ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

Αρχή Ψηφιακής Ασφάλειας

Έκθεση Δραστηριοτήτων 2021

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 2022

ΠΕΡΙΕΧΟΜΕΝΑ

ΓΡΑΦΗΜΑΤΑ

ΠΙΝΑΚΕΣ

ΧΑΙΡΕΤΙΣΜΟΣ ΕΠΙΤΡΟΠΟΥ ΕΠΙΚΟΙΝΩΝΙΩΝ

Η παρούσα έκθεση απολογισμού του έργου της Αρχής Ψηφιακής Ασφάλειας δεν αποτελεί απλώς μια τυπική διαδικασία, που προνοείται από τη σχετική νομοθεσία, αλλά παραθέτει ενώπιον του Προέδρου της Κυπριακής Δημοκρατίας το σύνολο των δραστηριοτήτων της Αρχής σε όλο το φάσμα των πεδίων αρμοδιότητας της κατά το έτος 2021. Αποτυπώνει την πορεία της επίτευξης των στόχων που είχαν τεθεί, τα λειτουργικά και ουσιαστικά ζητήματα, που κλήθηκε η ΑΨΑ να αντιμετωπίσει και να διαχειριστεί και την πρόοδο που έχει συντελεστεί στην κατεύθυνση της εκπλήρωσης της αποστολής της.

Σε ένα διεθνές περιβάλλον συνεχών προκλήσεων όπως η πανδημία, αλλά και των αυξανόμενων γεωπολιτικών εντάσεων, αποδείχθηκε πως η Κυβερνοασφάλεια βρίσκεται στην κορυφή των προκλήσεων για κάθε τομέα όπως η ασφάλεια, η υγεία, οι τηλεπικοινωνίες, η ναυτιλία, οι μεταφορές και η οικονομία μας. Είναι μια πραγματικότητα που μπήκε στην ζωή μας και επηρεάζει τις καθημερινές δραστηριότητες και ενέργειες του κράτους και των πολιτών του.

Αποστολή της Αρχής Ψηφιακής Ασφάλειας, μέσα από την υλοποίηση της Ευρωπαϊκής Οδηγίας NIS (Network and Information Security Directive), είναι η εδραίωση ενός ασφαλούς ψηφιακού περιβάλλοντος για κάθε πολίτη της Κύπρου και 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. Μέσα από τα πεπραγμένα της χρονιάς που παρουσιάζονται στην ετήσια έκθεση, ο αναγνώστης μπορεί να συμπεράνει πως η Αποστολή και οι Στόχοι της Αρχής επιτυγχάνονται στο έπακρο.

Η Αρχή Ψηφιακής Ασφάλειας, όπως διαφαίνεται από την έκθεση απολογισμού, έχει θέσει γερές βάσεις για συνεχή αναβάθμιση των επιπέδων Κυβερνοασφάλειας και έχει επιτύχει τους στρατηγικούς της στόχους θωρακίζοντας την κοινωνία μας και ενισχύοντας τη διεθνή μας ανταγωνιστικότητα με συνεπαγόμενη συμβολή στην εθνική οικονομία.

Η στελέχωση της Αρχής Ψηφιακής Ασφάλειας από εξειδικευμένους επαγγελματίες, απέφερε την επίτευξη του στόχου της προληπτικής και ενεργούς αντιμετώπισης κυβερνο-απειλών, ενισχύοντας με τον τρόπο αυτό την ψηφιακή ασφάλεια όλων των σημαντικών υποδομών και υπηρεσιών της χώρας. Ο τεχνικός και επιχειρησιακός τομέας της Αρχής, το Εθνικό CSIRT-CY λειτούργησε εξαιρετικά ικανοποιητικά.

Θερμές ευχαριστίες εκφράζω προς τη Διεύθυνση και το προσωπικό της Αρχής Ψηφιακής Ασφάλειας (ΑΨΑ) για την προσήλωση τους στην επίτευξη του οράματος και των στόχων της Αρχής, που με ζήλο και υπευθυνότητα, καθώς και με την ικανότητα του, ανταποκρίθηκε στις διάφορες προκλήσεις που αντιμετωπίσαμε και στάθηκε αλληλέγγυα προς την κοινωνία μας, επιφορτισμένη με το καθήκον της προστασίας από τις απειλές του Κυβερνοχώρου.

Τέλος, εκφράζω τις ευχαριστίες μου σε όλους τους συνεργάτες της ΑΨΑ για την εμπιστοσύνη τους στην Αρχή. Σε συνεργασία με την ΑΨΑ, η παροχή της πολύτιμης τεχνογνωσίας τους και η συνεχής στήριξη και συνεργασία τους, έφεραν ουσιαστικό αποτέλεσμα στη θωράκιση του τόπου μας.

Είμαι πεπεισμένος ότι και αυτή τη χρονιά μπορούμε να συνεχίσουμε να υπηρετούμε και να συνεισφέρουμε για τα συμφέροντα της Κύπρου, ανεξάρτητα από τις προκλήσεις με τις οποίες θα βρεθούμε αντιμέτωποι. Τα γερά θεμέλια της Αρχής έχουν δοκιμαστεί σε δύσκολες συγκυρίες. Η ανθεκτικότητα τους έχει αποδειχθεί ζωτική για να κατορθώσει να οικοδομήσει ένα ασφαλές περιβάλλον. Τα γεγονότα-σταθμοί του 2021 που ακολουθούν, αποτελούν ένα έμπρακτο δείγμα γραφής του έργου της Αρχής.

Γιώργος Μιχαηλίδης

Επίτροπος Επικοινωνιών

ΓΕΓΟΝΟΤΑ ΟΡΟΣΗΜΑ 2021

Το 2021 χαρακτηρίστηκε από πολλά επιτεύγματα και δράσεις:

Έκδοση δευτερογενών νομοθεσιών

Εντός του 2021, δημοσιεύθηκαν στην Επίσημη Εφημερίδα της Δημοκρατίας οι περί Διαδικασίας Αποφάσεις Δημόσιων Ακροάσεων (βλ. ενότητα 3.1.6), Δημόσιων Διαβουλεύσεων (βλ. ενότητα 3.1.5), Διοικητικών Προστίμων (βλ. ενότητα 3.1.4) και Κυβερνοασφάλειας σε δίκτυα επικοινωνιών πέμπτης γενιάς 5G (βλ. ενότητα 3.1.9).

Αξιολόγηση και επαναξιολόγηση της κρισιμότητας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών («Φορείς») στην Κυπριακή Δημοκρατία

Η ΑΨΑ, σε συνεργασία με εξωτερικούς συμβούλους, προχώρησε σε αξιολόγηση ή/και επαναξιολόγηση κρισιμότητας (criticality (re)assessment) των Φορέων στην Κύπρο. Το έργο αξιολόγησης του επιπέδου κρισιμότητας αποτελεί μια από τις πιο σημαντικές δραστηριότητες στα πλαίσια της εφαρμογής της Οδηγίας NIS και σημειώνεται ότι το εν λόγω έργο αξιολόγησης κρισιμότητας που διενεργήθηκε το 2018 έπρεπε να συνεχιστεί και να πραγματοποιηθεί συμπληρωματική αξιολόγηση και επαναξιολόγηση ορισμένων φορέων (βλ. ενότητα 3.1.7).

Ορισμός της Αρχής Ψηφιακής Ασφάλειας ως το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας στην Κυπριακή Δημοκρατία (NCCC-CY)

Τον Δεκέμβριο του 2021, η ΑΨΑ ορίστηκε ως το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας στην Κυπριακή Δημοκρατία (NCCC-CY). Το NCCC-CY θα παρέχει γνώση και θα διευκολύνει την πρόσβαση σε τεχνογνωσία για βιομηχανικά, τεχνολογικά και ερευνητικά θέματα κυβερνοασφάλειας. Επίσης, θα ενεργεί ως το σημείο επαφής σε εθνικό επίπεδο για την Κοινότητα Κυβερνοασφάλειας και θα υποστηρίζει το Ευρωπαϊκό Κέντρο Αρμοδιότητας στην εκπλήρωση της αποστολής και των στόχων του (βλ. ενότητα 7).

Αξιολόγηση του Multivendor Strategy των Παροχέων Ηλεκτρονικών Επικοινωνιών για την παροχή δικτύων και υπηρεσιών δικτύου κινητής τηλεφωνίας Πέμπτης Γενιάς 5G

Στα πλαίσια της στρατηγικής πολλαπλών προμηθευτών για δίκτυα 5G από τους παροχείς τηλεπικοινωνιών, ξεκίνησε η αξιολόγηση τους από την ΑΨΑ σύμφωνα με την Απόφαση για την Κυβερνοασφάλεια σε δίκτυα επικοινωνιών πέμπτης γενιάς 5G (βλ. ενότητα 3.1.9).

Ανάπτυξη της πλατφόρμας iDSAMPL, και ολοκλήρωση του σχετικού Ευρωπαϊκού Προγράμματος

Κατά το 2021, η ΑΨΑ ολοκλήρωσε συγχρηματοδοτούμενο έργο (βλ. ενότητα 9.1.2) με εξωτερικούς συνεργάτες, που αφορά στη δημιουργία ολοκληρωμένης πλατφόρμας διαχείρισης εμπλεκομένων φορέων (κυρίως για τους εποπτευόμενους φορείς).

Έναρξη της φάσης Υλοποίησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας

Μέσω των δραστηριοτήτων της ΑΨΑ, ξεκίνησε η υλοποίηση μεγάλου μέρους των δράσεων της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας (βλ. ενότητα 4).

Έναρξη διαδικασίας πρόσληψης των νέων μόνιμων στελεχών της ΑΨΑ

Μία σημαντική εξέλιξη το 2021, ήταν η έναρξη διαδικασίας για την πρόσληψη των νέων μόνιμων στελεχών της ΑΨΑ.

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 τον 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

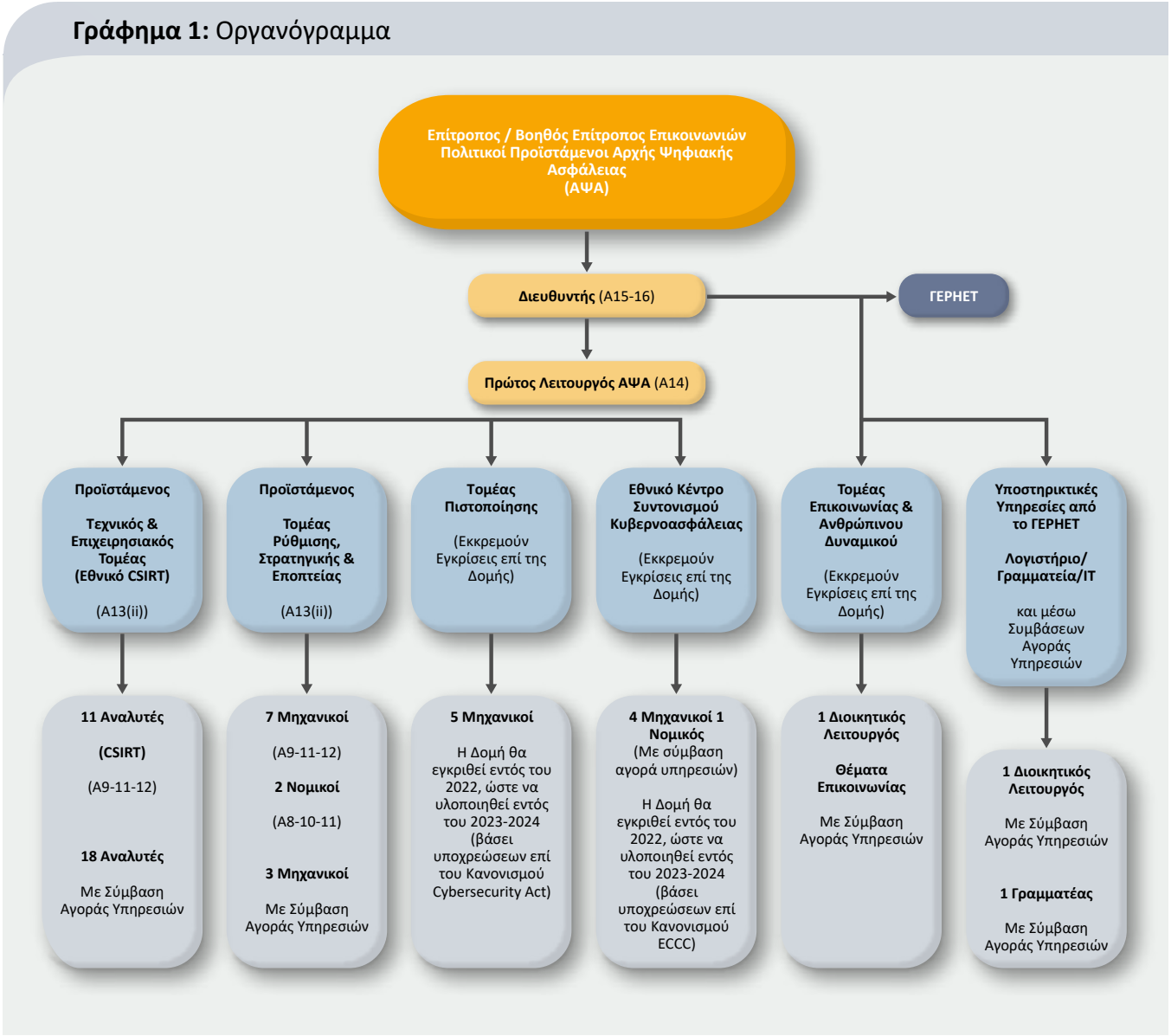
Η ΑΨΑ αποσκοπεί στην προστασία των κρίσιμων υποδομών πληροφοριών του κράτους και τη σωστή λειτουργία των τεχνολογιών επικοινωνιών και πληροφορικής του τόπου με τα απαιτούμενα επίπεδα ασφάλειας προς όφελος του κάθε χρήστη, των πολιτών, της οικονομίας και της χώρας ευρύτερα, έχοντας ως βασικούς στόχους:

- 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 φορέων για τη διασφάλιση σωστής και αποτελεσματικής συνεργασίας,
- τη διαμόρφωση και εποπτεία της εφαρμογής 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 στον κυβερνοχώρο, και κατ' επέκταση τις εξελίξεις στον τομέα της κυβερνοασφάλειας για την αναβάθμιση της ασφάλειας των κρίσιμων τομέων της Κυπριακής Δημοκρατίας, και
- την προώθηση και συντονισμό υλοποίησης της Εθνικής Στρατηγικής.

1.3 Οργανωτική Δομή

Η εγκεκριμένη οργανωτική δομή της ΑΨΑ παρουσιάζεται στο Γράφημα 1, στο οποίο αποτυπώνονται ενδεικτικά οι τομείς αρμοδιότητας της Αρχής.

Γράφημα 1: Οργανόγραμμα



1.3.1 Τομέας Ρύθμισης, Στρατηγικής και Εποπτείας

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

Στόχος του Τομέα ΡΣΕ είναι να προάγει την επίτευξη υψηλού επιπέδου ασφάλειας δικτύων και συστημάτων πληροφοριών, όλων των:

α Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ)
β Φορέων Κρίσιμων Υποδομών Πληροφοριών (ΦΚΠΥ)
γ Παροχέων Δικτύων ή/και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών
δ Παροχέων Ψηφιακών Υπηρεσιών

Ο Τομέας ΡΣΕ περιλαμβάνει μεταξύ άλλων πληθώρα υπηρεσιών που αφορούν κυρίως ρυθμιστικά πλαίσια, αξιολογήσεις κρισιμότητας και κινδύνων, καθορισμό και εποπτεία πλαισίων και διαδικασιών, καθώς και πρωτοβουλίες για ενίσχυση του επιπέδου κυβερνοασφάλειας σε δημόσιο και ιδιωτικό τομέα.

Επίσης, ένας από τους βασικούς ρόλους του Τομέα ΡΣΕ για τα επόμενα χρόνια είναι η ανάπτυξη και διαχείριση της υλοποίησης της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας.

1.3.2 Τεχνικός και Επιχειρησιακός Τομέας – NATIONAL CSIRT-CY

Ο Τομέας του Εθνικού CSIRT-CY 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-CY 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 δράση των πολιτών.

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

α Ειδοποιήσεις ασφαλείας για τυχόν ευπάθειες που ανευρίσκονται στην κάθε υποδομή ξεχωριστά
β Ειδοποιήσεις ασφαλείας για τις οποίες χρίζουν ενημέρωσης οι διαχειριστές συστημάτων σε όλες τις υποδομές
γ Έλεγχοι ασφαλείας (είτε απομακρυσμένοι, π.χ. με αισθητήρες, είτε κατ' ίδιαν με προγράμματα ανάλυσης)
δ Εκπαιδεύσεις σε θέματα κυβερνοασφάλειας (είτε απομακρυσμένες, είτε κατ' ίδιαν)
ε Αναφορές με βήματα μετριασμού, παραμετροποίησης και βελτιστοποίησης δικτύων και πολιτικών
στ Δράσεις ευαισθητοποίησης για τις επιπτώσεις των κυβερνοαπειλών

Οι υπηρεσίες ανταπόκρισης προσφέρονται σε οποιαδήποτε Κρίσιμη Υποδομή Πληροφοριών κρίνεται αναγκαία η άμεση εφαρμογή πολιτικής διαχείρισης περιστατικών ασφαλείας από το Εθνικό CSIRT-CY. Σε περίπτωση, δηλαδή, που ένα περιστατικό κυβερνοασφάλειας βρίσκεται σε εξέλιξη ή έχει μόλις εντοπιστεί από τον οργανισμό, τότε θα τεθεί σε λειτουργία η πολιτική διαχείρισης περιστατικών (Incident Management).

Σε ορισμένες περιπτώσεις είναι απαραίτητη η μετάβαση των αναλυτών της Υπηρεσίας στις εγκαταστάσεις ενός οργανισμού επί εικοσιτετράωρου βάσεως για τη συλλογή χρήσιμων στοιχείων

και ευρημάτων για σκοπούς ανάλυσης μέσω της χρήσης προηγμένων εργαστηρίων και εργαλείων που είναι διαθέσιμα στις εγκαταστάσεις της Υπηρεσίας. Σημειωτέων ότι, η Κυπριακή Δημοκρατία αριθμεί περί τις 66 Κρίσιμες Υποδομές Πληροφοριών.

Η διαχείρισης ενός περιστατικού εμπερικλείει μία σειρά άμεσων ενεργειών που λαμβάνονται για την αντιμετώπιση του, όπως:

α Συλλογή κακόβουλου λογισμικού/κώδικα/αρχείων
β Ανάλυση κακόβουλου λογισμικού/κώδικα/αρχείων
γ Δικανική ανάλυση κακόβουλου λογισμικού/κώδικα/αρχείων
δ Εξαγωγή βημάτων μετριασμού από την ανάλυση κακόβουλου λογισμικού/κώδικα/αρχείων (IoCs)
ε Βελτιστοποίηση της υποδομής βάσει των ευρημάτων της ανάλυσης με το πέρας του περιστατικού

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 τις υποχρεώσεις της χώρας μας για την υλοποίηση των απαιτήσεων του Κανονισμού (ΕΕ) 2019/881 για την Κυβερνοασφάλεια. Η Αρχή Ψηφιακής Ασφάλειας έχει αναλάβει τον ρόλο της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας (βλ. ενότητα 6).

Ο στόχος του Τομέα Πιστοποίησης Κυβερνοασφάλειας είναι να προάγει το θεσμό της πιστοποίησης κυβερνοασφάλειας (για προϊόντα και υπηρεσίες στον τομέα πληροφορικής και επικοινωνιών) 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).

1.3.4 Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας

Με απόφαση του Υπουργικού Συμβουλίου ημερομηνίας 21 Δεκεμβρίου 2021, η Αρχή Ψηφιακής Ασφάλειας ορίστηκε ως το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας στην Κυπριακή Δημοκρατία (NCCC-CY). Βασική αποστολή του Εθνικού Κέντρου Συντονισμού είναι να παρέχει γνώση και να διευκολύνει την πρόσβαση σε τεχνογνωσία για βιομηχανικά, τεχνολογικά και ερευνητικά θέματα κυβερνοασφάλειας. Το NCCC-CY θα ενεργεί ως το σημείο επαφής σε εθνικό επίπεδο για την Κοινότητα Κυβερνοασφάλειας και θα υποστηρίζει το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας στην εκπλήρωση της αποστολής και των στόχων του. Το NCCC-CY έχει υποβάλει αίτημα αξιολόγησης στην Ευρωπαϊκή Επιτροπή με σκοπό να λάβει έγκριση για τη διαχείριση ευρωπαϊκών χρηματοδοτήσεων, οι οποίες θα κατανέμονται στο εθνικό οικοσύστημα κυβερνοασφάλειας.

Κύριο μέλημα του Κέντρου είναι να διασφαλίσει ότι όλα τα ενδιαφερόμενα μέρη, και ιδίως οι μικρομεσαίες επιχειρήσεις, έχουν επαρκή υποστήριξη και πρόσβαση στη γνώση και στα αποτελέσματα της έρευνας και ανάπτυξης στον τομέα της κυβερνοασφάλειας, με στόχο να καταστούν επαρκώς ασφαλείς. Το Κέντρο θα αναλάβει δράσεις για να βοηθήσει τις μικρομεσαίες επιχειρήσεις στην Κύπρο να είναι ενεργές, ανταγωνιστικές και ικανές να συνεισφέρουν σημαντικά στην ηγετική θέση της Ευρωπαϊκής Ένωσης στον τομέα της κυβερνοασφάλειας. Το όραμα είναι να καταστεί η Κυπριακή Δημοκρατία πρωτοπόρος στον τομέα της κυβερνοασφάλειας, διασφαλίζοντας έναν αξιόπιστο και προστατευμένο κυβερνοχώρο για όλους τους πολίτες.

1.4 Στελέχωση

Κατά το 2021, δύο (2) μόνιμοι υπάλληλοι από το ΓΕΡΗΕΤ (Γραφείο Επιτρόπου για τη Ρύθμιση Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων), και συγκεκριμένα 1 Λειτουργός και 1 Βοηθός Γραμματειακός Λειτουργός, 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 ο Τομέας Ρύθμισης, Στρατηγικής και Εποπτείας στελεχώνεται από άλλα τέσσερα (4) άτομα: δύο (2) Νομικούς, μία (1) Διοικητική Λειτουργό και μία (1) Γραφέα.

Εντός του 2021, ολοκληρώθηκαν οι διαδικασίες του ΣΕΠΑ (Συμβούλιο Επιλογής και Προαγωγών ΑΨΑ) για τη στελέχωση της θέσης του Πρώτου Λειτουργού – Προϊστάμενου της ΑΨΑ, καθώς και δύο (2) θέσεων μόνιμων Νομικών Λειτουργών.

Εντός του 2022, αναμένεται ότι θα προκηρυχθούν ακόμα οκτώ (8) νέες θέσεις εργασίας για τη μόνιμη στελέχωση του Τομέα Ρύθμισης, Στρατηγικής και Εποπτείας, και επιπρόσθετα δώδεκα (12) θέσεις εργασίας για τη μόνιμη στελέχωση του Εθνικού CSIRT-CY.

1.5 Νέες Δομές

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

Ο περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμος του 2020 (Ν.89(Ι)/2020), εναρμονίζει πλήρως την εθνική νομοθεσία με το Ευρωπαϊκό νομικό πλαίσιο σχετικά με τα μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (Οδηγία (ΕΕ) 2016/1148 – «Οδηγία NIS»[1]) καθώς και για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (Οδηγία (ΕΕ) 2018/197[2]).

