ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ
Αθήνα, 07/03/2018
Α.Π.: 3218/2018

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ,
ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΕΝΗΜΕΡΩΣΗΣ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
Δ/νση: Φραγκούδη 11 και Αλ. Πάντου
Τ.Κ.: 101 63 Αθήνα
Πληρ.: ΛΕΑΝΔΡΟΣ ΜΑΓΛΑΡΑΣ
Τηλ.: 210 90988275
Email: l.maglaras@gsdp.gr
Φαξ: 210 9098 433 ή 213-1318433

Θέμα: Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας

Α Π Ο Φ Α Σ Η

Ο Υπουργός Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης

Έχοντας υπόψη:

α. το άρθρο 15 του π.δ. 82/2017 «Οργανισμός του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης» (Α΄ 117),

β. το αρ.159 του Κεφαλαίου Ι΄ του Ν.4389/2016 «Σύσταση Γενικής Γραμματείας Ψηφιακής Πολιτικής» (Α΄ 94),

γ. το αρ.4 του π.δ. 123/2016 (Α΄ 208) «Σύσταση Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης και Μετονομασία Υπουργείου Υποδομών, Μεταφορών και Δικτύων»,

δ. το π.δ. 125/2016 (Α΄ 210) «Διορισμός Υπουργών, Αναπληρωτών Υπουργών και Υφυπουργών»,

ε. την Εθνική Ψηφιακή Στρατηγική 2016-2021,

στ. την από 21-9-2017 αναρτημένη Εθνική Στρατηγική Κυβερνοασφάλειας (Αναθεώρηση 2) στον Ευρωπαϊκό Οργανισμό ENISA,

ζ. το από 16-2-2018 Υπηρεσιακό Σημείωμα του Αν. Προϊσταμένου Διεύθυνσης Κυβερνοασφάλειας της Γενικής Γραμματείας Ψηφιακής Πολιτικής.

ΑΠΟΦΑΣΙΖΟΥΜΕ

Την έγκριση της ακόλουθης Εθνικής Στρατηγικής Κυβερνοασφάλειας (Αναθεώρηση 3), σύμφωνα με τις διατάξεις του αρ.15 του π.δ.82/2017 (Α΄ 117).

Ο Υπουργός Ψηφιακής Πολιτικής,Τηλεπικοινωνιών και Ενημέρωσης

Νικόλαος Παππάς

ΑΚΡΙΒΕΣ ΑΝΤΙΓΡΑΦΟ
Η Προϊσταμένη του Τμήματος
Γραμματειακής Υποστήριξης
του Υπουργείου Ψηφιακής Πολιτικής,
Τηλεπικοινωνιών και Ενημέρωσης

Ελένη Χρόνη

ELENI CHRONI
07/03/2018 11:59:26

ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

- ΑΝΑΘΕΩΡΗΣΗ 3 -

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΣΥΝΟΨΗ

Στο παρόν κείμενο περιγράφεται η Εθνική Στρατηγική Κυβερνοασφάλειας, μέσω της οποίας αναπτύσσεται ο κεντρικός σχεδιασμός της Ελληνικής Πολιτείας αναφορικά με τον τομέα της ασφάλειας στον κυβερνοχώρο.

Δεδομένου ότι η χρήση του Διαδικτύου και των Τεχνολογιών Πληροφορικής και Επικοινωνιών συνεχώς αυξάνει σε κάθε πτυχή των δραστηριοτήτων του δημόσιου και του ιδιωτικού τομέα, ιδιαίτερη προσοχή πρέπει να δοθεί στην δημιουργία ενός ασφαλούς περιβάλλοντος Διαδικτύου, υποδομών και υπηρεσιών, που θα τονώσει την εμπιστοσύνη των πολιτών και θα τους οδηγήσει στην περαιτέρω χρήση νέων ψηφιακών προϊόντων και υπηρεσιών. Το ασφαλές περιβάλλον μαζί με την προώθηση των νέων υπηρεσιών και προϊόντων από τη μια και η διασφάλιση των προσωπικών δεδομένων και των δικαιωμάτων των πολιτών στον νέο ψηφιακό κόσμο από την άλλη, θεωρούνται βασικές προϋποθέσεις τόνωσης και προώθησης της οικονομικής ανάπτυξης στη χώρα μας.

Με τη θέσπιση της Εθνικής Στρατηγικής Κυβερνοασφάλειας ορίζονται οι βασικές αρχές για τη δημιουργία ενός ασφαλούς διαδικτυακού περιβάλλοντος στην Ελλάδα, τίθενται οι στρατηγικοί στόχοι και το πλαίσιο δράσεων μέσω του οποίου αυτοί θα εκπληρωθούν. Οι στόχοι και οι επιμέρους δράσεις προς επίτευξη αυτών περιγράφονται αναλυτικά στο παρόν.

Την εφαρμογή της Εθνικής Στρατηγικής Κυβερνοασφάλειας αναλαμβάνει η Εθνική Αρχή Κυβερνοασφάλειας, η οποία δημιουργείται για να καλύψει το οργανωτικό και συντονιστικό κενό ανάμεσα στους φορείς που δραστηριοποιούνται στην Ελλάδα στον τομέα της ασφάλειας στον κυβερνοχώρο, τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα. Επιπλέον, η Εθνική Αρχή Κυβερνοασφάλειας θα αποτιμά, θα αναθεωρεί και θα επικαιροποιεί την Εθνική Στρατηγική Κυβερνοασφάλειας εφόσον είναι αναγκαίο και το αργότερο κάθε τριετία.

