ΥΦΥΠΟΥΡΓΕΙΟ ΕΡΕΥΝΑΣ, ΚΑΙΝΟΤΟΜΙΑΣ ΚΑΙ ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ

ΑΡΧΗ ΨΗΦΙΑΚΗΣ ΑΣΦΑΛΕΙΑΣ

Έγγραφο Πολιτικής

Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας 2020

Ασφάλεια Δικτύων και Πληροφοριών και Προστασία Κρίσιμων Υποδομών Πληροφοριών

Ιούνιος 2020

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΣΥΝΟΨΗ (Executive Summary)

Τα συστήματα και οι τεχνολογίες επικοινωνιών και πληροφορίας αποτελούν σήμερα έναν από τους πιο σημαντικούς παράγοντες οικονομικής και κοινωνικής ανάπτυξης, ενώ αδιαμφισβήτητα αποτελούν απαραίτητα εργαλεία στα πλαίσια των λειτουργικών και κοινωνικών δομών κάθε χώρας. Παράλληλα με την ανάπτυξη του κυβερνοχώρου, γίνεται όλο και πιο ουσιαστική η ανάγκη προστασίας των ηλεκτρονικών συστημάτων οργανισμών όλων των ειδών, έτσι ώστε οποιαδήποτε δραστηριότητα μέσω των τεχνολογιών αυτών να είναι ασφαλής. Ένα βασικό σύστημα ασφάλειας πρέπει να καλύπτει την εμπιστευτικότητα, την ακεραιότητα και την απρόσκοπτη διαθεσιμότητα της υποδομής και των πληροφοριών, ενώ πρέπει να καθιστά τη λειτουργία της υποδομής αξιόπιστη, ευέλικτη και ελεγχόμενη.

Η παρούσα Στρατηγική στοχεύει στη εδραίωση ενός ασφαλούς ηλεκτρονικού περιβάλλοντος στην Κυπριακή Δημοκρατία, με ειδικές πρόνοιες και δράσεις για την προστασία των κρίσιμων υποδομών Πληροφοριών, όπου η διαταραχή ή καταστροφή τους θα είχε σοβαρές επιπτώσεις στις ζωτικής σημασίας κοινωνικές λειτουργίες του τόπου. Η εκπόνηση της Στρατηγικής αυτής έχει ακολουθήσει μια ολιστική προσέγγιση για την ανταπόκριση στις απειλές του κυβερνοχώρου, με την αναγνώριση ότι μια σωστή στρατηγική πρέπει να περιέχει πολλαπλά επίπεδα ασφάλειας.

Βασικός σκοπός της Στρατηγικής Κυβερνοσφάλειας της Κυπριακής Δημοκρατίας είναι η προστασία των κρίσιμων υποδομών πληροφοριών του κράτους και η λειτουργία των τεχνολογιών επικοινωνιών και πληροφορικής του τόπου με τα απαιτούμενα επίπεδα ασφάλειας, προς όφελος του κάθε χρήστη, της οικονομίας και της χώρας. Με την υλοποίηση των δράσεων της Στρατηγικής επιδιώκεται όπως η Κύπρος να καταστεί μια από τις πρωτοπόρες χώρες της περιοχής στα θέματα κυβερνοασφάλειας, για την προστασία των κρίσιμών 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.

Το παρόν έγγραφο αναθεωρεί και αντικαθιστά την πρώτη Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας και έχει ως βασικό στόχο την αντιμετώπιση των απειλών που εμφανίζονται στον κυβερνοχώρο, σε Εθνικό επίπεδο. Ως τομείς προτεραιότητας για την επίτευξη του στόχου αυτού έχουν εντοπιστεί:

- η οργάνωση των αρμοδίων φορέων του κράτους,
- η δημιουργία ολοκληρωμένου νομοθετικού και ρυθμιστικού πλαισίου,
- η δημιουργία ή η προσαρμογή των απαραίτητων δομών και μηχανισμών εντός της Κυπριακής Δημοκρατίας,
- η διαμόρφωση τεχνικών και οργανωτικών μέτρων και διαδικασιών (σε σχέση με την προετοιμασία, την προστασία, τον εντοπισμό και την ανταπόκριση σε συμβάντα),
- η ανάπτυξη των απαραίτητων ικανοτήτων και η σχετική κατάρτιση,
- η αποδοτική συνεργασία του κράτους με αρμόδιους φορείς του δημοσίου και ιδιωτικού τομέα,
- η ανάπτυξη της έρευνας και της καινοτομίας.

Ως εκ τούτου, το παρόν έγγραφο περιέχει μια σειρά από δράσεις για την επίτευξη των προαναφερθέντων στόχων, στους ακόλουθους τομείς (θεματικές ενότητες):

- Δομές και Διακυβέρνηση (Governance)
- Θεσμοθέτηση της συνεργασίας μεταξύ αρμόδιων δημόσιων φορέων
- Νομικό και Ρυθμιστικό Πλαίσιο
- Εθνικό Πλαίσιο Κυβερνοασφάλειας
- Αξιολόγηση και Διαχείριση Κινδύνων – Αξιολόγηση Κρισιμότητας
- Αντιμετώπιση Συμβάντων και Διαχείριση Κρίσεων
- Ανάπτυξη Δυνατοτήτων – Διοργάνωση και συμμετοχή σε Ασκήσεις
- Ανταλλαγή Πληροφοριών –Επίγνωση Κατάστασης (Situational Awareness)
- Ενημέρωση - Δημιουργία Κουλτούρας Ασφάλειας
- Εκπαίδευση και Κατάρτιση
- Έρευνα και Καινοτομία
- Συνεργασία με τον Ιδιωτικό τομέα
- Ασφάλεια για όλους (Security for All)
- Διεθνής Συνεργασία

Στα Παραρτήματα Ι, παρατίθεται μια σύνοψη των δράσεων για εύκολη αναφορά. Για την σύνταξη της Στρατηγικής πέραν από τις Εθνικές ανάγκες στα θέματα Κυβερνοασφάλειας, έχουν ληφθεί υπόψη, κατά κύριο λόγο οι συστάσεις του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), καθώς και οι συστάσεις άλλων διεθνών σωμάτων όπως η Διεθνής Ένωση Τηλεπικοινωνιών (ITU). Επίσης η παρούσα Στρατηγική εντάσσεται και λαμβάνει υπόψη την ευρύτερη Στρατηγική για την Εθνική Ασφάλεια της Κυπριακής Δημοκρατίας.

1. ΕΙΣΑΓΩΓΗ

1.1. Η Κυβερνοασφάλεια Σήμερα

Τα συστήματα και οι τεχνολογίες επικοινωνιών και πληροφορίας αποτελούν σήμερα έναν από τους πιο σημαντικούς παράγοντες οικονομικής και κοινωνικής ανάπτυξης, ενώ αδιαμφισβήτητα αποτελούν απαραίτητα εργαλεία στα πλαίσια των λειτουργικών και κοινωνικών δομών κάθε χώρας. Παράλληλα με την ανάπτυξη του κυβερνοχώρου, γίνεται όλο και πιο ουσιαστική η ανάγκη προστασίας των ηλεκτρονικών συστημάτων οργανισμών όλων των ειδών, έτσι ώστε οποιαδήποτε δραστηριότητα μέσω των τεχνολογιών αυτών να είναι ασφαλής. Ένα βασικό σύστημα ασφάλειας πρέπει να καλύπτει την εμπιστευτικότητα, την ακεραιότητα και την απρόσκοπτη διαθεσιμότητα της υποδομής και των πληροφοριών, ενώ πρέπει να καθιστά τη λειτουργία της υποδομής αξιόπιστη, ευέλικτη και ελεγχόμενη.

Η ασφάλεια των υποδομών αναφέρεται στη δυνατότητα και την ανθεκτικότητα τους να αντιμετωπίσουν κινδύνους και βλάβες που δυνατόν να προκληθούν στα διάφορα δομοστοιχεία τους. Τα μέτρα ασφάλειας που λαμβάνονται στοχεύουν κυρίως στην αύξηση της ετοιμότητας και την ενίσχυση των δυνατοτήτων πρόληψης, στον εντοπισμό και την αντίδραση σε ενδεχομένους κινδύνους, περιλαμβανομένων κακόβουλων ενεργειών ή και επιθέσεων, καθώς και στη λήψη μέτρων για μετριασμό και αποκατάσταση τυχόν βλαβών, δυσλειτουργιών και της διαθεσιμότητας των παρεχομένων υπηρεσιών, συμπεριλαμβανομένων και καταστάσεων έκτακτης ανάγκης ή κρίσης.

Στο παρόν έγγραφο, χρησιμοποιούνται οι όροι ***'ασφάλεια δικτύων και πληροφοριών'*** και ***'κυβερνοασφάλεια'***. Η 'ασφάλεια δικτύων και πληροφοριών' αναφέρεται στην διατήρηση των στοιχείων της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, όπως περιγράφονται πιο κάτω. Η 'κυβερνοασφάλεια' αναφέρεται στην ευρύτερη ασφάλεια των δικτυωμένων συστημάτων που λειτουργούν στον κυβερνοχώρο, ως επί το πλείστων δηλαδή συνδεδεμένων στο Διαδίκτυο, και ο όρος αυτός συμπεριλαμβάνει και την ασφαλή χρήση των συστημάτων αυτών από τελικούς χρήστες.[1]

Διευκρινίζεται ότι το επίπεδο ασφάλειας των πληροφοριών πρέπει να ξεκινά από τον καθορισμό της ***αξίας*** της πληροφορίας (και των υπηρεσιών), ανεξαρτήτως της μορφής στην οποία βρίσκεται (φυσική ή ηλεκτρονική). Αυτή η παράμετρος θα λαμβάνεται υπόψη κατά την υλοποίηση των Δράσεων του παρόντος εγγράφου, και ειδικότερα αυτών που έχουν να κάνουν με την ενημέρωση του πληθυσμού για σκοπούς καλλιέργειας επίγνωσης και κουλτούρας ασφάλειας. Σαν γενικότερη αρχή, η πληροφορία σε φυσική ή ηλεκτρονική μορφή θα πρέπει να προστατεύεται επαρκώς, ανάλογα με την αξία της.

Η ασφάλεια δικτύων και πληροφοριών αποτελεί βασικό επακόλουθο της ανάπτυξης και διάδοσης των νέων τεχνολογιών επικοινωνιών και πληροφορικής. Λαμβάνοντας υπόψη την παγκοσμιοποίηση των επικοινωνιών, ιδιαίτερα με τη χρήση του Διαδικτύου αλλά και των συνεχώς αυξανόμενων κινδύνων που αντιμετωπίζουν οι χρήστες σε όλα τα επίπεδα, καθίσταται επιτακτική η ανάγκη λήψης μέτρων επαρκούς προστασίας αλλά και καθολικής συνεργασίας μεταξύ όλων των φορέων της κοινωνίας, δημόσιου και ιδιωτικού τομέα, σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο. Οι πολίτες, οι επιχειρήσεις και οι

[1] Το πρότυπο ISO 27032 αναφέρεται στη "διατήρηση των στοιχείων της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας πληροφοριών στον κυβερνοχώρο και βασίζεται στην ασφάλεια των πληροφοριών, στην ασφάλεια των εφαρμογών, στην ασφάλεια δικτύων και στην ασφάλεια του Διαδικτύου ως θεμελιώδεις δομικές μονάδες.

κυβερνήσεις έχουν ανάγκη να εμπιστεύονται τα μέσα στα οποία διακινούνται σημαντικές πληροφορίες, προσωπικά και άλλα δεδομένα.

Η συνέχιση της ασφαλούς ανάπτυξης των τεχνολογιών επικοινωνιών και πληροφορικής είναι σημαντική για τους πολίτες και τις κοινωνίες, για την ανάπτυξη του τομέα εργασίας αλλά και της οικονομίας ευρύτερα, τόσο σε εθνικό αλλά και σε ευρωπαϊκό και διεθνές επίπεδο. Οι επενδύσεις στον τομέα της ασφάλειας, υποβοηθούν την αύξηση της εμπιστοσύνης των χρηστών στις νέες υπηρεσίες και συμβάλλουν στην ευρύτερη ανάπτυξη της οικονομίας και της κοινωνίας. Τόσο οι κυβερνήσεις όσο και οι επιχειρήσεις θα πρέπει να αξιολογήσουν τις επενδύσεις στο τομέα αυτό με βασικό κριτήριο το κόστος που θα έχουν σε περίπτωση αποτυχίας των μηχανογραφικών τους συστημάτων ή συστημάτων επικοινωνιών λόγω κακόβουλων ενεργειών ή φυσικών αιτιών.

Η ασφάλεια στον κόσμο της πληροφορικής και των ηλεκτρονικών επικοινωνιών αναφέρεται στη διασφάλιση τριών παραμέτρων[2]:

- της **εμπιστευτικότητας (confidentiality)** των πληροφοριών, δηλαδή το να επιτρέπεται η πρόσβαση στις πληροφορίες μόνο από εξουσιοδοτημένα πρόσωπα,
- της **ακεραιότητας (integrity)** των πληροφοριών, δηλαδή της προστασίας των πληροφοριών από οποιαδήποτε ανεπιθύμητη αλλοίωση ή καταστροφή,
- της **διαθεσιμότητας (availability)** των πληροφοριών ή συστημάτων, δηλαδή το να μπορεί ένα σύστημα να παρέχει την πληροφορία όταν του ζητηθεί.

Η διασφάλιση των πιο πάνω παραμέτρων στοχεύει στη διατήρηση της ασφάλειας δικτύων και πληροφοριών στο μεγαλύτερο δυνατό βαθμό σε σχέση με την:

- προστασία των πληροφοριών **κατά τη μεταφορά τους** (data in transit)
- προστασία των πληροφοριών **κατά την επεξεργασία τους** (data in processing)
- προστασία των πληροφοριών **κατά την αποθήκευση τους** (data in storage).

Πέραν από τη προστασία των υποδομών, συστημάτων και πληροφοριών, η διατήρηση υψηλού επιπέδου ασφάλειας με βάση τις παραμέτρους που αναφέρονται πιο πάνω είναι απαραίτητη για την οικοδόμηση **εμπιστοσύνης** στα πληροφοριακά συστήματα, τις επικοινωνίες και στις ηλεκτρονικές υπηρεσίες του κράτους και άλλων σημαντικών οργανισμών στην Κύπρο. Η ανάπτυξη εμπιστοσύνης των πολιτών στα συστήματα αυτά και η εξασφάλιση ασφαλών συναλλαγών στον κυβερνοχώρο θα συμβάλει σημαντικά στην οικονομική ανάπτυξη του τόπου και στην εκπλήρωση των στόχων του Ψηφιακού Θεματολογίου για την Κύπρο.

1.2. Κρίσιμες Υποδομές Πληροφορίας

Οι υποδομές πληροφοριών στην Κυπριακή Δημοκρατία είναι πλέον πάρα πολλές και έχουν διεισδύσει σχεδόν σε κάθε σημείο της ζωής του μέσου πολίτη. Οι υποδομές αυτές χρησιμοποιούνται όχι μόνο άμεσα (π.χ. με τη χρήση τηλεφώνου, Διαδικτύου, κλπ.), αλλά και έμμεσα αφού όλες σχεδόν οι ζωτικές υπηρεσίες στη χώρα που χρησιμοποιεί ο πολίτης υποστηρίζονται από υποδομές πληροφοριών. Ορισμένες από αυτές τις υποδομές αποτελούν ζωτικό τμήμα της Κυπριακής οικονομίας και της

[2] Οι παράμετροι αυτοί μαζί συντάσσουν την ευρύτερη έννοια της ***ανθεκτικότητας (resilience)*** των σχετικών υποδομών και συστημάτων.

κοινωνίας, είτε παρέχοντας βασικά αγαθά και υπηρεσίες ή αποτελώντας την πλατφόρμα στήριξης άλλων (κρίσιμων) υποδομών. Θεωρούνται έτσι *κρίσιμες υποδομές πληροφορίας*, δεδομένου ότι η αδρανοποίηση ή η καταστροφή τους θα είχε σοβαρές επιπτώσεις σε ζωτικής σημασίας δραστηριότητες της κοινωνίας.

Καθίσταται λοιπόν αναγκαία, μέσω ενός ευρύτερου πλαισίου στρατηγικής κυβερνοασφάλειας ενός κράτους, να δοθεί ιδιαίτερη έμφαση στην προστασία αυτών των κρίσιμων υποδομών πληροφορίας. Αριθμός δράσεων που περιγράφονται στο παρόν έγγραφο καλύπτουν την προστασία κρίσιμων υποδομών πληροφορίας, αλλά και τον ευρύτερο χώρο της κυβερνοασφάλειας, αφού οι δύο τομείς είναι πολύ στενά συνδεδεμένοι και αλληλοεπιδρούν ο ένας στον άλλο. Η ενότητα 3.5 «Αξιολόγηση και Διαχείριση Κινδύνων – Αξιολόγηση Κρισιμότητας», αναφέρεται σε μεγαλύτερη λεπτομέρεια στη διαδικασία που χρησιμοποιείται για τον καθορισμό των κρίσιμων υποδομών πληροφορίας στην Κυπριακή Δημοκρατία.

1.3. Σκοπός

Ο σκοπός της Στρατηγικής Κυβερνοσφάλειας της Κυπριακής Δημοκρατίας είναι η προστασία των κρίσιμων υποδομών πληροφοριών του κράτους και η λειτουργία των τεχνολογιών επικοινωνιών και πληροφορικής του τόπου με τα απαιτούμενα επίπεδα ασφάλειας, προς όφελος του κάθε χρήστη, της οικονομίας και της χώρας.

1.4. Όραμα

Η Κύπρος να 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 χρηματοδοτικές υπηρεσίες.

1.5. Στόχοι

Η παρούσα Στρατηγική και οι Δράσεις που καταγράφονται στο κεφάλαιο 3 πιο κάτω, προωθούν τους πιο κάτω βασικούς στόχους:

- την υποστήριξη των στόχων του κράτους που έχουν τεθεί στο στρατηγικό έργο 'Ψηφιακή Κύπρος' για την ανάπτυξη κατάλληλων συνθηκών προώθησης και υποστήριξης της Κοινωνίας της Πληροφορίας,
- την υποστήριξη επίτευξης των στόχων της Ψηφιακής Στρατηγικής της Κύπρου[3], με ιδιαίτερη έμφαση στον τομέα της Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών, και έμμεση υποστήριξη των υπολοίπων δραστηριοτήτων της,
- τη θεσμοθέτηση της συνεργασίας μεταξύ δημόσιων φορέων και αρμοδίων αρχών (Ασφάλεια υποδομών, Κυβερνοέγκλημα, Κυβερνοάμυνα και Διεθνής συνεργασία), και την ενίσχυση της

3 http://www.mcw.gov.cy/mcw/dec/dec.nsf/all/0BACA0B7B7848D2CC22579B500299BFA/$file/Main%20document%20digital%20strategy.pdf?openelement

συνεργασίας μεταξύ των αρμοδίων αρχών, των κρίσιμων υποδομών πληροφοριών και των επιχειρήσεων (συμπεριλαμβανομένων των μικρομεσαίων επιχειρήσεων (SMEs) και των Νεοφυών επιχειρήσεων (Start Ups)),

- τη δυνατότητα υποστήριξης των εθνικών σχεδιασμών για την προστασία των κρίσιμων υποδομών πληροφοριών (Critical Information Infrastructure Protection- CIIs) και ευρύτερα την προστασία των κρίσιμων υποδομών της Κυπριακής Δημοκρατίας (Critical Infrastructure Protection – CIP)
- τη διατήρηση και ανάπτυξη ενός ηλεκτρονικά ασφαλισμένου επιχειρηματικού περιβάλλοντος στην Κύπρο, την προώθηση της συνεργασίας δημόσιου και ιδιωτικού τομέα, και τη δημιουργία και ανάπτυξη οικοσυστημάτων για τη προώθηση της Κυβερνοασφάλειας σε τομεακό επίπεδο,
- την ανάπτυξη εμπιστοσύνης από τους πολίτες και επιχειρήσεις/οργανισμούς στην ασφάλεια της ηλεκτρονικής διακυβέρνησης, συμπεριλαμβανομένης της διατήρησης του απορρήτου πληροφοριών κατά την μεταφορά, επεξεργασία και αποθήκευση τους.
- την ενημέρωση της κοινωνίας στα ευαίσθητα θέματα κυβερνοασφάλειας, και την εδραίωση ενός ασφαλούς ηλεκτρονικού περιβάλλοντος στην Κυπριακή Δημοκρατία για όλους τους πολίτες της,
- την προώθηση και ενίσχυση προγραμμάτων κατάρτισης και εκπαιδευτικών προγραμμάτων για τους μαθητές, φοιτητές, εργαζόμενους, του επαγγελματίες του χώρου και τους πολίτες από όλα τα κοινωνικά στρώματα σε όλες τις ηλικίες στο μεγαλύτερο δυνατό βαθμό,
- την προώθηση και ενίσχυση προγραμμάτων έρευνας και καινοτομίας στο τομέα της Κυβερνοασφάλειας, την προώθηση ακαδημαϊκών και άλλων
- την μείωση ή και την αποφυγή των αρνητικών επιπτώσεων από απειλές στον κυβερνοχώρο και την αποτελεσματική αντιμετώπιση έκτακτων περιστατικών,
- την υποστήριξη των στόχων του Κανονισμού για την προστασία προσωπικών δεδομένων (General Data Protection Regulation – GDPR), και γενικότερα σε θέματα ιδιωτικότητας (privacy) αλλά και την εξισορρόπηση των ρυθμιστικών παρεμβάσεων μεταξύ ασφάλειας και ιδιωτικότητας.

1.6. Κατευθυντήριες Αρχές (Guiding Principles)

Η δομή και το περιεχόμενο του παρόντος εγγράφου βασίζεται στις πιο κάτω κατευθυντήριες αρχές:

- την υλοποίηση του οράματος της στρατηγικής για ολόκληρο το κράτος και για ολόκληρο το κοινωνικό σύνολο.
- την συνολική κατανόηση και ανάλυση του ψηφιακού περιβάλλοντος, και την προσαρμογή των δράσεων στις ιδιαίτερες συνθήκες της χώρας και στις προτεραιότητες του κράτους
- την ενεργό συμμετοχή όλων των ενδιαφερομένων μερών στην εφαρμογή της στρατηγικής και την αντιμετώπιση των αναγκών και των ευθυνών τους,
- την ανάπτυξη στενής συνεργασίας και συνεργιών μεταξύ των εμπλεκομένων φορέων, και μεταξύ των αρμοδίων αρχών σε όλα τα απαραίτητα επίπεδα, λαμβάνοντας υπόψη τις αρμοδιότητες των εμπλεκομένων υπηρεσιών, και των απαιτούμενων συνεργασιών σε εθνικό και διεθνές επίπεδο, την ανάπτυξη ολιστικής προσέγγισης για την ανταπόκριση στις απειλές από τον κυβερνοχώρο, επιτρέποντας την αποτελεσματική διαχείριση των κινδύνων στον κυβερνοχώρο και προάγοντας την ανθεκτικότητα των οικονομικών και κοινωνικών δραστηριοτήτων,

- την αναγνώριση ότι μια σωστή στρατηγική πρέπει να περιέχει πολλαπλά επίπεδα ασφάλειας (layered security, defence in depth),
- τη χρήση ανοικτών διαδικασιών σε όλα τα στάδια υλοποίησης της Στρατηγικής, και την αξιοποίηση των διαθέσιμων μέσων πολιτικής για την υλοποίηση καθενός από τους στόχους της στρατηγικής, λαμβάνοντας υπόψη τις ιδιαίτερες συνθήκες της χώρας
- τον καθορισμό υψηλών στόχων στο ανώτατο επίπεδο της κυβέρνησης και την επίδειξη βούλησης από την πολιτεία ώστε, η Στρατηγική και οι Δράσεις της να συνδράμουν πραγματικά στην οριστική αλλαγή και βελτίωση του επιπέδου ηλεκτρονικής ασφάλειας στην Κύπρο καθώς και στην οικονομική και κοινωνική ευημερία, μεγιστοποιώντας τη συμβολή των ΤΠΕ στην αειφόρο ανάπτυξη και την κοινωνική συνοχή.
- την υπεύθυνη ανάθεση των σχετικών ρόλων και αρμοδιοτήτων και την κατανομή επαρκών ανθρώπινων και οικονομικών πόρων,
- τον σεβασμό των θεμελιωδών ανθρώπινων δικαιωμάτων και αξιών.

1.7. Τομείς Προτεραιότητας

Η παρούσα Στρατηγική αναλύεται σε επιμέρους τομείς προτεραιότητας που έχουν εντοπιστεί για τη βέλτιστη προστασία των κρίσιμων υποδομών πληροφορίας, την ασφαλή χρήση των νέων τεχνολογιών και στην επίτευξη υψηλού επιπέδου κυβερνοασφάλειας. Οι τομείς στους οποίους δίδεται προτεραιότητα σε σχέση με τις ανάγκες της Κυπριακής Δημοκρατίας είναι οι ακόλουθοι, όπως φαίνονται και στο Γράφημα 1:

- **ανάπτυξη εμπιστοσύνης μεταξύ όλων των εμπλεκομένων** στην υλοποίηση της Στρατηγικής, για τη διασφάλιση σωστής και αποτελεσματικής συνεργασίας,
- **επέκταση του νομοθετικού πλαισίου** από τις αρμόδιες υπηρεσίες του κράτους που να καλύπτει όλες τις πτυχές της κυβερνοασφάλειας, συμπεριλαμβανομένου του κυβερνοεγκλήματος (cybercrime) και της προστασίας των προσωπικών δεδομένων,
- **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,
- **ανάπτυξη των απαραίτητων ικανοτήτων σε οργανισμούς και σε επιχειρήσεις καθώς και στις υπηρεσίες του κράτους** επί των θεμάτων κυβερνοασφάλειας,
- **αποδοτική συνεργασία του κράτους με αρμόδιους φορείς του δημόσιου και ιδιωτικού τομέα**, τόσο σε εθνικό όσο και σε διεθνές επίπεδο,
- **δημιουργία ή προσαρμογή των απαραίτητων δομών και μηχανισμών** εντός των αρμοδίων υπηρεσιών και ευρύτερα εντός της Κυπριακής Δημοκρατίας, ώστε να διασφαλιστούν οι απαιτήσεις και οι δυνατότητες άμεσης ανταπόκρισης σε συμβάντα και κρίσεις στον κυβερνοχώρο.
- **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 πληροφοριών της Κυπριακής Δημοκρατίας.

Γράφημα 1: Τομείς Προτεραιότητας της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας

2. ΠΕΡΙΒΑΛΛΟΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

2.1. Ευρωπαϊκή Πολιτική

Τα θέματα ασφάλειας αποτελούν σημαντικό πυλώνα του Ψηφιακού Θεματολογίου για την Ευρώπη. Με δεδομένες τις τεχνολογικές αλλαγές και τον ψηφιακό μετασχηματισμό που βρίσκεται σε εξέλιξη, αλλά και την αύξηση των προκλήσεων και των κίνδυνων από τον κυβερνοχώρο, η συγκεκριμένη Ευρωπαϊκή πολιτική καλύπτει σημαντικά θέματα που αφορούν τον τομέα της ασφάλειας:

- Κύριος στόχος είναι οι πολίτες / η κοινωνία, οι επιχειρήσεις (συμπεριλαμβανομένων των μικρομεσαίων επιχειρήσεων, ΜΜΕ) και οι δημόσιες διοικήσεις να έχουν ασφαλή πρόσβαση στην τελευταία τεχνολογία ψηφιακής ασφάλειας, λαμβάνοντας υπόψη την διαλειτουργικότητα, τον ανταγωνισμό, την αξιοπιστία και τον σεβασμό των θεμελιωδών δικαιωμάτων των πολιτών, συμπεριλαμβανομένου του δικαιώματος στην ιδιωτική ζωή. Αυτό επιτυγχάνεται με την βελτίωση των δυνατοτήτων αντιμετώπισης των κινδύνων στον κυβερνοχώρο, την ενίσχυση της ανθεκτικότητας των υποδομών και της συνεργασίας των αρμοδίων αρχών και των Κρατών Μελών στον τομέα της ασφάλειας των δικτύων και των συστημάτων πληροφοριών.

