ΑΡΧΗ ΨΗΦΙΑΚΗΣ
ΑΣΦΑΛΕΙΑΣ

Έκθεση Δραστηριοτήτων του έτους 2019

Υποβάλλεται στον Πρόεδρο της Δημοκρατίας σύμφωνα με την πρόνοια του άρθρου 26 του Ν.17(Ι)/2018 ο οποίος διέπει τη λειτουργία της Αρχής Ψηφιακής Ασφάλειας

Αύγουστος 2020

ΠΕΡΙΕΧΟΜΕΝΑ

ΧΑΙΡΕΤΙΣΜΟΣ ΕΠΙΤΡΟΠΟΥ

Η παρούσα έκθεση απολογισμού του έργου της Αρχής Ψηφιακής Ασφάλειας συνοψίζει το σύνολο των δραστηριοτήτων που υλοποιήθηκαν σε όλο το φάσμα των πεδίων αρμοδιότητας της κατά το έτος 2019.

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 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. 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, έχει ως κύριο στόχο την προληπτική και ενεργητική αντιμετώπιση κυβερνο-απειλών, ενισχύοντας με τον τρόπο αυτό την ψηφιακή ασφάλεια όλων των σημαντικών υποδομών και υπηρεσιών του κράτους. 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 2019:

- οριστικοποίηση του Εθνικού Πλαισίου Κυβερνοασφάλειας που διέπει τον τρόπο αναγνώρισης και εφαρμογής των κατάλληλων μέτρων ασφάλειας για τις κρίσιμες υποδομές πληροφοριών
- οριστικοποίηση και δημοσίευση του πλαισίου κοινοποίησης συμβάντων και περιστατικών ασφάλειας στην ΑΨΑ
- διενέργεια αξιολόγησης κινδύνων για τα νέα δίκτυα επικοινωνιών πέμπτης γενεάς (5G) σε εθνικό επίπεδο
- ανάληψη του ρόλου της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας
- έσοδα της τάξης των 549.000 ευρώ στο πλαίσιο χρηματοδότησης από ευρωπαϊκές πηγές για υλοποίηση προγραμμάτων

Εντός του 2019 ολοκληρώθηκε ο νομοτεχνικός έλεγχος του νέου Νόμου 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. Ο νέος Νόμος καθώς και σχετικοί κανονισμοί , κατόπιν της έγκρισης του Υπουργικού Συμβουλίου, προωθήθηκαν στη Βουλή των Αντιπροσώπων με την ψήφιση του να αναμένεται εντός του 2020. Επίσης, ολοκληρώθηκε ο νομοτεχνικός έλεγχος των Κανονισμών Επιλογής και Προαγωγών της ΑΨΑ και κατόπιν της έγκρισης του Υπουργικού Συμβουλίου προωθήθηκαν στη Βουλή των Αντιπροσώπων, 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 2019 ανέλαβε μεγάλο αριθμό δράσεων ενημέρωσης και ευαισθητοποίησης των πολιτών σχετικά με τις επιπτώσεις των απειλών στον κυβερνοχώρο. Παρέχει πληροφορίες μέσω του διαδικτύου για σημαντικές απειλές στον κυβερνοχώρο, αλλά και τεχνικές συμβουλές και οδηγίες για την εξασφάλιση ψηφιακής προστασίας. Επίσης, μέσω του CSIRT-CY, χειρίζεται 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 2019, έχει πραγματοποιήσει δεκάδες παρουσιάσεις ευαισθητοποίησης γύρω από την κυβερνοασφάλεια στις κρίσιμες υποδομές πληροφοριών, ενώ παρέχει 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 2019, 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 της επίθεσης και των επηρεαζόμενων συστημάτων, ενέργειες μετριασμού καθώς και αναγνώριση της συμπεριφοράς και δράσης του επιτιθέμενου. 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 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 τον Μάρτιο 2019 έχει αξιολογηθεί ότι βρίσκεται στο μέγιστο επίπεδο ωριμότητας του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών ENISA. Επίσης, μέσα σε λιγότερους από εννέα μήνες έχει καταστεί αναγνωρισμένος συνεργάτης (Accredited Member) του φορέα Trusted Introducer καθώς και μέλος του παγκόσμιου συνδέσμου Forum of Incident Response Teams (FIRST) που αφορά ομάδες CSIRT παγκοσμίως (έναντι της συνήθους χρονικής περιόδου των δύο έως τεσσάρων χρόνων).

Μια σημαντική εξέλιξη το 2019 ήταν ο ορισμός της Αρχής Ψηφιακής Ασφάλειας ως την αρμόδια εθνική αρχή πιστοποίησης κυβερνοασφαλειας, 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 έχει ενταχθεί στις καθημερινές δραστηριότητες και δράσεις 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 Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων

1. ΔΙΟΙΚΗΣΗ

Η Αρχή Ψηφιακής Ασφάλειας ("ΑΨΑ") έχει ιδρυθεί και λειτουργεί βάσει του Νόμου 17(Ι)/2018 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών και υπάγεται στον Επίτροπο Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων 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 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.

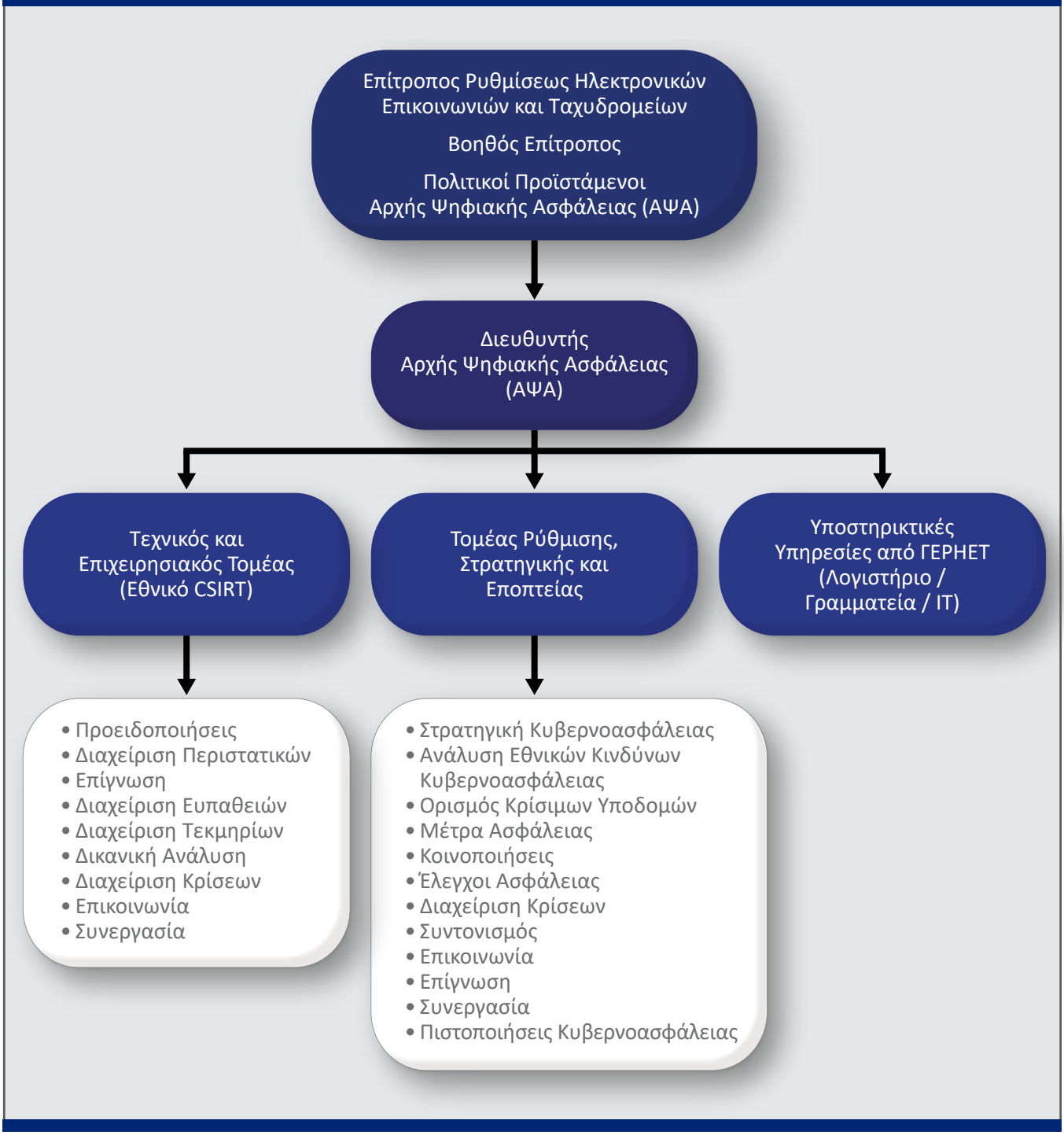
1.2. Στόχοι Αρχής Ψηφιακής Ασφάλειας

Η ΑΨΑ 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 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 ικανοποιητικό 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 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 και επιχειρησιακό βραχίονα της ΑΨΑ σε θέματα επιχειρησιακής συνέχειας των δικτύων πληροφοριακών συστημάτων των ουσιωδών και κρίσιμων υποδομών του κράτους.

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 επίσης συντονίζει 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 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. Τομέας Εθνικού CSIRT – Τεχνικός και Επιχειρησιακός Τομέας

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 ανέπτυξε λεπτομερείς και ολοκληρωμένες διαδικασίες λειτουργίας, διαχείρισης περιστατικών και ασφάλειας δικτύου, καθώς και συστήματα και εργαλεία πληροφορικής υψηλών προδιαγραφών με αποτέλεσμα σε σύντομο χρονικό διάστημα να καταστεί πλήρες μέλος της κοινότητας των CSIRT σε διεθνές και ευρωπαϊκό επίπεδο (FIRST[1], TI[2]).

Η λειτουργία του Εθνικού CSIRT περιλαμβάνει, 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

1.4. Στελέχωση

Κατά το 2019, τρεις (3) μόνιμοι υπάλληλοι από το ΓΕΡΗΕΤ (Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων), και συγκεκριμένα ένας (1) Ανώτερος Λειτουργός, ένας (1) Λειτουργός και μία (1) Γραμματέας, συνέχισαν να απασχολούνται αποκλειστικά 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 δεκαέξι (16) άτομα: ένα (1) προϊστάμενο και δεκαπέντε (15) αναλυτές, αφού εντός του έτους 2019 έξι (6) επιπλέον άτομα σύναψαν συμβάσεις παροχής υπηρεσιών.

Με την ψήφιση της αναθεωρημένης νομοθεσίας της ΑΨΑ και των Κανονισμών Πρόσληψης Προσωπικού, οι οποίες αναμένεται να ολοκληρωθούν εντός του 2020, 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

Ο Νόμος 17(Ι)/2018 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών έχει ιδρύσει επίσημα την ΑΨΑ και έχει εντάξει το Εθνικό CSIRT στη δομή της. Ο Νόμος παρέχει τις αρμοδιότητες στην ΑΨΑ για την πλήρη εφαρμογή της Οδηγίας NIS. Εντός του 2019, προωθήθηκαν περαιτέρω νομοθετικές ενέργειες για την αποτελεσματικότερη εφαρμογή του νέου πλαισίου, όπως αναφέρεται στην ενότητα 3.1 της παρούσας Έκθεσης.

