη, η ετοιμότητα εσωτερικής ασφάλειας και η αποτελεσματική αντιμετώπιση συμβάντων που δυνητικά μπορούν να πλήξουν τη λειτουργία υποδομών ζωτικής σημασίας, τόσο του δημόσιου, όσο και του ιδιωτικού τομέα, και ευρύτερα της κοινωνικοοικονομικής δράσης των πολιτών.

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

- Άμεση εφαρμογή πολιτικής διαχείρισης περιστατικών ασφαλείας σε περίπτωση που ένα περιστατικό κυβερνοασφάλειας βρίσκεται σε εξέλιξη ή έχει μόλις εντοπιστεί από τον οργανισμό,
- Συστήματα έγκαιρης προειδοποίησης για ανίχνευση ύποπτων δραστηριοτήτων στα συστήματα των κρίσιμων υποδομών πληροφοριών σε πραγματικό χρόνο,
- Ειδοποιήσεις ασφαλείας για τις οποίες χρήζουν ενημέρωσης οι διαχειριστές συστημάτων σε όλες τις υποδομές και αναφορές με βήματα μετριασμού, παραμετροποίησης και παρακαμπτήριές λύσεις,
- Δράσεις ευαισθητοποίησης για τις επιπτώσεις των κυβερνοαπειλών και εκπαιδεύσεις σε θέματα κυβερνοασφάλειας,
- Υπηρεσίες διαχείρισης τεκμηρίων ασφάλειας πληροφοριών μετά από καταστροφικά περιστατικά (δικανικές υπηρεσίες).

1.3.4 Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας (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, θα μεριμνά για την εφαρμογή των κανόνων που περιλαμβάνονται στα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ. Συγκεκριμένα, η ΕΑΠΚ θα εποπτεύει τους Οργανισμούς Αξιολόγησης Συμμόρφωσης (Conformity Assessment Body – CAB) και τα σχετικά τεχνικά εργαστήρια που διενεργούν τις τεχνικές αξιολογήσεις, οι οποίοι εμπλέκονται στις διαδικασίες πιστοποίησης. Επίσης, θα χειρίζεται τυχόν παράπονα που σχετίζονται με τους Οργανισμούς Αξιολόγησης Συμμόρφωσης ή/και με την πιστοποίηση προϊόντων και υπηρεσιών.

Απώτερος στόχος της ΕΑΠΚ είναι όπως συμβάλει στο να καταστεί η Κύπρος περιφερειακό κέντρο υπηρεσιών κυβερνοασφάλειας, τόσο μέσω των αρμοδιοτήτων της, αλλά και της συνεργασίας της με άλλες δομές.

1.3.5 Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY)

Η ΑΨΑ μετά από απόφαση του Υπουργικού Συμβουλίου την 21η Δεκεμβρίου 2021, ορίστηκε ως το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY) για την Κυπριακή Δημοκρατία. Παράλληλα, και με βάση την ίδια απόφαση του Υπουργικού Συμβουλίου, ορίστηκε ως μέλος της κοινοπραξίας του NCC-CY το Ίδρυμα Έρευνας και Καινοτομίας (ΙδΕΚ), με καθήκοντα οικονομικού διαχειριστή. Επίσης, ορίστηκε το Συμβούλιο του NCC-CY ως υπεύθυνο για τον καθορισμό του πλαισίου γενικής πολιτικής και για την εφαρμογή του Κανονισμού 2021/887 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρώπης της 20ης Μαΐου 2021 στην Κυπριακή Δημοκρατία. Ο Γενικός Διευθυντής του Υφυπουργείου Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής ή εκπρόσωπός του προεδρεύει του Συμβουλίου.

Το NCC-CY αποτελεί μέρος του Δικτύου 27 Εθνικών Κέντρων Συντονισμού Κυβερνοασφάλειας (NCCs) της Ευρώπης και μαζί με το Ευρωπαϊκό Κέντρο Αρμοδιότητας για την Κυβερνοασφάλεια (ECCC) διαδραματίζει βασικό ρόλο στην προώθηση ενός σταθερού και ασφαλούς κυβερνοχώρου, στην ενίσχυση της ανταγωνιστικότητας της Ευρώπης, στην ευαισθητοποίηση και την εκπαίδευση όλης της κοινωνίας, συμβάλλοντας παράλληλα στη χάραξη της πολιτικής της ΕΕ που αποσκοπεί στην ενίσχυση του επιπέδου κυβερνοασφάλειας στην Κύπρο και στην Ευρώπη ευρύτερα. Αυτό επιτυγχάνεται μέσω συνεργιών με τα κράτη μέλη και με φορείς της ΕΕ για τη δημιουργία μιας ισχυρής κοινότητας, ενισχύοντας την έρευνα και την καινοτομία, μέσω δράσεων ανάπτυξης δεξιοτήτων και ικανοτήτων και δημιουργώντας δράσεις και σχέδια χορηγιών για την οικονομική στήριξη των επιχειρήσεων στην Κύπρο.

1.4 Στελέχωση

Εντός του 2023 ολοκληρώθηκαν οι διαδικασίες του Συμβουλίου Επιλογής και Προαγωγών ΑΨΑ (ΣΕΠΑ) για τη στελέχωση του Τομέα Ρύθμισης, Στρατηγικής και Εποπτείας και του Εθνικού CSIRT-CY, όπου προσλήφθηκαν:

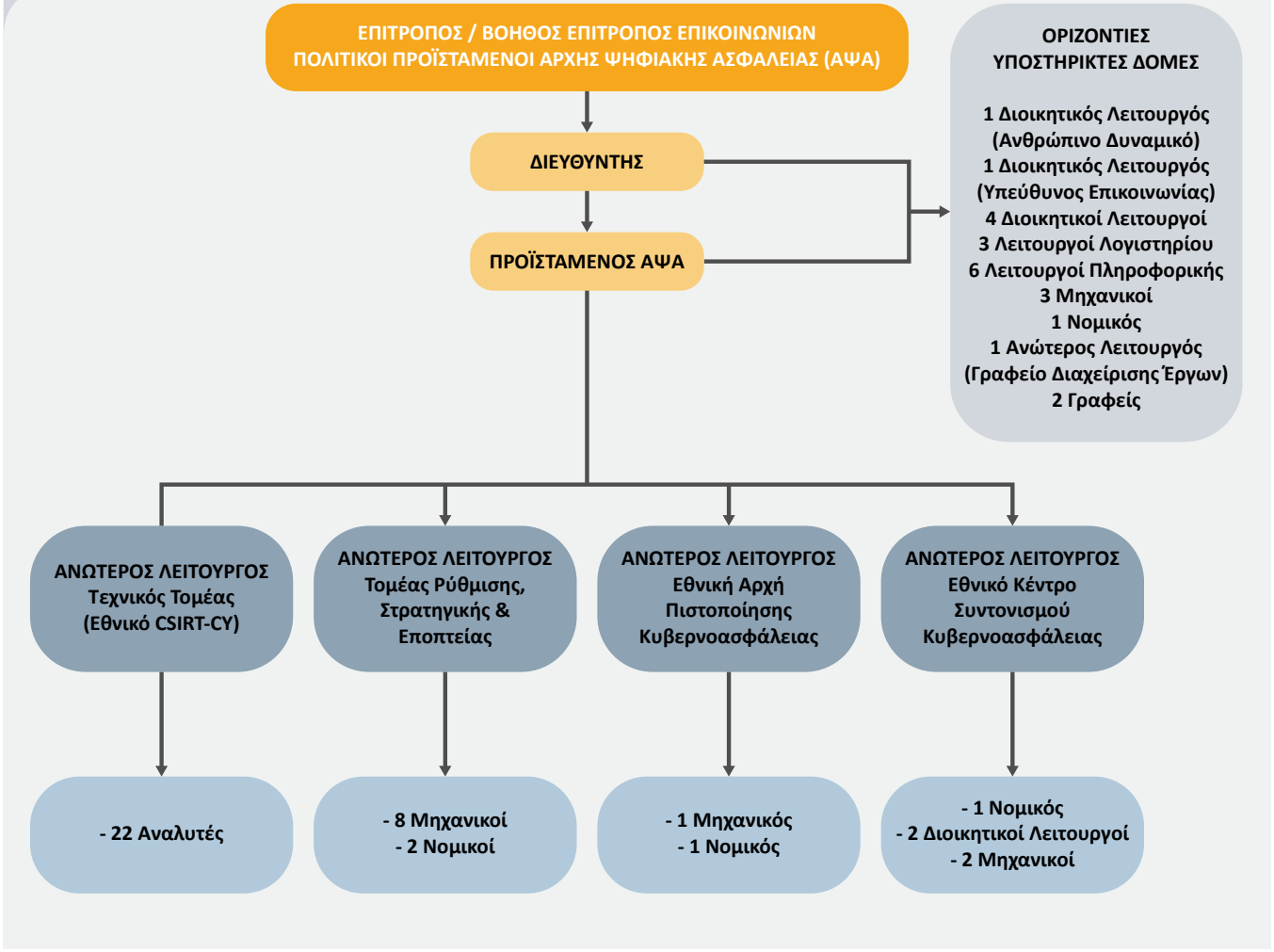
- Δύο (2) Ανώτεροι Μηχανικοί Ψηφιακής Ασφάλειας;
- Δεκαοκτώ (18) Μηχανικοί Ψηφιακής Ασφάλειας.

Σημειώνεται πως το προηγούμενο έτος ολοκληρώθηκαν οι αντίστοιχες διαδικασίες για την στελέχωση της θέσης του Πρώτου Λειτουργού – Προϊστάμενου της ΑΨΑ, καθώς και δύο (2) θέσεων μόνιμων Νομικών Λειτουργών. Ως εκ τούτου, ο συνολικός αριθμός των μόνιμων στελεχών ανέρχεται στα 23 άτομα. Επίσης, εντός του 2023 η ΑΨΑ απασχολούσε 45 συνεργάτες μέσω αγοράς υπηρεσιών.

Παράλληλα, εντός του 2023 σχεδιάστηκε πρόταση για μετάβαση του Εθνικού CSIRT σε λειτουργία επί εικοσιτετραώρου βάσης (24 ώρες, 7 μέρες την εβδομάδα) στη βάση ενός υβριδικού μοντέλου, το οποίο θα λειτουργήσει πλήρως εντός του 2024.

Καθώς η ΑΨΑ έχει αναλάβει νέες αρμοδιότητες (Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας και Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας), έχει ήδη προωθήσει πρόταση για τη δημιουργία σημαντικού αριθμού επιπρόσθετων μόνιμων θέσεων εργασίας τα επόμενα χρόνια, για τη συνεχόμενη θωράκιση και βελτίωση των επιπέδων κυβερνοασφάλειας στην Κυπριακή Δημοκρατία. Η εγκεκριμένη οργανωτική δομή της ΑΨΑ παρουσιάζεται στο γράφημα 2.

Γράφημα 2: Οργανόγραμμα ΑΨΑ



ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ ΤΗΣ ΑΡΧΗΣ ΨΗΦΙΑΚΗΣ ΑΣΦΑΛΕΙΑΣ

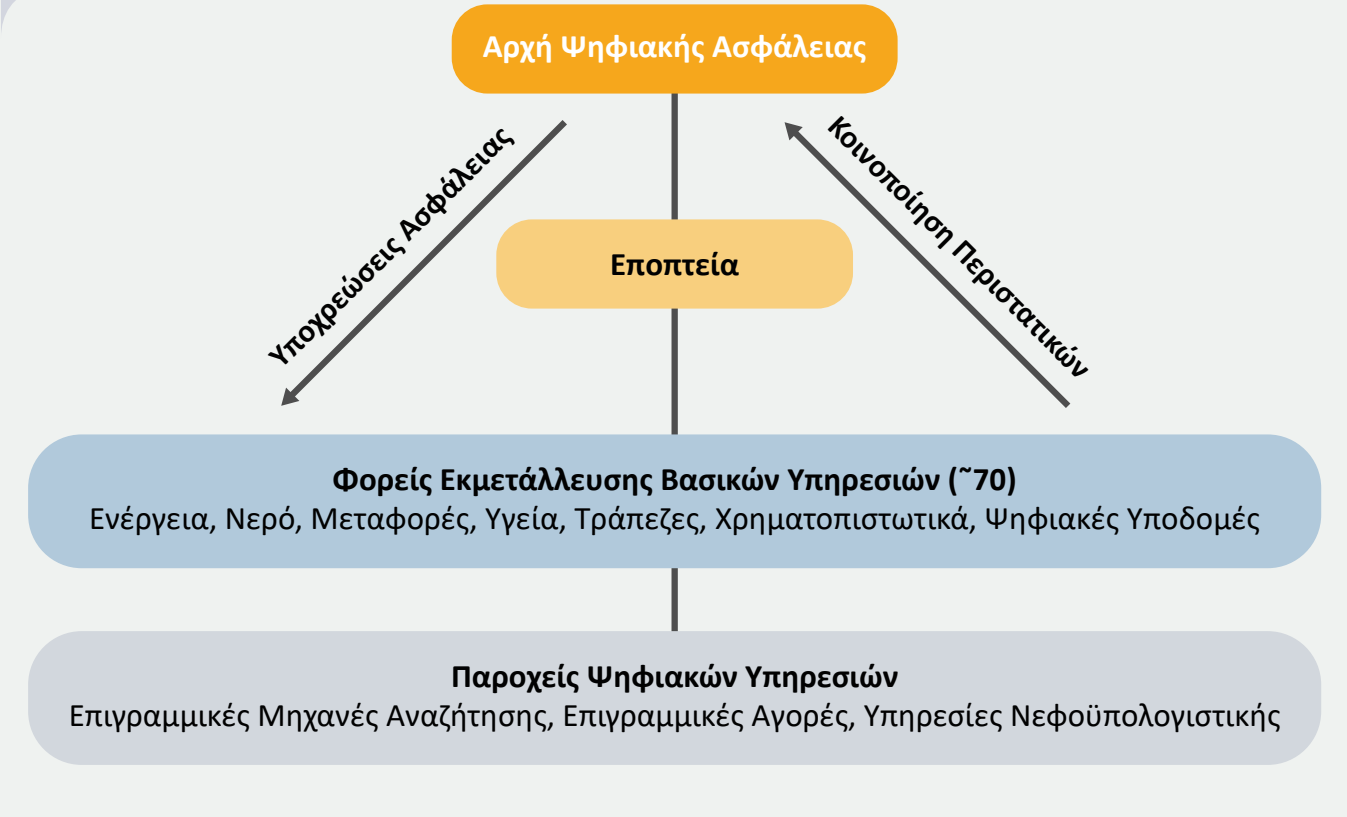
2. ΥΛΟΠΟΙΗΣΗ ΟΔΗΓΙΑΣ NIS ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

2.1 Οδηγία NIS

Η Οδηγία (ΕΕ) 2016/1148 για την ασφάλεια δικτύων και συστημάτων πληροφοριών (Οδηγία NIS) θεσπίζει μέτρα για την επίτευξη υψηλού κοινού επιπέδου ασφάλειας συστημάτων δικτύου και πληροφοριών εντός της Ευρωπαϊκής Ένωσης, με σκοπό την καλύτερη λειτουργία της εσωτερικής αγοράς. Για τον σκοπό αυτό, μεταξύ άλλων, η Οδηγία προβλέπει τις υποχρεώσεις των Κρατών Μελών, ώστε να θεσπίσουν μια εθνική στρατηγική για την ασφάλεια των συστημάτων δικτύων και πληροφοριών, και επίσης τις απαιτήσεις ασφάλειας και κοινοποίησης περιστατικών για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και για τους παρόχους ψηφιακών υπηρεσιών. Επιπρόσθετα, καθορίζει τις υποχρεώσεις των κρατών μελών στη διαδικασία ορισμού εθνικών αρμόδιων αρχών, ενιαίων κέντρων επαφής και Ομάδας Αντιμετώπισης Συμβάντων της Ασφάλειας Υπολογιστών (CSIRT).

Για την υλοποίηση της Οδηγίας στην Κυπριακή Δημοκρατία, η ΑΨΑ θέτει τις υποχρεώσεις ασφάλειας προς όλους τους κρίσιμους φορείς, εποπτεύει την υλοποίηση των σχετικών μέτρων και διαχειρίζεται κοινοποιήσεις περιστατικών κατά περίπτωση (βλ. γράφημα 3).

Γράφημα 3: Κύριες δραστηριότητες ΑΨΑ με τους κρίσιμους Φορείς



2.2 Νομοθεσία Αρχής Ψηφιακής Ασφάλειας

2.2.1 Νόμος ΑΨΑ – Ν.89(Ι)/2020 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών

Ο Νόμος 89(Ι)/2020 («Νόμος») της ΑΨΑ εναρμονίζει πλήρως την εθνική νομοθεσία με το Ευρωπαϊκό Νομικό πλαίσιο, σχετικά με τα μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύων και πληροφοριών σε φορείς εκμετάλλευσης βασικών υπηρεσιών και φορείς κρίσιμων υποδομών πληροφοριών (Οδηγία (ΕΕ) 2016/1148 – «Οδηγία NIS»). Επιπλέον, εναρμονίζει μερικώς (μόνο τα άρθρα 40/41) την εθνική νομοθεσία με το ευρωπαϊκό νομικό πλαίσιο αναφορικά με τον Ευρωπαϊκό Κώδικα Ηλεκτρονικών Επικοινωνιών (Οδηγία (ΕΕ) 2018/1972 - για την ασφάλεια των δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών). Σύμφωνα με τον Νόμο, η ΑΨΑ ορίστηκε ως η Εθνική Αρχή για την ασφάλεια δικτύων και συστημάτων πληροφοριών και ως υπεύθυνη για τον συντονισμό της υλοποίησης της Στρατηγικής Κυβερνοασφάλειας.

