Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων

Έγγραφο Πολιτικής

Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας

Ασφάλεια Δικτύων και Πληροφοριών και Προστασία Κρίσιμων Υποδομών Πληροφορίας

Version 1.0

23 Απριλίου 2012

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΣΥΝΟΨΗ

Τα συστήματα και οι τεχνολογίες επικοινωνιών και πληροφορίας αποτελούν σήμερα έναν από τους πιο σημαντικούς παράγοντες οικονομικής και κοινωνικής ανάπτυξης, ενώ ταυτόχρονα αποτελούν και απαραίτητα εργαλεία στα πλαίσια των λειτουργικών και κοινωνικών δομών κάθε χώρας. Γι'αυτό, δημιουργείται πλέον επιτακτική ανάγκη οι τεχνολογίες αυτές να παρέχουν ***ασφάλεια*** στη χρήση τους, η οποία ορίζεται ως η διατήρηση των αρχών της ***εμπιστευτικότητας***, ***ακεραιότητας*** και ***διαθεσιμότητας*** των πληροφοριών κατά τη ***μεταφορά***, ***επεξεργασία*** και ***αποθήκευσή*** τους. Αυτές οι αρχές οδηγούν στην οικοδόμηση ***εμπιστοσύνης*** στα πληροφοριακά συστήματα και τις ηλεκτρονικές υπηρεσίες, η οποία θεωρείται αναγκαίο συστατικό της συνεχιζόμενης ανάπτυξης σε αυτόν τον πολύτιμο τομέα της οικονομίας. Η ***ασφάλεια δικτύων και πληροφοριών***, και ευρύτερα η ***κυβερνοασφάλεια***, λειτουργεί για την διατήρηση των πιο πάνω αρχών.

Η Στρατηγική αυτή στοχεύει στη ***εδραίωση ενός ασφαλούς ηλεκτρονικού περιβάλλοντος*** στην Κυπριακή Δημοκρατία, με ειδικές πρόνοιες και δράσεις για την ***προστασία των κρίσιμων υποδομών πληροφορίας***, 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.

Η Ευρωπαϊκή Επιτροπή έχει θέσει ***υψηλούς στόχους για τον τομέα της ασφάλειας δικτύων και πληροφοριών***, οι οποίοι φαίνονται από τις εντατικοποιημένες εργασίες της στα θέματα αυτά, σε συνεργασία με τα κράτη-μέλη και με τον ENISA (European Network and Information Security Agency). Το νέο Ευρωπαϊκό Πλαίσιο Ηλεκτρονικών Επικοινωνιών δίδει ιδιαίτερη έμφαση στον τομέα της ασφάλειας και ακεραιότητας των δικτύων και υπηρεσιών, καθώς και στον τομέα της ***ασφάλειας των προσωπικών δεδομένων***. Από τους κυριότερους στόχους της Επιτροπής είναι η ***δημιουργία Εθνικών Σχεδίων Στρατηγικής*** για την ασφάλεια δικτύων και πληροφοριών (όπως το παρόν έγγραφο), η ***δημιουργία Εθνικών Σχεδίων Έκτακτης Ανάγκης*** για τα σχετικά θέματα και η ***δημιουργία Ομάδων Άμεσης Ανταπόκρισης*** (CERTs – Computer Emergency Response Teams) για συμβάντα παραβίασης της ηλεκτρονικής ασφάλειας.

Άνκαι ο τομέας της ασφάλειας δικτύων και πληροφοριών δεν είναι καινούργιος και έχουν διεκπεραιωθεί διάφορα σχετικά έργα από τις αρμόδιες αρχές του κράτους στο παρελθόν, το παρόν έγγραφο αντιπροσωπεύει την ***πρώτη οργανωμένη προσπάθεια για συντονισμένη 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 πλαισίου***, η ***διαμόρφωση τεχνικών και οργανωτικών μέτρων και διαδικασιών***, η ***ανάπτυξη των απαραίτητων ικανοτήτων και η σχετική κατάρτιση***, η ***αποδοτική συνεργασία του κράτους με αρμόδιους φορείς του δημοσίου και ιδιωτικού τομέα*** και η ***δημιουργία ή η προσαρμογή των απαραίτητων δομών και μηχανισμών εντός της Κυπριακής Δημοκρατίας***. Ως εκ τούτου, το παρόν έγγραφο περιέχει ***μια σειρά από δράσεις για την επίτευξη των προαναφερθέντων στόχων***, στους ακόλουθους τομείς:

- Οργανωτική Δομή
- Νομικό Πλαίσιο
- Συνεργασία Κράτους και Ιδιωτικού Τομέα
- Εντοπισμός Κρίσιμων Υποδομών Πληροφορίας
- Επισκόπηση Απειλών
- Εθνικό Πλαίσιο Κυβερνοασφάλειας
- Διαχείριση Περιστατικών
- Εθνικές και Διεθνείς Ασκήσεις
- Ανάπτυξη Ικανοτήτων
- Κουλτούρα Ασφάλειας
- Συνεργασία με Διεθνείς Φορείς και Ομάδες Εργασίας
- Δημιουργία Σχεδίου Έκτακτης Ανάγκης για τις Κρίσιμες Υποδομές Πληροφορίας
- Αλληλεξαρτήσεις.

Σύνοψη των δράσεων, μαζί με ένα γράφημα που να δείχνει τις αλληλεξαρτήσεις τους, παρουσιάζονται στα Παραρτήματα Ι και ΙΙ αντίστοιχα.

Το παρόν έγγραφο παρουσιάζει επίσης τις άμεσες ενέργειες που θα γίνουν εντός της Φάσης Α (βλ. παράγραφος 3.2), ως επίσης και τα επόμενα βήματα που πρέπει να ακολουθήσουν, όπως η λεπτομερής επέκταση των δράσεων, η κοστολόγηση υλοποίησης των δράσεων της Στρατηγικής, η ιεράρχηση και ο προγραμματισμός των δράσεων και η επακόλουθη αξιολόγηση των αποτελεσμάτων των εν λόγω δράσεων. Σημειώνεται επίσης ότι ***η Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας θα αναθεωρείται σε τακτική χρονική βάση***, λαμβάνοντας υπόψη τα αποτελέσματα της αξιολόγησης, καθώς και τις καινούργιες απειλές που εμφανίζονται (και θα συνεχίσουν να εμφανίζονται) στον κυβερνοχώρο. Ο στόχος είναι να γίνεται μια ολιστική αξιολόγηση των αποτελεσμάτων της εφαρμογής της στρατηγικής, η σχετική επικαιροποίηση της, και, όπου χρειάζεται, η αναγκαία αναθεώρησή της με γνώμονα να είναι διαχρονικά σωστή και να επιφέρει κατά το δυνατό το μέγιστο των ωφελημάτων της στην Κυπριακή κοινωνία.

1. ΕΙΣΑΓΩΓΗ

1.1 Ασφάλεια Δικτύου και Πληροφοριών

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 των οργανισμών, 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 πλείστον δηλαδή συνδεδεμένων στο Διαδίκτυο, και ο όρος αυτός συμπεριλαμβάνει και την ασφαλή χρήση των συστημάτων αυτών από τελικούς χρήστες.

Διευκρινίζεται ότι το επίπεδο ασφάλειας των πληροφοριών πρέπει να ξεκινά από τον καθορισμό της ***αξίας*** της πληροφορίας, 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 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 κυβερνήσεις έχουν ανάγκη να εμπιστεύονται τα μέσα στα οποία διακινούνται σημαντικές πληροφορίες, προσωπικά και άλλα δεδομένα.

Η ασφαλής ανάπτυξη 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 στο 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 από κακόβουλες ενέργειες ή φυσικά αίτια.

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

- 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,
- και 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 πληροφορίας 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 υπηρεσίες του κράτους που χρησιμοποιεί ο πολίτης υποστηρίζονται από υποδομές πληροφοριών. Ορισμένες από αυτές τις υποδομές αποτελούν ζωτικό τμήμα της Κυπριακής οικονομίας και της 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 του κράτους.

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 αλληλεπιδρούν ο ένας με τον άλλο.

Η παράγραφος 3.6 αναφέρεται σε μεγαλύτερη λεπτομέρεια στα κριτήρια που θα χρησιμοποιηθούν για τον ορισμό των κρίσιμων υποδομών πληροφορίας στην Κυπριακή Δημοκρατία. Το έργο που θα ακολουθήσει σύντομα για την ανάπτυξη Σχεδίου Έκτακτης Ανάγκης για τις κρίσιμες υποδομές πληροφορίας περιγράφεται στην παράγραφο 3.14 και αποτελεί προτεραιότητα του στρατηγικού σχεδιασμού.

1.3 Όραμα

Το όραμα της Στρατηγικής Ασφάλειας της Κυπριακής Δημοκρατίας είναι η λειτουργία των τεχνολογιών πληροφορικής και επικοινωνιών του τόπου με τα απαιτούμενα επίπεδα ασφάλειας, προς όφελος του κάθε χρήστη.

1.4 Στόχοι

Η ανάπτυξη της παρούσας στρατηγικής και οι δράσεις που έχουν προταθεί έχουν τους πιο κάτω στόχους:

- την διατήρηση και ανάπτυξη ενός ηλεκτρονικά ασφαλισμένου επιχειρηματικού περιβάλλοντος στην Κύπρο,
- την υποστήριξη των στόχων του κράτους που έχουν τεθεί στο στρατηγικό έργο 'Ψηφιακή Κύπρος' για την ανάπτυξη συνθηκών Κοινωνίας της Πληροφορίας,
- την ανάπτυξη εμπιστοσύνης από τους πολίτες και επιχειρήσεις/οργανισμούς για την ασφάλεια της ηλεκτρονικής διακυβέρνησης, συμπεριλαμβανομένου της διατήρησης του απορρήτου πληροφοριών σε στάση (αποθηκευμένα), μεταφορά και επεξεργασία,
- την εδραίωση ενός ασφαλούς ηλεκτρονικού περιβάλλοντος στην Κυπριακή Δημοκρατία για όλους τους πολίτες της,
- την αποφυγή δυσάρεστων επιπτώσεων από απειλές στον κυβερνοχώρο και την αποτελεσματική αντιμετώπιση έκτακτων περιστατικών,
- την δυνατότητα υποστήριξης ενός μελλοντικού ενιαίου εθνικού σχεδιασμού για την προστασία κρίσιμων υποδομών της Κυπριακής Δημοκρατίας (Critical Infrastructure Protection – CIP).

1.5 Κατευθυντήριες Αρχές (Guiding Principles)

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

- Τη δημιουργία Στρατηγικής στα πλαίσια συνεργασίας των αρμοδίων αρχών, λαμβάνοντας υπόψη τις αρμοδιότητες των εμπλεκομένων υπηρεσιών,
- Την ανάπτυξη ολιστικής προσέγγισης για την ανταπόκριση στις απειλές στον κυβερνοχώρο.
- 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 διεκπεραίωσης του Σχεδίου Στρατηγικής.
- Τον ορισμό υψηλών στόχων και τη βούληση η στρατηγική και οι δράσεις της να συνδράμουν πραγματικά στην οριστική αλλαγή και βελτίωση του επιπέδου ηλεκτρονικής ασφάλειας στην Κύπρο.

2. ΣΤΡΑΤΗΓΙΚΟ ΠΛΑΙΣΙΟ

2.1 Ευρωπαϊκή Πολιτική

Τα θέματα ασφάλειας αποτελούν σημαντικό πυλώνα του Ψηφιακού Θεματολογίου για την Ευρώπη. Η συγκεκριμένη Ευρωπαϊκή πολιτική καλύπτει σημαντικά θέματα που αφορούν τον τομέα της Ασφάλειας. Η πολιτική της Ευρωπαϊκής Επιτροπής στα θέματα της Ασφάλειας καλύπτεται σε βάθος στο έγγραφο στρατηγικής για την Ασφάλεια Δικτύων και Πληροφοριών (Network and Information Security, NIS). Επίσης, ως μέρος της εφαρμογής της ευρωπαϊκής πολιτικής στον τομέα αυτό, έχει θεσπιστεί και λειτουργεί από το 2004 ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (European Network and Information Security Agency, ENISA). Ο οργανισμός εδρεύει στο Ηράκλειο της Κρήτης και αναπτύσσει πανευρωπαϊκή και διεθνή δράση στον τομέα της ασφάλειας των δικτύων και πληροφοριών, βοηθώντας στην εφαρμογή της ευρωπαϊκής πολιτικής, στη διάχυση των πληροφοριών και των βέλτιστων πρακτικών, στην εναρμόνιση και το συντονισμό κοινών δράσεων, την οργάνωση και εκτέλεση ευρωπαϊκών και διεθνών ασκήσεων, καθώς και στο διεθνή συντονισμό και συνεργασία. Η ανανέωση του χρόνου λειτουργίας του ENISA, με διευρυμένους όρους εντολής, αποτελεί αντικείμενο έντονων διαβουλεύσεων αυτή τη περίοδο τόσο σε επίπεδο Συμβουλίου Υπουργών όσο και σε επίπεδο Ευρωκοινοβουλίου, δεδομένου ότι όλοι αναγνωρίζουν την αναγκαιότητα λειτουργίας ενός τέτοιου οργανισμού.

Το νέο Ευρωπαϊκό ρυθμιστικό πλαίσιο Ηλεκτρονικών Επικοινωνιών με ημερομηνία εφαρμογής σε πανευρωπαϊκό επίπεδο τον Μάιο του 2011, δίδει έμφαση στον τομέα της ασφάλειας, κυρίως σε θέματα που αφορούν (α) στην ασφάλεια και ακεραιότητα των δικτύων και των υπηρεσιών καθώς και στην εφαρμογή και επιβολή ρυθμιστικών μέτρων, και μηχανισμών συνεργασίας σε εθνικό και πανευρωπαϊκό επίπεδο, καθώς και στη δημιουργία εθνικών μηχανισμών κοινοποίησης συμβάντων παραβίασης ασφάλειας σε εθνικό και ευρωπαϊκό επίπεδο, τα οποία ενσωματώνονται στην «Οδηγία Πλαίσιο», αλλά και (β) της ασφάλειας προσωπικών δεδομένων, της επεξεργασίας και της παραβίασης της ασφάλειας προσωπικών δεδομένων, της προστασίας δεδομένων που φυλάσσονται σε τερματικό εξοπλισμό συνδρομητών, της χρήσης αυτομάτων συστημάτων κλήσης και επικοινωνίας χωρίς ανθρώπινη παρέμβαση, τα οποία ενσωματώνονται στην «Οδηγία προστασίας της ιδιωτικής ζωής για τις Ηλεκτρονικές Επικοινωνίες».

Επίσης, το τελευταίο διάστημα, τα θέματα ασφάλειας βρίσκονται ψηλά και στην ατζέντα του σχετικού Συμβουλίου Υπουργών Επικοινωνιών[1] της Ευρωπαϊκής Ένωσης. Το Συμβούλιο, στα πλαίσια της τελευταίων συναντήσεων του, μεταξύ άλλων, έχει εξετάσει την πολιτική και τις επακόλουθες δράσεις συμπεριλαμβανομένου της θέσπισης νέων οδηγιών για τα θέματα της ασφάλειας και ειδικότερα της προστασίας των Κρίσιμων Υποδομών Πληροφορικών (CIIP).

[1] Η συναφής στρατηγική για την Ασφάλεια στο Διαδίκτυο θα αποτελέσει μέρος των εργασιών του Συμβουλίου Υπουργών Τηλεπικοινωνιών και υπό τη Κυπριακή Προεδρία.

Το Συμβούλιο έχει επίσης ζητήσει από τα Κράτη Μέλη και την Ευρωπαϊκή Επιτροπή να συνεργαστούν μεταξύ τους και με τρίτες χώρες: (α) για τον εντοπισμό και τη διασφάλιση κρίσιμων στοιχείων των υποδομών που θα μπορούσαν, σε περίπτωση βλάβης ή καταστροφής, να επηρεάζουν σημαντικά τα κράτη μέλη, καθώς και (β) για την ανταλλαγή πληροφοριών και καλών πρακτικών, ενώ (γ) προτρέπει τα κράτη μέλη να ενθαρρύνουν την αποτελεσματική συνεργασία μεταξύ δημόσιων και ιδιωτικών φορέων, στα ίδια τα κράτη μέλη και σε τρίτες χώρες. Το Συμβούλιο ζητά επιπλέον την ετήσια ενημέρωση του ιδίου, καθώς και του Ευρωπαϊκού Κοινοβουλίου, από τα Κράτη Μέλη και την Ευρωπαϊκή Επιτροπή για τις ενέργειες τους στα θέματα αυτά.

Μετά το πέρας του Συμβουλίου Υπουργών Επικοινωνιών στις 27 Μαΐου 2011, που ασχολήθηκε με τα συγκεκριμένα θέματα, η Ευρωπαϊκή Επιτροπή, με ανακοίνωση της, επαναδιατύπωσε σαφώς τις ενέργειες στις οποίες αναμένει να προβούν τα κράτη μέλη της Ευρωπαϊκής Ένωσης, ζητώντας τη δέσμευση όλων των εμπλεκομένων στη προώθηση των κοινών στόχων. Συγκριμένα, η Ευρωπαϊκή Επιτροπή καλεί το Συμβούλιο και τα κράτη να δηλώσουν ισχυρή δέσμευση για τη βελτίωση και ενίσχυση της εθνικής ασφάλειας στον κυβερνοχώρο στα πλαίσια των δυνατοτήτων τους, με σκοπό να εξασφαλιστεί το υψηλότερο επίπεδο προστασίας εντός της Ευρωπαϊκής Ένωσης και πιο αποτελεσματική συνεργασία σε διεθνές επίπεδο.

