ΑΡΧΗ ΨΗΦΙΑΚΗΣ
ΑΣΦΑΛΕΙΑΣ

Έκθεση Δραστηριοτήτων του έτους 2020

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

Αύγουστος 2021

ΠΕΡΙΕΧΟΜΕΝΑ

ΧΑΙΡΕΤΙΣΜΟΣ ΕΠΙΤΡΟΠΟΥ

Η παρούσα έκθεση απολογισμού του έργου της Αρχής Ψηφιακής Ασφάλειας συνοψίζει το σύνολο των δραστηριοτήτων της Αρχής σε όλο το φάσμα των πεδίων αρμοδιότητας της κατά το έτος 2020.

Η Αρχή Ψηφιακής Ασφάλειας είναι η αρμόδια αρχή για την υλοποίηση της Ευρωπαϊκής Οδηγίας NIS (Network and Information Security Directive), με έμφαση στη βελτίωση και διατήρηση υψηλών επιπέδων Κυβερνοασφάλειας για όλους τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και Φορείς Κρίσιμων Υποδομών Πληροφοριών στην Κυπριακή Δημοκρατία. Βασικές Υπηρεσίες ορίζονται οι υπηρεσίες στους τομείς της ενέργειας, μεταφορών, υγείας, προμήθειας και διανομής νερού, οι τράπεζες, οι υποδομές χρηματοπιστωτικών αγορών και οι ψηφιακές υποδομές, ενώ ως Κρίσιμες Υποδομές Πληροφοριών ορίζονται οι Ηλεκτρονικές Επικοινωνίες, οι κυβερνητικές υπηρεσίες, οι υπηρεσίες ασφάλειας και έκτακτης ανάγκης, και τα συστήματα αποχέτευσης. Η λειτουργία της Αρχής Ψηφιακής Ασφάλειας είναι απαραίτητη για τη βελτίωση των επιπέδων και ικανοτήτων Κυβερνοασφάλειας στην Κύπρο, θωρακίζοντας την κοινωνία μας και ενισχύοντας τη διεθνή μας ανταγωνιστικότητα με συνεπαγόμενη συμβολή στην εθνική οικονομία.

Αποστολή της Αρχής Ψηφιακής Ασφάλειας είναι η 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. Επιπρόσθετα, ο τεχνικός και επιχειρησιακός τομέας της Αρχής, το Εθνικό CSIRT-CY[1], έχει ως κύριο στόχο την προληπτική και ενεργή αντιμετώπιση κυβερνο-απειλών, ενισχύοντας με τον τρόπο αυτό την ψηφιακή ασφάλεια όλων των σημαντικών υποδομών και υπηρεσιών της χώρας. Η Αρχή Ψηφιακής Ασφάλειας στελεχώνεται από εξειδικευμένους επαγγελματίες των κλάδων της Πληροφορικής, της Κυβερνοασφάλειας και Κυβερνο-διακυβέρνησης.

Αναφέρω συνοπτικά κάποια από τα σημαντικά επιτεύγματα της Αρχής Ψηφιακής Ασφάλειας κατά το 2020:

- εφαρμογή του Εθνικού Πλαισίου Κυβερνοασφάλειας που διέπει τον τρόπο αναγνώρισης και εφαρμογής των κατάλληλων μέτρων ασφάλειας για τις κρίσιμες υποδομές πληροφοριών
- εφαρμογή και δημοσίευση του πλαισίου κοινοποίησης συμβάντων και περιστατικών ασφάλειας στην ΑΨΑ
- εφαρμογή του πλαισίου μέτρων ασφάλειας για τα νέα δίκτυα επικοινωνιών πέμπτης γενεάς (5G) σε εθνικό επίπεδο
- ανάληψη του ρόλου της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας
- διοργάνωση εγχώριων και περιφερειακών εκπαιδεύσεων για την ασφάλεια στον κυβερνοχώρο και τις πιστοποιήσεις Κυβερνοασφάλειας
- χρηματοδοτήσεις από Ευρωπαϊκές πηγές ύψους 71.984 ευρώ (βάσει ταμειακών εισροών) για υλοποίηση προγραμμάτων

Εντός του 2020, ψηφίστηκε από τη Βουλή των Αντιπροσώπων και δημοσιεύτηκε ο νέος Νόμος σχετικά με την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών, ο οποίος περιγράφει με πλήρη λεπτομέρεια τις ολοκληρωμένες αρμοδιότητες της ΑΨΑ, μεταφέροντας πλήρως την Οδηγία NIS στην Εθνική Νομοθεσία. Το νομοσχέδιο ρυθμίζει θέματα προσωπικού, εσωτερικής λειτουργίας της ΑΨΑ και συνεργασίας της με άλλους αρμόδιους φορείς. Επίσης, ψηφίστηκαν και δημοσιεύτηκαν οι Κανονισμοί Επιλογής και Προαγωγών της ΑΨΑ, ως επίσης και οι Κανονισμοί Χρηματοδότησης της Αρχής Ψηφιακής Ασφάλειας.

Εκτός από την υποστήριξη των παραπάνω Κρίσιμων Υποδομών Πληροφοριών, η Αρχή Ψηφιακής Ασφάλειας, εντός του 2020, ανέλαβε μεγάλο αριθμό δράσεων ενημέρωσης και ευαισθητοποίησης των πολιτών σχετικά με τις επιπτώσεις των απειλών στον κυβερνοχώρο. Παρείχε πληροφορίες μέσω του διαδικτύου για σημαντικές απειλές στον κυβερνοχώρο, αλλά και τεχνικές συμβουλές και οδηγίες για την εξασφάλιση ψηφιακής προστασίας. Εν μέσω πανδημίας, η Υπηρεσία, μέσα από δημοσιεύσεις σε ηλεκτρονικά και έντυπα Μέσα Μαζικής Ενημέρωσης και μέσα από συνεντεύξεις σε εφημερίδες, ραδιόφωνο και τηλεόραση, παρείχε γενικότερη πληροφόρηση επί διαφόρων πτυχών της Κυβερνοασφάλειας, συμπεριλαμβανομένων

[1] CSIRT - Computer Security Incident Response Team (Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων)

των τεχνικών παραπληροφόρησης και ψηφιακής απάτης. Επίσης, το Εθνικό CSIRT-CY διοργάνωσε εκπαιδεύσεις μέσω διαδικτυακών παρουσιάσεων σχετικά με την «Ασφαλή Εργασία από το Σπίτι» καθώς και «Κυβερνοασφάλεια για Διαχειριστές Συστημάτων» Επίσης, μέσω του CSIRT-CY, χειρίστηκε αιτήματα των Κρίσιμων Υποδομών Πληροφοριών σε σχέση με την ασφάλεια των δικτύων και συστημάτων πληροφοριών τους μέσω ηλεκτρονικού ταχυδρομείου, της ιστοσελίδας του ή της Γραμμής Βοήθειας (1490). Εντός του έτους 2020, πραγματοποίησε δεκάδες παρουσιάσεις ευαισθητοποίησης γύρω από την Κυβερνοασφάλεια στις Κρίσιμες Υποδομές Πληροφοριών, ενώ παρείχε διαδραστικά σεμινάρια για την ευαισθητοποίηση στο θέμα της Κυβερνοασφάλειας σε μαθητές σχολείων της Κύπρου, καλύπτοντας ένα μεγάλο αριθμό μαθητών και καθηγητών αναφορικά με τρόπους ασφαλούς χρήσης του Διαδικτύου και άλλων ψηφιακών τεχνολογιών.

Κατά το 2020, ο τεχνικός και επιχειρησιακός βραχίονας της Αρχής Ψηφιακής Ασφάλειας, το Εθνικό CSIRT-CY ανταποκρίθηκε σε περιστατικά που αφορούσαν διάφορες κατηγορίες κυβερνοεπιθέσεων, όπως Intrusion, Phishing, Cryptomining, Ransomware και Malware. Η διαχείριση περιστατικών αφορούσε εντοπισμό των επιθέσεων και των επηρεαζόμενων συστημάτων, ενέργειες μετριασμού καθώς και αναγνώριση της συμπεριφοράς και δράσης των επιτιθέμενων. Στο πλαίσιο της υποστήριξης των Κρίσιμων Υποδομών Πληροφοριών δόθηκαν οδηγίες και προτεινόμενα μέτρα ασφάλειας για αντιμετώπιση και αποφυγή μελλοντικών παρόμοιων επιθέσεων.

Η Αρχή Ψηφιακής Ασφάλειας δίνει ιδιαίτερη έμφαση στις σχέσεις της με Ευρωπαϊκούς και Διεθνείς οργανισμούς στον ευρύτερο τομέα. Συμμετέχει ενεργά σε μεγάλο αριθμό Ευρωπαϊκών και άλλων διεθνών ομάδων εργασίας για ολόκληρο το φάσμα Κυβερνοασφάλειας, εκπροσωπώντας την Κυπριακή Δημοκρατία στον Ευρωπαϊκό Οργανισμό για την Κυβερνοασφάλεια, το ENISA (European Union Agency for Cybersecurity), την Ομάδα Συνεργασίας για την Ασφάλεια Δικτύων και Πληροφοριών (NIS Cooperation Group) και την Ευρωπαϊκή Ομάδα Πιστοποίησης Κυβερνοασφάλειας (European Cybersecurity Certification Group). Επίσης, το Εθνικό CSIRT-CY είναι μέλος του Πανευρωπαϊκού Δικτύου CSIRTs (CSIRT Network) και το Μάρτιο 2020 έχει αξιολογηθεί ότι βρίσκεται στο μέγιστο επίπεδο ωριμότητας του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών ENISA. Το Εθνικό CSIRT-CY είναι, από το 2019, αναγνωρισμένος συνεργάτης (Accredited Member) του φορέα Trusted Introducer (TI), καθώς και μέλος του παγκόσμιου συνδέσμου Forum of Incident Response and Security Teams (FIRST) που αφορά ομάδες CSIRT παγκοσμίως.

Μια σημαντική εξέλιξη το 2020 ήταν ο ορισμός της ΑΨΑ ως η αρμόδια εθνική αρχή πιστοποίησης Κυβερνοασφάλειας, με το Υπουργικό Συμβούλιο να της δίνει την εντολή να λάβει τα απαραίτητα μέτρα για να συμπεριλάβει τις σχετικές πρόνοιες στη νομοθεσία της για την εφαρμογή του Κανονισμού για την Κυβερνοασφάλεια στην Κύπρο, και να προωθήσει την ανάπτυξη τουλάχιστον ενός οργανισμού στην Κύπρο με τις κατάλληλες τεχνικές και οργανωτικές ικανότητες για να λειτουργήσει ως οργανισμός αξιολόγησης της συμμόρφωσης. Με αυτόν τον τρόπο, η Κυπριακή Δημοκρατία θα διασφαλίσει ότι μπορεί να προσφέρει το «ολοκληρωμένο πακέτο», με ανεπτυγμένες δομές ώστε να είναι σε θέση να χειρίζεται πιστοποιήσεις Κυβερνοασφάλειας, με τα σχετικά αναμενόμενα οφέλη για τη χώρα.

Η Κυβερνοασφάλεια είναι μια πραγματικότητα που επηρεάζει τις καθημερινές δραστηριότητες και ενέργειες του κράτους και των πολιτών, καθιστώντας την Αρχή Ψηφιακής Ασφάλειας ως την ασπίδα προστασίας της πολιτείας και της κοινωνίας έναντι επιβουλών οποιωνδήποτε επιδιώκουν να επηρεάσουν την ομαλή λειτουργία και ανάπτυξη του τομέα της ηλεκτρονικής επικοινωνίας. Κλείνοντας, θα ήθελα να μεταφέρω το μήνυμα ότι η Αρχή Ψηφιακής Ασφάλειας δεσμεύεται να συνεχίσει με τον ίδιο ζήλο το έργο της για την επίτευξη των στόχων της και την εδραίωση ενός ασφαλούς ψηφιακού περιβάλλοντος για κάθε πολίτη της Κύπρου.

Γιώργος Μιχαηλίδης

Επίτροπος Επικοινωνιών

1. ΔΙΟΙΚΗΣΗ

Η Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) λειτουργεί βάσει του Νόμου 89(Ι)/2020 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών και υπάγεται στον Επίτροπο Επικοινωνιών κ. Γιώργο Μιχαηλίδη και το Βοηθό Επίτροπο κ. Πέτρο Γαλίδη.

1.1. Όραμα Αρχής Ψηφιακής Ασφάλειας

Το Όραμα της ΑΨΑ είναι όπως η Κύπρος καταστεί μια από τις πρωτοπόρες χώρες της περιοχής στα θέματα υπηρεσιών 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 χρηματοοικονομικές υπηρεσίες.

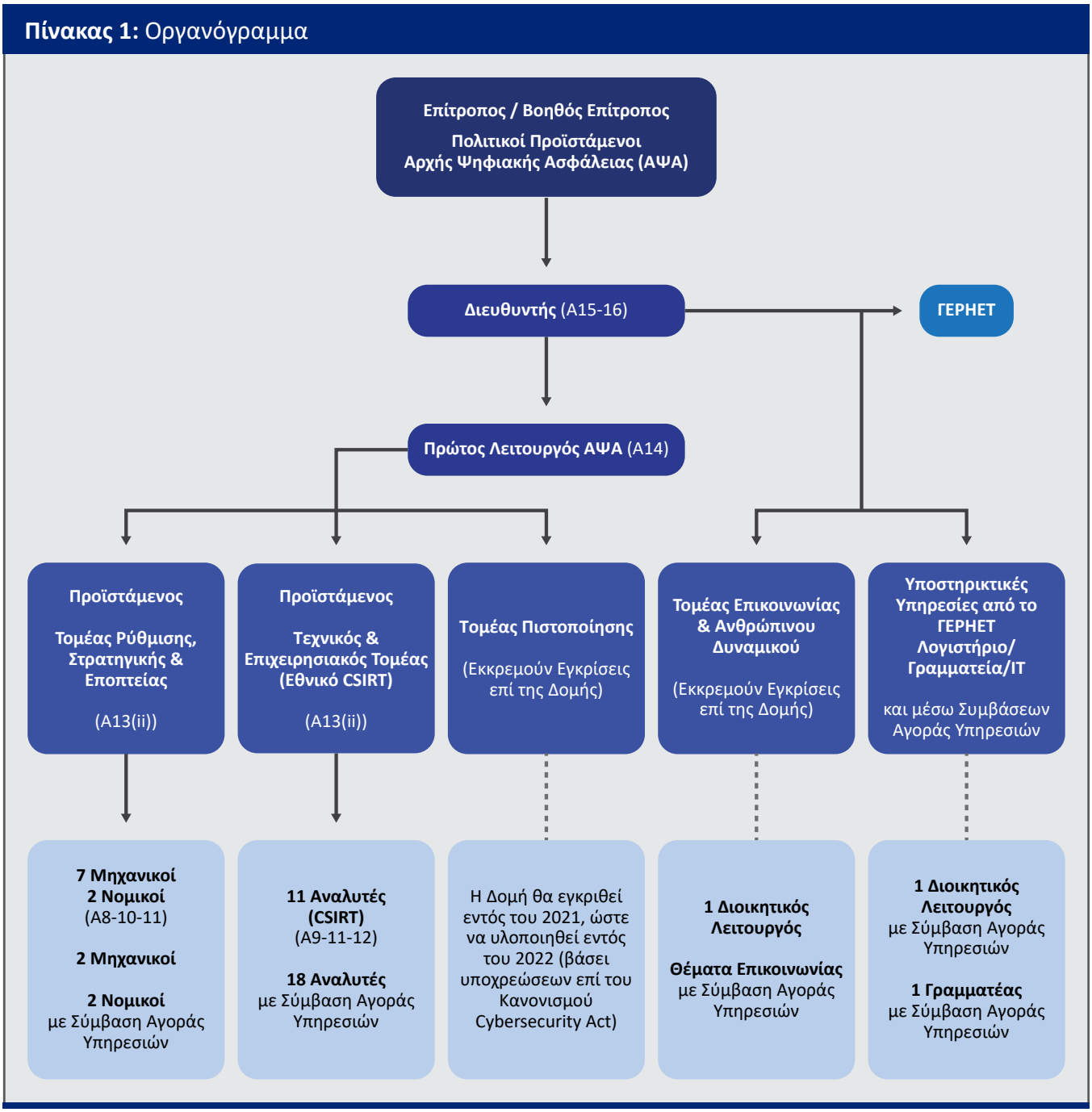
1.2. Στόχοι Αρχής Ψηφιακής Ασφάλειας

Η ΑΨΑ αποσκοπεί 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 και όλους τους εμπλεκόμενους φορείς
- την ανάπτυξη εμπιστοσύνης μεταξύ όλων των εμπλεκομένων 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) για 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 και 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 υψηλό βαθμό τις ταχύτατα εξελισσόμενες απειλές από τον κυβερνοχώρο, και κατ' επέκταση τις εξελίξεις στον τομέα της Κυβερνοασφάλειας για την αναβάθμιση της ασφάλειας των κρίσιμων τομέων της Κυπριακής Δημοκρατίας

1.3. Οργανωτική Δομή

Πίνακας 1: Οργανόγραμμα



Η προγραμματισμένη οργανωτική δομή της ΑΨΑ παρουσιάζεται στον Πίνακα 1, στον οποίο αποτυπώνονται ενδεικτικά οι τομείς αρμοδιότητας της Αρχής.

