ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

Αρχή Ψηφιακής Ασφάλειας

Έκθεση Δραστηριοτήτων 2022

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

Οκτώβριος 2023

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

ΧΑΙΡΕΤΙΣΜΟΣ ΕΠΙΤΡΟΠΟΥ

Στο πλαίσιο της ετήσιας έκθεσης απολογισμού του έργου της Αρχής Ψηφιακής Ασφάλειας (ΑΨΑ), θα ήθελα να επισημάνω τη σημασία της κυβερνοασφάλειας στη σύγχρονη εποχή μας. Η κυβερνοασφάλεια αποτελεί ένα ζωτικό θέμα για το κράτος, την οικονομία και τους πολίτες μας. Σε έναν ψηφιοποιημένο πλέον κόσμο, οι κυβερνοαπειλές αυξάνονται σε συχνότητα, πολυπλοκότητα και σοβαρότητα. Οι κυβερνοεπιθέσεις μπορούν να προκαλέσουν σοβαρές ζημιές στην οικονομία, στα συστήματα υγείας, στις ηλεκτρονικές επικοινωνίες, στη ναυτιλία, στις μεταφορές και σε πολλούς άλλους τομείς της καθημερινής μας ζωής.

Η παρούσα έκθεση απολογισμού αποτυπώνει τις δραστηριότητες που πραγματοποίησε η ΑΨΑ κατά το έτος 2022 για να αντιμετωπίσει τις προκλήσεις της κυβερνοασφάλειας. Η τεχνολογία έχει φέρει επανάσταση στις ζωές μας, και επηρεάζει τις καθημερινές δραστηριότητες και ενέργειες του κράτους και των πολιτών του, συνεπώς η ευρύτερη χρήση της δημιουργεί ευπάθειες που μπορούν να αξιοποιηθούν από πιθανές κυβερνοεπιθέσεις. Η αποστολή της ΑΨΑ, μέσα από την υλοποίηση της Ευρωπαϊκής Οδηγίας NIS (Network and Information Security Directive), είναι η εδραίωση ενός ασφαλούς ψηφιακού περιβάλλοντος για κάθε πολίτη της Κύπρου. Οφείλουμε στην κοινωνία να μεγιστοποιήσουμε τις προσπάθειες μας για επίτευξη της απαραίτητης ασφάλειας. Η παρούσα έκθεση αντικατοπτρίζει το αδιάληπτο έργο που διαδραματίζεται στην ΑΨΑ για τη διασφάλιση των κατάλληλων επιπέδων ασφάλειας των βασικών υπηρεσιών και κρίσιμων υποδομών πληροφοριών της Κυπριακής Δημοκρατίας, μέσω της ρύθμισης, στρατηγικής και εποπτείας της ψηφιακής ασφάλειας, τόσο στον ιδιωτικό, όσο και στον δημόσιο τομέα. Σε ό,τι αφορά την κυβερνοασφάλεια, είμαστε όσο δυνατοί όσο το πιο αδύνατο μας σημείο.

Το πείσμα, ο ζήλος και η ευρηματικότητα που επέδειξαν οι συνεργάτες της ΑΨΑ αλλά και του Εθνικού CSIRT-CY για να διασφαλίσουν την ασπίδα προστασίας της χώρας μας στον κυβερνοχώρο, δίνει στον καθένα μας ένα ξεχωριστό μήνυμα αισιοδοξίας. Το μήνυμα πως παρά τις όποιες αντίξοες συνθήκες, όταν υπάρχει θέληση και συνεργασία μπορούμε να αντιμετωπίσουμε τον οποιοδήποτε κίνδυνο. Αυτό, άλλωστε, μας δίδαξε και η χρονιά που πέρασε, πως δεν πρέπει να σταματούμε, παρά τα όποια εμπόδια, να δουλεύουμε για να προστατεύουμε την κοινωνία μας από τις απειλές του Κυβερνοχώρου, θέτοντας νέους στόχους και υλοποιώντας τους υφιστάμενους.

Καταληκτικά, θα ήθελα να ευχαριστήσω τη Διεύθυνση και το προσωπικό της για την προσήλωση τους στην επίτευξη του οράματος και των στόχων της ΑΨΑ. Ιδιαιτέρως, θα ήθελα να ευχαριστήσω όλους τους συνεργάτες της ΑΨΑ που συνέβαλαν στην ευαισθητοποίηση και κατ' επέκταση στην εφαρμογή των κατάλληλων μέτρων για να επιτευχθεί η κυβερνοασφάλεια στο μέγιστο βαθμό εντός της Δημοκρατίας. Κάθε χρονιά που διανύουμε, οι προκλήσεις και οι απειλές αυξάνονται με ραγδαίους ρυθμούς, για αυτό και εμείς δεν επαναπαυόμαστε, συνεχίζοντας να υπηρετούμε και να συνεισφέρουμε για τα συμφέροντα της Κύπρου. Τα γεγονότα-σταθμοί του 2022 που ακολουθούν, αποτελούν ένα έμπρακτο δείγμα του σημαντικού ρόλου και έργου της ΑΨΑ.

Γιώργος Μιχαηλίδης

Επίτροπος Επικοινωνιών

ΓΕΓΟΝΟΤΑ ΟΡΟΣΗΜΑ 2022

Το έτος 2022 ξεχώρισε για τις πολλές επιτυχίες και τις δράσεις που πραγματοποιήθηκαν:

Δημιουργία και στελέχωση του Εθνικού Κέντρου Συντονισμού Κυβερνοασφάλειας (NCC-CY)

Η βασική αποστολή του Εθνικού Κέντρου Συντονισμού Κυβερνοασφάλειας είναι να διασφαλίζει την παροχή γνώσης και τη διευκόλυνση της πρόσβασης σε τεχνογνωσία για θέματα κυβερνοασφάλειας σε βιομηχανικό, τεχνολογικό και ερευνητικό επίπεδο. Εντός του 2022, το NCC-CY έλαβε θετική αξιολόγηση από την Ευρωπαϊκή Επιτροπή για την ικανότητα του να διαχειρίζεται Ευρωπαϊκά κονδύλια. Ακολούθως, έλαβε την πρώτη του χρηματοδότηση μέσω του Ευρωπαϊκού προγράμματος 'Ψηφιακή Ευρώπη' για την ανάπτυξη του, την δημιουργία της κοινότητας κυβερνοασφάλειας αλλά και για την παροχή οικονομικής ενίσχυσης σε οντότητες που επιθυμούν να αναπτύξουν ή να ενισχύσουν την κυβερνοασφάλεια τους υπό την μορφή επιχορηγήσεων. (βλ. Ενότητα 1.3.5)

Δημιουργία και στελέχωση της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας (NCCA)

Η ΑΨΑ έχει ιδρύσει την Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας (NCCA) βάσει του Ευρωπαϊκού Κανονισμού (ΕΕ) 2019/881 για την Κυβερνοασφάλεια. Το NCCA αποσκοπεί στην εφαρμογή νέων συστημάτων πιστοποίησης κυβερνοασφάλειας για προϊόντα και υπηρεσίες, καθώς και για τεχνολογίες Cloud και 5G. Οι εταιρείες που δραστηριοποιούνται στην Ευρωπαϊκή Ένωση θα μπορούν να πιστοποιούν ψηφιακά προϊόντα, υπηρεσίες και διαδικασίες, μόνο μία φορά στην Κύπρο και θα αναγνωρίζονται σε όλη την Ευρώπη. Με τη συμμόρφωση με αυτά τα πρότυπα και τις πιστοποιήσεις, οι οργανισμοί μπορούν να αποδείξουν στους πελάτες, τους συνεργάτες και τις ρυθμιστικές αρχές ότι τα προϊόντα ή οι υπηρεσίες τους που έχουν πιστοποιηθεί, πληρούν συγκεκριμένες απαιτήσεις ασφάλειας. Ταυτόχρονα, παρέχουν διαβεβαίωση στις ρυθμιστικές αρχές και στην αγορά ότι δεσμεύονται να ακολουθούν καλές πρακτικές ασφάλειας. Ο στόχος του NCCA είναι η διατήρηση ενός υψηλού επιπέδου ανθεκτικότητας στον κυβερνοχώρο. (βλ. Ενότητα 1.3.4)

Συμμετοχή σε Συγχρηματοδοτούμενα Ευρωπαϊκά Ερευνητικά Προγράμματα

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 2022, χρηματοδοτήθηκαν τρία Ευρωπαϊκά προγράμματα με την ολική χρηματοδότηση από αυτά τα ευρωπαϊκά έργα να ανέρχεται στα €8,502,264. Πιο συγκεκριμένα, το Ευρωπαϊκό πρόγραμμα PHOENI2X το οποίο αφορά τη δημιουργία μιας πλατφόρμας ανθεκτικότητας στον κυβερνοχώρο το οποίο θα παρέχει δυνατότητες ανίχνευσης, πρόβλεψης, αυτοματοποίησης και ταχείας απόκρισης με την βοήθεια της τεχνητής νοημοσύνης. Μία ακόμη χρηματοδότηση που αξίζει να αναφερθεί αφορά το Ευρωπαϊκό συγχρηματοδοτούμενο έργο CYberSafety III, που στοχεύει στη δημιουργία μιας ασφαλούς διαδικτυακής κουλτούρας για μαθητές, γονείς και εκπαιδευτικούς. Μέσω του έργου CYberSafety III οι ενδιαφερόμενοι μπορούν να βρουν πληροφορίες και να χρησιμοποιήσουν εργαλεία, αλλά και να μοιραστούν εμπειρίες, τεχνογνωσία και καλές πρακτικές σε σχέση με την ασφαλή χρήση του διαδικτύου.

Τέλος το Ευρωπαϊκό συγχρηματοδοτούμενο έργο N4CY το οποίο αφορά την ανάπτυξη του Εθνικού Συντονιστικού Κέντρου Κυβερνοασφάλειας, που έχει ως βασική αποστολή την παροχή γνώσεων και την πρόσβαση σε τεχνογνωσία για βιομηχανικά, τεχνολογικά και ερευνητικά θέματα κυβερνοασφάλειας.

Πλαίσιο αξιολόγησης και ελέγχου ωριμότητας ικανότητας και συμμόρφωσης των κρίσιμων υποδομών πληροφοριών

Η ΑΨΑ προχώρησε με τη δημιουργία ενός ολοκληρωμένου μοντέλου διαβάθμισης επιπέδων ωριμότητας σε σχέση με τις απαιτήσεις της νομοθεσίας, το οποίο θα χρησιμοποιείται μελλοντικά από πιστοποιημένους και εγκεκριμένους επιθεωρητές στο πλαίσιο της εποπτείας των κρίσιμων υποδομών. Το σχετικό έργο εφαρμόζει μέρος της Εθνικής Στρατηγικής Κυβερνοασφάλειας (Δράση 9 - Εθνικό πλαίσιο Κυβερνοασφάλειας) και αποσκοπεί στην ενίσχυση του επιπέδου κυβερνοασφάλειας στην Κυπριακή Δημοκρατία (βλ. Ενότητα 2.3).

Εθνική Στρατηγική Κυβερνοασφάλειας

Ο σκοπός της Εθνικής Στρατηγικής Κυβερνοασφάλειας είναι η αναβάθμιση του επιπέδου Κυβερνοασφάλειας στη Δημοκρατία. Πιο συγκεκριμένα, εντός του έτους συστάθηκαν οι ομάδες εργασίας, ορίστηκαν οι συντονιστές και εγκρίθηκαν οι προϋπολογισμοί για την κάθε δράση. Ταυτόχρονα, καθορίστηκαν οι δράσεις για τα επόμενα έτη μέχρι το τέλος του 2024.

Ανάπτυξη Επιχειρησιακής Ετοιμότητας της Κυπριακής Δημοκρατίας στην Κυβερνοασφάλεια

Η ΑΨΑ και άλλες αρμόδιες αρχές έθεσαν ως προτεραιότητα την εφαρμογή σχεδιασμών διαχείρισης κρίσεων στον τομέα της κυβερνοασφάλειας. Το Εθνικό Συμβούλιο Κυβερνοασφάλειας αποφάσισε όπως η ΑΨΑ ετοιμάσει ένα μηχανισμό διαχείρισης κρίσεως στο μοντέλο της ΕΕ, με την δημιουργία ενός πλαισίου λειτουργίας που θα αποτελείται από σχέδια διαχείρισης κρίσεων κυβερνοασφάλειας, ενός ταμείου οικονομικής υποστήριξης και μιας Ειδικής Ομάδας έκτακτης ανάγκης (βλ. Ενότητα 6.3.6)

Πλατφόρμα Διαχείρισης ΑΨΑ (iDSAMPL–integrated Digital Security Authority Management Platform)

Η ηλεκτρονική πλατφόρμα iDSAMPL (integrated Digital Security Authority Management Platform) τέθηκε σε πλήρη λειτουργία για την διαχείριση των εποπτευόμενων οργανισμών της ΑΨΑ. Μέσω της εν λόγω πλατφόρμας οι φορείς εκπληρώνουν όλες τις υποχρεώσεις τους που απορρέουν από το Νόμο 89(Ι)/2020 και τις δυνάμει αυτού εκδοθείσες δευτερογενείς νομοθεσίες (π.χ. κοινοποίηση περιστατικών σύμφωνα με την Απόφαση Κ.Δ.Π. 39/2022 καθώς και υποβολή εγγράφων σύμφωνα με την Απόφαση Κ.Δ.Π. 389/2020, ως εκάστοτε τροποποιούνται ή/και αντικαθίστανται). (βλ. Ενότητα 2.6)

Η θαλάσσια κυβερνοασφάλεια στην Ανατολική Μεσόγειο ως πρότυπο

Η ΑΨΑ σε συνεργασία με την SANDIA National Laboratories (Αμερικάνικο Ερευνητικό Εργαστήριο) και το Ανοικτό Πανεπιστήμιο Κύπρου έχει προχωρήσει στη σύνταξη μιας σημαντικής μελέτης με τίτλο «Μια Περιφερειακή Προσέγγιση για τη Διακυβέρνηση και τη Διαχείριση Κινδύνων στον Κυβερνοχώρο της Ναυτιλίας - Η Ανατολική Μεσόγειος ως πρότυπο». Η μελέτη έχει ως στόχο την ενίσχυση της κυβερνοασφάλειας στον θαλάσσιο χώρο της Ανατολικής Μεσογείου μέσω της αποτελεσματικής συνεργασίας των χωρών της περιοχής. Μέσω της μελέτης, αναδεικνύεται ένα πλαίσιο διακυβέρνησης και διαχείρισης κινδύνων στον κυβερνοχώρο σε περιφερειακό και διεθνές επίπεδο, προσαρμοσμένο ειδικά στις ανάγκες του τομέα ναυτιλίας.

3+1 Ομάδα εργασίας για την ασφάλεια στον κυβερνοχώρο

Πραγματοποιήθηκε στην Ιερουσαλήμ η πρώτη συνάντηση του Cyber Security Working Group στο πλαίσιο της συνεργασίας 3+1 (τριμερής Κύπρου – Ελλάδας – Ισραήλ συν ΗΠΑ). Η συνάντηση πραγματοποιήθηκε με όλες τις Εθνικές Αρχές Ψηφιακής Ασφάλειας και επικεντρώθηκε στην ανταλλαγή εμπειριών, βέλτιστων πρακτικών και στη διεξαγωγή διαβουλεύσεων, με στόχο τη χαρτογράφηση ορισμένων από τους πιθανούς τομείς συνεργασίας για την αντιμετώπιση κοινών προκλήσεων και τον μετριασμό των αμοιβαίων απειλών στον κυβερνοχώρο, που σχετίζονται με τους τομείς της ναυτιλίας και της ενέργειας. (βλ. Ενότητα 8.2.5)

Παγκύπριες έρευνες για τη συλλογή στοιχείων και πληροφοριών για την κυβερνοασφάλεια

Η ΑΨΑ διεξήγαγε για πρώτη φορά δύο παγκύπριες έρευνες για τη συλλογή στοιχείων και πληροφοριών για την κυβερνοασφάλεια. Η πρώτη έρευνα απευθυνόταν σε επιχειρήσεις και η δεύτερη έρευνα απευθυνόταν σε πολίτες. Τα κυριότερα θέματα που αξιολογήθηκαν αφορούσαν τον τρόπο χειρισμού θεμάτων κυβερνοασφάλειας ή/και ψηφιακής ασφάλειας, την αποτίμηση της σημαντικότητας που αποδίδεται στα θέματα αυτά, τον τρόπο αντιμετώπισης περιστατικών κυβερνοεπιθέσεων, αλλά και τις συνέπειες από περιστατικά. (βλ. Ενότητα 10)

Συμμετοχή ΑΨΑ στην πανευρωπαϊκή άσκηση Cyber Europe 2022

Η ΑΨΑ συμμετείχε στην πανευρωπαϊκή άσκηση κυβερνοασφάλειας Cyber Europe 2022, η οποία απευθυνόταν τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα, με ευρεία συμμετοχή από τα κράτη-μέλη της Ευρωπαϊκής Ένωσης και από τα μέλη της Ευρωπαϊκής Ζώνης Ελεύθερων Συναλλαγών (ΕΖΕΣ). Η άσκηση Cyber Europe 2022 επικεντρώθηκε στην υγειονομική περίθαλψη και δοκίμασε την ανθεκτικότητα των ενδιαφερόμενων μερών, συμπεριλαμβανομένων των Εθνικών CSIRT, των αρμοδίων αρχών κυβερνοασφάλειας, των Υπουργείων Υγείας και των οργανισμών υγειονομικής περίθαλψης όπως νοσοκομεία και κλινικές, και παρόχους υπηρεσιών ηλεκτρονικής υγείας και ασφάλισης υγείας.

1. ΔΙΟΙΚΗΣΗ

Η ΑΨΑ λειτουργεί βάσει του Νόμου 89(Ι)/2020 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών και υπάγεται στον Επίτροπο Επικοινωνιών και τον Βοηθό Επίτροπο.

1.1 Το Όραμα της Αρχής Ψηφιακής Ασφάλειας

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

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:

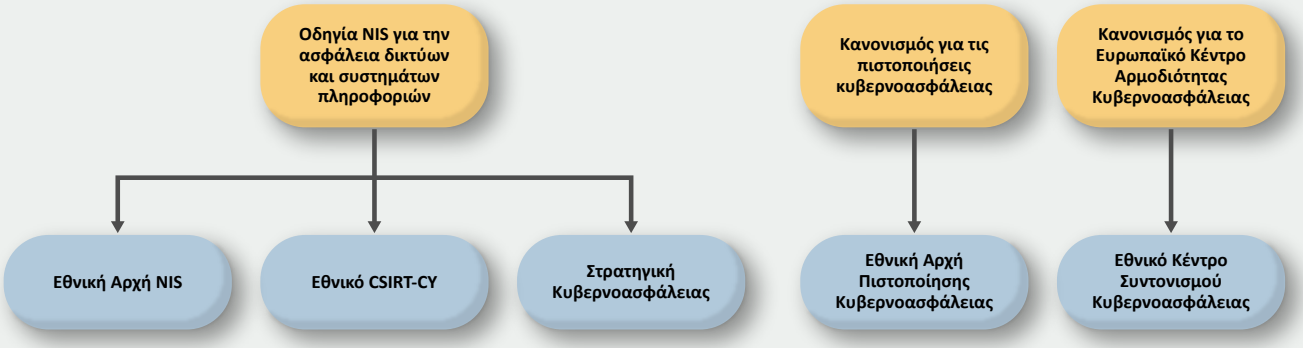
- τη θεσμοθέτηση και εφαρμογή διαφανούς νομοθετικού και ρυθμιστικού πλαισίου σε συνεργασία με όλες τις αρμόδιες υπηρεσίες του κράτους αλλά και όλους τους εμπλεκόμενους φορείς,
- την ανάπτυξη εμπιστοσύνης μεταξύ όλων των εμπλεκομένων φορέων για τη διασφάλιση σωστής και αποτελεσματικής συνεργασίας,
- τη 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 γενικότερα για την κυβερνοασφάλεια, έτσι ώστε να αναπτυχθεί σταδιακά η νοοτροπία και κατ' επέκταση η αλλαγή της κουλτούρας και συνεπώς της γενικής αντιμετώπισης σε θέματα κυβερνοασφάλειας.

1.3 Ρόλοι και 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 κεντροποιημένη 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 2022). Επίσης, στόχος του τομέα για τα επόμενα χρόνια 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. Συντονίζει και προσφέρει υποστήριξη στους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ) και Φορείς Κρίσιμων Υποδομών Πληροφοριών (ΦΚΥΠ) ώστε να εξασφαλιστεί ένα ελάχιστο επίπεδο ασφάλειας στον κυβερνοχώρο. 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 κοινωνικο-οικονομικής 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 παρακαμπτήριες λύσεις,
- δράσεις ευαισθητοποίησης για τις επιπτώσεις των κυβερνοαπειλών και εκπαιδεύσεις σε θέματα κυβερνοασφάλειας,
- υπηρεσίες διαχείρισης τεκμηρίων ασφάλειας πληροφοριών μετά από περιστατικά (δικανικές υπηρεσίες).

1.3.4 Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας (NCCA)

Η ΑΨΑ έχει αναλάβει τον ρόλο της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας, με σκοπό να διασφαλίσει ότι πληρούνται οι απαιτήσεις των ειδικών Ευρωπαϊκών σχημάτων πιστοποίησης αναφορικά με προϊόντα, διαδικασίες και υπηρεσίες στις τεχνολογίες πληροφορικής και επικοινωνιών. Η Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας (National Cybersecurity Certification Authority - NCCA) ως νέο τμήμα της ΑΨΑ, έχει δημιουργηθεί για την εφαρμογή των απαιτήσεων του Κανονισμού (ΕΕ) 2019/881 για την Κυβερνοασφάλεια. Στόχος είναι να προωθήσει την ανάπτυξη των διαδικασιών και των ικανοτήτων πιστοποίησης κυβερνοασφάλειας στην Κυπριακή Δημοκρατία, με απώτερο στόχο να μετατρέψει την Κύπρο σε περιφερειακό κέντρο πιστοποιήσεων.