Ως εκ τούτου, η Ευρωπαϊκή Επιτροπή προτίθεται να παρακολουθεί στενά τις επιδόσεις των κρατών μελών ως προς την επίτευξη τριών βασικών στόχων που προωθούνται σε ευρωπαϊκό επίπεδο:

(α) τη λειτουργία σε κάθε κράτος μέλος εθνικών / κυβερνητικών Ομάδων Άμεσης Ανταπόκρισης για Συμβάντα που σχετίζονται με την Ασφάλεια Δικτύων και Πληροφοριών (CERT)[2] και στη δημιουργία ενός κοινού και λειτουργικού δικτύου κυβερνητικών / εθνικών CERT στην Ευρώπη μέχρι το 2012, που να υποστηρίζεται από αποτελεσματικές εθνικές στρατηγικές.

(β) τη διοργάνωση τακτικών εθνικών και πανευρωπαϊκών ασκήσεων για την ασφάλεια στον κυβερνοχώρο (με απαραίτητη τη συμμετοχή των CERTs), στις οποίες θα συμπεριλαμβάνεται και μια πανευρωπαϊκή άσκηση η οποία έχει προγραμματιστεί για το δεύτερο εξάμηνο του 2012.

(γ) την ανάπτυξη εθνικών σχεδίων έκτακτης ανάγκης για την ασφάλεια δικτύων και πληροφοριών, και συμβάντων στον κυβερνοχώρο ενώ αναμένει από όλα τα μέρη να συμβάλουν στην ανάπτυξη ενός ευρωπαϊκού σχεδίου έκτακτων περιστατικών στον κυβερνοχώρο εντός του 2012. Με βάση τις εθνικές εμπειρίες, ένα τέτοιο σχέδιο θα πρέπει να θέσει τις βάσεις και τις κατάλληλες διαδικασίες για την αποτελεσματική επικοινωνία μεταξύ των κρατών μελών σε περίπτωση κοινών απειλών, των κακόβουλων παρεμβάσεων ή/και επιθέσεων στα οποία εμπλέκονται διάφορα κράτη μέλη.

Σε εθνικό επίπεδο τα έργα που αναφέρονται στα σημεία (β) και (γ) αποτελούν επιμέρους δράσεις του έργου ανάπτυξης της στρατηγικής της Κυπριακής Δημοκρατίας. Το έργο που αναφέρεται στο σημείο (α) βρίσκεται σε εξέλιξη στη Κυπριακή Δημοκρατία και ρυθμίζεται με ξεχωριστή δευτερογενή

[2] [2] Λόγω της σημαντικότητας του, το θέμα των CERT τυγχάνει ειδικού χειρισμού από το ΓΕΡΗΕΤ και τις αρμόδιες αρχές, με συγκεκριμένες, παράλληλες, ενέργειες εκ μέρους της πολιτείας.

νομοθεσία που εκδίδεται από τον ΕΡΗΕΤ, αλλά η σωστή λειτουργία των ομάδων CERTs/CSIRTs αποτελεί βασική προϋπόθεση για την ανάπτυξη του στρατηγικού σχεδιασμού που αναφέρεται στο παρόν έγγραφο. Τα ίδια θέματα αποτέλεσαν αντικείμενο ειδικής Υπουργικής Διάσκεψης που πραγματοποιήθηκε στην Ουγγαρία τον Απρίλιο του 2011, στα πλαίσια των εργασιών της Προεδρίας και της Ευρωπαϊκής Επιτροπής κατά το πρώτο εξάμηνο του 2011. Σε αυτή εκπροσωπήθηκαν όλα τα κράτη μέλη και η δραστηριότητα εντασσόταν στις δράσεις του Συμβουλίου Υπουργών Επικοινωνιών στον τομέα της Ασφάλειας Δικτύων και Πληροφοριών. Τα πορίσματα του συνεδρίου καλύπτουν με λεπτομέρεια τις υποχρεώσεις των κρατών μελών, στα ίδια θέματα που αναφέρονται στη παρούσα ενότητα. Ειδικότερα στα θέματα των CERTs, στα συμπεράσματα της Διάσκεψης αναφέρεται ρητά ότι:

«Τα κράτη μέλη πρέπει να θεσπίσουν και να θέσουν σε πλήρη λειτουργία εθνικές / κυβερνητικές ομάδες CERT όσο το δυνατόν συντομότερα, να παρέχουν τεχνική υποστήριξη στα όργανα της Ευρωπαϊκής Επιτροπής για τη δημιουργία του EU-CERT μέχρι το 2012, και να προωθήσουν τη δημιουργία ενός αποτελεσματικού δικτύου ομάδων CERT σε ευρωπαϊκό επίπεδο, στο οποίο θα συμμετέχει και το EU CERT».

Συνοψίζοντας, η Ευρωπαϊκή Ένωση το τελευταίο διάστημα εκτελεί, προετοιμάζει και προγραμματίζει ενέργειες ώστε να ενισχύσει τις δράσεις της σε σχέση με την ασφάλεια στον κυβερνοχώρο. Στόχος της είναι η αποτελεσματική αντιμετώπιση της ταχύτατα αυξανόμενης συχνότητας εγκλημάτων και επιθέσεων στον κυβερνοχώρο. Η Ευρωπαϊκή Επιτροπή ζητά από τις κυβερνήσεις των διαφόρων ευρωπαϊκών χωρών να εξετάσουν σοβαρά την ασφάλεια στον κυβερνοχώρο.

Ενδεικτική είναι η δήλωση της αντιπροέδρου της Ευρωπαϊκής Επιτροπής για το ψηφιακό θεματολόγιο, Neelie Kroes, η οποία δηλώνει στην ιστοσελίδα της Επιτροπής ότι:

«Οι επιθέσεις στον κυβερνοχώρο είναι μια πολύ πραγματική και συνεχώς αυξανόμενη απειλή. Οι επιθέσεις αυτές, είτε συμβαίνουν κατά μεμονωμένων χωρών, εταιρειών ή πιο πρόσφατα κατά της Ευρωπαϊκής Επιτροπής, μπορούν να παραλύσουν βασικές υποδομές «κλειδιά» και να προκαλέσουν τεράστιες, μακροπρόθεσμες ζημιές». Τονίζει επίσης ότι: *«Η ευρωπαϊκή ομάδα CERT αποτελεί ένδειξη της σοβαρότητας με την οποία θεσμικά όργανα της Ευρωπαϊκής Ένωσης εκλαμβάνουν την απειλή στην ασφάλεια στον κυβερνοχώρο».*

2.2 Η Ασφάλεια Δικτύων και Πληροφοριών στην Κυπριακή Δημοκρατία

Η Κυπριακή Δημοκρατία και ειδικότερα το Υπουργείο Συγκοινωνιών και Έργων (ΥΣΕ), και η αρμόδια συντονιστική αρχή[3] για την Ασφάλεια Δικτύων και Πληροφοριών στη Κύπρο, που είναι το Γραφείο του Επίτροπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων (ΓΕΡΗΕΤ), έχει αναγνωρίσει τον ουσιαστικό ρόλο των θεμάτων ασφάλειας στη προώθηση των νέων υπηρεσιών επικοινωνιών, στη

[3] Βάσει των προνοιών της νομοθεσίας που διέπει τη λειτουργία του, , το ΓΕΡΗΕΤ έχει αρμοδιότητα αναφορικά με την ασφάλεια των υποδομών ηλεκτρονικών επικοινωνιών καθώς και των πληροφοριών που διακινούνται ή αποθηκεύονται σε αυτές.

χρήση των νέων τεχνολογιών και γενικότερα στην ανάπτυξη της κοινωνίας της πληροφορίας. Προς αυτό το σκοπό έχουν προωθηθεί συγκεκριμένες ενέργειες, δράσεις και πολιτικές σε εθνικό επίπεδο:

(α) Το 2006, το Υπουργείο Συγκοινωνιών και Έργων (ΥΣΕ) έχει εγκρίνει έγγραφο πολιτικής[4] με βάση το οποίο προωθούνται, μέσω του ΓΕΡΗΕΤ, συγκεκριμένες δράσεις στο 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.

(β) Το ΥΣΕ έχει επίσης εγκρίνει το 2010, μετά από εισηγήσεις του ΓΕΡΗΕΤ, οι οποίες έτυχαν θετικής υποδοχής από τον ENISA, λεπτομερές κείμενο πολιτικής[5] για τη θέση σε λειτουργία ενός Κυβερνητικού και ενός Ακαδημαϊκού CERT. Τα Κυπριακά CERTs κτίζονται με τη προοπτική να καλύψουν και τον επιχειρηματικό τομέα σε δεύτερο στάδιο. Η ίδρυση των CERTs έχει θεσμοθετηθεί με Διάταγμα του ΕΡΗΕΤ ΚΔΠ 358/2010 το οποίο εκδόθηκε τον Αύγουστο του 2010.

(γ) 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[6], 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.

(δ) Η Κυπριακή Δημοκρατία, σε συνεργασία με τους εμπλεκόμενους φορείς, έχει δεσμευτεί μέσα από τις εργασίες του Συμβουλίου Υπουργών Επικοινωνιών, να συμβάλει στην Ευρωπαϊκή και διεθνή συνεργασία για την αντιμετώπιση των κινδύνων και προκλήσεων στο κυβερνοχώρο.

Τις προαναφερθείσες ενέργειες υιοθετεί και συμπληρώνει το σχέδιο στρατηγικής για την Ασφάλεια Δικτύων και Πληροφοριών και τη Κυβερνοασφάλεια που περιγράφεται στο παρόν έγγραφο. Στο πλαίσιο αυτής της εργασίας και με βάση της πρόνοιες του εθνικού σχεδίου και τις προτεραιότητες της Κυπριακής Δημοκρατίας, οι δράσεις στον τομέα της ασφάλειας δικτύων και πληροφοριών αποτελούν μέρος της ευρύτερης στρατηγικής για την ανάπτυξη της Κοινωνίας της Πληροφορίας[7], και επιτρέπουν στην Κύπρο να συμβάλει ενεργά στον ευρύτερο σχεδιασμό για τη προστασία των Ευρωπαϊκών κρίσιμων υποδομών πληροφοριών εντός του 2012 και στη συνέχεια.

[4] Έγγραφο πολιτικής για την ασφάλεια Δικτύων και Πληροφοριών 2006.
[5] Έγγραφο Πολιτικής για τη δημιουργία Φορέων Άμεσης Ανταπόκρισης για Περιστατικά και Συμβάντα που σχετίζονται με την Ασφάλεια Δικτύων και Πληροφορικών (CSIRT/CERT).
[6] Οδηγίες:"Better Regulation" Directive 2009/140/EC, και "Citizens' Rights" Directive 2009/136/EC.
[7] Βλ. έγγραφο στρατηγικής 'Ψηφιακή Κύπρος' το οποίο εγκρίθηκε από το Υπουργικό Συμβούλιο τον Φεβρουάριο του 2012.

2.3 Αρμόδιες Αρχές και Παρατηρητές της Κυπριακής Δημοκρατίας

Πέραν της πολιτικής και των δράσεων που αναφέρονται στην παράγραφο 2.2, στο ευρύτερο πεδίο του τομέα ασφάλειας των δικτύων και υπηρεσιών, των συστημάτων πληροφορικής, καθώς και των πληροφοριών που διακινούνται σε αυτά, δραστηριοποιούνται 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 μεταξύ τους οι οποίες πρέπει να τύχουν σύνθεσης για την υλοποίηση της παρούσας στρατηγικής.

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

- Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων (ΓΕΡΗΕΤ)
- Τμήμα Υπηρεσιών Πληροφορικής (ΤΥΠ)
- Αστυνομία Κύπρου
- Γενικό Επιτελείο Εθνικής Φρουράς (ΓΕΕΦ)
- Εθνική Αρχή Ασφάλειας
- Κεντρική Υπηρεσία Πληροφοριών (ΚΥΠ)
- Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- Υπουργείο Συγκοινωνιών και Έργων (ΥΣΕ)
- Τμήμα Ηλεκτρονικών Επικοινωνιών (ΤΗΕ)
- Δύναμη Πολιτικής Άμυνας
- Πυροσβεστική Υπηρεσία
- 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.

Μια σύντομη περίληψη των σχετικών αρμοδιοτήτων της κάθε αρχής όπως και της σχετικής στην κάθε περίπτωση νομοθεσίας παρατίθεται στο Παράρτημα ΙΙΙ.

Σημειώνεται ότι η αρμόδια Αρχή της Κυπριακής Δημοκρατίας που έχει την ευθύνη για τις **Διαβαθμισμένες Πληροφορίες (ΔΠ)** και τις **Διαβαθμισμένες Πληροφορίες Ευρωπαϊκής Ένωσης (ΔΠΕΕ)** 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 Παρόχων Υπηρεσιών Επικοινωνιών.

2.4 Οι Απειλές στον Κυβερνοχώρο Σήμερα

Η χρήση ηλεκτρονικών υπολογιστών και συστημάτων επικοινωνίας έχουν διεισδύσει πλέον σε τεράστιο βαθμό στη ζωή μας, και έτσι όλο και αυξάνεται ο βαθμός εξάρτησης μας στις τεχνολογίες αυτές για μεγάλο μέρος των δραστηριοτήτων μας. Οι τεχνολογίες αυτές χρησιμοποιούνται σήμερα σε πάρα πολλούς τομείς πέραν των επικοινωνιών, για την παραγωγή και μεταφορά ενέργειας, την διαχείριση των συστημάτων ύδρευσης/αποχέτευσης, τις χρηματοπιστωτικές υπηρεσίες, οι ένοπλες δυνάμεις, οι δυνάμεις ασφαλείας, τα κυβερνητικά τμήματα και υπηρεσίες, υγεία, κλπ. Αν και τα οφέλη που έχουν προκύψει από τις τεχνολογίες πληροφορίας και επικοινωνιών (ΤΠΕ) είναι τεράστια, οι τεχνολογίες των νέων δικτύων έχουν φέρει μαζί τους και πληθώρα θεμάτων ασφάλειας που αξιοποιούνται από κακόβουλα στοιχεία τα οποία στοχεύουν στην εκμετάλλευση ευάλωτων σημείων σε στοιχεία των υποδομών και των δικτύων, όπως υπολογιστές, διακομιστές, μεταγωγείς, κλπ.

Τα τελευταία χρόνια έχουν εμφανιστεί πολλαπλές απειλές στα δίκτυα επικοινωνίας, ειδικά με την μεγάλη αύξηση της χρήσης του διαδικτύου από τους πολίτες. Οι ΤΠΕ έχουν χρησιμοποιηθεί κακόβουλα για την κλοπή χρημάτων από τραπεζικούς λογαριασμούς, την πρόσβαση σε εμπιστευτικές πληροφορίες, την πρόκληση ζημιών σε σημαντικές ιστοσελίδες (με συνεπαγόμενη άρνηση πρόσβασης στο κοινό), κλπ. Παραδείγματα πληροφοριών που έχουν κλαπεί από εταιρείες αναφέρονται σε εμπιστευτικά συμβόλαια, σχέδια προϊόντων, στοιχεία πιστωτικών καρτών, αριθμούς λογαριασμών και άλλα προσωπικά στοιχεία. Τέτοια περιστατικά μπορεί να προκαλέσουν τις πλέον σοβαρές ζημιές σε ένα οργανισμό, αφού πέραν των άμεσων ζημιών πλήττεται και το καλό όνομα του οργανισμού καθώς και η εμπιστοσύνη των πελατών του. Αντίθετα μειώνεται σημαντικά η πιθανότητα τέτοιων περιστατικών εφόσον λαμβάνονται τα κατάλληλα μέτρα από ένα οργανισμό ή εταιρεία.

Παρατηρείται πλέον, σε παγκόσμιο επίπεδο, το γεγονός ότι όχι μόνο αυξάνεται η συχνότητα των επιθέσεων στον κυβερνοχώρο, αλλά επίσης και η πολυπλοκότητα των επιθέσεων αυτών. Το κοινό, στις πλείστες περιπτώσεις, δεν είναι ενήμερο για τον απολογισμό των επιθέσεων αυτών, αλλά και το είδος των ζημιών που προκαλούνται από αυτές. Ένα φαινόμενο που παρατηρείται πρόσφατα στον κυβερνοχώρο είναι αυτό των *'botnets'* – αυτοματοποιημένα εικονικά δίκτυα που εμπλέκουν μεγάλους αριθμούς υπολογιστών (έχουν αναφερθεί μέχρι και δεκάδες χιλιάδες), τα οποία ελέγχονται από κακόβουλους φορείς. Αυτοί οι υπολογιστές βρίσκονται σε σπίτια και επιχειρήσεις, και ίσως και σε κυβερνητικές υπηρεσίες, χωρίς οι ίδιοι οι χρήστες να το αντιλαμβάνονται ή να το γνωρίζουν, και χρησιμοποιούνται για μεγάλης κλίμακας επιθέσεις στον κυβερνοχώρο.