- Εστιάζεται επίσης στην καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο, κυρίως στην αντιμετώπιση εγκληματικών πράξεων που διαπράττονται στο διαδίκτυο μέσω δικτύων ηλεκτρονικών επικοινωνιών και συστημάτων πληροφοριών. Η εγκληματικότητα στον κυβερνοχώρο μπορεί να ταξινομηθεί σε εγκλήματα που αφορούν το Διαδίκτυο, σε online απάτη, πλαστογραφία και παράνομο περιεχόμενο στο Διαδίκτυο. Σημαντικές νομοθετικές δράσεις της ΕΕ για το έγκλημα στον κυβερνοχώρο είναι:
    - Η Οδηγία για τις επιθέσεις κατά των συστημάτων πληροφοριών (2013),
    - Η Οδηγία για την καταπολέμηση της σεξουαλικής εκμετάλλευσης παιδιών στο Διαδίκτυο και της παιδικής πορνογραφίας (2011),
    - Η Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (2002),
    - Η Απόφαση-πλαίσιο για την καταπολέμηση της απάτης και της πλαστογραφίας όσον αφορά τα μέσα πληρωμής πλην των μετρητών (2001).

- Επιπρόσθετα προωθείται η βελτίωση της πολιτικής - στρατιωτικής συνεργασίας μέσω συνεργειών μεταξύ πολιτικών και στρατιωτικών προσεγγίσεων για την προστασία κρίσιμων κρατικών υποδομών και ειδικότερα στους τομείς της έρευνας και ανάπτυξης. Εστιάζεται επίσης στην αποφυγή αλληλοεπικάλυψης, μέσω της στενότερης συνεργασίας μεταξύ κυβερνήσεων, ιδιωτικού τομέα και ακαδημαϊκού τομέα.

- Δίδεται επίσης έμφαση σε θέματα διεθνούς συνεργασίας για την προώθηση πολιτικών και την αντιμετώπιση των προκλήσεων του κυβερνοχώρου λαμβάνοντας υπόψη την ελευθερία της έκφρασης, την διαφάνεια και την εφαρμογή των νόμων, κανόνων και βασικών αξιών της ΕΕ στον κυβερνοχώρο.

Αποτελεί πλέον κοινή αντίληψη σε Ευρωπαϊκό επίπεδο ότι απαιτείται σημαντική βελτίωση όσον αφορά την ασφάλεια στον κυβερνοχώρο, σε συλλογικό επίπεδο στην Ευρωπαϊκή Ένωση (ΕΕ) αλλά και για το σύνολο των κρατών μελών, ιδιαίτερα σε θέματα θεσμοθέτησης διαδικασιών, δημιουργίας των κατάλληλων δομών, κατάρτισης και εκπαίδευσης, καθώς και ανταλλαγής πληροφοριών και επιχειρησιακής συνεργασίας.

Από τον Σεπτέμβριο του 2017 η ΕΕ, προωθεί επίσημα την αναθεώρηση του ευρωπαϊκού πλαισίου για την Κυβερνοασφάλεια. Στόχος των προτάσεων της ΕΕ είναι να καθοριστεί η πολιτική αλλά και στοχευμένες δράσεις που θα καταστήσουν την Ευρωπαϊκή Ένωση πρωταγωνιστή στον τομέα της Κυβερνοασφάλειας και θα την θέσουν σε καλύτερη θέση για να αντιμετωπίσει τις απειλές του κυβερνοχώρου και τους κινδύνους που τις συνοδεύουν, με άμεσο αντίκτυπο στην ασφάλεια και στην ευημερία της Ευρώπης. Η ΕΕ θεωρεί ότι οι προτάσεις της θα συμβάλουν στην ενίσχυση των ικανοτήτων όσον αφορά την τεχνολογία και τις δεξιότητες, καθώς και στη δημιουργία μιας ισχυρής ενιαίας αγοράς. Στοχεύει επίσης στην αποτροπή και στην πρακτική αντιμετώπιση επιθέσεων από τον κυβερνοχώρο μέσω της ενίσχυσης των μηχανισμών για την ανίχνευση, τον εντοπισμό και τη λογοδοσία των υπευθύνων.

Η προσέγγιση της ΕΕ βασίζεται σε τρεις βασικούς πυλώνες: την ανθεκτικότητα (resilience), την αποτρεπτικότητα (deterrence) και την άμυνα (defence). Προκειμένου να ανταποκριθεί στους νέους Ευρωπαϊκούς στόχους, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (European Union Agency for Network and Information Security - ENISA) θα διαδραματίζει βασικό ρόλο στη νέα προσέγγιση, στο πλαίσιο μόνιμων και αναβαθμισμένων όρων εντολής. Η αναθεωρημένη προσέγγιση προωθεί την επιχειρησιακή συνεργασία και την διαχείριση κρίσεων σε

Ευρωπαϊκό επίπεδο, μηχανισμό ταχείας αντιμετώπισης έκτακτων περιστατικών και τις διαδικασίες ενιαίας Ευρωπαϊκής Πιστοποίησης προϊόντων και υπηρεσιών.

Προωθείται επίσης η ίδρυση ενός ευρωπαϊκού κέντρου έρευνας και κατάρτισης στον τομέα της ασφάλειας στον κυβερνοχώρο που θα επιτρέψει την καλύτερη συνεργασία με τη βιομηχανία και άλλους ενδιαφερόμενους φορείς και θα ενισχύσει την καινοτομία σε ευρωπαϊκό επίπεδο. Τέλος, προγραμματίζεται η ανάπτυξη ταμείου για την αντιμετώπιση της εκτάκτων καταστάσεων που πιθανόν να προκύπτουν από τον κυβερνοχώρο η οποία αποτελεί καλή πρωτοβουλία για να βοηθηθούν τα κράτη μέλη και όλοι οι εμπλεκόμενοι, να αναπτύξουν τις δυνατότητες/ικανότητες τους καθώς και την αμοιβαία συνεργασία.

Κατά τον παρόντα χρόνο η πολιτική της Ευρωπαϊκής Ένωσης στα θέματα της Ασφάλειας Δικτύων και Πληροφοριών υλοποιείται με την μεταφορά στο Εθνικό δίκαιο των κρατών Μελών της ΕΕ και την εφαρμογή της Οδηγίας για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών[4] (ΕΕ/2016/1148, NIS Directive).

Η Οδηγία για τα NIS, στοχεύει στην εξασφάλιση ομοιόμορφου ελάχιστου επιπέδου ασφάλειας στον κυβερνοχώρο σε όλη την Ευρωπαϊκή Ένωση. Με την εφαρμογή της Οδηγίας, τα κράτη μέλη, ο ENISA και η Επιτροπή θα πρέπει να διασφαλίζουν ότι υλοποιούνται κατά το ελάχιστο τα ακόλουθα:

- Εθνική Στρατηγική για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών/ Κυβερνοασφάλειας καθώς και πλαίσιο συνεργασίας
- Ομάδα ανταπόκρισης σε περιστατικά και συμβάντα ασφάλειας (National Computer Security Incident Response Team – National CSIRT) σε όλα τα κράτη μέλη
- Δημιουργία ομάδας συνεργασίας σε επίπεδο ΕΕ (NIS Cooperation Group)
- Δημιουργία δικτύου CSIRT σε επίπεδο ΕΕ (CSIRT Network)
- Απαιτήσεις ασφάλειας και μηχανισμός κοινοποίησης περιστατικών
- Προσδιορισμός των «φορέων εκμετάλλευσης βασικών υπηρεσιών»[5] σε εθνικό επίπεδο
- Ενθάρρυνση της τυποποίησης.

Η οδηγία για το NIS εφαρμόζεται τουλάχιστον για τους φορείς εκμετάλλευσης βασικών υπηρεσιών σε κρίσιμους τομείς όπως:

- Ενέργεια
- Μεταφορές
- Τραπεζικές εργασίες
- Υποδομές χρηματοπιστωτικών αγορών
- Υγεία
- Παροχή και διανομή πόσιμου νερού
- Ψηφιακές υποδομές

καθώς επίσης και στους «παροχείς ψηφιακών υπηρεσιών», όπως:

[4] ΟΔΗΓΙΑ (ΕΕ) 2016/1148 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 6ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση

[5] Ο όρος «φορέας εκμετάλλευσης βασικών υπηρεσιών» στην Οδηγία NIS είναι σχεδόν ταυτόσημος με τον όρο «κρίσιμη υποδομή πληροφοριών», όπως βρίσκεται στο παρόν έγγραφο.

- Ηλεκτρονικών αγορών
- Ηλεκτρονικής αναζήτησης
- Cloud computing services.

Τα κράτη μέλη έχουν την ευχέρεια να διευρύνουν το πεδίο εφαρμογής της οδηγίας στη χώρα τους, σε σχέση με τον καθορισμό φορέων βασικών υπηρεσιών/κρίσιμων υποδομών πληροφοριών, ανάλογα με τις εκάστοτε εθνικές ιδιαιτερότητες.

2.2. Η Κυβερνοασφάλεια στην Κυπριακή Δημοκρατία

Η Κυπριακή Δημοκρατία έχει αναγνωρίσει τον ουσιαστικό ρόλο των θεμάτων ασφάλειας στη προώθηση των νέων υπηρεσιών επικοινωνιών, στη χρήση των νέων τεχνολογιών και γενικότερα στην ανάπτυξη της κοινωνίας της πληροφορίας. Προς το σκοπό έχουν προωθηθεί διαχρονικά, προωθούνται κατά τον παρόντα χρόνο και προγραμματίζονται για το ορατό μέλλον πολλαπλές ενέργειες, δράσεις και πολιτικές σε εθνικό επίπεδο και σε συνεργασία μεταξύ όλων των αρμοδίων αρχών και των εμπλεκομένων μερών στην Κυπριακή Δημοκρατία. Για σκοπούς πληρότητας και εύκολης αναφοράς, προηγούμενες δράσεις στον τομέα της Ασφάλειας Δικτύων και Πληροφοριών και της Κυβερνοασφάλειας αναφέρονται στο Παράρτημα ΙΙ.

Σε σχέση με την παρούσα κατάσταση και συγκεκριμένα από τον Απρίλιο του 2018 εισήθηκε στην Κυπριακή Δημοκρατία η νομοθεσία (Νόμος 17/(Ι)2018), περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών, με βάση την οποία ιδρύθηκε η Αρχή Ψηφιακής Ασφάλειας υπό τον Επίτροπο Επικοινωνιών, και η οποία έχει ορισθεί ως η αρμόδια αρχή για την εφαρμογή της Οδηγίας για την Ασφάλεια Δικτύων και Πληροφοριών (NIS Directive) στην Κυπριακή Δημοκρατία και τον συντονισμό ενεργειών για την εφαρμογή της Εθνικής Στρατηγικής για την Κυβερνοασφάλεια, και στην οποία εντάσσεται και η λειτουργία του Εθνικού CSIRT. Ο ιδρυτικός Νόμος έχει αντικατασταθεί τον Αύγουστο του 2020 με τον νέο Νόμο περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Ν. 89(Ι)/2020). Η νέα νομοθεσία παρέχει όλες τις εξουσίες στον Επίτροπο και την Αρχή Ψηφιακής Ασφάλειας για την εφαρμογή της οδηγίας NIS, ενώ όλες οι προαναφερόμενες εξουσίες του ΓΕΡΗΕΤ μεταφέρονται στην Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ). Οι συγκεκριμένες πολιτικές καθορίζονται σε αποφάσεις του Υπουργικού Συμβουλίου:

i. στις 22/10/16 το Υπουργικό Συμβούλιο ενέκρινε τη σύσταση του Εθνικού CSIRT (αρ. απόφασης 81.477) (βλ. άρθρο 9 της Οδηγίας NIS),
ii. στις 3/5/2017, το Υπουργικό Συμβούλιο ενέκρινε τον Πίνακα, με τις υποδομές πληροφοριών στην Κυπριακή Δημοκρατία, που έχουν χαρακτηρισθεί ως «κρίσιμες», για σκοπούς κυβερνοασφάλειας (αρ. απόφασης 82.518),
iii. στις 20/6/2017 (αρ. απόφασης: 82.816) και 28/6/2017 (αρ. απόφασης 82.898) αποφάσισε:
    - Τον ορισμό του Επιτρόπου, ως εθνικής Αρμόδιας Αρχής, βάσει του άρθρου 8 της Οδηγίας NIS, και
    - Τη δημιουργία δομής, κάτω από τον Επίτροπο, που θα λειτουργεί ως εθνική Αρμόδια Αρχή.

Με την νεότερη ειδική εναρμονιστική νομοθεσία του 2020, έχει επιτευχθεί η εναρμόνιση με το πλήρες πλαίσιο για την Ασφάλεια Δικτύων και Πληροφοριών και την Κυβερνοασφάλεια καθώς και τον καθορισμό των αρμοδιοτήτων και εξουσιών της Αρχής σύμφωνα με την Οδηγία NIS και την Οδηγία για τον Κώδικα Ηλεκτρονικών Επικοινωνιών στα θέματα Ασφάλεια.

Από τον Μάρτιο του 2020 έχει ιδρυθεί το Υφυπουργείο Έρευνας Καινοτομίας και Ψηφιακής Πολιτικής σύμφωνα με τον περί της Ίδρυσης Υφυπουργείου Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής και Διορισμού Υφυπουργού Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής παρά τω Προέδρω και Συναφών Θεμάτων Νόμο του 2020 (Ν. 14(Ι)/2020). Η διαχείριση των θεμάτων πολιτικής στον τομέα της Ψηφιακής Ασφάλειας και Κυβερνοασφάλειας έχουν μεταφερθεί στο Υφυπουργείο. Ο Υφυπουργός καθορίζει ή αναθεωρεί το πλαίσιο γενικής πολιτικής σε σχέση με τη ψηφιακή ασφάλεια. Η Αρχή οφείλει να ενεργεί αμερόληπτα και ανεξάρτητα, εφαρμόζοντας το εκάστοτε πλαίσιο γενικής πολιτικής για τη ψηφιακή Ασφάλεια.

Το νέο νομικό και ρυθμιστικό πλαίσιο Ασφάλειας Δικτύων και Πληροφοριών και Κυβερνοασφάλειας, συμπληρώνεται με την δημοσίευση δευτερογενούς νομοθεσίας από την Αρχή Ψηφιακής Ασφάλειας η οποία εστιάζεται στη καλύτερη εφαρμογή της Νομοθεσίας σε Εθνικό επίπεδο, και των σχετικών Οδηγιών και Κανονισμών της Ευρωπαϊκής Ένωσης σε Εθνικό και Ευρωπαϊκό επίπεδο. Αναμένεται ότι το ρυθμιστικό πλαίσιο θα προσαρμόζεται δυναμικά, σε συνεργασία και συνεννόηση με τα ενδιαφερόμενα μέρη, προς αντιμετώπιση των μεταβαλλόμενων προκλήσεων στον κυβερνοχώρο. Οι αρμόδιες ή και εμπλεκόμενες αρχές και παρατηρητές στην Κυπριακή Δημοκρατία αναφέρονται στο Παράρτημα ΙΙΙ της παρούσας Στρατηγικής.

Η Κυπριακή Δημοκρατία, σε συνεργασία με τους εμπλεκόμενους φορείς, και μέσα από τις εργασίες των Ευρωπαϊκών σωμάτων, προσβλέπει στο να συμβάλλει ενεργά στην προώθηση των στόχων της Ευρωπαϊκής πολιτικής και στην διεθνή συνεργασία για την αντιμετώπιση των κινδύνων και προκλήσεων στο κυβερνοχώρο.

2.3. Οι Απειλές στον Κυβερνοχώρο Σήμερα

Η χρήση επικοινωνιακών συστημάτων και ηλεκτρονικών υπολογιστών[6] έχουν διεισδύσει και επηρεάζουν, πλέον, όλες σχεδόν τις δραστηριότητες της ζωής μας,. Οι τεχνολογίες χρησιμοποιούνται σήμερα σε πάρα πολλούς κρίσιμους τομείς της κοινωνίας μας πέραν των μηχανογραφικών συστημάτων και των επικοινωνιών και υπηρεσιών διαδικτύου, όπως στη παραγωγή και μεταφορά ενέργειας, στη διαχείριση των συστημάτων ύδρευσης/αποχέτευσης, στις χρηματοπιστωτικές υπηρεσίες, στις ένοπλες δυνάμεις, στις δυνάμεις ασφαλείας, στα κυβερνητικά τμήματα και υπηρεσίες, στις υπηρεσίες υγείας, στις μεταφορές, στις ψηφιακές υποδομές, κλπ. Αν και τα οφέλη που έχουν προκύψει από τη χρήση των νέων τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ) είναι τεράστια και πολυδιάστατα, η αξιοποίηση τους συνοδεύεται και από μια πληθώρα θεμάτων ασφάλειας..

Τα τελευταία χρόνια έχουν εμφανιστεί πολλαπλές απειλές και κίνδυνοι στον κυβερνοχώρο. Οι ΤΠΕ είναι δυνατόν να χρησιμοποιηθούν κακόβουλα σε παράνομες δραστηριότητες όπως, για την κλοπή χρημάτων από τραπεζικούς λογαριασμούς, την πρόσβαση σε εμπιστευτικές, ευαίσθητες και προσωπικές πληροφορίες, την πρόκληση ζημιών σε σημαντικές ιστοσελίδες (με συνεπαγόμενη άρνηση πρόσβασης στο κοινό), μέχρι και υλικές ζημιές σε κρίσιμες εγκαταστάσεις, θέτοντας σε κίνδυνο ακόμη και ανθρώπινες ζωές. Μετά από κυβερνοεπιθέσεις εταιρείες, οργανισμοί και κρατικές υπηρεσίες έχουν απωλέσει πολύτιμες πληροφορίες όπως εμπιστευτικά συμβόλαια, σχέδια προϊόντων, στοιχεία

[6] Όχι μόνο οι κλασσικοί επιτραπέζιοι ή φορητοί υπολογιστές – πλέον χρησιμοποιούμε μια μεγάλη γκάμα από προϊόντα που είναι στην ουσία τους μικροί υπολογιστές: έξυπνα τηλέφωνα και ρολόγια, οικιακές συσκευές, αυτοκίνητα, tablets, παιχνιδοκονσόλες, τηλεοράσεις, συστήματα ελέγχου σε σπίτια και ξενοδοχεία, και πολλά άλλα.

πιστωτικών καρτών, αριθμούς λογαριασμών και άλλα επιχειρηματικά στοιχεία. Τέτοια περιστατικά μπορεί να προκαλέσουν σοβαρές ζημιές σε ένα οργανισμό, αφού πέραν των άμεσων ζημιών πλήττεται και το καλό του όνομα καθώς και η εμπιστοσύνη των πελατών του.

Η συχνότητα και η πολυπλοκότητα των επιθέσεων στον κυβερνοχώρο αυξάνεται ενώ πολλές επιχειρήσεις αρχίζουν να βιώνουν τις επιπτώσεις τους που είναι δυνατόν να επηρεάσουν την επιχειρηματική τους δραστηριότητα. Το κοινό, στις πλείστες των περιπτώσεων, δεν είναι ενήμερο για τα αποτελέσματα των επιθέσεων αυτών, αλλά και το είδος των ζημιών που προκαλούνται από αυτές. Οι απειλές συνεχώς εξελίσσονται, ενώ πολλές μορφές κακόβουλων λογισμικών εμφανίζονται καθημερινά (ransomware, advanced persistent threats (APT), Distributed Denial of Service (DDoS) και πολλά άλλα). Εκτός από τις επιπτώσεις σε πρόσωπα και επιχειρήσεις, μπορούν εύκολα να δημιουργηθούν προβλήματα και στα ίδια τα κράτη . Η σταθερότητα, η δύναμη και η ασφαλής λειτουργία ενός κράτους είναι πλέον πλήρως εξαρτώμενη από τη ομαλή λειτουργία των υποδομών της, και όπως φαίνεται από τις πιο πάνω αναφορές, οι κυβερνοεπιθέσεις δεν μπορούν να αγνοηθούν από κανένα.

3. ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΑΠΟΚΡΙΣΗ (Strategic Response)

Η στρατηγική ανταπόκριση της Κυπριακής Δημοκρατίας στις προαναφερθείσες απειλές, για επίτευξη των στόχων και του οράματος της παρούσας Στρατηγικής, αναλύεται στο παρόν κεφάλαιο. Η δομή της Στρατηγική της Κυπριακής Δημοκρατίας αποτελείται από πρωταρχικές θεματικές ενότητες (overarching themes) οι οποίες έχουν καταρτιστεί με βάση τις κατευθυντήριες αρχές και δεδομένων των τομέων προτεραιότητας που αναφέρονται στις ενότητες 1.6 και 1.7 αντίστοιχα. Για σκοπούς του παρόντος εγγράφου, το οποίο περιορίζεται στην αποτύπωση του πολιτικού και στρατηγικού σχεδιασμού του κράτους, η κάθε θεματική ενότητα που αναλύεται συνοπτικά στη παρούσα ενότητα, ενσωματώνει σειρά στρατηγικών στόχων, και εστιάζεται σε αριθμό δράσεων προς επίτευξη του σκοπού, του οράματος και των στόχων της Στρατηγικής.

Η κάθε δράση θα αναλύεται και θα κοστολογείται στην φάση υλοποίησης της Στρατηγικής και συγκεκριμένα κατά το στάδιο του προγραμματισμού και της ετοιμασίας του πλάνου υλοποίησης (project plan), όπου θα καθορίζονται οι επιμέρους στόχοι και ο αναμενόμενος αντίκτυπος από την εφαρμογή της κάθε δράσης ξεχωριστά, ενώ στη ίδια φάση θα προσδιορίζονται οι επιμέρους δραστηριότητες και τα παραδοτέα της. Επίσης κατά την ίδια φάση θα προσδιορίζονται όλα τα ενδιαφερόμενα μέρη και οι εμπλεκόμενοι φορείς που θα έχουν συμμετοχή κατά τη φάση υλοποίησης της, θα γίνεται αξιολόγηση κινδύνων, ενώ θα καταγράφονται οι μηχανισμοί εποπτείας των συγκεκριμένων δραστηριοτήτων, καθώς και οι δείκτες μέτρησης της επιτυχούς εφαρμογής της. Στην ενότητα 4 δίδεται μια πιο λεπτομερής περιγραφή του μηχανισμού διαχείρισης της Στρατηγικής και των δράσεων της.

Οι στρατηγικοί στόχοι τις Στρατηγικής ταξινομούνται και συνοψίζονται πιο κάτω. Στην κάθε θεματική ενότητα που ακολουθεί δίδεται η γενική περιγραφή της κάθε Δράσης. Σημειώνεται ότι οι θεματικές ενότητες δεν είναι απαραίτητα ανεξάρτητες μεταξύ τους, ενώ αρκετές από τις δραστηριότητες εντός των Δράσεων δύνανται να εμπίπτουν ή να συνδέονται με περισσότερες από μία θεματικές ενότητες και στρατηγικούς στόχους. Οι στρατηγικοί στόχοι συνοψίζονται ως ακολούθως:

- **Συνεργασία (Cooperation) και Ανάπτυξη Εμπιστοσύνης (Trust)** - Δημιουργία των κατάλληλων δομών για συνεργασία σε όλα τα επίπεδα και με όλους τους απαραίτητους εμπλεκόμενους, εντός και εκτός Κύπρου.

- **Κατανόηση Κατάστασης (Situational Awareness)** – Ανταλλαγή πληροφοριών, μαζί με ανάλυση τους και εξαγωγή συμπερασμάτων για την κατάσταση κυβερνοασφάλειας σε πραγματικό χρόνο, σε τεχνικό, επιχειρησιακό και στρατηγικό επίπεδο.

- **Διαχείριση Κινδύνων (Risk Management)** – Αναγνώριση απειλών, ευπαθειών και κινδύνων σε όλα τα επίπεδα, με την κατάλληλη διαχείριση τους.

- **Διαχείριση Περιστατικών και Κρίσεων (Incident and Crisis Management)** – Διαχείριση περιστατικών, τεχνικά/χαμηλής κρισιμότητας περιστατικά, σοβαρά περιστατικά (Major incidents), διαχείριση κρίσεων (Crisis management).

- **Ανάπτυξη Δυνατοτήτων (Capability Development)** – Συνεχής ανάπτυξη των απαραίτητων ικανοτήτων και δυνατοτήτων στο κράτος, σε οργανισμούς, επαγγελματίες και πολίτες, για υποστήριξη όλων των δραστηριοτήτων της Στρατηγικής.

- **Εκπαίδευση, Κατάρτιση και Επίγνωση (Awareness)** – Ειδική έμφαση στην ανάπτυξη επίγνωσης και κουλτούρας ασφάλειας σε όλα τα στρώματα της κοινωνίας καθώς και στην εξειδικευμένη εκπαίδευση και κατάρτιση των επαγγελματιών του τομέα.

- **Έρευνα και Καινοτομία (Innovation)** – Καινοτομία για ενίσχυση των δυνατών σημείων της Κύπρου σε νευραλγικούς τομείς όπου πρωτοπορεί, όπως τις οικονομικές υπηρεσίες και τη ναυτιλία, με υποστήριξη ερευνητικών και άλλων ευκαιριών χρηματοδότησης από διάφορες πηγές, και δημιουργία οικοσυστημάτων κυβερνοασφάλειας.

- **Νομικό και Ρυθμιστικό πλαίσιο** - Ανάπτυξη νομικού, κανονιστικού και ρυθμιστικού πλαισίου για την προστασία της κοινωνίας από τις απειλές και το έγκλημα στον κυβερνοχώρο και για την προώθηση ενός ασφαλούς περιβάλλοντος για την χρήση των νέων τεχνολογιών, σύμφωνα με τις αρχές της συμμετοχικότητας σε ένα περιβάλλον εμπιστοσύνης.