1. ΕΙΣΑΓΩΓΗ

Η αυξανόμενη χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνιών ΤΠΕ επιτρέπει την ταχύτατη μεταφορά, επεξεργασία και αποθήκευση τεράστιου όγκου δεδομένων την οποία οι σημερινές κοινωνίες εκμεταλλεύονται όλο και περισσότερο προς όφελος της οικονομικής, κοινωνικής, τεχνολογικής, πολιτιστικής και επιστημονικής τους ανάπτυξης. Παράλληλα η διάδοση του διαδικτύου προσφέρει την άμεση πρόσβαση στα δεδομένα αυτά και την ανταλλαγή πληροφοριών μεταλλάσσοντας ριζικά την κοινωνική και οικονομική ζωή. Η οικονομία, το εμπόριο και οι επιχειρήσεις βασίζονται όλο και περισσότερο στις ψηφιακές υποδομές για την περαιτέρω ανάπτυξή τους. Η Δημόσια Διοίκηση προσβλέπει στην ψηφιακή τεχνολογία, ως μέσο βελτίωσης των παρεχόμενων υπηρεσιών και της ορθολογικής χρήσης των πληροφοριακών πόρων της. Η ανοιχτή και ελεύθερη πρόσβαση στο διαδίκτυο, η εμπιστευτικότητα, η ακεραιότητα, διαθεσιμότητα και ανθεκτικότητα των συστημάτων ΤΠΕ αποτελούν τη βάση της ευημερίας, της εθνικής ασφάλειας αλλά και της διασφάλισης των θεμελιωδών δικαιωμάτων και ελευθεριών.

Καθώς η κοινωνία μας εξαρτάται όλο και περισσότερο από τα συστήματα επικοινωνιών και πληροφορικής, η ασφάλειά τους αποτελεί πλέον μείζον θέμα εθνικού ενδιαφέροντος, ενώ ταυτόχρονα παρατηρείται μία συνεχώς αυξανόμενη ανάγκη για προστασία των χρηστών ψηφιακών υπηρεσιών και ιδίως νεαρής ηλικίας. Ο όρος “κυβερνοασφάλεια” αναφέρεται σε όλες εκείνες τις δράσεις και τις ενέργειες που ενδείκνυνται και πρέπει να γίνουν, προκειμένου να διασφαλιστεί η προστασία του κυβερνοχώρου από εκείνες τις απειλές που είναι άμεσα συνυφασμένες με αυτόν και που μπορούν να βλάψουν τα αλληλοεξαρτώμενα συστήματα Τεχνολογιών Πληροφορικής και Επικοινωνιών ΤΠΕ. Η Εθνική Στρατηγική Κυβερνοασφάλειας αποτελεί εργαλείο για τη βελτίωση της διαδικτυακής ασφάλειας, εξασφαλίζοντας την ακεραιότητα, διαθεσιμότητα και ανθεκτικότητα των κρίσιμων υποδομών και την εμπιστευτικότητα της διακινούμενης ψηφιακής πληροφορίας, διασφαλίζοντας, παράλληλα, τις αρχές της ανοιχτής κοινωνίας, τις συνταγματικές ελευθερίες και τα ατομικά δικαιώματα.

2. ΓΕΝΙΚΕΣ ΑΡΧΕΣ ΚΑΙ ΣΤΟΧΟΙ

Η ανάπτυξη και θωράκιση των ψηφιακών υπηρεσιών και αγορών αποτελεί βασικό άξονα στήριξης της εθνικής οικονομίας και προσφέρει ανταγωνιστικό πλεονέκτημα τόσο σε εθνικό όσο και σε Ευρωπαϊκό επίπεδο. Καθώς η χώρα μας συνεχίζει να αναπτύσσεται και να επενδύει στους τομείς των ψηφιακών αγορών, δικτύων και υπηρεσιών τόσο του ιδιωτικού όσο και του Δημόσιου τομέα καθίσταται απαραίτητη η δημιουργία Εθνικής Στρατηγικής Κυβερνοασφάλειας. Βασικές αρχές της Εθνικής Στρατηγικής Κυβερνοασφάλειας αποτελούν:

Α. Η ανάπτυξη και εδραίωση ενός ασφαλούς και ανθεκτικού κυβερνοχώρου ο οποίος θα ρυθμίζεται στη βάση εθνικών, ευρωπαϊκών και διεθνών κανόνων, προτύπων και ορθών πρακτικών και στον οποίο οι πολίτες, και οι φορείς του δημόσιου και ιδιωτικού τομέα θα δραστηριοποιούνται και θα αλληλεπιδρούν με ασφάλεια, σύμφωνα με τις αξίες που διέπουν ένα κράτος δικαίου, όπως, ενδεικτικά, της ελευθερίας, της δικαιοσύνης και της διαφάνειας.