2.2.2 Τροποποίηση Νόμου

Η νέα Οδηγία (ΕΕ) 2022/2555 («**Οδηγία NIS2**»)[2], η οποία εγκρίθηκε τον Δεκέμβριο του 2022 από το Ευρωπαϊκό Κοινοβούλιο και από το Συμβούλιο της Ευρωπαϊκή Ένωσης σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, προβλέπει νομικά μέτρα για την ενίσχυση του συνολικού επιπέδου κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση. Η νέα Οδηγία θέτει ακόμα πιο υψηλούς στόχους κυβερνοασφάλειας για τις βασικές και σημαντικές οντότητες στο κάθε κράτος μέλος της ΕΕ, με γνώμονα τη μεγιστοποίηση της κοινωνικής ανθεκτικότητας μέσω δομημένων προσεγγίσεων κυβερνοασφάλειας σε πολλαπλά επίπεδα.

Η αρχική 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 ΕΕ.

Με σκοπό την εναρμόνιση της Οδηγίας NIS2 στην εθνική νομοθεσία, η ΑΨΑ ετοίμασε πλήρες τροποποιητικό νομοσχέδιο σχετικά με την εν λόγω εναρμόνιση. Σημειώνεται ότι, η Οδηγία NIS2 θα τεθεί σε εφαρμογή στις 18 Οκτωβρίου 2024 και την ίδια μέρα η Οδηγία NIS θα παύσει να ισχύει.

Στις 21 Αυγούστου 2023, η ΑΨΑ ανακοίνωσε τη διεξαγωγή της Δημόσιας Διαβούλευσης ΑΨΑ 01/2023[3] επί του Νόμου που τροποποιεί τον περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμο του 2020 (Ν. 89(Ι)/2020), κατά τη διάρκεια της οποίας κλήθηκαν τα ενδιαφερόμενα μέρη και οι ενδιαφερόμενοι φορείς να υποβάλουν τις απόψεις τους επί του περιεχομένου του τροποποιητικού νομοσχεδίου, το οποίο θα ενσωματώσει πλήρως την Οδηγία NIS2 στην Κυπριακή νομοθεσία.

Σημειώνεται ότι στο προσχέδιο του νόμου που τροποποιεί τον Νόμο 89(Ι)/2020, ενσωματώθηκαν επίσης και νέοι ρόλοι και αρμοδιότητες της ΑΨΑ για την κάλυψη των πιο κάτω:

- Εναρμόνιση με τα σημεία (δ), (ε), (στ) και (θ) του άρθρου 3(3) της Οδηγίας 2014/53/ΕΕ, που αφορούν τον ραδιοεξοπλισμό (Radio Equipment Directive – RED) και μεταφέρονται από το Νόμο 112(Ι)/2004 στο Νόμο 89(Ι)/2020, μετά από σχετικές διαβουλεύσεις με τον Υφυπουργό Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής
- Τροποποίηση συγκεκριμένων διατάξεων στην υφιστάμενη νομοθεσία της ΑΨΑ, μετά από εισηγήσεις που έλαβε η ΑΨΑ κατά τη διενέργεια της Δημόσιας Διαβούλευσης για την περί

[2] *https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32022L2555*
[3] *https://dsa.cy/category/announcements/public-consultation-dsa-01-2023*

Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κυβερνοασφάλεια Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών Πέμπτης Γενιάς 5G) Απόφαση του 2020 (Κ.Δ.Π. 408/2020), με σκοπό τη βελτίωση της συνεργασίας μεταξύ ΑΨΑ και Αστυνομίας Κύπρου,

- Τροποποίηση συγκεκριμένων διατάξεων για την ενοποίηση των διοικητικών δομών της ΑΨΑ υπό την εποπτεία του Επιτρόπου Επικοινωνιών. Οι υπό αναφορά αλλαγές συνάδουν με την πολιτική απόφαση για τη δομή της Νομοθεσίας του Επιτρόπου Επικοινωνιών, με τη δημιουργία Νόμου Ομπρέλα (υφιστάμενος Νόμος 112(I)/2004). Ο εν λόγω Νόμος Ομπρέλα θα καλύπτει όλα τα θέματα που αφορούν τη διοίκηση και το ανθρώπινο δυναμικό της υπηρεσίας. Επιπλέον, θα καλύπτει και τη δημιουργία τριών κάθετων / ειδικών νομοθεσιών για τα ρυθμιστικά θέματα στους τομείς αρμοδιότητας του Επιτρόπου Επικοινωνιών (Ηλεκτρονικές Επικοινωνίες, Ταχυδρομικές Υπηρεσίες και Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών).

Με το πέρας της Δημόσιας Διαβούλευσης ΑΨΑ 01/2023, η ΑΨΑ αξιολόγησε τα σχόλια των ενδιαφερόμενων φορέων και προέβη στις απαραίτητες αλλαγές επί του τροποποιητικού νομοσχεδίου, το οποίο αναμένεται να τύχει νομοτεχνικού ελέγχου από τη Νομική Υπηρεσία και να εγκριθεί από το Υπουργικό Συμβούλιο εντός του 2024, όπου μετέπειτα θα ψηφιστεί από τη Βουλή των Αντιπροσώπων.

2.3 Εποπτεία Μέτρων Ασφάλειας σε Κρίσιμους Φορείς

Ως αναφέρεται στην Ενότητα 2.1, η ΑΨΑ θέτει υποχρεώσεις ασφάλειας προς όλους τους κρίσιμους φορείς και εποπτεύει την υλοποίηση των σχετικών μέτρων. Τα μέτρα αυτά εξειδικεύονται στην Απόφαση ΚΔΠ 389/2020 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών), όπου περιλαμβάνεται ένας κατάλογος 70 τεχνικών και οργανωτικών μέτρων για ολιστική προσέγγιση των Φορέων όσο αφορά στην επίτευξη ενός υψηλού επιπέδου κυβερνοασφάλειας.

Κατά το έτος 2023, η ΑΨΑ προχώρησε στην υλοποίηση αριθμού 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 389/2020 (μεταξύ άλλων, έγγραφα διαχείρισης κινδύνων, διακυβέρνησης και σχεδιασμού επιχειρησιακής συνέχειας).
- Διεκπεραίωση συναντήσεων προόδου στους δεκαπέντε (15) πιο κρίσιμους Φορείς, για να διαπιστωθεί το επίπεδο εφαρμογής των προνοιών της Απόφασης ΚΔΠ 389/2020, και ειδικά, τον έλεγχο υλοποίησης και εφαρμογής των μέτρων ασφαλείας για αντιμετώπιση των υψηλότερων σε κρισιμότητα κινδύνων που εντοπίζονται από τους φορείς. Στις σχετικές συναντήσεις, εξετάστηκε η πρόοδος που επιτεύχθηκε όσον αφορά:
  - Την υλοποίηση και εφαρμογή των μέτρων ασφάλειας που αντιμετωπίζουν τους υψηλότερους σε επίπεδο κινδύνους που εντοπίζουν οι φορείς (Άρθρο 21(1)(γ) ΚΔΠ 389/2020 – πρώτο σημείο).
  - Το σχέδιο δράσης που υποβλήθηκε από τους Φορείς για υλοποίηση του συνόλου του πλαισίου κυβερνοασφάλειας ΚΔΠ 389/2020, έπειτα από διενέργεια αξιολόγησης κινδύνων (Άρθρο 21(1)(γ) ΚΔΠ 389/2020 – δεύτερο σημείο).
  - Την υλοποίηση των ευρημάτων ελέγχου αρχείων (Document Review Findings and Action Plan) για τους Φορείς που έχουν καταθέσει τέτοια στοιχεία, κατ' απαίτηση της περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών) Απόφασης του 2020 (Κ.Δ.Π. 389/2020).

- Ανάπτυξη Μοντέλου Ωριμότητας Κυβερνοασφάλειας πέντε επιπέδων (five level Cybersecurity Maturity Model), το οποίο είναι δομημένο πάνω στις απαιτήσεις (τεχνικά και οργανωτικά μέτρα) της Απόφασης Κ.Δ.Π. 389/2020. Το επίπεδο 3 έχει καθοριστεί ως το επίπεδο με τις ελάχιστες απαιτήσεις της νομοθεσίας, ώστε να μπορεί να αναγνωρίσει το επίπεδο τόσο των Φορέων που έχουν ήδη ικανοποιήσει τις απαιτήσεις, όσο και αυτών που δεν έχουν ικανοποιήσει ακόμα τις απαιτήσεις της νομοθεσίας. Στα πλαίσια υλοποίησης του Μοντέλου Ωριμότητας έχει επίσης ολοκληρωθεί σημαντική εργασία δημιουργίας μιας σειράς εγγράφων του πλαισίου ελέγχου, όπως ερωτηματολόγιο ανανέωσης βασικών στοιχείων φορέα, οδηγίες προς τους επιθεωρητές, έκθεση ελέγχου, περιγραφή του ρόλου του Ελεγκτή Ωριμότητας Κυβερνοασφάλειας και διαδικασία διεξαγωγής επιθεώρησης. Το μοντέλο αυτό θα χρησιμοποιηθεί τόσο από τους ίδιους τους Φορείς για να επιμετρούν το επίπεδο ωριμότητας και συμμόρφωσής τους με τις πρόνοιες της νομοθεσίας που αφορά τα μέτρα ασφάλειας, αλλά κυρίως θα αποτελέσει το εργαλείο ελέγχου και αξιολόγησης από μέρους των εξωτερικών ελεγκτών των εποπτευόμενων Φορέων.
- Πιλοτικές επιθεωρήσεις για την εφαρμογή του μοντέλου ωριμότητας, σε τέσσερις (4) επιλεγμένους Φορείς. Οι εμπειρίες, η ανατροφοδότηση και τα αποτελέσματα που είχαν εξαχθεί από τις επιθεωρήσεις αυτές βοήθησαν στον περαιτέρω εμπλουτισμό και διόρθωση του Μοντέλου.
- Αξιολόγηση κενών (Gap Assessment) σε επιλεγμένους φορείς σχετικά με μέτρα για την επίτευξη υψηλού επιπέδου ασφάλειας δικτύων και συστημάτων πληροφοριών.

2.4 Κοινοποίηση Περιστατικών Παραβίασης Ψηφιακής Ασφάλειας

Η Απόφαση ΚΔΠ 39/2022, σχετικά με τις κοινοποιήσεις περιστατικών ασφάλειας, εφαρμόζεται υποχρεωτικά από όλους τους Φορείς και Παροχείς. 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 και Παρόχων. Συνεπώς, ενεργοποιείται η υποχρέωση των Φορέων και Παροχέων 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 2023, υποβλήθηκαν στην ΑΨΑ δεκατέσσερεις (14) κοινοποιήσεις περιστατικών, συμπεριλαμβανομένου τόσο των υποχρεωτικών, αλλά και εθελοντικών κοινοποιήσεων, οι οποίες έτυχαν διαχείρισης κατά περίπτωση (βλ. επίσης Ενότητα 3).

2.5 Πλατφόρμα Διαχείρισης Εμπλεκόμενων Φορέων

Η ηλεκτρονική πλατφόρμα iDSAMPL (integrated Digital Security Authority Management Platform) δημιουργήθηκε από την ΑΨΑ ως η ολοκληρωμένη πλατφόρμα διαχείρισης των εποπτευόμενων Φορέων, οι οποίοι τη χρησιμοποιούν για να εκπληρώνουν τις υποχρεώσεις τους που προκύπτουν από τον Νόμο 89(Ι)/2020 και τις αντίστοιχες δευτερογενείς νομοθεσίες που έχουν εκδοθεί με βάση αυτόν.

Κατά το έτος 2023, η πλατφόρμα χρησιμοποιείται από περίπου 70 Φορείς (όπως αυτοί έχουν αναγνωρισθεί βάσει της Οδηγίας NIS), αλλά με την υλοποίηση και εφαρμογή της Οδηγίας NIS2 (περί τα τέλη του έτους 2024) αναμένεται ότι οι Φορείς θα πολλαπλασιαστούν, με ενδεχόμενο να ξεπεράσουν ακόμη και τους 500.

Οι υφιστάμενες λειτουργικότητες της πλατφόρμας είναι οι εξής:

- Διαχείριση στοιχείων επικοινωνίας των Φορέων (Contact Management)
- Κοινοποίηση και Διαχείριση Περιστατικών (Incident Reporting and Management)
- Διαχείριση συμμόρφωσης των Φορέων (Compliance Management)
- Διαχείριση Κινδύνων (Risk Management)
- Διαχείριση ελέγχων (Audit Management)
- Διαχείριση ενεργειών μετριασμού (Mitigation Actions Management)
- Αποστολή ειδοποιήσεων (Alerts and Notifications).

Λόγω της αναμενόμενης μεγάλης αύξησης στον αριθμό των εποπτευόμενων φορέων με τη νέα Οδηγία NIS2, έχει κριθεί απαραίτητο να δημιουργηθεί αναβαθμισμένη έκδοση της πλατφόρμας, προσαρμοσμένη στις νέες απαιτήσεις. Ήδη από τον Νοέμβριο του 2023 έχει ξεκινήσει η ανάλυση των νέων αναγκών που προκύπτουν από την Οδηγία NIS2 με την καταγραφή των αλλαγών και αναπροσαρμογών που απαιτούνται να γίνουν στην πλατφόρμα. Η πρώτη έκδοση της αναβαθμισμένης πλατφόρμας αναμένεται να ολοκληρωθεί περί τα τέλη του 2024.

Επιπρόσθετα, λόγω του ότι εντός του 2024 η ΑΨΑ θα προχωρήσει στη διενέργεια ελέγχων συμμόρφωσης για εφαρμογή της Απόφασης ΚΔΠ 389/2020, ξεκίνησε από τον Οκτώβριο του 2023 ανάλυση απαιτήσεων για την ανάπτυξη ενός εργαλείου για τη διαχείριση των ελέγχων που θα διενεργούνται από πιστοποιημένους ελεγκτές από το Μητρώο Ελεγκτών Κυβερνοασφάλειας. Η υλοποίηση, ο έλεγχος και η εφαρμογή του σχετικού εργαλείου θα ολοκληρωθεί το πρώτο εξάμηνο του 2024.

3. ΔΙΑΧΕΙΡΙΣΗ ΣΥΜΒΑΝΤΩΝ ΚΑΙ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

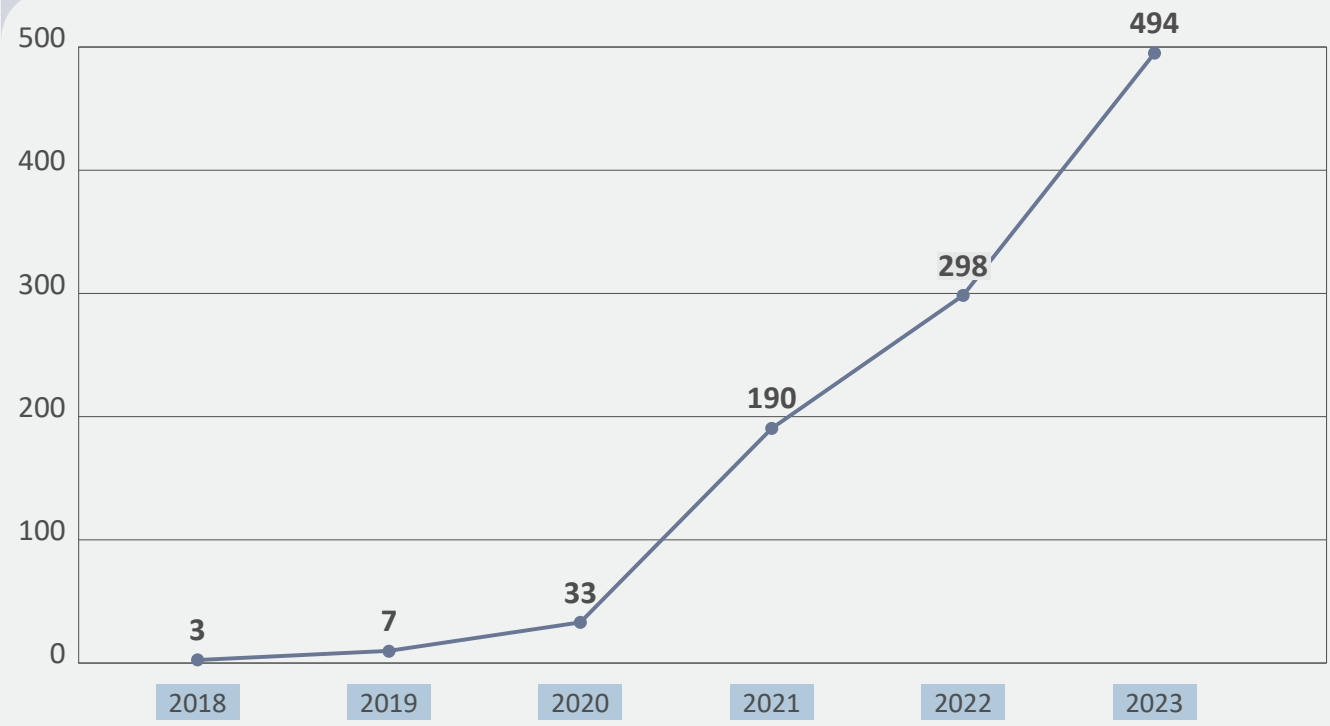
3.1 Διαδικασίες Εθνικού CSIRT-CY

Η Εθνική Ομάδα Αντιμετώπισης Συμβάντων της Ασφάλειας Υπολογιστών της Κύπρου (CSIRT-CY) εφαρμόζει ένα σύνολο διαδικασιών διαχείρισης από τη στιγμή που θα εντοπίσει ένα περιστατικό έως την επίλυσή του. Οι εν λόγω διαδικασίες έχουν αξιολογηθεί και εγκριθεί από διεθνείς και ευρωπαϊκούς οργανισμούς όπως το FIRST[4], ο TI[5] και ο ENISA[6]. Ως οι σημαντικότεροι στόχοι του Εθνικού CSIRT-CY έχουν τεθεί, η αντιμετώπιση περιστατικών κυβερνοασφάλειας και ο περιορισμός των επιδράσεών τους.