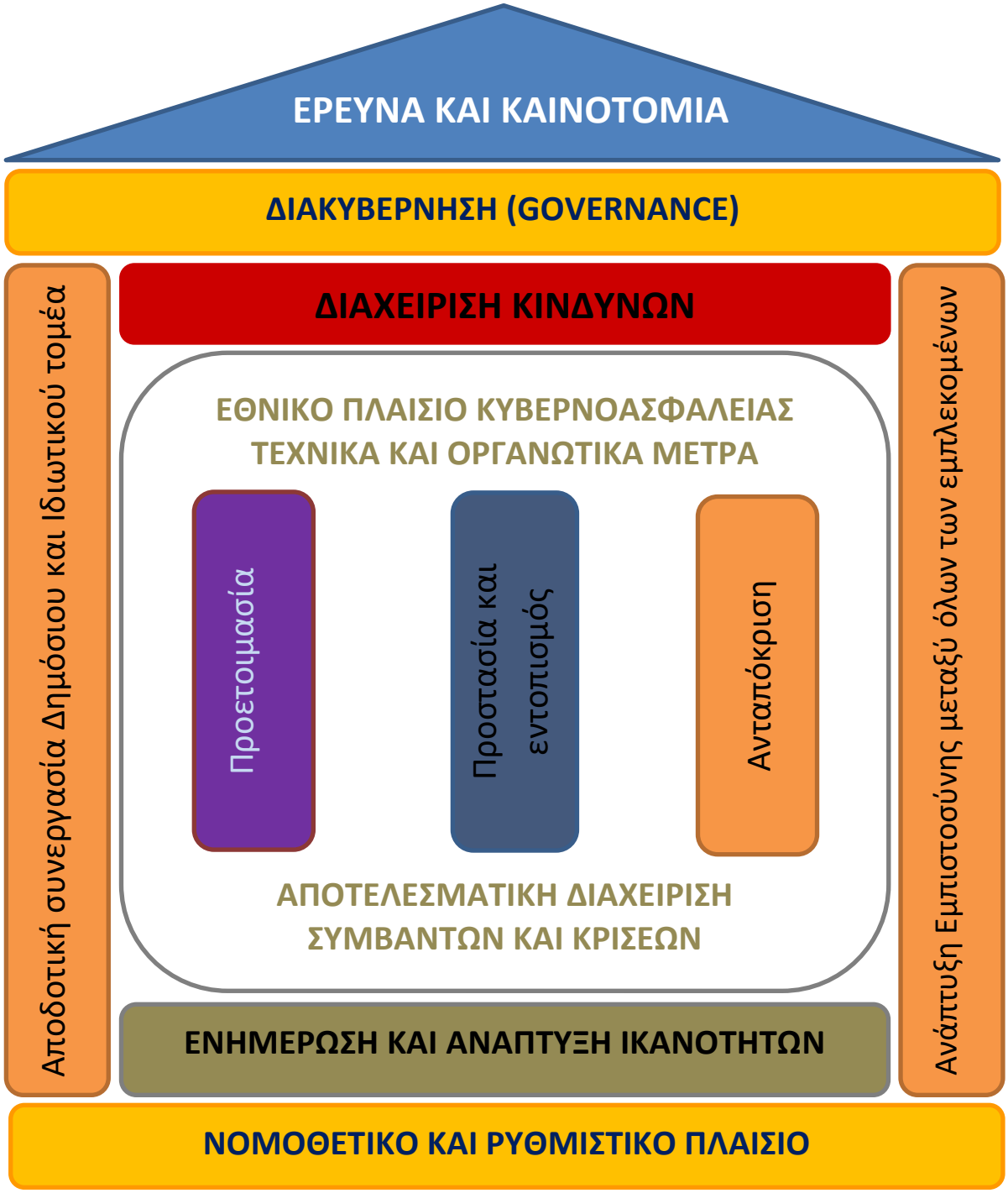
- **Μείωση και αποτελεσματική διερεύνηση αδικημάτων που διαπράττονται στον Κυβερνοχώρο** – Καταπολέμηση της παιδικής πορνογραφίας, της παράνομης πρόσβασης σε δεδομένα ηλεκτρονικού υπολογιστή, των ρατσιστικών σχολίων μέσω διαδικτύου, της οικονομικής απάτης, των εκβιασμών μέσω διαδικτύου, αλλά και άλλων αδικημάτων όπως αυτά ποινικοποιούνται από την εθνική μας νομοθεσία.

Για την καλύτερη κατανόηση των δραστηριοτήτων που καθορίζει η Στρατηγική, το γράφημα 2 παρουσιάζει πως οι στρατηγικοί στόχοι, είναι δυνατόν να συμβάλουν στις κοινά αποδεκτές/εφαρμοστέες ενέργειες[7] για την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας.

Γράφημα 2: Θεματικές Ενότητες Στρατηγικής σε σχέση με τον κύκλο ενεργειών για την αντιμετώπιση περιστατικών κυβερνοασφάλειας

[7] Αναγνώριση (Identify) – Αναγνώριση στοιχείων υποδομής, απειλών, ευπαθειών, κινδύνων και άλλων σημαντικών στοιχείων για κατανόηση του περιβάλλοντος κυβερνοασφάλειας.
Προστασία (Protect) – Προστασία των υποδομών, υπηρεσιών και πληροφοριών με βάση τουςις κινδύνους που έχουν αναγνωριστεί (διαχείριση κινδύνων).
Ανίχνευση (Detect) – Ανίχνευση περιστατικών όταν συμβαίνουν, συμπεριλαμβανομένων και προσπαθειών επίθεσης.
Ανταπόκριση (Respond) – Διαχείριση περιστατικών, είτε αυτά είναι απλά τεχνικά περιστατικά, είτε είναι κάποιας μορφής επιχειρησιακή ή στρατηγική / πολιτική κρίση.
Ανάκαμψη (Recover) – Ανάκαμψη μετά από επιτυχημένη επίθεση, και επαναφορά στα κανονικά επίπεδα λειτουργίας.
Αξιολόγηση (Evaluate) – Αξιολόγηση των αποτελεσμάτων των Δράσεων της Στρατηγικής, για κατανόηση των επιπτώσεων τους στα επίπεδα κυβερνοασφάλειας στην Κύπρο.
Βελτίωση (Improve) – Βελτίωση Δράσεων και των αποτελεσμάτων τους, καθώς και συστάσεις για βελτίωση των επιπέδων κυβερνοασφάλειας στην Κύπρο.

Επίσης, το γράφημα 3 δείχνει τη σχέση των Θεματικών ενοτήτων με τους Τομείς Προτεραιότητας της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, που αναφέρονται στην ενότητα 1.7 του παρόντος εγγράφου, με σκοπό την καλύτερη κατανόηση της δομής αλλά και των βασικών πυλώνων στους οποίους στηρίζεται η παρούσα στρατηγική.



Γράφημα 3: Σχέση Θεματικών ενοτήτων με τους Τομείς Προτεραιότητας της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας

3.1. Θεματική Ενότητα 1 – Δομές και Διακυβέρνηση (Governance)

Στρατηγικοί στόχοι: Γενική Δράση Καλύπτει όλους τους στόχους

Η κυβερνοασφάλεια αποτελεί μεγάλο και πολύπλοκο κεφάλαιο όσον αφορά τη διακυβέρνηση της ασφάλειας σε ένα κράτος, και απαιτεί την εμπλοκή μεγάλου αριθμού φορέων του δημόσιου τομέα. Ο κάθε αρμόδιος φορέας έχει τους δικούς του τομείς ευθύνης και είναι σημαντικό να διατηρούνται ξεκάθαροι ρόλοι. Λόγω της πολυπρόσωπης αυτής συμμετοχής στη διαχείριση των επιμέρους πτυχών της κυβερνοασφάλειας, επιβάλλεται να γίνει αντιληπτό και αποδεκτό από όλους ότι η διατήρηση της ασφάλειας στον ηλεκτρονικό χώρο μπορεί να επιτευχθεί **μόνο** με την αποδοτική συνεργασία των εμπλεκομένων φορέων στα πλαίσια μιας ενιαίας και συντονισμένης αντιμετώπισης των διαφόρων απειλών που έχουν ήδη αναφερθεί.

Ως εκ τούτου, ο συντονισμός των αρμόδιων φορέων του κράτους καθίσταται απαραίτητος. Στην Κυπριακή Δημοκρατία έχουν γίνει αρκετά βήματα τα τελευταία χρόνια (βλ. ενότητα 2.2) προς την κατεύθυνση της ανάπτυξης ικανοτήτων στην κυβερνοασφάλεια, και επιβάλλεται ο θεσμοθετημένος πλέον συντονισμός και ανάθεση αρμοδιοτήτων στον τομέα αυτό.

Η δραστηριότητα αυτή είναι αποδοτική όταν γίνεται στη βάση μηχανισμού που συντονίζει τις προσπάθειες της Κυπριακής Δημοκρατίας, ολιστικά, για την άρτια ανταπόκριση της έναντι των απειλών που εμφανίζονται σήμερα καθώς και των αναδυόμενων απειλών στον κυβερνοχώρο.

Με βάση το υφιστάμενο νομικό πλαίσιο **ο Υφυπουργός Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής Παρά τω Προέδρω, καθορίζει ή αναθεωρεί το πλαίσιο γενικής πολιτικής** σε σχέση με την Ψηφιακή Ασφάλεια στην Κύπρο.

Επίσης στη βάση του ίδιου νομικού πλαισίου **έχει δημιουργηθεί η Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ)**, ως αποτέλεσμα των δραστηριοτήτων για δημιουργία εθνικής ανεξάρτητης δομής για την κυβερνοασφάλεια στην Κύπρο, συμπεριλαμβανομένων των υποχρεώσεων της Κυπριακής Δημοκρατίας που απορρέουν από την Οδηγία NIS (βλ. θεματική ενότητα 3), με πολιτικό προϊστάμενο τον Επίτροπο Επικοινωνιών[8] (βλ. θεματική ενότητα 2.2), και η οποία είναι υπεύθυνη για:

- το συντονισμό της υλοποίησης της παρούσας Στρατηγικής, υπό την πολιτική εποπτεία του Υφυπουργού και στη βάση των στρατηγικών και πολιτικών αποφάσεων του Εθνικού Συμβουλίου Κυβερνοασφάλειας, μέσω δομημένης διαχείρισης προγράμματος (Strategy Programme Management – βλ. θεματική ενότητα 4), περιλαμβανομένου του συντονισμού κάποιων Δράσεων της Στρατηγικής,
- την πλήρη εφαρμογή της Οδηγίας NIS, μέσω της άσκησης των σχετικών αρμοδιοτήτων της Αρχής που περιγράφονται στην κείμενη Νομοθεσία (βλ. θεματική ενότητα 3),
- την λειτουργία του Εθνικού CSIRT (Computer Security Incident Response Team) (βλ. θεματική ενότητα 6),
- συνεργασία και υποστήριξη του Υφυπουργείου για τον καθορισμό και αναθεώρηση της πολιτικής για την ψηφιακής ασφάλεια και συνεργασία με τις αρμόδιες αρχές για τα επιμέρους

[8] Ο όρος Επίτροπος Επικοινωνιών αποτελεί μετονομασία του όρου Επίτροπος Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων στη βάση σχετικής απόφασης του Υπουργικού Συμβουλίου και τροποποίησης του Νόμου περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων 112(Ι)2004.

θέματα κυβερνοασφάλειας (κυβερνοέγκλημα, κυβερνοάμυνα, σχετικές εξωτερικές σχέσεις) (βλ. θεματική ενότητα 1 και θεματική ενότητα 2),

- συνεργασία στα πλαίσια άλλων σχετικών δραστηριοτήτων σε εθνικό επίπεδο, π.χ. Βασικό Εθνικό Σχέδιο (ΒΕΣ) «ΖΗΝΩΝ», Πλαίσιο SENDAI[9], Εθνική Στρατηγική Ασφάλειας, αξιολογήσεις κινδύνων σε εθνικό επίπεδο, κλπ.).

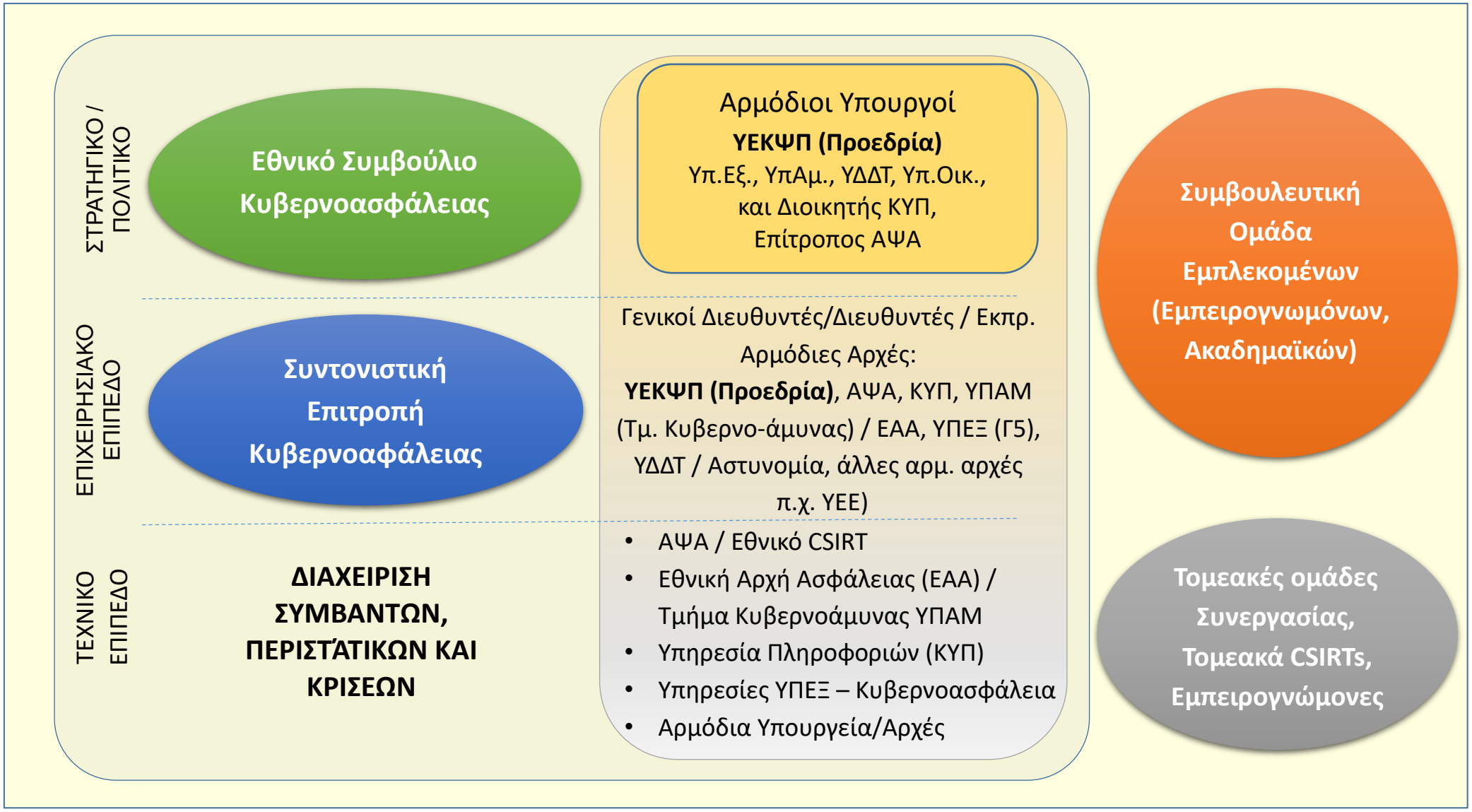
Κατά την άσκηση των αρμοδιοτήτων της η Αρχή πρέπει:

- να ενεργεί αμερόληπτα και ανεξάρτητα εφαρμόζοντας το εκάστοτε πλαίσιο γενικής πολιτικής που αναφέρεται στη προηγούμενη παράγραφο,
- να έχει την **κατάλληλη νομική εξουσία και καθορισμένη αρμοδιότητα** για να μπορέσει να επιτελέσει το έργο της,
- να διαθέτει την **απαραίτητη τεχνογνωσία** για να ανταποκριθεί σωστά στις υποχρεώσεις του ρόλου,
- να διαθέτει τους **απαραίτητους συνδέσμους** και να διατηρεί **καλές σχέσεις συνεργασίας** με τους αρμόδιους φορείς του κράτους, τους χειριστές κρίσιμων υποδομών πληροφοριών της Κύπρου, των εμπλεκομένων του ιδιωτικού τομέα, και των διεθνών ομάδων εργασίας και φόρουμ σχετικά με το θέμα.
- να διαθέτει τους **απαραίτητους πόρους** και μηχανισμούς όπως πολιτική βούληση, χρηματοδότηση, χρόνο, και προσωπικό.

Η παρούσα Δράση θα εξετάζει τη δημιουργία των αρμοδίων σωμάτων και ομάδων, με στόχο την καλύτερη εφαρμογή της Στρατηγικής, καθώς και την αποτελεσματικότερη ανταπόκριση της Κυπριακής Δημοκρατίας έναντι των απειλών του κυβερνοχώρου (βλ. γράφημα 3):

- **Εθνικό Συμβούλιο Κυβερνοασφάλειας (National Cybersecurity Council)**, με υψηλόβαθμη εκπροσώπηση από τις κύριες εμπλεκόμενες αρμόδιες αρχές, σε επίπεδο Υπουργού / Διοικητή / Επιτρόπου ως ακολούθως: ασφάλεια δικτύων και πληροφοριών (Υφυπουργείο Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής και Αρχή Ψηφιακής Ασφάλειας), κυβερνοέγκλημα (Υπουργείο Δικαιοσύνης και Δημόσιας Τάξης, Αστυνομία Κύπρου), κυβερνοάμυνα (Υπουργείο Άμυνας, Γενικό Επιτελείο Εθνικής Φρουράς, Εθνική Αρχή Ασφάλειας), διεθνής συνεργασία (Υπουργείο Εξωτερικών), δαπάνες κυβερνοασφάλειας (Υπουργείο Οικονομικών) και Υπηρεσίες Πληροφοριών (Κυπριακή Υπηρεσία Πληροφοριών). Την προεδρία του σώματος θα αναλάβει ο Υφυπουργός Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής Παρά τω Προέδρω, ο οποίος θα υποστηρίζεται από την Αρχή Ψηφιακής Ασφάλειας για την παρακολούθηση της εφαρμογής της Στρατηγικής, ως η αρμόδια Αρχή για τον συντονισμό της υλοποίησης της Στρατηγικής. Το σώμα θα παρακολουθεί την εξέλιξη της υλοποίησης της Στρατηγικής Κυβερνοασφάλειας σε τακτά χρονικά διαστήματα (π.χ. κάθε 6 μήνες ή 1 χρόνο), θα ενημερώνεται για την εκάστοτε κατάσταση της κυβερνοασφάλειας στην Κυπριακή Δημοκρατίας, και, όπου απαιτείται, θα δίνει κατευθυντήριες γραμμές για τη βελτίωση της κυβερνοασφάλειας ευρύτερα. Επίσης, το σώμα αυτό θα συγκαλείτε 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.

[9] http://www.unisdr.org/we/coordinate/sendai-framework



Γράφημα 1: Δομές Κυβερνοασφάλειας στην Κυπριακή Δημοκρατία

- **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. Την προεδρία του της Επιτροπής θα αναλάβει ο Γενικός Διευθυντής του Υφυπουργείου Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής, ο οποίος θα υποστηρίζεται από την Αρχή Ψηφιακής Ασφάλειας σε σχέση με τις δραστηριότητες της Επιτροπής για την παρακολούθηση της εφαρμογής της Στρατηγικής. Στο σώμα αυτό θα αναγνωρίζονται οι αλληλεξαρτήσεις και θα 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 θα εξετάζει επίσης τις αλληλεξαρτήσεις και αλληλοεπιδράσεις μεταξύ των επιμέρους στρατηγικών των αρμοδίων αρχών και των δράσεων που προτείνονται ή και προωθούνται, παρόλο που η κάθε μια έχει τους δικούς της συγκεκριμένους και ξεχωριστούς στόχους, για την επιτυχή υλοποίηση τους και για πιθανές συνεργίες και την αποφυγή επικαλύψεων. Θα πρέπει το θέμα της στρατηγικής ανταπόκρισης στις απειλές ως προς την κυβερνοασφάλεια, να αντιμετωπίζεται ολιστικά και είναι απαραίτητο να γίνει κατανοητό το γεγονός ότι, αρκετές από αυτές τις Δράσεις πρέπει να εφαρμοστούν συνδυασμένα, με στόχο την μεγιστοποίηση της επιτυχίας μιας τέτοιας ανταπόκρισης. Επίσης, το σώμα αυτό θα συγκαλείται σε περιπτώσεις κρίσης κυβερνοασφάλειας, η οποία επηρεάζει την Κυπριακή Δημοκρατία σε μεγάλο βαθμό (βλ. ενότητα 3.7), σύμφωνα με τα ισχύοντα σχέδια διαχείρισης κρίσεων της Δημοκρατίας για την Κυβερνοασφάλεια.

- **Συμβουλευτική Ομάδα Εμπλεκομένων (Stakeholder Advisory Group)**, με εκπροσώπηση εμπλεκομένων φορέων (όπως π.χ. για το ηλεκτρονικό εμπόριο και την ηλεκτρονική διακυβέρνηση), ακαδημαϊκών ιδρυμάτων, φορέων εκμετάλλευσης βασικών υπηρεσιών, φορέων κρίσιμων υποδομών πληροφοριών, παροχέων ηλεκτρονικών επικοινωνιών, παροχέων ψηφιακών υπηρεσιών, μη-κυβερνητικών οργανώσεων, σχετικών εταιρειών και άλλων οργανισμών του ιδιωτικού τομέα. Γενικά, θα πρέπει να υπάρχει μηχανισμός ανατροφοδότησης για όλα τα σχετικά ενδιαφερόμενα μέρη όσο αφορά στην υλοποίηση της παρούσας Στρατηγικής. Σε τακτά χρονικά διαστήματα, θα παρουσιάζονται τα αποτελέσματα των Δράσεων της Στρατηγικής, καθώς και ο προγραμματισμός και εστίαση των επόμενων δραστηριοτήτων, για ενημέρωση αλλά και για καθοδήγηση των αρμοδίων αρχών, όπου απαιτείται.

- **Τομεακές Ομάδες Συνεργασίας (Sectoral Cooperation Groups), και πιθανή δημιουργία τομεακών δομών (π.χ. τομεακών CSIRT)** για τη συνεργασία, συντονισμό και ανταλλαγή πληροφοριών καθώς και την πιο αποδοτική και εξειδικευμένη αντιμετώπιση περιστατικών, εντός των κρίσιμων τομέων που καθορίζονται από το Υπουργικό Συμβούλιο, για τη διατήρηση των βασικών λειτουργιών του κράτους και της κοινωνίας.

- **Ομάδες Εργασίας (Working Groups)**, για την επιτυχή υλοποίηση των Δράσεων της Στρατηγικής. Οι ομάδες αυτές θα συστήνονται ανάλογα με τις ανάγκες της κάθε Δράση, όποτε κρίνεται απαραίτητο.

Στη συνεργασία μεταξύ των κύριων αρμοδίων αρχών για θέματα ασφάλειας δικτύων και πληροφοριών, ψηφιακής ασφάλειας, κυβερνοασφάλειας, κυβερνοεγκλήματος, κυβερνοάμυνας και σχετικές εξωτερικές σχέσεις, θα λαμβάνεται υπόψη το γεγονός ότι αρκετές από τις Δράσεις που περιγράφονται στην παρούσα Στρατηγική, έχουν οριζόντιο χαρακτήρα. Ταυτόχρονα, στον σχεδιασμό της κάθε Δράσης, θα λαμβάνονται υπόψη και άλλες δραστηριότητες που οι αρμόδιες αρχές θα υλοποιούν, στους τομείς αρμοδιότητας τους.

Δράσεις:

Δράση 1 - Δημιουργία κατάλληλων δομών και ομάδων για την επιτυχή υλοποίηση της Στρατηγικής, και την αποτελεσματική αντιμετώπιση των απειλών που εμφανίζονται στον κυβερνοχώρο, καθώς και τις αναδυόμενες απειλές που θα εμφανίζονται στο μέλλον. Όπου κρίνεται αναγκαίο, θα μελετάται η ανάγκη δημιουργίας νέων ή ενίσχυσης υφιστάμενων δομών (π.χ. τομεακά CSIRT) και συνεργασιών για τη διατήρηση υψηλών επιπέδων κυβερνοασφάλειας στην Κυπριακή Δημοκρατία. Σε όλες τις εργασίες της Στρατηγικής, θα λαμβάνονται υπόψη οι αλληλεξαρτήσεις, όπου αυτές εμφανίζονται.

3.2. Θεματική ενότητα 2 – Θεσμοθέτηση της συνεργασίας μεταξύ αρμοδίων δημόσιων φορέων

<u>Στρατηγικοί στόχοι:</u> Συνεργασία και Ανάπτυξη Εμπιστοσύνης, Κατανόηση Κατάστασης, Διαχείριση Κινδύνων, Διαχείριση Περιστατικών και Κρίσεων

Βασικός στόχος της Στρατηγικής είναι η δημιουργία ενός μηχανισμού για τον προσδιορισμό και την ένταξη των κυβερνητικών φορέων που επηρεάζονται ή είναι υπεύθυνοι για την εφαρμογή της. Η επίτευξη διακυβερνητικής δέσμευσης, ο αποδοτικός συντονισμός και η συνεχής συνεργασία θα πρέπει να αποτελούν βασικές λειτουργίες αυτών των κυβερνητικών θεσμών, και οι οποίες απαιτούνται για να διασφαλιστεί ότι οι μηχανισμοί διακυβέρνησης που αναφέρονται στην θεματική ενότητα 1 και οι πόροι που διαθέτει η Κυπριακή Δημοκρατία, αποφέρουν τα επιθυμητά αποτελέσματα στα οποία αποβλέπει η Στρατηγική.

Η αποτελεσματική επικοινωνία και ο συντονισμός εξασφαλίζουν ότι όλα τα υπουργεία, οι αρμόδιες αρχές και οι κυβερνητικές υπηρεσίες γνωρίζουν την αποστολή, τις αρμοδιότητες και τα καθήκοντα των αρμόδιων αρχών και κρατικών υπηρεσιών που ασχολούνται με τα συναφή θέματα κυβερνοασφαλειας. Η δέσμευση και η συνεπής εφαρμογή της πολιτικής του κράτους από όλες τις αρμόδιες αρχές και κρατικές υπηρεσίες σε συνεχή βάση, αποτελούν απαραίτητα στοιχεία προκειμένου να διασφαλιστεί η εκπλήρωση του οράματος και των στόχων της στρατηγικής.

Στα πλαίσια της θεσμοθετημένης συνεργασίας των αρμόδιων δημόσιων φορέων, ειδική έμφαση θα δοθεί, από όλους τους εμπλεκόμενους, στην υλοποίηση των προνοιών του Cybersecurity Package[10], που εξέδωσε η Ευρωπαϊκή Επιτροπή τον Σεπτέμβριο του 2017. Η Αρχή Ψηφιακής Ασφάλειας θα

[10] Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN

συνεργάζεται με τις αρμόδιες αρχές στον μέγιστο δυνατό βαθμό, στα πλαίσια των αρμοδιοτήτων της, για την υποστήριξη των στόχων ως προς την αποτελεσματική πάταξη του κυβερνοεγκλήματος, την αποτροπή κυβερνοεπιθέσεων, την ανάπτυξη ικανοτήτων κυβερνοάμυνας, και την ενδυνάμωση της διεθνούς συνεργασίας σε θέματα κυβερνοασφάλειας. Πιο συγκεκριμένα, οι αρμόδιες αρχές θα πρέπει να λάβάνουν μέτρα, μεταξύ άλλων, για τα ακόλουθα:

- Εντοπισμό δραστών κακόβουλων ενεργειών,
- Ενίσχυση του νομοθετικού, κανονιστικού και ρυθμιστικού πλαισίου,
- Συνεργασία δημόσιου και ιδιωτικού τομέα για την πάταξη του κυβερνοεγκλήματος,
- Ενίσχυση των μηχανισμών αντιμετώπισης κυβερνοεπιθέσεων σε πολιτικό επίπεδο,
- Ενίσχυση ικανοτήτων αποτροπής μέσω της αμυντικής θωράκισης,
- Συμπερίληψη της κυβερνοασφάλειας στο πλαίσιο της οικοδόμησης διεθνών σχέσεων,
- Ανάπτυξη ικανοτήτων, δυνατοτήτων και συνεργασιών στους τομείς του κυβερνοεγκλήματος, της κυβερνοάμυνας και της διεθνούς συνεργασίας,
- Διασφάλιση της συνοχής μεταξύ της εθνικής και της εξωτερικής πολιτικής της χώρας, έτσι ώστε ένα υπουργείο ή/και μια κρατική υπηρεσία να μην υπονομεύει την αξιοπιστία της άλλης, αντιπροσωπεύοντας διαφορετικές θέσεις στον ίδιο τομέα πολιτικής.
- Συνδρομή σε προσπάθειες εδραίωσης της σταθερότητας στον κυβερνοχώρο,
- Αναγνώριση και αντιμετώπιση υβριδικών απειλών.

Δράση:

Δράση 2 - Δημιουργία μηχανισμού για τον συντονισμό των Υπουργείων, των αρμοδίων αρχών και των εμπλεκομένων κρατικών υπηρεσιών, στη βάση των δομών που αναφέρονται στην θεματική ενότητα 1, με κύριο στόχο, μεταξύ άλλων, την διεξαγωγή περιοδικών συναντήσεων στις οποίες να συμμετέχουν όλοι οι ενδιαφερόμενοι φορείς με στόχο την ενημέρωση τους για τα σχέδια δράσεων που αφορούν τις υπηρεσίες του κράτους, την συνεργασία και τον συντονισμό ενεργειών.
Ένα παράδειγμα μηχανισμού συνεργασίας θα ήταν η δημιουργία μιας ειδικής ομάδας εργασίας για την αντιμετώπιση συγκεκριμένου θέματος.