Εκτός από τις επιπτώσεις σε πρόσωπα όπως αναφέρονται πιο πάνω, μπορούν εύκολα να δημιουργηθούν προβλήματα και στα κράτη τα ίδια. Η παρεμβολή στις επικοινωνίες ενός κράτους ήταν πάντα ένα αναπόσπαστο μέρος των στρατιωτικών αναμετρήσεων. Σήμερα, καθώς πολλά από τα επικοινωνιακά συστήματα ενός Στρατού συμπεριλαμβάνουν και ηλεκτρονικούς υπολογιστές, κάποια κράτη έχουν ήδη αναπτύξει ηλεκτρονικά όπλα για επιθέσεις στον κυβερνοχώρο τα οποία μπορούν πλέον να χρησιμοποιήσουν σαν μέρος μιας ευρείας στρατιωτικής επίθεσης ή τρομοκρατικών ενεργειών. Επίσης, οποιαδήποτε τρωτά σημεία στις ΤΠΕ των Ενόπλων Δυνάμεων μπορούν να οδηγήσουν σε διαρροή ευαίσθητων πληροφοριών προς μη εξουσιοδοτημένους χρήστες. Η λειτουργία των σημερινών ενόπλων δυνάμεων βασίζεται σε μεγάλο βαθμό σε ΤΠΕ και μια σοβαρή

κυβερνοεπίθεση θα μπορούσε να έχει δραματικές συνέπειες στις αμυντικές ικανότητες μιας χώρας. 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.

Σημειώνεται ότι η στρατηγική ανταπόκριση (βλ. κεφάλαιο 3) και οι δράσεις που περιγράφονται στο παρόν έγγραφο δεν αφορούν το χειρισμό στρατιωτικών θεμάτων ασφάλειας δικτύων και πληροφοριών και το χειρισμό συναφών θεμάτων τρομοκρατίας, αλλά η σχετική αναφορά καταδεικνύει τη μεγάλη εξάρτηση των τεχνολογιών που αναφέρονται στο παρόν έγγραφο με την ασφαλή λειτουργία και των στρατιωτικών δικτύων επικοινωνιών και πληροφοριών.

3. ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΑΠΟΚΡΙΣΗ

3.1 Τομείς Προτεραιότητας

Η στρατηγική ανταπόκριση της Κυπριακής Δημοκρατίας στις προαναφερθείσες απειλές αναλύεται σε επιμέρους τομείς προτεραιότητας που έχουν εντοπιστεί για τη βέλτιστη προστασία των κρίσιμων υποδομών πληροφορίας. Οι τομείς στους οποίους δίδεται προτεραιότητα σε σχέση με τις ανάγκες της Κυπριακής Δημοκρατίας είναι οι ακόλουθοι, όπως φαίνονται και στο Γράφημα 1:

Γράφημα 1: Προτεραιότητες της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας

- η **οργάνωση των αρμόδιων φορέων του κράτους** που να διασφαλίζει σωστή και αποτελεσματική συνεργασία,
- η **δημιουργία ολοκληρωμένου νομοθετικού πλαισίου** από τις αρμόδιες υπηρεσίες του κράτους που να καλύπτει όλες τις πτυχές της ασφάλειας δικτύων και πληροφοριών, συμπεριλαμβανομένου του κυβερνοεγκλήματος (cybercrime) και της προστασίας των προσωπικών δεδομένων,
- η **διαμόρφωση τεχνικών και οργανωτικών μέτρων και διαδικασιών** για την αύξηση της ασφάλειας των σχετικών χώρων, εξοπλισμού και λογισμικού στον απαιτούμενο βαθμό,

- η **ανάπτυξη των απαραίτητων ικανοτήτων και η κατάρτιση** επί των θεμάτων ασφάλειας, τόσο των άμεσα εμπλεκομένων όσο και του κοινού,
- η **αποδοτική συνεργασία του κράτους με αρμόδιους φορείς του δημόσιου και ιδιωτικού τομέα**, τόσο σε εθνικό όσο και σε διεθνές επίπεδο,
- η **δημιουργία ή η 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.

3.2 Διαχωρισμός Δράσεων – Φάσεις Α και Β

Το υπόλοιπο του παρόντος κεφαλαίου παρουσιάζει τις δράσεις που έχουν εντοπιστεί για την εκτέλεση του στρατηγικού σχεδιασμού. Η οργανωτική δομή και οι διαθέσιμοι πόροι για την υλοποίηση των δράσεων δεν βρίσκονται σε επίπεδο που να επιτρέπει την άμεση έναρξη όλων των δράσεων που έχουν εντοπιστεί, και έτσι η κάθε δράση που ακολουθεί αναφέρει και την φάση στην οποία θα εκτελεστεί:

- **Φάση Α**
  - Η Φάση Α θα περιέχει τις δράσεις που το ΓΕΡΗΕΤ είναι σε θέση να ξεκινήσει στο άμεσο μέλλον με τους διαθέσιμους πόρους που έχει στο παρόν στάδιο.
- **Φάση Β**
  - Η Φάση Β περιέχει τις δράσεις που το ΓΕΡΗΕΤ θα είναι σε θέση να συντονίσει αφού εξεταστεί νέα οργανωτική δομή, με τους απαραίτητους πόρους για την επιτυχή διεκπεραίωση της Στρατηγικής στο σύνολο της.

Η κάθε δράση αναφέρει τη φάση στην οποία θα εκτελεστεί και οι δράσεις που αναφέρουν και τις δύο φάσεις θα τύχουν μερικής εκτέλεσης στην κάθε φάση. Σημειώνεται ότι αυτό δε σημαίνει ότι οι δράσεις που θα υλοποιηθούν στη Φάση Α θα ολοκληρωθούν εντός της εν λόγω φάσης. Οι πλείστες δράσεις της Στρατηγικής αυτής θα συνεχίσουν να εκτελούνται μακροπρόθεσμα για τη συνεχόμενη προστασία του κυβερνοχώρου στην Κύπρο.

3.3 Οργανωτική Δομή

Το θέμα της ασφάλειας δικτύων και πληροφοριών αποτελεί μεγάλο και πολύπλοκο κεφάλαιο, για τη διαχείριση του οποίου έχουν εμπλοκή πολλοί φορείς του δημόσιου τομέα, όπως φαίνεται και στην παράγραφο 2.3. Ο κάθε αρμόδιος φορέας έχει τους δικούς του τομείς ευθύνης και είναι σημαντικό να τηρηθεί αυτός ο διαχωρισμός. Λόγω της πολυπρόσωπης αυτής συμμετοχής στη διαχείριση των επιμέρους πτυχών της ασφάλειας 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. Η δραστηριότητα αυτή είναι αποδοτική όταν γίνεται από μια οντότητα/ομάδα η οποία να είναι σε θέση να συντονίσει τις προσπάθειες της Κυπριακής Δημοκρατίας για την άρτια ανταπόκριση της έναντι των

απειλών που εμφανίζονται σήμερα καθώς και των αναδυόμενων απειλών στον κυβερνοχώρο. Η οντότητα/ομάδα αυτή θα πρέπει:

- 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 παρόχους των δικτύων επικοινωνιών της Κύπρου, των εμπλεκομένων του ιδιωτικού τομέα, των διεθνών ομάδων εργασίας και φόρουμ σχετικά με το θέμα.

Λαμβάνοντας υπόψη ότι ο καταρτισμός ολοκληρωμένης οργανωτικής δομής είναι μεν απαραίτητος για την αποδοτική προώθηση των δράσεων του στρατηγικού σχεδιασμού, αλλά οι σχετικές διαδικασίες προς αυτή τη κατεύθυνση επηρεάζονται και από εξωγενείς παράγοντες που σχετίζονται με την οικονομική κατάσταση που διάγει ο τόπος σήμερα και τις χρονοβόρες διαδικασίες στελέχωσης, η υλοποίηση μιας τέτοιας δομής θα προωθηθεί ως Φάση Β της υλοποίησης του προτεινόμενου στρατηγικού σχεδίου ούτως ώστε:

- να μην καθυστερήσει ο προγραμματισμός και η εκτέλεση δράσεων επειγούσης φύσεως και άμεσης προτεραιότητας για τις οποίες το νομικό πλαίσιο είναι καθορισμένο,
- να αξιοποιηθούν οι υφιστάμενες δομές στο μέγιστο δυνατό βαθμό με σταδιακή αναβάθμιση τους στο επιθυμητό επίπεδο,
- η οικονομική επιβάρυνση να είναι σταδιακή και στα πλαίσια των δυνατοτήτων της Κυπριακής οικονομίας,
- οι Κυπριακές Αρχές να είναι σε θέση να ανταποκριθούν στις άμεσες υποχρεώσεις τους σε εθνικό και Ευρωπαϊκό επίπεδο όπου οι εργασίες προωθούνται με γρήγορους και απαιτητικούς ρυθμούς,
- να δοθεί ο απαραίτητος χρόνος σωστής αξιολόγησης των αναγκών, σε σχέση με τις απαιτήσεις υλοποίησης, συντονισμού και εποπτείας του μηχανισμού ανταπόκρισης στις απαιτήσεις εφαρμογής της στρατηγικής και των σχετικών δράσεων.

Ως εκ τούτου, στη Φάση Α θα καθοριστεί το πλαίσιο συνεργασίας του ΓΕΡΗΕΤ, ως συντονιστικού φορέα, και των Αρμοδίων Αρχών για την υλοποίηση των ενεργειών με άμεση προτεραιότητα όπως είναι ο καταρτισμός του σχεδίου προστασίας των κρίσιμων υποδομών πληροφοριών, η λειτουργία του κυβερνητικού CSIRT/CERT, η αξιολόγηση και η ενίσχυση της ετοιμότητας των δικτυακών υποδομών ως προς την αντοχή τους στην έκθεση κινδύνων και την αντιμετώπιση απειλών ασφάλειας, η διαχείριση και η κοινοποίηση συμβάντων παραβίασης της ασφάλειας δικτύων, συστημάτων και πληροφοριών, η διοργάνωση εθνικών ασκήσεων και η συμμετοχή σε ευρωπαϊκές ασκήσεις. Οι ενέργειες αυτές αναφέρονται στις ευρύτερες αρμοδιότητες του ΓΕΡΗΕΤ στο τομέα της ασφάλειας δικτύων και πληροφοριών, ενώ από αυτές οι συγκεκριμένες δράσεις με προτεραιότητα που εντάσσονται ειδικά στο σχέδιο στρατηγικής που καλύπτει το παρόν έγγραφο, αναφέρονται στην παράγραφο 4.1. Στη φάση

αυτή χρειάζεται μια συμφωνημένη βάση συνεργασίας μεταξύ των αρμοδίων αρχών, η οποία θα διευρύνεται και θα αναπροσαρμόζεται ανάλογα με τη πρόοδο του συνολικού έργου.

Δράση 1 - Φάση Α - Καθορισμός του πλαισίου συνεργασίας και ανταλλαγής πληροφοριών με το ΓΕΡΗΕΤ, αλλά και μεταξύ των δημοσίων αρχών ώστε το ΓΕΡΗΕΤ να είναι σε θέση να αναλάβει αποτελεσματικά τον συντονισμό της στρατηγικής ανταπόκρισης του κράτους στον τομέα της κυβερνοασφάλειας και της προστασίας των κρίσιμων υποδομών πληροφορίας, καθώς και στην οργάνωση των δράσεων που αφορούν τους υπόλοιπους εμπλεκόμενους φορείς στους τομείς προτεραιότητας με άμεση δυνατότητα εφαρμογής.

Ο μηχανισμός προγραμματισμού και εκτέλεσης των υφιστάμενων δράσεων για την ασφάλεια των δικτύων και πληροφοριών που εμπίπτουν στις αρμοδιότητες του ΓΕΡΗΕΤ, βασίζεται στην υφιστάμενη του οργανωτική δομή. Η υφιστάμενη δομή δεν επαρκεί για την ανάληψη και την εκτέλεση των δράσεων που προσδιορίζονται στο παρόν έγγραφο. Επομένως, παράλληλα με τις άμεσες προτεραιότητες που προωθεί το γραφείο με βάση τις τρέχουσες και επείγουσες εθνικές και ευρωπαϊκές υποχρεώσεις και ανάγκες της Κυπριακής Δημοκρατίας, το ΓΕΡΗΕΤ σε συνεργασία με τις άλλες αρμόδιες αρχές της Δημοκρατίας θα προβεί σε μελέτη και υποβολή εισηγήσεων για τον καθορισμό από τον αρμόδιο Υπουργό Συγκοινωνιών και Έργων (ΥΣΕ), πολιτικής για νέα οργανωτική δομή της υπηρεσίας, ώστε να είναι σε θέση να αναλάβει το τεράστιο έργο συντονισμού του τομέα της ασφάλειας των δικτύων και πληροφοριών.

Δράση 2 - Φάση Α - Το ΓΕΡΗΕΤ θα προβεί, στο κατάλληλο χρόνο και σε συντονισμό με τις άλλες αρμόδιες αρχές, σε μελέτη για τον καθορισμό πολιτικής για την νέα οργανωτική δομή της υπηρεσίας, ώστε να είναι σε θέση να συντονίσει τις προσπάθειες της Κυπριακής Δημοκρατίας για την άρτια υλοποίηση, εφαρμογή και εποπτεία του συνόλου των δράσεων και την αποτελεσματική ανταπόκριση στις απειλές που εμφανίζονται σήμερα στον ηλεκτρονικό χώρο, καθώς και για τις αναδυόμενες απειλές που θα εμφανίζονται στο μέλλον.

Το ΓΕΡΗΕΤ θα συντονίσει επίσης τη δημιουργία ομάδων εργασίας, οι οποίες θα αναλάβουν την διεκπεραίωση των υπολοίπων δράσεων που προκύπτουν από το παρόν έγγραφο. Οι ομάδες αυτές θα συγκροτηθούν από προσωπικό με την κατάλληλη τεχνογνωσία από τις αρμόδιες υπηρεσίες του κράτους, καθώς και από εμπειρογνώμονες του ιδιωτικού τομέα και αντιπροσώπους των διαχειριστών κρίσιμων υποδομών πληροφορίας. Βλέπετε επίσης την παράγραφο 3.5.

Για εντοπισμό και αξιολόγηση των ενδεχόμενων κινδύνων, πιθανόν να απαιτείται η πρόσβαση των μελών των ομάδων εργασίας σε διαβαθμισμένες πληροφορίες, δηλαδή σε πληροφορίες που αφορούν στα τρωτά σημεία των κρίσιμων υποδομών κάθε δικτύου/συστήματος το οποίο θα αξιολογηθεί ως

σημαντικό. Λαμβάνοντας υπόψη ότι, εκτός από τις μελέτες αξιολόγησης κινδύνων, πρέπει παράλληλα να εξεταστούν οι στρατηγικές για αντιμετώπιση των κινδύνων αυτών, καθώς επίσης και να ετοιμαστούν τα σχετικά σχέδια έκτακτης ανάγκης για αποκατάσταση τυχόν καταστροφών, η σύνθεση των ομάδων εργασίας θα πρέπει να μελετηθεί έτσι ώστε να εξασφαλίζεται η εμπιστευτικότητα.

Δράση 3 - Φάση Α/Β - Συγκρότηση ομάδων εργασίας, με αντιπροσώπους από το δημόσιο και ιδιωτικό τομέα (όπου είναι απαραίτητο), για την διεκπεραίωση των δράσεων της Στρατηγικής.

3.4 Νομικό Πλαίσιο

Η Κυπριακή Δημοκρατία σήμερα παρέχει ήδη μεγάλη κάλυψη στο νομικό πλαίσιο που διέπει τα θέματα της ασφάλειας δικτύων και πληροφοριών, καθώς και του ηλεκτρονικού εγκλήματος. Χρειάζεται όμως να γίνει εντοπισμός **όλων** των σχετικών νομοθεσιών και να εκσυγχρονιστούν όπου παρίσταται ανάγκη, καθώς και να προωθηθεί καινούργια πρωτογενής και δευτερογενής νομοθεσία για να καλυφθούν όλες οι πρόνοιες της παρούσας στρατηγικής. Η νομοθεσία αυτή, μαζί με την εφαρμογή της, θα πρέπει να συμπεριλαμβάνει διαδικασίες πρόληψης, απώθησης και δυναμικής ανταπόκρισης σε όλες τις μορφές του κυβερνοεγκλήματος, και να είναι επίσης εναρμονισμένη με τις σχετικές νομοθεσίες και οδηγίες της Ευρωπαϊκής Ένωσης.

Τα θέματα ασφάλειας δικτύων και πληροφοριών και προστασίας κρίσιμων υποδομών πληροφορίας απαιτούν την διεθνή συνεργασία με άλλα κράτη-μέλη της Ευρωπαϊκής Ένωσης και πιθανότατα και με τρίτες χώρες. Ως εκ τούτου, δύναται να προκύψουν νομικές ιδιαιτερότητες 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 εκτός της Κύπρου για επίλυση προβλημάτων όταν αυτά προκύπτουν.

Δράση 4 - Φάση Β - Δημιουργία κατάλληλου νομικού πλαισίου για την πλήρη ενεργοποίηση και υποστήριξη των προνοιών της Στρατηγικής Κυβερνοασφάλειας. Θα πρέπει να εξεταστούν όλες οι σχετικές νομοθεσίες των αρμοδίων αρχών εφόσον προκύπτει ανάγκη προσαρμογής.

3.5 Συνεργασία Κράτους και Ιδιωτικού Τομέα

Το κράτος θα καταβάλει σημαντική προσπάθεια στον χώρο της ασφάλειας δικτύων και πληροφοριών, και ιδιαίτερα στην προστασία των κρίσιμων υποδομών πληροφορίας της Κύπρου. Η στρατηγική πρωτοβουλία στα θέματα αυτά δεν μπορεί παρά να προέρχεται από το κράτος, ως επίσης και η διασφάλιση της συνεργασίας με αρμόδιους φορείς σε εθνικό και διεθνές επίπεδο.