3.2 Διαχείριση Περιστατικών

Κατά το έτος 2023 το Εθνικό CSIRT κατέγραψε συνολικά 494 περιστατικά. Όπως φαίνεται και στο γράφημα 4 πιο κάτω, τα τελευταία χρόνια υπάρχει μια αυξητική τάση στον αριθμό των περιστατικών που κοινοποιήθηκαν στο Εθνικό CSIRT. Αυτή η τάση δεν οφείλεται μόνο στην αύξηση των κυβερνοεπιθέσεων στις υποδομές της Κυπριακής Δημοκρατίας, αλλά αντικατοπτρίζει επίσης την αμοιβαία εμπιστοσύνη που έχει δημιουργηθεί μεταξύ των φορέων κρίσιμων υποδομών και του Εθνικού CSIRT. Αυτό οδηγεί στην κοινοποίηση, ακόμη και εθελοντικά, κάθε ύποπτου περιστατικού από τους φορείς κρίσιμων υποδομών, προκειμένου να λάβουν άμεση ανταπόκριση και αποτελεσματική υποστήριξη.

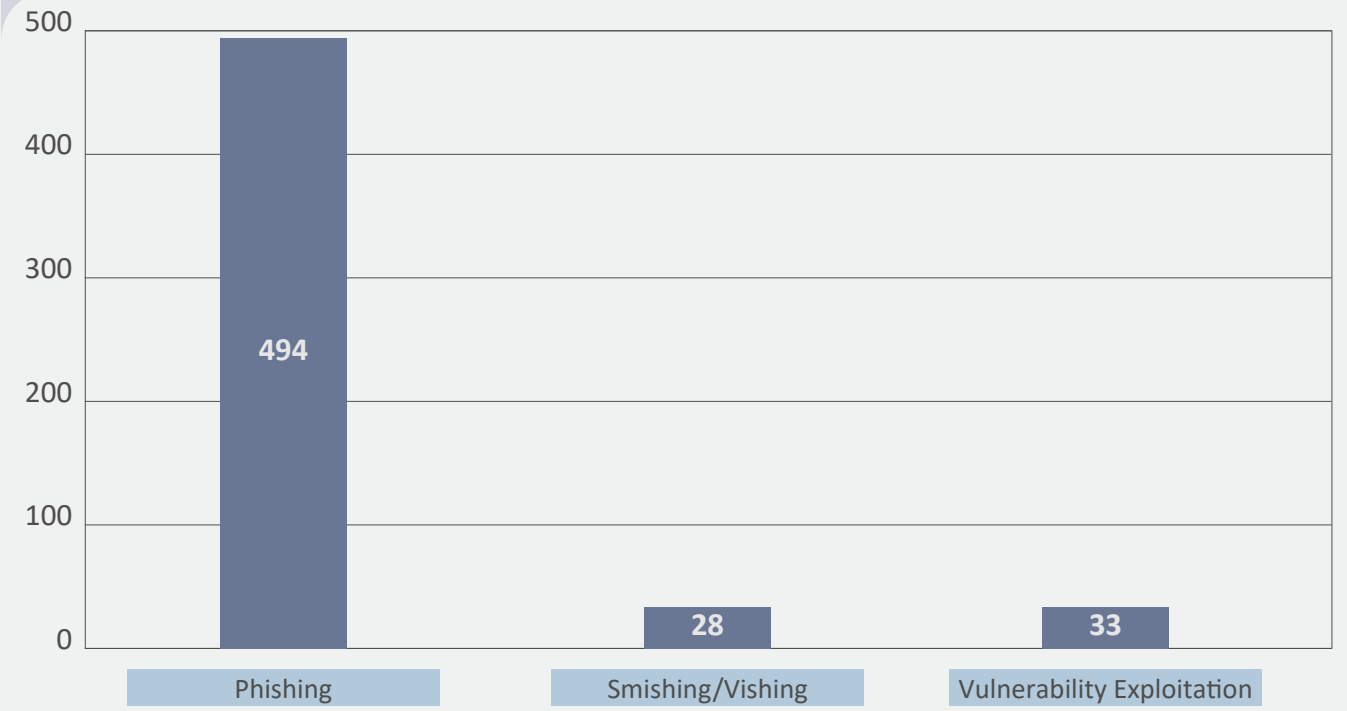
Γράφημα 4: Καταγεγραμμένα περιστατικά ανά έτος



[4] *FIRST: Forum of Incident Response and Security Teams*
[5] *Trusted Introducer*
[6] *ENISA: European Union Agency for Cybersecurity*

Όσον αφορά την ανάλυση των περιστατικών, το Εθνικό CSIRT κατέγραψε αυξημένο αριθμό αναφορών σχετικά με περιστατικά επιθέσεων Phishing, συμπεριλαμβανομένων των επιθέσεων Smishing και Vishing, όπως αποτυπώνεται στο Γράφημα 5. Η επίθεση Phishing / Smishing / Vishing, γνωστή και ως ηλεκτρονικό ψάρεμα, αποτελεί μια μορφή απάτης που διεξάγεται είτε μέσω ηλεκτρονικού ταχυδρομείου (Phishing) είτε μέσω μηνυμάτων κινητών τηλεφώνων (Smishing) ή μέσω τηλεφωνικών κλήσεων (Vishing). Στόχος των επιτιθέμενων είναι να εξαπατήσουν το θύμα με σκοπό την υποκλοπή ευαίσθητων πληροφοριών ή χρηματικού ποσού και την εγκατάσταση κακόβουλου λογισμικού.

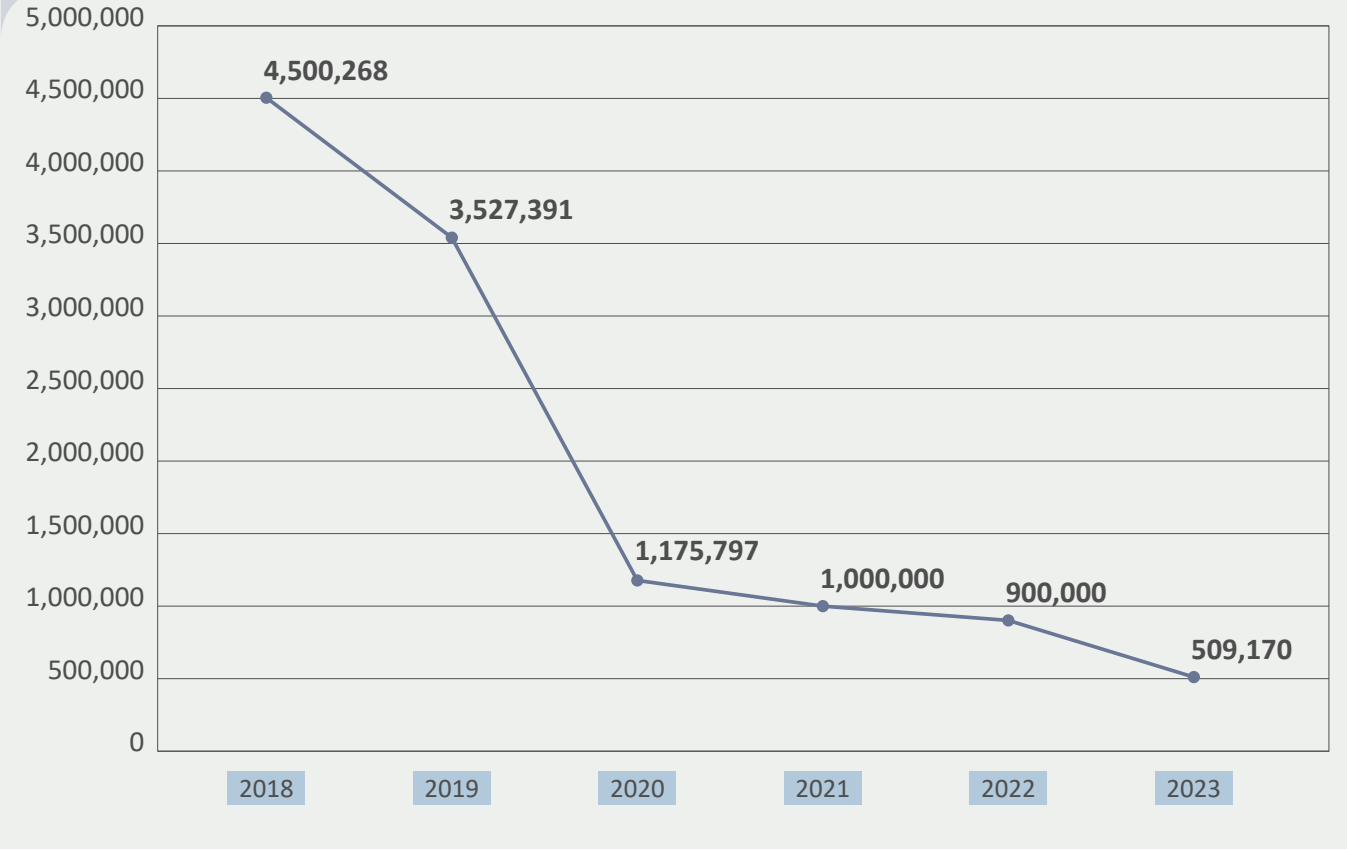
Γράφημα 5: Περιστατικά Phising/Smishing/Vishing για το 2023



3.3 Προληπτικές Ειδοποιήσεις (Alerts)

Μια από τις σημαντικότερες δραστηριότητες του Εθνικού CSIRT-CY είναι η συλλογή πληροφοριών για ευπάθειες, με τη χρήση εξειδικευμένων πλατφόρμων, αλλά και την αποστολή σχετικών ειδοποιήσεων στις κρίσιμες υποδομές. Οι ειδοποιήσεις και το περιεχόμενό τους συμβάλουν σημαντικά στην προσπάθεια πρόληψης πιθανών κυβερνοεπιθέσεων. Σύμφωνα με το Γράφημα 6, το 2023 έχουν κοινοποιηθεί 509,170 ειδοποιήσεις ευπαθειών προς τους φορείς κρίσιμων υποδομών. Η μείωση των ευπαθειών, συγκριτικά με τις προηγούμενες χρονιές, αποδεικνύει μια αξιόλογη βελτίωση στη θωράκιση του εθνικού κυβερνοχώρου και της ευρύτερης κυβερνοασφάλειας. Παρόλα αυτά, ο αριθμός των ευπαθειών χρήζει περαιτέρω βελτίωσης μέσα από την ενεργότερη εμπλοκή των κρίσιμων υποδομών με τη λήψη στοχευμένων μέτρων και στρατηγικής προστασίας.

Γράφημα 6: Κοινοποιημένες αδυναμίες που θα μπορούσαν να καταλήξουν σε περιστατικό κυβερνοασφάλειας ανά έτος



3.4 Υποδομή Εθνικού CSIRT-CY (Εθνική Ομάδα Αντιμετώπισης Συμβάντων της Ασφάλειας Υπολογιστών)

Το Εθνικό CSIRT-CY διασφαλίζει τη διαρκή ανάπτυξη και εκσυγχρονισμό της υποδομής του με εξειδικευμένα εργαλεία, που επιτρέπουν την πραγματοποίηση συστηματικών ελέγχων στις κρίσιμες υποδομές πληροφοριών της Κυπριακής Δημοκρατίας. Μέσω αυτών των εργαλείων, εκτιμάται το επίπεδο ασφάλειας των κρίσιμων υποδομών πληροφοριών και εντοπίζονται πιθανές αδυναμίες και ευπάθειες. Αυτό επιτρέπει την παροχή των απαραίτητων συστάσεων για τη συνεχή ενίσχυση των μέτρων ασφαλείας που λαμβάνουν οι υποδομές, προκειμένου να αντιμετωπίζονται αποτελεσματικά οι κυβερνοαπειλές.

Ορισμένα από τα εργαλεία που αξιοποιεί το Εθνικό CSIRT-CY είναι:

- Εξειδικευμένοι αισθητήρες για την πραγματοποίηση ελέγχων ασφαλείας στα δίκτυα των κρίσιμων υποδομών πληροφοριών σε πραγματικό χρόνο. Οι αισθητήρες ελέγχονται από την υποδομή του Κέντρου Επιχειρήσεων Ασφάλειας (Security Operations Centre - SOC) του Εθνικού CSIRT και επιτρέπουν στην ομάδα SOC να ανιχνεύει και να αναλύει ύποπτες και κακόβουλες ενέργειες στις κρίσιμες υποδομές πληροφοριών, προκειμένου να παρέχονται έγκαιρες προειδοποιήσεις σε περίπτωση που προκύψουν περιστατικά κυβερνοασφάλειας.
- Πλατφόρμα εκπαίδευσης και κατάρτισης (Cyber Range), η οποία υποστηρίζει τη δημιουργία εικονικών δικτύων και υποδομών πληροφοριών, με σκοπό την πραγματοποίηση ασκήσεων κυβερνοασφάλειας με ρεαλιστικά σενάρια σε διάφορους τομείς, όπως η ναυτιλία, η ενέργεια και οι ηλεκτρονικές επικοινωνίες.
- Εργαλεία για εκτέλεση δοκιμών διείσδυσης (penetration testing) στα συστήματα, δίκτυα και

τις εφαρμογές ενός οργανισμού. Στόχος των δοκιμών είναι να βοηθήσουν στην προστασία του οργανισμού από επιθέσεις και να διασφαλίσουν ότι οι ευπάθειες του συστήματος ανακαλύπτονται και διορθώνονται πριν να τύχουν εκμετάλλευσης από κακόβουλους επιτιθέμενους. Επίσης, οι δοκιμές διείσδυσης μπορούν να χρησιμοποιηθούν για να επιβεβαιωθεί η συμμόρφωση με συγκεκριμένους κανονισμούς ή πρότυπα ασφάλειας.

- Η πλατφόρμα CyMap Analyzer της οποίας η εγκατάσταση και η λειτουργία ολοκληρώθηκε με επιτυχία σε συνεργασία με το Πανεπιστήμιο Κύπρου, πραγματοποιεί σε καθημερινή βάση σάρωση του εθνικού διαδικτυακού χώρου (IPv4/IPv6) που είναι προσβάσιμος από το Εθνικό CSIRT-CY. Έχει τη δυνατότητα συλλογής, επεξεργασίας και αποθήκευσης πληροφοριών που σχετίζονται με ευπάθειες και κακόβουλα λογισμικά και την εξαγωγή των πληροφοριών σε μορφή αναφοράς.

3.5 Εκπαιδεύσεις Εθνικού CSIRT-CY (Εθνική Ομάδα Αντιμετώπισης Συμβάντων της Ασφάλειας Υπολογιστών)

Η ομάδα του Εθνικού CSIRT-CY υποβάλλεται σε συνεχή εκπαίδευση για την ενίσχυση των δυνατοτήτων της. Η εκπαίδευση αυτή διεξάγεται ποικιλοτρόπως, όπως με τη συμμετοχή σε εργαστήρια και σεμινάρια τόσο εντός όσο και εκτός Κύπρου, καθώς και με τη συμμετοχή σε εθνικές και πανευρωπαϊκές ασκήσεις.

Επισημαίνονται κάποιες εκπαιδευτικές δράσεις που έλαβε μέρος το προσωπικό του Εθνικού CSIRT-CY εντός του 2023:

- Αναπτύχθηκε πολυεπίπεδο πρόγραμμα εκπαίδευσης για τις εξειδικεύσεις των ομάδων του CSIRT-CY (π.χ. Ομάδα Δικανικής Ανάλυσης, Ομάδα Ανάλυσης Κακόβουλων Λογισμικών) και ήδη ολοκληρώθηκαν οι πρώτες εκπαιδεύσεις,
- Συμμετοχή στην άσκηση Interregional CyberDrill for Europe and Asia-Pacific (βλ. Ενότητα 6.2.4), η οποία διοργανώθηκε από τη Διεθνή Ένωση Τηλεπικοινωνιών και φιλοξενήθηκε από την ΑΨΑ,
- Εκπαίδευση μέσω του Joint Cybersecurity Operations Platform (CEF-JCOP), ενός Ευρωπαϊκού συγχρηματοδοτούμενου έργου (βλ. Ενότητα 9.1.1),
- Εκπαίδευση μέσω του Ευρωπαϊκού συγχρηματοδοτούμενου έργου Phoenix (Power System's Shield against complex Incidents and extensive cyber and privacy attacks) (βλ. Ενότητα 9.1.2).

3.6 Πλατφόρμα Έγκαιρων Προειδοποιήσεων (Early Warning System)

Μέσα στο πλαίσιο της συνεχούς παρακολούθησης και της έγκαιρης ενημέρωσης για κυβερνοεπιθέσεις, το εθνικό CSIRT έχει συνεχή επικοινωνία με πλατφόρμες (threat intelligence feeds) που περιέχουν δείκτες παραβίασης (Indicators of Compromise - IOCs). Μερικά παραδείγματα από αυτούς τους δείκτες παραβίασης είναι η διεύθυνση IP, τα ονόματα χώρου (domain names), οι τιμές κατακερματισμού (hashes) αρχείων, οι διευθύνσεις ηλεκτρονικού ταχυδρομείου και άλλα. Το εθνικό CSIRT παρέχει ειδοποιήσεις στις κρίσιμες υποδομές όταν κάποιος από αυτούς τους δείκτες εμφανιστεί σε μια από τις υποδομές.

3.7 Κέντρο Επιχειρήσεων (Security Operation Center - SOC)

Το υπερσύγχρονο Κέντρο Επιχειρήσεων SOC του εθνικού CSIRT-CY ενσωματώνει τεχνολογίες τελευταίας γενιάς, για την παρακολούθηση της κίνησης στο δίκτυο μέσω αισθητήρων και την ανίχνευση απειλών στις κρίσιμες υποδομές της Δημοκρατίας.