3.3. Θεματική ενότητα 3 – Νομικό, Ρυθμιστικό και Πολιτικό Πλαίσιο

Στρατηγικοί στόχοι: Γενική Δράση, Καλύπτει όλους τους στόχους

Τα θέματα της κυβερνοασφάλειας και του ηλεκτρονικού εγκλήματος καλύπτονται επαρκώς νομοθετικά στην Κυπριακή Δημοκρατία.. Παρόλα αυτά παραμένει η ανάγκη συνεχούς επικαιροποίησης και εκσυγχρονισμού **όλων** των σχετικών νομοθεσιών , καθώς και η ανάγκη προώθησης νέας πρωτογενούς και δευτερογενούς νομοθεσίας για σκοπούς εναρμόνισης με την όποια νεότερη Ευρωπαϊκή νομοθεσία, καθώς και την κάλυψη ειδικών προνοιών της παρούσας Στρατηγικής. Ειδική έμφαση θα δοθεί στις υποχρεώσεις που απορρέουν από την οδηγία NIS, την επικείμενη αναθεώρηση της νομοθεσίας για τις ηλεκτρονικές επικοινωνίες στα θέματα της ασφάλειας δικτύων και πληροφοριών, τον νέο Κανονισμό για τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), την

Ευρωπαϊκή νομοθεσία που αναμένεται να προκύψει από την υλοποίηση του Νέου Ευρωπαϊκού πακέτου για την Κυβερνοασφάλεια (Cybersecurity package) συμπεριλαμβανομένων θεμάτων κυβερνοεγκλήματος, τον Κανονισμό για την προστασία προσωπικών δεδομένων[11] (General Data Protection Regulation – GDPR), και γενικότερα σε θέματα ιδιωτικότητας (privacy) και διαφύλαξης των βασικών δικαιωμάτων (σε περίπτωση ποινικών ερευνών και διώξεων), σύμφωνα με την αρχή των θεμελιωδών ανθρωπίνων δικαιωμάτων, καθώς και πολλά άλλα.

Ειδικότερα η Οδηγία NIS, (ΕΕ) 2016/1148 σχετικά με την ασφάλεια συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ευρωπαϊκή Ένωση (βλ. ενότητα 2.1) αντιπροσωπεύει την πρώτη οριζόντια νομοθετική πράξη της ΕΕ που πραγματεύεται τις προκλήσεις στον τομέα της ασφάλειας στον κυβερνοχώρο και αποτελεί πραγματική τομή για την ανθεκτικότητα και τη συνεργασία στην Ευρώπη όσον αφορά την ασφάλεια στον κυβερνοχώρο. Η Κυπριακή Δημοκρατία είναι πλήρως δεσμευμένη για την επίτευξη του στόχου υψηλού κοινού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών στην Ευρωπαϊκή Ένωση, η οποία θεωρείται απολύτως απαραίτητη τόσο για το πολιτικό όσο και για το επιχειρησιακό επίπεδο που εκπροσωπούνται από τις δομές που δημιουργούνται στην Κύπρο (βλ. ενότητα 3.1). Η παρούσα Θεματική ενότητα δίνει έμφαση στην αποτελεσματική εφαρμογή και επιβολή του σχετικού Κυπριακού Νόμου[12].

Η στρατηγική ενθαρρύνει τη δημιουργία μιας διαδικασίας για την παρακολούθηση της εφαρμογής και της αναθεώρησης της νομοθεσίας και των νομικών μηχανισμών διακυβέρνησης, τον εντοπισμό κενών και αλληλεπικαλυπτόμενων αρμοδιοτήτων και τον εντοπισμό και την ιεράρχηση των τομέων που απαιτούν εκσυγχρονισμό.

Τα θέματα κυβερνοασφάλειας απαιτούν την Ευρωπαϊκή και διεθνή συνεργασία με άλλα κράτη-μέλη της Ευρωπαϊκής Ένωσης και πιθανότατα και με τρίτες χώρες. Ως εκ τούτου, είναι δυνατόν να προκύψουν νομικά θέματα στην επεξεργασία και αντιμετώπιση ηλεκτρονικών απειλών που μπορούν να προέρχονται από πηγές εκτός των ορίων της Κυπριακής Δημοκρατίας. Επομένως θεωρείται αναγκαία η δημιουργία του κατάλληλου νομικού υποβάθρου και για την αποτελεσματική συνεργασία με φορείς εντός και εκτός της Κύπρου, για επίλυση προβλημάτων όταν αυτά προκύπτουν. Στη θεματική ενότητα αυτή, θα εξεταστούν επίσης νομικά εργαλεία με τα οποία το κράτος να μπορεί να προωθεί συγκεκριμένα μέτρα, με στόχο την βελτίωση των επιπέδων κυβερνοασφάλειας σε όλους τους τομείς, είτε αυτοί θεωρούνται κρίσιμοι είτε όχι. Σχετικά παραδείγματα είναι η παροχή διαφόρων κινήτρων σε μικρομεσαίες επιχειρήσεις για την ανάπτυξη των δυνατοτήτων τους και τα επίπεδα κυβερνοασφάλειας τους, μέσω προγράμματος πιστοποίησης οργανισμών ή παρέχοντας πρόσβαση σε κυβερνητικά έργα και προγράμματα χορηγιών μόνο από εταιρείες που συμμορφώνονται με τα ελάχιστα επίπεδα κυβερνοασφάλειας. Θα εξεταστούν επίσης διάφοροι τρόποι παροχής κινήτρων, με την καθοδήγηση της Συμβουλευτικής Ομάδας Εμπλεκομένων (βλ. ενότητα 3.1).

Η θεματική ενότητα περιλαμβάνει τη θέσπιση εθνικών μηχανισμών συμμόρφωσης (τόσο για την επιβολή όσο και για τα κίνητρα). Αυτοί οι μηχανισμοί θα πρέπει να δημιουργηθούν για την πρόληψη, την καταπολέμηση και τον μετριασμό των ενεργειών που στρέφονται κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των συστημάτων και των υποδομών ΤΠΕ, και απειλώντας δεδομένα υπολογιστών, σύμφωνα με το εθνικό και Ευρωπαϊκό νομικό πλαίσιο.

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[12] Νόμος 17(Ι)2018 και όποιος Νόμος τον τροποποιεί ή τον αντικαθιστά.

Τέλος κάτω από τη παρούσα θεματική ενότητα, η στρατηγική ενθαρρύνει την ανάπτυξη ικανοτήτων επιβολής του νόμου στον κυβερνοχώρο, συμπεριλαμβανομένης της κατάρτισης και της εκπαίδευσης διαφόρων εμπλεκόμενων φορέων καταπολέμησης του εγκλήματος στον κυβερνοχώρο (π.χ. δικαστές, εισαγγελείς, δικηγόροι, αστυνομικοί, ιατροδικαστές και άλλοι ερευνητές). Οι αρχές επιβολής του νόμου πρέπει να λαμβάνουν εξειδικευμένη κατάρτιση για την ερμηνεία και την εφαρμογή της εθνικής και ευρωπαϊκής νομοθεσίας στον τομέα του κυβερνοεγκλήματος, την αποτελεσματική ανίχνευση, αποτροπή, διερεύνηση και δίωξη εγκλημάτων στον κυβερνοχώρο και να συνεργάζονται αποτελεσματικά με τους φορείς της βιομηχανίας και των διεθνών φορέων επιβολής του νόμου (π.χ. INTERPOL, Europol) για την αντιμετώπιση του κυβερνοεγκλήματος και την ενίσχυση της ασφάλειας στον κυβερνοχώρο (βλ. θεματική ενότητα 14 και θεματική ενότητα 15). Το στοιχείο αυτό θα πρέπει να λαμβάνει υπόψη την θεματική ενότητα 10 για την εκπαίδευση κατάρτιση και την ανάπτυξη ικανοτήτων και την θεματική ενότητα 9 για την ευαισθητοποίηση και την ενημέρωση.

Δράσεις:

Δράση 3 - Πλήρης υλοποίηση όλων των προνοιών και του ρυθμιστικού πλαισίου της Οδηγίας NIS, σε όλα τα επίπεδα, με έμφαση στις κρίσιμες υποδομές πληροφοριών και τους φορείς εκμετάλλευσης βασικών υπηρεσιών.

Δράση 4 - Ενίσχυση του υφιστάμενου νομικού, κανονιστικού και ρυθμιστικού πλαισίου για την πλήρη ενεργοποίηση και υποστήριξη των προνοιών της Στρατηγικής Κυβερνοασφάλειας, και την δημιουργία νέων νομοθεσιών όπου χρειάζεται. Θα πρέπει να εξεταστούν όλες οι σχετικές νομοθεσίες των αρμοδίων αρχών εφόσον προκύπτει ανάγκη προσαρμογής. Θα πρέπει να εξεταστεί το νομικό πλαίσιο συνεργασίας και ανταλλαγής πληροφοριών με τρίτες χώρες και οργανισμούς του ιδιωτικού τομέα, καθώς και της προώθησης πιθανού πλαισίου πολιτικής για την παροχής κινήτρων σε επιχειρήσεις για την αναβάθμιση και ενίσχυση των επιπέδων κυβερνοασφάλειας στις υποδομές τους. Θα πρέπει να αναθεωρηθεί ή και να καθοριστεί νέα διαδικασία για την παρακολούθηση της εφαρμογής και της αναθεώρησης της νομοθεσίας καθώς και μηχανισμοί ελέγχου συμμόρφωσης.

3.4. Θεματική ενότητα 4 – Εθνικό Πλαίσιο Κυβερνοασφάλειας

Στρατηγικοί στόχοι: Διαχείριση Κινδύνων, Ανάπτυξη Δυνατοτήτων

Η Θεματική ενότητα αυτή προβλέπει την ανάπτυξη ενός ολοκληρωμένου Εθνικού Πλαισίου Κυβερνοασφάλειας, το οποίο αποτελεί μια από τις κύριες δραστηριότητες της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας. Αφορά στην πρόληψη συμβάντων στον κυβερνοχώρο με δυσμενείς επιπτώσεις σε εθνικό επίπεδο. 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, θα διαχειρίζονται τους κινδύνους που είναι σχετικοί με την κυβερνοασφάλεια. Ο στόχος είναι να επεκταθεί το υφιστάμενο πλαίσιο το οποίο θα μπορεί να

χρησιμοποιηθεί από τον κάθε φορέα, ανεξάρτητα από το βαθμό ευαισθησίας και αξίας των πληροφοριών που χειρίζεται. Ενδεικτικά, το πλήρες Εθνικό Πλαίσιο Κυβερνοασφάλειας θα περιλαμβάνει, μεταξύ άλλων, δραστηριότητες όπως:

- Καθορισμό αξίας και ευαισθησίας πληροφοριών και υποδομών
- Αναλύσεις και διαχείριση επικινδυνότητας (risk assessment and management)
- Ανάλυση και διαχείριση ευπαθειών (vulnerability analysis and management)
- Καθορισμό πιθανών μέτρων ασφάλειας (security controls)
- Μεθοδολογία επιλογής μέτρων ασφάλειας
- Εφαρμογή μέτρων ασφάλειας
- Δοκιμές διείσδυσης (penetration testing)
- Έλεγχο συμμόρφωσης (review and compliance audits).

Το Εθνικό Πλαίσιο Κυβερνοασφάλειας είναι δυνατόν να περιέχει μεγάλο αριθμό μέτρων ασφάλειας, τα οποία όμως, δε θα εφαρμόζονται απαραίτητα σε όλες τις περιπτώσεις. Ως εκ τούτου το Πλαίσιο θα περιλαμβάνει μεθοδολογία επιλογής μέτρων ασφάλειας, ώστε να επιλέγονται και να εφαρμόζονται όσα μέτρα ασφάλειας είναι αναγκαία για την κάθε περίπτωση, πάντα με βάση τα αποτελέσματα μιας σωστής και δομημένης αξιολόγησης κινδύνων. Όπου είναι δυνατό, θα προωθείται η χρήση σχετικών προτύπων, τα οποία έχουν αναπτυχθεί με γνώμονα τις καλές πρακτικές (good practices) για την αποτελεσματική προστασία από απειλές του κυβερνοχώρου.

Οι ειδικοί στόχοι της παρούσας Δράσης συνοψίζονται ως εξής:

1. Η αποτελεσματική και συνεχής ενίσχυση της θωράκισης των δικτύων και πληροφοριών της Δημόσιας Υπηρεσίας, του Ευρύτερου Δημόσιου Τομέα και των Κρίσιμων Υποδομών Πληροφορίας από σχετικές απειλές του κυβερνοχώρου.
2. Ανάπτυξη ενιαίας μεθοδολογίας για χρήση σε όλους τους τομείς, που να επιτρέπει συγκρίσιμα επίπεδα ασφάλειας, βάσει των αναγκών της κάθε υπηρεσίας / τμήματος / οργανισμού / επιχείρησης.
3. Πλαίσιο που να επιτρέπει μετρήσιμα αποτελέσματα ελέγχων και αξιολόγησης για τα επίπεδα κυβερνοασφάλειας στην Κυπριακή Δημοκρατία.

Σημειώνεται ότι οι συγκεκριμένοι στόχοι που θα τεθούν ως προς τα επίπεδα προστασίας των συστημάτων που αναφέρονται στη παρούσα θεματική ενότητα, θα προσδιοριστούν από την ανάλυση της αξιολόγησης κινδύνων (risks) στον κάθε τομέα και λαμβάνοντας υπόψη το κόστος υλοποίησης των συγκεκριμένων μέτρων σε σχέση με το όφελος ως προς την αντιμετώπιση των σχετικών απειλών από τον κυβερνοχώρο.

Δράση:

Δράση 5 - Ανάπτυξη ενός Εθνικού Πλαισίου Κυβερνοασφάλειας το οποίο θα προωθεί την προστασία των κρίσιμων υποδομών πληροφοριών στην Κυπριακή Δημοκρατία, ως επίσης όλων των κυβερνητικών υπηρεσιών του κράτους.

3.5. Θεματική ενότητα 5 – Αξιολόγηση και Διαχείριση Κινδύνων – Αξιολόγηση Κρισιμότητας

Στρατηγικοί στόχοι: Διαχείριση Κινδύνων

Το πλαίσιο των μέτρων προστασίας των κρίσιμων υποδομών πληροφοριών, όπως αναδεικνύεται και επεξηγείται στο παρόν έγγραφο και ειδικότερα στην Θεματική ενότητα 4 πιο πάνω, είναι αναγκαίο για την ελαχιστοποίηση των αρνητικών επιπτώσεων και καταστροφικών συνεπειών από πιθανές κακόβουλες ενέργειες ή φυσικές καταστροφές στις υποδομές, σε εθνικό επίπεδο εντός της Κυπριακής Δημοκρατίας. Επίσης όπως προκύπτει από της υποχρεώσεις της Κύπρου σε σχέση με το εφαρμοστέο Ευρωπαϊκό δίκαιο, το πλαίσιο είναι απαραίτητο για την αντιμετώπιση πιθανών επιπτώσεων σε υποδομές άλλων χωρών ή/και οργανισμών, λόγω της μεγάλης αλληλεπίδρασης και αλληλοσύνδεσης των διεθνών δικτύων επικοινωνίας και της σύνδεσης πολλών κρίσιμων υποδομών της Κυπριακής Δημοκρατίας με Ευρωπαϊκά δίκτυα (στην Ευρωπαϊκή Ένωση και με άλλα Κράτη Μέλη) που συνεπάγεται.

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 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.

Σε Ευρωπαϊκό επίπεδο, τα τελευταία χρόνια δίδεται ψηλή προτεραιότητα, στα θέματα ανάλυσης επικινδυνότητας, σε διάφορα επίπεδα και σχεδόν σε όλους τους τομείς. Ως εκ τούτου, η Κυπριακή Δημοκρατία προβαίνει σε ανάλογες αναλύσεις σε διάφορους τομείς, όπως σε πρόσφατο έργο της Πολιτικής Άμυνας (βρίσκεται σε εξέλιξη), το οποίο αναλύει την επικινδυνότητα σε αριθμό τομέων που σχετίζονται με το Βασικό Εθνικό Σχέδιο «ΖΗΝΩΝ» (πλημμύρες, σεισμούς, διακοπή δικτύων επικοινωνίας, κλπ). Η τακτική εκτέλεση αξιολόγησης επικινδυνότητας για την κυβερνοασφάλεια συνάδει με αυτές τις δραστηριότητες και θα δώσει πιο ολοκληρωμένη πληροφόρηση σε αυτούς που λαμβάνουν αποφάσεις σχετικά με την επικινδυνότητα και την αντιμετώπιση της (risk decision makers).

3.5.1. Αξιολόγηση Επικινδυνότητας και Αξιολόγηση Κρισιμότητάς σε Εθνικό επίπεδο

Η αξιολόγηση επικινδυνότητας σε εθνικό επίπεδο, αποσκοπεί στην ανάπτυξη ενός εθνικού μητρώου κινδύνων, το οποίο αποθηκεύεται και να διαβιβάζεται με ασφάλεια, ώστε να επιτρέπεται η κρατική εποπτεία των κινδύνων και των προσεγγίσεων που λαμβάνονται για τη διαχείριση αυτών. Η ΑΨΑ θα πρέπει να αναπτύξει μια μέθοδο ιεράρχησης των κινδύνων βάσει της εκτίμησης της πιθανότητας πραγματοποίησης των κινδύνων και των επιπτώσεών τους. Οι κίνδυνοι που αναγνωρίζονται βάσει των πιο πάνω δραστηριοτήτων θα πρέπει να παρακολουθούνται συστηματικά, ενώ θα χρησιμοποιούνται ως καθοδήγηση για την εκτέλεση των υπολοίπων Δράσεων της Στρατηγικής.

Στα πλαίσια της διαδικασίας διαχείρισης εθνικών κινδύνων κυβερνοασφάλειας, πρέπει να απαντάται το ερώτημα για το ποιες ακριβώς υποδομές θα πρέπει να θεωρούνται ‘κρίσιμες’. Απαιτείται ο εντοπισμός και αξιολόγηση των πραγματικά κρίσιμων υποδομών στην Κυπριακή Δημοκρατία και η στόχευση τους για την καλύτερη δυνατή προστασία. Οι κρίσιμες αυτές υποδομές εντοπίζονται και αξιολογούνται βάσει της μεθοδολογίας που έχει αναπτυχθεί σε σχετική δράση της πρώτης Εθνικής Στρατηγικής

Κυβερνοασφάλειας, ως αυτή τροποποιείται και βελτιώνεται, και η μεθοδολογία αυτή αποτελεί αναπόσπαστο μέρος της διαχείρισης κινδύνων σε εθνικό επίπεδο. Για τη βελτιστοποίηση της αξιολόγησης αυτής, θα πρέπει να διενεργούνται σχετικές αξιολογήσεις κινδύνων από τον κάθε φορέα που χειρίζεται κρίσιμες υποδομές (βλ. θεματική ενότητα 3.4 - Πλαίσιο Κυβερνοασφάλειας).

3.5.2. Αξιολόγηση επικινδυνότητας και διαχείριση κινδύνων σε επίπεδο κρίσιμων υποδομών πληροφοριών και βασικών υπηρεσιών

Η ΑΨΑ ως αρμόδια αρχή θα πρέπει να καθορίσει μια συνεκτική προσέγγιση για την αξιολόγηση των κινδύνων και σε επίπεδο κρίσιμων υποδομών πληροφοριών και βασικών υπηρεσιών, η οποία πρέπει να ακολουθείται από όλες τις κυβερνητικές οντότητες και τους φορείς εκμετάλλευσης κρίσιμων υποδομών πληροφορίων και βασικών υπηρεσιών, που εντοπίζονται σε εθνικό επίπεδο. Η προσέγγιση θα πρέπει επίσης να οδηγεί στον εντοπισμό των βασικών στοιχείων του ενεργητικού και των υπηρεσιών των κρίσιμων υποδομών πληροφοριών και βασικών υπηρεσιών, οι οποίες είναι κρίσιμες για την εύρυθμη λειτουργία της κοινωνίας και της οικονομίας, καθώς και τις απειλές και τους κινδύνους που συνδέονται με αυτές. Επιπλέον, θα πρέπει να προσδιοριστούν οι ευθύνες των βασικών φορέων σε κάθε τομέα όσον αφορά την εκτίμηση, αποδοχή και αντιμετώπιση των εθνικών κινδύνων στον κυβερνοχώρο.

Η ΑΨΑ θα πρέπει επίσης να καθορίσει μια κοινή μεθοδολογία για τη διαχείριση των κινδύνων ασφάλειας στον κυβερνοχώρο. Αυτό θα διασφαλίσει την αποτελεσματικότητα και τη συνοχή σε όλους τους οργανισμούς και θα διευκολύνει την ανταλλαγή πληροφοριών σχετικά με τους κινδύνους μεταξύ των αλληλοεξαρτώμενων συστημάτων. Η μεθοδολογία είναι δυνατόν να λαμβάνει υπόψη τα διεθνή πρότυπα, καθώς μπορεί να μειώσει το κόστος και να αποφέρει καλύτερη αλληλεπίδραση με τον ιδιωτικό τομέα. Η μεθοδολογία θα πρέπει να παρέχει καθοδήγηση σχετικά με την ανάθεση ρόλων και αρμοδιοτήτων για διάφορες πτυχές διαχείρισης κινδύνου, όπως η εκτίμηση των απειλών, η αποτίμηση των περιουσιακών στοιχείων, η εφαρμογή και η διατήρηση των μέτρων μετριασμού των επιπτώσεων και η αποδοχή του εναπομένοντος κινδύνου. Η μεθοδολογία θα πρέπει να περιλαμβάνει πρόγραμμα πιστοποίησης που θα συμβάλλει στην αξιολόγηση και τελικά στη βελτίωση της συμμόρφωσης. Είναι σημαντικό ότι για τη σύναψη συμβάσεων και την ανάπτυξη υποδομών ή υπηρεσιών, η μεθοδολογία διαχείρισης των κινδύνων θα πρέπει επιπλέον να παρέχει καθοδήγηση σχετικά με την ελαχιστοποίηση του κινδύνου μέσω ασφαλούς αρχιτεκτονικής και σχεδιασμού, αναγνωρίζοντας ότι η ασφάλεια επιτυγχάνεται καλύτερα όταν αποτελεί αναπόσπαστο μέρος της διαδικασίας σχεδιασμού ενός προϊόντος, μιας διαδικασίας ή μιας υπηρεσίας (security by design).

Δράσεις:

Δράση 6 - Αξιολόγηση και διαχείριση των κινδύνων κυβερνοασφάλειας στην Κυπριακή Δημοκρατία, μέσω μιας δομημένης μεθοδολογίας για τον εντοπισμό των κρίσιμων υποδομών πληροφορίας και των κινδύνων που δύναται να τις επηρεάσουν, με ανάλυση των πιθανών επιπτώσεων και των επιλογών μετριασμού (risk treatment options), καθώς και της συνεχούς βελτίωσης.

6.1 Η αξιολόγηση κινδύνων θα διενεργείται σε τακτά χρονικά διαστήματα (κάθε 2 χρόνια) για επικαιροποίηση των αποτελεσμάτων και καθοδήγηση του συνόλου των Δράσεων της Στρατηγικής, σύμφωνα με τις πρόνοιες της οδηγίας NIS και της κείμενης εθνικής νομοθεσίας.

6.2 Η αξιολόγηση κρισιμότητας θα διενεργείται κάθε δύο χρόνια ή/και ενωρίτερα εφόσον προκύπτει ανάγκη σύμφωνα με τις πρόνοιες της οδηγίας NIS και της κείμενης εθνικής νομοθεσίας.

Δράση 7 - Ανάπτυξη συνεκτικής μεθοδολογίας για την αξιολόγηση και διαχείριση κινδύνων σε επίπεδο κρίσιμων υποδομών πληροφοριών και βασικών υπηρεσιών.

3.6. Θεματική ενότητα 6 – Αντιμετώπιση Συμβάντων και Διαχείριση Κρίσεων

Στρατηγικοί στόχοι: Διαχείριση Περιστατικών και Κρίσεων

Αν και οι δράσεις που αναφέρονται στην Θεματική ενότητας 4 (Ανάπτυξη Εθνικού Πλαισίου Κυβερνοασφάλειας) και στην Θεματική ενότητα 5 (Αξιολόγηση και Διαχείριση Κινδύνων – Διαχείριση Κρισιμότητας), αποσκοπούν στην ελαχιστοποίηση των κινδύνων και την αποτροπή περιστατικών κυβερνοασφάλειας, οι κίνδυνοι, οι απειλές και τα περιστατικά δεν μπορούν να εκμηδενιστούν. Ω εκ τούτου και λόγω της πάντοτε υπαρκτής πιθανότητας εκδήλωσης συμβάντων με δυσμενείς επιπτώσεις, κρίνεται απαραίτητο όπως διασφαλιστούν οι δυνατότητες διαχείρισης περιστατικών (incident management), με την ανάπτυξη ικανοτήτων προς το σκοπό αυτό σε εθνικό επίπεδο.

3.6.1. Λειτουργία Ομάδων Διαχείρισης περιστατικών Κυβερνοαασφάλειας (CSIRT - Computer Security Incident Response Team)

Πρόσφατα έχει ιδρυθεί το Εθνικό CSIRT[13] (Computer Security Incident Response Team) της Κύπρου (CSIRT-CY), το οποίο υποστηρίζει τις κρίσιμες υποδομές πληροφοριών όσο αφορά στην αντιμετώπιση μεγάλων συμβάντων και επιθέσεων στον κυβερνοχώρο. Κύρια λειτουργία ενός CSIRT είναι η πρόληψη σοβαρών συμβάντων που σχετίζονται με την ασφάλεια δικτύων και πληροφοριών καθώς επίσης και η άμεση ανταπόκριση σε ένα τέτοιο συμβάν αν προκύψει. Σημειώνεται με έμφαση ότι για τη σωστή λειτουργία ενός CSIRT απαιτούνται: α) αναγκαίες υποδομές και β) στελέχωση, κατάρτιση και εκπαίδευση του προσωπικού. Βασική προϋπόθεση για τη σωστή λειτουργία των εν λόγω υπηρεσιών είναι η έμπρακτη υποστήριξη του κράτους. Οι εξειδικευμένες ομάδες CSIRT θα πρέπει να παρέχουν ένα σύνολο τόσο προληπτικών όσο και αντιδραστικών λειτουργιών, καθώς και προληπτικών και εκπαιδευτικών υπηρεσιών. Οι ομάδες αυτές μπορούν να αυξήσουν την ικανότητα μιας χώρας να ανταποκρίνεται γρήγορα και να ανακάμπτει από κυβερνοεπιθέσεις, καθώς και να βελτιώσει την ανθεκτικότητά της Κυπριακής Δημοκρατίας έναντι των απειλών από τον Κυβερνοχώρο, μειώνοντας τις πιθανές συνολικές οικονομικές και επιχειρησιακές επιπτώσεις στις κρίσιμες υποδομές πληροφοριών.