Β. Η συνεχής βελτίωση των δυνατοτήτων μας στην προστασία από κυβερνοεπιθέσεις με έμφαση στις κρίσιμες υποδομές και η διασφάλιση της επιχειρησιακής συνέχειας.

Γ. Η θεσμική θωράκιση του εθνικού πλαισίου κυβερνοασφάλειας, για την αποτελεσματική αντιμετώπιση περιστατικών κυβερνοεπιθέσεων και την ελαχιστοποίηση των επιπτώσεων από απειλές στον κυβερνοχώρο.

Δ. Η ανάπτυξη ισχυρής κουλτούρας ασφάλειας των πολιτών, του δημόσιου και ιδιωτικού τομέα, αξιοποιώντας τις σχετικές δυνατότητες της ακαδημαϊκής κοινότητας και εν γένει των φορέων του δημόσιου και ιδιωτικού τομέα.

Οι επιμέρους στόχοι της Εθνικής Στρατηγικής Κυβερνοασφάλειας συνοψίζονται σε:

Αναβάθμιση του επιπέδου πρόληψης, αξιολόγησης, ανάλυσης και αποτροπής των απειλών για την ασφάλεια των συστημάτων και υποδομών ΤΠΕ.

1. Ενίσχυση της ικανότητας των φορέων του δημόσιου και ιδιωτικού τομέα στην πρόληψη και την αντιμετώπιση των συμβάντων κυβερνοασφάλειας, στην βελτίωση της ανθεκτικότητας και στη δυνατότητα ανάκτησης των συστημάτων ΤΠΕ έπειτα από κυβερνοεπιθέσεις.
2. Η δημιουργία ενός αποτελεσματικού πλαισίου συντονισμού και συνεργασίας με τον καθορισμό των επιμέρους αρμοδιοτήτων και ρόλων των εμπλεκόμενων φορέων του δημόσιου και ιδιωτικού τομέα για την εφαρμογή της Εθνικής Στρατηγικής Κυβερνοασφάλειας.
3. Ενεργό συμμετοχή της χώρας στις διεθνείς πρωτοβουλίες και δράσεις κυβερνοασφάλειας των διεθνών οργανισμών για την ενίσχυση της εθνικής ασφάλειας.
4. Ευαισθητοποίηση όλων των κοινωνικών φορέων και ενημέρωση των χρηστών για ασφαλή χρήση του κυβερνοχώρου.
5. Συνεχή προσαρμογή του εθνικού θεσμικού πλαισίου στις νέες τεχνολογικές απαιτήσεις και στις Ευρωπαϊκές κατευθύνσεις για την αποτελεσματική καταπολέμηση παράνομων πράξεων που είναι συνυφασμένες με τη δράση στον κυβερνοχώρο.
6. Προώθηση της καινοτομίας, της έρευνας και της ανάπτυξης σε θέματα ασφάλειας και της συνεργασίας των εμπλεκομένων φορέων.
7. Αξιοποίηση βέλτιστων διεθνών πρακτικών.

Η υιοθέτηση, η εφαρμογή και η εποπτεία της Εθνικής Στρατηγικής Κυβερνοασφάλειας θα συμβάλει στη δημιουργία ενός ισχυρού κράτους δικαίου, με υψηλό επίπεδο ασφάλειας και βαθμό ανθεκτικότητας στις κυβερνοαπειλές, με σεβασμό στα προσωπικά δεδομένα, στα ατομικά και κοινωνικά δικαιώματα, το οποίο θα παρέχει ποιοτικές ηλεκτρονικές υπηρεσίες σε πολίτες και επιχειρήσεις ενώ παράλληλα θα λειτουργήσει και σαν μοχλός ανάπτυξης των

επιχειρήσεων και της οικονομίας, θέτοντας κοινούς κανόνες προς όλους τους εμπλεκόμενους φορείς.

3. ΠΛΑΙΣΙΟ ΔΡΑΣΕΩΝ – ΣΤΡΑΤΗΓΙΚΟΙ ΣΤΟΧΟΙ

Η Εθνική Στρατηγική Κυβερνοασφάλειας περιλαμβάνει δύο επιμέρους φάσεις. Την ανάπτυξη και υλοποίηση της Στρατηγικής σε πρώτο στάδιο και την αξιολόγηση και αναθεώρηση της σε δεύτερο στάδιο. Οι φάσεις αυτές ορίζουν έναν συνεχή κύκλο ζωής, με την έννοια ότι η Εθνική Στρατηγική πρώτα αναπτύσσεται και υλοποιείται, στην συνέχεια αξιολογείται, βάσει προκαθορισμένων δεικτών αξιολόγησης και, εφόσον κριθεί απαραίτητο, αναθεωρείται και επικαιροποιείται.