Η επίβλεψη και ανάλυση στον κυβερνοχώρο υποβοηθείται από 24 οθόνες υψηλής ευκρίνειας, σε διάταξη που προσφέρουν μια πανοραμική θέα του ψηφιακού χώρου υπό προστασία σε πραγματικό χρόνο. Οι αναλυτές του εθνικού CSIRT-CY παρακολουθούν την ψηφιακή δραστηριότητα, εντοπίζοντας έγκαιρα τις ανωμαλίες, ξεκινώντας άμεσα τις απαιτούμενες ενέργειες για την αντιμετώπισή τους.

3.8 Ομάδα Ανάπτυξης Λογισμικού CSIRT-CY

Η Ομάδα Ανάπτυξης Λογισμικού συστάθηκε τον Αύγουστο του 2023, με στόχο να καταστήσει την ΑΨΑ πιο αυτάρκη όσον αφορά την ανάπτυξη και συντήρηση τεχνολογικών λύσεων όπως ιστοσελίδες, διαδικτυακές εφαρμογές, εφαρμογές κινητού τηλεφώνου, συστήματα αυτοματοποίησης, εργαλεία τεχνητής νοημοσύνης και συστήματα συλλογής και διαχείρισης δεδομένων. Η Ομάδα ανήκει στο δυναμικό του Εθνικού CSIRT-CY και βρίσκεται υπό την καθοδήγηση και την εποπτεία του Προϊσταμένου του Εθνικού CSIRT-CY, όμως αναλαμβάνει έργα που αφορούν την κάλυψη των ευρύτερων αναγκών της Αρχής. Η Ομάδα αποτελείται από δύο Μηχανικούς Ψηφιακής Ασφάλειας με ακαδημαϊκή και εργασιακή εμπειρία στους τομείς της πληροφορικής, της μηχανικής λογισμικού, του ψηφιακού μετασχηματισμού και της τεχνητής νοημοσύνης.

Τα καθήκοντα της ομάδας περιλαμβάνουν μεταξύ άλλων:

- Την εκπόνηση έργων ανάπτυξης λογισμικού για την κάλυψη των αναγκών της ΑΨΑ.
- Την αξιολόγηση και παροχή εισηγήσεων σχετικά με συγκεκριμένα εργαλεία λογισμικού, συστήματα και πλατφόρμες που διαθέτει η ΑΨΑ.
- Την ανάλυση των απαιτήσεων και καταγραφή των τεχνικών προδιαγραφών για έργα ανάπτυξης λογισμικού που ανατίθενται σε εξωτερικούς συνεργάτες.
- Την παροχή εμπειρογνωμοσύνης για θέματα ανάλυσης συστημάτων και τεχνολογίας λογισμικού σε άλλες ομάδες του Εθνικού CSIRT-CY.

Από τη σύσταση της, η Ομάδα Ανάπτυξης Λογισμικού έχει προχωρήσει στην ανάλυση απαιτήσεων, ανάπτυξη, έλεγχο και συντήρηση των ακόλουθων έργων:

- Εργαλείο Διαχείρισης της Κατάστασης των Αισθητήρων του Εθνικού Κέντρου Επιχειρήσεων Ασφαλείας

- Εργαλείο Διαχείρισης Κακόβουλων Συνδέσμων
- Εργαλείο Διαχείρισης του Συστήματος του Εθνικού Κέντρου Επιχειρήσεων Ασφαλείας
- Εργαλείο Διασύνδεσης των Συστημάτων Διαχείρισης Περιστατικών της ΑΨΑ

Περαιτέρω, η Ομάδα Ανάπτυξης Λογισμικού έχει ασχοληθεί με την ανάλυση των απαιτήσεων και τον καθορισμό των προδιαγραφών για την πλατφόρμα διαχείρισης της Κοινότητας του Εθνικού Κέντρου Συντονισμού Κυβερνοασφάλειας (NCC-CY).

Πέραν από τη συντήρηση και αναβάθμιση των υφιστάμενων εργαλείων, εντός του 2024 η Ομάδα θα ασχοληθεί και με νέα έργα ανάπτυξης λογισμικού όπως για παράδειγμα:

- Εργαλείο μέσω του οποίου οι πολίτες θα μπορούν να υποβάλουν δυνητικά κακόβουλους συνδέσμους (URLs), έτσι ώστε αυτοί να τύχουν ανάλυσης σε πραγματικό χρόνο από τους αναλυτές του Εθνικού Κέντρου Επιχειρήσεων Ασφαλείας.
- Ολοκληρωμένη πλατφόρμα για τη διαχείριση της διαδικασίας των ελέγχων (audits) που θα διενεργεί η ΑΨΑ στις Κρίσιμες Υποδομές.

4. ΠΙΣΤΟΠΟΙΗΣΕΙΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

4.1 Ο Κανονισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια

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) / Information and Communication Technologies (ICT). Ο Κανονισμός αυτός θεσμοθετεί το Ευρωπαϊκό Πλαίσιο Πιστοποίησης Κυβερνοασφάλειας, το οποίο θεσπίστηκε με στόχο την αναβάθμιση του επιπέδου κυβερνοασφάλειας εντός της Ένωσης και την εναρμονισμένη προσέγγιση των ευρωπαϊκών σχημάτων πιστοποίησης κυβερνοασφάλειας, με απώτερο στόχο τη δημιουργία ψηφιακής ενιαίας αγοράς για ΤΠΕ.

Η πιστοποίηση των προϊόντων, υπηρεσιών και διαδικασιών που πιστοποιούνται βάσει των Ευρωπαϊκών Σχημάτων Πιστοποίησης Κυβερνοασφάλειας, αναγνωρίζονται επίσημα σε ολόκληρη την Ένωση. Αυτή η προσέγγιση θα διευκολύνει τις διασυνοριακές συναλλαγές των επιχειρήσεων και των αγοραστών, ώστε να κατανοούν καλύτερα τα χαρακτηριστικά ασφαλείας του προϊόντος ή της υπηρεσίας που αγοράζουν. Το πρώτο σχήμα πιστοποίησης που θα ληφθεί υπόψη για χρήση στην αξιολόγηση προϊόντων και υπηρεσιών είναι βασισμένο σε Κοινά Κριτήρια (Common Criteria - EUCC)[7] το οποίο αναμένεται να εκδοθεί αρχές του 2024. Τα επόμενα σχήματα που θα εκδοθούν θα σχετίζονται με υπηρεσίες νεφοϋπολογιστικής (Cloud Services), καθώς και τον εξοπλισμό και την υποδομή του δικτύου ηλεκτρονικών επικοινωνιών πέμπτης γενεάς (5G).

Βάσει του Κανονισμού (ΕΕ) 2019/881 η Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας είναι αρμόδια για την εποπτεία και εφαρμογή των κανόνων που συγκαταλέγονται σε ευρωπαϊκά σχήματα πιστοποίησης κυβερνοασφάλειας στην επικράτειά της. Επίσης, είναι αρμόδια για την εξουσιοδότηση των Οργανισμών Αξιολόγησης Συμμόρφωσης (Conformity Assessment Body – CAB) για ορισμένα επίπεδα πιστοποιήσεων, και ηγείται των δραστηριοτήτων πιστοποίησης κυβερνοασφάλειας του εκάστοτε κράτους-μέλους.

4.2 Εθνικό Πλαίσιο και Δραστηριότητες

Η ΑΨΑ, ως η αρμόδια Εθνική Αρχή Πιστοποιήσεων Κυβερνοασφάλειας (ΕΑΠΚ), έχοντας τις κατάλληλες εξουσίες και αρμοδιότητες, έχει ως στόχο να προωθήσει την εφαρμογή του πλαισίου πιστοποίησης κυβερνοασφάλειας στην Κύπρο.

Κύριο μέλημα της ΕΑΠΚ είναι να προαγάγει τον θεσμό της πιστοποίησης κυβερνοασφάλειας, με στόχο να αναπτύξει αλλά και να εμβαθύνει τις σχετικές ικανότητες της Κυπριακής Δημοκρατίας στον ευρύτερο τομέα της πιστοποίησης κυβερνοασφάλειας, με αποτέλεσμα η Κύπρος να καταστεί περιφερειακό κέντρο υπηρεσιών κυβερνοασφάλειας και να επωφεληθεί των πλεονεκτημάτων που θα ακολουθήσουν.

Ο ρόλος της ΑΨΑ είναι ζωτικής σημασίας, καθώς θα διαθέτει την αρμοδιότητα να επιβλέπει ολόκληρο το πλαίσιο πιστοποίησης στην Κύπρο και να παρακολουθεί την εφαρμογή του. Η ΑΨΑ θα παρέχει υποστήριξη και βοήθεια στο έργο του Κυπριακού Οργανισμού Προώθησης Ποιότητας (ΚΟΠΠ), ο οποίος είναι υπεύθυνος για τη διαπίστευση φορέων διασφάλισης ποιότητας στην Κύπρο και θα λειτουργεί ως Εθνικός Οργανισμός Διαπίστευσης.

[7] *Common Criteria: αποτελούν πλαίσιο μέσω του οποίου προδιαγράφονται οι απαιτήσεις σχετικά με τη λειτουργία και την επιβεβαίωση της ασφάλειας πληροφοριακών συστημάτων. Βάσει των προδιαγραφών αυτών, κατασκευαστές σχετικών προϊόντων μπορούν να διασφαλίσουν ότι τα προϊόντα τους ανταποκρίνονται στις σχετικές απαιτήσεις, με τα προϊόντα να ελέγχονται από διαπιστευμένα τεχνικά εργαστήρια για να εξακριβωθεί κατά πόσο πληρούν τις εν λόγω απαιτήσεις.*

5. ΕΝΙΣΧΥΣΗ ΚΑΙ ΑΝΑΠΤΥΞΗ ΙΚΑΝΟΤΗΤΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΚΥΠΡΙΑΚΗ ΑΓΟΡΑ

5.1 Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY)

Το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας της Κύπρου (National Coordination Center - NCC-CY), μέσω του Ευρωπαϊκού Έργου N4CY που αφορά την ίδρυση και τη λειτουργία του, και που συγχρηματοδοτείται από το πρόγραμμα «Ψηφιακή Ευρώπη» και την Κυπριακή Δημοκρατία, ξεκίνησε τη δράση του τον Ιανουάριο του 2023 και έκτοτε έχει δρομολογήσει αρκετές και πολυδιάστατες δράσεις για την ενίσχυση της κυβερνοασφάλειας. Το NCC-CY στηρίζει και συμμετέχει ενεργά στις εργασίες του Ευρωπαϊκού Κέντρου Αρμοδιότητας Κυβερνοασφάλειας (ECCC) καθώς είναι μέλος και συμμετέχει και στις 7 ομάδες εργασίας του. Εντός του έτους 2023, συμμετείχε σε πολυάριθμες συναντήσεις, τόσο των ομάδων εργασίας, τις συναντήσεις του Governing Board του ECCC, αλλά και των εκδηλώσεων δικτύωσης όλων των NCCs.

Πέραν της στήριξης προς το ECCC κατά το έτος 2023 σημειώθηκαν, μεταξύ άλλων, οι πιο κάτω κύριες δράσεις:

5.2 Δημιουργία Κοινότητας Κυβερνοασφάλειας

Η δημιουργία της Κοινότητας Κυβερνοασφάλειας ξεκίνησε τον Δεκέμβριο του 2023 με την εγγραφή διαφόρων οντοτήτων σε αυτήν. Ο σκοπός της Κοινότητας είναι να συγκεντρώσει όλα τα ενδιαφερόμενα μέρη από τον ιδιωτικό τομέα, τον ακαδημαϊκό χώρο και την έρευνα που έχουν εμπειρία στον τομέα της Κυβερνοασφάλειας ούτως ώστε να ενθαρρύνει την ενεργό συμμετοχή και συνεισφορά σε ερευνητικά και εκπαιδευτικά προγράμματα με απώτερο στόχο τη διευκόλυνση της διάδοσης πληροφοριών, ικανοτήτων και δεξιοτήτων μεταξύ των μελών της. Για σκοπούς καλύτερης οργάνωσης και διαχείρισης των μελών της Κοινότητας, το NCC-CY ξεκίνησε την διαδικασία ανάπτυξης προηγμένης πλατφόρμας (OpenXeco), η οποία αναμένεται να ολοκληρωθεί περί τα μέσα του 2024.

5.3 Σχέδιο Χορηγιών - Ενίσχυση Κυβερνοασφάλειας στις Κυπριακές Μικρομεσαίες Επιχειρήσεις 2023

Κατά το έτος 2023 ανακοινώθηκε, σε συνεργασία με το ΙΔΕΚ, το πρώτο πιλοτικό εθνικό σχέδιο χορηγιών για στήριξη των μικρομεσαίων επιχειρήσεων του τόπου, με συνολικό προϋπολογισμό 1.000.000 ΕΥΡΩ. Η ένταση ενίσχυσης της χορηγίας ήταν στο 60%, με ελάχιστη χρηματοδότηση τις 20.000 ΕΥΡΩ και μέγιστη τις 60.000 ΕΥΡΩ. Η πρόσκληση για υποβολή προτάσεων άνοιξε στις 8 Δεκεμβρίου 2023 και συγχρηματοδοτήθηκε από την Κυπριακή Δημοκρατία και το Πρόγραμμα «Ψηφιακή Ευρώπη» της Ευρωπαϊκής Ένωσης στο πλαίσιο υλοποίησης του Ευρωπαϊκού Έργου «N4CY – Development of the National Cybersecurity Coordination Centre of the Republic of Cyprus.

5.4 Ανάπτυξη Πιστοποίησης μέσω της δημιουργίας του «Πλαισίου Κυβερνο-υγιεινής για ΜμΕ»

Αναγνωρίζοντας ότι το 99% του συνόλου των επιχειρήσεων της Κύπρου εμπίπτουν στην κατηγορία «μικρομεσαία επιχείρηση» και σε συνάρτηση με τις τεράστιες επιπτώσεις που μπορούν να επιφέρουν οι κυβερνοεπιθέσεις σε αυτή την κατηγορία των επιχειρήσεων, το NCC-CY δημιούργησε το πλαίσιο Κυβερνο-Υγιεινής. Το πλαίσιο αυτό αποτελεί ένα σύστημα πιστοποίησης το οποίο περιλαμβάνει 11 (έντεκα) σημεία ελέγχου που με την εφαρμογή τους μια επιχείρηση διασφαλίζει ένα βασικό τουλάχιστον επίπεδο κυβερνοασφάλειας. Το πλαίσιο κυβερνο-υγιεινής είναι αναπόσπαστο κομμάτι του σχεδίου

χορηγιών, που συνεπάγεται ότι μια εταιρεία για να λάβει τη σχετική χρηματοδότηση, θα πρέπει να πιστοποιηθεί με το συγκεκριμένο σχήμα πιστοποίησης, αφού περάσει τον έλεγχο/επιθεώρηση από εγκεκριμένο φορέα πιστοποίησης. Ανεξάρτητα, όμως, το Πλαίσιο Κυβερνο-υγιεινής είναι διαθέσιμο στην ιστοσελίδα του NCC-CY και μπορεί να χρησιμοποιηθεί από οποιονδήποτε σαν βέλτιστη πρακτική.

5.5 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Η ΑΨΑ πραγματοποίησε σεμινάρια, εκπαιδεύσεις και εκδηλώσεις προς τρίτους με σκοπό την ευαισθητοποίηση και την εκπαίδευσή τους σε θέματα κυβερνοασφάλειας (βλ Ενότητα 8). Παράλληλα, η ΑΨΑ μέσω του διαδικτύου και συγκεκριμένα των ιστοσελίδων (www.dsa.cy και www.ncc.cy) και των Μέσων Κοινωνικής Δικτύωσης παρέχουν συμβουλές και ενημερώσεις για ο,τιδήποτε αφορά την κυβερνοασφάλεια τόσο σε τοπικό όσο και σε Ευρωπαϊκό επίπεδο.

5.6 Ακαδημία Τεχνολογίας Πληροφοριών, Επικοινωνιών & Κυβερνοασφάλειας (ICT)

Με την ίδρυση της Ακαδημίας Τεχνολογίας Πληροφοριών, Επικοινωνιών & Κυβερνοασφάλειας (ICT Academy), η ΑΨΑ στοχεύει στη διοργάνωση εγχώριων και διεθνών σεμιναρίων και συνεδρίων κατάρτισης και εκπαίδευσης, τόσο του προσωπικού της όσο και προσωπικού άλλων αρμοδίων αρχών, κρίσιμων υποδομών πληροφοριών της Δημοκρατίας, καθώς επίσης και εκδηλώσεων ενημέρωσης και δικτύωσης. Η Ακαδημία, η οποία λειτούργησε το Δεκέμβριο του 2023, έχει όραμα να καταστεί ένα αυτοσυντηρούμενο Περιφερειακό Κέντρο Εκπαίδευσης επαγγελματιών στον τομέα του ICT. Επιπρόσθετα, βασικός σκοπός της Ακαδημίας είναι να βοηθήσει στη στελέχωση θέσεων στην αγορά εργασίας, μέσω της επανειδίκευσης ή της αναβάθμισης δεξιοτήτων επαγγελματιών. Η μεγάλη ανάγκη σε προγράμματα επανειδίκευσης και αναβάθμισης δεξιοτήτων προκύπτει λόγω σημαντικών ελλείψεων ανθρώπινου δυναμικού στον κλάδο της Τεχνολογίας Πληροφοριών, Επικοινωνιών και Κυβερνοασφάλειας (ICT) στην αγορά εργασίας.

Εκτός από την τεχνική εκπαίδευση, η Ακαδημία θα δίνει έμφαση στην ευαισθητοποίηση του κοινού και των επιχειρήσεων για τους κινδύνους που ενέχει η ψηφιακή εποχή, σε συνεργασία με άλλους κρατικούς και ιδιωτικούς φορείς, συμπεριλαμβανομένου του Πανεπιστημιακού κλάδου.