Η ΑΨΑ 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 γενικότερα παράπονα, σχετικά με την πιστοποίηση προϊόντων και υπηρεσιών.

1.3.5 Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY)

Η αποστολή του Εθνικού Κέντρου Συντονισμού είναι να παρέχει γνώση και να διευκολύνει την πρόσβαση σε τεχνογνωσία σχετικά με βιομηχανικά, τεχνολογικά και ερευνητικά θέματα κυβερνοασφάλειας σε φορείς από τη βιομηχανία, τον δημόσιο τομέα, την ακαδημαϊκή και ερευνητική κοινότητα.

Το NCC ενεργεί ως το σημείο επαφής σε εθνικό επίπεδο για την Κοινότητα Κυβερνοασφάλειας και υποστηρίζει το Ευρωπαϊκό Κέντρο Αρμοδιότητας Κυβερνοασφάλειας (European Cybersecurity Competence Centre - ECCC) και το Δίκτυο των Εθνικών Κέντρων Συντονισμού στην εκπλήρωση της αποστολής και των στόχων τους. Η Κοινότητα συγκεντρώνει ενδιαφερόμενα μέρη από τον ιδιωτικό τομέα, τον δημόσιο τομέα, τη βιομηχανία, τον ακαδημαϊκό χώρο και την έρευνα, συνδυάζοντας γνώση, ικανότητα και εμπειρία σε θέματα κυβερνοασφάλειας, με απώτερο σκοπό να μπορεί να συμβάλει στο μέγιστο στην αποστολή του ECCC. Τέλος, μέσω των δράσεων του το NCC-CY θα βοηθά τις επιχειρήσεις στη Κύπρο, κυρίως τις μικρομεσαίες επιχειρήσεις (ΜμΕ), να αποκτήσουν ένα ενεργό ρόλο, να είναι ανταγωνιστικές και ικανές για να μπορούν να συνεισφέρουν σημαντικά στην ηγετική θέση της Ευρωπαϊκής Ένωσης στον τομέα της κυβερνοασφάλειας.

1.4 Στελέχωση

Οι εγκεκριμένες οργανικές θέσεις της ΑΨΑ κατά την 31η Δεκεμβρίου 2022, απαριθμούνται ως εξής:

- Ένας (1) Πρώτος Μηχανικός Ψηφιακής Ασφάλειας.
- Δύο (2) Ανώτεροι Μηχανικοί Ψηφιακής Ασφάλειας (2 κενές θέσεις που πρόκειται να πληρωθούν εντός 2023).
- Δύο (2) Λειτουργοί Νομικών Θεμάτων.
- Δεκαοκτώ (18) Μηχανικοί Ψηφιακής Ασφάλειας (18 κενές θέσεις που πρόκειται να πληρωθούν εντός 2023).

Επίσης, εντός του 2022, η ΑΨΑ απασχολούσε το ακόλουθο προσωπικό:

- Δύο (2) Προϊστάμενοι (με αγορά υπηρεσιών)
- Δύο (2) Λειτουργοί Τεχνικών Θεμάτων (απόσπαση από το ΓΕΡΗΕΤ)
- Δύο (2) Νομικοί Λειτουργοί (με αγορά υπηρεσιών)
- Δεκαεννιά (19) Αναλυτές Κυβερνοασφάλειας (με αγορά υπηρεσιών)
- Επτά (7) Διοικητικοί / Οικονομικοί Λειτουργοί (με αγορά υπηρεσιών)
- Δύο (2) Γραφείς (με αγορά υπηρεσιών)

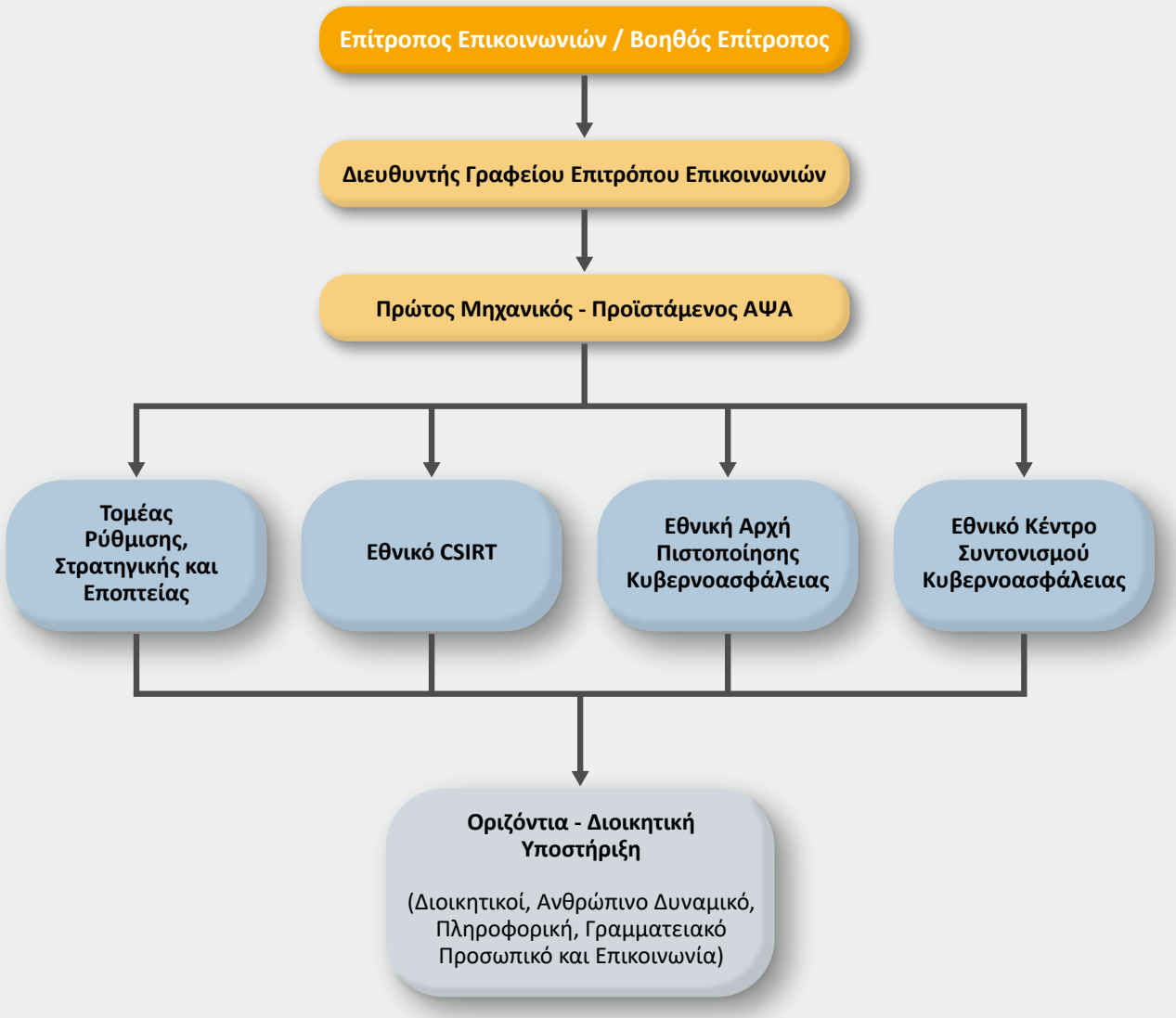
Εντός του 2022, ολοκληρώθηκαν οι διαδικασίες του ΣΕΠΑ (Συμβούλιο Επιλογής και Προαγωγών ΑΨΑ) για τη στελέχωση της θέσης του Πρώτου Λειτουργού – Προϊστάμενου της ΑΨΑ, καθώς και δύο (2) θέσεων μόνιμων Νομικών Λειτουργών.

Επίσης, για βελτίωση των μελλοντικών διαδικασιών στελέχωσης, η ΑΨΑ προχώρησε στην δημιουργία εσωτερικού Συστήματος Διαχείρισης Αιτήσεων Πρόσληψης που αποτελεί μια ενιαία πλατφόρμα διαχείρισης των αιτήσεων για τις θέσεις που πρέπει να στελεχώνονται. Μέσω του συγκεκριμένου συστήματος θα γίνεται η διαχείριση των αιτήσεων που προκηρύσσονται σε όλα τα στάδια της διαδικασίας πρόσληψης και στελέχωσης.

Εντός του 2023, αναμένεται ότι θα προκηρυχθούν οι δύο (2) κενές θέσεις Ανώτερων Μηχανικών Ψηφιακής Ασφάλειας και οι δεκαοκτώ (18) κενές θέσεις Μηχανικών Ψηφιακής Ασφάλειας, για τη μόνιμη στελέχωση του Τομέα Ρύθμισης, Στρατηγικής και Εποπτείας, και του Εθνικού CSIRT-CY. Καθώς η ΑΨΑ αναλαμβάνει νέες αρμοδιότητες (όπως, Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας, Εθνικό Κέντρο

Συντονισμού Κυβερνοασφάλειας, Εθνικό SOC (Security Operations Centre)), και με την απόφαση για μετάβαση του Εθνικού CSIRT σε λειτουργία επί βάσης 24 ώρες / 365 μέρες το χρόνο, η ΑΨΑ σχεδιάζει τη δημιουργία σημαντικού αριθμού επιπρόσθετων 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

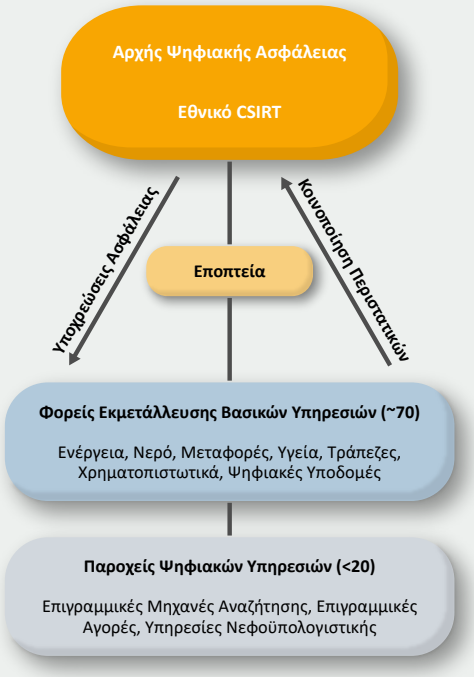
2. ΥΛΟΠΟΙΗΣΗ ΟΔΗΓΙΑΣ NIS ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

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 να θεσπίσουν εθνική στρατηγική για την ασφάλεια των συστημάτων δικτύων και πληροφοριών, απαιτήσεις ασφάλειας και κοινοποίησης για τους Φορείς εκμετάλλευσης βασικών υπηρεσιών και για τους παρόχους ψηφιακών υπηρεσιών και καθορίζει τις υποχρεώσεις των κρατών μελών να ορίζουν εθνικές αρμόδιες αρχές, ενιαία κέντρα επαφής και CSIRT με καθήκοντα σχετικά με την ασφάλεια των συστημάτων δικτύων και πληροφοριών.

Για την υλοποίηση της Οδηγίας στην Κυπριακή Δημοκρατία, η ΑΨΑ θέτει 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 ολόκληρη την Ένωση (Οδηγία (ΕΕ) 2016/1148 – «Οδηγία NIS»). Επιπλέον, εναρμονίζει μερικώς την εθνική νομοθεσία με το ευρωπαϊκό νομικό πλαίσιο αναφορικά με τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (Οδηγία (ΕΕ) 2018/1972 - άρθρα 40/41 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 η εθνική αρχή για το συντονισμό της υλοποίησης της Στρατηγικής Κυβερνοασφάλειας.

2.2.2 Τροποποίηση Νόμου

Με σκοπό την ενσωμάτωση στο Νόμο της ΑΨΑ των νέων ρόλων και αρμοδιοτήτων της, η ΑΨΑ ετοίμασε και προώθησε, εντός του 2022, τροποποιητικό νομοσχέδιο για κάλυψη των πιο κάτω:

- Διασφάλιση της εφαρμογής του Κανονισμού (ΕΕ) 2019/881 στην Κυπριακή Δημοκρατία (βλ. Ενότητα 4) και βάσει σχετικής Απόφασης του Υπουργικού Συμβουλίου, την ανάληψη του ρόλου της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας από την ΑΨΑ,
- Διασφάλιση της εφαρμογής του Κανονισμού (ΕΕ) 2021/887 στην Κυπριακή Δημοκρατία (βλ. Ενότητα 4) και βάσει σχετικής Απόφασης του Υπουργικού Συμβουλίου, την ανάληψη του ρόλου του Εθνικού Κέντρου Συντονισμού για την Κυβερνοασφάλεια,
- Εναρμόνιση με τα σημεία (δ), (ε), (στ) και (θ) του άρθρου 3(3) της Οδηγίας 2014/53/ΕΕ, που αφορούν τον ραδιοεξοπλισμό και μεταφέρονται από το Νόμο 112(Ι)/2004 στο Νόμο 89(Ι)/2020, μετά από διαβουλεύσεις μεταξύ του Υφυπουργείου Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής και του Επιτρόπου Επικοινωνιών,
- Τροποποίηση συγκεκριμένων διατάξεων στον Νόμο, μετά από εισηγήσεις που έλαβε η ΑΨΑ κατά τη διενέργεια της Δημόσιας Διαβούλευσης για την περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κυβερνοασφάλεια Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών Πέμπτης Γενιάς 5G) Απόφαση του 2020 (Κ.Δ.Π. 408/2020),
- Τροποποίηση 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(Ι)/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).

Το τροποποιητικό νομοσχέδιο, έτυχε νομοτεχνικού ελέγχου από τη Νομική Υπηρεσία και εγκρίθηκε από το Υπουργικό Συμβούλιο το 2022, και αναμένεται να ψηφιστεί από τη Βουλή των Αντιπροσώπων εντός του 2023.

2.2.3 Δευτερογενής Νομοθεσία

Εντός του 2022, εκδόθηκε η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Παροχέων Δικτύων ή/και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών) Απόφαση (Κ.Δ.Π. 41/2022)[2]. Η υπό αναφορά Απόφαση καθορίζει ελάχιστες επιπρόσθετες υποχρεώσεις, τις οποίες πρέπει να τηρούν οι παροχείς δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, πέραν από τις υποχρεώσεις που καθορίζονται στην περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών) Απόφαση του 2020, ως εκάστοτε τροποποιείται ή/και αντικαθίσταται (Κ.Δ.Π. 389/2020)[3]. Επιπλέον, καταργεί και αντικαθιστά το περί Ασφάλειας Δικτύων και Πληροφοριών Διάταγμα του 2011 (Κ.Δ.Π. 253/2011)[4].

Επίσης, εντός του 2022, εκδόθηκε η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κοινοποίηση Συμβάντων) Απόφαση του 2022 (Κ.Δ.Π. 39/2022)[5] η οποία αναθεώρησε και αντικατέστησε την σχετική Απόφαση του 2019 (ΚΔΠ 218/2019)[6]. Το περί της κοινοποίησης των

[2] https://dsa.cy/images/pdf-upload/Decision-41-2022.pdf
[3] https://dsa.cy/images/pdf-upload/Decision-389-2020.pdf
[4] https://dsa.cy/images/pdf-upload/Order-253-2011.pdf
[5] https://dsa.cy/images/pdf-upload/Decision-39-2022.pdf
[6] https://dsa.cy/images/pdf-upload/Decision-218-2019.pdf

παραβιάσεων ασφάλειας ή απώλειας ακεραιότητας δικτύων ή/και υπηρεσιών Διάταγμα του 2013 (Κ.Δ.Π. 371/2013)[7] και η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κοινοποίηση Συμβάντων) Απόφαση του 2019 (Κ.Δ.Π. 218/2019) καταργήθηκαν και αντικαταστάθηκαν με την έκδοση της νέας Απόφαση ΚΔΠ 39/2022. Επίσης, εντάχθηκαν πρόνοιες με σκοπό να διασφαλίζεται νομικά η ηλεκτρονική υποβολή των εντύπων κοινοποίησης μέσω της πλατφόρμας iDSAMPL (integrated Digital Security Authority Management Platform) της Αρχής, που τέθηκε σε λειτουργία εντός του 2022.

2.2.4 Οδηγία NIS2

Η Οδηγία NIS αποτέλεσε την πρώτη νομοθετική πράξη της Ευρωπαϊκής Ένωσης σχετικά με την ασφάλεια δικτύων και συστημάτων πληροφοριών. Παρόλο που συνέβαλε στη σημαντική αύξηση του επιπέδου κυβερνοανθεκτικότητας της Ένωσης, η επανεξέταση της ήταν επιβεβλημένη καθώς ο αριθμός, το μέγεθος, η επινοητικότητα και η συχνότητα, όπως επίσης και ο αντίκτυπος των περιστατικών αυξήθηκαν σε σημαντικό βαθμό και αποτελούν μείζονα απειλή για τη λειτουργία των συστημάτων δικτύων και πληροφοριών.

Στις 14 Δεκεμβρίου 2022, υπογράφηκε από το Ευρωπαϊκό Κοινοβούλιο και από το Συμβούλιο της Ευρώπης η Οδηγία (ΕΕ) 2022/2555 (Οδηγία NIS2) σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, η οποία δημοσιεύθηκε στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης στις 27 Δεκεμβρίου 2022.

Βάσει της Οδηγίας NIS2, οι οντότητες θα χωρίζονται πλέον σε δύο κατηγορίες: βασικές οντότητες (essential entities) και σημαντικές οντότητες (important entities). Εκτός από τους τομείς που είχαν συμπεριληφθεί στην Οδηγία NIS, η Οδηγία NIS2 επεκτείνεται σε αρκετούς νέους δημόσιους και ιδιωτικούς τομείς, όπως, μεταξύ άλλων, παρόχους υπηρεσιών εμπιστοσύνης, παρόχους πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης, παρόχους υπηρεσιών κέντρου δεδομένων (data centres), εταιρείες που ασχολούνται με ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών κ.ά., ως αναφέρονται στο Παράρτημα Ι και Παράρτημα ΙΙ της Οδηγίας NIS2. Η επέκταση του πεδίου εφαρμογής της Οδηγίας NIS2, με την οποία ουσιαστικά υποχρεώνονται περισσότερες οντότητες και τομείς να λάβουν μέτρα διαχείρισης των κινδύνων στον τομέα της κυβερνοασφάλειας, θα συμβάλει στην αύξηση του επιπέδου κυβερνοασφάλειας στην Ευρώπη τόσο μεσοπρόθεσμα όσο και μακροπρόθεσμα.

Εντός του 2022, η Αρχή ξεκίνησε τη μελέτη της Οδηγίας NIS2 με σκοπό τη μεταφορά των προνοιών της στην εθνική νομοθεσία καθώς η Οδηγία NIS2 θα τεθεί σε εφαρμογή στις 18 Οκτωβρίου 2024 και την ίδια μέρα η Οδηγία NIS θα παύσει να ισχύει.

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 389/2020 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών), όπου περιλαμβάνεται ένας κατάλογος 70 μέτρων για ολιστική προσέγγιση των Φορέων όσο αφορά στην επίτευξη ενός υψηλού επιπέδου κυβερνοασφάλειας.

Λαμβάνοντας υπόψη την υποχρέωση που είχαν οι Φορείς για ηλεκτρονική υποβολή όλων των προβλεπόμενων εγγράφων με βάση τις απαιτήσεις του άρθρου 13 της Απόφασης, η ΑΨΑ, εντός του 2022, προχώρησε σε ανασκόπηση των εγγράφων που υπέβαλαν οι Φορείς για τα θέματα, μεταξύ άλλων, διαχείρισης κινδύνων και σχεδιασμού επιχειρησιακής συνέχειας. Η ΑΨΑ απέστειλε επίσης έκθεση στον κάθε φορέα, σχετικά με την αξιολόγηση (document review) των εγγράφων που είχαν υποβληθεί.

Εντός του 2023 η ΑΨΑ θα προχωρήσει στην αξιολόγηση της προόδου εφαρμογής των εν λόγω μέτρων

[7] https://dsa.cy/images/pdf-upload/EC_Order_NotificationsSecurityBreaches_GR_25-10 2013_VM_0.pdf

με στόχο την όσο το δυνατόν καλύτερη προστασία των κρίσιμων υποδομών πληροφοριών που διαχειρίζονται οι Φορείς.

Παράλληλα, στα πλαίσια των αρμοδιοτήτων της η ΑΨΑ έχει ως υποχρέωση την παρακολούθηση συμμόρφωσης των Φορέων με τη σχετική Απόφαση. Για το σκοπό αυτό η ΑΨΑ έχει αναλάβει την ανάπτυξη ενός μοντέλου ωριμότητας ικανοτήτων (Capability Maturity Model). Το μοντέλο αυτό:

- θα χρησιμοποιηθεί τόσο από τους ίδιους τους Φορείς για να επιμετρούν το επίπεδο ωριμότητας και συμμόρφωσης τους με τις πρόνοιες της δευτερογενούς νομοθεσίας που αφορά τα μέτρα ασφάλειας, και
- θα αποτελέσει το εργαλείο ελέγχου και αξιολόγησης από μέρους των εξωτερικών ελεγκτών των εποπτευόμενων Φορέων. Το αποτέλεσμα της εργασίας των ελεγκτών θα είναι ο καθορισμός τυχόν αποκλίσεων, καθώς επίσης και προτεινόμενο σχέδιο δράσης για γεφύρωση των αποκλίσεων αυτών.

