ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

NATIONAL CYBERSECURITY AUTHORITY

ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020 -2025

Δεκέμβριος

2020

Επεξήγηση όρων

ΦΕΒΥ (OES):	Φορέας Εκμετάλλευσης Βασικών Υπηρεσιών (Operator of Essential Services)
ΠΨΥ (DSP):	Πάροχος Ψηφιακών Υπηρεσιών (Digital Service Provider)
CERT ή CSIRT:	Computer Emergency Response Team ή Computer Security Incident Response Team
SLA:	Service Level Agreement – Συμφωνητικό Επιπέδου Υπηρεσίας
SOC:	Security Operations Center
SIEM:	Security Information & Event Management
SOAR:	Security Orchestration and Response
MDR:	Managed Detection and Response
ΤΠΕ:	Τεχνολογία/ες Πληροφοριών και Επικοινωνίας
Φορείς:	Όρος που συμπεριλαμβάνει τους φορείς της ευρύτερης Δημόσιας Διοίκησης, τους Φ.Ε.Β.Υ., του ΠΨΥ και εν γένει οργανισμούς οι οποίοι υπάγονται στις διατάξεις του 4577/2018
ΓΓΤΤ	Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων
MSSP	Managed Security Service Provider (Οργανισμοί που παρέχουν διαχειριζόμενες υπηρεσίες ασφάλειας)
ΥΑΠΔ	Υπεύθυνος Ασφάλειας Πληροφοριών και Δικτύων

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Πινακας Εικονων

1 ΕΙΣΑΓΩΓΗ

Η διαρκής προσαρμογή, η πρόληψη και η έγκαιρη αντίδραση στις προκλήσεις ενός διαρκώς μεταβαλλόμενου περιβάλλοντος, αποτελούν το ισχυρότερο θεμέλιο για την αποτελεσματική διαμόρφωση μιας ολοκληρωμένης στρατηγικής αντιμετώπισης των κυβερνοεπιθέσεων. Από το 2018 και την 3η αναθεώρηση της Εθνικής Στρατηγικής για την Κυβερνοασφάλεια η μεσολάβηση σημαντικών τεχνολογικών εξελίξεων (π.χ. δίκτυα 5ης γενιάς, τεχνητή νοημοσύνη, IoT), σε συνδυασμό με την ανάγκη αυξημένης χρήσης των νέων τεχνολογιών και ψηφιακών εφαρμογών για την εξυπηρέτηση πολιτών και επιχειρήσεων εν μέσω της ραγδαίας εξάπλωσης μιας πρωτοφανούς πανδημίας (COVID - 19), με συνταρακτικές συνέπειες για την ανθρωπότητα, καθιστούν αναγκαία την άμεση αξιολόγηση και ανατροφοδότηση του στρατηγικού σχεδιασμού για την κυβερνοασφάλεια της χώρας. Είναι γεγονός, άλλωστε, ότι όσο περισσότερο στηρίζεται η κοινωνία και η οικονομία στην ψηφιοποίηση διαδικασιών και υπηρεσιών, τόσο αυξάνεται η επιφάνεια επίθεσης (attack surface), άλλως το εύρος των ευκαιριών, για την πραγματοποίηση κακόβουλων ενεργειών, καλώντας όλους τους αρμόδιους εμπλεκόμενους φορείς σε έγκαιρο σχεδιασμό και αποτελεσματική αντίδραση.

Η χώρα μας, μετέχοντας σε όλα τα κατά περίπτωση ευρωπαϊκά και διεθνή fora και αναγνωρίζοντας τη θεμελιώδη σημασία της θωράκισης της ασφάλειας των συστημάτων και δικτύων πληροφορικής και επικοινωνιών, έχει λάβει ήδη μια σειρά από σημαντικές πρωτοβουλίες με γνώμονα την ανταπόκριση στις διεθνείς και ενωσιακές απαιτήσεις, τη διαμόρφωση ενός ασφαλούς περιβάλλοντος για τις νέες τεχνολογίες και την αύξηση της εμπιστοσύνης των πολιτών και επιχειρήσεων σε ψηφιακές εφαρμογές και υπηρεσίες προς όφελος της οικονομίας και της κοινωνίας. Μεταξύ των πρωτοβουλιών αυτών διακρίνονται: η θέση σε ισχύ του ν. 4577/2018 «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις» (Α' 199) και η έκδοση της υπουργικής απόφασης 1027/2019 (Α' 3739) με βάση την οποία καθορίστηκε το πλαίσιο υποχρεώσεων για τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (Φ.Ε.Β.Υ.) και τους Παρόχους Ψηφιακών Υπηρεσιών (Π.Ψ.Υ.), συμπεριλαμβανομένων των απαιτήσεων ασφαλείας που οφείλουν να τηρούν, η αναβάθμιση της Εθνικής Αρχής Κυβερνοασφάλειας σε Γενική Διεύθυνση του Υπουργείου Ψηφιακής Διακυβέρνησης, η οργάνωση και συμμετοχή των αρμόδιων υπηρεσιών σε ασκήσεις ετοιμότητας, η χρήση προηγμένων συστημάτων πρόληψης και αντιμετώπισης ηλεκτρονικών επιθέσεων κ.λπ.

Υπό το πρίσμα αυτό, και λαμβάνοντας υπόψη τις σύγχρονες απαιτήσεις και ανάγκες, η Εθνική Αρχή Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης, ως επισπεύδουσα Υπηρεσία σύμφωνα με τις διατάξεις του ν.4577/2018 και του π.δ. 40/2020 (Α' 85), προβαίνει με το παρόν σε επικαιροποίηση του εθνικού στρατηγικού σχεδιασμού για την κυβερνοασφάλεια, ώστε να αξιολογηθεί η υφιστάμενη κατάσταση, να αναγνωρισθούν οι νέες προκλήσεις και να διαμορφωθεί ένα κατάλληλο στρατηγικό πλαίσιο άμεσης εφαρμογής.

2 ΑΝΑΛΥΣΗ ΥΦΙΣΤΑΜΕΝΗΣ ΚΑΤΑΣΤΑΣΗΣ

2.1 ΈΝΑ ΔΙΑΡΚΩΣ ΜΕΤΑΒΑΛΛΟΜΕΝΟ ΠΕΡΙΒΑΛΛΟΝ ΑΠΕΙΛΩΝ

Οι τεχνολογικές εξελίξεις, η ψηφιακή διακυβέρνηση αλλά και η ευημερία των χωρών μελών της Ευρωπαϊκής Ένωσης, έχουν καταστήσει τα κράτη-μέλη στόχους πληθώρας κυβερνοεπιθέσεων. Από απειλές που προέρχονται από μεμονωμένους εγκληματίες , μέχρι επιθέσεις φερόμενες ως απόρροια ενεργειών τρίτων κρατών, το περιβάλλον κυβερνοαπειλών είναι διαρκώς μεταβαλλόμενο, οδηγώντας σε μια εγγενή αδυναμία άμεσης προστασίας του. Οι εν λόγω συνθήκες επιβεβαιώνουν την ανάγκη για μια περιοδικά αναθεωρούμενη στρατηγική, η οποία θα θέτει τους κανόνες αντιμετώπισης ή μετριασμού του αντίκτυπου των εν λόγω απειλών.

Στην Ευρωπαϊκή Ένωση έχουν παρατηρηθεί επιθέσεις οι οποίες είχαν ποικίλους στόχους, όπως αποτυπώνεται στην κάτωθι εικόνα από την μελέτη ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends.

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➲	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➲	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Εικόνα 1. ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends

Ήδη με βάση τα τελευταία στοιχεία του ENISA (ETL 2020, List of top 15 threats, enisa.europa.eu):

- οι επιθέσεις τύπου phishing έχουν ήδη ανέλθει στην 3η θέση, με τα web application attacks να κατεβαίνουν στην 4η,
- οι επιθέσεις spam ανέβηκαν στην 5η θέση και οι επιθέσεις DDoS κατέβηκαν στην 6η θέση
- οι επιθέσεις identity theft ανέβηκαν από τη 13η στην 7η θέση
- η περίπτωση των botnets βρίσκεται πλέον στη 10η θέση
- η περίπτωση physical manipulation, damage, theft and loss κατέβηκε στην 11η θέση
- ομοίως η περίπτωση information leakage κατέβηκε στη 12η θέση
- στη 13η θέση ανήλθαν τα ransomware
- στη 14η θέση ανήλθαν οι περιπτώσεις cyberespionage
- στη 15η θέση βρίσκονται οι περιπτώσεις cryptojacking

Εικόνα 2. ENISA, ETL 2020 (enisa.europa.eu), Top 15 Threats

Πιο αναλυτικά, οι ανωτέρω απειλές περιγράφονται ως εξής:

2.1.1 Κακόβουλο λογισμικό (malicious software)

Λογισμικό το οποίο έχει σχεδιαστεί ειδικά για να προκαλέσει ζημιά ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα υπολογιστή. Περιλαμβάνει ιούς(viruses), worms, trojan horses κ.λπ. Σε αυτή την κατηγορία ανήκει και το λογισμικό λύτρων (ransomware), το οποίο όμως εξετάζεται χωριστά λόγω της ιδιαιτερότητάς του.

2.1.2 Επιθέσεις από το διαδίκτυο (web based attacks)

Πρόκειται για απειλές που στοχεύουν απευθείας στο χρήστη μέσω εκμετάλλευσης αδυναμιών στους φυλλομετρητές (browsers), καθώς και στα συστήματα διαχείρισης περιεχομένου (content management systems). Κυριότερα είδη επιθέσεων αυτής της κατηγορίας αποτελούν τα browser exploits, drive-by downolads, watering hole attacks κ.α.

2.1.3 Phishing

Κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου ή τηλεφωνικές συνδιαλλαγές, οι οποίες αποσκοπούν στο να παραπλανήσουν τους χρήστες και να αποκαλύψουν εμπιστευτικές πληροφορίες.

2.1.4 Επιθέσεις σε διαδικτυακές εφαρμογές (web application attacks)

Επιθέσεις που στοχεύουν σε διαδικτυακές εφαρμογές (web applications). Οι εν λόγω εφαρμογές λόγω της καθολικής χρήσης τους στην προσφορά περιεχομένου αποτελούν στόχο πολλαπλών ειδών επιθέσεων, με κυριότερες τα cross-site scripting (XSS), SQL injection, path traversal, local file inclusion κ.α.

2.1.5 Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου

Αναφερόμενες και ως SPAM, αυτές οι επιθέσεις περιλαμβάνουν την αποστολή ανεπιθύμητης αλληλογραφίας σε χρήστες. Η εν λόγω αλληλογραφία χαρακτηρίζεται από το πολύ μικρό κόστος αποστολής των μηνυμάτων, την ενόχληση που προκαλεί στους χρήστες, αλλά και την εν δυνάμει μετεξέλιξη των μηνυμάτων σε απειλή phishing.

2.1.6 Επιθέσεις άρνησης υπηρεσίας (Denial of Service – DoS attacks)

Επιθέσεις κατά τις οποίες μεγάλος όγκος διαδικτυακής κίνησης στοχεύει σε μια υπηρεσία, με σκοπό να καταστεί αδύνατο από τα συστήματα να εξυπηρετήσουν νόμιμα αιτήματα. Ουσιαστικά, εκμεταλλεύονται την πεπερασμένη χωρητικότητα συστημάτων και δικτύων, ώστε να καταστήσουν αδύνατη την παροχή υπηρεσιών (απώλεια διαθεσιμότητας).

2.1.7 Κλοπή ταυτότητας χρήστη (identity theft)

Ο επιτιθέμενος αποκτά δεδομένα προσωπικού χαρακτήρα του χρήστη (passwords, social security numbers κ.α.), με αποτέλεσμα την ιδιοποίηση της ταυτότητας του χρήστη (impersonation) και με σκοπό το οικονομικό όφελος (αγορές προϊόντων μέσω πιστωτικών καρτών, παράνομη επιστροφή φόρου κ.λπ.) εις βάρος του.

2.1.8 Παραβιάσεις προσωπικών δεδομένων

Επιθέσεις οι οποίες αποσκοπούν στη διαρροή, αλλοίωση ή μη διαθεσιμότητα προσωπικών δεδομένων. Σύμφωνα με τον Κανονισμό της Ε.Ε. 2016/679, τέτοιου είδους επιθέσεις

νοούνται ως παραβιάσεις δεδομένων προσωπικού χαρακτήρα οι οποίες χρήζουν άμεσης αντιμετώπισης.

2.1.9 Εσωτερικές απειλές (insider threat)

Απειλές που προέρχονται από στελέχη Φορέων που εργάζονται ή εργάζονταν σε έναν Οργανισμό, καθώς και εξωτερικών συνεργατών, οι οποίοι κατέχουν εσωτερική πληροφόρηση σχετικά με τις πρακτικές ασφάλειας, τα υπολογιστικά συστήματα και τα δεδομένα του Οργανισμού. Οι εν λόγω απειλές μπορούν να οδηγήσουν σε πλήθος επιθέσεων που περιγράφονται στην παρούσα ενότητα, συνήθως με πολύ μεγάλο αντίκτυπο για τον Φορέα και είναι εξαιρετικά δύσκολο να διαγνωσθούν ή/και αντιμετωπισθούν.

2.1.10 Botnets

Δίκτυα τα οποία αποτελούνται από υπολογιστικές συσκευές ανυποψίαστων χρηστών που έχουν μολυνθεί με κακόβουλο λογισμικό και ελέγχονται κεντρικά από κάποιον επιτιθέμενο, προκειμένου να χρησιμοποιηθούν ομαδικά στην αποστολή μηνυμάτων ανεπιθύμητης αλληλογραφίας, σε επιθέσεις άρνησης υπηρεσίας, σε cryptojacking, κλπ.

2.1.11 Φυσικές απειλές

Απειλές που στοχεύουν στην καταστροφή ή αλλοίωση ή κλοπή εξοπλισμού, με απώτερο στόχο την διαρροή ή/και καταστροφή δεδομένων ή την άρνηση υπηρεσίας.

2.1.12 Διαρροή δεδομένων

Διαρροή δεδομένων σε μη εξουσιοδοτημένους χρήστες. Τα δεδομένα μπορεί να περιλαμβάνουν οικονομικά στοιχεία, πατέντες, δεδομένα με κατοχυρωμένα πνευματικά δικαιώματα, πλάνα στρατηγικής ανάπτυξης κλπ.

2.1.13 Λογισμικό λύτρων (ransomware)

Κακόβουλο λογισμικό (malware) το οποίο κρυπτογραφεί τα δεδομένα του πληροφοριακού συστήματος, για την αποκρυπτογράφηση των οποίων ο επιτιθέμενος απαιτεί λύτρα (συνήθως σε μορφή κρυπτονομίσματος).

2.1.14 Ηλεκτρονική κατασκοπία

Κατασκοπία μέσω του κυβερνοχώρου, η οποία μπορεί να περιλαμβάνει χρήση εξειδικευμένων εργαλείων για την άντληση στοιχείων ή/και χρήση συνδυασμού των προαναφερθέντων απειλών. Συνήθως αυτή η μορφή επίθεσης αναφέρεται ως «στοχευμένη» (λόγω του ότι οι επιτιθέμενοι έχουν πολύ συγκεκριμένους στόχους) με απώτερο στόχο την υποκλοπή ευαίσθητων, για τον οργανισμό, πληροφοριών.

2.1.15 Cryptojacking

Τεχνικές που χρησιμοποιούν την υπολογιστική ισχύ του υπολογιστή του χρήστη με σκοπό την άντληση (mining) κρυπτονομισμάτων (bitcoins).

2.2 ΠΑΡΑΓΟΝΤΕΣ ΑΠΕΙΛΩΝ (THREAT AGENTS)

Οι βασικοί παράγοντες απειλών (threat agents) συνοψίζονται στις κάτωθι κατηγορίες, για τις οποίες παρέχεται μια γενική διαβάθμιση αναφορικά με το επίπεδο δυσκολίας αναγνώρισης των επιθέσεων, του αντικτύπου τους και της πιθανότητας εκδήλωσής τους[1].

2.2.1 Κυβερνοεγκληματίες (Cybercriminals)

Το κυβερνοέγκλημα (cybercrime), ως όρος, χρησιμοποιείται για να χαρακτηρίσει κάθε κακόβουλη ενέργεια η οποία αποσκοπεί στο να επιφέρει αντίκτυπο στις επιχειρησιακές λειτουργίες ενός οργανισμού. Κατά συνέπεια, οι κυβερνοεγκληματίες, ως παράγοντες απειλών, είναι ομάδες ή μεμονωμένα φυσικά πρόσωπα που χρησιμοποιούν την τεχνολογία (ΤΠΕ) για την τέλεση κακόβουλων ενεργειών[2]. Οι εν λόγω παράγοντες συχνά εμπλέκονται σε παράνομες δοσοληψίες στο επονομαζόμενο Dark Web, όπου προβαίνουν σε αγοροπωλησία κακόβουλων εφαρμογών ή πληροφοριών για πιθανούς στόχους.

Το κυβερνοέγκλημα, στο πλαίσιο της παρούσας Στρατηγικής, δύναται να περιλαμβάνει:

- Τρομοκρατικές ενέργειες (κυβερνο-τρομοκρατία).
- Επιθέσεις άρνησης υπηρεσίας (Denial of Service, DoS – cyber extortion).
- Κυβερνο-πόλεμο (cyber warfare).

Ειδική κατηγορία θεωρούνται οι επονομαζόμενοι script kiddies που χρησιμοποιούν εργαλεία ανεπτυγμένα από τρίτα μέρη ή/και άλλους παράγοντες απειλών (π.χ. hackers), οι οποίοι αποζητούν τη φήμη μέσω της πράξης τους ή την απόκτηση μικρών χρηματικών ποσών έναντι της μη αποκάλυψης προσωπικών δεδομένων (π.χ. προσωπικές φωτογραφίες) ή της αποκρυπτογράφησης συστημάτων (εφόσον έχουν αυτά μολυνθεί με κακόβουλο λογισμικό όπως ransonware). Παρόλο που δύνανται να επηρεάσουν τη συνέχεια των επιχειρησιακών λειτουργιών, η διαφορά με τους υπόλοιπους έγκειται στη μη οργανωμένη φύση των επιθέσεών τους ή/και τη μη στοχοποίηση Φορέων

[1] Η γενική διαβάθμιση προκύπτει βάσει ερευνών στον τομέα της κυβερνοασφάλειας (π.χ. του ENISA και λοιπών φορέων).