1.5.2 Ανάπτυξη Πολιτικών και Διαδικασιών Εθνικού CSIRT-CY

Κατά το 2021, 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:

α Διαχείριση περιστατικών (Incident Management)
- Ανάπτυξη εφαρμογής για διαχείριση περιστατικών phishing - Phishing Reporting Program
- Ανάπτυξη εφαρμογής για αναγνώριση κακόβουλων IP τα οποία διενεργούν κατανεμημένη άρνηση παροχής υπηρεσιών - DDOS attribute/IP Tools

β Συλλογή πληροφοριών για απειλές (threat intelligence)
- Ανάπτυξη εφαρμογής (PARSE) για την έγκαιρη ενημέρωση σχετικά με ευπάθειες που εντοπίζονται σε διευθύνσεις πρωτοκόλλων διαδικτύου IP των Κρίσιμων Υποδομών

γ Έλεγχο τρωτών σημείων (vulnerability testing).

[1] Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση - https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L1148&from=el

[2] Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Δεκεμβρίου 2018 για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (Αναδιατύπωση) (Κείμενο που παρουσιάζει ενδιαφέρον για το ΕΟΧ) - https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32018L1972

2. ΟΙΚΟΝΟΜΙΚΕΣ ΚΑΤΑΣΤΑΣΕΙΣ

2.1 Μη Ελεγμένες Οικονομικές Καταστάσεις για το έτος 2021

Οι οικονομικές καταστάσεις της ΑΨΑ για το έτος που έληξε την 31η Δεκεμβρίου 2021, ετοιμάστηκαν όπως προβλέπεται από το άρθρο 48 του Ν. 89(Ι)/2020. Οι βασικότερες πληροφορίες για την καταγραφή δαπανών και εσόδων, που περιέχονται στις προκαταρτικές μη ελεγμένες οικονομικές καταστάσεις για το έτος που έληξε στις 31 Δεκεμβρίου 2021, απεικονίζονται στο Γράφημα 2 και περιλαμβάνουν:

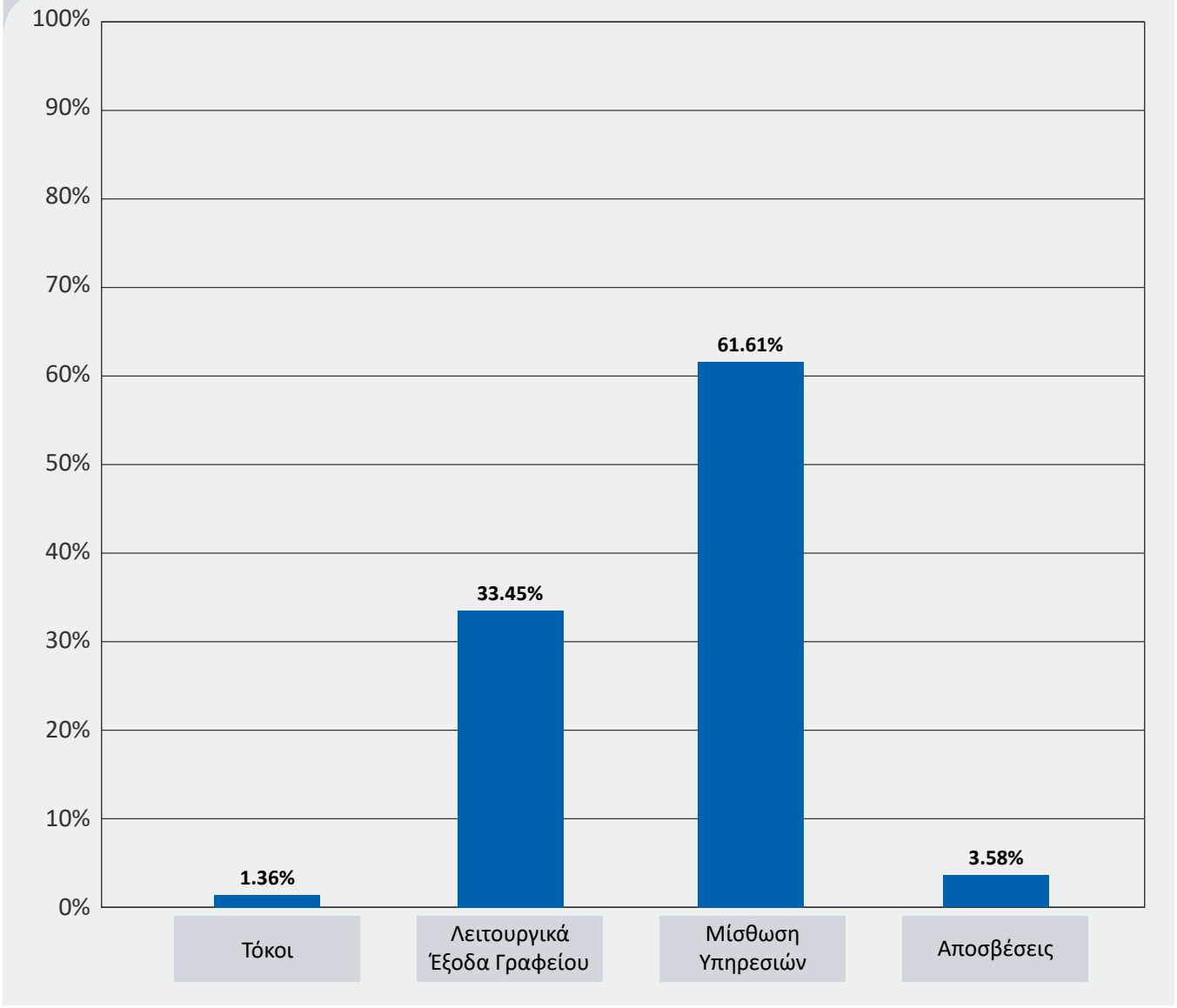
Πίνακας 1: Μη Ελεγμένη Κατάσταση Συνολικών Εισοδημάτων 2021

	2021 €	2020 €
Έσοδα		
Άλλα έσοδα*	5.783.122	1.723.437
Έσοδα Χρηματοδότησης (Τόκοι)	-	-
	5.783.122	**1.723.437**
Έξοδα		
Έξοδα Χρηματοδότησης (Τόκοι)	33.085	2.988
Λειτουργικά έξοδα γραφείου	814.538	508.223
Μίσθωση υπηρεσιών	1.500.463	934.466
Αποσβέσεις εξοπλισμού και εγκαταστάσεων	42.439	222.249
Αποσβέσεις άϋλου ενεργητικού	44.744	94.541
	2.435.269	**1.762.467**
Πλεόνασμα/(έλλειμμα) έτους από συνήθεις εργασίες	3.347.853	(39.030)
Συνολικά εισοδήματα για το έτος	**3.347.853**	**(39.030)**

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

* Τα Άλλα Έσοδα αποτελούνται από Ευρωπαϊκά συγχρηματοδοτούμενα προγράμματα καθώς επίσης και χορηγίες από τα Υπουργεία Άμυνας και Εξωτερικών για σκοπούς ανάπτυξης υποδομών κυβερνοάμυνας και κυβερνοασφάλειας.

Γράφημα 2: Κατανομή Δαπανών για το 2021



Πίνακας 2: Μη Ελεγμένη Κατάσταση Χρηματοοικονομικής Θέσης στις 31 Δεκεμβρίου 2021

	2021 €	2020 €
ΠΕΡΙΟΥΣΙΑΚΑ ΣΤΟΙΧΕΙΑ		
Μη κυκλοφορούντα περιουσιακά στοιχεία		
Εγκαταστάσεις και εξοπλισμός	1.009.513	736.741
Άϋλα στοιχεία ενεργητικού	286.812	271.362
Σύνολο μη κυκλοφορούντων περιουσιακών στοιχείων	**1.296.325**	**1.008.103**
Κυκλοφορούντα περιουσιακά στοιχεία		
Χρεώστες και προπληρωμές	7.857.609	4.868.219
Μετρητά στην τράπεζα	5.523.690	5.523.690
Σύνολο κυκλοφορούντων περιουσιακών στοιχείων	**13.381.299**	**8.633.004**
ΣΥΝΟΛΟ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ	**14.677.624**	**9.641.107**
ΙΔΙΑ ΚΕΦΑΛΑΙΑ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ		
Ίδια κεφάλαια		
Αποθεματικά	(3.484.101)	167.706
Σύνολο ιδίων κεφαλαίων	**(3.484.101)**	**167.706**
Τρέχουσες υποχρεώσεις		
Πιστωτές και οφειλόμενα έξοδα	6.537.093	800.900
Προεισπραχθέντα τέλη	8.418.460	5.716.966
Κρατική χορηγία	3.206.172	2.955.535
Ολικό τρεχουσών υποχρεώσεων	**18.161.725**	**9.473.401**
ΟΛΙΚΟ ΙΔΙΩΝ ΚΕΦΑΛΑΙΩΝ ΚΑΙ ΥΠΟΧΡΕΩΣΕΩΝ	**14.677.624**	**9.641.107**

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

* Το Αποθεματικό ύψους (€3,448,101) για το έτος 2021 προκύπτει από την αναγνώριση υποχρέωσης αναπροσαρμογής τελών, αναγνώριση ποσών που εισπράχθηκαν από Υπουργεία και για τα οποία δεν έχουν εκτελεστεί ακόμη έργα και αναπροσαρμογή της κρατικής χορηγίας προς επιστροφή.

3. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

3.1 Νομοθεσία Αρχής Ψηφιακής Ασφάλειας

Σύμφωνα με την ισχύουσα Νομοθεσία (Νόμος 89(I)/2020) («Νόμος»), ο Επίτροπος Επικοινωνιών («Επίτροπος») ορίστηκε ως ο επικεφαλής της Αρχής Ψηφιακής Ασφαλείας («ΑΨΑ»), η οποία είναι υπεύθυνη και για τον συντονισμό της υλοποίησης της Στρατηγικής Κυβερνοασφάλειας, δυνάμει των διατάξεων του άρθρου 3 του Νόμου 17(I)/2018, ο οποίος καταργήθηκε και αντικαταστάθηκε με τον Νόμο 89(I)/2020, και βάσει του οποίου συνεχίζει να είναι ο επικεφαλής της ΑΨΑ και να έχει τις αρμοδιότητες που προβλέπονται στις διατάξεις του Νόμου. Η Αρχή, σύμφωνα με τις διατάξεις του Νόμου, λειτουργεί ως η αρμόδια εθνική αρχή για την εφαρμογή των διατάξεων του Νόμου.

Η ΑΨΑ, μέρος της οποίας αποτελεί το Εθνικό CSIRT–CY (άρθρο 6 (9) του Ν. 89(I)/2020), προσφέρει υπηρεσίες πρόληψης και αντιμετώπισης απειλών, ευπαθειών και περιστατικών κυβερνοασφάλειας. Επιπλέον, το Εθνικό CSIRT–CY προσφέρει υπηρεσίες ανάπτυξης, οι οποίες, μεταξύ άλλων, περιλαμβάνουν τη συνεχή ανάπτυξη τεχνολογιών που μπορούν να αξιοποιηθούν και να παρέχουν υποστήριξη στα συστήματα και δίκτυα πληροφοριών των Φορέων («Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, Φορείς Κρίσιμων Υποδομών Πληροφοριών, Παροχείς Δικτύων ή/και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών και Παροχείς Ψηφιακών Υπηρεσιών»). Σε θέματα αντιμετώπισης περιστατικών και συμβάντων, η ΑΨΑ, σύμφωνα με τις πρόνοιες της Οδηγία NIS και του Νόμου 89(I)/2020, λειτουργεί το Εθνικό CSIRT-CY σε συνεχή βάση (24/7, 365 μέρες το χρόνο) για τη διαχείριση περιστατικών κυβερνοασφάλειας στα συστήματα και δίκτυα των Φορέων. Τέτοια περιστατικά είναι δυνατόν να επιφέρουν τεράστιες ζημιές και αρνητικές συνέπειες σε Οργανισμούς, Υπηρεσίες και Εταιρείες, που εάν δεν τύχουν του κατάλληλου χειρισμού είναι δυνατόν να επιφέρουν τεράστιο οικονομικό ή και κοινωνικό κόστος.

Η ΑΨΑ χρηματοδοτείται από τους Φορείς, σύμφωνα με τη μεθοδολογία υπολογισμού τελών που καθορίζεται στους περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Τέλη) Κανονισμούς του 2020 (Κ.Δ.Π. 359/2020), οι οποίοι εκδοθήκαν από το Υπουργικό Συμβούλιο και εγκρίθηκαν από τη Βουλή των Αντιπροσώπων δυνάμει των διατάξεων της ισχύουσας Νομοθεσίας της Αρχής.

3.1.1 Τροποποίηση της Νομοθεσίας περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών

Εντός του 2021 τροποποιήθηκε ο Νόμος 89(I)/2020 με σκοπό τη διασφάλιση της εφαρμογής του Κανονισμού (ΕΕ) 2019/881[4] στην Κυπριακή Δημοκρατία τη μεταφορά απαραίτητων προνοιών από τον Κανονισμό (ΕΕ) 2019/881 ούτως ώστε να υλοποιηθεί ο Κανονισμός στην Κυπριακή Δημοκρατία, βάσει της Απόφασης του Υπουργικού Συμβουλίου με αρ.88.139/11.9.2019, και τη διασφάλιση της εφαρμογής τουμεταφορά απαραίτητων προνοιών από τον Κανονισμόού (ΕΕ) 2021/887[5] με σκοπό να υλοποιηθεί ο Κανονισμός (ΕΕ) 2021/887 στην Κυπριακή Δημοκρατία, βάσει της Απόφασης του Υπουργικού Συμβουλίου που λήφθηκε στις 21.12.2021.

Επίσης, με την υπό αναφορά τροποποίηση, προστέθηκαν εναρμονίστηκαν στο Νόμο 89(I)/2020 τα σημεία (δ), (ε), (στ) και (θ) του άρθρο 3 (3) από την Οδηγία 2014/53/ΕΕ[6]. Τα συγκεκριμένα σημεία του άρθρου (3) της Οδηγίας, αφορούν τον ραδιοεξοπλισμό και μεταφέρονται από το Νόμο 112(I)/2004 στο Νόμο 89(I)/2020, μετά από διαβουλεύσεις μεταξύ του ΥΕΚΨΠ και του Επιτρόπου Επικοινωνιών.

[3] https://dsa.cy/images/pdf-upload/Regulation-359-2020.pdf

[4] Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του Κανονισμού (ΕΕ) 526/2013 (πράξη για την κυβερνοασφάλεια) - https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32019R0881&from=RO

[5] Κανονισμός (ΕΕ) 2021/887 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 2021 για τη σύσταση του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού - https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32021R0887&from=EN

[6] Οδηγία 2014/53/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 16ης Απριλίου 2014 σχετικά με την εναρμόνιση των νομοθεσιών των κρατών μελών σχετικά με τη διαθεσιμότητα ραδιοεξοπλισμού στην αγορά και την κατάργηση της Οδηγίας 1999/5/ΕΚ - https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32014L0053&from=lv

Παράλληλα, έγινε τροποποίηση των διατάξεων στην υφιστάμενη νομοθεσία της Αρχής μετά από εισηγήσεις που έλαβε η ΑΨΑ κατά τη διενέργεια της Δημόσιας Διαβούλευσης για την περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κυβερνοασφάλεια Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών Πέμπτης Γενιάς 5G) Απόφαση του 2020 (Κ.Δ.Π. 408/2020)[7].

Τέλος, τροποποιήθηκαν διατάξεις για την ενοποίηση των διοικητικών δομών της Αρχής υπό την εποπτεία του Επιτρόπου Επικοινωνιών. Οι υπό αναφορά αλλαγές συνάδουν με την πολιτική απόφαση για τη δομή της Νομοθεσίας του Επιτρόπου Επικοινωνιών, με τη δημιουργία Νόμου Ομπρέλα (υφιστάμενος Νόμος 112(I)/2004).

Ο εν λόγω Νόμος Ομπρέλα θα καλύπτει όλα τα θέματα που αφορούν την διοίκηση και το ανθρώπινο δυναμικό της υπηρεσίας. Επιπλέον, θα καλύπτει και την δημιουργία τριών κάθετων/ειδικών νομοθεσιών για τα ρυθμιστικά θέματα στους τομείς αρμοδιότητας του Επιτρόπου Επικοινωνιών (Ηλεκτρονικές Επικοινωνίες, Ταχυδρομικές Υπηρεσίες και Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών).

Το τροποποιητικό νομοσχέδιο, μετά τον νομοτεχνικό έλεγχο που θα τύχει από τη Νομική Υπηρεσία, αναμένεται να εγκριθεί από το Υπουργικό Συμβούλιο και να ψηφιστεί από τη Βουλή των Αντιπροσώπων εντός του 2022.

3.1.2 Εθνικό Πλαίσιο Κυβερνοασφάλειας

Εντός του 2021, η Αρχή τροποποίησε την 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)[8], μετά από τη διεξαγωγή σχετικής Δημόσιας Διαβούλευσης[9].

Η υπό αναφορά τροποποίηση της Απόφασης έγινε με σκοπό τη συμμόρφωση και των παροχέων δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών και των παροχέων ψηφιακών υπηρεσιών, επιπρόσθετα από τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και Φορείς Κρίσιμων Υποδομών Πληροφοριών, σύμφωνα με τις απαιτήσεις και τις υποχρεώσεις του Νόμου 89(I)/2020, ως εκάστοτε τροποποιείται ή/και αντικαθίσταται, της Οδηγίας (ΕΕ) 2016/1148, καθώς και της Οδηγίας (ΕΕ) 2018/1972.

Τα ενδιαφερόμενα μέρη κλήθηκαν να υποβάλουν τις απόψεις τους για την προτεινόμενη Απόφαση και το περιεχόμενο της, ως μέρος της υπό αναφορά Δημόσιας Διαβούλευσης. Με τη δημοσίευσή της (εντός του 2022), η εν λόγω Απόφαση θα περιλαμβάνεται σε δευτερογενή νομοθεσία (Κανονιστική Διοικητική Πράξη) της Αρχής και θα εκδοθεί δυνάμει του σχετικού Νόμου 89(I)/2020, ως αυτός τροποποιείται ή/και αντικαθίσταται, εντός του 2022.

Επιπλέον, σύμφωνα με τις πρόνοιες της Απόφασης Κ.Δ.Π. 389/2020 οι Φορείς είχαν υποχρέωση μέχρι τις 31 Δεκεμβρίου 2021 να υποβάλουν ηλεκτρονικά όλα τα προβλεπόμενα έγγραφα, λαμβάνοντας υπόψη τις απαιτήσεις του άρθρου 13 της εν λόγω Απόφασης, στην Αρχή για αξιολόγηση. Τα έγγραφα έπρεπε να συνοδεύονται από λεπτομερές πρόγραμμα υλοποίησης των απαραίτητων μέτρων ασφάλειας για μείωση των κινδύνων που έχουν εντοπιστεί σε αποδεκτά επίπεδα.

Η Αρχή, εντός του 2022, θα προχωρήσει σε αξιολόγηση των εγγράφων που υπέβαλαν οι Φορείς σύμφωνα με τις πρόνοιες της Απόφασης Κ.Δ.Π. 389/2020.

[7] *https://dsa.cy/images/pdf-upload/Decision-408-2020.pdf*
[8] *https://dsa.cy/images/pdf-upload/Decision-389-2020.pdf*
[9] *Δημόσια Διαβούλευση ΑΨΑ 05/2021 - Η περί Τροποποιήσεως της περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών) Απόφασης του 2020, - https://dsa.cy/activities/public-consultations/public-consultation-dsa-05-2021*

3.1.3 Κοινοποίηση Περιστατικών Παραβίασης Ψηφιακής Ασφάλειας

Εντός του 2021, η Αρχή ξεκίνησε την αναθεώρηση της περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κοινοποίηση Συμβάντων) Απόφαση του 2019 (Κ.Δ.Π. 218/2019)[10] και εντός του 2021 διεξήχθη σχετική Δημόσια Διαβούλευση[11].

Η Απόφαση θα τυγχάνει εφαρμογής από όλους τους φορείς εκμετάλλευσης βασικών υπηρεσιών, φορείς κρίσιμων υποδομών πληροφοριών, παροχείς δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών και τους παροχείς ψηφιακών υπηρεσιών («Φορείς και Παροχείς»). Με την υπό αναφορά Απόφαση καθορίζονται τα κριτήρια, τα κατώτατα όρια και οι συνθήκες υπό τις οποίες ένα συμβάν ασφάλειας έχει σοβαρό ή/και σημαντικό αντίκτυπο στην παροχή των υπηρεσιών των ως άνω φορέων και παροχέων, και ως εκ τούτου ενεργοποιεί την υποχρέωση των φορέων και των παροχέων αυτών για υποβολή κοινοποίησης περιστατικών κυβερνοασφάλειας στην Αρχή. Περαιτέρω, ρυθμίζεται η διαδικασία υποβολής των κοινοποιήσεων, και ιδίως το περιεχόμενο των κοινοποιήσεων, ο τρόπος υποβολής τους και οι προθεσμίες που πρέπει να τηρηθούν από τους Φορείς και τους Παροχείς.

Το περί της κοινοποίησης των παραβιάσεων ασφάλειας ή απώλειας ακεραιότητας δικτύων ή/και υπηρεσιών Διάταγμα του 2013 (Κ.Δ.Π. 371/2013)[12] και η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κοινοποίηση Συμβάντων) Απόφαση του 2019 (Κ.Δ.Π. 218/2019) θα καταργηθούν και θα αντικατασταθούν με την έκδοση της νέας Απόφασης περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κοινοποίηση Συμβάντων). Η νέα Απόφαση αναμένεται να εκδοθεί εντός του 2022, λαμβάνοντας υπόψη τις πρόνοιες των κατευθυντήριων γραμμών του ENISA του 2020, για τις κοινοποιήσεις συμβάντων σχετικά με τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών, με σκοπό τη συμπερίληψη και των παροχέων δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών (βλ. θεματική ενότητα 4.6).

Ενημερωτικά, οι πρόνοιες της εν λόγω νέας Απόφασης θα παραμείνουν ίδιες με τις πρόνοιες της Απόφασης περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κοινοποίηση Συμβάντων) Απόφαση του 2019 (Κ.Δ.Π. 218/2019). Ωστόσο, θα συμπεριληφθούν οι παροχείς δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, θα προστεθεί κατώτατο όριο κοινοποίησης για τους παροχείς δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και επιπρόσθετος πίνακας στο έντυπο κοινοποιήσεων με πληροφορίες που ζητούνται μόνο από τους παροχείς Δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών. Επιπρόσθετα, θα ενταχθούν πρόνοιες με σκοπό να διασφαλίζεται νομικά η ηλεκτρονική υποβολή των εντύπων κοινοποίησης μέσω της πλατφόρμας iDSAMPL (integrated Digital Security Authority Management Platform) που θα τεθεί σε λειτουργία εντός του 2022.

3.1.4 Διοικητικά Πρόστιμα

Στις 18 Ιουνίου 2021 δημοσιεύθηκε στην Επίσημη Εφημερίδα της Δημοκρατίας η περί Συλλογής Πληροφοριών και Επιβολής Διοικητικού Προστίμου Απόφαση του 2021 (Κ.Δ.Π. 251/2021)[13]. Πριν δημοσιευθεί η εν λόγω Απόφαση τέθηκε σε Δημόσια Διαβούλευση, και τα σχόλια των ενδιαφερομένων μερών που κατατέθηκαν λήφθηκαν υπόψη πριν την έκδοσή της.