1.3.1. Τομέας Ρύθμισης, Στρατηγικής και Εποπτείας

Ο Τομέας Ρύθμισης, Στρατηγικής και Εποπτείας αποτελεί το ρυθμιστικό βραχίονα της ΑΨΑ, σε θέματα επιχειρησιακής συνέχειας των δικτύων πληροφοριακών συστημάτων των ουσιωδών και κρίσιμων υποδομών της χώρας.

Στόχος του Τομέα Ρύθμισης είναι να προάγει την επίτευξη υψηλού επιπέδου ασφάλειας δικτύων και συστημάτων πληροφοριών, συμπεριλαμβανομένων όλων των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών / Φορέων Κρίσιμων Υποδομών Πληροφοριών της Δημοκρατίας και των παροχέων ψηφιακών υπηρεσιών που έχουν την έδρα τους στη Δημοκρατία, καθώς και η ασφαλής λειτουργία των επικοινωνιών και των συστημάτων πληροφοριών προς όφελος όλων των πολιτών, της οικονομίας και της χώρας ευρύτερα. Βασικές Υπηρεσίες ορίζονται οι υπηρεσίες στους τομείς της ενέργειας, μεταφορών, υγείας, προμήθειας και διανομής πόσιμου νερού, οι τράπεζες, οι υποδομές χρηματοπιστωτικών αγορών και οι ψηφιακές υποδομές, ενώ Κρίσιμες Υποδομές Πληροφοριών ορίζονται ως οι ηλεκτρονικές επικοινωνίες, οι κυβερνητικές υπηρεσίες, οι υπηρεσίες ασφάλειας και έκτακτης ανάγκης και οι αποχετεύσεις.

Ο Ρυθμιστικός τομέας συντονίζει επίσης την υλοποίηση της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας.

Η λειτουργία του τομέα Ρύθμισης, Στρατηγικής και Εποπτείας περιλαμβάνει, μεταξύ άλλων, τις ακόλουθες υπηρεσίες:

- ετοιμασία Πρωτογενούς και Δευτερογενούς Νομοθεσίας και καθορισμός ρυθμιστικού πλαισίου Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών
- διενέργεια Αξιολόγησης Κρισιμότητας και αναθεώρηση καταλόγου κρίσιμων Υποδομών Πληροφοριών
- διενέργεια Αξιολόγησης Κινδύνων Κυβερνοασφάλειας σε εθνικό επίπεδο
- υλοποίηση δράσεων βάσει αποτελεσμάτων αξιολόγησης επικινδυνότητας
- καθορισμός πλαισίου μέτρων ασφάλειας και ελέγχου συμμόρφωσης
- καθορισμός διαδικασιών κοινοποίησης περιστατικών παραβίασης ασφάλειας
- εποπτεία εφαρμογής πλαισίου Κυβερνοασφάλειας από φορείς εκμετάλλευσης βασικών υπηρεσιών, φορείς κρίσιμων υποδομών πληροφοριών, παροχέων ηλεκτρονικών επικοινωνιών και παροχέων ψηφιακών υπηρεσιών
- διαχείριση κρίσεων σε σχέση με θέματα Ασφάλειας Δικτύων και Πληροφοριών και Κυβερνοασφάλειας
- ανάπτυξη και διαχείριση της υλοποίησης της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας
- επιμόρφωση και ενημέρωση σε θέματα που αφορούν την Κυβερνοασφάλεια
- συμμετοχή σε ευρωπαϊκά και διεθνή σώματα, επιτροπές και κοινότητες
- συμμετοχή σε ευρωπαϊκά συγχρηματοδοτούμενα προγράμματα
- προετοιμασία για λειτουργία της ΑΨΑ ως Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας.

1.3.2. Τεχνικός και Επιχειρησιακός Τομέας – Εθνικό CSIRT

Το Εθνικό CSIRT (Computer Security Incident Response Team), δηλαδή η Εθνική Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων, αποτελεί τον τεχνικό και επιχειρησιακό βραχίονα της ΑΨΑ στα θέματα διαχείρισης περιστατικών Κυβερνοασφάλειας και είναι υπεύθυνο για την πρόληψη και διαχείριση συμβάντων κυβερνοεπιθέσεων στις κρίσιμες υποδομές πληροφοριών της Κυπριακής Δημοκρατίας.

Στόχος του Εθνικού CSIRT είναι η πρόληψη και η ετοιμότητα εσωτερικής ασφάλειας, καθώς 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 την κοινωνικοοικονομική ζωή των πολιτών. Συντονίζει και προσφέρει υποστήριξη στους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και Φορείς Κρίσιμων Υποδομών Πληροφοριών, ώστε να εξασφαλίσουν ένα ελάχιστο επίπεδο ασφάλειας, εφαρμόζοντας πρακτικές προληπτικής δράσης και αντίδρασης με στόχο τη μείωση των κινδύνων στο εσωτερικό τους δίκτυο από περιστατικά ασφάλειας στον κυβερνοχώρο, ενώ είναι σε θέση να ανταποκρίνεται σε τέτοιου είδους περιστατικά όταν αυτά συμβούν. Το Εθνικό CSIRT αναλαμβάνει, επίσης, δράσεις ευαισθητοποίησης προκειμένου να εκπαιδεύσει τους πολίτες της Κυπριακής Δημοκρατίας και τους διάφορους εθνικούς φορείς σχετικά με τις δυσμενείς επιπτώσεις των απειλών στον κυβερνοχώρο.

Το Εθνικό CSIRT διαθέτει ολοκληρωμένες διαδικασίες λειτουργίας, διαχείρισης περιστατικών και ασφάλειας δικτύου, καθώς και συστήματα και εργαλεία πληροφορικής υψηλών προδιαγραφών, ενώ είναι πλήρες μέλος της κοινότητας των CSIRT σε διεθνές και ευρωπαϊκό επίπεδο (FIRST[2], TI[3]).

Το Εθνικό CSIRT παρέχει, μεταξύ άλλων, τις ακόλουθες υπηρεσίες:

- υπηρεσίες αποκατάστασης, οι οποίες ενεργοποιούνται μετά από καταστροφικά περιστατικά όπου υπάρχει απώλεια υπηρεσίας ή πληροφοριών
- υπηρεσίες πρόληψης καταστροφικών περιστατικών
- υπηρεσίες διαχείρισης/χειρισμού τεκμηρίων ασφάλειας πληροφορίας μετά από καταστροφικά περιστατικά
- υπηρεσίες διαχείρισης ποιότητας της ασφάλειας δικτύων και πληροφοριών

1.3.3. Τομέας Πιστοποίησης Κυβερνοασφάλειας

Ο Τομέας Πιστοποίησης Κυβερνοασφάλειας αποτελεί νέο τομέα της Αρχής Ψηφιακής Ασφάλειας, ο οποίος δημιουργήθηκε για να αναλάβει τα θέματα που προκύπτουν από την υλοποίηση των απαιτήσεων του Κανονισμού (ΕΕ) 2019/881 για την Κυβερνοασφάλεια, καθώς η Αρχή Ψηφιακής Ασφάλειας έχει αναλάβει το ρόλο της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας (βλ. ενότητα 6).

Ο στόχος του Τομέα Πιστοποίησης Κυβερνοασφάλειας είναι να προάγει το θεσμό της πιστοποίησης Κυβερνοασφάλειας και να αναπτύξει τις σχετικές ικανότητες της Κυπριακής Δημοκρατίας, με απώτερο στόχο η Κύπρος να καταστεί περιφερειακό κέντρο πιστοποιήσεων, με όλα τα συνεπαγόμενα οφέλη. Ο τομέας αυτός θα εκτελεί τις λειτουργίες της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας, συμπεριλαμβανομένων της αδειοδότησης και εποπτείας των οργανισμών αξιολόγησης της συμμόρφωσης, της εποπτείας της αγοράς όσον αφορά σε πιστοποιημένα προϊόντα και κατασκευαστές, τη συνεργασία με σχετικούς φορείς στην Κύπρο και τη συμμετοχή στα αρμόδια Ευρωπαϊκά σώματα (ECCG - European Cybersecurity Certification Group).

1.4. Στελέχωση

Κατά το 2020, τρεις (3) μόνιμοι υπάλληλοι από το ΓΕΡΗΕΤ (Γραφείο Επιτρόπου για τη Ρύθμιση Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων), και συγκεκριμένα 1 Ανώτερος Λειτουργός, 1 Λειτουργός και 1 Γραμματέας, συνέχισαν να απασχολούνται με τις εργασίες της ΑΨΑ στον τομέα της υλοποίησης της Ευρωπαϊκής Οδηγίας για την Ασφάλεια Δικτύων και Πληροφοριών και της Εθνικής Στρατηγικής για την Κυβερνοασφάλεια. Η ομάδα του Εθνικού CSIRT απαρτίζεται από δεκατέσσερα (14) άτομα: ένα (1) προϊστάμενο και δεκατρείς (13) αναλυτές, ενώ στον Ρυθμιστικό Τομέα απασχολούνται άλλα τέσσερα (4) άτομα: δύο (2) νομικοί, μία (1) διοικητική και μία (1) γραφέας.

[1] FIRST: Forum of Incident Response and Security Teams
[2] TI: Trusted Introducer

Με την ψήφιση της αναθεωρημένης νομοθεσίας της ΑΨΑ και των Κανονισμών Πρόσληψης Προσωπικού, οι οποίες αναμένεται να ολοκληρωθούν εντός του 2021, θα προκηρυχθούν έντεκα (11) νέες θέσεις εργασίας για τη στελέχωση του Τομέα Ρύθμισης, Στρατηγικής και Εποπτείας, και επιπρόσθετα δώδεκα (12) θέσεις εργασίας για τη μόνιμη στελέχωση του Εθνικού CSIRT.

1.5. Εναρμόνιση με το Ευρωπαϊκό Πλαίσιο για την Ασφάλεια Δικτύων και Πληροφοριών και την Κυβερνοασφάλεια

Τον Αύγουστο του 2020 η Βουλή των Αντιπροσώπων ψήφισε το Νόμο 89(Ι)/2020 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών, ο οποίος εναρμονίζει πλήρως την εθνική νομοθεσία με το ευρωπαϊκό νομικό πλαίσιο για την αποτελεσματικότερη εφαρμογή της Οδηγίας NIS και της Οδηγίας EECC (άρθρο 40 και 41) στα θέματα Ασφάλειας Δικτύων και Πληροφοριών. Ο Νόμος 17(Ι)/2018 καταργήθηκε και αντικαταστάθηκε από τον Νόμο 89(Ι)/2020.

1.6. Ανάπτυξη Πολιτικών και Διαδικασιών Εθνικού CSIRT

Κατά το 2020, το Εθνικό CSIRT-CY κατάρτισε, αναθεώρησε, επικαιροποίησε και εφάρμοσε διαδικασίες και πολιτικές που καλύπτουν όλες τις πτυχές λειτουργίας του Οργανισμού, όπως την ασφάλεια συστημάτων, την ασφάλεια δικτύου, και τις διαδικασίες λειτουργίας των στελεχών.

Το Εθνικό CSIRT-CY έχει αναπτύξει επίσης διαδικασία αντιμετώπισης κρίσιμων περιστατικών σε περιπτώσεις τόσο φυσικών καταστροφών, όσο και κρίσιμων περιστατικών Κυβερνοασφάλειας, και έχει δημιουργήσει ειδικές διαδικασίες για την αντιμετώπιση και τη διαχείριση περιστατικών Κυβερνοασφάλειας, όπως φαίνονται πιο κάτω:

- Διαχείριση περιστατικών (Incident Management)
  - Εγχειρίδιο Διαχείρισης Περιστατικών
  - Εγχειρίδιο Οδηγού Κυβερνοασφάλειας
  - Ανάπτυξη εφαρμογής διαχείρισης περιστατικών και ειδοποιήσεων
  - Ανάπτυξη εφαρμογής ανάλυσης διευθύνσεων IP που λαμβάνονται από εργαλεία
  - Ανάπτυξη εφαρμογής για την λήψη πληροφοριών από το VirusTotal[4] μέσω του VirusTotal API[5]
- Συλλογή πληροφοριών για απειλές (threat intelligence)
  - Ανάπτυξη εφαρμογής για καταχώρηση πληροφοριών για περιστατικά που λαμβάνουν χώρα διεθνώς
  - Ανάπτυξη εφαρμογής για καταχώρηση πληροφοριών για εγχώρια περιστατικά
  - Ανάπτυξη εφαρμογής για την καταχώρηση πληροφοριών για παράγοντες απειλής (threat actors)
  - Ανάπτυξη εφαρμογής για την καταχώρηση πληροφοριών για κακόβουλο λογισμικό
  - Ανάπτυξη εφαρμογής για τη λήψη πληροφοριών από την πλατφόρμα Anomali[6] μέσω της διεπαφής που ονομάζεται ThreatStream API
- Διαχείριση κακόβουλων λογισμικών (malware analysis)
  - Δημιουργία εφαρμογής ανάλυσης αρχείων καταγραφής από εργαλεία εντοπισμού κακόβουλων αρχείων (Loki και Thor) - έπεται η περαιτέρω ανάπτυξη της εφαρμογής για την ανάλυση αρχείων καταγραφής από το λογισμικό Splunk[7] και λειτουργικό σύστημα Windows
- Έλεγχο τρωτών σημείων (vulnerability testing)
  - Ανάπτυξη διαδικασίας για τη διενέργεια δοκιμών διείσδυσης (penetration testing procedure)

[4] Virus Total είναι μια διαδικτυακή υπηρεσία που αναλύει ύποπτα αρχεία και διευθύνσεις URL για τον εντοπισμό τύπων κακόβουλου λογισμικού και κακόβουλου περιεχομένου χρησιμοποιώντας μηχανές προστασίας από ιούς και σαρωτές ιστότοπων.

[5] API -Application Programming Interface - ή Διασύνδεση Προγραμματισμού Εφαρμογών, είναι η διεπαφή των προγραμματιστικών διαδικασιών που παρέχει ένα λειτουργικό σύστημα, βιβλιοθήκη ή εφαρμογή προκειμένου να επιτρέπει να γίνονται προς αυτά αιτήσεις από άλλα προγράμματα ή/και ανταλλαγή δεδομένων.

[6] Anomali – Πλατφόρμα που παρέχει πληροφορίες και έγκαιρη ανίχνευση απειλών και εξασφαλίζει τη μείωση του κινδύνου παραβιάσεων ασφαλείας και τη βελτίωση της παραγωγικότητας της ομάδας ασφαλείας.

[7] Splunk Enterprise – Λογισμικό που παρέχει γρήγορο τρόπο συγκέντρωσης, ανάλυσης και λήψης απαντήσεων από τα δεδομένα ενός δικτύου με τη βοήθεια της μηχανικής μάθησης και της ορατότητας σε πραγματικό χρόνο.