Αναγνωρίζεται όμως το γεγονός ότι **ο ρόλος του ιδιωτικού τομέα** στην ασφάλεια και ειδικότερα στην προστασία κρίσιμων υποδομών πληροφορίας **είναι εξαιρετικά σημαντικός**, για τους ακόλουθους λόγους:

- Ως επί το πλείστον, ο ιδιωτικός τομέας (συμπεριλαμβανομένου του ημικρατικού οργανισμού ηλεκτρονικών επικοινωνιών) χειρίζεται τις κρίσιμες υποδομές επικοινωνιών του κράτους, π.χ. τα δημόσια δίκτυα επικοινωνίας που χρησιμοποιούν τόσο τα διάφορα κυβερνητικά τμήματα, όσο και ο επιχειρηματικός/ακαδημαϊκός κόσμος και οι πολίτες του κράτους.
- Το κράτος βασίζεται στον ιδιωτικό τομέα όχι μόνο για τα δίκτυα επικοινωνίας, αλλά και για τον εξοπλισμό που χρησιμοποιεί, και την υλοποίηση αρκετών εκ των ενεργειών που σχετίζονται με την ασφάλεια δικτύων και πληροφοριών, είτε αυτές γίνονται από τους ίδιους, για σκοπούς ασφάλειας ή καλύτερης λειτουργίας των συστημάτων και των υπηρεσιών τους, ή επιβάλλονται με νομοθετικά ή και ρυθμιστικά μέτρα.
- Θεωρείται δεδομένο ότι στον ιδιωτικό τομέα υπάρχει συσσωρευμένη τεχνογνωσία και εξειδικευμένο ανθρώπινο δυναμικό, ενώ υπάρχουν επίσης οργανωμένα σύνολα που μπορούν να βοηθήσουν και να συμβάλουν στη βέλτιστη ανάπτυξη της Κυπριακής Δημοκρατίας στον τομέα αυτό.

Με γνώμονα τα πιο πάνω, η Κυπριακή Δημοκρατία θέτει ως προτεραιότητα τη διαβούλευση με τον ιδιωτικό τομέα για την επίτευξη των στόχων της, την υλοποίηση των προνοιών της στρατηγικής, την συνεχόμενη βελτίωση των δράσεων και των επιδράσεων της στρατηγικής καθώς και για την εξασφάλιση περαιτέρω τεχνογνωσίας και εξειδίκευσης.

Δράση 5 - Φάση Α/Β - Εκτενής επισκόπηση του ιδιωτικού τομέα, για τον εντοπισμό ομάδων και εμπλεκομένων (stakeholders) οι οποίοι μπορούν να συμβάλουν θετικά στην προσπάθεια για αύξηση του επιπέδου ηλεκτρονικής ασφάλειας στην Κυπριακή Δημοκρατία, δημιουργώντας συνάμα και τη βάση για στενούς δεσμούς συνεργασίας.

Κατά την εκτέλεση της πιο πάνω δράσης, το Κράτος θα επιδιώξει τη συνεργασία με υπάρχουσες αρχές οι οποίες καθορίζουν τον τρόπο λειτουργίας καίριων τομέων, όπως για παράδειγμα την Κεντρική Τράπεζα της Κύπρου για τις τράπεζες. Συνάμα με αυτό, θα εφαρμοστεί ένας μηχανισμός περιοδικής ενημέρωσης προς τον ιδιωτικό τομέα, αναφορικά με την εξέλιξη της προόδου των προγραμματισμένων δράσεων, ώστε οι ενέργειες του δημόσιου και ιδιωτικού τομέα για την υλοποίηση της Στρατηγικής να βρίσκονται σε σύγκλιση.

Πέραν από το πιο πάνω, επισημαίνεται επίσης το μοντέλο του Συνεταιρισμού Δημοσίου-Ιδιωτικού τομέα (Public Private Partnerships - PPPs), το οποίο θεωρείται σε πανευρωπαϊκό και διεθνές επίπεδο ως ένα αποτελεσματικό μοντέλο συνεργασίας μεταξύ φορέων του δημοσίου και του ιδιωτικού τομέα. Με την κατάλληλη προεργασία, θα διερευνηθεί η δυνατότητα, να συσταθεί ένα δυναμικό PPP στον

τομέα της προστασίας κρίσιμων υποδομών πληροφορίας, στα πλαίσια συνεργασίας του κράτους και του ιδιωτικού τομέα, 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 ασφαλείας,
- διευκολύνει την ανταλλαγή πληροφοριών σχετικά με νέες απειλές στον κυβερνοχώρο και λύσεις για την αποφυγή τους,
- επιτρέψει την συνεργασία στην έρευνα και καινοτομία στον σχετικό τομέα,
- βοηθήσει ώστε να τεθούν ψηλοί αλλά και εφικτοί στόχοι για την υλοποίηση του οράματος της στρατηγικής,
- θα συνεργάζεται με PPPs σε άλλες χώρες της Ευρωπαϊκής Ένωσης στον ίδιο τομέα, μέσω ενεργής συμμετοχής στις σχετικές ομάδες εργασίας.

Δράση 6 - Φάση Β - Διερεύνηση της δυνατότητας δημιουργίας δυναμικού PPP – Public Private Partnership στον τομέα της προστασίας κρίσιμων υποδομών στην Κυπριακή Δημοκρατία και προώθηση της ενεργής συνεργασίας με διεθνείς φορείς και συμμετοχής σε διεθνή φόρα. Η χρήση του PPP για οικοδόμηση εμπιστοσύνης μεταξύ κρατικού και ιδιωτικού τομέα θα είναι πρωτίστης σημασίας.

3.6 Εντοπισμός Κρίσιμων Υποδομών Πληροφορίας

Η ανάγκη προστασίας των κρίσιμων υποδομών πληροφοριών, όπως αναδεικνύεται και επεξηγείται στο παρόν έγγραφο, επιβάλλεται 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 καθώς και πιθανών επιπτώσεων σε άλλες χώρες που συνεπάγεται η μεγάλη αλληλεπίδραση και αλληλοσύνδεση των διεθνών δικτύων επικοινωνίας. Τίθεται όμως το ερώτημα για το ποιές ακριβώς υποδομές, θα θεωρηθούν 'κρίσιμες'. Ο κάθε αρμόδιος φορέας (εταιρείες τηλεπικοινωνιών, κυβερνητικά τμήματα, υπηρεσίες του κράτους, δυνάμεις ασφαλείας, ένοπλες δυνάμεις, νοσηλευτήρια, χρηματοπιστωτικά ιδρύματα, Αρχή Ηλεκτρισμού, υδατοπρομήθεια, κλπ) θα θεωρεί ότι η υποδομή του είναι κρίσιμης σημασίας και η βέλτιστη κατάσταση *θα ήταν* η πλήρης προστασία όλων των υποδομών πληροφορίας της Κυπριακής Δημοκρατίας ανεξαιρέτως.

Καθώς όμως δεν είναι εφικτή μια τέτοια προσέγγιση, 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 θα εντοπιστούν και θα αξιολογηθούν βάσει προκαθορισμένων κριτηρίων. Στον καθορισμό των κριτηρίων, πέραν από τα εθνικά δεδομένα, λαμβάνονται υπόψη και οι σχετικές εργασίες της Ευρωπαϊκής Επιτροπής και του ENISA (European Network and Information Security Agency), με κατάλληλη προσαρμογή στα δεδομένα της Κύπρου. Στην

αξιολόγηση για το καθορισμό των κρίσιμων υποδομών θα πρέπει να συμμετέχει τόσο ο δημόσιος όσο και ο ιδιωτικός τομέας , στα πλαίσια κατάλληλης/λων ομάδας/δων εργασίας.

Τα βήματα που θα ακολουθηθούν για τον εντοπισμό των κρίσιμων υποδομών πληροφορίας θα περιλαμβάνουν τα ακόλουθα:

- **καθορισμός υπηρεσιών** για στόχευση (π.χ. voice communications, data communications, data storage, data processing), που ενδεχομένως να είναι κρίσιμες,
- **εντοπισμός υποδομών** που είναι τεχνικά αναγκαίες για την λειτουργία των εν λόγω υπηρεσιών,
- **εισαγωγή αντικειμενικών κριτηρίων** για το επίπεδο προστασίας που χρειάζεται το κάθε δομικό στοιχείο, με κατηγοριοποίηση των υποδομών και χρήση αντικειμενικών κριτηρίων όπως τον αριθμό επηρεαζόμενων χρηστών, τον βαθμό ευαισθησίας των πληροφοριών που συγκεντρώνονται, αποθηκεύονται, διακινούνται ή τυγχάνουν επεξεργασίας στις υποδομές αυτές, κλπ.,
- **έλεγχος κριτηρίων** με εισαγωγή σεναρίων απώλειας λειτουργίας των επιλεγμένων υποδομών στα πλαίσια διενέργειας τακτικών ασκήσεων.

Δράση 7 - Φάση Α - Εντοπισμός και αξιολόγηση των κρίσιμων υποδομών στην Κυπριακή Δημοκρατία για την καλύτερη στόχευση των ενεργειών και δράσεων για την προστασία τους, με τη συμβολή τόσο του ιδιωτικού όσο και του δημόσιου τομέα.

3.7 Επισκόπηση Απειλών

Το κεφάλαιο 2.4 αναφέρθηκε στις γενικές απειλές που μπορούν να εμφανιστούν στον κυβερνοχώρο. Είναι σημαντικό να σημειωθεί όμως το ότι είναι περιορισμένες οι διαθέσιμες πληροφορίες για το συγκεκριμένο μείγμα απειλών που εμφανίζονται στην Κύπρο και που πιθανώς θα αναδυθούν στο μέλλον. Η προστασία των υποδομών πληροφορίας μπορεί βέβαια να επιτευχθεί με γενικά μέτρα μόνο, αλλά θα βελτιωθεί αισθητά η στρατηγική ανταπόκριση στις απειλές του κυβερνοχώρου εάν είναι γνωστές οι κύριες απειλές που υπάρχουν και που παρουσιάζονται στην Κυπριακή Δημοκρατία. Αυτό θα επιτρέψει, όχι μόνο την καλύτερη στόχευση των μέτρων ανταπόκρισης, αλλά και την σωστή στόχευση των πιο διαδομένων απειλών εάν τα απαραίτητα προστατευτικά μέτρα τοποθετηθούν σταδιακά μέσω ενός εφικτού προγράμματος υλοποίησης των προνοιών της παρούσας Στρατηγικής.

Επιβάλλεται λοιπόν να γίνει μια ολοκληρωμένη επισκόπηση των απειλών και επιθέσεων στον κυβερνοχώρο που έχουν εκδηλωθεί ευρέως σε Ευρωπαϊκά κράτη, συμπεριλαμβανομένου και της Κύπρου, για να επιτευχθεί η καλύτερη στόχευση των μέτρων ανταπόκρισης όπως αναφέρεται πιο πάνω. Η επισκόπηση αυτή θα συνδεθεί με τις πιο διαδεδομένες απειλές που θα δείξουν οι σχετικές Ευρωπαϊκές και άλλες διεθνείς μελέτες για μια πιο ολοκληρωμένη και σωστή στόχευση.

Δράση 8 - Φάση Β - Εκτενής έρευνα για καταγραφή των σημερινών απειλών και των επιθέσεων στον κυβερνοχώρο που έχουν δημοσιευτεί στην Κύπρο, μαζί με παρακολούθηση των καινούργιων απειλών που εμφανίζονται στον Ευρωπαϊκό και διεθνή χώρο.

3.8 Εθνικό Πλαίσιο Κυβερνοασφάλειας

Ο πιο εύκολος και αποτελεσματικός τρόπος για την επίτευξη ενός ικανοποιητικού επιπέδου ασφάλειας σε όλες τις κρίσιμες υποδομές πληροφορίας της Κυπριακής Δημοκρατίας είναι ο καθορισμός ενός Εθνικού Πλαισίου Κυβερνοασφάλειας, το οποίο θα χρησιμοποιηθεί ως βάση για την προστασία των κρίσιμων υποδομών πληροφορίας του κράτους, και για την διατήρηση της Ασφάλειας Πληροφοριών (Information Assurance). Το πλαίσιο αυτό θα πρέπει να αναπτυχθεί και να καθοριστεί βάσει διεθνών προτύπων ασφάλειας και να περιλαμβάνει (μεταξύ άλλων) τα ακόλουθα:

- Διοίκηση και Διαχείριση Κινδύνων (Risk Management)
- Εκτίμηση της ευπάθειας των συστημάτων πληροφορικής (Vulnerability Assessment)
- Τακτικές δοκιμές διείσδυσης (Penetration Testing)
- Διαχείριση χώρων, εξοπλισμού και λογισμικού
- Κατάλληλη εξουσιοδότηση και διαπίστευση προσωπικού
- Φυσική ασφάλεια και ασφάλεια περιβάλλοντος χώρου (Environmental Management)
- Αξιοποίηση των CERT για αντιμετώπιση περιστατικών (βλ. παράγραφος 3.9)
- Συνεχής παρακολούθηση ηλεκτρονικών επικοινωνιών για κακόβουλες επιθέσεις για εντοπισμό περιστατικών που βρίσκονται υπό εξέλιξη (Continuous Monitoring).

Το πλαίσιο αυτό θα πρέπει να υιοθετηθεί από όλες τους διαχειριστές κρίσιμων υποδομών πληροφορίας, και θα πρέπει επίσης η χρήση του να εξεταστεί και να εφαρμοστεί σε μετέπειτα στάδιο από τα υπόλοιπα κυβερνητικά τμήματα και άλλους σημαντικούς οργανισμούς εντός της Κυπριακής Δημοκρατίας. Για την επίτευξη του στόχου αυτού, το Εθνικό Πλαίσιο Κυβερνοασφάλειας θα αναπροσαρμοστεί και θα διαμορφωθεί ώστε να προωθηθεί επιπλέον και στον υπόλοιπο ιδιωτικό τομέα, για την βέλτιστη προστασία όλων αυτών που χρησιμοποιούν υπηρεσίες ηλεκτρονικών επικοινωνιών.

Δράση 9 - Φάση Β - Ανάπτυξη ενός Εθνικού Πλαισίου Κυβερνοασφάλειας το οποίο θα προωθεί την προστασία των κρίσιμων υποδομών πληροφορίας στην Κυπριακή Δημοκρατία, ως επίσης όλων των κυβερνητικών υπηρεσιών του κράτους.

Σημειώνεται ότι οι συγκεκριμένοι στόχοι που θα τεθούν ως προς τα επίπεδα προστασίας τα οποία θα υλοποιηθούν σε σχέση με τις τεχνολογίες και τα συστήματα αυτά, θα προσδιοριστούν από την

ανάλυση των επιτρεπτών επιπέδων κινδύνων (risks) στον κάθε τομέα και ισοζυγίζοντας αυτά με το κόστος υλοποίησης των συγκεκριμένων μέτρων ανταπόκρισης στις απειλές στον κυβερνοχώρο. Ένα σύνηθες μέτρο που χρησιμοποιείται είναι η διατήρηση του σχετικού ετήσιου κόστους κάτω από την εκτιμώμενη ετήσια ζημιά ή απώλεια από τις απειλές που εκδηλώνονται στα δίκτυα και συστήματα επικοινωνιών και πληροφορίας.

3.9 Διαχείριση Περιστατικών (Incident Response)

Η διασφάλιση της πλήρους λειτουργικότητας Ομάδων Άμεσης Ανταπόκρισης για Συμβάντα που σχετίζονται με την Ασφάλεια Δικτύων και Πληροφοριών (CSIRTs/CERTs), αποτελεί μεταξύ άλλων αναπόσπαστο μέρος του συνολικού σχεδιασμού, αλλά και της εκπλήρωσης των υποχρεώσεων μας ως Κυπριακή Δημοκρατία.

Κύρια λειτουργία ενός CERT 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/CERT 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.

Στα πλαίσια της ευρωπαϊκής συνεργασίας στον τομέα της ασφάλειας των πληροφοριών, εντάσσεται και η συνεργασία των CSIRTs/CERTs που λειτουργούν σε κάθε Κράτος Μέλος. Με στόχο την ένταξη των Κυπριακών CSIRT/CERT στους εν λόγω μηχανισμούς συνεργασίας, θα πρέπει να διασφαλισθεί η πλήρης λειτουργία τους ώστε να εξασφαλισθεί η αναγκαία πιστοποίηση του για να καταστεί δυνατή η συμμετοχή τους στις Ευρωπαϊκές ομάδες εργασίας.

Δράση 10 - Φάση Α - Διασφάλιση της πλήρους λειτουργικότητας των Φορέων Άμεσης Ανταπόκρισης για περιστατικά και συμβάντα που σχετίζονται με την Ασφάλεια Δικτύων και Πληροφοριών (CSIRT/CERT) με άμεση προτεραιότητα την πλήρη λειτουργία του Κυβερνητικού CSIRT/CERT. Θα εξασφαλιστεί επίσης η αναγκαία πιστοποίηση τους και η δυνατότητα συμμετοχής τους στις σχετικές Ευρωπαϊκές ομάδες εργασίας.