Η Απόφαση θεσμοθετεί τόσο τα δικαιώματα όσο και τις υποχρεώσεις των προσώπων (νομικών και φυσικών) αναφορικά με τη δυνατότητα της Αρχής να ζητά πληροφορίες και να διεξάγει έρευνες και ελέγχους στα αρχεία, βιβλία, άλλα έγγραφα και στοιχεία αποθηκευμένα σε συστήματα πληροφοριών ή/και σε ηλεκτρονικούς υπολογιστές των εκάστοτε προσώπων, καθώς επίσης και τη διαδικασία αναφορικά με τη δυνατότητα της Αρχής να επιβάλει διοικητικά πρόστιμα ή και άλλες διοικητικές κυρώσεις σε περίπτωση που διαπιστώνεται παράβαση της σχετικής κείμενης νομοθεσίας,

[10] *https://dsa.cy/images/pdf-upload/Decision-218-2019.pdf*
[11] *Δημόσια Διαβούλευση ΑΨΑ 06/2021 – Η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κοινοποίηση Συμβάντων) Απόφαση - https://dsa.cy/activities/public-consultations/public-consultation-dsa-06-2021*
[12] *https://dsa.cy/images/pdf-upload/EC_Order_NotificationsSecurityBreaches_GR_25-10 2013_VM_0.pdf*
[13] *https://dsa.cy/images/pdf-upload/Decision-251-2021.pdf*

διασφαλίζοντας ταυτόχρονα και τα δικαιώματα των υπό κρίση παραβατών, όπως το δικαίωμα ακροάσεως κλπ.

3.1.5 Δημόσιες Διαβουλεύσεις

Στις 18 Ιουνίου 2021 δημοσιεύθηκε στην Επίσημη Εφημερίδα της Δημοκρατίας η περί Διαδικασίας Δημόσιων Διαβουλεύσεων Απόφαση του 2021 (Κ.Δ.Π. 252/2021)[14]. Πριν δημοσιευθεί η εν λόγω Απόφαση τέθηκε σε Δημόσια Διαβούλευση, και τα σχόλια των ενδιαφερομένων μερών που κατατέθηκαν λήφθηκαν υπόψη πριν την έκδοσή της.

Η Απόφαση θεσμοθετεί τη διαδικασία διενέργειας Δημόσιων Διαβουλεύσεων με εκπροσώπους της Δημοκρατίας, με φορείς εκμετάλλευσης βασικών υπηρεσιών, φορείς κρίσιμων υποδομών πληροφοριών, με παροχείς ψηφιακών υπηρεσιών ή/και παροχείς δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, και με οποιαδήποτε άλλα πρόσωπα ή οργανισμούς, όποτε η Αρχή κρίνει σκόπιμο, σύμφωνα με τις απαιτήσεις και τις υποχρεώσεις του Νόμου 89(Ι)/2020.

3.1.6 Δημόσιες Ακροάσεις

Στις 6 Αυγούστου 2021 δημοσιεύθηκε στην Επίσημη Εφημερίδα της Δημοκρατίας η περί Διαδικασίας Δημόσιων Ακροάσεων Απόφαση του 2021 (Κ.Δ.Π. 345/2021)[15]. Πριν δημοσιευθεί η εν λόγω Απόφαση τέθηκε σε δημόσια διαβούλευση[16], και τα σχόλια των ενδιαφερομένων μερών που κατατέθηκαν λήφθηκαν υπόψη πριν την έκδοσή της.

Η Απόφαση καθορίζει τη διαδικασία διενέργειας Δημόσιων Ακροάσεων, σύμφωνα με τις απαιτήσεις και τις υποχρεώσεις του Νόμου 89(Ι)/2020. Η διαδικασία Δημόσιας Ακρόασης, θεσμοθετεί τόσο τα δικαιώματα όσο και τις υποχρεώσεις των προσώπων (φορείς εκμετάλλευσης βασικών υπηρεσιών, φορείς κρίσιμων υποδομών πληροφοριών, παροχείς δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών και παροχείς ψηφιακών υπηρεσιών, και οποιαδήποτε άλλα νομικά ή φυσικά πρόσωπα ή οργανισμούς που εκάστοτε κρίνει η Αρχή, βάσει των αρμοδιοτήτων της που απορρέουν από τον περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμο) αναφορικά με τη δυνατότητα της Αρχής να διεξάγει Δημόσιες Ακροάσεις.

3.1.7 Αξιολόγηση Κρισιμότητας Υποδομών

Η ΑΨΑ, σε συνεργασία με εξωτερικούς συμβούλους, το 2021 ολοκλήρωσε τη διεξαγωγή έργου για την αξιολόγηση και επαναξιολόγηση της κρισιμότητας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών («Φορείς») στην Κυπριακή Δημοκρατία. Η αξιολόγηση πραγματοποιήθηκε στο πλαίσιο των αρμοδιοτήτων και των διαδικασιών που εφαρμόζει η ΑΨΑ βάσει του Νόμου 89(Ι)/2020. Συγκεκριμένα, η Αρχή έχει υποχρέωση (Άρθρο 27, Εδάφιο 5 του Νόμου), ανά διετία, να επανεξετάζει και, εφόσον απαιτείται, να επικαιροποιεί τον κατάλογο των Φορέων. Επιπλέον, ενόψει της υποχρέωσης της Αρχής να κοινοποιεί τους Φορείς της Κυπριακής Δημοκρατίας στα αρμόδια Ευρωπαϊκά σώματα, δηλαδή στην Ομάδα Συνεργασίας για την Ασφάλεια Δικτύων και Πληροφοριών (NIS Cooperation Group), στην Ευρωπαϊκή Επιτροπή και στον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), η ΑΨΑ προχώρησε σε αξιολόγηση ή/και επαναξιολόγηση κρισιμότητας (criticality (re)assessment) των Φορέων στην Κύπρο. Το έργο αξιολόγησης του επιπέδου κρισιμότητας αποτελεί μια από τις πιο σημαντικές δραστηριότητες στα πλαίσια της εφαρμογής της Οδηγίας NIS και σημειώνεται ότι το εν λόγω έργο αξιολόγησης κρισιμότητας που διενεργήθηκε το 2018 έπρεπε να συνεχιστεί και να πραγματοποιηθεί συμπληρωματική αξιολόγηση και επαναξιολόγηση ορισμένων φορέων.

[14] *https://dsa.cy/images/pdf-upload/Decision-252-2021.pdf*
[15] *https://dsa.cy/images/pdf-upload/Decision-345-2021.pdf*
[16] *Δημόσια Διαβούλευση ΑΨΑ 03/2021 - Δημόσιες Ακροάσεις - https://dsa.cy/activities/public-consultations/public-consultation-dsa-03-2021*

Τα αποτελέσματα της εκτίμησης κρισιμότητας των Φορέων, που διενήργησε η Αρχή Ψηφιακής Ασφάλειας, εγκρίθηκαν με Απόφαση του Υπουργικού Συμβουλίου, ημερομηνίας 02/09/2021, η οποία χαρακτηρίζεται ως απόρρητη και δεν δημοσιεύεται στην Επίσημη Εφημερίδα της Δημοκρατίας (άρθρο 27(10) του Νόμου 89(Ι)/2020). Σε συνέχεια της υπό αναφορά Απόφασης του Υπουργικού Συμβουλίου, ο Επίτροπος, στις 08/11/2021, λαμβάνοντας υπόψη την υπό αναφορά Απόφαση του Υπουργικού Συμβουλίου, τις πρόνοιες της Νομοθεσίας, και ιδίως τα άρθρα 17(ιδ), 17(ιε), 27 και 46, και τους τομείς και υποτομείς που περιλαμβάνονται στο Παράρτημα ΙΙ της Οδηγίας NIS (στις περιπτώσεις το Φορέων που κρίθηκαν ως Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών), εξέδωσε ξεχωριστές Αποφάσεις προς του Φορείς στις οποίες καθοριζόταν το επίπεδο κρισιμότητας για τον κάθε Φορέα για τις υπηρεσίες που ορίζονται στο Παράρτημα της κάθε Απόφασης, καθώς και ο καθορισμός του κάθε Φορέα (εάν ορίστηκε Φορέας Εκμετάλλευσης Βασικών Υπηρεσιών ή Φορέας Κρίσιμων Υποδομών Πληροφοριών). Σύμφωνα με τις Αποφάσεις, κάθε Φορέας οφείλει να συμμορφώνεται με τις υποχρεώσεις που απορρέουν από τον ορισμό του ως Φορέα Εκμετάλλευσης Βασικών Υπηρεσιών ή/και Φορέα Κρίσιμων Υποδομών Πληροφοριών, όπως αυτό προβλέπεται στο Νόμο και στις δυνάμει αυτού εκδοθείσες δευτερογενείς Νομοθεσίες, ως αυτά εκάστοτε τροποποιούνται ή/και αντικαθίστανται.

3.1.8 Ανάπτυξη Νέας Νομοθεσίας για τα Μέτρα Ασφάλειας Παροχέων Δικτύων ή/και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών

Εντός του 2021, η Αρχή ξεκίνησε την ετοιμασία σχετικής δευτερογενούς Νομοθεσίας για τα Μέτρα Ασφάλειας Παροχέων Δικτύων ή/και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών.

Στις 26 Αυγούστου 2021 ανακοινώθηκε η διεξαγωγή της Δημόσιας Διαβούλευσης[17] επί της Απόφασης περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Παροχέων Δικτύων ή/και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών).

Η Απόφαση καθορίζει ελάχιστες επιπρόσθετες υποχρεώσεις, τις οποίες πρέπει να τηρούν οι παροχείς δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, πέραν από τις υποχρεώσεις που καθορίζονται στην περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών) Απόφαση του 2020, ως εκάστοτε τροποποιείται ή/και αντικαθίσταται (Κ.Δ.Π. 389/2020). Η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Παροχέων Δικτύων ή/και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών) Απόφαση του 2021, καταργεί και αντικαθιστά το Περί Ασφάλειας Δικτύων και Πληροφοριών Διάταγμα του 2011 (Κ.Δ.Π. 253/2011)[18] (βλ. θεματική ενότητα 4.6).

Τα ενδιαφερόμενα μέρη κλήθηκαν να υποβάλουν τις απόψεις τους για την προτεινόμενη Απόφαση και το περιεχόμενο της, ως μέρος της υπό αναφορά Δημόσιας Διαβούλευσης. Η εν λόγω Απόφαση θα περιλαμβάνεται σε δευτερογενή νομοθεσία (Κανονιστική Διοικητική Πράξη) της Αρχής και θα εκδοθεί δυνάμει του σχετικού Νόμου 89(Ι)/2020, ως αυτός τροποποιείται ή/και αντικαθίσταται.

Με το πέρας της Δημόσιας Διαβούλευσης λήφθηκαν υπόψη τα σχόλια των εμπλεκομένων φορέων, και η σχετική Απόφαση αναμένεται να οριστικοποιηθεί και να δημοσιευθεί εντός του 2022.

3.1.9 Κυβερνοασφάλεια σε δίκτυα επικοινωνιών πέμπτης γενεάς (5G Cybersecurity)

Στις 16 Ιουλίου 2021 δημοσιεύθηκε στην Επίσημη Εφημερίδα της Δημοκρατίας η περί Τροποποιήσεως της περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κυβερνοασφάλεια Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών Πέμπτης Γενιάς 5G) Απόφασης του 2020, Απόφαση του 2021 (Κ.Δ.Π. 310/2021)[19]. Πριν δημοσιευθεί η εν λόγω Απόφαση διεξήχθη τηλεδιάσκεψη με τους παροχείς

[17] *Δημόσια Διαβούλευση ΑΨΑ 04/2021 - Η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Παροχέων Δικτύων ή/και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών) Απόφαση - https://dsa.cy/activities/public-consultations/public-consultation-dsa-04-2021*
[18] *https://dsa.cy/images/pdf-upload/Order-253-2011.pdf*
[19] *https://dsa.cy/images/pdf-upload/Decision-310-2021.pdf*

δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών («παροχείς») κατά τη διάρκεια της οποίας οι παροχείς ενημερώθηκαν για την τροποποίηση και ήταν σύμφωνοι με την τροποποίηση της Απόφασης.

Η τροποποίηση της περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κυβερνοασφάλεια Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών Πέμπτης Γενιάς 5G) Απόφασης του 2020 έγινε με σκοπό να καθοριστεί ο τρόπος υποβολής των εγγράφων που αναφέρονται στην Απόφαση Κ.Δ.Π. 408/2020, η οποία υποβολή θα γίνεται μέσω της πλατφόρμας iDSAMPL (βλ. ενότητα 3.2.2) που θα τεθεί σε λειτουργία εντός του 2022.

3.2 Ανάπτυξη Υποδομών και Εργαλείων

3.2.1 Υποδομή Εθνικού CSIRT-CY

Η υποδομή του Εθνικού CSIRT-CY αναβαθμίζεται συνεχώς λαμβάνοντας υπόψη τα καλύτερα ευρωπαϊκά και διεθνή πρότυπα που αφορούν τις ομάδες CSIRTs και 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 2021 προμηθεύτηκε εξειδικευμένα εργαλεία και προγράμματα με σκοπό τη διενέργεια συστηματικών ελέγχων ασφαλείας στις Κρίσιμες Υποδομές Πληροφοριών.

Μεταξύ άλλων, το Εθνικό CSIRT-CY, αξιοποιεί την εξής υποδομή:

α Πλατφόρμα καταγραφής μηχανογραφικού εξοπλισμού
β Εγκατάσταση εξειδικευμένων αισθητήρων στην υποδομή SOC (Security Operations Centre) του Εθνικού CSIRT-CY, οι οποίοι προσφέρουν ελέγχους ασφαλείας σε πραγματικό χρόνο – βασισμένοι σε πρωτόκολλα δικτύου για ανίχνευση και ανάλυση ύποπτων και κακόβουλων ενεργειών, στις Κρίσιμες Υποδομές Πληροφοριών, με σκοπό την έγκαιρη προειδοποίηση περιστατικών κυβερνοασφάλειας
γ Υποδομή και πλατφόρμα περιβάλλοντος κατάρτισης, το οποίο υποστηρίζει τη δημιουργία ρεαλιστικών δικτύων και υποδομών τεχνολογίας πληροφοριών, με στόχο τη δημιουργία και την ανάπτυξη ασκήσεων κυβερνοασφάλειας σε διάφορους τομείς, συμπεριλαμβανομένων της ναυτιλίας, της ενέργειας και των ηλεκτρονικών επικοινωνιών
δ Αυτοματοποιημένα κανάλια πληροφόρησης για δημιουργία αυτόματων και χειροκίνητων αναφορών και ειδοποιήσεων προς Κρίσιμες Υποδομές Πληροφοριών.

3.2.2 Ολοκληρωμένη Πλατφόρμα Διαχείρισης Εμπλεκόμενων Φορέων ΑΨΑ

Κατά το 2021, η ΑΨΑ ολοκλήρωσε συγχρηματοδοτούμενο έργο (βλ. ενότητα 9.1.2) με εξωτερικούς συνεργάτες, που αφορά στη δημιουργία ολοκληρωμένης πλατφόρμας διαχείρισης εμπλεκομένων φορέων (κυρίως για τους εποπτευόμενους φορείς). Το έργο αυτό ξεκίνησε το Δεκέμβριο του 2019 και είχε ως αντικείμενο την αναβάθμιση του υφιστάμενου συστήματος RCMS (Risk and Compliance Management System) της ΑΨΑ.

Κατά το 2021, στο αναβαθμισμένο σύστημα iDSAMPL (integrated Digital Security Authority Management Platform):

- Ολοκληρώθηκε η δεύτερη φάση παραμετροποίησης και ανάπτυξης της πλατφόρμας με βάση τις απαιτήσεις του έργου,

- ολοκληρώθηκε μια σειρά εκπαιδεύσεων για τη λειτουργία και δομή του συστήματος, καθώς και για γενικά θέματα αξιολογήσεων κινδύνων, επιχειρησιακής συνέχειας και διαδικασιών ελέγχων (audits),
- οριστικοποιήθηκαν 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, είτε σε εθνικό ή τομεακό επίπεδο,
- συνέχισαν και ολοκληρώθηκαν οι δοκιμαστικοί έλεγχοι στη λειτουργία της πλατφόρμας, και
- ξεκίνησε η ανάπτυξη επιπρόσθετων λειτουργιών και διορθώσεων στην πλατφόρμα, για να είναι όσο πιο εύχρηστη γίνεται κατά τη λειτουργία της.

Η πλατφόρμα iDSAMPL αναμένεται να τεθεί σε πλήρη λειτουργία τους πρώτους μήνες του 2022, λειτουργώντας ως ολοκληρωμένη πλατφόρμα διαχείρισης των εποπτευόμενων οργανισμών στην ΑΨΑ (συμπεριλαμβανομένης της κοινοποίησης περιστατικών). Η ΑΨΑ εξασφάλισε σημαντική χρηματοδότηση (€99.585) για το έργο αυτό από τον HaDEA (Health and Digital 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.

3.3 Οδηγία NIS 2

Στις 16 Δεκεμβρίου 2020, η Ευρωπαϊκή Επιτροπή παρουσίασε την πρόταση της για μια νέα Οδηγία με σκοπό την επίτευξη κοινού υψηλού επιπέδου ασφάλειας στον κυβερνοχώρο σε ολόκληρη την Ευρωπαϊκή Ένωση. Η προτεινόμενη Οδηγία μελετήθηκε σε βάθος από την Αρχή Ψηφιακής Ασφάλειας, η οποία παρακολούθησε στενά τη διαδικασία διαπραγμάτευσης της πρότασης σε Ευρωπαϊκό Επίπεδο και υπέβαλλε ανά τακτά χρονικά διαστήματα τις θέσεις και τις εισηγήσεις της στη Μόνιμη Αντιπροσωπεία της Κυπριακής Δημοκρατίας στην Ευρωπαϊκή Ένωση.

Η συμβιβαστική πρόταση, όπως διαμορφώθηκε μετά από τις εισηγήσεις των Κρατών Μελών, εγκρίθηκε στις 24 Νοεμβρίου 2021 από την COREPER, προχωρώντας στη φάση των τριλόγων. Στη φάση των τριλόγων, η οποία αναμένεται να ολοκληρωθεί εντός του 2022, η Ευρωπαϊκή Επιτροπή, το Ευρωπαϊκό Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο θα παραθέσουν τις εισηγήσεις τους για τη διαμόρφωση συγκεκριμένων σημείων, και θα πραγματοποιηθεί διαβούλευση με τη Γαλλική Προεδρία για την κατάληξη σε συμβιβαστικές προτάσεις. Η ΑΨΑ θα συνεχίσει να παρακολουθεί στενά τις εξελίξεις σχετικά με την πρόοδο διαπραγμάτευσης της Οδηγίας και να συμβάλει στη διαμόρφωση της θέσης της Κυπριακής Δημοκρατίας, σε συνεργασία με τη Μόνιμη Αντιπροσωπεία και το Υφυπουργείο Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής.

4. ΥΛΟΠΟΙΗΣΗ ΣΤΡΑΤΗΓΙΚΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

4.1 Διακυβέρνηση / Συντονισμός Στρατηγικής Κυβερνοασφάλειας

Μετά την αναθεώρηση τον Δεκέμβριο 2020 της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, έγιναν τα ακόλουθα βήματα:

α Δημιουργία των αρμοδίων σωμάτων και ομάδων, με στόχο την καλύτερη εφαρμογή της Στρατηγικής. Στο πλαίσιο αυτό συστάθηκαν οι παρακάτω ομάδες:
- **Εθνικό Συμβούλιο Κυβερνοασφάλειας (National Cybersecurity Council)**, με υψηλόβαθμη εκπροσώπηση από τις κύριες εμπλεκόμενες αρμόδιες αρχές, σε επίπεδο Υπουργού/Διοικητή/Επιτρόπου
- **Συντονιστική Επιτροπή Κυβερνοασφάλειας (Cybersecurity Steering Committee)**, με εκπροσώπηση από τις ίδιες εμπλεκόμενες αρχές όπως στο Εθνικό Συμβούλιο Κυβερνοασφάλειας, σε επίπεδο Γενικών Διευθυντών ή/και Διευθυντών Υπηρεσιών ή/και υπευθύνων τομέων ή/και εξουσιοδοτημένων εκπροσώπων τους, καθώς και αντίστοιχους εκπροσώπους άλλων Αρχών που η συμμετοχή τους κρίνεται χρήσιμη, με απόφαση του Προέδρου και της Συντονιστικής Επιτροπής
- **Ομάδες Εργασίας (Working Groups)**, ανάλογα με τις ανάγκες της εκάστοτε δράσης

β Σύγκλιση Συντονιστικής Επιτροπής Κυβερνοασφάλειας μέσω της πραγματοποίησης έξι συνεδριών οι οποίες έλαβαν χώρα το χρονικό διάστημα Μαρτίου – Νοεμβρίου 2021

γ Συγγραφή των σχεδίων δράσεων και προγραμμάτων εργασίας των θεματικών ενοτήτων της Εθνικής Στρατηγικής Κυβερνοασφάλειας

δ Κατανομή συντονιστών στις δράσεις της Εθνικής Στρατηγικής Κυβερνοασφάλειας

4.2 Υλοποίηση Δράσεων Στρατηγικής Κυβερνοασφάλειας

Εντός του 2021, μέσω των δραστηριοτήτων της ΑΨΑ, ξεκίνησε η υλοποίηση μεγάλου μέρους των δράσεων της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας. Οι Δράσεις αυτές εμπίπτουν στις Θεματικές Ενότητες οι οποίες αναλύονται σε συγκεκριμένες ενότητες αυτής της Έκθεσης, ως ακολούθως:

Πίνακας 3: Θεματικές Ενότητες
Θεματική Ενότητα 1 Δομές και Διακυβέρνηση (βλ. ενότητα 4.2.1)
Θεματική Ενότητα 2 Θεσμοθέτηση της συνεργασίας μεταξύ αρμοδίων δημόσιων φορέων (βλ. ενότητα 4.2.2)
Θεματική Ενότητα 3 Νομικό, Ρυθμιστικό και Πολιτικό Πλαίσιο (βλ. ενότητα 4.2.3)
Θεματική Ενότητα 4 Εθνικό Πλαίσιο Κυβερνοασφάλειας (βλ. ενότητα 4.2.4)
Θεματική ενότητα 5 Αξιολόγηση και Διαχείριση Κινδύνων – Αξιολόγηση Κρισιμότητας (βλ. ενότητα 4.2.5)

Θεματική Ενότητα 6
- Αντιμετώπιση Συμβάντων και Διαχείριση Κρίσεων (βλ. ενότητα4.2.6)

Θεματική Ενότητα 7
- Ανάπτυξη Δυνατοτήτων – Διοργάνωση και Συμμετοχή σε Ασκήσεις (βλ. ενότητα4.2.7)

Θεματική Ενότητα 8
- Ανταλλαγή Πληροφοριών – Επίγνωση Κατάστασης (βλ. ενότητα 4.2.8)

Θεματική Ενότητα 9
- Ενημέρωση – Δημιουργία Κουλτούρας Ασφάλειας (βλ. ενότητα 4.2.9)

Θεματική Ενότητα 10
- Εκπαίδευση και Κατάρτιση (βλ. ενότητα 4.2.10)

Θεματική Ενότητα 11
- Έρευνα και Καινοτομία (βλ. ενότητα 4.2.11)

Θεματική Ενότητα 12
- Συνεργασία με τον Ιδιωτικό Τομέα (βλ. ενότητα 4.2.12)

Θεματική Ενότητα 13
- Ασφάλεια για Όλους (βλ. ενότητα 4.2.13)

Θεματική Ενότητα 14
- Διεθνής Συνεργασία (βλ. ενότητα 4.2.14)

Θεματική Ενότητα 15
- Αντιμετώπιση Αδικημάτων στον Κυβερνοχώρο (βλ. ενότητα 4.2.15)

4.2.1 Θεματική Ενότητα 1 – Δομές και Διακυβέρνηση

Η Θεματική Ενότητα 1 της Στρατηγικής Κυβερνοασφάλειας αφορά τα αρμόδια σώματα και ομάδες που έχουν δημιουργηθεί για την καλύτερη εφαρμογή της Στρατηγικής, καθώς και την αποτελεσματικότερη ανταπόκριση της Κυπριακής Δημοκρατίας έναντι των απειλών του κυβερνοχώρου.

