ΑΡΧΗ ΨΗΦΙΑΚΗΣ
ΑΣΦΑΛΕΙΑΣ

Έκθεση Δραστηριοτήτων του έτους 2018

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

Αύγουστος 2019

ΠΕΡΙΕΧΟΜΕΝΑ

ΧΑΙΡΕΤΙΣΜΟΣ ΕΠΙΤΡΟΠΟΥ 4

1. ΔΙΟΙΚΗΣΗ 6

1.1 Όραμα Αρχής Ψηφιακής Ασφάλειας 6
1.2 Στόχοι Αρχής Ψηφιακής Ασφάλειας 6
1.3 Οργανωτική Δομή 7
1.3.1 Τομέας Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών, Συντονισμός Κυβερνοασφάλειας - Ρυθμιστικός Τομέας 8
1.3.2 Τομέας Εθνικού CSIRT – Επιχειρησιακός Τομέας 8
1.4 Στελέχωση 10
1.5 Εκπαίδευση 10
1.6 Εναρμόνιση με το Ευρωπαϊκό Πλαίσιο για την Ασφάλεια Δικτύων και Πληροφοριών και την Κυβερνοασφάλεια ... 11
1.7 Δημιουργία Δομών για Συμμόρφωση με τον Ευρωπαϊκό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων (General Data Protection Regulation - GDPR) 11
1.8 Ανάπτυξη Πολιτικών και Διαδικασιών Εθνικού CSIRT 12
1.9 Δημιουργία Ιστοσελίδας ΑΨΑ και Εθνικού CSIRT 13

2. ΟΙΚΟΝΟΜΙΚΕΣ ΚΑΤΑΣΤΑΣΕΙΣ 15

2.1 Μη Ελεγμένες Οικονομικές Καταστάσεις για το έτος 2018 15

3. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ 18

3.1 Νομοθεσία ΑΨΑ 18
3.1.1 Νόμος 17(Ι)/2018 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών 18
3.1.2 Αναθεωρημένος Νόμος περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών 18
3.1.3 Κανονισμοί Χρηματοδότησης ΑΨΑ 18
3.1.4 Αξιολόγηση Κρισιμότητας Υποδομών 18
3.2 Νομοθεσία Ηλεκτρονικών Επικοινωνιών για την Ασφάλεια Δικτύων και Πληροφοριών 19
3.1.5 Μέτρα Ασφάλειας NIS 19
3.1.6 Κοινοποίηση Περιστατικών Παραβίασης Ψηφιακής Ασφάλειας 19
3.1.7 Εγγραφές Παροχέων Ψηφιακών Υπηρεσιών 19
3.3 Ανάπτυξη Υποδομών και Εργαλείων 20
3.3.1 Υποδομή Εθνικού CSIRT 20
3.3.2 Ολοκληρωμένη Πλατφόρμα Διαχείρισης ΑΨΑ 20

4. ΥΛΟΠΟΙΗΣΗ ΣΤΡΑΤΗΓΙΚΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ 22

4.1 Υλοποίηση Δράσεων Στρατηγικής Κυβερνοασφάλειας 22
4.2 Εθνικό Πλαίσιο Κυβερνοασφάλειας 22

4.3 Ασκήσεις Κυβερνοασφάλειας 22
4.4 Δημιουργία Κουλτούρας Κυβερνοασφάλειας - Awareness 23
4.5 Αναθεώρηση της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας 24

5. ΔΙΑΧΕΙΡΙΣΗ ΣΥΜΒΑΝΤΩΝ ΚΑΙ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 25

5.1 Διαχείριση Περιστατικών 25
5.2 Διαχείριση Κρίσεων 25
5.2.1 ΒΕΣ "ΖΗΝΩΝ": ΕΕΣ "ΑΡΙΣΤΕΑΣ" 25
5.2.2 Συμμετοχή σε άλλα ΕΕΣ του ΒΕΣ "ΖΗΝΩΝ" 25

6. ΕΘΝΙΚΕΣ & ΔΙΕΘΝΕΙΣ ΣΧΕΣΕΙΣ 26

6.1 Συνεργασία με Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και Φορείς Κρίσιμων Υποδομών Πληροφοριών ... 26
6.2 Συνεργασία με Κρατικές Αρχές 26
6.3 Συνεργασία με Κράτη-Μέλη 27
6.4 Συνεργασία με Τρίτες Χώρες 27
6.4.1 Μνημόνιο Συναντίληψης με Israeli National Cyber Directorate 27
6.4.2 Πρόταση Συνεργασίας με Σουλτανάτο του Ομάν 27
6.5 Διεθνείς Εκπροσώπηση 28
6.6 Συνέδρια 28
6.6.1 1ο Ετήσιο Συνέδριο ΑΨΑ 28
6.6.2 2ο Ετήσιο Συνέδριο ΑΨΑ 29
6.6.3 Συνέδριο ITU – Cyber Drill 30

7. ΑΛΛΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ 32

7.1 Συμμετοχή σε Ευρωπαϊκά Συγχρηματοδοτούμενα Προγράμματα 32
7.1.1 CEF CSIRT-CY 32
7.1.2 CEF CYberSafety 32
7.1.3 CEF Ακαδημαϊκό CSIRT 33

ΓΡΑΦΗΜΑΤΑ

Γράφημα 1: Κατανομή Δαπανών για το 2018 16
Γράφημα 2: Κατανομή Εσόδων για το 2018 16

ΠΙΝΑΚΕΣ

Πίνακας 1: Οργανόγραμμα 7
Πίνακας 2: Μη Ελεγμένη Κατάσταση Συνολικών Εισοδημάτων 2018 15
Πίνακας 3: Μη Ελεγμένη Κατάσταση Χρηματοοικονομικής Θέσης στις 31 Δεκ. 2018 17

ΧΑΙΡΕΤΙΣΜΟΣ ΕΠΙΤΡΟΠΟΥ

Η παρούσα έκθεση απολογισμού του έργου της Αρχής Ψηφιακής Ασφάλειας συνοψίζει το σύνολο των δραστηριοτήτων που υλοποιήθηκαν σε όλο το φάσμα των πεδίων αρμοδιότητας της, κατά το έτος 2018.

Τον Απρίλιο του 2018, έχει εισαχθεί στην Κυπριακή Δημοκρατία η Νομοθεσία περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Νόμος 17(Ι)2018) στα πλαίσια εναρμόνισης με την Ευρωπαϊκή Οδηγία για την Ασφάλεια Δικτύων και Πληροφοριών (NIS Directive). Με βάση τη νομοθεσία αυτή, ιδρύθηκε η Αρχή Ψηφιακής Ασφάλειας υπό τον Επίτροπο Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων, και η οποία ορίσθηκε ως η αρμόδια αρχή για την εφαρμογή της Ευρωπαϊκής Οδηγίας για την Ασφάλεια Δικτύων και Πληροφοριών (NIS Directive) στην Κυπριακή Δημοκρατία και την εφαρμογή της Εθνικής Στρατηγικής για την Κυβερνοασφάλεια. Η Αρχή Ψηφιακής Ασφάλειας έχει ιδιαίτερα σημαντικές αρμοδιότητες στον σημερινό κόσμο όπου όλα συνδέονται και επικοινωνούν μεταξύ τους. Η τεχνολογία έχει διεισδύσει πλέον σε όλους τους τομείς της καθημερινής μας ζωής, είτε είμαστε άμεσοι χρήστες μέσω κινητών συσκευών τηλεφωνίας και ηλεκτρονικών υπολογιστών, είτε ως έμμεσοι χρήστες με πληθώρα άλλων συσκευών και υποδομών. Τα συστήματα που χρησιμοποιούμε ως έμμεσοι χρήστες βρίσκονται παντού και σε όλες σχεδόν τις καθημερινές μας δραστηριότητες, από τον μεγάλο αριθμό συνδεδεμένων συσκευών που έχουμε στα σπίτια μας (τηλεοράσεις, συστήματα συναγερμού, κλιματιστικά, κ.λπ.), μέχρι και τις εθνικές κρίσιμες υποδομές οι οποίες παρέχουν υπηρεσίες ζωτικής σημασίας, όπως ηλεκτρική ενέργεια, νερό, μεταφορές, επικοινωνίες, υγεία και τράπεζες.

Οφείλουμε, ως πολιτεία, να κατανοήσουμε τη σημασία της ψηφιακής τεχνολογίας στην κοινωνία μας, και να ενεργήσουμε δυναμικά για την κατάλληλη προστασία των πληροφοριών και υποδομών, ώστε να θεμελιώνεται σωστά και να συνεχίσει να αναπτύσσεται η ψηφιακή οικονομία μας. Προς το σκοπό αυτό, έχουμε αναγνωρίσει τα κύρια σημεία μιας ολιστικής προσέγγισης για την ασφάλεια στον κυβερνοχώρο, τα οποία διέπουν τη λειτουργία και κατευθύνουν τις δραστηριότητες της Αρχής Ψηφιακής Ασφάλειας.

Πρώτον, πρέπει να στοχεύουμε στην Ασφάλεια Για Όλους - τις κρίσιμες υποδομές πληροφοριών, το κράτος, όλες τις επιχειρήσεις (συμπεριλαμβανομένων και των μικρομεσαίων επιχειρήσεων), και τους πολίτες τους ίδιους. Η Ασφάλεια Για Όλους είναι απαραίτητη προϋπόθεση για την επίτευξη των στόχων μας και την αποκόμιση των πολλαπλών οφελών από την ψηφιακή οικονομία.
Δεύτερον, πρέπει να κατανοηθεί από όλους τους εμπλεκόμενους ότι η ασφάλεια είναι προϊόν ομαδικής προσπάθειας. Απαιτείται συνεργασία σε όλα τα επίπεδα, μεταξύ επιχειρήσεων, φορέων κρίσιμων υποδομών πληροφοριών, αρχών σε εθνικό επίπεδο, καθώς και σε διακρατικό, ευρωπαϊκό και διεθνές επίπεδο. Χωρίς την αποδοτική συνεργασία σε αυτά τα επίπεδα, η οποία να θεμελιώνεται στην πραγματική εμπιστοσύνη μεταξύ των μερών, δεν θα είμαστε έτοιμοι να αντιμετωπίσουμε σοβαρά περιστατικά στον κυβερνοχώρο.

Τρίτον, η προστασία και η περαιτέρω ανάπτυξη αποκτά ιδιαίτερα μεγάλη σημασία, καθώς πρέπει να ενδυναμώσουμε ακόμα περισσότερο τους κρίσιμους τομείς της οικονομίας μας, όπως τη ναυτιλία και τις διεθνείς χρηματοοικονομικές υπηρεσίες, στους οποίους η Κύπρος κατέχει ψηλή θέση σε παγκόσμιο επίπεδο.

Τέταρτον, ο τομέας της κυβερνοασφάλειας χαρακτηρίζεται από ραγδαίες εξελίξεις σε σχεδόν καθημερινή βάση. Οι διάφορες απειλές στον κυβερνοχώρο αυξάνονται διαρκώς, τόσο σε όγκο όσο και σε πολυπλοκότητα, και έτσι πρέπει η προσέγγιση μας να είναι ανάλογη. Στην Αρχή Ψηφιακής Ασφάλειας η προσέγγιση μας μπορεί να συνοψιστεί πολύ απλά: Think Big, Start Small and Scale Fast.

Κλείνοντας, θα ήθελα να μεταφέρω το μήνυμα ότι η Αρχή Ψηφιακής Ασφάλειας είναι ανοικτή και προωθεί συνεργασίες με διάφορους τρόπους και σε πολλά επίπεδα που να αποσκοπούν στην επίτευξη των στόχων μας και την εδραίωση ενός ασφαλούς ψηφιακού περιβάλλοντος για κάθε πολίτη της Κύπρου.

Γιώργος Μιχαηλίδης

Επίτροπος Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων

1. ΔΙΟΙΚΗΣΗ

Από τις 5 Απριλίου 2018, και με βάση το Νόμο 17(Ι)2018 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών, η Αρχή Ψηφιακής Ασφάλειας υπάγεται διοικητικά υπό τον Επίτροπο Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων κ. Γιώργο Μιχαηλίδη και τον Βοηθό Επίτροπο κ. Πέτρο Γαλίδη.