Οι απαιτήσεις της νομοθεσίας, σε συνδυασμό με το ως άνω μοντέλο ωριμότητας, θα τροφοδοτήσουν τη δημιουργία ενός εξειδικευμένου πλαισίου ελέγχων, το οποίο θα βασίζεται στις διεθνείς βέλτιστες πρακτικές και πρότυπα και θα περιλαμβάνει απαιτούμενα προσόντα ελεγκτών (ρόλοι και αρμοδιότητες), καθώς επίσης και πρότυπα εγγράφων ελέγχου.

Εντός του 2022 έχει ολοκληρωθεί η ανάπτυξη του μοντέλου ωριμότητας. Κατά το 2023, η ΑΨΑ θα προχωρήσει στην επόμενη φάση του έργου που είναι η προδιαγραφή των ελάχιστων απαιτούμενων προσόντων, ρόλων και αρμοδιοτήτων των ελεγκτών, καθώς και τον προσδιορισμό της όλης διαδικασίας επιτόπιων ελέγχων.

2.4 Κοινοποίηση Περιστατικών Παραβίασης Ψηφιακής Ασφάλειας

Η Απόφαση ΚΔΠ 39/2022 για τις κοινοποιήσεις περιστατικών τυγχάνει εφαρμογής από όλους τους Φορείς και Παροχείς, και καθορίζει τα κριτήρια, τα κατώτατα όρια και τις συνθήκες υπό τις οποίες ένα περιστατικό ασφάλειας έχει σοβαρό ή/και σημαντικό αντίκτυπο στην παροχή των υπηρεσιών των ως άνω Φορέων και Παροχέων. Ως εκ τούτου, ενεργοποιεί την υποχρέωση των Φορέων και των Παροχέων αυτών για υποβολή κοινοποίησης περιστατικών στην ΑΨΑ, που σχετίζονται με την απώλεια ή επηρεασμό των βασικών χαρακτηριστικών της ασφάλειας των υπηρεσιών τους δηλαδή την εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και αυθεντικότητα. Περαιτέρω, ρυθμίζεται η διαδικασία υποβολής των κοινοποιήσεων, και ιδίως το περιεχόμενο των κοινοποιήσεων, ο τρόπος υποβολής τους και οι προθεσμίες που πρέπει να τηρηθούν από τους Φορείς και τους Παροχείς.

Κατά το 2022, υποβλήθηκαν επτά (7) κοινοποιήσεις περιστατικών στην ΑΨΑ, οι οποίες έτυχαν διαχείρισης κατά περίπτωση (βλ. επίσης Ενότητα 3).

2.5 Αξιολόγηση Κρισιμότητας Υποδομών

Η ΑΨΑ διενεργεί, σε τακτά χρονικά διαστήματα, αξιολογήσεις και επαναξιολογήσεις κρισιμότητας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών («Φορείς») στην Κυπριακή Δημοκρατία, με βάση το Άρθρο 27(5) του Νόμου. Επιπλέον, έχει υποχρέωση όπως κοινοποιεί στοιχεία που σχετίζονται με τους Φορείς στην Κυπριακή Δημοκρατία στα αρμόδια Ευρωπαϊκά σώματα, δηλαδή στην Ομάδα Συνεργασίας για την Ασφάλεια Δικτύων και Πληροφοριών (NIS Cooperation Group), στην Ευρωπαϊκή Επιτροπή και στον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA). Τα αποτελέσματα της αξιολόγησης κρισιμότητας τυγχάνουν έγκρισης από το Υπουργικού Συμβούλιο.

Κατά το 2022 συνεχίστηκε η παρακολούθηση της κατάστασης όσον αφορά τους Φορείς στο σύνολο τους, και δεν διαπιστώθηκε οποιαδήποτε ανάγκη για ορισμό νέων ή/και επαναξιολόγηση υφιστάμενων Φορέων. Δεδομένης της ψήφισης της νέας Ευρωπαϊκής Οδηγίας NIS2 (βλ. Ενότητα 2.2.4), όπου

διευρύνονται σημαντικά οι τομείς κάλυψης και διαφοροποιείται η κατηγοριοποίηση Φορέων σε Βασικές και Σημαντικές Οντότητες, προγραμματίζεται αναθεώρηση της διαδικασίας αξιολόγησης (με βάση τις νέες πρόνοιες) και διενέργεια της επόμενης αξιολόγησης κρισιμότητας εντός του 2024.

2.6 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. Η ΑΨΑ προχώρησε στην ανάπτυξη της πλατφόρμας με σκοπό να αποτελέσει το κύριο μέσο διαχείρισης της συμμόρφωσης των Φορέων με τις πρόνοιες της νομοθεσίας, ιδιαίτερα λόγω του σχετικά μεγάλου αριθμού των Φορέων (γύρω στους 70 κατά το τέλος του 2022, αριθμός ο οποίος αναμένεται να πολλαπλασιαστεί με την υλοποίηση της Οδηγίας NIS2 το 2024). Η εν λόγω πλατφόρμα περιλαμβάνει λειτουργίες σχετικά με:

- τη διαχείριση στοιχείων επικοινωνίας των Φορέων (Contact Management)
- την κοινοποίηση και διαχείριση περιστατικών (Incident Reporting and Management)
- τη διαχείριση συμμόρφωσης των Φορέων (Compliance Management)
- τη διαχείριση κινδύνων (Risk Management)
- τη διαχείριση ελέγχων (Audit Management)
- τη διαχείριση ενεργειών μετριασμού (Mitigation Actions Management)
- την αποστολή ειδοποιήσεων (Alerts and Notifications)

Η ΑΨΑ οργάνωσε διαδικτυακή παρουσίαση της πλατφόρμας iDSAMPL προς όλους τους Φορείς τον Μάρτιο του 2022. Μετά από την ολοκλήρωση της σχετικής μεταβατικής περιόδου, από την 1η Ιουνίου 2022, οι Φορείς είναι σε θέση να χρησιμοποιούν την πλατφόρμα για να εκπληρώνουν τις υποχρεώσεις τους που απορρέουν από το Νόμο 89(I)/2020 και τις δυνάμει αυτού εκδοθείσες δευτερογενείς νομοθεσίες.

3. ΔΙΑΧΕΙΡΙΣΗ ΣΥΜΒΑΝΤΩΝ ΚΑΙ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

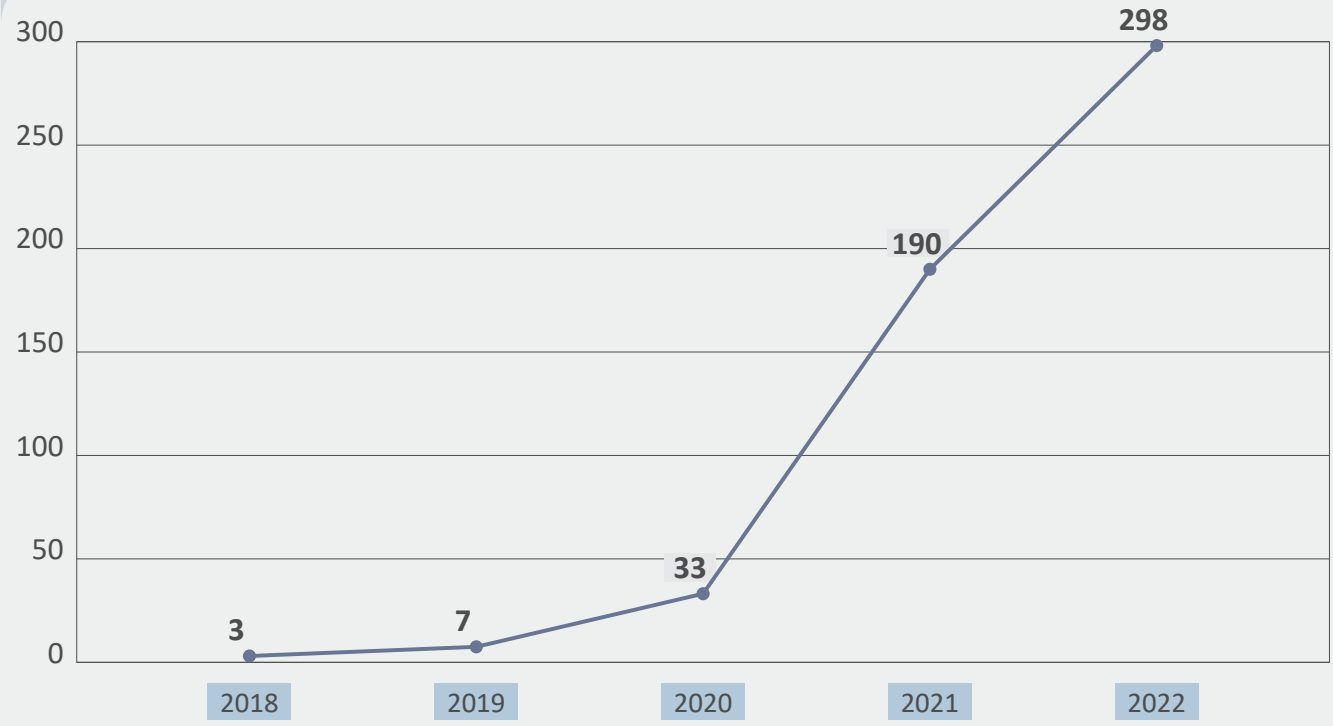
3.1 Διαδικασίες Εθνικού CSIRT-CY

Η Εθνική Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων της Κύπρου (CSIRT-CY) προχωρεί με την εφαρμογή ενός συνόλου διαδικασιών διαχείρισης από τη στιγμή που θα εντοπίσει ένα περιστατικό έως την επίλυση του. Οι εν λόγω διαδικασίες έχουν αξιολογηθεί και εγκριθεί από διεθνείς και ευρωπαϊκούς οργανισμούς όπως το FIRST[8], ο TI[9] και ο ENISA[10]. Ως οι σημαντικότεροι στόχοι του Εθνικού CSIRT-CY έχουν τεθεί η αντιμετώπιση περιστατικών κυβερνοασφάλειας και ο περιορισμός των επιδράσεων τους. Βέβαια, η διενέργεια των εν λόγω διαδικασιών επέρχεται σε προκαθορισμένο χρονικό πλαίσιο και αφού γίνει η κατάταξη των περιστατικών ανάλογα με το βαθμό επικινδυνότητας και σημαντικότητάς τους.

3.2 Διαχείριση Περιστατικών

Κατά το έτος 2022, έχουν κοινοποιηθεί στο Εθνικό CSIRT συνολικά 298 περιστατικά. Διαβάζοντας το παρακάτω Γράφημα 4, μπορούμε να διακρίνουμε μια αυξητική πορεία στον αριθμό των περιστατικών που έχουν κοινοποιηθεί στο Εθνικό CSIRT. Αυτό ασφαλώς, δεν οφείλεται μόνο στη ραγδαία αύξηση των περιστατικών κυβερνοεπιθέσεων στην Κυπριακή Δημοκρατία, αλλά αναδεικνύει την αμοιβαία σχέση εμπιστοσύνης που έχει χτιστεί μεταξύ των φορέων κρίσιμων υποδομών και του Εθνικού CSIRT, που έχει ως αποτέλεσμα να κοινοποιούν ακόμη και σε εθελοντική βάση κάθε ύποπτο περιστατικό που έχει υποπέσει στην προσοχή τους έτσι ώστε να λάβουν άμεση ανταπόκριση και κατάλληλη βοήθεια.

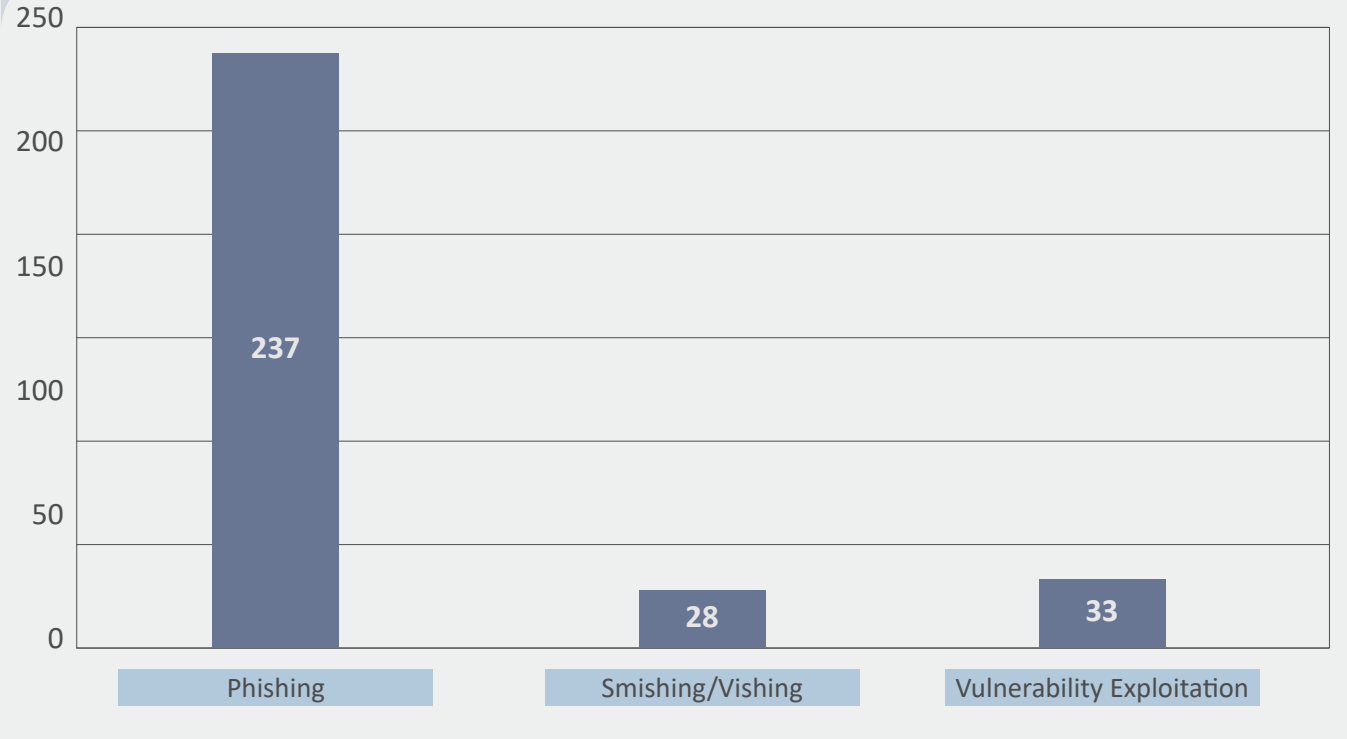
Γράφημα 4: Καταγεγραμμένα περιστατικά ανά έτος



[8] *FIRST: Forum of Incident Response and Security Teams*
[9] *Trusted Introducer*
[10] *ENISA: European Union Agency for Cybersecurity*

Αξίζει να σημειωθεί πως το έτος 2022, το Εθνικό CSIRT-CY αντιμετώπισε αυξημένο αριθμό αναφορών σχετικά με περιστατικά επιθέσεων Phishing (συμπεριλαμβανομένου Smishing & Vishing) (βλ. Γράφημα 5). Η επίθεση Phishing / Smishing / Vishing, ή αλλιώς ηλεκτρονικό ψάρεμα, είναι μια μορφή απάτης είτε μέσω ηλεκτρονικού ταχυδρομείου, μηνυμάτων κινητών τηλεφώνων αλλά ακόμη και τηλεφωνικών κλήσεων αντίστοιχα, όπου οι επιτιθέμενοι εξαπατούν το ανυποψίαστο θύμα με απώτερο σκοπό την υποκλοπή ευαίσθητων πληροφορίων ή την εγκατάσταση κάποιου κακόβουλου λογισμικού. Στις πλείστες των περιπτώσεων το Εθνικό CSIRT λάμβανε αναφορές από τον τραπεζικό τομέα ένεκα των αυξημένων κακόβουλων συνδέσμων που προσποιούνταν χρηματοπιστωτικά ιδρύματα και υπηρεσίες διαδικτυακών συναλλαγών.

Γράφημα 5: Περιστατικά Phising/Smishing/Vishing για το 2022

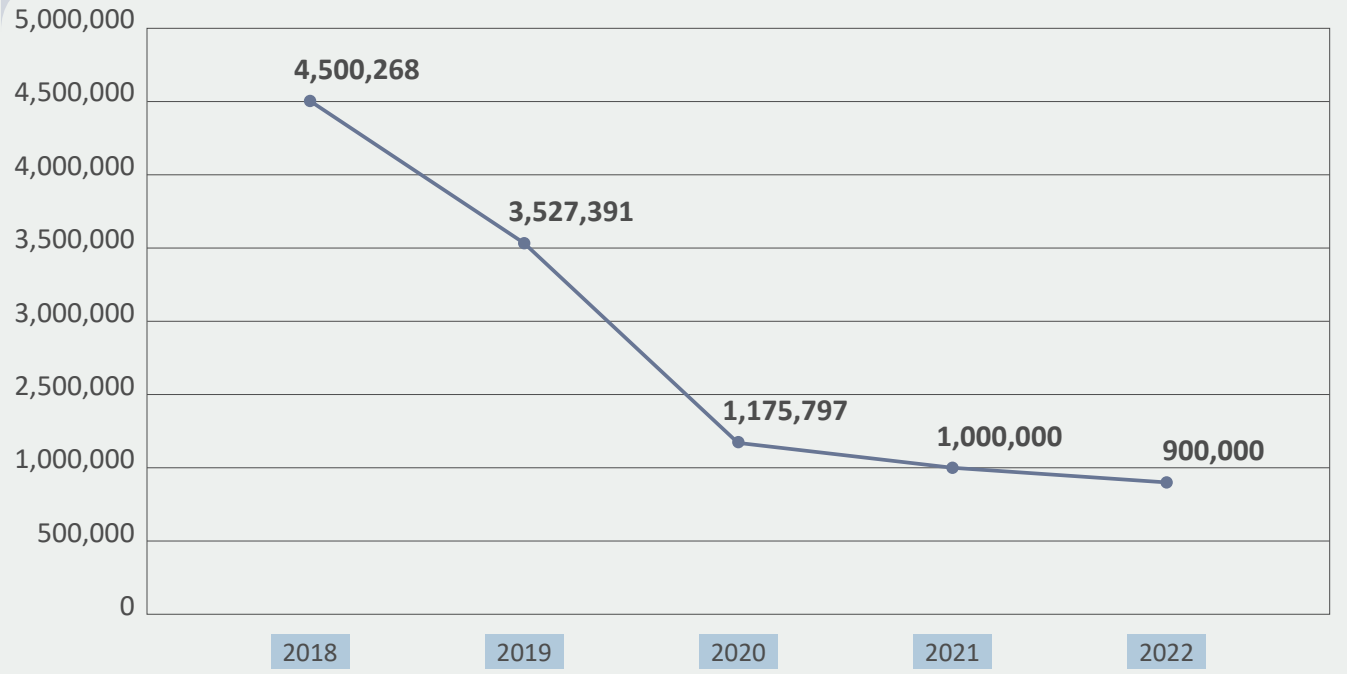


3.3 Προληπτικές Ειδοποιήσεις (Alerts)

Μια από τις σημαντικότερες δραστηριότητες του Εθνικού CSIRT-CY είναι η συλλογή πληροφοριών για ευπάθειες με τη χρήση εξειδικευμένων πλατφόρμων (Cyber Threat Intelligence Platforms - CTIP) και η αποστολή σχετικών ειδοποιήσεων στις κρίσιμες υποδομές. Οι ειδοποιήσεις αυτές περιλαμβάνουν τις διευθύνσεις IP που έχουν εντοπιστεί ως ύποπτες, καθώς και τις κατηγορίες συμβάντων (events) στις οποίες ανήκουν αυτά τα καταγεγραμμένα συμβάντα. Οι αναφορές αυτές και το περιεχόμενό τους είναι σημαντικά για την προσπάθεια πρόληψης πιθανών κυβερνοεπιθέσεων. Με την αποστολή των ειδοποιήσεων, οι φορείς που διαχειρίζονται τις κρίσιμες υποδομές ενημερώνονται για τις ύποπτες δραστηριότητες που εντοπίζονται, προσφέροντας τους τη δυνατότητα να λάβουν τα απαραίτητα μέτρα ασφάλειας για την προστασία των υποδομών τους από δυνητικές κυβερνοεπιθέσεις και να αποτρέψουν τυχόν αρνητικές επιπτώσεις. Οι ειδοποιήσεις αυτές αποτελούν σημαντικό εργαλείο για την ενίσχυση της κυβερνοασφάλειας και την προαγωγή της πρόληψης και αντίδρασης πιθανών κυβερνοεπιθέσεων.

Σύμφωνα με το Γράφημα 6, το έτος 2022 έχουν κοινοποιηθεί 900,000 ειδοποιήσεις ευπαθειών προς τους φορείς κρίσιμων υποδομών. Από το παρακάτω Γράφημα συμπεράνουμε μια αξιόλογη βελτίωση στη θωράκιση του εθνικού κυβερνοχώρου και της ευρύτερης κυβερνοασφάλειας, κάτι το οποίο χρήζει περαιτέρω βελτίωσης μέσα από την ενεργότερη εμπλοκή των κρίσιμων υποδομών με την 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

Το Εθνικό CSIRT-CY διασφαλίζει ότι η υποδομή του αναπτύσσεται και εκσυγχρονίζεται διαρκώς, σύμφωνα με τις τελευταίες κατευθυντήριες γραμμές και πρότυπα σχετικά με την κυβερνοασφάλεια που εκδίδουν οι οργανισμοί της Ευρωπαϊκής Ένωσης. Σε αυτό το πλαίσιο, εντός του 2022, αποκτήθηκαν εξειδικευμένα εργαλεία τα οποία βοηθούν στην πραγματοποίηση συστηματικών ελέγχων στις κρίσιμες υποδομές πληροφοριών της Κυπριακής Δημοκρατίας. Με αυτό τον τρόπο επιτυγχάνεται η εκτίμηση του επιπέδου ασφάλειας των κρίσιμων υποδομών πληροφοριών και ο εντοπισμός αδυναμιών και ευπαθειών, έτσι ώστε να γίνονται οι απαραίτητες συστάσεις για τη συνεχή ενίσχυση των μέτρων που λαμβάνουν οι υποδομές.