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

1.6. Δημιουργία Δομών για Συμμόρφωση με τον Ευρωπαϊκό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων (General Data Protection Regulation - GDPR)

Στο πλαίσιο της Δράσης 11 του ευρωπαϊκού συγχρηματοδοτούμενου προγράμματος Connecting Europe Facility (CEF) για την ανάπτυξη και βελτίωση του Εθνικού CSIRT (2016-CY-IA-0129) (βλ. ενότητα 8.1.1), έγινε αξιολόγηση, καθορισμός των πολιτικών, διαδικασιών και δομών, καθώς και ετοιμασία σχετικών εγγράφων στα πλαίσια της συμμόρφωσης με τον Ευρωπαϊκό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων (GDPR). Για την υλοποίηση των σχετικών ρυθμίσεων ξεκίνησαν διαβουλεύσεις με την Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για εξειδικευμένα και ευαίσθητα θέματα που αφορούν την αποτελεσματική διεκπεραίωση των κατά Νόμο εργασιών του Εθνικού CSIRT. Ταυτόχρονα, προωθήθηκαν και οι αντίστοιχες διαδικασίες για τις υπόλοιπες δομές της ΑΨΑ με τη βοήθεια εξωτερικών συμβούλων, οι οποίες ολοκληρώθηκαν εντός του 2019.

Προς αυτό το σκοπό, ο Επίτροπος Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων έχει ορίσει Λειτουργό Προσωπικών Δεδομένων (Data Protection Officer - DPO), ο οποίος λειτουργεί ανεξάρτητα από τις δομές της ΑΨΑ και ο οποίος αναφέρεται απευθείας στον Επίτροπο για θέματα προστασίας προσωπικών δεδομένων.

1.7. Ανάπτυξη Πολιτικών και Διαδικασιών Εθνικού CSIRT

Κατά το έτος 2019, το Εθνικό CSIRT-CY, στο πλαίσιο της συνεχούς επικαιροποίησης των πολιτικών λειτουργίας του, αναθεώρησε και προσάρμοσε όλες τις εσωτερικές διαδικασίες του σύμφωνα με τις τρέχουσες ανάγκες του και το διεθνές πρότυπο SIM3[3]. Οι διαδικασίες καλύπτουν όλες τις πτυχές λειτουργίας της Ομάδας, όπως την ασφάλεια συστημάτων, την ασφάλεια δικτύου, τις διαδικασίες λειτουργίας των στελεχών και την ασφάλεια του κτιρίου.

Μια από τις καινοτομίες που εφάρμοσε ήταν η υλοποίηση του πλαισίου διαχείρισης περιστατικών (Incident Handling Management) στη βάση του πλαισίου Information Technology Infrastructure Library (ITIL) για τις εσωτερικές του διαδικασίες αλλά και για τη δημιουργία Πολιτικών Ασφάλειας που αφορούν τον τομέα της διαχείρισης υπηρεσιών στο χώρο της κυβερνοασφάλειας της Κυπριακής Δημοκρατίας. Το πλαίσιο ITIL είναι πρωτοπόρος παγκόσμιος δόκιμος οδηγός παροχής υπηρεσιών τεχνολογίας πληροφοριών ο οποίος αναπτύχθηκε στη βάση βέλτιστων πρακτικών και εφαρμόζεται από ανεπτυγμένους οργανισμούς, συμπεριλαμβανομένων και κρίσιμων υποδομών πληροφοριών, και απευθύνεται σε άτομα και επιχειρήσεις που είναι υπεύθυνα για το σχεδιασμό, την παρακολούθηση και διαχείριση υπηρεσιών υψηλής ποιότητας στον τομέα της πληροφορικής.

Ωστόσο, το Εθνικό CSIRT-CY είναι ο μοναδικός οργανισμός στην Κύπρο και στο εξωτερικό που υιοθετεί τη συγκεκριμένη προσέγγιση σε συνδυασμό με το πλαίσιο διαχείρισης περιστατικών FIRST (Forum of Incident Response and Security Teams).

Σε πρόσφατη αξιολόγηση ωριμότητας από τον οργανισμό της Ευρωπαϊκής Ένωσης European Union Agency for Cybersecurity (ENISA) για την Κυβερνοασφάλεια σχετικά με το “CSIRT Maturity Assessment”, έχει αναδείξει το Εθνικό CSIRT-CY της Κύπρου ως το πιο γρήγορα αναπτυσσόμενο Εθνικό CSIRT στην Ευρωπαϊκή Ένωση και του έχει απονέμει πιστοποιητικό με επίπεδο “Advanced"σχετικά με το “CSIRT Maturity Assessment”. Αυτό είχε σαν αποτέλεσμα να προταθεί από την ENISA η συμμετοχή μας και σε μελλοντικά peer review assessments άλλων χωρών παρόμοια με την εξέταση που είχαμε για τη δική μας ομάδα, και ως επακόλουθο δύο μέλη της ομάδας του Εθνικού CSIRT-CY έχουν εκπαιδευτεί και πιστοποιηθεί ως SIM3 Auditors.

[3] SIM3: Μοντέλο για Security Incident Management Maturity που χρησιμοποιείται για την αξιολόγηση ωριμότητας ενός CSIRT.

Γράφημα 1: Πιστοποιητικό Εθνικού CSIRT για "CSIRT Maturity Assessment"– ENISA

Η πρόληψη διαρροής δεδομένων είναι επίσης ένα από τα πιο σημαντικά τεχνικά χαρακτηριστικά που θα πρέπει να τηρούνται σε ένα οργανισμό όπως το Εθνικό CSIRT-CY, και ως εκ τούτου, και προς αποτροπή διαρροής δεδομένων, το Εθνικό CSIRT-CY έχει ξεκινήσει, εντός του 2019, διαδικασία γενικής λύσης στα εργαλεία της ασφάλειας, ταξινόμησης δεδομένων και κρυπτογράφησης (DLP - Data Loss Prevention).

1.8. Δημιουργία Ιστοσελίδας ΑΨΑ και Εθνικού CSIRT

Η ΑΨΑ έχει προχωρήσει στο σχεδιασμό ιστοσελίδας (https://dsa.cy) για την πληρέστερη ενημέρωση των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών, των Φορέων Κρίσιμων Υποδομών Πληροφοριών, των παροχέων ηλεκτρονικών επικοινωνιών και των παροχέων ψηφιακών υπηρεσιών. Η ιστοσελίδα παρέχει πληροφορίες με νέα και ανακοινώσεις, την οργάνωση της ΑΨΑ, τη σχετική νομοθεσία, τη Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, τις δραστηριότητες της ΑΨΑ και σχετικές εκδηλώσεις.

Το Εθνικό CSIRT-CY, μέσω της ιστοσελίδας του (https://csirt.cy) συνεχίζει να προσφέρει σημαντικές πληροφορίες σχετικά με την αύξηση ευαισθητοποίησης τόσο των διαχειριστών συστημάτων, αλλά και των χρηστών ενός οργανισμού σε σχέση με τις προφυλάξεις που πρέπει να λαμβάνονται σε συνεχή βάση, αλλά κυρίως κατά περιόδους κρίσεων, με σκοπό την ενδυνάμωση των θεμελίων της άμυνας ενός οργανισμού στον κυβερνοχώρο. Επίσης, μέσα στο 2019, έγινε αναβάθμιση των υπηρεσιών που προσφέρει μέσα από την ιστοσελίδα και οι οποίες περιλαμβάνουν:

- Ενημερωτικά άρθρα που περιλαμβάνουν Indicators of Compromise (IoCs)
- Ειδοποιήσεις περί θεμάτων ασφαλείας
- Ειδοποιήσεις που περιλαμβάνουν πληροφορίες σχετικά με αναβαθμίσεις ασφαλείας
- Ανακοινώσεις για εκπαιδεύσεις και άλλες εκδηλώσεις
- Νομοθεσίες

Μέχρι το τέλος του 2019 είχαν αναρτηθεί 528 ενημερώσεις, προειδοποιήσεις και άρθρα στην ιστοσελίδα του Εθνικού CSIRT-CY σχετικά με περιστατικά κυβερνοασφάλειας. Επίσης, η επισκεψιμότητα της ιστοσελίδας περιλάμβανε 9.866 χρήστες, οι οποίοι είχαν πρόσβαση σε 12.736 διαφορετικά τμήματα της ιστοσελίδας, όπως ενημερώσεις, προειδοποιήσεις και άρθρα.

2. ΟΙΚΟΝΟΜΙΚΕΣ ΚΑΤΑΣΤΑΣΕΙΣ

2.1. Μη Ελεγμένες Οικονομικές Καταστάσεις για το έτος 2019

Οι οικονομικές καταστάσεις της Αρχής Ψηφιακής Ασφάλειας για το έτος που έληξε την 31η Δεκεμβρίου 2019 ετοιμάστηκαν όπως προβλέπεται από το άρθρο 25 του Ν. 17(Ι)/2018. Οι βασικότερες πληροφορίες για την κατανομή δαπανών και εσόδων, που περιέχονται στις μη ελεγμένες οικονομικές καταστάσεις για το έτος που έληξε στις 31 Δεκεμβρίου 2019, απεικονίζονται στο Γράφημα 2 και περιλαμβάνουν:

- έσοδα ύψους €2.228.912 και δαπάνες ύψους €1.469.345
- πλεόνασμα έτους ύψους €759.567

Πίνακας 2: Μη Ελεγμένη Κατάσταση Συνολικών Εισοδημάτων 2019

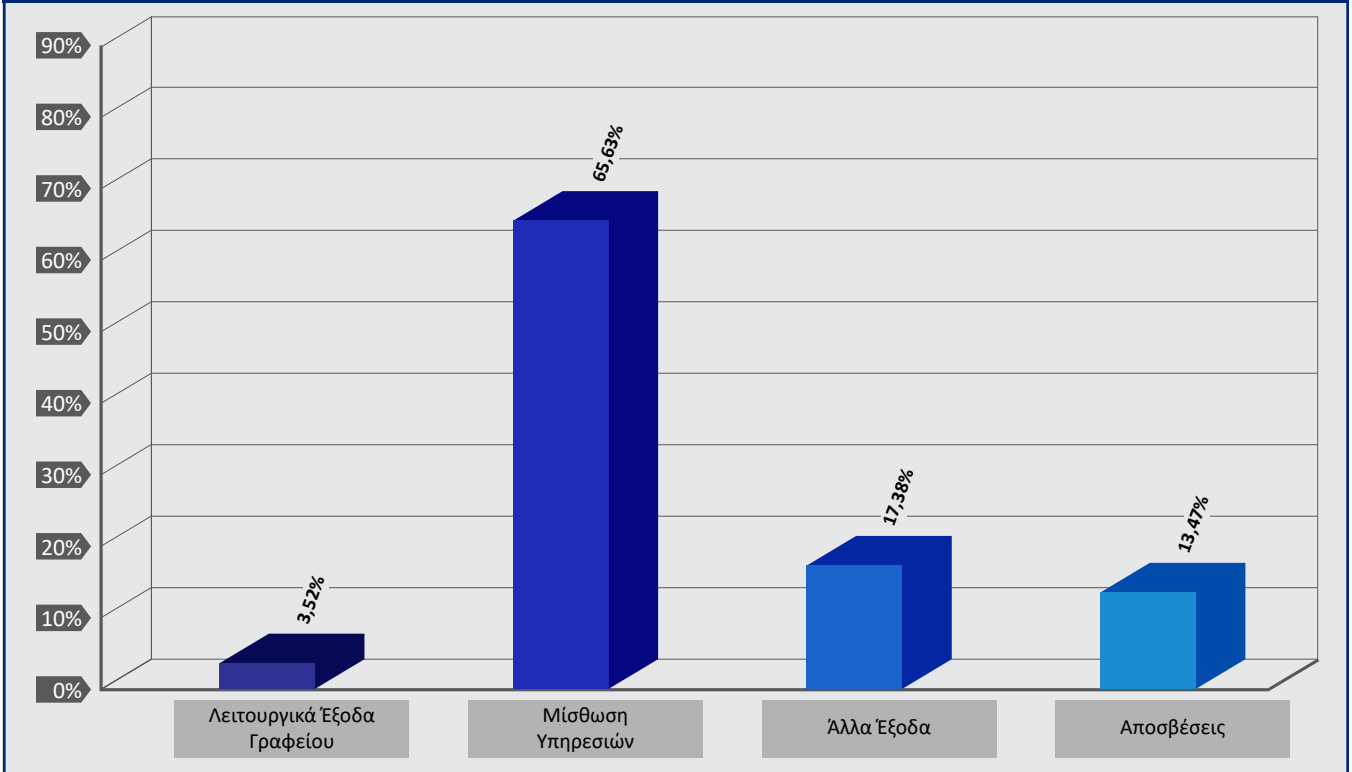
	2019 €	2018 €
Έσοδα		
Άλλα έσοδα*	2.228.859	1.040.000
Τόκοι	53	57
	2.228.912	**1.040.057**
Έξοδα		
Κόστος προσωπικού**	0	0
Οδοιπορικά	604	35
Λειτουργικά έξοδα γραφείου	51.718	11.019
Μίσθωση υπηρεσιών	964.299	860.288
Άλλα έξοδα	254.839	70.446
Αποσβέσεις εξοπλισμού και εγκαταστάσεων	126.136	38.323
Αποσβέσεις άυλου ενεργητικού	71.749	24.755
	1.469.345	**1.004.867**
Πλεόνασμα/(Έλλειμμα) έτους από συνήθεις εργασίες	759.567	35.190
Συνολικά εισοδήματα για το έτος	**759.567**	**35.190**

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

* Η πίστωση στο κονδύλι άλλα έσοδα για το 2018 αφορά χορηγία ΥΜΕΕ, και για το 2019 αφορά χορηγία ΥΜΕΕ, μεταφορά κεφαλαίου από ΓΕΡΗΕΤ σε ΑΨΑ που αφορά την υπόλοιπη χρηματοδότηση υλοποίησης ευρωπαϊκού προγράμματος και κατάθεση χρηματοδότησης για τη δημιουργία ακαδημαϊκού CSIRT.