2. ΟΙΚΟΝΟΜΙΚΕΣ ΚΑΤΑΣΤΑΣΕΙΣ

2.1. Μη Ελεγμένες Οικονομικές Καταστάσεις για το έτος 2020

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

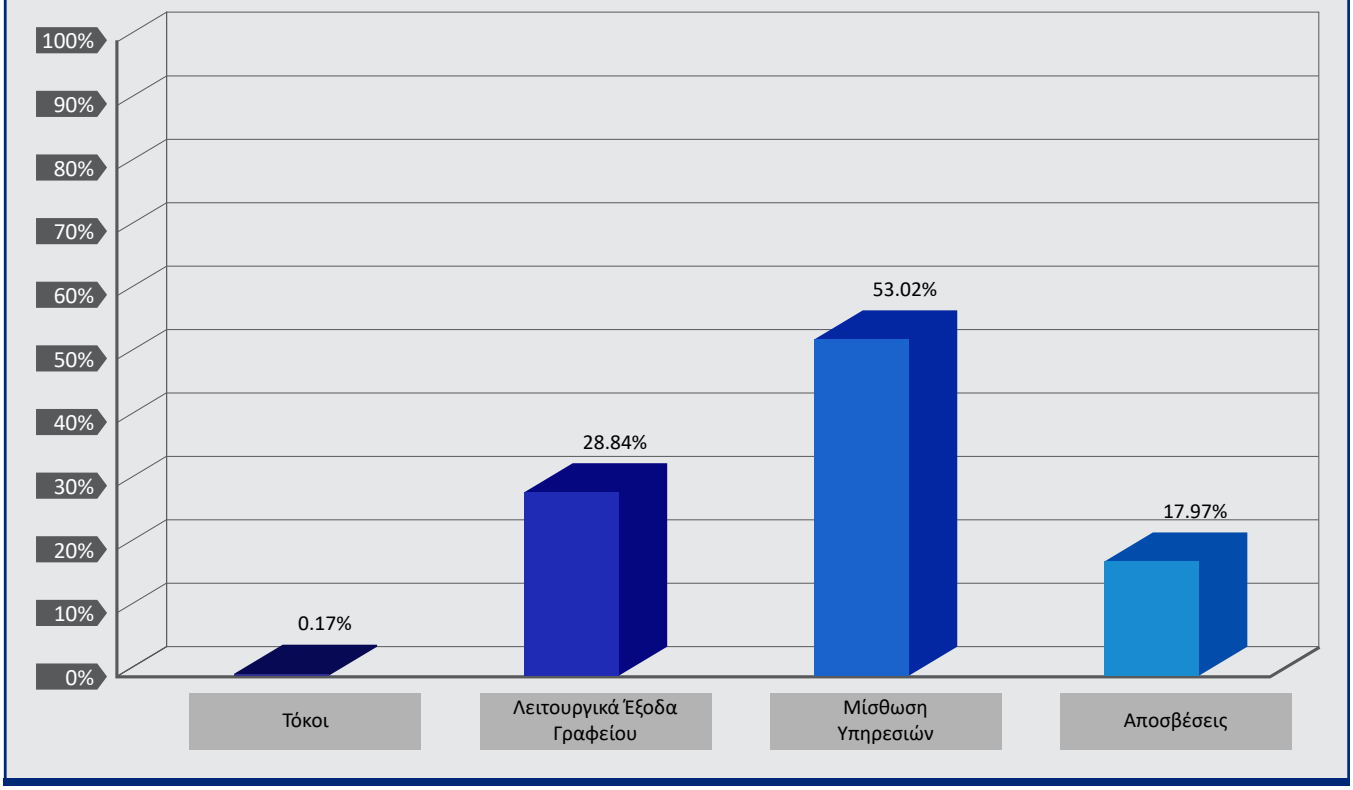
Πίνακας 2: Μη Ελεγμένη Κατάσταση Συνολικών Εισοδημάτων 2020

	2020 €	2019 €
Έσοδα		
Άλλα έσοδα*	1.723.437	1.473.324
Έσοδα Χρηματοδότησης (Τόκοι)	0	53
	1.723.437	**1.473.377**
Έξοδα		
Έξοδα Χρηματοδότησης (Τόκοι)	2.988	0
Λειτουργικά έξοδα γραφείου	508.223	307.161
Μίσθωση Υπηρεσιών	934.466	964.299
Αποσβέσεις εξοπλισμού και εγκαταστάσεων	222.249	126.136
Αποσβέσεις άυλου ενεργητικού	94.541	71.749
	1.762.467	**1.469.345**
Πλεόνασμα/(Έλλειμμα) έτους	(39.030)	4.032
Συνολικά εισοδήματα για το έτος	**(39.030)**	**4.032**

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

* Τα Άλλα Έσοδα προέρχονται από Ευρωπαϊκά συγχρηματοδοτούμενα προγράμματα καθώς επίσης και χορηγίες από το Υπουργείο Άμυνας για σκοπούς ανάπτυξης υποδομών κυβερνοάμυνας.

Γράφημα 1: Κατανομή Δαπανών για το 2020



Πίνακας 3: Μη Ελεγμένη Κατάσταση Χρηματοοικονομικής Θέσης στις 31 Δεκ. 2020

	2020 €	2019 €
ΠΕΡΙΟΥΣΙΑΚΑ ΣΤΟΙΧΕΙΑ		
Μη κυκλοφορούντα περιουσιακά στοιχεία		
Εγκαταστάσεις και εξοπλισμός	736.741	553.784
Άυλα στοιχεία ενεργητικού	271.362	87.973
Συνολο μη κυκλοφορούντων περιουσιακών στοιχείων	**1.008.103**	**641.757**
Κυκλοφορούντα περιουσιακά στοιχεία		
Χρεώστες και προπληρωμές	4.868.219	32.998
Μετρητά στην τράπεζα	3.764.785	3.346.705
Σύνολο κυκλοφορούντων περιουσιακών στοιχείων	**8.633.004**	**3.379.703**
Σύνολο περιουσιακών στοιχείων	**9.641.107**	**4.021.460**
ΙΔΙΑ ΚΕΦΑΛΑΙΑ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ		
Ίδια κεφάλαια		
Αποθεματικά*	167.706	39.222
Σύνολο ιδίων κεφαλαίων	**167.706**	**39.222**
Τρέχουσες υποχρεώσεις		
Πιστωτές και οφειλόμενα έξοδα	800.900	1.026.703
Προεισπραχθέντα Τέλη	5.716.966	0
Κρατική Χορηγία	2.955.535	2.955.535
Ολικό τρεχουσών υποχρεώσεων	**9.473.401**	**3.982.238**
Ολικό Ιδίων Κεφαλαίων και Υποχρεώσεων	**9.641.107**	**4.021.460**

** Το αποθεματικό ύψους €167,706 για το έτος 2020 προκύπτει από το αποθεματικό για το έτος 2019 (€39,222), μείον έλλειμμα έτους 2020 (€39,030), πλέον αναπροσαρμογή λόγω μη ελεγμένων οικονομικών καταστάσεων (€167,514).*

3. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

3.1. Νομοθεσία Αρχής Ψηφιακής Ασφάλειας

Τον Αύγουστο του 2020 αναθεωρήθηκε ο περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμος (Ν. 89(Ι)/2020) που διέπει τη λειτουργία της Αρχής Ψηφιακής Ασφάλειας, στο πλαίσιο εναρμόνισης με την Ευρωπαϊκή Οδηγία NIS 2016/1148[8]. Ο εν λόγω Νόμος επικαιροποίησε τις σχετικές πρόνοιες του Νόμου 17(Ι)/2018 και επέκτεινε τις αρμοδιότητες, εξουσίες και καθήκοντα της Αρχής.

Ο Επίτροπος Επικοινωνιών ορίστηκε ως ο επικεφαλής της Αρχής και ως η Εθνική Αρχή για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών.

Με τη λειτουργία της ΑΨΑ διασφαλίζεται η προστασία των κρίσιμων υποδομών πληροφοριών της Δημοκρατίας τόσο στον ιδιωτικό όσο και στο δημόσιο τομέα, καθώς και των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών. Η ΑΨΑ χρηματοδοτείται από τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, τους Φορείς Κρίσιμων Υποδομών Πληροφοριών, τους παροχείς Ηλεκτρονικών Επικοινωνιών και τους παροχείς Ψηφιακών Υπηρεσιών στην Κύπρο, σύμφωνα με τη μεθοδολογία υπολογισμού τελών που καθορίζεται σε Κανονισμούς που εκδίδονται από τη Βουλή δυνάμει των διατάξεων του σχετικού Νόμου (βλ. ενότητα 3.1.3).

3.1.1. Αναθεώρηση Νομοθεσίας περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών

Κατόπιν της έγκρισης του Νομοσχεδίου της Αρχής Ψηφιακής Ασφάλειας από το Υπουργικό Συμβούλιο, το Νομοσχέδιο που αφορά την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών προωθήθηκε στη Βουλή των Αντιπροσώπων, ψηφίστηκε και δημοσιεύθηκε στην Επίσημη Εφημερίδα της Δημοκρατίας τον Αύγουστο του 2020.

Ο Νόμος 89(Ι)/2020 ρυθμίζει θέματα προσωπικού, εσωτερικής λειτουργίας της ΑΨΑ και συνεργασίας της με άλλους αρμόδιους φορείς και όρισε τον Επίτροπο Επικοινωνιών ως τον επικεφαλής της Αρχής και ως η Εθνική Αρχή για την ασφάλεια δικτύων και συστημάτων πληροφοριών.

Επιπλέον, ο Νόμος 89(Ι)/2020 ρυθμίζει τις αρμοδιότητες της Αρχής σε θέματα Ασφάλειας Δικτύων και Πληροφοριών και Κυβερνοασφάλειας στον τομέα Ηλεκτρονικών Επικοινωνιών. Οι εν λόγω αρμοδιότητες της Αρχής στον τομέα των Ηλεκτρονικών Επικοινωνιών μεταφέρθηκαν από το ΓΕΡΗΕΤ (Γραφείο Επιτρόπου για τη Ρύθμιση Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων[9]) στην ΑΨΑ.

3.1.2. Κανονισμοί Πρόσληψης Προσωπικού

Στις 13 Αυγούστου 2020 δημοσιεύθηκαν στην Επίσημη Εφημερίδα της Δημοκρατίας οι περί της Αρχής Ψηφιακής Ασφάλειας (Όροι Πρόσληψης και Υπηρεσίας Υπαλλήλων) Κανονισμοί του 2020 (Κ.Δ.Π. 360/2020). Οι εν λόγω Κανονισμοί εγκρίθηκαν από το Υπουργικό Συμβούλιο και ψηφίστηκαν από τη Βουλή των Αντιπροσώπων, δυνάμει των σχετικών διατάξεων του περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμου του 2020.

Οι σχετικοί Κανονισμοί καθορίζουν, ρυθμίζουν και προβλέπουν διαδικασίες και άλλα ζητήματα που αφορούν την πρόσληψη, μονιμοποίηση, προαγωγή, όρους υπηρεσίας, κατηγορίες θέσεων, αφυπηρέτηση και ωφελήματα αφυπηρέτησης των μελών του προσωπικού της Αρχής. Τα μέλη του προσωπικού της Αρχής διορίζονται από το ΣΕΠΑ (Συμβούλιο Επιλογής και Προαγωγών της Αρχής Ψηφιακής Ασφάλειας), είτε μόνιμα, είτε με σύμβαση για ορισμένο χρονικό διάστημα, σύμφωνα με τις σχετικές διαδικασίες, όπως καθορίζονται στους εν λόγω Κανονισμούς. Επιπλέον, το ΣΕΠΑ δύναται

[8] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L1148&from=el
[9] https://ocecpr.ee.cy/

να εγκρίνει προσαυξήσεις με βάση τα προσόντα, την πείρα και τις εμπειρίες του προσώπου που διορίζεται, κατ' αναλογία των κριτηρίων που ισχύουν στη Δημόσια Υπηρεσία, τοποθετώντας το σε οποιοδήποτε σημείο της κλίμακας ή των συνδυασμένων κλιμάκων που προβλέπονται από το Σχέδιο Υπηρεσίας της θέσης.

3.1.3. Κανονισμοί Χρηματοδότησης Αρχής Ψηφιακής Ασφάλειας

Στις 13 Αυγούστου 2020 δημοσιεύθηκαν στην Επίσημη Εφημερίδα της Δημοκρατίας οι Περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Τέλη) Κανονισμοί του 2020 (Κ.Δ.Π. 359/2020). Οι εν λόγω Κανονισμοί εγκρίθηκαν από το Υπουργικό Συμβούλιο και ψηφίστηκαν από τη Βουλή των Αντιπροσώπων, δυνάμει των άρθρων 11 και 45 του περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμου του 2020.

Τα τέλη χρηματοδότησης της Αρχής υπολογίζονται με βάση προκαθορισμένη μεθοδολογία που καταγράφεται στους σχετικούς Κανονισμούς. Το τέλος είναι διαφορετικό για κάθε εταιρεία, οργανισμό ή υπηρεσία, του ιδιωτικού ή δημόσιου τομέα, και υπολογίζεται λαμβάνοντας υπόψη τον προϋπολογισμό εσόδων της Αρχής, τον αριθμό των Φορέων που υπόκεινται σε ρύθμιση βάσει προνοιών του Νόμου, τα ακαθάριστα ετήσια έσοδα/προϋπολογισμό του κάθε φορέα, και το επίπεδο κρισιμότητας των σχετικών υποδομών πληροφοριών που διαχειρίζεται.

3.1.4. Εθνικό Πλαίσιο Κυβερνοασφάλειας

Στις 21 Αυγούστου 2020 δημοσιεύθηκε στην Επίσημη Εφημερίδα της Δημοκρατίας η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών) Απόφαση του 2020 (Κ.Δ.Π. 389/2020), η οποία αποτελεί το πρώτο και σημαντικότερο σκέλος του Εθνικού Πλαισίου Κυβερνοασφάλειας. Πριν δημοσιευθεί η εν λόγω Απόφαση τέθηκε σε Δημόσια Διαβούλευση, και τα σχόλια των ενδιαφερομένων μερών που κατατέθηκαν λήφθηκαν υπόψη πριν την έκδοσή της.

Με την Απόφαση Κ.Δ.Π. 389/2020 καθορίζεται το πλαίσιο των ελάχιστων μέτρων ασφάλειας δικτύων και συστημάτων πληροφοριών, το οποίο έχει ως στόχο να βοηθήσει τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και τους Φορείς Κρίσιμων Υπηρεσιών Πληροφοριών στην Κυπριακή Δημοκρατία, να συμμορφωθούν με τις απαιτήσεις και τις υποχρεώσεις του Νόμου 89(Ι)/2020 και της Οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS).

Το πλαίσιο αυτό διαμορφώνει μια δομημένη προσέγγιση ελέγχου και διαδικασιών που θα εξασφαλίζει ένα ελάχιστο επίπεδο ασφάλειας συστημάτων δικτύων και πληροφοριών στους Φορείς Εκμετάλλευσής Βασικών Υπηρεσιών και τους Φορείς Κρίσιμων Υποδομών Πληροφοριών στην Κυπριακή Δημοκρατία. Το περιεχόμενο του πλαισίου περιέχει μια ολοκληρωμένη προσέγγιση εντοπισμού, αξιολόγησης και επιλογής μέτρων για τη διαχείριση κινδύνων στον κυβερνοχώρο, με έμφαση στη διατήρηση των στοιχείων της εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας και αυθεντικότητας των πληροφοριών, δικτύων και υπηρεσιών που παρέχουν οι εν λόγω φορείς στην Κυπριακή κοινωνία. Τα σχετικά μέτρα καλύπτουν όλο το φάσμα σχετικών δραστηριοτήτων προετοιμασίας, προστασίας, ετοιμότητας, διαχείρισης περιστατικών και επαναφοράς σε κανονικά επίπεδα λειτουργίας μετά από σοβαρά περιστατικά.

3.1.5. Κοινοποίηση Περιστατικών Παραβίασης Ψηφιακής Ασφάλειας

Η υποχρέωση κοινοποίησης περιστατικών που οφείλουν να υποβάλουν οι Φορείς προς την Αρχή απορρέει από την περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κοινοποίηση Συμβάντων) Απόφαση του 2019 (Κ.Δ.Π. 218/2019).

Η νομοθεσία αυτή περιλαμβάνει ολοκληρωμένο πλαίσιο, διαδικασίες και έντυπα κοινοποίησης περιστατικών που οφείλουν να υποβάλλουν οι διάφοροι Φορείς προς την Αρχή, δηλαδή οι Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, οι Φορείς Κρίσιμων Υποδομών Πληροφοριών και οι παροχείς Ψηφιακών Υπηρεσιών. Επίσης, η Απόφαση Κ.Δ.Π. 218/2019 περιλαμβάνει και τις διαδικασίες διασυνοριακών κοινοποιήσεων σύμφωνα με τις πρόνοιες της Οδηγίας NIS 2016/1148[10].

Κατά το 2020, η ΑΨΑ συνέχισε την υλοποίηση του έργου για την ηλεκτρονική υποβολή περιστατικών μέσω εξειδικευμένης πλατφόρμας, η οποία θα ολοκληρωθεί και θα τεθεί σε λειτουργία εντός του 2021 (βλ. σχετική ενότητα 3.3.2).

3.1.6. Εγγραφές Παροχέων Ψηφιακών Υπηρεσιών

Στις 28 Αυγούστου 2020 δημοσιεύθηκε στην Επίσημη Εφημερίδα της Δημοκρατίας η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Εγγραφή Παροχέων Ψηφιακών Υπηρεσιών) Απόφαση του 2020 (Κ.Δ.Π. 403/2020). Πριν δημοσιευθεί η εν λόγω Απόφαση τέθηκε σε Δημόσια Διαβούλευση, και τα σχόλια των ενδιαφερομένων μερών που κατατέθηκαν λήφθηκαν υπόψη πριν την έκδοσή της.

Με την εν λόγω Απόφαση καθορίζεται η διαδικασία υποβολής αίτησης για σκοπούς εγγραφής στο μητρώο των Παροχέων Ψηφιακών Υπηρεσιών.

3.1.7. Διοικητικά Πρόστιμα

Εντός του 2020, η Αρχή ξεκίνησε την ετοιμασία σχετικής δευτερογενούς νομοθεσίας για τη Συλλογή Πληροφοριών και Επιβολής Διοικητικού Προστίμου. Με την εν λόγω νομοθεσία θα καθορίζεται η διαδικασία επιβολής Διοικητικών Κυρώσεων, συμπεριλαμβανομένου Διοικητικού Προστίμου, κατά προσώπου που διενεργεί πράξη ή τελεί σε παράλειψη κατά παράβαση των σχετικών διατάξεων του Νόμου της Αρχής.

Η Απόφαση θα τεθεί σε Δημόσια Διαβούλευση και, λαμβάνοντας υπόψη τα σχόλια των εμπλεκομένων φορέων, αναμένεται να οριστικοποιηθεί και δημοσιευθεί εντός του 2021.

3.1.8. Δημόσιες Διαβουλεύσεις

Εντός του 2020, η Αρχή ξεκίνησε την ετοιμασία σχετικής δευτερογενούς νομοθεσίας για τη διαδικασία διενέργειας Δημόσιων Διαβουλεύσεων.