Οι εμπλεκόμενοι φορείς κατανέμονται σε δύο επίπεδα, στο στρατηγικό και στο επιχειρησιακό. Η Εθνική Αρχή Κυβερνοασφάλειας, η οποία σύμφωνα με το Προεδρικό Διάταγμα 82/2017 (Α΄ 117) συστάθηκε και λειτουργεί στην Γενική Γραμματεία Ψηφιακής Πολιτικής του Υπουργείου Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης, αποτελεί ένα φορέα υψηλού πολιτικού-κυβερνητικού επιπέδου με διευρυμένες αρμοδιότητες, παρακολουθεί, υλοποιεί και φέρει τη συνολική ευθύνη της Εθνικής Στρατηγικής Κυβερνοασφάλειας. Η Εθνική Αρχή Κυβερνοασφάλειας, δύναται να ασκεί τις αρμοδιότητές της με τη συνδρομή ενός Εθνικού Συμβουλευτικού Οργάνου / Φόρουμ, στο οποίο θα συμμετέχουν εμπλεκόμενοι φορείς δημόσιου και ιδιωτικού τομέα, και σε στενή συνεργασία με το εθνικό Computer Emergency Response Team (CERT). Στο πλαίσιο των αρμοδιοτήτων της θα παρακολουθεί, συντονίζει και αξιολογεί το έργο των εμπλεκόμενων φορέων προς επίτευξη των στρατηγικών δράσεων – στόχων. Στο επιχειρησιακό επίπεδο ανήκουν, μεταξύ άλλων, οι ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Teams — CSIRT), γνωστές επίσης ως «ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική» (Computer Emergency Response Teams — CERT) του δημοσίου και του ιδιωτικού τομέα, επιφορτισμένα με την αντιμετώπιση των κυβερνοπεριστατικών (κυβερνοάμυνα) στο πλαίσιο των αρμοδιοτήτων τους.

Στη συνέχεια ορίζεται το πλαίσιο των απαιτούμενων δράσεων για την υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας:

3.1. Ορισμός των Φορέων που συμμετέχουν στην Εθνική Στρατηγική Κυβερνοασφάλειας – Αποτύπωση φορέων (stake holders)

Η Εθνική Στρατηγική αφορά κυρίως στους σημαντικούς, για την εύρυθμη λειτουργία της κοινωνίας, φορείς.

Είναι συναφώς, απαραίτητος ο σαφής καθορισμός των εμπλεκόμενων, δημόσιων και ιδιωτικών φορέων, που θα συμβάλουν στην ανάπτυξη και υλοποίηση της εθνικής στρατηγικής.

3.2. Ορισμός των Κρίσιμων Υποδομών

Ορισμός και καταγραφή των Κρίσιμων Υποδομών (τόσο του δημόσιου όσο και του ιδιωτικού τομέα) και καταγραφή των μεταξύ τους εξαρτήσεων.

3.3. Αποτίμηση Επικινδυνότητας σε Εθνικό Επίπεδο

Εκπόνηση μελέτης αποτίμησης επικινδυνότητας σε εθνικό επίπεδο, ακολουθώντας μια επιστημονική και τεχνολογική διαδικασία που συνοπτικά βασίζεται στην αναγνώριση, ανάλυση και αποτίμηση των επιπτώσεων των κινδύνων και οδηγεί στον καθορισμό ενός σχεδίου προστασίας των κρίσιμων υποδομών ανά τομέα ή/και ανά φορέα. Η μελέτη, η οποία θα αναθεωρείται το αργότερο κάθε τριετία, θα λάβει υπόψη της όλες τις πιθανές απειλές, ιδιαίτερα αυτές που σχετίζονται με κακόβουλες ενέργειες (πχ κυβερνοέγκλημα, κυβερνοεπιθέσεις), αλλά και τους κινδύνους που σχετίζονται με φυσικά φαινόμενα, τεχνικές αστοχίες ή δυσλειτουργίες και ανθρώπινα λάθη. Επίσης, θα ληφθούν υπόψη οι απειλές που προκύπτουν από την αλληλεξάρτηση των συστημάτων επικοινωνιών και πληροφοριών των φορέων που συμμετέχουν στην Εθνική Στρατηγική και ιδιαίτερα των κρίσιμων υποδομών, ενώ περαιτέρω θα αξιολογείται η έκταση και η κρισιμότητα των επιπτώσεων σε εθνικό επίπεδο.

3.4. Καταγραφή και βελτίωση Υφιστάμενου Θεσμικού Πλαισίου

Πρωταρχικό στάδιο στην ανάπτυξη και υλοποίηση της Εθνικής Στρατηγικής αποτελεί η καταγραφή και αξιολόγηση του υφιστάμενου θεσμικού πλαισίου και

των δομών που λειτουργούν για την εξυπηρέτηση των στόχων της Εθνικής Στρατηγικής:

- Νομοθετικές ρυθμίσεις, ρόλοι και αρμοδιότητες φορέων που σχετίζονται με την Κυβερνοασφάλεια (πχ επεξεργασία προσωπικών δεδομένων, ηλεκτρονικές επικοινωνίες, άρση του απορρήτου των επικοινωνιών, ακεραιότητα και διαθεσιμότητα των δικτύων κλπ).

- Κανονιστικές πράξεις που εξειδικεύονται ανά τομέα (πχ τραπεζικό) και η ως τώρα επίπτωσή τους στη βελτίωση της Κυβερνοασφάλειας (πχ κανονισμοί και ελεγκτικός ρόλος της Τράπεζας της Ελλάδος).

- Δομές, φορείς και υπηρεσίες, του ιδιωτικού ή δημόσιου τομέα, που έχουν επιχειρησιακό ρόλο στη διασφάλιση της Κυβερνοασφάλειας (πχ ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Teams — CSIRTs).