6. ΥΛΟΠΟΙΗΣΗ ΣΤΡΑΤΗΓΙΚΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

6.1 Εισαγωγή και Διακυβέρνηση

Η Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας αποτελεί το κύριο εργαλείο για την αναγνώριση, την καταγραφή, τον προγραμματισμό και την παρακολούθηση σημαντικών δράσεων σε Εθνικό επίπεδο. Στόχος είναι η σημαντική βελτίωση των επιπέδων κυβερνοασφάλειας στη χώρα, καλύπτοντας τους πυλώνες της ασφάλειας δικτύων και πληροφοριών, του κυβερνοεγκλήματος, της κυβερνοάμυνας και των σχετικών εξωτερικών σχέσεων.

Η πρώτη Στρατηγική αναπτύχθηκε από το ΓΕΡΗΕΤ και τέθηκε σε εφαρμογή το 2013, με σχετική έγκριση από το Υπουργικό Συμβούλιο, και αποτέλεσε τα πρώτα συντονισμένα βήματα της Κυπριακής Δημοκρατίας στον τομέα της κυβερνοασφάλειας. Το Δεκέμβριο του 2020, έπειτα από αξιολόγηση ωριμότητας σε εθνικό επίπεδο που διενεργήθηκε από το Πανεπιστήμιο της Οξφόρδης το 2017, καθώς και αλλαγές στην σχετική Ευρωπαϊκή Στρατηγική και την συσσωρευμένη εμπειρία από την υλοποίησή της, εκδόθηκε η αναθεωρημένη Στρατηγική Κυβερνοασφάλειας της ΚΔ.

Κατά το έτος 2023, συνεχίστηκαν οι εργασίες για την υλοποίηση της Στρατηγικής με χρονικό ορίζοντα ολοκλήρωσης μέχρι το τέλος του 2024. Οι σχετικές εργασίες περιγράφονται στις υπόλοιπες υποενότητες.

6.2 Υλοποίηση Δράσεων Στρατηγικής Κυβερνοασφάλειας

6.2.1 Νομικό, Ρυθμιστικό και Πολιτικό Πλαίσιο

Η παρούσα Θεματική Ενότητα αποσκοπεί στην πλήρη υλοποίηση των προνοιών του ρυθμιστικού πλαισίου του Νόμου 89(Ι)/2020, αλλά και στην ενίσχυση του υφιστάμενου νομικού, κανονιστικού και ρυθμιστικού πλαισίου για την πλήρη ενεργοποίηση και υποστήριξη των προνοιών της Στρατηγικής Κυβερνοασφάλειας, με την ανάπτυξη νέων νομοθεσιών (περιλαμβανομένων και των δευτερογενών), όπου απαιτείται, για συνεχόμενη βελτίωση των επιπέδων κυβερνοασφάλειας στην Κυπριακή Δημοκρατία. Με σκοπό την εναρμόνιση της Οδηγίας (ΕΕ) 2022/2555 («Οδηγία NIS2») στην εθνική νομοθεσία, η ΑΨΑ ετοίμασε τροποποιητικό νομοσχέδιο σχετικά με την εν λόγω εναρμόνιση. Ταυτόχρονα, με τη νέα οδηγία η ΑΨΑ αναλαμβάνει επιπρόσθετους ρόλους και αρμοδιότητες.

6.2.2 Εθνικό Πλαίσιο Κυβερνοασφάλειας

Η παρούσα Θεματική Ενότητα προσβλέπει στην περαιτέρω ανάπτυξη και εδραίωση ενός ολοκληρωμένου Εθνικού Πλαισίου Κυβερνοασφάλειας, το οποίο τέθηκε σε εφαρμογή από το 2020. Εντός του 2023, ολοκληρώθηκε η ανάπτυξη του Μοντέλου Ωριμότητας Κυβερνοασφάλειας (Cybersecurity Maturity Model). Το Μοντέλο, το οποίο είναι δομημένο πάνω στις απαιτήσεις της Απόφασης Κ.Δ.Π 389/2020, θα μπορεί να χρησιμοποιηθεί από τους Φορείς για να επιμετρούν το επίπεδο ωριμότητας και συμμόρφωσης τους με τις πρόνοιες της δευτερογενούς νομοθεσίας που αφορά τα μέτρα ασφάλειας, και επιπρόσθετα θα αποτελέσει το εργαλείο ελέγχου και αξιολόγησης από μέρους των εξωτερικών ελεγκτών των εποπτευόμενων Φορέων.

Επίσης, στο πλαίσιο των εργασιών του Εθνικού Κέντρου Συντονισμού Κυβερνοασφάλειας, το Εθνικό Πλαίσιο Κυβερνοασφάλειας έχει πλέον εμπλουτιστεί με τη δημιουργία πλαισίου και σχήματος πιστοποίησης κυβερνο-υγιεινής για τις μικρομεσαίες επιχειρήσεις.

Για περισσότερες πληροφορίες για το μοντέλο ωριμότητας κυβερνοασφάλειας και το πλαίσιο κυβερνο-υγιεινής, βλ. ενότητες 2.3 και 5.4 αντίστοιχα.

Τέλος, εντός του έτους 2023, η ΑΨΑ, μέσω της δημιουργίας μιας ολοκληρωμένης εργαλειοθήκης με πρότυπα πολιτικών/διαδικασιών, επιδιώκει να ενισχύσει τις κρίσιμες υποδομές της Κυπριακής Δημοκρατίας σε σχέση με την κυβερνοασφάλεια προσφέροντας καθοδήγηση για συμμόρφωση με τις απαιτήσεις και τις υποχρεώσεις της Απόφασης Κ.Δ.Π 389/2020 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών.

6.2.3 Αντιμετώπιση Συμβάντων και Διαχείριση Κρίσεων

Η παρούσα Θεματική Ενότητα προσβλέπει στην οικοδόμηση ενός ανθεκτικού και ουσιαστικού οικοσυστήματος διαχείρισης κρίσεων στον κυβερνοχώρο σε εθνικό επίπεδο, καθώς και συμβολή στις σχετικές εργασίες σε ευρωπαϊκό επίπεδο. Μέσα από αυτό το πλαίσιο εγκαθιδρύθηκε η απρόσκοπτη εποπτεία και παρακολούθηση σε εικοσιτετράωρη βάση της Εθνικής Ομάδας Αντιμετώπισης Συμβάντων της Ασφάλειας Υπολογιστών (CSIRT-CY) για τους κρίσιμους φορείς της Κυπριακής Δημοκρατίας. Επίσης, θεσπίστηκε ο θεσμός της επιφυλακής, με σκοπό την άμεση ανταπόκριση σε περίπτωση περιστατικού, μειώνοντας το χρόνο ανταπόκρισης σε κυβερνοεπιθέσεις και αυξάνοντας την ανθεκτικότητα των κρίσιμων φορέων.

Το 2023, το Εθνικό CSIRT κλήθηκε να διαχειριστεί και να διερευνήσει 2 (δύο) επιθέσεις που πραγματοποιήθηκαν σε κρίσιμες υποδομές. Βοήθησε στη διαχείριση και αντιμετώπιση των περιστατικών και κατέληξε στον τύπο του κακόβουλου λογισμικού που χρησιμοποιήθηκε. Με το τέλος των περιστατικών, το Εθνικό CSIRT πρότεινε μέτρα μετριασμού και εισηγήσεις για βελτίωση της ασφάλειας των συστημάτων των κρίσιμων υποδομών. Η ΑΨΑ ενεργοποίησε άμεσα τον μηχανισμό υποστήριξης του ENISA (Support Action) και στις 2 (δύο) περιπτώσεις, με σκοπό την καλύτερη δυνατή αντιμετώπιση των περιστατικών.

6.2.4 Ανάπτυξη Δυνατοτήτων – Διοργάνωση και Συμμετοχή σε Ασκήσεις

Η παρούσα Θεματική Ενότητα επιδιώκει την ανάπτυξη και προώθηση μέτρων, προγραμμάτων και δραστηριοτήτων για την ανάπτυξη πραγματικών ικανοτήτων κυβερνοασφάλειας στους οργανισμούς που διαχειρίζονται κρίσιμες υποδομές πληροφοριών, καθώς και σε άλλους οργανισμούς και εταιρείες, όπου κρίνεται αναγκαίο. Επίσης, στοχεύει στη διασφάλιση ελάχιστου επιπέδου γνώσεων και δυνατοτήτων αντιμετώπισης των προκλήσεων στον κυβερνοχώρο.

Κατά το έτος 2023 πραγματοποιήθηκαν εκπαιδεύσεις με θέμα την ευαισθητοποίηση (awareness) και εκπαίδευση κρίσιμων υποδομών πληροφοριών στον τομέα της κυβερνοασφάλειας. Επίσης, διοργανώθηκαν τακτικές εθνικές ασκήσεις στη βάση ρεαλιστικών σεναρίων, με ταυτόχρονη ενεργή συμμετοχή σε Πανευρωπαϊκές και άλλες διεθνείς ασκήσεις (βλ. Ενότητα 8).

6.2.5 Ενημέρωση – Δημιουργία Κουλτούρας Ασφάλειας

Η παρούσα Θεματική Ενότητα έχει ως στόχο την προώθηση της επίγνωσης και της κουλτούρας ασφάλειας σε όλους τους χρήστες των συστημάτων επικοινωνίας, πληροφοριών και υπηρεσιών διαδικτύου στην Κύπρο. Οι δράσεις περιλαμβάνουν ενημερώσεις και σεμινάρια για ευαισθητοποίηση μεγάλου εύρους χρηστών αυτών των συστημάτων και υπηρεσιών, προκειμένου να επιτευχθεί ένα ικανοποιητικό επίπεδο ενημέρωσης και επιμόρφωσης που αφορά πιθανές απειλές κυβερνοασφάλειας.

Η ΑΨΑ κατά το έτος 2023 έχει πραγματοποιήσει μεγάλο αριθμό εκπαιδεύσεων και ενημερωτικών ημερίδων σχετικά με την ανάπτυξη των δεξιοτήτων και επίγνωση στα θέματα κυβερνοασφάλειας, ως περιγράφονται πιο πάνω. Απώτερος στόχος των εκπαιδεύσεων ήταν η προώθηση της ανάπτυξης «κουλτούρας ασφάλειας» σε όλα τα κυβερνητικά τμήματα και υπηρεσίες του κράτους, καθώς και σε ιδιωτικές επιχειρήσεις (βλ. ενότητα 8). Επίσης, πραγματοποιήθηκε μεγάλος αριθμός δραστηριοτήτων επίγνωσης σε σχολεία σε όλη την επικράτεια της Κυπριακής Δημοκρατίας.

6.2.6 Εκπαίδευση και Κατάρτιση

Η παρούσα Θεματική Ενότητα έχει ως στόχο την ανάπτυξη εξειδικευμένου ανθρώπινου δυναμικού, ώστε να εφαρμόζει αποτελεσματικά τις πρόνοιες της Στρατηγικής, τόσο σε μεσοπρόθεσμο όσο και σε μακροπρόθεσμο ορίζοντα. Επιπλέον, στόχος είναι η ενσωμάτωση αυτών των γνώσεων στα Σχέδια Υπηρεσίας για σχετικές θέσεις εργασίας και η προώθηση ενεργειών για συνεχή εκπαίδευση και κατάρτιση του προσωπικού.

Η ΑΨΑ, κατά το έτος 2023, είχε ενεργό ρόλο στην υλοποίηση των δράσεων στα θέματα που αφορούν την κατάρτιση και πιστοποίηση. Σε συνεργασία με την Κυπριακή Ακαδημία Δημόσιας Διοίκησης (ΚΑΔΔ), στο πλαίσιο του Εθνικού Σχεδίου Δράσης για Ψηφιακές Δεξιότητες, 2021-2025 και της Εθνικής Στρατηγικής Κυβερνοασφάλειας και με το Υφυπουργείο Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής, άρχισε τον Οκτώβριο του 2023 μία σειρά εκπαιδευτικών εργαστηρίων με θέμα «Εκπαίδευση και ανάπτυξη κουλτούρας ηλεκτρονικής ασφάλειας/ κυβερνοασφάλειας».

Οι εν λόγω εκπαιδεύσεις αναμένεται να ολοκληρωθούν μέχρι τον Ιανουάριο του 2026 και διαχωρίζονται σε τρία μαθησιακά επίπεδα. Συνολικά θα διοργανωθούν μέχρι και 150 μονοήμερα εκπαιδευτικά προγράμματα, με δυνατότητα συμμετοχής περίπου 2500 λειτουργών της δημόσιας υπηρεσίας, σύμφωνα με τις ανάγκες μάθησης που έχουν καταγραφεί σε βασικά και εξειδικευμένα επίπεδα.

6.2.7 Έρευνα και Καινοτομία

Η παρούσα Ενότητα επικεντρώνεται στην προώθηση και υποστήριξη της έρευνας και καινοτομίας στον τομέα της κυβερνοασφάλειας στην Κυπριακή Δημοκρατία.

Εντός του έτους 2023, η ΑΨΑ και το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY) διοργάνωσε ημερίδες με σκοπό να προβάλει και να ενθαρρύνει τους ενδιαφερόμενους για συμμετοχή σε νέα προγράμματα «Digital Europe» και «Horizon Europe». Επιπρόσθετα, και μέσα από την συμβολή του NCC-CY στην ομάδα εργασίας «Strategic Agenda», συμβάλλει στη διαμόρφωση της πολιτικής της Ευρώπης για τα μελλοντικά προγράμματα που θα εξαγγελθούν. Παράλληλα και μέσα από τη δημιουργία της Κοινότητας Κυβερνοασφάλειας του Εθνικού Κέντρου Συντονισμού Κυβερνοασφάλειας, δημιουργήθηκε επιτροπή με μέλη αντιπροσώπους των Κυπριακών Πανεπιστημίων, στα πλαίσια της οποίας συζητούνται και ανταλλάσσονται απόψεις (μεταξύ άλλων) για ανάπτυξη της Έρευνας και της Καινοτομίας.

6.2.8 Ασφάλεια για Όλους

Η παρούσα Θεματική Ενότητα περιλαμβάνει τη στήριξη των μικρομεσαίων επιχειρήσεων και των απλών πολιτών της χώρας μέσω σημαντικών δράσεων για την ασφάλεια του Διαδικτύου των Πραγμάτων (Internet of Things), καθώς και την εφαρμογή κατάλληλων μέτρων για την πιστοποίηση της κυβερνοασφάλειας σε προϊόντα και υπηρεσίες που έχουν ευρεία χρήση.

Όσον αφορά την έκδοση των πρώτων Ευρωπαϊκών σχημάτων πιστοποίησης παρατηρήθηκε μια καθυστέρηση και αναμένεται ότι κατά τις αρχές του 2024 θα εκδοθεί το σχήμα για τα Κοινά Κριτήρια (EUCC), ενώ περί τα τέλη του ίδιου χρόνου το σχήμα για τις υπηρεσίες νεφοϋπολογιστικής (EUCS). Σκοπός των σχημάτων είναι να διασφαλίζεται η ορθή λειτουργία της εσωτερικής αγοράς, σε συνδυασμό με την επίτευξη ενός υψηλού επιπέδου κυβερνοασφάλειας, κυβερνοανθεκτικότητας και κυβερνοεμπιστοσύνης εντός της ΕΕ.

Επιπρόσθετα, η ΑΨΑ ολοκλήρωσε με επιτυχία το έργο CEF A4CEF - Advancing Cybersecurity Certification Capabilities with Cross-border exchange and Enhancing (business) Flows (βλ. Ενότητα 9.1.7) που είχε σαν στόχο την επέκταση των δραστηριοτήτων της ΑΨΑ στον τομέα πιστοποιήσεων κυβερνοασφάλειας και κατά συνέπεια την προώθηση ασφαλέστερων προϊόντων, υπηρεσιών και διαδικασιών μέσω της απόκτησης πιστοποιητικών.

6.2.9 Διεθνής Συνεργασία

Η παρούσα Θεματική Ενότητα στοχεύει στην επίτευξη μιας αποτελεσματικής συνεργασίας μεταξύ της Κυπριακής Δημοκρατίας, των άλλων κρατών μελών της Ευρωπαϊκής Ένωσης, καθώς και τρίτων χωρών στα θέματα κυβερνοασφάλειας. Αυτό επιτυγχάνεται μέσω της εκπροσώπησης της Κυπριακής Δημοκρατίας και της ενεργού συμμετοχής της σε σχετικές ομάδες εργασίας. Επιπλέον, αποσκοπεί στον καθορισμό μακροπρόθεσμων στόχων για τη διεθνή συνεργασία, αναπτύσσοντας συνεργασίες με τις αρμόδιες αρχές και οργανισμούς σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο.

Η ΑΨΑ, διατηρεί ενεργή συμμετοχή σε μεγάλο αριθμό ομάδων εργασίας σε Ευρωπαϊκό και Διεθνές επίπεδο, όπως καταγράφεται λεπτομερώς στην ενότητα 7.

7. ΕΘΝΙΚΕΣ ΚΑΙ ΔΙΕΘΝΕΙΣ ΣΧΕΣΕΙΣ

7.1 Συνεργασία με Κρατικές Αρχές

Η ΑΨΑ συνάπτει Μνημόνια Συνεργασίας με φορείς που διέπονται από το Νόμο 89(Ι)/2020 ή άλλες Αρχές ή οργανισμούς ή εταιρείες με τις οποίες συνεργάζεται. Πρωταρχικός στόχος της σύναψης των Μνημονίων είναι η θεσμοθέτηση της συνεργασίας μεταξύ των συμμετεχόντων, κυρίως για την προώθηση των θεμάτων κυβερνοασφάλειας και την ενίσχυση του επιπέδου κυβερνοασφάλειας στην Κυπριακή Δημοκρατία. Το πλαίσιο συνεργασίας και οι σχετικές δράσεις επικεντρώνονται στους ακόλουθους τομείς:

- Ανταλλαγή πληροφοριών
- Επιχειρησιακή συνεργασία
- Εκπαίδευση και κατάρτιση
- Εφαρμογή σχεδίων διαχείρισης κρίσεων
- Τεχνική υποστήριξη

Ο πιο κάτω πίνακας παραθέτει τα Μνημόνια Συνεργασίας της ΑΨΑ με συνεργάτες εντός της Κυπριακής Δημοκρατίας κατά το 2023.