Με την εν λόγω Νομοθεσία θα καθορίζεται η διαδικασία διενέργειας Δημόσιων Διαβουλεύσεων με εκπροσώπους της Δημοκρατίας, Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, Φορείς Κρίσιμων Υποδομών Πληροφοριών, Παροχείς Ψηφιακών Υπηρεσιών και Παροχείς Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών, και με οποιαδήποτε άλλα πρόσωπα, οργανισμούς ή άλλα ενδιαφερόμενα μέρη, όποτε η Αρχή εκάστοτε κρίνει σκόπιμο, σύμφωνα με τις απαιτήσεις και τις υποχρεώσεις του Νόμου.

Η Απόφαση θα τεθεί σε Δημόσια Διαβούλευση και, λαμβάνοντας υπόψη τα σχόλια των εμπλεκομένων φορέων, αναμένεται να οριστικοποιηθεί και δημοσιευθεί εντός του 2021.

[10] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L1148&from=el

3.1.9. Αξιολόγηση Κρισιμότητας Υποδομών

Η ΑΨΑ, σε συνεργασία με εξωτερικούς συμβούλους, ξεκίνησε τη διεξαγωγή έργου για την αξιολόγηση και επαναξιολόγηση της κρισιμότητας σχετικών φορέων στην Κυπριακή Δημοκρατία. Η αξιολόγηση πραγματοποιείται στο πλαίσιο των αρμοδιοτήτων και των διαδικασιών που εφαρμόζει η ΑΨΑ βάσει του Νόμου 89(Ι)/2020. Η εργασία αποτελεί αναθεώρηση και συμπλήρωση της διαδικασίας που είχε προηγηθεί το 2018.

Η μεθοδολογία που εφαρμόζεται έχει εγκριθεί από το Υπουργικό Συμβούλιο και έχει κοινοποιηθεί στην Ευρωπαϊκή Επιτροπή στο πλαίσιο της προηγούμενης διαδικασίας που πραγματοποιήθηκε το 2018.

Πιο αναλυτικά, ο στόχος του έργου είναι η αξιολόγηση (για νέους) και η επαναξιολόγηση (για όσους είχαν αξιολογηθεί και το 2018, αλλά ο τομέας ή ο υποτομέας τους παρουσιάζει αλλαγές) κρισιμότητας οργανισμών και υπηρεσιών οι οποίοι είναι δυνατόν να ορισθούν ως Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών ή Φορείς Κρίσιμων Υποδομών Πληροφοριών στην Κυπριακή Δημοκρατία. Σύμφωνα με το Άρθρο 27, Εδάφιο 5 του Νόμου 89(Ι)/2020, η αξιολόγηση κρισιμότητας πρέπει να αναθεωρείται τουλάχιστον κάθε δύο χρόνια. Η διαδικασία αποτελεί αναθεώρηση της αξιολόγησης του Νοεμβρίου 2018.

Η επιλογή των φορέων που τυγχάνουν αξιολόγησης στην παρούσα φάση, βασίστηκε σε κριτήρια που έχουν προκαθοριστεί βάσει της Οδηγίας (ΕΕ) 2016/1148, του Νόμου 89(Ι)/2020 και της μεθοδολογίας καθορισμού Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών, σε σχέση με την κρισιμότητα της λειτουργίας και των υπηρεσιών τους σε εθνικό επίπεδο, καθώς και στη βάση συστάσεων Αρμόδιων Αρχών του κράτους. Η αξιολόγηση επικεντρώνεται σε:

- Ανάλυση των χαρακτηριστικών των παρεχόμενων βασικών ή/και κρίσιμων υπηρεσιών
- Αξιολόγηση της κρισιμότητας των υπηρεσιών που παρέχουν ή/και των πληροφοριών που διαχειρίζονται, σε σχέση με περιστατικά που είναι δυνατόν να επηρεάσουν την Κυβερνοασφάλεια των εν λόγω υπηρεσιών και υποδομών

Τα αποτελέσματα του έργου θα τύχουν της έγκρισης του Υπουργικού Συμβουλίου, σχετικά με τον καθορισμό των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών για την Κυπριακή Δημοκρατία. Η εν λόγω Υπουργική Απόφαση είναι απόρρητη και δεν δημοσιεύεται. Ωστόσο, ο κάθε φορέας θα ενημερωθεί ξεχωριστά με Ατομική Διοικητική Πράξη για τα αποτελέσματα που τον αφορούν. Τα αποτελέσματα θα αξιοποιηθούν επίσης για τη σωστή και αποτελεσματική υλοποίηση αριθμού Δράσεων της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας.

Το έργο ξεκίνησε το Νοέμβριο του 2020 και εντός του 2021 αναμένεται να καθοριστούν από το Υπουργικό Συμβούλιο οι Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και οι Φορείς Κρίσιμων Υποδομών Πληροφοριών, όπως διαφαίνεται στη σχετική αξιολόγηση του επιπέδου κρισιμότητας τους για την Κύπρο.

3.2. Νομοθεσία Ηλεκτρονικών Επικοινωνιών για την Ασφάλεια Δικτύων και Πληροφοριών

Εντός του 2020, τα θέματα ασφάλειας των Ηλεκτρονικών Επικοινωνιών μεταφέρθηκαν από το ΓΕΡΗΕΤ στην ΑΨΑ με τροποποίηση του Νόμου 112(Ι)/2004 από το οποίο διαγράφηκαν τα σχετικά άρθρα βάσει του τροποποιητικού Νόμου, Ν. 90(Ι)/2020. Πριν την τροποποίηση του Ν. 112(Ι)/2004, τα θέματα αυτά τύγχαναν χειρισμού από την ομάδα για την Ασφάλεια Δικτύων και Πληροφοριών του ΓΕΡΗΕΤ (Γραφείο Επιτρόπου για τη Ρύθμιση Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων). Με τη ψήφιση του νέου Νόμου της Αρχής (Ν. 89(Ι)/2020), οι εν λόγω Διατάξεις μεταφέρθηκαν στο Νόμο της Αρχής, κατ' εφαρμογή των σχετικών αποφάσεων του Υπουργικού Συμβουλίου.

Το περί Γνωστοποίησης Παραβιάσεων Προσωπικών Δεδομένων από τους Παροχείς Δημόσια Διαθέσιμων Υπηρεσιών Ηλεκτρονικών Επικοινωνιών Διάταγμα του 2015 (Κ.Δ.Π. 190/2015), το περί της Κοινοποίησης των Παραβιάσεων Ασφάλειας ή Απώλειας Ακεραιότητας Δικτύων ή και Υπηρεσιών Διάταγμα του 2013 (Κ.Δ.Π. 371/2013), το περί Ασφάλειας Δικτύων και Πληροφοριών Διάταγμα του 2011 (Κ.ΔΠ. 253/2011) και το περί Δημιουργίας Φορέων Άμεσης Ανταπόκρισης για Περιστατικά και Συμβάντα που Σχετίζονται με την Ασφάλεια Δικτύων και Πληροφοριών (CISRT-CERT) Διάταγμα του 2010 (Κ.Δ.Π. 358/2010), τύγχαναν χειρισμού από την ομάδα για την Ασφάλεια Δικτύων και Πληροφοριών του ΓΕΡΗΕΤ, ενώ μετά τη ψήφιση του Ν.89(Ι)/2020 εφαρμόζονται από την Αρχή Ψηφιακής Ασφάλειας.

Όσον αφορά στην υποχρέωση των παροχέων δημόσιων δικτύων ή δημόσια διαθέσιμων υπηρεσιών Ηλεκτρονικών Επικοινωνιών να κοινοποιούν κάθε παραβίαση της ασφάλειας ή απώλειας της ακεραιότητας δικτύων ή και υπηρεσιών που έχει σημαντικό αντίκτυπο στη λειτουργία των δικτύων ή υπηρεσιών τους, αυτή απορρέει από το Διάταγμα Κ.Δ.Π. 371/2013. Το εν λόγω Διάταγμα αναφέρεται ως το περί της Κοινοποίησης των Παραβιάσεων Ασφάλειας ή Απώλειας Ακεραιότητας Δικτύων ή και Υπηρεσιών Διάταγμα του 2013. Το Διάταγμα Κ.Δ.Π. 371/2013 καθορίζει τη διαδικασία και το περιεχόμενο της κοινοποίησης που οφείλουν να υποβάλλουν οι Παροχείς Ηλεκτρονικών Επικοινωνιών για τις παραβιάσεις της ασφάλειας ή για την απώλεια της ακεραιότητας των δικτύων που έχουν σημαντικό αντίκτυπο στη λειτουργία των υποδομών ή των υπηρεσιών τους.

3.2.1. Κυβερνοασφάλεια σε δίκτυα επικοινωνιών πέμπτης γενεάς (5G Cybersecurity)

Τον Ιανουάριο 2020, η Ευρωπαϊκή Ένωση προχώρησε με την έκδοση της εργαλειοθήκης[11] για την ασφάλεια των δικτύων επικοινωνιών 5G, οπότε η Αρχή προχώρησε σε ανάλυση της και τον καταρτισμό σχετικού προγράμματος δράσεων για την πλήρη υλοποίηση των προνοιών της. Το πρόγραμμα δράσεων κατατέθηκε στην Ευρωπαϊκή Επιτροπή ως η σχετική υποχρέωση της Κυπριακής Δημοκρατίας. Ως μέρος των σχετικών εργασιών, η ΑΨΑ προχώρησε στην ανάλυση, ανάπτυξη, διαβούλευση και έκδοση Απόφασης (δευτερογενούς νομοθεσίας) για τη θέσπιση συγκεκριμένων ολοκληρωμένων υποχρεώσεων ασφάλειας προς τους παροχείς δικτύων Ηλεκτρονικών Επικοινωνιών 5G.

Στις 11 Σεπτεμβρίου 2020, δημοσιεύθηκε στην Επίσημη Εφημερίδα της Δημοκρατίας η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κυβερνοασφάλεια Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών Πέμπτης Γενιάς 5G) Απόφαση του 2020 (Κ.Δ.Π. 408/2020). Η Απόφαση αυτή έχει ως σκοπό την εισαγωγή ελάχιστων απαιτήσεων ασφαλείας, ικανών να μετριάσουν τους κύριους κινδύνους που αφορούν την ασφάλεια των Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών Πέμπτης Γενιάς (5G). Η προαναφερθείσα Απόφαση καθορίζει επιπρόσθετα ειδικότερα μέτρα, με την επιφύλαξη των μέτρων που καθορίζονται στην Απόφαση Μέτρων Ασφάλειας του 2020 (Κ.Δ.Π. 389/2020) και στο Διάταγμα του 2011 (Κ.Δ.Π. 253/2011), όσον αφορά το δίκτυο και την υπηρεσία ηλεκτρονικών υπηρεσιών Πέμπτης Γενιάς (5G).

[11] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

Επίσης, η ΑΨΑ προχώρησε στη διενέργεια τεχνοκρατικής αξιολόγησης των προμηθευτών εξοπλισμού 5G που χρησιμοποιούν ή προτίθενται να χρησιμοποιήσουν οι παροχείς δικτύων στην Κυπριακή Δημοκρατία, με σκοπό τον εντοπισμό τυχόν προμηθευτών υψηλού κινδύνου. Ως μέρος των επακόλουθων ενεργειών για την υλοποίηση της εργαλειοθήκης, οι παροχείς δικτύων έχουν προθεσμία μέχρι το τέλος Μαΐου 2021 να υποβάλουν στην ΑΨΑ ολοκληρωμένη στρατηγική πολλαπλών προμηθευτών, για μείωση των επιπέδων εξάρτησης τους από μεμονωμένους προμηθευτές.

3.3. Ανάπτυξη Υποδομών και Εργαλείων

3.3.1. Υποδομή Εθνικού CSIRT

Η υποδομή του Εθνικού CSIRT-CY αναβαθμίζεται συνεχώς λαμβάνοντας υπόψη τα καλύτερα ευρωπαϊκά και διεθνή πρότυπα που αφορούν τις ομάδες CSIRTs, τις καλύτερες πρακτικές και τις κατευθυντήριες γραμμές της Ευρωπαϊκής Ένωσης, με στόχο να προσφέρει υπηρεσίες υψηλού επιπέδου στον τομέα της Κυβερνοασφάλειας.

Στο πλαίσιο των δραστηριοτήτων της Υπηρεσίας για προστασία των Κρίσιμων Υποδομών Πληροφοριών της Κυπριακής Δημοκρατίας, το Εθνικό CSIRT-CY κατά το 2020 προμηθεύτηκε εξειδικευμένα εργαλεία και προγράμματα με σκοπό τη διενέργεια συστηματικών ελέγχων ασφαλείας στις Κρίσιμες Υποδομές Πληροφοριών του Κράτους. Μεταξύ άλλων, το Εθνικό CSIRT-CY, αξιοποιεί την εξής υποδομή:

- πλατφόρμα στην οποία πραγματοποιούνται εξομοιώσεις κυβερνοεπιθέσεων, η οποία επιτρέπει στους αναλυτές του Εθνικού CSIRT-CY, αλλά και στους υπεύθυνους ασφαλείας μιας υποδομής, να εντοπίσουν κενά ασφαλείας, καθώς και να παρέχουν προτάσεις για πιθανούς τρόπους αντιμετώπισής τους
- παραμετροποιημένους αισθητήρες, οι οποίοι προσφέρουν ελέγχους ασφαλείας σε πραγματικό χρόνο, βασισμένοι σε πρωτόκολλα δικτύου για ανίχνευση και ανάλυση ύποπτων και κακόβουλων ενεργειών
- εξειδικευμένα λογισμικά δικανικού εργαστηρίου με δυνατότητα ανάκτησης, ανάλυσης και αναφοράς δεδομένων από κινητές συσκευές, υπολογιστές και πηγές cloud
- αυτοματοποιημένα κανάλια πληροφόρησης για δημιουργία αυτόματων και χειροκίνητων αναφορών και ειδοποιήσεων προς Κρίσιμες Υποδομές Πληροφοριών
- εξειδικευμένα εργαλεία:
  - συλλογής πληροφοριών για απειλές στον κυβερνοχώρο
  - αξιολόγηση ύποπτων αρχείων
  - συνεχούς παρακολούθησης των βασικών διαδικτυακών οικοσυστημάτων
  - άμεσης ανταπόκρισης που μπορούν να δώσουν άμεσα αποτελέσματα έτσι ώστε να περιοριστεί και να καταπολεμηθεί τυχόν κυβερνοεπίθεση

Επίσης, κατά το 2020, το Εθνικό CSIRT-CY προχώρησε στην ενσωμάτωση στην υποδομή του ολοκληρωμένης γενικής λύσης εργαλείων ασφαλείας, ταξινόμησης δεδομένων και κρυπτογράφησης, αφού η πρόληψη διαρροής δεδομένων είναι ένα από τα πιο σημαντικά τεχνικά χαρακτηριστικά που θα πρέπει να τηρούνται σε ένα οργανισμό.

3.3.2. Ολοκληρωμένη Πλατφόρμα Διαχείρισης Εμπλεκόμενων Φορέων ΑΨΑ

Κατά το 2020, η ΑΨΑ ολοκλήρωσε τη δεύτερη φάση συγχρηματοδοτούμενου έργου (βλ. ενότητα 8.1.2), με εξωτερικούς συνεργάτες, που αφορά δημιουργία ολοκληρωμένης πλατφόρμας διαχείρισης εμπλεκομένων φορέων (κυρίως για τους εποπτευόμενους φορείς). Το έργο αυτό ξεκίνησε το Δεκέμβριο του 2019 και έχει ως αντικείμενο την αναβάθμιση του υφιστάμενου συστήματος RCMS (Risk and Compliance Management System) της ΑΨΑ.

Κατά το 2020, στο αναβαθμισμένο σύστημα iDSAMPL (integrated Digital Security Authority Management Platform):

- Αναπτύχθηκαν και οριστικοποιήθηκαν οι επιπρόσθετες απαιτήσεις για την περαιτέρω ανάπτυξη των διαφόρων λειτουργιών της πλατφόρμας
  - Customer Relationship Management (διαχείριση των σχέσεων με πελάτες)
  - Data Management (διαχείριση δεδομένων)
  - Risk Management (διαχείριση κινδύνου)
  - Incident Management (διαχείριση περιστατικών)
    Compliance Management (διαχείρισης συμμόρφωσης)
  - Audit Management (διαχείριση ελέγχων)
  - Alerts and Notifications (προειδοποιήσεις και κοινοποιήσεις)
- Ολοκληρώθηκε η πρώτη φάση παραμετροποίησης και ανάπτυξης της πλατφόρμας με βάση τις απαιτήσεις του έργου
- Ολοκληρώθηκαν οι πρώτες (αρχικές) εκπαιδεύσεις για τη λειτουργία και δομή του συστήματος
- Εγκαταστάθηκαν και παραμετροποιήθηκαν οι απαραίτητοι εξυπηρετητές (servers) στην υποδομή της ΑΨΑ για φιλοξενία του συστήματος και σύνδεση του με σχετική ιστοσελίδα μέσω της οποίας η πλατφόρμα θα είναι διαθέσιμη στους εμπλεκόμενους φορείς
- Αναπτύχθηκαν αλλαγές στην υφιστάμενη μεθοδολογία της ΑΨΑ για την αξιολόγηση κινδύνων Κυβερνοασφάλειας σε εθνικό επίπεδο, για να χρησιμοποιείται η πλατφόρμα για τη συλλογή και επεξεργασία των σχετικών στοιχείων
- Ξεκίνησαν οι δοκιμαστικοί έλεγχοι στη λειτουργία της πλατφόρμας
- Ξεκίνησε η ανάπτυξη επιπρόσθετων διαδικασιών και ροές εργασιών (workflows) για τη χρήση της πλατφόρμας από το προσωπικό της ΑΨΑ με δομημένο τρόπο, όταν αυτή ολοκληρωθεί

Με την ολοκλήρωση της πλατφόρμας, κατά το πρώτο εξάμηνο του 2021, το σύστημα θα λειτουργεί ως ολοκληρωμένη πλατφόρμα διαχείρισης των εποπτευόμενων οργανισμών στην ΑΨΑ. Η ΑΨΑ πέτυχε σημαντική χρηματοδότηση (€99.585) για το έργο αυτό από τον INEA (Innovation and Networks Executive Agency) της Ευρωπαϊκής Ένωσης μέσω του προγράμματος CEF (Connecting Europe Facility). Η ανάπτυξη ενός ολοκληρωμένου συστήματος διαχείρισης (stakeholder management platform) κρίθηκε αναγκαία λόγω του μεγάλου αριθμού των φορέων τους οποίους θα εποπτεύει η ΑΨΑ σε θέματα ασφάλειας δικτύων και πληροφοριών.