Η δομή που δημιουργήθηκε στο υψηλότερο επίπεδο είναι το Εθνικό Συμβούλιο Κυβερνοασφάλειας, όπου υπάρχει υψηλόβαθμη εκπροσώπηση από τις κύριες εμπλεκόμενες Αρμόδιες Αρχές, σε επίπεδο Υπουργού / Διοικητή / Επιτρόπου. Το Εθνικό Συμβούλιο Κυβερνοασφάλειας παρακολουθεί την εξέλιξη της υλοποίησης της Στρατηγικής Κυβερνοασφάλειας σε τακτά χρονικά διαστήματα (π.χ. κάθε 6 μήνες ή 1 χρόνο), ενημερώνεται για την εκάστοτε κατάσταση της κυβερνοασφάλειας στην Κυπριακή Δημοκρατία, και, όπου απαιτείται, δίνει κατευθυντήριες γραμμές για τη βελτίωση της κυβερνοασφάλειας ευρύτερα. Επίσης, το σώμα αυτό συγκαλείται σε περιπτώσεις μείζονος κρίσης κυβερνοασφάλειας, η οποία επηρεάζει την Κυπριακή Δημοκρατία σε εθνικό επίπεδο, σύμφωνα με τα ισχύοντα σχέδια διαχείρισης κρίσεων της Δημοκρατίας για την κυβερνοασφάλεια.

Η δεύτερη δομή η οποία έχει δημιουργηθεί είναι η Συντονιστική Επιτροπή Κυβερνοασφάλειας, όπου υπάρχει εκπροσώπηση από τις ίδιες εμπλεκόμενες Αρχές όπως στο Εθνικό Συμβούλιο Κυβερνοασφάλειας, σε επίπεδο Γενικών Διευθυντών ή/και Διευθυντών Υπηρεσιών ή/και

υπευθύνων τομέων ή/και εξουσιοδοτημένων εκπροσώπων τους. Στο σώμα αυτό αναγνωρίζονται οι αλληλεξαρτήσεις και διασφαλίζεται η συνεργασία μεταξύ των αρμοδίων αρχών της Δημοκρατίας ώστε, να αξιοποιούνται στο μέγιστο βαθμό οι γνώσεις των ειδικών/τεχνοκρατών στην κάθε Αρχή. Η εν λόγω Επιτροπή εξετάζει επίσης τις αλληλεξαρτήσεις και αλληλοεπιδράσεις μεταξύ των επιμέρους στρατηγικών των Αρμοδίων Αρχών και των δράσεων που προτείνονται ή και προωθούνται για την επιτυχή υλοποίηση τους και την αποφυγή επικαλύψεων. Η Συντονιστική Επιτροπή Κυβερνοασφάλειας πραγματοποιεί συναντήσεις τουλάχιστον σε μηνιαία ή διμηνιαία βάση.

Επίσης, υπάρχουν ομάδες στο τεχνικό επίπεδο, οι οποίες συμβάλουν στη διαχείριση συμβάντων, περιστατικών και κρίσεων κυβερνοασφάλειας.

Εντός του 2022 αναμένεται να ξεκινήσει μελέτη για την ανάδειξη των πιθανών αναγκών δημιουργίας νέων δομών και ενίσχυσης των υφιστάμενων δομών για τη διατήρηση υψηλών επιπέδων κυβερνοασφάλειας στην Κυπριακή Δημοκρατία.

4.2.2 Θεματική Ενότητα 2 – Θεσμοθέτηση της συνεργασίας μεταξύ αρμοδίων δημόσιων φορέων

Η Θεματική Ενότητα 2 της Στρατηγικής Κυβερνοασφάλειας αφορά τη θεσμοθέτηση συνεργασίας μεταξύ των αρμόδιων δημοσίων φορέων. Πρόκειται για την δημιουργία μηχανισμού για τον συντονισμό των Υπουργείων, των Αρμόδιων Αρχών και των εμπλεκομένων κρατικών Υπηρεσιών, στη βάση των δομών που αναφέρονται στη Θεματική Ενότητα 1. Σκοπός είναι η αποτελεσματική επικοινωνία μεταξύ των εμπλεκόμενων φορέων για την καλύτερη δυνατή υλοποίηση των δράσεων της Εθνικής Στρατηγικής.

Κατά το 2021, υπήρχε συνεχής συνεργασία μεταξύ της Αρχής και όλων των εμπλεκομένων φορέων, Υπουργείων και άλλων κρατικών Υπηρεσιών, μέσω συχνών διαδικτυακών και φυσικών συναντήσεων. Ενδεικτικά, στα πλαίσια της Θεματικής Ενότητας 9 που αφορά την ενημέρωση και δημιουργία κουλτούρας ασφάλειας, έγινε σύγκλιση όλων των συντονιστών των δράσεων της Στρατηγικής, εντός των οποίων περιλαμβάνονται δραστηριότητες ενημέρωσης και ευαισθητοποίησης. Σκοπός της συνάντησης ήταν να συγκεντρωθούν εντός της Δράσης 9.1 όλες οι δραστηριότητες που αφορούν ευαισθητοποίηση του κοινού σε θέματα κυβερνοασφάλειας.

Κατά τη διάρκεια του 2022, η Αρχή στοχεύει στη συνέχιση της συνεργασίας της με όλους τους εμπλεκόμενους φορείς, κρατικούς και μη, στην προσπάθεια υλοποίησης και διεκπεραίωσης των δραστηριοτήτων που προβλέπονται στα εκάστοτε σχέδια δράσεων.

4.2.3 Θεματική Ενότητα 3 – Νομικό, Ρυθμιστικό και Πολιτικό Πλαίσιο

Η θεματική Ενότητα 3 της Στρατηγικής Κυβερνοασφάλειας αποσκοπεί στην πλήρη υλοποίηση όλων των προνοιών και του ρυθμιστικού πλαισίου της Οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS), σε όλα τα επίπεδα, με έμφαση στις κρίσιμες υποδομές πληροφοριών και τους φορείς εκμετάλλευσης βασικών υπηρεσιών. Επίσης, η παρούσα Θεματική Ενότητα αποσκοπεί στην ενίσχυση του υφιστάμενου νομικού, κανονιστικού και ρυθμιστικού πλαισίου για την πλήρη ενεργοποίηση και υποστήριξη των προνοιών της Στρατηγικής Κυβερνοασφάλειας, καθώς και τη δημιουργία νέων νομοθεσιών, όπου χρειάζεται. Οι δραστηριότητες αυτές έχουν ως στόχο και σκοπό την ανάπτυξη του νομικού, ρυθμιστικού και πολιτικού πλαισίου για την προστασία ολόκληρης της κοινωνίας από τις απειλές στον κυβερνοχώρο και για την προώθηση ενός ασφαλούς περιβάλλοντος για τη χρήση των νέων τεχνολογιών, σύμφωνα με τις αρχές της συμμετοχικότητας σε ένα περιβάλλον εμπιστοσύνης.

Οι κύριες δραστηριότητες της παρούσας Θεματικής Ενότητας αφορούν την εναρμόνιση της Ευρωπαϊκής Οδηγίας (ΕΕ) 2016/1148 με το Εθνικό Δίκαιο, την εναρμόνιση της Ευρωπαϊκής Οδηγίας

(ΕΕ) 2018/1972 με το Εθνικό Δίκαιο, σχετικά με τα θέματα Ασφάλειας (άρθρο 40 και 41), την αξιολόγηση κρισιμότητας, τη μεταφορά εφαρμόσιμων/εκτελεστικών μέτρων από τον Κανονισμό (ΕΕ) 2019/881 καθώς και την εναρμόνιση της Οδηγίας NIS2 με το Εθνικό Δίκαιο, μόλις αυτή ψηφιστεί από το Ευρωπαϊκό Κοινοβούλιο (βλ. θεματικές ενότητες 3.1).

Επίσης, η παρούσα θεματική ενότητα αποσκοπεί στη διευθέτηση περιλαμβάνονται συντονιστικές δραστηριότητες συντονιστικών δραστηριοτήτων μεταξύ των νομικών ομάδων των αρμοδίωναρμόδιων αρχών και τον νομοτεχνικό έλεγχο σχετικών νομοθεσιών όπου οι αρμόδιες Αρχές χρειάζεται να αλληλοενημερώνονται ή/και να συνεργάζονται ή/και διαβουλεύονται σχετικά με την εξέταση προσχεδίων νομοσχεδίων και την υλοποίηση των Νομοθεσιών που εμπίπτουν στο πλαίσιο της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας. Επιπλέον, η ΑΨΑ προχωρεί με τη σύναψη Μνημονίων Συνεργασίας με τρίτες χώρες, Υπηρεσίες, φορείς και οργανισμούς του Δημόσιου και Ιδιωτικού Τομέα, όσο αφορά στην εξειδικευμένη κατάρτιση για την ερμηνεία και εφαρμογή της Εθνικής και Ευρωπαϊκής Νομοθεσίας στον τομέα της Κυβερνοασφάλειας.

4.2.4 Θεματική Ενότητα 4 – Εθνικό Πλαίσιο Κυβερνοασφάλειας

Η Θεματική ενότητα 4 προβλέπει την ανάπτυξη ενός ολοκληρωμένου Εθνικού Πλαισίου Κυβερνοασφάλειας στην Κυπριακή Δημοκρατία. Το Εθνικό Πλαίσιο Κυβερνοασφάλειας έχει ως στόχο τον καθορισμό του τρόπου με τον οποίο οι διάφορες Υπηρεσίες και Τμήματα της Δημόσιας Υπηρεσίας, αλλά και οι χειριστές κρίσιμων υποδομών πληροφοριών, διαχειρίζονται τους κινδύνους που είναι σχετικοί με την κυβερνοασφάλεια. Το πλαίσιο θα συμβάλει στην πρόληψη συμβάντων στον κυβερνοχώρο τα οποία έχουν δυσμενείς επιπτώσεις σε εθνικό επίπεδο. Ο στόχος είναι να επεκταθεί το υφιστάμενο πλαίσιο έτσι ώστε να μπορεί να χρησιμοποιηθεί από τον κάθε φορέα, ανεξάρτητα από το βαθμό ευαισθησίας των πληροφοριών που χειρίζεται.

Εντός του 2021, η Αρχή Ψηφιακής Ασφάλειας προχώρησε στη μελέτη του εγγράφου κατευθυντήριων γραμμών του ENISA «Guideline on Security Measures under the EECC»[20], το οποίο περιλαμβάνει μέτρα ασφάλειας για τον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και του συμπληρωματικού «5G Supplement»[21]. Περαιτέρω, μελετήθηκαν οι κατευθυντήριες γραμμές του ENISA για το θέμα της κοινοποίησης περιστατικών «Technical Guideline on Incident Reporting under the EECC»[22]. Στη βάση των εν λόγω κατευθυντήριων γραμμών, η ΑΨΑ προχώρησε στην ενημέρωση του νομοθετικού πλαισίου ασφάλειας για τους παροχείς ηλεκτρονικών επικοινωνιών, (βλ. ενότητα3.1.8), αλλά και στην ενημέρωση του οριζόντιου πλαισίου όσον αφορά την κοινοποίηση περιστατικών κυβερνοασφάλειας (βλ. ενότητα 3.1.3).

Η εργασία μελέτης των κατευθυντήριων γραμμών που εκδίδει ο ENISA για τον εμπλουτισμό του Εθνικού Πλαισίου Κυβερνοασφάλειας θα συνεχιστεί και εντός του 2022.

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

Η Θεματική Ενότητα 5 πραγματεύεται την ανάγκη ολοκληρωμένης προσέγγισης της Κυπριακής Δημοκρατίας όσο αφορά στην αναγνώριση, αξιολόγηση και διαχείριση κινδύνων κυβερνοασφάλειας, με ειδική έμφαση στην κατανόηση και αξιολόγηση κρισιμότητας υποδομών και φορέων. Η προσέγγιση που ενδείκνυται για το σωστό σχεδιασμό ενός προγράμματος ασφάλειας, πρέπει να περιλαμβάνει δομημένη μεθοδολογία για την κατανόηση των κινδύνων όπως προβλέπεται στην Οδηγία NIS. Η εφαρμογή αξιολόγησης κινδύνων σε εθνικό επίπεδο, προϋποθέτει ότι πρέπει να αναγνωρίζονται και να κατανοούνται επαρκώς οι κίνδυνοι που είναι δυνατό να επηρεάσουν την Κυπριακή Δημοκρατία σε επίπεδο κράτους. Θα πρέπει να διενεργείται, σε τακτά χρονικά διαστήματα (π.χ. κάθε 2 χρόνια), αξιολόγηση κινδύνων σε εθνικό επίπεδο, για θέματα κυβερνοασφάλειας. Η δραστηριότητα αυτή

[20] *https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc*
[21] *https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc*
[22] *https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc*

ξεκίνησε ήδη στην Κύπρο, και εφαρμόστηκε σε εθνικό επίπεδο για πρώτη φορά την περίοδο 2015-2016, και θα συνεχιστεί κατά την υλοποίηση της παρούσας Στρατηγικής.

Κατά το 2021, εκπονήθηκαν συγκεκριμένα προγράμματα εργασίας για τα θέματα αξιολόγησης κινδύνων σε εθνικό επίπεδο, τα οποία περιλαμβάνουν δραστηριότητες ανάπτυξης μεθοδολογιών αξιολόγησης κρισιμότητας, risk aggregation και διενέργεια σχετικών αξιολογήσεων. Καταρτίστηκε επίσης το πρώτο παραδοτέο, που αφορά στην αναθεωρημένη μεθοδολογία αξιολόγησης κινδύνων σε εθνικό και τομεακό επίπεδο, με τη συμπερίληψη συγκεκριμένου τρόπου συνδυασμού κινδύνων μέσω του risk aggregation.

Οι σχετικές εργασίες θα συνεχιστούν το 2022, με την αναθεώρηση κλιμάκων επιπτώσεων, την αναθεώρηση της συνδεδεμένης μεθοδολογίας για την αξιολόγηση κρισιμότητας εποπτευόμενων φορέων, δοκιμαστικές εφαρμογές του risk aggregation και τη δημιουργία επικαιροποιημένου καταλόγου κρίσιμων υποδομών πληροφοριών στην Κύπρο.

4.2.6 Θεματική Ενότητα 6 – Αντιμετώπιση Συμβάντων και Διαχείριση Κρίσεων

Η Θεματική Ενότητα 6 αποσκοπεί στην αντιμετώπιση συμβάντων και διαχείριση κρίσεων και σχετίζεται με την ανάπτυξη ικανοτήτων και συνεργειών σε εθνικό επίπεδο προκειμένου να διασφαλιστεί η αποτελεσματική διαχείριση και αντιμετώπιση περιστατικών κυβερνοασφάλειας. Πιο συγκεκριμένα, οι δράσεις που περιλαμβάνονται στη συγκεκριμένη θεματική ενότητα αφορούν:

- την περαιτέρω συνεργασία και ανταλλαγή πληροφοριών μεταξύ Εθνικής Αρχής Ασφαλείας και Εθνικού CSIRT-CY, την εδραίωση και ανάπτυξη του Στρατιωτικού (Military) CSIRT, καθώς και την ανάπτυξη μηχανισμών και διαδικασιών (SOPs) συνεργασίας με το Εθνικό CSIRT
- την καθοδήγηση και ανάπτυξη λεπτομερών διαδικασιών και μέτρων που θα λαμβάνονται όταν μια κρίση μεγάλης εμβέλειας επηρεάσει αρνητικά σε μεγάλο βαθμό τη λειτουργία των κρίσιμων υποδομών πληροφορίας στην Κυπριακή Δημοκρατία.

Κατά την εκπόνηση της εν λόγω θεματικής, εντός του 2021, έγινε συνάντηση των εμπλεκόμενων φορέων και προχώρησε η εφαρμογή πιλοτικής πλατφόρμας ανταλλαγής πληροφοριών (Threat Intelligence) στο Στρατιωτικό CSIRT, καθώς επίσης και η εγκατάσταση μηχανογραφικού εξοπλισμού (διακομιστές, υπολογιστές, τηλεοράσεις, δικανικό εργαστήριο).

Κατά το 2022 θα πραγματοποιηθεί πραγματοποιήθηκε συνάντηση για την επικαιροποίηση των σχεδίων έκτακτης ανάγκης/αντιμετώπισης κρίσεων σε θέματα κυβερνοασφάλειας και προγραμματίζεται η συμμετοχή της ΑΨΑ σε πανευρωπαϊκή άσκηση κυβερνοασφάλειας στον τομέα της υγείας.

4.2.7 Θεματική Ενότητα 7 – Ανάπτυξη Δυνατοτήτων – Διοργάνωση και Συμμετοχή σε Ασκήσεις

Η υλοποίηση της θεματικής Ενότητας 7, που αφορά στην ανάπτυξη δυνατοτήτων / διοργάνωση και συμμετοχή σε ασκήσεις, βασίζεται σε δύο βασικούς πυλώνες:

- την ανάπτυξη και προώθηση μέτρων, προγραμμάτων και δραστηριοτήτων για την ανάπτυξη πραγματικών ικανοτήτων κυβερνοασφάλειας στους οργανισμούς που διαχειρίζονται κρίσιμες υποδομές πληροφοριών, καθώς και σε άλλους οργανισμούς και εταιρείες, όπου κρίνεται αναγκαίο,
- τον προγραμματισμό και τη διοργάνωση τακτικών εθνικών ασκήσεων για την κυβερνοασφάλεια, στη βάση ρεαλιστικών σεναρίων, καθώς και την ενεργή συμμετοχή σε πανευρωπαϊκές και άλλες διεθνείς ασκήσεις.

Εντός του 2021 και στα πλαίσια υλοποίησης των ανωτέρω δράσεων πραγματοποιήθηκαν συναντήσεις μεταξύ των συντονιστικών φορέων για επικαιροποίηση των υφιστάμενων πολιτικών και διαδικασιών

και για ανάπτυξη του τρόπου συνεργασίας για το μέλλον.

Κατά το 2022 αναμένεται μεταξύ άλλων η διοργάνωση ή/και συμμετοχή σε ασκήσεις σε διμερές και τριμερές επίπεδο, καθώς και η συμμετοχή σε πανευρωπαϊκές ασκήσεις για κάθε επίπεδο εμπλοκής (Στρατηγικό, Επιχειρησιακό και Τακτικό).

4.2.8 Θεματική Ενότητα 8 – Ανταλλαγή Πληροφοριών – Επίγνωση Κατάστασης

Στόχος της Θεματικής Ενότητας 8 είναι η δημιουργία των συνθηκών και διαύλων συνεργασίας και ανταλλαγής πληροφοριών διατομεακά, μεταξύ οργανισμών, με την Αρχή Ψηφιακής Ασφάλειας και όπου αλλού χρειάζεται, για αποτελεσματικότερη ενημέρωση και συντονισμό όσον αφορά την ανταπόκριση σε απειλές και συμβάντα στον κυβερνοχώρο. Επιπλέον, μέσω της συγκεκριμένης θεματικής, θα προωθηθεί η δημιουργία ενός δυναμικού PPP (Public Private Partnership) στον τομέα της ανταλλαγής πληροφοριών, με τη συνδρομή όλων των εμπλεκόμενων φορέων κρίσιμων υποδομών πληροφοριών και των αρμοδίων Αρχών του κράτους.

Παράλληλα, στα πλαίσια εκπόνησης της εν λόγω θεματικής, θα αναπτυχθεί ένας ολιστικός μηχανισμός επίγνωσης της κατάστασης για την ανταλλαγή πληροφοριών και τη συνεργασία σε πραγματικό χρόνο, με τη συμβολή όλων των εμπλεκομένων φορέων.

Κατά το 2021 πραγματοποιήθηκαν συναντήσεις μεταξύ των συντονιστικών φορέων για το σχεδιασμό και τη δημιουργία δικτύου ασφαλούς επικοινωνίας για την ανταλλαγή πληροφοριών και την ενίσχυση της επίγνωσης κατάστασης αναφορικά με θέματα κυβερνοασφάλειας.

4.2.9 Θεματική Ενότητα 9 – Ενημέρωση – Δημιουργία Κουλτούρας Ασφάλειας

Το πεδίο δράσης της Θεματικής Ενότητας 9 θα έχει ως στόχο την προώθηση επίγνωσης και κουλτούρας ασφάλειας όλων των χρηστών συστημάτων επικοινωνίας, πληροφοριών και υπηρεσιών διαδικτύου, σε συνεργασία με όλους τους εμπλεκόμενους φορείς και τα ενδιαφερόμενα μέρη, σε όλο το εύρος της κυπριακής κοινωνίας. Ειδικότερα, οι δράσεις που περιλαμβάνονται αποσκοπούν στην ενημέρωση και ευαισθητοποίηση όλων των χρηστών των συστημάτων επικοινωνίας και πληροφοριών και των υπηρεσιών διαδικτύου με τις απαραίτητες εκείνες ικανότητες (γνώσεις, στάσεις και δεξιότητες), οι οποίες θα συμβάλουν στην επίτευξης ενός ικανοποιητικού επιπέδου ενημέρωσης και επιμόρφωσης για τις πιθανές απειλές κυβερνοασφάλειας και την εξασφάλιση της εγρήγορσης και ανταπόκρισης έναντι των σχετικών προκλήσεων, απειλών και κινδύνων.

Εντός του 2021 και στα πλαίσια υλοποίησης της συγκεκριμένης δράσης, πραγματοποιήθηκαν συναντήσεις με συντονιστικούς φορείς άλλων δράσεων της εθνικής στρατηγικής προκειμένου να διασφαλισθεί ότι έχουν συγκεντρωθεί εντός της παρούσας Θεματικής Ενότητας όλες οι δραστηριότητες που σχετίζονται με θέματα ενημέρωσης και ευαισθητοποίησης του κοινού. Παράλληλα, έγινε διαχωρισμός των δραστηριοτήτων σε εκείνες που αφορούν, συγκεκριμένα, το ακροατήριο παιδιά-γονείς-εκπαιδευτικοί, και σε εκείνες που αφορούν το ευρύτερο σύνολο της κοινωνίας. Επιπρόσθετα, η Αρχή Ψηφιακής Ασφάλειας, στα πλαίσια του συγχρηματοδοτούμενου ευρωπαϊκού προγράμματος CYberSafety[23], συμμετέχει ενεργά στην ευαισθητοποίηση του κοινού μέσα από επιμορφωτικά σεμινάρια που απευθύνονται σε παιδιά, γονείς και καθηγητές και στόχο έχουν την διαρκή εγρήγορσή τους σε ζητήματα κυβερνοασφάλειας.

Εντός του 2022 αναμένεται η δημιουργία/συνέχιση των εκστρατειών ενημέρωσης και ευαισθητοποίησης του κοινού, καθώς και η διοργάνωση ημερίδων και διαλέξεων γύρω από θέματα που αφορούν την ασφάλεια στον κυβερνοχώρο. Επιπλέον, η Αρχή Ψηφιακής Ασφάλειας θα παρέχει τεχνογνωσία σε φορείς και Υπηρεσίες που έχουν αναλάβει το συντονισμό ανάλογων σεμιναρίων και απευθύνονται σε όλο το φάσμα της κοινωνίας.