- Υφιστάμενα σχέδια αντιμετώπισης έκτακτων αναγκών (όπως Εγνατία, Ξενοκράτης κλπ).

- Ευρωπαϊκές και άλλες διεθνείς οδηγίες και κανονισμοί σχετικά με την ασφάλεια των δικτύων και πληροφοριών καθώς και των κρίσιμων υποδομών.

Η λεπτομερής καταγραφή και αξιολόγηση της αποτελεσματικότητας του υφιστάμενου θεσμικού πλαισίου και των σχετικών δομών θα οδηγήσει στον εντοπισμό των σημείων εκείνων που δεν καλύπτονται επαρκώς ή εμφανίζουν επικαλύψεις, αλλά και των σημείων εκείνων που χρήζουν βελτίωσης και αποτελεσματικότερου συντονισμού. Ως αποτέλεσμα της δράσης αυτής θα είναι η υιοθέτηση των απαραίτητων νομοθετικών ρυθμίσεων, με σεβασμό στις συνταγματικές ελευθερίες και στα ατομικά δικαιώματα, καθώς και στο Διεθνές Δίκαιο, σε συμφωνία με την ευρύτερη κοινωνική και πολιτική κατάσταση, αλλά και τις απαιτήσεις της Εθνικής Στρατηγικής Κυβερνοασφάλειας ώστε να επιτευχθούν οι στόχοι της.

Η Εθνική Στρατηγική αποτυπώνει τη συσχέτισή της όχι μόνο με το υφιστάμενο θεσμικό πλαίσιο, αλλά και με άλλες Στρατηγικές σε εθνικό ή διεθνές επίπεδο (πχ Εθνικός Κανονισμός Ασφαλείας (ΕΚΑ), Εθνική Στρατιωτική Στρατηγική, Στρατηγική για την Ηλεκτρονική Διακυβέρνηση κλπ). Επίσης, είναι εναρμονισμένη με τις επιταγές των σχετικών ευρωπαϊκών κανονισμών και οδηγιών (ιδιαιτέρα δε με την Οδηγία (ΕΕ) 2016/1148 Του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση – Οδηγία NIS).

3.5. Εθνικό Σχέδιο Έκτακτης Ανάγκης στον Κυβερνοχώρο

Κατάρτιση Εθνικού Σχεδίου Έκτακτης Ανάγκης στον Κυβερνοχώρο, το οποίο θα καθορίζει τις δομές και τα μέτρα για την αντιμετώπιση των σημαντικών περιστατικών που πραγματοποιούνται σε κρίσιμα συστήματα επικοινωνιών και πληροφορικής των φορέων που συμμετέχουν στην Εθνική Στρατηγική Κυβερνοασφάλειας και την αποκατάσταση των υπηρεσιών που οι φορείς αυτοί προσφέρουν στην κοινωνία.

Στους κύριους στόχους του Εθνικού Σχεδίου Έκτακτης Ανάγκης περιλαμβάνονται ο καθορισμός και η περιγραφή των κριτηρίων που χρησιμοποιούνται ώστε ένα περιστατικό να χαρακτηριστεί κρίσιμο, ο ορισμός των σημαντικών διαδικασιών και των δράσεων για τη αντιμετώπισή του καθώς και ο ορισμός, των ρόλων και αρμοδιοτήτων των διαφόρων φορέων που διαχειρίζονται το συγκεκριμένο περιστατικό.

3.6. Καθορισμός Βασικών Απαιτήσεων Ασφάλειας

Όλοι οι φορείς που συμμετέχουν στην Εθνική Στρατηγική Κυβερνοασφάλειας οφείλουν να λαμβάνουν τα τεχνικά και οργανωτικά μέτρα που διασφαλίζουν την ασφαλή και απρόσκοπτη λειτουργία των συστημάτων επικοινωνίας και πληροφοριών τους και να ελαχιστοποιούν τις επιπτώσεις ενός περιστατικού ασφαλείας. Τα μέτρα αυτά περιλαμβάνουν μέτρα πρόληψης αλλά και αντιμετώπισης περιστατικών ασφάλειας.

Η Εθνική Αρχή Κυβερνοασφάλειας θα ορίσει (πχ μέσω κανονιστικών πράξεων) τις ελάχιστες απαιτήσεις ασφάλειας και τα αντίστοιχα τεχνικά και οργανωτικά μέτρα, βάσει της αποτίμησης επικινδυνότητας σε εθνικό επίπεδο, που οι φορείς οφείλουν να εφαρμόζουν ώστε να επιτύχουν ένα θεμελιώδες και κοινό επίπεδο ασφάλειας.

Η θέσπιση ενός ελαχίστου, κοινού και εναρμονισμένου επιπέδου απαιτήσεων και μέτρων μεταξύ των φορέων, που θα εφαρμόζεται κατά την υλοποίηση, την αξιολόγηση και τον έλεγχο ορθής εφαρμογής, είναι ιδιαίτερα σημαντική.

Περαιτέρω, ενισχύεται η δυνατότητα ανταλλαγής πληροφοριών μεταξύ των φορέων, αφού υπάρχει μια «κοινή γλώσσα», ενώ επίσης διευκολύνεται η αναφορά περιστατικών ασφαλείας και η εφαρμογή κοινών πρακτικών ασφάλειας.