[2] Στο πλαίσιο της Στρατηγικής Κυβερνοασφάλειας, εξετάζονται οι κυβερνοεπιθέσεις και όχι οι κακόβουλες ενέργειες του οργανωμένου εγκλήματος το οποίο δύναται να χρησιμοποιήσει ΤΠΕ για να αυξήσει τον αντίκτυπό του (π.χ. εμπόριο σαρκός). Κατά συνέπεια, η Στρατηγική επικεντρώνεται στην αντιμετώπιση των «cyber-dependent crimes» και όχι των «cyber-enabled» (HM Government, National Cyber Security Strategy 2016-2021, UK)

2.2.2 Τρίτα κράτη

Ο εν λόγω παράγοντας περιλαμβάνει ομάδες οι οποίες είτε ανήκουν, είτε χρηματοδοτούνται από κράτη και αποσκοπούν, κατά βάση, στο να εξαπολύσουν επιθέσεις που θα επιφέρουν μεγάλο αντίκτυπο στην παροχή βασικών / ουσιωδών υπηρεσιών από Φορείς. Τέτοιου είδους επιθέσεις έχουν ως κύριο στόχο τη διακοπή υπηρεσιών (π.χ. μέσω επιθέσεων άρνησης υπηρεσίας – DoS/DDoS) ή μη εξουσιοδοτημένης πρόσβασης σε διαβαθμισμένα δεδομένα. Ιδιαίτερη μνεία πρέπει να γίνει σε περιπτώσεις κυβερνο-κατασκοπείας, όπου διακρίνεται, τα τελευταία έτη[3], έξαρση επιθέσεων σε Φ.Ε.Β.Υ.

Οι επιθέσεις αυτής της κατηγορίας διακρίνονται, συνήθως, για την επίμονη φύση τους (persistence) και το γεγονός ότι έχουν σχεδιαστεί λεπτομερώς για να επιφέρουν καίρια πλήγματα.

Είθισται ομάδες του κυβερνοχώρου να επιτίθενται σε φορείς Δημόσιας Διοίκησης ή Φ.Ε.Β.Υ. / Π.Ψ.Υ. στο όνομα ενός τρίτου κράτους. Οι επιθέσεις αυτές, που κατά βάση αποσκοπούν σε αλλοίωση ιστοσελίδων ή/και προσωρινή άρνηση υπηρεσιών, πρέπει να αντιμετωπιστούν αφενός με σοβαρότητα, αφετέρου όμως στο πλαίσιο ακτιβιστικών ενεργειών και όχι ως απόρροια ενεργειών τρίτων κρατών.

2.2.3 Ακτιβιστές

Αυτό-αποκαλούμενοι ακτιβιστές ή αντίστοιχες ομάδες που προβαίνουν σε κακόβουλες ενέργειες όπως επιθέσεις άρνησης υπηρεσιών, αλλοίωση ιστοσελίδων, επιθέσεις/αντεπιθέσεις σε κράτη, κλπ. Στόχος των ακτιβιστών (συχνά αναφερόμενοι ως hacktivists) είναι η προώθηση κάποιας κοινωνικής αλλαγής ή πολιτικής ατζέντας ή αντεπίθεσης για την τόνωση του εθνικού φρονήματος, η οποία συχνά συνοδεύεται από προειδοποίηση για παύση της «γενεσιουργού αιτίας» υπό την απειλή της παράτασης ή/και επανάληψης ή/και κλιμάκωσης της επίθεσης.

2.2.4 Εσωτερικές απειλές

Ο παράγοντας αυτός αφορά σε υπαλλήλους οργανισμών που προβαίνουν, είτε εκούσια, είτε ακούσια, σε κακόβουλες ενέργειες. Λόγω της φύσης και του επιπέδου πρόσβασης σε συστήματα και πληροφορίες ενός Φορέα, καθώς και της προσέγγισης περιμετρικής ασφάλειας που υιοθετούν αρκετοί Φορείς, οι εσωτερικές απειλές αποτελούν τον μεγαλύτερο παράγοντα απειλών και έναν από τους πιο δύσκολους στην αναγνώριση και αντιμετώπισή τους.

[3] ENISA Threat Landscape Report, 2018

2.3 ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ - ΝΕΕΣ ΠΡΟΚΛΗΣΕΙΣ (ΔΙΚΤΥΑ 5G, ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ, BIG DATA, CLOUD COMPUTING, IOT).

Οι τεχνολογικές εξελίξεις παρουσιάζουν ταχύτατους ρυθμούς σε παγκόσμιο επίπεδο, περνώντας σε μια νέα τροχιά εφαρμογών και δικτύωσης. Στο πλαίσιο της νέας τεχνολογίας δικτύων 5ης γενιάς, όπου οι ταχύτητες συνδεσιμότητας εκτιμάται να φτάσουν έως και 20 Gigabits ανά δευτερόλεπτο[4], επιτρέπεται η βελτιστοποίηση της αξιοποίησης νέων τεχνολογιών από τη μονάδα του νοικοκυριού (smart home) και της επιχείρησης (smart business) μέχρι το επίπεδο των πόλεων, τις λεγόμενες έξυπνες πόλεις (smart cities), αλλά και ολόκληρους τομείς υπηρεσιών.

Οι νέες τεχνολογίες, όπως η τεχνητή νοημοσύνη (artificial intelligence), η δυνατότητα περαιτέρω ανάπτυξης έξυπνων μηχανών (έξυπνα κινητά τηλέφωνα, έξυπνα αυτοκίνητα, έξυπνες συσκευές), σε συνδυασμό με τεχνολογίες νέφους (cloud computing) και τις νέες δυνατότητες δικτύωσης των δικτύων 5ης γενιάς, έχουν τεράστιο εύρος εφαρμογών στους τομείς της υγείας (Internet of Medical Things - IoMT, ψηφιακό σύστημα υγείας, διασύνδεση υπηρεσιών παροχής υγείας και υγειονομικών πόρων), των μεταφορών (σε επίπεδο οχήματος, οδηγού, αλλά και υποδομής, με αποτέλεσμα καινοτόμες υπηρεσίες στους τομείς της οδικής ασφάλειας, του ταξιδιού, των logistics κ.λπ.), τον κατασκευαστικό τομέα (Industry 4.0), τον αγροδιατροφικό τομέα, αλλά και άλλους τομείς όπως την εθνική άμυνα (Internet of Military Things). Με το δεδομένο αυτό δεν είναι τυχαίο ότι ήδη γίνεται λόγος για Internet of Everything (IoE), ή άλλως η δια-δικτύωση των πάντων.

Παράλληλα με τις εξελίξεις αυτές, η πανδημία COVID-19 έθεσε νέα δεδομένα και νέες απαιτήσεις σε όλο το φάσμα της οικονομικής και κοινωνικής ζωής. Οι προκλήσεις και οι αδυναμίες λειτουργίας της φυσικής επαφής των ανθρώπων υπό το φως των αυξημένων κινδύνων μετάδοσης της ασθένειας, τα μέτρα περιορισμού που λαμβάνονται σε παγκόσμια κλίμακα, η παύση λειτουργίας καταστημάτων και χώρων συνάθροισης κοινού, αναζητούν εναλλακτικές μέσα στον ψηφιακό κόσμο: την τηλεδιάσκεψη (teleconference, telco), τη βιντεο-κλήση (video call), την απομακρυσμένη πρόσβαση (remote access), το ηλεκτρονικό κατάστημα (e-shop), το ψηφιακό κράτος (digital state).

Όλες οι ανωτέρω ταχύτατες εξελίξεις, σε συνδυασμό με την αυξανόμενη ζήτηση για ψηφιακές εφαρμογές και υπηρεσίες, ενέχουν σημαντικές προκλήσεις. Όσο ταχύτερα εξαπλώνεται ο ψηφιακός κόσμος σε κάθε έκφανση της καθημερινής οικονομικής και κοινωνικής ζωής, τόσο εξαπλώνεται και η επιφάνεια (surface) για κακόβουλες και παράνομες ενέργειες. Όσο οι νέες υπηρεσίες μας επιτρέπουν μεγαλύτερη προσωποποίηση και εστίαση στις δικές μας ανάγκες, τόσο αυξάνονται οι κίνδυνοι για την εκμετάλλευση ή παραβίαση των προσωπικών μας δεδομένων. Όσο ευχερέστερη καθίσταται η επικοινωνία μας με φίλους και συνεργάτες σε όλο τον πλανήτη, τόσο εξίσου εύκολη μπορεί να καταστεί η αξιοποίηση της έκθεσής μας σε ιστοτόπους κοινωνικής δικτύωσης (social networking) για την πραγματοποίηση έκνομων ενεργειών. Πρόκειται για ελάχιστα παραδείγματα, που καταδεικνύουν ότι όχι μόνο η ίδια η τεχνολογία, αλλά κυρίως ο τρόπος που τη χρησιμοποιούμε, κρύβουν κινδύνους. Για τους λόγους αυτούς, ο σχεδιασμός και η εφαρμογή μιας ολιστικής Στρατηγικής Κυβερνοασφάλειας, οφείλουν να

[4] Βλ. IMT-2020 (ITU) https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Documents/S01-1_Requirements for IMT-2020_Rev.pdf

εστιάζουν στη διαρκή εισροή γνώσης και κατανόησης των σύγχρονων τεχνολογικών εξελίξεων, την πρόβλεψη ειδικών δικλείδων ασφαλείας, αλλά και τη διαρκή ενημέρωση και ευαισθητοποίηση των χρηστών στο πλαίσιο της προαγωγής της κυβερνο-υγιεινής (cyber-hygiene).

2.4 Η Εθνικη Στρατηγικη Κυβερνοασφαλειας 2018. Προτεραιοτητες και αξιολογηση.

Το Μάρτιο του 2018, κατόπιν εισήγησης της Εθνικής Αρχής Κυβερνοασφάλειας, εκδόθηκε η 3η Αναθεώρηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας (ΑΔΑ: Ψ4Ρ7465ΧΘο-Ζ6Ω). Στην εν λόγω στρατηγική προσδιορίσθηκαν ως γενικές αρχές:

- Η ανάπτυξη και εδραίωση ενός ασφαλούς και ανθεκτικού κυβερνοχώρου.
- Η συνεχής βελτίωση των δυνατοτήτων μας στην προστασία από κυβερνοεπιθέσεις με έμφαση στις κρίσιμες υποδομές και η διασφάλιση της επιχειρησιακής συνέχειας.
- Η θεσμική θωράκιση του εθνικού πλαισίου κυβερνοασφάλειας, για την αποτελεσματική αντιμετώπιση περιστατικών κυβερνοεπιθέσεων και την ελαχιστοποίηση των επιπτώσεων από απειλές στον κυβερνοχώρο.
- 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.

Επιπλέον, τέθηκαν συνολικά δεκατρείς (13) στόχοι, πάνω στους οποίους δομήθηκε το στρατηγικό πλάνο της Εθνικής Αρχής:

Εικόνα 3. Οι 13 στόχοι της 3ης Αναθεώρησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας (2018)

Αναφορικά με τον τρέχοντα στρατηγικό σχεδιασμό κυβερνοασφάλειας, η χώρα μας υιοθετεί τα ευρωπαϊκά πρότυπα και μεθοδολογίες για την κατάρτιση του σχεδιασμού αυτού και τη στοχοθεσία του.

Κατόπιν αυτών, η Εθνική Αρχή Κυβερνοασφάλειας, στο πλαίσιο της αξιολόγησης του στρατηγικού σχεδιασμού, αξιοποίησε σχετικό εργαλείο αξιολόγησης (national cybersecurity strategies evaluation tool), το οποίο έχει αναπτυχθεί από τον Ευρωπαϊκό

Οργανισμό Κυβερνοασφάλειας (ENISA) και συμπεριλαμβάνει συνολικά δεκαπέντε (15) στόχους.

Εικόνα 4. 15 στόχοι για την αξιολόγηση των εθνικών στρατηγικών κυβερνοασφάλειας ENISA (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool)

Λαμβάνοντας υπόψη τα συμπεράσματα της ανάλυσης αποκλίσεων (gap analysis), η οποία πραγματοποιήθηκε από την Εθνική Αρχή Κυβερνοασφάλειας, οι τομείς στρατηγικού ενδιαφέροντος για την 4η Αναθεώρηση εκτείνονται σε έξι (6) διαστάσεις: Σχεδιασμός έκτακτης ανάγκης, Αναφορές περιστατικών (Incident reporting), Ασφάλεια και προστασία της ιδιωτικότητας, Έρευνα και Ανάπτυξη, Συμπράξεις Δημοσίου – Ιδιωτικού Τομέα (ΣΔΙΤ), Επενδύσεις στα μέτρα ασφάλειας. Πιο αναλυτικά, για κάθε ένα από τα ανωτέρω, ειδικοί τομείς έμφασης αναλύονται στον κατωτέρω πίνακα:

Στρατηγικές προτεραιότητες	
Σχεδιασμός έκτακτης ανάγκης	- Εθνικός σχεδιασμός διαχείρισης κρίσεων - Περιοδικές προσαρμογές του σχεδιασμού έκτακτης ανάγκης - Διαμοιρασμός πληροφοριών - Ανάπτυξη της ικανότητας διαχείρισης κινδύνων (προσδιορισμός, ανάλυση και αξιολόγηση των επιπτώσεων του κινδύνου, αξιολόγηση ευπαθειών) - Αναφορές απειλών στον κυβερνοχώρο - Χρήση πλατφορμών - Ανάπτυξη εθνικού μητρώου κινδύνων - Εργαλεία και πλατφόρμες για επίγνωση της κατάστασης
Αναφορές περιστατικών (Incident reporting)	- Συντονισμός με πλαίσιο NISD, GDPR, άρθρο 13a και eIDAS - Βέλτιστες πρακτικές για τη σύνταξη ετήσιων αναφορών συμβάντων σε εθνικό επίπεδο - Σχέδια αναφοράς τομεακών συμβάντων και αναφορών πεδίου
Ασφάλεια και προστασία της ιδιωτικότητας	- Συντονισμός με πλαίσιο ασφάλειας δεδομένων προσωπικού χαρακτήρα - Κατάρτιση και ευαισθητοποίηση
Έρευνα και Ανάπτυξη	- Καθορισμός προτεραιοτήτων - Μηχανισμοί ανάπτυξης και διάχυσης καινοτομιών (π.χ. startups, clusters κ.λπ.) - Χρηματοδότηση R&D
ΣΔΙΤ	- Εθνικό πλαίσιο - Χρηματοδότηση και κίνητρα
Επενδύσεις στα μέτρα ασφάλειας	- Βέλτιστες πρακτικές - Υποστήριξη σε startups and MME (SMEs) - Διαδικασίες

Εικόνα 5. Στρατηγικοί τομείς έμφασης για την αναθεώρηση της στρατηγικής

3 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΩΝ ΑΡΧΩΝ ΚΑΙ ΤΟΥ ΟΡΑΜΑΤΟΣ ΑΝΑΠΤΥΞΗΣ ΤΗΣ ΕΘΝΙΚΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020 - 2025

3.1 ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΑΡΧΕΣ

Με το παρόν πλαίσιο ορίζονται οι βασικές αρχές που διέπουν την προστασία των Φορέων, οι οποίες αποτελούν τους πυλώνες στους οποίους στηρίζεται η Στρατηγική:

— Όλες οι ενέργειες που προδιαγράφονται στην Στρατηγική και το Σχέδιο Δράσης αποσκοπούν στην προστασία των πολιτών και των δομών των Φορέων, αποτελώντας τη βάση όπου στηρίζεται η ψηφιακή διακυβέρνηση και ευημερία της χώρας.

— Όλες οι κυβερνοαπειλές και οι παράγοντες που ενδέχεται να επηρεάσουν την επιχειρησιακή συνέχεια της Δημόσιας Διοίκησης και λοιπών εμπλεκόμενων Φορέων αναγνωρίζονται, καταγράφονται, κατηγοριοποιούνται και αντιμετωπίζονται με τη δέουσα επιμέλεια.

— Η προστασία της ανθρώπινης ζωής και δικαιωμάτων (όπως ιδίως η προστασία των προσωπικών δεδομένων), αποτελεί σημείο ύψιστης σημασίας για τη Στρατηγική. Η Αρχή και οι Φορείς λαμβάνουν κάθε εφικτό μέτρο ώστε να διασφαλίζεται η προστασία των πολιτών σε συμμόρφωση με την κείμενη νομοθεσία και κανονισμούς.

— Η επιτυχής υλοποίηση της Στρατηγικής απαιτεί συλλογική προσπάθεια και σύμπραξη μεταξύ των Φορέων. Κατά συνέπεια, προκρίνεται η συνεργασία μεταξύ ιδιωτικών και δημοσίων φορέων, η ενίσχυση της έρευνας και ανάπτυξης στον τομέα της κυβερνοασφάλειας, καθώς και η ανταλλαγή πληροφοριών μεταξύ εθνικών και ευρωπαϊκών φορέων, με γνώμονα τη διαρκή βελτιστοποίηση της Στρατηγικής και των μέτρων υλοποίησής της.

— Η αποτελεσματικότητα της Στρατηγικής ως προς τη διασφάλιση της συνέχειας των επιχειρησιακών δραστηριοτήτων των Φορέων βασίζεται στη διαρκή ενημέρωση και εκπαίδευση όλων των εμπλεκόμενων Φορέων και των πολιτών.

— Η Στρατηγική ορίζει το πλαίσιο για να καθορισθούν συγκεκριμένοι στόχοι, ρόλοι και αρμοδιότητες, καθώς και δείκτες που θα συνδράμουν στη διαρκή αξιολόγηση και αναθεώρησή της, σε ευθυγράμμιση με το μεταβαλλόμενο περιβάλλον ΤΠΕ και απειλών, αλλά και των ζητούμενων, από τους πολίτες, υπηρεσιών.

3.2 ΔΙΑΤΥΠΩΣΗ ΤΟΥ ΣΤΡΑΤΗΓΙΚΟΥ ΟΡΑΜΑΤΟΣ

Υπό το πρίσμα των ανωτέρω αρχών και προτεραιοτήτων, η διατύπωση του οράματος για τη νέα Εθνική Στρατηγική Κυβερνοασφάλειας έχει ως ακολούθως:

«Ένα σύγχρονο και ασφαλές ψηφιακό περιβάλλον πληροφοριακών και δικτυακών υποδομών, εφαρμογών και υπηρεσιών προς όφελος της οικονομικής και κοινωνικής ευημερίας, με την

εγγύηση της προστασίας των θεμελιωδών δικαιωμάτων των πολιτών, την ανάπτυξη κουλτούρας ασφαλούς χρήσης των ψηφιακών υπηρεσιών και εφαρμογών, και την επαύξηση της εμπιστοσύνης των πολιτών και επιχειρήσεων στις ψηφιακές τεχνολογίες.»