Πίνακας 1: Μνημόνια Συνεργασίας μεταξύ της ΑΨΑ και συνεργατών της Κυπριακής Δημοκρατίας(ΜμΕ)
Ανοικτό Πανεπιστήμιο Κύπρου
Κυπριακός Οργανισμός Τυποποίησης (CYS)
Κεντρική Τράπεζα Κύπρου
Υφυπουργείο Ναυτιλίας
Κυπριακός Σύνδεσμος Πληροφορικής -Cyprus Computer Society
Ίδρυμα Έρευνας και Καινοτομίας (ΙΔΕΚ)
Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως και Αστυνομία Κύπρου
Επίτροπος Ισότητας των Φύλων

7.2 Χώρες της Ευρωπαϊκής Ένωσης και Τρίτες Χώρες

Εντός του έτους 2023 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.

7.3 Διεθνής Εκπροσώπηση

Κατά το έτος 2023, η ΑΨΑ εκπροσωπήθηκε σε επιτροπές εθνικού και διεθνούς επιπέδου από τον Επίτροπο, τον Βοηθό Επίτροπο, τον Διευθυντή και στελέχη της ΑΨΑ, ανάλογα με το αντικείμενο της κάθε επιτροπής και το απαιτούμενο επίπεδο εκπροσώπησης. Οι συμμετοχές αποτελούν μέρος της άσκησης των δραστηριοτήτων της ΑΨΑ σε διεθνές επίπεδο. Οι διεθνείς οργανισμοί και επιτροπές στις οποίες η ΑΨΑ συμμετείχε είναι:

Πίνακας 2: Διεθνείς οργανισμοί και Επιτροπές που συμμετέχει η ΑΨΑ
ENISA (European Union Agency for Cybersecurity)
ECASEC (European Competent Authorities for the Security of Electronic Communications)
NIS Cooperation Group and relevant Work Streams
Συμβούλιο της Ευρωπαϊκής Ένωσης (συμβολή σε συζητήσεις και διαμόρφωση της οδηγίας NIS2)
CyCLONe (Cyber Crisis Liaison Officers Network)
ECCG (European Cybersecurity Certification Group) and related sub-groups
OSCE (Organization for Security and Co-operation in Europe)
CSIRT Community Groups (FIRST, TI)
CSIRTs Network
ITU (International Telecommunications Union)
ECCC (European Cybersecurity Competence Centre)

7.4 Πρόγραμμα Δράσης Στήριξης του ENISA (CYBERSECURITY SUPPORT ACTION)

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.

Κατά το έτος 2023 η ΑΨΑ κατάφερε να εξαντλήσει όλο τον προϋπολογισμό που είχε διατεθεί σε σχετικό σχέδιο για την Κύπρο. Οι υποδομές στην Κύπρο επωφελήθηκαν με διάφορες υπηρεσίες όπως αξιολογήσεις κινδύνων, δοκιμές διείσδυσης, εκπαιδεύσεις, και άλλα. Συνολικά, έχουν επωφεληθεί από ENISA Support Action 37 κρίσιμες υποδομές της Κυπριακής Δημοκρατίας. Τριάντα μία (31) υποδομές από τον Δημόσιο τομέα, μία (1) από τον τομέα της Ενέργειας, μία (1) από τον τομέα των Τηλεπικοινωνιών, μία (1) από τον τομέα των Επικοινωνιών, μία (1) από τον τομέα της Υγείας και δύο (2) υποδομές στον Τραπεζικό τομέα.

8. ΣΥΝΕΔΡΙΑ, ΕΚΔΗΛΩΣΕΙΣ ΚΑΙ ΑΣΚΗΣΕΙΣΣΧΕΣΕΙΣ

Εντός του 2023 η ΑΨΑ διοργάνωσε και συμμετείχε σε διάφορες εκδηλώσεις για την προώθηση και διάδοση των βέλτιστων πρακτικών στον τομέα της κυβερνοασφάλειας. Αρκετές από τις εκδηλώσεις πραγματοποιήθηκαν υπό την αιγίδα της ΑΨΑ, με κύριους ομιλητές τον Επίτροπο Επικοινωνιών και τον Βοηθό Επίτροπο, με απώτερο σκοπό την προώθηση της κουλτούρας της κυβερνοασφάλειας.

8.1 Διοργάνωση Συνεδρίων, Εκδηλώσεων και Ασκήσεων από την ΑΨΑ

8.1.1 Εκπαιδευτικό Σεμινάριο «Διαχείριση κινδύνων ασφαλείας πληροφοριών στις Κρίσιμες Υποδομές»

Η ΑΨΑ διοργάνωσε διήμερο εκπαιδευτικό σεμινάριο με θέμα την «Διαχείριση κινδύνων ασφάλειας πληροφοριών στις Κρίσιμες Υποδομές». Στόχος του σεμιναρίου ήταν η αξιολόγηση των γνώσεων και δεξιοτήτων των κρίσιμων υποδομών, η αναγνώριση του περιβάλλοντος και των ιδιαίτερων συνθηκών του οργανισμού ή της υπηρεσίας τους, και ο σχεδιασμός ενός απλού και αποτελεσματικού πλαισίου διαχείρισης κινδύνων βάσει διεθνώς αναγνωρισμένων μεθοδολογιών διαχείρισης κινδύνων (π.χ ISO 31000:2018 και το ISO 27005:2018).

Σεμινάριο με Τίτλο : «Διαχείριση κινδύνων ασφάλειας πληροφοριών στις Κρίσιμες Υποδομές»

8.1.2 Εκπαιδευτικό Σεμινάριο «Πλαίσιο Μέτρων Ασφαλείας» προς ΦΚΥΠ και ΦΕΒΥ

Η ΑΨΑ οργάνωσε μονοήμερο εκπαιδευτικό σεμινάριο σχετικά με το Εθνικό Πλαίσιο Κυβερνοασφάλειας για τους εποπτευόμενους φορείς, σε μια προσπάθεια για συνεχόμενη ανάπτυξη ικανοτήτων και ενδυνάμωση της συνεργασίας της με τους Φορείς.

Το σεμινάριο παρείχε τη δυνατότητα στους συμμετέχοντες να αναγνωρίσουν και να κατανοήσουν τα μέτρα σχετικά με την ασφάλεια δικτύων και πληροφοριών που περιέχονται στο Πλαίσιο Μέτρων Ασφαλείας (Παράρτημα ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020) στο περιβάλλον και στις ιδιαίτερες συνθήκες του οργανισμού τους ή της υπηρεσίας τους, και να μπορέσουν να τα εφαρμόσουν αναλογικά με τις υποδομές τους.


Σεμινάριο με Τίτλο : «Πλαίσιο Μέτρων Ασφαλείας»

8.1.3 Εκπαιδευτικό Σεμινάριο «Επιχειρησιακή συνέχεια και Ανάκαμψη από Καταστροφές στις Κρίσιμες Υποδομές»

Η ΑΨΑ διοργάνωσε με επιτυχία διήμερο εκπαιδευτικό σεμινάριο με θέμα «Επιχειρησιακή Συνέχεια και Ανάκαμψη από Καταστροφές στις Κρίσιμες Υποδομές» σχετικά με τις απαιτήσεις των υφιστάμενων νόμων και αποφάσεων της ΑΨΑ για τον χειρισμό περιστατικών ασφάλειας πληροφοριών. Οι συμμετέχοντες δοκίμασαν τις γνώσεις τους στις αποφάσεις που καλούνται να λαμβάνουν στους οργανισμούς / υπηρεσίες τους, προκειμένου να προστατέψουν το οργανισμό τους από ένα καταστροφικό συμβάν.


Σεμινάριο με Τίτλο : «Επιχειρησιακή συνέχεια και Ανάκαμψη από Καταστροφές στις Κρίσιμες Υποδομές»

8.1.4 Εκπαιδευτικό Σεμινάριο για τις Προεδρικές Εκλογές 2023

Ενόψει των Προεδρικών εκλογών του 2023, η ΑΨΑ πραγματοποίησε διαδικτυακό σεμινάριο με θέμα την «Ενίσχυση επιπέδων ασφαλείας των συστημάτων» με στόχο την ευαισθητοποίηση και ενημέρωση του προσωπικού εκλογών, σχετικά με τις βέλτιστες πρακτικές για ασφαλέστερη πλοήγηση στο Διαδίκτυο, καθώς και τους αυξανόμενους κινδύνους στον κυβερνοχώρο κατά την διεξαγωγή των εκλογών.

8.1.5 Εκπαιδευτικά Σεμινάρια στον Οργανισμό Κρατικών Υπηρεσιών Υγείας (ΟΚΥπΥ)

Η ΑΨΑ πραγματοποίησε 28 σεμινάρια ενημέρωσης και ευαισθητοποίησης των εργαζομένων του ΟΚΥπΥ σχετικά με τις βέλτιστες πρακτικές για ασφαλέστερη πλοήγηση στο Διαδίκτυο, καθώς και τους αυξανόμενους κινδύνους στον κυβερνοχώρο.

8.1.6 1ο Συνέδριο «Γυναίκες στην κυβερνοασφάλεια: Προκλήσεις, Εμπειρίες και Σχέδια για το Μέλλον»

Η ΑΨΑ πραγματοποίησε το 1ο Συνέδριο με θέμα «Γυναίκες στην κυβερνοασφάλεια: Προκλήσεις, Εμπειρίες και Σχέδια για το Μέλλον».

Το συνέδριο απευθυνόταν σε γυναίκες που ασχολούνται με τον τομέα της Κυβερνοασφάλειαςκαι επικεντρώθηκε σε θέματα ανθρωπίνου δυναμικού, προκλήσεις που αντιμετωπίζουν οι γυναίκες στον κλάδο, δυσκολίες, ανέλιξη και σχέδια για το μέλλον.

Συνέδριο με Τίτλο : «Γυναίκες στην κυβερνοασφάλεια: Προκλήσεις, Εμπειρίες και Σχέδια για το Μέλλον»

8.1.7 Ευρωπαϊκός Μήνας Κυβερνοασφάλειας 2023 (European Cybersecurity Month - ECSM)

Η ΑΨΑ, στα πλαίσια των δραστηριοτήτων της για συνεχόμενη βελτίωση των επιπέδων κυβερνοασφάλειας στην Κυπριακή Δημοκρατία, συμμετείχε για ακόμη μια χρονιά στον Ευρωπαϊκό Μήνα Κυβερνοασφάλειας (ECSM) της Ευρωπαϊκής Ένωσης για την προώθηση της ασφάλειας στο διαδίκτυο.

Η εκστρατεία επικεντρώθηκε στην κοινωνική μηχανική (social engineering) και είχε ως στόχο να προσελκύσει την προσοχή των χρηστών όλων των ηλικιών στις διάφορες τεχνικές κοινωνικής μηχανικής που χρησιμοποιούν οι επιτιθέμενοι εναντίον τους και που θα τους βοηθούσε να είναι προσεκτικοί μέσα από διάφορες δραστηριότητες και πληροφορίες.

8.1.8 Ημερίδα Κυβερνοασφάλειας "EMERGING THREATS IN CYBERSPACE" σε συνεργασία με το ΥΠΑΜ και το Ανοικτό Πανεπιστήμιο

Η ΑΨΑ συνδιοργάνωσε με το Υπουργείου Άμυνας (ΥΠΑΜ) και το Ανοικτό Πανεπιστήμιο Κύπρου, επιμορφωτική Ημερίδα Κυβερνοασφάλειας στους χώρους του Υπουργείου Οικονομικών, με θέμα "Emerging Threats In Cyberspace" όπου συμμετείχαν στρατιωτικό προσωπικό της Εθνικής Φρουράς και του Υπουργείου Άμυνας.

Σκοπός της ημερίδας ήταν η ενημέρωση του προσωπικού για ενδεχόμενες απειλές που προέρχονται από την χρήση διαδικτύου, προκειμένου να λαμβάνουν τα απαραίτητα μέτρα για την προστασία τόσο των πληροφορίων που διαχειρίζονται όσο και των προσωπικών τους δεδομένων.

Ημερίδα με Τίτλο : "EMERGING THREATS IN CYBERSPACE

8.1.9 Εκπαιδευτικό Σεμινάριο για Παρουσίαση Εργαλειοθήκης για Καθοδήγηση και Βοήθημα σχετικά με Υποχρεώσεις Κρίσιμων Φορέων

Η ΑΨΑ, στις 6 Οκτωβρίου, διοργάνωσε εκπαιδευτικό σεμινάριο για την παρουσίαση εργαλειοθήκης (πρότυπα πολιτικών, μεθοδολογιών και εγγράφων) που αποτελούν καθοδήγηση και βοήθημα σχετικά με την υλοποίηση των υποχρεώσεων κρίσιμων φορέων. Η εργαλειοθήκη παρέχεται δωρεάν σε όλους τους κρίσιμους φορείς (και άλλα ενδιαφερόμενα μέρη), και το περιεχόμενο της θα πρέπει να προσαρμόζεται κατάλληλα από τους φορείς σε περίπτωση επιλογής χρήσης του.

Η εκδήλωση πραγματοποιήθηκε σε συνεργασία με την εταιρεία PwC στο "Experience Center".

Εκπαιδευτικό Σεμινάριο για Παρουσίαση Εργαλειοθήκης

8.1.10 Εκπαιδευτικό σεμινάριο στο Δημαρχείο Λευκωσίας

Στο πλαίσιο των εκπαιδεύσεών της, η ΑΨΑ οργάνωσε σεμινάριο για το Δημαρχείο Λευκωσίας, που είχε ως σκοπό την ενημέρωση του προσωπικού για τις ενδεχόμενες απειλές που προέρχονται από τη χρήση του διαδικτύου, προκειμένου να λαμβάνουν τα απαραίτητα μέτρα για την προστασία τόσο των πληροφοριών που διαχειρίζονται, όσο και των προσωπικών τους δεδομένων.

Εκπαιδευτικό σεμινάριο στο Δημαρχείο Λευκωσίας

8.1.11 Εκπαιδευτικό σεμινάριο στον Σύνδεσμο Εγκεκριμένων Λογιστών Κύπρου (ΣΕΛΚ)

Η ΑΨΑ διοργάνωσε επιμορφωτικό σεμινάριο για τον ΣΕΛΚ με θέμα «Αναγνώριση κινδύνων & Βέλτιστες πρακτικές για την ασφαλή χρήση του Διαδικτύου». Το σεμινάριο αφορούσε τεχνικές και τακτικές που χρησιμοποιούν τα κακόβουλα άτομα / ομάδες για να επιτεθούν με σκοπό να εξασφαλίσουν πρόσβαση σε πόρους όπου δεν έχουν δικαιώματα, να καταστρέψουν ευαίσθητες και σημαντικές πληροφορίες, να αποσπάσουν χρήματα από χρήστες ή να διακόψουν τη ροή εργασιών μιας επιχείρησης.

Εκπαιδευτικό σεμινάριο στον ΣΕΛΚ

8.1.12 Συνάντηση Ενδιαφερόμενων Μερών (Stakeholders meeting)

Στις 19 Δεκεμβρίου 2023, πραγματοποιήθηκε η ετήσια Συνάντηση των Ενδιαφερόμενων Μερών (Stakeholders Meeting) της ΑΨΑ, στους χώρους της νέας Ακαδημίας Τεχνολογίας, Πληροφορικής και Επικοινωνιών (ICT Academy). Στην εκδήλωση συμμετείχαν πέραν των 150 συνέδρων, στα πλαίσια της οποίας πραγματοποιήθηκαν παρουσιάσεις από τον Επίτροπο Επικοινωνιών και άλλους Κρατικούς Αξιωματούχους, εμπειρογνώμονες από τον ιδιωτικό τομέα, και αντιπροσώπους διεθνών Οργανισμών όπως τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA). Οι σύνεδροι είχαν την ευκαιρία μεταξύ άλλων να ενημερωθούν για τις τοπικές και διεθνείς εξελίξεις στην κυβερνοασφάλεια, αλλά και για τις προσπάθειες που καταβάλλει η ΑΨΑ για να ενισχύσει τον τομέα και την προστασία των κρίσιμων υποδομών του τόπου.

8.1.13 3+1 Cyber Security Working Group (CSWG) meeting

Στις 2 και 3 Μαΐου 2023, πραγματοποιήθηκε στο Εκπαιδευτικό Κέντρο CYCLOPS στην Λάρνακα, άσκηση Κυβερνοασφάλειας με τις Ομάδες Εργασίας για την Κυβερνοασφάλεια των χωρών Κύπρου, Ισραήλ, Ελλάδας και Αμερικής. Απώτερος στόχος ήταν η διερεύνηση για το πώς οι χώρες μπορούν να συνεργαστούν με στόχο την αντιμετώπιση κακόβουλων απειλών στον κυβερνοχώρο, τη διασφάλιση του θαλάσσιου κυβερνοχώρου και την οικοδόμηση ανθεκτικότητας στην περιοχή της Ανατολικής Μεσογείου. Επιπρόσθετα, παρουσιάστηκαν και συζητήθηκαν τα αποτελέσματα της μελέτης "Regional Approach to Maritime Cybersecurity Governance and Risk Management: The Eastern Mediterranean as a Model".