Η ίδρυση του Εθνικού CSIRT δε σημαίνει ότι δε θα λειτουργούν άλλα CSIRT στην Κύπρο (π.χ. κυβερνητικό, ακαδημαϊκό, πιθανά τομεακά, κλπ), αλλά η λειτουργία τους θα είναι συμπληρωματική και θα

[13] http://www.csirt.cy

εποπτεύεται από την Αρχή Ψηφιακής Ασφάλειας. Εντός της παρούσας Θεματικής ενότητας, προβλεπεται η αξιολόγηση των αναγκών για κάλυψη υπηρεσιών CSIRT σε τακτά χρονικά διαστήματα, και σε περιπτώσεις όπου κρίνεται απαραίτητο θα τεκμηριώνεται η ανάγκη και θα προωθείται η δημιουργία επιπρόσθετων CSIRT, όπως για παράδειγμα τομεακά CSIRT, ή/και θα ενισχύεται κατάλληλα το εθνικό CSIRT. Οι ανάγκες θα προσδιορίζονται σε σχέση με την κατανόηση και επίγνωση της κατάστασης όσο αφορά τις κυβερνοαπειλές και σχετικά περιστατικά στην Κύπρο, καθώς και με τους στρατηγικούς σχεδιασμούς του κράτους για προώθηση σημαντικών τομέων της οικονομίας (π.χ. εμπορική ναυτιλία, οικονομικές υπηρεσίες, κλπ.). Θα εξεταστούν τα οφέλη από τη δημιουργία τομεακών CSIRT σε τέτοιους σημαντικούς τομείς της οικονομίας, και όπου κρίνεται επωφελές θα προωθηθεί η δημιουργία τους στα πλαίσια ολοκληρωμένου σχεδιασμού.

Στα πλαίσια της ευρωπαϊκής συνεργασίας στον τομέα της ασφάλειας των πληροφοριών, όπως αυτή περιγράφεται στην Οδηγία NIS, εντάσσεται και η συνεργασία των CSIRTs που λειτουργούν σε κάθε κράτος μέλος. Με στόχο την ένταξη των Κυπριακών CSIRT στους εν λόγω μηχανισμούς συνεργασίας, θα πρέπει να διασφαλισθεί η πλήρης λειτουργία τους ώστε να εξασφαλισθεί η αναγκαία πιστοποίηση τους για να καταστεί δυνατή η συμμετοχή τους στις Ευρωπαϊκές ομάδες εργασίας.

Θα πρέπει να δημιουργηθεί ξεκάθαρο πλαίσιο και διαδικασίες με λεπτομέρειες για τον τρόπο και τις διαδικασίες κοινοποίησης συμβάντων προς τα αρμόδια σώματα (CSIRT-CY/ΑΨΑ – τομεακά CSIRT) για να μπορέσει να προτεραιοποιηθεί κατάλληλα η ανταπόκριση. Το πλαίσιο αυτό θα πρέπει να είναι συμφωνημένο και να τυγχάνει σεβασμού από όλους τους εμπλεκομένους και να περιέχει στοιχεία όσον αφορά αρχιτεκτονική, διεπαφές και πρότυπα για τη δομημένη ανταλλαγή πληροφοριών ώστε να βελτιστοποιείται η ανταπόκριση σε μεγάλα συμβάντα (βλ. θεματική ενότητα 3.6 - Αντιμετώπιση Συμβάντων και Διαχείριση Κρίσεων).

3.6.2. Διαχείριση κρίσεων

Όπως επεξηγείται και πιο πάνω, κανένα τεχνολογικό σύστημα ή δέσμη μέτρων και δράσεων, όσο περιεκτικά και να είναι, **δεν μπορούν να προστατέψουν σε απόλυτο βαθμό** τον κυβερνοχώρο, και ειδικά τις κρίσιμες υποδομές πληροφοριών μιας οποιασδήποτε χώρας. Με γνώμονα το γεγονός αυτό, επιβάλλεται η αναθεώρηση και επικαιροποίηση του σχετικού Σχεδίου Έκτακτης Ανάγκης (Contingency Plan) για τις Κρίσιμες Υποδομές Πληροφοριών. Ο στόχος του σχεδίου αυτού είναι η καθοδήγηση και η 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. Το σχέδιο που αναπτύσσεται κάτω από την παρούσα Στρατηγική, πρέπει να αποτελεί μέρος του γενικού εθνικού σχεδίου έκτακτης ανάγκης της Κυπριακής Δημοκρατίας. Οι σχεδιασμοί πρέπει να είναι ευθυγραμμισμένοι με την ευρύτερη Εθνική πολιτική.

Το εθνικό σχέδιο έκτακτης ανάγκης για την κυβερνοασφάλεια θα πρέπει να εξετάζει τα ευρήματα από τις εθνικές αξιολογήσεις κινδύνου (βλ. θεματική ενότητα 3.5 - Αξιολόγηση και Διαχείριση Κινδύνων – Αξιολόγηση Κρισιμότητας) και τις ενδεχόμενες διατομεακές εξαρτήσεις που θα μπορούσαν να επηρεάσουν τη συνέχεια των λειτουργιών των υποδομών ζωτικής σημασίας, καθώς και κάθε μηχανισμό αντιμετώπισης καταστροφών. Επιπλέον, θα πρέπει να παρέχει μια επισκόπηση των εθνικών μηχανισμών αντιμετώπισης περιστατικών, καθώς να επισημαίνει και να ταξινομεί τα περιστατικά στον κυβερνοχώρο, με βάση τον αντίκτυπό τους στα κρίσιμα στοιχεία ενεργητικού και στις υπηρεσίες. Ειδικότερα η δημιουργία και ανάπτυξη του Σχεδίου Έκτακτης Ανάγκης συμπεριλαμβάνει τις ακόλουθες ενέργειες:

- την ανάπτυξη κατηγοριών και ιεράρχησης των κρίσιμων υποδομών, βάσει της συμβολής τους στην διατήρηση ζωτικών υπηρεσιών επικοινωνίας και πληροφορίας και βάσει των σχετικών αποτελεσμάτων της τακτικής αξιολόγησης κινδύνων (βλ. θεματική ενότητα 5 - Αξιολόγηση και Διαχείριση Κινδύνων – Αξιολόγηση Κρισιμότητας),
- την ανάπτυξη συστημάτων και διαδικασιών "early warning" για την παρακολούθηση των υποδομών, με τη βοήθεια του Εθνικού CSIRT,
- τη δημιουργία (ή βελτίωση ήδη υπαρχόντων) δικτύων επικοινωνίας έκτακτης ανάγκης τα οποία να είναι ανεξάρτητα από τα κύρια δίκτυα και, εάν είναι δυνατόν, χρησιμοποιώντας άλλο φυσικό μέσο επικοινωνίας (π.χ. ενσύρματα, κινητά και δορυφορικά δίκτυα),
- την ανάπτυξη **πλήρων** διαδικασιών επικοινωνίας και διαχείρισης μιας κρίσης μεταξύ των διαχειριστών κρίσιμων υποδομών πληροφορίας και επικοινωνίας για να επιτευχθεί αποδοτική συνεργασία μεταξύ τους,
- τη διεξαγωγή τακτικών εθνικών ασκήσεων με ρεαλιστικά σενάρια κρίσης για δοκιμασία και βελτίωση των πιο πάνω διαδικασιών,
- τον εντοπισμό διαθέσιμων πόρων σε επίπεδο εξοπλισμού και υποδομής, όπου αυτό κριθεί χρήσιμο ή απαραίτητο, μεταξύ των εμπλεκομένων υπηρεσιών, και τη δημιουργία συνεργιών για αλληλοκάλυψη των πόρων και αλληλοϋποστήριξη των υπηρεσιών σε περίπτωση έκτακτης ανάγκης.

Σημειώνεται ότι οι πιο πάνω πρόνοιες, όπου υπάρχει ανάγκη, θα αξιοποιηθούν στα πλαίσια της συμβολής της Κύπρου στις εργασίες διαμόρφωσης του Rapid Emergency Response Blueprint[14] για την συνεργασία μεταξύ των χωρών της ΕΕ και για την συνεργασία με τις ευρωπαϊκές δομές.

Δράσεις:

Δράση 8 - Εδραίωση του Εθνικού (και άλλων κατά περίπτωση - τομεακών) CSIRT στην Κύπρο, με ανάπτυξη των κατάλληλων διαδικασιών και διεπαφών ανταλλαγής πληροφοριών, ώστε να επιτυγχάνεται η αποτελεσματική ανταπόκριση και διαχείριση συμβάντων στην Κυπριακή Δημοκρατία.

Δράση 9 - Ανάπτυξη επικαιροποιημένου σχεδίου έκτακτης ανάγκης για αντιμετώπιση κρίσεων σε θέματα κυβερνοασφάλειας και χρήση του σε όλες τις σχετικές ασκήσεις (σύνδεση με δράση 11).

[14] http://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=3&year=2017&number=6100&version=ALL

3.7. Θεματική ενότητα 7 – Ανάπτυξη Δυνατοτήτων – Διοργάνωση και Συμμετοχή σε Ασκήσεις

Στρατηγικοί στόχοι: Ανάπτυξη Δυνατοτήτων, Συνεργασία, Εκπαίδευση, Κατάρτιση και Επίγνωση

3.7.1. Ανάπτυξη Ικανοτήτων

Ως μέρος των δραστηριοτήτων για την πλήρη υλοποίηση της Οδηγίας NIS (βλ. θεματική ενότητα 3 - Νομικό και Ρυθμιστικό Πλαίσιο), οι χειριστές κρίσιμων υποδομών πληροφοριών θα πρέπει να συμμορφώνονται με συγκεκριμένες υποχρεώσεις κυβερνοασφάλειας, και θα υπόκεινται σε σχετικούς ελέγχους συμμόρφωσης. Είναι αναμενόμενο ότι δε θα είναι όλοι οι χειριστές κρίσιμων υποδομών πληροφοριών στο ίδιο επίπεδο όσο αφορά τις δυνατότητες τους στην αποτελεσματική προστασία από απειλές στον κυβερνοχώρο, τουλάχιστο στα αρχικά στάδια εφαρμογής της Οδηγίας.

Ως εκ τούτου, θα πρέπει να υπάρχει η δυνατότητα υποστήριξης των προσπαθειών τέτοιων οργανισμών και θα πρέπει να μελετηθούν τρόποι με τους οποίους μπορούν να βοηθηθούν για να αναπτύξουν περαιτέρω τις δυνατότητες τους. Ως πολύπλευρο θέμα, η διατήρηση υψηλών επιπέδων κυβερνοασφάλειας απαιτεί εξειδίκευση και πολυδιάστατη κατάρτιση, και έτσι είναι σημαντική η ανάπτυξη δυνατοτήτων στα θέματα αυτά. Παράλληλα, θα μπορούν και άλλοι οργανισμοί να επωφεληθούν από τις σχετικές προσπάθειες υποστήριξης των εμπλεκομένων μερών, και θα μελετηθούν οι βέλτιστοι τρόποι με τους οποίους θα μπορεί το κράτος να υποστηρίζει τις ενέργειες αυτές.

Όπως αναφέρεται στην ενότητα 2.3 (Αρμόδιες Αρχές) της Στρατηγικής, υπάρχουν πολλοί εμπλεκόμενοι φορείς που πρέπει να συνεργάζονται για την αποτελεσματική αντιμετώπιση απειλών από τον κυβερνοχώρο. Ένας σημαντικός τομέας συνεργασίας είναι και η "ανάπτυξη δυνατοτήτων" Τονίζεται ότι ο όρος "ανάπτυξη δυνατοτήτων", δεν αναφέρεται μόνο σε τεχνικά και οργανωτικά μέτρα, αλλά επεκτείνεται και σε δομές, συστήματα διοίκησης και αναγκαίους πόρους (Θεματική ενότητα 1), όπως σε κατάλληλο ανθρώπινο δυναμικό και οικονομικές δυνατότητες, σε θέματα συνεργασίας (Θεματικές ενότητες 2, 12, 14), σε κατάλληλους επιχειρησιακούς σχεδιασμούς (Θεματικές ενότητες 4, 6), στο γνωστικό υπόβαθρο (Θεματική ενότητα 10) και το ανάλογο νομικό πλαίσιο (Θεματική ενότητα 3) κλπ. Η ΑΨΑ θα πρέπει να προωθεί μέτρα για την για συνεχή εκπαίδευση και κατάρτιση του προσωπικού των κρίσιμων υποδομών πληροφοριών και των βασικών υπηρεσιών (Θεματική ενότητα 10), είτε με πρωτοβουλίες της Αρχής, είτε των ίδιων των οργανισμών. Σε κάθε περίπτωση η ΑΨΑ θα πρέπει να διασφαλίζει ένα ελάχιστο επίπεδο γνώσεων και δυνατοτήτων αντιμετώπισης των προκλήσεων από τον κυβερνοχώρο.

Πέραν από τα πιο πάνω βασικός κανόνας για την "ανάπτυξη δυνατοτήτων" αποτελεί η συνεχής αξιολόγηση, η προσομοίωση πραγματικών καταστάσεων και ό έλεγχος σωστής εφαρμογής των επιχειρησιακών σχεδιασμών, των δομών, των γνώσεων, του νομοθετικού πλαισίου και γενικά όλων των στοιχείων που απαιτούνται για την αποδοτική ανταπόκριση στις απειλές, τους κινδύνους και τα περιστατικά από τον Κυβερνοχώρο. Ο ποιο αποδοτικός τρόπος αξιολόγησης και ελέγχου της ετοιμότητας των εμπλεκομένων ομάδων στην διαχείριση των θεμάτων Κυβερνμοασφάλειας, είναι ο προγραμματισμός και η διενέργεια ασκήσεων τόσο σε εθνικό όσο και σε ευρωπαϊκό και διεθνές επίπεδο.

3.7.2. Διοργάνωση και συμμετοχή σε Ασκήσεις

Η στρατηγική ενθαρρύνει την οργάνωση και τον συντονισμό εθνικών, ευρωπαϊκών και διεθνών ασκήσεων για την ασφάλειας στον κυβερνοχώρο και την αντιμετώπιση περιστατικών κυβερνοασφάλειας. Οι εν λόγω ασκήσεις μπορούν να έχουν διαφορετικές μορφές (π.χ. προσομοιώσεις

ή ασκήσεις σε πραγματικό χρόνο) και να στοχεύουν στην άσκηση της τεχνικής κοινότητας και των υπευθύνων στην λήψη αποφάσεων.

Οι ασκήσεις στον κυβερνοχώρο και άλλοι μηχανισμοί προσομοίωσης κρίσεων μπορούν να βοηθήσουν τις χώρες να αναπτύξουν τη θεσμική ικανότητα αποτελεσματικής αντιμετώπισης των περιστατικών, να δοκιμάσουν διαδικασίες διαχείρισης κρίσεων και μηχανισμούς επικοινωνίας, να επαληθεύσουν την επιχειρησιακή ικανότητα των CSIRTs να ανταποκριθούν υπό την πίεση, και να εντοπίσουν τις αλληλεξαρτήσεις του τομέα.

Ομοίως, οι ευρωπαϊκές και διεθνείς ασκήσεις στον κυβερνοχώρο μπορούν να συμβάλουν στην ενίσχυση της ικανότητας αντίδρασης στον κυβερνοχώρο μεταξύ των κρατών, να κατανοήσουν τις διασυνοριακές εξαρτήσεις, να οικοδομήσουν εμπιστοσύνη μεταξύ των χωρών και να βελτιώσουν το συνολικό διεθνές επίπεδο ανθεκτικότητας και ετοιμότητας.

Η διενέργεια τέτοιων ασκήσεων έχει αποδειχτεί, επίσης, ως ένα πολύ σημαντικό εργαλείο για την διασφάλιση της ετοιμότητας των αρμόδιων φορέων για να αντιμετωπίσουν μια πιθανή κρίση, π.χ. μια απώλεια σημαντικού μέρους ενός μεγάλου δικτύου επικοινωνιών. Οι ασκήσεις που διεξάγονται στα Κράτη Μέλη καθώς επίσης και σε Πανευρωπαϊκό επίπεδο, έχουν δείξει ότι παρά την ύπαρξη κατάλληλων μηχανισμών αντιμετώπισης μιας τέτοιας κρίσης, το στοιχείο που συνήθως λείπει, για να είναι αποτελεσματική η ανταπόκριση σε μια κρίση, είναι οι **λεπτομέρειες για τον συντονισμού της συνεργασίας** μεταξύ των αρμόδιων φορέων (π.χ. ποιος θα επικοινωνήσει με ποιόν σε περίπτωση κρίσης, πως ακριβώς επιτυγχάνεται η γρήγορη συνεργασία μεταξύ φορέων, κλπ).

Η Κυπριακή Δημοκρατία έχει πολλά να κερδίσει από την διοργάνωση και την ενεργή συμμετοχή της σε τέτοιες ασκήσεις. Ασφαλώς το όφελος μεγιστοποιείται από την διεξαγωγή παρόμοιων εθνικών ασκήσεων με ρεαλιστικά σενάρια. Η διεξαγωγή τέτοιων ασκήσεων θα συμβάλει στην μεγιστοποίηση του βαθμού ετοιμότητας της Κυπριακής Δημοκρατίας να ανταπεξέλθει σε σημαντικά συμβάντα στον χώρο της κυβερνοασφάλειας που ενδεχομένως να επηρεάσουν μεγάλο μέρος του πληθυσμού.

Δράσεις:

Δράση 10 - 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. Οι ικανότητες αυτές θα πρέπει να καλύπτουν το πλήρες φάσμα δραστηριοτήτων κυβερνοασφάλειας – Identify, Detect, Protect, Respond, Recover στα πλαίσια συνεχούς βελτίωσης.

Δράση 11 - Προγραμματισμός και διοργάνωση τακτικών εθνικών ασκήσεων για την κυβερνοασφάλεια, στη βάση ρεαλιστικών σεναρίων, καθώς και ενεργή συμμετοχή σε Πανευρωπαϊκές και άλλες διεθνείς ασκήσεις (σύνδεση με Δράση 9).

3.8. Θεματική ενότητα 8 – Ανταλλαγή Πληροφοριών – Επίγνωση Κατάστασης (Situational Awareness)

Στρατηγικοί στόχοι: Συνεργασία, Κατανόηση Κατάστασης, Εκπαίδευση, **Κατάρτιση και Επίγνωση**

3.8.1. Ανταλλαγή Πληροφοριών

Η συνεχώς αυξανόμενη χρήση των νέων τεχνολογιών και η εξάρτηση βασικών λειτουργιών της οικονομίας και της κοινωνίας ενός κράτους από την αξιοποίηση τους, σε συνδυασμό με την συνεπακόλουθη αύξηση των απειλών, των κινδύνων και της πολυπλοκότητας των περιστατικών ασφάλειας, αυξάνουν την σημασία και τη σοβαρότητα των πιθανών επιπτώσεων (impacts) από κυβερνοεπιθέσεις, ειδικότερα σε κρίσιμα συστήματα. Ο κάθε οργανισμός από μόνος του είναι δύσκολο να παρακολουθεί και να αναλύει τον τεράστιο όγκος πληροφοριών που πρέπει να λαμβάνει υπόψη για την αντιμετώπιση των προκλήσεων, των απειλών, των κινδύνων και των ευπαθειών που εντοπίζονται, καθώς και των επιπτώσεων σε περιπτώσεις περιστατικών. Η διεθνής εμπειρία αναδεικνύει συνεχώς τη σημασία της συνεργασίας και της ανταλλαγής εμπειριών και πληροφοριών σε όλα τα επίπεδα. Η ανταλλαγή πληροφοριών καθίσταται πολύτιμο και αναντικατάστατο εργαλείο νοουμένου ότι γίνεται με σωστό και δομημένο τρόπο, στα πλαίσια συνεργασίας και αμοιβαίας εμπιστοσύνης:

- **Μεταξύ οργανισμών στον ίδιο τομέα (sector, π.χ. ενέργεια, μεταφορές, κλπ)**
  - Πολλές από τις στοχευμένες επιθέσεις που παρατηρούνται στον κυβερνοχώρο έχουν συνήθως ως στόχους οργανισμούς στον ίδιο τομέα, π.χ. τράπεζες. Όταν παρατηρούνται επιθέσεις εντός Κύπρου σε ένα τομέα, ενδιαφέρει άμεσα τους υπόλοιπους οργανισμούς στον ίδιο τομέα για πιο αποτελεσματική προστασία.
- **Μεταξύ οργανισμών σε διάφορους τομείς και ΑΨΑ / Εθνικό CSIRT**
  - Η συγκέντρωση πληροφοριών για απειλές και επιθέσεις κεντρικά, θα βοηθήσει όλους τους εμπλεκόμενους οργανισμούς στην αντιμετώπιση τέτοιων απειλών, καθώς και για αποτελεσματική διαχείριση κρίσεων στον κυβερνοχώρο. Εννοείται ότι αυτού του είδους ανταλλαγή πληροφοριών θα είναι αμφίδρομη, και προς όφελος όλων των εμπλεκομένων.
- **Μεταξύ κρατών-μελών της ΕΕ και άλλων κρατών όπου χρειάζεται**
  - Η διεθνής συνεργασία (βλ. θεματική ενότητα 3.14 – Διεθνής Συνεργασία), προϋποθέτει την αποτελεσματική ανταλλαγή πληροφοριών, για διαχείριση συμβάντων και κρίσεων που έχουν αντίκτυπο πέραν της μίας χώρας. Οποιαδήποτε ανταλλαγή θα πρέπει να γίνεται με γνώμονα την ανωνυμία και την προστασία ευαίσθητων πληροφοριών, αναλόγως της περίπτωσης.

Πέραν από την ανταλλαγή πληροφοριών όσο αφορά απειλές και συμβάντα στον κυβερνοχώρο, θα πρέπει να προάγεται και η έγκαιρη πληροφόρηση όσο αφορά ευπάθειας (vulnerabilities) σε συστήματα που προσφέρονται από την Κυπριακή αγορά, σε συντονισμό με εταιρείες και πελάτες (coordinated vulnerability disclosure).

Θα εξερευνηθεί η πιο κατάλληλη μορφή συνεργασίας για εδραίωση της ανταλλαγής πληροφοριών μεταξύ των εμπλεκομένων, και μια πιθανή μορφή είναι αυτή της σύμπραξης δημόσιου-ιδιωτικού τομέα (public-private partnership). Είναι σημαντικό να κατανοηθεί ότι υπάρχει αμοιβαίο όφελος σε τέτοιου είδους συνεργασία. Υπενθυμίζεται ότι ως επί το πλείστον, ο ιδιωτικός τομέας (συμπεριλαμβανομένου των ημικρατικών οργανισμών) χειρίζεται μεγάλο μέρος των κρίσιμων υποδομών στην Κύπρο.

3.8.2. Επίγνωση Κατάστασης (Situational Awareness)

Ο όρος 'επίγνωση / κατανόηση κατάστασης (situational awareness)', σε σχέση με την κυβερνοασφάλεια, αναφέρεται σε διάφορα επίπεδα γνώσης / κατανόησης για την εκάστοτε κατάσταση απειλών (δηλαδή σε σχέση με τις απειλές που αφορούν τα οικία συστήματα και τις τυχόν επιθέσεις που είναι δυνατόν να εκδηλωθούν εναντίων των οικείων συστημάτων). Επίσης αναφέρεται στις ικανότητες αντιμετώπισης συμβάντων από τους διάφορους εμπλεκομένους φορείς, στις σχετιζόμενες επιθέσεις που είναι δυνατόν να εκδηλώνονται σε άλλες χώρες, στις ευπάθειες των συστημάτων, ως επίσης και στο επίπεδο υλοποίησης τεχνικών και οργανωτικών μέτρων (κυρίως στις κρίσιμες υποδομές πληροφοριών) κατάλληλων ως προς το επίπεδο κινδύνου.

Η συνεχής και λεπτομερής αποτύπωση της κατάστασης κυβερνοασφάλειας σε εθνικό επίπεδο, απαιτεί στενή συνεργασία μεταξύ των εμπλεκομένων αρμοδίων αρχών του δημοσίου τομέα, όπως την Αρχή Ψηφιακής Ασφάλειας, το Εθνικό CSIRT, την Αστυνομία, την Εθνική Φρουρά (αν χρειάζεται), τις υπηρεσίες πληροφοριών, άλλα CSIRT, άλλες αρμόδιες αρχές (βλ. ενότητα 2.3) κλπ. Σε κάθε περίπτωση χρειάζεται η συμβολή των κρίσιμων υποδομών πληροφοριών, αναλόγως της κατάστασης. Η συλλογή και η επεξεργασία πληροφοριών σε κεντρικό επίπεδο (στην ΑΨΑ), και η μετέπειτα διάχυση τους σε όποια σημεία κρίνεται αναγκαίο, θα βελτιστοποιήσει το όφελος που θα προκύψει από την υλοποίηση των σχετικών δράσεων.

Η εν λόγω δραστηριότητα συνδέεται άμεσα με τη διαχείριση εθνικών κινδύνων (βλ. θεματική ενότητα 3.5 - Αξιολόγηση και Διαχείριση Κινδύνων – Αξιολόγηση Κρισιμότητας), αν και τα αποτελέσματα της θα είναι πιο άμεσα και θα αποτυπώνουν την κατάσταση ανά πάσα στιγμή (real time situational awareness). Απαραίτητη προϋπόθεση είναι η δημιουργία αποδοτικού μηχανισμού ανταλλαγής πληροφοριών, χωρίς την υλοποίηση της οποίας θα είναι δύσκολη η επιτυχία της της παρούσας δραστηριότητα. Η επιτυχής εφαρμογή της δράσης 13, θα βοηθήσει τις αρμόδιες αρχές να πετύχουν καλύτερα επίπεδα ετοιμότητας για αντιμετώπιση συμβάντων και κρίσεων στον κυβερνοχώρο, με συνεπαγόμενη μείωση των ανεπιθύμητων επιπτώσεων στην Κυπριακή Δημοκρατία.

Δράσεις:

Δράση 12 - (α) 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 (συμπεριλαμβανομένων: Information Sharing Analysis Centers - ISACs).
(β) Προώθηση της δημιουργίας ενός δυναμικού PPP στον τομέα της ανταλλαγής πληροφοριών, με τη συνδρομή όλων των εμπλεκόμενων φορέων κρίσιμων υποδομών πληροφοριών και των αρμοδίων αρχών του κράτους.

Δράση 13 - Ανάπτυξη ολιστικού μηχανισμού επίγνωσης της κατάστασης (situational awareness), για την ανταλλαγή πληροφοριών και την συνεργασία σε πραγματικό χρόνο (real time), με τη συμβολή όλων των εμπλεκομένων φορέων, συμπεριλαμβανομένων όλων των αρμοδίων αρχών στους τομείς της κυβερνοασφάλειας, του κυβερνοεγκλήματος, της κυβερνοάμυνας και της διεθνούς συνεργασίας σε συναφή θέματα, και με κεντρική συλλογή, επεξεργασία και παρουσίαση πληροφοριών, για αύξηση των επιπέδων ετοιμότητας για αντιμετώπιση συμβάντων και κρίσεων στον κυβερνοχώρο.

3.9. Θεματική ενότητα 9 – Ενημέρωση – Δημιουργία Κουλτούρας Ασφάλειας

Στρατηγικοί στόχοι: Εκπαίδευση, Κατάρτιση και Επίγνωση, Συνεργασία, Ανάπτυξη Δυνατοτήτων

Το εύρος των πιθανών απειλών και των κινδύνων από τον κυβερνοχώρο, όπως αναφέρεται στην ενότητα 2.3, θα πρέπει πλέον να απασχολεί **όλους** τους χρήστες μηχανογραφικών και επικοινωνιακών υποδομών, δικτύων, αλλά και τερματικών συσκευών που χρησιμοποιούνται, σχεδόν από το σύνολο των πολιτών της Κυπριακής Δημοκρατίας, οι πλείστοι των οποίων κάνουν πλέον τακτική χρήση του Διαδικτύου.

Είναι πολύ σημαντικό οι χρήστες του Διαδικτύου, καθώς επίσης και οι χρήστες μηχανογραφικών και επικοινωνιακών συστημάτων, σε κάθε χώρο εργασίας, να ενημερώνονται και να έχουν ένα ικανοποιητικό επίπεδο γνώσεων για τις πιθανές απειλές κυβερνοασφάλειας από τις οποίες πρέπει να προφυλάσσονται.