3.7. Αντιμετώπιση Περιστατικών Ασφάλειας

Στην περίπτωση περιστατικού κυβερνοασφάλειας, οι φορείς που συμμετέχουν στην Εθνική Στρατηγική οφείλουν να είναι έτοιμοι να αντιδράσουν αποτελεσματικά. Η γνώση των τεχνικών λεπτομερειών των περιστατικών που καλούνται να αντιμετωπίσουν οι φορείς, η ανάλυση αυτών και η διασπορά της γνώσης απαιτείται, βοηθούν όλους τους συμμετέχοντες να προετοιμαστούν καλύτερα ώστε να αντιμετωπίσουν το περιστατικό αλλά και να προβούν στις απαραίτητες διορθωτικές ενέργειες σε σχέση με τα μέτρα ασφάλειας που έχουν λάβει, ώστε να ελαχιστοποιηθεί ο κίνδυνος επανάληψής του. Με τον τρόπο αυτό, ενισχύεται η ετοιμότητα και η ικανότητα αντιμετώπισης περιστατικών ασφάλειας και ανάκαμψης μετά από αυτά, σε εθνικό επίπεδο. Η διαχείριση των κρίσιμων περιστατικών πραγματοποιείται σύμφωνα με το Εθνικό Σχέδιο Έκτακτης Ανάγκης στον Κυβερνοχώρο.

Ιδιαίτερο ρόλο κατά την αντιμετώπιση περιστατικών ασφάλειας φέρουν οι ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Teams — CSIRT)), των οποίων ο κύριος ρόλος είναι ο συντονισμός των δράσεων κατά τη διαχείριση του περιστατικού από τους εμπλεκόμενους φορείς, βάσει καθορισμένων ρόλων, αρμοδιοτήτων και

διαδικασιών αλλά και επιχειρησιακών και επικοινωνιακών δυνατοτήτων. Σε εθνικό επίπεδο ήδη λειτουργούν ή μπορούν να δημιουργηθούν και άλλες ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών ανά τομέα. Επιπρόσθετα, το Εθνικό CERT αποσκοπεί στη βελτιστοποίηση του επιπέδου πρόληψης, αξιολόγησης και ανάλυσης των απειλών μεταξύ των φορέων που συμμετέχουν στην Εθνική Στρατηγική. Το Εθνικό CERT, σε συνεργασία με τα άλλα CSIRT/CERT που λειτουργούν εντός της χώρας αλλά και με άλλα εθνικά CSIRT/CERT με τα οποία έχει συγκροτήσει ένα δίκτυο συνεργασίας, παρακολουθεί διαρκώς σε εθνικό και διεθνές επίπεδο τις απειλές και τις ευπάθειες των συστημάτων επικοινωνιών και πληροφορικής, τις αναλύει και τις αξιολογεί, με βάση τις ιδιαιτερότητες της χώρας, και ενημερώνει τους φορείς ώστε να ενισχυθεί η ετοιμότητά τους στην αντιμετώπιση περιστατικών ασφάλειας.

3.8. Εθνικές Ασκήσεις Ετοιμότητας

Οι Εθνικές Ασκήσεις Ετοιμότητας αποτελούν σημαντικό εργαλείο για την αξιολόγηση της ετοιμότητας των φορέων που συμμετέχουν και τον εντοπισμό των αδυναμιών και της ευπάθειας των συστημάτων. Μέσω της προσομοίωσης περιστατικών ασφάλειας παρέχεται η δυνατότητα να αντιμετωπισθούν περιστατικά ασφάλειας σε συνθήκες που αναλογούν σε πραγματικά περιστατικά, με την εφαρμογή σχετικών μέτρων ασφάλειας που έχουν ληφθεί καθώς και συναφών καταρτισθέντων σχεδίων έκτακτης ανάγκης, ώστε οι φορείς να προβούν στις σχετικές βελτιώσεις και επικαιροποιήσεις. Περαιτέρω, με τις ασκήσεις αυτές ενισχύεται η ανταλλαγή πληροφοριών και γνώσεων, η συνεργασία μεταξύ των φορέων που συμμετέχουν ενώ ενδυναμώνεται, παράλληλα η κουλτούρα της συνεργασίας για την αύξηση του επίπεδου Κυβερνοασφάλειας στη χώρα.

Οι ασκήσεις ετοιμότητας διεξάγονται σε τακτά χρονικά διαστήματα. Οι ασκήσεις εποπτεύονται από την Εθνική Αρχή Κυβερνοασφάλειας και σχεδιάζονται βάσει σαφώς ορισμένων χρονοδιαγραμμάτων, ρόλων, σεναρίων και στόχων. Τα αποτελέσματα των ασκήσεων και ιδιαίτερα η γνώση που έχει αποκτηθεί πρέπει να κοινοποιούνται στους εμπλεκόμενους στις ασκήσεις, αλλά

και σε άλλους αρμόδιους φορείς. Επιδιώκεται η συμμετοχή της Ελλάδας σε ευρωπαϊκές και διεθνείς ασκήσεις ετοιμότητας.