** Το CSIRT από τον 11/2017 στελεχώνεται με μίσθωση υπηρεσιών.

Γράφημα 2: Κατανομή Δαπανών για το 2019



Πίνακας 3: Μη Ελεγμένη Κατάσταση Χρηματοοικονομικής Θέσης στις 31 Δεκ. 2019

	2019 €	2018 €
ΠΕΡΙΟΥΣΙΑΚΑ ΣΤΟΙΧΕΙΑ		
Μη κυκλοφορούντα περιουσιακά στοιχεία		
Εγκαταστάσεις και εξοπλισμός	553.784	171.154
Άυλα στοιχεία ενεργητικού	87.973	50.261
Συνολο μη κυκλοφορούντων περιουσιακών στοιχείων	**631.757**	**221.415**
Κυκλοφορούντα περιουσιακά στοιχεία		
Χρεώστες και προπληρωμές	32.998	15.415
Μετρητά στην τράπεζα	3.346.705	673.787
Σύνολο κυκλοφορούντων περιουσιακών στοιχείων	**3.379.703**	**689.202**
ΣΥΝΟΛΟ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ	**4.011.460**	**910.617**
ΙΔΙΑ ΚΕΦΑΛΑΙΑ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ		
Ίδια κεφάλαια		
Αποθεματικά	794.757	35.190
Σύνολο ιδίων κεφαλαίων	**794.757**	**35.190**
Τρέχουσες υποχρεώσεις		
Πιστωτές και οφειλόμενα έξοδα	1.016.703	875.427
Προεισπραχθέντα Τέλη	2.200.000	-
Ολικό τρεχουσών υποχρεώσεων	**3.216.703**	**875.427**
ΟΛΙΚΟ ΙΔΙΩΝ ΚΕΦΑΛΑΙΩΝ ΚΑΙ ΥΠΟΧΡΕΩΣΕΩΝ	**4.011.460**	**910.617**

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

3. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

3.1. Νομοθεσία Αρχής Ψηφιακής Ασφάλειας

Στις 5 Απριλίου 2018 ιδρύθηκε βάσει νομοθεσίας η ΑΨΑ ως ανεξάρτητη αρχή για την εφαρμογή των διατάξεων του περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμου του 2018 (17(Ι)/2018), στο πλαίσιο εναρμόνισης με την Ευρωπαϊκή Οδηγία NIS 2016/1148, η οποία αφορά μέτρα για υψηλό κοινό επίπεδο ασφάλειας δικτύων και συστημάτων πληροφοριών. Η ΑΨΑ λειτουργεί ως η εθνική αρμόδια αρχή για την ασφάλεια δικτύων και συστημάτων πληροφοριών και κυβερνοασφάλειας, και συμπεριλαμβάνει το Εθνικό CSIRT ως τον εθνικό φορέα άμεσης ανταπόκρισης σε συμβάντα που σχετίζονται με 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 παρόχους ηλεκτρονικών επικοινωνιών και παρόχους ψηφιακών υπηρεσιών στην Κύπρο, σύμφωνα με τη μεθοδολογία υπολογισμού τελών που καθορίζεται σε κανονισμούς που εκδίδονται από τη Βουλή δυνάμει των διατάξεων σχετικού νόμου.

3.1.1. Αναθεώρηση Νομοθεσίας περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών

Εντός του 2019 ολοκληρώθηκε ο νομοτεχνικός έλεγχος του νέου Νόμου σχετικά με την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών και κατόπιν της έγκρισης του Υπουργικού Συμβουλίου προωθήθηκε στη Βουλή των Αντιπροσώπων.

Τον Νοέμβριο του 2019 ολοκληρώθηκαν οι συζητήσεις στην Κοινοβουλευτική Επιτροπή Μεταφορών Επικοινωνιών και Έργων και εντός του 2020 αναμένεται η προώθηση του στην ολομέλεια και η ψήφιση του από το σώμα.

Ο Νόμος μεταφέρει τις αρμοδιότητες σε θέματα ασφάλειας δικτύων και πληροφοριών και κυβερνοασφάλειας στον τομέα Ηλεκτρονικών Επικοινωνιών από το ΓΕΡΗΕΤ στην ΑΨΑ, και περιγράφει με πλήρη λεπτομέρεια τις ολοκληρωμένες αρμοδιότητες της ΑΨΑ, μεταφέροντας πλήρως την Οδηγία NIS στην Εθνική Νομοθεσία. Ο Νόμος ρυθμίζει θέματα προσωπικού, εσωτερικής λειτουργίας της ΑΨΑ και συνεργασίας της με άλλους αρμόδιους φορείς.

3.1.2. Κανονισμοί Πρόσληψης Προσωπικού

Εντός του 2019 ολοκληρώθηκε ο νομοτεχνικός έλεγχος των Κανονισμών Επιλογής και Προαγωγών της ΑΨΑ και κατόπιν της έγκρισης του Υπουργικού Συμβουλίου προωθήθηκαν στη Βουλή των Αντιπροσώπων. Το Νοέμβριο του 2019 ολοκληρώθηκαν οι συζητήσεις στην Κοινοβουλευτική Επιτροπή Μεταφορών Επικοινωνιών και Έργων και εντός του 2020 αναμένεται η προώθηση στην ολομέλεια και η ψήφιση τους από το σώμα.

3.1.3. Κανονισμοί Χρηματοδότησης Αρχής Ψηφιακής Ασφάλειας

Εντός του 2019 ολοκληρώθηκε, επίσης ο νομοτεχνικός έλεγχος των Κανονισμών Χρηματοδότησης της ΑΨΑ και κατόπιν της έγκρισης του Υπουργικού Συμβουλίου προωθήθηκαν στην Βουλή των Αντιπροσώπων. Τον Νοέμβριο του 2019 ολοκληρώθηκαν οι συζητήσεις στην Κοινοβουλευτική Επιτροπή Μεταφορών Επικοινωνιών και Έργων και εντός του 2020 αναμένεται η προώθηση τους στην ολομέλεια και η ψήφιση τους από το σώμα.

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 του δημόσιου τομέα και υπολογίζεται λαμβάνοντας υπόψη τον προϋπολογισμό εσόδων της Αρχής, τον αριθμό των φορέων που υπόκεινται σε ρύθμιση βάσει των προνοιών του Νόμου, τα ακαθάριστα ετήσια έσοδα/προϋπολογισμό του κάθε φορέα, και το επίπεδο κρισιμότητας των σχετικών υποδομών πληροφοριών που διαχειρίζονται.

3.1.4. Μέτρα Ασφάλειας NIS

Κατά το 2019, η ΑΨΑ ολοκλήρωσε την ανάπτυξη ολιστικού πλαισίου μέτρων ασφάλειας, σύμφωνα με τις πρόνοιες της Οδηγίας NIS. Το πλαίσιο αυτό διαμορφώνει μια δομημένη προσέγγιση ελέγχου και διαδικασιών που θα εξασφαλίζει ένα ελάχιστο επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών στους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και τους Φορείς Κρίσιμων Υποδομών Πληροφοριών στην Κύπρο. Το περιεχόμενο του πλαισίου περιέχει μια ολοκληρωμένη προσέγγιση εντοπισμού, αξιολόγησης και επιλογής μέτρων για τη διαχείριση κινδύνων στον κυβερνοχώρο, με ειδική εστίαση στη διατήρηση των στοιχείων της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της αυθεντικότητας των δικτύων, πληροφοριών 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.

Το πλαίσιο αυτό τέθηκε σε δημόσια διαβούλευση και έχει ετοιμαστεί σε μορφή δευτερογενούς νομοθεσίας, λαμβάνοντας υπόψη τα αποτελέσματα της δημόσιας διαβούλευσης. Η σχετική νομοθεσία είναι έτοιμη και θα εκδοθεί με την ψήφιση του αναθεωρημένου Νόμου της ΑΨΑ εντός του 2020. Επίσης, εντός του 2020, προγραμματίζεται η ανάπτυξη ολοκληρωμένου πλαισίου ελέγχου για την αποτελεσματική εποπτεία των σχετικών φορέων ως προς την υλοποίηση των μέτρων ασφάλειας.

3.1.5. Κοινοποίηση Περιστατικών Παραβίασης Ψηφιακής Ασφάλειας

Κατά το 2019, η ΑΨΑ ολοκλήρωσε την ετοιμασία σχετικής νομοθεσίας για τις κοινοποιήσεις περιστατικών παραβίασης ψηφιακής ασφάλειας. Η νομοθεσία τέθηκε σε δημόσια διαβούλευση και εκδόθηκε (ΚΔΠ 218/2019), λαμβάνοντας υπόψη τα σχετικά σχόλια των εμπλεκομένων φορέων. Η νομοθεσία αυτή περιλαμβάνει ολοκληρωμένο πλαίσιο, διαδικασίες και έντυπα κοινοποίησης περιστατικών που οφείλουν να υποβάλλουν οι διάφοροι φορείς προς την ΑΨΑ, δηλαδή οι Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, οι Φορείς Κρίσιμων Υποδομών Πληροφοριών, οι παροχείς ηλεκτρονικών επικοινωνιών και οι παροχείς ψηφιακών υπηρεσιών, καθώς και τις διαδικασίες διασυνοριακών κοινοποιήσεων σύμφωνα με τις πρόνοιες της Οδηγίας NIS.

Επίσης, η ΑΨΑ ξεκίνησε έργο για την ηλεκτρονική υποβολή περιστατικών μέσω εξειδικευμένης πλατφόρμας, η οποία θα ολοκληρωθεί και θα τεθεί σε λειτουργία εντός του 2020 (βλ. σχετική ενότητα 3.4.2).

3.1.6. Εγγραφές Παροχέων Ψηφιακών Υπηρεσιών

Κατά το 2019, ολοκληρώθηκε και τέθηκε σε δημόσια διαβούλευση προσχέδιο Απόφασης για τις εγγραφές των παροχέων ψηφιακών υπηρεσιών στην Κύπρο. Το κείμενο της νομοθεσίας αυτής έχει ολοκληρωθεί, λαμβάνοντας υπόψη τα σχετικά σχόλια των εμπλεκομένων φορέων, και θα εκδοθεί με την ψήφιση του αναθεωρημένου Νόμου της ΑΨΑ εντός του 2020.