[23] *https://cybersafety.cy/en/*

4.2.10 Θεματική Ενότητα 10 – Εκπαίδευση και Κατάρτιση

Η Θεματική Ενότητα 10 στοχεύει στην ανάπτυξη κατάλληλου ανθρώπινου δυναμικού το οποίο θα έχει τις απαραίτητες τεχνικές γνώσεις και πιστοποιήσεις για την άρτια εφαρμογή των προνοιών της Στρατηγικής, μεσοπρόθεσμα και μακροπρόθεσμα. Επιπλέον στόχος είναι η ενσωμάτωση των γνώσεων αυτών στα Σχέδια Υπηρεσίας για σχετικές θέσεις εργασίας, καθώς επίσης και η προώθηση ενεργειών για την κατάλληλη εκπαίδευση και κατάρτιση προσωπικού.

Εντός του 2021 και στα πλαίσια της εν λόγω δράσης, ολοκληρώθηκαν οι ακόλουθες ενέργειες:

α Πραγματοποιήθηκε ανάληψη συντονιστικού ρόλου:
- από πλευράς Παιδαγωγικού Ινστιτούτου, στα θέματα που αφορούν τη Σχολική Εκπαίδευση
- από πλευράς Διεύθυνσης Ανώτερης Εκπαίδευσης του Υπουργείου Παιδείας, στα θέματα που αφορούν την Ακαδημαϊκή Εκπαίδευση, και
- από πλευράς Αρχής Ψηφιακής Ασφάλειας, στα θέματα που αφορούν την Κατάρτιση και Πιστοποίηση

β Έγινε η συγγραφή του προσχεδίου της δράσης για τον σαφή καθορισμό των ενεργειών και δραστηριοτήτων που πρέπει να ολοκληρωθούν, σε καθορισμένο χρονικό διάστημα, προκειμένου να έρθει εις πέρας η εν λόγω δράση.

γ Εστάλησαν προσκλήσεις για τη συμμετοχή των φορέων στις ομάδες εργασίας και συλλέχθηκαν οι απαντητικές επιστολές προκειμένου να γίνει η σύγκλιση των ομάδων και υπο-ομάδων εργασίας.

Εντός του 2022, αναμένεται να γίνει σύγκλιση των ομάδων και υπο-ομάδων εργασίας προκειμένου να προχωρήσει η υλοποίηση των σχετικών δραστηριοτήτων. Αναμένεται επίσης να ξεκινήσει η χαρτογράφηση της υφιστάμενης κατάστασης σε θέματα που σχετίζονται με την κυβερνοασφάλεια, τόσο στη σχολική και ακαδημαϊκή εκπαίδευση όσο και στα θέματα πιστοποίησης και κατάρτισης. Τα αποτελέσματα της εκάστοτε αποτύπωσης θα συμπεριληφθούν σε μία έκθεση/αναφορά η όποια ενδέχεται να δημοσιευθεί. Επιπλέον, θα ξεκινήσει η διαδικασία προκειμένου να καταρτισθούν, αρχικά τα προφίλ των αποφοίτων και στη συνέχεια τα προφίλ των επαγγελματιών, έτσι ώστε να καθοριστούν, με σαφή τρόπο, οι γνώσεις και δεξιότητες που απαιτούνται από τον καθένα σε θέματα κυβερνοασφάλειας.

4.2.11 Θεματική Ενότητα 11 – Έρευνα και Καινοτομία

Η συγκεκριμένη ενότητα πραγματεύεται την υποστήριξη και την προώθηση της παραγωγής έρευνας και καινοτομίας στην Κυπριακή Δημοκρατία στον τομέα της κυβερνοασφάλειας, και τον σχεδιασμό και την ανάπτυξη «οικοσυστημάτων» για την αξιοποίηση των συνεργειών που δημιουργούνται από τη δεσπόζουσα θέση της Κύπρου σε τομείς όπου παρουσιάζεται αυξημένη δραστηριότητα, όπως τους τομείς των οικονομικών υπηρεσιών, της ναυτιλίας και της ενέργειας. Η δράση έχει, επίσης, ως στόχο την προσέλκυση εταιρειών τεχνολογίας και κυβερνοασφάλειας και τη δραστηριοποίηση τους στην Κύπρο.

Κατά το 2021, ξεκίνησε η ανάπτυξη του σχεδίου της Αρχής, σε συνεργασία με το Υπουργείο Άμυνας, για την χρηματοδότηση της έρευνας και καινοτομίας στην Κύπρο. Επίσης, έγινε προσπάθεια για προώθηση ευρημάτων, τεχνολογιών και εργαλείων που σχετίζονται με την κυβερνοασφάλεια. Επιπρόσθετα, η Αρχή εντάχθηκε και συμμετείχε σε διάφορα σεμινάρια και παρευρέθηκε σε συναντήσεις με την ευρύτερη Ευρωπαϊκή κοινότητα που είχαν θέμα την έρευνα και καινοτομία σε θέματα κυβερνοασφάλειας.

Για το 2022, η Αρχή προγραμματίζει την οριστικοποίηση προγραμμάτων χρηματοδότησης για θέματα έρευνας στον τομέα της κυβερνοασφάλειας, τη συνέχιση της προώθησης νέων ευρημάτων,

τεχνολογιών και εργαλείων που σχετίζονται με την κυβερνοασφάλεια, τη δημιουργία πλατφόρμας ενημέρωσης του ευρύτερου κοινού, καθώς και τη συνέχιση της συνεργασίας της με την ευρύτερη Ευρωπαϊκή ερευνητική κοινότητα μέσω των χρηματοδοτικών προγραμμάτων της Ευρωπαϊκής Ένωσης. Το Εθνικό Κέντρο Συντονισμού για θέματα Κυβερνοασφάλειας (National Cybersecurity Coordination Centre - NCCC-CY) βλ. ενότητα 7) είναι ένα από τα προγράμματα χρηματοδότησης για θέματα έρευνας και καινοτομίας στον τομέα της κυβερνοασφάλειας που θα αναπτυχθεί το έτος 2022 -.

4.2.12 Θεματική Ενότητα 12 – Συνεργασία με τον Ιδιωτικό Τομέα

Η συγκεκριμένη θεματική ενότητα αφορά την ανάπτυξη συνεργασίας με τον ιδιωτικό τομέα, τη σύναψη επίσημης εταιρικής σχέσης δημόσιου-ιδιωτικού τομέα (PPP – Public Private Partnership), και την επίτευξη επιμέρους στόχων σε θέματα ενημέρωσης, καινοτομίας, εκπαίδευσης και κατάρτισης. Στο πλαίσιο της Θεματικής Ενότητας 12, πραγματοποιείται διεύρυνση των σχέσεων με τον ιδιωτικό τομέα, με σκοπό την προώθηση και την ενίσχυση της ασφάλειας στον κυβερνοχώρο για τις επιχειρήσεις.

Εντός του 2021 πραγματοποιήθηκαν συναντήσεις με την ηγεσία του ΚΕΒΕ, στο πλαίσιο της οποίας καθορίστηκαν οι διάφοροι τομείς όπου θα μπορούσε να αναπτυχθεί συνεργασία μεταξύ της Αρχής Ψηφιακής Ασφάλειας και του ιδιωτικού τομέα. Συζητήθηκε η προώθηση του "Cybersecurity Made in Europe Label"[24] στην Κύπρο, ενός θεσμού που οργανώνεται από τον Ευρωπαϊκό Οργανισμό Κυβερνοασφάλειας (ECSO – European Cyber Security Organisation), ο οποίος στοχεύει στην προώθηση των ευρωπαϊκών εταιρειών που ασχολούνται με τον τομέα της κυβερνοασφάλειας τόσο στην ευρωπαϊκή όσο και στην παγκόσμια αγορά. Παράλληλα, το ΚΕΒΕ και η ΑΨΑ προχώρησαν σε μελέτη για την καταγραφή της ανάγκης και του ενδιαφέροντος των επιχειρήσεων για διοργάνωση σεμιναρίων κατάρτισης για θέματα κυβερνοασφάλειας. Η ομάδα εργασίας έχει συλλέξει τα δεδομένα και θα προχωρήσει σε έκδοση σχετικής αναφοράς και σε προγραμματισμό των σεμιναρίων εντός του 2022.

Επίσης, εντός του 2022 σχεδιάζεται να γίνει περαιτέρω ανάπτυξη συνεργειών μεταξύ της ΑΨΑ και του ιδιωτικού τομέα. Η ΑΨΑ έχει αναλάβει το ρόλο του Εθνικού Κέντρου Συντονισμού για θέματα κυβερνοασφάλειας (βλ. ενότητα 7), συνεπώς έχει την ευθύνη για το συντονισμό της Εθνικής Κοινότητας Κυβερνοασφάλειας και για την κατανομή των χρηματοδοτήσεων που θα εξασφαλίζονται από το ECCC (Ευρωπαϊκό Κέντρο Αρμοδιότητας Κυβερνοασφάλειας)[25] στο τοπικό οικοσύστημα και ιδιαίτερα στις μικρομεσαίες επιχειρήσεις. Ακόμη, η ΑΨΑ θα ενημερώνει τους ενδιαφερόμενους φορείς και τις επιχειρήσεις σχετικά με τις εξελίξεις στο ECCC και τις ευκαιρίες χρηματοδότησης τους μέσω των δράσεων των Ευρωπαϊκών Προγραμμάτων «Ορίζοντας Ευρώπη» και «Ψηφιακή Ευρώπη», οι οποίες σχετίζονται με τον τομέα της Κυβερνοασφάλειας.

4.2.13 Θεματική Ενότητα 13 – Ασφάλεια για Όλους

Η Στρατηγική Κυβερνοασφάλειας προσεγγίζει τα θέματα ασφάλειας στον κυβερνοχώρο ολιστικά. Πέραν από την προστασία των Βασικών Υπηρεσιών των Κρίσιμων Υποδομών Πληροφοριών, θα πρέπει να λαμβάνονται υπόψη και να στηρίζονται οι μικρομεσαίες επιχειρήσεις, καθώς και οι πολίτες της χώρας. Η ευαισθητοποίηση σχετικά με τις απειλές και τους κινδύνους ασφάλειας στον κυβερνοχώρο, αλλά και τον αντίκτυπό τους στην κοινωνία, έχει καταστεί ζωτικής σημασίας. Μέσω της ευαισθητοποίησης, οι πολίτες και οι εταιρικοί χρήστες μπορούν να μάθουν πώς να συμπεριφέρονται στον ηλεκτρονικό κόσμο και να προστατεύονται από τους τυπικούς κινδύνους. Η παρούσα Θεματική Ενότητα περιλαμβάνει σημαντικές δράσεις για την ασφάλεια του Διαδικτύου των Πραγμάτων (Internet of Things), καθώς και την εφαρμογή κατάλληλων σχημάτων για την πιστοποίηση κυβερνοασφάλειας σε προϊόντα και υπηρεσίες που έχουν ευρεία χρήση.

Κατά το 2021, οι σχετικές δραστηριότητες εστιάστηκαν στην ανάπτυξη και ενδυνάμωση των δομών και διαδικασιών πιστοποίησης, ώστε η Κυπριακή Δημοκρατία να μπορέσει να παρέχει υπηρεσίες

[24] *https://ecs-org.eu/initiatives/cybersecurity-made-in-europe*
[25] *https://cybersecurity-centre.europa.eu/index_en*

πιστοποίησης κυβερνοασφάλειας προϊόντων και υπηρεσιών, κυρίως μέσω της συμμετοχής της ΑΨΑ σε δύο σχετικά συγχρηματοδοτούμενα προγράμματα που έχει εξασφαλίσει από την Ευρωπαϊκή Ένωση (βλ. ενότητες 9.1.3 και 9.1.4). Επίσης, ο Επίτροπος Επικοινωνιών και στελέχη της ΑΨΑ, επισκέφθηκαν Ευρωπαϊκές χώρες με ανεπτυγμένες δομές πιστοποίησης (Γαλλία και Γερμανία), με στόχο την παρουσίαση της Κυπριακής προσέγγισης και την ανταλλαγή βέλτιστων πρακτικών.

Οι σχετικές εργασίες θα συνεχιστούν το 2022, με τη συνεχιζόμενη ανάπτυξη των ικανοτήτων πιστοποίησης στην Κύπρο, καθώς και με την εκπόνηση συγκεκριμένου προγράμματος εργασίας για την ασφάλεια του Διαδικτύου των Πραγμάτων.

4.2.14 Θεματική Ενότητα 14 – Διεθνής Συνεργασία

Η συγκεκριμένη Θεματική Ενότητα έχει ως στόχο την καλή συνεργασία της Κυπριακής Δημοκρατίας με τα υπόλοιπα κράτη μέλη της Ευρωπαϊκής Ένωσης, αλλά και τρίτες χώρες, μέσω της εκπροσώπησης και της ενεργού συμμετοχής της ΑΨΑ στις σχετικές ομάδες εργασίας. Επίσης, αποσκοπεί στον καθορισμό των μακροπρόθεσμων στόχων της διεθνούς συνεργασίας, αναπτύσσοντας συνέργειες με τις εμπλεκόμενες Αρμόδιες Αρχές και οργανισμούς σε Εθνικό, Ευρωπαϊκό και Διεθνές επίπεδο.

Εντός του 2021 πραγματοποιήθηκαν κοινές εκπαιδεύσεις με το European Security and Defence College (ESDC)[26] και συμμετοχή σε ομάδες εργασίας σε Ευρωπαϊκό επίπεδο. Επίσης, υπογράφτηκαν Μνημόνια Συνεργασίας / Συναντίληψης με χώρες εκτός Ευρωπαϊκής Ένωσης (βλ. ενότητα8.2).

4.2.15 Θεματική Ενότητα 15 – Αντιμετώπιση Αδικημάτων στον Κυβερνοχώρο

Η Θεματική Ενότητα 15 περιλαμβάνει συγκεκριμένες δραστηριότητες που αφορούν κυρίως την αντιμετώπιση αδικημάτων στον κυβερνοχώρο. Συγκεκριμένα, προβλέπει την:

- παρακολούθηση του Νομικού Πλαισίου και των πρωτοβουλιών σε Ευρωπαϊκό Επίπεδο σχετικά με την διατήρηση και απόκτηση ηλεκτρονικών / ψηφιακών αποδεικτικών στοιχείων που θα βοηθήσει στην αποτελεσματική διερεύνηση των υποθέσεων,
- ανάπτυξη των ικανοτήτων του προσωπικού, με την παράλληλη αναβάθμιση του χώρου εργασίας και των μέσων διερεύνησης, καθώς και την περαιτέρω εκπαίδευση του προσωπικού,
- στοχευμένη ενημέρωση όλων των οργανωμένων συνόλων για σκοπούς πρόληψης των αδικημάτων που διαπράττονται στον κυβερνοχώρο,
- ενίσχυση της συνεργασίας μεταξύ του δημόσιου και ιδιωτικού τομέα κατά τη διερεύνηση ποινικών υποθέσεων.

Εντός του 2021 υπήρχε συνεχής συνεργασία μεταξύ της ΑΨΑ και της Αστυνομίας Κύπρου για την αντιμετώπιση αδικημάτων στον κυβερνοχώρο.

Επίσης, πραγματοποιήθηκαν εκπαιδεύσεις και σεμινάρια:

- στον τραπεζικό τομέα, για τη διαχείριση κίνδυνων καθώς και την προώθηση εκπαιδευτικού και ενημερωτικού υλικού για πρόληψη και διαχείριση σχετικών απειλών,
- σε σχολεία, που απευθυνόταν σε μαθητές και εκπαιδευτικούς για την εκπαίδευση και ανάπτυξη δεξιοτήτων για την ασφαλή χρήση του Διαδικτύου,
- στο ανθρώπινο δυναμικό της Αστυνομίας Κύπρου, για την εξασφάλιση της εγρήγορσης και ανταπόκρισης έναντι των σχετικών προκλήσεων, απειλών και κινδύνων στον κυβερνοχώρο.

Κατά το 2022 αναμένεται, μεταξύ άλλων, η διοργάνωση ή/και συμμετοχή σε εκπαιδευτικά σεμινάρια και πανευρωπαϊκές ασκήσεις όλων των εμπλεκόμενων φορέων (δημόσιων και ιδιωτικών) για την καλύτερη και αποτελεσματικότερη διερεύνηση ποινικών υποθέσεων. Επίσης, αναμένεται η δημιουργία / συνέχιση των εκστρατειών ενημέρωσης και ευαισθητοποίησης του κοινού καθώς

[26] *https://esdc.europa.eu/*

και η διοργάνωση ημερίδων και διαλέξεων γύρω από θέματα που αφορούν την ασφάλεια στον κυβερνοχώρο.

4.3 Διεξαγωγή Αξιολόγησης Ωριμότητας Κυβερνοασφάλειας για την Κυπριακή Δημοκρατία

Η εφαρμογή της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, από το 2013 και μετά, είχε ως αποτέλεσμα την επίτευξη αρκετών σημαντικών στόχων για την Κύπρο στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων τη δημιουργία της Αρχής Ψηφιακής Ασφάλειας, η οποία περιλαμβάνει και το Εθνικό CSIRT-CY. Κατά το 2017, διενεργήθηκε ολοκληρωμένη αξιολόγηση της κατάστασης στην Κύπρο σε σχέση με τον τομέα της κυβερνοασφάλειας, βάσει επιστημονικού μοντέλου που αναπτύχθηκε από το Πανεπιστήμιο της Οξφόρδης στο Ηνωμένο Βασίλειο (Capacity Maturity Model for Nations – CMM)[27]. Η διαδικασία αυτή οδήγησε σε αποτύπωση των επιπέδων ωριμότητας σε διάφορους τομείς της κυβερνοασφάλειας, και στην καταγραφή μεγάλου αριθμού συστάσεων για βελτίωση. Στη συνέχεια, αναθεωρήθηκε η Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, η οποία δημοσιεύθηκε τον Δεκέμβριο 2020.

Η ΑΨΑ ξεκίνησε τον Ιούλιο 2021 έργο αξιολόγησης ωριμότητας κυβερνοασφάλειας με το Πανεπιστήμιο της Οξφόρδης, για επικαιροποίηση των αποτελεσμάτων της προηγούμενης αξιολόγησης που διενεργήθηκε το 2017, λαμβάνοντας υπόψη τις σημαντικές εξελίξεις και τα επιτεύγματα των τελευταίων χρόνων που έχει πετύχει η Κυπριακή Δημοκρατία, όπως τη δημιουργία της Αρχής Ψηφιακής Ασφάλειας και του Εθνικού CSIRT-CY. Η διαδικασία αυτή διενεργήθηκε με βάση το επιστημονικό μοντέλο που αναπτύχθηκε από το Πανεπιστήμιο της Οξφόρδης (Capacity Maturity Model for Nations – CMM). Θα λειτουργήσει υποστηρικτικά σε σχέση με την υλοποίηση των Δράσεων της αναθεωρημένης Στρατηγικής Κυβερνοασφάλειας, παρέχοντας αντικειμενική πληροφόρηση και καλύτερη κατανόηση όσον αφορά στους τομείς όπου θα πρέπει να δοθεί περισσότερη έμφαση κατά την υλοποίηση.

Οι ερευνητές από το Πανεπιστήμιο της Οξφόρδης μελέτησαν μεγάλο όγκο διαθέσιμων εγγράφων και δημόσια διαθέσιμων πληροφοριών, και διεξήγαγαν συζητήσεις στρογγυλής τραπέζης στις 21-23/9/21 με σημαντικό αριθμό εκπροσώπων εμπλεκομένων μερών από οργανισμούς του δημόσιου τομέα, νομοθέτες, υπεύθυνους χάραξης πολιτικής, Αρχές επιβολής του νόμου, τον τομέα της άμυνας, πανεπιστήμια, μη-κυβερνητικούς οργανισμούς, παρόχους ηλεκτρονικών επικοινωνιών, τράπεζες, καθώς και την καθοδηγητική ομάδα για την ανάπτυξη και συντονισμό της Στρατηγικής Κυβερνοασφάλειας.

[27] *https://gcscc.ox.ac.uk/the-cmm*

5. ΔΙΑΧΕΙΡΙΣΗ ΣΥΜΒΑΝΤΩΝ ΚΑΙ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

5.1 Διαχείριση Περιστατικών

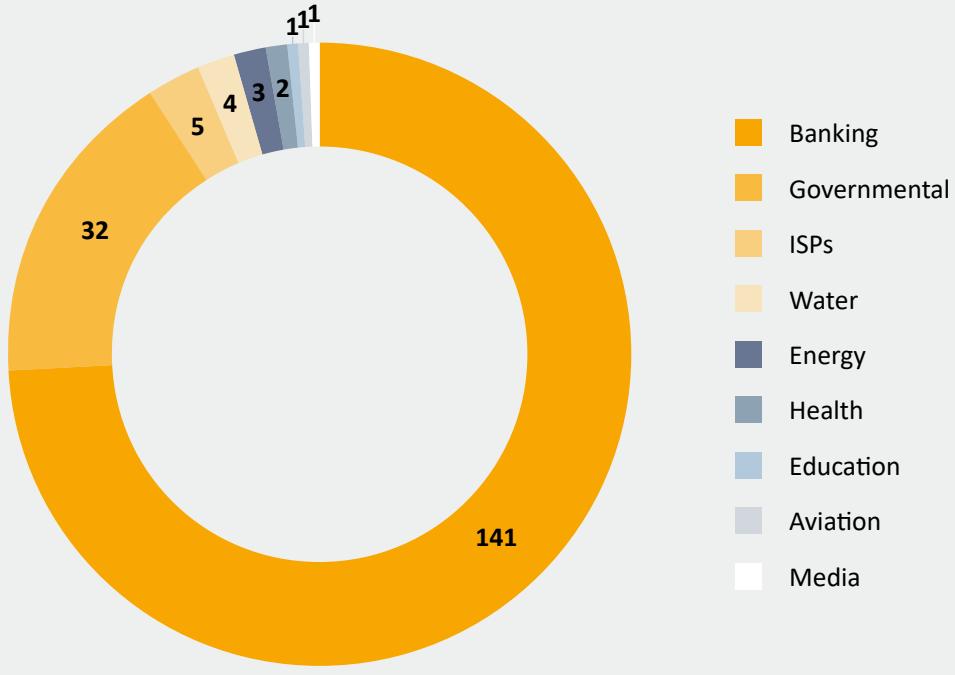
Το Εθνικό CSIRT-CY, από τη στιγμή εντοπισμού ενός περιστατικού έως και την επίλυσή του, εφαρμόζει ένα σύνολο διαδικασιών οι οποίες έχουν τύχει αξιολόγησης και έχουν εγκριθεί από διεθνείς και ευρωπαϊκούς οργανισμούς, όπως το FIRST[28], ο TI[29] και ο ENISA[30].Αρχικά, ενεργοποιείται η Διαδικασία Καταχώρησης Περιστατικού και ακολουθεί η Διαδικασία Διαχείρισης Περιστατικού η οποία αποτελείται από τα ακόλουθα στάδια:

α Ανάθεση χειριστή περιστατικού και κλιμάκωση (αν χρειάζεται)
β Ανάλυση περιστατικού
γ Δικανική ανάλυση
δ Μετριασμός περιστατικού
ε Συντονισμός και υποβολή αναφορών
στ Κλείσιμο περιστατικού
ζ 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.

Συνολικά το 2021, λόγω της πανδημίας COVID-19, το Εθνικό CSIRT-CY έλαβε αυξημένο αριθμό κοινοποιήσεων περιστατικών που σχετίζονται με επιθέσεις Phishing (190 κοινοποιήσεις). Οι περισσότερες κοινοποιήσεις αφορούσαν τον τραπεζικό τομέα και σχετίζονταν με κακόβουλους συνδέσμους που υποδύονταν χρηματοπιστωτικά ιδρύματα και υπηρεσίες διαδικτυακών συναλλαγών. Επιπλέον, έγιναν κοινοποιήσεις περιστατικών που περιλάμβαναν phishing domains και είχαν ως θέμα την πανδημία του COVID-19.