4. ΥΛΟΠΟΙΗΣΗ ΣΤΡΑΤΗΓΙΚΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

4.1. Υλοποίηση Δράσεων Στρατηγικής Κυβερνοασφάλειας

Εντός του 2020, μέσω των δραστηριοτήτων της ΑΨΑ υλοποιήθηκε μεγάλο μέρος των Δράσεων της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας. Οι Δράσεις αυτές αναλύονται σε συγκεκριμένες ενότητες αυτής της Έκθεσης, ως ακολούθως:

Δράση 2	Δομές (βλ. ενότητα 1.3),
Δράση 4	Νομικό Πλαίσιο (βλ. ενότητα 3.1),
Δράση 7	Εντοπισμός και Αξιολόγηση των Κρίσιμων Υποδομών της Κυπριακής Δημοκρατίας (βλ. ενότητα 3.1.9),
Δράση 9	Εθνικό Πλαίσιο Κυβερνοασφάλειας (βλ. ενότητα 4.2)
Δράση 11	Εθνικό CSIRT-CY (βλ. ενότητα 1.3.2, ενότητα 3.3.1),
Δράση 12	Εθνικές και Διεθνείς Ασκήσεις (βλ. ενότητα 4.3)
Δράση 13	Εκπαίδευση και Κατάρτιση (βλ. ενότητα 7.5),
Δράση 14	Δημιουργία Κουλτούρας Κυβερνοασφάλειας - Awareness (βλ. ενότητα 4.4)
Δράση 15	Διεθνείς Συνεργασίες (βλ. ενότητα 7)

Επίσης, καθώς η πρώτη Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας έκλεισε τον κύκλο της, κατά το 2020 οριστικοποιήθηκε και εκδόθηκε η δεύτερη Στρατηγική (βλ. ενότητα 4.5).

Σημειώνεται ότι τον Δεκέμβριο 2020 αναθεωρήθηκε και εκδόθηκε σε νέα έκδοση η Στρατηγική Κυβερνοασφάλεια.

4.2. Εθνικό Πλαίσιο Κυβερνοασφάλειας

Εντός του 2020, συνεχίστηκε η υλοποίηση του πρώτου σημαντικού παραδοτέου της Ομάδας Εργασίας για τη Δράση 9 της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, η οποία είχε ως στόχο την ετοιμασία του Εθνικού Πλαισίου Κυβερνοασφάλειας. Με βάση τον εν λόγω σχεδιασμό, ένας σημαντικός αριθμός κρίσιμων μέτρων ασφάλειας έχουν τεθεί σε εφαρμογή με μικρό σχετικά κόστος και σε σύντομο χρονικό διάστημα, μέχρι την εφαρμογή του πλήρους Εθνικού Πλαισίου Κυβερνοασφάλειας. Σε πρώτο στάδιο, τα μέτρα εφαρμόζονται στους οργανισμούς της Δημόσιας Υπηρεσίας.

Επίσης, κατά το 2020 ολοκληρώθηκε και εκδόθηκε το πρώτο και σημαντικότερο σκέλος του ολοκληρωμένου Εθνικού Πλαισίου Κυβερνοασφάλειας στη μορφή της Απόφασης Κ.Δ.Π. 389/2020 (βλ. ενότητα 3.1.4). Το Εθνικό Πλαίσιο Κυβερνοασφάλειας που έχει ετοιμάσει η ΑΨΑ είναι οριζόντιο και εφαρμόζεται αρχικά στους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και Φορείς Κρίσιμων Υποδομών Πληροφοριών της Κυπριακής Δημοκρατίας, αλλά μπορεί να καλύψει και τις ανάγκες άλλων μεγάλων οργανισμών στην Κυπριακή Δημοκρατία, αν επιθυμούν να το αξιοποιήσουν. Στη συνέχεια, η ΑΨΑ εξετάζει την ανάπτυξη συγκεκριμένων κάθετων ρυθμίσεων για τομείς όπου παρουσιάζονται ειδικές ανάγκες, όπως για παράδειγμα στον τομέα των Ηλεκτρονικών Επικοινωνιών. Κατά το 2021 αναμένεται η έκδοση κάθετων ρυθμίσεων για τον τομέα αυτό, καθώς και εξέταση άλλων τομέων για πιθανές μελλοντικές ρυθμίσεις (π.χ. ενέργεια, υγεία, κλπ.).

4.3. Ασκήσεις Κυβερνοασφάλειας

Στο πλαίσιο ενδυνάμωσης των τεχνικών ικανοτήτων στη διαχείριση απειλών Κυβερνοπολέμου, στις 28 Σεπτεμβρίου μέχρι τις 2 Οκτωβρίου 2020 πραγματοποιήθηκε η διακλαδική διακρατική διακυβερνητική άσκηση «ΠΑΝΟΠΤΗΣ 2020».

Η Αρχή Ψηφιακής Ασφάλειας/Εθνικό CSIRT-CY, συμμετείχαν στην Άσκηση μαζί με Εφέδρους του 51 Λόχου Κυβερνοάμυνας (ΛΚΥΒ) και υπηρεσίες του δημοσίου, ιδιωτικού και ακαδημαϊκού τομέα. Η άσκηση περιλάμβανε εντοπισμό και αντιμετώπιση διαφόρων περιστατικών Κυβερνοασφάλειας, καλύπτοντας τόσο μεμονωμένα συμβάντα, όσο και περιστατικά μεγαλύτερης έκτασης, τα οποία απαιτούσαν συντονισμένη ανταπόκριση σε πολλαπλά επίπεδα. Τα επεισόδια κάλυψαν πλειάδα αντικειμένων κυβερνοάμυνας, όπως ανάλυση ιομορφικού λογισμικού, ψηφιακή διερεύνηση πειστηρίων σε διαφορετικά συστήματα Η/Υ, δρομολογητών, έλεγχο ευπαθειών εφαρμογών και εντοπισμό/ανάλυση παραβίασης υποδομής δικτύου.

Επίσης, κατά το πρώτο τρίμηνο του 2020, το Εθνικό CSIRT-CY συμμετείχε ενεργά στην προετοιμασία της πανευρωπαϊκής άσκησης "CYBER EUROPE 2020" η οποία επρόκειτο να πραγματοποιηθεί τον Ιούνιο του 2020 με σενάριο στον Τομέα της Υγείας. Ωστόσο, η άσκηση αναβλήθηκε λόγω της πανδημίας COVID-19.

4.4. Δημιουργία Κουλτούρας Κυβερνοασφάλειας - Awareness

Στο πλαίσιο ενημέρωσης και εκπαίδευσης των επαγγελματιών στο χώρο της Κυβερνοασφάλειας, η ομάδα του Εθνικού CSIRT-CY διοργάνωσε τηλεκπαίδευση με όλους τους λειτουργούς ασφαλείας και τεχνικούς διαχειριστές των Κρίσιμων Υποδομών Πληροφοριών της Κύπρου.

Επίσης, έγιναν διάφορες στοχευμένες ενέργειες προς το κοινό για πληροφόρηση αναφορικά με την ασφαλή χρήση των ψηφιακών τεχνολογιών στην καθημερινότητα των πολιτών. Με παραδείγματα κατανοητά σε μη-τεχνικούς χρήστες, έγινε προσπάθεια ευαισθητοποίησης του κοινού, αναφορικά με τεχνικές ασφαλούς χρήσης ψηφιακών τεχνολογιών και την αναγνώριση πιθανών προσπαθειών παραπλάνησης από κακόβουλους δρώντες στο διαδίκτυο.

4.5. Αναθεώρηση της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας

Κατά το 2020, η ΑΨΑ ολοκλήρωσε την αναθεώρηση της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, αξιοποιώντας δεδομένα από διάφορες πηγές:

- τα αποτελέσματα της αξιολόγησης με τίτλο "Cybersecurity Capacity Assessment"[12] από το Πανεπιστήμιο της Οξφόρδης
- τους Οδηγούς Καλών Πρακτικών, μεταξύ άλλων, από τον ENISA, τον ΟΑΣΕ, την ITU και τον οργανισμό Meridian
- το "Πακέτο Κυβερνοασφάλειας της ΕΕ"[13] ("EU Cybersecurity Package")
- τα διδάγματα από την εφαρμογή της υφιστάμενης Στρατηγικής

Ολοκληρώθηκαν επίσης όλες οι σχετικές διαβουλεύσεις με αρμόδια Υπουργεία και άλλες Αρχές της Δημοκρατίας, και η αναθεωρημένη Στρατηγική έτυχε της έγκρισης του Υπουργικού Συμβουλίου στις 16 Δεκεμβρίου 2020. Δημοσιεύτηκε στην ιστοσελίδα της ΑΨΑ το Δεκέμβριο 2020 και αναμένεται ότι θα αποτελέσει τον εθνικό οδηγό για την ανάπτυξη δραστηριοτήτων Κυβερνοασφάλειας για τα επόμενα 4 χρόνια.

[12] Αξιολόγηση της τρέχουσας κατάστασης στην Κύπρο σε σχέση με τον τομέα της Κυβερνοασφάλειας που έγινε το 2017, βάσει επιστημονικού μοντέλου που αναπτύχθηκε από το Πανεπιστήμιο της Οξφόρδης.

[13] https://ec.europa.eu/digital-single-market/en/cyber-security

5. ΔΙΑΧΕΙΡΙΣΗ ΣΥΜΒΑΝΤΩΝ ΚΑΙ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

5.1. Διαχείριση Περιστατικών

Το Εθνικό CSIRT-CY, από τη στιγμή εντοπισμού ενός περιστατικού έως και την επίλυσή του, εφαρμόζει ένα σύνολο διαδικασιών οι οποίες έχουν τύχει αξιολόγησης και έχουν εγκριθεί από διεθνείς και ευρωπαϊκούς οργανισμούς, όπως το FIRST (Forum of Incident Response and Security Teams), ο TI (Trusted Introducer) και ο ENISA (European Union Agency for Cybersecurity). Αρχικά, ενεργοποιείται η Διαδικασία Καταχώρησης Περιστατικού και ακολουθεί η Διαδικασία Διαχείρισης Περιστατικού η οποία αποτελείτε από τα ακόλουθα στάδια:

- Ανάθεση χειριστή περιστατικού και κλιμάκωση (αν χρειάζεται)
- Ανάλυση περιστατικού
- Δικανική ανάλυση
- Μετριασμός περιστατικού
- Συντονισμός και υποβολή αναφορών
- Κλείσιμο περιστατικού
- Βελτίωση διαδικασιών μετά από ανάλυση

Η διαχείριση περιστατικών Κυβερνοασφάλειας και ο μετριασμός των επιπτώσεων τους αποτελούν τους κύριους στόχους του Εθνικού CSIRT-CY. Ωστόσο, οι διαδικασίες αυτές εκτελούνται σε προκαθορισμένο χρόνο, ανάλογα με την κατηγοριοποίηση και την προτεραιοποίηση του περιστατικού.

Εντός του 2020 καταγράφηκαν πενήντα (50) περιστατικά, εκ των οποίων τα τριάντα-τέσσερα (34) αφορούσαν Κρίσιμες Υποδομές Πληροφοριών, ενώ τα υπόλοιπα δέκα-έξι (16) άλλους φορείς και υπηρεσίες. Το Εθνικό CSIRT – CY χειρίστηκε περιστατικά σε διάφορους φορείς τα οποία ενέπιπταν στις κατηγορίες Phishing, Malware, Distributed Denial of Service (DDoS), Malvertising και Domain Spoofing.

Διεθνώς, έχει διαπιστωθεί ραγδαία αύξηση στον αριθμό των κυβερνοεπιθέσεων, τόσο σε Ευρωπαϊκές χώρες, όσο και σε τρίτες χώρες, όπου η πανδημία, και όχι μόνο, χρησιμοποιήθηκε ως δόλωμα για παραπλάνηση χρηστών με σκοπό την υποκλοπή πληροφοριών ή την εξαπάτηση. Συγκεκριμένα, παρατηρήθηκε σημαντική αύξηση των αναφορών για περιστατικά Phishing (Κατηγορίας Fraud) σε σχέση με το 2019. Αυτό οφείλεται και στις ιστοσελίδες που εμφανίστηκαν έχοντας ως θέμα την πανδημία του COVID-19, όπου, σύμφωνα με στοιχεία και πληροφόρηση του Εθνικού CSIRT, ταυτοποιήθηκαν σαράντα-εννέα (49) phishing domains που είχαν ως θέμα την πανδημία του COVID-19.

Κατά το έτος 2020, το Εθνικό CSIRT-CY έλαβε 19.033 ηλεκτρονικά μηνύματα ως ειδοποιήσεις από τις πλατφόρμες συλλογής πληροφοριών, όπως ShadowServer, CERT Bund, MISP, Abuse Helper και Team Cymru, με περίπου 12.000 γεγονότα (events) που πιθανόν να εξελίσσονταν σε περιστατικά (incidents).

Μετά από σχετική ανάλυση των μηνυμάτων και την εξεύρεση βημάτων μετριασμού, το Εθνικό CSIRT-CY διαβίβασε περίπου 3.000 ηλεκτρονικά μηνύματα προς τις Κρίσιμες Υποδομές Πληροφοριών που περιείχαν 220.386 ύποπτες Διευθύνσεις Πρωτοκόλλου Διαδικτύου (IPs) για την ενημέρωση των εμπλεκόμενων φορέων και για τυχόν ενέργειες εκ μέρους τους.

Οι ειδοποιήσεις που αποστέλλονται στην κάθε Κρίσιμη Υποδομή Πληροφοριών, εμπεριέχουν τις ύποπτες διευθύνσεις IP της υποδομής και τις κατηγορίες γεγονότων (events) στις οποίες εμπίπτει το καταγεγραμμένο γεγονός, βάσει της κατηγοριοποίησης περιστατικών του ENISA. Οι ειδοποιήσεις αυτές και το περιεχόμενο τους είναι σημαντικές στην προσπάθεια αποτροπής εκδήλωσης πιθανών κυβερνοεπιθέσεων.

6. ΠΙΣΤΟΠΟΙΗΣΕΙΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

6.1. Ο Κανονισμός της ΕΕ για την Κυβερνοασφάλεια

Ο Κανονισμός (ΕΕ) 2019/881[14] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου "σχετικά με τον ENISA (European Union Agency for Cybersecurity) και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών", ενισχύει τον οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο (ENISA) και θεσπίζει ένα πανευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας προϊόντων, υπηρεσιών και διαδικασιών τεχνολογιών πληροφοριών και επικοινωνίας (ΤΠΕ). Οι εταιρίες που δραστηριοποιούνται στην ΕΕ θα επωφελούνται (προαιρετικά προς το παρόν) από την πιστοποίηση των προϊόντων, των διαδικασιών και υπηρεσιών τους σε ένα μόνο κράτος-μέλος, με τα πιστοποιητικά τους να αναγνωρίζονται σε ολόκληρη την Ευρωπαϊκή Ένωση. Αναμένεται ότι η ευρεία υιοθέτηση της πιστοποίησης Κυβερνοασφάλειας θα εξαρτηθεί από τη δυναμική της αγοράς και από τυχόν ρυθμιστικές εξελίξεις (π.χ. όσον αφορά τη χρήση πιστοποιημένων προϊόντων σε κρίσιμες υποδομές κ.λπ.).

Το πλαίσιο πιστοποίησης προωθεί ευρωπαϊκά σχήματα πιστοποίησης τα οποία αποτελούν ολοκληρωμένο σύνολο κανόνων, τεχνικών απαιτήσεων, προτύπων και διαδικασιών. Αυτά τα σχήματα θα περιλαμβάνουν μεταξύ άλλων τις κατηγορίες προϊόντων και υπηρεσιών που καλύπτουν τις απαιτήσεις Κυβερνοασφάλειας, με αναφορά σε πρότυπα ή τεχνικές προδιαγραφές στον τύπο αξιολόγησης (assurance) (π.χ. αυτο-αξιολόγηση ή αξιολόγηση τρίτων) και στο επιδιωκόμενο επίπεδο διασφάλισης, δηλαδή βασικό, ουσιαστικό ή υψηλό.