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

- Εξειδικευμένους αισθητήρες, με τη χρήση των οποίων πραγματοποιούνται έλεγχοι ασφάλειας στα δίκτυα των κρίσιμων υποδομών πληροφοριών σε πραγματικό χρόνο. Οι αισθητήρες εγκαταστάθηκαν στο πλαίσιο του ερευνητικού προγράμματος SENTINEL, σε συνεργασία με το Ανοικτό Πανεπιστήμιο Κύπρου και ελέγχονται από την υποδομή του Security Operations Centre (SOC) του Εθνικού CSIRT. Οι αισθητήρες 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.
- Δοκιμές διείσδυσης (penetration testing), που αποτελεί μια τεχνική ασφαλείας υπολογιστών μέσω της οποίας εντοπίζονται ευπάθειες στα συστήματα, τα δίκτυα και τις εφαρμογές ενός οργανισμού. Η διαδικασία των δοκιμών διείσδυσης αποτελείται από τέσσερα βασικά στάδια: συλλογή πληροφοριών, σάρωση δικτύου και ευπαθειών, απόκτηση και διατήρηση πρόσβασης και τελική ανάλυση και αναφορά.

Στόχος των δοκιμών είναι να βοηθήσουν στην προστασία του οργανισμού από επιθέσεις και να διασφαλιστεί 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.

- Σε εξέλιξη βρίσκεται το έργο ανάπτυξης της πλατφόρμας CTIP (Cyber Threat Intelligence Platform), σε συνεργασία με το Πανεπιστήμιο Κύπρου. Μέσω της πλατφόρμας CTIP θα πραγματοποιείται καθημερινή σάρωση του εθνικού διαδικτυακού χώρου (IPv4/IPv6) που είναι προσβάσιμος από το Εθνικό CSIRT-CY, με σκοπό τη συλλογή, επεξεργασία και αποθήκευση δεδομένων που σχετίζονται με κακόβουλο λογισμικό και ευπάθειες υλικού ή λογισμικού. Η πλατφόρμα θα παρέχει στους χρήστες, μεταξύ άλλων, τη δυνατότητα τροποποίησης των ρυθμίσεων σάρωσης, επιλογής των πρωτοκόλλων που χρησιμοποιούνται, και εξαγωγής των αποθηκευμένων πληροφοριών σε μορφή αναφοράς. Το έργο αναμένεται να ολοκληρωθεί εντός του 2023.

3.5 Εκπαιδεύσεις Εθνικού CSIRT-CY

Για την ενίσχυση της ομάδας του Εθνικού CSIRT-CY και την συνεχή προστασία των συστημάτων της Κυπριακής Δημοκρατίας από κυβερνοεπιθέσεις, η ομάδα του Εθνικού CSIRT-CY εκπαιδεύεται συνεχώς. Οι εκπαιδεύσεις λαμβάνουν διάφορες μορφές, όπως η παρακολούθηση εργαστηρίων και σεμιναρίων εντός και εκτός Κύπρου και η συμμετοχή σε εγχώριες και πανευρωπαϊκές ασκήσεις.
Κάποιες εκπαιδευτικές δράσεις που συμμετείχε το προσωπικό του Εθνικού CSIRT-CY εντός του 2022 και ξεχωρίζουν είναι οι εξής:

- Συμμετοχή σε σεμινάριο ISO/IEC 27001:2022 - Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
- Συμμετοχή στην ετήσια εθνική άσκηση κυβερνοάμυνας ΠΑΝΟΠΤΗΣ 2022 που διοργάνωσε η Διεύθυνση Κυβερνοάμυνας (ΔΙΚΥΒ) του ΓΕΕΘΑ. Τα επεισόδια που εξεταστήκανε αφορούσαν Network Forensics, Malware Analysis and Windows & Linux Forensics.
- Συμμετοχή στην Πανευρωπαϊκή άσκηση Cyber Europe 2022 που διοργανώνει ο ENISA με την συμμετοχή όλων των Ευρωπαϊκών χωρών. Τη χρονιά αυτή το σενάριο που αναπτύχθηκε αφορούσε τον τομέα της Υγείας και συμπεριλάμβανε την εμπλοκή εθνικών CSIRTs, Αρχών Κυβερνοασφάλειας, Υπουργεία Υγείας, οργανισμούς υγειονομικής περίθαλψης (π.χ. νοσοκομεία/κλινικές), παρόχους υπηρεσιών ηλεκτρονικής υγείας και παρόχους ασφάλισης υγείας.
- Εκπαίδευση μέσω του Ευρωπαϊκού συγχρηματοδοτούμενου έργου Joint Cybersecurity Operations Platform (CEF-JCOP) (βλ. Ενότητα 9.1.1).
- Εκπαίδευση μέσω του Ευρωπαϊκού συγχρηματοδοτούμενου έργου Power System's Shield against complex iNcI²dents and extensive cyber and privacy attacks (PHOENi²X Project) (βλ. Ενότητα 9.1.2).

4. ΠΙΣΤΟΠΟΙΗΣΕΙΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

4.1 Ο Κανονισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια

Με την έκδοση του Κανονισμού 2019/881 της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, θεσμοθετήθηκε το Ευρωπαϊκό Πλαίσιο Πιστοποίησης Κυβερνοασφάλειας, το οποίο θεσπίστηκε με στόχο την αναβάθμιση του επιπέδου κυβερνοασφάλειας εντός της Ένωσης και επιτρέποντας εναρμονισμένη προσέγγιση των ευρωπαϊκών σχημάτων πιστοποίησης κυβερνοασφάλειας, με απώτερο στόχο τη δημιουργία ψηφιακής ενιαίας αγοράς για προϊόντα Τεχνολογίας Πληροφοριών και Επικοινωνίας (ΤΠΕ)- Information and Communication Technologies (ICT), υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ.

Οι εταιρίες που δραστηριοποιούνται στην Ευρωπαϊκή Ένωση θα επωφελούνται προαιρετικά (προς το παρόν) από την πιστοποίηση των προϊόντων, των διαδικασιών και υπηρεσιών τους σε ένα κράτος-μέλος μόνο, με την πιστοποίηση να αναγνωρίζεται επίσημα σε ολόκληρη την Ένωση. Αυτή η προσέγγιση διευκολύνει τις διασυνοριακές συναλλαγές των επιχειρήσεων και των αγοραστών, ώστε να κατανοούν καλύτερα τα χαρακτηριστικά ασφαλείας του προϊόντος ή της υπηρεσίας που αγοράζουν. Αναμένεται ότι το πρώτο σχήμα πιστοποίησης που θα ληφθεί υπόψη για χρήση στην αξιολόγηση προϊόντων και υπηρεσιών είναι το σχήμα για τα Κοινά Κριτήρια (Common Criteria - EUCC)[11]. Τα επόμενα σχήματα που θα εκδοθούν θα σχετίζονται με υπηρεσίες νεφοϋπολογιστικής, καθώς και τον εξοπλισμό και την υποδομή του δικτύου ηλεκτρονικών επικοινωνιών πέμπτης γενεάς (5G).

Ο Κανονισμός (ΕΕ) 2019/881 προϋποθέτει σχετικές απαιτήσεις όσον αφορά την εφαρμογή του Ευρωπαϊκού Πλαισίου Πιστοποίησης Κυβερνοασφάλειας σε εθνικό επίπεδο κράτους-μέλους. Στις σχετικές απαιτήσεις εμπίπτει η σύσταση της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας (ΕΑΠΚ National Cybersecurity Certification Authority - NCCA). Η Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας είναι αρμόδια για την εποπτεία και εφαρμογή των κανόνων που συγκαταλέγονται σε ευρωπαϊκά σχήματα πιστοποίησης κυβερνοασφάλειας στην επικράτεια της. Επίσης, είναι αρμόδια για την εξουσιοδότηση των Οργανισμών Αξιολόγησης Συμμόρφωσης (ΟΑΣ - Conformity Assessment Body – CAB) για ορισμένα είδη πιστοποιήσεων, και ηγείται των δραστηριοτήτων πιστοποίησης κυβερνοασφάλειας του εκάστοτε κράτους-μέλους.

4.2 Εθνικό Πλαίσιο και Δραστηριότητες

Η ΑΨΑ έχει οριστεί ως η αρμόδια Εθνική Αρχή Πιστοποιήσεων Κυβερνοασφάλειας (ΕΑΠΚ) από το Υπουργικό Συμβούλιο. Ρόλος της είναι να προωθήσει την εφαρμογή του πλαισίου πιστοποίησης στην Κύπρο, και εργάζεται για την πραγματοποίηση των απαραίτητων αλλαγών στην πρωτογενή της νομοθεσία (βλ. Ενότητα 2.2.1), ώστε να έχει τις κατάλληλες εξουσίες και αρχές για να εκπληρώσει τον ρόλο της ως ΕΑΠΚ.

Κύριο μέλημα της ΕΑΠΚ είναι να προάξει 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 πιστοποιήσεων και να επωφεληθεί με τα πλεονεκτήματα που θα ακολουθήσουν.

Εντός του 2022, η ΑΨΑ (με τους συνεργάτες της) ολοκλήρωσε και παρουσίασε τα αποτελέσματα για το πρώτο συγχρηματοδοτούμενο έργο B4C - Building up the Cybersecurity Certification Capabilities of Cyprus σε άλλες σχετικές αρχές των κρατών-μελών της Ευρωπαϊκής Ένωσης (Μάϊος 2022). Στόχος του έργου ήταν η ανάπτυξη των δυνατοτήτων της Κυπριακής Δημοκρατίας ώστε να μπορεί να προσφέρει ένα ευρύ φάσμα υπηρεσιών πιστοποίησης κυβερνοασφάλειας σε προϊόντα, υπηρεσίες και διαδικασίες. Ο ρόλος της ΑΨΑ είναι καθοριστικός καθώς θα έχει την εξουσία να επιβλέπει ολόκληρο το πλαίσιο

[11] 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.

πιστοποίησης στην Κύπρο και να παρακολουθεί την εφαρμογή του. Η ΑΨΑ θα υποστηρίζει και θα βοηθά επίσης το έργο του Κυπριακού Οργανισμού Προώθησης Ποιότητας (ΚΟΠΠ), ο οποίος είναι υπεύθυνος για τη διαπίστευση οργανισμών αξιολόγησης συμμόρφωσης στην Κύπρο και θα έχει τον ρόλο του Εθνικού Οργανισμού Διαπίστευσης.

Το 2022, η ΑΨΑ συνέχισε τις σχετικές δραστηριότητες ανάπτυξης της μέσω της συμμετοχής της στο επιπρόσθετο συγχρηματοδοτούμενο πρόγραμμα A4CEF - Advancing Cybersecurity Certification Capabilities with Cross Border Exchange and Enhancing (business) Flows. Το έργο αναμένεται να ολοκληρωθεί εντός του 2023, με επίκεντρο την περαιτέρω ανάπτυξη των δυνατοτήτων της ΑΨΑ και την επέκταση των δραστηριοτήτων της στον τομέα της πιστοποίησης κυβερνοασφάλειας (βλ. Ενότητα 9.1.3).

5. ΕΝΙΣΧΥΣΗ ΚΑΙ ΑΝΑΠΤΥΞΗ ΙΚΑΝΟΤΗΤΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΚΥΠΡΙΑΚΗ ΑΓΟΡΑ

5.1 Κανονισμός/Δημιουργία Εθνικού Κέντρου Συντονισμού Κυβερνοασφάλειας (NCC-CY)

Με τη θέσπιση του Κανονισμού (ΕΕ) 2021/887 για τη σύσταση του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας και του Δικτύου Εθνικών Κέντρων Συντονισμού, κάθε κράτος μέλος είχε την υποχρέωση μέχρι το τέλος του 2021 να ορίσει μια οντότητα η οποία θα ενεργεί ως το Εθνικό Κέντρο Συντονισμού με απώτερο σκοπό την ανάπτυξη της κυβερνοασφάλειας σε εθνικό επίπεδο. Κατόπιν απόφασης του Υπουργικού Συμβουλίου, η ΑΨΑ ορίστηκε ως το Εθνικό Κέντρο Συντονισμού (National Cybersecurity Coordination Centre - NCC-CY) για θέματα κυβερνοασφάλειας στην Κυπριακή Δημοκρατία. Παράλληλα, ορίστηκε το Ίδρυμα Έρευνας και Καινοτομίας (ΙδΕΚ) ως μέλος της κοινοπραξίας του NCC-CY με καθήκοντα οικονομικού διαχειριστή, υπεύθυνο για την διαχείριση και κατανομή των χρηματοδοτήσεων που θα εξασφαλίζει το NCC-CY μέσω των Ευρωπαϊκών προγραμμάτων για κατανομή σε τρίτα μέρη.

Με την ίδια απόφαση ορίστηκε και το Συμβούλιο του NCC-CY ως υπεύθυνο για τον καθορισμό του πλαισίου γενικής πολιτικής για την εφαρμογή του Κανονισμού στην Κυπριακή Δημοκρατία. Πρόεδρος του Συμβουλίου ορίστηκε ο Γενικός Διευθυντής του Υφυπουργείου Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής. Ως μέλη του Συμβουλίου, ορίστηκαν οι Γενικοί Διευθυντές των Υπουργείων Δικαιοσύνης, Εξωτερικών, Άμυνας, Οικονομικών, Παιδείας, Ενέργειας καθώς και ο Επίτροπος Επικοινωνιών και ο Πρόεδρος του Συμβουλίου του ΙδΕΚ ή οι εκπρόσωποι τους.

5.2 Ανάπτυξη του NCC-CY

Το NCC-CY έχει ως κύριο στόχο να διασφαλίσει ότι τα ενδιαφερόμενα μέρη και κυρίως οι μικρομεσαίες επιχειρήσεις (ΜμΕ) έχουν επαρκή υποστήριξη και πρόσβαση στη γνώση και στα αποτελέσματα της έρευνας και ανάπτυξης στον τομέα της κυβερνοασφάλειας. Στο πλαίσιο αυτής της αποστολής, είναι προτεραιότητα η παροχή βοήθειας σε ΜμΕ στην Κύπρο ώστε να είναι ενεργές, ανταγωνιστικές και ικανές να συνεισφέρουν σημαντικά στην ηγετική θέση της Ευρωπαϊκής Ένωσης στον τομέα της κυβερνασφάλειας.

Στις 17 Φεβρουαρίου 2022, υποβλήθηκε αίτημα στην Ευρωπαϊκή Επιτροπή για την αξιολόγηση της ικανότητας του NCC-CY να διαχειρίζεται μελλοντικά Ευρωπαϊκά κονδύλια. Στις 4 Μαΐου 2022, το NCC-CY έλαβε επιτυχώς τη σχετική έγκριση από την Ευρωπαϊκή Επιτροπή, η οποία του επιτρέπει όπως διεκδικεί και διαχειρίζεται σημαντικά Ευρωπαϊκά κονδύλια για διοχέτευση στην Κυπριακή αγορά. Κατόπιν ανακοινώσεως της δράσης «Deploying The Network of National Coordination Centres With Member States», το NCC-CY ετοίμασε ολοκληρωμένη πρόταση για συγχρηματοδότηση μέσω του προγράμματος «Ψηφιακή Ευρώπη» (Digital Europe Programme – DEP). Συγκεκριμένα, στις 31 Μαΐου 2022, το NCC-CY υπέβαλε πρόταση για την ανάπτυξη του NCC-CY για θέματα κυβερνοασφάλειας στην Κυπριακή Δημοκρατία. Στις 22 Αυγούστου 2022, λήφθηκε απάντηση πως η πρόταση ήταν επιτυχής. Ο συνολικός προϋπολογισμός του έργου ανέρχεται στα €2.558.370, με συνεισφορά του DEP το 50% και το υπόλοιπο 50% από την ΑΨΑ. Από το συνολικό προϋπολογισμό το ποσό του €1,000,000 θα δοθεί ως χρηματοδότηση υπό μορφή χορηγιών (βλ. επίσης Ενότητα 9.2.1).

Το NCC-CY πέτυχε να είναι ένα από τα πρώτα πέντε Εθνικά Κέντρα Συντονισμού από όλη την Ευρώπη που έλαβε έγκριση για συγχρηματοδότηση από την Ευρωπαϊκή Επιτροπή, το οποίο αποτελεί σημαντικό επίτευγμα. Στα πλαίσια αυτής της δράσης, το NCC-CY είναι έτοιμο ώστε να κατανέμει στην επόμενη διετία χρηματοδοτήσεις στο εθνικό οικοσύστημα κυβερνοασφάλειας. Εντός του 2022, και μέσω αυτής της πρότασης, το NCC-CY προχώρησε σε πλήρη προγραμματισμό του συνόλου των δραστηριοτήτων

του για τα έτη 2023-24. Εντός του 2023, το NCC-CY θα ξεκινήσει την οικονομική ενίσχυση υπό την μορφή επιχορηγήσεων, κυρίως σε μικρομεσαίες επιχειρήσεις. Επιπλέον, θα δημιουργήσει ένα σχήμα πιστοποίησης προσαρμοσμένο κυρίως για τις ΜμΕ όπου μια οντότητα θα μπορεί να αιτηθεί επιχορήγηση για την εφαρμογή του. Το σχήμα πιστοποίησης θα αποτελείται από ένα πλαίσιο κριτηρίων και διαδικασιών ελέγχου, το οποίο θα εξασφαλίζει ένα επαρκές επίπεδο κυβερναοσφάλειας, με έμφαση στη βασική κυβερνο-υγιεινή.

Επιπρόσθετα, θα ενεργεί ως σημείο επαφής σε εθνικό επίπεδο για την Κοινότητα Κυβερνοασφάλειας. Η Κοινότητα συγκεντρώνει ενδιαφερόμενα μέρη από τον ιδιωτικό τομέα, τον δημόσιο τομέα, τη βιομηχανία, τον ακαδημαϊκό χώρο και την έρευνα, συνδυάζοντας γνώση, ικανότητα και εμπειρία σε θέματα κυβερνοασφάλειας. Παράλληλα, 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. Το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας θα αξιολογεί την αίτηση ένταξης μέλους στην Κοινότητα για επιβεβαίωση ότι πληρούνται τα απαιτούμενα κριτήρια ένταξης. Επιπλέον, θα δημιουργήσει και τη Συμβουλευτική Επιτροπή του NCC-CY, με στόχο την αποτελεσματική επικοινωνία μεταξύ του NCC-CY και των εκπροσώπων της Κοινότητας. Στόχος είναι, η συνεχής παροχή συμβουλών και ανατροφοδότησης προκειμένου να βελτιωθεί και να ενισχυθεί η λειτουργικότητα του NCC-CY.

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. 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. Έπειτα από αξιολόγηση ωριμότητας σε εθνικό επίπεδο, που διενεργήθηκε από το Πανεπιστήμιο της Οξφόρδης το 2017 (βλ. Ενότητα 6.2), καθώς και αλλαγές στη σχετική Ευρωπαϊκή Στρατηγική και τη συσσωρευμένη εμπειρία από την υλοποίηση της, αναθεωρήθηκε η Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, με την έκδοση της δεύτερης Στρατηγικής τον Δεκέμβριο 2020.

Μετά τη δημιουργία των αρμοδίων σωμάτων και ομάδων κατά το 2021 για τη διακυβέρνηση της Στρατηγικής, συνεχίστηκαν οι εργασίες συντονισμού κατά το 2022, μέσω της πραγματοποίησης δύο (2) συνεδριών της Συντονιστικής Επιτροπής Κυβερνοασφάλειας και μιας (1) συνεδρίας του Εθνικού Συμβουλίου Κυβερνοασφάλειας. Η παρούσα έκδοση της Στρατηγικής έχει χρονικό ορίζοντα υλοποίησης μέχρι το τέλος του 2024.