Βασικά στοιχεία του οράματος συνιστούν:

- Η οικοδόμηση ενός σύγχρονου ψηφιακού περιβάλλοντος: Ένα ψηφιακό περιβάλλον που επιτρέπει τη διαρκή εισροή και ανάπτυξη των νέων τεχνολογιών και καινοτομιών στην ψηφιακή εποχή.
- Το υψηλό επίπεδο κυβερνοασφάλειας: Σε όλο το φάσμα των πληροφοριακών υποδομών, εφαρμογών και υπηρεσιών, προσαρμοσμένο στις διαρκώς μεταβαλλόμενες προκλήσεις και απαιτήσεις
- Η προστασία των θεμελιωδών δικαιωμάτων: Ιδίως των προσωπικών δεδομένων, της διαφύλαξης της ιδιωτικότητας, της ανάπτυξης της προσωπικότητας, της ισότητας και της συμμετοχής στην ψηφιακή κοινωνία
- Η ανάπτυξη κουλτούρας ασφαλούς χρήσης: Υπό την έννοια της ψηφιακής παιδείας, της διαρκούς ενημέρωσης και ευαισθητοποίησης στους κινδύνους και τις παγίδες των νέων τεχνολογιών
- Η επαύξηση της εμπιστοσύνης στην ψηφιακή διακυβέρνηση: Ως το βασικό επίτευγμα ενός ασφαλούς ψηφιακού περιβάλλοντος, δηλ. η αξιοποίηση των νέων τεχνολογιών σε όλο το φάσμα της κοινωνικής και οικονομικής ζωής προς όφελος των πολιτών και των επιχειρήσεων και της κοινωνικοοικονομικής ευημερίας.

4 ΜΕΘΟΔΟΛΟΓΙΑ ΑΝΑΠΤΥΞΗΣ ΤΗΣ ΣΤΡΑΤΗΓΙΚΗΣ

4.1 ΠΕΝΤΕ (5) ΣΤΡΑΤΗΓΙΚΟΙ ΣΤΟΧΟΙ

Σε ένα πρώτο επίπεδο, αξιοποιούνται τα αποτελέσματα της ανάλυσης των στρατηγικών προτεραιοτήτων, ώστε να διαμορφωθούν πέντε (5) συνολικά εμβληματικοί στόχοι ανάπτυξης του στρατηγικού σχεδιασμού, οι οποίοι καλύπτουν και τους δεκαπέντε (15) ειδικούς στόχους ανάπτυξης στρατηγικής του ENISA για τα κράτη μέλη της Ε.Ε., ως ακολούθως:

ΣΤΡΑΤΗΓΙΚΟΙ ΣΤΟΧΟΙ	ΚΑΛΥΠΤΟΜΕΝΟΙ ΣΤΟΧΟΙ ENISA ΓΙΑ ΚΡΑΤΗ ΜΕΛΗ
1. Ένα λειτουργικό σύστημα διακυβέρνησης [5]	Ανάπτυξη εθνικών σχεδίων έκτακτης ανάγκης στον κυβερνοχώρο
	Συμμετοχή σε διεθνείς συνεργασίες
	Θεσμοθέτηση της συνεργασίας μεταξύ δημόσιων οργανώσεων
2. Θωράκιση κρίσιμων υποδομών, ασφάλεια και νέες τεχνολογίες	Προστασία της υποδομής κρίσιμων πληροφοριών
	Θέσπιση βασικών μέτρων ασφαλείας
	Εξισορρόπηση την ασφάλειας με την προστασία της ιδιωτικής ζωής
3. Βελτιστοποίηση διαχείρισης περιστατικών, καταπολέμηση του κυβερνοεγκλήματος και προστασία της ιδιωτικότητας	Καθιέρωση μηχανισμών αναφοράς συμβάντων
	Καθιέρωση ικανότητας αντιμετώπισης συμβάντων
	Αντιμετώπιση του εγκλήματος στον κυβερνοχώρο
4. Ένα σύγχρονο επενδυτικό περιβάλλον με έμφαση στην προαγωγή της Έρευνας και Ανάπτυξης	Προώθηση της Έρευνας και Ανάπτυξης
	Παροχή κινήτρων στον ιδιωτικό τομέα για επενδύσεις σε μέτρα ασφαλείας
	Αξιοποίηση Συμπράξεων Δημόσιου και Ιδιωτικού τομέα (ΣΔΙΤ)
5. Ανάπτυξη ικανοτήτων (capacity building), προαγωγή της ενημέρωσης και ευαισθητοποίησης	Αύξηση της ευαισθητοποίησης των χρηστών
	Οργάνωση ασκήσεων ασφάλειας στον κυβερνοχώρο
	Ενίσχυση των προγραμμάτων κατάρτισης και εκπαίδευσης

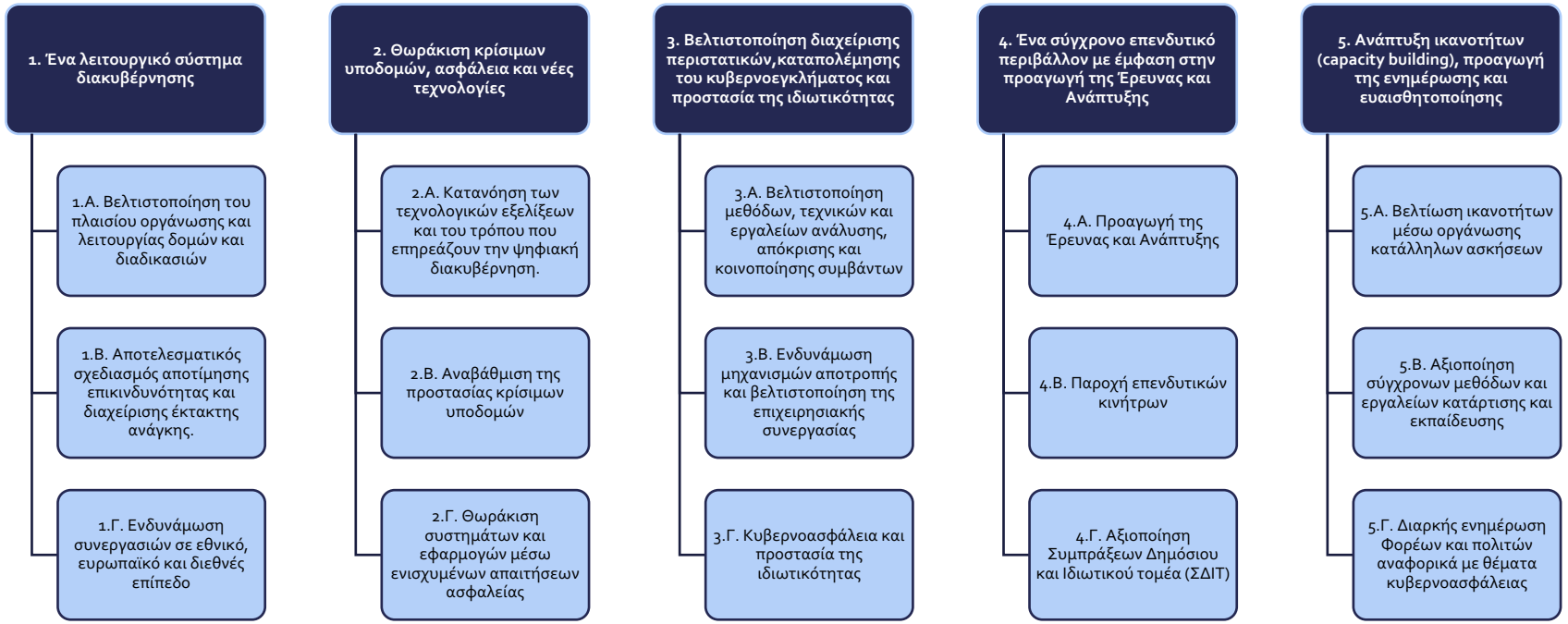
Εικόνα 6. Προσδιορισμός Στρατηγικών Στόχων βάσει των στρατηγικών προτεραιοτήτων

[5] Σημειώνεται ότι εφεξής η αναφορά σε σύστημα διακυβέρνησης αφορά το σύστημα διακυβέρνησης κυβερνοασφάλειας

Εικόνα 7. Πέντε στρατηγικοί στόχοι ανάπτυξης του στρατηγικού σχεδιασμού

4.2 Δεκαπεντε (15) Ειδικοι Στοχοι

Για κάθε έναν από τους ανωτέρω στρατηγικούς στόχους αναπτύσσονται ειδικοί στόχοι, οι οποίοι αποσκοπούν στην εξειδίκευση και καλύτερη διαχείριση του στρατηγικού πλαισίου (cascade effect). Εν συνεχεία, οι ειδικοί στόχοι εξειδικεύονται σε δραστηριότητες, οι οποίες καλύπτουν όλο το φάσμα της αναγνώρισης, πρόληψης και προστασίας, αποτροπής και ανάκαμψης από κυβερνοεπιθέσεις.



Εικόνα 8. Πλαίσιο στοχοθεσίας της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020-2025

5 ΒΑΣΙΚΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ (STAKEHOLDER MAPPING)

Στο πλαίσιο της 3ης Αναθεώρησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας τέθηκε ως βασικός στόχος η αποτύπωση των εμπλεκομένων φορέων (stakeholder mapping). Κατωτέρω παρατίθεται μια αναλυτική αποτύπωση των εμπλεκομένων φορέων, ο συντονισμός και η εμπλοκή των οποίων σε όλα τα στάδια εφαρμογής της εθνικής στρατηγικής αναδεικνύεται σε κρίσιμο παράγοντα επιτυχίας (critical success factor).

5.1 ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ - ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ (NATIONAL CYBERSECURITY AUTHORITY)

Η Γενική Διεύθυνση Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης (Εθνική Αρχή Κυβερνοασφάλειας) είναι αρμόδια για τη διαχείριση της Στρατηγικής και τον συντονισμό των Φορέων κατά την υλοποίηση των απαιτούμενων μέτρων. Μέσω του Στρατηγικού Σχεδίου, στοχεύει στον ορισμό κατάλληλων οργανωτικών, τεχνικών και λειτουργικών μέτρων, στην υλοποίησή τους από τους Φορείς, στην αξιολόγηση της Στρατηγικής, καθώς και στην αναθεώρησή της. Ειδικότερα, στις αρμοδιότητες της Αρχής συγκαταλέγονται μεταξύ άλλων:

— Συνολική διαχείριση εθνικής στρατηγικής κυβερνοασφάλειας

— Καθορισμός βασικών απαιτήσεων ασφάλειας.

— Διαχείριση θεσμικού πλαισίου.

— Συλλογή πολιτικών ασφαλείας και τήρηση σχετικού μητρώου

— Συλλογή και επεξεργασία σχεδίων αποκατάστασης για τους Φ.Ε.Β.Υ.

— Επεξεργασία των πολιτικών και διαδικασιών ασφαλείας για την πρόληψη και αντιμετώπιση περιστατικών ασφαλείας).

— Προσδιορισμός, επικαιροποίηση και αξιολόγηση των υπηρεσιών και λειτουργιών που βασίζονται ή επηρεάζουν την ασφάλεια των πληροφοριών (όπως ιδίως υπηρεσίες cloud, στρατηγική και οδηγίες ασφάλειας για την κινητή τηλεφωνία, νέες εφαρμογές αλληλογραφίας), Υποστήριξη έρευνας και ανάπτυξης.

— Υλοποίηση πλαισίου κυβερνοασφάλειας και διαχείρισης συμβάντων.

— Έλεγχος και αξιολόγηση Φορέων.

— Διαχείριση υποδομής παρακολούθησης κρίσιμων υποδομών.

- Διενέργεια τεχνικών ελέγχων ασφάλειας (π.χ. δοκιμές παρείσδυσης), εκπαιδευτικών προγραμμάτων Φορέων, τεχνικών εκπαιδεύσεων διαχειριστών και ασκήσεων κυβερνοασφάλειας, καθώς και ενημερώσεων ΥΑΠΔ Φορέων.
- Έκδοση προτύπων και εγκυκλίων.
- Έκδοση βασικών αρχών ασφαλούς αρχιτεκτονικής Φορέων.
- Καταγραφή δεικτών KPI/KRI αποτελεσματικότητας υλοποίησης Στρατηγικής στους φορείς.
- Απόκριση σε συμβάντα ασφάλειας της Αρχής ή/και Φορέων – συντονισμός δράσεων.
- Διαχείριση μητρώου συμβάντων.
- Διαχείριση κρίσεων και ενεργοποίηση Εθνικού σχεδίου έκτακτης ανάγκης.
- Αξιολόγηση και αναθεώρηση βασικών απαιτήσεων ασφάλειας.
- Αξιολόγηση και αναθεώρηση μετρικών KPI/KRI και Εθνικού σχεδίου έκτακτης ανάγκης.
- Εποπτεία και συντονισμός ΥΑΠΔ Φορέων.
- Διαχείριση μητρώου ΥΑΠΔ.
- Συνεργασία με εθνικές αρχές (ΑΠΔΠΧ, ΑΔΑΕ, κλπ) και ακαδημαϊκούς φορείς σε θέματα Κυβερνοασφάλειας
- Συνεργασία, εκπροσώπηση και διαχείριση επικοινωνίας σε ευρωπαϊκό και διεθνές επίπεδο (φορείς, κράτη μέλη, κλπ.).
- Συντονισμός δράσεων ευαισθητοποίησης Φορέων και κοινού.
- Συντονισμός δράσεων κατάρτισης, ενημέρωσης και επιμόρφωσης στελεχών.

5.2 Εθνικη Αρχη Αντιμετωπισης Ηλεκτρονικων Επιθεσεων – Εθνικο CERT (Ε.Υ.Π.)

Με τις διατάξεις του π.δ. 96/2020 (Α' 232), με τις οποίες τροποποιήθηκαν οι διατάξεις του π.δ. 1/2017 (Α' 2) που αφορούν την οργάνωση των Υπηρεσιών της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.), καθορίσθηκαν οι αρμοδιότητες της Διεύθυνσης Κυβερνοχώρου της Ε.Υ.Π., στις οποίες περιλαμβάνονται:

α) τεχνικής φύσεως θέματα ασφάλειας πληροφοριών (Εθνική Αρχή INFOSEC) και ειδικότερα για την ασφάλεια των εθνικών επικοινωνιών, των συστημάτων τεχνολογίας πληροφοριών, καθώς και για την αξιολόγηση και πιστοποίηση των διαβαθμισμένων συσκευών και συστημάτων ασφάλειας επικοινωνιών και πληροφορικής,

β) η αξιολόγηση και πιστοποίηση κρυπτοσυστημάτων, καθώς και την υποστήριξη των Ενόπλων Δυνάμεων (Ε.Δ.) και των υπηρεσιών του δημοσίου τομέα σε θέματα κρυπτασφάλειας (Εθνική Αρχή CRYPTO),

γ) η εξασφάλιση των εθνικών ηλεκτρονικών συσκευών τηλεπικοινωνιών από διαρροές λόγω ανεπιθύμητων, ηλεκτρομαγνητικών και μη μεταδόσεων (Εθνική Αρχή TEMPEST),

δ) οι αρμοδιότητες Ομάδας Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT), εντός του εθνικού πλέγματος Κυβερνοασφάλειας που καθορίζει η Εθνική Αρχή Κυβερνοασφάλειας, για τις κυβερνοεπιθέσεις εναντίον των δημοσίων φορέων της χώρας, που δεν εμπίπτουν στην αρμοδιότητα της Διεύθυνσης Κυβερνοάμυνας του Γ.Ε.ΕΘ.Α. (CSIRT). Ειδικότερα, το Εθνικό CERT της Ε.Υ.Π. υποστηρίζει την Προεδρία της Κυβέρνησης και τα Υπουργεία, με εξαίρεση το Υπουργείο Εθνικής Άμυνας, για την πρόληψη, την έγκαιρη προειδοποίηση και την αντιμετώπιση κυβερνοεπιθέσεων, εναντίον τους.

5.3 Διεύθυνση Κυβερνοαμυνας (Υπουργειο Εθνικης Άμυνας) (ΓΕΕΘΑ/ΔΙΚΥΒ)

Η Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ αποτελεί την Ελληνική Αρμόδια Ομάδα Απόκρισης Κυβερνοπεριστατικών (Computer Security Incident Response Team - CSIRT) σχετικά με την απόκριση περιστατικών στον στρατιωτικό τομέα – κυβερνοάμυνα (military CSIRT), την απόκριση περιστατικών σε φορείς που εμπίπτουν στο πεδίο εφαρμογής του ν. 4577/2018 (Φ.Ε.Β.Υ., Π.Ψ.Υ.) και την επιχειρησιακή ολοκλήρωση. Αποστολή της ανωτέρω Υπηρεσίας συνιστά η μείωση του κινδύνου εθνικών προκλήσεων στον τομέα της ασφάλειας του κυβερνοχώρου και των επικοινωνιών.

5.4 Διωξη Ηλεκτρονικου Εγκληματος (ΕΛ.ΑΣ.)

Με το π.δ. 178/2014 (Α' 281) προβλέφθηκε η ίδρυση και η διάρθρωση της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα την Αθήνα και η ίδρυση και διάρθρωση Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα τη Θεσσαλονίκη. Η αποστολή της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος συμπεριλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος είναι αυτοτελής κεντρική Υπηρεσία και υπάγεται απευθείας στον κ. Αρχηγό της Ελληνικής Αστυνομίας. Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, στην εσωτερική της δομή, αποτελείται από πέντε τμήματα που συμπληρώνουν όλο το φάσμα προστασίας του χρήστη και ασφάλειας του Κυβερνοχώρου.

Έτσι, στη νέα αναβαθμισμένη δομή της αποτελείται από τα ακόλουθα Τμήματα:

- Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών,
- Τμήμα Καινοτόμων Δράσεων και Στρατηγικής,
- Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων,

- Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης και
- Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων

5.5 Αρχη Προστασιας Δεδομενων Προσωπικου Χαρακτηρα (Α.Π.Δ.Π.Χ.)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) αποτελεί συνταγματικά κατοχυρωμένη ανεξάρτητη αρχή, με αποστολή την εποπτεία της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων, του νόμου 4624/2019, του νόμου 3471/2006 και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, και ασκεί τις αρμοδιότητες που της ανατίθενται κάθε φορά. Ειδικότερα, η Α.Π.Δ.Π.Χ. είναι επιφορτισμένη με την παρακολούθηση της εφαρμογής των διατάξεων του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679 (ΓΚΠΔ), με σκοπό την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων που τα αφορούν και τη διευκόλυνση της ελεύθερης κυκλοφορίας των δεδομένων στην Ένωση (άρθρο 51 παρ. 1, αιτ. 123 του ΓΚΠΔ). Συμβάλλει στη συνεκτική εφαρμογή του ΓΚΠΔ σε ολόκληρη την Ένωση και για το σκοπό αυτό συνεργάζεται με τις εποπτικές αρχές των κρατών μελών της ΕΕ και με την Επιτροπή (άρθρο 51 παρ. 2, αιτ. 123 του ΓΚΠΔ).