Οι αρμόδιες αρχές στην Κυπριακή Δημοκρατία θα πρέπει να αξιοποιήσουν και να διευρύνουν τα υφιστάμενα προγράμματα ενημέρωσης που υλοποιούνται σήμερα στην Κύπρο, τις βέλτιστες πρακτικές αντιμετώπισης των προκλήσεων από τον κυβερνοχώρο, καθώς και τις δραστηριότητες που προωθούνται βάση της υφιστάμενης Στρατηγικής Κυβερνοασφάλειας και συγκεκριμένα του εγκεκριμένου από το Υπουργικό Συμβούλιο Εθνικού Προγράμματος Ενημέρωσης για τα θέματα κυβερνοασφάλειας (για παιδιά, γονείς εκπαιδευτικούς και γενικά την κοινωνία) . Το διευρυμένο πρόγραμμα ενημέρωση θα περιέχει (τουλάχιστο) τα ακόλουθα:

- Δημιουργία πληροφοριακού υλικού, καθώς και χρήση διαθέσιμου υλικού από εξωτερικές πηγές (π.χ. ENISA, Safer Internet for Kids κλπ.), για το σύνολο των πολιτών για τα θέματα ασφαλούς χρήσης του Διαδικτύου, με στην προστασία προσωπικών δεδομένων, σωστή συμπεριφορά στον κυβερνοχώρο και στην προστασία των παιδιών στο Διαδίκτυο,
- Διανομή του εν λόγω πληροφοριακού υλικού με την αξιοποίηση πολλαπλών μέσων, π.χ. τηλεόραση, ραδιόφωνο, SMS, ιστοσελίδες, φυλλάδια/βιβλιαράκια, διαλέξεις, μέσα κοινωνικής δικτύωσης κλπ.
- Δημιουργία εκπαιδευτικών σεμιναρίων μικρής διάρκειας με στόχο τους εργαζόμενους,
- Δημιουργία εξειδικευμένων σεμιναρίων για δημόσιους υπαλλήλους και χρήστες κυβερνητικών συστημάτων πληροφοριών που εμπεριέχουν ευαίσθητα δεδομένα,
- Προώθηση της ανάπτυξης ‘κουλτούρας ασφάλειας’ σε όλα τα κυβερνητικά τμήματα και υπηρεσίες του κράτους, καθώς και σε ιδιωτικές επιχειρήσεις.

Ως μέρος της υλοποίησης της σχετικής αντίστοιχης Δράσης στην προηγούμενη Στρατηγική, για την ανάπτυξη κουλτούρας ασφάλειας, προωθήθηκε η ανάπτυξη και η έγκριση από το Υπουργικό Συμβούλιο, της στρατηγικής για την ασφαλή χρήση του διαδικτύου για παιδιά, γονείς και εκπαιδευτικούς[15]. Η στρατηγική καλύπτει ένα ευρύ φάσμα θεμάτων με βασικό στόχο την δημιουργική και ασφαλή αξιοποίηση του Διαδικτύου και των νέων τεχνολογιών. Προωθεί την ανάπτυξη γνώσεων και δεξιοτήτων για την αξιοποίηση των δυνατότητων του Διαδικτύου και των νέων τεχνολογικών καθώς και τους τρόπους αντιμετώπισής των προκλήσεων που προκύπτουν από την χρήση τους. Συγκεκριμένα προωθεί την καλλιέργεια κουλτούρας ασφάλειας, και την ανάπτυξη και εφαρμογή οριζόντιων δεξιοτήτων - όπως την κριτική διαχείριση των πληροφοριών, την υπεύθυνη κοινωνική συμπεριφορά, την αυτόνομη μάθηση, επικοινωνία και συνεργασία και επίλυση προβλημάτων. Η στρατηγική περιλαμβάνει δράσεις που αφορούν τα παιδιά, αλλά και εκπαιδευτικούς, γονείς καθώς και το ευρύτερο κοινό, και οι οποίες στοχεύουν στη καθιέρωση κουλτούρας για την δημιουργική αξιοποίηση του διαδικτύου με ασφάλεια και υπευθυνότητα για ένα καλύτερο διαδίκτυο για τα παιδιά και την κοινωνία ευρύτερα.

Μια από τις δράσεις που προκύπτουν από την εν λόγω στρατηγική, αφορά στη δημιουργία ενός «κέντρου» (φυσικού χώρου αλλά και δικτύου συνεργασίας) που να προωθεί την ασφαλή αξιοποίηση των ψηφιακών τεχνολογιών και ειδικά του Διαδικτύου. Η δημιουργία ενός τέτοιου κέντρου θα έχει μεγάλη επίδραση στην επιτυχή εκπλήρωση του σκοπού και των στόχων της παρούσας Στρατηγικής Κυβερνοασφάλειας, και ειδικότερα μπορεί να αποτελέσει ένα πολύ σημαντικό εργαλείο για την ανάπτυξη κουλτούρας ασφάλειας και επίγνωσης στα θέματα κυβερνοασφάλειας. Η δραστηριότητα αυτή προέκυψε τόσο από τις εισηγήσεις των εμπλεκόμενων φορέων όσο και από τη ανάλυση των αναγκών, των απόψεων και των εισηγήσεων τόσο των παιδιών, των εκπαιδευτικούς και των γονέων όσο και του συνόλου της Κυπριακής κοινωνίας. Για τη δημιουργία του κέντρου αναπτύχθηκε συγκεκριμένη πρόταση που εγκρίθηκε από το Υπουργικό Συμβούλιο ενώ προωθείται ειδικότερη τεχνοοικονομική μελέτη που θα επιτρέψει την πρακτική υλοποίηση του «κέντρου». Το «κέντρο» προβλέπεται να αξιοποιηθεί και από διάφορες κρατικές υπηρεσίες και θεσμούς της Κυπριακής κοινωνίας. Το «κέντρο» θα διαδραματίζει επίσης σημαντικό ρόλο σε θέματα εκπαίδευσης και κατάρτισης που αναφέρονται στη θεματική ενότητας 10, καθώς και σε θέματα έρευνας και καινοτομίας στα θέματα κυβερνοασφάλειας και χρήσης των νέων τεχνολογιών που αναφέρονται στην θεματική ενότητα 11 - Έρευνα και Καινοτομία και θεματική ενότητα 12- Συνεργασία με τον Ιδιωτικό Τομέα .

Εντός της παρούσας Δράσης, θα δοθεί έμφαση και θα στηριχθεί η υλοποίηση της ειδικής στρατηγικής για τα παιδιά, γονείς και εκπαιδευτικούς, συμπεριλαμβανομένης της δημιουργίας και λειτουργίας του προαναφερόμενου κέντρου.

Γενικότερα η διαμόρφωση του κατάλληλου γνωσιολογικού επιπέδου στην Κυπριακή Δημοκρατία, σε συνδυασμό με την δημιουργία εξειδικευμένου ανθρώπινου δυναμικού για θέσεις-κλειδιά στον τομέα, μακροπρόθεσμα θα συνδράμει σημαντικά στην διασφάλιση των συστημάτων πληροφορικής που είναι συνδεδεμένα στον κυβερνοχώρο.

[15] https://www.esafecyprus.ac.cy/ethniki-stratigiki

Δράση:

Δράση 14 - Προώθηση και ολοκλήρωση του Εθνικού Προγράμματος Ενημέρωσης (Awareness) για τα θέματα κυβερνοασφάλειας που θα καλύπτει όλους τους χρήστες ηλεκτρονικών συστημάτων, από κυβερνητικούς και ιδιωτικούς υπάλληλους, καθώς και το κοινωνικό σύνολο.
(α) Η ανάπτυξη του ολοκληρωμένου Προγράμματος θα γίνει σε συνεργασία με όλους τους εμπλεκόμενους φορείς και τα ενδιαφερόμενα μέρη σχετικά με τα θέματα της κυβερνοασφάλειας, με στόχο την πλήρη κατανόηση των αναγκών και την συνεχή βελτίωση των επιπέδων επίγνωσης και της κουλτούρας ασφάλειας όσο αφορά τον κυβερνοχώρο. Το πρόγραμμα θα περιλαμβάνει εκστρατείες ευαισθητοποίησης που θα στοχεύουν, σε στελέχη επιχειρήσεων και το ευρύ κοινό.
(β) Θα προωθηθεί επίσης εφαρμογή της στρατηγικής για τα παιδιά, γονείς και εκπαιδευτικούς καθώς και η δημιουργία και λειτουργία του «κέντρου» για την ασφαλή αξιοποίηση ψηφιακών τεχνολογιών και του Διαδικτύου, να στόχο την αξιοποίηση του σε εθνικό αλλά και περιφερειακό και ευρωπαϊκό επίπεδο. Συντονιστής της συγκεκριμένης δράσης είναι το Παιδαγωγικό Ινστιτούτο Κύπρου εκ μέρους του Υπουργείου Παιδείας και Πολιτισμού.

3.10. Θεματική ενότητα 10 – Εκπαίδευση και Κατάρτιση

Στρατηγικοί στόχοι: Ανάπτυξη Δυνατοτήτων, Εκπαίδευση, Κατάρτιση και Επίγνωση, Συνεργασία

Η παρούσα θεματική ενότητα εστιάζεται στις δραστηριότητες που σχετίζονται με την προώθηση της δημιουργίας ικανοτήτων κυβερνοασφάλειας μέσω της εκπαίδευσης και της κατάρτισης προσωπικού κυβερνητικών φορέων, επιχειρήσεων και άλλων οργανισμών - που είναι ζωτικής σημασίας για το κράτος και για να καταστεί δυνατή η ανάπτυξη της ψηφιακής οικονομία της χώρας. Η παρούσα θεματική ενότητα συνδέεται και επεκτείνει τους στόχους της θεματικής ενότητας 9 πέραν από τα θέματα ενημέρωσης στα θέματα πιο εξειδικευμένης εκπαίδευσης και κατάρτισης. Συνδέεται επίσης με τα θέματα ανάπτυξης ικανοτήτων της θεματικής ενότητας 7 - Ανάπτυξη Δυνατοτήτων – Διοργάνωση και Συμμετοχή σε Ασκήσεις, καθώς και με τα θέματα έρευνας και καινοτομίας της θεματικής ενότητας 11 - Έρευνα και Καινοτομία.

Σε σχέση με την παρούσα θεματική ενότητα η στρατηγική έχει ως στόχο να διευκολύνει την ανάπτυξη προγραμμάτων σπουδών ώστε να επιταχυνθεί η ανάπτυξη των δεξιοτήτων κυβερνοασφάλειας σε όλο φάσμα του εκπαιδευτικού συστήματος. Αυτό περιλαμβάνει την ανάπτυξη εξειδικευμένων προγραμμάτων εκμάθησης και σπουδών στα σχολεία πρωτοβάθμιας, δευτεροβάθμιας εκπαίδευσης ενσωματώνοντας σχετική ύλη για θέματα κυβερνοασφαλειας σε όλα τα προγράμματα πληροφορικής και τεχνολογίας. Περιλαμβάνει επίσης την προώθηση και ενίσχυση των σχετικών προγραμμάτων, στην τριτοβάθμιας εκπαίδευση και τη δημιουργία ειδικών προπτυχιακών και μεταπτυχιακών προγραμμάτων σε θέματα κυβερνοασφάλειας.

Η κατάλληλη κατάρτιση και η ανάπτυξη ικανοτήτων στον τομέα της κυβερνοασφάλειας είναι απαραίτητη προϋπόθεση για την ομαλή λειτουργία των συστημάτων ασφάλειας πληροφοριών, καθώς

επίσης και για να είναι εφικτή η σωστή υλοποίηση οποιωνδήποτε δράσεων σχετικά με το θέμα. Είναι πλέον γεγονός ότι, σε παγκόσμιο επίπεδο, υπάρχει μεγάλη έλλειψη κατάλληλα εκπαιδευμένων επαγγελματιών σε θέματα κυβερνοασφάλειας.

Η ανάπτυξη των σχετικών ικανοτήτων είναι μείζονος σημασίας και βασικός στόχος της Στρατηγικής είναι η δημιουργία κατάλληλα καταρτισμένου ανθρώπινου δυναμικού, τόσο στον δημοσίο όσο και στον ιδιωτικό τομέα, που θα έχει την απαραίτητη τεχνική γνώση και εμπειρία για να υλοποιήσει τις πρόνοιες της Στρατηγικής, αλλά και για να συμβάλει στη μεγιστοποίηση των επιπέδων κυβερνοασφάλειας στην Κύπρο.

Ως εκ τούτου, το κράτος θα πρέπει να υποστηρίζει συνεχώς την κατάλληλη εκπαίδευση προσωπικού στο ευρύ φάσμα των θεμάτων κυβερνοασφάλειας μέσω, μεταξύ άλλων, των πιο κάτω ενεργειών:

- Εντοπισμός κατάλληλων και διαθέσιμων εκπαιδευτικών προγραμμάτων και προώθηση πιστοποιήσεων, (εθνικής και διεθνής πιστοποίησης) για τους επαγγελματίες ασφαλείας, βάσει των αναγκών που έχουν εντοπιστεί από την κυβέρνηση και τη βιομηχανία,
- Προώθηση και αξιοποίηση των προγραμμάτων κατάρτισης εντός του κράτους, η τεχνική κατάρτιση θα πρέπει να συμπληρώνεται με πρωτοβουλίες επικεντρωμένες στη διαχείριση του κινδύνου
- Δημιουργία κατάλληλα καταρτισμένου ανθρώπινου δυναμικού με τις απαραίτητες εξειδικευμένες γνώσεις, μέσω της ανάπτυξης προγραμμάτων κατάρτισης στον τομέα της ασφάλειας στον κυβερνοχώρο και ανάπτυξης δεξιοτήτων για εμπειρογνώμονες και μη ειδικούς τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα.
- Ενσωμάτωση σχετικών πιστοποιήσεων και πείρας σε σχέδια υπηρεσίας του δημόσιου τομέα που έχουν σχέση με την κυβερνοασφάλειας, και την διασφάλιση προοπτικών ανέλιξης στο προσωπικό του δημόσιου τομέα που εξειδικεύεται στα θέματα κυβερνοασφάλειας
- Προώθηση σχολικών προγραμμάτων τα οποία να ευαισθητοποιήσουν και να ενθαρρύνουν το ενδιαφέρον των μαθητών στα θέματα ασφάλειας δικτύων και πληροφοριών και να τους ενημερώνουν για τις ευκαιρίες σταδιοδρομίας στα θέματα κυβερνοασφάλειας.
- Αξιολόγηση από το κράτος του ενδεχομένου δημιουργίας διαφόρων προγραμμάτων παροχής κινήτρων, όπως υποτροφίες ή και επιχορηγήσεις για ιδιωτικά προγράμματα εκπαίδευσης, καθώς και κινήτρων προς τα ακαδημαϊκά ιδρύματα για την αύξηση του αριθμού αποφοίτων καταρτισμένων σε θέματα κυβερνοασφάλειας
- Προώθηση και στήριξη της δραστηριοποίησης των σχολών ανώτερης και ανώτατης εκπαίδευσης στον Κυπριακό χώρο στον τομέα της ασφάλειας δικτύων και πληροφοριών και της κυβερνοασφάλειας, μέσω της ενσωμάτωσης σχετικών θεμάτων στα προγράμματα τους.
- Αντιμετώπιση του χάσματος μεταξύ των φύλων στην εκπαίδευση και κατάρτιση εμπειρογνωμόνων στον τομέα της κυβερνοασφάλειας, μέσω μιας ισορροπημένη προσέγγισης που να προωθεί, να ενθαρρύνει και να διευκολύνει την μεγαλύτερη εμπλοκή των γυναικών σε όλες τις προσπάθειες που αποσκοπούν στην ανάπτυξη δεξιοτήτων σε θέματα κυβερνοασφάλειας,
- Αξιοποίηση των συνεργιών που θα δημιουργηθούν με την ίδρυση και λειτουργία του «κέντρου» για την ασφαλή αξιοποίηση των ψηφιακών τεχνολογιών και ειδικά του Διαδικτύου που αναφέρεται στη θεματική ενότητα 9 Ενημέρωση – Δημιουργία Κουλτούρας Ασφάλειας και στη Δράση 14(β).

Τονίζεται ότι η έμφαση σε αυτή τη Δράση είναι στην εκπαίδευση επαγγελματιών στον τομέα κυβερνοασφάλειας και όχι στην ενημέρωση του κοινού (βλ. Θεματική ενότητα 3.9 Ενημέρωση – Δημιουργία Κουλτούρας Ασφάλειας).

Δράση:

Δράση 15 - 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, και ενσωμάτωση των γνώσεων αυτών στα σχέδια υπηρεσίας για σχετικές θέσεις εργασίας.
Προώθηση ενεργειών για την κατάλληλη εκπαίδευση και κατάρτιση προσωπικού όπως αυτές καταγράφονται στη παρούσα θεματική ενότητα 10.

3.11. Θεματική ενότητα 11– Έρευνα και Καινοτομία

Στρατηγικοί στόχοι: Έρευνα και Καινοτομία

Η ταχύτητα με την οποία εξελίσσεται το περιβάλλον του κυβερνοχώρου σήμερα, και κατ' επέκταση ο τομέας της κυβερνοασφάλειας, καταδεικνύει τη μεγάλη ανάγκη προώθησης υψηλού επιπέδου έρευνας στον σημαντικό αυτό τομέα, αλλά και της στήριξης πρωτοβουλιών στην παραγωγή καινοτομίας. Μια χώρα για να είναι σε θέση να αντιμετωπίσει, σε ικανοποιητικό βαθμό, τις ταχύτατα εξελισσόμενες απειλές από τον κυβερνοχώρο, θα πρέπει και να είναι σε θέση να αναπτύσσει συνεχώς τις δυνατότητες άμυνας της, και να φροντίζει ώστε οι τεχνολογίες και οι διαδικασίες να εξελίσσονται με τον ίδιο ρυθμό.

Σε ακαδημαϊκό επίπεδο είναι απαραίτητη η υποστήριξη και η συνεχής επικαιροποίηση των εκπαιδευτικών προγραμμάτων που προσφέρονται από ακαδημαϊκά ιδρύματα μέσω της διενέργειας υψηλού επιπέδου έρευνας. Επιπρόσθετα η δραστηριοποίηση σε ερευνητικές δραστηριότητες (όχι μόνο από ακαδημαϊκά ιδρύματα αλλά και από ερευνητικά ιδρύματα και εταιρείες που δραστηριοποιούνται στο χώρο), είναι δυνατόν να τύχει χρηματοδότησης από Ευρωπαϊκούς και Διεθνείς οργανισμούς και προγράμματα, με το ανάλογο όφελος στην εθνική οικονομία.

3.11.1. Προώθηση Έρευνας και Καινοτομίας – Αξιοποίηση Χρηματοδοτικών ευκαιριών

Στη παρούσα θεματική ενότητα η στρατηγική επιδιώκει να προωθήσει ένα περιβάλλον που να διεγείρει τη βασική και εφαρμοσμένη έρευνα σε θέματα κυβερνοασφάλειας μεταξύ των κρίσιμων τομέων και των διαφόρων ομάδων ενδιαφερομένων, ώστε να στηριχθούν οι στόχοι της στρατηγικής. Οι στόχοι της στρατηγικής στη παρούσα θεματική ενότητα εστιάζονται στην ανάπτυξη προγραμμάτων έρευνας και καινοτομίας σε θέματα κυβερνοασφάλειας τόσο σε κρατικούς όσο και σε ιδιωτικούς ερευνητικούς οργανισμούς και ακαδημαϊκά ιδρύματα, και στην αποτελεσματική διάδοση νέων ευρημάτων, τεχνολογιών, διαδικασιών και εργαλείων. Επιδιώκεται επίσης η δημιουργία δεσμών με τη διεθνή ερευνητική κοινότητα στους επιστημονικούς τομείς που σχετίζονται με την ασφάλεια στον κυβερνοχώρο, όπως μεταξύ άλλων, η επιστήμη των υπολογιστών, η τεχνίτη νοημοσύνη, η ηλεκτρονική μηχανική, τα εφαρμοσμένα μαθηματικά και η κρυπτογραφία, αλλά και σε μη τεχνικά πεδία όπως οι κοινωνικές και πολιτικές επιστήμες, η διοίκηση επιχειρήσεων και η ψυχολογία κλπ. Η στρατηγική προτρέπει στην αξιολόγηση μηχανισμών και στη παροχή κινήτρων μέσω επιχορηγήσεων, φορολογικών

ελαφρύνσεων, διαγωνισμών και άλλες πρωτοβουλιών που ενθαρρύνουν την ανάπτυξη καινοτόμων λύσεων, προϊόντων και υπηρεσιών σχετικά με την ασφάλεια στον κυβερνοχώρο.

Για την επίτευξη των στόχων της παρούσας Στρατηγικής, το κράτος έχει την βούληση να προωθήσει δυναμικά την έρευνα και την καινοτομία στον τομέα της κυβερνοασφάλειας, με κύριο στόχο την κάλυψη των αναγκών και την επίλυση προβλημάτων σε εθνικό επίπεδο αλλά και την στήριξη των Ευρωπαϊκών και διεθνών προσπαθειών για την ανάπτυξη του τομέα της Κυβερνοασφάλειας αλλά και την επαγγελματική και επιστημονική ανάπτυξη νέων επιστημόνων.

Η περαιτέρω προώθηση της έρευνας και καινοτομίας στον τομέα της Κυβερνοασφάλειας είναι δυνατόν να επιτευχθεί μέσω της συνεργασίας του ιδιωτικού αλλά και του δημόσιου τομέα με τα τοπικά αλλά και διεθνή ακαδημαϊκά και άλλα ερευνητικά ιδρύματα και οργανισμούς. Η συνεργασία αυτή θα πρέπει να σχεδιαστεί με γνώμονα την μεγιστοποίηση του οφέλους που μπορεί η Κύπρος να αποκομίσει αξιοποιώντας ενεργά τις διάφορες χρηματοδοτικές ευκαιρίες που υπάρχουν, τόσο σε εθνικό επίπεδο (π.χ. μέσω του νέου εθνικού κέντρου ενημέρωσης (awareness), και εκπαίδευσης – Center of Excellence) όσο και σε Ευρωπαϊκό επίπεδο (μέσω των χρηματοδοτικών προγραμμάτων όπως το CEF – Connecting Europe Facility, τον οργανισμό ECSO – European Cyber Security Organisation, τα προγράμματα H2020 – Horizon 2020 Programme, SME – Small and Medium Enterprise research and innovation support, κλπ.), αλλά και σε διεθνές επίπεδο στα πλαίσια συνεργασίας με διεθνείς οργανισμού όπως. μεταξύ άλλων, την Διεθνής Ένωση Τηλεπικοινωνιών (ITU – International Telecommunications Union) και ο Οργανισμός για την Ασφάλεια και Συνεργασία στη Ευρώπη (ΟΑΣΕ), καθώς και την προσέλκυση επενδύσεων.

Το κράτος θα υποστηρίξει τις προσπάθειες και τις πρωτοβουλίες από εταιρείες και ακαδημαϊκά και ερευνητικά ιδρύματα, στον μέγιστο δυνατό βαθμό. Όπου είναι δυνατόν, η Αρχή Ψηφιακής Ασφάλειας θα υποστηρίζει αλλά και θα λαμβάνει μέρος ενεργά σε συγχρηματοδοτούμενα έργα, και θα στηρίζει τις εγχώριες προσπάθειες για μεγιστοποίηση του οφέλους για την Κυπριακή κοινωνία και την αξιοποίηση των χρηματοδοτικών ευκαιριών προς όφελος των ενδιαφερομένων μερών και της οικονομίας.

3.11.2. Σχεδιασμός και Ανάπτυξη Οικοσυστημάτων

Ένας από τους βασικούς πυλώνες της παρούσας Στρατηγικής που σχετίζεται άμεσα με την προώθηση της έρευνας και της καινοτομίας, είναι ο σχεδιασμός, η ανάπτυξη και η δημιουργία οικοσυστημάτων κυβερνοασφάλειας. Οι συγκεκριμένες δραστηριότητες σε θέματα Κυβερνοασφάλειας προωθούνται για πρώτη φορά στην Κυπριακή Δημοκρατία. Η ανάπτυξη οικοσυστημάτων έχει ως κύριο στόχο να αξιοποιήσει τις συνέργειες που δημιουργούνται με την αξιοποίηση της δεσπόζουσας θέσης της Κύπρου σε τομείς όπως η εμπορική ναυτιλία ή και σε τομείς που η χώρα πρωτοπορεί ή παρουσιάζει αυξημένη δραστηριότητα, όπως στις οικονομικές υπηρεσίες ή και στην ενέργεια κλπ.

Η ανάπτυξη οικοσυστημάτων κυβερνοασφάλειας σε κρίσιμους τομείς της οικονομίας έχει ως κύριο στόχο την αναβάθμιση του προϊόντος της Κύπρου, συνδράμοντας σε περαιτέρω στην ανάπτυξη των εν λόγω τομέων και γενικότερα στην αναβάθμιση της κατάστασης της κυβερνοασφάλειας στην Κύπρο. Έχει επίσης ως στόχο την υποβοήθηση των Ευρωπαϊκών και διεθνών προσπαθειών ενίσχυσης της κυβερνοασφάλειας σε κρίσιμους τομείς διεθνούς ενδιαφέροντος.

Μια σημαντική πρωτοβουλία που προωθείται από την Αρχή Ψηφιακής Ασφάλειας και τυγχάνει της στήριξης των αρμοδίων αρχών του κράτους αφορά την δημιουργία του οικοσυστήματος “International Maritime Ecosystem for Cybersecurity”. Το Οικοσύστημα αφορά την παροχή υπηρεσιών Κυβερνοασφάλειας στον τομέα της Ναυτιλίας σε διεθνές επίπεδο. Πρόκειται για ένα έργο καινοτόμο και

με ιδιαίτερη σημασία στο πλαίσιο ανάπτυξης της διεθνούς και εθνικής ασφάλειας και της οικονομικής σταθερότητας. Το προτεινόμενο έργο αναμένεται να αναβαθμίσει τον στρατηγικό ρόλο της Κυπριακής Δημοκρατίας σε περιφερειακό επίπεδο, αξιοποιώντας τη θέση της Κύπρου στο χώρο της διεθνούς ναυτιλίας. Η 1η φάση του έργου αφορά τη διενέργεια μελετών στα πλαίσια πρότασης συγχρηματοδοτούμενου έργου που έχει υποβληθεί κάτω από το πρόγραμμα CEF Transport της Ευρωπαϊκής Επιτροπής. Η 2^{η} φάση του έργου θα εστιάζεται στην λειτουργία και ανάπτυξη του οικοσυστήματος με την εμπλοκή περισσοτέρων ενδιαφερομένων μερών, αρμοδίων αρχών, οργανισμών, παροχέων συστημάτων και υπηρεσιών, ναυτιλιακών εταιριών κλπ.

Γενικά, επενδύοντας στον σχεδιασμό, την λειτουργία και την ανάπτυξη οικοσυστημάτων κυβερνοασφάλειας το κράτος προσβλέπει στην καλύτερη αξιοποίηση των δυνατοτήτων του ακαδημαϊκού τομέα και των επιχειρήσεων, στην ανάπτυξη συνεργιών με εξειδικευμένες δραστηριότητες του κράτους και στην ανάπτυξη και εξειδίκευση των ικανοτήτων του εγχώριου ανθρώπινου δυναμικού σε κρίσιμους τομείς για την οικονομία και την κοινωνία. Οι συγκεκριμένες δραστηριότητες έχουν επίσης ως στόχο την προσέλκυση εταιρειών τεχνολογίας και κυβερνοασφάλειας και την δραστηριοποίηση τους στην Κύπρο, καθώς και την προώθηση ενεργειών για την σύσταση και δημιουργία καινοτόμων επιχειρήσεων στον τομέα.

Δράσεις:

Δράση 16 - Υποστήριξη και προώθηση της παραγωγής έρευνας και καινοτομίας στην Κυπριακή Δημοκρατία στον τομέα της κυβερνοασφάλειας. Οι ερευνητικές δραστηριότητες που θα προωθούνται θα πρέπει να έχουν άμεση σχέση με τις ανάγκες που εντοπίζονται εντός της Κύπρου αλλά και σε Ευρωπαϊκό και διεθνές επίπεδο και να μπορούν να υποστηρίξουν τους στόχους της παρούσας Στρατηγικής.