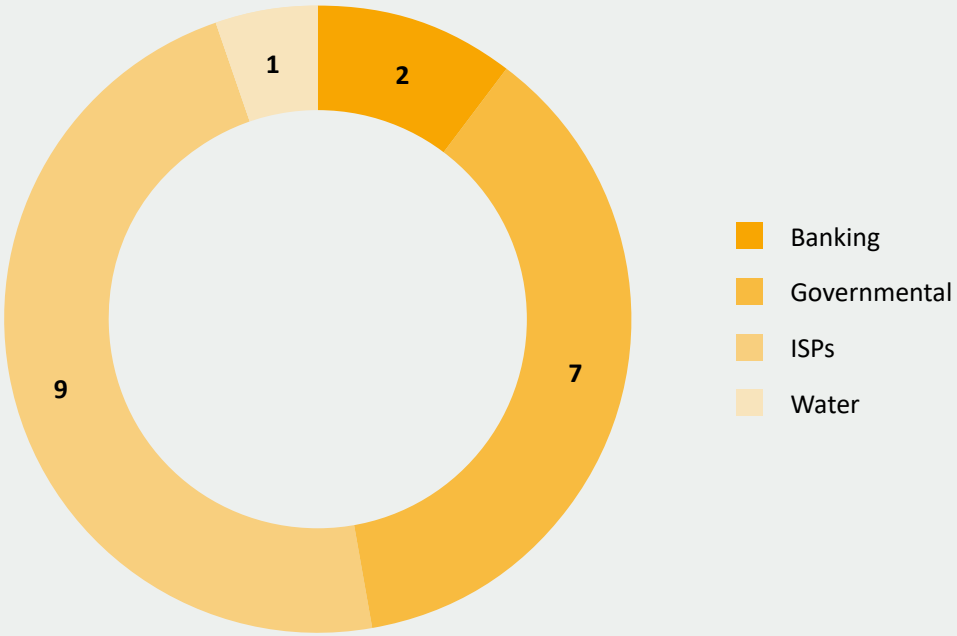
Γράφημα 3: Phishing



Σημείωση: Αφορά αριθμητικές υποθέσεις

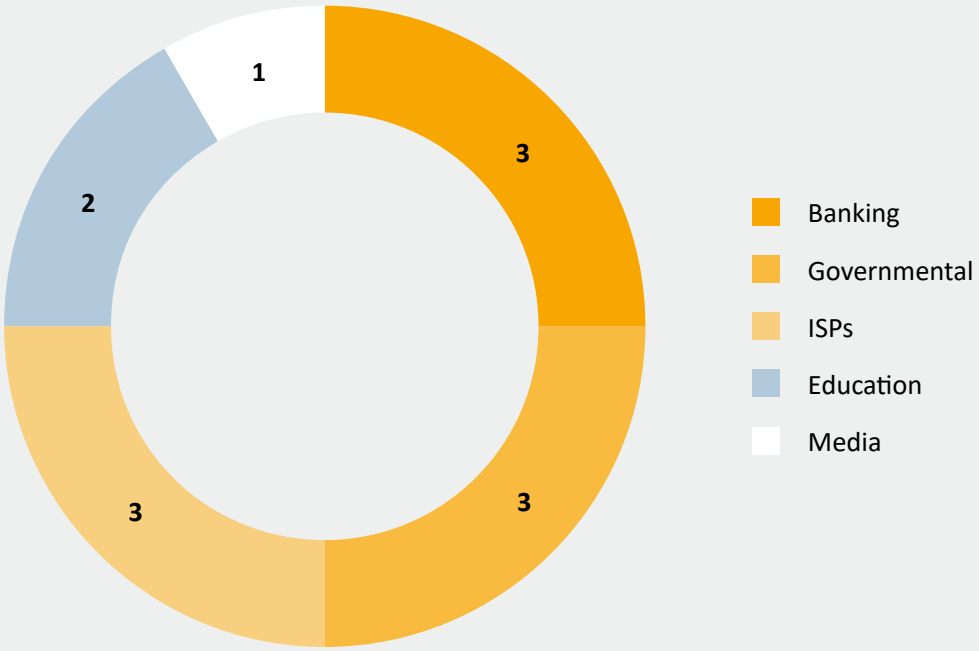
[28] *FIRST: Forum of Incident Response and Security Teams*
[29] *TI: Trusted Introducer*
[30] *https://www.enisa.europa.eu/*

Γράφημα 4: Malicious Code



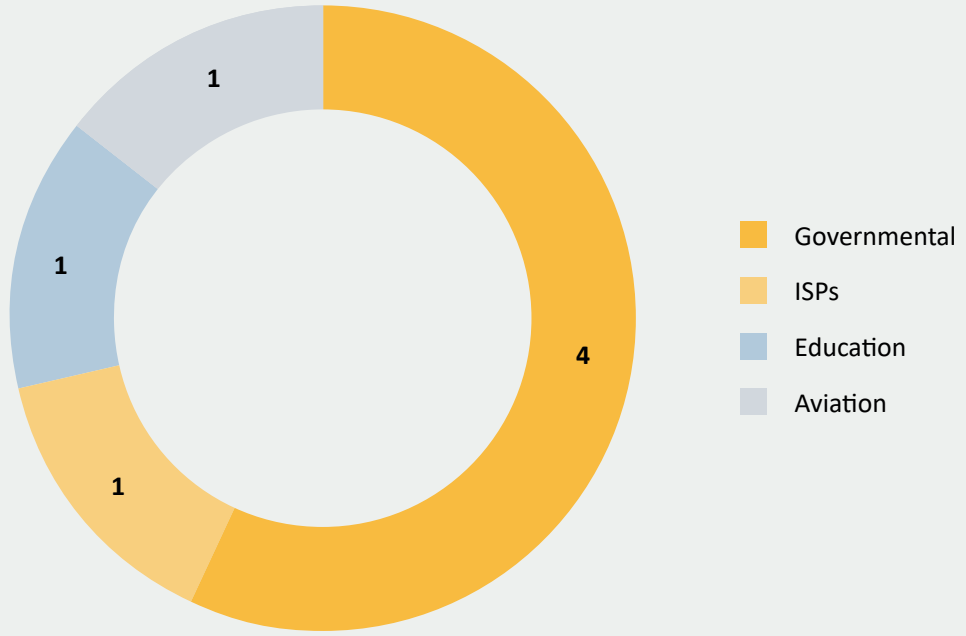
Σημείωση: Αφορά αριθμητικές υποθέσεις

Γράφημα 5: Unauth. Access to Information



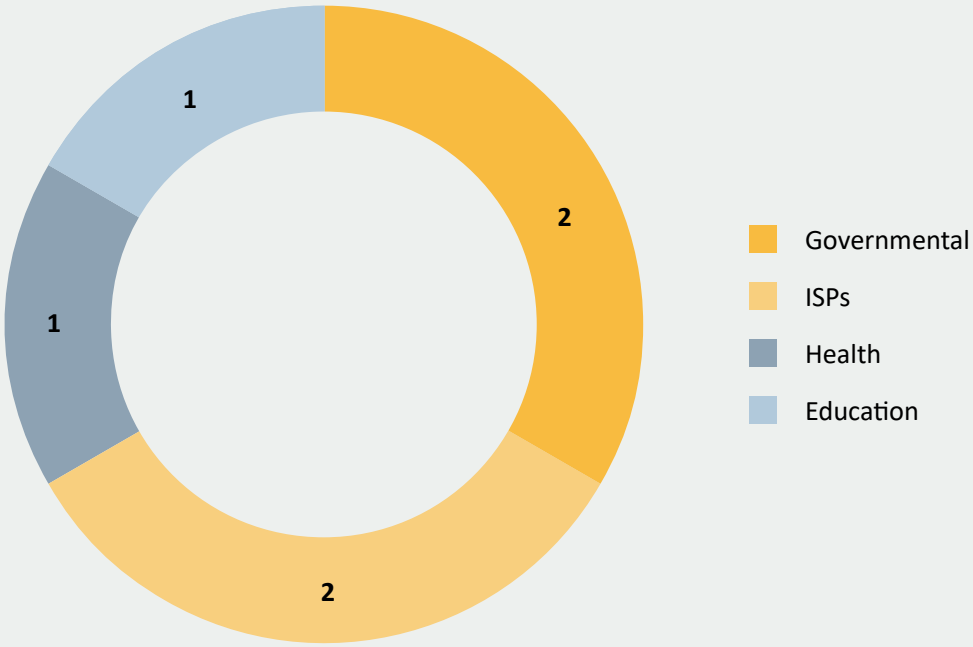
Σημείωση: Αφορά αριθμητικές υποθέσεις

Γράφημα 6: Intrusion Attempt



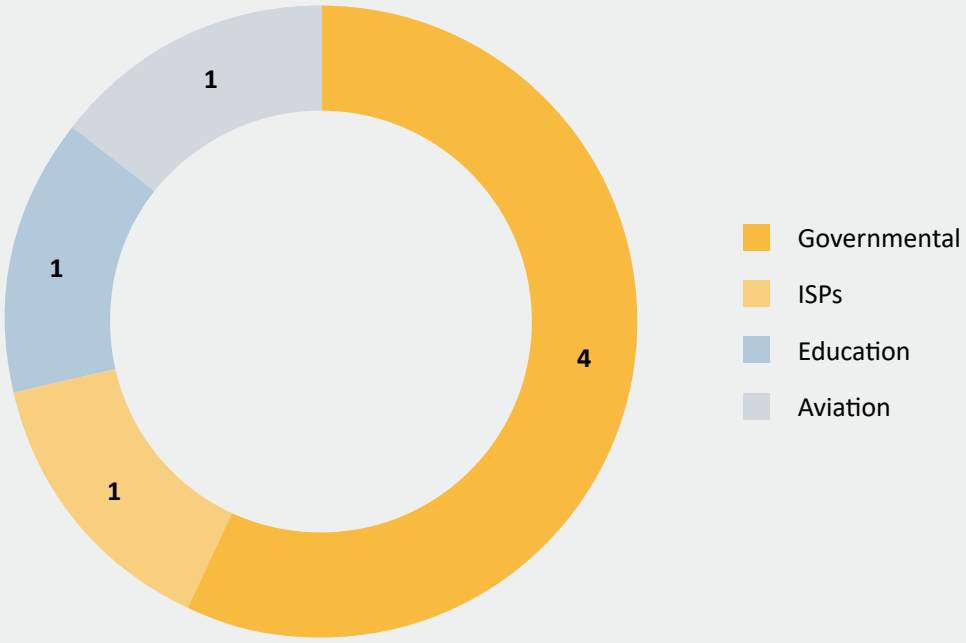
Σημείωση: Αφορά αριθμητικές υποθέσεις

Γράφημα 7: Vulnerability Exploitation



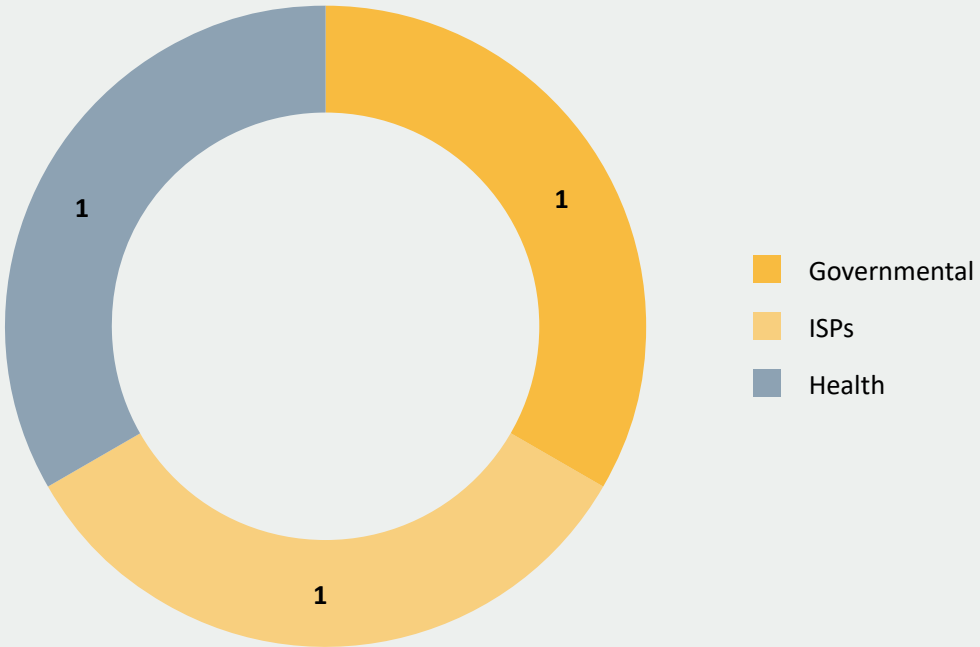
Σημείωση: Αφορά αριθμητικές υποθέσεις

Γράφημα 8: Impersonation



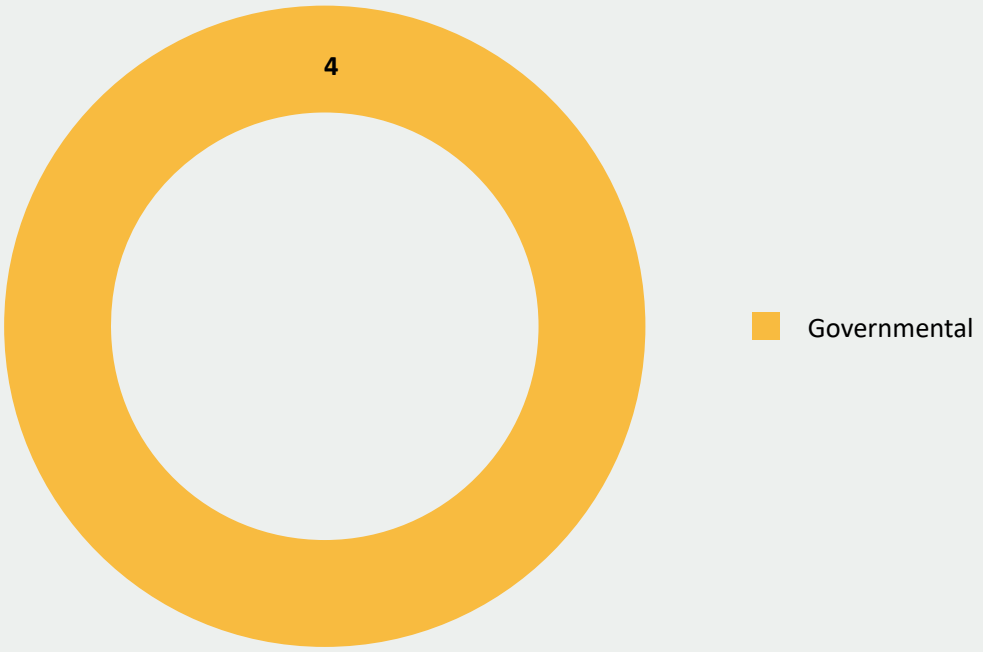
Σημείωση: Αφορά αριθμητικές υποθέσεις

Γράφημα 9: DDoS



Σημείωση: Αφορά αριθμητικές υποθέσεις

Γράφημα 10: Ransomware



Σημείωση: Αφορά αριθμητικές υποθέσεις

Πέραν των ανωτέρω αναφορών, και εντός του 2021, το Εθνικό CSIRT–CY χειρίστηκε περιστατικά σε διάφορους φορείς τα οποία ενέπιπταν στις κατηγορίες Malware, Distributed Denial of Service (DDoS) και Malvertising.

Κατά το έτος 2021, το Εθνικό CSIRT-CY έλαβε 21.984 ηλεκτρονικά μηνύματα ως ειδοποιήσεις από τις πλατφόρμες συλλογής πληροφοριών.

Μετά από σχετική ανάλυση των μηνυμάτων και την εξεύρεση βημάτων μετριασμού, το Εθνικό CSIRT-CY διαβίβασε περί των 3000 ηλεκτρονικών μηνυμάτων προς τις κρίσιμες υποδομές πληροφοριών που περιείχαν 146.016 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 συμβάντων (events) στις οποίες εμπίπτει το καταγεγραμμένο συμβάν, 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[31] 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 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[32] (τα οποία μπορούν να αποτελέσουν τη βάση για την αξιολόγηση πολλών από τους προβλεπόμενους τύπους προϊόντων/υπηρεσιών, τις υπηρεσίες νεφοϋπολογιστικής, εξοπλισμούς και υποδομές δικτύων ηλεκτρονικών επικοινωνιών πέμπτης γενεάς (5G) 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.

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

[32] ***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 Εθνικό Πλαίσιο

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 έπρεπε να εφαρμοστεί μέχρι τον Ιούνιο του 2021. Η ΑΨΑ ετοίμασε και προώθησε τις απαραίτητες αλλαγές στην πρωτογενή νομοθεσία της, ώστε να έχει τις κατάλληλες αρμοδιότητες και εξουσίες για να επιτελέσει το ρόλο της ως ΕΑΠΚ. Αναμένεται να ολοκληρωθεί εντός του 2022.

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" (βλ. ενότητα 9.1.3). Το έργο αυτό έχει ως στόχο την ολοκληρωμένη ανάπτυξη των δυνατοτήτων της Κυπριακής Δημοκρατίας, ώστε να είναι δυνατή η προσφορά ενός ευρέως φάσματος υπηρεσιών πιστοποίησης της Κυβερνοασφάλειας σε προϊόντα, υπηρεσίες και διαδικασίες. Το έργο αυτό ολοκληρώθηκε εντός του 2021, με τις ακόλουθες δραστηριότητες:

- Συντονισμός εμπλεκομένων φορέων
- Αύξηση επιχειρησιακών ικανοτήτων (παραγωγή καλών πρακτικών και καθοδήγησης για τη διαπίστευση και εποπτεία των οργανισμών αξιολόγησης της συμμόρφωσης)
- Διενέργεια πιλοτικών πιστοποιήσεων σε Κύπρο και Γαλλία
- Οργάνωση, συντονισμός, ετοιμασία παρουσιάσεων διοργάνωση αποστολής σε ANSSI Γαλλίας και BSI Γερμανίας

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.

Επίσης, κατά το 2021, η ΑΨΑ πέτυχε επιπρόσθετη σημαντική συγχρηματοδότηση από την Ευρωπαϊκή Ένωση (πρόγραμμα A4CEF - Advancing Cybersecurity Certification Capabilities with Cross-border exchange and Enhancing (business) Flows – βλ. ενότητα 9.1.4). Το έργο ξεκίνησε τον Ιούλιο 2021, και αναμένεται να ολοκληρωθεί εντός του 2023, εστιάζοντας κυρίως στην περαιτέρω ανάπτυξη των σχετικών ικανοτήτων της ΑΨΑ και την επέκταση των δραστηριοτήτων της, και στην πιστοποίηση υπηρεσιών νεφοϋπολογιστικής.

7. ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ - NCCC-CY

Στις 20 Μαΐου 2021, εγκρίθηκε ο Κανονισμός (ΕΕ) 2021/887 (Κανονισμός) για τη σύσταση του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας (Ευρωπαϊκό Κέντρο Αρμοδιότητας)[33] και του Δικτύου Εθνικών Κέντρων Συντονισμού. Το Ευρωπαϊκό Κέντρο Αρμοδιότητας αποτελεί μια νέα ευρωπαϊκή οντότητα, η οποία στοχεύει στην αύξηση των ικανοτήτων και στην προώθηση της ανταγωνιστικότητας στον τομέα της κυβερνοασφάλειας στην Ευρώπη. Το Ευρωπαϊκό Κέντρο Αρμοδιότητας θα έχει την ευθύνη για τη διαχείριση των κεφαλαίων για την κυβερνοασφάλεια στο πλαίσιο του πολυετούς δημοσιονομικού πλαισίου 2021-2027 και θα συμβάλει στη δημιουργία ενός διασυνδεδεμένου βιομηχανικού και ερευνητικού οικοσυστήματος κυβερνοασφάλειας σε ολόκληρη την ΕΕ. Για την επίτευξη των πιο πάνω στόχων θα συνεργάζεται στενά με ένα Δίκτυο Εθνικών Κέντρων Συντονισμού για την οικοδόμηση μιας ισχυρής κοινότητας κυβερνοασφάλειας.

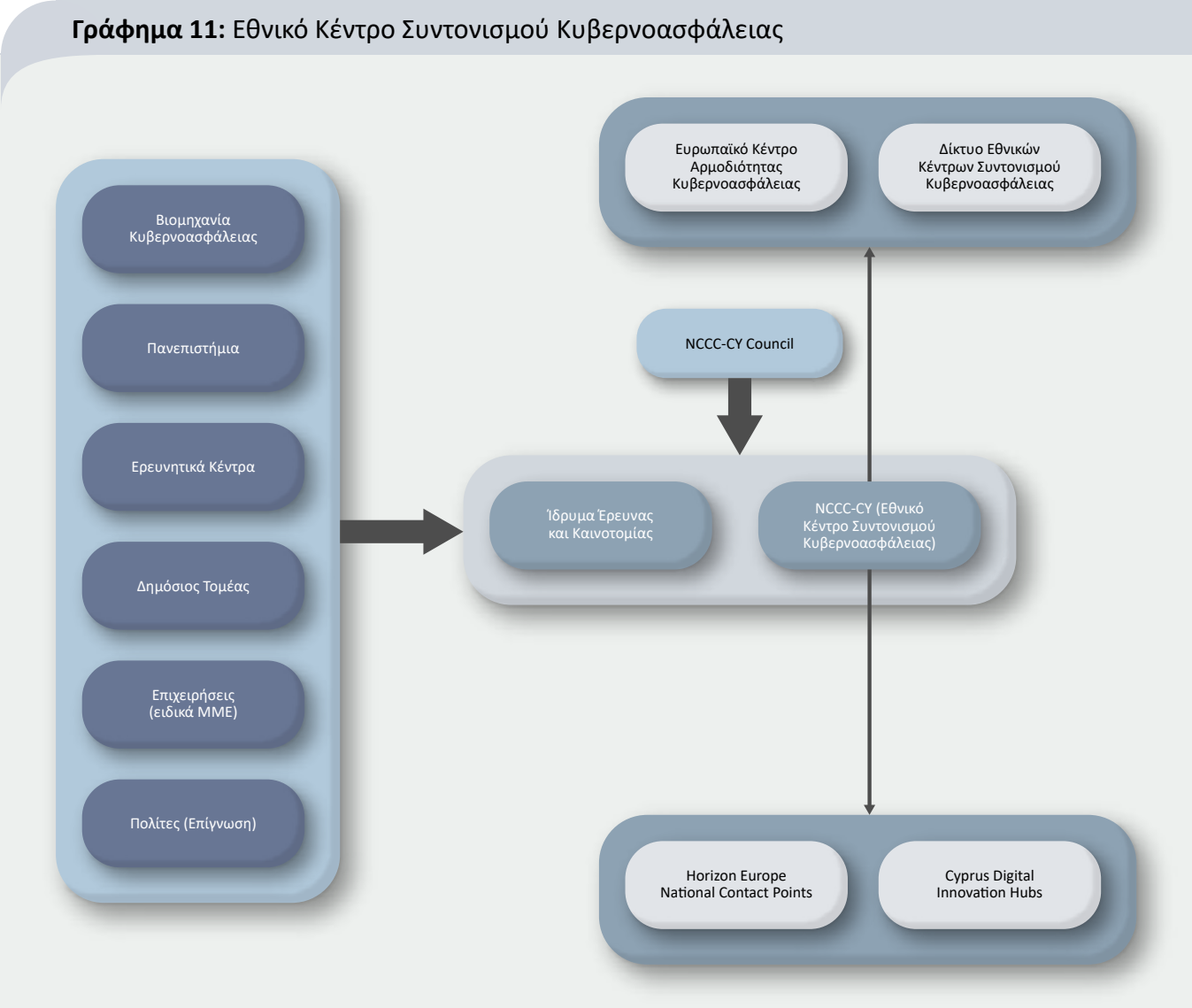
Συνεπώς, σύμφωνα και με το Άρθρο 6(1) του Κανονισμού, τα Κράτη Μέλη έχουν την υποχρέωση να ορίσουν μια οντότητα η οποία θα ενεργεί ως Εθνικό Κέντρο Συντονισμού για θέματα Κυβερνοασφάλειας. Με απόφαση του Υπουργικού Συμβουλίου ημερομηνίας 21 Δεκεμβρίου 2021, η Αρχή Ψηφιακής Ασφάλειας ορίστηκε ως το Εθνικό Κέντρο Συντονισμού για θέματα Κυβερνοασφάλειας στην Κυπριακή Δημοκρατία (National Cybersecurity Coordination Centre - NCCC-CY), ενώ το Ίδρυμα Έρευνας και Καινοτομίας ορίστηκε ως μέλος της κοινοπραξίας του Εθνικού Κέντρου Συντονισμού, με καθήκοντα Οικονομικού Διαχειριστή. Δηλαδή, το Ίδρυμα Έρευνας και Καινοτομίας θα έχει την ευθύνη για τη διαχείριση και κατανομή των χρηματοδοτήσεων που θα εξασφαλίζει το Εθνικό Κέντρο Συντονισμού μέσω των Ευρωπαϊκών προγραμμάτων.