8.1.14 2023 Διαπεριφερειακή άσκηση της ITU Ευρώπης και Ασίας-Ειρηνικού στον κυβερνοχώρο (2023 Interregional Cyberdrill for Europe and Asia-Pacific)

Η ΑΨΑ σε συνεργασία με το Γραφείο Ανάπτυξης Τηλεπικοινωνιών (BDT) της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU) φιλοξένησε και είχε την ευθύνη για την ομαλή διεκπεραίωση του προγράμματος της διαπεριφερειακής άσκησης της ITU Ευρώπης και Ασίας-Ειρηνικού στον κυβερνοχώρο. Στο πλαίσιο της άσκησης πραγματοποιήθηκαν ομιλίες και συζητήσεις σε πάνελ που εξέτασαν ζητήματα όπως η κατάσταση της κυβερνοασφάλειας στις περιοχές Ασίας-Ειρηνικού και Ευρώπης, οι βέλτιστες πρακτικές για την προστασία υποδομών πληροφοριών ζωτικής σημασίας, το σχέδιο αντιμετώπισης κρίσεων στον κυβερνοχώρο σε εθνικό επίπεδο για την αντιμετώπιση νέων απειλών, καθώς και το ρόλο των συμπράξεων στην προώθηση της διπλωματίας στον κυβερνοχώρο.

Στόχος των ομιλιών και των συζητήσεων ήταν να παρέχουν μια σαφή εικόνα στους συμμετέχοντες για τον καίριο ρόλο των εταιρικών σχέσεων στην ενίσχυση της διπλωματίας στον κυβερνοχώρο και τη σημασία της συνεργασίας οργανισμών από διαφορετικούς τομείς για την αντιμετώπιση κρίσεων στον κυβερνοχώρο. Επίσης, παρουσιάστηκαν μελέτες περιπτώσεων (case-studies) από την Ευρώπη και την Ασία-Ειρηνικού, και αναλύθηκαν τα διαπεριφερειακά διδάγματα που αντλήθηκαν από αυτές.

2023 Διαπεριφερειακή άσκηση της ITU Ευρώπης και Ασίας-Ειρηνικού στον κυβερνοχώρο

8.2 Συμμετοχή ΑΨΑ σε Συνέδρια και Εκδηλώσεις

8.2.1 Εκπροσώπηση και συμμετοχή ΑΨΑ στο συνέδριο «2nd European Cybersecurity Skills Conference 2023»

Η ΑΨΑ συμμετείχε στο 2ο Ευρωπαϊκό Συνέδριο Δεξιοτήτων Κυβερνοασφάλειας του ENISA, το οποίο πραγματοποιήθηκε στην Ισπανία. Το συνέδριο επικεντρώθηκε στην πρόοδο και τις προκλήσεις της υιοθέτησης του Ευρωπαϊκού Πλαισίου Δεξιοτήτων Κυβερνοασφάλειας (ECSF) και τον ρόλο του ENISA όσον αφορά την Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας της ΕΕ.

Στόχος του ήταν να φέρει σε επαφή την κοινότητα των δεξιοτήτων κυβερνοασφάλειας, την ανταλλαγή εμπειριών και ορθών πρακτικών. Σε αυτό το πλαίσιο ο ENISA και οι συνδιοργανωτές προσκάλεσαν την ΑΨΑ σε ένα πάνελ συζήτησης με θέμα: “From Strategy to actions: National Policy Initiatives Endorsing the ECSF”.

2nd European Cybersecurity Skills Conference 2023

8.2.2 Συμμετοχή ΑΨΑ στην Διεθνή Έκθεση Βιβλίου Λεμεσού (Limassol International Book Fair)

Η ΑΨΑ συμμετείχε στη 2η Διεθνή Έκθεση Βιβλίου Λεμεσού (Limassol International Book Fair) η οποία πραγματοποιήθηκε στις 17- 19 Νοεμβρίου, στους Χαρουπόμυλους Λανίτη στη Λεμεσό. Στα πλαίσια των δραστηριοτήτων της για συνεχόμενη βελτίωση των επιπέδων κυβερνοασφάλειας στην Κυπριακή Δημοκρατία, η ΑΨΑ παρουσίασε την έκδοση Παιδικής Εικονογραφημένης ιστορίας για την Κυβερνοασφάλεια, όπως επίσης και τη διοργάνωση ενός διαδραστικού παιχνιδιού για παιδιά με γρίφους που αφορούσαν την κυβερνοασφάλεια. Η ΑΨΑ συμμετείχε στη Διεθνή Έκθεση με δικό της περίπτερο, στοχεύοντας στην ενημέρωση των επισκεπτών για την κυβερνοασφάλεια.

Διεθνής Έκθεση Βιβλίου Λεμεσού

9. ΣΥΜΜΕΤΟΧΗ ΣΕ ΕΥΡΩΠΑΪΚΑ ΣΥΓΧΡΗΜΑΤΟΔΟΤΟΥΜΕΝΑ ΠΡΟΓΡΑΜΜΑΤΑ

9.1 Τρέχοντα Έργα

9.1.1 Joint Cybersecurity Operations Platform (CEF-JCOP)

Το έργο Joint Cybersecurity Operations Platform (JCOP) αποσκοπεί στο σχεδιασμό και την ανάπτυξη μιας πλατφόρμας επιχειρησιακής ασφάλειας που προσαρμόζεται στις ανάγκες των κρατών μελών της ΕΕ. Η πρωτοβουλία περιλαμβάνει τρεις βασικούς τομείς δράσης: (1) Συλλογή & Ανάλυση πληροφοριών (Threat Intelligence), (2) Ανίχνευση & Ανταπόκριση σε κυβερνοεπιθέσεις (Alerting and Incident Response), (3) Υποστήριξη προγραμμάτων εκπαίδευσης στην κυβερνοασφάλεια (Cybersecurity Operations Training).

Το έργο άρχισε τον Αύγουστο του 2021 και θα ολοκληρωθεί τέλη Ιουλίου 2024. Το ποσό χρηματοδότησης του έργου ανέρχεται στα €200,625, ενώ ο συνολικός προϋπολογισμός φτάνει τα €267,500.

9.1.2 Power System's SHield against cOmplEx iNcI^{2}dents and eXtensive cyber and privacy attacks (PHOENi^{2}X Project)

Το έργο PHOENI2X, το οποίο αποσκοπεί στον σχεδιασμό και την υλοποίηση ενός πλαισίου ανθεκτικότητας στον κυβερνοχώρο με την υποστήριξη τεχνολογίας τεχνητής νοημοσύνης (AI). Το PHOENI2X θα παρέχει δυνατότητες ενορχήστρωσης, αυτοματοποίησης και ανταπόκρισης με στόχο την επιχειρησιακή συνέχεια, ανάκαμψη, αντιμετώπιση περιστατικών και ανταλλαγή πληροφοριών.

Το έργο ξεκίνησε τον Ιούλιο του 2022 και έχει διάρκεια 3 ετών, με συνολικό προϋπολογισμό €4,825,000.

9.1.3 SYNAPSE

Το έργο SYNAPSE έχει ως στόχο την δημιουργία μιας ολοκληρωμένης πλατφόρμας διαχείρισης κινδύνων και ανθεκτικότητας στον κυβερνοχώρο. Η πλατφόρμα αυτή θα ενσωματώνει μηχανισμούς που θα εξασφαλίζουν τρεις βασικούς πυλώνες: 1. Επίγνωση της κατάστασης, 2. Αντιμετώπιση περιστατικών, 3. Ετοιμότητα. Οι δυνατότητες της πλατφόρμας θα επιτρέπουν τη δυναμική διαχείριση κινδύνων, την προληπτική ανίχνευση, παρακολούθηση και εντοπισμό επιθέσεων και την αντιμετώπιση πιθανών απειλών, προσφέροντας εγγύηση επιχειρησιακής συνέχειας ανά πάσα στιγμή.

Το έργο άρχισε τον Νοέμβριο του 2023, και έχει διάρκεια 3 χρόνια με συνολικό προϋπολογισμό €7,573,750.

9.1.4 CY-TRUST

Το έργο CYTRUST («Cypriot secToRial secToRial secUrity operationS cenTres») στοχεύει στην αύξηση της ικανότητας της Κυπριακής Δημοκρατίας να υπερασπίζεται τις υποδομές και τους πολίτες της από απειλές στον κυβερνοχώρο, μέσω της εισαγωγής Τομεακών Επιχειρησιακών Κέντρων Ασφάλειας (Sectorial Security Operations Centres). Τα Τομεακά Κέντρα Επιχειρήσεων Ασφάλειας θα διασυνδέονται με την Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) Κύπρου, η οποία είναι η Εθνική Αρμόδια Αρχή για την ασφάλεια του κυβερνοχώρου της Κύπρου. Η ΑΨΑ έχει συντονιστικό ρόλο σε αυτό το έργο.

Το έργο ξεκίνησε τον Νοέμβριο του 2023 και αναμένεται να διαρκέσει 36 μήνες, με συνολικό προϋπολογισμό €3.864.583,20, εκ των οποίων το 50%, δηλαδή €1,932,291.60 ευρώ είναι επιχορήγηση από την Ευρωπαϊκή Ένωση. Τον Δεκέμβριο του 2023 λάβαμε το 80% του ποσού, δηλαδή €1,545,833.28.

9.1.5 europeAn THreat intelligence, rEspoNse and prepAredness platform (ATHENA)

Η πρόταση του έργου ATHENA αποσκοπεί στην παροχή μιας πλατφόρμας πληροφόρησης, αντίδρασης και ετοιμότητας για αντιμετώπιση Ευρωπαϊκών απειλών.

Στο έργο αυτό η ΑΨΑ κατέχει τον ρόλο του συντονιστή ενώ συμμετέχουν επίσης οι Εθνικές Αρχές κυβερνοασφάλειας της Κύπρου, της Ελλάδας, της Βουλγαρίας και της Μάλτας. Η πρόταση ATHENA θα υιοθετήσει ένα προσχέδιο Κέντρων Επιχειρήσεων Κυβερνοασφάλειας (Cyber Security Operations Centres - CSOCs) για διασυνοριακή συνεργασία και συντονισμό, με σκοπό τη δημιουργία ενός Συμπλέγματος Συντονισμένης Απόκρισης για τα κράτη μέλη της ΕΕ και άλλες επιλέξιμες οντότητες.

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€.

9.1.6 SecAwarenessTruss

Κρίσιμοι τομείς όπως οι τηλεπικοινωνίες, η ενέργεια, η ναυτιλία και η υγεία βασίζονται σε πολύπλοκες υποδομές ΤΠΕ και τεχνολογίες όπως Διαδίκτυο των Πραγμάτων (Internet of Things – IoT) και τεχνητή νοημοσύνη (Artificial Intelligence – AI). Στους παραπάνω τομείς, υπάρχει ανάγκη για εξειδικευμένο προσωπικό κυβερνοασφάλειας. Το έργο SecAwarenessTruss με στόχο την κάλυψη αυτής της ανάγκης, θα προσφέρει μια πλατφόρμα κυβερνοασφάλειας με εκπαιδευτικά προγράμματα για οργανισμούς κρίσιμων υποδομών. Στο SecAwarenessTruss συμμετέχουν 10 οργανισμοί από Ελλάδα και Κύπρο, με υποστήριξη από το Υπουργείο Ψηφιακής Διακυβέρνησης και την Εθνική Αρχή Κυβερνοασφάλειας της Ελλάδος. Τα αποτελέσματα περιλαμβάνουν την δημιουργία μιας πλατφόρμας κυβερνοασφάλειας που θα προσφέρει προγράμματα κατάρτισης, και την ανάπτυξη μιας βάσης πληροφοριών για απειλές.

Το έργο θα διαρκέσει 3 χρόνια και ο συνολικός προϋπολογισμός ανέρχεται σε 3,539,646€.

9.1.7 CEF A4CEF - Advancing Cybersecurity Certification Capabilities with Cross-border exchange and Enhancing (business) Flows

Το έργο είχε ως απώτερο σκοπό την επέκταση των δραστηριοτήτων της ΑΨΑ στον τομέα πιστοποιήσεων κυβερνοασφάλειας, σύμφωνα με την Εθνική Στρατηγική Κυβερνοασφάλειας. Οι στόχοι που επιτεύχθηκαν περιλαμβάνουν την ενίσχυση της Εθνικής Αρχής Τυποποίησης της Ιρλανδίας (NSAI), την ανάπτυξη δεξιοτήτων με επικαιροποιημένο εκπαιδευτικό υλικό για υπηρεσίες νεφοϋπολογιστικής, την ανταλλαγή καλών πρακτικών μεταξύ Κύπρου και Ιρλανδίας, την ανάπτυξη ολοκληρωμένου μοντέλου για την υποστήριξη του Ευρωπαϊκού Πλαισίου Πιστοποίησης Κυβερνοασφάλειας, και τη χρήση δραστηριοτήτων ενημέρωσης και επικοινωνίας σε ευρωπαϊκά φόρουμ.

Το έργο A4CEF ξεκίνησε τον Ιούλιο του 2021 και ολοκληρώθηκε με επιτυχία τον Μάη του 2023. Ο συνολικός προϋπολογισμός του έργου ήταν €280,000.

9.1.8 CEF CYberSafety IV

Το CYberSafety IV συνεχίζει το επιτυχημένο έργο προκειμένου να προωθηθεί μια ασφαλής διαδικτυακή κουλτούρα για μαθητές, γονείς και εκπαιδευτικούς.

Μέσω του έργου CYberSafety προσφέρεται:

- Πλατφόρμα ευαισθητοποίησης, η οποία απευθύνεται σε μαθητές, γονείς, εκπαιδευτικούς και σε άτομα που εργάζονται με παιδιά και έχει ως στόχο να προάγει την καλύτερη και ασφαλέστερη χρήση του διαδικτύου μέσα από την οποία θα αναπτυχθούν συγκεκριμένα εργαλεία και υπηρεσίες, σε συνεργασία με διάφορα σχολεία και εθνικούς φορείς.
- Γραμμή Βοήθειας (Helpline), η οποία παρέχει υποστήριξη σε νεαρά άτομα όπως επίσης και τους γονείς τους σε ό,τι σχετίζεται με επιβλαβείς επαφές, προσβλητικές συμπεριφορές (π.χ. διαδικτυακό εκφοβισμό, ρητορική μίσους, sexting) και ανεπιθύμητο ή επιβλαβές διαδικτυακό υλικό.
- Γραμμή Καταγγελιών (Hotline), μέσα από την οποία το κοινό έχει τη δυνατότητα να καταγγείλει υποθέσεις που σχετίζονται με παράνομο διαδικτυακό υλικό σεξουαλικής κακοποίησης παιδιών (CSAM).

Το έργο υλοποιείται με την συνδρομή και την συνεργασία από ευρωπαϊκούς φορείς όπως τους οργανισμούς Core Service Platform, Better Internet for Kids και INHOPE και έχει διάρκεια 24 μήνες. Ξεκίνησε στις αρχές Οκτώβριου 2022 και τελειώνει τον Σεπτέμβριο 2024, με συνολικό προϋπολογισμό €1,118,894.72.

9.1.9 CYQCI

Το έργο Cyprus Quantum Communication Infrastructure (CYQCI) είναι το πρώτο έργο που ασχολείται με την ανάπτυξη κβαντικών επικοινωνιών στην Κύπρο, εισάγαγοντας την τεχνολογία στο νησί και θέτοντας τα θεμέλια για την ενεργό συμμετοχή της χώρας στην Ευρωπαϊκή Πρωτοβουλία EuroQCI για την οικοδόμηση πανευρωπαϊκού δικτύου κβαντικής επικοινωνίας.

Περαιτέρω, δημιουργείται ένα κέντρο τεχνογνωσίας κβαντικών επικοινωνιών το οποίο διαμέσου των ερευνών, μαθημάτων εκπαίδευσης και κατάρτισης, καθώς και της υποστήριξης της μελλοντικής καινοτομίας, θα καταστεί δυνατή η συμβολή στην αλυσίδα εφοδιασμού της Ένωσης για τις σχετικές τεχνολογίες και υπηρεσίες.

Το έργο έχει ξεκινήσει τον Ιανουάριο του 2023 με διάρκεια 32 μήνες και έχει συνολικό προϋπολογισμό €7.512.843,43.

9.2 Μελλοντικά Έργα

9.2.1 5G Tactic

Το ευρωπαϊκό συγχρηματοδοτούμενο έργο 5G TACTIC αποσκοπεί στην ανάπτυξη ασφαλών, ανοικτών και διαλειτουργικών λύσεων πέμπτης γενεάς (5G). Το έργο θα φέρει σε συνεργασία εθνικές ρυθμιστικές αρχές, αρχές κυβερνοασφάλειας, καινοτόμες ευρωπαϊκές μικρομεσαίες επιχειρήσεις στον τομέα της τεχνολογίας, παρόχους υποδομών, φορείς εκμετάλλευσης κινητών δικτύων και ερευνητικά και ακαδημαϊκά ινστιτούτα.

Οι δραστηριότητες του έργου περιλαμβάνουν:

- Ανάπτυξη μιας εργαλειοθήκης κυβερνοασφάλειας πέμπτης γενεάς.
- Εκτεταμένη ανάλυση ασφάλειας με αξιολόγηση και δοκιμές ως επίσης και εισηγήσεις για σχετικά

μέτρα μετριασμού για τη λύση πέμπτης γενεάς που προτείνεται από το έργο.
- Πιλοτική εφαρμογή και αξιολόγηση ανοικτών λύσεων πέμπτης γενεάς πολλαπλών προμηθευτών, λαμβάνοντας υπόψη τις πτυχές ασφάλειας.
- Δραστηριότητες κατάρτισης που απευθύνονται σε τεχνικά ακροατήρια και ακροατήρια του τομέα της κυβερνοασφάλειας, καθώς και σε ευρωπαϊκές ρυθμιστικές και αρχές κυβερνοασφάλειας.

Το έργο έχει εγκριθεί, θα ξεκινήσει τον Ιανουάριο 2024, αναμένεται να διαρκέσει 36 μήνες και θα έχει συνολικό προϋπολογισμό ύψους €2.605.592.