Δράση 17 - Αξιολόγηση και δημιουργία οικοσυστημάτων κυβερνοασφάλειας σε τομείς όπου η Κυπριακή Δημοκρατία πρωτοπορεί ή παρουσιάζει αυξημένη δραστηριότητα, όπως η εμπορική ναυτιλία, οι οικονομικές υπηρεσίες ή ενέργεια και σχετικές δραστηριότητες. Τα οικοσυστήματα θα κτιστούν πάνω στην εμπειρία μας ως χώρα στους τομείς αυτούς, με την υποστήριξη του δημόσιου τομέα, με την εμπλοκή ακαδημαϊκών ιδρυμάτων και του ιδιωτικού τομέα, και με στόχο την προσέλκυση εταιρειών και οργανισμών τεχνολογίας στην Κύπρο προς όφελος της οικονομίας, του κράτους και της κοινωνίας.

3.12. Θεματική ενότητα 12 – Συνεργασία με τον Ιδιωτικό Τομέα

Στρατηγικοί στόχοι: Συνεργασία, Κατανόηση κατάστασης, Εκπαίδευση, Κατάρτιση και Επίγνωση, Ανάπτυξη Ικανοτήτων

Δεδομένου ότι η κυβερνοασφάλεια αποτελεί σημαντική πρόκληση για την απρόσκοπτη και ασφαλή λειτουργία των κρίσιμων υποδομών της χώρας, πολλές από τις οποίες ανήκουν ή/και τυγχάνουν διαχείρισης από τον ιδιωτικό τομέα, η συνεργασία με τους εμπλεκόμενους οργανισμούς του ιδιωτικού τομέα αποτελεί αναγκαιότητα. Τέτοιες υποδομές εντοπίζονται μεταξύ άλλων στους τομείς της ενέργειας, των μεταφορών, της υγείας, της προμήθειας νερού, των τραπεζών και χρηματοπιστωτικών υπηρεσιών. Καθώς όλοι ξέρουμε ότι, η ασφάλεια και οι κίνδυνοι δεν είναι μόνο τεχνολογικοί, δεν αρκούν μόνο οι τεχνολογικές λύσεις για την προστασία των συστημάτων και των λειτουργιών των επιχειρήσεων και των οργανισμών. Θα πρέπει να διασφαλίζεται ότι υπάρχει επαρκείς επίγνωση των κινδύνων, καθώς και κατάρτιση και απόκτηση εξειδικευμένων γνώσεων από τα στελέχη όλων των οργανισμών. Η Αρχή Ψηφιακής Ασφάλειας θα συμβάλει ενεργά στη προσπάθεια κατάρτισης του εξειδικευμένου προσωπικού των οργανισμών σε θέματα κυβερνοασφάλειας.

3.12.1. Δημιουργία δικτύου εθνικών σημείων επαφής με τον ιδιωτικό τομέα

Στα πλαίσια υλοποίησης της Στρατηγικής το κράτος αντιλαμβάνεται και κατανοεί τις εξαρτήσεις που υπάρχουν με τις δραστηριότητες του ιδιωτικού τομέα, για την προώθηση και την ενίσχυση της ασφάλειας στον κυβερνοχώρο. Στόχος της στρατηγικής είναι να προσδιορίσει ένα δίκτυο έγκυρων εθνικών σημείων επαφής για τους κρίσιμους τομείς και κλάδους που είναι ουσιώδεις για τη λειτουργία και την αποκατάσταση των κρίσιμων υπηρεσιών και υποδομών. Οι ενέργειες αυτές συνδέονται και με τις δραστηριότητες της θεματικής ενότητας 1 για την δημιουργία Συμβουλευτικής Ομάδας Εμπλεκομένων (Stakeholder Advisory Group) , και της σύσταση Τομεακών Ομάδων Συνεργασίας (Sectoral Cooperation Groups). Στα πλαίσια των δομών που θα δημιουργηθούν, θα καθοριστεί ο ρόλος, η εμπλοκή, οι δεσμεύσεις και οι ευθύνες όλων των συμμετεχόντων από τον ιδιωτικό και τον δημόσιο τομέα.

Το δίκτυο εθνικών σημείων επαφής με τον ιδιωτικό τομέα θα λειτουργεί συμβουλευτικά προς τον Επίτροπο και την ΑΨΑ αλλά και την πολιτεία ευρύτερα. Μέσα από τη λειτουργία του δικτύου θα δίνεται η δυνατότητα κατάθεσης και συζήτησης απόψεων και εισηγήσεων για την καλύτερη εφαρμογή του ρυθμιστικού πλαισίου σε τομεακό και εθνικό επίπεδο, καθώς και την αξιολόγηση και την αντιμετώπιση ειδικότερων τομεακών θεμάτων. Θα λειτουργεί επίσης ως μέσο ανταλλαγής πληροφοριών και βέλτιστων πρακτικών σε τομεακό αλλά και εθνικό επίπεδο.

3.12.2. Δημιουργία επίσημης εταιρικής σχέσης δημόσιου-ιδιωτικού τομέα (PPP - Public Private Partnership)

Η στρατηγική ενθαρρύνει τη δημιουργία επίσημης εταιρικής σχέσης δημόσιου-ιδιωτικού τομέα (PPP) για την αύξηση της ασφάλειας των βασικών υπηρεσιών και των κρίσιμων υποδομών πληροφοριών. Οι εταιρικές σχέσεις δημόσιου-ιδιωτικού τομέα (PPP), αποτελούν το καλύτερο μέσο για την αποτελεσματική προστασία των κρίσιμων υποδομών και τη διαχείριση των κινδύνων ασφαλείας τόσο βραχυπρόθεσμα όσο και μακροπρόθεσμα. Είναι απαραίτητες για την ενίσχυση της εμπιστοσύνης μεταξύ τους και μεταξύ των επιχειρήσεων, της βιομηχανίας και της κυβέρνησης. Ωστόσο, η καθιέρωση βιώσιμων εταιρικών σχέσεων προϋποθέτει ότι όλοι οι συμμετέχοντες και οι ενδιαφερόμενοι έχουν μια σαφή αντίληψη των στόχων της εταιρικής σχέσης και των ωφελημάτων ασφαλείας που προκύπτουν από τη συνεργασία.

Στο πλαίσιο της συγκριμένης συνεργασίας του κράτους και του ιδιωτικού τομέα, θα προωθηθεί η σύσταση ενός PPP (Public Private Parnership) στον τομέα της προστασίας των κρίσιμων υποδομών πληροφοριών, το οποίο να:

- συνδράμει στην οικοδόμηση εμπιστοσύνης μεταξύ του κρατικού και του ιδιωτικού τομέα στα θέματα της ασφάλειας δικτύων και πληροφοριών,
- δημιουργήσει ένα ασφαλές πλαίσιο συνεργασίας για την επίτευξη κοινών στόχων στα θέματα κυβερνοασφάλειας,
- διευκολύνει την ανταλλαγή πληροφοριών σχετικά με νέες απειλές στον κυβερνοχώρο και λύσεις για την αποφυγή τους.
- στηρίζει πρωτοβουλίες για την δημιουργία Information Sharing Analysis Centers – ISACs, τα οποία αναφέρονται στην Θεματική ενότητα 8 και την Δραστηριότητα 12(α).
- να δημιουργεί αποτελεσματικές δομές συντονισμού και διαδικασιών και πρωτοκόλλων για την ανταλλαγή πληροφοριών (βλ. θεματική ενότητα 8 - Ανταλλαγή πληροφοριών), την οικοδόμηση εμπιστοσύνης, τον εντοπισμό σημείων βελτίωσης, και την ανταλλαγή ιδεών, προσεγγίσεων και βέλτιστων πρακτικών για την ενίσχυση της ασφάλειας (βλ. θεματική ενότητα 1 – Δομές και διακυβέρνηση), καθώς και τη βελτίωση του διεθνούς συντονισμού (βλ. θεματική ενότητα 14 - Διεθνής συνεργασία).

Δράση:

Δράση 18 - Οριζόντια δράση για την δημιουργία PPPs για την επίτευξη επιμέρους στόχων των ειδικών δράσεων όπως στην καινοτομία, την ενημέρωση, την εκπαίδευση και κατάρτιση κλπ αλλά και την επίτευξη ειδικότερων στόχων όπως, μεταξύ άλλων, τη δημιουργία πλατφόρμας για την ανταλλαγή τεχνικών (και άλλων, κατά περίπτωση) πληροφοριών μεταξύ της ΑΨΑ και όλων των εμπλεκομένων, για την βελτίωση των επιπέδων πληροφόρησης προς όλους και την ανάπτυξη περιβάλλοντος εμπιστοσύνης.
Θα εξεταστούν επίσης και άλλες μορφές συνεργασίας που θα μπορούσαν να ενταχθούν στην εν λόγω προσπάθεια, όπως π.χ. τη συμμετοχή σε κοινά συστήματα ή/και υπηρεσίες προστασίας από μεγάλες επιθέσεις (Distributed Denial of Service - DDoS), κλπ., την συμμέτοχή σε κοινά χρηματοδοτικά προγράμματα

3.13. Θεματική ενότητα 13 – Ασφάλεια για όλους (Security for All)

Θεματικές Ενότητες: Κατανόηση Κατάστασης, Διαχείριση Κινδύνων, Διαχείριση Περιστατικών, Εκπαίδευση, Κατάρτιση και Επίγνωση

Η στρατηγική, προσεγγίζει τα θέματα ασφάλειας στον Κυβερνοχώρο ολιστικά. Πέραν από την προστασία των Βασικών Υπηρεσιών των Κρίσιμων Υποδομών Πληροφοριών, τους παροχείς Ηλεκτρονικών Επικοινωνιών, το Κράτος και τα ενδιαφερόμενα μέρη από τον ιδιωτικό τομέα θα πρέπει να λαμβάνονται υπόψη και να στηρίζονται οι Μικρομεσαίες Επιχειρήσεις, 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.

Οι δραστηριότητες ευαισθητοποίησης και ενημέρωσης πρέπει πραγματοποιούνται σε συνεχή βάση και να χρησιμοποιούν ποικίλες μεθόδους παράδοσης για να προσεγγίσουν ευρύ κοινό, όπως αναλύεται στη Θεματική ενότητα 9 - Ενημέρωση και Δημιουργία Κουλτούρας Ασφάλειας. Επιπλέον όλοι οι εμπλεκόμενοι φορείς και αρμόδιες αρχές όπως η ΑΨΑ, το Εθνικό CSIRT, η υπηρεσία κυβερνοεγκλήματος της Αστυνομίας, το Παιδαγωγικό Ινστιτούτο ως ο συντονιστής της στρατηγικής για τη ασφάλεια των παιδιών στο διαδίκτυο, οι παροχείς υπηρεσιών διαδικτύου, αλλά και άλλα εμπλεκόμενα μέρη θα πρέπει να ενημερώνουν σε συνεχή βάση το κοινό για κινδύνους που εμφανίζονται και για μέτρα προφύλαξης από κακόβολες ενέργειες, κυρίως σε σχέση με υπηρεσίες διαδικτύου. Προς αυτό το σκοπό μπορούν να χρησιμοποιούνται ιστοσελίδες σχεδιασμένες για την παροχή πληροφοριών, υπηρεσίες παροχής στήριξης όπως η υπηρεσία 1480 (Cybersafety helpline και Hotline), τα μέσα κοινωνικής δικτύωσης, εφαρμογές σε υπολογιστές και έξυπνες φορητές συσκευές κλπ.

Πέραν από τα θέματα ενημέρωσης, εκπαίδευσης και κατάρτισης απώτερος στόχος της Στρατηγικής είναι η ευρύτερη στήριξη των πολιτών στην αντιμετώπιση περιστατικών κυβερνοασφάλειας με την ενεργή εμπλοκή του Εθνικού CSIRT. Η εφαρμογή δράσεων όπως η δημιουργία και λειτουργία υπηρεσίας υποστήριξης (help desk), που να στελεχώνεται για παράδειγμα με ειδικευόμενο προσωπικό ή/και φοιτητές θα μπορούσε να συνεισφέρει ποικιλοτρόπως στην στήριξη των πολιτών αλλά και στην κατάρτιση προσωπικού. Ένας σημαντικός μηχανισμός για την αναβάθμιση της κυβερνοασφάλειας αλλά και την ανάπτυξη της εμπιστοσύνης του κοινωνικού συνόλου, αποτελεί η πιστοποίηση προϊόντων και υπηρεσιών. Η παρούσα Στρατηγική επιδιώκει την προώθηση της εφαρμογής κατάλληλων σχημάτων πιστοποίησης όπως αυτή έχει εγκριθεί στον Κανονισμό της Ευρωπαϊκής Ένωσης Cybersecurity Act[16] (EU Cybersecurity Certification Framework). Μέσω των σχετικών δραστηριοτήτων και ενεργειών της Αρχής Ψηφιακής Ασφάλειας, ως η αρμόδια αρχή, θα πρέπει να δοθεί έμφαση στην πιστοποίηση προϊόντων και υπηρεσιών μέσω της συνεργασίας στο πλαίσιο των Ευρωπαϊκών μηχανισμών αλλά και τη δημιουργία των κατάλληλων εθνικών δομών.

3.13.1. Διαδίκτυο των πράγματων (Internet of Things - IoT)

Τα τελευταία χρόνια, το Διαδίκτυο συνδέει ένα τεράστιο αριθμό χρηστών αλλά και συνδεδεμένων συσκευών – πλέον υπάρχουν ψυγεία και άλλες οικιακές συσκευές, αυτοκίνητα, συσκευές υγείας, κάμερες κλειστού κυκλώματος, τηλέφωνα, θυροτηλέφωνα, μέχρι και λαμπτήρες, τα οποία έχουν τη δυνατότητα σύνδεσης στο Διαδίκτυο. Οι συνδεδεμένες συσκευές (Internet of Things - IoT), βρίσκονται πλέον στα περισσότερα σπίτια και αποτελούν μέρος της καθημερινής μας ζωής, χωρίς απαραίτητα την επαρκή να ενημέρωση και ευαισθητοποίηση των καταναλωτών για τους κινδύνους από κακόβουλες επιθέσεις μέσω των συσκευών αυτών. Τέτοιες συσκευές έχουν χρησιμοποιηθεί στο πρόσφατο παρελθόν για τη διενέργεια μεγάλων επιθέσεων (π.χ. Distributed Denial of Service – DDoS) έναντι διαφόρων στόχων ανά το παγκόσμιο.

Ταυτόχρονα, τα συστήματα ελέγχου και άλλες συσκευές που αποτελούν μέρος, κρίσιμων υποδομών της βιομηχανίας είναι πλέον συνδεδεμένα στις περισσότερες περιπτώσεις στο Διαδίκτυο. Αυτό γίνεται για ευκολία και ευελιξία στη χρήση και διαχείριση τέτοιων υποδομών. Λόγω των πιθανών ευπαθειών που

[16] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

παρουσιάζουν αρκετά από τα εν λόγω συστήματα, οι επιπτώσεις από τυχόν επιθέσεις, είναι σοβαρές και μπορούν να προκαλέσουν σοβαρές ζημιές, μέχρι και να θέσουν σε κίνδυνο ανθρώπινες ζωές.

Τα συγκεκριμένα συστήματα και συσκευές (IoT), μπορούν να κατηγοριοποιηθούν σε τέσσερεις κατηγορίες:

1. Η συσκευή δεν περιλαμβάνει οποιεσδήποτε πρόνοιες ασφάλειας, συνήθως λόγω μικρού μεγέθους και ελάχιστες δυνατότητες για λειτουργίες πέραν των βασικών λειτουργιών της. Επίσης, οι συσκευές συνήθως εξακολουθούν να έχουν την βασική παραμετροποίηση που τους δόθηκε κατά την κατασκευή τους (default insecure configuration).
2. Η συσκευή εξακολουθεί να μην περιλαμβάνει πρόνοιες ασφάλειας, αλλά η πρόσβαση προς και από τη συσκευή ελέγχεται από κάποια ενδιάμεση συσκευή (web service, gateway, κλπ.) η οποία μπορεί να προστατέψει τη συσκευή IoT σε ορισμένο βαθμό.
3. Η συσκευή περιλαμβάνει βασικές λειτουργίες ασφάλειας ανεξάρτητα, όπως για παράδειγμα ακεραιότητα και εμπιστευτικότητα επικοινωνίας.
4. Συσκευές στις οποίες ενσωματώνονται μέτρα ασφάλειας και προστασίας κατά την κατασκευή τους, στο επίπεδο που κρίνεται αναγκαίο.

Δυστυχώς, παρατηρείται ότι οι πλείστες συσκευές IoT, σε παγκόσμια βάση, παραμένουν στο πρώτο επίπεδο ασφάλειας, αν και καταβάλλονται αρκετές προσπάθειες από Κράτη, οργανισμούς ή αρμόδιους φορείς, για την αύξηση των επιπέδων ασφάλειας προς όφελος των χρηστών αλλά και άλλων συνδεδεμένων συστημάτων. Πέραν από τα προβλήματα που εντοπίζονται στο επίπεδο συσκευών, υπάρχουν και άλλες ευπάθειες που σχετίζονται με το σύνολο συσκευών IoT εντός ενός οργανισμού (ειδικά σε βιομηχανικά συστήματα), όπως για παράδειγμα ανεπαρκή φύλαξη βασικών κωδικών ασφαλείας, ενεργοποιημένη απομακρυσμένη πρόσβαση, συστήματα που δεν είναι ενημερωμένα (unpatched systems), μη-ασφαλή πρωτόκολλα, κλπ.

Στη παρούσα θεματική ενότητα αναμένεται να μελετηθούν τα θέματα που σχετίζονται με την ασφάλεια των συνδεδεμένων συσκευών στο διαδίκτυο (Internet of Things). Βασικός Στόχος είναι η παρακολούθηση της κατάστασης σε σχέση με προϊόντα που διατίθενται ή και χρησιμοποιούνται ευρέως στην Κυπριακή αγορά, και η έκδοση κατευθυντήριων γραμμών (guidelines) για τη σωστή χρήση τους και την λήψη μέτρων προφύλαξης από τους χρήστες. Τα αποτελέσματα των εργασιών της παρούσας δράσης θα μπορούσαν να τροφοδοτήσουν τις εργασίες για την βελτίωση του νομικού και ρυθμιστικού πλαισίου (βλ. θεματική ενότητα 3 – Νομικό και Ρυθμιστικό πλαίσιο) και για την βελτίωση των πολιτικών ασφαλείας που αξιολο9γούνται ή και καλύπτονται σε διάφορες άλλες δράσεις όπως η αξιολόγηση κινδύνων, το εθνικό πλαίσιο κυβερνοασφάλειας, η διαχείριση συμβάντων κλπ.).

Στη συνέχεια καταγράφονται κάποιες βασικές αρχές για την ασφάλεια των συσκευών και συστημάτων που συνδέονται στο διαδίκτυο, που ενδεχομένως θα ληφθούν υπόψη κατά την υλοποίηση της σχετικής Δράσης:

- ενσωμάτωση πρακτικών και λειτουργιών ασφάλειας στο στάδιο ανάπτυξης και παραγωγής των προϊόντων,
- ενσωμάτωση λειτουργιών για δυνατότητα ανάκτησης δικανικών (forensic) δεδομένων,
- ανταλλαγή πληροφοριών για την κατάσταση ασφάλειας διαφόρων συσκευών που διατίθενται στην αγορά (βλ. θεματική ενότητα 8 - Ανταλλαγή Πληροφοριών – Επίγνωση Κατάστασης),

- υποχρεώσεις για τη παροχή της δυνατότητας απομακρυσμένων ενημερώσεων ασφάλειας (remote security updates),
- προώθηση της ανάπτυξης εμπιστοσύνης και χρήσης προϊόντων τα οποία θα πιστοποιούνται με τα Ευρωπαϊκά σχήματα πιστοποίησης (βλ. EU Cybersecurity Certification Framework),
- αυθεντικοποίηση (authentication) συσκευών από τα δίκτυα στα οποία συνδέονται,
- υποχρεώσεις για ασφαλή παραμετροποίηση (system hardening) για συστήματα τα οποία πρέπει να έχουν απευθείας συνδέσεις σε βιομηχανικά συστήματα IoT,
- και άλλα μέτρα που θα αποφασιστούν κατά την υλοποίηση της παρούσας Δράσης.

3.13.2. Προστασία της ιδιωτικής ζωής και των δεδομένων

Η στρατηγική κυβερνοασφάλειας στοχεύει στη λήψη ισορροπημένων μέτρων για την ασφάλεια των υποδομών και των πληροφοριών έχοντας υπόψη την προστασία της ιδιωτικής ζωής κα των προσωπικών δεδομένων. Η εξισορρόπηση μεταξύ των δύο αποτελεί πρόκληση δεδομένου ότι κατά την εφαρμογή των δράσεων της Στρατηγικής πρέπει να λαμβάνεται σοβαρά υπόψη το δικαίωμα της ιδιωτικής ζωής των πολιτών. Η προστασία της ιδιωτικής ζωής αποτελεί οριζόντιο ζήτημα και σχετίζεται με τις περισσότερες από τις δραστηριότητες που αναφέρονται στην στρατηγική.

Στη παρούσα θεματική ενότητα ο κύριος στόχος της στρατηγικής είναι όπως στον καθορισμό των οποιανδήποτε μέτρων ή ενεργειών να λαμβάνονται υπόψη τόσο οι ανάγκες σε θέματα ασφάλειας όσο οι ασφαλιστικές δικλίδες για την προστασία της ιδιωτικής ζωής και των δεδομένων των πολιτών. Προς αυτό το σκοπό κατά τον πιο λεπτομερή σχεδιασμό των δράσεων θα πρέπει:

- να λαμβάνονται υπόψη οι ευρωπαϊκές και οι εθνικές νομικές απαιτήσεις για την προστασία των δεδομένων κατά τη σύνταξη σχετικών κανονιστικών κειμένων για την ασφάλεια στον κυβερνοχώρο.
- όπου χρειάζεται να γίνεται διαβούλευση με την αρμόδια αρχή για την προστασία των προσωπικών δεδομένών σχετικά με κανονιστικά κείμενα που σχετίζονται με την ασφάλεια στον κυβερνοχώρο.
- να εξετάζονται τα μέτρα συμμόρφωσης του νόμου προστασίας δεδομένων κατά τη διαβούλευση σε σχέση με τα ελάχιστα μέτρα ασφαλείας εκτός εάν αυτά αφορούν θέματα εθνικής ασφάλειας
- όπου κρίνεται απαραίτητο να υπάρχει συνεργασία μεταξύ της ΑΨΑ και της υπηρεσία της Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Δράσεις:

Δράση 19 - Μελέτη και παρακολούθηση της κατάστασης σχετικά με ευπάθειες, διορθώσεις και γενικά την ασφάλεια των συσκευών που συνδέονται στο διαδίκτυο και ενπίπτουν στη κατηγορία (IoT- Internet of Things), στην Κυπριακή Δημοκρατία, συμπεριλαμβανομένου των βιομηχανικών συστημάτων ελέγχου που βρίσκονται στις κρίσιμες βιομηχανικές υποδομές πληροφοριών, και τροφοδότηση της δράσης και την βελτιστοποίηση του νομικού και ρυθμιστικού πλαισίου.
Στον κατάλληλο χρόνο θα εκδίδονται κατευθυντήριες γραμμές για την ασφάλεια συσκευών και συστημάτων IoT προς οργανισμούς, εταιρείες και πολίτες, με την εισαγωγή

συγκεκριμένων υποχρεώσεων για φορείς που διαχειρίζονται κρίσιμες υποδομές πληροφοριών και στις οποίες λειτουργούν βιομηχανικά συστήματα ελέγχου.

Δράση 20 - Δημιουργία από την ΑΨΑ των εθνικών δομών πιστοποίησης σύμφωνα με τον Κανονισμό της Ευρωπαϊκής Ένωσης Cybersecurity Act.

3.14. Θεματική ενότητα 14 – Διεθνής Συνεργασία

<u>Στρατηγικοί στόχοι:</u> Συνεργασία, Διαχείριση περιστατικών και κρίσεων, Ανάπτυξη ικανοτήτων, Εκπαίδευση, κατάρτιση και επίγνωση

Η ασφάλεια στον κυβερνοχώρο διαδραματίζει όλο και περισσότερο ρόλο σε πολλούς διαφορετικούς τομείς των διεθνών σχέσεων, συμπεριλαμβανομένων των ανθρωπίνων δικαιωμάτων, της οικονομικής ανάπτυξης, του εμπορίου, του ελέγχου των εξοπλισμών, της ασφάλειας, της σταθερότητας, της ειρήνης και της επίλυσης των συγκρούσεων.

Η στρατηγική αναγνωρίζει ότι, τα θέματα της ασφάλειας στον κυβερνοχώρο δεν περιορίζονται στο εθνικό επίπεδο καθώς και την ανάγκη συνεργασίας με άλλα κράτη, οργανισμούς και διεθνείς παράγοντες. Τα προβλήματα και οι απειλές στον κυβερνοχώρο δε μπορούν να αντιμετωπιστούν επαρκώς από οποιαδήποτε χώρα μεμονωμένα. Οι διεθνείς δεσμεύσεις με τους δημόσιους και ιδιωτικούς φορείς είναι καθοριστικής σημασίας για τη διευκόλυνση ενός εποικοδομητικού διαλόγου, την ανάπτυξη μηχανισμών εμπιστοσύνης και συνεργασίας, την εξεύρεση αμοιβαία αποδεκτών λύσεων σε κοινές προκλήσεις και τη δημιουργία μιας παγκόσμιας κουλτούρας ασφάλειας στον κυβερνοχώρο.

Το κράτος αναγνωρίζει ότι τα θέματα διεθνούς συνεργασίας για την ασφάλεια στον κυβερνοχώρο αποτελούν αναπόσπαστο στοιχείο του εξωτερικής πολιτικής της χώρας. Για το σκοπό αυτό, η στρατηγική ενθαρρυνθεί την ανάπτυξη και χρήση δεξιοτήτων που εστιάζονται στα θέματα του κυβερνοχώρου (κυβερνο-διπλωματία), συμπληρωματικά προς τις παραδοσιακές μεθόδους και διαδικασίες διπλωματίας.

Στο πλαίσιο εφαρμογής της δράσης που προβλέπει η παρούσα θεματική ενότητα θα πρέπει να καθοριστούν οι μακροπρόθεσμοι στόχοι της διεθνούς συνεργασίας, προσδιορίζοντας τις εμπλεκόμενες αρμόδιες αρχές και οργανισμούς σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο.

Η Κυπριακή Δημοκρατία έχει τη βούληση να συμμετέχει και να υποστηρίξει μεταξύ άλλων τις εργασίες για τη θέσπιση διεθνών κανόνων για την ασφάλεια στον κυβερνοχώρο και μέτρα οικοδόμησης εμπιστοσύνης, την ανάπτυξη δυνατοτήτων στον κυβερνοχώρο, και την συμμετοχή στην ανάπτυξη διεθνών προτύπων στον τομέα της ασφάλειας στον κυβερνοχώρο. Η αποδοτική συμμετοχή της Κύπρου στα ευρωπαϊκά και διεθνή σώματα προϋποθέτει τον συντονισμό των διαφόρων αρμοδίων αρχών σε

εθνικό επίπεδο, ώστε οι θέσεις των εκπροσώπων της Κυπριακής Δημοκρατίας στα διάφορα σώματα να είναι εναρμονισμένες και να έχουν τύχει του κατάλληλου συντονισμού.