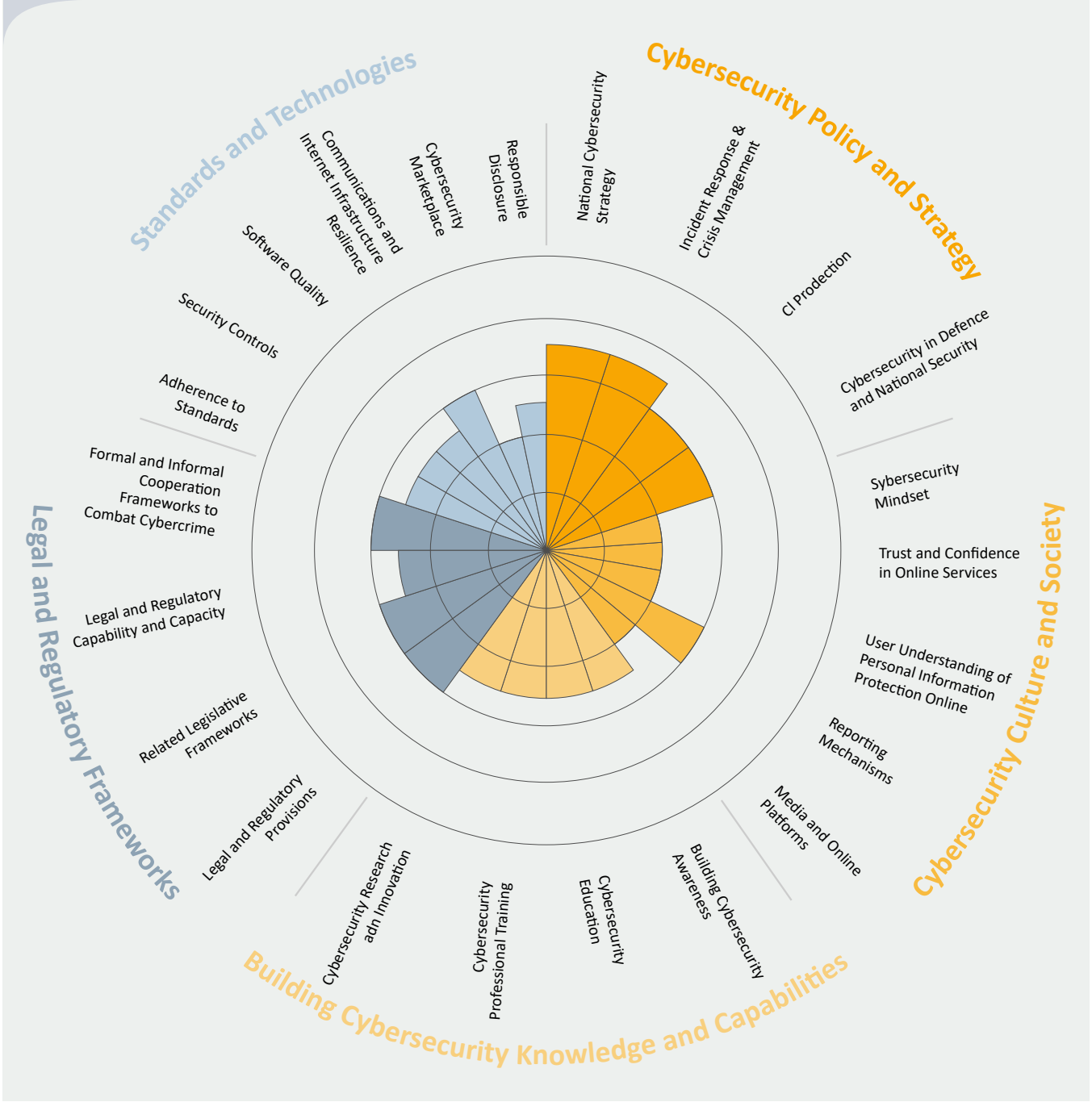
Δεδομένης της ψήφισης της νέας Ευρωπαϊκής Οδηγίας NIS2 (βλ. Ενότητα 2.2.4), όπου απαιτείται η συμπερίληψη νέων προνοιών στις Στρατηγικές των κρατών μελών της Ευρωπαϊκής Ένωσης, και με το πέρας του χρονικού ορίζοντα υλοποίησης της παρούσας εθνικής Στρατηγικής, η ΑΨΑ προγραμματίζει αναθεώρηση της Στρατηγικής με σκοπό την έγκριση της 3ης έκδοσης, μέχρι το τέλος του 2024.

6.2 Διεξαγωγή Αξιολόγησης Ωριμότητας Κυβερνοασφάλειας για την Κυπριακή Δημοκρατία

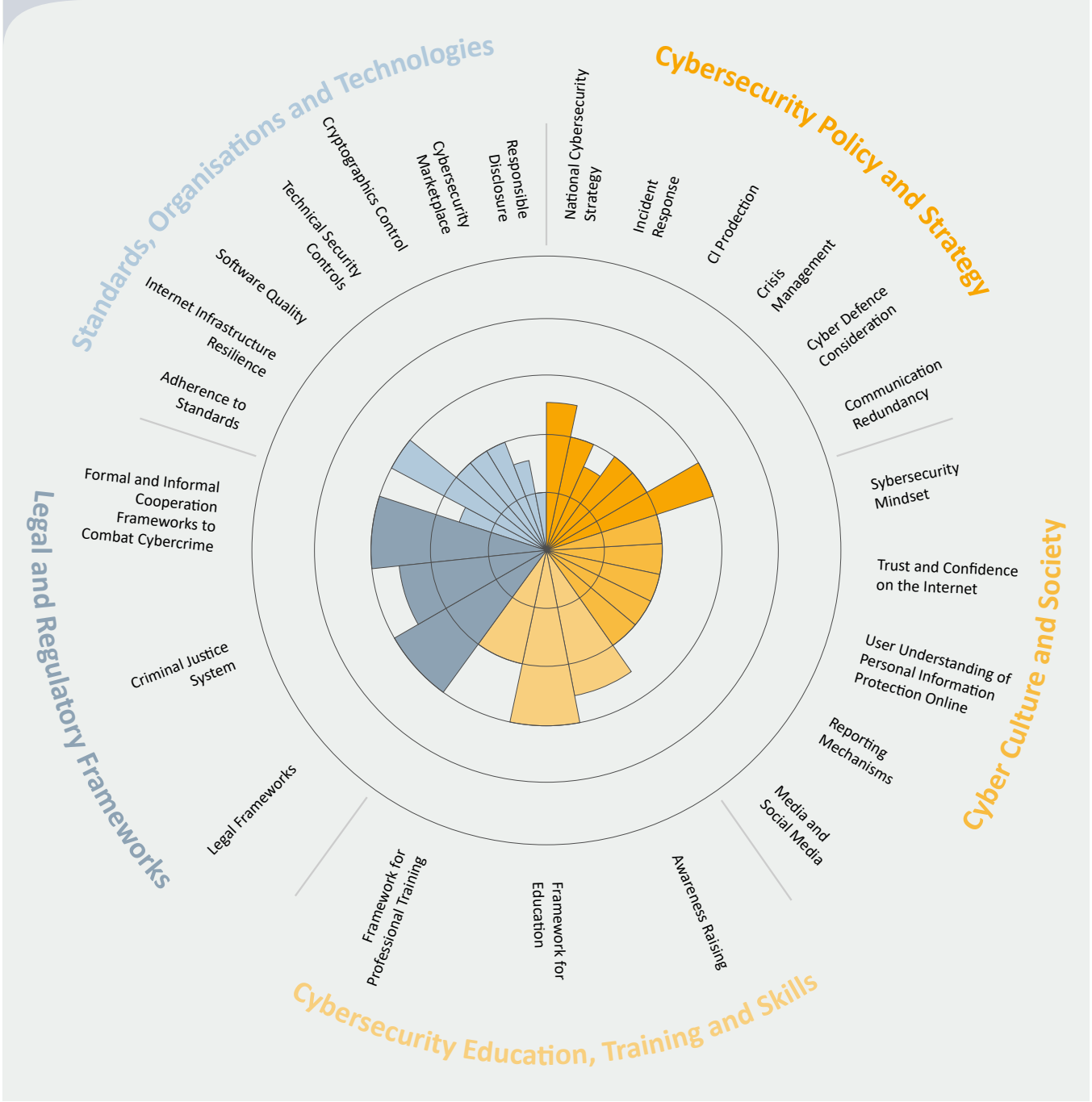
Η ΑΨΑ ξεκίνησε τον Ιούλιο 2021, έργο αξιολόγησης ωριμότητας κυβερνοασφάλειας με το Πανεπιστήμιο της Οξφόρδης, για επικαιροποίηση των αποτελεσμάτων της προηγούμενης αξιολόγησης που διενεργήθηκε το 2017, λαμβάνοντας υπόψη τις σημαντικές εξελίξεις και τα επιτεύγματα των τελευταίων χρόνων που έχει πετύχει η Κυπριακή Δημοκρατία, όπως τη δημιουργία της ΑΨΑ και του Εθνικού CSIRT-CY. Η διαδικασία αυτή διενεργήθηκε με βάση το επιστημονικό μοντέλο που αναπτύχθηκε από το Πανεπιστήμιο της Οξφόρδης (Capacity Maturity Model for Nations – CMM). Οι σχετικές αξιολογήσεις έχουν ως σκοπό την καλύτερη κατανόηση του επιπέδου ωριμότητας της Κύπρου στην κυβερνοασφάλεια, και περιλαμβάνουν μεγάλο αριθμό σχετικών συστάσεων για την περαιτέρω βελτίωση της ωριμότητας της χώρας στα πολύ σημαντικά αυτά θέματα.

Κατά το 2022, ολοκληρώθηκε η εν λόγω μελέτη, η οποία έδειξε σημαντικές βελτιώσεις στους τομείς αρμοδιότητας της ΑΨΑ, όπως φαίνεται στην αποτύπωση στο Γράφημα 7 (έναντι της αποτύπωσης στο Γράφημα 8). Τα Γραφήματα αυτά δείχνουν το επίπεδο ωριμότητας σε σειρά τομέων και υπο-τομέων που σχετίζονται με την κυβερνοασφάλεια, όπως θέματα πολιτικής και στρατηγικής, κουλτούρας στην κοινωνία, ανάπτυξη γνώσεων και ικανοτήτων, νομικά και ρυθμιστικά πλαίσια, και χρήση προτύπων και τεχνολογιών.

Γράφημα 7: Αποτύπωση των επιπέδων ωριμότητας κυβερνοασφάλειας της Κυπριακής Δημοκρατίας (2022)



Γράφημα 8: Αποτύπωση των επιπέδων ωριμότητας κυβερνοασφάλειας της Κυπριακής Δημοκρατίας (2017)



6.3 Υλοποίηση Δράσεων Στρατηγικής Κυβερνοασφάλειας

6.3.1 Θεματική Ενότητα 1 – Δομές και Διακυβέρνηση

Η παρούσα Θεματική Ενότητα αναφέρεται στα αρμόδια σώματα και ομάδες που έχουν δημιουργηθεί για την υλοποίηση της Στρατηγικής και την αντιμετώπιση των προκλήσεων κυβερνοασφάλειας από την Κυπριακή Δημοκρατία. Σε αυτό το πλαίσιο, έχει δημιουργηθεί το Εθνικό Συμβούλιο Κυβερνοασφάλειας, το οποίο αποτελείται από εκπροσώπους των κύριων αρμόδιων αρχών σε υψηλό βαθμό, όπως Υπουργούς, Διοικητές και Επιτρόπους. Το Εθνικό Συμβούλιο Κυβερνοασφάλειας παρακολουθεί την πρόοδο της υλοποίησης της Στρατηγικής σε τακτά χρονικά διαστήματα, ενημερώνεται για την τρέχουσα κατάσταση της κυβερνοασφάλειας στην Κύπρο και δίνει κατευθυντήριες γραμμές για τη βελτίωση της κυβερνοασφάλειας στη χώρα.

Έχει δημιουργηθεί επίσης η Συντονιστική Επιτροπή Κυβερνοασφάλειας, η οποία απαρτίζεται από εκπροσώπους των εμπλεκόμενων Αρχών, όπως στο Εθνικό Συμβούλιο Κυβερνοασφάλειας. Συγκεκριμένα, συμμετέχουν εκπρόσωποι από τις Γενικές Διευθύνσεις ή/και τις Διευθύνσεις Υπηρεσιών ή/και τους υπευθύνους τομέων ή/και τους εξουσιοδοτημένους εκπροσώπους τους. Στο πλαίσιο αυτής της Επιτροπής διασφαλίζεται η συνεργασία μεταξύ των αρμοδίων αρχών της Δημοκρατίας, έτσι ώστε να αξιοποιούνται στο έπακρο οι γνώσεις των ειδικών και των τεχνοκρατών σε κάθε Αρχή, και να παρακολουθείται η υλοποίηση της Στρατηγικής στο σύνολο της.

6.3.2 Θεματική Ενότητα 2 – Θεσμοθέτηση της συνεργασίας μεταξύ αρμόδιων δημόσιων φορέων

Η παρούσα Θεματική Ενότητα έχει θεσμοθετήσει μηχανισμό για το συντονισμό και αποτελεσματική επικοινωνία μεταξύ Υπουργείων, Αρμόδιων Αρχών και εμπλεκόμενων Υπηρεσιών με στόχο να επιτευχθεί η βέλτιστη υλοποίηση των δράσεων της Εθνικής Στρατηγικής, με βάση τις δομές που συστάθηκαν στη Θεματική Ενότητα 1.

Εντός του 2022, υποβλήθηκε αριθμός παραδοτέων από ομάδες εργασίας των Θεματικών Ενοτήτων. Η ΑΨΑ συνεχίζει την συνεργασία της με όλους τους εμπλεκόμενους φορείς, και όπου κρίνεται απαραίτητο αξιολογείται η εισαγωγή επιπροσθέτων εμπλεκόμενων φορέων για υλοποίηση και διεκπεραίωση των δραστηριοτήτων που προβλέπονται στα εκάστοτε σχέδια δράσεων.

6.3.3 Θεματική Ενότητα 3 – Νομικό, Ρυθμιστικό και Πολιτικό Πλαίσιο

Η παρούσα Θεματική Ενότητα αποσκοπεί στην πλήρη υλοποίηση των προνοιών και του ρυθμιστικού πλαισίου της Οδηγίας NIS, αλλά και στην ενίσχυση του υφιστάμενου νομικού, κανονιστικού και ρυθμιστικού πλαισίου για την πλήρη ενεργοποίηση και υποστήριξη των προνοιών της Στρατηγικής Κυβερνοασφάλειας, με ανάπτυξη νέων νομοθεσιών, όπου απαιτείται. Σχετικές εξελίξεις εντός του 2022, όσον αφορά στις νομοθεσίες της Αρχής, συνοψίζονται στην Ενότητα 2.2.

6.3.4 Θεματική Ενότητα 4 – 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. Έχει ως στόχο τον καθορισμό του τρόπου με τον οποίο οι διάφορες Υπηρεσίες και Τμήματα της Δημόσιας Υπηρεσίας, αλλά και οι χειριστές κρίσιμων υποδομών πληροφοριών, προσεγγίζουν την ανάπτυξη της ασφάλειας τους και τη διαχείριση σχετικών κινδύνων και θεμάτων επιχειρησιακής συνέχειας. Στόχος είναι η ουσιαστική συμβολή του στην πρόληψη συμβάντων και περιστατικών στον κυβερνοχώρο, καθώς και στη σημαντική αναβάθμιση των επιπέδων κυβερνοασφάλειας σε ολόκληρη τη χώρα.

Εντός του 2022, αναπτύχθηκαν τομεακά μέτρα ασφάλειας για τις ηλεκτρονικές επικοινωνίες και

ενημέρωση του πλαισίου που αφορά την υποβολή περιστατικών κυβερνοασφάλειας στην ΑΨΑ (βλ. Ενότητα 2.2.3). Επίσης, η ΑΨΑ προβαίνει σε συνεχή αξιολόγηση των νέων κατευθυντήριων γραμμών που εκδίδονται από τον ENISA, και του τρόπου αξιοποίησης τους με ενδεχόμενη εισαγωγή τους στο Εθνικό Πλαίσιο Κυβερνοασφάλειας, κατά περίπτωση.

Εντός του 2023, και στα πλαίσια των εργασιών του Εθνικού Κέντρου Συντονισμού Κυβερνοασφάλειας, το Εθνικό Πλαίσιο Κυβερνοασφάλειας θα εμπλουτιστεί με τη δημιουργία πλαισίου και σχήματος πιστοποίησης κυβερνο-υγιεινής για τις μικρομεσαίες επιχειρήσεις (βλ. Ενότητα 5).

6.3.5 Θεματική Ενότητα 5 – Αξιολόγηση και Διαχείριση Κινδύνων και Αξιολόγηση Κρισιμότητας

Η παρούσα Θεματική Ενότητα πραγματεύεται την ανάγκη για ολοκληρωμένη προσέγγιση στην αναγνώριση, αξιολόγηση και διαχείριση κινδύνων κυβερνοασφάλειας, με έμφαση στην κατανόηση και αξιολόγηση κρισιμότητας υποδομών και φορέων. Όπως αναφέρεται στην Ενότητα 2.2.4, προγραμματίζεται αναθεώρηση της διαδικασίας αξιολόγησης (με βάση τις πρόνοιες της νέας Οδηγίας NIS2) και διενέργεια της επόμενης αξιολόγησης κρισιμότητας εντός του 2024.

Εντός του 2023, παράλληλα με τη μελέτη της Οδηγίας NIS2, θα μελετηθεί η ανάγκη αναθεώρησης της εθνικής μεθοδολογίας αξιολόγησης κινδύνων κυβερνοασφάλειας, λαμβάνοντας υπόψη τις αναθεωρημένες πρόνοιες της Οδηγίας, καθώς και τη διασύνδεση με νέες νομοθετικές ρυθμίσεις σε Ευρωπαϊκό επίπεδο, όπως τη νέα Οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων[12].

6.3.6 Θεματική Ενότητα 6 – Αντιμετώπιση Συμβάντων και Διαχείριση Κρίσεων

Η παρούσα Θεματική Ενότητα αποσκοπεί στη διασφάλιση δυνατοτήτων διαχείρισης περιστατικών μέσω ανάπτυξης ικανοτήτων σε εθνικό και τομεακό επίπεδο. Στο πλαίσιο αυτό έχει γινεί η σύσταση, λειτουργία και εποπτεία των Ομάδων Διαχείρισης Περιστατικών Κυβερνοασφάλειας (CSIRTs) σε εθνικό, κυβερνητικό και τομεακό επίπεδο. Επίσης έχει θεσμοθετηθεί η συνεργασία των αρμοδίων αρχών σε εθνικό επίπεδο, καθώς και η συμμετοχή σε ευρωπαϊκά και διεθνή δίκτυα, όπως το CSIRTs Network, το EU CyCLONe, κ.ά., συμβάλλοντας στην αποτελεσματική αντιμετώπιση των κυβερνοαπειλών και της εγκληματικότητας στον κυβερνοχώρο σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο (βλ. Ενότητα 3).

Επιπρόσθετα, περιλαμβάνει τη διαμόρφωση και εφαρμογή σχεδίων διαχείρισης κρίσεων στον τομέα της κυβερνοασφάλειας. Συγκεκριμένα, εντός του 2022 δρομολογήθηκε η δημιουργία και εφαρμογή εθνικών σχεδίων έκτακτης ανάγκης για την κυβερνοασφάλεια (π.χ. πλαίσια ΖΗΝΩΝ και ΚΥΠΣΕΑ) όπως επίσης και Σχεδίων Διαχείρισης Έκτακτης Ανάγκης (Contingency Plans). Το Εθνικό Συμβούλιο Κυβερνοασφάλειας αποφάσισε όπως η ΑΨΑ ετοιμάσει ένα μηχανισμό διαχείρισης κρίσεως στο μοντέλο της ΕΕ, με την δημιουργία ενός πλαισίου λειτουργείας που θα αποτελείται από τα σχέδια διαχείρισης κρίσεων κυβερνοασφάλειας που θα αναπτυχθούν, ενός ταμείου οικονομικής υποστήριξης και μιας Ειδικής Ομάδας Έκτακτης Ανάγκης που θα απαρτίζεται από εμπειρογνώμονες του δημοσίου και ιδιωτικού τομέα.

6.3.7 Θεματική Ενότητα 7 – 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.

[12] *https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32022L2557 – Οδηγία (ΕΕ) 2022/2557 για την ανθεκτικότητα των κρίσιμων οντοτήτων*

Κατά το έτος 2022 έχουν πραγματοποιηθεί εκπαιδεύσεις τύπου 'Train the Trainer' με θέμα την ευαισθητοποίηση (awareness) σε συνεργασία με το Τμήμα Κυβερνοάμυνας του ΥΠΑΜ. Επίσης έχουν πραγματοποιηθεί εκπαιδεύσεις σε κρίσιμες υποδομές πληροφοριών, και επιπρόσθετα έγινε διοργάνωση τακτικών εθνικών ασκήσεων στη βάση ρεαλιστικών σεναρίων, με ταυτόχρονη ενεργή συμμετοχή σε Πανευρωπαϊκές και άλλες διεθνείς ασκήσεις (βλ. Ενότητα 8).

6.3.8 Θεματική Ενότητα 8 – Ανταλλαγή Πληροφοριών – Επίγνωση Κατάστασης

Η παρούσα Θεματική Ενότητα αποσκοπεί στην δημιουργία συνεργασίας και ανταλλαγής πληροφοριών ανάμεσα σε οργανισμούς και την ΑΨΑ, με σκοπό να επιτευχθεί αποτελεσματικότερη ενημέρωση και συντονισμός για την αντιμετώπιση απειλών και συμβάντων στον κυβερνοχώρο. Επιπλέον, έχει ως στόχο τη δημιουργία ενός δυναμικού PPP (Public Private Partnership) στον τομέα της ανταλλαγής πληροφοριών, με τη συμμετοχή όλων των εμπλεκόμενων φορέων κρίσιμων υποδομών πληροφοριών και των αρμοδίων αρχών του κράτους. Η επίγνωση της κατάστασης της κυβερνοασφάλειας απαιτεί συνεχή και λεπτομερή παρακολούθηση των τρεχουσών απειλών στον κυβερνοχώρο.

Επίσης, δημιουργούνται αποδοτικοί μηχανισμοί ανταλλαγής πληροφοριών σε πραγματικό χρόνο, που επιτρέπουν την ταχεία ανταπόκριση σε πιθανές απειλές και την αντιμετώπισή τους. Παράλληλα, γίνεται συνεχής αναβάθμιση του επιπέδου ετοιμότητας και της ικανότητας αντιμετώπισης των θεμάτων κυβερνοασφάλειας, κυβερνοεγκλήματος, κυβερνοάμυνας και διεθνούς συνεργασίας σε σχετικά θέματα, με την χρήση των πιο σύγχρονων τεχνολογιών και πρακτικών.

6.3.9 Θεματική Ενότητα 9 – 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. Περιλαμβάνει ενημέρωση και ευαισθητοποίηση μεγάλου εύρους χρηστών αυτών των συστημάτων και υπηρεσιών, με τις απαραίτητες γνώσεις, στάσεις και δεξιότητες, προκειμένου να επιτευχθεί ένα ικανοποιητικό επίπεδο ενημέρωσης και επιμόρφωσης που αφορά πιθανές απειλές κυβερνοασφάλειας.