3.2. Νομοθεσία Ηλεκτρονικών Επικοινωνιών για την Ασφάλεια Δικτύων και Πληροφοριών

Τα θέματα αυτά διέπονται από το Νόμο 112(I)/2004, ως έχει τροποποιηθεί, και τύγχαναν χειρισμού από την ομάδα για την Ασφάλεια Δικτύων και Πληροφοριών του ΓΕΡΗΕΤ. Εντός του 2020, προγραμματίζεται όπως οι συγκεκριμένες πρόνοιες διαγραφούν από το Νόμο 112(I)/2004 και μεταφερθούν στο νέο νόμο της ΑΨΑ, κατ' εφαρμογή των σχετικών αποφάσεων του Υπουργικού Συμβουλίου.

Προς αυτό το σκοπό ετοιμάστηκε τροποποιητικό νομοσχέδιο στο Νόμο 112(I)2004 του ΓΕΡΗΕΤ ο οποίος κατόπιν της έγκρισης του Υπουργικού Συμβουλίου προωθήθηκε στη Βουλή των Αντιπροσώπων για ψήφιση του από το σώμα.

3.3. Κυβερνοασφάλεια σε Δίκτυα Επικοινωνιών Πέμπτης Γενεάς (5G Cybersecurity)

Τον Μάρτιο 2019, η Ευρωπαϊκή Επιτροπή εξέδωσε Σύσταση σχετικά με την κυβερνοασφάλεια των δικτύων ηλεκτρονικών επικοινωνιών πέμπτης γενεάς (5G). Η Σύσταση πρότεινε συγκεκριμένα μέτρα εντός του 2019 από το κάθε κράτος μέλος της ΕΕ. Οι κυριότερες δραστηριότητες που προέβλεπε η Σύσταση ήταν η διενέργεια εθνικής αξιολόγησης κινδύνων για τα δίκτυα επικοινωνιών 5G από το κάθε κράτος-μέλος, η δημιουργία κοινής σχετικής αξιολόγησης κινδύνων σε ευρωπαϊκό επίπεδο, και η ανάπτυξη κοινής ευρωπαϊκής εργαλειοθήκης με μέτρα αντιμετώπισης των εντοπισμένων κινδύνων (5G Toolbox).

Κατά το 2019, η ΑΨΑ προχώρησε σε αγορά υπηρεσιών υποστήριξης, με αντικείμενο την έρευνα και διενέργεια εθνικής αξιολόγησης κινδύνου κυβερνοασφάλειας για δίκτυα ηλεκτρονικών επικοινωνιών 5G. Στην εν λόγω εργασία, λήφθηκαν υπόψη όλες οι απαιτήσεις και συστάσεις του σχετικού εγγράφου της Ευρωπαϊκής Επιτροπής, μαζί με τα δεδομένα που επικρατούν στην Κύπρο σχετικά με την ανάπτυξη των δικτύων 5G, για την εκπλήρωση των σχετικών υποχρεώσεων μας ως κράτος μέλος, ούτως ώστε τα αποτελέσματα του έργου να έχουν πραγματική αξία και χρήση σε μετέπειτα δραστηριότητες της ΑΨΑ. Σημειώνεται ότι η ΑΨΑ απέσπασε πολύ θετικά σχόλια από εκπροσώπους της Ευρωπαϊκής Επιτροπής σχετικά με την ποιότητα και το εύρος των παραδοτέων του έργου αυτού.

Με την έκδοση της εργαλειοθήκης τον Ιανουάριο 2020, η ΑΨΑ προχωρά σε ανάλυση των προνοιών της, τον καταρτισμό σχετικού προγράμματος δράσεων και την ανάπτυξη δευτερογενούς νομοθεσίας για τη θέσπιση συγκεκριμένων υποχρεώσεων ασφάλειας προς τους παροχείς δικτύων ηλεκτρονικών επικοινωνιών 5G.

3.4. Ανάπτυξη Υποδομών και Εργαλείων

3.4.1. Υποδομή Εθνικού CSIRT

Ο σχεδιασμός του δικτύου του Εθνικού CSIRT-CY και οι σχετικές διαδικασίες έχουν σχεδιαστεί ώστε οι υπηρεσίες να προσφέρονται μέσω απομονωμένων συστημάτων με στόχο την καλύτερη και ασφαλέστερη επεξεργασία δεδομένων, αφού κύρια αποστολή του οργανισμού είναι η προστασία των κρίσιμων υποδομών πληροφοριών της Κυπριακής Δημοκρατίας.

Η υποδομή αναβαθμίζεται συνεχώς λαμβάνοντας υπόψη τα καλύτερα ευρωπαϊκά 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.

Εντός του 2019 το Εθνικό CSIRT-CY έχει προμηθευτεί εξειδικευμένα εργαλεία και προγράμματα για συστηματικούς ελέγχους ασφαλείας στις κρίσιμες υποδομές πληροφοριών του κράτους, όπως:

- Την πλατφόρμα Nagios, η οποία προσφέρει συνεχή ανάλυση διαδικτυακών διακομιστών και διακομιστών ηλεκτρονικής αλληλογραφίας σε πραγματικό χρόνο και εξασφαλίζει την ακεραιότητα και τη διαθεσιμότητα των διαδικτυακών υπηρεσιών των κρίσιμων υποδομών της Κυπριακής Δημοκρατίας, τις εμπορικές τράπεζες, τους παρόχους υπηρεσιών διαδικτύου και τους παρόχους ηλεκτρονικών υπηρεσιών
- Την πλατφόρμα Hardenize, η οποία επιβλέπει την ασφάλεια και διαμόρφωση της ιστοσελίδας και του ηλεκτρονικού ταχυδρομείου ενός οργανισμού, καθώς και των πιστοποιητικών εγκυρότητας και ασφαλείας περιήγησης. Εντός του 2019 έχει γίνει έλεγχος σε 530 domain names .cy και .gov.cy
- Το εργαλείο Netsparker, το οποίο διεκπεραιώνει εξ' αποστάσεως έλεγχο ιστοσελίδων για ανεύρεση τρωτών σημείων. Μέχρι το τέλος του 2019, μετά τη συγκατάθεση τους, έχουν γίνει 33 έλεγχοι σε κρίσιμες υποδομές πληροφοριών της Κυπριακής Δημοκρατίας
- Παραμετροποιημένοι Αισθητήρες (Sensors), οι οποίοι προφέρουν ελέγχους ασφαλείας σε πραγματικό χρόνο βασισμένοι σε πρωτόκολλα δικτύου για ανίχνευση και ανάλυση ύποπτων και κακόβουλων ενεργειών

Επίσης, το Εθνικό CSIRT-CY για το έτος 2019 έχει προχωρήσει στην αγορά υπηρεσιών για την εξασφάλιση συστημάτων για την πρόληψη διαρροής δεδομένων, την ταξινόμηση δεδομένων, την κρυπτογράφηση και Two Factor Authentication (2FA). Τα συγκεκριμένα συστήματα αναμένεται να τεθούν σε εφαρμογή εντός του 2020.

3.4.2. Ολοκληρωμένη Πλατφόρμα Διαχείρισης Εμπλεκόμενων Φορέων ΑΨΑ

Κατά το 2019, η ΑΨΑ ολοκλήρωσε την πρώτη φάση έργου, με εξωτερικούς συνεργάτες, για τη δημιουργία ολοκληρωμένης πλατφόρμας διαχείρισης εμπλεκομένων φορέων (κυρίως για τους εποπτευόμενους φορείς). Το έργο αυτό ξεκίνησε το Δεκέμβριο του 2018 και έχει ως αντικείμενο την αναβάθμιση του υφιστάμενου συστήματος RCMS (Risk and Compliance Management System) της ΑΨΑ, το οποίο απέκτησε από το ΓΕΡΗΕΤ, και το οποίο αποτελούσε μέρος της υλοποίησης του έργου για την ανάλυση επικινδυνότητας για θέματα κυβερνοασφάλειας σε εθνικό επίπεδο (National Level Cyber Risk Assessment - αρ. προσφοράς ΓΕΡΗΕΤ 06/2014). Το σύστημα αυτό μεταφέρθηκε στην ΑΨΑ μετά την ίδρυση της στα πλαίσια της ανάληψης όλων των προηγούμενων αρμοδιοτήτων του ΓΕΡΗΕΤ στον τομέα της ασφάλειας δικτύων και πληροφοριών και της κυβερνοασφάλειας.

Κατά το 2019, στο αναβαθμισμένο σύστημα RCMS προστέθηκαν λειτουργίες που αφορούν την ηλεκτρονική διαχείριση εμπλεκομένων (Customer Relationship Management Module) και αναπτύχθηκε ηλεκτρονική πλατφόρμα για την υποβολή περιστατικών κυβερνοασφάλειας στην ΑΨΑ. Επίσης, ξεκίνησε η δεύτερη φάση ανάπτυξης της πλατφόρμας μέσω του συγχρηματοδοτούμενου έργου CEF iDSAMPL (βλ. ενότητα 8.1.4), με την οποία το σύστημα θα εξελιχτεί σε ολοκληρωμένη πλατφόρμα διαχείρισης των κινδύνων των εποπτευόμενων οργανισμών στην ΑΨΑ, με λειτουργίες διαχείρισης κινδύνων, όπως risk management, incident and loss management και compliance management. Η ΑΨΑ πέτυχε σημαντική χρηματοδότηση (ύψους €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. Με τις κατάλληλες αλλαγές και αναβαθμίσεις, η πλατφόρμα iDSAMPL θα καλύψει μεγάλο μέρος των αναγκών της ΑΨΑ που εντοπίζονται στα πλαίσια των αρμοδιοτήτων της. Το έργο αυτό αναμένεται να ολοκληρωθεί στις αρχές του 2021.

4. ΥΛΟΠΟΙΗΣΗ ΣΤΡΑΤΗΓΙΚΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

4.1. Υλοποίηση Δράσεων Στρατηγικής Κυβερνοασφάλειας

Εντός του 2019, διάφορες δραστηριότητες που έγιναν από την ΑΨΑ υλοποιούν μεγάλο μέρος 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 Κρίσιμων Υποδομών Πληροφοριών (βλ. ενότητα 3.1.4),
Δράση 9	Εθνικό Πλαίσιο Κυβερνοασφάλειας (βλ. ενότητα 4.2)
Δράση 11	Εθνικό CSIRT (βλ. ενότητα 1.3.2, ενότητα 3.4.1),
Δράση 12	Εθνικές και Διεθνείς Ασκήσεις (βλ. ενότητα 4.3)
Δράση 13	Εκπαίδευση και Κατάρτιση (βλ. ενότητα 7.6),
Δράση 14	Δημιουργία Κουλτούρας Κυβερνοασφάλειας - Awareness (βλ. ενότητα 4.4)
Δράση 15	Διεθνής Συνεργασία (βλ. ενότητα 7)

4.2. Εθνικό Πλαίσιο Κυβερνοασφάλειας

Εντός του 2019, συνεχίστηκε η υλοποίηση του πρώτου σημαντικού παραδοτέου της Ομάδας Εργασίας για τη Δράση 9 της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, η οποία έχει 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.

Εντός του 2020, αναμένεται η έναρξη του Εθνικού Πλαισίου Κυβερνοασφάλειας που έχει ετοιμάσει η ΑΨΑ τόσο στους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και τους Φορείς Κρίσιμων Υποδομών Πληροφοριών όσο και στο δημόσιο ευρύτερα. Ειδικότερα για την υλοποίηση του πλαισίου στο δημόσιο, η ΑΨΑ συνεργάστηκε με άλλες αρμόδιες κρατικές υπηρεσίες για τη δημιουργία του θεσμού του Chief Information Security Officer (CISO) για εφαρμογή του πλαισίου στις υποδομές του δημοσίου.