Δράση 11 - Φάση Β - Επαναξιολόγηση από το ΓΕΡΗΕΤ, σε συνεργασία με τα CSIRT/CERT, της επέκτασης των δραστηριοτήτων τους ή τη δημιουργία πρόσθετων ομάδων CSIRT/CERT για κάλυψη αναγκών του ιδιωτικού τομέα και της επιχειρηματικής κοινότητας.

3.10 Εθνικές και Διεθνείς Ασκήσεις (Cyber Exercises)

Η μεγάλη ανάγκη συνεργασίας του κράτους με διάφορους φορείς, τόσο του δημόσιου όσο και του ιδιωτικού τομέα, έχει εξεταστεί στις παραγράφους 3.2 και 3.5. Η ανάπτυξη συνεργασίας, και προπάντων η οικοδόμηση εμπιστοσύνης είναι μέγιστης σημασίας.

Όμως, δεν αρκεί μόνο ώστε να δημιουργηθούν μηχανισμοί συνεργασίας, εάν αυτοί οι μηχανισμοί δεν εξετάζονται και δοκιμάζονται σε τακτική βάση, ιδιαίτερα με προσομοίωση καταστάσεων κρίσης. Η διενέργεια τέτοιων ασκήσεων έχει αποδειχτεί 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 έχουν διεξαχθεί μέχρι τώρα σε άλλα κράτη μέλη και επίσης σε Πανευρωπαϊκό επίπεδο, έχουν δείξει ότι αν και σε πολλές περιπτώσεις υπάρχουν οι κατάλληλοι μηχανισμοί αντιμετώπισης μιας τέτοιας κρίσης, το στοιχείο που συνήθως λείπει για να είναι αποτελεσματική η ανταπόκριση σε μια κρίση, είναι οι **λεπτομέρειες του συντονισμού της συνεργασίας** μεταξύ των αρμόδιων φορέων, δηλαδή ποιός θα επικοινωνήσει με ποιόν σε περίπτωση κρίσης, πως ακριβώς επιτυγχάνεται η γρήγορη συνεργασία μεταξύ φορέων, κλπ.

Η ανάγκη διεξαγωγής ασκήσεων για αντιμετώπιση ρεαλιστικών σεναρίων (όπου οι εμπλεκόμενοι φορείς (players) δεν ξέρουν εκ των προτέρων τι θα συμβεί) έχει αναγνωριστεί σε Ευρωπαϊκό επίπεδο και έχει ήδη διεξαχθεί η πρώτη Πανευρωπαϊκή άσκηση (Cyber Europe 2010). 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 αντεπεξέλθει σε σημαντικά συμβάντα στον χώρο της ασφάλειας δικτύων και πληροφοριών που ενδεχομένως να επηρεάσουν μεγάλο μέρος του πληθυσμού.

Σημειώνεται ότι η εμπιστευτικότητα πρέπει να λαμβάνεται υπόψη κατά τη συνεργασία και ανταλλαγή πληροφοριών και εμπειριών με διεθνείς φορείς και ομάδες εργασίας, όπως περιγράφεται στην παράγραφο 3.2 για τη συγκρότηση των ομάδων εργασίας.

Δράση 12 - Φάση Α - Προγραμματισμός και διοργάνωση τακτικών εθνικών ασκήσεων για την κυβερνοασφάλεια, με αυξανόμενα ρεαλιστικά σενάρια, καθώς και ενεργή συμμετοχή σε Πανευρωπαϊκές και άλλες διεθνείς ασκήσεις.

3.11 Ανάπτυξη Ικανοτήτων (Training)

Η κατάλληλη κατάρτιση και η ανάπτυξη ικανοτήτων στον τομέα της ασφάλειας του κυβερνοχώρου είναι απαραίτητη προϋπόθεση για την ομαλή λειτουργία των συστημάτων ασφάλειας, ως επίσης για να εφικτή η σωστή υλοποίηση οποιωνδήποτε δράσεων σχετικά με το θέμα. Η ανάπτυξη των σχετικών ικανοτήτων είναι μείζονος σημασίας και ο στόχος είναι η δημιουργία ενός συνόλου ανθρώπινου

δυναμικού, τόσο εντός όσο και εκτός του δημοσίου τομέα που θα έχει την απαραίτητη τεχνική γνώση και εμπειρία για να υλοποιήσει τις πρόνοιες της στρατηγικής.

Ως εκ τούτου, το κράτος θα υποστηρίξει την κατάλληλη εκπαίδευση προσωπικού στα θέματα ηλεκτρονικής ασφάλειας, μέσω των πιο κάτω ενεργειών:

- Εντοπισμός κατάλληλων και διαθέσιμων εκπαιδευτικών προγραμμάτων και πιστοποιήσεων,
- Προώθηση της αξιοποίησης των προγραμμάτων αυτών εντός του κράτους,
- Δημιουργία ενός συνόλου ανθρώπινου δυναμικού με τις απαραίτητες εξειδικευμένες γνώσεις,
- Ενσωμάτωση σχετικών πιστοποιήσεων και πείρας σε σχέδια υπηρεσίας που έχουν σχέση με την ηλεκτρονική ασφάλεια,
- Προώθηση και στήριξη της δραστηριοποίησης των σχολών ανώτερης και ανώτατης εκπαίδευσης στον Κυπριακό χώρο στον τομέα της ασφάλειας δικτύων και πληροφοριών, μέσω της ενσωμάτωσης θεμάτων ηλεκτρονικής ασφάλειας στα προγράμματα τους και της διεξαγωγής σχετικών ερευνητικών προγραμμάτων.

Τονίζεται ότι η έμφαση σε αυτή τη δράση είναι στην εκπαίδευση επαγγελματιών στον τομέα ηλεκτρονικής ασφάλειας και όχι στην ενημέρωση του κοινού (βλ. παράγραφος 3.12).

Δράση 13 - Φάση Β - 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.

3.12 Κουλτούρα Ασφάλειας (Awareness)

Οι διαστάσεις των πιθανών απειλών για την ηλεκτρονική ασφάλεια, όπως αναπτύχθηκαν στο κεφάλαιο 2.4, δείχνουν καθαρά το ότι το θέμα αυτό θα πρέπει να απασχολεί **όλους** τους χρήστες υποδομών πληροφορίας, καθώς τα σημεία εισόδου κακόβουλων και επιβλαβών δεδομένων/στοιχείων στον τοπικό κυβερνοχώρο τα οποία μπορεί να είναι ένας οποιοσδήποτε συνδεδεμένος ηλεκτρονικός υπολογιστής. Αυτό συμπεριλαμβάνει το σύνολο των πολιτών της Κυπριακής Δημοκρατίας, οι πλείστοι των οποίων κάνουν πλέον τακτική χρήση του Διαδικτύου.

Είναι πολύ σημαντικό οι χρήστες του Διαδικτύου, ως επίσης και οι χρήστες των συστημάτων πληροφορικής σε κάθε χώρο εργασίας να έχουν ένα ικανοποιητικό επίπεδο γνώσεων για τις πιθανές απειλές από τις οποίες πρέπει να προφυλάσσονται.

Η Κυπριακή Δημοκρατία θα προωθήσει ένα Εθνικό Πρόγραμμα Ενημέρωσης για τα θέματα ηλεκτρονικής ασφάλειας, το οποίο θα περιέχει τα ακόλουθα:

- Δημιουργία πληροφοριακού υλικού, καθώς και χρήση διαθέσιμου υλικού από εξωτερικές πηγές (π.χ. ENISA), για τους πολίτες για τα θέματα ασφαλής χρήσης του Διαδικτύου, με

επικέντρωση στην προστασία προσωπικών δεδομένων, σωστή συμπεριφορά στον κυβερνοχώρο και στην προστασία των παιδιών στο Διαδίκτυο,

- Διανομή του εν λόγω πληροφοριακού υλικού με την αξιοποίηση πολλών μέσων, π.χ. τηλεόραση, ραδιόφωνο, SMS, ιστοσελίδες, φυλλάδια/βιβλιαράκια, διαλέξεις, κλπ.
- Δημιουργία εκπαιδευτικών σεμιναρίων μικρής διάρκειας με στόχο τους εργαζόμενους,
- Δημιουργία εξειδικευμένων σεμιναρίων για κυβερνητικούς χρήστες συστημάτων πληροφορίας που εμπεριέχουν ευαίσθητα δεδομένα ή/και διαβαθμισμένα έγγραφα,
- Προώθηση της ανάπτυξης 'κουλτούρας ασφάλειας' σε όλα τα κυβερνητικά τμήματα και υπηρεσίες του κράτους, καθώς και σε ιδιωτικές επιχειρήσεις.

Δράση 14 - Φάση Β - Ανάπτυξη ενός ολοκληρωμένου Εθνικού Προγράμματος Ενημέρωσης (Awareness) για τα θέματα ηλεκτρονικής ασφάλειας που θα καλύπτει όλους τους χρήστες ηλεκτρονικών συστημάτων, από κυβερνητικούς υπάλληλους μέχρι και πολίτες του κράτους.

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.

3.13 Συνεργασία με Διεθνείς Φορείς και Ομάδες Εργασίας

Όπως έχει αναφερθεί εκτενώς και προηγουμένως στην παράγραφο 3.5, η συνεργασία του φορέα υπεύθυνου για την διασφάλιση του κυβερνοχώρου στη Κυπριακή Δημοκρατία δεν αποτελεί απλά επιλογή, αλλά καθίσταται άκρως αναγκαία για την επίτευξη στόχων και επιθυμητών αποτελεσμάτων. Τα προβλήματα και οι απειλές στον κυβερνοχώρο δεν μπορούν να αντιμετωπιστούν επαρκώς από οποιαδήποτε χώρα μεμονωμένα. Επομένως απαιτείτε εποικοδομητική συνεργασία και μεταξύ κρατών σε Ευρωπαϊκό επίπεδο.

Η Κυπριακή Δημοκρατία, μέσω των δραστηριοτήτων του ΓΕΡΗΕΤ αλλά και άλλων αρμόδιων αρχών, ήδη εκπροσωπείται σε μεγάλο βαθμό στις πλείστες σχετικές ομάδες εργασίας και διεθνή φόρα τα οποία λειτουργούν κάτω από την επίβλεψη της Ευρωπαϊκής Επιτροπής και του ENISA. Αναπόσπαστο μέρος της παρούσας στρατηγικής είναι η συνεχείς εκπροσώπηση της Κυπριακής Δημοκρατίας στα εν λόγω φόρα και ομάδες εργασίες, με στόχο την **ενεργή** συμμετοχή και την συμβολή της Κύπρου στις σημαντικές αποφάσεις και στα έργα των ομάδων αυτών. Θα δημιουργηθούν στενοί δεσμοί με τους αντίστοιχους αρμόδιους φορείς σε άλλα κράτη μέλη της Ευρωπαϊκής Ένωσης και θα αξιοποιηθούν οι σύνδεσμοι αυτοί για την διαρκή ανάπτυξη και βελτίωση της στρατηγικής ανταπόκρισης της Κυπριακής Δημοκρατίας στα θέματα ηλεκτρονικής ασφάλειας.

Θα συνεχιστεί επίσης η πλήρης **υποστήριξη των ενεργειών και δράσεων σε κοινοτικό επίπεδο** οι οποίες αποσκοπούν στην **βελτίωση της ηλεκτρονικής ασφάλειας Ευρωπαϊκών υποδομών πληροφορίας**, καθώς και η **συμμετοχή σε άλλες διεθνείς δραστηριότητες και σχετικές ομάδες**[8].

Σημειώνεται ότι η εμπιστευτικότητα πρέπει να λαμβάνεται υπόψη κατά τη συνεργασία και ανταλλαγή πληροφοριών και εμπειριών με διεθνείς φορείς και ομάδες εργασίας, όπως περιγράφεται στην παράγραφο 3.2 για τη συγκρότηση των ομάδων εργασίας.

Δράση 15 - Φάση Α - Θα συνεχιστεί η καλή συνεργασία της Κυπριακής Δημοκρατίας με τα υπόλοιπα κράτη μέλη στην Ευρωπαϊκή Ένωση, 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 ηλεκτρονικής ασφάλειας σε ολόκληρη την Ευρώπη.

3.14 Δημιουργία Σχεδίου Έκτακτης Ανάγκης (Contingency Plan) για τις Κρίσιμες Υποδομές Πληροφορίας

Τα μέτρα και οι δράσεις που έχουν αναφερθεί πιο πάνω θα συνδράμουν σε μεγάλο βαθμό στην μεγάλη βελτίωση της ηλεκτρονικής ασφάλειας στην Κυπριακή Δημοκρατία, συμπεριλαμβανομένου του δημόσιου και του ιδιωτικού τομέα. Η υλοποίηση όλων των δράσεων με οργανωμένο και αποτελεσματικό τρόπο θα βοηθήσει έτσι στην επίτευξη των στόχων για μια πιο ασφαλισμένη ψηφιακή κοινωνία.

Όμως, 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 δημιουργία Σχεδίου Έκτακτης Ανάγκης (Contingency Plan) για τις Κρίσιμες Υποδομές Πληροφορίας. Ο στόχος του σχεδίου αυτού θα 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, όπως θα καθοριστούν στη δράση για τον εντοπισμό κρίσιμων υποδομών πληροφορίας (βλ. παράγραφος 3.6).

Η δημιουργία και ανάπτυξη του Σχεδίου Έκτακτης Ανάγκης θα γίνει ταυτόχρονα με τον εντοπισμό των κρίσιμων υποδομών πληροφορίας της Κυπριακής Δημοκρατίας και θα συμπεριλάβει τις ακόλουθες ενέργειες:

- Την ανάπτυξη κατηγοριών και ιεράρχησης των κρίσιμων υποδομών, βάσει της συμβολής τους στην διατήρηση ζωτικών υπηρεσιών επικοινωνίας και πληροφορίας,

[8] Όπως είναι για παράδειγμα το IMPACT (International Multilateral Partnership Against Cyber Threats).

- Τον καθορισμό του επιπέδου προστασίας που χρειάζεται να έχει το κάθε κομμάτι της υποδομής (π.χ. εφεδρεία, εναλλακτικές οδεύσεις, φυσική ασφάλεια, κλπ.) για να μειωθεί στο ελάχιστο η επιρροή της βλάβης ή καταστροφής τους,
- Την ανάπτυξη συστημάτων και διαδικασιών "early warning" για την παρακολούθηση των υποδομών, ίσως με την βοήθεια των CERTs,
- 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 (βλ. παράγραφος 3.10) για δοκιμασία και βελτίωση των πιο πάνω διαδικασιών,
- Τον καθορισμό όλων των κρίσιμων υποδομών πληροφορίας που περιέχουν συνδέσεις με άλλες χώρες, ή που παρέχουν υπηρεσίες που μπορούν να επηρεάσουν τη λειτουργία υποδομών πληροφορίας σε άλλες χώρες,
- 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.

Ο ENISA έχει ετοιμάσει ένα ολοκληρωμένο έγγραφο[9] με τις βέλτιστες πρακτικές για την ανάπτυξη εθνικών σχεδίων έκτακτης ανάγκης για τις κρίσιμες υποδομές πληροφορίας, το οποίο θα ληφθεί σοβαρά υπόψη για την ανάπτυξη του σχετικού σχεδίου για την Κυπριακή Δημοκρατία, και το οποίο τονίζει έντονα τη σημασία ύπαρξης μιας ολοκληρωμένης στρατηγικής κυβερνοασφάλειας και προστασίας κρίσιμων υποδομών πληροφορίας ως βάση. Σημειώνεται ότι οι πιο πάνω πρόνοιες, όπου υπάρχει ανάγκη, θα αξιοποιηθούν στα πλαίσια της συμβολής της Κύπρου στην εργασία για το καταρτισμό ενός ευρύτερου Ευρωπαϊκού Σχεδίου Έκτακτης Ανάγκης για την προστασία κρίσιμων Ευρωπαϊκών υποδομών πληροφορίας, των οποίων η μη κανονική λειτουργία θα έχει επιπτώσεις σε περισσότερα από ένα μόνο κράτος μέλος.

Δράση 16 - Φάση Α - Ανάπτυξη ενός Εθνικού Σχεδίου Έκτακτης Ανάγκης (Contingency Plan) που θα περιέχει λεπτομερείς διαδικασίες επικοινωνίας και δράσεις σε περίπτωση κρίσης ο οποία επηρεάσει σε μεγάλο βαθμό τις κρίσιμες υποδομές πληροφορίας στην Κυπριακή Δημοκρατία, με σκοπό τη διατήρηση των λειτουργιών που παρέχουν σε αποδεκτά επίπεδα μέχρι την πλήρη αποκατάσταση.

[9] ENISA Good Practice Guide on National Contingency Plans for Critical Information Infrastructure

3.15 Αλληλεξαρτήσεις - Dependencies

Στο παρόν έγγραφο αποδίδεται ιδιαίτερη σημασία στην αλληλεξάρτηση και αλληλοεπίδραση μεταξύ των δράσεων που προτείνονται παρόλο που η κάθε μια έχει τους δικούς της συγκεκριμένους και ξεχωριστούς στόχους, για την επιτυχή έκβαση της. Θα πρέπει το θέμα της στρατηγικής ανταπόκρισης στις απειλές ως προς την ασφάλεια δικτύων και πληροφοριών, 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.