Η ΑΨΑ κατά το έτος 2022 έχει πραγματοποιήσει εκπαιδεύσεις και ενημερωτικές ημερίδες σχετικά με την ανάπτυξη των δεξιοτήτων 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).

6.3.10 Θεματική Ενότητα 10 – 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, σε στενή συνεργασία με το Παιδαγωγικό Ινστιτούτο του Υπουργείου Παιδείας, κατά το έτος 2022, είχε ενεργό ρόλο στην υλοποίηση των δράσεων στα θέματα που αφορούν την κατάρτιση και πιστοποίηση όπως αυτές προκύπτουν από το σχετικό πρόγραμμα εργασίας. Επιπλέον, δρομολογείται η διαδικασία προκειμένου να καταρτιστούν τα προφίλ των αποφοίτων και των επαγγελματιών και να καθοριστούν, με σαφήνεια, οι γνώσεις και δεξιότητες που απαιτούνται σε θέματα κυβερνοασφάλειας. Επίσης έγινε αναθεώρηση του προγράμματος εργασίας, καθώς και συζητήσεις με τους άλλους Συντονιστές (Παιδαγωγικό Ινστιτούτο και Διεύθυνση Ανώτερης Εκπαίδευσης του Υπουργείου Παιδείας).

6.3.11 Θεματική Ενότητα 11 – Έρευνα και Καινοτομία

Η παρούσα Θεματική Ενότητα πραγματεύεται την υποστήριξη και την προώθηση της έρευνας και καινοτομίας στον τομέα της κυβερνοασφάλειας στην Κυπριακή Δημοκρατία, καθώς και τον σχεδιασμό και την ανάπτυξη "οικοσυστημάτων" για την αξιοποίηση των συνεργειών που δημιουργούνται από τη δεσπόζουσα θέση της Κύπρου σε τομείς με αυξημένη δραστηριότητα, όπως για παράδειγμα οι οικονομικές υπηρεσίες, η ναυτιλία και η ενέργεια. Στόχος είναι επίσης η προσέλκυση τεχνολογικών εταιρειών με ενεργή ενασχόληση σε θέματα κυβερνοασφάλειας και η ενεργοποίησή τους στην Κύπρο.

Εντός του 2022, και έπειτα από απόφαση Υπουργικού Συμβουλίου όπου ορίστηκε η ΑΨΑ ως το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας, αναπτύχθηκε ολοκληρωμένο πρόγραμμα εργασιών για τα έτη 2023-24, για το οποίο η Αρχή πέτυχε σημαντική Ευρωπαϊκή χρηματοδότηση (βλ. Ενότητα 5).

6.3.12 Θεματική Ενότητα 12 – Συνεργασία με τον Ιδιωτικό Τομέα

Η παρούσα Θεματική Ενότητα αφορά τη δημιουργία επίσημης εταιρικής σχέσης δημόσιου-ιδιωτικού τομέα (PPP - Public Private Partnership), η οποία κρίνεται απαραίτητη για την ενίσχυση της εμπιστοσύνης μεταξύ των επιχειρήσεων, της βιομηχανίας και της κυβέρνησης στα θέματα της ασφάλειας δικτύων και πληροφοριών. Επιπρόσθετα, θα λειτουργήσει ως μέσο για την αποτελεσματική προστασία των κρίσιμων υποδομών και τη διαχείριση των κινδύνων ασφαλείας τόσο βραχυπρόθεσμα όσο και μακροπρόθεσμα.

Κατά το έτος 2022 πραγματοποιήθηκαν συναντήσεις με το Κυπριακό Εμπορικό και Βιομηχανικό Επιμελητήριο (ΚΕΒΕ), όπου παρουσιάστηκαν τα αποτελέσματα έρευνας που πραγματοποίησε η ΑΨΑ για την καταγραφή των αναγκών των επιχειρήσεων για την πραγματοποίηση εκπαιδευτικών σεμιναρίων κατάρτισης, όπως επίσης και τα αποτελέσματα του Ευρωβαρόμετρού σχετικά με την κυβερνοασφάλεια στις μικρομεσαίες επιχειρήσεις (βλ. Ενότητα 10). Συζητήθηκε το πλαίσιο συνεργασίας ΑΨΑ-ΚΕΒΕ και δρομολογήθηκαν οι επόμενες ενέργειες που θα πραγματοποιηθούν από κοινού, όπως μεταξύ άλλων την προώθηση του θεσμού του Cybersecurity Made In Europe Label[13] στην Κύπρο, την πραγματοποίηση εκπαιδευτικών σεμιναρίων και σεμιναρίων κατάρτισης σε θέματα κυβερνοασφάλειας για τις επιχειρήσεις, και τον καθορισμό λίστας επιχειρήσεων οι οποίες επιθυμούν να λαμβάνουν συχνές ενημερώσεις για θέματα κυβερνοασφάλειας.

6.3.13 Θεματική Ενότητα 13 – 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.

Η ΑΨΑ έχει οριστεί ως η Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας, τμήμα το οποίο στελεχώθηκε κατά το 2022 και το οποίο παρακολουθεί στενά τις σχετικές εξελίξεις σε Ευρωπαϊκό επίπεδο. Τα πρώτα Ευρωπαϊκά σχήματα πιστοποίησης αναμένονται να εκδοθούν εντός του 2023 καλύπτοντας την κυβερνοασφάλεια σε προϊόντα και υπηρεσίες, καθώς και στη νεφοϋπολογιστική και στις τεχνολογίες κινητής τηλεφωνίας 5G (βλ. Ενότητα 4).

6.3.14 Θεματική Ενότητα 14 – 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.

[13] https://www.digitalsme.eu/cybersecurity-label/

Η ΑΨΑ ως η αρμόδια αρχή για την εφαρμογή της Οδηγίας NIS στην Κύπρο (βλ. Ενότητα 2), παρακολουθεί συνεχώς τις εξελίξεις σε Ευρωπαϊκό επίπεδο και προωθεί τις θέσεις της Κυπριακής Δημοκρατίας, μέσω της συμμετοχής της στις ομάδες εργασίας του NIS Cooperation Group και του ENISA (European Union Agency for Cybersecurity), του ΟΑΣΕ (Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη) και του ECSO (European Cyber Security Organisation). Παράλληλα, είναι υπεύθυνη για την εκπροσώπηση της Κύπρου στο CyCLONe (Cyber Crisis Liaison Organisation Network) και στο CSIRTs Network. Παρακολουθεί επίσης, με την ιδιότητα της ως Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας (βλ. Ενότητα 4), τις εργασίες του ECCG (European Cybersecurity Certification Group). Τέλος, αναπτύσσει συνεργασίες με Ευρωπαϊκές και τρίτες χώρες στα σχετικά θέματα (βλ. Ενότητες 7.2 και 7.3).

6.3.15 Θεματική Ενότητα 15 – Αντιμετώπιση Αδικημάτων στον Κυβερνοχώρο

Η παρούσα Θεματική Ενότητα περιλαμβάνει συγκεκριμένες δραστηριότητες που αφορούν κυρίως την αντιμετώπιση αδικημάτων στον κυβερνοχώρο, μέσω της παρακολούθησης του σχετικού νομικού πλαισίου, της ανάπτυξης των ικανοτήτων του προσωπικού, της ενημέρωσης όλων των οργανωμένων συνόλων για σκοπούς πρόληψης των αδικημάτων που διαπράττονται στον κυβερνοχώρο, και της ενίσχυσης της συνεργασίας μεταξύ του δημόσιου και ιδιωτικού τομέα κατά τη διερεύνηση ποινικών υποθέσεων.

Γίνεται συνεχής παρακολούθηση του Νομικού πλαισίου σε συνεργασία με το Υπουργείο Δικαιοσύνης, τη Νομική Υπηρεσία και την Διεύθυνση Ευρωπαϊκής Ένωσης της Αστυνομίας. Οι εξελίξεις που υπάρχουν στον τομέα αυτό είναι ο νέος κανονισμός για την παιδική πορνογραφία που αναμένεται να ψηφιστεί εντός του 2023 και ο οποίος θα υποχρεώνει τους παροχείς γενικά να εντοπίζουν, αναφέρουν και προβαίνουν στην φραγή υλικού. Επίσης, στην βάση του κανονισμού θα δημιουργηθεί ανεξάρτητο κέντρο σε Ευρωπαϊκό Επίπεδο για να συντονίζει τους παροχείς. Το θέμα θα παρακολουθείται σε συνεργασία με την Διεύθυνση Ευρωπαϊκής Ένωσης της Αστυνομίας και την Αστυνομία Κύπρου.

Κατά το 2023 αναμένεται, μεταξύ άλλων, η διοργάνωση ή/και συμμετοχή σε εκπαιδευτικά σεμινάρια και πανευρωπαϊκές ασκήσεις όλων των εμπλεκόμενων φορέων (δημόσιων και ιδιωτικών) για την καλύτερη και αποτελεσματικότερη διερεύνηση ποινικών υποθέσεων. Επίσης, αναμένεται η δημιουργία/συνέχιση των εκστρατειών ενημέρωσης και ευαισθητοποίησης του κοινού καθώς και η διοργάνωση ημερίδων και διαλέξεων γύρω από θέματα που αφορούν την ασφάλεια στον κυβερνοχώρο.

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 αυτό επικεντρώνεται 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 Αρχής με συνεργάτες εντός της Κυπριακής Δημοκρατίας, με αναφορά στους επιπρόσθετους ειδικούς στόχους του εκάστοτε Μνημονίου, και τις ενέργειες που πραγματοποιήθηκαν εντός του 2022.

Πίνακας 1: Μνημόνια Συνεργασίας μεταξύ της ΑΨΑ και συνεργατών

Συμμετέχων Οργανισμός	Ειδικοί Στόχοι Μνημονίου	Ενέργειες εντός του 2022
Ανοικτό Πανεπιστήμιο Κύπρου	Υποστήριξη στρατηγικών στόχων όσον αφορά την ανάλυση απειλών στον κυβερνοχώρο της Κύπρου. Εκσυγχρονισμό της λειτουργίας της ΑΨΑ όσον αφορά στην ανίχνευση απειλών και στα υψηλού επιπέδου εκπαιδευτικά εργαλεία.	Πραγματοποιήθηκαν επαφές και συζητήσεις αναφορικά με την αναθεώρηση και επικαιροποίηση του υφιστάμενου Μνημονίου Συνεργασίας που είχε υπογραφτεί το 2020. Αναμένεται υπογραφή του αναθεωρημένου Μνημονίου εντός 2023.
Κυπριακός Οργανισμός Τυποποίησης (CYS)	Ανάπτυξη μοντέλου αξιολόγησης ωριμότητας δυνατοτήτων στην κυβερνοασφάλεια, για κρίσιμες υποδομές σε σχέση με τη νομοθεσία της ΑΨΑ. Ανάπτυξη πλαισίου ελέγχου για την εφαρμογή του Εθνικού Πλαισίου Κυβερνοασφάλειας (βλ. Ενότητα 2.3)	Συνεχίστηκε η συνεργασία μεταξύ της ΑΨΑ και του Κυπριακού Οργανισμού Τυποποίησης για την ανάπτυξη του μοντέλου αξιολόγησης ωριμότητας και του πλαισίου ελέγχου, που θα συμβάλουν ενεργά στην υποστήριξη της ασφάλειας στον κυβερνοχώρο και κατ' επέκταση της εφαρμογής της Οδηγίας NIS. Οι σχετικές εργασίες αναμένεται να ολοκληρωθούν εντός του 2023.
Κεντρική Τράπεζα Κύπρου	Κοινοποίηση περιστατικών κυβερνοασφάλειας ή/και ψηφιακής ασφάλειας που θα αποστέλλει η Κεντρική Τράπεζα (υποχρεωτικές και εθελοντικές κοινοποιήσεις) στην ΑΨΑ.	Πραγματοποιήθηκαν επαφές και συζητήσεις για την οριστικοποίηση του περιεχομένου και των διαδικασιών που καλύπτει το Μνημόνιο. Αναμένεται η υπογραφή του Μνημονίου εντός του 2023.

Υφυπουργείο Ναυτιλίας	Αντιμετώπιση των κινδύνων του κυβερνοχώρου στον τομέα της ναυτιλίας. Δημιουργία πλαισίου παροχής εκπαίδευσης και κατάρτισης για θέματα κυβερνοασφάλειας. Παροχή καθοδήγησης και προστασίας από τις απειλές και επιθέσεις στον κυβερνοχώρο.	Εντός του 2022, οριστικοποιήθηκε και υπεγράφη το Μνημόνιο.
Κέντρο Αριστείας cyens - Centre of Excellence	Δημιουργία λύσεων αντιμετώπισης περιστατικών κυβερνοασφάλειας. Εκπόνηση προγραμμάτων και προτάσεων για συγχρηματοδοτούμενα έργα σε εθνικό και ευρωπαϊκό επίπεδο.	Εντός του 2022, οριστικοποιήθηκε και υπεγράφη το Μνημόνιο.
Κυπριακός Σύνδεσμος Πληροφορικής -Cyprus Computer Society	Συνδιοργάνωση εκδηλώσεων, σεμιναρίων, διαλέξεων, διαγωνισμών και συνεδριών. Συμμετοχή σε συμβουλευτικά σώματα και/ή συμβούλια των Συμμετεχόντων κατόπιν πρόσκλησης συμμετοχής. Εκπαίδευση, καθοδήγηση και συμμετοχή σε κοινές θεματικές δράσεις. Συμμετοχή και συνεργασία σε σχετικά Ευρωπαϊκά προγράμματα.	Εντός του 2022, οριστικοποιήθηκε και υπεγράφη το Μνημόνιο.
Ίδρυμα Έρευνας και Καινοτομίας (ΙδΕΚ)	Δημιουργία της Κοινοπραξίας για την υλοποίηση των προνοιών του Κανονισμού (ΕΕ) 2021/887 για το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας και του δικτύου των εθνικών κέντρων συντονισμού (βλ. Ενότητα 5).	Εντός του 2022, οριστικοποιήθηκε και υπεγράφη το Μνημόνιο.

7.2 Χώρες της Ευρωπαϊκής Ένωσης και Τρίτες Χώρες

Εντός του 2022, υπεγράφη Μνημόνιο Συνεργασίας μεταξύ του Υφυπουργείου Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής (ΥΕΚΨΠ) και του Συμβουλίου Κυβερνοασφάλειας των Ηνωμένων Αραβικών Εμιράτων για θέματα που σχετίζονται με την κυβερνοασφάλεια και τη συνεργασία στον κυβερνοχώρο. Σημειώνεται ότι, οι τομείς συνεργασίας που καθορίζονται στο Μνημόνιο αποτελούν αρμοδιότητες διαφόρων Αρχών που είναι αρμόδιες για κλάδους της διοίκησης κυβερνητικών τμημάτων και ως εκ τούτου η εφαρμογή των διατάξεων του Μνημονίου θα εποπτεύεται από διάφορους φορείς. Στην Κυπριακή Δημοκρατία οι Αρμόδιες Αρχές περιλαμβάνουν, αλλά δεν περιορίζονται, στο ΥΕΚΨΠ και την ΑΨΑ, και στα Ηνωμένα Αραβικά Εμιράτα η Αρμόδια Αρχή είναι το Συμβούλιο Κυβερνοασφάλειας. Την εφαρμογή του Μνημονίου στην Κυπριακή Δημοκρατία θα την επιβλέπει το ΥΕΚΨΠ.

Επιπλέον, πραγματοποιήθηκαν αρκετές επαφές συνεργασίας με τις αντίστοιχες υπηρεσίες του Ισραήλ, με αξιωματούχους του Σουλτανάτου του Ομάν, το Καζακστάν, την Αλβανία και τη Σαουδική Αραβία για τους τομείς της εκπαίδευσης και ανταλλαγής τεχνογνωσίας όσον αφορά την κυβερνοασφάλεια.

Τέλος, πραγματοποιηθήκαν επαφές συνεργασίας για την υπογραφή Μνημονίου Συνεργασίας μεταξύ της ΑΨΑ και της αρμόδιας αρχής της Σερβίας για θέματα κυβερνοασφάλειας και ηλεκτρονικών επικοινωνιών. Το εν λόγω Μνημόνιο Συνεργασίας αναμένεται να υπογραφεί εντός του 2023.

7.3 Διεθνής Εκπροσώπηση

Κατά το έτος 2022, η ΑΨΑ εκπροσωπήθηκε σε επιτροπές εθνικού και διεθνούς επιπέδου από τον Επίτροπο, το Βοηθό Επίτροπο, τον Διευθυντή και τα 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 έχει συμμετάσχει είναι:

Πίνακας 2: Διεθνείς οργανισμοί και Επιτροπές που συμμετάσχει 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)
GFCE (Global Forum on Cyber Expertise)
ECCC (European Cybersecurity Competence Centre)
ECSO (European CyberSecurity Organization)

8. ΣΥΝΕΔΡΙΑ ΚΑΙ ΕΚΔΗΛΩΣΕΙΣ

Εντός του 2022, 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 και Εκδηλώσεων από την ΑΨΑ

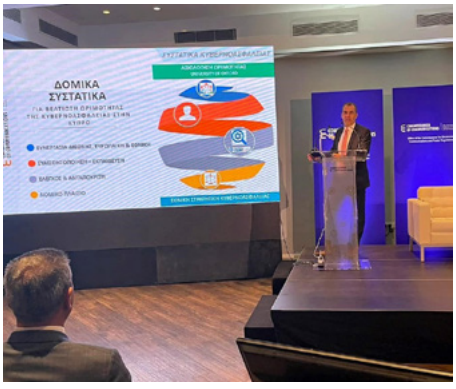
8.1.1 Εκπαιδεύσεις ESDC (European Security and Defence College)

Από το σεμινάριο με Τίτλο «The Role of the EU Cyber Ecosystem in the Global Cyber Security Stability».

Η ΑΨΑ συμμετείχε ως συνδιοργανώτρια με το Υπουργείο Άμυνας και το Ευρωπαϊκό Κολέγιο Ασφάλειας και Άμυνας (ESDC – European Security and Defence College), στο σεμινάριο «The Role of the EU Cyber Ecosystem in the Global Cyber Security Stability», που πραγματοποιήθηκε μεταξύ 27 και 29 Απριλίου 2022 στο κέντρο «Ζήνων» στη Λάρνακα. Στην εν λόγω εκδήλωση συμμετείχαν 60 άτομα από τους τομείς της κυβερνοασφάλειας, του κυβερνοεγκλήματος και της κυβερνοάμυνας, από διάφορα κράτη όπως Αλγερία, Ισραήλ, Ιορδανία, Λίβανος, Κατάρ, Βέλγιο, Τσεχική Δημοκρατία, Σλοβακία, Ισπανία, καθώς και θεσμικά όργανα και οργανισμοί της Ευρωπαϊκής Ένωσης, όπως η Ευρωπαϊκή Επιτροπή, η EUROPOL, η ENISA, η EU-LISA, η CERT-EU, το EUISS και το EUROCONTROL.

8.1.2 2η Συνάντηση Ενδιαφερόμενων Μερών και Αρχών στο χώρο της Κυβερνοασφάλειας στην Κύπρο.

Η ΑΨΑ πραγματοποίησε τη δεύτερη συνάντηση Ενδιαφερόμενων Μερών και Αρχών στο χώρο της κυβερνοασφάλειας στην Κύπρο. Την ημερίδα παρακολουθήσαν περίπου 160 εμπειρογνώμονες από αρμόδιους Φορείς Κρίσιμων Υποδομών Πληροφοριών και Αρχές της Κυπριακής Δημοκρατίας. Στόχος της εκδήλωσης ήταν η ενίσχυση των σχέσεων μεταξύ των Φορέων και της ΑΨΑ στον τομέα της κυβερνοασφάλειας. Συγκεκριμένα παρουσιάστηκε το επίπεδο ωριμότητας της κυβερνοασφάλειας στην Κύπρο αλλά και στην Ευρώπη, καθώς επίσης και τις προκλήσεις που αντιμετωπίζουν οι κρίσιμες υποδομές.



Από την 2η Συνάντηση Ενδιαφερόμενων Μερών και Αρχών στο χώρο της Κυβερνοασφάλειας στην Κύπρο.

Από την 2η Συνάντηση Ενδιαφερόμενων Μερών και Αρχών στο χώρο της Κυβερνοασφάλειας στην Κύπρο.

8.1.3 Cybersecurity Workshop in the Maritime Domain

Η ΑΨΑ και το Υφυπουργείο Ναυτιλίας, με την υποστήριξη των Εθνικών Εργαστηρίων της Sandia Αμερικής (Sandia National Laboratories USA) και το Ανοικτό Πανεπιστήμιο Κύπρου (Open University Cyprus), συνδιοργάνωσαν διήμερα σεμινάρια στο Εκπαιδευτικό Κέντρο CYCLOPS στη Λάρνακα, με σκοπό την ανάπτυξη ενός περιφερειακού πλαισίου για την ενίσχυση της ανθεκτικότητας της κυβερνοασφάλειας σε όλον τον ναυτιλιακό τομέα. Επιπλέον στόχοι ήταν επίσης η αύξηση της ευαισθητοποίησης στον τομέα της κυβερνοασφάλειας και η ενίσχυση των ικανοτήτων στον κυβερνοχώρο στον τομέα της ναυτιλίας.

Τα εργαστήρια απευθύνονταν σε ανώτατα και μεσαία διοικητικά στελέχη φορέων και εταιρειών στον τομέα της ναυτιλίας εντός της Κυπριακής Δημοκρατίας, με συνολική συμμετοχή 30 ατόμων ανά σεμινάριο.