3.9. Ευαισθητοποίηση χρηστών – πολιτών

Η ευαισθητοποίηση σχετικά με τις απειλές και τις ευπάθειες που σχετίζονται με την Κυβερνοασφάλεια, καθώς και τις επιπτώσεις αυτών στην κοινωνία, είναι ζωτικής σημασίας. Μέσω κατάλληλων και στοχευμένων εκστρατειών ενημέρωσης – εκπαίδευσης τόσο για τους χρήστες των φορέων που συμμετέχουν στην Εθνική Στρατηγική Κυβερνοασφάλειας όσο και για τους πολίτες γενικότερα, ενισχύεται η γνώση σχετικά με τους κινδύνους του διαδικτυακού περιβάλλοντος, ώστε να επισχυθεί η προστασία από συνήθεις απειλές, κάτι που εκτιμάται ότι εν τέλει θα αυξήσει σημαντικά το επίπεδο Κυβερνοασφάλειας της χώρας.

Οι δράσεις, οι μηχανισμοί και οι μέθοδοι που σχετίζονται με την ευαισθητοποίηση χρηστών – πολιτών εξαρτώνται από το κοινό στο οποίο απευθύνονται. Η σχεδίαση, οργάνωση και υλοποίηση του προγράμματος ευαισθητοποίησης των χρηστών – πολιτών εποπτεύεται από την Εθνική Αρχή Κυβερνοασφάλειας και ενδεικτικά περιλαμβάνει εκστρατείες ενημέρωσης προς τους πολίτες (πχ μέσω του Υπουργείου Παιδείας στην πρωτοβάθμια και δευτεροβάθμια εκπαίδευση), εκπαιδευτικές δράσεις (πχ σε συνεργασία με τους πανεπιστημιακούς φορείς) για τους διαχειριστές και χρήστες των συστημάτων επικοινωνιών και πληροφορικής των φορέων, προβολή μέσω ιστοσελίδων κλπ.

3.10. Μηχανισμοί Αξιόπιστης Ανταλλαγής Πληροφοριών

Η ανταλλαγή πληροφοριών, πέραν των υποχρεωτικών που αναφέρονται στην παρ.3.6 μεταξύ των ιδιωτικών φορέων που συμμετέχουν στην Εθνική Στρατηγική Κυβερνοασφάλειας και των εποπτικών τους φορέων στο δημόσιο καθώς και της Εθνικής Αρχής Κυβερνοασφάλειας έχει ιδιαίτερη σημασία για την υλοποίηση της Εθνικής Στρατηγικής. Οι ιδιωτικοί φορείς καλούνται να ανταλλάσσουν πληροφορίες που αφορούν στα συστήματα επικοινωνιών και πληροφορικής που λειτουργούν, στις πολιτικές ασφάλειας που έχουν υλοποιήσει, στις ευπάθειες, στις απειλές και στα περιστατικά ασφάλειας που

αντιμετωπίζουν. Αντίστοιχα, οι δημόσιοι φορείς καλούνται να ανταλλάσσουν πληροφορίες που έχουν συλλέξει οι φορείς, οι οποίες ενδέχεται να θέσουν σε κίνδυνο το επιθυμητό επίπεδο κυβερνοασφάλειας. Με τον συσχετισμό των πληροφοριών αυτών είναι δυνατή η ανάλυση της εξέλιξης των απειλών που σχετίζονται με την Κυβερνοασφάλεια της χώρας.

Είναι απαραίτητο να αναπτυχθούν εκείνοι οι μηχανισμοί για την αξιόπιστη ανταλλαγή πληροφοριών μέσα σε ένα πλαίσιο αμοιβαίας εμπιστοσύνης και σεβασμού στο ρόλο και στις αρμοδιότητες όλων των φορέων που συμμετέχουν στην Εθνική Στρατηγική Κυβερνοασφάλειας.

Στο στάδιο αυτό, αλλά πιθανόν και σε μεταγενέστερη φάση, μπορεί να εξετασθεί η ανάπτυξη συμπράξεων ιδιωτικού και δημόσιου τομέα που θα θεσπιστούν με γνώμονα ένα κοινό πεδίο εφαρμογής και θα χρησιμοποιήσουν καλά καθορισμένους ρόλους προκειμένου να επιτύχουν τους κοινούς στόχους.

3.11. Υποστήριξη Ερευνητικών και Αναπτυξιακών Προγραμμάτων και Ακαδημαϊκών Προγραμμάτων Εκπαίδευσης

Η ουσιαστική υποστήριξη, εκ μέρους της πολιτείας, των προσπαθειών της ακαδημαϊκής κοινότητας για τη συμμετοχή της σε εθνικά, ευρωπαϊκά ή άλλα διεθνή ερευνητικά και αναπτυξιακά προγράμματα, και την προσαρμογή των προγραμμάτων σπουδών, σχετικά με θέματα που άπτονται της Εθνικής Στρατηγικής Κυβερνοασφάλειας, αποτελεί ουσιώδη παράμετρο στην ενδυνάμωση του επιπέδου της Κυβερνοασφάλειας της χώρας, ιδιαίτερα αν ληφθεί υπόψη ότι το πεδίο αυτό αποτελεί ένα διαρκώς εξελισσόμενο τομέα υψηλής τεχνολογίας και εξειδικευμένων γνώσεων.