Τα πιστοποιητικά που θα προκύπτουν θα αναγνωρίζονται σε όλα τα κράτη-μέλη της ΕΕ, διευκολύνοντας τις διασυνοριακές συναλλαγές των επιχειρήσεων και τους αγοραστές ώστε να κατανοούν καλύτερα τα χαρακτηριστικά ασφαλείας του προϊόντος ή της υπηρεσίας που αγοράζουν. Σημειώνεται ότι, τα πρώτα σχήματα πιστοποίησης που αναμένεται ότι θα εξεταστούν περιλαμβάνουν σχήματα που σχετίζονται με τα Κοινά Κριτήρια[15] (τα οποία μπορούν να αποτελέσουν τη βάση για την αξιολόγηση πολλών από τους προβλεπόμενους τύπους προϊόντων/υπηρεσιών, τις υπηρεσίες νεφοϋπολογιστικής και τα προϊόντα Internet of Things – IoT).

6.2. Αρμοδιότητες των Κρατών Μελών της ΕΕ

Ο Κανονισμός για την Κυβερνοασφάλεια περιλαμβάνει ορισμένες απαιτήσεις για την εφαρμογή του πλαισίου πιστοποίησης Κυβερνοασφάλειας της ΕΕ σε επίπεδο κράτους-μέλους. Μεταξύ αυτών είναι η σύσταση (ή ορισμός) Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας - ΕΑΠΚ (National Cybersecurity Certification Authority – NCCA). Η ΕΑΠΚ θα είναι υπεύθυνη για την εποπτεία και εφαρμογή των κανόνων που περιλαμβάνονται στα ευρωπαϊκά σχήματα πιστοποίησης Κυβερνοασφάλειας στην επικράτεια της, την εξουσιοδότηση των Οργανισμών Αξιολόγησης της Συμμόρφωσης (ΟΑΣ – Conformity Assessment Body - CAB) και θα ηγείται των δραστηριοτήτων πιστοποίησης Κυβερνοασφάλειας του κράτους-μέλους. Εκτός από την έγκριση της ΕΑΠΚ, οι ΟΑΣ πρέπει να διαπιστεύονται από τον Εθνικό Φορέα Διαπίστευσης (National Accreditation Body – NAB) - στην Κύπρο είναι ο Κυπριακός Οργανισμός Προώθησης Ποιότητας (ΚΟΠΠ) - για τα σχήματα τα οποία θα εκδίδουν πιστοποιητικά. Οι ελάχιστες εξουσίες και αρμοδιότητες της ΕΑΠΚ, καθώς και οι λεπτομέρειες για το γενικό πλαίσιο πιστοποίησης Κυβερνοασφάλειας, σε επίπεδο ΕΕ και σε εθνικό επίπεδο, καθορίζονται στον προαναφερθέντα Κανονισμό.

[14] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[15] 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.

6.3. Η Προσέγγιση της Κύπρου

Η Αρχή Ψηφιακής Ασφάλειας έχει οριστεί ως η αρμόδια Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας (ΕΑΠΚ) από το Υπουργικό Συμβούλιο το Σεπτέμβριο του 2019, και ενημερώθηκαν σχετικά τα αρμόδια σώματα της Ευρωπαϊκής Επιτροπής. Στο πλαίσιο της Απόφασης του Υπουργικού Συμβουλίου, η ΑΨΑ έχει την εντολή να προωθήσει την εφαρμογή του πλαισίου πιστοποίησης στην Κύπρο, το οποίο πρέπει να εφαρμοστεί μέχρι τον Ιούνιο του 2021. Η Αρχή συμμετέχει ενεργά στις σχετικές Επιτροπές, ομάδες εργασίας και σώματα της Ευρωπαϊκής Ένωσης για θέματα πιστοποίησης Κυβερνοασφάλειας. Επιπλέον, μέσω του πλαισίου της εν λόγω Απόφασης, η ΑΨΑ έχει εντολή να προωθήσει την ανάπτυξη τουλάχιστον ενός οργανισμού στην Κύπρο με τις κατάλληλες τεχνικές και οργανωτικές ικανότητες για να λειτουργήσει ως οργανισμός αξιολόγησης της συμμόρφωσης (Conformity Assessment Body – CAB). Οι προαναφερόμενες ενέργειες αποσκοπούν στη δημιουργία ενός μέρους του "ολοκληρωμένου πακέτου", με ανεπτυγμένες δομές, ώστε το κράτος μας να είναι σε θέση να χειρίζεται πιστοποιήσεις Κυβερνοασφάλειας προς όφελος της χώρας μας.

Η ΑΨΑ, εξασφαλίζοντας σχετική χρηματοδότηση μέσα από το ανταγωνιστικό πρόγραμμα του "CEF - Connecting Europe Facility", ξεκίνησε εντός του 2020 το έργο με τίτλο "B4C - Building up the Cybersecurity Certification Capabilities of Cyprus". Το έργο αυτό έχει ως στόχο την ολοκληρωμένη ανάπτυξη των δυνατοτήτων της Κυπριακής Δημοκρατίας, ώστε να είναι δυνατή η προσφορά ενός ευρέος φάσματος υπηρεσιών πιστοποίησης της Κυβερνοασφάλειας σε προϊόντα, υπηρεσίες και διαδικασίες. Σε συντομία, το έργο περιλαμβάνει τις ακόλουθες δραστηριότητες, οι οποίες ολοκληρώθηκαν εντός του 2020:

- Συντονισμός εμπλεκομένων (ΑΨΑ, Κυπριακή Εταιρεία Πιστοποίησης, Red Alert Labs)
- Ανάπτυξη και παράδοση σχετικών εκπαιδεύσεων για το Ευρωπαϊκό Πλαίσιο Πιστοποίησης Κυβερνοασφάλειας για το σχήμα πιστοποίησης EU Common Criteria και για το προτεινόμενο σχήμα πιστοποίησης Eurosmart IoT
- Ανάλυση του Κανονισμού για την Κυβερνοασφάλεια και ετοιμασία σχετικών τροποποιήσεων στο Νόμο της ΑΨΑ, Ν.89(Ι)/2020, σχετικά με τις εξουσίες και αρμοδιότητες της ως η Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας
- Προετοιμασία για τη δεύτερη φάση του έργου (ανάπτυξη ικανοτήτων)

Η ΑΨΑ έχει ολοκληρώσει την ετοιμασία της σχετικής τροποποιητικής Νομοθεσίας, η οποία, κατόπιν της έγκρισης του Υπουργικού Συμβουλίου, αναμένεται να προωθηθεί στη Βουλή των Αντιπροσώπων για ψήφιση εντός του 2021.

Στο Νομοσχέδιο μεταφέρθηκαν συγκεκριμένες πρόνοιες από τον Κανονισμό (ΕΕ) 2019/881, όσον αφορά τις απαραίτητες αρμοδιότητες και εξουσίες της Αρχής για να καταστεί δυνατή η εφαρμογή του πλαισίου σε Εθνικό Επίπεδο.

Σημειώνεται ότι, η ΑΨΑ συνεργάζεται στενά με τον Κυπριακό Οργανισμό Τυποποίησης (CYS) και την Κυπριακή Εταιρεία Πιστοποίησης (ΚΕΠ) για να φέρει εις πέρας τους ανωτέρω στόχους. Η ΚΕΠ είναι θυγατρική εταιρία του Εθνικού Φορέα Προτύπων της Κύπρου, του Κυπριακού Οργανισμού Τυποποίησης (CYS).

Ο ρόλος της ΑΨΑ είναι καθοριστικός καθώς θα έχει τις νομικές εξουσίες και αρμοδιότητες να εποπτεύει αποτελεσματικά ολόκληρο το πλαίσιο πιστοποίησης εντός της χώρας και να παρακολουθεί την εφαρμογή του, καθώς και να υποστηρίζει ενεργά και να συνδράμει το έργο του Κυπριακού Οργανισμού Προώθησης Ποιότητας (ΚΟΠΠ), ως ο Εθνικός Οργανισμός Διαπίστευσης. Το έργο B4C αναμένεται να ολοκληρωθεί στο τέλος του 2021, και περιλαμβάνει επίσης την εκτέλεση δύο πιλοτικών πιστοποιήσεων Κυβερνοασφάλειας.

7. ΕΘΝΙΚΕΣ & ΔΙΕΘΝΕΙΣ ΣΧΕΣΕΙΣ

Η συνεργασία και η ανάπτυξη εμπιστοσύνης με άλλες αρχές και το σύνολο των εμπλεκόμενων φορέων, αποτελεί βασικό πυλώνα και προτεραιότητα της Αρχής για τη σωστή και αποδοτική επιτέλεση του σκοπού της, τόσο σε εθνικό όσο και σε ευρωπαϊκό και διεθνές επίπεδο. Τα θέματα ασφάλειας, ιδιαίτερα στον κυβερνοχώρο, δεν μπορούν να αντιμετωπιστούν μεμονωμένα, αλλά απαιτείται συλλογική προσπάθεια στη διαχείριση τους.

Η Οδηγία NIS στηρίζεται στη φιλοσοφία και έχει ως βασική επιδίωξη τη συνεργασία και την ανάπτυξη εμπιστοσύνης με τη δημιουργία των πανευρωπαϊκών ομάδων συνεργασίας (βλ. ενότητα 7.4), την ομάδα Συνεργασίας (NIS Cooperation Group) και το δίκτυο συνεργασίας CSIRT (CSIRT network). Παράλληλα, προωθεί τη συνεργασία ανάμεσα σε όλους τους κρίσιμους τομείς και φορείς που διαχειρίζονται ουσιώδεις υπηρεσίες σε εθνικό και ευρωπαϊκό επίπεδο.

Προς αυτό το σκοπό, η ΑΨΑ αναπτύσσει σημαντικές πρωτοβουλίες για την ενίσχυση και προώθηση συνεργασιών σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο.

7.1. Συνεργασία με Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, Φορείς Κρίσιμων Υποδομών Πληροφοριών και άλλους σημαντικούς φορείς της Δημοκρατίας

7.1.1. Εφαρμογή του περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμου του 2020 (Ν. 89(Ι)/2020)

Στο πλαίσιο της εφαρμογής του περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμου του 2020 (Ν. 89(Ι)/2020), ο οποίος δημοσιεύτηκε τον Αύγουστο 2020, εστάλησαν επιστολές προς τον κάθε Φορέα Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέα Κρίσιμων Υποδομών Πληροφοριών, με τις οποίες κοινοποιήθηκε η Απόφαση του Επιτρόπου Επικοινωνιών για ορισμό τους ως Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών ή ως Φορείς Κρίσιμων Υποδομών Πληροφοριών.

Με στόχο την άσκηση των αρμοδιοτήτων και εξουσιών της, η ΑΨΑ, κατ' εφαρμογή του Άρθρου 19 του Νόμου Ν. 89(Ι)/2020, ζήτησε από τους Φορείς να ορίσουν άτομα για επικοινωνία με την ΑΨΑ για ρυθμιστικά θέματα ασφάλειας δικτύων και συστημάτων πληροφοριών και Κυβερνοασφάλειας, για τη λήψη ανακοινώσεων και ενημερωτικών δελτίων για τη διαχείριση περιστατικών παραβίασης ασφάλειας δικτύων και πληροφοριών και Κυβερνοασφάλειας, καθώς και άτομα για την κοινοποίηση στην ΑΨΑ περιστατικών παραβίασης ασφάλειας.

Η ΑΨΑ απέστειλε, επίσης, γραπτή ενημέρωση σχετικά με την εφαρμογή των περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Τέλη) Κανονισμών του 2020 (Κ.Δ.Π. 359/2020), βάσει των οποίων οι Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και Φορείς Κρίσιμων Υποδομών Πληροφοριών έχουν υποχρέωση να συμβάλουν στη χρηματοδότηση της λειτουργίας της Αρχής. Η ΑΨΑ ενημέρωσε τους Φορείς για την ενεργοποίηση της διαδικασίας είσπραξης τελών για το έτος 2021, με το ύψος της συνεισφοράς του κάθε Φορέα να καθορίζεται με βάση οικονομικό μοντέλο το οποίο ορίζεται στους περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Τέλη) Κανονισμούς του 2020 (Κ.Δ.Π.359/2020).

7.1.2. Ενέργειες από Εθνικό CSIRT-CY

Το Εθνικό CSIRT-CY, στο πλαίσιο των προληπτικών υπηρεσιών που προσφέρει στους Φορείς Κρίσιμων και Βασικών Υποδομών Πληροφοριών, παρέχει συνεχή και έγκυρη πληροφόρηση και ενημέρωση με σκοπό την ενδυνάμωση της ασφάλειας των υποδομών τους στον κυβερνοχώρο.

Οι παρακάτω διαδικτυακές εκπαιδεύσεις έχουν πραγματοποιηθεί με στόχο την ενημέρωση και ευαισθητοποίηση των εργαζομένων στις Κρίσιμες Υποδομές Πληροφοριών. Λόγω των πρωτόγνωρων συνθηκών που διανύει ο πλανήτης εξαιτίας της πανδημίας του COVID-19, όλες οι εκπαιδεύσεις πραγματοποιήθηκαν διαδικτυακά. Συγκεκριμένα, πραγματοποιήθηκαν οι ακόλουθες δραστηριότητες:

- τηλεδιάσκεψη μέσω του προγράμματος WEBEX με θέμα «Security Awareness for Remote Workers», όπου παρουσιάστηκαν μέτρα ασφαλείας κατά την εργασία εξ' αποστάσεως (π.χ. από το σπίτι)
- διαδικτυακή παρουσίαση σε Φορείς Κρίσιμων Υποδομών για την χρήση της πλατφόρμας MISP

Επίσης, το Εθνικό CSIRT-CY πρόσφερε σημαντικές πληροφορίες για την ευαισθητοποίηση, τόσο των διαχειριστών συστημάτων, όσο και των χρηστών στους οργανισμούς. Οι πληροφορίες αυτές αφορούσαν τα μέτρα προστασίας που πρέπει να λαμβάνονται, και σχετίζονται με τα ακόλουθα:

- οδηγία και πολιτική ασφάλειας χρηστών και διαχειριστών
- βέλτιστες πρακτικές σχετικά με τη χρήση κωδικών πρόσβασης και τη διαχείριση Active Directory

Επιπρόσθετα, στο πλαίσιο της εποπτείας του Εθνικού CSIRT-CY κατά το τρίτο τρίμηνο του 2020, πραγματοποιήθηκε έλεγχος επαλήθευσης στοιχείων επικοινωνίας με τις όλες τις Κρίσιμες Υποδομές Πληροφοριών της Κυπριακής Δημοκρατίας, καθώς και άσκηση χρόνου απόκρισης στην περίπτωση περιστατικού. Η άσκηση που διεξήχθη αφορούσε την επαλήθευση στοιχείων επικοινωνίας και χρόνου απόκρισης των Κρίσιμων Πληροφοριακών Υποδομών, μέσω ηλεκτρονικού μηνύματος και τηλεφωνικής επικοινωνίας.

7.2. Συνεργασία με Κρατικές Αρχές

7.2.1. Μνημόνιο Συνεργασίας με Ανοιχτό Πανεπιστήμιο Κύπρου

Στις 13 Οκτωβρίου 2020 υπογράφηκε Μνημόνιο Συνεργασίας μεταξύ της Αρχής Ψηφιακής Ασφάλειας και του Ανοικτού Πανεπιστημίου Κύπρου - Εργαστήριο Κυβερνοασφάλειας και Τηλεπικοινωνιών.

Σκοπός του Μνημονίου συνεργασίας είναι η Ανάπτυξη ενός συστήματος Κυβερνοασφάλεια/ Κυβερνοάμυνας για την προστασία των κρίσιμων υποδομών, καθώς και η ανάπτυξη μιας πλατφόρμας τύπου Cyber Range, η οποία θα χρησιμοποιείται για σκοπούς εκπαίδευσης σε θέματα Κυβερνοασφάλειας.

7.2.2. Μνημόνιο Συνεργασίας με τον Κυπριακό Οργανισμό Τυποποίησης (CYS)

Στις 9 Ιουλίου 2020 υπογράφηκε Μνημόνιο Συνεργασίας μεταξύ της Αρχής Ψηφιακής Ασφάλειας και του Κυπριακού Οργανισμού Τυποποίησης (CYS) για τη δημιουργία μοντέλου αξιολόγησης ωριμότητας δυνατοτήτων και πλαισίου ελέγχου (CMAAF - capability maturity assessment and audit framework). Σκοπός του Μνημονίου Συνεργασίας είναι ο καθορισμός του πλαισίου συνεργασίας μεταξύ της ΑΨΑ και του CYS που θα συμβάλει ενεργά στην υποστήριξη της ευρωπαϊκής ασφάλειας στον κυβερνοχώρο, στο πλαίσιο της εφαρμογής της Οδηγίας για την ασφάλεια των δικτύων και συστημάτων πληροφοριών (Οδηγία NIS). Επιπλέον, σκοπός του είναι ο καθορισμός του πλαισίου συνεργασίας για την ανάπτυξη μοντέλου αξιολόγησης ωριμότητας δυνατοτήτων στην Κυβερνοασφάλεια και την ανάπτυξη πλαισίου ελέγχου για την εφαρμογή του Εθνικού Πλαισίου Κυβερνοασφάλειας. Το σχετικό έργο CMAAF, αντικείμενο του Μνημονίου, ξεκίνησε το 2020 και αναμένεται να ολοκληρωθεί εντός του 2021.