1.1. Όραμα Αρχής Ψηφιακής Ασφάλειας

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

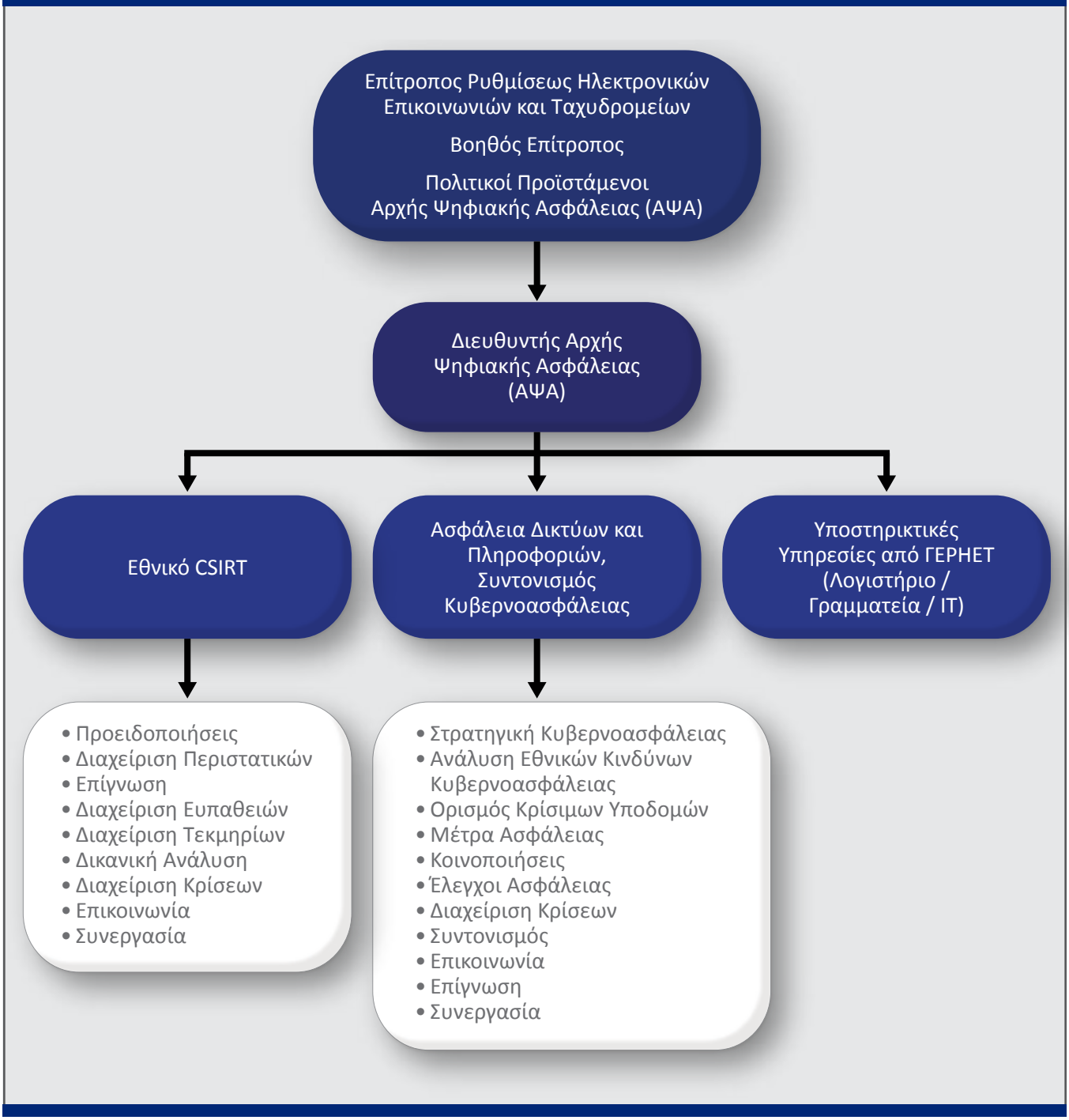
1.2. Στόχοι Αρχής Ψηφιακής Ασφάλειας

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

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

1.3. Οργανωτική Δομή

Πίνακας 1: Οργανόγραμμα



Η οργανωτική δομή της Αρχής Ψηφιακής Ασφάλειας (“ΑΨΑ”) παρουσιάζεται στο Γράφημα 1, στο οποίο αποτυπώνονται ενδεικτικά οι τομείς αρμοδιότητας της Αρχής.

1.3.1. Τομέας Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών, Συντονισμός Κυβερνοασφάλειας - Ρυθμιστικός Τομέας

Ο τομέας Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών αποτελεί το ρυθμιστικό και επιχειρησιακό βραχίονα της ΑΨΑ σε θέματα επιχειρησιακής συνέχειας των δικτύων πληροφοριακών συστημάτων των ουσιωδών και κρίσιμων υποδομών του κράτους.

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

Ο ρυθμιστικός τομέας είναι, επίσης, υπεύθυνος για το συντονισμό της εφαρμογής της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας.

Η λειτουργία του τομέα Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών περιλαμβάνει, μεταξύ άλλων, τις ακόλουθες υπηρεσίες:

- **α.** ετοιμασία Πρωτογενούς και Δευτερογενούς Νομοθεσίας και καθορισμός ρυθμιστικού πλαισίου Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών,
- **β.** διενέργεια Αξιολόγησης Κρισιμότητας και αναθεώρηση καταλόγου κρίσιμων Υποδομών Πληροφοριών,
- **γ.** διενέργεια Αξιολόγησης Κινδύνων Κυβερνοασφάλειας σε εθνικό επίπεδο,
- **δ.** υλοποίηση αποτελεσμάτων αξιολόγησης επικινδυνότητας,
- **ε.** καθορισμός πλαισίου μέτρων ασφάλειας και ελέγχου συμμόρφωσης,
- **στ.** καθορισμός διαδικασιών κοινοποίησης περιστατικών παραβίασης ασφάλειας,
- **ζ.** εποπτεία εφαρμογής πλαισίου κυβερνοασφάλειας από φορείς εκμετάλλευσης βασικών υπηρεσιών, φορείς κρίσιμων υποδομών πληροφοριών, παροχέων ηλεκτρονικών επικοινωνιών και παροχέων ψηφιακών υπηρεσιών,
- **η.** διαχείριση κρίσεων σε σχέση με θέματα Ασφάλειας Δικτύων και Πληροφοριών και Κυβερνοασφάλειας,
- **θ.** ανάπτυξη και διαχείριση της εφαρμογής της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας,
- **ι.** επιμόρφωση και ενημέρωση σε θέματα που αφορούν την κυβερνοασφάλεια,
- **ια.** συμμετοχή σε ευρωπαϊκά και διεθνή σώματα, επιτροπές και κοινότητες, και
- **ιβ.** συμμετοχή σε ευρωπαϊκά συγχρηματοδοτούμενα προγράμματα.

1.3.2. Τομέας Εθνικού CSIRT – Επιχειρησιακός Τομέας

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

Το Εθνικό CSIRT άρχισε τις εργασίες του τον Νοέμβριο του 2017. Τον Ιούνιο του 2018 έγιναν τα επίσημα

εγκαίνια του Εθνικού CSIRT από την Υπουργό Μεταφορών, Επικοινωνιών και Έργων, κα Βασιλική Αναστασιάδου, και το Διευθυντή του τομέα Τηλεπικοινωνιών της Διεθνούς Ένωσης Τηλεπικοινωνίων (ITU-T), κ. Brahima Sanou.

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

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

Η λειτουργία του Εθνικού CSIRT περιλαμβάνει, μεταξύ άλλων, τις ακόλουθες υπηρεσίες:

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

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

1.4. Στελέχωση

Κατά το 2018, 3 μόνιμοι υπάλληλοι από το ΓΕΡΗΕΤ (Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων), και συγκεκριμένα 1 Ανώτερος Λειτουργός, 1 Λειτουργός και 1 Γραμματέας, απασχολούνται αποκλειστικά με τις εργασίες της ΑΨΑ στον τομέα της εφαρμογής της Ευρωπαϊκής Οδηγίας για την Ασφάλεια Δικτύων και Πληροφοριών και της Εθνικής Στρατηγικής για την Κυβερνοασφάλεια. Με την ψήφιση της Δευτερογενούς Νομοθεσίας, η οποία αναμένεται να ολοκληρωθεί εντός του 2019, θα προκηρυχθούν 11 νέες θέσεις εργασίας για τη στελέχωση της ΑΨΑ.

Το Εθνικό CSIRT έχει στελεχωθεί προσωρινά με τη σύναψη συμβάσεων παροχής υπηρεσιών με συνολικά 12 άτομα: 1 υπεύθυνου ομάδας και 11 αναλυτών.

Εντός του 2018, έχουν επίσης ετοιμαστεί οι κανονισμοί πρόσληψης του προσωπικού της ΑΨΑ και του Εθνικού CSIRT.

1.5. Εκπαίδευση

Η εκπαίδευση των μελών της ΑΨΑ και του Εθνικού CSIRT είναι συνεχής και λαμβάνει διάφορες μορφές, όπως παρακολούθηση εργαστηρίων ειδικά σχεδιασμένων για την Υπηρεσία, παρακολούθηση σεμιναρίων εντός και εκτός Κύπρου, και συμμετοχή/παρακολούθηση Ομάδων Εργασίας διεθνών σωμάτων.

Στα πλαίσια δημιουργίας διεθνών σχέσεων και κλίματος εμπιστοσύνης μέσα από τη συμμετοχή σε διεθνή φόρα, καθώς και σε προγράμματα της Διεθνούς Ένωσης Τηλεπικοινωνίων (International Telecommunications Union - ITU), αναπτύχθηκαν καρποφόρες συνεργασίες με παγκοσμίως αναγνωρισμένους οργανισμούς, όπως τον οργανισμό ENISA (European Union Agency for Network and Information Security), τον οργανισμό FIRST (Forum of Incident Response and Security Teams), αλλά και αντίστοιχες ομάδες αντιμετώπισης ηλεκτρονικών επιθέσεων, όπως αυτή της Ρουμανίας, της Πολωνίας και του Ισραήλ, μέσα από τις οποίες διεξήχθησαν εξειδικευμένες εκπαιδευτικές δραστηριότητες και ανταλλαγή υλικού.

Επίσης, εξειδικευμένοι σύμβουλοι από το εξωτερικό διενήργησαν εκπαιδεύσεις προς το Εθνικό CSIRT και εμπλεκόμενους φορείς στην Κύπρο σε θέματα σχετικά με την κυβερνοασφάλεια. Η θεματολογία των εκπαιδεύσεων αυτών περιλάμβανε, μεταξύ άλλων, την ακόλουθη θεματολογία:

1. Πλατφόρμα FireEye
2. Πλατφόρμα Splunk
3. Πλατφόρμα ANOMALI
4. Real world cases of cybersecurity incidents - ITU
5. Evidence Collection & Introduction Digital Forensics - Deloitte
6. Introduction to Penetration Testing & Cyber Defence and Network Security Monitoring - Deloitte
7. Security Workshops for Incident Responders - Runesec
8. Incident investigation with supporting tools - CERT Polska
9. Malware Analysis and Memory Forensics & Incident Management – ENISA
10. GDPR - Adacom
11. Introduction to Forensics - Deloitte
12. Introduction to Digital Forensics - Deloitte
13. Malware Analysis - Deloitte
14. Introduction to Penetration Testing - Deloitte
15. Πλατφόρμα MISP (Malware Information Sharing Platform) - CIRCL

Πέραν από την εκπαίδευση του προσωπικού και με στόχο την ενημέρωση και διαφάνεια, η ΑΨΑ διασφάλισε εκπαιδεύσεις σε αρκετά από τα πιο πάνω θέματα προς συνεργαζόμενες κρατικές υπηρεσίες, όπως το Γραφείο Καταπολέμησης Ηλεκτρονικού Εγκλήματος της Αστυνομίας Κύπρου, την Εθνική Αρχή Ασφάλειας, την Κυπριακή Υπηρεσία Πληροφοριών, το Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, το Τμήμα Υπηρεσιών Πληροφορικής και το Κυπριακό Ερευνητικό και Ακαδημαϊκό Δίκτυο.

Επίσης, η ΑΨΑ προσέφερε προγράμματα ενημέρωσης και κατάρτισης σε Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, Φορείς Κρίσιμων Υποδομών Πληροφοριών, παροχείς ηλεκτρονικών επικοινωνιών και παροχείς ψηφιακών υπηρεσιών. Η θεματολογία, εκτός των προαναφερθέντων, κάλυψε και την Οδηγία NIS, τη λειτουργία του Εθνικού CSIRT και τις βασικές υπηρεσίες που προσφέρει στους φορείς.

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

Ο Νόμος 17(Ι)2018 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών έχει ιδρύσει επίσημα την Αρχή Ψηφιακής Ασφάλειας και έχει εντάξει το Εθνικό CSIRT στη δομή της Αρχής. Ο Νόμος παρέχει τις αρμοδιότητες στην Αρχή για την πλήρη εφαρμογή της Οδηγίας NIS, παρόλο που, εντός του 2019, προγραμματίζονται περαιτέρω νομοθετικές ενέργειες για την αποτελεσματικότερη εφαρμογή του νέου πλαισίου.