4.3. Ασκήσεις Κυβερνοασφάλειας

Τον Ιούνιο του 2019, η ΑΨΑ συμμετείχε στην ελληνική Διακλαδική Άσκηση Κυβερνοάμυνας "ΠΑΝΟΠΤΗΣ 2019", υπό το συντονισμό του ΓΕΕΘΑ. Η άσκηση διεξήχθη σε πανελλαδικό επίπεδο και σε αυτή συμμετείχαν προσωπικό από τις ελληνικές Ένοπλες Δυνάμεις και τα Σώματα Ασφαλείας, φορείς του δημόσιου και ιδιωτικού τομέα, καθώς και της ακαδημαϊκής κοινότητας. Περισσότεροι από 200 συμμετέχοντες έλαβαν μέρος στην άσκηση για τον εντοπισμό και την 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 τεκμηρίων σε διαφορετικά λειτουργικά συστήματα Η/Υ, drones και δρομολογητές, έλεγχο ευπαθειών εφαρμογών διαδικτύου και ιστού και εντοπισμό/ανάλυση παραβίασης δικτυακής υποδομής, καθώς και σενάρια με επιθέσεις σε συστήματα βιομηχανικού ελέγχου SCADA/ICS.

Κατά τη διάρκεια του 2019, η ΑΨΑ συμμετείχε ενεργά στην προετοιμασία της πανευρωπαϊκής άσκησης "CYBER EUROPE 2020", υπό το συντονισμό του οργανισμού ENISA και τη συμμετοχή όλων των κρατών-μελών της Ευρωπαϊκής Ένωσης. Η άσκηση διεξάγεται κάθε δύο χρόνια, και το 2020 θα έχει ως πρωταγωνιστή στο σενάριο τον τομέα Υγείας.

Η ΑΨΑ συμμετείχε επίσης, κατά το 2019, στις ακόλουθες ασκήσεις σε εθνικό και ευρωπαϊκό επίπεδο:

- Άσκηση CyberSOPEx για έλεγχο των διαδικασιών συνεργασίας του CSIRTs Network
- Άσκηση EU ELEx 2019 για ετοιμότητα και συνεργασία μεταξύ κρατών-μελών της ΕΕ, με έμφαση στις Ευρωεκλογές
- Άσκηση ΑΓΗΣΙΜΑΧΟΣ 2019 για διαχείριση κρίσεων στην Κυπριακή Δημοκρατία

4.4. Δημιουργία Κουλτούρας Κυβερνοασφάλειας - Awareness

Το 2019 συνεχίστηκαν διάφορες δράσεις για την υλοποίηση της νέας Εθνικής Στρατηγικής για ένα Καλύτερο Διαδίκτυο για τα Παιδιά στην Κύπρο, η οποία είχε εγκριθεί από το Υπουργικό Συμβούλιο το Δεκέμβριο του 2017. Προς αυτό το σκοπό, συστάθηκε και συνεδρίασε για πρώτη φορά η διυπουργική επιτροπή, που έχει ορισθεί για την εποπτεία εφαρμογής της Στρατηγικής και την ίδρυση και λειτουργία εθνικού κέντρου ενημέρωσης, εκπαίδευσης και έρευνας. Το κέντρο αναμένεται να συμβάλει τα μέγιστα στην επίτευξη των στόχων της πολιτικής του κράτους στον τομέα της κυβερνοασφάλειας.

Επίσης, συνεχίστηκαν οι εργασίες της ομάδας για την προώθηση των σχετικών προγραμμάτων ασφάλειας στο διαδίκτυο (security και safety) για παιδιά/μαθητές, εκπαιδευτικούς και γονείς, που λειτουργεί υπό το συντονισμό του Παιδαγωγικού Ινστιτούτου, εκ μέρους του Υπουργείου Παιδείας και Πολιτισμού, και το γενικό συντονισμό της ΑΨΑ.

Εντός του 2019, ξεκίνησαν οι εργασίες της Δράσης του ευρωπαϊκού προγράμματος CEF με τίτλο CYber-Safety II (αριθμός Δράσης 2018-CY-IA-0012). Το ευρωπαϊκό πρόγραμμα συνέχισε και εντός του 2019 τις εργασίες του πρώτου προγράμματος CYberSafety με την ίδια σύνθεση και αναθεωρημένο πρόγραμμα δραστηριοτήτων.

Οι εργασίες ενημέρωσης και εκπαίδευσης όλων των ομάδων - στόχων αποτελούν σημαντικό στοιχείο στην προώθηση της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας καθώς θα συμβάλουν στην καλύτερη υλοποίηση των υπολοίπων δράσεων της Στρατηγικής και θα βοηθήσουν όλους τους πολίτες να αντιμετωπίσουν κινδύνους, να αποκτήσουν εμπιστοσύνη και να επωφεληθούν των ευκαιριών που φέρνουν μαζί τους οι νέες ψηφιακές τεχνολογίες.

4.5. Αναθεώρηση της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας

Κατά το 2019, η ΑΨΑ ολοκλήρωσε τη διαδικασία αναθεώρησης της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, αξιοποιώντας δεδομένα από διάφορες πηγές, όπως:

- τα αποτελέσματα της αξιολόγησης με τίτλο "Cybersecurity Capacity Assessment"[4] από το Πανεπιστήμιο της Οξφόρδης
- τους Οδηγούς Καλών Πρακτικών, μεταξύ άλλων, από τον ENISA, την ITU (International Telecommunication Union) και τον οργανισμό Meridian
- το "Πακέτο Κυβερνοασφάλειας" της ΕΕ[5] ("EU Cybersecurity Package")
- τα διδάγματα από την εφαρμογή της υφιστάμενης Στρατηγικής

Η Στρατηγική έχει προωθηθεί στα αρμόδια Υπουργεία για οριστικοποίηση και έγκριση από το Υπουργικό Συμβούλιο εντός του 2020.

[4] 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

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

5. ΔΙΑΧΕΙΡΙΣΗ ΣΥΜΒΑΝΤΩΝ ΚΑΙ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

5.1. Διαχείριση Περιστατικών

Η διαχείριση περιστατικών κυβερνοασφάλειας και ο μετριασμός του κάθε προβλήματος που δημιουργείται αποτελούν τον κύριο στόχο του Εθνικού CSIRT-CY. Λαμβάνοντας υπόψη την κρισιμότητα του κάθε οργανισμού, των υπηρεσιών που επηρεάζονται καθώς και την κρισιμότητα του κάθε περιστατικού, το Εθνικό CSIRT-CY είναι σε θέση να προβεί στις ανάλογες ενέργειες για τη μετρίαση και επίλυση του κάθε περιστατικού. Τα περιστατικά είναι χωρισμένα σε 3 κατηγορίες, αναλόγως της κρισιμότητας και επικινδυνότητας τους, και υπάρχει για κάθε κατηγορία διαφορετικός χρόνος απόκρισης. Ο οργανισμός εξυπηρετεί τις κρίσιμες υποδομές πληροφοριών της Κυπριακής Δημοκρατίας, τις τράπεζες, τους παρόχους υπηρεσιών διαδικτύου και τους παρόχους ηλεκτρονικών υπηρεσιών όλο το 24ωρο.

Κατά το 2019, το Εθνικό CSIRT-CY χειρίστηκε περιστατικά που αφορούσαν:

- διαρροή ευαίσθητων πληροφοριών, όπου κλήθηκε να αναλάβει και να συντονίσει την αντιμετώπιση του περιστατικού. Αρχικά, έγινε έλεγχος τρωτών σημείων εσωτερικού δικτύου σε υπολογιστές και διακομιστές της κρίσιμης υποδομής. Μέσα από τον έλεγχο και την ανάλυση εντοπίστηκαν μολυσμένα αρχεία σε υπολογιστές και διακομιστές. Αυτό είχε σαν αποτέλεσμα τη δημιουργία αναφοράς για την επίλυση και παραμετροποίηση τους καθώς και προτάσεις για θωράκιση του δικτύου τους
- επίθεση σε συστήματα και αλλαγή των Domain Name Server (DNS) Records σε κρίσιμη υποδομή παραπέμποντας τους χρήστες των οργανισμών σε υπηρεσίες που χειρίζονταν κακόβουλα άτομα με σκοπό να υποκλαπούν διαπιστευτήρια του ηλεκτρονικού ταχυδρομείου τους. Το Εθνικό CSIRT-CY ανταποκρίθηκε και εντόπισε την επίθεση, δηλαδή τον τρόπο συμπεριφοράς και τη δράση του επιτιθέμενου. Δόθηκαν οδηγίες και προτεινόμενα μέτρα αντιμετώπισης για αποφυγή τέτοιων επιθέσεων. Ακολούθως, ενημερώθηκαν οι Αρμόδιες Αρχές
- ανάλυση κακόβουλων ηλεκτρονικών μηνυμάτων (Phishing Emails) με εξειδικευμένα εργαλεία και λογισμικά. Το Εθνικό CSIRT-CY απέστειλε ειδοποιήσεις και ενημερώσεις προς όλες τις κρίσιμες υποδομές για αποφυγή τέτοιων κίνδυνων και απειλών
- ανταπόκριση και δικανική ανάλυση κακόβουλου λογισμικού Ransomware που είχε ως αποτέλεσμα την κρυπτογράφηση πληροφοριών και δεδομένων συγκεκριμένης κρίσιμης υποδομής. Μετά τον επιτυχημένο χειρισμό της συγκεκριμένης υπόθεσης, ετοιμάστηκε και προωθήθηκε πρόταση για θωράκιση του δικτύου όλων των κρίσιμων υποδομών της Κυπριακής Δημοκρατίας

Κατά το έτος 2019, ο οργανισμός έλαβε περίπου 10.521 ηλεκτρονικά μηνύματα από τις πλατφόρμες πληροφόρησης Shadow Server, CERT Bund, MISP, Abuse Helper και Team Cymru. Μετά από επεξεργασία των στοιχείων που λαμβάνονται και σχετικές ενέργειες για το μετριασμό τους, το Εθνικό CSIRT-CY διαβίβασε περίπου 3.500 ηλεκτρονικά μηνύματα προς τις κρίσιμες υποδομές πληροφοριών που περιείχαν 24.068 ύποπτες IP διευθύνσεις που τους αφορούσαν με εισηγήσεις για σχετικές ενέργειες.

5.2. Διαχείριση Κρίσεων

5.2.1. ΒΕΣ "ΖΗΝΩΝ": ΕΕΣ "ΑΡΙΣΤΕΑΣ"

Το Ειδικό Εθνικό Σχέδιο (ΕΕΣ) "ΑΡΙΣΤΕΑΣ" αφορά τη διαχείριση κρίσεως που έχει προκληθεί από "Καταστροφή ή/και μεγάλης διάρκειας διακοπή δικτύων επικοινωνίας και ενημέρωσης" στην Κύπρο. Το σχέδιο αυτό πηγάζει από το Βασικό Εθνικό Σχέδιο (ΒΕΣ) "ΖΗΝΩΝ", το οποίο εγκρίθηκε από το Υπουργικό Συμβούλιο τον Ιανουάριο του 2013 και αποτελεί το βασικό σχέδιο διαχείρισης κρίσεων της Κυπριακής Δημοκρατίας σε ειρηνική περίοδο. Περιγράφει και επεξηγεί τις ενέργειες και τους ρόλους όλων των εμπλεκόμενων μερών έτσι ώστε με συντονισμένες και αποτελεσματικές διαδικασίες να είναι δυνατή η αντιμετώπιση κρίσης που δυνατόν να εκδηλωθεί ως αποτέλεσμα προβλήματος στην παροχή υπηρεσιών και δικτύων Ηλεκτρονικών Επικοινωνιών (ΗΕ) και Επίγειας Ψηφιακής Τηλεόρασης (ΕΨΤ).