7.2.3. Μνημόνιο Συνεργασίας με Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως

Μετά από σχετικές επαφές και συζητήσεις που έγιναν κατά το 2020 μεταξύ του Υπουργείου Δικαιοσύνης και Δημοσίας Τάξεως και της Αρχής Ψηφιακής Ασφάλειας, άρχισαν οι διεργασίες για τη σύναψη Μνημονίου Συνεργασίας για σκοπούς καθορισμού του πλαισίου συνεργασίας μεταξύ του Υπουργείου Δικαιοσύνης και Δημοσίας Τάξεως (ΥΔΔΤ)/Αστυνομίας (ΓΚΗΕ & ΔΕΗΔ) και της ΑΨΑ σε θέματα τα οποία άπτονται της καταπολέμησης ηλεκτρονικού εγκλήματος και ενίσχυσης του επιπέδου Κυβερνοασφάλειας στην Κυπριακή Δημοκρατία μέσω της υπηρεσίας της Αστυνομίας και ειδικότερα του Γραφείου Καταπολέμησης του Ηλεκτρονικού Εγκλήματος.

Εντός του 2020, το Μνημόνιο στάλθηκε στη Νομική Υπηρεσία για νομοτεχνικό έλεγχο και εντός του 2021 αναμένεται να ολοκληρωθεί και να υπογραφεί.

7.2.4. Μνημόνιο Συνεργασίας με Κεντρική Τράπεζα

Μετά από σχετικές επαφές και συζητήσεις που έγιναν κατά το 2020 μεταξύ της Κεντρικής Τράπεζας και της Αρχής Ψηφιακής Ασφάλειας, άρχισαν οι διεργασίες για τη σύναψη Μνημονίου Συνεργασίας για σκοπούς κοινοποίησης περιστατικών που θα αποστέλλει η Κεντρική Τράπεζα (υποχρεωτικές και εθελοντικές κοινοποιήσεις) στην Αρχή Ψηφιακής Ασφάλειας.

Εντός του 2021 αναμένεται ότι το Μνημόνιο θα τύχει νομοτεχνικού ελέγχου και θα υπογραφεί.

7.3. Συνεργασία με Τρίτες Χώρες

7.3.1. Εφαρμογή Μνημονίου Συναντίληψης με Israeli National Cyber Directorate

Στο πλαίσιο του Μνημονίου Συναντίληψης που υπογράφηκε το Δεκέμβριο του 2019 μεταξύ των Υπουργών Εξωτερικών των δύο χωρών, κατά τη διάρκεια του έτους 2020, πραγματοποιήθηκαν αρκετές επαφές συνεργασίας με την αντίστοιχη Υπηρεσία του Ισραήλ Israeli National Cyber Directorate σε διάφορους τομείς που αφορούν την Κυβερνοασφάλεια.

7.3.2. Πρόταση Συνεργασίας με Σουλτανάτο του Ομάν

Κατά το 2020, συνεχίστηκαν οι επαφές με αξιωματούχους του Σουλτανάτου του Ομάν μέσω του Υπουργείου Εξωτερικών και άρχισαν οι διεργασίες για τη σύναψη Μνημονίου Συναντίληψης στους τομείς της εκπαίδευσης και ανταλλαγής τεχνογνωσίας στα θέματα που αφορούν στην Κυβερνοασφάλεια.

Στόχος του Μνημονίου είναι η διεύρυνση των σχέσεων ανάμεσα στις δύο αντίστοιχες υπηρεσίες ως μέρος μιας ευρύτερης στρατηγικής. Το Μνημόνιο Συναντίληψης αναμένεται να υπογραφεί εντός του 2021.

7.3.3. Άλλες συνεργασίες με τρίτες χώρες

Μετά από σχετικές επαφές που έγιναν εντός του 2020 με αξιωματούχους της Αλβανίας μέσω του Υπουργείου Εξωτερικών, άρχισαν οι διεργασίες για τη σύναψη Μνημονίου Συναντίληψης στους τομείς της εκπαίδευσης και ανταλλαγής τεχνογνωσίας σε ότι αφορά την Κυβερνοασφάλεια.

Το Μνημόνιο Συναντίληψης μεταξύ της ΑΨΑ και των αρμοδίων Αρχών της Αλβανίας αναμένεται να υπογραφεί εντός του 2021.

7.4. Διεθνής Εκπροσώπηση

Η εκπροσώπηση της ΑΨΑ σε επιτροπές σε εθνικό και διεθνές επίπεδο κατά το 2020 αναλήφθηκε από τον Επίτροπο, το Βοηθό Επίτροπο, τον Αναπληρωτή Διευθυντή και τα στελέχη της Αρχής, ανάλογα με το επίπεδο εκπροσώπησης που απαιτείτο ή/και το αντικείμενο της κάθε επιτροπής. Αναφέρονται ενδεικτικά οι διάφοροι διεθνείς οργανισμοί και επιτροπές στις οποίες συμμετείχε η ΑΨΑ στο πλαίσιο της άσκησης των αρμοδιοτήτων της:

ENISA (European Union Agency for Cybersecurity) o MB (Management Board) o NLO (National Liaison Officers) Network o Cyber Crisis Cooperation and Exercises
Article 13a Expert Group for the security of electronic communications (έχει μετονομαστεί πλέον σε **ECASEC – European Competent Authorities for the Security of Electronic Communications)**
NAPAC (National Public Authorities Representative Committee of European Cyber Security Organisation, ECSO)
NIS Cooperation Group and relevant Work Streams o Work Stream 2 – Security Measures o Work Stream 3 – Incident Reporting o Work Stream 5 – Digital Service Providers o Work Stream 7 – Coordinated response to large scale cybersecurity incidents and crises o Work Stream 8 – Energy o Work Stream 10 – Digital Infrastructures o Ah-hoc additional COVID-19 coordination meetings o 5G Workstream (+ standardisation/certification sub-group) o NIS Review (Questionnaire(s), DSA interview, etc.)
CyCLONe – Cyber Crisis Liaison Officers Network
European Cybersecurity Certification Group (ECCG) and related sub-groups o ECCG Sub-group on scheme governance and maintenance
OSCE (Organization for Security and Co-operation in Europe)
CSP (Cyber Security Professionals) **Governance Board**
CSIRT Community Groups (FIRST, TI)
CSIRT Network
CERT-EU
ITU (International Telecommunication Union)
GFCE (Global Forum on Cyber Expertise)
GSCG (General Security Competence Group)

Ειδική αναφορά γίνεται στα ευρωπαϊκά σώματα τα οποία επηρεάζουν άμεσα τη λειτουργία και τις εργασίες της ΑΨΑ, την εναρμόνιση και την εφαρμογή της Οδηγίας NIS και της εθνικής νομοθεσίας. Συγκεκριμένα, η ΑΨΑ συμμετέχει στην Ομάδα Συνεργασίας NIS Cooperation Group, τη λειτουργία του οποίου συντονίζει το εκάστοτε κράτος-μέλος που έχει την προεδρία του Συμβουλίου της Ευρωπαϊκής Ένωσης και καθορίζει τις πολιτικές εφαρμογής του ευρωπαϊκού νομοθετικού πλαισίου από όλα τα κράτη-μέλη. Εντός του 2020, έγιναν τέσσερεις (4) συναντήσεις της ομάδας συνεργασίας, όπου συζητήθηκαν οι λεπτομέρειες υλοποίησης της Οδηγίας NIS σε στρατηγικό επίπεδο και έγινε συντονισμός ως προς την ενιαία προσέγγιση για την υλοποίησή της. Πραγματοποιήθηκε επίσης μεγάλος αριθμός έκτακτων συναντήσεων για συζήτηση των επιπτώσεων της πανδημίας COVID-19 στα δίκτυα Ηλεκτρονικών

Ειδική αναφορά γίνεται στα ευρωπαϊκά σώματα τα οποία επηρεάζουν άμεσα τη λειτουργία και τις εργασίες της ΑΨΑ, την εναρμόνιση και την εφαρμογή της Οδηγίας NIS και της εθνικής νομοθεσίας. Συγκεκριμένα, η ΑΨΑ συμμετέχει στην Ομάδα Συνεργασίας NIS Cooperation Group, τη λειτουργία του οποίου συντονίζει το εκάστοτε κράτος-μέλος που έχει την προεδρία του Συμβουλίου της Ευρωπαϊκής Ένωσης και καθορίζει τις πολιτικές εφαρμογής του ευρωπαϊκού νομοθετικού πλαισίου από όλα τα κράτη-μέλη. Εντός του 2020, έγιναν τέσσερεις (4) συναντήσεις της ομάδας συνεργασίας, όπου συζητήθηκαν οι λεπτομέρειες υλοποίησης της Οδηγίας NIS σε στρατηγικό επίπεδο και έγινε συντονισμός ως προς την ενιαία προσέγγιση για την υλοποίησή της. Πραγματοποιήθηκε επίσης μεγάλος αριθμός έκτακτων συναντήσεων για συζήτηση των επιπτώσεων της πανδημίας COVID-19 στα δίκτυα Ηλεκτρονικών Επικοινωνιών και για θέματα σχετικά με την Κυβερνοασφάλεια.

Επίσης, ειδική αναφορά γίνεται στο Ευρωπαϊκό Δίκτυο των Εθνικών CSIRT (CSIRTs Network), του οποίου το Εθνικό CSIRT-CY είναι ενεργό μέλος. Το CSIRTs Network είναι μια πλατφόρμα που ιδρύθηκε μέσω της Οδηγίας NIS, η οποία επιτρέπει την ανταλλαγή πληροφοριών, την ανταλλαγή γνώσεων και την άμεση βοήθεια και αλληλοϋποστήριξη μεταξύ των Εθνικών CSIRT σε περιστατικά Κυβερνοασφάλειας. Στις συναντήσεις του CSIRTs Network δίνεται η δυνατότητα συζήτησης για θέματα που αφορούν όλη την ευρωπαϊκή κοινότητα με θεματολογία όπως νέες απειλές για το τρέχον έτος, τρόποι επίλυσης προβλημάτων που προκύπτουν από κυβερνοεπιθέσεις και τρόποι με τους οποίους μια Εθνική Ομάδα CSIRT μπορεί να εξελιχθεί.

7.5. Εκπαιδεύσεις/Συνέδρια

7.5.1. Εκπαιδεύσεις για πιστοποιήσεις κυβερνοασφάλειας IoT

Η ΑΨΑ διοργάνωσε με επιτυχία εκπαιδευτικό πρόγραμμα για τις πιστοποιήσεις Κυβερνοασφάλειας στις 4 Δεκεμβρίου 2020, με τη συμμετοχή, τόσο μελών του προσωπικού της, όσο και συνεργατών από άλλες αρμόδιες αρχές και εμπλεκομένων από τον ιδιωτικό τομέα. Η εκπαίδευση αποτελεί μέρος της υλοποίησης ευρωπαϊκού συγχρηματοδοτούμενου προγράμματος το οποίο συντονίζει η ΑΨΑ, με τίτλο B4C – Building up the Cybersecurity Certification Capabilities of Cyprus. Η ΑΨΑ πέτυχε την εν λόγω συγχρηματοδότηση εντός του 2020 στο πλαίσιο ανταγωνιστικού προγράμματος και με τη συμμετοχή άλλων σχετικών φορέων. Η συγκεκριμένη εκπαίδευση είχε σκοπό την ενημέρωση των εμπλεκομένων για σχετικά σχήματα πιστοποίησης για το Διαδίκτυο των Πραγμάτων (IoT - Internet of Things), τα οποία θα προωθηθούν για υλοποίηση ως μέρος του Ευρωπαϊκού Κανονισμού για την Κυβερνοασφάλεια. Οι επιχειρήσεις που δραστηριοποιούνται στον τομέα του IoT θα μπορούν να πιστοποιούν τα προϊόντα τους σχετικά με την Κυβερνοασφάλεια μόνο σε ένα κράτος μέλος και τα σχετικά πιστοποιητικά θα τυγχάνουν αναγνώρισης, αυτόματα, σε πανευρωπαϊκό επίπεδο.

7.5.2. Περιφερειακές εκπαιδεύσεις

Η ΑΨΑ διοργάνωσε περιφερειακό εκπαιδευτικό πρόγραμμα που απευθυνόταν σε αστυνομικές αρχές με θέμα την ασφάλεια στον κυβερνοχώρο. Η εκπαίδευση πραγματοποιήθηκε στο πλαίσιο του προγράμματος CYCLOPS. Συγκεκριμένα, η εκπαίδευση επικεντρώθηκε στην έρευνα (investigation) και τις προκλήσεις που μπορεί να επιφέρει στον τομέα ασφάλειας και διαχείρισης κινδύνων η παράνομη αγοραπωλησία μέσω Darknet Markets (DNMs).

7.5.3. Εκπαιδεύσεις Εθνικού CSIRT-CY

Στο πλαίσιο της ενδυνάμωσης της ομάδας του Εθνικού CSIRT-CY και της προσπάθειας για τη συνεχή θωράκιση των συστημάτων της Κυπριακής Δημοκρατίας στον κυβερνοχώρο, η εκπαίδευση των μελών του Εθνικού CSIRT-CY είναι συνεχής και λαμβάνει διάφορες μορφές, όπως, παρακολούθηση εργαστηρίων και σεμιναρίων εντός και εκτός Κύπρου ειδικά σχεδιασμένων για την Υπηρεσία, συμμετοχή/παρακολούθηση Ομάδων Εργασίας και συμμετοχή σε εγχώριες και πανευρωπαϊκές ασκήσεις.

Κατά τη διάρκεια του 2020, πραγματοποιήθηκαν οι πιο κάτω εκπαιδεύσεις στο προσωπικό του Εθνικού CSIRT-CY:

- *Προηγμένη ανάλυση κακόβουλου λογισμικού & αντίστροφος τεχνικός σχεδιασμός (Advanced Malware Analysis & Advanced Reverse Engineering)*
  Η εκπαίδευση πραγματοποιήθηκε από τις 3 έως τις 7 Μαρτίου 2020 και συμπεριελάμβανε τεχνική θεματολογία με κύριο στόχο την ανάλυση Malware (κακόβουλου λογισμικού). Η εκπαίδευση επικεντρώθηκε στην εκμάθηση μεθοδολογιών για τη σωστή ανάλυση κακόβουλων αρχείων με στόχο την εύρεση Indicators of Compromise (IoCs) και τη δημιουργία βημάτων μετριασμού βάσει αυτών.
- *Άσκηση αντιμετώπισης κυβερνοπολέμου "ΠΑΝΟΠΤΗΣ 2020"*
  Στο πλαίσιο ενδυνάμωσης των τεχνικών ικανοτήτων κατά της απειλής Κυβερνοπολέμου, πραγματοποιήθηκε η Διακλαδική, Διακρατική και Διακυβερνητική άσκηση «ΠΑΝΟΠΤΗΣ 2020» από τις 28 Σεπτεμβρίου 2020 μέχρι τις 2 Οκτωβρίου 2020. Η Αρχή Ψηφιακής Ασφάλειας / Εθνικό CSIRT-CY, συμμετείχαν στην Άσκηση μαζί με Έφεδρους του 51 Λόχου Κυβερνοάμυνας (ΛΚΥΒ), και υπηρεσίες του Δημοσίου, Ιδιωτικού και ακαδημαϊκού τομέα. Η άσκηση περιλάμβανε εντοπισμό και αντιμετώπιση διαφόρων περιστατικών Κυβερνοασφάλειας, καλύπτοντας τόσο μεμονωμένα συμβάντα, όσο και περιστατικά ευρύτερης έκτασης, που απαιτούσαν συντονισμένη ανταπόκριση σε πολλαπλά επίπεδα. Τα επεισόδια κάλυψαν πλειάδα αντικειμένων κυβερνοάμυνας όπως, ανάλυση ιομορφικού λογισμικού, ψηφιακή διερεύνηση πειστηρίων σε διαφορετικά λειτουργικά συστήματα Η/Υ, δρομολογητών, έλεγχο ευπαθειών εφαρμογών διαδικτύου και εντοπισμό/ ανάλυση παραβίασης δικτυακής υποδομής.
- *Εκπαίδευση πιστοποίησης ηθικού χάκερ (Certified Ethical Hacker - CEH)*
  Η εκπαίδευση παρείχε όλες τις απαραίτητες γνώσεις που απαιτούνται για την ασφάλεια δικτύων και συστημάτων πληροφοριών. Ασχολήθηκε με την εις βάθος κατανόηση διαφόρων τύπων επιθέσεων από κακόβουλες ομάδες, καθώς και προληπτικών μέτρων. Η εκπαίδευση έχει ολοκληρωθεί για μέρος της Ομάδας του Εθνικού CSIRT-CY το Δεκέμβριο του 2020, ωστόσο, λαμβάνοντας υπόψη τη σημαντικότητά της, συνεχίζεται η παρακολούθησή της και από την υπόλοιπη ομάδα. Με το πέρας της εκπαίδευσης, όλοι οι Αναλυτές του Εθνικού CSIRT-CY θα έχουν την κατανόηση των αδυναμιών και των τρωτών σημείων ενός συστήματος, γεγονός το οποίο θα ενισχύσει τους ελέγχους ασφαλείας στις Κρίσιμες Υποδομές Πληροφοριών της Κυπριακής Δημοκρατίας, με απώτερο στόχο την ελαχιστοποίηση των κινδύνων κυβερνοεπίθεσης.
- *Διαδικτυακή εκπαίδευση ανάλυσης κακόβουλου λογισμικού και ασφάλεια ψηφιακής εγκληματολογίας (Malware Analysis and Digital Forensics Security)*
  Η εκπαίδευση πραγματοποιήθηκε από τις 25 μέχρι τις 26 Νοεμβρίου 2020 από το Ακαδημαϊκό CSIRT σε συνεργασία με τον οργανισμό ENISA και τη συμβολή του Πανεπιστημίου Κύπρου, του Ευρωπαϊκού Πανεπιστημίου, και του Εθνικού CSIRT-CY. Τα θέματα που παρουσιάστηκαν αφορούσαν Malware Analysis και Reverse Engineering, καθώς και Network Forensics που αφορά τα IoT[16] and Mobile Devices.