Συγκεκριμένα, εντός του 2019, προγραμματίζονται νομοθετικές ρυθμίσεις σχετικά με τις διαδικασίες κοινοποίησης των περιστατικών ασφάλειας δικτύων και πληροφοριών και κυβερνοασφάλειας, οι οποίες περιλαμβάνουν τον καθορισμό και την εφαρμογή του πλαισίου μέτρων ασφάλειας για τις ουσιώδεις υπηρεσίες και τις κρίσιμες υποδομές πληροφοριών, καθώς και τη μεταβίβαση των αρμοδιοτήτων σε θέματα ασφάλειας ηλεκτρονικών επικοινωνιών από το ΓΕΡΗΕΤ στην ΑΨΑ.

Το Νοέμβριο του 2018, και σύμφωνα με τις διατάξεις του Νόμου 17(Ι)2018 και τις πρόνοιες της Οδηγίας NIS, επανακαθορίστηκαν από το Υπουργικό Συμβούλιο οι Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και οι Φορείς Κρίσιμων Υποδομών Πληροφοριών. Για το θέμα έχει γίνει σχετική κοινοποίηση στην Ευρωπαϊκή Επιτροπή.

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

Στο πλαίσιο της Δράσης 11 του ευρωπαϊκού συγχρηματοδοτούμενου προγράμματος Connecting Europe Facility (CEF) για την ανάπτυξη και βελτίωση του Εθνικού CSIRT (2016-CY-IA-0129) (βλ. ενότητα 7.1.1), έγινε αξιολόγηση, καθορισμός των πολιτικών, διαδικασιών και δομών, καθώς και ετοιμασία σχετικών εγγράφων στα πλαίσια της συμμόρφωσης με τον Ευρωπαϊκό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων (GDPR). Για την υλοποίηση των σχετικών ρυθμίσεων ξεκίνησαν διαβουλεύσεις με την Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για εξειδικευμένα και ευαίσθητα θέματα που αφορούν την αποτελεσματική διεκπεραίωση των κατά Νόμο εργασιών του Εθνικού CSIRT.

Ταυτόχρονα, προωθήθηκαν και οι αντίστοιχες διαδικασίες για τις υπόλοιπες δομές της ΑΨΑ με τη βοήθεια εξωτερικών συμβούλων, οι οποίες αναμένεται να ολοκληρωθούν εντός του 2019.

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

1.8. Ανάπτυξη Πολιτικών και Διαδικασιών Εθνικού CSIRT

Μέσω του ευρωπαϊκού συγχρηματοδοτούμενου προγράμματος Connecting Europe Facility (CEF) (βλ. ενότητα 7.1.1) και σε συνεργασία με εμπειρογνώμονες σε θέματα προτύπων, διαδικασιών και συναφών νομοθεσιών (ISO27001: Information Security, GDPR κ.λπ.), το Εθνικό CSIRT κατάρτισε και εφάρμοσε διαδικασίες και πολιτικές που επιτρέπουν την ταχεία, ομαλή και επαγγελματική λειτουργία της Ομάδας. Η εντατική εργασία για τη δημιουργία των πολιτικών και διαδικασιών αυτών ξεκίνησε προς το τέλος του 2017, και συνεχίστηκε καθ' όλη τη διάρκεια του 2018. Στο πλαίσιο της συνεχούς επικαιροποίησης τους, όλα τα έγγραφα αναμένεται να αναθεωρηθούν εντός του 2019 για να προσαρμοστούν σύμφωνα με τις τρέχουσες ανάγκες και δεδομένα της Ομάδας. Οι διαδικασίες και οι πολιτικές που δημιουργήθηκαν καλύπτουν όλες τις πτυχές λειτουργίας της Ομάδας, όπως την ασφάλεια Συστημάτων, την ασφάλεια Δικτύου, τις διαδικασίες λειτουργίας των στελεχών και την ασφάλεια του κτιρίου.

Τα έγγραφα που αναπτύχθηκαν στα πλαίσια της πιο πάνω εργασίας είναι, μεταξύ άλλων, τα ακόλουθα:

1. CSIRT-CY - Code of Practice and Acceptable Use
2. CSIRT-CY - Employee Handbook
3. CSIRT-CY - Training Policy
4. CSIRT-CY - External Networking Outreach and P2P
5. CSIRT-CY - Organisational Framework
6. CSIRT-CY - Service Level Description
7. CSIRT-CY - Incident Handling SOP
8. CSIRT-CY - Information Security in IT Operations
9. CSIRT-CY - Information Security Top Policy
10. CSIRT-CY - Overview of Incident Handling Processes
11. CSIRT-CY - Internal Audit Procedure Plan and Schedule
12. CSIRT-CY - Secure Information and Sources Management
13. CSIRT-CY - Reporting Process
14. CSIRT-CY - Major Incident handling
15. CSIRT-CY - CEF UI
16. CSIRT-CY - GDPR Risk Analysis
17. CSIRT-CY - GDPR Retention policy

Βασική δραστηριότητα του Εθνικού CSIRT είναι η διαχείριση περιστατικών (Incident Management) στο πλαίσιο ITIL (Information Technology Infrastructure Library) σε σχέση με τις εσωτερικές του διαδικασίες, αλλά και η εφαρμογή Πολιτικών Ασφάλειας που αφορούν τον τομέα διαχείρισης υπηρεσιών στο χώρο της κυβερνοασφάλειας της Κυπριακής Δημοκρατίας. Το Εθνικό CSIRT είναι ο μοναδικός οργανισμός που υιοθετεί την εφαρμογή του πλαισίου ITIL στις διαδικασίες διαχείρισης περιστατικών, γεγονός που αποτελεί παγκόσμια καινοτομία στο χώρο των CSIRT. Το ITIL είναι ένα πλαίσιο για τη διαχείριση υπηρεσιών πληροφορικής, το οποίο βασίζεται σε βέλτιστες πρακτικές με στόχο τη βελτίωση των διαδικασιών και υπηρεσιών IT, μείωση του κόστους λειτουργίας, βελτίωση στην εξυπηρέτηση των πελατών και αύξηση της παραγωγικότητας με βάση τη σωστή διαχείριση κινδύνων.

Τα οφέλη που προκύπτουν από την υιοθέτηση της εφαρμογής του πλαισίου ITIL εξασφαλίζουν στην ομάδα του Εθνικού CSIRT:

- βελτίωση των διαδικασιών και μεθόδων που χρησιμοποιούνται για διαχείριση περιστατικών,
- βελτίωση της ποιότητας των υπηρεσιών που προσφέρονται στις Κρίσιμες Υποδομές,
- αύξηση της παραγωγικότητας, της αποδοτικότητας και της αποτελεσματικότητας του οργανισμού μέσω αξιόπιστων υπηρεσιών πληροφορικής,

- βελτίωση της επικοινωνίας και ενημέρωσης μεταξύ του προσωπικού και των Κρίσιμων Υποδομών, και
- αύξηση του βαθμού ικανοποίησης των Κρίσιμων Υποδομών.

Επιπλέον, το Εθνικό CSIRT, στο πλαίσιο διαχείρισης περιστατικών, έχει αναπτύξει τη διαδικασία επίλυσης κρίσιμων περιστατικών σε περιπτώσεις τόσο φυσικών καταστροφών όσο και κρίσιμων περιστατικών κυβερνοασφάλειας. Σε συνδυασμό με τις πολιτικές που προαναφέρθηκαν, το Εθνικό CSIRT έχει δημιουργήσει ειδικές διαδικασίες για την αντιμετώπιση και διαχείριση περιστατικών στο χώρο της κυβερνοασφάλειας, όπως:

- Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας (Incident Handling Procedure),
- Διαδικασία Εντοπισμού και Ανάλυσης Περιστατικών Ασφάλειας (Detection and Analysis), και
- Διαδικασία Διενέργειας Δοκιμών Διείσδυσης (Penetration Testing Procedure).

Το Εθνικό CSIRT πρωτοπορεί, επίσης, με την ανάπτυξη εξειδικευμένου συστήματος διαχείρισης περιστατικών, το οποίο αναμένεται να τεθεί σε πλήρη εφαρμογή εντός του 2019. Ο σχεδιασμός και η διαμόρφωση της πλατφόρμας CEFUI (όπως έχει ονομαστεί) καθιστά εύκολη και γρήγορη την αξιοποίηση διάφορων εργαλείων ανάλυσης και συλλογής πληροφοριών, και δίνει τη δυνατότητα γρήγορης συγκέντρωσης και γνωστοποίησης πληροφοριών σε φορείς κρίσιμων υποδομών, όπου αυτό κρίνεται απαραίτητο.

Στόχος της πλατφόρμας CEFUI, από επιχειρησιακής άποψης, είναι:

- αυτόματη και τακτική ανάκτηση δεδομένων από πολλαπλές πηγές,
- συσχέτιση και συνδυασμός πληροφοριών και δεδομένων που παράγονται ως αποτέλεσμα της ανάλυσης από πολλαπλά ανεξάρτητα εργαλεία,
- γρήγορη αποστολή ειδοποιήσεων στους φορείς κρίσιμων υποδομών μέσω συστήματος προειδοποίησης,
- καταγραφή των ενεργειών σχετικά με τη διερεύνηση των γεγονότων, και
- διατήρηση πληροφοριών σε σύστημα βάσης δεδομένων που ανήκει και διατηρείται αποκλειστικά από τον οργανισμό.

Σε πρόσφατη αξιολόγηση ωριμότητας στη βάση Ευρωπαϊκής Οδηγίας, ο Οργανισμός ENISA (European Union Agency for Network and Information Security) της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια, έχει αναδείξει το Εθνικό CSIRT της Κύπρου ως το πιο γρήγορα αναπτυσσόμενο κρατικό CSIRT στην Ευρωπαϊκή Ένωση, ενώ οι διεθνείς οργανισμοί FIRST και TI έχουν διαπιστεύσει τη λειτουργία της Ομάδας εντός του πρώτου έτους λειτουργίας της, σε χρόνο σημαντικά μικρότερο της συνήθους διαδικασίας.

Οι διαδικασίες, οι πολιτικές και η υποδομή του Εθνικού CSIRT θα είναι καθοριστικά στα πλαίσια της εξέτασης για επίσημη πιστοποίηση από τον οργανισμό Trusted Introducer εντός του 2019 με στόχο την ένταξη στις 24 πιστοποιημένες ομάδες (εκ των οποίων 6 μόνο είναι Εθνικά CSIRTs) από τις 340 και πλέον που είναι εγγεγραμμένες στον εν λόγω οργανισμό. Αυτή η διαπίστευση θα κατατάξει τον οργανισμό μας στην ομάδα των εκλεκτών CSIRTs παγκοσμίως.

1.9. Δημιουργία Ιστοσελίδας ΑΨΑ και Εθνικού CSIRT

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

Το Εθνικό CSIRT έχει επίσης δημιουργήσει τη δική του ιστοσελίδα (https//csirt.cy), η οποία παρέχει ειδοποιήσεις σχετικά με την κυβερνοασφάλεια, σχετικές νομοθεσίες, δημόσιες διαβουλεύσεις,

εκδηλώσεις της Ομάδας, καθώς και νέα και ανακοινώσεις. Μέχρι το τέλος του 2018 είχαν αναρτηθεί στην ιστοσελίδα του Εθνικού CSIRT 220 ενημερώσεις, προειδοποιήσεις και άρθρα σχετικά με περιστατικά κυβερνοασφάλειας. Η ιστοσελίδα του Εθνικού CSIRT, κατά το 2018, είχε 333 νέους χρήστες, οι οποίοι είχαν πρόσβαση σε 5.632 διαφορετικά τμήματα της ιστοσελίδας.

2. ΟΙΚΟΝΟΜΙΚΕΣ ΚΑΤΑΣΤΑΣΕΙΣ

2.1. Μη Ελεγμένες Οικονομικές Καταστάσεις για το έτος 2018

Οι οικονομικές καταστάσεις της Αρχής Ψηφιακής Ασφάλειας για το έτος που έληξε την 31η Δεκεμβρίου 2018, που είναι και οι πρώτες οικονομικές καταστάσεις, ετοιμάστηκαν όπως προβλέπεται από το άρθρο 25 του Ν.17(Ι)/2018. Οι βασικότερες πληροφορίες για την καταγραφή δαπανών και εσόδων, που περιέχονται στις μη ελεγμένες οικονομικές καταστάσεις για το έτος που έληξε στις 31 Δεκεμβρίου 2018, απεικονίζονται στα Γραφήματα 1 και 2 και περιλαμβάνουν:

α. έσοδα ύψους €1.040.057 και δαπάνες ύψους €1.004.787, και
β. πλεόνασμα έτους ύψους €35.270.