Βασική αποστολή του Εθνικού Κέντρου Συντονισμού είναι να παρέχει γνώση και να διευκολύνει την πρόσβαση σε τεχνογνωσία για βιομηχανικά, τεχνολογικά και ερευνητικά θέματα κυβερνοασφάλειας. Το NCCC-CY θα ενεργεί ως το σημείο επαφής σε εθνικό επίπεδο για την Κοινότητα Κυβερνοασφάλειας και θα υποστηρίζει το Ευρωπαϊκό Κέντρο Αρμοδιότητας στην εκπλήρωση της αποστολής και των στόχων του.

Κύριο μέλημα του NCCC-CY είναι να διασφαλίσει ότι όλα τα ενδιαφερόμενα μέρη, και ιδίως οι μικρομεσαίες επιχειρήσεις, έχουν επαρκή υποστήριξη και πρόσβαση στη γνώση και στα αποτελέσματα της έρευνας και ανάπτυξης στον τομέα της κυβερνοασφάλειας, με στόχο να καταστούν επαρκώς ασφαλείς. Το Κέντρο θα αναλάβει δράσεις για να βοηθήσει τις μικρομεσαίες επιχειρήσεις στην Κύπρο να είναι ενεργές, ανταγωνιστικές και ικανές να συνεισφέρουν σημαντικά στην ηγετική θέση της Ευρωπαϊκής Ένωσης στον τομέα της κυβερνοασφάλειας. Το όραμα είναι να καταστεί η Κυπριακή Δημοκρατία ως πρωτοπόρος στον τομέα της κυβερνοασφάλειας, διασφαλίζοντας έναν αξιόπιστο και προστατευμένο κυβερνοχώρο για όλους τους πολίτες και τις επιχειρήσεις.

[33] *https://cybersecurity-centre.europa.eu/index_en*

Γράφημα 11: Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας



Σύμφωνα με το Άρθρο 7 του Κανονισμού, το NCCC-CY έχει τις ακόλουθες αρμοδιότητες:

- να στηρίζει το Ευρωπαϊκό Κέντρο Αρμοδιότητας Κυβερνοασφάλειας στην επίτευξη της αποστολής και των στόχων του, ιδίως όσον αφορά τον συντονισμό της Κοινότητας Κυβερνοασφάλειας σε εθνικό επίπεδο, ενεργώντας ως σημείο επαφής,
- να παρέχει εμπειρογνωμοσύνη και να συμβάλλει ενεργά στα στρατηγικά καθήκοντα που αναφέρονται στο Άρθρο 5 του Κανονισμού, λαμβάνοντας υπόψη τις σχετικές εθνικές και περιφερειακές προκλήσεις για την κυβερνοασφάλεια σε διάφορους τομείς,
- να προωθεί, ενθαρρύνει και διευκολύνει τη συμμετοχή της κοινωνίας των πολιτών, των επιχειρήσεων (ιδίως των νεοφυών επιχειρήσεων και των ΜΜΕ), της ακαδημαϊκής και ερευνητικής κοινότητας, και άλλων ενδιαφερομένων μερών σε εθνικό επίπεδο σε διασυνοριακά έργα και τις σχετικές με την κυβερνοασφάλεια δράσεις που χρηματοδοτούνται μέσω των σχετικών προγραμμάτων της Ευρωπαϊκής Ένωσης,
- να παρέχει τεχνική βοήθεια στα ενδιαφερόμενα μέρη, στηρίζοντάς τα κατά το στάδιο υποβολής της αίτησής τους για έργα που διαχειρίζεται το Ευρωπαϊκό Κέντρο Αρμοδιότητας Κυβερνοασφάλειας,
- να επιδιώκει συνέργειες με συναφείς δραστηριότητες σε εθνικό, περιφερειακό και τοπικό επίπεδο, όπως με τις εθνικές πολιτικές για την έρευνα, την ανάπτυξη και την καινοτομία στον τομέα της κυβερνοασφάλειας, ιδίως με τις πολιτικές που αναφέρονται στην Εθνική Στρατηγική Κυβερνοασφάλειας,

- να υλοποιεί ειδικές δράσεις οι οποίες έχουν λάβει επιχορηγήσεις από το Κέντρο Αρμοδιότητας, μεταξύ άλλων, μέσω της οικονομικής ενίσχυσης τρίτων σύμφωνα με το Άρθρο 204 του Δημοσιονομικού Κανονισμού (ΕΕ) 2018/1046, με την επιφύλαξη των αρμοδιοτήτων της καθώς και άλλων αρμοδίων Αρχών στη Δημοκρατία σχετικά με την εκπαίδευση και λαμβανομένων υπόψη των σχετικών καθηκόντων του ENISA, να συνεργάζεται με τις εθνικές αρχές σχετικά με πιθανή συμβολή στην προώθηση και τη διάδοση εκπαιδευτικών προγραμμάτων κυβερνοασφάλειας,
- να προωθεί και να διαδίδει τα σχετικά αποτελέσματα των εργασιών του δικτύου των Εθνικών Κέντρων Συντονισμού, της Κοινότητας Κυβερνοασφάλειας και του Ευρωπαϊκού Κέντρου Αρμοδιότητας Κυβερνοασφάλειας σε εθνικό, περιφερειακό ή τοπικό επίπεδο,
- να αξιολογεί τις αιτήσεις που υποβάλλουν οντότητες εγκατεστημένες στη Δημοκρατία για να γίνουν μέλη της Κοινότητας Κυβερνοασφάλειας,
- να στηρίζει και να προωθεί τη συμμετοχή συναφών οντοτήτων στις δραστηριότητες που προκύπτουν στους κόλπους του Ευρωπαϊκού Κέντρου Αρμοδιότητας Κυβερνοασφάλειας, του δικτύου των Εθνικών Κέντρων Συντονισμού και της Κοινότητας Κυβερνοασφάλειας, και να παρακολουθεί το επίπεδο δέσμευσης προς την έρευνα, τις εξελίξεις και την ανάπτυξη εφαρμογών κυβερνοασφάλειας, καθώς και το ποσό των δημόσιων επιχορηγήσεων σε αυτούς τους τομείς.

Εντός του 2022, το NCCC-CY θα προβεί στις απαραίτητες ενέργειες και θα αναπτύξει τις κατάλληλες διαδικασίες ώστε να είναι σε θέση να ανταποκριθεί αποτελεσματικά στα καθήκοντα και τις αρμοδιότητες του. Παράλληλα, το NCCC-CY θα υποβάλει αίτηση έτσι ώστε να αξιολογηθεί από την Ευρωπαϊκή Επιτροπή ως ικανό να διαχειρίζεται ευρωπαϊκές χρηματοδοτήσεις. Στόχος είναι το NCCC-CY να διεκδικήσει σημαντική χρηματοδότηση μέσω της δράσης «Deploying The Network Of National Coordination Centres With Member States» του προγράμματος «Ψηφιακή Ευρώπη», την οποία θα κατανέμει στο εθνικό οικοσύστημα κυβερνοασφάλειας.

8. 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 3.3), την Ομάδα Συνεργασίας (NIS Cooperation Group) και το δίκτυο συνεργασίας CSIRT (CSIRTs 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.

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

8.1.1 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, στάλθηκαν επιστολές προς τον κάθε Φορέα Εκμετάλλευσης Βασικών Υπηρεσιών («ΦΕΒΥ») και Φορέα Κρίσιμων Υποδομών Πληροφοριών («ΦΚΥΠ») («Φορείς»), οι οποίοι ορίστηκαν ως ΦΕΒΥ και ΦΚΥΠ μετά την αξιολόγηση κρισιμότητας που διενήργησε η Αρχή εντός του 2018 και το 2021 (βλ. θεματική ενότητα 3.1.7)

Η Αρχή Ψηφιακής Ασφάλειας, με στόχο την άσκηση των αρμοδιοτήτων και εξουσιών της, κατ' εφαρμογή του Άρθρου 19 του Νόμου Ν. 89(Ι)/2020, ζήτησε από τους Φορείς να ορίσουν ή/και να επικαιροποιήσουν τα άτομα που όρισαν το 2020 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 τα άτομα για την κοινοποίηση στην ΑΨΑ περιστατικών παραβίασης ασφάλειας.

Επίσης, η ΑΨΑ απέστειλε στους Φορείς που ορίστηκαν για πρώτη φορά ως ΦΕΒΥ και ΦΚΥΠ, 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 ΦΕΒΥ και ΦΚΥΠ έχουν υποχρέωση να συμβάλουν στη χρηματοδότηση της λειτουργίας της Αρχής. Η ΑΨΑ ενημέρωσε όλους τους Φορείς για την ενεργοποίηση της διαδικασίας είσπραξης τελών για το έτος 2022, 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).

8.1.2 Ενέργειες από Εθνικό CSIRT-CY

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

Για την επίτευξη του στόχου αυτού, το Εθνικό CSIRT-CY:

α Σχεδίασε και υλοποίησε την εγκατάσταση εξειδικευμένων αισθητήρων σε υποδομή SOC (Security Operations Centre) του Εθνικού CSIRT-CY, οι οποίοι προσφέρουν ελέγχους ασφαλείας σε πραγματικό χρόνο – βασισμένοι σε πρωτόκολλα δικτύου για ανίχνευση και ανάλυση ύποπτων και κακόβουλων ενεργειών, στις Κρίσιμες Υποδομές Πληροφοριών, με σκοπό την έγκαιρη προειδοποίηση περιστατικών κυβερνοασφάλειας.

β Σχεδίασε και υλοποίησε υποδομή και πλατφόρμα περιβάλλοντος κατάρτισης, το οποίο υποστηρίζει τη δημιουργία ρεαλιστικών δικτύων και υποδομών τεχνολογίας πληροφοριών, με στόχο τη δημιουργία και την ανάπτυξη ασκήσεων κυβερνοασφάλειας σε διάφορους τομείς, συμπεριλαμβανομένων της Ναυτιλίας, Ενέργειας και ηλεκτρονικών επικοινωνιών.

γ Εφάρμοσε αυτοματοποιημένα κανάλια πληροφόρησης για τη δημιουργία αυτόματων και χειροκίνητων αναφορών και ειδοποιήσεων προς τις Κρίσιμες Υποδομές Πληροφοριών.

8.2 Συνεργασία με Κρατικές Αρχές

8.2.1 Μνημόνιο Συνεργασίας με Ανοιχτό Πανεπιστήμιο Κύπρου

Μετά από σχετικές επαφές και συζητήσεις που έγιναν εντός του 2021 μεταξύ του Ανοικτού Πανεπιστημίου Κύπρου [Ερευνητικό Εργαστήριο Κυβερνοασφάλειας και Τηλεπικοινωνιών] και της Αρχής Ψηφιακής Ασφάλειας, άρχισαν οι διεργασίες για τη Σύναψη Μνημονίου Συνεργασίας για τη δημιουργία συστήματος έγκαιρης προειδοποίησης, διαχείρισης συμβάντων, εκπαίδευσης και κατάρτισης.

Σκοπός του Μνημονίου είναι ο καθορισμός του πλαισίου συνεργασίας μεταξύ των Μερών για τη δημιουργία συστήματος έγκαιρης προειδοποίησης, διαχείρισης συμβάντων, εκπαίδευσης και κατάρτισης και για τη διερεύνηση και την ανάπτυξη ικανοτήτων ευαισθητοποίησης σε καταστάσεις άμυνας, μέσω δραστηριοτήτων κατάρτισης και εκπαίδευσης υψηλής ποιότητας σύμφωνα με τα ευρήματα και τα αποτελέσματα του έργου και έχοντας υπόψη τις ανάγκες σε διάφορες υποδομές πληροφοριών ζωτικής σημασίας. Επίσης, σκοπός του Μνημονίου είναι ο καθορισμός του πλαισίου συνεργασίας μεταξύ των Μερών για την υποστήριξη των στρατηγικών στόχων οι οποίοι περιλαμβάνονται στη Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας όσον αφορά την πρόοδο ανάλυσης κυβερνοαπειλών στον κυβερνοχώρο της Κύπρου και η οποία σχετίζεται με τη λειτουργία υποδομών ζωτικής σημασίας πληροφοριών και την ανάπτυξη κατάλληλου προσωπικού ασφαλείας στον κυβερνοχώρο, την υποστήριξη των στρατηγικών στόχων, καθώς και ο καθορισμός του πλαισίου συνεργασίας που θα διέπει τη σχέση, τις διαδικασίες, τα πνευματικά δικαιώματα των παραδοτέων του έργου και άλλα συναφή θέματα, όπως αυτά καθορίζονται στο υπό αναφορά Μνημόνιο.

Το υπό αναφορά Μνημόνιο θα αντικαταστήσει το Μνημόνιο που υπογράφτηκε το 2020 μεταξύ της Αρχής Ψηφιακής Ασφάλειας και του Ανοικτού Πανεπιστημίου Κύπρου – Εργαστήριο Κυβερνοασφάλειας και Τηλεπικοινωνιών.

Εντός του 2022, αναμένεται ότι το Μνημόνιο θα υπογραφεί.

8.2.2 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, συνέχισε να αναπτύσσεται εντός του 2021 και αναμένεται να ολοκληρωθεί εντός του 2022.

8.2.3 Μνημόνιο Συνεργασίας με Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως

Το Μάη του 2021 υπεγράφη Μνημόνιο Συνεργασίας μεταξύ του Υπουργείου Δικαιοσύνης και Δημοσίας Τάξεως (ΥΔΔΤ), της Αστυνομίας Κύπρου (Υποδιεύθυνση Ηλεκτρονικού Εγκλήματος) και της Αρχής Ψηφιακής Ασφάλειας. Σκοπός του εν λόγω Μνημονίου είναι ο καθορισμός του πλαισίου συνεργασίας μεταξύ των προαναφερόμενων Υπηρεσιών σε θέματα τα οποία άπτονται της καταπολέμησης ηλεκτρονι

8.2.4 Μνημόνιο Συνεργασίας με Κεντρική Τράπεζα Κύπρου

Εντός του 2021, συνεχίστηκαν οι επαφές και οι συζητήσεις που άρχισαν εντός του 2020 μεταξύ της Κεντρικής Τράπεζας και της Αρχής Ψηφιακής Ασφάλειας για τη σύναψη Μνημονίου Συνεργασίας για σκοπούς κοινοποίησης περιστατικών κυβερνοασφάλειας ή/και ψηφιακής ασφάλειας που θα αποστέλλει η Κεντρική Τράπεζα (υποχρεωτικές και εθελοντικές κοινοποιήσεις) στην Αρχή Ψηφιακής Ασφάλειας.

Εντός του 2022, αναμένεται ότι το Μνημόνιο θα υπογραφεί.

8.2.5 Μνημόνιο Συνεργασίας με το Τμήμα Πολιτικής Αεροπορίας

Εντός του 2021 και μετά από σχετικές επαφές και συζητήσεις που έγιναν μεταξύ του Τμήματος Πολιτικής Αεροπορίας και της Αρχής Ψηφιακής Ασφάλειας ξεκίνησαν οι διεργασίες για τη σύναψη Μνημονίου Συνεργασίας στους ακόλουθους τομείς:

- ανταλλαγή πληροφοριών,
- επιχειρησιακή συνεργασία,
- εφαρμογή σχεδιασμών διαχείρισης κρίσεων, και
- τεχνική υποστήριξη, σχετικά με θέματα στον τομέα της κυβερνοασφάλειας.

Εντός του 2022, αναμένεται ότι το Μνημόνιο θα υπογραφεί.

8.2.6 Μνημόνιο Συνεργασίας με Πανεπιστήμιο Κύπρου

Στις 3 Νοεμβρίου 2021 υπογράφηκε Μνημόνιο Συνεργασίας μεταξύ της Αρχής Ψηφιακής Ασφάλειας και του Πανεπιστημίου Κύπρου.

Σκοπός του Μνημονίου Συνεργασίας ήταν η σύναψη Συμφωνίας Ερευνητικής Συνεργασίας για την ανάπτυξη μιας πλατφόρμας Cyber Threat Intelligence. Η πλατφόρμα θα πραγματοποιεί σαρώσεις του εθνικού διαδικτυακού χώρου με σκοπό τη συλλογή, αποθήκευση και επεξεργασία δεδομένων για τον εντοπισμό ευπαθειών και κακόβουλων προγραμμάτων.

Η υπογραφή της Συμφωνίας Ερευνητικής Συνεργασίας μεταξύ της ΑΨΑ και του Πανεπιστημίου Κύπρου πραγματοποιήθηκε στις 27 Δεκεμβρίου 2021, και η ανάπτυξη του έργου αναμένεται να ολοκληρωθεί μέχρι το τέλος του 2023.

8.2.7 Μνημόνιο Συνεργασίας με την Εθνική Αρχή Στοιχημάτων

Τον Αύγουστο του 2021 υπεγράφη το Μνημόνιο Συνεργασίας μεταξύ της Εθνικής Αρχής Στοιχημάτων και της Αρχής Ψηφιακής Ασφάλειας. Σκοπός του υπό αναφορά Μνημονίου είναι ο καθορισμός του πλαισίου συνεργασίας μεταξύ της Εθνικής Αρχής Στοιχημάτων και της Αρχής Ψηφιακής Ασφάλειας σε θέματα που αφορούν τη διαχείριση περιστατικών κυβερνοασφάλειας ή/και ψηφιακής ασφάλειας, την ενίσχυση του επιπέδου κυβερνοασφάλειας της Εθνικής Αρχής Στοιχημάτων, καθώς και την ανταλλαγή πληροφοριών, τεχνολογίας και εμπειριών μεταξύ των Μερών.

8.2.8 Μνημόνιο Συνεργασίας με το Υφυπουργείο Ναυτιλίας

Μετά από σχετικές επαφές και συζητήσεις που έγιναν εντός του 2021 μεταξύ του Υφυπουργείου Ναυτιλίας και της Αρχής Ψηφιακής Ασφάλειας, άρχισαν οι διεργασίες για τη Σύναψη Μνημονίου Συνεργασίας για καθορισμό του πλαισίου συνεργασίας μεταξύ του Υφυπουργείου και της ΑΨΑ σε θέματα που αφορούν τον τομέα της κυβερνοασφάλειας.

8.3 Χώρες της Ευρωπαϊκής Ένωσης και Τρίτες Χώρες

Κατά τη διάρκεια του έτους 2021, πραγματοποιήθηκαν αρκετές επαφές συνεργασίας με τις αντίστοιχες υπηρεσίες της Πολωνίας και του Ισραήλ και με αξιωματούχους του Σουλτανάτου του Ομάν, το Καζακστάν και την Αλβανία για τους τομείς της εκπαίδευσης και ανταλλαγής τεχνογνωσίας όσον αφορά την κυβερνοασφάλεια.

8.4 Διεθνής Εκπροσώπηση

Η εκπροσώπηση της ΑΨΑ σε επιτροπές σε διεθνές επίπεδο κατά το 2021 αναλήφθηκε από τον Επίτροπο, το Βοηθό Επίτροπο, τον 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:

Πίνακας 4: Διεθνής Εκπροσώπηση

ENISA (European Union Agency for Cybersecurity)
- MB (Management Board)
- NLO (National Liaison Officers) Network
- Cyber Crisis Cooperation and Exercises
- Ad-Hoc Working Group on Security Operation Centres (SOCs)

ECASEC (European Competent Authorities for the Security of Electronic Communications)

NIS Cooperation Group and relevant Work Streams
- Work Stream 2 – Security Measures
- Work Stream 3 – Incident Reporting
- Work Stream 5 – Digital Service Providers
- Work Stream 7 – Coordinated response to large scale cybersecurity incidents and crises
- Work Stream 8 – Energy
- Work Stream 10 – Digital Infrastructures
- Work Stream 12 - Health
- Ah-hoc additional COVID-19 coordination meetings
- 5G Work stream (+ standardisation/certification sub-group)

Συζητήσεις και διαμόρφωση της **νέας Οδηγίας NIS2**

CyCLONe – Cyber Crisis Liaison Officers Network

European Cybersecurity Certification Group (ECCG) and related sub-groups
- ECCG Sub-group on scheme governance and maintenanc

OSCE (Organization for Security and Co-operation in Europe)

CSP (Cyber Security Professionals) **Governance Board**

CSIRT Community Groups (FIRST, TI)

CSIRTs Network

ITU (International Telecommunications Union)

GFCE (Global Forum on Cyber Expertise)

GSCG (General Security Competence Group)

ECCC (European Cybersecurity Competence Centre) Governing Board

ECSO
- NAPAC (National Public Authorities Representative Committee)
- Working Group 1: Standardization, Certification and Supply Chain Management
- Working Group 5: Education, Training, Awareness, Cyber Ranges

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 2021, πραγματοποιήθηκαν 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.

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.

8.5 Εκπαιδεύσεις/Συνέδρια

8.5.1 Ενημερωτική Ημερίδα για Εποπτευόμενους Φορείς

Στα πλαίσια της υλοποίησης της Οδηγίας (ΕΕ) για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών και της εθνικής εναρμονιστικής νομοθεσίας, η ΑΨΑ οργάνωσε ενημερωτική ημερίδα για τους φορείς εκμετάλλευσης βασικών υπηρεσιών (ΦΕΒΥ) και τους φορείς κρίσιμων υποδομών πληροφοριών (ΦΚΥΠ). Η ημερίδα διοργανώθηκε για την πληρέστερη ενημέρωση των εμπλεκόμενων φορέων για τις δραστηριότητες της ΑΨΑ, και ειδικότερα για τις βασικές υποχρεώσεις των φορέων έναντι της σχετικής νομοθεσίας. Πιο αναλυτικά, το περιεχόμενο της ημερίδας είχε ως ακολούθως:

- Χρονοδιάγραμμα υλοποίησης Οδηγίας NIS στην Κύπρο και προγραμματισμένες ενέργειες 2021
- Εισαγωγή στην Αρχή Ψηφιακής Ασφάλειας
- Εμπλεκόμενα Μέρη – Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και Φορείς Κρίσιμων Υποδομών Πληροφοριών
- Ευρωπαϊκή Οδηγία NIS[34]
- Μέτρα Ασφάλειας (Security Measures)
- Κοινοποίηση Περιστατικών (Incident Notification)
- Πλατφόρμα Διαχείρισης ΑΨΑ (iDSAMPL – integrated Digital Security Authority Management Platform)
- Σχετική Νομοθεσία

Στην ημερίδα, την οποία χαιρέτισε ο Επίτροπος Επικοινωνιών κ. Γιώργος Μιχαηλίδης, συμμετείχαν πάνω από 120 άτομα από το σύνολο των ΦΕΒΥ και ΦΚΥΠ της Κύπρου.