5.2.2. Συμμετοχή σε άλλα ΕΕΣ του ΒΕΣ "ΖΗΝΩΝ"

Η ΑΨΑ συμμετέχει επίσης στα σχέδια ΕΕΣ "ΕΓΚΕΛΑΔΟΣ", "ΠΟΛΥΒΙΟΣ"και "ΠΡΟΜΗΘΕΑΣ".

5.2.3. Ετοιμασία εξειδικευμένου σχεδίου διαχείρισης Κρίσεων για την Κυβερνοασφάλεια κάτω από το ΒΕΣ "ΖΗΝΩΝ"

Η ΑΨΑ, σε συνεργασία με άλλες αρμόδιες Αρχές της Δημοκρατίας, εντός του 2019 εξασφάλισε έγκριση και ξεκίνησε τη δημιουργία εξειδικευμένου σχεδίου διαχείρισης Κρίσεων για την Κυβερνοασφάλεια κάτω από το ΒΕΣ "ΖΗΝΩΝ". Το σχέδιο αναμένεται να προχωρήσει και να ολοκληρωθεί εντός του 2020.

6. ΠΙΣΤΟΠΟΙΗΣΕΙΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

6.1. Ο Κανονισμός της ΕΕ για την Κυβερνοασφάλεια

Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο υιοθέτησαν και δημοσίευσαν το νόμο της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881) τον Ιούνιο του 2019. Ο Κανονισμός ενισχύει τον οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο (ENISA) και θεσπίζει ένα πανευρωπαϊκό πλαίσιο πιστοποίησης για την ασφάλεια στον κυβερνοχώρο για προϊόντα, υπηρεσίες και διαδικασίες τεχνολογιών πληροφορικών και επικοινωνίας (ΤΠΕ). Οι εταιρείες που δραστηριοποιούνται στην ΕΕ θα επωφεληθούν (προαιρετικά) από την πιστοποίηση των προϊόντων, των διαδικασιών και των 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 θα προωθήσει ευρωπαϊκά σχήματα πιστοποίησης ως ολοκληρωμένο σύνολο κανόνων, τεχνικών απαιτήσεων, προτύπων και διαδικασιών. Τα σχήματα αυτά θα περιλαμβάνουν, μεταξύ άλλων: (α) τις κατηγορίες προϊόντων και υπηρεσιών που καλύπτονται, (β) τις απαιτήσεις κυβερνοασφάλειας, π.χ. με αναφορά σε πρότυπα ή τεχνικές προδιαγραφές, (γ) τον τύπο αξιολόγησης (π.χ. αυτοαξιολόγηση ή αξιολόγηση τρίτων), και (δ) το επιδιωκόμενο επίπεδο διασφάλισης (π.χ. βασικό, ουσιαστικό ή/και υψηλό). Τα τρία επίπεδα διασφάλισης θα είναι ανάλογα με το επίπεδο του κινδύνου που συνδέεται με την προβλεπόμενη χρήση του προϊόντος, της υπηρεσίας ή της διαδικασίας ΤΠΕ, καθώς και με το απαιτούμενο βάθος δοκιμών για σκοπούς αξιολόγησης της συμμόρφωσης. Για παράδειγμα, ένα υψηλό επίπεδο διασφάλισης σημαίνει ότι το προϊόν που πιστοποιήθηκε έχει περάσει τις υψηλότερες δοκιμές ασφαλείας.

Τα πιστοποιητικά που προκύπτουν θα αναγνωρίζονται σε όλα τα κράτη-μέλη της ΕΕ, διευκολύνοντας τις διασυνοριακές συναλλαγές των επιχειρήσεων και τους αγοραστές να κατανοούν 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 Common Criteria[6] (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 την 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 για τα οποία θα εκδίδουν πιστοποιητικά. Οι ελάχιστες

[6] Τα 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 διασφαλίσου 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.

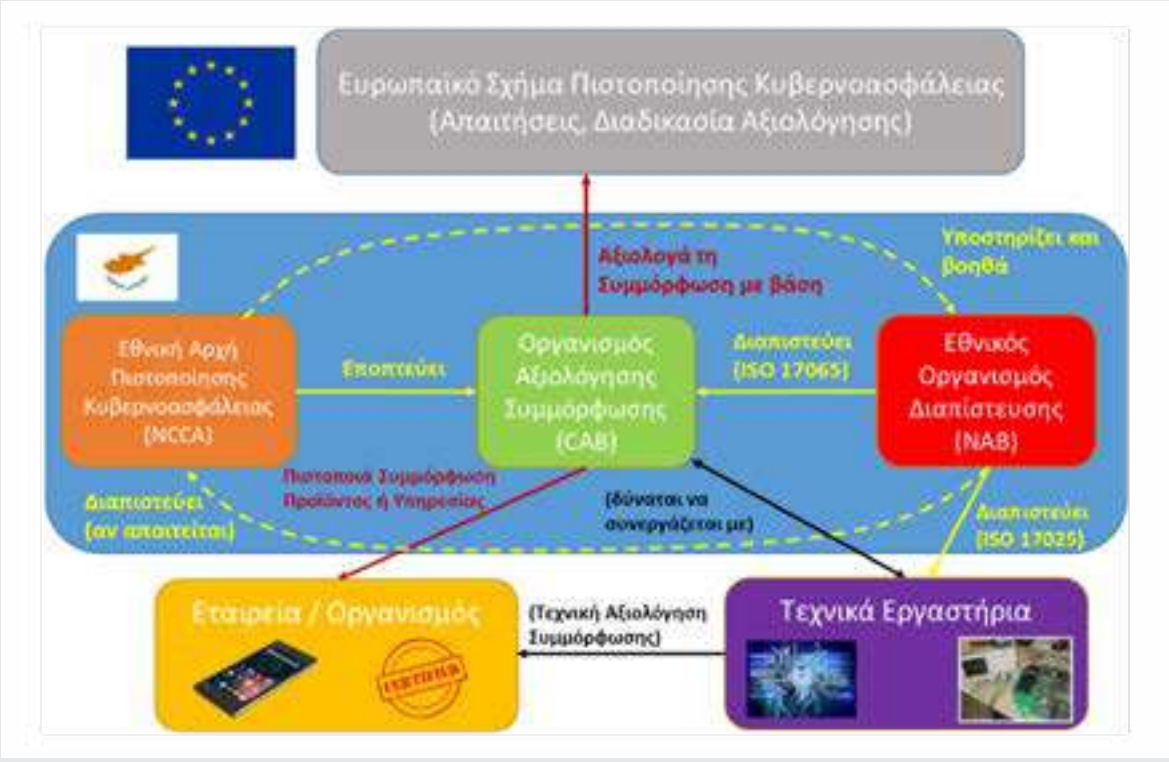
εξουσίες και αρμοδιότητες της ΕΑΠΚ, καθώς και λεπτομέρειες για το γενικό πλαίσιο πιστοποίησης κυβερνοασφάλειας σε επίπεδο ΕΕ και σε εθνικό επίπεδο καθορίζονται στον Κανονισμό.

6.3. Η Προσέγγιση της Κύπρου

Το Υπουργικό Συμβούλιο έχει ορίσει την ΑΨΑ ως την αρμόδια εθνική αρχή πιστοποίησης κυβερνοασφαλειας. Στο πλαίσιο της απόφασης αυτής, η ΑΨΑ έχει 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, έως τον Ιούνιο του 2021, 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.

Εντός του 2019, η ΑΨΑ έχει ξεκινήσει ένα εσωτερικό έργο για την εκπλήρωση των χρονοδιαγραμμάτων που ορίζονται στον Κανονισμό, και διεκδικεί χρηματοδότηση από την ΕΕ (βλ. ενότητα 8.2.1) για τη δημιουργία των δυνατοτήτων πιστοποίησης της κυβερνοασφάλειας σύμφωνα με τον Κανονισμό. Συνεργάζεται στενά με την Κυπριακή Εταιρεία Πιστοποίησης (ΚΕΠ) για να φέρει σε πέρας τους στόχους που αναφέρθηκαν παραπάνω. Η ΚΕΠ είναι θυγατρική του Εθνικού Φορέα Προτύπων της Κύπρου, του Κυπριακού Οργανισμού Τυποποίησης (CYS).

Γράφημα 3: Πλαίσιο Πιστοποίησης Κυβερνοασφάλειας



Η ρύθμιση που θα αναπτυχθεί στην Κύπρο θα ακολουθήσει τις πρόνοιες του Κανονισμού, όπως φαίνεται στο ανωτέρω γράφημα. Στον πυρήνα των δραστηριοτήτων πιστοποίησης βρίσκεται ο οργανισμός

αξιολόγησης της συμμόρφωσης (ένας ή περισσότεροι σε κάθε κράτος μέλος), ο οποίος θα αξιολογεί τη συμμόρφωση των προϊόντων, υπηρεσιών και διαδικασιών ΤΠΕ με βάση τα διάφορα Σχήματα Πιστοποίησης Κυβερνοασφάλειας της ΕΕ που θα δημοσιευτούν. Σύμφωνα με τις σχετικές πρόνοιες του Κανονισμού, οι ΟΑΣ μπορούν είτε να αναπτύξουν δικά τους εργαστήρια τεχνικών δοκιμών, είτε να βασίζονται σε διαπιστευμένα εργαστήρια τρίτων για το τμήμα τεχνικής αξιολόγησης της διαδικασίας πιστοποίησης. Τέτοια εργαστήρια πρέπει να είναι διαπιστευμένα από τον ΚΟΠΠ, προκειμένου να διασφαλίζεται ότι πληρούν τις σχετικές απαιτήσεις που ορίζονται στον Κανονισμό. Επιπλέον, οι ΟΑΣ πρέπει επίσης να εξουσιοδοτούνται από την ΑΨΑ, όταν τα σχήματα πιστοποίησης περιλαμβάνουν ειδικές πρόσθετες απαιτήσεις που πρέπει να πληρούνται. Ο ρόλος της ΑΨΑ είναι καίριος, καθώς θα έχει τις νομικές εξουσίες και αρμοδιότητες να εποπτεύει αποτελεσματικά ολόκληρο το πλαίσιο πιστοποίησης εντός της χώρας και να παρακολουθεί την εφαρμογή του, και θα υποστηρίζει ενεργά και θα συνδράμει στο έργο του ΚΟΠΠ όπου είναι απαραίτητο.

7. ΕΘΝΙΚΕΣ & ΔΙΕΘΝΕΙΣ ΣΧΕΣΕΙΣ

Η συνεργασία και η ανάπτυξη εμπιστοσύνης με άλλες αρχές και με το σύνολο των εμπλεκόμενων φορέων αποτελεί βασικό πυλώνα και προτεραιότητα της Αρχής για τη σωστή και αποδοτική άσκηση των αρμοδιοτήτων και τη διεκπεραίωση των εργασιών της ΑΨΑ, τόσο σε εθνικό όσο και σε ευρωπαϊκό και διεθνές επίπεδο. Τα θέματα ασφάλειας στον κυβερνοχώρο δεν μπορούν να αντιμετωπιστούν μεμονωμένα, άρα 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 7.5): 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

Η ΑΨΑ, στα πλαίσια της ενημέρωσης, εκπαίδευσης και δημιουργίας κλίματος εμπιστοσύνης μεταξύ οργανισμών, έχει διοργανώσει εκπαιδεύσεις προς τους Φορείς Κρίσιμων Υποδομών Πληροφοριών. Συγκεκριμένα, έχουν γίνει 23 παρουσιάσεις σε εκπροσώπους Φορέων Κρίσιμων Υποδομών Πληροφοριών αναφορικά με τη διαδικτυακή απάτη ηλεκτρονικού “ψαρέματος"(phishing) από την ομάδα του Εθνικού CSIRT.