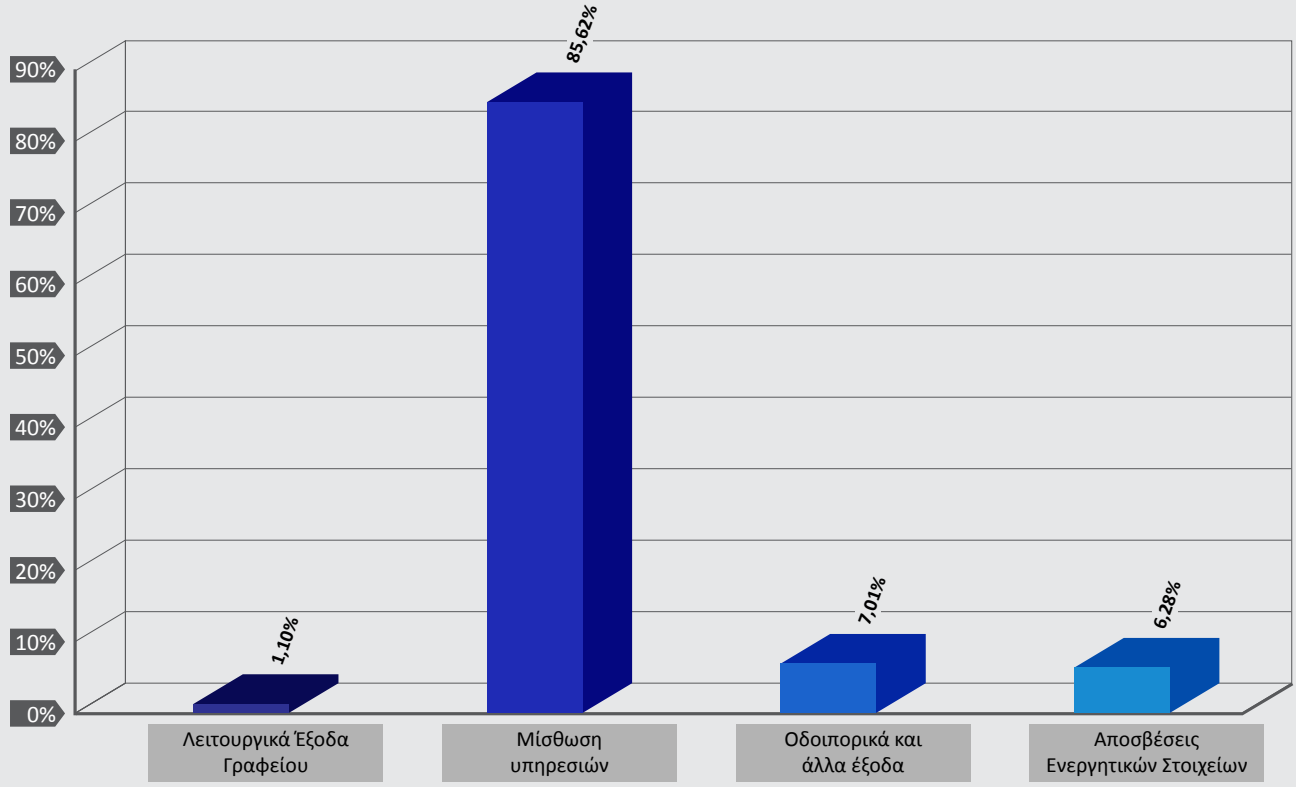
Πίνακας 2: Μη Ελεγμένη Κατάσταση Συνολικών Εισοδημάτων 2018

	2018 €
Έσοδα	
Άλλα έσοδα*	1.040.000
Τόκοι	57
	1.040.057
Έξοδα	
Κόστος προσωπικού**	0
Οδοιπορικά	35
Λειτουργικά έξοδα γραφείου	11.019
Μίσθωση υπηρεσιών	860.289
Άλλα έξοδα	70.366
Αποσβέσεις εξοπλισμού και εγκαταστάσεων	38.323
Αποσβέσεις άυλου ενεργητικού	24.755
	1.004.787
Πλεόνασμα/(Έλλειμμα) έτους από συνήθεις εργασίες	35.270
Συνολικά εισοδήματα για το έτος	**35.270**

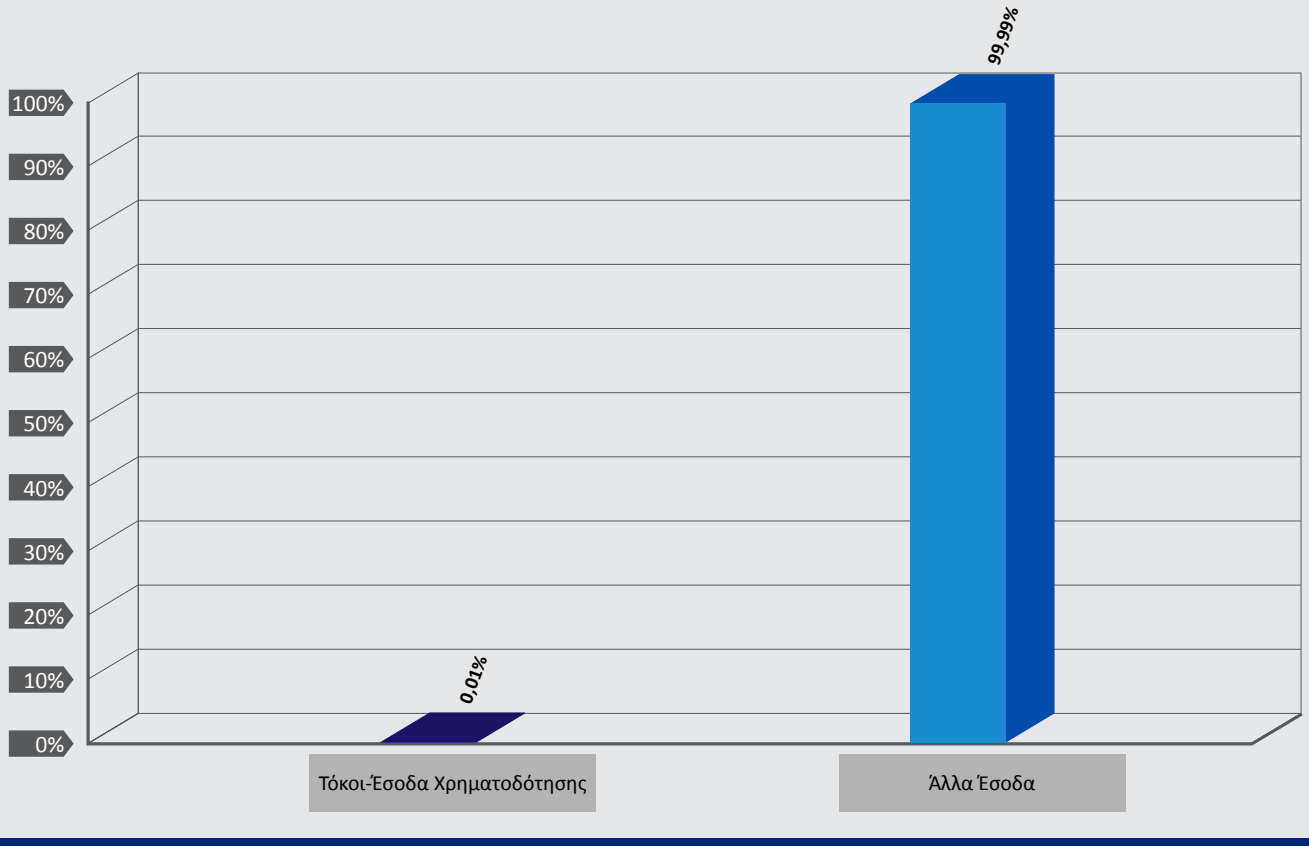
Σημείωση: Τα στοιχεία αφορούν τις μη ελεγμένες οικονομικές καταστάσεις, τα οποία δύναται να αναπροσαρμοστούν με την ετοιμασία των ελεγμένων οικονομικών καταστάσεων.

* Η πίστωση στο κονδύλι άλλα έσοδα για το 2018 αφορά χορηγία ΥΜΕΕ.
** Το CSIRT-CY στελεχώνεται με άτομα υπό καθεστώς αγοράς υπηρεσιών.

Γράφημα 1: Κατανομή Δαπανών για το 2018



Γράφημα 2: Κατανομή Εσόδων για το 2018



Πίνακας 3: Μη Ελεγμένη Κατάσταση Χρηματοοικονομικής Θέσης στις 31 Δεκ. 2018

	2018 €
ΠΕΡΙΟΥΣΙΑΚΑ ΣΤΟΙΧΕΙΑ	
Μη κυκλοφορούντα περιουσιακά στοιχεία	
Εγκαταστάσεις και εξοπλισμός	171.154
Άυλα στοιχεία ενεργητικού	50.261
Συνολο μη κυκλοφορούντων περιουσιακών στοιχείων	**221.415**
Κυκλοφορούντα περιουσιακά στοιχεία	
Χρεώστες και προπληρωμές	15.415
Μετρητά στην τράπεζα	673.787
Σύνολο κυκλοφορούντων περιουσιακών στοιχείων	**689.202**
ΣΥΝΟΛΟ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ	**910.617**
ΙΔΙΑ ΚΕΦΑΛΑΙΑ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ	
Ίδια κεφάλαια	
Αποθεματικά	35.270
Σύνολο ιδίων κεφαλαίων	**35.270**
Τρέχουσες υποχρεώσεις	
Πιστωτές και οφειλόμενα έξοδα	875.347
Ολικό τρεχουσών υποχρεώσεων	**875.347**
ΟΛΙΚΟ ΙΔΙΩΝ ΚΕΦΑΛΑΙΩΝ ΚΑΙ ΥΠΟΧΡΕΩΣΕΩΝ	**910.617**

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

3. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

3.1. Νομοθεσία ΑΨΑ

Στις 5 Απριλίου 2018, ιδρύθηκε βάσει νομοθεσίας η Αρχή Ψηφιακής Ασφάλειας ως ανεξάρτητη αρχή για την εφαρμογή των διατάξεων του περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμου του 2018 (17(Ι)/2018) στα πλαίσια εναρμόνισης με την Ευρωπαϊκή Οδηγία NIS 2016/1148, η οποία αφορά μέτρα για υψηλό κοινό επίπεδο ασφάλειας δικτύων και συστημάτων πληροφοριών. Η Αρχή Ψηφιακής Ασφάλειας λειτουργεί ως η εθνική αρμόδια αρχή για την ασφάλεια δικτύων και συστημάτων πληροφοριών και κυβερνοασφάλειας, μέρος της οποίας αποτελεί το Εθνικό CSIRT ως ο εθνικός φορέας άμεσης ανταπόκρισης σε συμβάντα που σχετίζονται με την ασφάλεια δικτύων και συστημάτων πληροφοριών. Με τη λειτουργία της Αρχής διασφαλίζεται η προστασία των κρίσιμων υποδομών πληροφοριών της Δημοκρατίας τόσο στον ιδιωτικό όσο και στο δημόσιο τομέα, καθώς και των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών του κράτους. Η ΑΨΑ χρηματοδοτείται από τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, τους Φορείς Κρίσιμων Υποδομών Πληροφοριών, τους παρόχους ηλεκτρονικών επικοινωνιών και παρόχους ψηφιακών υπηρεσιών στην Κύπρο, σύμφωνα με τη μεθοδολογία υπολογισμού τελών που καθορίζεται σε κανονισμούς που εκδίδονται δυνάμει των διατάξεων σχετικού νόμου.

3.1.1. Νόμος 17(Ι)/2018 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών

Στις 5 Απριλίου 2018, ψηφίστηκε ο Νόμος 17(Ι)/2018 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (https://dsa.cy/legislation/laws), βάσει του οποίου ιδρύθηκε η Αρχή Ψηφιακής Ασφάλειας και περιγράφει τις αρμοδιότητες της σύμφωνα με τις πρόνοιες της Οδηγίας NIS.

3.1.2. Αναθεωρημένος Νόμος περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών

Κατά το 2018, ετοιμάστηκε αναθεωρημένος Νόμος σχετικά με την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών, ο οποίος μεταφέρει τις αρμοδιότητες σε θέματα ασφάλειας δικτύων και πληροφοριών και κυβερνοασφάλειας στον τομέα Ηλεκτρονικών Επικοινωνιών από το ΓΕΡΗΕΤ στην ΑΨΑ, και ο οποίος περιγράφει με πλήρη λεπτομέρεια τις ολοκληρωμένες αρμοδιότητες της ΑΨΑ. Το νομοσχέδιο ρυθμίζει θέματα προσωπικού, εσωτερικής λειτουργίας της ΑΨΑ και συνεργασίας της με άλλους αρμόδιους φορείς. Η έγκριση του εν λόγω Νόμου από το Υπουργικό Συμβούλιο και η ψήφιση του από τη Βουλή αναμένεται εντός του 2019.

3.1.3. Κανονισμοί Χρηματοδότησης ΑΨΑ

Κατά το 2018, ετοιμάστηκαν οι Κανονισμοί περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Τέλη), που αφορούν τη χρηματοδότηση της ΑΨΑ. Επίσης, ολοκληρώθηκε σχετική Δημόσια Διαβούλευση για τους εν λόγω κανονισμούς, ως επίσης και οι διαβουλεύσεις με τα αρμόδια Υπουργεία και υπηρεσίες του κράτους. Η ψήφιση τους από τη Βουλή αναμένεται εντός του 2019.