[16] Internet of Things

- *Διαδικτυακές εκπαιδεύσεις FIRST (Forum of Incident Response and Security Teams)*
  - Building an Intelligence-Driven Organization
  - Turning Data into Actional Intelligence
  - Deep Dark Web? - Is Criminal Intel from 'Dark Web' Really Still Effective?
  - How Threat Reporting by Cybersecurity Firms Systematically Underrepresents Threats to Civil Society
  - CTI Collaboration Using STIX and Elasticsearch
  - Sighting Use Cases
  - MalDomain ML: A Machine Learning Model to Find Malicious Domains Before They Go Bad
  - rcATT: Retrieving ATT&CK Tactics and Techniques in Cyber Threat Reports
  - Rethinking the Graph Visualization for Threat Reports
  - xHunt... An Anime Fan's Attack Campaign in the Middle East
  - Narrator: Generating Intelligence Reports from Structured Data
  - Obtaining Cyber Threat Intelligence through Reverse Engineering
  - Bringing Intelligence into Cyber Deception with MITRE ATT&CK
  - Understanding What's Next; Combining Red Team Findings and Adversary Playbooks
  - How I Became Our Own Worst Enemy, I Mean Adversary
  - From ‘Fog of War’ to Reducing Noise in Daily Operations

8. ΑΛΛΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

8.1. Συμμετοχή σε Ευρωπαϊκά Συγχρηματοδοτούμενα Προγράμματα

8.1.1. CEF CYberSafety II & III

Στις 31 Δεκεμβρίου 2020 ολοκληρώθηκε με επιτυχία η Δράση "CYberSafety II" (CEF 2018-CY-IA 0012) στο πλαίσιο του προγράμματος Connecting Europe Facility (CEF) - Telecom. Στόχος της Δράσης ήταν η δημιουργία κουλτούρας ασφαλούς διαδικτύου για τα παιδιά. Το έργο εντάσσεται στο πλαίσιο υλοποίησης της «Εθνικής στρατηγικής για ένα ασφαλέστερο διαδίκτυο για τα παιδιά στην Κύπρο». Το πρόγραμμα υλοποιήθηκε από 8 συνολικά εταίρους με το Παιδαγωγικό Ινστιτούτο Κύπρου να είναι ο συντονιστής της Δράσης και είχε συνολική διάρκεια 2 χρόνια.

Οι δράσεις της ΑΨΑ περιλάμβαναν τηη παράδοση σεμιναρίων προς μαθητές και εκπαιδευτικούς Γυμνασίων και Λυκείων της Κύπρου για την εκπαίδευση και ανάπτυξη δεξιοτήτων για την ασφαλή χρήση του διαδικτύου. Η πρωτοτυπία στην προσέγγιση της ΑΨΑ στο πρόγραμμα αυτό αφορά το ότι τα σεμινάρια ήταν διαδραστικά, προσφέροντας μια εμπειρία μοναδική και ιδιαίτερα ενδιαφέρουσα στους συμμετέχοντες. Οι εκπαιδεύσεις περιλάμβαναν τις ακόλουθες θεματικές ενότητες:

- Ασφαλής Χρήση των Δημόσιων Δικτύων WiFi - Διάλεξη
- Κίνδυνοι από τη χρήση των Δημόσιων Δικτύων WiFi - Εργαστήριο
- Κακόβουλα λογισμικά και πρακτικές για την αποφυγή τους - Διάλεξη/Εργαστήριο
- Κακόβουλο Λογισμικό Υποκλοπής Δεδομένων KEYLOGGER - Διάλεξη/Εργαστήριο
- Ασφάλεια λογισμικών και αναβαθμίσεις - Διάλεξη/Εργαστήριο
- Κίνδυνοι Εγκατάστασης Λογισμικών APKs (Third Party Applications) - Διάλεξη/Εργαστήριο
- Ασφαλής πλοήγηση στο διαδίκτυο και η διαφορά μεταξύ των πρωτοκόλλων HTTP vs HTTPs (όπως εμφανίζονται στους συνδέσμους - URL) - Διάλεξη/Εργαστήριο

Το πρώτο τρίμηνο του 2020, στο πλαίσιο του πιο πάνω προγράμματος, έχουν πραγματοποιηθεί 19 εκπαιδεύσεις σε 4 σχολεία δημοτικής και μέσης εκπαίδευσης με συνολικό αριθμό συμμετεχόντων τους 300 μαθητές και μαθήτριες και 39 εκπαιδευτικούς.

Ωστόσο, λόγω της παγκόσμιας έξαρσης της πανδημίας COVID-19 μετά τον Απρίλιο του 2020, δεν κατέστη δυνατόν να πραγματοποιηθεί καμία εκπαίδευση με φυσική παρουσία. Συγκεκριμένα, είχαν διευθετηθεί 33 εκπαιδεύσεις σε 11 σχολεία μέσης εκπαίδευσης με συνολικό αριθμό συμμετεχόντων 1.196, αλλά ακυρώθηκαν λόγω της πανδημίας.

Κατά την έναρξη της νέας σχολικής χρονιάς το Σεπτέμβριο του 2020, η Αρχή Ψηφιακής Ασφάλειας σχεδίασε ακόμα 2 διαδικτυακές διαλέξεις ώστε να προστεθούν κάποιες επιλογές για εκπαιδεύσεις εν μέσω της πανδημίας, με θέμα τις βέλτιστες πρακτικές για την ασφαλή χρήση του Διαδικτύου και την ασφαλή χρήση και αναγνώριση κακόβουλων ή ύποπτων ηλεκτρονικών μηνυμάτων. Συνολικά, πραγματοποιήθηκαν 3 εκπαιδεύσεις σε 1 σχολείο μέσης εκπαίδευσης σε συνολικά 60 μαθητές / μαθήτριες και 2 εκπαιδευτικούς.

Εντός του 2020 υποβλήθηκε αίτηση με συντονιστή το Παιδαγωγικό Ινστιτούτο Κύπρου, για τη συγχρηματοδότηση της συνέχισης του έργου αυτού με την επωνυμία "CYberSafety III" (2020-CY-IA-0069) στο πλαίσιο του ιδίου προγράμματος Connecting Europe Facility (CEF) – Telecom. Η διάρκεια της Δράσης αυτής θα είναι 15 μήνες, ενώ η υλοποίηση της αποτελεί ιδιαίτερη πρόκληση υπό το φως των δεδομένων της πανδημίας που ταλανίζει τον τομέα της παιδείας.

8.1.2. CEF iDSAMPL– integrated Digital Security Authority Management Platform

Στόχος του έργου είναι η αναβάθμιση του υφιστάμενου συστήματος RCMS (Risk and Compliance Management System) της ΑΨΑ (βλ. ενότητα 3.3.2).

Κατά το 2020, η ΑΨΑ συνέχισε την εκπόνηση του έργου, για το οποίο πέτυχε την έγκριση χρηματοδότησης μέσω του Ευρωπαϊκού προγράμματος CEF Telecom 2018. Το ποσό χρηματοδότησης ανέρχεται στις €99.585, με το συνολικό προϋπολογισμό του έργου να ανέρχεται σε €132.780.

Το έργο θα ολοκληρωθεί κατά το πρώτο εξάμηνο του 2021.

8.1.3. CEF B4C – Building up the Cybersecurity Certification Capabilities of Cyprus

Στόχος του έργου είναι η αναβάθμιση των ικανοτήτων της Κυπριακής Δημοκρατίας σχετικά με τη διενέργεια πιστοποιήσεων Κυβερνοασφάλειας. Η ΑΨΑ πέτυχε τη σχετική χρηματοδότηση μετά από ανταγωνιστική διαδικασία κατά το 2020, και, μέσω του έργου αυτού, υλοποιεί μεγάλο μέρος των σχεδιασμών της Κυπριακής Δημοκρατίας για το Ευρωπαϊκό Πλαίσιο Πιστοποίησης Κυβερνοασφάλειας (βλ. ενότητα 6.1).

Έχουν προσδιορισθεί οι ακόλουθοι στόχοι ούτως ώστε το έργο:

- να καθορίσει τις πρόνοιες του Κανονισμού που πρέπει να μεταφερθούν στο νόμο της ΑΨΑ, προκειμένου η Αρχή να διαθέτει τις κατάλληλες εξουσίες και αρμοδιότητες
- να αναπτύξει τις εσωτερικές ικανότητες της ΑΨΑ για την αποτελεσματική ανάληψη των υποχρεώσεων ελέγχου και εποπτείας των πιστοποιήσεων Κυβερνοασφάλειας στην Κύπρο
- να προωθήσει την ανταλλαγή βέλτιστων πρακτικών και σχετικών πληροφοριών για την πιστοποίηση, με την υποστήριξη ομότιμων στην πιστοποίηση ασφάλειας στον κυβερνοχώρο εντός της ΕΕ

Το έργο περιλαμβάνει μια σειρά εκπαιδεύσεων που καλύπτουν ολόκληρη τη διαδικασία πιστοποίησης από την αρχή έως το τέλος, συμπεριλαμβανομένων των αλληλεπιδράσεων μεταξύ των διαφόρων εμπλεκόμενων φορέων.

Η πρόταση για συγχρηματοδότηση είχε υποβληθεί κάτω από το πρόγραμμα CEF Telecom 2019 - Cyber Security τον Νοέμβριο 2019 και σε αυτή συμμετέχουν επίσης η Κυπριακή Εταιρεία Πιστοποίησης και η γαλλική εταιρεία Red Alert Labs Ltd. Το έργο έχει διάρκεια 18 μηνών και ξεκίνησε τον Ιούλιο του 2020 με συνολικό προϋπολογισμό €160.000 (από τα οποία €40.000 θα καλυφθούν από τους προϋπολογισμούς των συμμετεχόντων, και €120.000 από τη συγχρηματοδότηση της ΕΕ). Το έργο αναμένεται να ολοκληρωθεί στο τέλος του 2021.

8.2. Νέες Προτάσεις για Ευρωπαϊκή Χρηματοδότηση

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

Η ΑΨΑ είχε κύριο ρόλο στην ετοιμασία και υποβολή πρότασης για Ευρωπαϊκή συγχρηματοδότηση ύψους €210.000 για την περαιτέρω αναβάθμιση των ικανοτήτων της Κυπριακής Δημοκρατίας σχετικά με τη διενέργεια πιστοποιήσεων Κυβερνοασφάλειας, με έμφαση στον τομέα των υπηρεσιών νεφοϋπολογιστικής. Οι βασικότεροι στόχοι του έργου είναι:

- αξιοποίηση και επέκταση των αποτελεσμάτων που παράγονται από το υφιστάμενο έργο B4C (Δράση CEF 2019-EU-IA-0109)
- ενίσχυση των εσωτερικών δυνατοτήτων της Εθνικής Αρχής Προτύπων της Ιρλανδίας (NSAI)

- ενίσχυση των εσωτερικών δυνατοτήτων όλων των συνεργατών στο έργο, μέσω νέου εκπαιδευτικού υλικού για την πιστοποίηση υπηρεσιών νεφοϋπολογιστικής, και μέσω της πρακτικής εφαρμογής των διαδικασιών πιστοποίησης με τη διεξαγωγή σχετικών πιλοτικών πιστοποιήσεων
- διασυνοριακή ανταλλαγή βέλτιστων πρακτικών και σχετικών πληροφοριών που σχετίζονται με δραστηριότητες αξιολόγησης της συμμόρφωσης (συμπεριλαμβανομένης ολόκληρης της «αλυσίδας αξίας» του Ευρωπαϊκού Πλαισίου Πιστοποίησης Κυβερνοασφάλειας), μέσω δομημένης αμφίδρομης ανταλλαγής μεταξύ Κύπρου και Ιρλανδίας
- οικοδόμηση ενός ολοκληρωμένου μοντέλου αναφοράς για άμεση υποστήριξη του πλήρους φάσματος των δραστηριοτήτων πιστοποίησης της Κυβερνοασφάλειας από το Α έως το Ω, μέσω της ανάπτυξης ενός ολοκληρωμένου μοντέλου αναφοράς για όλους τους εμπλεκομένους, τις αλληλεπιδράσεις και τις ροές, όπως ορίζεται στο Ευρωπαϊκό Πλαίσιο Πιστοποίησης Κυβερνοασφάλειας
- αποτελεσματική διάδοση των αποτελεσμάτων του προηγούμενου έργου σε μεγάλο αριθμό ενδιαφερομένων στις εμπλεκόμενες χώρες και σε ολόκληρη την Ευρώπη, μέσω δομημένων δραστηριοτήτων διάδοσης και επικοινωνίας σε σχετικές ομάδες εργασίας και σε άλλα ευρωπαϊκά φόρα

Η πρόταση για συγχρηματοδότηση έχει υποβληθεί κάτω από το πρόγραμμα CEF Telecom 2020 τον Δεκέμβριο 2020 και σε αυτή συμμετέχουν επίσης η Κυπριακή Εταιρεία Πιστοποίησης και η γαλλική εταιρεία Red Alert Labs Ltd, καθώς και ο εθνικός οργανισμός τυποποίησης (NSAI) της Ιρλανδίας. Σε περίπτωση που η σχετική αίτηση εγκριθεί, το έργο θα διαρκέσει 2 χρόνια και αναμένεται να ξεκινήσει εντός του 2021 με συνολικό προϋπολογισμό €280.000.

8.2.2. CEF JCOP – Joint Cybersecurity Operations Platform

Τα περιστατικά Κυβερνοασφάλειας συμβαίνουν όλο και πιο συχνά, ανεξαρτήτως του πόσο προετοιμασμένος μπορεί να είναι ένας οργανισμός. Ο οργανισμός ENISA, μέσω της αναφοράς «ENISA Threat Landscape» για το 2020, δηλώνει ότι «κατά την επόμενη δεκαετία, οι κίνδυνοι στον κυβερνοχώρο θα γίνουν όλο και πιο δύσκολο να εκτιμηθούν και να ερμηνευθούν λόγω της αυξανόμενης πολυπλοκότητας των επιθέσεων». Αναφέρεται, επίσης, αύξηση εξελιγμένων και στοχευμένων επιθέσεων ransomware κατά του δημόσιου τομέα, των οργανισμών υγειονομικής περίθαλψης και άλλων βιομηχανιών, καθώς και ο αυξημένος αριθμός υβριδικών απειλών, τόσο στον κυβερνοχώρο, όσο και στο φυσικό κόσμο. Η πανδημία COVID-19 έχει επίσης επιδεινώσει την έκθεση σε κίνδυνο. Αξίζει να σημειωθεί ότι ο ENISA έχει χαρακτηρίσει την περίοδο που διανύουμε ως «παραγωγική περίοδο για κακόβουλους χρήστες που πραγματοποιούν επιθέσεις με θέμα την πανδημία».

Με κίνητρο τα παραπάνω, η πρόταση που έχει κατατεθεί στο πλαίσιο του Ευρωπαϊκού προγράμματος CEF από την ΑΨΑ και τους συνεργάτες της περιλαμβάνει το σχεδιασμό και την ανάπτυξη πλατφόρμας επιχειρησιακής ασφάλειας στον κυβερνοχώρο προσαρμοσμένη στις ανάγκες των κρατών μελών της ΕΕ. Συνεργάτες της ΑΨΑ στο έργο είναι η Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων με το Υπουργείο Ψηφιακής Διακυβέρνησης της Ελλάδος, το Πολυτεχνείο Κρήτης, το Πανεπιστήμιο του Όσλο, το Technische Universitaet Braunschweig Γερμανίας, το Norwegian National Security Authority, και η εταιρεία Sphynx Analytics Limited. Η πλατφόρμα θα περιλαμβάνει εργαλειοθήκη και μεθόδους που διευκολύνουν την κοινή επίγνωση της κατάστασης, την ετοιμότητα και τη συντονισμένη διαχείριση περιστατικών, αλλά και την ανταπόκριση σε περιστατικά Κυβερνοασφάλειας, σύμφωνα με το πλαίσιο της ΕΕ για την Κυβερνοασφάλεια, ως αυτό έχει θεσπιστεί μέσω της Οδηγίας NIS.