3.12. Συνεργασίες σε Διεθνές Επίπεδο

Δεδομένου ότι ο κυβερνοχώρος και το Διαδίκτυο αποτελούν ένα παγκόσμιο πληροφοριακό περιβάλλον, η αντιμετώπιση των απειλών και ευπαθειών των συστημάτων επικοινωνιών και πληροφορικής ανάγεται σε παγκόσμια προσπάθεια, που απαιτεί τη συνεργασία σε διεθνές επίπεδο. Είναι

συνεπώς σημαντική η ενεργός παρουσία και συμμετοχή της χώρας μας σε όλο το φάσμα της διεθνούς συνεργασίας για το θέμα της ασφάλειας του κυβερνοχώρου, στο πλαίσιο των υφιστάμενων στόχων/επιδιώξεων της εθνικής εξωτερικής πολιτικής και των κατευθύνσεων για την άσκησή της και σύμφωνα με την κείμενη νομοθεσία. Ειδικότερα, απαιτείται η συστηματική συνεργασία με χώρες που έχουν υιοθετήσει παρεμφερή, εν προκειμένω, στρατηγική και των οποίων οι επιλογές χαρακτηρίζονται από συμβατότητα με τις αντίστοιχες ελληνικές. Στόχος της συνεργασίας θα είναι η ανταλλαγή εμπειριών και βέλτιστων πρακτικών, καθώς και η διακρίβωση δυνατοτήτων για την από κοινού ανάπτυξη κατάλληλων μέσων, με σκοπό την αντιμετώπιση απειλών και προκλήσεων που αφορούν την ασφάλεια του κυβερνοχώρου. Επίσης θα αξιοποιηθεί, στο μέγιστο δυνατό βαθμό, η συμβολή της χώρας μας στη διαμόρφωση και υλοποίηση σχετικών αποφάσεων που έχουν υιοθετηθεί στο πλαίσιο διεθνών Οργανισμών στους οποίους συμμετέχει η Ελλάδα, με σκοπό τόσο την ενίσχυση της κυβερνοασφάλειας σε εθνικό επίπεδο, όσο και τον εναρμονισμό μεταξύ των συναφών διεθνών μηχανισμών πολυμερούς διαβούλευσης και δράσης, λαμβανομένης, βεβαίως, υπ' όψιν και της αυτονομίας λήψης αποφάσεων σε εθνικό επίπεδο.

3.13. Αξιολόγηση και Αναθεώρηση της Εθνικής Στρατηγικής

Η υλοποίηση των στρατηγικών στόχων της Εθνικής Στρατηγικής Κυβερνοασφάλειας παρακολουθείται από την Εθνική Αρχή Κυβερνοασφάλειας, με σκοπό την αξιολόγηση και την πιθανή αναθεώρηση της Στρατηγικής. Η αξιολόγηση της Στρατηγικής βασίζεται σε μια προκαθορισμένη μεθοδολογία, η οποία θα κάνει χρήση ποιοτικών και ποσοτικών δεικτών αποτελεσματικότητας και στη βάση διεθνών προτύπων, και καταλήγει σε μια αναφορά που θα προτείνει συγκεκριμένα μέτρα βελτίωσης, εντός ενός προκαθορισμένου χρονοδιαγράμματος. Η Εθνική Αρχή Κυβερνοασφάλειας παρακολουθεί τα διεθνή πρότυπα προκειμένου να υιοθετεί βέλτιστες πρακτικές τις οποίες στη συνέχεια υποδεικνύει στους αρμόδιους φορείς για εφαρμογή. Κατά τη φάση αυτή, είναι επιτακτική η ανάγκη συμμετοχής όλων των φορέων που εμπλέκονται στην Εθνική Στρατηγική, στο πλαίσιο των θεσμικών και διοικητικών τους αρμοδιοτήτων.

4. ΕΠΙΛΟΓΟΣ

Η Εθνική Στρατηγική Κυβερνοασφάλειας θα αναπτυχθεί στη βάση του ανωτέρου πλαισίου δράσεων και ενεργειών το οποίο θα δημιουργήσει και τις συνθήκες υλοποίησης του εθνικού οράματός μας για το επιθυμούμενο επίπεδο κυβερνοασφάλειας (βλέπε κεφάλαιο 3). Η υλοποίηση των προαναφερθέντων συνεπάγεται την ενδυνάμωση της συνεργασίας δημόσιου και ιδιωτικού τομέα, η οποία θεωρείται ιδιαίτερα σημαντική για την επίτευξη του όλου εγχειρήματος αλλά και ιδιαίτερα δυσχερής, δεδομένου του μικρού βαθμού ωρίμανσης και εμπειρίας. Ωστόσο, τα πλεονεκτήματα αυτής της συνεργασίας θα είναι πολλαπλασιαστικά για το κράτος και τη δημόσια διοίκηση, για τους πολίτες και το επίπεδο των παρεχόμενων υπηρεσιών ασφαλείας αλλά και για τον ιδιωτικό τομέα (πάροχοι ευρυζωνικών υπηρεσιών, ιδιωτικές επιχειρήσεις).