3.1.4. Αξιολόγηση Κρισιμότητας Υποδομών

Η ΑΨΑ σε συνεργασία με εξωτερικούς συμβούλους προχώρησε στη διεξαγωγή έργου για την αξιολόγηση κρισιμότητας των υποδομών. Το έργο ξεκίνησε τον Αύγουστο του 2018 και είχε ως αντικείμενο την ανάλυση της κρισιμότητας για δυνητικά κρίσιμες υποδομές πληροφοριών στην Κυπριακή Δημοκρατία, σύμφωνα με τις πρόνοιες του Νόμου 17(Ι)/2018 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών.

Εντός του 2018, καθορίστηκαν από το Υπουργικό Συμβούλιο οι βασικές υπηρεσίες που είναι ζωτικής

σημασίας για τη λειτουργία του κράτους, της κοινωνίας και της οικονομίας της Κύπρου. Στο πλαίσιο της ίδιας διαδικασίας καθορίστηκαν και οι Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και οι Φορείς Κρίσιμων Υποδομών Πληροφοριών, ενώ αξιολογήθηκε το επίπεδο κρισιμότητας τους για την Κύπρο.

3.1.5. Μέτρα Ασφάλειας NIS

Η ΑΨΑ συνεργάστηκε με εξωτερικούς συμβούλους για την ετοιμασία Πλαισίου Μέτρων Ασφάλειας, σύμφωνα με την Οδηγία NIS, με το οποίο θα διαμορφωθεί ένα δομημένο πλαίσιο ελέγχου και διαδικασιών που θα εξασφαλίζει ένα ελάχιστο επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών στους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και τους Φορείς Κρίσιμων Υποδομών Πληροφοριών στην Κύπρο. Το έργο ξεκίνησε τον Οκτώβριο του 2018 και είχε ως αντικείμενο τη μελέτη βέλτιστων πρακτικών (και άλλων πηγών) και την ετοιμασία ολοκληρωμένου πλαισίου μέτρων ασφάλειας με σκοπό την εφαρμογή και υλοποίηση τους από τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και τους Φορείς Κρίσιμων Υποδομών Πληροφοριών στην Κύπρο.

Εντός του 2018, ολοκληρώθηκε το προσχέδιο του εν λόγω Πλαισίου με τη συμβολή των Κρίσιμων Υποδομών Πληροφοριών, καθώς και οι προτεινόμενες ενέργειες για την υλοποίηση του Πλαισίου στην Κύπρο. Το Πλαίσιο θα τεθεί σε δημόσια διαβούλευση εντός του 2019 με την ολοκλήρωση του έργου.

3.1.6. Κοινοποίηση Περιστατικών Παραβίασης Ψηφιακής Ασφάλειας

Η ΑΨΑ, στα πλαίσια έργου με εξωτερικούς συμβούλους, προχώρησε στην ετοιμασία σχετικής νομοθεσίας για τις κοινοποιήσεις περιστατικών παραβίασης ψηφιακής ασφάλειας. Από το έργο προέκυψε επίσης το προσχέδιο Δευτερογενούς Νομοθεσίας, το οποίο περιλαμβάνει, μεταξύ άλλων, τις διαδικασίες κοινοποίησης περιστατικών που οφείλουν να υποβάλλουν οι διάφοροι φορείς προς την ΑΨΑ, δηλαδή οι Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, οι Φορείς Κρίσιμων Υποδομών Πληροφοριών, οι παροχείς ηλεκτρονικών επικοινωνιών και οι παροχείς ψηφιακών υπηρεσιών, καθώς και τις διαδικασίες διασυνοριακών κοινοποιήσεων σύμφωνα με τις πρόνοιες της Οδηγίας NIS. Η σχετική νομοθεσία για τις κοινοποιήσεις περιστατικών παραβίασης ψηφιακής ασφάλειας θα τεθεί σε δημόσια διαβούλευση εντός του 2019, με στόχο την εφαρμογή της κατά το ίδιο έτος.

3.1.7. Εγγραφές Παροχέων Ψηφιακών Υπηρεσιών

Εντός του 2018, ετοιμάστηκε προσχέδιο Απόφασης για τις εγγραφές των παροχέων ψηφιακών υπηρεσιών στην Κύπρο. Η Απόφαση αυτή θα τεθεί σε δημόσια διαβούλευση εντός του 2019.

3.2. Νομοθεσία Ηλεκτρονικών Επικοινωνιών για την Ασφάλεια Δικτύων και Πληροφοριών

Τα θέματα αυτά διέπονται από τη νομοθεσία 112(Ι)/2004, ως έχει τροποποιηθεί, και τύγχαναν χειρισμού από την ομάδα για την Ασφάλεια Δικτύων και Πληροφοριών, η οποία επιλαμβάνεται και των θεμάτων της ΑΨΑ. Εντός του 2019, προγραμματίζεται όπως οι συγκεκριμένες πρόνοιες διαγραφούν από το Νόμο 112(Ι)/2004 και μεταφερθούν στο νέο νόμο περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών, κατ' εφαρμογή των σχετικών αποφάσεων του Υπουργικού Συμβουλίου.

Λεπτομέρειες αναφορικά με την παρακολούθηση της εφαρμογής του σχετικού Διατάγματος για την Ασφάλεια των Δικτύων και Πληροφοριών 253/2011 μέσα στο έτος 2018 περιλαμβάνονται στην Ετήσια Έκθεση 2018 του ΓΕΡΗΕΤ.

3.3. Ανάπτυξη Υποδομών και Εργαλείων

3.3.1. Υποδομή Εθνικού CSIRT

Στα πλαίσια του έργου Connecting Europe Facility (CEF) για την ανάπτυξη και βελτίωση της υποδομής του Εθνικού CSIRT (βλ. ενότητα 7.1.1), πραγματοποιήθηκε ανάλυση κινδύνου για το δίκτυο (LAN) και την υποδομή της Ομάδας. Η αξιολόγηση επικεντρώθηκε σε τέσσερις τομείς και συγκεκριμένα: Συστήματα, Δίκτυο, Ανθρώπινους Παράγοντες και Περιβαλλοντικούς Παράγοντες. Κύριος στόχος της ανάλυσης ήταν να επιτευχθεί το μέγιστο επίπεδο ασφάλειας για την υποδομή που να πληροί όλα τα χαρακτηριστικά και τις καλές πρακτικές στον τομέα της κυβερνοασφάλειας.

Η υποδομή της Ομάδας σχεδιάστηκε λαμβάνοντας υπόψη τα καλύτερα ευρωπαϊκά πρότυπα που αφορούν CSIRTs, τις καλύτερες πρακτικές και τις κατευθυντήρες γραμμές τις Ευρωπαϊκής Ένωσης με στόχο να μπορεί να προσφέρει υπηρεσίες υψηλού επιπέδου στον τομέα της.

Λαμβάνοντας υπόψη ότι η κύρια αποστολή της Ομάδας είναι η προστασία των κρίσιμων υποδομών, ο σχεδιασμός του δικτύου και οι σχετικές διαδικασίες έχουν γίνει με τρόπο ώστε οι υπηρεσίες που προσφέρονται να είναι απομονωμένες για την καλύτερη και ασφαλέστερη επεξεργασία δεδομένων. Επίσης, έχει δημιουργηθεί απομονωμένο εργαστήριο για αξιολόγηση κακόβουλων αρχείων (reverse engineering, malware analysis και sandbox), ενώ έχουν εφαρμοστεί αυτοματοποιημένα προγράμματα για την αποστολή ειδοποιήσεων στους κρίσιμους φορείς και την ανταλλαγή πληροφοριών μέσω της σύζευξης με εξειδικευμένες ευρωπαϊκές πλατφόρμες.

Μέχρι το τέλος του 2018, η Ομάδα έλαβε περίπου 10.521 ηλεκτρονικά μηνύματα από τις πλατφόρμες Shadow Server, CERT Bund, MISP, Abuse Helper και Team Cymru. Μετά από σχετική επεξεργασία, το Εθνικό CSIRT διαβίβασε περίπου 6.000 ηλεκτρονικά μηνύματα προς τις Εθνικές Υποδομές Κρίσιμων Πληροφοριών για την ενημέρωση τους, καθώς και συστάσεις για σχετικές ενέργειες από μέρους τους.

Λόγω του σωστού σχεδιασμού και παραμετροποίησης, καθώς και της εφαρμογής της νέας υποδομής, το Εθνικό CSIRT είναι σε θέση να υποστηρίζει όλες τις προσφερόμενες υπηρεσίες σε ψηλό επαγγελματικό επίπεδο. Εντός του 2018, ετοιμάστηκαν διαδικασίες και πολιτικές οι οποίες συνοδεύουν τη νέα υποδομή, ώστε, εντός του 2019, το Εθνικό CSIRT να εξετασθεί και να πιστοποιηθεί από τον οργανισμό Trusted Introducer (TI). Σημειώνεται ότι μόνο 23 οργανισμοί (εκ των οποίων μόνο 6 από αυτούς είναι Εθνικά CSIRTs), σε σύνολο πέραν των 340, είναι σήμερα πιστοποιημένοι από τον TI. Με την υλοποίηση του εν λόγω στόχου, το Εθνικό CSIRT θα έχει καταφέρει να πιστοποιηθεί σε εξαιρετικά σύντομο χρονικό διάστημα από την έναρξη λειτουργίας του, αφού η διαδικασία πιστοποίησης από τον TI ανέρχεται κατά μέσο όρο στα 7-8 χρόνια.

3.3.2. Ολοκληρωμένη Πλατφόρμα Διαχείρισης ΑΨΑ

Η ΑΨΑ υπέγραψε συμφωνία με εξωτερικούς συνεργάτες για τη δημιουργία ολοκληρωμένης πλατφόρμας διαχείρισης. Το έργο αυτό ξεκίνησε το Δεκέμβριο του 2018 και έχει ως αντικείμενο την αναβάθμιση του υφιστάμενου συστήματος RCMS (Risk and Compliance Management System) της Αρχής Ψηφιακής Ασφάλειας, το οποίο απέκτησε το ΓΕΡΗΕΤ ως μέρος της υλοποίησης του έργου για την ανάλυση επικινδυνότητας για θέματα κυβερνοασφάλειας σε εθνικό επίπεδο (National Level Cyber Risk Assessment – αρ. προσφοράς ΓΕΡΗΕΤ 06/2014). Το σύστημα αυτό μεταφέρθηκε στην ΑΨΑ μετά την ίδρυση της στα πλαίσια της ανάληψης όλων των προηγούμενων αρμοδιοτήτων του ΓΕΡΗΕΤ στον τομέα της ασφάλειας δικτύων και πληροφοριών και της κυβερνοασφάλειας.

Το αναβαθμισμένο σύστημα RCMS θα καλύπτει διάφορες ανάγκες στα πλαίσια της διαχείρισης κινδύνων σε οργανισμούς, όπως risk management, incident and loss management και compliance management. Η ανάπτυξη ενός ολοκληρωμένου συστήματος διαχείρισης (stakeholder management

platform) κρίθηκε αναγκαία λόγω του μεγάλου αριθμού των φορέων τους οποίους θα εποπτεύει η ΑΨΑ σε θέματα ασφάλειας δικτύων και πληροφοριών. Με τις κατάλληλες αλλαγές και αναβαθμίσεις, η υφιστάμενη πλατφόρμα RCMS που διαθέτει η ΑΨΑ, θα καλύψει τις αρχικές ανάγκες που εντοπίζονται στα πλαίσια εφαρμογής των καθηκόντων της. Το έργο αυτό αναμένεται να ολοκληρωθεί εντός του 2019. Η ΑΨΑ έχει υποβάλει πρόταση για ευρωπαϊκή συγχρηματοδότηση του εν λόγω έργου για την οποία αναμένεται σχετική απόφαση εντός του 2019. Το έργο θα διαρκέσει 18 μήνες και αναμένεται να ξεκινήσει εντός του 2019 με συνολικό προϋπολογισμό €129.000.