Επιπρόσθετα, κατά την περίοδο των Ευρωεκλογών, πραγματοποιήθηκε συνάντηση με εκπροσώπους Κοινοβουλευτικών Κομμάτων, όπου τα μέλη του Εθνικού CSIRT-CY παρουσίασαν τις πιο κάτω διαλέξεις στα πλαίσια ενημέρωσης για τους κινδύνους που διατρέχουν κατά την περίοδο των εκλογών:

- Access Control (Έλεγχος Πρόσβασης)
- Phishing (Ηλεκτρονικό “ψάρεμα”)
- DDoS attack/ Website Defacement

Επίσης, έχουν πραγματοποιηθεί δυο (2) ασκήσεις κυβερνοασφάλειας. Η μία άσκηση αφορούσε την επικοινωνία και τον συντονισμό των εμπλεκόμενων φορέων, και η δεύτερη άσκηση αφορούσε εικονικά περιστατικά κυβερνοασφάλειας. Επιπλέον, λήφθηκαν οργανωτικά και τεχνικά μέτρα για την ομαλή διεξαγωγή των εκλογών και εντοπισμό κακόβουλων λογισμικών.

7.2. Συνεργασία με Κρατικές Αρχές

Στα πλαίσια των δραστηριοτήτων της, η ΑΨΑ συνεργάζεται στενά με άλλες κρατικές αρχές, αναλόγως αναγκών και πάντα με σκοπό την αλληλοβοήθεια και την επίτευξη κοινών στόχων σχετικά με την κυβερνοασφάλεια του κράτους. Αναφέρονται πιο κάτω ενδεικτικά παραδείγματα:

- Το Εθνικό CSIRT-CY, στο πλαίσιο συνεργασίας με το Υπουργείο Άμυνας, προχώρησε στην αγορά υπηρεσιών για την Προμήθεια Εξοπλισμού για το Κέντρο Έκτακτης Ανάγκης (DR – Disaster Recovery) της Αρχής. Υπολογίζεται ότι εντός του 2020 το Κέντρο Έκτακτης Ανάγκης θα είναι σε λειτουργία για την πρόληψη και αντιμετώπιση κρίσιμων περιστατικών κυβερνοασφάλειας
- Η ΑΨΑ ανέπτυξε σημαντική συνεργασία με το Υπουργείο Άμυνας για την ανάπτυξη υποδομών Κυβερνοασφάλειας για την Κυπριακή Δημοκρατία
- Η ΑΨΑ συνεργάζεται σε συνεχόμενη βάση με το Υπουργείο Εξωτερικών σε έργα κοινού ενδιαφέροντος
- Η ΑΨΑ, σε συνεργασία με τη Δύναμη Πολιτικής Άμυνας, συμμετείχε σε peer review της Ευρωπαϊκής Ένωσης για θέματα πολιτικής προστασίας και διαχείρισης κινδύνων και κρίσεων στην Κυπριακή Δημοκρατία, με πολύ θετικές αναφορές στην σχετική έκθεση που ετοίμασαν οι εμπειρογνώμονες της ΕΕ

7.3. Διμερείς Συνεργασίες με Κράτη-Μέλη της Ευρωπαϊκής Ένωσης

Η ΑΨΑ έχει υπογράψει συμφωνίες με κράτη-μέλη, όπως η Ρουμανία και η Ελλάδα, ενώ έχει συνεργαστεί με κράτη-μέλη, όπως η Πολωνία και η Πορτογαλία, για τη διενέργεια εκπαιδεύσεων και την ανταλλαγή γνώσεων.

7.4. Συνεργασία με Τρίτες Χώρες

7.4.1. Εφαρμογή Μνημονίου Συναντίληψης με Israeli National Cyber Directorate

Μετά την υπογραφή του Μνημονίου Συναντίληψης μεταξύ της ΑΨΑ (Εθνικού CSIRT-CY) και του Israeli National Cyber Directorate [INCD], το 2019 πραγματοποιήθηκαν επαφές για οργάνωση της συνεργασίας με τις αρμόδιες υπηρεσίες οι οποίες θα συνεχιστούν και κατά το έτος 2020.

7.4.2. Πρόταση Συνεργασίας με Σουλτανάτο του Ομάν

Κατά το 2019, μετά από σχετικές επαφές που είχαν γίνει με αξιωματούχους του Σουλτανάτου του Ομάν μέσω του Υπουργείου Εξωτερικών, άρχισαν διεργασίες για τη συμφωνία του περιεχομένου του Μνημονίου Συναντίληψης στους τομείς της εκπαίδευσης και ανταλλαγής τεχνογνωσίας στους διάφορους τομείς που αφορούν την κυβερνοασφάλεια. Το Μνημόνιο Συναντίληψης αναμένεται να υπογραφεί εντός του 2020.

7.4.3. Άλλες συνεργασίες με τρίτες χώρες

Εντός του 2020, η ΑΨΑ (Εθνικό CSIRT-CY) θα υπογράψει Μνημόνιο Συναντίληψης με Αλβανία και Σκόπια στους τομείς της εκπαίδευσης και ανταλλαγής τεχνογνωσίας σε ότι αφορά την κυβερνοασφάλεια.

7.5. Διεθνής Εκπροσώπηση

Η εκπροσώπηση της ΑΨΑ σε επιτροπές σε εθνικό και διεθνές επίπεδο κατά το 2019 αναλήφθηκε από τον Επίτροπο, τον Βοηθό Επίτροπο, το 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 Αρχής:

ENISA (European Union Agency for Network and Information Security) o MB (Management Board) o NLO (National Liaison Officers) o Cyber Crisis Cooperation and Exercises
Article 13a Expert Group 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 1 – Identification of Operators of Essential Services 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 9 – Cybersecurity Capacity Building o Work Stream 10 – Digital Infrastructures
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)
Cyber Security Coordination
CSP (Cyber Security Professionals) **Governance Board**
CSIRT Community Groups (FIRST, TI)
CSIRT Network
CERT-EU
ITU (International Telecommunication Union)

Επίσης, η ΑΨΑ εκπροσωπεί την Κυπριακή Δημοκρατία στα ακόλουθα διεθνή σώματα:

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 στο **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 2019, έγιναν πέντε (5) συναντήσεις του NIS Cooperation Group, όπου συζητήθηκαν οι λεπτομέρειες υλοποίησης της Οδηγίας NIS σε στρατηγικό επίπεδο και έγινε συντονισμός ως προς την ενιαία προσέγγιση για την υλοποίηση της.

Επίσης, ειδική αναφορά γίνεται στο **CSIRTs Network**, του οποίου το Εθνικό CSIRT είναι ενεργό μέλος. Το CSIRTs Network είναι μια πλατφόρμα που ιδρύθηκε βάσει της Οδηγίας NIS, η οποία επιτρέπει την ανταλλαγή πληροφοριών, την ανταλλαγή γνώσεων και της άμεσης βοήθειας 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.

7.6. Εκπαιδεύσεις/Συνέδρια

7.6.1. Εκπαιδεύσεις

Κατά τη διάρκεια του 2019, πραγματοποιήθηκαν οι πιο κάτω εκπαιδεύσεις στο προσωπικό του Εθνικού CSIRT-CY:

- **Cybersecurity Organizational and Defensive Capabilities**
  Υπό την αιγίδα του Ευρωπαϊκού Κολλεγίου Ασφάλειας και Άμυνας (European Security and Defence Collage - ESDC), η ΑΨΑ και το Εθνικό CSIRT-CY διοργάνωσε την εν λόγω εκπαίδευση μεταξύ 13 και 15 Μαΐου 2019 στη Λευκωσία. Η εκπαίδευση αφορούσε τις προκλήσεις στον κυβερνοχώρο στους τομείς της πληροφόρησης, της διαχείρισης κινδύνων και του χειρισμού περιστατικών. Στην εκπαίδευση συμμετείχε το προσωπικό του Εθνικού CSIRT-CY και εκπρόσωποι από αντιπροσωπίες του εξωτερικού (Ελλάδα, Ολλανδία και Ιταλία), το Στρατιωτικό CSIRT καθώς και κρίσιμες υποδομές της Κυπριακής Δημοκρατίας. Οι εκπαιδευτές ήταν από την Σχολή Ευελπίδων Ελλάδας, τον ευρωπαϊκό οργανισμό ENISA, το Ανοικτό Πανεπιστήμιο Κύπρου, την NRD Cyber Security, το Joint Research Center και το OSINT Search.

- **Advanced Malware Analysis**
  Η εκπαίδευση πραγματοποιήθηκε από τις 10 έως τις 12 Ιουλίου 2019 από την Deloitte Βελγίου στα γραφεία της Deloitte στη Λευκωσία, και συμπεριλάμβανε τρεις ενότητες: το Business Continuity Plan, τη νέα νομοθεσία για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα, GDPR, καθώς και τεχνική εκπαίδευση για ανάλυση malware (κακόβουλου λογισμικού).

- **DarkWeb Investigations**
  Η εκπαίδευση πραγματοποιήθηκε στις 29 και 30 Ιουλίου 2019 στη Λευκωσία από μέλη της Ομάδας Έρευνας Εσωτερικής Ασφάλειας Αμερικής (U.S. Homeland Security Investigations (HSI)) και αφορούσε την Ασφάλεια στον κυβερνοχώρο. Πιο συγκεκριμένα, έγινε αναφορά στις προκλήσεις που μπορεί να επιφέρει το DarkWeb στον τομέα ασφάλειας της πληροφόρησης και

της διαχείρισης κινδύνων, όπως παράνομη αγοραπωλησία μέσω σκοτεινού δικτύου (Darknet markets (DNMs)).

- **Mobile and Memory Forensics Training**
  Η εκπαίδευση πραγματοποιήθηκε από 1 μέχρι 2 Αυγούστου 2019 στη Λευκωσία από τον ευρωπαϊκό οργανισμό ENISA (European Union Agency for Network and Security) και αφορούσε την κινητή τεχνολογία (Mobile technology) και τις απειλές ασφάλειας που μπορούν να επηρεάσουν τα λειτουργικά συστήματα στις έξυπνες συσκευές κινητών τηλεφώνων.

7.6.2. Συνέδριο Trusted Introducer - TF58

Η 58η Συνάντηση TF-CSIRT διεξήχθη με επιτυχία από τις 16 έως τις 17 Σεπτεμβρίου 2019 στο ξενοδοχείου Annabelle στην Πάφο υπό την αιγίδα της ΑΨΑ και του Εθνικού CSIRT-CY. Στόχος ήταν η διασυνοριακή συνεργασία, η ανταλλαγή πληροφοριών και η ενδυνάμωση σχέσεων εμπιστοσύνης μεταξύ όλων των εκπροσώπων αντίστοιχων εθνικών ομάδων. Η σχέση εμπιστοσύνης είναι από τους κρίσιμους παράγοντες επιτυχίας στην προώθηση της κοινοτικής γνώσης, εστιάζοντας στη δημιουργία και ανάπτυξη νέων Εθνικών Ομάδων Αντιμετώπισης Ηλεκτρονικών Επιθέσεων ενδυναμώνοντας έτσι τη συνεργασία μεταξύ των μελών του δικτύου CSIRT.

Στο συνέδριο συμμετείχαν εκπρόσωποι από το European Security and Defence College (ESDC), τον ευρωπαϊκό οργανισμό ENISA, τους οργανισμούς FIRST και Trusted Introducer, το Ακαδημαϊκό CSIRT της Κύπρου, καθώς και δεκάδες εκπροσώπους Εθνικών Ομάδων CSIRT από το εξωτερικό. Επίσης, παρευρέθηκαν εκπρόσωποι των κρίσιμων υποδομών πληροφοριών της Κυπριακής Δημοκρατίας καθώς και ιδιωτικές κυπριακές εταιρείες που δραστηριοποιούνται στον τομέα της Κυβερνοασφάλειας.

8. ΑΛΛΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

8.1. Συμμετοχή σε Ευρωπαϊκά Συγχρηματοδοτούμενα Προγράμματα

8.1.1. CEF CSIRT-CY

Στις 20 Σεπτεμβρίου 2019 ολοκληρώθηκε με επιτυχία η Δράση “Development and Enhancement of the Capabilities of the Cyprus National CSIRT"(CEF 2016-CY-IA-0129) στο πλαίσιο του προγράμματος Connecting Europe Facility (CEF) - Telecom. Στόχος της Δράσης ήταν η ενίσχυση των υποδομών και περαιτέρω ανάπτυξη των διαδικασιών του Εθνικού CSIRT για την προστασία του κυβερνοχώρου των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών, των παροχέων ηλεκτρονικών επικοινωνιών και των παροχέων ψηφιακών υπηρεσιών της Κυπριακής Δημοκρατίας.

Με την ολοκλήρωση της Δράσης έχουν ενισχυθεί σημαντικά οι δυνατότητες του Εθνικού CSIRT ώστε να παρέχει προληπτικές υπηρεσίες και υπηρεσίες σε περίπτωση συμβάντων ασφάλειας στους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, τους Φορείς Κρίσιμων Υποδομών Πληροφοριών, τους παροχείς ηλεκτρονικών επικοινωνιών και παροχείς ψηφιακών υπηρεσιών στην Κύπρο. Η Δράση έθεσε, επίσης, τα θεμέλια για τη διάνοιξη οδών διασυνοριακής συνεργασίας και ανταλλαγής πληροφοριών με άλλα ευρωπαϊκά CSIRTs, χρησιμοποιώντας ήδη υπάρχουσες ή υπό ανάπτυξη υποδομές, εργαλεία, μηχανισμούς και άλλα βασικά εργαλεία που χρησιμοποιούν οι κοινότητες CSIRT ανά τον κόσμο (π.χ. πλατφόρμα MISP).

Το πρόγραμμα υλοποιήθηκε από στελέχη του οργανισμού και με τη συμβολή πέντε (5) οργανισμών από την Κύπρο και το εξωτερικό. Το έργο είχε συνολική διάρκεια δύο (2) χρόνια και ξεκίνησε τον Οκτώβριο του 2017 με συνολικό προϋπολογισμό €1.283.283.

8.1.2. CEF CYberSafety II

Η ΑΨΑ συνεχίζει τη συμμετοχή της στο ευρωπαϊκό συγχρηματοδοτούμενο πρόγραμμα “CYberSafety II"(2018-CY-IA-0012), του οποίου ηγείται το Παιδαγωγικό Ινστιτούτο Κύπρου που, μαζί με άλλους έξι (6) οργανισμούς στην Κύπρο, έχει στόχο τη 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".

Στόχος του προγράμματος είναι η ενημέρωση και ευαισθητοποίηση των παιδιών στην Κύπρο μέσω εκπαιδεύσεων σε μαθητές Γυμνασίων, Λυκείων και Τεχνικών Σχολών με συγκεκριμένη θεματολογία που αφορά την ασφαλή χρήση του διαδικτύου. Οι Δράσεις της ΑΨΑ περιλαμβάνουν, μεταξύ άλλων, την παροχή σεμιναρίων προς μαθητές και εκπαιδευτικούς Γυμνασίων και Λυκείων της Κύπρου μέσα από τις οποίες μπορούν να εκπαιδευτούν και να αναπτύξουν σχετικές δεξιότητες ασφαλούς χρήσης του διαδικτύου. Η πρωτοτυπία στην προσέγγιση της ΑΨΑ στο πρόγραμμα αυτό αφορά το ότι τα σεμινάρια είναι διαδραστικά, προσφέροντας μια εμπειρία μοναδική και ιδιαίτερα ενδιαφέρουσα στους συμμετέχοντες.

Κατά τη διάρκεια του 2019 πραγματοποιήθηκαν πέντε (5) εκπαιδεύσεις σε Σχολεία Μέσης εκπαίδευσης οι οποίες ολοκληρώθηκαν με επιτυχία και ιδιαίτερα θετικές εντυπώσεις από τους μαθητές και τις διευθύνσεις των σχολείων. Συγκεκριμένα, εκπαιδεύτηκαν και παρακολούθησαν τις εν λόγω εκπαιδεύσεις συνολικά 300 μαθητές και μαθήτριες. Αξιοσημείωτο είναι το γεγονός ότι, μετά το πέρας των εκπαιδεύσεων, αρκετές διευθύνσεις σχολείων υπέβαλαν εκ νέου αιτήσεις για επιπλέον εκπαιδευτικά σεμινάρια σε μελλοντικό χρόνο.

8.1.3. CEF Ακαδημαϊκό CSIRT

Το Σεπτέμβριο του 2019, η ΑΨΑ, στο πλαίσιο συνεργασίας με το Κυπριακό Ερευνητικό και Ακαδημαϊκό Δίκτυο για την υλοποίηση του συγχρηματοδοτούμενου έργου "Establishment of Cypriot Academic CSIRT", συμμετείχε στη διαδικασία πρόσληψης δύο (2) αναλυτών με σκοπό τον άμεσο σχεδιασμό και την υλοποίηση του δικτύου του Ακαδημαϊκού CSIRT.

Η ΑΨΑ βρίσκεται από την πρώτη στιγμή δίπλα στο νεοσύστατο Ακαδημαϊκό CSIRT συμμετέχοντας ως συνεργάτης (Partner) στο ευρωπαϊκό πρόγραμμα για τη σύσταση και αναβάθμιση του, δίνοντας κατευθυντήριες γραμμές και τεχνική υποστήριξη, όπου χρειάζεται.

Για την επίτευξη των στόχων του προγράμματος, την πιο εύκολη επικοινωνία και στενή συνεργασία, αλλά και την εξοικονόμηση δημοσίων κονδυλίων, συμφωνήθηκε όπως το Ακαδημαϊκό CSIRT συστεγαστεί με το Εθνικό CSIRT.

Από τις αρχές Σεπτεμβρίου 2019 οι δύο υπηρεσίες συστεγάζονται και συνεργάζονται στενά με κοινό στόχο την προστασία των κρίσιμων υποδομών που είναι κάτω από την εποπτεία τους και την ολική προστασία του κυβερνοχώρου της Κυπριακής Δημοκρατίας. Με σκοπό τη σύσταση και αναβάθμιση της Ακαδημαϊκής Ομάδας, δόθηκαν κατευθυντήριες γραμμές και τεχνική υποστήριξη από το Εθνικό CSIRT, όπως σχετικές εκπαιδεύσεις για την ετοιμασία των διαδικασιών λειτουργίας, καθώς και την εκπαίδευση του προσωπικού, που αφορούσαν την πιο κάτω θεματολογία:

- Διαχείριση Περιστατικών Ασφάλειας (Incident Handling)
- Λογισμικό Καταγραφής και Διαχείρισης Περιστατικών RTIR (ticketing system)
- Ανάλυση Απειλών (Threat Intelligence)
- Ανεύρεση Απειλών (Threat Hunting)
- Ανάλυση Κακόβουλου Λογισμικού (Malware Analysis)

8.1.4. CEF iDSAMPL

Το έργο πραγματεύεται την αναβάθμιση του υφιστάμενου συστήματος RCMS (Risk and Compliance Management System) της ΑΨΑ, το οποίο απέκτησε το ΓΕΡΗΕΤ (Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων) ως μέρος της υλοποίησης του έργου για την ανάλυση επικινδυνότητας, σε εθνικό επίπεδο, για θέματα κυβερνοασφάλειας (National Level Cyber Risk Assessment – αρ. προσφοράς ΓΕΡΗΕΤ 06/2014). Το σύστημα αυτό μεταφέρθηκε στην ΑΨΑ μετά την ίδρυση της, καθώς έχει αναλάβει όλες τις προηγούμενες αρμοδιότητες του ΓΕΡΗΕΤ στον τομέα της ασφάλειας δικτύων και πληροφοριών και της κυβερνοασφάλειας.

Κατά το 2019, η ΑΨΑ πέτυχε την έγκριση χρηματοδότησης για το εν λόγω έργο, 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.

Η υλοποίηση του έργου ξεκίνησε το Σεπτέμβριο 2019, και περιλαμβάνει την περαιτέρω αναβάθμιση και παραμετροποίηση όλων των modules της υφιστάμενης πλατφόρμας RCMS της ΑΨΑ, για τη δημιουργία ολοκληρωμένου συστήματος διαχείρισης όλων των θεμάτων συμμόρφωσης των εποπτευομένων φορέων της ΑΨΑ. Τα μέρη του συστήματος έχουν ως ακολούθως:

- Διαχείριση Κινδύνων (Risk Management Module)
- Διαχείριση Περιστατικών (Incident Management Module)
- Διαχείριση Συμμόρφωσης (Compliance Management Module)
- Διαχείριση Ελέγχων (Audit Management Module)
- Παρακολούθηση Επακόλουθων Ενεργειών (Actions Monitoring Module)

- Ειδοποιήσεις (Alerts and Notifications Module)
- Δημιουργία Εκθέσεων και Εγγράφων (Reporting and Document Management Module)
- Διαχείριση Πρόσβασης και Δεδομένων (Access and Data Management Module)
- Διαχείριση Σχέσης Πελατών (Customer Relationship Management Module)
- Ροές Εργασιών (Workflows Module)

Το έργο αυτό περιλαμβάνει επιπρόσθετες δραστηριότητες σχετικά με εκπαιδεύσεις προσωπικού της ΑΨΑ σε θέματα της πλατφόρμας και σε θέματα διαχείρισης κινδύνων και επιχειρησιακής συνέχειας, και προγραμματίζεται να ολοκληρωθεί στις αρχές του 2021.

8.2. Νέες Προτάσεις για Ευρωπαϊκή Χρηματοδότηση

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

Η ΑΨΑ ετοίμασε και υπέβαλε πρόταση για ευρωπαϊκή συγχρηματοδότηση €120.000, για την αναβάθμιση των ικανοτήτων της Κυπριακής Δημοκρατίας σχετικά με τη διενέργεια πιστοποιήσεων κυβερνοασφάλειας (βλ. κεφάλαιο 6 της παρούσας Έκθεσης).

Στον Κανονισμό 2019/881 για την κυβερνοασφάλεια, προβλέπονται διάφοροι ρόλοι σχετικά με την πιστοποίηση της ασφάλειας στον κυβερνοχώρο, συμπεριλαμβανομένων εκείνων των εθνικών αρχών πιστοποίησης κυβερνοασφάλειας (National Cybersecurity Certification Authority – NCCA), των οργανισμών αξιολόγησης της συμμόρφωσης (Conformity Assessment Body - CAB) και το εθνικό σώμα διαπίστευσης (National Accreditation Body - NAB). Ειδικότερα, το άρθρο 58 του Κανονισμού εξετάζει τον ορισμό, τα καθήκοντα, τις αρμοδιότητες και τις εξουσίες της NCCA όσον αφορά το ρόλο της ως της αρχής που έχει την κύρια ευθύνη για την πιστοποίηση ασφάλειας στον κυβερνοχώρο σε εθνικό επίπεδο. Το προτεινόμενο αυτό έργο αποσκοπεί στη σημαντική βελτίωση των δυνατοτήτων της ΑΨΑ στην πιστοποίηση, και στην προώθηση της συνεργασίας μεταξύ της ΑΨΑ και άλλων παρόμοιων αρχών σε άλλα κράτη-μέλη της ΕΕ.

Στόχος του έργου είναι:

- να προσδιορίσει τις πρόνοιες του Κανονισμού που πρέπει να μεταφερθούν στο νόμο της ΑΨΑ, προκειμένου να έχει τις κατάλληλες εξουσίες και αρμοδιότητες
- να δημιουργήσει 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 NCCA, NAB, CAB και άλλων σχετικών φορέων.

Η πρόταση για συγχρηματοδότηση έχει 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. Θα διαρκέσει 18 μήνες και αναμένεται να ξεκινήσει εντός του 2020 με συνολικό προϋπολογισμό €160.000 (από τα οποία €40.000 αντιστοιχούν στους προϋπολογισμούς των συμμετεχόντων, και €120.000 στη συγχρηματοδότηση της ΕΕ).