Το πρώτο εργαστήριο διοργανώθηκε στις 19-20 Ιουλίου 2022 και είχε ως Θέμα «Cybersecurity Workshop: Increasing Cybersecurity Awareness and Enhancing Cyber Competencies in the Maritime Domain.»

Το δεύτερο εργαστήριο διοργανώθηκε στις 13-14 Δεκεμβρίου 2022 και είχε ως Θέμα «Cybersecurity Workshop: Preventing Cyber Aggression in the Maritime Domain».

Από το πρώτο εργαστήριο με θέμα: «Cybersecurity Workshop: Increasing Cybersecurity Awareness and Enhancing Cyber Competencies in the Maritime Domain.» Ιούλιος 2022

Από το πρώτο εργαστήριο με θέμα: «Cybersecurity Workshop: Increasing Cybersecurity Awareness and Enhancing Cyber Competencies in the Maritime Domain.» Ιούλιος 2022

Από το δεύτερο εργαστήριο με θέμα: «Cybersecurity Workshop: Preventing Cyber Aggression in the Maritime Domain». Δεκέμβριος 2022

Από το δεύτερο εργαστήριο με θέμα: «Cybersecurity Workshop: Preventing Cyber Aggression in the Maritime Domain». Δεκέμβριος 2022

8.1.4 Ευρωπαϊκός Μήνας Κυβερνοασφάλειας (European Cyber Security Month - ECSM)

Η ΑΨΑ συμμετείχε στην ετήσια εκστρατεία της ΕΕ για την προώθηση της ασφάλειας στο διαδίκτυο, η οποία ονομάζεται Ευρωπαϊκός Μήνας Κυβερνοασφάλειας (ECSM) και διοργανώνεται για 10η συνεχόμενη χρονιά. Η εκστρατεία συντονίζεται από τον Οργανισμό για την Κυβερνοασφάλεια της Ευρωπαϊκής Ένωσης (ENISA) και υποστηρίζεται από πολλούς εταίρους, όπως η Ευρωπαϊκή Επιτροπή, κυβερνητικοί οργανισμοί, εταιρείες και ακαδημαϊκοί φορείς. Στόχος της εκστρατείας είναι να ενημερώσει τους πολίτες της Ένωσης για την κυβερνοασφάλεια και να τους παρέχει συμβουλές για την προστασία τους από κυβερνοαπειλές.

Η επετειακή εκστρατεία του 2022 είχε ως κεντρικό θέμα το Phishing και το Ransomware. Καθ' όλη τη διάρκεια του Οκτωβρίου, ο ECSM διοργάνωσε δράσεις και εκδηλώσεις για να ευαισθητοποιήσει το κοινό και να προωθήσει καλές συνήθειες κυβερνοασφάλειας. Όπως κάθε χρόνο, καθ' όλη τη διάρκεια του Οκτωβρίου, ο ECSM έφερε σε επαφή πολίτες της ΕΕ, κράτη μέλη, την Ευρωπαϊκή Επιτροπή, φορείς της ΕΕ και κυβερνητικούς οργανισμούς, τον ιδιωτικό τομέα και την ακαδημαϊκή κοινότητα με σκοπό την προώθηση καλών συνηθειών κυβερνοασφάλειας.

Σχετικά με τον Ευρωπαϊκό Μήνα Κυβερνοασφάλειας (ECSM) η ΑΨΑ σε συνεργασία με διάφορους οργανισμούς διοργάνωσε διάφορες δραστηριότητες για ενίσχυση της εκστρατείας Κυβερνοασφάλειας:

Σεμινάριο προς τις Μικρομεσαίες Επιχειρήσεις με θέμα «Cyber Security Essentials for SMEs»

Σεμινάριο με Τίτλο : «Cyber Security Essentials for SMEs»

Το Κυπριακό Εμπορικό και Βιομηχανικό Επιμελητήριο (ΚΕΒΕ) σε συνεργασία με την ΑΨΑ διοργανώσαν μία σειρά σεμιναρίων σε Λευκωσία, Λάρνακα και Λεμεσό με θέμα: «Cyber Security Essentials for SMEs». Οι εκπαιδεύσεις έγιναν σε συνεργασία με το Ευρωπαϊκό Πανεπιστήμιο Κύπρου. Σκοπός των σεμιναρίων ήταν η ευαισθητοποίηση των εργαζομένων στις μικρό-μεσαίες επιχειρήσεις (ΜμΕ) στον τομέα της κυβερνοασφάλειας. Στα σεμινάρια συμμετείχαν περίπου 100 άτομα από ΜμΕ.

Εκστρατεία ενημέρωσης ΑΣΠΙΣ ΙΙ

Η ΑΨΑ, η Αστυνομία Κύπρου (Υποδιεύθυνση Ηλεκτρονικού Εγκλήματος), η Κεντρική Τράπεζα της Κύπρου και ο Σύνδεσμος Τραπεζών Κύπρου ένωσαν δυνάμεις, τεχνογνωσία και εμπειρίες, σε μια κοινή εκστρατεία ενημέρωσης, με στόχο τη δημιουργία ασπίδας προστασίας έναντι των όσων χρησιμοποιούν ηλεκτρονικές μεθόδους με σκοπό την εξαπάτηση πολιτών ή/και οργανισμών.

Η εκστρατεία με το όνομα ΑΣΠΙΣ (ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ και INFORMATION SECURITY), στοχεύει στην ενημέρωση για τις συνήθεις πρακτικές που εφαρμόζουν επιτήδειοι, προκειμένου να επιτύχουν πρόσβαση στα προσωπικά δεδομένα και τους τραπεζικούς λογαριασμούς τους ή να τους εμπλέξουν σε ψεύτικες διαδικασίες με σκοπό την απόσπαση χρηματικών ποσών.

Η ενημερωτική καμπάνια είχε θέμα τις Ηλεκτρονικές Απάτες, το Phishing, Smishing, Vishing και Ransomware, η οποία απευθύνεται σε όλους τους πολίτες και κυρίως στις ομάδες εκείνες, οι οποίες αποτελούν συχνότερους και ευκολότερους στόχους.

Εκστρατεία ενημέρωσης ΑΣΠΙΣ ΙΙ

Εκστρατεία ενημέρωσης ΑΣΠΙΣ ΙΙ

Διαδικτυακό σεμινάριο στα μέλη του ΕΤΕΚ με θέμα «Κυβερνοασφάλεια: Βέλτιστες πρακτικές για την ασφαλή χρήση του Διαδικτύου και αναγνώριση κινδύνων»

Διαδικτυακό Σεμινάριο με θέμα: «Κυβερνοασφάλεια: Βέλτιστες πρακτικές για την ασφαλή χρήση του Διαδικτύου και αναγνώριση κινδύνων»

Σε συνεργασία με το ΕΤΕΚ, πραγματοποιήθηκε σεμινάριο που εστιαζόταν στις τεχνικές και τακτικές που χρησιμοποιούνται από κακόβουλα άτομα, με σκοπό να καταστρέψουν ευαίσθητες και σημαντικές πληροφορίες, να αποσπάσουν χρήματα από χρήστες ή να διακόψουν τη ροή εργασιών μιας επιχείρησης. Το σεμινάριο κάλυψε τις βέλτιστες πρακτικές για την ασφαλή χρήση του Διαδικτύου, ώστε να αναγνωρίζουν οι χρήστες τους βασικούς κινδύνους και να προφυλάσσονται κατάλληλα.

Το σεμινάριο πραγματοποιήθηκε διαδικτυακά με συμμετοχή 50 και πλέον ατόμων.

Διημερίδα Train the Trainers Awareness program

Η ΑΨΑ, σε συνεργασία με το Υπουργείο Άμυνας της Κυπριακής Δημοκρατίας και την Εθνική Αρχή Ασφάλειας, διοργάνωσαν επιμορφωτική διημερίδα κυβερνοασφάλειας με θέμα «Train the Trainers Awareness Program», στην αίθουσα ενημέρωσης του Κέντρου Διαχείρισης Κρίσεων «Ζήνων» στην Λάρνακα. Στη διημερίδα συμμετείχαν 60 μέλη της Εθνικής Φρουράς, η οποία έγινε με σκοπό την επαύξηση του επιπέδου επίγνωσης των στελεχών της Εθνικής Φρουράς στις πιο κάτω Ενότητες:

- εθνική δομή και νομικό πλαίσιο στον τομέα της κυβερνοασφάλειας,
- τακτικές, τεχνικές και διαδικασίες σε κυβερνοεπιθέσεις,
- δομή Στρατιωτικού CSIRT,
- προστασία Ψηφιακών Διαβαθμισμένων Πληροφοριών,
- βασικά σενάρια κυβερνοεπιθέσεων.

Διημερίδα «Train the Trainers Awareness program»

Διοργάνωση του 1ου Cyber Security Weekend

Η ΑΨΑ και το Κυπριακό Εμπορικό και Βιομηχανικό Επιμελητήριο (ΚΕΒΕ) διοργάνωσαν το πρώτο Cyber Security Weekend σε ξενοδοχείο στην Αγία Νάπα.

Στόχος του Cyber Security Weekend ήταν να ενημερώσει και να ευαισθητοποιήσει τις επιχειρήσεις σε σχέση με τη σημαντικότητα της επένδυσης στον τομέα της κυβερνοασφάλειας. Κατά τη διάρκεια του Cyber Security Weekend, πραγματοποιήθηκαν ενημερωτικές και εκπαιδευτικές ενέργειες, καθώς επίσης και κατ' ιδίαν συναντήσεις με εξειδικευμένες εταιρείες κυβερνοασφάλειας, ούτως ώστε να εντοπισθούν οι ανάγκες κάθε εταιρείας ξεχωριστά, και να αναπτυχθούν συνέργειες.

Στιγμιότυπα από το Cyber Security Weekend

Στιγμιότυπα από το Cyber Security Weekend

8.2 Συμμετοχή ΑΨΑ σε Συνέδρια και Εκδηλώσεις

8.2.1 Ημέρα Ασφαλούς Διαδικτύου 2022

Διαδικτυακό Σεμινάριο με θέμα: «Μαζί για ένα καλύτερο Διαδίκτυο»

Στα πλαίσια της Ημέρας Ασφαλούς Διαδικτύου, πραγματοποιήθηκε στις 8 Φεβρουαρίου 2022 ημερίδα, με θέμα: «Μαζί για ένα καλύτερο Διαδίκτυο.» Την ημερίδα, η οποία πραγματοποιήθηκε διαδικτυακά, διοργάνωσε το Παιδαγωγικό Ινστιτούτο του Υπουργείου Παιδείας, Πολιτισμού, Αθλητισμού και Νεολαίας, σε συνεργασία με τη Cyta, και με την υποστήριξη της ΑΨΑ και των άλλων εταίρων του Ευρωπαϊκού Έργου «Κέντρο Ασφαλούς Διαδικτύου - CYberSafety» και απευθυνόταν σε μαθητές και εκπαιδευτικούς από σχολεία όλης της Κύπρου. Η ημερίδα είχε ως στόχο να καλλιεργήσει την υπευθυνότητα, το σεβασμό και τη δημιουργική αξιοποίηση του Διαδικτύου στη ζωή μας, και να περάσει το μήνυμα ότι είναι καθήκον όλων, της Πολιτείας, των φορέων που ασχολούνται με το Διαδίκτυο, των εκπαιδευτικών, των γονέων, των νέων και των παιδιών, να συνεισφέρουν, ώστε το Διαδίκτυο να καταστεί ένας καλύτερος και ασφαλέστερος χώρος επικοινωνίας, ψυχαγωγίας και μάθησης.

8.2.2 Συμμετοχή Επιτρόπου Επικοινωνιών στο GITEX GLOBAL 2022

Ο Επίτροπος Επικοινωνιών, ήταν ένας εκ των ομιλητών στο GITEX 3.0, την 42η έκδοση της μεγαλύτερης έκθεσης τεχνολογίας και startup στον κόσμο #GITEXGLOBAL η οποία πραγματοποιήθηκε στις 10-12 Μαΐου 2022. Η έκθεση είχε ως θέμα: «Πρέπει να αρχίσουμε να εξετάζουμε την ασφάλεια στον κυβερνοχώρο ως μέρος του ESG - Environmental, social and governance strategy». Η συζήτηση επικεντρώθηκε στο πλαίσιο της οικοδόμησης της στρατηγικής ESG με τη μέτρηση του κινδύνου στον κυβερνοχώρο που θα βοηθήσει τους οργανισμούς και τις ρυθμιστικές αρχές.

8.2.3 Συμμετοχή ΑΨΑ στην εκδήλωση με τίτλο Θάλασσα 2022 – Γνώρισε την Ναυτιλία

Η ΑΨΑ συμμετείχε στην εκδήλωση με τίτλο “Θάλασσα 2022 – Γνώρισε την Ναυτιλία” που διοργάνωσε το Υφυπουργείο Ναυτιλίας και ο Δήμος Λεμεσού, η οποία πραγματοποιήθηκε στις 23 Μαΐου 2022. Η ομάδα της ΑΨΑ παρουσίασε εκπαιδευτικό υλικό, τόσο μέσω εξειδικευμένης πλατφόρμας ενημέρωσης όσο και μέσω πλατφόρμας online παιχνιδιού ερωτήσεων, που παρέχεται σε σχολεία στο πλαίσιο του έργου CyberSafety, προκειμένου να ενισχυθεί η ευαισθητοποίηση ως προς την ασφάλεια στη χρήση του διαδικτύου.

8.2.4 Εκπροσώπηση ΑΨΑ στο διεθνές συνέδριο ITU World Telecommunications Development Conference

Η ΑΨΑ, μαζί με το ΓΕΡΗΕΤ και το Τμήμα Ηλεκτρονικών Επικοινωνιών, συμμετείχε στο διεθνές συνέδριο World Telecommunications Development Conference της Διεθνής Ένωσης Τηλεπικοινωνιών που διεξήχθη στις 6-16 Ιουνίου 2022, εκπροσωπώντας την Κυπριακή Δημοκρατία στο Κιγκάλι της Δημοκρατίας της Ρουάντας.

Το συνέδριο WTDC λαμβάνει χώρα κάθε 4 χρόνια, καθορίζοντας την πορεία της Διεθνής Ένωσης Τηλεπικοινωνιών για την ερχόμενη τετραετία, με ειδική έμφαση στην ανάπτυξη των υπηρεσιών τηλεπικοινωνιών σε παγκόσμιο επίπεδο και καλύπτοντας θέματα, έργα και προγράμματα ανάπτυξης τηλεπικοινωνιών. Το συνέδριο καθορίζει τις σχετικές στρατηγικές, στόχους για την παγκόσμια ανάπτυξη τηλεπικοινωνιών, παρέχοντας κατεύθυνση για τις δραστηριότητες της Διεθνής Ένωσης Τηλεπικοινωνιών. Κατά τη διάρκεια του συνεδρίου, η ΑΨΑ εστίασε σε σειρά θεμάτων κυβερνοασφάλειας, καθώς είναι πλέον κατανοητό από όλους ότι δεν νοείται ανάπτυξη στις τηλεπικοινωνίες χωρίς αυτές να είναι ασφαλισμένες.

8.2.5 Συμμετοχή ΑΨΑ σε Ομάδα Εργασίας 3+1 για την κυβερνοασφάλεια στο Ισραήλ

Η ΑΨΑ στις 23 Σεπτεμβρίου 2022 συμμετείχε σε Ομάδα Εργασίας 3+1 για την κυβερνοασφάλεια στο Ισραήλ, με εμπειρογνώμονες από Κύπρο, Ελλάδα, Ισραήλ, ΗΠΑ με σκοπό την αντιμετώπιση κοινών προκλήσεων σχετικά με την προστασία της θαλάσσιας περιοχής, ενέργειας και των κρίσιμων υποδομών και συστημάτων.

8.2.6 Διοργάνωση 2ο Συνέδριου Κυβερνοασφάλειας από την ΙΜΗ

Το 2ο συνέδριο Κυβερνοασφάλειας που διοργανώθηκε με επιτυχία από την ΙΜΗ, το οποίο πραγματοποιήθηκε στις 26 Οκτωβρίου 2022, ακολουθώντας τις εξελίξεις του πολέμου στην Ουκρανία αλλά και της Πανδημίας COVID-19, οι οποίες ανέδειξαν νέα ρίσκα και απειλές στον κυβερνοχώρο, συγκέντρωσε εμπειρογνώμονες και φορείς του κλάδου της κυβερνοασφάλειας οι οποίοι συζήτησαν την ασφάλεια στον κυβερνοχώρο σε ένα δυναμικά εξελισσόμενο παγκόσμιο περιβάλλον. Ο Επίτροπος Επικοινωνιών και ο Επικεφαλής του Εθνικού CSIRT – CY συμμετείχαν ως ομιλητές.

8.2.7 4ο Συνέδριο InfoCom Security

Το 4ο Συνέδριο InfoCom Security Cyprus, το οποίο πραγματοποιήθηκε στις 8 Δεκεμβρίου 2022, αποτέλεσε μια μεγάλη ευκαιρία ενημέρωσης για την εξέλιξη των ψηφιακών απειλών και του κυβερνοεγκλήματος, τις επιθέσεις στα δίκτυα των επιχειρήσεων και των οργανισμών του δημοσίου και ιδιωτικού τομέα. Χαιρετισμό απηύθυνε ο Βοηθός Επίτροπος Επικοινωνιών στην έναρξη του συνεδρίου, και η ΑΨΑ εκπροσωπήθηκε από τον Προϊστάμενο ΑΨΑ ο οποίος παρουσίασε το έργο της ΑΨΑ.

8.2.8 Συμμετοχή στο e-Cyber Health

Το e-Cyber Health πραγματοποιήθηκε στις 12 Δεκεμβρίου 2022 και αποτέλεσε το πρώτο συνέδριο για την κυβερνο – υγεία, υπό την αιγίδα του Υπουργείου Υγείας. Υποστηρικτές του συνεδρίου ήταν η Ευρωπαϊκή Επιτροπή, ο Κυπριακός Οργανισμός Τυποποίησης, ο Κυπριακός Σύνδεσμος Πληροφορικής, ο Κυπριακός Σύνδεσμος Προστασίας Πληροφοριών & Ιδιωτικότητας και η ΑΨΑ.

Στο συνέδριο καλύφθηκαν θέματα που σχετίζονταν με τάσεις και εξελίξεις στον τομέα της ασφάλειας στον κυβερνοχώρο καθώς και σύγχρονες τεχνολογικές λύσεις, εργαλεία και πρότυπα που ενισχύουν τους μηχανισμούς προστασίας των επιχειρήσεων ενάντια σε εξελιγμένες επιθέσεις.

9. ΣΥΜΜΕΤΟΧΗ ΣΕ ΕΥΡΩΠΑΪΚΑ ΣΥΓΧΡΗΜΑΤΟΔΟΤΟΥΜΕΝΑ ΠΡΟΓΡΑΜΜΑΤΑ

9.1 Τρέχοντα Έργα

9.1.1 Joint Cybersecurity Operations Platform (CEF-JCOP)

Στα πλαίσια του ευρωπαϊκού προγράμματος CONNECTING EUROPE FACILITY (CEF), η ΑΨΑ, σε συνεργασία με άλλα ευρωπαϊκά ιδρύματα, προχώρησαν με το σχεδιασμό και την ανάπτυξη της Κοινής Πλατφόρμας Επιχειρήσεων Κυβερνοασφάλειας (JCOP) για τα κράτη μέλη της ΕΕ.

Ο μακροπρόθεσμος στόχος του έργου είναι η χρήση της πλατφόρμας από μεγάλο εύρος ευρωπαϊκών φορέων. Η συγκεκριμένη πλατφόρμα περιλαμβάνει τρεις βασικούς πυλώνες:

α Τη συλλογή και ανάλυση πληροφοριών (Threat Intelligence): Συλλογή, ανάλυση και ανταλλαγή πληροφοριών σχετικά με απειλές και παράγοντες απειλών.
β Την προειδοποίηση και αντιμετώπιση συμβάντων: Ταχεία ειδοποίηση μεταξύ διαφορετικών μερών εντός της ΕΕ, η οποία μπορεί να χρησιμοποιηθεί είτε προληπτικά είτε για να ανταποκριθεί σε τρέχοντα συμβάντα.
γ Την υποστήριξη εκπαιδευτικών προγραμμάτων (Cybersecurity Operations Training): Συνεχή ενημέρωση και εκπαίδευση, μέσω της συλλογής, στην πλατφόρμα, εξειδικευμένου εκπαιδευτικού υλικού για διάφορα θέματα κυβερνοασφάλειας.

Το έργο άρχισε τον Αύγουστο 2021, και έχει διάρκεια 3 χρόνια με συνολικό προϋπολογισμό €1.703.226.

9.1.2 Power System's SHield against cOmplEx iNcI²dents and eXtensive cyber and privacy attacks (PHOENi²X Project)

Το έργο PHOENi²X στοχεύει στο σχεδιασμό, την ανάπτυξη και υλοποίηση ενός πλαισίου ανθεκτικότητας στον κυβερνοχώρο. Αυτό το πλαίσιο θα παρέχει δυνατότητες ανίχνευσης, πρόβλεψης, αυτοματοποίησης και ταχείας απόκρισης με βάση την τεχνητή νοημοσύνη για:

- την ανταπόκριση σε περιστατικά στον κυβερνοχώρο καθώς και απειλές στον κυβερνοχώρο,
- την ασφαλή ανταλλαγή πληροφοριών, και
- τη λειτουργική αποκατάσταση των εθνικών αρχών ψηφιακής ασφάλειας των κρατών μελών της Ευρωπαϊκής Ένωσης και των κρίσιμων υποδομών.