4. ΥΛΟΠΟΙΗΣΗ ΣΤΡΑΤΗΓΙΚΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

4.1. Υλοποίηση Δράσεων Στρατηγικής Κυβερνοασφάλειας

Εντός του 2018, διάφορες δραστηριότητες που έγιναν από την ΑΨΑ υλοποιούν μεγάλο μέρος Δράσεων της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας. Οι Δράσεις αυτές αναλύονται σε συγκεκριμένες ενότητες αυτής της Έκθεσης, ως ακολούθως:

Δράση 2	Δομές (βλ. ενότητα 1.3),
Δράση 4	Νομικό Πλαίσιο (βλ. ενότητα 3.1),
Δράση 7	Εντοπισμός Κρίσιμων Υποδομών Πληροφοριών (βλ. ενότητα 3.1.4),
Δράση 9	Εθνικό Πλαίσιο Κυβερνοασφάλειας (βλ. ενότητα 4.2)
Δράση 11	Εθνικό CSIRT (βλ. ενότητα 1.3.2, ενότητα 1.8, ενότητα 3.3.1),
Δράση 12	Εθνικές και Διεθνείς Ασκήσεις (βλ. ενότητα 4.3)
Δράση 13	Εκπαίδευση και Κατάρτιση (βλ. ενότητα 1.5),
Δράση 14	Δημιουργία Κουλτούρας Κυβερνοασφάλειας - Awareness (βλ. ενότητα 4.4)
Δράση 15	Διεθνής Συνεργασία (βλ. ενότητα 6)

4.2. Εθνικό Πλαίσιο Κυβερνοασφάλειας

Εντός του 2018, συνεχίστηκε η υλοποίηση του πρώτου σημαντικού παραδοτέου της Ομάδας Εργασίας για τη Δράση 9 της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, η οποία έχει ως στόχο την ετοιμασία του Εθνικού Πλαισίου Κυβερνοασφάλειας. Με βάση τον εν λόγω σχεδιασμό, ένας σημαντικός αριθμός κρίσιμων μέτρων ασφάλειας έχουν τεθεί σε εφαρμογή με μικρό σχετικά κόστος και σε σύντομο χρονικό διάστημα μέχρι την εφαρμογή του πλήρους Εθνικού Πλαισίου Κυβερνοασφάλειας. Σε πρώτο στάδιο τα μέτρα εφαρμόζονται στους οργανισμούς της Δημόσιας Υπηρεσίας.

4.3. Ασκήσεις Κυβερνοασφάλειας

Εντός του 2018, η ΑΨΑ συμμετείχε ενεργά στην προετοιμασία της πανευρωπαϊκής άσκησης "CYBER EUROPE 2018", υπό το συντονισμό του ENISA και τη συμμετοχή όλων των κρατών-μελών της Ευρωπαϊκής Ένωσης. Η ΑΨΑ συντόνισε επιτυχώς τις δραστηριότητες προετοιμασίας για τη συμμετοχή της Κύπρου στην εν λόγω άσκηση, κατά την οποία περισσότεροι από 1.000 επαγγελματίες στον τομέα της ασφάλειας στον κυβερνοχώρο από όλη την Ευρώπη (πάνω από 30 χώρες), ένωσαν τις δυνάμεις τους για να αντιμετωπίσουν μια προσομοίωση μαζικών κυβερνοεπιθέσεων ευρείας κλίμακας στον τομέα της αεροναυτιλίας. Η άσκηση βασιζόταν σε δραστηριότητες τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο με στόχο τη βελτίωση της ανθεκτικότητας των πληροφοριακών υποδομών ζωτικής σημασίας (κρίσιμες υποδομές πληροφοριών). Η ΑΨΑ είχε συνδρομή σε όλα τα στάδια προγραμματισμού της άσκησης, η οποία διεξήχθη τον Ιούνιο 2018, με την επιτυχή συμμετοχή του Εθνικού CSIRT, του Τμήματος Πολιτικής Αεροπορίας, της Hermes Airports και της CYTA.

Επίσης, στις 28 Μαρτίου 2018, πραγματοποιήθηκε η Παγκύπρια Άσκηση της Πολιτικής Άμυνας ("ΠΑ") "ΕΓΚΕΛΑΔΟΣ 2018", που προέβλεπε σεισμό με επίκεντρο τη Λάρνακα ισχύος 7,3 στην κλίμακα Ρίχτερ. Στην άσκηση ζητήθηκε από την ΠΑ να συμμετάσχει και η ΑΨΑ, όπως προβλέπει και το Ειδικό Εθνικό Σχέδιο ("ΕΕΣ") "ΕΓΚΕΛΑΔΟΣ". Με βάση το σενάριο της Άσκησης, ενεργοποιήθηκε και το ΕΕΣ "ΑΡΙΣΤΕΑΣ". Στην άσκηση, εκτός από το ΓΕΡΗΕΤ/ΑΨΑ, συμμετείχαν (όπως προβλέπει και το ΕΕΣ "ΑΡΙΣΤΕΑΣ") οι παροχείς ΑΤΗΚ, CABLENET, PRIMETEL, MTN, VELISTER και ΡΙΚ. Για τους σκοπούς της άσκησης εξετάστηκε η ικανότητα σύνταξης της Ομάδας Χειρισμού Κρίσεως υπό το συντονισμό της ΑΨΑ, όπως προνοείται

από το σχέδιο. Επίσης, εξετάστηκε η αποτελεσματικότητα της επικοινωνίας και ανταλλαγής εκθέσεων τρέχουσας κατάστασης, μεταξύ:

- ΓΕΡΗΕΤ/ΑΨΑ - Παροχέων,
- ΓΕΡΗΕΤ/ΑΨΑ - Κέντρου Επιχειρήσεων ΠΑ, και
- ΓΕΡΗΕΤ/ΑΨΑ - ΥΜΕΕ.

Στα πλαίσια της άσκησης εκτελέστηκαν διάφορα σενάρια που περιλάμβαναν περιστατικά διακοπής παροχής υπηρεσιών και εξετάστηκε η ετοιμότητα των εμπλεκόμενων παροχέων για την αποτελεσματική ανταπόκριση τους με στόχο τη μείωση των επιπτώσεων και αποκατάσταση των βλαβών. Μετά το πέρας της άσκησης έγινε ο ενδεδειγμένος απολογισμός, όπου σε συνεργασία με όλους τους εμπλεκόμενους φορείς εντοπίστηκαν οι ελλείψεις και αδυναμίες τόσο σε επίπεδο του ιδίου του Σχεδίου "ΑΡΙΣΤΕΑΣ" όσο και στο επίπεδο συντονισμού και βελτίωση των συνεργειών με άλλα ΕΕΣ του Βασικού Εθνικού Σχεδίου ("ΒΕΣ") "ΖΗΝΩΝ", έτσι ώστε να γίνουν οι κατάλληλες ενέργειες για βελτίωση. Τέλος, διαπιστώθηκε από όλους τους εμπλεκόμενους η ανάγκη για προγραμματισμό και διεξαγωγή και άλλων τακτικών ασκήσεων στα πλαίσια του ΕΕΣ "ΑΡΙΣΤΕΑΣ".

Επίσης, τον Ιούνιο του 2018, η ΑΨΑ, μέσω εκπροσώπων του Εθνικού CSIRT, συμμετείχε στην ελληνική Διακλαδική Άσκηση Κυβερνοάμυνας "ΠΑΝΟΠΤΗΣ 2018", υπό το συντονισμό του ΓΕΕΘΑ. Η άσκηση διεξήχθη σε πανελλαδικό επίπεδο και σε αυτή συμμετείχαν προσωπικό από τις ελληνικές Ένοπλες Δυνάμεις και τα Σώματα Ασφαλείας, φορείς του δημόσιου και ιδιωτικού τομέα, καθώς και της ακαδημαϊκής κοινότητας. Περισσότεροι από 200 συμμετέχοντες έλαβαν μέρος στην άσκηση για τον εντοπισμό και την αντιμετώπιση διαφόρων περιστατικών κυβερνοασφάλειας, καλύπτοντας τόσο μεμονωμένα συμβάντα όσο και περιστατικά ευρύτερης έκτασης που απαιτούσαν συντονισμένη ανταπόκριση σε πολλαπλά επίπεδα. Τα επεισόδια κάλυψαν πλειάδα αντικειμένων κυβερνοάμυνας, όπως ανάλυση ιομορφικού λογισμικού, ψηφιακή διερεύνηση πειστηρίων σε διαφορετικά λειτουργικά συστήματα Η/Υ, drones και δρομολογητές, έλεγχο ευπαθειών εφαρμογών διαδικτύου και ιστού και εντοπισμό/ανάλυση παραβίασης δικτυακής υποδομής.

4.4. Δημιουργία Κουλτούρας Κυβερνοασφάλειας - Awareness

Το 2018 ξεκίνησε η υλοποίηση της νέας Εθνικής Στρατηγικής για ένα Καλύτερο Διαδίκτυο για τα Παιδιά στην Κύπρο, η οποία είχε εγκριθεί από το Υπουργικό Συμβούλιο τον Δεκέμβριο του 2017. Προς αυτό το σκοπό, συστάθηκε και συνεδρίασε για πρώτη φορά η διυπουργική επιτροπή, που έχει ορισθεί για την εποπτεία εφαρμογής της Στρατηγικής και την ίδρυση και λειτουργία εθνικού κέντρου ενημέρωσης, εκπαίδευσης και έρευνας. Το κέντρο αναμένεται να συμβάλει τα μέγιστα στην επίτευξη των στόχων της πολιτικής του κράτους στον τομέα της κυβερνοασφάλειας.

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

Εντός του 2018, ολοκληρώθηκαν επίσης οι εργασίες της Δράσης του ευρωπαϊκού προγράμματος CEF με τίτλο CYberSafety (αριθμός Δράσης 2015-CY-IA-0034). Το πρόγραμμα έχει εγκριθεί εκ νέου από τις υπηρεσίες της Ευρωπαϊκής Ένωσης και θα συνεχίσει τις εργασίες του εντός του 2019 με την ίδια σύνθεση και αναθεωρημένο πρόγραμμα δραστηριοτήτων.

Οι εργασίες ενημέρωσης και εκπαίδευσης όλων των ομάδων - στόχων αποτελούν σημαντικό στοιχείο στην προώθηση της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, καθώς θα συμβάλουν τα μέγιστα στην καλύτερη υλοποίηση των υπολοίπων δράσεων της Στρατηγικής και θα βοηθήσουν όλους

τους πολίτες να αντιμετωπίσουν τους κινδύνους, να αποκτήσουν εμπιστοσύνη και να επωφεληθούν των ευκαιριών που φέρνουν μαζί τους οι νέες ψηφιακές τεχνολογίες.

4.5. Αναθεώρηση της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας

Κατά το 2018, η ΑΨΑ προχώρησε στη διαδικασία αναθεώρησης της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, αξιοποιώντας δεδομένα από διάφορες πηγές:

- τα αποτελέσματα της αξιολόγησης με τίτλο "Cybersecurity Capacity Assessment"[3] από το Πανεπιστήμιο της Οξφόρδης,
- τους Οδηγούς Καλών Πρακτικών, μεταξύ άλλων, από τον ENISA, την ITU και τον οργανισμό Meridian,
- το "Πακέτο Κυβερνοασφάλειας" της ΕΕ[4] ("EU Cybersecurity Package"), και
- τα διδάγματα από την εφαρμογή της υφιστάμενης Στρατηγικής.

Η Στρατηγική αναμένεται να ολοκληρωθεί και να προωθηθεί μέσω των αρμοδίων Υπουργείων για έγκριση από το Υπουργικό Συμβούλιο εντός του 2019.

[3] Αξιολόγηση της τρέχουσας κατάστασης στην Κύπρο σε σχέση με τον τομέα της κυβερνοασφάλειας που έγινε το 2017, βάσει επιστημονικού μοντέλου που αναπτύχθηκε από το Πανεπιστήμιο της Οξφόρδης
[4] https://ec.europa.eu/digital-single-market/en/cyber-security

5. ΔΙΑΧΕΙΡΙΣΗ ΣΥΜΒΑΝΤΩΝ ΚΑΙ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

5.1. Διαχείριση Περιστατικών

Η διαχείριση περιστατικών κυβερνοασφάλειας αποτελεί τον κύριο στόχο του Εθνικού CSIRT. Βάσει της δημοσιευμένης μελέτης του οργανισμού ENISA για την κατηγοριοποίηση και ταξινόμηση περιστατικών, το Εθνικό CSIRT έχει δημιουργήσει πολιτικές και διαδικασίες για τη σωστή διαχείριση περιστατικών κυβερνοασφάλειας σε όλους τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, τους Φορείς Κρίσιμων Υποδομών Πληροφοριών, τους παροχείς ηλεκτρονικών επικοινωνιών και τους παροχείς ψηφιακών υπηρεσιών. Λαμβάνοντας υπόψη την κρισιμότητα του κάθε οργανισμού, των υπηρεσιών που επηρεάζονται, καθώς και την κρισιμότητα του κάθε περιστατικού, το Εθνικό CSIRT είναι σε θέση να προβαίνει στις ανάλογες ενέργειες για τη μετρίαση και επίλυση του κάθε περιστατικού.

Η Ομάδα ξεκίνησε ενεργά να εξυπηρετεί τις κρίσιμες υποδομές στα τέλη του 2018, μετά από σχετική απόφαση του Υπουργικού Συμβουλίου για τον ορισμό των κρίσιμων υποδομών.