Αλληλεξαρτήσεις διακρίνονται επίσης και σε άλλα επίπεδα αυτής της ανταπόκρισης. Όπως φαίνεται στην παράγραφο 2.3, υπάρχουν διάφορες αρμόδιες αρχές του κράτους που χειρίζονται θέματα ασφάλειας, η κάθε μια στο τομέα αρμοδιότητας της. Παρά το γεγονός ότι πρέπει να αποφεύγονται οι επικαλύψεις, θα πρέπει να αναγνωριστούν οι αλληλεξαρτήσεις και να διασφαλιστεί η συνεργασία μεταξύ τους ώστε να αξιοποιούνται στο μέγιστο βαθμό οι γνώσεις των ειδικών στην κάθε αρχή. Οι αλληλεξαρτήσεις μεταξύ των αρμοδίων αρχών είναι αρκετές, γι' αυτό επιβάλλεται να γίνει σωστή μελέτη για τον εντοπισμό τους, καθώς και η ενσωμάτωση τους σε όποιες μελλοντικές δράσεις ή/και σχέδια έκτακτης ανάγκης δημιουργηθούν.

Επιπλέον, οι χειριστές των κρίσιμων υποδομών πληροφορίας, θα πρέπει να μελετήσουν, ως μέρος των ενεργειών τους για διαχείριση κινδύνων και ρίσκου και για την δημιουργία σχεδίων επιχειρησιακής συνέχειας, τις αλληλεξαρτήσεις που έχουν για τον ασφαλή χειρισμό των υποδομών τους, σε όλα τα επίπεδα. Δηλαδή, να απαντηθούν τα ερωτήματα:

- **Από ποιούς εξαρτάται η επιχείρηση στα θέματα ασφάλειας;**
- **Ποιοι εξαρτώνται από την επιχείρηση στα θέματα ασφάλειας;**

Σημειώνεται ότι μια αρχική εκτίμηση των αλληλεξαρτήσεων μεταξύ των δράσεων του παρόντος εγγράφου παρουσιάζεται στο Παράρτημα ΙΙ.

Δράση 17 - Φάση Α/Β - Εντοπισμός και μελέτη των αλληλεξαρτήσεων που ισχύουν για την υλοποίηση της παρούσας Στρατηγικής. Οι αλληλεξαρτήσεις αυτές εντοπίζονται αρχικά στις σχέσεις μεταξύ των δράσεων, στις σχέσεις μεταξύ των αρμόδιων αρχών του κράτους, και στις σχέσεις των χειριστών κρίσιμων υποδομών με τους προμηθευτές, τους πελάτες και το προσωπικό τους. Οι εξαρτήσεις αυτές θα πρέπει να τύχουν αναγνώρισης και αποδοχής από όλους τους εμπλεκόμενους φορείς.

4. ΕΠΟΜΕΝΑ ΒΗΜΑΤΑ

4.1 Άμεσες Ενέργειες – Φάση Α

Από τις δράσεις που έχουν εντοπιστεί και περιγραφεί στο παρόν έγγραφο, ορισμένες έχει κριθεί ότι η υλοποίηση τους πρέπει να ξεκινήσει άμεσα, ανεξάρτητα από την εξέλιξη και την υλοποίηση των υπολοίπων προνοιών της στρατηγικής ανταπόκρισης. Λαμβάνοντας υπόψη τις ενέργειες που προτεραιοποιούνται στην παράγραφο 3.2, με αναφορά στις συγκεκριμένες δράσεις του σχεδίου στρατηγικής, μέσα στο 2012 θα πρέπει να ξεκινήσει ο εντοπισμός των κρίσιμων υποδομών πληροφορίας (παράγραφος 3.6), η ανάπτυξη Εθνικού Σχεδίου Έκτακτης Ανάγκης για τις υποδομές αυτές (παράγραφος 3.14), η διασφάλιση της πλήρεις λειτουργικότητας των Φορέων Άμεσης Ανταπόκρισης για περιστατικά και συμβάντα που σχετίζονται με την Ασφάλεια Δικτύων και Πληροφοριών (CSIRT/CERT) και ο προγραμματισμός και η συμμετοχή της Κύπρου στην πανευρωπαϊκή άσκηση CyberEurope 2012 (παράγραφος 3.10).

Οι δράσεις που θα διεκπεραιωθούν στη Φάση Α είναι οι ακόλουθες:

- Δράση 1 – Καθορισμός Πλαισίου Συνεργασίας
- Δράση 2 – Μελέτη για Νέα Οργανωτική Δομή
- Δράση 3 (μερική υλοποίηση) – Συγκρότηση Ομάδων Εργασίας
- Δράση 5 (μερική υλοποίηση) – Επισκόπηση του Ιδιωτικού Τομέα
- Δράση 7 – Εντοπισμός Κρίσιμων Υποδομών Πληροφορίας
- Δράση 10 – Διασφάλιση της Πλήρους Λειτουργικότητας των CERTs
- Δράση 12 – Εθνικές και Διεθνείς Ασκήσεις
- Δράση 15 – Διεθνής Συνεργασία
- Δράση 16 – Ανάπτυξη Εθνικού Σχεδίου Έκτακτης Ανάγκης για τις Κρίσιμες Υποδομές Πληροφοριών
- Δράση 17 (μερική υλοποίηση) – Εντοπισμός και Μελέτη Αλληλεξαρτήσεων

Το παρόν έγγραφο παραθέτει συνοπτικά τις πιο σημαντικές δράσεις που έχουν εντοπιστεί για μια σωστή στρατηγική ανταπόκριση, ώστε να διασφαλιστεί ο κυβερνοχώρος και γενικά τα δίκτυα και οι πληροφορίες που χρησιμοποιούνται σε καθημερινή βάση, πλέον από το σύνολο της Κυπριακής κοινωνίας. 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.

4.2 Κοστολόγηση Υλοποίησης Δράσεων

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.

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.

4.3 Προγραμματισμός Δράσεων 2012 – 2015

Οι ενέργειες που αναφέρονται στις ενότητες 4.1 και 4.2 είναι σημαντικές ώστε να προχωρήσει ο σωστός προγραμματισμός των δράσεων της στρατηγικής ανταπόκρισης, βάσει βεβαίως και των πόρων που θα διατεθούν από το κράτος για την υλοποίηση της Στρατηγικής. Ο προγραμματισμός αυτός θα γίνει βάσει των αποτελεσμάτων λεπτομερούς αξιολόγησης, κοστολόγησης και ιεράρχησης των δράσεων σε σχέση με τη προτεραιοποίηση τους, ώστε να προχωρήσει η υλοποίηση της Στρατηγικής Ανταπόκρισης με τον πιο σωστό και αποτελεσματικό τρόπο βάσει των διαθέσιμων πόρων. Το αποτέλεσμα της διαδικασίας αυτής θα είναι ένα αναλυτικό χρονοδιάγραμμα που θα επιτρέπει την παρακολούθηση της υλοποίησης όλων των δράσεων της παρούσας Στρατηγικής.

4.4 Αξιολόγηση Αποτελεσμάτων Εφαρμογής και Αναθεώρηση Σχεδίου Στρατηγικής

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.

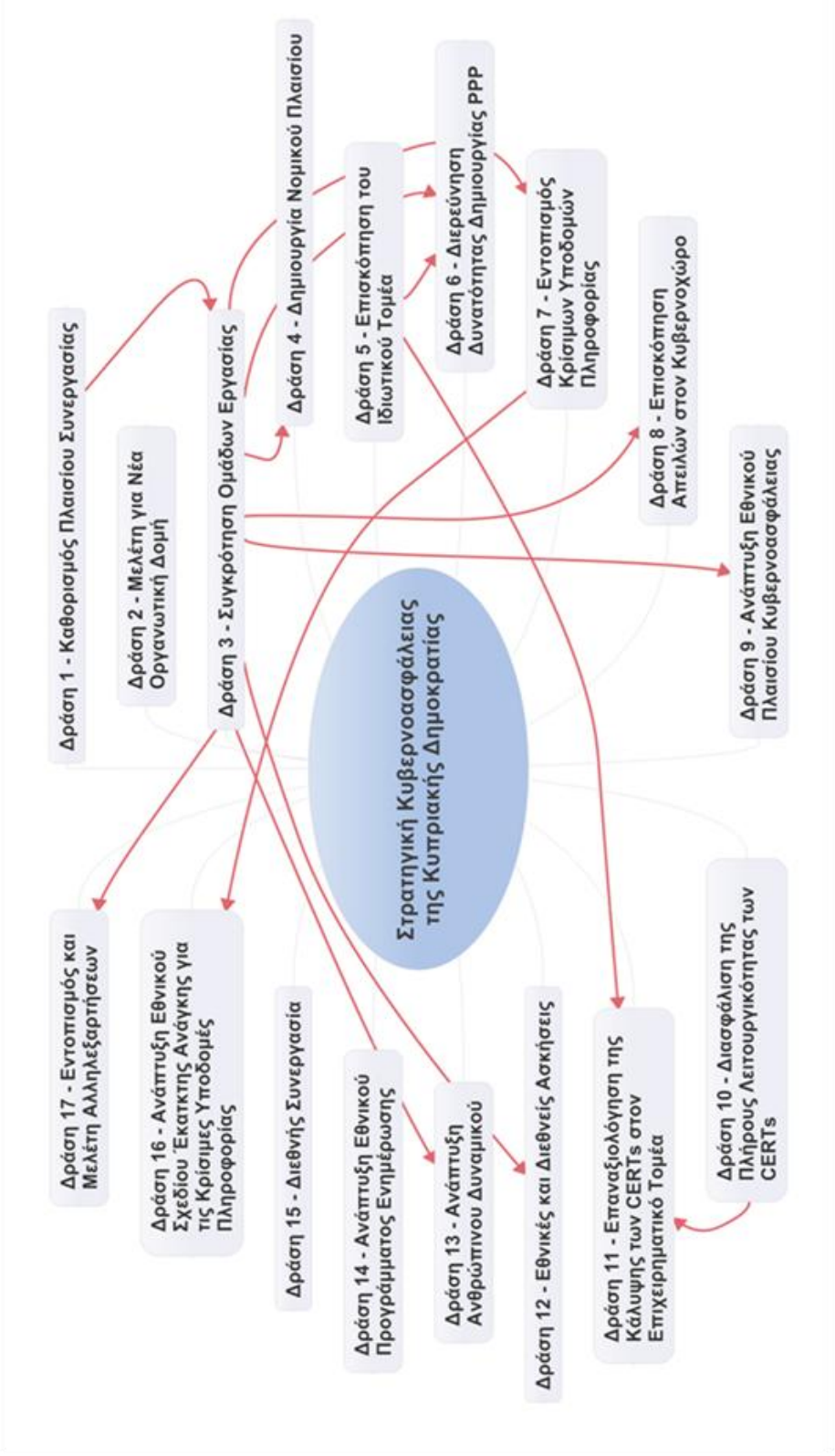
Η λεπτομερής επέκταση των δράσεων της στρατηγικής, όπως αναφέρεται στην παράγραφο 4.1, θα συμπεριλαμβάνει δείκτες και κριτήρια αξιολόγησης για την κάθε δράση, όπου αυτό είναι εφικτό. Τα αποτελέσματα της αξιολόγησης θα επιτρέψουν την ορθή αναθεώρηση της στρατηγικής με σημαντικά ωφελήματα στην Κυπριακή κοινωνία.

ΠΑΡΑΡΤΗΜΑ Ι - ΣΥΝΟΨΗ ΔΡΑΣΕΩΝ

- **Φάση Α**
  - Η Φάση Α θα περιέχει τις δράσεις που το ΓΕΡΗΕΤ είναι σε θέση να ξεκινήσει στο άμεσο μέλλον με τους διαθέσιμους πόρους που έχει στο παρόν στάδιο.
- **Φάση Β**
  - Η Φάση Β περιέχει τις δράσεις που το ΓΕΡΗΕΤ θα είναι σε θέση να συντονίσει αφού εξεταστεί νέα οργανωτική δομή, με τους απαραίτητους πόρους για την επιτυχή διεκπεραίωση της Στρατηγικής στο σύνολο της.

ΠΑΡΑΡΤΗΜΑ ΙΙ - ΑΛΛΗΛΕΞΑΡΤΗΣΕΙΣ ΔΡΑΣΕΩΝ

Το πιο κάτω σχήμα δείχνει ενδεικτικά τις εξαρτήσεις των δράσεων μεταξύ τους. Είναι εμφανής η μεγάλη σημασία της συγκρότησης των Ομάδων Εργασίας για σωστή υλοποίηση της Στρατηγικής.



ΠΑΡΑΡΤΗΜΑ ΙΙΙ - ΑΡΜΟΔΙΕΣ ΑΡΧΕΣ, ΠΑΡΑΤΗΡΗΤΕΣ ΚΑΙ ΝΟΜΟΘΕΣΙΕΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

Αρμόδιες Αρχές

Όνομα Αρχής	Σχετικές Αρμοδιότητες
Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων (ΓΕΡΗΕΤ)	Το ΓΕΡΗΕΤ είναι το κατά νόμο υπεύθυνο Γραφείο όσον αφορά το συντονισμό των θεμάτων της ασφάλειας δικτύων ηλεκτρονικών επικοινωνιών και πληροφοριών στην επικράτεια της Κυπριακής Δημοκρατίας. Η σχετική αρμοδιότητα πηγάζει από το Νόμο 112(Ι)/2004,ως τροποποιείται, (άρθρα 2(2)(ζ)&(ι), 3(2), 18(3)(στ) 19(1), 37(5), 39(2)(ιε), 39(2)(ιστ), 42(6), 55(2)(β), 69(2)(η), 70(4)(β), 80(α), 97, 98, 98Α), και την αρμοδιότητα του ΓΕΡΗΕΤ να εκπροσωπεί την Κύπρο στο Διοικητικό Συμβούλιο του ENISA και να ενεργεί ως κεντρικός σύνδεσμος επικοινωνίας και συντονισμού στην Κύπρο με την υπηρεσία. Στα πλαίσια των αρμοδιοτήτων του αυτών συντονίζει την αμφίδρομη ενημέρωση των κυπριακών αρχών, των ενδιαφερομένων μερών και των καταναλωτών εντός της Κυπριακής Δημοκρατίας με τις αρμόδιες υπηρεσίες της Ευρωπαϊκής Ένωσης για θέματα και δραστηριότητες που αφορούν την ασφάλεια δικτύων και πληροφοριών. Το ΓΕΡΗΕΤ έχει την ευθύνη για την δημιουργία και τον συντονισμό των ενεργειών αρμόδιων φορέων για τον καταρτισμό φορέα/φορέων Άμεσης Ανταπόκρισης για Συμβάντα που σχετίζονται με την Ασφάλεια Δικτύων και Πληροφοριών (CSIRTs - Computer Security Incident Response Teams ή CERTs - Computer Emergency Response Teams), στην Κύπρο. Επίσης ασκεί εποπτεία και έλεγχο της δραστηριότητας των πιο πάνω φορέων - CSIRT/CERT. Το ΓΕΡΗΕΤ θεσπίζει με δευτερογενή νομοθεσία τις ελάχιστες προδιαγραφές ασφάλειας για δημόσια δίκτυα και δίκτυα που προσφέρουν υπηρεσίες ηλεκτρονικών επικοινωνιών σε τρίτα πρόσωπα, και ελέγχει το επίπεδο εφαρμογής των οργανωτικών, διαδικαστικών και τεχνικών μέτρων που λαμβάνονται προς το σκοπό αυτό. Το ΓΕΡΗΕΤ αναλαμβάνει επίσης την ευθύνη του πλαισίου παραλαβής και κοινοποίησης παραβιάσεων ασφάλειας, στα δίκτυα, και την συνεργασία που απαιτείται σε εθνικό επίπεδο αλλά και με άλλα Κράτη Μέλη της Ευρωπαϊκής Ένωσης τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) και την Ευρωπαϊκή Επιτροπή. Επίσης συμβουλεύει τον Υπουργό Συγκοινωνιών για θέματα στρατηγικής στο τομέα της ασφάλειας δικτύων και πληροφοριών συμπεριλαμβανομένου

	της προστασίας Κρίσιμων Υποδομών Πληροφοριών και συντονίζει την εφαρμογή δράσεων για την εφαρμογή της σχετικής πολιτικής του κράτους, καθώς και την ενημέρωση των ενδιαφερομένων μερών και του κοινού στα θέματα ασφάλειας.
	Σχετικές Νομοθεσίες
	Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004, Ν. 112(Ι)/2004, ως τροποποιείται. Το Περί Δημιουργίας Φορέων Άμεσης Ανταπόκρισης για περιστατικά και συμβάντα που σχετίζονται με την Ασφάλεια Δικτύων και Πληροφοριών (CSIRT/CERT), Διάταγμα του 2010 ,Κ.Δ.Π. 358/2010. Το Περί Ασφάλειας Δικτύων και Πληροφοριών Διάταγμα του 2011, Κ.Δ.Π. 253/2011.
Όνομα Αρχής	**Σχετικές Αρμοδιότητες**
Τμήμα Υπηρεσιών Πληροφορικής (ΤΥΠ)	Το Τμήμα Υπηρεσιών Πληροφορικής (ΤΥΠ) του Υπουργείου Οικονομικών είναι: • Ο Αρμόδιος Κυβερνητικός Φορέας για θέματα σχετικά με την προώθηση και εφαρμογή της Πληροφορικής και η-Διακυβέρνησης στο Δημόσιο Τομέα • Η Επιχειρησιακή Αρχή Συστημάτων Πληροφορικής (Information Technology Systems Operational Authority) για τα Υπουργεία και Υπηρεσίες της Κυπριακής Δημοκρατίας • Μέλος της Συμβουλευτικής Επιτροπής Ειδών Διπλής Χρήσης και Στρατιωτικού Εξοπλισμού.
	Σχετικές Νομοθεσίες
	Ο Περί Δημόσιας Υπηρεσίας Νόμος του 1990 (Ν.1(Ι)/1990). Οι περί Κανονισμών Ασφαλείας Διαβαθμισμένων Πληροφοριών, Εγγράφων και Υλικού και για Συναφή Θέματα Νόμοι του 2002 έως 2008 (Ν.216(Ι)/2002, Ν.6(Ι)/2004 και Ν.75(Ι)/2008). Ο Περί της Εισαγωγής και Εξαγωγής Ελεγχόμενων Ειδών και της Διενέργειας Ελεγχόμενων Δραστηριοτήτων Νόμος του 2011 (Ν.1(Ι)/2011).
Όνομα Αρχής	**Σχετικές Αρμοδιότητες**
Αστυνομία Κύπρου	**<u>Τμήμα Ανιχνεύσεως Εγκλημάτων (Γ)</u>** Το Γραφείο Καταπολέμησης Ηλεκτρονικού Εγκλήματος, ΓΚΗΕ, σύμφωνα με τη διοικητική πράξη της Αστυνομίας Κύπρου, Αστυνομική Διάταξη 3/45, αποστολή του είναι η διερεύνηση εγκλημάτων που γίνονται μέσω διαδικτύου και ηλεκτρονικών υπολογιστών κατά παράβαση του Νόμου