9.3 Υποβληθέντες Προτάσεις για συγχρηματοδότηση

9.3.1 Unifying & Upgrading Certification Capabilities across Europe (TrustBoost)

Τον Σεπτέμβρη του 2023 η ΑΨΑ συμμετείχε στην πρόταση «Ενοποίηση & Αναβάθμιση Δυνατοτήτων Πιστοποίησης στην Ευρώπη (TrustBoost)» στην κατηγορία Ψηφιακή Ευρώπη - Digital Europe Programme (DIGITAL) για συγχρηματοδότηση, με συντονιστή του έργου την Εθνική Αρχή Τυποποίησης της Ιρλανδίας. Το έργο περιλαμβάνει συνεργασία μεταξύ εθνικών αρχών και φορέων αξιολόγησης της συμμόρφωσης για την προώθηση ενός ασφαλούς και συμβατού ψηφιακού οικοσυστήματος εντός της Ευρωπαϊκής Ένωσης μέσω της ανταλλαγής γνώσεων, της βελτίωσης και της ευθυγράμμισης των δυνατοτήτων όλων των ενδιαφερομένων μερών.

Το συνολικό κόστος για την ΑΨΑ είναι €153.887, εκ του οποίου το 50% θα καλυφθεί από τη χορηγία της ΕΕ. Ο συνολικός προϋπολογισμός του έργου θα ανέλθει σε €3.169.019.

10. ΣΤΑΤΙΣΤΙΚΑ ΚΑΙ ΕΡΕΥΝΕΣ

10.1 Έρευνες Παρατηρητηρίου

Η ΑΨΑ συλλέγει και αξιολογεί στοιχεία και πληροφορίες που αφορούν την κυβερνοασφάλεια ή/και ψηφιακή ασφάλεια, ώστε να μπορεί να εξάγει χρήσιμα συμπεράσματα τα οποία θα αξιοποιηθούν για περαιτέρω ενέργειες στα πλαίσια των αρμοδιοτήτων της, όπως η διοργάνωση εκπαιδευτικών σεμιναρίων για την ενίσχυση γνώσεων και δεξιοτήτων σε θέματα κυβερνοασφάλειας, καθώς και εκστρατείες ενημέρωσης και ευαισθητοποίησης τόσο των πολιτών όσο και των επιχειρήσεων.

Σε αυτό το πλαίσιο, εντός του έτους 2023, η ΑΨΑ διεξήγαγε 2 (δυο) Παγκύπριες έρευνες για τη συλλογή στοιχείων και πληροφοριών για την κυβερνοασφάλεια στην κυπριακή επικράτεια[8]. Τα κυριότερα θέματα που αξιολογηθήκανε 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 περιστατικά. Η πρώτη έρευνα απευθυνόταν σε επιχειρήσεις και η δεύτερη έρευνα απευθυνόταν σε πολίτες. Οι 2 (δυο) έρευνες διεξήχθησαν παράλληλα τους μήνες Οκτώβριο-Δεκέμβριο 2023 σε δείγμα 1006 πολιτών και 444 επιχειρήσεων από ένα ευρύ φάσμα στους τομείς της βιομηχανίας, του εμπορίου και των υπηρεσιών.

Τα κυριότερα αποτελέσματα της έρευνας που αφορά τις επιχειρήσεις:

1. Σχεδόν οι μισές επιχειρήσεις (49%) δέχθηκαν κάποια επίθεση/παραβίαση τους τελευταίους 12 μήνες με μέσο όρο 1 επίθεση την εβδομάδα σημειώνοντας αύξηση από τις 3-4 επιθέσεις το μήνα σε σχέση με πέρσι.
2. Από τις επιχειρήσεις που δέχθηκαν επίθεση, για τις μισές σχεδόν (46%) υπήρξε οικονομικό κόστος που ανέρχεται σε 27 χιλιάδες ευρώ κατά μέσο όρο δηλαδή έχει αυξηθεί κατά περίπου 4 χιλιάδες ευρώ σε σχέση με πέρσι.
3. Η πιο συχνή επίθεση που δέχονται οι επιχειρήσεις είναι το phishing δηλαδή απατηλά μηνύματα μέσω ηλεκτρονικού ταχυδρομείου με 43% (αύξηση κατά 7 ποσοστιαίες μονάδες σε σχέση με πέρσι).
4. Σχεδόν μία στις τέσσερις επιχειρήσεις έχει περισσότερο από 1 χρόνο να προβεί σε δημιουργία ή ενημέρωση ή αναθεώρηση των πολιτικών τους για την κυβερνοασφάλεια ώστε να συμβαδίζουν με τις τεχνολογικές εξελίξεις.
5. Υπάρχει άγνοια των επιχειρήσεων για σεμινάρια που προσφέρονται με θέματα την κυβερνοασφάλεια αφού σχεδόν οι μισές επιχειρήσεις (46%) δεν γνωρίζουν για αυτά ενώ μόλις 17% 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.
6. Το ποσό το οποίο κατά μέσο όρο επενδύουν οι επιχειρήσεις σε εργαλεία και υπηρεσίες κυβερνοασφάλειας ανά έτος ανήλθε περίπου στις 11 χιλιάδες ευρώ.

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

1. Το 53% των πολιτών δέχθηκε επίθεση τους τελευταίους 12 μήνες με μέσο όρο 25,9 παραβιάσεις/επιθέσεις τον χρόνο, σημειώνοντας σημαντική αύξηση από πέρσι της τάξεως του 25% περίπου.
2. Από τους πολίτες που δέχθηκαν επίθεση για το 19% υπήρξε κάποιο κόστος που ανέρχεται στα 141 ευρώ κατά μέσο όρο. Αξιοσημείωτο είναι το γεγονός πως παρόλο που ο μέσος όρος επιθέσεων αυξήθηκε από 20,9 σε 25,9 παρατηρείται μείωση του κόστους κυβερνοεπιθέσεων (-177 ευρώ) γεγονός που πιθανόν να οφείλεται στην αυξημένη ικανότητα των πολιτών (+9%) να αναγνωρίζουν τα απατηλά μηνύματα.

[8] https://dsa.cy/category/press-releases/consumers-survey-2023

3. Η πιο συχνή επίθεση που δέχονται οι πολίτες είναι το phishing δηλαδή απατηλά μηνύματα μέσω ηλεκτρονικού ταχυδρομείου με 36% παρουσιάζοντας αύξηση 6 ποσοστιαίων μονάδων σε σχέση με πέρσι.
4. Στην περίπτωση των πολιτών που δεν δέχτηκαν κάποιου είδους επίθεση/παραβίαση τον τελευταίο χρόνο, το 89% δεν αποκλείουν το ενδεχόμενο να πέσουν θύμα κακόβουλης επίθεσης στο μέλλον. Το ποσοστό αυτό αυξήθηκε κατά 7% σε σχέση με πέρσι το οποίο καταδεικνύει ότι οι πολίτες είναι πιο συνειδητοποιημένοι για τους κινδύνους του διαδικτύου.
5. Υπάρχει άγνοια των πολιτών για προσφερόμενα σεμινάρια για θέματα που αφορούν την κυβερνοασφάλεια αφού το 74% δήλωσε άγνοια για αυτά ενώ μόνο το 11% έχει συμμετάσχει σε αυτά. 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 τη δεύτερη στη σειρά χαρτογράφηση της εικόνας σε θέματα κυβερνοασφάλειας στις επιχειρήσεις και στους πολίτες. Η χαρτογράφηση θα συνεχιστεί σε ετήσια βάση και θα εμπλουτίζεται με βάση τις εξελίξεις και τις ανάγκες σε πληροφόρηση που θα προκύπτουν.

11. ΟΙΚΟΝΟΜΙΚΑ

11.1 Μη Ελεγμένες Οικονομικές Καταστάσεις για το έτος 2023

Οι οικονομικές καταστάσεις της ΑΨΑ για το έτος που έληξε την 31η Δεκεμβρίου 2023, ετοιμάστηκαν όπως προβλέπεται από το άρθρο 48 (2) του Ν. 89(Ι)/2020. Οι βασικότερες πληροφορίες για την καταγραφή εσόδων και δαπανών, που περιέχονται στις προκαταρτικές μη ελεγμένες οικονομικές καταστάσεις για το έτος που έληξε στις 31 Δεκεμβρίου 2023, απεικονίζονται στα Γραφήματα και περιλαμβάνουν:

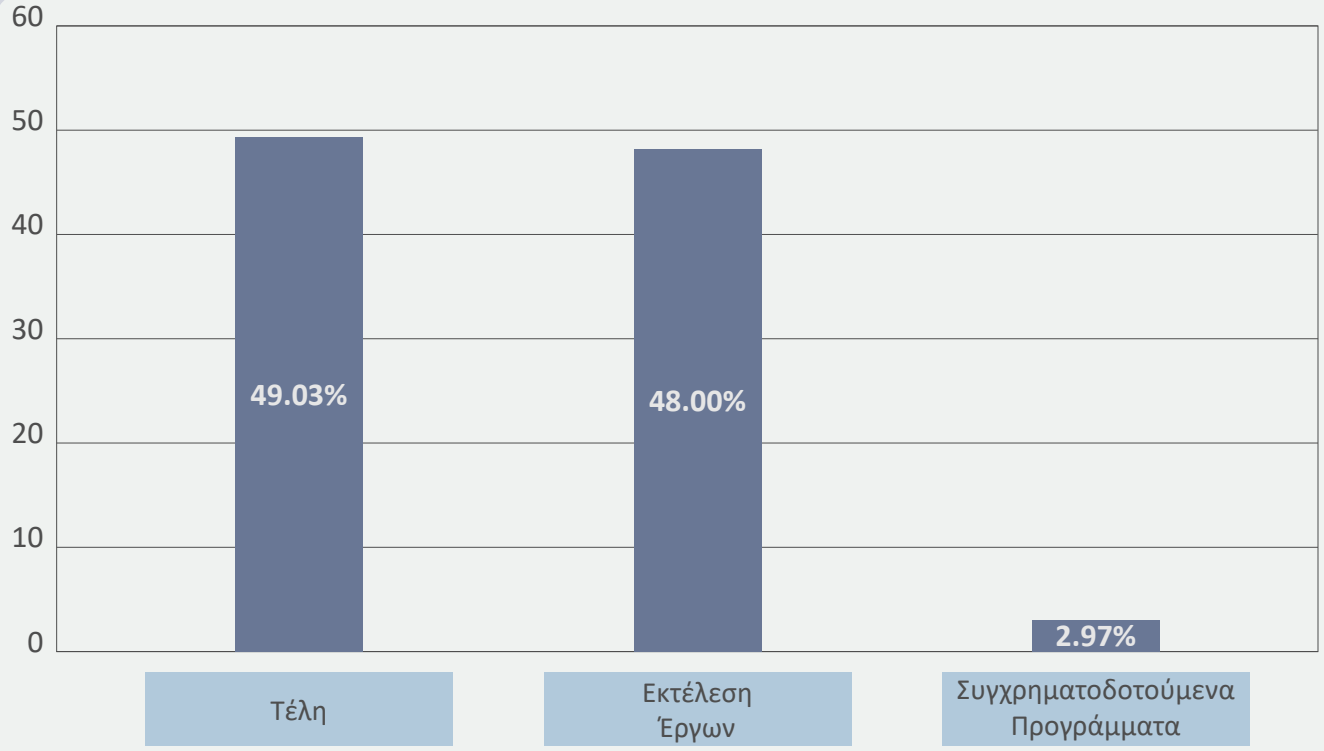
α. έσοδα ύψους €9,953,121 και
β. δαπάνες ύψους €6,664,222

Πίνακας 3: Μη Ελεγμένες οικονομικές καταστάσεις της ΑΨΑ για το έτος που έληξε την 31η Δεκεμβρίου 2023.

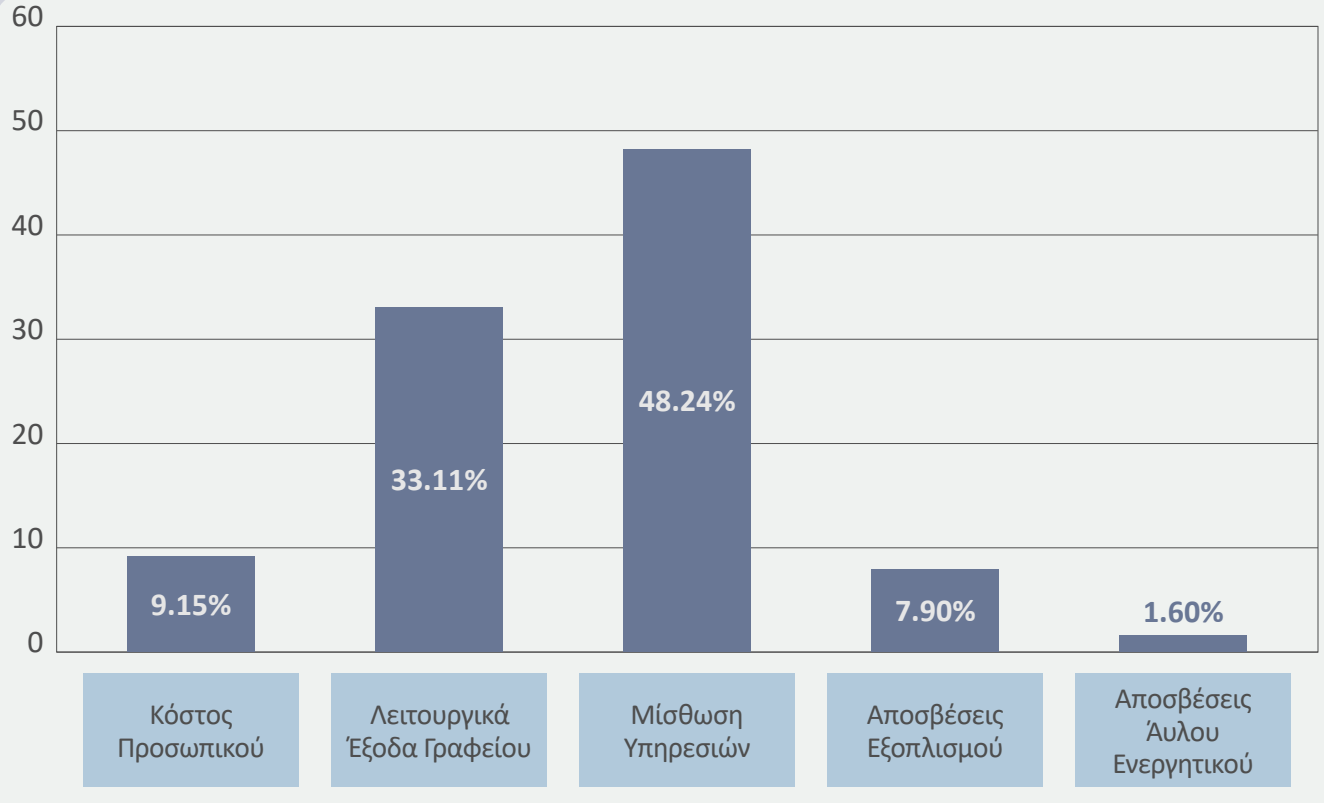
	2023 €	2022 €
Έσοδα		
Έσοδα από τέλη	4,879,598	8,336,171
Έσοδα από συγχρηματοδοτούμενα προγράμματα	4,777,430	215,354
Εκτέλεση έργων για άλλα τμήματα / Υπουργεία	296,093	622,703
	9,953,121	**9,174,228**
Δαπάνες		
Κόστος προσωπικού	609,981	186,667
Έξοδα χρηματοδότησης (Τόκοι)	-	-
Λειτουργικά έξοδα γραφείου	2,206,837	2,110,370
Μίσθωση υπηρεσιών	3,214,571	1,439,935
Αποσβέσεις εξοπλισμού και εγκαταστάσεων	526,481	359,157
Αποσβέσεις άυλου ενεργητικού	106,352	95,446
	6,664,222	**4,191,575**
Πλεόνασμα έτους από συνήθεις εργασίες	3,288,899	4,982,653
Συνολικά εισοδήματα για το έτος	**3,288,899**	**4,982,653**

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

Γράφημα 7: Κατανομή Εσόδων για το 2023



Γράφημα 8: Κατανομή Δαπανών για το 2023



Πίνακας 4: Μη Ελεγμένη Κατάσταση Χρηματοοικονομικής Θέσης στις 31 Δεκεμβρίου 2023

	2023 €	2022 €
ΠΕΡΙΟΥΣΙΑΚΑ ΣΤΟΙΧΕΙΑ		
Μη κυκλοφορούντα περιουσιακά στοιχεία		
Εγκαταστάσεις και εξοπλισμός	2,189,361	1,438,854
Άυλα στοιχεία ενεργητικού	366,138	188,786
Σύνολο μη κυκλοφορούντων περιουσιακών στοιχείων	**2,555,499**	**1,627,640**
Κυκλοφορούντα περιουσιακά στοιχεία		
Χρεώσεις και προπληρωμές	8,064,863	8,201,115
Μετρητά στο ταμείο και στις τράπεζες	12,821,515	9,787,649
Σύνολο κυκλοφορούντων περιουσιακών στοιχείων	**20,886,378**	**17,988,764**
ΣΥΝΟΛΟ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ	**23,441,877**	**19,616,404**
ΙΔΙΑ ΚΕΦΑΛΑΙΑ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ		
Ίδια κεφάλαια		
Αποθεματικά	8,913,225	6,496,679
Σύνολο ιδίων κεφαλαίων	**8,913,225**	**6,496,679**
Τρέχουσες υποχρεώσεις		
Πιστωτές και οφειλόμενα έξοδα	2,540,959	3,126,106
Προεισπραχθέντα τέλη	9,911,393	7,717,319
Υποχρεώσεις σχεδίου συντάξεων και χορηγημάτων στους υπαλλήλους	2,076,300	2,276,300
Ολικό τρεχουσών υποχρεώσεων	**14,528,652**	**13,119,725**
ΟΛΙΚΟ ΙΔΙΩΝ ΚΕΦΑΛΑΙΩΝ ΚΑΙ ΥΠΟΧΡΕΩΣΕΩΝ	**23,441,877**	**19,616,404**

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