Στο παρελθόν, και από την ημέρα έναρξης λειτουργίας της Ομάδας, πολλοί οργανισμοί που δεν είχαν οριστεί ως κρίσιμες υποδομές, επικοινώνησαν εθελοντικά με το Εθνικό CSIRT για να κοινοποιήσουν περιστατικά. Τα κοινοποιημένα περιστατικά έτυχαν ανάλυσης και επίλυσης από το Εθνικό CSIRT. Λόγω του μικρού διαστήματος που αφορούσαν (Νοέμβριου-Δεκεμβρίου 2018), τα περιστατικά που αναφέρθηκαν ήταν περιορισμένα.

5.2. Διαχείριση Κρίσεων

5.2.1. ΒΕΣ "ΖΗΝΩΝ": ΕΕΣ "ΑΡΙΣΤΕΑΣ"

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

5.2.2. Συμμετοχή σε άλλα ΕΕΣ του ΒΕΣ "ΖΗΝΩΝ"

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

6. 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 εφαρμογή των αρμοδιοτήτων και τη διεκπεραίωση των εργασιών της ΑΨΑ, τόσο σε εθνικό όσο και σε ευρωπαϊκό και διεθνές επίπεδο. Τα θέματα ασφάλειας ιδιαίτερα στον κυβερνοχώρο δεν μπορούν να αντιμετωπιστούν μεμονωμένα, άρα απαιτείται συλλογική προσπάθεια στη διαχείριση τους.

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

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

6.1. Συνεργασία με Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και Φορείς Κρίσιμων Υποδομών Πληροφοριών

Το Εθνικό CSIRT στα πλαίσια της ενημέρωσης, εκπαίδευσης και δημιουργίας κλίματος εμπιστοσύνης μεταξύ οργανισμών έχει διοργανώσει μεγάλο αριθμό εκπαιδεύσεων προς τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και Φορείς Κρίσιμων Υποδομών Πληροφοριών με θεματολογία που αφορά την κυβερνοασφάλεια και την Οδηγία NIS. Επίσης, έγιναν παρουσιάσεις στους οργανισμούς αυτούς με θέμα τη λειτουργία του Εθνικού CSIRT και τις βασικές υπηρεσίες που προσφέρει.

6.2. Συνεργασία με Κρατικές Αρχές

Η Αρχή Ψηφιακής Ασφάλειας έχει στενή συνεργασία με διάφορα υπουργεία της Κυπριακής Δημοκρατίας, ως ακολούθως:

- Υπουργείο Μεταφορών, Επικοινωνιών και Έργων, σε θέματα στρατηγικής και πολιτικής ασφάλειας δικτύων και πληροφοριών,
- Υπουργείο Άμυνας, σε θέματα κυβερνοάμυνας,
- Υπουργείο Δικαιοσύνης, σε θέματα κυβερνοεγκλήματος,
- Υπουργείο Εξωτερικών, σε θέματα διεθνούς και ευρωπαϊκής συνεργασίας, και
- Υπουργείο Οικονομικών, σε οικονομικά θέματα κυβερνοασφάλειας και χρηματοδότησης δράσεων.

Επίσης, η ΑΨΑ έχει συνεργαστεί, μεταξύ άλλων, με τις ακόλουθες υπηρεσίες του Κράτους εντός του 2018:

- Γραφείο Καταπολέμησης Ηλεκτρονικού Εγκλήματος της Αστυνομίας Κύπρου, με ανταλλαγή πληροφοριών και αλληλοϋποστήριξη σε περιπτώσεις αντιμετώπισης περιστατικών κυβερνοασφάλειας/κυβερνοεγκλήματος,
- Εθνική Αρχή Ασφάλειας, για προστασία διαβαθμισμένων και άλλων ευαίσθητων πληροφοριών για αντιμετώπιση περιστατικών κυβερνοασφάλειας και λήψης μέτρων στις κρίσιμες υποδομές πληροφοριών,
- Κυπριακή Υπηρεσία Πληροφοριών, στα πλαίσια ανταλλαγής πληροφοριών και αλληλοενημέρωσης για την επίτευξη των κοινών στόχων προστασίας και θωράκισης της Κυπριακής Δημοκρατίας έναντι απειλών στον κυβερνοχώρο,
- Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, για την αντιμετώπιση και

πρόληψη περιστατικών επηρεασμού της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας προσωπικών δεδομένων,

- Κεντρική Τράπεζα της Κύπρου, σε θέματα που αφορούν την εποπτεία των τραπεζικών ιδρυμάτων στην Κύπρο στον τομέα της κυβερνοασφάλειας,
- Τμήμα Υπηρεσιών Πληροφορικής, σε θέματα που αφορούν την προστασία των συστημάτων πληροφορικής των κυβερνητικών υπηρεσιών και λειτουργίας του κυβερνητικού CSIRT,
- Τμήμα Ηλεκτρονικών Επικοινωνιών, σε θέματα συντονισμού για την εφαρμογή της Ψηφιακής Στρατηγικής της Κύπρου, και
- Κυπριακό Ερευνητικό και Ακαδημαϊκό Δίκτυο, σε θέματα λειτουργίας του ακαδημαϊκού CSIRT.

Η ΑΨΑ συνεργάστηκε με άλλες αρχές σε συναφή θέματα, όπως τη Δύναμη της Πολιτικής Άμυνας με την οποία τον Νοέμβριο του 2018 συμμετείχε σε Αξιολόγηση Ομοτίμων (Peer Review) για το Πρόγραμμα Εθνικής Αξιολόγησης Κινδύνων της Κυπριακής Δημοκρατίας. Η αξιολόγηση διοργανώθηκε από την Ευρωπαϊκή Επιτροπή σε συνεργασία με τη Δύναμη Πολιτικής Άμυνας. Το πρόγραμμα peer review χρηματοδοτείται από την Ευρωπαϊκή Επιτροπή. Η Κύπρος έχει ενταχθεί εθελοντικά στο εν λόγω πρόγραμμα. Η συμμετοχή στο πρόγραμμα αυτό κρίθηκε από το Υπουργείο Εσωτερικών ως ευκαιρία για περισσότερη τριβή με το θέμα και απόκτηση γνώσης, αλλά προπαντός επίγνωσης για το θέμα, δεδομένης της έλλειψης εμπειρίας σε ό,τι αφορά την αξιολόγηση κινδύνων (risk assessment) σε εθνικό επίπεδο.

Η ΑΨΑ συμμετείχε στην εν λόγω αξιολόγηση ενεργά συμβάλλοντας με τις εμπειρίες και γνώσεις που έχει αποκτήσει στο θέμα της αξιολόγησης κινδύνων σε εθνικό επίπεδο για θέματα κυβερνοασφάλειας. Μερικά από τα στοιχεία της προσέγγισης της ΑΨΑ στα σχετικά θέματα εντοπίστηκαν ως παραδείγματα καλών πρακτικών και η ΑΨΑ αποκόμισε αρκετά θετικά σχόλια από τους εμπειρογνώμονες της Ευρωπαϊκής Επιτροπής. Η τελική έκθεση θα ετοιμαστεί από την Ευρωπαϊκή Επιτροπή εντός του 2019.

6.3. Συνεργασία με Κράτη-Μέλη

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

6.4. Συνεργασία με Τρίτες Χώρες

6.4.1. Μνημόνιο Συναντίληψης με Israeli National Cyber Directorate

Εντός του 2018, η ΑΨΑ και το Israeli National Cyber Directorate [INCD] υπέγραψαν Μνημόνιο Συναντίληψης για την αντιμετώπιση κοινών απειλών στον κυβερνοχώρο και την προώθηση της εθνικής ετοιμότητας στον τομέα της κυβερνοασφάλειας, αναγνωρίζοντας ότι και τα δύο μέρη δραστηριοποιούνται ανεξάρτητα για τη διασφάλιση ενός ασφαλούς και σταθερού περιβάλλοντος. Το Μνημόνιο Συναντίληψης υπογράφηκε στις 20/12/2018 από την Επίτροπο, κ. Γιώργο Μιχαηλίδη, και από τον κ. Yigal Una εκ μέρους του Israeli National Cyber Directorate.

6.4.2. Πρόταση Συνεργασίας με Σουλτανάτο του Ομάν

Το Δεκέμβριο 2018, πραγματοποιήθηκε στο Μουσκάτ συνάντηση με αξιωματούχους του Σουλτανάτου του Ομάν στα πλαίσια της οποίας συμφωνήθηκε όπως υπογραφεί Μνημόνιο Συναντίληψης στους τομείς της εκπαίδευσης και ανταλλαγής τεχνογνωσίας στους διάφορους τομείς που αφορούν την κυβερνοασφάλεια.

6.5. Διεθνείς Εκπροσώπηση

Η εκπροσώπηση της ΑΨΑ σε επιτροπές σε εθνικό και διεθνές επίπεδο κατά το 2018 αναλήφθηκε από τον Επίτροπο, τον Βοηθό Επίτροπο, το Διευθυντή και τα στελέχη της Αρχής, ανάλογα με το επίπεδο εκπροσώπησης που απαιτείτο ή/και το αντικείμενο της κάθε επιτροπής. Αναφέρονται ενδεικτικά οι διάφοροι διεθνείς οργανισμοί και επιτροπές στις οποίες συμμετείχε η ΑΨΑ στο πλαίσιο της άσκησης των αρμοδιοτήτων της Αρχής:

ENISA (European Union Agency for Network and Information Security) o MB (Management Board) o NLO (National Liaison Officers) o Cyber Crisis Cooperation and Exercises
Article 13a Expert Group
NAPAC (National Public Authorities Representative Committee of European Cyber Security Organisation ECSO)
NIS Cooperation Group and relevant Work Streams
GFCE (Global Forum on Cyber Expertise)
OSCE (Organization for Security and Co-operation in Europe)
GSCG (General Security Competence Group)
Cyber Security Coordination
CSP (Cyber Security Professionals) Governance Board
CSIRT Community Groups (FIRST, TI)
CSIRT Network
CERT-EU
ITU (International Telecommunication Union)

Ειδική αναφορά γίνεται στα ευρωπαϊκά σώματα τα οποία επηρεάζουν άμεσα τη λειτουργία και τις εργασίες της ΑΨΑ και του Εθνικού CSIRT, την εναρμόνιση και την εφαρμογή της Οδηγίας NIS και της εθνικής νομοθεσίας. Συγκεκριμένα, η ΑΨΑ συμμετέχει στο NIS Cooperation Group, τη λειτουργία του οποίου συντονίζει το εκάστοτε κράτος-μέλος που έχει την προεδρία της Ευρωπαϊκής Ένωσης και καθορίζει τις πολιτικές εφαρμογής του ευρωπαϊκού νομοθετικού πλαισίου από όλα τα κράτη-μέλη. Εντός του 2018, έγιναν 5 συναντήσεις του NIS Cooperation Group, όπου συζητήθηκαν οι λεπτομέρειες υλοποίησης της Οδηγίας NIS σε στρατηγικό επίπεδο και έγινε συντονισμός ως προς την ενιαία προσέγγιση για την υλοποίηση της.

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

6.6. Συνέδρια

Η Αρχή Ψηφιακής Ασφάλειας πραγματοποίησε 3 συνέδρια/εκδηλώσεις κατά το 2018.

6.6.1. 1ο Ετήσιο Συνέδριο ΑΨΑ

Το 1ο συνέδριο πραγματοποιήθηκε στις 25 Ιανουαρίου 2018 στο ξενοδοχείο Χίλτον με θέμα την Ψηφιακή Ασφάλεια στην Κύπρο. Στο συνέδριο συμμετείχαν διακόσιοι και πλέον εκπρόσωποι από

υπουργεία και ανεξάρτητες αρχές της Κυπριακής Δημοκρατίας, εθνικούς και ιδιωτικούς φορείς κρίσιμων υποδομών πληροφοριών, ακαδημαϊκά ιδρύματα, επιχειρήσεις και εκπρόσωποι οργανισμών και εταιρειών από το εξωτερικό. Οι συμμετέχοντες προέρχονταν κυρίως από τους τομείς της ενέργειας, των μεταφορών, της υγείας, της υδατοπρομήθειας, των τραπεζικών και χρηματοπιστωτικών υπηρεσιών, των ηλεκτρονικών επικοινωνιών, των ψηφιακών υποδομών και των κρατικών υπηρεσιών ασφάλειας.

Στο συνέδριο παρουσιάστηκε ένα ευρύ φάσμα θεμάτων σχετικών με την κυβερνοασφάλεια, μεταξύ των οποίων τα αποτελέσματα μελέτης του Πανεπιστημίου της Οξφόρδης για τα επίπεδα κυβερνοασφάλειας στην Κύπρο. Η έκθεση περιλάμβανε τα επιτεύγματα, τις πιθανές αδυναμίες αλλά και τις προοπτικές που δημιουργούνται στον τομέα της κυβερνοασφάλειας, με σκοπό τη βελτίωση του επιπέδου ασφάλειας στην Κύπρο. Παρουσιάστηκαν επίσης τα σχέδια του Επιτρόπου για την αναθεώρηση της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, το νέο Πλαίσιο Κυβερνοασφάλειας (Cybersecurity Package) της Ευρωπαϊκής Επιτροπής και οι ενέργειες σε εθνικό επίπεδο για την υλοποίηση της Οδηγίας NIS (Network and Information Security) στην Κύπρο.