	22(III)/2004. Ο εν λόγω νόμος είναι ο νόμος με τον οποίο η Κυπριακή Δημοκρατία κύρωσε τη Σύμβαση του Συμβουλίου της Ευρώπης κατά του Εγκλήματος μέσω του Διαδικτύου που υπογράφτηκε στη Βουδαπέστη στις 23/11/2001. Το Δικανικό Εργαστήριο Ηλεκτρονικών Δεδομένων, ΔΕΗΔ, σύμφωνα με τη διοικητική πράξη της Αστυνομίας Κύπρου, Αστυνομική Διάταξη 3/49, αποστολή του είναι η συλλογή και η δικανική εξέταση ηλεκτρονικών τεκμηρίων και η παρουσίαση επιστημονικής μαρτυρίας στο δικαστήριο. **Τμήμα Τεχνικής και Επιστημονικής Υποστήριξης (Δ)** Η λειτουργία του Κλάδου Τηλεπικοινωνιών διέπεται από την Αστυνομική Διάταξη 2/5. Ο Κλάδος Τηλεπικοινωνιών είναι επιφορτισμένος με την φροντίδα, συντήρηση και ικανοποιητική λειτουργία του τηλεπικοινωνιακού εξοπλισμού της Αστυνομίας. Επίσης παρέχει τεχνική και επιστημονική υποστήριξη στα άλλα τμήματα της Αστυνομίας αναφορικά με τον Τεχνικό Εξοπλισμό. **Τμήμα Μελετών και Ανάπτυξης** Το Τμήμα διατηρεί και διαχειρίζεται Κεντρικό Σύστημα Η.Υ. και Δίκτυο που καλύπτει όλη την ελεύθερη επικράτεια της Κυπριακής Δημοκρατίας. σε Αστυνομικές Διευθύνσεις και Σταθμούς, με τις ανάλογες Εφαρμογές και Βάσεις Δεδομένων, που σχετίζονται με την αποστολή της Αστυνομίας. Επίσης υποστηρίζει Συστήματα ανταλλαγής πληροφοριών που σχετίζονται με την διεθνή αστυνομική συνεργασία, όπως τα Συστήματα της Interpol, Europol και Τρομοκρατίας.
	Σχετικές Νομοθεσίες
	Ο Περί της Σύμβασης κατά του Εγκλήματος μέσω του Διαδικτύου (Κυρωτικός) Νόμος του 2004 (22(III)/2004). Αστυνομική Διάταξη 2/5 Αστυνομική Διάταξη 3/45 Αστυνομική Διάταξη 3/49
Όνομα Αρχής	**Σχετικές Αρμοδιότητες**
Γενικό Επιτελείο Εθνικής Φρουράς (ΓΕΕΦ)	**Αρχή Ασφαλείας Πληροφοριών Τεχνικής Φύσης (INFOSEC)** Ασκεί αρμοδιότητα ως προς τον προσδιορισμό και την εφαρμογή μέτρων ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών και των διαβαθμισμένων πληροφοριών Ευρωπαϊκής Ένωσης, που αποτελούν αντικείμενο επεξεργασίας, αποθήκευσης ή διαβίβασης σε συστήματα επικοινωνιών, επεξεργασίας πληροφοριών ή άλλα ηλεκτρονικά συστήματα, από το ενδεχόμενο να προσβληθεί, τυχαία ή εσκεμμένα η εμπιστευτικότητα η ακεραιότητα ή η διαθεσιμότητα τους από τη μη εξουσιοδοτημένη πρόσβαση χρηστών και την χωρίς άδεια αλλοίωση, εξάλειψη ή τροποποίηση

	τους. **<u>Αρχή Διαπίστευσης Ασφάλειας</u>** Η Αρχή Διαπίστευσης Ασφάλειας (ΑΔΑ), που είναι το Υπουργείο Άμυνας/ Γενικό Επιτελείο Εθνικής Φρουράς και είναι υπεύθυνη για την εξασφάλιση της συμμόρφωσης της πολιτικής ασφάλειας της ΚΔ σε σχέση με τα συστήματα Αυτόματης Επεξεργασίας Δεδομένων (ΑΕΔ), έχει τις παρακάτω αρμοδιότητες: (i) Την έγκριση λειτουργίας ενός συστήματος Αυτόματης Επεξεργασίας Δεδομένων, σε ορισμένο επίπεδο διαβάθμισης (περιλαμβανομένων όπου αρμόζει, ειδικών κατηγοριών διαβάθμισης) στο επιχειρησιακό του περιβάλλον. (ii) Την κατά περίπτωση συγκρότηση επιτροπών διαπίστευσης (Ad Hoc) με τη συμμετοχή των εμπλεκομένων φορέων ή τη μεταβίβαση της αρμοδιότητας αυτής σε κατάλληλους φορείς. Οι φορείς αυτοί είναι δυνατό να προέρχονται από δημόσιους, ημικρατικούς και ιδιωτικούς φορείς. (iii) Τον καθορισμό της πολιτικής ή στρατηγικής διαπίστευσης ως τμήμα της συνολικής πολιτικής της ασφάλειας, που θα αναφέρει σαφώς τις συνθήκες υπό τις οποίες καλείται να διαπιστεύσει ένα σύστημα ΑΕΔ. **<u>Επιχειρησιακή Αρχή Συστημάτων Πληροφορικής (ΙΤΣΟΑ/ΓΕΕΦ)</u>** Ευθύνεται για την εφαρμογή και τη λειτουργία των ελέγχων και των ειδικών μέτρων ασφαλείας ενός συστήματος. Η αρμοδιότητα αυτή ισχύει καθ΄όλη τη διάρκεια του κύκλου ζωής του συστήματος, από το στάδιο του βασικού σχεδιασμού μέχρι την τελική του απόσυρση.
	Σχετικές Νομοθεσίες
	Οι περί Κανονισμών Ασφαλείας Διαβαθμισμένων Πληροφοριών, Εγγράφων και Υλικού και για Συναφή Θέματα Νόμοι του 2002 έως 2008 (Ν.216(Ι)/2002, Ν.6(Ι)/2004 και Ν.75(Ι)/2008). Τα Περί Ασφαλείας Διαβαθμισμένων Πληροφοριών, Έγγραφων και Υλικού της Ευρωπαϊκής Ένωσης Διατάγματα του 2004 (Κ.Δ.Π. 673/2004 και 67/2005).
Όνομα Αρχής	**Σχετικές Αρμοδιότητες**
Εθνική Αρχή Ασφάλειας	Η Εθνική Αρχή Ασφάλειας (ΕΑΑ) έχει την ευθύνη για την εποπτεία και έλεγχο της τήρησης των όρων ασφαλείας που πρέπει να τηρούνται για τις ΔΠ και για τις ΔΠΕΕ. Ειδικότερα οι αρμοδιότητες της ΕΑΑ καθορίζονται λεπτομερώς στο άρθρο 5 του Ν.216(Ι)/2002.
	Σχετικές Νομοθεσίες

	Οι περί Κανονισμών Ασφαλείας Διαβαθμισμένων Πληροφοριών, Εγγράφων και Υλικού και για Συναφή Θέματα Νόμοι του 2002 έως 2008 (Ν.216(Ι)/2002, Ν.6(Ι)/2004 και Ν.75(Ι)/2008).
Όνομα Αρχής	**Σχετικές Αρμοδιότητες**
Κεντρική Υπηρεσία Πληροφοριών (ΚΥΠ)	Η αποστολή της ΚΥΠ περιλαμβάνει: 1. Την ασφάλεια της Κυπριακής Δημοκρατίας από: (α) κατασκοπευτικές δραστηριότητες ξένων οργανώσεων και υπηρεσιών, (β) ενέργειες που τείνουν να υπονομεύσουν τη συνταγματική τάξη και το δημοκρατικό πολίτευμα της χώρας, και (γ) τη διεθνή τρομοκρατία. 2. Τη διαβίβαση στρατηγικών εκτιμήσεων προς την Κυβέρνηση, για λήψη πολιτικών αποφάσεων. 3. Την προστασία της οικονομίας της Κυπριακής Δημοκρατίας και της ευημερίας του λαού. 4. Την πρόληψη, ανίχνευση και καταπολέμηση του σοβαρού εγκλήματος.
	Σχετικές Νομοθεσίες
	Ο Περί Αστυνομίας Νόμος του 2004 (Ν.73(Ι)/2004). Αστυνομική Διάταξη 1/65 της 9ης Ιανουαρίου 2012.
Όνομα Αρχής	**Σχετικές Αρμοδιότητες**
Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα	Για σκοπούς προστασίας των προσωπικών δεδομένων οι υπεύθυνοι επεξεργασίας (όσοι επεξεργάζονται προσωπικά δεδομένα) κοινοποιούν στο Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα τα μέτρα που λαμβάνουν για την ασφάλεια και προστασία των δεδομένων στο έντυπο Γνωστοποίησης Σύστασης και Λειτουργίας Αρχείου / Έναρξης Επεξεργασίας, το οποίο καταχωρείται στο Μητρώο Επεξεργασιών που τηρεί ο Επίτροπος. Η γενική περιγραφή των μέτρων επιτρέπει στους λειτουργούς του Γραφείου του Επιτρόπου να εκτιμήσουν προκαταρκτικά σε κάποιο βαθμό αν τα μέτρα εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας.
	Σχετικές Νομοθεσίες
	Ο περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του

	Ατόμου) Νόμου του 2001 (Νόμος 138(I)/2001), όπως έχει τροποποιηθεί (σχετικά είναι τα άρθρα 7 και 10).
Όνομα Αρχής	**Σχετικές Αρμοδιότητες**
Υπουργείο Συγκοινωνιών και Έργων (ΥΣΕ)	Το Υπουργείο Συγκοινωνιών και Έργων είναι η αρμόδια αρχή στα θέματα πολιτικής στον τομέα της ασφάλειας των δικτύων σύμφωνα με Ν. 112(I)/2004. Επίσης, σύμφωνα με την απόφαση του Υπουργικού Συμβουλίου με αρ. 68.442 και ημερ. 18.2.2009, ο Υπουργός Συγκοινωνιών και Έργων είναι ο πολιτικός υπεύθυνος για την Κοινωνία της Πληροφορίας, με εκτελεστικό βραχίονα το Τμήμα Ηλεκτρονικών Επικοινωνιών.
	Σχετικές Νομοθεσίες
	Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004, Ν. 112(I)/2004, ως τροποποιείται.
Όνομα Αρχής	**Σχετικές Αρμοδιότητες**
Τμήμα Ηλεκτρονικών Επικοινωνιών (ΤΗΕ)	Οι αρμοδιότητες του Τμήματος Ηλεκτρονικών Επικοινωνιών (ΤΗΕ) που σχετίζονται με το περιεχόμενο του εγγράφου στρατηγικής και οι σχετικές νομοθεσίες είναι: (i) Σύμφωνα με την Απόφαση του Υπουργικού Συμβουλίου με αριθμό 68.442 και ημερομηνία 18 Φεβρουαρίου 2009 η πολιτική ευθύνη για την Κοινωνία της Πληροφορίας ανατίθεται στον Υπουργό Συγκοινωνιών και Έργων, με εκτελεστικό βραχίονα, αναφορικά με τη διαμόρφωση και εφαρμογή ολοκληρωμένης εθνικής στρατηγικής, το ΤΗΕ. Με βάση αυτή την Απόφαση το ΤΗΕ σε συνεργασία με τη Συμβουλευτική Επιτροπή για την Κοινωνία της Πληροφορίας ετοίμασε έγγραφο στρατηγικής με τίτλο «Ψηφιακή Στρατηγική της Κύπρου», το οποίο εγκρίθηκε από το Υπουργικό Συμβούλιο με Απόφαση του στις 8/02/2012. Η ασφάλεια δικτύων και πληροφοριών είναι ένα από τα Μέτρα της Ψηφιακής Στρατηγικής της Κύπρου (βλ. Μέτρο 5). (ii) Σύμφωνα με τις πιο κάτω πρόνοιες των περί Ραδιοεπικοινωνιών Νόμων του 2002 μέχρι 2006 ((Ν.146(I)/2002, Ν.15(I)/2003, Ν.16(I)/2004, Ν.180(I)/2004 και Ν.74(I)/2006)), το ΤΗΕ είναι υπεύθυνο για την προστασία των ασύρματων δικτύων ηλεκτρονικών επικοινωνιών από επιβλαβείς παρεμβολές: • Άρθρο 3 Παράγραφος (2) (γ): Ο Υπουργός και ο Διευθυντής εκπληρώνουν τα καθήκοντα τους και ασκούν τις αρμοδιότητες και τις εξουσίες τους, με στόχο την προαγωγή της αποτελεσματικής και δίκαιης διαχείρισης και χρήσης του φάσματος ραδιοσυχνοτήτων, διασφαλίζοντας την αποφυγή

	επιβλαβών παρεμβολών και λαμβάνοντας υπόψη θέματα δημόσιας υγείας ·» και • Άρθρο 4 Παράγραφος (2) (ι): «Ο Διευθυντής έχει τις ακόλουθες εξουσίες αναφορικά με την εφαρμογή του παρόντος Νόμου: λαμβάνει τα κατάλληλα μέτρα για την παρεμπόδιση επιβλαβών παρεμβολών·» Σύμφωνα με την Απόφαση του Υπουργικού Συμβουλίου, το Μάρτιο του 2008, ανατέθηκε στο ΤΗΕ η εφαρμογή του πλαισίου ηλεκτρονικών υπογραφών. Το ΤΗΕ, ως η Αρμόδια Αρχή για την εφαρμογή του πλαισίου ηλεκτρονικών υπογραφών στην Κύπρο, βρίσκεται στη διαδικασία τροποποίησης του υφιστάμενου Νόμου που διέπει τις ηλεκτρονικές υπογραφές (περί του Νομικού Πλαισίου για τις ηλεκτρονικές υπογραφές καθώς και για συναφή θέματα Νόμοι του 2004 - Ν. 188(Ι)/2004, Ν 34(Ι)/2009). Επιπρόσθετα, το ΤΗΕ έχει ετοιμάσει το περί Ηλεκτρονικών Υπογραφών Διάταγμα (Παροχή Υπηρεσιών Αναγνωρισμένης Πιστοποίησης). Το διάταγμα καθορίζει τις διαδικασίες εθελοντικής διαπίστευσης Παροχέων Υπηρεσιών Πιστοποίησης.
	Σχετικές Νομοθεσίες
	Οι περί Ραδιοεπικοινωνιών Νόμοι του 2002 μέχρι 2006 ((Ν.146(Ι)/2002, Ν.15(Ι)/2003, Ν.16(Ι)/2004, Ν.180(Ι)/2004 και Ν.74(Ι)/2006)). Οι περί του Νομικού Πλαισίου για τις ηλεκτρονικές υπογραφές καθώς και για συναφή θέματα Νόμοι του 2004 - Ν. 188(Ι)/2004, Ν 34(Ι)/2009).
Όνομα Αρχής	**Σχετικές Αρμοδιότητες**
Δύναμη Πολιτικής Άμυνας	Με την ψήφιση των περί Προσδιορισμού και Χαρακτηρισμού των Ευρωπαϊκών Υποδομών Ζωτικής Σημασίας και Αξιολόγησης της Ανάγκης Βελτίωσης της Προστασίας τους Κανονισμών του 2012 και τη δημοσίευσή τους στην Επίσημη Εφημερίδα της Δημοκρατίας στις 20/01/2012, η Πολιτική Άμυνα, ως συντονιστική αρχή, έχει αναλάβει, σε συνεργασία με τις αρμόδιες κατά περίπτωση Υπηρεσίες, να προσδιορίζει τις ενδεχόμενες Ευρωπαϊκές Υποδομές Ζωτικής Σημασίας. Σύμφωνα με τους υπό αναφορά Κανονισμούς, Ευρωπαϊκές Υποδομές Ζωτικής Σημασίας ερμηνεύονται ως οι υποδομές ζωτικής σημασίας, που βρίσκονται εντός της Δημοκρατίας και των οποίων η διακοπή λειτουργίας ή η καταστροφή θα είχε σημαντικό αντίκτυπο στη Δημοκρατία και σε ακόμα ένα τουλάχιστον κράτος μέλος. Οι Κανονισμοί εφαρμόζονται στους τομείς της ενέργειας και των μεταφορών και στους υποτομείς αυτών. Στα πλαίσια εφαρμογής των υπό αναφορά Κανονισμών και της Οδηγίας 2008/114/ΕΚ, έχουν ξεκινήσει οι διαδικασίες, ώστε η Πολιτική Άμυνα να

	εγγραφεί στο Δίκτυο Πληροφοριών Προειδοποίησης για τις Υποδομές Ζωτικής Σημασίας – CIWIN, μέσω του οποίου γίνεται η ανταλλαγή πληροφοριών και βέλτιστων πρακτικών, σε σχέση με την ασφάλεια των κρίσιμων υποδομών, μεταξύ των κρατών μελών. Η πρόσβαση στο σύστημα γίνεται με τη χρήση κωδικού σε οποιοδήποτε ηλεκτρονικό υπολογιστή, που είναι συνδεδεμένος με το διαδίκτυο.
	Σχετικές Νομοθεσίες
	Οι περί Προσδιορισμού και Χαρακτηρισμού των Ευρωπαϊκών Υποδομών Ζωτικής Σημασίας και Αξιολόγησης της Ανάγκης Βελτίωσης της Προστασίας τους Κανονισμοί του 2012.
Όνομα Αρχής	**Σχετικές Αρμοδιότητες**
Μονάδα Καταπολέμησης Αδικημάτων Συγκάλυψης (ΜΟΚΑΣ)	Η Μονάδα Καταπολέμησης Αδικημάτων Συγκάλυψης είναι αρμόδια για τη συλλογή και ταξινόμηση πληροφοριών καθώς και διερεύνησης υποθέσεων σε σχέση με υποθέσεις νομιμοποίησης εσόδων από παράνομες δραστηριότητες και υποθέσεις χρηματοδότησης τρομοκρατίας. Η Μονάδα είναι επίσης η Αρχή Ανάκτησης Περιουσιακών Στοιχείων (Asset Recovery Office) της Κύπρου.
	Σχετικές Νομοθεσίες
	Οι Περί της Παρεμπόδισης και Καταπολέμησης της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες Νόμοι του 2007 και 2010.