Ο ρόλος της ΑΨΑ στο Ευρωπαϊκό πρόγραμμα PHOENi²X είναι ενεργός όσον αφορά τις διαδικτυακές αλλά και τις δια ζώσης συναντήσεις που γίνονται με τα μέλη της κοινοπραξίας. Ταυτόχρονα, η ΑΨΑ έχει και εποπτικό ρόλο, καθότι επιβλέπει την ορθή τήρηση των διαδικασιών, των χρονοδιαγραμμάτων και αξιολογεί τα παραδοτέα για την ορθή εφαρμογή των κανόνων ασφαλείας που αφορούν το χειρισμό διαβαθμισμένων πληροφοριών της Ευρωπαϊκής Ένωσης.

Το έργο άρχισε τον Ιούλιο 2021, και έχει διάρκεια 3 χρόνια με συνολικό προϋπολογισμό €4.825.000.

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

Το έργο A4CEF αποσκοπεί στην επέκταση των δραστηριοτήτων της ΑΨΑ στον τομέα πιστοποιήσεων κυβερνοασφάλειας, καλύπτοντας σχετικούς στόχους που έχουν τεθεί εντός της Εθνικής Στρατηγικής Κυβερνοασφάλειας. Το έργο έχει τους ακόλουθους στόχους:

- την αξιοποίηση και επέκταση του προηγούμενου έργου B4C (Δράση CEF 2019-EU-IA-0109) για πιστοποιήσεις κυβερνοασφάλειας,
- την ενίσχυση της Εθνικής Αρχής Προτύπων της Ιρλανδίας (NSAI),

- την ανάπτυξη δεξιοτήτων του ανθρώπινου δυναμικού, παρέχοντας επικαιροποιημένο εκπαιδευτικό υλικό για την πιστοποίηση υπηρεσιών νεφοϋπολογιστικής (Cloud Computing Services), και πραγματοποίηση πιλοτικών πιστοποιήσεων,
- την ανταλλαγή καλών πρακτικών μεταξύ Κύπρου και Ιρλανδίας που σχετίζονται με δραστηριότητες αξιολόγησης της συμμόρφωσης,
- την ανάπτυξη ενός ολοκληρωμένου μοντέλου, με στόχο την οικοδόμηση ενός προτύπου αναφοράς για άμεση υποστήριξη του πλήρους φάσματος των δραστηριοτήτων πιστοποίησης της κυβερνοασφάλειας όπως ορίζονται στο Ευρωπαϊκό Πλαίσιο Πιστοποίησης Κυβερνοασφάλειας,
- τη χρήση δομημένων δραστηριοτήτων ενημέρωσης και επικοινωνίας σε σχετικές ομάδες εργασίας και σε άλλα ευρωπαϊκά φόρουμ.

Το έργο ξεκίνησε τον Ιούλιο 2021 και αναμένεται να ολοκληρωθεί εντός του 2023, με συνολικό προϋπολογισμό €280,000.

9.1.4 CEF CYberSafety III

Το ευρωπαϊκό συγχρηματοδοτούμενο έργο CYberSafety - A better internet for children in Cyprus (Ένα καλύτερο Διαδίκτυο για τα παιδιά στην Κύπρο) στοχεύει στη δημιουργία μιας ασφαλούς διαδικτυακής κουλτούρας για μαθητές, γονείς και εκπαιδευτικούς. Μέσω του έργου CYberSafety οι ενδιαφερόμενοι μπορούν να βρουν πληροφορίες και να χρησιμοποιήσουν εργαλεία, αλλά και να μοιραστούν εμπειρίες, τεχνογνωσία και καλές πρακτικές σε σχέση με την ασφαλή χρήση του διαδικτύου. Ο ρόλος της ΑΨΑ σε αυτή την 3η φάση του έργου είναι η ενημέρωση και ευαισθητοποίηση των παιδιών για την κυβερνασφάλεια καθώς και την ανάπτυξη δεξιοτήτων για την ασφαλή χρήση του διαδικτύου, μέσω διαδραστικών εκπαιδεύσεων σε Γυμνάσια, Λύκεια και Τεχνικές Σχολές.

Το έργο συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση μέσω του Ευρωπαϊκού προγράμματος CEF Telecom. Ξεκίνησε τον Ιανουάριο του 2020 και ολοκληρώθηκε στις 30/09/2022 με συνολικό προϋπολογισμό €764.907,14.

9.2 Μελλοντικά Εγκεκριμένα Έργα

9.2.1 N4CY

Το N4CY στοχεύει στην ανάπτυξη του Εθνικού Κέντρου Συντονισμού Κυβερνοασφάλειας (National Cybersecurity Coordination Centre – NCC-CY) της Κυπριακής Δημοκρατίας αλλά και στην ενίσχυση της ικανότητάς του να εκπληρώνει την αποστολή και τους στόχους του. Στο έργο, το ΙΔΕΚ εντάχθηκε ως συνεργάτης (Beneficiary) και το Υφυπουργείο Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής (ΥΕΚΨΠ) ως Συνδεδεμένος Εταίρος (Associated Partner - AP). Πιο συγκεκριμένα, το έργο N4CY, πέραν της ανάπτυξης του NCC-CY, θα παρέχει οικονομική υποστήριξη υπό την μορφή επιχορηγήσεων σε ΜμΕ, θα προωθήσει την ευαισθητοποίηση και την εκπαίδευση στην κυβερνοασφάλεια και θα θέσει ένα επαρκές επίπεδο κυβερνοασφάλειας για τις μικρομεσαίες επιχειρήσεις, με την εφαρμογή του οποίου θα μπορούν οι επιχειρήσεις να αποκτούν πιστοποίηση για την ασφάλεια τους στον κυβερνοχώρο.

Το έργο εγκρίθηκε εντός του 2022 και έχει συνολικό προϋπολογισμό €2.558.370. Για την οικονομική υποστήριξη των ΜμΕ θα διανεμηθεί το συνολικό ποσό του €1.000.000.

9.2.2 CEF CYberSafety IV

Ο στόχος του CYberSafety IV είναι να ενισχύσει και να αναπτύξει το υφιστάμενο Κέντρο Ασφαλούς Διαδικτύου (Safer Internet Centre - SIC) στην Κύπρο, η οποία απευθύνεται σε παιδιά, γονείς και εκπαιδευτικούς, παιδαγωγούς και άλλους επαγγελματίες σχετικά με την καλύτερη και ασφαλέστερη χρήση του διαδικτύου, και αποτελεί συνέχιση και ενίσχυση του έργου CYberSafety III.

Το έργο CyberSafety IV εγκρίθηκε εντός του 2022, θα έχει διάρκεια από τις αρχές του 2023 μέχρι τον Σεπτέμβριο του 2024, με τον συνολικό προϋπολογισμό να ανέρχεται σε €1.118.894,72.

9.2.3 CYQCI

Το έργο Cyprus Quantum Communication Infrastructure (CYQCI) θα είναι το πρώτο έργο που θα ασχοληθεί με την ανάπτυξη κβαντικών επικοινωνιών στην Κύπρο, εισάγοντας 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. Το CYQCI αποσκοπεί στην ανάπτυξη ενός προηγμένου πειραματικού κβαντικού δικτύου, στην κατασκευή ενός πλήρως λειτουργικού οπτικού επίγειου σταθμού (Optical Ground Station - OGS) και την σύνδεση του με την υπόλοιπη Ευρωπαϊκή Ένωση, καθώς και στην συμβολή στις διεθνείς προσπάθειες τυποποίησης για τις κβαντικές επικοινωνίες.

Περαιτέρω, θα δημιουργηθεί 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 προτεινόμενο δίκτυο θα εκτείνεται στις τρεις μεγάλες πόλεις της Κύπρου, αξιοποιώντας το υφιστάμενο δίκτυο οπτικών επικοινωνιών και επιδεικνύοντας τουλάχιστον 6 περιπτώσεις χρήσης και 11 τελικούς χρήστες, για τις εφαρμογές διασφάλισης της επικοινωνίας μεταξύ δημόσιων οργανισμών, κρίσιμων υποδομών, ακαδημαϊκών ιδρυμάτων και βιομηχανικών υπηρεσιών.

Το έργο εγκρίθηκε εντός του 2022, θα ξεκινήσει τον Ιανουάριο του 2023 με διάρκεια 32 μήνες και έχει συνολικό προϋπολογισμό €7.512.843,43.

9.3 Υποβληθέντες Προτάσεις για συγχρηματοδότηση

9.3.1 ASPECT

Το έργο ASPECT αποσκοπεί στην εισαγωγή μιας αυτόνομης ρομποτικής πλατφόρμας με δυνατότητες τεχνητής νοημοσύνης, η οποία θα ανιχνεύει, ταυτοποιεί, ταξινομεί και ανταποκρίνεται γρήγορα σε πιθανές απειλές, καθώς και θα επιθεωρεί και αναφέρει τις ζημιές και να προτείνει την καλύτερη δυνατή διαδικασία δράσης για τους πρώτους ανταποκριτές και τους τελικούς χρήστες. Η πλατφόρμα έχει σχεδιαστεί για την ανίχνευση, ανάλυση και επιθεώρηση ενός ευρέος φάσματος απειλών, συμπεριλαμβανομένων των υποβρύχιων, υπόγειων και απειλών από υψόμετρο. Θα προσφέρει καινοτόμα μέσα ανάλυσης και επικοινωνίας, φορητές συσκευές και αυτόνομες ρομποτικές συσκευές για την αξιολόγηση των απειλών, τη μείωση του χρόνου ανταπόκρισης και τη διευκόλυνση της έγκυρης αντιμετώπισης απειλών χωρίς αρχικό κίνδυνο για τους ανθρώπινους χειριστές του συστήματος.

Η ημερομηνία υποβολής της πρότασης ήταν η 23η Νοεμβρίου 2022 και οι εμπλεκόμενες χώρες είναι η Ισπανία, Ελλάδα, Ηνωμένο Βασίλειο, Ρουμανία, Γερμανία, Ισπανία, και Τσεχία.

Το έργο, αν εγκριθεί, αναμένεται ότι θα ξεκινήσει εντός του 2023, με συνολικό προϋπολογισμό €5.938.661,94.

9.3.2 DetectThreat

Το έργο DetectThreat στοχεύει στην ενίσχυση της κυβερνοασφάλειας στις ευρωπαϊκές υποδομές ζωτικής σημασίας, μέσω της ανάπτυξης εργαλείων τεχνητής νοημοσύνης με την δυνατότητα πρόβλεψης απειλών στον κυβερνοχώρο, καθώς και του σχεδιασμού ασκήσεων ψηφιακής ασφάλειας και εκπαιδευτικών προγραμμάτων προς τους τελικές χρήστες στους τομείς των τηλεπικοινωνιών, ναυτιλίας και σιδηρόδρομων.

Επιπρόσθετα, το DetectThreat έχει ένα ολοκληρωμένο σχέδιο για την εισαγωγή τρίτων μερών με τη χρήση του μηχανισμού Financial Support for Third Parties (FSTP). Εν συνεχεία, το DetectThreat στοχεύει στην ίδρυση νεοφυής επιχείρησης για την περαιτέρω ανάπτυξη του έργου.

Η ημερομηνία υποβολής της πρότασης ήταν η 16η Νοεμβρίου 2022 και οι εμπλεκόμενες χώρες είναι η Φινλανδία, Ιταλία, Ιρλανδία, Ισπανία, Ελλάδα, Φινλανδία, Κροατία, Ρουμανία, και Ελβετία.

Το έργο, αν εγκριθεί, αναμένεται ότι θα ξεκινήσει εντός του 2023 και θα έχει διάρκεια 36 μήνες με συνολικό προϋπολογισμό €6.780.739,25.

9.3.3 SYNAPSE

Το έργο SYNAPSE στοχεύει στο σχεδιασμό, την ανάπτυξη και την δημιουργία μιας Ολοκληρωμένης Πλατφόρμας Διαχείρισης Κινδύνων και Ανθεκτικότητας στην Κυβερνοασφάλεια. Η προτεινόμενη πλατφόρμα θα περιλαμβάνει:

- την ανταπόκριση σε περιστατικά μέσω μηχανισμών αυτοματοποίησης και ενορχήστρωσης διαδικασιών, καλύπτοντας επίσης οργανωτικές / επιχειρηματικές πτυχές.
- την εξαγωγή και ανάλυση κυβερνοαπειλών για επίγνωση της κατάστασης μέσα από Τεχνητή Νοημοσύνη,
- συστήματα έγκαιρης προειδοποίησης επιθέσεων και κυνηγιού απειλών (threat hunting),
- προσαρμοσμένες μεθόδους εκπαίδευσης για την ασφάλεια στον κυβερνοχώρο, το απόρρητο και την επιχειρησιακή συνέχεια,
- η διαχείριση τεχνικού και οικονομικού κινδύνου υποστηρίζοντας αναλύσεις κινδύνου-οφέλους (συμπεριλαμβανομένων των σεναρίων what-if),
- την ενημέρωση για λήψη αποφάσεων και ενεργοποίηση συστημάτων μεταφοράς κινδύνου με ασφάλιση μέσω έξυπνων συμβολαίων (smart contract-enabled).

Η ημερομηνία υποβολής της πρότασης ήταν η 16η Νοεμβρίου 2022 και οι εμπλεκόμενες χώρες ήταν Ιταλία, Γερμανία, Ελλάδα, Ισπανία, Ιρλανδία, Πολωνία, Νορβηγία και Ελβετία.

Το έργο, αν εγκριθεί, αναμένεται ότι θα ξεκινήσει εντός του 2023 θα έχει διάρκεια 3 χρόνια με συνολικό προϋπολογισμό €7.629.500.

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 2022 η ΑΨΑ διεξήγαγε για πρώτη φορά δύο παγκύπριες έρευνες για τη συλλογή στοιχείων και πληροφοριών για την κυβερνοασφάλεια στην Κυπριακή επικράτεια[14]. Τα κυριότερα θέματα που αξιολογήθηκαν αφορούσαν τον τρόπο χειρισμού θεμάτων κυβερνοασφάλειας ή/και ψηφιακής ασφάλειας, την αποτίμηση της σημαντικότητας που αποδίδεται στα σχετικά 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 έρευνες διεξήχθησαν παράλληλα τους μήνες Οκτώβριο-Νοέμβριο 2022 σε δείγμα 1025 πολιτών και 450 επιχειρήσεων, από ένα ευρύ φάσμα στους τομείς της βιομηχανίας, του εμπορίου και των υπηρεσιών.

Τα κυριότερα αποτελέσματα των ερευνών ήταν τα ακόλουθα:

Στις επιχειρήσεις:

- Σχεδόν οι μισές επιχειρήσεις (46%) δέχθηκαν κάποια επίθεση/παραβίαση τους τελευταίους 12 μήνες, με μέσο όρο 3-4 επιθέσεις τον μήνα.
- Από τις επιχειρήσεις που δέχθηκαν επίθεση, για τις μισές σχεδόν (48%) υπήρξε οικονομικό κόστος που ανέρχεται σε σχεδόν €23.000 κατά μέσο όρο.
- Η πιο συχνή επίθεση που δέχονται οι επιχειρήσεις είναι το phishing, δηλαδή απατηλά μηνύματα μέσω ηλεκτρονικού ταχυδρομείου με ποσοστό 36%.
- Σχεδόν μία στις πέντε επιχειρήσεις έχει περισσότερο από 2 χρόνια να προβεί σε δημιουργία ή ενημέρωση ή αναθεώρηση των πολιτικών τους για την κυβερνοασφάλεια ώστε να συμβαδίζουν με τις τεχνολογικές εξελίξεις.
- Υπάρχει άγνοια των επιχειρήσεων για σεμινάρια που προσφέρονται με θέμα την κυβερνοασφάλεια, αφού οι μισές επιχειρήσεις 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.

Στους πολίτες

- Το 40% των πολιτών δέχθηκε επίθεση τους τελευταίους 12 μήνες, με την πιο συχνή επίθεση που δέχονται οι πολίτες να είναι επίσης το phishing, δηλαδή απατηλά μηνύματα μέσω ηλεκτρονικού ταχυδρομείου με 30% και με μέσο όρο 20,9 παραβιάσεις/επιθέσεις τον χρόνο.
- Από τους πολίτες που δέχθηκαν επίθεση, για το 19% υπήρξε κάποιο κόστος που ανέρχεται στα €318 κατά μέσο όρο.
- Στην περίπτωση των πολιτών που δεν δέχτηκαν κάποιου είδους επίθεση/παραβίαση τους τελευταίους 12 μήνες, το 82% δεν αποκλείουν το ενδεχόμενο να πέσουν θύμα κακόβουλης επίθεσης στο μέλλον.
- Υπάρχει άγνοια των πολιτών για προσφερόμενα σεμινάρια για θέματα που αφορούν την κυβερνοασφάλεια, αφού το 82% δήλωσε άγνοια για αυτά ενώ μόνο το 9% 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 αποφυγή ύποπτων ιστοσελίδων και η συχνή αλλαγή κωδικών.

Οι έρευνες αυτές αποτελούν μια πρώτη χαρτογράφηση της εικόνας σε επιχειρήσεις και πολίτες σε θέματα κυβερνοασφάλειας. Αναμένεται αφενός να υπάρξει διαχρονική συλλογή των στοιχείων σε ετήσια βάση, και αφετέρου εμπλουτισμός των ερωτηματολογίων με βάση τις εξελίξεις και τις ανάγκες σε πληροφόρηση που θα προκύπτουν.

[14] *https://dsa.cy/category/press-releases/consumers-survey*

ΟΙΚΟΝΟΜΙΚΑ

11. ΜΗ ΕΛΕΓΜΕΝΕΣ ΟΙΚΟΝΟΜΙΚΕΣ ΚΑΤΑΣΤΑΣΕΙΣ ΓΙΑ ΤΟ ΕΤΟΣ 2022

Οι οικονομικές καταστάσεις της ΑΨΑ για το έτος που έληξε την 31η Δεκεμβρίου 2022, ετοιμάστηκαν όπως προβλέπεται από το άρθρο 48 του Ν. 89(Ι)/2020. Οι βασικότερες πληροφορίες για την καταγραφή δαπανών και εσόδων, που περιέχονται στις προκαταρτικές μη ελεγμένες οικονομικές καταστάσεις για το έτος που έληξε στις 31 Δεκεμβρίου 2022, απεικονίζονται στον Πίνακα 3 και Πίνακα 4 και στο Γράφημα 9 και περιλαμβάνουν:

Πίνακας 3: Μη Ελεγμένη Κατάσταση Συνολικών Εισοδημάτων 2022

	2022 €	2021 €
Έσοδα		
Εισοδήματα*	9,174,228	5,783,122
Άλλα έσοδα	-	-
	9,174,228	**5,783,122**
Έξοδα		
Κόστος Προσωπικού	186,667	-
Έξοδα Χρηματοδότησης (Τόκοι)	-	33,085
Λειτουργικά έξοδα γραφείου	2,110,370	814,538
Μίσθωση υπηρεσιών	1,439,935	1,500,463
Αποσβέσεις εξοπλισμού και εγκαταστάσεων	359,157	42,439
Αποσβέσεις άϋλου ενεργητικού	95,446	44,744
	4,191,575	**2,435,269**
Πλεόνασμα έτους από συνήθεις εργασίες	4,982,653	3,347,853
Συνολικά εισοδήματα για το έτος	**4,982,653**	**3,347,853**

Σημείωση: Τα στοιχεία αφορούν τις προκαταρτικές μη ελεγμένες οικονομικές καταστάσεις και δύναται να αναπροσαρμοστούν με την ετοιμασία των ελεγμένων οικονομικών καταστάσεων.

* Τα Εισοδήματα της ΑΨΑ προέρχονται από τέλη, συγχρηματοδοτούμενα προγράμματα και εκτέλεση έργων για άλλα Τμήματα/Υπουργεία.

Πίνακας 4: Μη Ελεγμένη Κατάσταση Χρηματοοικονομικής Θέσης στις 31 Δεκεμβρίου 2022

	2022 €	2021 €
ΠΕΡΙΟΥΣΙΑΚΑ ΣΤΟΙΧΕΙΑ		
Μη κυκλοφορούντα περιουσιακά στοιχεία		
Εγκαταστάσεις και εξοπλισμός	1,438,854	1,009,513
Άϋλα στοιχεία ενεργητικού	188,786	286,812
Σύνολο μη κυκλοφορούντων περιουσιακών στοιχείων	**1,627,640**	**1,296,325**
Κυκλοφορούντα περιουσιακά στοιχεία		
Χρεώστες και προπληρωμές	8,201,115	7,857,609
Μετρητά στην τράπεζα	9,787,649	5,523,690
Σύνολο κυκλοφορούντων περιουσιακών στοιχείων	**17,988,764**	**13,381,299**
ΣΥΝΟΛΟ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ	**19,616,679**	**14,677,624**
ΙΔΙΑ ΚΕΦΑΛΑΙΑ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ		
Ίδια κεφάλαια		
Αποθεματικά	6,496,679	(3,484,101)
Σύνολο ιδίων κεφαλαίων	**6,496,679**	**(3,484,101)**
Τρέχουσες υποχρεώσεις		
Πιστωτές και οφειλόμενα έξοδα	5,402,406	6,537,093
Προεισπραχθέντα τέλη	7,717,319	8,418,460
Κρατική χορηγία	-	3,206,172
Ολικό τρεχουσών υποχρεώσεων	**13,119,725**	**18,161,725**
ΟΛΙΚΟ ΙΔΙΩΝ ΚΕΦΑΛΑΙΩΝ ΚΑΙ ΥΠΟΧΡΕΩΣΕΩΝ	**19,616,404**	**14,677,624**

Σημείωση: Τα στοιχεία αφορούν τις προκαταρτικές μη ελεγμένες οικονομικές καταστάσεις και δύναται να αναπροσαρμοστούν με την ετοιμασία των ελεγμένων οικονομικών καταστάσεων.

Γράφημα 9: Κατανομή Δαπανών για το 2022