Όσον αφορά στην εξωτερική συνεργασία, κατά τον παρόντα χρόνο, η Κυπριακή Δημοκρατία, μέσω των σχετικών δραστηριοτήτων των διαφόρων αρμόδιων αρχών, εκπροσωπείται ήδη στα ευρωπαϊκά σώματα και στις σχετικές ομάδες εργασίας καθώς και σε διεθνή φόρα. Αναπόσπαστο μέρος της παρούσας Στρατηγικής είναι η συνεχείς και η εποικοδομητική εκπροσώπηση της Κυπριακής Δημοκρατίας στα ευρωπαϊκά και διεθνή σώματα, με στόχο την ενεργή συμμετοχή και την συμβολή της Κύπρου στις εργασίες και στις σημαντικές αποφάσεις των σωμάτων αυτών. Θα πρέπει να συνεχίσουν και να ενισχυθούν οι στενοί δεσμοί με τους αντίστοιχους αρμόδιους φορείς σε άλλα κράτη μέλη της Ευρωπαϊκής Ένωσης και διεθνών οργανισμών με στόχο την αξιοποίηση της διεθνούς συνεργασίας για την διαρκή ανάπτυξη και βελτίωση της στρατηγικής ανταπόκρισης της Κυπριακής Δημοκρατίας στα θέματα κυβερνοασφάλειας.

Ταυτόχρονα θα πρέπει να συνεχιστεί η συμμετοχή και η συνεργασία των αρμοδίων αρχών της Κυπριακής Δημοκρατίας στις Ευρωπαϊκές δράσεις οι οποίες αποσκοπούν στην βελτίωση της ηλεκτρονικής ασφάλειας Ευρωπαϊκών υποδομών πληροφοριών. Σημειώνεται ότι, η εμπιστευτικότητα πρέπει να λαμβάνεται υπόψη κατά τη συνεργασία και ανταλλαγή πληροφοριών και εμπειριών με διεθνείς φορείς και ομάδες εργασίας.

Δράση:

Δράση 21 - Θα ενισχυθούν οι διεπαφές και το πεδίο συνεργασίας με όλους τους εμπλεκόμενους εντός Κύπρου, πάντα με γνώμονα τη διαφάνεια και την επίτευξη κοινών στόχων για το όφελος ολόκληρης της χώρας. Επίσης, θα συνεχιστεί η καλή συνεργασία της Κυπριακής Δημοκρατίας με τα υπόλοιπα κράτη μέλη στην Ευρωπαϊκή Ένωση, αλλά και τρίτες χώρες, μέσω της εκπροσώπησης της και την ενεργή συμμετοχή στις σχετικές ομάδες εργασίας και φόρα. Η συνεργασία αυτή θα υποστηρίζει τις ενέργειες και δράσεις σε κοινοτικό επίπεδο για την βελτίωση της κυβερνοασφάλειας σε ολόκληρη την Ευρώπη αλλά και διεθνώς.

3.15. Θεματική ενότητα 15 – Αντιμετώπιση αδικημάτων στον Κυβερνοχώρο

<u>Στρατηγικοί στόχοι:</u> Συνεργασία, Μείωση και αποτελεσματική διερεύνηση αδικημάτων που διαπράττονται στον Κυβερνοχώρο, Ανάπτυξη ικανοτήτων, Εκπαίδευση, κατάρτιση και επίγνωση

Η ραγδαία ανάπτυξη της τεχνολογίας των πληροφοριών έχει καταστήσει δυνατή τη διάπραξη ενός ευρέως φάσματος ποινικών αδικημάτων με τη χρήση του διαδικτύου και των συστημάτων πληροφοριών και των άλλων ηλεκτρονικών μέσων, τα οποία απαιτούν εξειδικευμένη διερεύνηση εκ μέρους των Αρχών Επιβολής του Νόμου. Για το σκοπό αυτό από το 2007 έχει συσταθεί στα Αρχηγείο Αστυνομίας το Γραφείο Καταπολέμησης Ηλεκτρονικού Εγκλήματος και του Δικανικού Εργαστηρίου Ηλεκτρονικών Δεδομένων (ΓΚΗΕ & ΔΕΗΔ).

Οι προκλήσεις που αντιμετωπίζουν οι αρμόδιες αρχές είναι πολλές και πολυδιάστατες για την καταπολέμηση της παιδικής πορνογραφίας, της παράνομης πρόσβασης σε δεδομένα ηλεκτρονικού υπολογιστή, των ρατσιστικών σχολίων μέσω διαδικτύου, της οικονομικής απάτης, των εκβιασμών μέσω διαδικτύου, αλλά και άλλων αδικημάτων όπως αυτά ποινικοποιούνται από την εθνική μας νομοθεσία.

Η Κυπριακή Δημοκρατία έχει προχωρήσει στην κύρωση της Σύμβασης της Βουδαπέστης κατά του εγκλήματος μέσω του διαδικτύου, καθώς και στο Πρόσθετο Πρωτόκολλο για ενίσχυση της διεθνούς συνεργασίας και τη πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία. Ταυτόχρονα αναγνωρίζει την ανάγκη υιοθέτησης νομικών κανόνων για τη διατήρηση και απόκτηση ηλεκτρονικών αποδεικτικών στοιχείων στα πλαίσια ποινικών διαδικασιών, αλλά και την παρακολούθηση των εργασιών που πραγματοποιούνται σε ευρωπαϊκό επίπεδο.

Πέραν από το νομικό πλαίσιο, υπάρχει ανάγκη ανάπτυξης ικανοτήτων του προσωπικού αλλά και απόκτησης κατάλληλων μέσων για καταπολέμηση του κυβερνοεγκλήματος. Για επίτευξη αυτού του στόχου, το προσωπικό του ΓΚΗΕ μετέχει σε ετήσια βάση σε ειδικά προγράμματα εκπαίδευσης. Συνεπώς οι δράσεις θα πρέπει να λαμβάνουν υπόψη το εργασιακό περιβάλλον, την αναβάθμιση του χώρου εργασίας, των μέσων διερεύνησης του ΓΚΗΕ & ΔΕΗΔ, αλλά και τις εκπαιδεύσεις του προσωπικού.

Περαιτέρω, η στρατηγική λαμβάνει υπόψη ότι το ΓΚΗΕ & ΔΕΗΔ είναι μεταξύ άλλων υπηρεσιών, υπεύθυνο να ενημερώσει το κοινό για θέματα πρόληψης του κυβερνοαγκλήματος. Στο τομέα αυτό χρειάζεται στοχευμένη ενημέρωση όλων των οργανωμένων συνόλων, αλλά και εκπόνηση χρονοδιαγραμμάτων για τις προγραμματισμένες διαλέξεις που αναμένεται να πραγματοποιηθούν.

Επίσης, αναγνωρίζει ότι στο πλαίσιο της συνεργασίας, σε Εθνικό επίπεδο υπάρχει συνεργασία τόσο με τον δημόσιο όσο και με τον ιδιωτικό τομέα και σε Διεθνές επίπεδο υπάρχει συνεργασία με Interpol, FBI, Συμβούλιο της Ευρώπης, Europol, CEPOL, Eurojust, ENISA και ENJ. Παρόλο αυτά, θα πρέπει να επικεντρωθούν οι δράσεις στην περαιτέρω ενίσχυση της συνεργασίας τόσο με τον ιδιωτικό τομέα (παροχείς) κατά τη διερεύνηση ποινικών υποθέσεων, όσο και με την Eurojust κατά τη διερεύνηση διασυνοριακών κυβερνοεγκλημάτων.

Δράσεις:

Δράση 22 - Συνεχής παρακολούθηση και αξιολόγηση του νομικού πλαισίου για την διατήρηση και απόκτηση ηλεκτρονικών αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών σε εθνικό και Ευρωπαϊκό επίπεδο.

Δράση 23 - Ανάπτυξη ικανοτήτων του προσωπικού, με αναβάθμιση του χώρου εργασίας, των μέσων διερεύνησης καθώς και της εκπαίδευσης το προσωπικού.

Δράση 24 - Στοχευμένη ενημέρωση όλων των οργανωμένων συνόλων για σκοπούς πρόληψης των αδικημάτων που διαπράττονται στον κυβερνοχώρο.

Δράση 25 - Ενίσχυση της συνεργασίας μεταξύ του δημόσιου και ιδιωτικού τομέα κατά τη διερεύνηση ποινικών υποθέσεων, αλλά και της συνεργασίας σε διεθνές επίπεδο κατά τη διερεύνηση διασυνοριακών αδικημάτων που διαπράττονται στον κυβερνοχώρο.

4. Διαχείριση Στρατηγικής

Η Στρατηγική ανταπόκριση της Κυπριακής Δημοκρατίας στις προκλήσεις από τους κινδύνους και τις απειλές στον Κυβερνοχώρο επιτυγχάνεται εφόσον εφαρμόζονται με επιτυχία οι Δράσεις, προστατεύονται τα δίκτυα και οι πληροφορίες που χρησιμοποιούνται σε καθημερινή βάση, τυχόν περιστατικά ασφάλειας τυγχάνουν του ενδεδειγμένου χειρισμού και αντιμετωπίζεται το κυβερνοέγκλημα στον μέγιστο δυνατό βαθμό, για το σύνολο της Κυπριακής κοινωνίας.

4.1. Κεντρική Εποπτεία και Διαχείριση της Στρατηγικής

Για σκοπούς παρακολούθησης ελέγχου της υλοποίησης της Στρατηγικής, θα αναπτυχθεί ένα ολοκληρωμένο (και ενιαίο) Πλάνο Διαχείρισης Έργου (Program Management Plan), το οποίο θα αποτελεί ταυτόχρονα τον οδηγό για την υλοποίηση των Δράσεων για περίοδο περίπου τεσσάρων (4) ετών, και το μέσο για την διαχείριση της Στρατηγικής στο σύνολο της. Το έγγραφο αυτό θα καλύπτει μια σειρά από θέματα που αφορούν τη Στρατηγική , και θα συμπεριλαμβάνει (τουλάχιστο) τα ακόλουθα:

- Διεπαφές συνεργασίας και δραστηριοποίηση εμπλεκομένων (Stakeholder Engagement)
    - με δημιουργία τομεακών ομάδων συνεργασίας (sectoral cooperation groups), όπου κρίνεται αναγκαίο (βλ. ενότητα 3.1)
- Διαχείριση αλληλεξαρτήσεων μεταξύ Δράσεων (Interdependencies Management)
- Διαχείριση και βελτιστοποίηση οφέλους (Benefits Management)
- Δομημένη διαχείριση επικοινωνιών (Communications Management)
    - π.χ. τακτική επικοινωνία με τους εμπλεκομένους, διάχυση αποτελεσμάτων Στρατηγικής, ενημέρωση άλλων φορέων, κλπ.
- Δημιουργία δεικτών απόδοσης (Key Performance Indicators – KPIs) για μέτρηση των αποτελεσμάτων των Δράσεων
- Καταγραφή στόχων για το επιθυμητό επίπεδο κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, με αναφορά στο μοντέλο Cybersecurity Capacity Maturity Model for Nations[17] του Πανεπιστημίου της Οξφόρδης
- Διαχείριση Κινδύνων (Risk Management) για αναγνώριση και διαχείριση τυχόν κινδύνων και συνθηκών που θα μπορούσαν δυνητικά να επηρεάσουν αρνητικά τη διεκπεραίωση της Στρατηγικής και την επιτυχία των Δράσεων της
- Παρακολούθηση των αποτελεσμάτων των Δράσεων και καταγραφή τρόπων βελτίωσης για μελλοντικές Στρατηγικές – lessons learned
- Προώθηση της Στρατηγικής στο σύνολο της με γνώμονα τη συνεχή βελτίωση – continuous improvement.

Με στόχο την καλύτερη ανατροφοδότηση για την αποτελεσματική εφαρμογή της Στρατηγικής στην Κυπριακή Δημοκρατία, θα πραγματοποιείται ανά διετία αξιολόγηση ωριμότητας της Κυπριακής κοινωνίας σε θέματα Κυβερνοασφάλειας όπως για παράδειγμα το Cybersecurity Maturity Model που εφαρμόστηκε στην Κύπρο το καλοκαίρι του 2017. Το μοντέλο εφαρμόστηκε σε σχέση με αποτελέσματα

[17] https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0

στην εφαρμογή της πρώτης Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας με σκοπό την αναθεώρηση της στην παρούσα στρατηγική.

4.2. Διαχείριση Δράσεων

Η υλοποίηση των επιμέρους Δράσεων της Στρατηγικής αποτελεί περίπλοκο εγχείρημα, καθώς τα θέματα είναι πολυδιάστατα και απαιτείται η συμβολή αρκετών εμπλεκομένων. Οι προσπάθειες αυτές θα είναι πιο αποτελεσματικές με την υιοθέτηση αρχών και διαδικασιών για την διαχείριση των έργων (project management) που αφορούν την υλοποίηση της κάθε Δράσης, καθιστώντας την εφαρμογή της Στρατηγικής και όλες τις επιμέρους δραστηριότητες πιο αποτελεσματικές. Με την έναρξη υλοποίησης των Δράσεων της παρούσας Στρατηγικής **θα πρέπει να αναπτυχθούν προγράμματα εργασιών για την κάθε Δράση (όπου δεν υπάρχουν ήδη από την φάση υλοποίησης της προηγούμενης στρατηγικής), με σαφή χρονοδιαγράμματα, παραδοτέα, κοστολόγηση και εκτίμηση των απαραίτητων ανθρώπινων πόρων για την βελτιστοποίηση των αποτελεσμάτων.**

Ταυτόχρονα, αναγνωρίζεται ότι οι Δράσεις που περιλαμβάνονται στην παρούσα Στρατηγική παρουσιάζουν μεταξύ τους κοινά και αλληλεξαρτήσεις. Μια Δράση μπορεί να επηρεάζει ή να τροφοδοτεί αποτελέσματα μια άλλη. Επίσης υπάρχουν Δράσεις με κοινούς στόχους, ή που αφορούν τους ίδιους εμπλεκόμενους. Ως εκ τούτου, πρέπει να ακολουθηθεί μια δομημένη και ολιστική προσέγγιση όσον αφορά την υλοποίηση της Στρατηγικής στο σύνολο της, με γνώμονα την επίτευξη των βέλτιστων αποτελεσμάτων

Η κάθε Δράση όμως, για να υλοποιηθεί σωστά, θα πρέπει να αναλυθεί και να επεκταθεί λεπτομερώς, ώστε να εντοπιστούν όλες οι ενέργειες που πρέπει να γίνουν. Θα ακολουθήσει μια λεπτομερής ανάλυση και επέκταση της κάθε Δράσης της στρατηγικής ανταπόκρισης, μαζί με τον εντοπισμό των πόρων και διαδικασιών που θα χρειαστούν στα πλαίσια της υλοποίησης της.

Όπως αναφέρεται και στην ενότητα 0, θα ακολουθήσει αμέσως και ετοιμασία ολοκληρωμένου Πλάνου Διαχείρισης Προγράμματος (Program Management Plan), το οποίο θα αποτελεί συνάμα τον οδηγό για την υλοποίηση των Δράσεων σε μια περίοδο περίπου 4 ετών. Ο χρονικός ορίζοντας των 4 ετών έχει επιλεγεί για να συγχρονίσει την υλοποίηση της Στρατηγικής με τους κύκλους διενέργειας των κυριοτέρων μεγάλων δραστηριοτήτων της (π.χ. την αξιολόγηση κινδύνων σε εθνικό επίπεδο, τις ασκήσεις, τις τακτικές αξιολογήσεις επιπέδων κυβερνοασφάλειας, κλπ.).

Στα πλαίσια της πιο λεπτομερούς αξιολόγησης και ανάλυσης των επιμέρους Δράσεων, στο βαθμό που είναι εφικτό, θα εκτιμηθεί το κόστος υλοποίησης της κάθε Δράσης καθώς και η χρονική περίοδος κατά την οποία θα απαιτηθεί ο προϋπολογισμός σχετικών κονδυλίων, με βάση την λεπτομερή επέκταση των Δράσεων και των ενεργειών που θα εντοπιστούν. Η κοστολόγηση αυτή θα γίνει σε συνεργασία με τις αρμόδιες αρχές, και σε κάθε περίπτωση με γνώμονα τη σημαντικότητα της κάθε Δράσης και το εύρος εφαρμογής, ούτως ώστε η κοστολόγηση να είναι όσο το δυνατόν πιο ρεαλιστική, για κυβερνητικές υπηρεσίες.

Παράλληλα με την κοστολόγηση θα γίνει ιεράρχηση των Δράσεων που περιγράφονται στο παρόν έγγραφο, οι οποίες θα αξιολογηθούν (ανεξάρτητα από την κοστολόγηση τους), ως προς την σημαντικότητα και τη κρισιμότητα τους σε σχέση με το αποτέλεσμα που αναμένεται να επιφέρουν για ένα πιο ασφαλές ηλεκτρονικό περιβάλλον στην Κυπριακή Δημοκρατία. Σημειώνεται ότι η ενέργεια αυτή θα γίνει ανεξάρτητα από την διαδικασία κοστολόγησης των Δράσεων που αναφέρεται πιο πάνω. Η

ιεράρχηση αυτή θα συμπεριληφθεί στο Πλάνο Διαχείρισης Προγράμματος, με εκτίμηση του χρόνου υλοποίησης της κάθε Δράσης μέσα στο συνολικό τετραετές πρόγραμμα.

Για να επιτευχθεί αποτελεσματική στρατηγική ανταπόκριση, θα πρέπει η υλοποίηση της να τυγχάνει τακτικής και αυστηρής αξιολόγησης. Προς το σκοπό αυτό, τα αποτελέσματα της εφαρμογής των μέτρων και των προνοιών που εμπεριέχονται στις σχετικής δράσεις θα τυγχάνουν σχετικής ποιοτικής και ποσοτικής ανάλυσης ανάλογα με τη περίπτωση. Μια σωστή Στρατηγική Κυβερνοασφάλειας δεν πρέπει να θεωρείται ως ένα 'τελικό σχέδιο', αλλά αντιθέτως η υλοποίηση της θα πρέπει να παρακολουθείται στενά και να αναθεωρείται σε τακτά χρονικά διαστήματα. Η αναθεώρηση αυτή θα πρέπει να λαμβάνει υπόψη τα αποτελέσματα της αξιολόγησης, ως επίσης και τις καινούργιες απειλές που εμφανίζονται (και θα συνεχίσουν να εμφανίζονται) στον κυβερνοχώρο καθώς και όποια άλλα νέα δεδομένα εμφανίζονται σε αυτό το χώρο.

Η λεπτομερής επέκταση των Δράσεων της Στρατηγικής, όπως αναφέρεται στο κεφάλαιο 3, θα συμπεριλαμβάνει δείκτες και κριτήρια αξιολόγησης για την κάθε Δράση, όπου αυτό είναι εφικτό. Τα αποτελέσματα της αξιολόγησης θα επιτρέψουν την ορθή αναθεώρηση της Στρατηγικής με σημαντικά οφέλη στην Κυπριακή κοινωνία.

ΠΑΡΑΡΤΗΜΑ Ι - ΣΥΝΟΨΗ ΔΡΑΣΕΩΝ

ΠΑΡΑΡΤΗΜΑ ΙΙ - ΑΝΑΠΤΥΞΗ ΠΟΛΙΤΙΚΗΣ ΚΑΙ ΣΤΡΑΤΗΓΙΚΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΚΥΠΡΙΑΚΗ ΔΗΜΟΚΡΑΤΙΑ – ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Η Διαχείριση θεμάτων για την Ασφάλεια Δικτύων και πληροφοριών και τον συντονισμό για την εφαρμογή της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας γινόταν μέχρι τον Απρίλιο του 2018 από το ΓΕΡΗΕΤ στη βάση του Νόμου 112(Ι)2004. Οι ενέργειες που προηγήθηκαν της παρούσας κατάστασης και της ανάπτυξής της δεύτερης Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας αναφέρονται επιγραμματικά στη συνέχεια:

1. Στη βάση αρμοδιοτήτων που πηγάζουν από το Νόμο 112(Ι)/2004 (άρθρα 2(2)(ζ) και (ι), 2(3), 18(3)(στ), 19(1), 37(5), 39(2)(ιστ), 42(7), 55(2)(β), 80(α), 97, 98) και την αρμοδιότητα του ΓΕΡΗΕΤ να εκπροσωπεί την Κύπρο στο Διοικητικό Συμβούλιο του ENISA και να ενεργεί ως κεντρικός φορέας συντονισμού στην Κύπρο μεταξύ αρμοδίων εθνικών αρχών, το ΓΕΡΗΕΤ είχε αναλάβει μέχρι της παρούσης τον συντονισμό των θεμάτων της ασφάλειας δικτύων ηλεκτρονικών επικοινωνιών και πληροφοριών στην επικράτεια της Κυπριακής Δημοκρατίας και τον συντονισμό της εφαρμογής της Στρατηγικής Κυβερνοασφάλειας.

   Εντός του προαναφερόμενου πλαισίου έχουν προωθηθεί διαχρονικά και προωθούνται συγκεκριμένες ενέργειες, δράσεις και πολιτικές σε εθνικό επίπεδο:

1. Το 2006, το Υπουργείο Συγκοινωνιών και Έργων (ΥΣΕ) εγκρίνει έγγραφο πολιτικής[18] με βάση το οποίο προωθούνται, μέσω του ΓΕΡΗΕΤ, συγκεκριμένες δράσεις στον τομέα της ασφάλειας δικτύων και πληροφοριών συμπεριλαμβανομένων: της εγκαθίδρυσης Ομάδων Άμεσης Ανταπόκρισης για Συμβάντα που σχετίζονται με την Ασφάλεια Δικτύων και Πληροφοριών (CERTs/CSIRTs), της δημιουργίας θεσμικού πλαισίου για την ασφάλεια και την ακεραιότητα των υποδομών, αλλά και της ενημέρωσης όλων των επηρεαζόμενων και ευρύτερα της Κυπριακής κοινωνίας για τα θέματα ασφάλειας.

2. Το 2010 το ΥΣΕ , μετά από εισηγήσεις του ΓΕΡΗΕΤ και τις θετικές αξιολόγησης από τον ENISA, εγκρίνει λεπτομερές κείμενο πολιτικής[19] για τη θέση σε λειτουργία ενός Κυβερνητικού και ενός Ακαδημαϊκού CSIRT. Τα Κυπριακά CSIRTs κτίζονται με την προοπτική να καλύψουν και τον επιχειρηματικό τομέα σε δεύτερο στάδιο. Η ίδρυση των CSIRTs έχει θεσμοθετηθεί με Διάταγμα του ΕΡΗΕΤ ΚΔΠ 358/2010 το οποίο εκδόθηκε τον Αύγουστο του 2010.

3. Εντός του 2012 εισάγονται στο Νόμο περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων, 112(Ι)2004, νέες πρόνοιες με βάση το νέο πλαίσιο της Ευρωπαϊκής Ένωσης στο τομέα των Ηλεκτρονικών Επικοινωνιών[20], μεταξύ άλλων για τα θέματα ασφάλειας δικτύων και πληροφοριών. Οι νέες πρόνοιες του ευρωπαϊκού πλαισίου έχουν τεθεί σε εφαρμογή, σε Ευρωπαϊκό επίπεδο, από τις 25 Μαΐου 2011.

[18] Έγγραφο πολιτικής για την Ασφάλεια Δικτύων και Πληροφοριών 2006.
[19] Έγγραφο Πολιτικής για τη δημιουργία Φορέων Άμεσης Ανταπόκρισης για Περιστατικά και Συμβάντα που σχετίζονται με την Ασφάλεια Δικτύων και Πληροφορικών (CSIRT/CERT).
[20] Οδηγίες:"Better Regulation" Directive 2009/140/EC, και "Citizens' Rights" Directive 2009/136/EC.

4. Τις προαναφερθείσες ενέργειες υιοθετεί και συμπληρώνει η πρώτη Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας που υιοθετήθηκε από το Υπουργικό Συμβούλιο τον Φεβρουάριο και τέθηκε σε εφαρμογή τον Μάρτιο του 2013. Η Στρατηγική αυτή καλύπτει επίσης οριζόντια θέματα και δράσεις στους τομείς του κυβερνοεγκλήματος και της κυβερνοάμυνας. Περιλαμβάνει 17 δράσεις με τεχνικά, οργανωτικά και νομοθετικά μέτρα, προωθεί τα θέματα ενημέρωσης και κατάρτισης και ενισχύει τη συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα. Το παρόν έγγραφο αναθεωρεί και εκσυγχρονίζει την Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας.

ΠΑΡΑΡΤΗΜΑ ΙΙΙ - ΑΡΜΟΔΙΕΣ ΑΡΧΕΣ, ΚΑΙ ΠΑΡΑΤΗΡΗΤΕΣ ΣΤΗΝ ΚΥΠΡΙΑΚΗ ΔΗΜΟΚΡΑΤΙΑ

Πέραν της πολιτικής και των δράσεων που αναφέρονται στην ενότητα 2.2, στο ευρύτερο πεδίο του τομέα ασφάλειας των δικτύων και υπηρεσιών, των συστημάτων πληροφορικής, καθώς και των πληροφοριών που διακινούνται σε αυτά, προωθούνται και άλλες σημαντικές δράσεις από διάφορες αρχές στη Κυπριακή Δημοκρατία οι οποίες έχουν άμεση ή έμμεση εμπλοκή σε κρίσιμα θέματα ασφάλειας. Η κάθε αρχή έχει άμεσες ή έμμεσες αρμοδιότητες στον τομέα ασφάλειας δικτύων και πληροφοριών, καθώς και αλληλοσυνδέσεις και αλληλεξαρτήσεις μεταξύ τους, οι οποίες πρέπει να λαμβάνονται σοβαρά υπόψη και είναι δυνατόν να επηρεάζουν ουσιαστικά την υλοποίηση της παρούσας στρατηγικής.

Οι αρμόδιες αρχές της Κυπριακής Δημοκρατίας που εμπλέκονται στο παρόν στάδιο είναι οι ακόλουθες:

- Υφυπουργείο Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής (ΥΜΕΕ)
- Υπουργείο Δικαιοσύνης και Δημόσιας Τάξης (ΥΔΔΤ)
- Υπουργείο Άμυνας (ΥΠΑΜ)
- Υπουργείο Εξωτερικών (ΥΠΕΞ)
- Υπουργείο Οικονομικών
- Υπουργείο Παιδείας και Πολιτισμού
- Υπουργείο Ενέργειας, Εμπορίου και Τουρισμού
- Υπουργείο Εσωτερικών
- Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ)
- Τμήμα Υπηρεσιών Πληροφορικής (ΤΥΠ)
- Αστυνομία Κύπρου (ΑΚ)
- Γενικό Επιτελείο Εθνικής Φρουράς (ΓΕΕΦ)
- Εθνική Αρχή Ασφάλειας (ΕΑΑ)
- Κυπριακή Υπηρεσία Πληροφοριών (ΚΥΠ)
- Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΓΕΠΔΠΧ)
- Τμήμα Ηλεκτρονικών Επικοινωνιών (ΤΗΕ)
- Δύναμη Πολιτικής Άμυνας (ΠΑ)
- Μονάδα Καταπολέμησης Αδικημάτων Συγκάλυψης (ΜΟΚΑΣ).

Αρχές της Κυπριακής Δημοκρατίας που κρίνεται σκόπιμο να τηρούνται ενήμερες (παρατηρητές) στο παρόν στάδιο είναι οι ακόλουθες:

- Νομική Υπηρεσία της Δημοκρατίας
- Γενικός Ελεγκτής της Δημοκρατίας
- Υπηρεσία Εσωτερικού Ελέγχου
- Κεντρική Τράπεζα της Κύπρου.

Σημειώνεται ότι η αρμόδια Αρχή της Κυπριακής Δημοκρατίας που έχει την ευθύνη για τις **Διαβαθμισμένες Πληροφορίες (ΔΠ)** και τις **Διαβαθμισμένες Πληροφορίες Ευρωπαϊκής Ένωσης (ΔΠ ΕΕ)** είναι η **Εθνική Αρχή Ασφάλειας.** Παρόλο που το έγγραφο αυτό δεν απευθύνεται αποκλειστικά ή με άμεσο τρόπο στην προστασία των Διαβαθμισμένων Πληροφοριών, η διακίνηση των εν λόγω πληροφοριών επί της ουσίας υλοποιείται μέσα από την επικοινωνιακή υποδομή των Παροχέων Ηλεκτρονικών Επικοινωνιών.