Στο ανωτέρω πλαίσιο, η Α.Π.Δ.Π.Χ., μεταξύ άλλων:

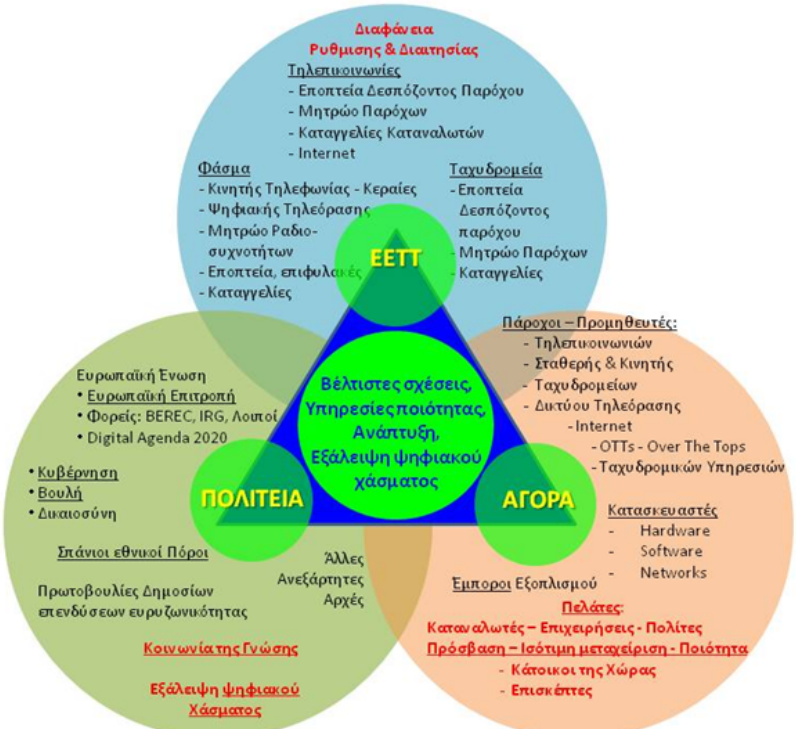
- Παρακολουθεί και επιβάλλει την εφαρμογή του ΓΚΠΔ.
- Προωθεί την ευαισθητοποίηση του κοινού στα ζητήματα προστασίας προσωπικών δεδομένων και των υπευθύνων και εκτελούντων επεξεργασία2 σχετικά με τις υποχρεώσεις τους δυνάμει του ΓΚΠΔ. Ειδική προσοχή αποδίδεται σε δραστηριότητες που απευθύνονται ειδικά σε παιδιά.
- Συμβουλεύει το εθνικό κοινοβούλιο, την κυβέρνηση και άλλα όργανα και οργανισμούς για νομοθετικά και διοικητικά μέτρα που σχετίζονται με την προστασία των προσωπικών δεδομένων.
- Παρέχει κατόπιν αιτήματος πληροφορίες στα υποκείμενα των δεδομένων σχετικά με την άσκηση των δικαιωμάτων τους.
- Χειρίζεται τις υποβληθείσες για παράβαση διατάξεων του ΓΚΠΔ καταγγελίες.
- Διενεργεί έρευνες σχετικά με την εφαρμογή του ΓΚΠΔ.
- Καταρτίζει και διατηρεί κατάλογο6 σε σχέση με την απαίτηση για διενέργεια εκτίμησης αντικτύπου (άρθρο 35 παρ. 4 του ΓΚΠΔ) και να παρέχει συμβουλές σχετικά με τις πράξεις επεξεργασίας του άρθρου 36 παρ. 2 του ΓΚΠΔ.
- Εγκρίνει κώδικες δεοντολογίας και κριτήρια πιστοποίησης και σχεδιάζει κριτήρια διαπίστευσης.
- Συνεργάζεται με άλλες εποπτικές αρχές μέσω ανταλλαγής πληροφοριών και να παρέχει αμοιβαία συνδρομή σε αυτές με σκοπό τη διασφάλιση της συνεκτικότητας εφαρμογής του ΓΚΠΔ.
- Συμβάλλει στις δραστηριότητες του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων – ΕΣΠΔ.

– Διαθέτει εξουσίες ελέγχου, καθώς και διορθωτικές, συμβουλευτικές και αδειοδοτικές εξουσίες, όπως αυτές εξειδικεύονται και αναλύονται στο άρθρο 58 του ΓΚΠΔ.

5.6 Εθνικη Επιτροπη Τηλεπικοινωνιων Και Ταχυδρομειων (Ε.Ε.Τ.Τ.)

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) είναι Ανεξάρτητη Διοικητική Αρχή. Αποτελεί τον Εθνικό Ρυθμιστή που ρυθμίζει, εποπτεύει και ελέγχει: (α) την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρίες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου και (β) την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρίες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς. Επιπλέον, η Ε.Ε.Τ.Τ. αποτελεί την αρχή ανταγωνισμού στις ανωτέρω αγορές της αρμοδιότητας της και διαθέτει όλες τις εξουσίες και τα δικαιώματα της Επιτροπής Ανταγωνισμού κατά την εφαρμογή της νομοθεσίας του ελεύθερου ανταγωνισμού στις εν λόγω αγορές (Ν.3959/2011 (Α' 93), άρθρα 101/102 ΣΛΕΕ και Κανονισμός 1/2003 ΕΚ του Συμβουλίου). Η εφαρμογή της νομοθεσίας περί ελεύθερου ανταγωνισμού από την Ε.Ε.Τ.Τ. στις αγορές της αποκλειστικής της αρμοδιότητας προβλεπόταν από τον νόμο Ν.2867/2000, τον μετέπειτα νόμο Ν.3431/2006, καθώς και τον ισχύοντα νόμο Ν.4070/2012 (ΦΕΚ 82Α/2012).

Η θέση της Ε.Ε.Τ.Τ. στο Οικοσύστημα των Επικοινωνιών και της Τεχνολογίας Πληροφορικής και οι σχέσεις της με την Πολιτεία συνοψίζεται στην ακόλουθη εικόνα:



Εικόνα 9 Η θέση της Ε.Ε.Τ.Τ. στο Οικοσύστημα των Επικοινωνιών και της Τεχνολογίας Πληροφορικής και οι σχέσεις της με την Πολιτεία (Πηγή: https://www.eett.gr/opencms/opencms/EETT/EETT/AboutEETT/)

5.7 ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΑΠΟΡΡΗΤΟΥ ΕΠΙΚΟΙΝΩΝΙΩΝ (Α.Δ.Α.Ε.)

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) έχει σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Η Α.Δ.Α.Ε είναι συνταγματικά κατοχυρωμένη ανεξάρτητη αρχή που απολαύει διοικητικής αυτοτέλειας. Έδρα της είναι η Αθήνα, μπορεί όμως με απόφασή της να εγκαθιστά και να λειτουργεί γραφεία και σε άλλες πόλεις της Ελλάδας. Οι αποφάσεις της Α.Δ.Α.Ε. κοινοποιούνται με μέριμνά της στον Υπουργό Δικαιοσύνης, ενώ στο τέλος κάθε έτους υποβάλλεται Έκθεση των πεπραγμένων της στον Πρόεδρο της Βουλής, στον Υπουργό Δικαιοσύνης και στους αρχηγούς των κομμάτων που εκπροσωπούνται στη Βουλή και στο Ευρωπαϊκό Κοινοβούλιο.

Οι κύριες αρμοδιότητες της Α.Δ.Α.Ε. είναι:

- Η διενέργεια τακτικών και έκτακτων ελέγχων σε εγκαταστάσεις δημόσιων υπηρεσιών ή και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες.
- Ο έλεγχος από πλευράς νομιμότητας σε ό,τι αφορά τους όρους και τις διαδικασίες που ακολουθούνται κατά την εφαρμογή των διατάξεων για άρση του απορρήτου, σύμφωνα με τα προβλεπόμενα στην κείμενη νομοθεσία.
- Η διενέργεια ακροάσεων παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών και ταχυδρομικών υπηρεσιών για πιθανές παραβάσεις της κείμενης νομοθεσίας για τη διασφάλιση του απορρήτου των επικοινωνιών.
- Η επιβολή των προβλεπόμενων διοικητικών κυρώσεων, σε περίπτωση που διαπιστώνεται παραβίαση της κείμενης νομοθεσίας περί απορρήτου των επικοινωνιών.
- Η έκδοση κανονιστικών και άλλων αναγκαίων πράξεων αναφορικά με τα εφαρμοστέα μέτρα για τη διασφάλιση του απορρήτου των επικοινωνιών.
- Η έκδοση γνωμοδοτήσεων, συστάσεων και υποδείξεων επί θεμάτων της αρμοδιότητας της Αρχής.
- Η εξέταση καταγγελιών για παραβίαση του απορρήτου τηλεφωνικών και διαδικτυακών επικοινωνιών ή επικοινωνιών μέσω ταχυδρομικών υπηρεσιών.

5.8 ΚΕΝΤΡΟ ΜΕΛΕΤΩΝ ΑΣΦΑΛΕΙΑΣ (Κ.Ε.Μ.Ε.Α.)

Το ΚΕ.ΜΕ.Α. είναι επιστημονικός, ερευνητικός και συμβουλευτικός φορέας που σκοπός του είναι η διεξαγωγή θεωρητικής και εφαρμοσμένης έρευνας και η εκπόνηση μελετών, ιδίως σε στρατηγικό επίπεδο, για θέματα που αφορούν την Πολιτική Ασφάλειας, καθώς και η παροχή υπηρεσιών, γνωμοδοτικού και συμβουλευτικού χαρακτήρα, σε θέματα ασφάλειας γενικότερα.

Είναι νομικό πρόσωπο ιδιωτικού δικαίου με έδρα την Αθήνακαι εποπτεύεται από τον Υπουργό Προστασίας του Πολίτη (πρώην Δημόσιας Τάξης και Προστασίας του Πολίτη). Για την εκπλήρωση των στόχων του το ΚΕ.ΜΕ.Α.:

α. διεξάγει ερευνητικά προγράμματα και μελέτες για θέματα εσωτερικής ασφάλειας που αφορούν στο Υπουργείο Προστασίας του Πολίτη (πρώην Δημόσιας Τάξης και Προστασίας του Πολίτη) και τις υπηρεσίες που υπάγονται σε αυτό, καθώς και άλλους φορείς του εσωτερικού,

β. εκπονεί και εκτελεί ερευνητικά προγράμματα ως εκπρόσωπος των εποπτευόμενων από το Υπουργείο Προστασίας του Πολίτη (πρώην Δημόσιας Τάξης και Προστασίας του Πολίτη) φορέων, για λογαριασμό ή σε συνεργασία με αντίστοιχους φορείς της Ευρωπαϊκής Ένωσης, άλλων κρατών ή διεθνών οργανισμών σύμφωνα με τους αντίστοιχους κανόνες και διαδικασίες

γ. αναπτύσσει συνεργασία σε εθνικό και διεθνές επίπεδο με οργανισμούς και υπηρεσίες, ερευνητικά και εκπαιδευτικά κέντρα και ιδρύματα, κοινωνικούς, επιστημονικούς και παραγωγικούς φορείς, δημόσιους και ιδιωτικούς, καθώς και με Μ.Κ.Ο.,

δ. προβαίνει στη μελέτη του εγκληματικού φαινομένου και των ποιοτικών και ποσοτικών μεταβολών της εγκληματικότητας στην ελληνική Επικράτεια και της γεωγραφικής κατανομής της, καθώς και στο σχεδιασμό μεθόδων και πρακτικών στην άσκηση αντεγκληματικής πολιτικής,

ε. προτείνει την εναρμόνιση των μέτρων πρόληψης και καταστολής του εγκλήματος με τις συνταγματικές αρχές, τα ατομικά και πολιτικά δικαιώματα, τη νομιμότητα και το σεβασμό της αξίας του ανθρώπου,

στ. παρακολουθεί και μελετά τις τεχνολογικές εξελίξεις των συστημάτων ασφάλειας και αξιολογεί τα νέα επιτεύγματα στο χώρο αυτόν,

ζ. διατυπώνει προτάσεις για την αξιοποίηση της τεχνογνωσίας που κατέχει

η. υποστηρίζει διαδικασίες διασυνοριακής συνεργασίας,

θ. οργανώνει και διεξάγει συνέδρια, δημοσιεύει ερευνητικά και γενικότερα επιστημονικά πορίσματα και συναφή έργα, πραγματοποιεί εκπαιδευτικά σεμινάρια και παρέχει πιστοποιημένες εκπαιδεύσεις σε θέματα ασφάλειας και εκπονεί πιστοποιημένες μελέτες σε τέτοια θέματα

ι. αναπτύσσει οποιαδήποτε άλλη συναφή με τους σκοπούς του δραστηριότητα και

ια. αποτελεί φορέα πιστοποίησης διαδικασιών, μελετών, σχεδίων για την ασφάλεια, φορέων, οργανισμών και επιχειρήσεων του Ιδιωτικού και Δημοσίου Τομέα

5.9 ΛΟΙΠΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ

Πέραν των ανωτέρω εμπλεκομένων φορέων, στους βασικούς εμπλεκόμενους φορείς συγκαταλέγονται:

- Τα Υπουργεία, ως επιτελικές πολιτικοδιοικητικές δομές, μέσω των οποίων διαμορφώνεται και υλοποιείται το κυβερνητικό έργο. Ειδικότερα, πέρα από τα Υπουργεία που έχουν οριζόντιο χαρακτήρα (π.χ. Υπουργείο Εσωτερικών, Υπουργείο Οικονομικών), σημαντικό ρόλο έχουν και τα τομεακά Υπουργεία, στα οποία αναπτύσσονται συγκεκριμένοι τομείς πολιτικής (π.χ. Υπουργείο Περιβάλλοντος και Ενέργειας, Υπουργείο Υποδομών και Μεταφορών, Υπουργείο Παιδείας και Θρησκευμάτων), με εξέχουσα σημασία για τη συνολική λειτουργία της κοινωνικοοικονομικής ζωής.
- Οι Φ.Ε.Β.Υ./Π.Ψ.Υ., σύμφωνα με το πλαίσιο του ν. 4577/2018 και της υ.α. υπ' αριθμ. 1027/2019 (Β' 3739).

ΣΤΡΑΤΗΓΙΚΟΙ ΣΤΟΧΟΙ	ΕΙΔΙΚΟΙ ΣΤΟΧΟΙ	ΒΑΣΙΚΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ
1. Ένα λειτουργικό σύστημα διακυβέρνησης	1.Α. Βελτιστοποίηση του πλαισίου οργάνωσης και λειτουργίας δομών και διαδικασιών	Ε.Α.Κ.,φορείς κεντρικής δημόσιας διοίκησης, Εθνικό CERT, CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ
	1.Β. Αποτελεσματικός σχεδιασμός αποτίμησης επικινδυνότητας και διαχείρισης έκτακτης ανάγκης.	Ε.Α.Κ., φορείς Κεντικής Δημόσιας Διοίκησης, Φ.Ε.Β.Υ./ Π.Ψ.Υ., CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ, Εθνικό CERT, ΚΕΜΕΑ
	1.Γ. Ενδυνάμωση συνεργασιών σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο	Ε.Α.Κ., ΥΠΕΞ, Εθνικό CERT
2. Θωράκιση κρίσιμων υποδομών, ασφάλεια και νέες τεχνολογίες	2.Α. Κατανόηση των τεχνολογικών εξελίξεων και του τρόπου που επηρεάζουν την ψηφιακή διακυβέρνηση.	Ε.Α.Κ., Ερευνητικοί – Επιστημονικοί φορείς, Α.Δ.Α.Ε., Ε.Ε.Τ.Τ., Γ.Γ.Ε.Τ., ΥΠΕΞ, Εθνικό CERT
	2.Β.Αναβάθμιση της προστασίας κρίσιμων υποδομών	Ε.Α.Κ., Φ.Ε.Β.Υ. / Π.Ψ.Υ., CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ, Εθνικό CERT
	2.Γ.Θωράκιση συστημάτων και εφαρμογών μέσω ενισχυμένων απαιτήσεων ασφαλείας	Ε.Α.Κ., φορείς Κεντικής Δημόσιας Διοίκησης, Φ.Ε.Β.Υ./ Π.Ψ.Υ., CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ, Εθνικό CERT, ΚΕΜΕΑ
3. Βελτιστοποίηση διαχείρισης περιστατικών, καταπολέμησης του κυβερνοεγκλήματος και προστασία της ιδιωτικότητας	3.Α. Βελτιστοποίηση μεθόδων, τεχνικών και εργαλείων ανάλυσης, απόκρισης και κοινοποίησης συμβάντων	Ε.Α.Κ., ΓΕΕΘΑ/ΔΙΚΥΒ, Εθνικό CERT, ΕΛ.ΑΣ/Δ.Η.Ε.
	3.Β. Ενδυνάμωση μηχανισμών αποτροπής και βελτιστοποίηση της επιχειρησιακής συνεργασίας	Ε.Α.Κ., ΓΕΕΘΑ/ΔΙΚΥΒ, Εθνικό CERT, ΕΛ.ΑΣ/Δ.Η.Ε.
	3.Γ. Κυβερνοασφάλεια και προστασία της ιδιωτικότητας	Ε.Α.Κ., ΑΠΔΠΧ, ΑΔΑΕ
4. Ένα σύγχρονο επενδυτικό περιβάλλον με έμφαση στην προαγωγή της Έρευνας και Ανάπτυξης	4.Α. Προαγωγή της Έρευνας και Ανάπτυξης	Ε.Α.Κ., Γενική Γραμματεία Έρευνας και Τεχνολογίας, Υπουργείο Ανάπτυξης και Επενδύσεων, Υπουργείο Οικονομικών, ΚΕΤΥΑΚ/ΕΥΠ
	4.Β. Παροχή επενδυτικών κινήτρων	Ε.Α.Κ., Υπουργείο Ανάπτυξης και Επενδύσεων, Υπουργείο Οικονομικών
	4.Γ. Αξιοποίηση Συμπράξεων Δημόσιου και Ιδιωτικού τομέα (ΣΔΙΤ)	Ε.Α.Κ., Υπουργείο Ανάπτυξης και Επενδύσεων, Υπουργείο Οικονομικών
5. Ανάπτυξη ικανοτήτων (capacity building), προαγωγή της ενημέρωσης και ευαισθητοποίησης	5.Α. Βελτίωση ικανοτήτων μέσω οργάνωσης κατάλληλων ασκήσεων	Ε.Α.Κ., ΓΕΕΘΑ/ΔΙΚΥΒ, Εθνικό CERT, ΕΛ.ΑΣ/Δ.Η.Ε.
	5.Β. Αξιοποίηση σύγχρονων μεθόδων και εργαλείων κατάρτισης και εκπαίδευσης	Ε.Α.Κ., Υπουργείο Παιδείας και Θρησκευμάτων, Επιστημονικοί και Ερευνητικοί φορείς

	5.Γ. Διαρκής ενημέρωση Φορέων και πολιτών αναφορικά με θέματα κυβερνοασφάλειας	Όλοι οι εμπλεκόμενοι φορείς, πολίτες, επιχειρήσεις

Εικόνα 10 Βασικοί εμπλεκόμενοι φορείς ανά Στρατηγικό και Ειδικό Στόχο της Εθνικής Στρατηγικής για την Κυβερνοασφάλεια 2020-2025

6 ΚΡΙΣΙΜΟΙ ΠΑΡΑΓΟΝΤΕΣ ΕΠΙΤΥΧΙΑΣ (CRITICAL SUCCESS FACTORS)

6.1 ΑΝΑΛΥΣΗ S.W.O.T.