Κατά τη διάρκεια του συνεδρίου διενεργήθηκε, επίσης, ανοικτή συζήτηση. Στη συζήτηση συμμετείχαν ο Επίτροπος Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων μαζί με εκπρόσωπο του ENISA, εκπρόσωπο της PwC Ισραήλ και εκπρόσωπο του CERT Ρουμανίας, οι οποίοι απάντησαν σε ερωτήσεις που τέθηκαν από τους συνέδρους. Η συζήτηση επικεντρώθηκε γύρω από τη θεματική ενότητα: “Πως μπορούμε να συνεργαστούμε για την ασφάλεια στον κυβερνοχώρο στην Κύπρο”.

6.6.2. 2ο Ετήσιο Συνέδριο ΑΨΑ

Το 2ο συνέδριο πραγματοποιήθηκε στις 26 Ιουνίου 2018 στο Συνεδριακό Κέντρο Φιλοξενία με θέμα την Ευρωπαϊκή Οδηγία NIS και την κυβερνοασφάλεια στην Κύπρο. Στο συνέδριο συμμετείχαν πέραν των εκατό εκπροσώπων υπουργείων και ανεξάρτητων αρχών της Κυπριακής Δημοκρατίας, εθνικών και ιδιωτικών φορέων κρίσιμων υποδομών πληροφοριών, ακαδημαϊκών ιδρυμάτων, επιχειρήσεων και εκπρόσωποι οργανισμών και εταιρειών από το εξωτερικό.

Στόχος του συνεδρίου ήταν η γνωριμία με τη νεοσυσταθείσα Αρχή Ψηφιακής Ασφάλειας και το Εθνικό CSIRT, και συγκεκριμένα τον τρόπο με τον οποίο οι νέες υπηρεσίες μπορούν να συμβάλουν στη δημιουργία ενός ασφαλούς ψηφιακού περιβάλλοντος στην Κύπρο. Στο συνέδριο παρουσιάστηκαν οι ενέργειες σε εθνικό επίπεδο για την υλοποίηση της Ευρωπαϊκής Οδηγίας NIS (Network and Information Security) για την Ασφάλεια Δικτύων και Πληροφοριών, καθώς και οι υπηρεσίες του Εθνικού CSIRT, το οποίο με τη λειτουργία του ενισχύει την πρόληψη και την ετοιμότητα στον τομέα της ψηφιακής ασφάλειας και την αποτελεσματική αντιμετώπιση συμβάντων κυβερνοασφάλειας στην Κύπρο. Επιπρόσθετα, εμπειρογνώμονες παρείχαν πρακτικές προσεγγίσεις ως προς τους τρόπους εναρμόνισης με τις απαιτήσεις της Οδηγίας NIS και την εφαρμογή κατάλληλων μέτρων ασφάλειας από τους εμπλεκόμενους φορείς.

Στο συνέδριο απηύθυναν χαιρετισμό η κα Αφροδίτη Κουφτερού, εκ μέρους της Υπουργού Μεταφορών, Επικοινωνιών και Έργων, η κα. Rosheen Awotar-Mauree, εκπρόσωπος της Διεθνούς Ένωσης Τηλεπικοινωνίων ITU, και ο Επίτροπος Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων, κ. Γιώργος Μιχαηλίδης, ο οποίος παρουσίασε το όραμα και τους στόχους της Αρχής Ψηφιακής Ασφάλειας, τις άμεσες δραστηριότητες της νέας υπηρεσίας και τη σημασία τους για την οικονομία, την κοινωνία και τους πολίτες της Κυπριακής Δημοκρατίας.

6.6.3. Συνέδριο ITU – Cyber Drill

Το συνέδριο της Αρχής Ψηφιακής Ασφάλειας και της Ομάδας του Εθνικού CSIRT με θέμα “ITU Cyber Drill - ALERT (Applied Learning for Emergency Response Teams) for Europe Region” πραγματοποιήθηκε στη Λεμεσό στις 26 - 30 Νοεμβρίου 2018.

Στο συνέδριο συμμετείχαν εκπρόσωποι του διεθνούς οργανισμού ITU, της Ευρωπαϊκής Επιτροπής, των Ευρωπαϊκών οργανισμών ENISA και DECAF, του οργανισμού Regional Cooperation Council (RCC), του οργανισμού FIRST, δεκάδες εκπρόσωποι Εθνικών Ομάδων από το εξωτερικό εντός και εκτός Ευρωπαϊκής Ένωσης, εκπρόσωποι των κρίσιμων υποδομών της Κυπριακής Δημοκρατίας και εταιρείες που δραστηριοποιούνται στον τομέα της κυβερνοασφάλειας.

Τις δύο πρώτες μέρες πραγματοποιήθηκε εκπαίδευση με θέμα “CIRT Management” από το FIRST

στα μέλη του Εθνικού και Ακαδημαϊκού CSIRT της Κυπριακής Δημοκρατίας και στους εκπρόσωπους των κρίσιμων υποδομών. Η τρίτη μέρα ήταν η επίσημη έναρξη του συνεδρίου με πέραν των 215 συμμετεχόντων. Στα πλαίσια της τρίτης μέρας, πραγματοποιήθηκαν πάνω από 30 παρουσιάσεις σε θέματα όπως Incident Response, Malware Analysis, Threat Intelligence και Cyber Security Crisis Management.

Το συνέδριο συνέχισε την τέταρτη και πέμπτη μέρα με κύριο θέμα την αντιμετώπιση ηλεκτρονικών επιθέσεων σε θεωρητικό άλλα και επιχειρησιακό επίπεδο.

Στόχος του συνεδρίου ήταν να φέρει σε επαφή τους υπεύθυνους λήψης αποφάσεων σε διοικητικό επίπεδο διοίκησης με τους επαγγελματίες υπεύθυνους για την αναβάθμιση και διατήρηση υψηλών επιπέδων ασφάλειας στον κυβερνοχώρο και τα συστήματα των φορέων βασικών υπηρεσιών της Κυπριακής Δημοκρατίας, όπως της εκμετάλλευσης ενέργειας, νερού, μεταφορών, υγείας, τραπεζών και τηλεπικοινωνιών.

Η καθιέρωση αυτών των συνεδρίων είναι ζωτικής σημασίας αφού επιτρέπει τη διεθνή συνεργασία μεταξύ χωρών με κοινούς στόχους, όπως την ανάπτυξη της οικονομίας, την αύξηση των δυνατοτήτων κάθε χώρας στον κυβερνοχώρο, τη διασφάλιση της ασφάλειας, αλλά και τη διεθνή ενίσχυση της ανταγωνιστικότητας κάθε χώρας. Επίσης, αποτελεί μέρος της ευρύτερης στρατηγικής μας ώστε να καταστεί η Κύπρος περιφερειακό κέντρο εκπαίδευσης για την κυβερνοασφάλεια.

7. ΑΛΛΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

7.1. Συμμετοχή σε Ευρωπαϊκά Συγχρηματοδοτούμενα Προγράμματα

7.1.1. CEF CSIRT-CY

Η Αρχή Ψηφιακής Ασφάλειας ηγείται της Δράσης στα πλαίσια του προγράμματος Connecting Europe Facility (CEF) με τίτλο "Development and Enhancement of the Capabilities of the Cyprus National CSIRT" και στοχεύει στην ενίσχυση των υποδομών και διαδικασιών του Εθνικού CSIRT για την προστασία του κυβερνοχώρου των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών, των παροχέων ηλεκτρονικών επικοινωνιών και των παροχέων ψηφιακών υπηρεσιών της Κυπριακής Δημοκρατίας.

Συγκεκριμένα, η Δράση ενισχύει την περαιτέρω ανάπτυξη και βελτίωση των δυνατοτήτων του Εθνικού CSIRT ώστε να παρέχει προληπτικές υπηρεσίες και υπηρεσίες σε περίπτωση συμβάντων ασφάλειας στους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, τους Φορείς Κρίσιμων Υποδομών Πληροφοριών και τους παροχείς ηλεκτρονικών επικοινωνιών και παροχείς ψηφιακών υπηρεσιών στην Κύπρο. Η Δράση στοχεύει επίσης στη διευκόλυνση της διασυνοριακής συνεργασίας και ανταλλαγής πληροφοριών με άλλα ευρωπαϊκά CSIRT, χρησιμοποιώντας ήδη υπάρχουσες ή υπό-ανάπτυξη υποδομές, εργαλεία, μηχανισμούς και άλλα βασικά εργαλεία που χρησιμοποιούν οι κοινότητες CSIRT ανά τον κόσμο (π.χ. πλατφόρμα MISP). Η διασυνοριακή συνεργασία θα διευκολυνθεί επίσης με τη συμμετοχή στο δίκτυο CSIRT, σύμφωνα με το Άρθρο 12 της Οδηγίας NIS, και μέσω των συνεδριάσεων της ομάδας εργασίας για τις ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (TF-CSIRT).

Το πρόγραμμα υλοποιείται στο πλαίσιο συνεργασίας με πέντε (5) οργανισμούς από την Κύπρο και το εξωτερικό. Το εν λόγω έργο έχει διάρκεια 2 χρόνια και ξεκίνησε τον Οκτώβριο του 2017 με συνολικό προϋπολογισμό €1.283.283. Το έργο συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση μέσω του προγράμματος CEF Telecom.

7.1.2. CEF CYberSafety

Η Αρχή Ψηφιακής Ασφάλειας συμμετέχει επίσης στο Ευρωπαϊκό συγχρηματοδοτούμενο έργο "CYberSafety" με στόχο τη δημιουργία κουλτούρας ασφαλούς διαδικτύου για τα παιδιά. Το έργο "CYberSafety" στοχεύει στη δημιουργία μιας πλατφόρμας, όπου οι ενδιαφερόμενοι θα μπορούν να βρουν πληροφορίες και να χρησιμοποιήσουν εργαλεία, αλλά και να μοιραστούν εμπειρίες, εμπειρογνωμοσύνη και καλές πρακτικές που σχετίζονται με την ασφάλεια στο διαδίκτυο. Στόχος της πλατφόρμας είναι επίσης να συνεισφέρει σε μια ευρωπαϊκή προσέγγιση παρέχοντας ανατροφοδότηση σχετικά με θέματα που αφορούν το ασφαλές διαδίκτυο για τα παιδιά στην Κύπρο. Αυτό θα επιτευχθεί επιπλέον μέσω της γραμμής στήριξης Helpline, όπου οι χρήστες μπορούν να έχουν υποστήριξη από εξειδικευμένους επιστήμονες σε πραγματικό χρόνο σε θέματα αναφορικά με τη χρήση των διαδικτυακών τεχνολογιών. Επιπρόσθετα, η γραμμή Hotline θα εξασφαλίσει ότι οι χρήστες θα μπορούν να καταγγείλουν παράνομο περιεχόμενο και ενέργειες που σχετίζονται με παράνομη πορνογραφία, ρατσισμό και ξενοφοβία. Τα συμβάντα θα προωθούνται στην κατάλληλη αρχή για περαιτέρω διερεύνηση και δράση.

Το πρόγραμμα "CYberSafety" υλοποιείται στο πλαίσιο μιας συνεργασίας 8 οργανισμών από την Κύπρο και ξεκίνησε τις δράσεις του τον Ιούλιο του 2016, με συντονιστή το Παιδαγωγικό Ινστιτούτο του Υπουργείου Παιδείας και Πολιτισμού. Το έργο συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση μέσω του ευρωπαϊκού προγράμματος CEF Telecom.

7.1.3. CEF Ακαδημαϊκό CSIRT

Το έργο με τίτλο "Establishment of Cypriot Academic CSIRT" υλοποιείται στο πλαίσιο συνεργασίας της Αρχής Ψηφιακής Ασφάλειας με το Κυπριακό Ερευνητικό και Ακαδημαϊκό Δίκτυο. Το εν λόγω έργο ξεκίνησε το Σεπτέμβριο του 2018 με συντονιστή το Κυπριακό Ερευνητικό και Ακαδημαϊκό Δίκτυο και έχει συνολική διάρκεια 2 χρόνια.

Στόχος του προγράμματος είναι η ανάπτυξη του ακαδημαϊκού CSIRT στην Κύπρο, η οποία συμπεριλαμβάνει μεταξύ άλλων τα ακόλουθα:

- το σχεδιασμό και υλοποίηση του δικτύου του ακαδημαϊκού CSIRT,
- την ετοιμασία των διαδικασιών λειτουργίας του ακαδημαϊκού CSIRT,
- τη συμμόρφωση με το Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων GDPR, και
- την εκπαίδευση του προσωπικού και των ακαδημαϊκών εμπλεκόμενων φορέων.

Το έργο συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση μέσω του προγράμματος CEF Telecom.