8.5.2 Εκπαίδευση και Συζητήσεις για Υβριδικές Απειλές στην Ευρωπαϊκή Ένωση

Προσωπικό της ΑΨΑ συμμετείχε στις 10 με 11 Ιουνίου 2021 σε εκπαίδευση και συζητήσεις για το σημαντικό θέμα των υβριδικών απειλών στην Ευρωπαϊκή Ένωση. Υβριδική απειλή θεωρείται η πιθανή χρήση μη-στρατιωτικών μέσων από κράτη για την επίτευξη διάφορων στόχων εκτός της επικράτειας τους. Την τελευταία δεκαετία έχει αλλάξει δυναμικά το πεδίο απειλών που αντιμετωπίζουν η Ευρωπαϊκή Ένωση και τα Κράτη Μέλη, με τις υβριδικές απειλές να αυξάνονται όλο και περισσότερο. Η ΑΨΑ παρακολουθεί στενά τα σχετικά θέματα, καθώς ο κυβερνοχώρος και σχετικές απειλές

[34] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016L1148

χρησιμοποιούνται ως υβριδικό μέσο επίτευξης τέτοιων στόχων, και αυξάνεται συνεχώς η σημασία της επίτευξης υψηλού επιπέδου κυβερνοασφάλειας στην Κυπριακή Δημοκρατία.

Η σχετική εκπαίδευση εστιάστηκε σε διπλωματικά, νομικά και επιχειρησιακά θέματα που σχετίζονται με υβριδικές απειλές, καθώς και σε στρατηγικά θέματα ασφάλειας. Συζητήθηκαν η φύση των υβριδικών απειλών, οι υβριδικές απειλές στον τομέα της κυβερνοασφάλειας, οι υβριδικές απειλές στο πεδίο της παραπληροφόρησης, σχετικοί κίνδυνοι για την Ευρωπαϊκή Ένωση και τα Κράτη Μέλη, και τρόποι για αύξηση της ανθεκτικότητας σε Κρατικό και Ενωσιακό επίπεδο για επιτυχή αντιμετώπιση τέτοιων απειλών.

8.5.3 Εκπαίδευση για Πιστοποιήσεις Κυβερνοασφάλειας στον τομέα της Νεφοϋπολογιστικής

Στο πλαίσιο της υλοποίησης του συγχρηματοδοτούμενου έργου A4CEF "Advancing Cybersecurity Certification Capabilities with Cross-border exchange and Enhancing (business) Flows" (βλ. ενότητα 9.1.4), η ΑΨΑ συμμετείχε σε εκπαιδευτικό πρόγραμμα για πιστοποιήσεις κυβερνοασφάλειας που συνδιοργάνωσε μαζί με τους εταίρους της στο έργο. Η εκπαίδευση εστιάστηκε στο υπό διαμόρφωση Ευρωπαϊκό σχήμα πιστοποίησης κυβερνοασφάλειας για τις υπηρεσίες νεφοϋπολογιστικής, και κάλυψε θέματα κυβερνοασφάλειας υπηρεσιών, ρόλους και αρμοδιότητες, επίπεδα πιστοποίησης, μέτρα ασφάλειας και τις σχετικές διαδικασίες πιστοποίησης. Στην εκπαίδευση έλαβαν μέρος επίσης οι εταίροι του έργου (ΑΨΑ, Κυπριακή Εταιρεία Πιστοποίησης, Red Alert Labs (Γαλλία) και National Standards Authority of Ireland), καθώς και μεγάλος αριθμός ενδιαφερομένων μερών από την Ιρλανδία.

8.5.4 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 2021, πραγματοποιήθηκαν οι πιο κάτω εκπαιδεύσεις στο προσωπικό του Εθνικού CSIRT-CY:

- Splunk end-users training.
- Tetrane Training (Malware Analysis)
- Hack Attacks Webinar
- Free Pluralsight training (εργαλείο Nmap)
- The role of the EU Cyber Ecosystem in the Global Cyber Security Stability (Bucharest)
- Offensive-Security PEN-200 (Penetration Testing with Kali Linux)
- Building and Leading Security Operations Centers (SANS)
- ITU Training
- ΠΑΝΟΠΤΗΣ 2021
- Certified Ethical Hacker.

8.5.5 Εκπαιδεύσεις ESDC (European Security and Defence College)

Στο πλαίσιο της συνεργασίας της με το Ευρωπαϊκό Κολέγιο Ασφάλειας και Άμυνας (ESDC – European Security and Defence College), η Αρχή Ψηφιακής Ασφάλειας συμμετείχε ως συνδιοργανώτρια στην εκπαίδευση «Critical Infrastructures Protection Course – Module 2», η οποία πραγματοποιήθηκε μεταξύ 23 και 25 Φεβρουαρίου 2021. Η εκπαίδευση επικεντρώθηκε στην ασφάλεια και την προστασία των κρίσιμων υποδομών από φυσικές επιθέσεις και κυβερνοεπιθέσεις, με ιδιαίτερη αναφορά στους

κινδύνους που υπάρχουν και στην ανάγκη για πιστή εφαρμογή της Οδηγίας NIS. Στο πλαίσιο της εκπαίδευσης πραγματοποιήθηκε επίσης άσκηση με τη χρήση σεναρίου επίθεσης στις κρίσιμες υποδομών των Κρατών Μελών.

Επιπρόσθετα, με συνεργασία της Αρχής Ψηφιακής Ασφάλειας, του Κέντρου Συντονισμού Έρευνας και Διάσωσης και του ESDC, πραγματοποιήθηκε μεταξύ 6 και 8 Ιουλίου 2021 η εκπαίδευση «The role of the EU Cyber Ecosystem in the Global Cyber Security Stability». Η εκπαίδευση αφορούσε, μεταξύ άλλων, τις προκλήσεις στον κυβερνοχώρο στους τομείς της πληροφόρησης, της διαχείρισης κινδύνων και του χειρισμού περιστατικών. Στην εκπαίδευση συμμετείχε το προσωπικό του Εθνικού CSIRT-CY, εμπειρογνώμονες σε θέματα κυβερνοασφάλειας από το εξωτερικό, το Στρατιωτικό CSIRT, καθώς και οι Κρίσιμες Υποδομές Πληροφοριών της Κυπριακής Δημοκρατίας.

Επιπρόσθετα, προσωπικό της Αρχής Ψηφιακής Ασφάλειας παρακολούθησε την εκπαίδευση «Course on cyber threat management», η οποία διοργανώθηκε από το ESDC και τον ENISA μεταξύ 13 και 15 Οκτωβρίου 2021. Οι συμμετέχοντες είχαν την ευκαιρία να ενημερωθούν σχετικά με τις βασικές μεθοδολογίες και τεχνικές επιθέσεων, τα βασικά είδη κυβερνοκινδύνων, τα μέτρα ασφάλειας και τη σημασία τους στην αποτροπή επιθέσεων, καθώς και τη διαχείριση του Cyber Threat Intelligence.

8.6 Ευρωπαϊκός Μήνας Κυβερνοασφάλειας (ECSM)

Η ΑΨΑ συμμετείχε στην ετήσια εκστρατεία του ευρωπαϊκού μήνα κυβερνοασφάλειας (ECSM – European Cyber Security Month) της Ευρωπαϊκής Ένωσης για την προώθηση της ασφάλειας στο διαδίκτυο μεταξύ των πολιτών. Η ετήσια εκστρατεία ευαισθητοποίησης για την κυβερνοασφάλεια, η οποία διανύει τον 9ο χρόνο ζωής της, συντονίζεται από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) και υποστηρίζεται από την Ευρωπαϊκή Επιτροπή, όλα τα κράτη μέλη της ΕΕ και περισσότερους από 300 εταίρους από τον δημόσιο και τον ιδιωτικό τομέα. Η εκστρατεία διεξάγεται κάθε χρόνο κατά τον μήνα Οκτώβριο και προωθεί επικαιροποιημένες συστάσεις για την κυβερνοασφάλεια με σκοπό την οικοδόμηση εμπιστοσύνης στις διαδικτυακές υπηρεσίες και την υποστήριξη των πολιτών όσον αφορά την προστασία των προσωπικών, οικονομικών και επαγγελματικών τους δεδομένων στο διαδίκτυο. Υπάρχει ειδικά διαμορφωμένη ιστοσελίδα για το ECSM[35] όπου προβάλλονται όλες τις δραστηριότητες που προγραμματίζονται σε αυτό το πλαίσιο.

8.6.1 Σπουδές και Καριέρα στην Κυβερνοασφάλεια

Σε συνεργασία με το Πανεπιστήμιο UCLan Cyprus πραγματοποιήθηκε στις 22 Οκτωβρίου 2021 σεμινάριο με τίτλο “Σπουδές και Καριέρα στην Κυβερνοασφάλεια”. Στόχος του σεμιναρίου ήταν να αναδείξει την πολύπλευρη φύση της κυβερνοασφάλειας και να ενημερώσει τους νέους, τους γονείς και τους συμβούλους σταδιοδρομίας σχετικά με τα σημεία εισόδου και τις ευκαιρίες σταδιοδρομίας στην κυβερνοασφάλεια. Επιπλέον, το σεμινάριο παρέθεσε τις γνώσεις και τις δεξιότητες που σχετίζονται με την κυβερνοασφάλεια τις οποίες αναπτύσσουν οι νέοι μέσω των σπουδών τους στον τομέα (σε επίπεδο πτυχίου ή μεταπτυχιακού). Το σεμινάριο πραγματοποιήθηκε διαδικτυακά, η συμμετοχή ήταν δωρεάν και ήταν ανοικτό για όλους.

8.6.2 Ασφάλεια στο Διαδίκτυο για άτομα τρίτης ηλικίας

Σε συνεργασία με το CYBER.EUC Research Center του Ευρωπαϊκού Πανεπιστημίου Κύπρου, πραγματοποιήθηκε διαδικτυακό σεμινάριο με στόχο την ενημέρωση των ατόμων τρίτης ηλικίας για τους κινδύνους που ελλοχεύουν με την χρήση του διαδικτύου και πώς να προστατευτούν. Τα άτομα τρίτης ηλικίας χρησιμοποιούν τα κοινωνικά δίκτυα και το διαδίκτυο ολοένα και περισσότερο. Παρόλο που η χρήση του διαδικτύου προσφέρει πολλαπλά οφέλη και ευκαιρίες, την ίδια στιγμή φαίνεται να

[35] *https://cybersecuritymonth.eu/*

εκθέτει τα άτομα αυτά σε κινδύνους που αγνοούν, με αποτέλεσμα να γίνονται τα «εύκολα» θύματα για τους επιτήδειους που δρουν στο διαδίκτυο. Το σεμινάριο διεξήχθη διαδικτυακά και μεταδιδόταν ζωντανά μέσω των μέσων κοινωνικής δικτύωσης.

8.6.3 Ενημέρωση Μικρομεσαίων Επιχειρήσεων σε θέματα κυβερνοασφάλειας

Σε συνεργασία με το CYBER.EUC Research Center του Ευρωπαϊκού Πανεπιστημίου Κύπρου και με την υποστήριξη του Κυπριακού Εμπορικού και Βιομηχανικού Επιμελητηρίου, πραγματοποιήθηκε διαδικτυακό σεμινάριο για την ενημέρωση των μικρομεσαίων επιχειρήσεων σε θέματα κυβερνοασφάλειας. Οι μικρομεσαίες επιχειρήσεις αποτελούν διαχρονικά στόχους κυβερνοεπιθέσεων, όμως οι κίνδυνοι έχουν αυξηθεί σε μεγάλο βαθμό τα τελευταία δύο χρόνια λόγω της αυξανόμενης υιοθέτησης ψηφιακών τεχνολογιών. Το σεμινάριο κάλυψε διάφορα θέματα σχετικά με την κυβερνοασφάλεια, όπως οι μέθοδοι επίθεσης, τα ψηφιακά αποτυπώματα και οι καλές πρακτικές που πρέπει να ακολουθούνται από τις επιχειρήσεις.

9. ΑΛΛΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

9.1 Συμμετοχή σε Ευρωπαϊκά Συγχρηματοδοτούμενα Προγράμματα

9.1.1 CEF CYberSafety III

Το ευρωπαϊκό συγχρηματοδοτούμενο έργο "CYberSafety - Ένα καλύτερο διαδίκτυο για τα παιδιά στην Κύπρο"[36], με τη συμμετοχή όλων των εθνικών εμπλεκόμενων φορέων, έχει ως στόχο τη δημιουργία μιας κουλτούρας ασφαλούς διαδικτύου σε μαθητές, γονείς και εκπαιδευτικούς. Πρόκειται για μια συντονισμένη προσπάθεια οργανισμών και φορέων σε εθνικό επίπεδο για την ασφάλεια στο διαδίκτυο, το οποίο εντάσσεται στο πλαίσιο της εφαρμογής της Εθνικής Στρατηγικής για την Κυβερνοασφάλεια στην Κύπρο (βλ. ενότητα 4.11). Μέσα από το έργο CYberSafety οι ενδιαφερόμενοι μπορούν να βρουν πληροφορίες και να χρησιμοποιήσουν εργαλεία, αλλά και να μοιραστούν εμπειρίες, εμπειρογνωμοσύνη και καλές πρακτικές σε σχέση με την ασφαλή χρήση του διαδικτύου. Η ΑΨΑ συνεχίζει τις δράσεις για τη δημιουργία κουλτούρας σε παιδιά και νέους για την ασφαλή χρήση του διαδικτύου συμμετέχοντας στον 3ο κύκλο Προγράμματος CEF (Connecting Europe Facility) με το έργο "CYberSafety III" (CEF 2020-CY-IA-0069). Το Πρόγραμμα συντονίζει το Παιδαγωγικό Ινστιτούτο Κύπρου και η υλοποίηση του πραγματοποιείται σε συνεργασία με άλλους έξι οργανισμούς στην Κύπρο.

Ο ρόλος της ΑΨΑ σε αυτή την 3η φάση του έργου είναι η ενημέρωση και ευαισθητοποίηση των παιδιών στην Κύπρο μέσω διαδραστικών εκπαιδεύσεων σε μαθητές Γυμνασίων, Λυκείων και Τεχνικών Σχολών ανάπτυξη δεξιοτήτων για την ασφαλή χρήση του διαδικτύου, καθώς επίσης και η ανάπτυξη εφαρμογής για κινητά με τη μορφή παιγνιδιού μέσω των οποίων οι μαθητές μπορούν να εκπαιδευτούν και να αναπτύξουν σχετικές δεξιότητες ασφαλούς χρήσης του διαδικτύου. Κατά τη διάρκεια του 2021 πραγματοποιήθηκε σειρά διαδραστικών εκπαιδευτικών σεμιναρίων σε σχολεία Μέσης Εκπαίδευσης, οι οποίες ολοκληρώθηκαν με επιτυχία και ιδιαίτερα θετικές εντυπώσεις από τους μαθητές και τους εκπαιδευτικούς.

Οι δράσεις της ΑΨΑ περιλάμβαναν σεμινάρια 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 έγκειται στο ότι τα σεμινάρια ήταν διαδραστικά, προσφέροντας μια εμπειρία μοναδική και ιδιαίτερα ενδιαφέρουσα στους συμμετέχοντες.

Η συνέχιση των μέτρων λόγω της πανδημίας COVID-19 καθ' όλη τη διάρκεια του 2021 δεν επέτρεψε να πραγματοποιηθούν εκπαιδεύσεις με φυσική παρουσία. Για το λόγο αυτό, η ΑΨΑ σχεδίασε δύο διαδικτυακές διαλέξεις ώστε να προστεθούν κάποιες επιλογές για εκπαιδεύσεις εν μέσω της πανδημίας, με τις ακόλουθες θεματικές ενότητες:

- Ενημέρωση και ευαισθητοποίηση σχετικά με τις βέλτιστες πρακτικές για ασφαλέστερη πλοήγηση στο Διαδίκτυο, εστιάζοντας σε θέματα που αφορούν κινδύνους από σύνδεση σε άγνωστα ασύρματα δίκτυα Wifi, αναγνώριση κινδύνων στο διαδίκτυο, ύποπτες/ψευδείς ιστοσελίδες και πρακτικές αναγνώρισης τους, HTTP vs HTTPS, κίνδυνος χρήσης λογισμικών APK σε κινητές συσκευές, ασφάλεια λογισμικών και αναβαθμίσεις, κακόβουλα λογισμικά και πρακτικές για την αποφυγή τους, κακόβουλο λογισμικό υποκλοπής δεδομένων.
- Εκπαίδευση μαθητών/μαθητριών σχετικά με τις διαφορές ενός αυθεντικού ηλεκτρονικού μηνύματος με ένα ύποπτο ή κακόβουλο. Οι μαθητές/μαθήτριες είχαν τη δυνατότητα, με τη χρήση προκαθορισμένων ηλεκτρονικών μηνυμάτων, να αναγνωρίσουν τις διαφορές που παρατηρούνται σε ένα ηλεκτρονικό μήνυμα και να εντοπίσουν σε πραγματικό χρόνο τις διαφορές και τις μεθόδους εξαπάτησης.

[36] *https://cybersafety.cy/en/*

Το έργο συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση μέσω του ευρωπαϊκού προγράμματος CEF Telecom, έχει διάρκεια 20 μηνών και ξεκίνησε τον Ιανουάριο του 2020, με τον προϋπολογισμό που αφορά την ΑΨΑ να ανέρχεται στα €37,904 (από τα οποία €18,952 θα καλυφθούν από τον προϋπολογισμό της ΑΨΑ και €18,952 μέσω χρηματοδότησης από την ΕΕ).

9.1.2 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 3.2.2).

Κατά το 2021, η ΑΨΑ ολοκλήρωσε 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 τον συνολικό προϋπολογισμό του έργου να ανέρχεται σε €132,780.

9.1.3 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).

Το έργο έχει τους ακόλουθους επιμέρους στόχους:

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

Η πρόταση για συγχρηματοδότηση είχε υποβληθεί κάτω από το πρόγραμμα CEF Telecom 2019 - Cyber Security τον Νοέμβριο 2019. 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 ολοκληρώθηκε στο τέλος του 2021.

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

Στόχος του έργου είναι η περαιτέρω επέκταση των δραστηριοτήτων της ΑΨΑ για τις πιστοποιήσεις κυβερνοασφάλειας. Η ΑΨΑ πέτυχε τη σχετική χρηματοδότηση μετά από ανταγωνιστική διαδικασία κατά το 2021, και, μέσω του έργου αυτού, συνεχίζει και επεκτείνει τους σχεδιασμούς της Κυπριακής Δημοκρατίας για το Ευρωπαϊκό Πλαίσιο Πιστοποίησης Κυβερνοασφάλειας (βλ. ενότητα 6.1).

Το έργο έχει τους ακόλουθους επιμέρους στόχους:

- 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. Το έργο αναμένεται να ολοκληρωθεί εντός του 2023, με συνολικό προϋπολογισμό €280,000.

9.1.5 CEF JCOP – Joint Cybersecurity Operations Platform

Στα πλαίσια του Ευρωπαϊκού προγράμματος CONNECTING EUROPE FACILITY (CEF), η Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ), σε συνεργασία με:

- τη Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων της Ελλάδος,
- το Υπουργείο Ψηφιακής Διακυβέρνησης της Ελλάδος,
- το Πολυτεχνείο Κρήτης,
- το Πανεπιστήμιο του Όσλο Νορβηγίας,
- το Technische Universitaet Braunschweig Γερμανίας,
- το Norwegian National Security Authority, και
- την εταιρεία Sphynx Analytics Limited,

προχωρούν με το σχεδιασμό και την ανάπτυξη της πλατφόρμας Joint Cybersecurity Operations Platform (JCOP), μιας πλατφόρμας επιχειρησιακής ασφάλειας στον κυβερνοχώρο προσαρμοσμένης στις ανάγκες των κρατών μελών της ΕΕ. Μακροπρόθεσμος στόχος του έργου είναι η περαιτέρω ενσωμάτωση της πλατφόρμας και από άλλους ευρωπαϊκούς φορείς.
Αναλυτικότερα, η λύση JCOP περιλαμβάνει τρεις βασικούς πυλώνες:

- **Συλλογή και ανάλυση πληροφοριών (Threat Intelligence):** για συγκέντρωση, ανάλυση και ανταλλαγή πληροφοριών σχετικά με απειλές και φορείς απειλών.
- **Ανίχνευση και ανταπόκριση έναντι κυβερνοεπιθέσεων (Alerting and Incident Response):** για ταχεία ειδοποίηση μεταξύ των διαφόρων μερών εντός της ΕΕ, η οποία μπορεί να χρησιμοποιηθεί είτε προληπτικά, είτε για απόκριση σε τρέχοντα περιστατικά.
- **Υποστήριξη προγραμμάτων εκπαίδευσης (Cybersecurity Operations Training):** για τη συνεχή ενημέρωση και επιμόρφωση, μέσω της συγκέντρωσης, στην πλατφόρμα, εξειδικευμένου εκπαιδευτικού υλικού σχετικά με ποικίλα θέματα κυβερνοασφάλειας.

Το ποσό χρηματοδότησης του έργου ανέρχεται στις €200,625, με το συνολικό προϋπολογισμό του έργου να ανέρχεται σε €267,500.

9.1.6 CYCLOPS - Cyprus Center for Land, Open Seas and Port Security

Στόχος του έργου είναι η δημιουργία Εργαστηρίων Εκπαίδευσης Κυβερνοασφάλειας. Η Αρχή Ψηφιακής Ασφάλειας παρέλαβε εξοπλισμό που περιλάμβανε 26 φορητούς υπολογιστές και αριθμό περιφερειακών συσκευών, μαζί με το σχετικό λογισμικό και δικτυακό εξοπλισμό για σκοπούς εκπαίδευσης και ανάπτυξης ικανοτήτων σε εκπαιδεύσεις με θεματολογία την κυβερνοασφάλεια. Ο εξοπλισμός εμπίπτει στο πλαίσιο των χρηματοδοτούμενων από τις ΗΠΑ δραστηριοτήτων του Κυπριακού Κέντρου για την Ασφάλεια στην Ξηρά, την Ανοικτή Θάλασσα και τα Λιμάνια (CYCLOPS), του κυπριακού εκπαιδευτικού κέντρου που θα χρησιμεύσει ως περιφερειακός κόμβος εκπαίδευσης, εστιάζοντας σε τομείς που σχετίζονται με την ασφάλεια, συμπεριλαμβανομένης της ασφάλειας στον κυβερνοχώρο. Ο εξοπλισμός θα υποστηρίξει απτά το έργο της Αρχής Ψηφιακής Ασφάλειας για την ενίσχυση των δυνατοτήτων κυβερνοασφάλειας σε εθνικό και περιφερειακό επίπεδο.

Ο Επίτροπος Επικοινωνιών κ. Γιώργος Μιχαηλίδης, είχε την τιμή να παραλάβει από την Εξοχότητά της, την Πρέσβειρα των ΗΠΑ κ. Judith G. Garber, εξοπλισμό υλικού (hardware) και λογισμικού (sofrware) για το Εργαστήριο Εκπαιδεύσεων Κυβερνοασφάλειας CYCLOPS παρουσία του Πολιτικού Διευθυντή του Υπουργείου Εξωτερικών κ. Ευάγγελου Σάββα και εκπροσώπησης του Υπουργείου Άμυνας της Κύπρου. Κατά τη διάρκεια του χαιρετισμού του, μεταξύ άλλων, ανέφερε ότι «Το CYCLOPS είναι μια πολύ καλή πλατφόρμα για ενεργή συνεργασία, τόσο σε εθνικό όσο και σε διεθνές επίπεδο και υποστηρίζουμε σθεναρά τις πρωτοβουλίες στο πλαίσιο αυτό».