Η υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας είναι άρρηκτα συνδεδεμένη αφενός με τη λειτουργία της Γενικής Διεύθυνσης Κυβερνοασφάλειας, αφετέρου με την υλοποίησή της από τους εμπλεκόμενους φορείς. Προκειμένου να αναλυθούν επαρκώς οι εσωτερικοί και εξωτερικοί παράγοντες που θα συμβάλουν στην επιτυχή υλοποίηση της Στρατηγικής και διασφάλισης των παρεχόμενων υπηρεσιών στους πολίτες, ο παρακάτω πίνακας συνοψίζει τα δυνατά σημεία (Strengths), αδύνατα σημεία (Weaknesses), ευκαιρίες (Opportunities) και απειλές (Threats), εν είδη ανάλυσης SWOT.

Δυνατά σημεία	**Ευκαιρίες**
— Δέσμευση του Υπουργείου Ψηφιακής Διακυβέρνησης, αλλά και της Κυβέρνησης συνολικά, για τη χάραξη και υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας. — Τεχνογνωσία στελεχών Αρχής και ευέλικτες διαδικασίες. — Ύπαρξη φορέων (δημόσιοι, όπως ΓΓΕΘΑ/ΔΙΚΥΒ, ΕΥΠ, αλλά και ιδιωτικοί) οι οποίοι εξειδικεύονται σε θέματα κυβερνοασφάλειας.	— Υλοποίηση στρατηγικής ψηφιακής διακυβέρνησης στη χώρα, η οποία εισάγει την έννοια της κυβερνοασφάλειας από τον σχεδιασμό και εξ ορισμού (security by design and by default). — Συμπράξεις με δημόσιους και ιδιωτικούς φορείς (π.χ. μέσω ΣΔΙΤ) οι οποίοι μπορούν να συνδράμουν την Αρχή στο έργο της.
Αδύνατα σημεία	**Απειλές**
— Κίνητρα προσέλκυσης και διατήρησης προσωπικού με κατάλληλα – υψηλά τεχνικά προσόντα. — Δημοσιονομικοί περιορισμοί και σύνθετες διαδικασίες πραγματοποίησης προμηθειών και παροχής υπηρεσιών — Κατακερματισμός και πολυπλοκότητα δομών και διαδικασιών – προκλήσεις στο συντονισμό	— Μέθοδος λειτουργίας (modus operandi) επιτιθέμενων – παραγόντων απειλών, που δεν συνάδουν με καμία επιχειρησιακή ή λειτουργική πρακτική (π.χ. ωράριο, αριθμός στελεχών, μισθολογικά κίνητρα, κλπ.). — Ταχύς ρυθμός τεχνολογικών εξελίξεων – εγγενείς δυσκολίες στην παρακολούθηση και κατανόηση

Κατά συνέπεια, η επιτυχία της Στρατηγικής εξαρτάται από συγκεκριμένες προϋποθέσεις (critical success factors), οι οποίες πρέπει να ληφθούν υπόψη από όλους τις εμπλεκόμενους φορείς, συμπεριλαμβανομένων και των κατά περίπτωση αρμόδιων φορέων.

6.2 ΠΡΟΫΠΟΘΕΣΕΙΣ ΠΟΥ ΑΦΟΡΟΥΝ ΤΗΝ ΑΡΧΗ

— Επάρκεια πόρων - στελέχωση.

Η επαρκής στελέχωση τις Αρχής, σύμφωνα με τις ισχύουσες οργανικές διατάξεις είναι απαραίτητη για την επαρκή ανάληψη αρμοδιοτήτων και την επίτευξη των στόχων της Στρατηγικής. Λόγω της φύσης του έργου που καλείται να επιτελέσει η Αρχή, τα στελέχη της παρέχουν εξειδικευμένες υπηρεσίες, ενώ παράλληλα θα πρέπει να βρίσκονται σε ετοιμότητα για παροχή εργασίας και πέραν του συνήθους ωραρίου απασχόλησης που ισχύει για το προσωπικό του δημοσίου.

— Περαιτέρω ενδυνάμωση ρυθμιστικού πλαισίου

Στο πλαίσιο της αποτελεσματικής υλοποίησης των αρμοδιοτήτων της Αρχής, κρίσιμη αναδεικνύεται η σημασία της περαιτέρω ενδυνάμωσης του ρυθμιστικού πλαισίου, ιδίως μέσω της θέσπισης σαφών και συνεκτικών ρυθμίσεων, λαμβάνοντας υπόψη τους κανόνες και τις αρχές της Καλής Νομοθέτησης.

— Ευελιξία συμπράξεων μέσω ΣΔΙΤ.

Σε περιπτώσεις που η Αρχή κρίνει ότι η σύμπραξη με ιδιωτικούς φορείς (μέσω ΣΔΙΤ) θα προσδώσει σημαντικά οφέλη στο έργο της, θα πρέπει η Αρχή να είναι σε θέση να συμπράξει με φορείς του ιδιωτικού τομέα με όρους ανάλογης ευελιξίας.

— Επαρκής χρηματοδότηση για τον σχεδιασμό, ανάπτυξη και υλοποίηση των δράσεων.

Η επαρκής χρηματοδότηση και ανάθεση κονδυλίων προς την Αρχή είναι απαραίτητη για να υποστηρίξει τον ολοκληρωμένο σχεδιασμό, ανάπτυξη, υλοποίηση και παρακολούθηση των δράσεων του Στρατηγικού Σχεδίου.

— Κατάλληλος εξοπλισμός

Για την εκπλήρωση της αποστολής και των αρμοδιοτήτων της Αρχής, κρίνεται επίσης απαραίτητη η ενδυνάμωσή της με σύγχρονο εξοπλισμό, υλικοτεχνικές υποδομές και εγκαταστάσεις.

6.3 ΠΡΟΫΠΟΘΕΣΕΙΣ ΠΟΥ ΑΦΟΡΟΥΝ ΤΟΥΣ ΦΟΡΕΙΣ

— Κίνητρα επένδυσης. Ένας από τους βασικούς στόχους της Στρατηγικής αποτελεί η ενίσχυση επενδυτικών προγραμμάτων στην κυβερνοασφάλεια από τον ιδιωτικό τομέα και λοιπούς Φορείς. Θα πρέπει να παρασχεθούν τα κατάλληλα κίνητρα (π.χ. οικονομικά – φορολογικές ελαφρύνσεις) ώστε οι φορείς δημοσίου και ιδιωτικού τομέα να επενδύσουν στην κυβερνοασφάλεια.

— Κίνητρα συνεργασίας. Συγχρόνως, θα πρέπει να δοθούν κατάλληλα κίνητρα ώστε να διευκολυνθεί η συνεργασία μεταξύ φορέων δημοσίου/ ιδιωτικού τομέα και εκπαιδευτικών ιδρυμάτων, ώστε να προαχθούν οι στόχοι συνεργασίας με ιδιωτικούς φορείς οι οποίοι μπορεί να παράσχουν κρίσιμες πληροφορίες και υπηρεσίες στην Αρχή, να υποστηρίξουν την έρευνα και ανάπτυξη στον τομέα της κυβερνοασφάλειας, καθώς και να ενισχύσουν τη διενέργεια εκπαιδευτικών προγραμμάτων.

7 ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ 1. ΕΝΑ ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

7.1 ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ 1.Α.: ΒΕΛΤΙΣΤΟΠΟΙΗΣΗ ΤΟΥ ΠΛΑΙΣΙΟΥ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΛΕΙΤΟΥΡΓΙΑΣ ΔΟΜΩΝ ΚΑΙ ΔΙΑΔΙΚΑΣΙΩΝ

Θεμελιώδη προτεραιότητα για την εφαρμογή της Εθνικής Στρατηγικής Κυβερνοασφάλειας συνιστά η ανάπτυξη ενός ολοκληρωμένου συστήματος διακυβέρνησης του «ελληνικού κυβερνοχώρου», υπό το συντονιστικό ρόλο της Αρχής, στο πλαίσιο του οποίου:

- Αντιμετωπίζονται ολιστικά όλοι οι τομείς παρέμβασης για την κυβερνοασφάλεια[6]
- Καθορίζονται σαφείς ρόλοι και αρμοδιότητες για όλους τους εμπλεκόμενους φορείς
- Προβλέπονται σαφείς, εκ των προτέρων καθορισμένες διαδικασίες, βάσει των οποίων το σύστημα διακυβέρνησης οργανώνεται, λειτουργεί και εξελίσσεται.

Υπό το πρίσμα των ανωτέρω αρχών, διαμορφώνεται ένα σύστημα το οποίο έχει την Εθνική Αρχή Κυβερνοασφάλειας ως επιτελικό πυλώνα (lead agency) και κατόπιν ένα δίκτυο φορέων και υπευθύνων ασφαλείας σε επίπεδο: α. προληπτικών ενεργειών και β. απόκρισης και διασφάλισης επιχειρησιακής συνέχειας:

Κρίσιμοι τομείς του ν. 4577/2018 (Φ.Ε.Β.Υ. – Π.Ψ.Υ.)

- Ενέργεια (Υπουργείο Περιβάλλοντος και Ενέργειας, Φ.Ε.Β.Υ. – Π.Ψ.Υ.)
- Μεταφορές (Υπουργείο Υποδομών και Μεταφορών, Φ.Ε.Β.Υ. – Π.Ψ.Υ.)
- Τράπεζες (Υπουργείο Ανάπτυξης και Επενδύσεων – ΤτΕ, Φ.Ε.Β.Υ. – Π.Ψ.Υ.)
- Υποδομές χρηματιστηριακών αγορών (Υπουργείο Ανάπτυξης και Επενδύσεων, Φ.Ε.Β.Υ. – Π.Ψ.Υ.)
- Τομέας της υγείας (Υπουργείο Υγείας, Φ.Ε.Β.Υ. – Π.Ψ.Υ.)
- Προμήθεια και διανομή πόσιμου νερού (Υπουργείο Υποδομών και Μεταφορών, Φ.Ε.Β.Υ. – Π.Ψ.Υ.)
- Ψηφιακή υποδομή (IXP, DNS, TLD) (Υπουργείο Ψηφιακής Διακυβέρνησης – Ε.Ε.Τ.Τ. , Φ.Ε.Β.Υ. – Π.Ψ.Υ.)

Κρίσιμοι τομείς (εκτός ν.4577/2018)

- Τηλεπικοινωνίες (Υπουργείο Ψηφιακής Διακυβέρνησης, Ε.Ε.Τ.Τ., Α.Δ.Α.Ε.)
- Δικαιοσύνη (Υπουργείο Δικαιοσύνης, Δικαστική Λειτουργία)
- Παιδεία (Υπουργείο Παιδείας και Θρησκευμάτων)

Δημόσιο - Δημόσια Διοίκηση

- Κεντρική Δημόσια Διοίκηση (ν. 4622/2019, Α΄ 133):
  (α) Η Προεδρία της Δημοκρατίας,

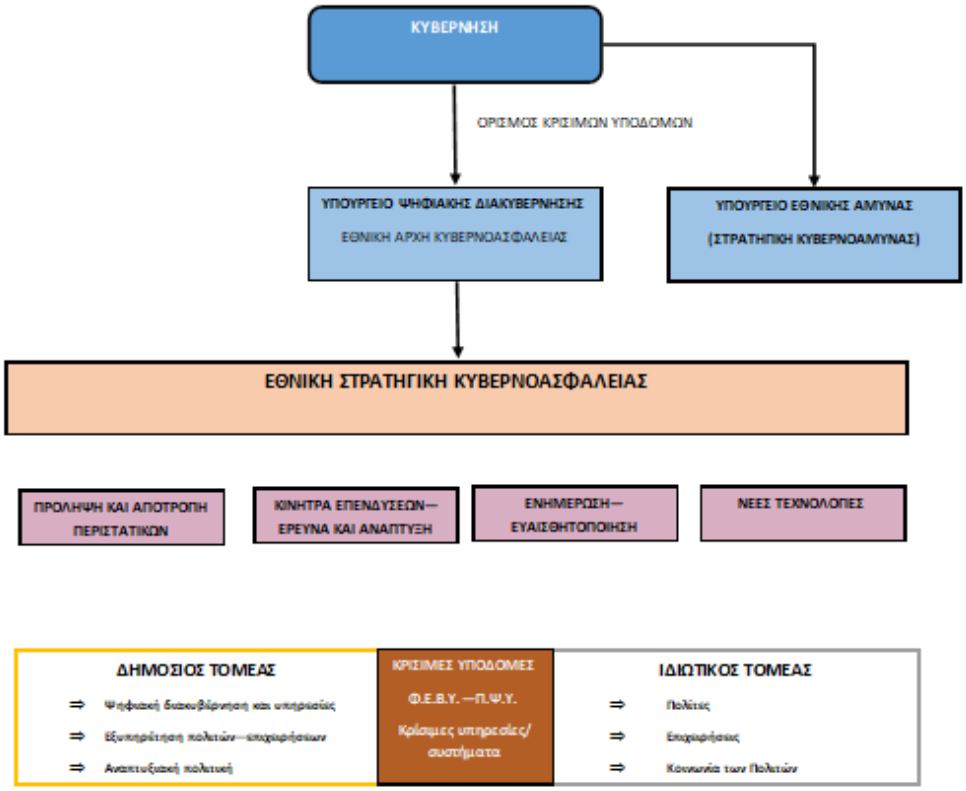
[6] Σημειώνεται ότι από το ανωτέρω πλαίσιο εξαιρούνται τα διαβαθμισμένα κατά Ε.Κ.Α. Συστήματα Επικοινωνιών και Πληροφορικής (Σ.Ε.Π.)

(β) η Προεδρία της Κυβέρνησης,
(γ) τα Υπουργεία και οι αποκεντρωμένες ή περιφερειακές υπηρεσίες τους,
(δ) οι Αποκεντρωμένες Διοικήσεις και
(ε) οι Ανεξάρτητες Αρχές.

- Ο.Τ.Α. α' και β΄ βαθμού
- Λοιποί φορείς Γενικής Κυβέρνησης (Ν.Π.Δ.Δ., Ν.Π.Ι.Δ., εταιρίες του δημοσίου, δημόσιες επιχειρήσεις κ.λπ.)

Ιδιωτικός τομέας

- Εξυπηρέτηση πολιτών
- Επιχειρήσεις
- Κοινωνία των Πολιτών



Εικόνα 11 Πλαίσιο διακυβέρνησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020-2025

Ειδικότερα, στις εμβληματικές δραστηριότητες του εν λόγω ειδικού στόχου συγκαταλέγονται, μεταξύ άλλων:

7.1.1 Ανάπτυξη ολοκληρωμένου συστήματος διαχείρισης κυβερνοασφάλειας για φορείς του δημοσίου

Με γνώμονα τη βελτιστοποίηση της διακυβέρνησης και την επαύξηση της κυβερνοασφάλειας συστημάτων και δικτύων του δημοσίου, κρίσιμη δράση συνιστά η ανάπτυξη ενός ολοκληρωμένου πλαισίου διαχείρισης της κυβερνοασφάλειας δημοσίων φορέων προκειμένου να:

- ✓ Προλαμβάνονται και αντιμετωπίζονται περιστατικά
- ✓ Αξιοποιείται η πιο σύγχρονη τεχνολογία σε δημόσιες υποδομές και υπηρεσίες με ασφαλή τρόπο
- ✓ Διαχέεται άμεσα και έγκαιρα η γνώση για τρόπους θωράκισης συστημάτων δικτύου και πληροφοριών

Υπό το πρίσμα αυτό απαιτούνται:

- Λειτουργική αναδιοργάνωση - ενδυνάμωση των υπηρεσιών πληροφορικής και ηλεκτρονικής διακυβέρνησης
- Ορισμός Υπευθύνων Ασφάλειας Πληροφοριακών Συστημάτων και Δικτύων
- Κεντρική έκδοση οδηγιών, κατευθύνσεων, ειδοποιήσεων και απαιτήσεων ασφάλειας από την Εθνική Αρχή Κυβερνοασφάλειας
- Αναβάθμιση του σχεδιασμού ασφάλειας πληροφοριακών συστημάτων και δικτύων δημοσίων φορέων στη βάση μεθοδολογίας ανάλυσης κινδύνου
- Αναβάθμιση του CERT με γνώμονα τη βελτιστοποίηση της απόκρισης και αντιμετώπισης περιστατικών.

Εικόνα 12 Πολιτικές και απαιτήσεις ασφάλειας για δημόσιους φορείς

7.1.2 Ανάπτυξη πλαισίου προαγωγής της αριστείας στον τομέα της κυβερνοασφάλειας (cybersecurity excellence management framework)

Επιπλέον εμβληματική δράση αποτελεί η διαμόρφωση και εφαρμογή ενός ολοκληρωμένου πλαισίου για την προαγωγή της αριστείας στον τομέα της κυβερνοασφάλειας. Συγκεκριμένα, με το παρόν πλαίσιο πρόκειται να συλλεχθούν διεθνείς και ευρωπαϊκές καλές πρακτικές σε έναν πρακτικό οδηγό (handbook) με συστάσεις και οδηγίες, προκειμένου οι φορείς να μπορούν εύκολα και γρήγορα να λάβουν άμεσα μέτρα ενδυνάμωσης του επιπέδου κυβερνοασφάλειάς τους. Ο οδηγός αυτός θα πλαισιώνεται περαιτέρω από ένα εργαλείο αυτο-αξιολόγησης (self assessment tool), καθώς και από ένα σύστημα αναγνώρισης και παροχής κινήτρων, μέσω του οποίου θα αναδεικνύονται οι φορείς που έχουν σημειώσει τις υψηλότερες επιδόσεις.

7.2 Ειδικος Στοχος 1.Β.: Αποτελεσματικος σχεδιασμος αποτιμησης επικινδυνοτητας και διαχειρισης εκτακτης αναγκης.