Παρατηρητές

Όνομα	Σχετικές Αρμοδιότητες
Γενικός Ελεγκτής της Δημοκρατίας	Ο Γενικός Ελεγκτής είναι ο προϊστάμενος της Ελεγκτικής Υπηρεσίας, η οποία, σύμφωνα με το Σύνταγμα, είναι ανεξάρτητη Υπηρεσία της Δημοκρατίας και δεν υπάγεται σε οποιοδήποτε Υπουργείο. Σύμφωνα με το άρθρο 116 του Συντάγματος, ο Γενικός Ελεγκτής, βοηθούμενος από τον Βοηθό Γενικό Ελεγκτή, ελέγχει, εν ονόματι της Δημοκρατίας, κάθε πληρωμή ή είσπραξη και κάθε λογαριασμό χρηματικών διαθεσίμων ή λοιπού ενεργητικού ή υποχρεώσεων που έχουν αναληφθεί από τη Δημοκρατία ή για λογαριασμό της, του οποίου η διαχείριση γίνεται από τη Δημοκρατία ή εν ονόματι αυτής, θεωρώντας και ελέγχοντας συνάμα κάθε τέτοιο λογαριασμό.

Εκτός από τον έλεγχο των Κρατικών Λογαριασμών, ο Γενικός Ελεγκτής έχει την ευθύνη, σύμφωνα με τις διατάξεις ειδικών Νόμων ή διοικητικές διευθετήσεις, για τον έλεγχο των λογαριασμών των Νομικών Προσώπων Δημοσίου Δικαίου ή άλλων Οργανισμών, Ειδικών Ταμείων και των Αρχών Τοπικής Αυτοδιοίκησης.

Οι εξουσίες και τα καθήκοντα του Γενικού Ελεγκτή ασκούνται είτε από τον ίδιο προσωπικά είτε από υπαλλήλους που ενεργούν σύμφωνα με τις οδηγίες του.

Με βάση συνταγματικές και νομικές διατάξεις, ο Γενικός Ελεγκτής οφείλει να εξετάζει τις οικονομικές και άλλες δραστηριότητες των Κυβερνητικών Υπηρεσιών, Νομικών Προσώπων Δημοσίου Δικαίου και Αρχών Τοπικής Αυτοδιοίκησης, για να ικανοποιείται ότι:

(i) Λαμβάνονται όλα τα απαραίτητα μέτρα για την εξασφάλιση της είσπραξης του δημόσιου χρήματος και ότι όλα τα έσοδα εισπράττονται σύμφωνα με τους Νόμους, Κανονισμούς ή άλλες οδηγίες.
(ii) Τα έξοδα διενεργούνται κατά τον πιο οικονομικό και αποτελεσματικό τρόπο.
(iii) Όλα τα ποσά δαπανώνται για τις υπηρεσίες και σκοπούς για τους οποίους παραχωρήθηκαν και ότι η δαπάνη είναι σύμφωνη με τη σχετική εξουσιοδότηση.
(iv) Όλα τα περιουσιακά στοιχεία φυλάγονται κατάλληλα, καταμετρούνται και επαληθεύεται η ύπαρξή τους.

Στα πλαίσια των καθηκόντων της, η Ελεγκτική Υπηρεσία διεξάγει, μεταξύ άλλων, ελέγχους αναφορικά με την ασφάλεια μηχανογραφικών συστημάτων. Ειδικότερα, κατά τον έλεγχο εξετάζονται θέματα τα οποία αφορούν:

(i) Στη φυσική ασφάλεια εξοπλισμού, λογισμικού, δεδομένων και αντιγράφων ασφαλείας.
(ii) Στην πρόσβαση των χρηστών στο σύστημα.
(iii) Στην καταχώριση δεδομένων και στις διαδικασίες εσωτερικού ελέγχου αναφορικά με την ορθότητα των καταχωρίσεων.
(iv) Στη διαχείριση των προβλημάτων που εντοπίζονται στη λειτουργία των συστημάτων από τους χρήστες.
(v) Στις διαδικασίες που αφορούν τυχόν τροποποιήσεις ή/και αναβαθμίσεις στο λογισμικό.
(vi) Στις διαδικασίες εντοπισμού/αναγνώρισης και διαχείρισης κινδύνων.
(vii) Στην ετοιμασία εξειδικευμένων σχεδίων αντιμετώπισης εκτάκτων αναγκών.
(viii) Στην εκπαίδευση των διαχειριστών των συστημάτων, των ομάδων υποστήριξης και των χρηστών.
(ix) Στην ενημέρωση/αναθεώρηση των εγχειριδίων χρήσης των συστημάτων.

Σχετικές Νομοθεσίες

Το Σύνταγμα της Κυπριακής Δημοκρατίας - ΜΕΡΟΣ VI, ΚΕΦΑΛΑΙΟ II – Γενικός Ελεγκτής και Βοηθός Γενικός Ελεγκτής, άρθρα 115 – 117.

Ο περί της Καταθέσεως Στοιχείων και Πληροφοριών στο Γενικό Ελεγκτή της Δημοκρατίας Νόμος του 2002. Οι κύριες πρόνοιες του Νόμου, ο οποίος τέθηκε σε εφαρμογή στις 12.7.2002, είναι οι ακόλουθες:

> Ο Γενικός Ελεγκτής έχει εξουσία να ζητά οποιαδήποτε στοιχεία ή πληροφορίες σε οποιαδήποτε μορφή, περιλαμβανομένης και της ηλεκτρονικής μορφής, και οποιεσδήποτε γραπτές ή προφορικές εξηγήσεις που κατά την κρίση του είναι αναγκαίες για τον έλεγχο, από τους Υπουργούς, τους δημόσιους υπαλλήλους, τους Προέδρους, τα μέλη των Συμβουλίων και τους υπαλλήλους των νομικών προσώπων δημοσίου δικαίου, τους Δημάρχους, τους Κοινοτάρχες, τα μέλη των Δημοτικών και Κοινοτικών Συμβουλίων και τους υπαλλήλους τους, τους αξιωματούχους και τους υπαλλήλους των διάφορων Υπηρεσιών της Δημοκρατίας, άλλων αρχών ή Συμβουλίων που συστάθηκαν ή θα συσταθούν με Νόμο ή από άλλους Οργανισμούς, οι οποίοι ελέγχονται από το Γενικό Ελεγκτή.

Όλα τα πιο πάνω πρόσωπα οφείλουν:

(i) Να μη δίνουν ψευδή στοιχεία και πληροφορίες.
(ii) Να μην αποκρύπτουν οποιεσδήποτε πληροφορίες ή στοιχεία.
(iii) Να μην εμποδίζουν την πλήρη και ελεύθερη πρόσβαση στα σχετικά αρχεία.
(iv) Να μην επηρεάζουν οποιοδήποτε πρόσωπο, το οποίο πρόκειται να δώσει στοιχεία ή πληροφορίες.
(v) Να μην υποκινούν οποιοδήποτε πρόσωπο για απόκρυψη στοιχείων.
(vi) Παράβαση των πιο πάνω συνεπάγεται φυλάκιση μέχρι και ένα χρόνο ή/και πρόστιμο μέχρι £1.000.

Με βάση τον ίδιο νόμο ο Γενικός Ελεγκτής έχει εξουσία να απαιτήσει από οποιοδήποτε πρόσωπο, το οποίο λαμβάνει χορηγία/εγγύηση/δάνειο από το Πάγιο Ταμείο ή άλλο Ταμείο του Δημοσίου, όπως παράσχει σ' αυτόν όλα τα απαιτούμενα στοιχεία, για εξακρίβωση του τρόπου διάθεσης του σχετικού ποσού.

Επίσης κατοχυρώνεται και νομικά η εξουσία του Γενικού Ελεγκτή να διεξάγει διαχειριστικό έλεγχο σε οποιοδήποτε ελεγχόμενο Οργανισμό, για να διαπιστώσει αν αυτός λειτουργεί και χρησιμοποιεί τους διαθέσιμους πόρους του με οικονομικό, αποδοτικό και αποτελεσματικό τρόπο.

Οι περί Νομικών Προσώπων Δημοσίου Δικαίου (Έλεγχος Λογαριασμών) Νόμοι του 1983 έως 2007 (Ημικρατικοί Οργανισμοί)

Σύμφωνα με τους πιο πάνω Νόμους, ο Γενικός Ελεγκτής ανέλαβε την ευθύνη του ετήσιου ελέγχου των λογαριασμών όλων των Νομικών Προσώπων Δημοσίου Δικαίου (Ημικρατικών Οργανισμών) για τους οποίους δεν γινόταν ειδική μνεία στη νομοθεσία τους ότι ελέγχονται από το Γενικό Ελεγκτή.

Οι λογαριασμοί του ΝΠΔΔ πρέπει να ετοιμάζονται μέχρι το τέλος Φεβρουαρίου του έτους που έπεται του έτους στο οποίο αφορά ο διεξαγόμενος έλεγχος.

Ο Γενικός Ελεγκτής πρέπει να ολοκληρώσει τον έλεγχο και να υποβάλει τους ελεγμένους λογαριασμούς μαζί με την έκθεσή του μέχρι το τέλος Μαΐου, η οποία κατατίθεται στη Βουλή των Αντιπροσώπων μέχρι τις 15 Ιουνίου.

Με βάση τη σχετική Νομοθεσία, οι Οργανισμοί αυτοί μπορούν να διορίζουν και ιδιώτες ελεγκτές, νοουμένου ότι ο διορισμός και η αμοιβή τους εγκρίνεται από το Γενικό Ελεγκτή.

Σε αυτή την περίπτωση οι ιδιώτες ελεγκτές πρέπει να υποβάλουν την έκθεσή τους, μαζί με τους ελεγμένους λογαριασμούς, στο Γενικό Ελεγκτή, μέχρι τις 30 Απριλίου. Ο Γενικός Ελεγκτής μπορεί να διεξαγάγει, κατά την κρίση του, επιπρόσθετο διαχειριστικό ή άλλο έλεγχο.

Οι περί Δήμων Νόμοι του 1985 μέχρι 1997

Όλοι οι Δήμοι πρέπει να τηρούν κατάλληλα λογιστικά βιβλία και να ετοιμάζουν οικονομικές καταστάσεις μέχρι τις 30 Απριλίου του έτους που έπεται του έτους στο οποίο αφορά ο διεξαγόμενος έλεγχος.

Οι οικονομικές καταστάσεις, αφού πιστοποιηθούν από το Δήμαρχο και το Δημοτικό Ταμία, υποβάλλονται για έλεγχο στο Γενικό Ελεγκτή. Οι ελεγμένες οικονομικές καταστάσεις υποβάλλονται από το Γενικό Ελεγκτή, μαζί με την έκθεσή του, στο Δημοτικό Συμβούλιο, τη Βουλή των Αντιπροσώπων και τον Υπουργό Εσωτερικών, ο οποίος μεριμνά για τη δημοσίευση τους στην Επίσημη Εφημερίδα.

Ο Γενικός Ελεγκτής έχει την εξουσία να ζητά οποιαδήποτε πληροφορία ή εξήγηση από οποιοδήποτε μέλος του Συμβουλίου ή Δημοτικό υπάλληλο και το δικαίωμα πρόσβασης σε οποιοδήποτε πρακτικό, λογαριασμό, συμβόλαιο, τιμολόγιο ή άλλο έγγραφο, για σκοπούς ελέγχου.

Ο περί Κοινοτήτων Νόμος του 1999 (Ν.86(Ι)/99).

Σύμφωνα με το Νόμο, κάθε Κοινοτικό Συμβούλιο πρέπει να τηρεί κατάλληλα λογιστικά βιβλία και να ετοιμάζει οικονομικές καταστάσεις μέχρι το τέλος Μαρτίου του έτους που έπεται του οικονομικού έτους στο οποίο αφορά ο διεξαγόμενος έλεγχος.

	Οι οικονομικές καταστάσεις υποβάλλονται για έλεγχο στο Γενικό Ελεγκτή. Οι ελεγμένες οικονομικές καταστάσεις υποβάλλονται στον οικείο Έπαρχο, μαζί με την Έκθεση και τις παρατηρήσεις του Γενικού Ελεγκτή. Επιπρόσθετα από τον ετήσιο οικονομικό έλεγχο, ο Γενικός Ελεγκτής μπορεί κατά την κρίση του να διεξαγάγει οποιοδήποτε διαχειριστικό ή άλλο έλεγχο.
Όνομα	**Σχετικές Αρμοδιότητες**
Υπηρεσία Εσωτερικού Ελέγχου	Ο Έφορος Εσωτερικού Ελέγχου έχει την εξουσία να εξετάζει και να αξιολογεί την επάρκεια και αποτελεσματικότητα των συστημάτων εσωτερικού ελέγχου καθώς επίσης και του περιβάλλοντος πληροφοριών των ελεγχόμενων οργανισμών. Με βάση το άρθρο 10 του πιο κάτω νόμου, ο Έφορος και η Υπηρεσία Εσωτερικού Ελέγχου είναι ανεξάρτητη και δεν επιτρέπεται να έχουν οποιαδήποτε άμεση ή έμμεση αρμοδιότητα για, ή εξουσία πάνω, στις δραστηριότητες που αποτελούν αντικείμενο ελέγχου ούτε να συμμετέχουν σε οποιαδήποτε απόφαση εκτελεστικής φύσεως.
	Σχετικές Νομοθεσίες
	Ο Περί Εσωτερικού Ελέγχου Νόμος Ν.114(Ι) του 2003.
Όνομα	**Σχετικές Αρμοδιότητες**
Κεντρική Τράπεζα της Κύπρου	Η Κεντρική Τράπεζα της Κύπρου αποτελεί αναπόσπαστο μέρος του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών και ενεργεί καθ'όσον αφορά τις αρμοδιότητες του εν λόγω Συστήματος σύμφωνα με τις κατευθυντήριες γραμμές και οδηγίες της Ευρωπαϊκής Κεντρικής Τράπεζας. Βασικές αρμοδιότητες της Κεντρικής Τράπεζας, μεταξύ άλλων, είναι οι ακόλουθες: (i) Η εποπτεία των τραπεζών (ii) η διασφάλιση της σταθερότητας του χρηματοοικονομικού συστήματος (iii) η προώθηση, ρύθμιση και επίβλεψη της ομαλής λειτουργίας των συστημάτων πληρωμών, εκκαθάρισης ή και διακανονισμού συναλλαγών (iv) η συλλογή, επεξεργασία και διανομή στατιστικών στοιχειών. Η ύπαρξη μιας ασφαλούς υποδομής πληροφοριών είναι καθοριστική για τη διαφύλαξη των πιο πάνω.
	Σχετικές Νομοθεσίες

	Οι Περί της Κεντρικής Τράπεζας της Κύπρου Νόμοι του 2002 έως 2007. Οι Περί του Πλαισίου Αρχών Λειτουργίας & Κριτηρίων Αξιολόγησης της Οργανωτικής Δομής, Εσωτερικής Διακυβέρνησης και των Συστημάτων Εσωτερικού Ελέγχου των Τραπεζών Οδηγίες του 2006 έως 2012.