Η αποτελεσματική προστασία έναντι απειλών που μπορεί να επηρεάσουν την παροχή υπηρεσιών στους πολίτες προϋποθέτει κατ' αρχάς την αναγνώριση και καταγραφή των απειλών αυτών. Η αναγνώριση των απειλών κυβερνοασφάλειας βασίζεται σε δομημένη μεθοδολογία που αναπτύσσεται για αυτό το σκοπό, στο πλαίσιο της οποίας προάγεται η συνεργασία με φορείς όπως η Εθνική Υπηρεσία Πληροφοριών, το ΓΕΕΘΑ, και ο Ευρωπαϊκός Οργανισμός Ασφάλειας Πληροφοριών και Δικτύων (ENISA). Θεμελιώδεις παρεμβάσεις στο πλαίσιο του εν λόγω στόχου συνιστούν η ανάπτυξη μεθοδολογίας ανάλυσης δεδομένων και μητρώου καταγραφής απειλών, η διαμόρφωση εθνικού σχεδιασμού αποτίμησης επικινδυνότητας και ο εθνικός σχεδιασμός έκτακτης ανάγκης.

Ειδικότερα, στις εμβληματικές δραστηριότητες του εν λόγω ειδικού στόχου συγκαταλέγονται, μεταξύ άλλων:

7.2.1 Αξιολόγηση κινδύνων και κατάρτιση Εθνικού Σχεδίου Αποτίμησης Επικινδυνότητας

Η αξιολόγηση των κινδύνων κυβερνοασφάλειας και η αποτελεσματική διαχείρισή τους αποτελούν έναν από τους βασικούς πυλώνες της κυβερνοασφάλειας και της ψηφιακής διακυβέρνησης. Για το σκοπό αυτό απαιτείται:

- ο καθορισμός συγκεκριμένου πλαισίου βάσει του οποίου οι Φορείς θα αναγνωρίζουν τις κρίσιμες επιχειρησιακές δραστηριότητες και πληροφοριακούς πόρους που τις υποστηρίζουν,
- ο καθορισμός συγκεκριμένου πλαισίου βάσει του οποίου οι Φορείς θα αναγνωρίζουν τους εξωτερικούς και εσωτερικούς παράγοντες οι οποίοι δύναται να επηρεάσουν την ασφάλεια των πληροφοριακών πόρων,

- η κατάρτιση προφίλ απειλών και αξιολόγηση των αδυναμιών που οι απειλές ενδέχεται να εκμεταλλευτούν,
- η κατάρτιση σχεδίου αντιμετώπισης κινδύνων κυβερνοασφάλειας.

Επίσης, καίρια δράση συνιστά η εκπόνηση μελέτης αποτίμησης επικινδυνότητας σε εθνικό επίπεδο, ακολουθώντας μια επιστημονική 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, λαμβάνει 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.

7.2.2 Εκπόνηση Εθνικού Σχεδίου Έκτακτης Ανάγκης

Οι ανωτέρω δράσεις θα αποτελέσουν αρωγό για την υποστήριξη του Εθνικού Σχεδίου Έκτακτης Ανάγκης, ενώ θα διευκολυνθεί η κατηγοριοποίηση των Φορέων αναλόγως των υπηρεσιών που προσφέρουν και η συμμόρφωση με την κείμενη νομοθεσία και κανονισμούς (όπως ενδεικτικά NIS Directive και Ν. 4577/2018).

Το Εθνικό Σχέδιο Έκτακτης Ανάγκης αποτελεί τον οδηγό για την αντιμετώπιση συμβάντων που κρίνονται ως σοβαρές διαταράξεις για τις παρεχόμενες από τους Φορείς υπηρεσίες και υπάγεται στη σφαίρα της διαχείρισης κρίσεων (crisis management). Κατά συνέπεια, το Σχέδιο περιλαμβάνει τα κριτήρια τα οποία κατηγοριοποιούν ένα συμβάν ως κρίση, τους ρόλους αναφορικά με τη διαχείριση των κρίσεων και τις αρμοδιότητές τους, καθώς και τις ενέργειες που θα πρέπει να λάβουν χώρα για την επιτυχή αντιμετώπιση του συμβάντος, ενεργοποιώντας ταυτόχρονα όλες τις κατάλληλες δικλείδες που θα μετριάσουν τις επιπτώσεις και θα αποτρέψουν τη διακοπή της παροχής υπηρεσιών. Το Εθνικό Σχέδιο Έκτακτης Ανάγκης ενεργοποιείται για απόκριση σε συμβάντα τα οποία προκαλούν σοβαρή διατάραξη στην παροχή υπηρεσιών από τους Φορείς, ή θέτουν σε κίνδυνο την εν γένει παροχή υπηρεσιών προς τους πολίτες. Τέτοιου είδους συμβάντα αναφέρονται ως κρίσεις, με το Σχέδιο να αποτελεί το εγχειρίδιο διαχείρισης κρίσεων (crisis management).

Το Εθνικό Σχέδιο Έκτακτης Ανάγκης περιλαμβάνει τα ακόλουθα:

- **Ορισμοί (διαχείριση κρίσεων, επιχειρησιακή συνέχεια).**

Περιλαμβάνονται όλοι οι ορισμοί αναφορικά με τη διαχείριση κρίσεων, ώστε να εμπλεκόμενα μέρη να ευθυγραμμιστούν αναφορικά με τη χρησιμοποιούμενη ορολογία και να αναπτύσσεται κοινή γλώσσα επικοινωνίας.

- **Κριτήρια.**

Κριτήρια τα οποία ορίζουν πότε ένα συμβάν θεωρείται ως κρίση ή/και απαιτεί την ενεργοποίηση του Εθνικού Σχεδίου Έκτακτης Ανάγκης.

- **Σενάρια, ρόλοι και αρμοδιότητες.**

Περιγραφή σεναρίων που υπάγονται στον ορισμό κρίσης, βάσει των προαναφερθέντων κριτηρίων.

Καταγραφή ρόλων και κομβικών ενδιαφερόμενων μερών (key stakeholders), καθώς και των αρμοδιοτήτων τους σε κατάσταση ετοιμότητας, ενεργοποίησης του Σχεδίου και ανάκαμψης.

Περιγραφή ενεργειών κατά τη διάρκεια μιας κρίσης.

- **Συσχετισμοί με σχέδια επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφές.**

Καταγραφή συσχετισμών με σχέδια επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφές, ώστε να διευκολύνεται η επίλυση μιας κρίσης και να εκτελούνται οι απαιτούμενες ενέργειες για ανάκαμψη και επιστροφή στην κανονικότητα.

Τεχνολογίες και πόροι για την αναγνώριση, την αντιμετώπιση και την ανάκαμψη.

- **Εκτίμηση, ανάλυση και αναγνώριση ευπαθειών/κινδύνων.**

Καταγραφή αποτελεσμάτων αξιολόγησης κινδύνων κυβερνοασφάλειας που ενδέχεται να οδηγήσουν σε κρίση.

- **Αναγνώριση επικείμενης κρίσης (Identify Crisis signals).**

Μεθοδολογία έγκαιρης αναγνώρισης επικείμενης κρίσης, με στόχο την άμεση ενεργοποίηση του Σχεδίου.

- **Επικοινωνία για τη διαχείριση κρίσης (επικοινωνία μεταξύ Φορέων, διαχείριση σχέσεων, επικοινωνία με τα Μ.Μ.Ε., επικοινωνία με αρμόδια υπουργεία, κ.λπ.)**

Στοιχεία επικοινωνίας, έτοιμα μηνύματα, απόδοση ρόλων.

- **Επιλογές ασκήσεων.**

Ανάλυση ασκήσεων.

Ενδεικτικά σενάρια.

Σχέδιο διενέργειας ασκήσεων.

7.2.3 Αξιοποίηση σύγχρονων μηχανισμών ανταλλαγής πληροφοριών

Η ανταλλαγή πληροφοριών 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.

7.3 Ειδικος Στοχος 1.Γ.: Ενδυναμωση συνεργασιων σε εθνικο, ευρωπαϊκο και διεθνες επιπεδο

Οι σύγχρονες τεχνολογίες έχουν συμβάλει στην ανάπτυξη ενός έντονα διασυνδεδεμένου περιβάλλοντος που δεν οριοθετείται από σύνορα. Με στόχο την διαφύλαξη των κοινών συμφερόντων, έχει αναπτυχθεί ο κλάδος της κυβερνοδιπλωματίας που προωθεί την υπεύθυνη συμπεριφορά στον κυβερνοχώρο σε επίπεδο κρατών. Παράλληλα, οι διασυνοριακές εξαρτήσεις επιβάλλουν τη διεθνή συνεργασία με στόχο την επίτευξη ενός κοινά υψηλού επιπέδου ασφάλειας. Σε αυτό το πλαίσιο, η χώρα μας οφείλει να συντηρήσει και να ενισχύσει την παρουσία της και τη συμμετοχή της σε όλο το φάσμα της διεθνούς συνεργασίας στοχεύοντας:

- στην διασφάλιση συνεργασιών για την από κοινού ανάπτυξη μέσων αντιμετώπισης απειλών και προκλήσεων,
- στη δημιουργία και ενίσχυση συμμαχιών για την από κοινού αντιμετώπιση κυβερνοεπιθέσεων,
- στην εξασφάλιση πρόσβασης σε πληροφορίες και τεχνογνωσία
- στην από κοινού διαμόρφωση νομοθετικών προτάσεων σε ευρωπαϊκό επίπεδο
- στην από κοινού υλοποίηση αποφάσεων που έχουν υιοθετηθεί στο πλαίσιο διεθνών οργανισμών στους οποίους συμμετέχει η Ελλάδα

Ειδικότερα, στις δραστηριότητες του εν λόγω ειδικού στόχου συγκαταλέγονται:

- Ενίσχυση της Ελληνικής παρουσίας και συμμετοχής σε διεθνείς συμμαχίες για θέματα κυβερνοασφάλειας
- Υποστήριξη των συνεργασιών με τρίτες χώρες για μεταφορά τεχνογνωσίας από και προς αυτές με στόχο την ενίσχυση του κοινά υψηλού επιπέδου ασφάλειας και την αποδοτικότερη αντιμετώπιση των διασυνοριακών απειλών.
- Δημιουργία μεθόδου καθορισμού των προσδοκώμενων συνεργασιών για θέματα κυβερνοασφάλειας και σύναψη συμφώνων συνεργασίας με τρίτες χώρες. Δημιουργία μοντέλου διαχείρισής τους ώστε μέσω της συνεργασίας να επιτυγχάνεται πρόοδος στην περαιτέρω ανάπτυξη του εθνικού επιπέδου ασφάλειας, ικανοτήτων και ευαισθητοποίησης.

7.4 Εμβληματικες δραστηριοτητες

ΣΤΟΧΟΙ	ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	ΟΡΟΣΗΜΑ
1.Α. Βελτιστοποίηση του πλαισίου οργάνωσης και λειτουργίας δομών και διαδικασιών	**1.Α.1.** Ανάπτυξη ολοκληρωμένου συστήματος διαχείρισης κυβερνοασφάλειας για φορείς του δημοσίου	**Q2 2021**
	1.Α.2. Ανάπτυξη πλαισίου προαγωγής της αριστείας στον τομέα της κυβερνοασφάλειας (cybersecurity excellence management framework)	**Q3 2022 – συνεχής δραστηριότητα**
	1.Α.3. Εκπόνηση τομεακών σχεδίων δράσης (π.χ. Energy, Healthcare, Transport, Finance, Telco, Maritime κ.λπ.)	**Q4 2024**
	1.Α.4. Ενδυνάμωση μηχανισμών ανταλλαγής πληροφοριών (information sharing)	**Q2 2022**
1.Β. Αποτελεσματικός σχεδιασμός αποτίμησης επικινδυνότητας και διαχείρισης έκτακτης ανάγκης.	**1.Β.1.** Ανάπτυξη μεθοδολογίας ανάλυσης δεδομένων και μητρώου καταγραφής απειλών	**Q4 2021**
	1.Β.2. Εθνικός σχεδιασμός αποτίμησης επικινδυνότητας	**Q4 2021 – συνεχής αξιολόγηση και επικαιροποίηση**
	1.Β.3. Εθνικός σχεδιασμός έκτακτης ανάγκης	**Q4 2021 – συνεχής αξιολόγηση και επικαιροποίηση**
1.Γ. Ενδυνάμωση συνεργασιών σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο	**1.Γ.1.** Ενίσχυση της Ελληνικής παρουσίας και συμμετοχής σε διεθνείς συμμαχίες για θέματα κυβερνοασφάλειας	**Συνεχής δραστηριότητα**
	1.Γ.2. Υποστήριξη των συνεργασιών με τρίτες χώρες για μεταφορά τεχνογνωσίας από και προς αυτές με στόχο την ενίσχυση του κοινά υψηλού επιπέδου ασφάλειας και την αποδοτικότερη αντιμετώπιση των διασυνοριακών απειλών.	**Συνεχής δραστηριότητα**
	1.Γ.3. Δημιουργία μεθόδου καθορισμού των προσδοκώμενων συνεργασιών για θέματα κυβερνοασφάλειας και σύναψη συμφώνων συνεργασίας με τρίτες χώρες.	**Q4 2021 – Συνεχής δραστηριότητα**
	1.Γ.4. Δημιουργία μοντέλου διαχείρισής τους ώστε μέσω της συνεργασίας να επιτυγχάνεται πρόοδος στην	**Q4 2021 – Συνεχής δραστηριότητα**

	περαιτέρω ανάπτυξη του εθνικού επιπέδου ασφάλειας, ικανοτήτων και ευαισθητοποίησης	

8 ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ 2. ΘΩΡΑΚΙΣΗ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ, ΑΣΦΑΛΕΙΑ ΚΑΙ ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

8.1 Ειδικος Στοχος 2.Α.: Κατανοηση των τεχνολογικων εξελιξεων και του τροπου που επηρεαζουν την ψηφιακη διακυβερνηση.

Ο ψηφιακός μετασχηματισμός της Δημόσιας Διοίκησης και η παροχή ηλεκτρονικών υπηρεσιών στους πολίτες είναι άρρηκτα συνδεδεμένα με την τεχνολογία, καθώς και με τις εξελίξεις στον τομέα ΤΠΕ (όπως ενδεικτικά 5G, IoT, Τεχνητή Νοημοσύνη, κλπ.). Οι εν λόγω τεχνολογίες αφενός επηρεάζουν τη δομή της ψηφιακής διακυβέρνησης μέσω της παροχής κατάλληλων εργαλείων για την άμεση εξυπηρέτηση των αιτημάτων των πολιτών και τη μείωση της γραφειοκρατίας, αφετέρου επιτάσσουν την υιοθέτηση αρχών κυβερνοασφάλειας από τον σχεδιασμό και εξ ορισμού(security by design and by default), ώστε να διασφαλιστεί η προστασία υποδομών και δεδομένων και η συμμόρφωση με την κείμενη νομοθεσία και τους κανονισμούς (όπως ενδεικτικά EU GDPR[7] και 4624/2019[8], NIS Directive[9] και 4577/2018[10], ePrivacy[11], κλπ.).

Ειδικότερα, στις εμβληματικές δραστηριότητες του εν λόγω ειδικού στόχου συγκαταλέγονται, μεταξύ άλλων:

8.1.1 Κυβερνοασφάλεια των δικτύων 5ης γενιάς (5G)

Στο πλαίσιο του ευρωπαϊκού συντονισμού και συνεργασίας για τη διαφύλαξη της κυβερνοασφάλειας των δικτύων 5G, η Ευρωπαϊκή Επιτροπή εξέδωσε την υπ' αριθμ. 2019/534 Σύσταση προς τα κράτη μέλη, τα σχετικά όργανα - οργανισμούς και άλλους φορείς της Ε.Ε., καθώς και την ομάδα συνεργασίας που συστάθηκε βάσει της οδηγίας (ΕΕ) 2016/1148 (NIS Cooperation Group). Σύμφωνα με την εν λόγω Σύσταση, απαραίτητα βήματα για μια ενιαία προσέγγιση στην αντιμετώπιση των κινδύνων για την κυβερνοασφάλεια των δικτύων 5G καθορίστηκαν: α. η διενέργεια εθνικών αναλύσεων κινδύνου (risk assessments), β. η κατάρτιση μιας ευρωπαϊκής ανάλυσης κινδύνου, γ. η ανάπτυξη μιας ευρωπαϊκής εργαλειοθήκης με μέτρα αντιμετώπισης των κινδύνων (5G Cybersecurity Toolbox), και δ. η εφαρμογή μέτρων της εργαλειοθήκης

Ο κύριος κορμός των μέτρων, αφορά στα στρατηγικά και στα τεχνικά μέτρα. Τα βασικότερα ζητήματα αφορούν τις διαδικασίες ασφάλειας των δικτύων 5ης γενιάς (5G), του

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504
[8] https://www.dpa.gr/portal/page?_pageid=33,213319&_dad=portal&_schema=PORTAL
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
[10] http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wG3UHk-ZeQumndtvSoClrL8Rc9TCA8iZVd5MXDoLzQTLWPU9yLzB8V68knBzLCmTXKaO6fpVZ6Lx3UnKl3nP8NxdnJ5r9cmWyJWelDvWS_18kAEhATUkJbox1LIdQ163nV9K--td6SIuSLjo42Rt6sw_v8IVsRLp-lpJxuPF8A2aUEUyrG8UBge
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

εξοπλισμού και τη διαφοροποίηση-ανεξαρτητοποίηση των παρόχων από τους προμηθευτές εξοπλισμού 5G. Περιληπτικά τα προτεινόμενα μέτρα αποτυπώνονται κατωτέρω:

Στρατηγικά μέτρα:	
Μέτρα ελέγχων – περιορισμών και απαγορεύσεων	α. Η ενδυνάμωση των εθνικών ρυθμιστικών αρχών για την επιβολή – παρακολούθηση περαιτέρω μέτρων ασφαλείας β. Η επαύξηση του ελεγκτικού τους ρόλου γ. Η διενέργεια αναλύσεων κινδύνου από τους παρόχους, τα κράτη – μέλη ή/και την ίδια την Ε.Ε. για τη διακρίβωση του προφίλ των προμηθευτών δ. Η δυνατότητα επιβολής περιορισμών ή/και απαγορεύσεων για τη διαφύλαξη κρίσιμων ή ευαίσθητων αγαθών (π.χ. core network, network management, access control) σε προμηθευτές υψηλού ρίσκου ε. Η δυνατότητα επιβολής περιορισμών στο outsourcing των λειτουργιών σε MSPs, περιλαμβανομένης της φυσικής και virtual υποδομής στ. Μέτρα ελέγχου των Άμεσων Ξένων Επενδύσεων (Α.Ξ.Ε.)
Μέτρα λειτουργίας της αγοράς	α. Εξασφάλιση ότι κάθε MNO έχει κατάλληλη στρατηγική για την αποφυγή των εξαρτήσεων από ένα μοναδικό προμηθευτή β. Εξασφάλιση εναλλακτικών επιλογών σε προμηθευτές εντός της αγοράς γ. Αξιοποίηση ενωσιακών (και εθνικών) μηχανισμών για τη διαμόρφωση πολιτικών και στρατηγικών επενδύσεων στην καινοτομία, την έρευνα και τις νέες τεχνολογίες με ειδικό στόχο την προαγωγή της αειφόρου λειτουργίας σε όλο το μήκος της αλυσίδας αξίας του 5G
Τεχνικά μέτρα:	
Πολιτικές ασφάλειας για τους MNOs	α. Εξασφάλιση της εφαρμογής των βασικών απαιτήσεων ασφάλειας β. Εξασφάλιση ότι οι πάροχοι και οι προμηθευτές τους εφαρμόζουν τα μέτρα ασφαλείας που περιλαμβάνονται στα πρότυπα για το 5G γ. Διασφάλιση αυστηρών ελέγχων πρόσβασης δ. Ενίσχυση της ασφάλειας των virtual λειτουργιών του δικτύου ε. Ασφάλεια NOC – SOC, παρακολούθηση και λειτουργία του δικτύου στ. Ενίσχυση της φυσικής ασφάλειας ζ. Ενίσχυση της ασφάλειας λογισμικού η. Διασφάλιση ανθεκτικότητας και επιχειρησιακής συνέχειας (resilience and continuity) θ. Έλεγχος security standards των προμηθευτών στο στάδιο της προμήθειας από τους παρόχους
Προαγωγή ενός συστήματος πιστοποίησης σε ενωσιακό επίπεδο	α. Σε πρώτο στάδιο για τα συστήματα δικτύου/εξοπλισμού πελατών που σχετίζονται με 5G β. Σε επόμενο στάδιο, ενδεχομένως, για προμηθευτές εξοπλισμού που σχετίζεται με 5G γ. Χρήση πιστοποίησης από την ΕΕ για άλλα προϊόντα και υπηρεσίες ΤΠΕ που δεν σχετίζονται με το 5G (συνδεδεμένες συσκευές, υπηρεσίες cloud)

8.1.2 Industrial Internet of Things

Στο πλαίσιο της συγκεκριμένης δραστηριότητας, η Εθνική Αρχή Κυβερνοασφάλειας θα συλλέξει στοιχεία που απεικονίζουν το βαθμό ενσωμάτωσης τεχνολογιών Industrial Internet of Things πάνω στη ήδη υπάρχοντα SCADA συστήματα. Τα συστήματα SCADA είναι βιομηχανικά συστήματα ελέγχου (industrial control systems) και συνθέτουν τον πυρήνα υλοποίησης των βασικών υπηρεσιών (π.χ. διανομή, μεταφορά, διύλιση κ.α.) από τους ΦΕΒΥ που εκτελούν βιομηχανικές διεργασίες. Πρόκειται για legacy συστήματα που υπάρχουν εδώ και δεκαετίες.

Το Industrial Internet of Things αναφέρεται σε τεχνολογίες όπως είναι οι διασυνδεδεμένοι αισθητήρες (connected sensors) και άλλες συσκευές, οι οποίες δικτυώνονται με τα υπάρχοντα βιομηχανικά συστήματα και εισάγουν νέα κανάλια ανταλλαγής πληροφορίας μεταξύ διασυνδεδεμένων σταθμών και του Cloud, με συνέπεια την αύξηση της επιφάνειας επίθεσης (attack surface) και τη συνακόλουθη ανάγκη εφαρμογής εξειδικευμένων μέτρων ασφάλειας.

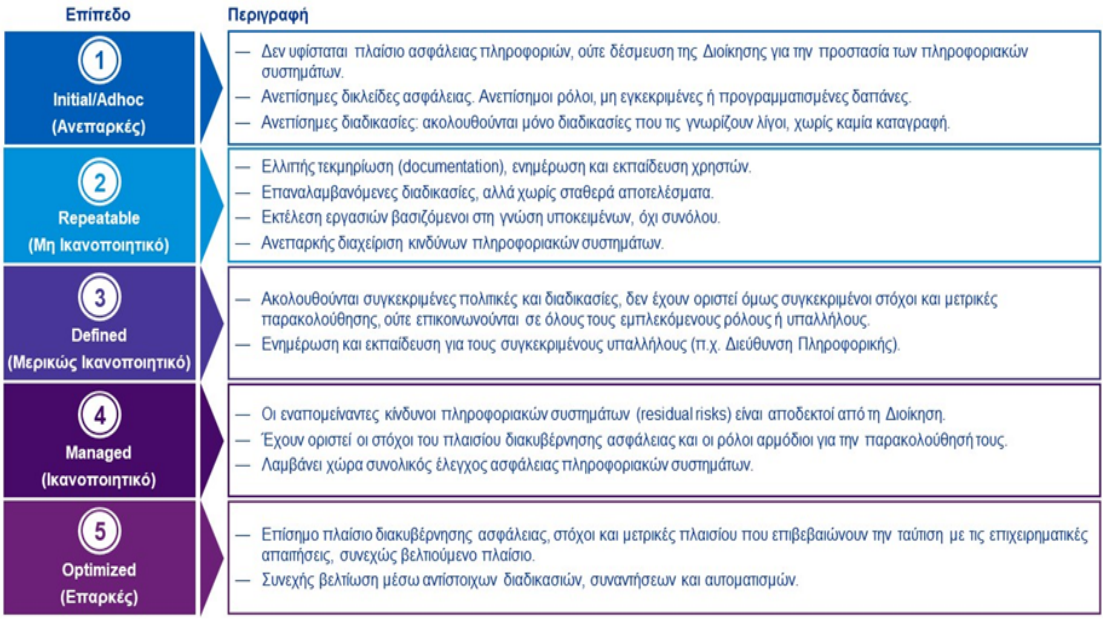
8.1.3 Artificial Intelligence

Η τεχνητή νοημοσύνη καθιστά τις μηχανές ικανές να «κατανοούν» το περιβάλλον τους, να επιλύουν προβλήματα και να δρουν προς την επίτευξη ενός συγκεκριμένου στόχου. Ο υπολογιστής λαμβάνει δεδομένα (ήδη έτοιμα ή συλλεγμένα μέσω αισθητήρων), τα επεξεργάζεται και ανταποκρίνεται βάσει αυτών. Το νέο αυτό περιβάλλον εισάγει νέες απειλές και καινοτόμους τρόπους επιθέσεων στα εν λόγω συστήματα, όπως για παράδειγμα την εισαγωγή αλλοιωμένων δεδομένων στους εταιρικούς αλγόριθμους μηχανικής μάθησης (machine learning) με σκοπό την λήψη από αυτά λανθασμένων αποφάσεων, με επικίνδυνες επιπτώσεις. Επίσης, οι αλγόριθμοι machine learning μπορούν να χρησιμοποιηθούν και από τους ίδιους τους επιτιθέμενους με σκοπό την ταχύτερη παραγωγή εξελιγμένου malware που θα δύναται να παρακάμπτει τα δικτυακά συστήματα ανίχνευσης εισβολών. Στο πλαίσιο της συγκεκριμένης δραστηριότητας, η Εθνική Αρχή Κυβερνοασφάλειας θα εκπονήσει εξειδικευμένα μέτρα ασφάλειας για την προστασία των συστημάτων τεχνητής νοημοσύνης από επιθέσεις.

8.2 Ειδικος Στοχος 2.Β..: Αναβαθμιση της προστασιας κρισιμων υποδομων

Η Αρχή θα παρέχει υποστήριξη στους φορείς δημόσιας διοίκησης αλλά και σε λοιπούς εμπλεκόμενους φορείς για την αποτελεσματική προστασία κρίσιμων υποδομών, σε άξονες όπως η υλοποίηση των βασικών αρχών και απαιτήσεων κυβερνοασφάλειας, ο έλεγχος και η αξιολόγηση των Φορέων, η διενέργεια τεχνικών ελέγχων ασφάλειας, καθώς και η τακτική αξιολόγηση των Φορέων μέσω των κατάλληλων ελέγχων. Θεμελιώδεις παρεμβάσεις στο πλαίσιο του εν λόγω στόχου αφορούν στην ανάπτυξη και εφαρμογή ολοκληρωμένου συντονιστικού πλαισίου για τους CISO, στην ανάπτυξη ειδικών πρακτικών ανίχνευσης, ποσοτικοποίησης, προτεραιοποίησης, έγκαιρης προειδοποίησης και διαχείρισης κινδύνων για κρίσιμες υποδομές, καθώς και στην εκπόνηση threat

landscape reports. Περαιτέρω, στο πλαίσιο της βελτιστοποίησης της αξιολόγησης και ανατροφοδότησης του σχεδιασμού ασφαλείας για τις κρίσιμες υποδομές, καίρια δράση συνιστά η δημιουργία πρότυπων ερωτηματολογίων ώστε οι Φορείς να είναι σε θέση να αποτυπώσουν το τρέχον επίπεδο ωριμότητάς τους και ετοιμότητας στο να αποκριθούν σε συμβάντα ασφάλειας και να συμμορφωθούν με τις διατάξεις της κείμενης νομοθεσίας.



Εικόνα 13 Μοντέλο ωριμότητας για την αξιολόγηση των φορέων βάσει του επιπέδου κυβερνοασφάλειας.

- Το ερωτηματολόγιο περιλαμβάνει τα ελάχιστα απαιτούμενα μέτρα που πρέπει να λάβει ένας φορέας.
- Η απόδοση των επιπέδων ωριμότητας αποσκοπεί στην καταγραφή της υφιστάμενης κατάστασης, ώστε ο φορέας να είναι σε θέση να λάβει τα κατάλληλα μέτρα για τη βελτίωση του υπάρχοντος πλαισίου κυβερνοασφάλειας.
- Όσο μικρότερο το επίπεδο ωριμότητας, τόσο μεγαλύτερος ο κίνδυνος εκμετάλλευσης αδυναμιών από παράγοντες απειλών.

8.3 Ειδικος Στοχος 2.Γ.: Θωρακιση συστηματων και εφαρμογων μεσω ενισχυμενων απαιτησεων ασφαλειας

Η αποτελεσματική θωράκιση συστημάτων και εφαρμογών, στο πλαίσιο μιας ολοκληρωμένης εκτίμησης των παραγόντων απειλών και κινδύνων, προϋποθέτει τη διαμόρφωση ενός συνεκτικού και εφαρμόσιμου πλαισίου ανάλογων απαιτήσεων ασφαλείας. Βασικές παραμέτρους στον εν λόγω σχεδιασμό συνιστούν η ανάπτυξη και διαχείριση μητρώου υποδομών (hardware), λογισμικού (software), καθώς και άυλων πληροφοριακών αγαθών σε κρίσιμους τομείς (δημόσιο, κρίσιμες υποδομές), η διενέργεια κατηγοριοποίησης φορέων για τον προσδιορισμό ενισχυμένων απαιτήσεων ασφαλείας, η ανάγκη έκδοσης ενισχυμένων απαιτήσεων ασφαλείας (οριζόντια και τομεακά) λαμβάνοντας υπόψη τα διεθνή και ευρωπαϊκά πρότυπα και πλαίσια πιστοποίησης. Παράλληλα, για την αποτελεσματική τήρηση των απαιτήσεων ασφαλείας, απαιτείται η

ανάπτυξη ενός συστήματος ελέγχων (audit) εφαρμογής των απαιτήσεων ασφάλειας, στο πλαίσιο του οποίου θα συντάσσονται εκθέσεις με ευρήματα και ανάλογες συστάσεις.

Ειδικότερα, στις εμβληματικές δραστηριότητες του εν λόγω ειδικού στόχου συγκαταλέγονται, μεταξύ άλλων:

8.3.1 Ανάπτυξη και διαχείριση μητρώου υποδομών (hardware), λογισμικού (software) και άυλων πληροφοριακών αγαθών.

Στο πλαίσιο της παρούσας δράσης, η Εθνική Αρχή Κυβερνοασφάλειας θα προβεί σε:

- καταγραφή σε κατάλληλο και ενημερωμένο κατάλογο (μητρώο) όλων των πόρων που απαιτούνται για την παροχή ή υποστήριξη των βασικών υπηρεσιών των ΦΕΒΥ και ΠΨΥ
- τη διασφάλιση της ανθεκτικότητας των συστημάτων που υποστηρίζουν βασικές υπηρεσίες έναντι απειλών, με την εφαρμογή των κατάλληλων διαδικασιών δοκιμών και τεχνικών ελέγχων των ΦΕΒΥ και ΠΨΥ, σε συνεργασία με τους κατά περίπτωση αρμόδιους φορείς
- τη διενέργεια των απαραίτητων ελέγχων για την προστασία του λογισμικού και των εφαρμογών στους τομείς αρμοδιότητας της Κυβερνοασφάλειας των ΦΕΒΥ και ΠΨΥ, σύμφωνα με τις απαιτήσεις ασφαλείας (ιδίως λειτουργικά συστήματα, εφαρμογές, συστήματα διαχείρισης βάσεων δεδομένων, εφαρμογές PCI, COTS), και σε συνεργασία με τους κατά περίπτωση αρμόδιους φορείς,
- τη διενέργεια ελέγχων για την προστασία των δικτύων, του υλικού και των συστημάτων των ΦΕΒΥ και ΠΨΥ σύμφωνα με τις απαιτήσεις ασφαλείας (πρόληψη/ανίχνευση εισβολής) σε συνεργασία με τους κατά περίπτωση αρμόδιους φορείς,
- τον καθορισμό και την κατηγοριοποίηση των πληροφοριακών αγαθών (information assets) και την τήρηση σχετικού μητρώου αποθετηρίου σε συνεργασία με τους κατά περίπτωση αρμόδιους φορείς,
- την έκδοση κατευθυντήριων γραμμών και οδηγιών ως προς την Κυβερνοασφάλεια για την προστασία των πληροφοριακών αγαθών, σύμφωνα με τις απαιτήσεις ασφαλείας (συμπεριλαμβανομένων των απαιτήσεων ιδιωτικότητας και προστασίας των δεδομένων προσωπικού χαρακτήρα, κρυπτογράφησης, PKI, backup, DLP, διατήρηση/καταστροφή δεδομένων).
- την παροχή υποστήριξης για την προστασία της περιμέτρου δικτύου, σύμφωνα με τις απαιτήσεις ασφαλείας (firewalls, DMZ, συνδέσεις δικτύου, σύνδεση τρίτων, απομακρυσμένη πρόσβαση, VPN κ.λπ.) σε συνεργασία με τους κατά περίπτωση αρμόδιους φορείς.

8.3.2 Έκδοση απαιτήσεων ασφαλείας

Η Εθνική Αρχή Κυβερνοασφάλειας θα ορίσει 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. Υπό το πρίσμα αυτό κρίνεται απαραίτητη 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. 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.

Κατά συνέπεια, οι εμπλεκόμενοι φορείς απαιτείται να υλοποιήσουν συγκεκριμένα μέτρα κυβερνοασφάλειας ώστε να διασφαλίσουν την προστασία των πληροφοριακών πόρων τους. Λόγω της φύσης του κάθε Φορέα και των κανονιστικών απαιτήσεων που ενδέχεται να διέπουν τη λειτουργία του, η Αρχή θα ορίσει τις βασικές αρχές και απαιτήσεις που θα πρέπει να πληρούνται (cyber security baselines) αναλόγως της κατηγοριοποίησής τους. Τα μέτρα αυτά περιλαμβάνουν μέτρα πρόληψης αλλά και αντιμετώπισης περιστατικών ασφάλειας. Οι απαιτήσεις κυβερνοασφάλειας θα διευκολύνουν τον ορισμό ενός ενιαίου πλαισίου προστασίας των Φορέων, καθώς και τον αποτελεσματικό έλεγχο εφαρμογής τους. Ταυτόχρονα, θα αποτελέσουν τη βάση έκδοσης προτύπων και εγκυκλίων από την Αρχή, θεσμοθέτησης και παρακολούθησης δεικτών (KPIs, KRIs), αναθεώρησης βάσει εξελίξεων ΤΠΕ και οδηγιών από εθνικούς και ευρωπαϊκούς φορείς, καθώς και του συντονισμού των Φορέων κατά την απόκριση σε συμβάντα κυβερνοασφάλειας.

8.3.3 Ανάπτυξη συστήματος ελέγχων κυβερνοασφάλειας

Με γνώμονα την επαύξηση της προστασίας των οικείων φορέων, η Εθνική Αρχή Κυβερνοασφάλειας θα αναλάβει:

- τη διαμόρφωση και επεξεργασία προγράμματος ελέγχου για την εφαρμογή του Εθνικού Στρατηγικού Σχεδίου Κυβερνοασφάλειας,
- τη διενέργεια τακτικών και έκτακτων ελέγχων στις εγκαταστάσεις, τον εξοπλισμό και τις τεχνολογικές υποδομές από Ομάδες Επιθεώρησης Ελέγχου που συγκροτούνται από την Εθνική Αρχή Κυβερνοασφάλειας με τη σύνταξη σχετικών αναφορών υποδεικνύοντας τις απαιτούμενες διορθωτικές επεμβάσεις και την παρακολούθηση της εφαρμογής τους, σε συνεργασία με τους κατά περίπτωση αρμόδιους φορείς,
- τη σύνταξη των εκθέσεων διενέργειας ελέγχων ασφαλείας πληροφοριών και δικτύων
- την εξασφάλιση της επάρκειας των ελέγχων για την εκπλήρωση των πολιτικών, προτύπων και απαιτήσεων ασφάλειας,
- την εξασφάλιση της επάρκειας των ελέγχων ως προς την πλήρωση των απαιτήσεων απορρήτου, της ιδιωτικότητας και προστασίας δεδομένων προσωπικού χαρακτήρα
- τη διατύπωση συστάσεων και την εισήγηση μέτρων και δράσεων για τη βελτίωση της εφαρμογής του στρατηγικού σχεδιασμού για την Κυβερνοασφάλεια.

8.4 ΕΜΒΛΗΜΑΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

ΣΤΟΧΟΙ	ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	ΟΡΟΣΗΜΑ
2.Α. Κατανόηση των τεχνολογικών εξελίξεων και του τρόπου που επηρεάζουν την ψηφιακή διακυβέρνηση.	**2.Α.1.** Εφαρμογή ολοκληρωμένου πλαισίου κυβερνοασφάλειας για τα δίκτυα 5G	**Q4 2021 - συνεχής δραστηριότητα**
	2.Α.2. Εφαρμογή πλαισίου μέτρων και δράσεων για την Τεχνητή Νοημοσύνη	**Q4 2021 – συνεχής δραστηριότητα**
	2.Α.3. Εφαρμογή πλαισίου μέτρων και δράσεων για το Internet of Things (IoT)	**Q4 2021 – συνεχής δραστηριότητα**
	2.Α.4. Ανάπτυξη ενισχυμένης συνεργασίας με ακαδημαϊκούς και ερευνητικούς φορείς πάνω στις νέες τεχνολογίες	**Q4 2021 – συνεχής δραστηριότητα**
2.Β.Αναβάθμιση της προστασίας κρίσιμων υποδομών	**2.Β.1.** Καθορισμός και επικαιροποίηση καταλόγου κρίσιμων υποδομών	**Q4 2022**
	2.Β.2. Ανάπτυξη και εφαρμογή ενιαίου συντονιστικού πλαισίου για τους CISO	**Q1 2022**
	2.Β.3.Ανάπτυξη πρακτικών ανίχνευσης, ποσοτικοποίησης, προτεραιοποίησης, έγκαιρης προειδοποίησης και διαχείρισης κινδύνων για κρίσιμες υποδομές	**Q4 2022**
	2.Β.4. Εκπόνηση threat landscape reports	**Q4 2025**
2.Γ.Θωράκιση συστημάτων και εφαρμογών μέσω ενισχυμένων απαιτήσεων ασφαλείας	**2.Γ.1**.Ανάπτυξη και διαχείριση μητρώου υποδομών (hardware), λογισμικού (software) και άυλων πληροφοριακών αγαθών σε κρίσιμους τομείς (δημόσιο, κρίσιμες υποδομές)	**Q4 2021 – συνεχής δραστηριότητα**
	2.Γ.2. Κατηγοριοποίηση φορέων για τον προσδιορισμό ενισχυμένων απαιτήσεων ασφαλείας	**Q2 2023**
	2.Γ.3. Έκδοση ενισχυμένων απαιτήσεων ασφαλείας (οριζόντια και τομεακά) λαμβάνοντας υπόψη τα διεθνή και ευρωπαϊκά standards και πλαίσια πιστοποίησης	**Συνεχής δραστηριότητα**
	2.Γ.4. Έκδοση ειδικών απαιτήσεων ασφάλειας σε έργα ΤΠΕ	**Q4 2022 - συνεχής δραστηριότητα**
	2.Γ.5. Ανάπτυξη συστήματος ελέγχων (audit) εφαρμογής των απαιτήσεων ασφάλειας	**Q4 2021 – συνεχής δραστηριότητα**
	2.Γ.6. Ανάπτυξη ολοκληρωμένου συστήματος αξιολόγησης επιπέδου ωριμότητας φορέων	**Q4 2021 – συνεχής δραστηριότητα**

9 ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ 3. ΒΕΛΤΙΣΤΟΠΟΙΗΣΗ ΔΙΑΧΕΙΡΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ, ΚΑΤΑΠΟΛΕΜΗΣΗΣ ΤΟΥ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

9.1 Ειδικος Στοχος 3.Α.: Βελτιστοποιηση μεθοδων, τεχνικων και εργαλειων αναλυσης, αποκρισης και κοινοποιησης συμβαντων

Η γνώση των τεχνικών λεπτομερειών των περιστατικών που καλούνται να αντιμετωπίσουν οι φορείς, η ανάλυση αυτών και η διασπορά της γνώσης απαιτείται, προκειμένου όλοι οι συμμετέχοντες να προετοιμάζονται αποτελεσματικότερα στην αντιμετώπιση περιστατικών αλλά και να προβαίνουν στις απαραίτητες διορθωτικές ενέργειες σε σχέση με τα μέτρα ασφάλειας που έχουν λάβει, ώστε να ελαχιστοποιείται 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 ενισχύεται η ετοιμότητά τους στην αντιμετώπιση περιστατικών ασφάλειας. Ειδικότερα, το πλαίσιο διαχείρισης συμβάντων κυβερνοασφάλειας περιλαμβάνει τον καθαρισμό κατάλληλων υποδομών, την ανάθεση ρόλων και αρμοδιοτήτων, τη λειτουργία cyber hotline ώστε οι Φορείς (ΦΕΒΥ και ΠΨΥ) να είναι σε θέση να αναφέρουν συμβάντα ασφάλειας, τη συνεργασία με φορείς όπως η Εθνική Υπηρεσία Πληροφοριών και η Διεύθυνση Κυβερνοάμυνας (ΓΓΕΘΑ/ΔΙΚΥΒ), τη χρήση υποδομής λειτουργιών κυβερνοασφάλειας (SOC), την εκπόνηση οδηγιών αντιμετώπισης συμβάντων κυβερνοασφάλειας (operations handbook), καθώς και λίστας με λοιπά συμπραττόμενα τρίτα μέρη. Στην περίπτωση περιστατικού κυβερνοασφάλειας, οι φορείς που συμμετέχουν στην Εθνική Στρατηγική οφείλουν να είναι έτοιμοι να αντιδράσουν αποτελεσματικά. Υπό το ανωτέρω πρίσμα, θα πρέπει να υπάρξει μέριμνα για την ανίχνευση, προτεραιοποίηση, ανάλυση, απόκριση και ανάκτηση από ύποπτα συμβάντα και περιστατικά ασφαλείας, καθώς και τη συνεργασία με τη Διεύθυνση Κυβερνοάμυνας

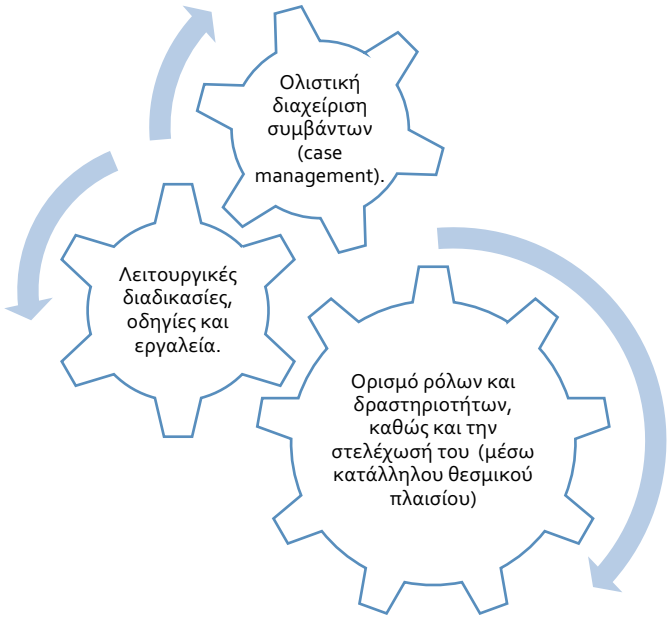
του ΓΕΕΘΑ (ΓΕΕΘΑ/ΔΙΚΥΒ), την Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT) και την Τεχνικής Φύσεως Αρχή Ασφάλειας Πληροφοριών (INFOSEC) της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.), καθώς επίσης και με άλλα CERTs που δραστηριοποιούνται στην Ελλάδα.

Ειδικότερα, στις εμβληματικές δραστηριότητες του εν λόγω ειδικού στόχου συγκαταλέγονται, μεταξύ άλλων:

9.1.1 Σύσταση Κέντρου Παρακολούθησης Κρίσιμων Υποδομών Security Operations Center – SOC)

Κρίνεται απαραίτητη η ανάπτυξη δυνατότητας παρακολούθησης και απόκρισης σε συμβάντα ασφάλειας και η ανταλλαγή στοιχείων με τους αρμόδιους Φορείς. Η εν λόγω δυνατότητα παρέχεται μέσω υποδομής Κέντρου Παρακολούθησης Κρίσιμων Υποδομών (Security Operations Center – SOC) και σύστασης Ομάδας Απόκρισης Κυβερνοπεριστατικών (CSIRT).

Η λειτουργία Κέντρου Παρακολούθησης Κρίσιμων Υποδομών (SOC), απαιτεί, κατ' ελάχιστον, τα ακόλουθα:



Εικόνα 14 Λειτουργία SOC

Σκοπός του Κέντρου αποτελεί η διαρκής παρακολούθηση των κρίσιμων υποδομών Φορέων και η έγκαιρη αναγνώριση και αντιμετώπιση των περιστατικών ασφάλειας.

Αρμοδιότητες:

— Υλοποίηση και διαχείριση κατάλληλων εργαλείων.

Η εκτέλεση των εργασιών του Κέντρου στηρίζεται, εκτός από τα στελέχη του, σε εργαλεία. Τα εν λόγω εργαλεία αποσκοπούν στη συλλογή στοιχείων από τα αρχεία καταγραφής (log files) και στον συσχετισμό τους (correlation) με γνώμονα την

αποτελεσματική αναγνώριση απειλών. Ταυτόχρονα, επιτρέπουν τη σύσταση προφίλ της δικτυακής κίνησης του Φορέα, τον ορισμό κατάλληλων δεικτών και ειδοποιήσεων (alerts), καθώς και την επέμβαση στο δίκτυο για την αποφυγή επέκτασης μιας επίθεσης ή μόλυνσης με κακόβουλο λογισμικό.

— Διερεύνηση ύποπτων ενεργειών με σκοπό την αναγνώριση απειλών.

Η διερεύνηση ύποπτων ενεργειών είναι απαραίτητη για τον μετριασμό λανθασμένων ειδοποιήσεων (false positives), ήτοι καταστάσεις όπου νόμιμη δικτυακή κίνηση κατηγοριοποιείται ως παράνομη, αλλά και false negatives, ήτοι καταστάσεις όπου παράνομη δικτυακή κίνηση βαίνει απαρατήρητη, κατηγοριοποιημένη ως νόμιμη.

Ταυτόχρονα, με τη χρήση των κατάλληλων εργαλείων και διαδικασιών, τα στελέχη του Κέντρου είναι σε θέση να προβούν στις αρχικές ενέργειες απόκρισης – triage, κατά τις οποίες αποφασίζεται εάν μια ενέργεια χρήζει περαιτέρω διερεύνησης, θεωρούμενη ως συμβάν ή όχι.

Η διερεύνηση ύποπτων ενεργειών αποτελεί διεργασία κρίσιμης σημασίας, ιδιαίτερα εάν εμπλέκονται προσωπικά δεδομένα και μια ενέργεια πρέπει να αντιμετωπιστεί και ως παραβίαση προσωπικών δεδομένων.

— Διασφάλιση επιχειρησιακής συνέχειας Φορέων.

Μέσω της έγκαιρης αναγνώρισης και αποτροπής (ή μετριασμού) συμβάντων, διασφαλίζεται η συνέχεια των επιχειρησιακών λειτουργιών των Φορέων. Συγχρόνως, μέσω της παρακολούθησης της δικτυακής κίνησης, το Κέντρο θα δίνει στοιχεία στη Δ/νση Πρόληψης και Προστασίας για τη σύνταξη κατάλληλων οδηγιών προς τους Φορείς.

— Υποστήριξη ενεργειών Δ/νσεων Αρχής.

Οι ενέργειες του Κέντρου είναι συμπληρωματικές των Δ/νσεων της Αρχής, παρέχοντας στοιχεία για τους Φορείς, είτε μεμονωμένα, είτε συγκεντρωτικά, ώστε να υπάρχει, ανά πάσα στιγμή, εικόνα για την κατάσταση των Φορέων αναφορικά με το εφαρμοσμένο πλαίσιο κυβερνοασφάλειας.

9.1.2 Δημιουργία Cyber hotline

Με σκοπό την άμεση και αποτελεσματική αντιμετώπιση συμβάντων ασφάλειας, προτείνεται να δημιουργηθούν κατάλληλες διεπαφές επικοινωνίας με τους ΦΕΒΥ και ΠΨΥ.

Πιο συγκεκριμένα θα δημιουργηθεί:

— Τηλέφωνο επικοινωνίας.

— Διεύθυνση ηλεκτρονικού ταχυδρομείου.

Η συγκεκριμένη διεύθυνση / mailbox θα αποστέλλει το μήνυμα στο Κέντρο (SOC) για περαιτέρω διερεύνηση.

Τα ανωτέρω στοιχεία συμπληρώνουν την ήδη αναρτημένη, στον ανωτέρω σύνδεσμο, φόρμα υποβολής αναφοράς περιστατικού.

9.1.3 Υποδομή SOC και Case Management

Η λειτουργία του Κέντρου (SOC) στηρίζεται επίσης σε χρήση εξειδικευμένων εργαλείων που αποσκοπούν στην (α) παρακολούθηση δικτυακής κίνησης και αναγνώρισης συμβάντων, αλλά και (β) στη διαχείριση, εσωτερικά του Κέντρου, των περιπτώσεων (case management).

Τα βασικά εργαλεία ενός Κέντρου (SOC), συνοψίζονται ως ακολούθως:

— Σύστημα Security Information and Event Management (SIEM).

Αποτελεί ένα από τα βασικότερα εργαλεία ενός Κέντρου (SOC), το οποίο αποσκοπεί:

(α) Στη συγκέντρωση των στοιχείων από τις συσκευές υπό παρακολούθηση (logs), την ασφαλή αποθήκευσή τους και την ανάλυση από τους Αναλυτές αναλόγως των αναγκών.

(β) Στον συσχετισμό των στοιχείων (log correlation) με σκοπό την αναγνώριση απειλών που θα μπορούσαν να επηρεάσουν την επιχειρησιακή συνέχεια και λειτουργία ενός Φορέα.

— Σύστημα Security Orchestration, Automation and Response (SOAR).

Τα συστήματα SIEM, ενώ αποτελούν ένα βασικό βοήθημα των αναλυτών για την έγκαιρη διάγνωση συμβάντων, δεν περιλαμβάνουν, ως λειτουργικότητα, την απόκριση σε συμβάντα, ήτοι την εφαρμογή ή αλλαγή συγκεκριμένων κανόνων στα υπό παρακολούθηση συστήματα. Για αυτούς τους σκοπούς, γίνεται παράλληλη χρήση εργαλείων SOAR, η οποία είναι σε θέση να αυτοματοποιήσει τις ενέργειες απόκρισης, βάσει κανόνων αλλά και άμεσης συνεργασίας με το σύστημα SIEM.

Λόγω της έξαρσης κυβερνοεπιθέσεων, τα συστήματα SOAR έχουν πλέον καταστεί απαραίτητα για ένα Κέντρο (SOC). Λαμβάνοντας επίσης υπόψη την έλλειψη στελεχών κυβερνοασφάλειας που παρατηρείται σε παγκόσμιο επίπεδο , τα εν λόγω εργαλεία χρησιμοποιούνται ώστε να καλύψουν το εν λόγω κενό, προστατεύοντας τους Φορείς και επιτρέποντας στα υπάρχοντα στελέχη να επικεντρωθούν σε άλλα αντικείμενα.

— Σύστημα Case Management.

Τα εν λόγω συστήματα έρχονται να καλύψουν το διαχειριστικό μέρος της λειτουργίας του Κέντρου (SOC). Κάθε περίπτωση που υπόκειται σε διερεύνηση, αποτελεί και υπόθεση (case) την οποία διαχειρίζονται διαφορετικά στελέχη, ακόμα και μεταξύ βαρδιών.

Το σύστημα case management αποσκοπεί:

(α) Στην αποτελεσματική διαχείριση της εκάστοτε υπόθεσης, συμπεριλαμβάνοντας πληθώρα στοιχείων όπως ημερομηνία και ώρα, εμπλεκόμενους Αναλυτές, περιγραφή της υπόθεσης, ενέργειες που έχουν λάβει χώρα ή/και έχουν προγραμματιστεί, αποτελέσματα επικοινωνίας με τους Φορείς, οδηγίες από Μηχανικούς – SMEs, κλπ.

(β) Στην παρακολούθηση της εξέλιξης μιας υπόθεσης από τους Επικεφαλής, καταγραφή χρονικής διάρκειας επίλυσης της υπόθεσης, καταγραφή διαχειριστικών

μετρικών (π.χ. χρόνοι απόκρισης, πλήθος επικοινωνίας με Φορέα, κλπ.) και παραγωγή αντίστοιχων εφαρμογών.

Σε ένα σύγχρονο Κέντρο (SOC), η χρήση του συστήματος case management καθίσταται επιτακτική, με προτεραιότητα (αρκετές φορές) έναντι ενός κεντρικού SIEM εργαλείου.

9.1.4 Ανάπτυξη μητρώου συμβάντων, εργαλεία threat intelligence και προστασία ιστοτόπων

Περαιτέρω, στο πλαίσιο της βελτιστοποίησης μεθόδων, τεχνικών και εργαλείων ανάλυσης, απόκρισης και κοινοποίησης συμβάντων σχεδιάζονται οι ακόλουθες δράσεις:

- η κατάρτιση και διαχείριση μητρώου συμβάντων (επίσημα ή/και ανώνυμα), συμπεριλαμβανομένων όλων των πληροφοριών που αφορούσαν το συμβάν, ενέργειες που έλαβαν χώρα, αποτελέσματα, lessons learned,
- η λειτουργία συστήματος προστασίας κυβερνητικών ιστοτόπων,
- η ανάπτυξη προγράμματος παρακολούθησης και αξιολόγησης επιπέδου ασφάλειας ελληνικού κυβερνοχώρου (threat intelligence tool),
- η εγκατάσταση και παραμετροποίηση open source εργαλείου συστήματος αυτόματης ειδοποίησης για την διαθεσιμότητα των ιστοτόπων και των δικτυακών συσκευών
- η εγκατάσταση open source πλατφόρμας για vulnerability assessment και διενέργεια ελέγχων Τρωτότητας (Penetration tests)
- Η εγκατάσταση και παραμετροποίηση open source εργαλείου για ανταλλαγή δεικτών IOCs με άλλους οργανισμούς κυβερνοασφάλειας (Εθνικό CERT, CERT/ΔΙΚΥΒ, CERT ΕΔΗΤΕ, 4thCERT)

9.2 Ειδικος Στοχος 3.Β.: Ενδυναμωση μηχανισμων αποτροπης και βελτιστοποιηση της επιχειρησιακης συνεργασιας

Η καταπολέμηση του κυβερνοεγκλήματος απαιτεί κατάλληλα εργαλεία που θα έχουν στην διάθεσή τους οι αρμόδιοι Φορείς για την συντονισμένη αντιμετώπισή του, δεδομένου ότι είναι ένας από τους παράγοντες απειλών που ενδέχεται να επιφέρουν πολύ μεγάλο αντίκτυπο στις παρεχόμενες από τους Φορείς υπηρεσίες. Ως εκ τούτου κρίνεται απαραίτητη η ενίσχυση του νομοθετικού πλαισίου και των αρμόδιων υπηρεσιών που θα επιφορτιστούν με την καταστολή του. Ειδικότερα, στο πλαίσιο του εν λόγω στόχου καίριο ρόλο διαδραματίζει η δημιουργία πλαισίου συνεργασίας (πραγματοποίηση συναντήσεων, αξιολόγηση επιπέδου συμμόρφωσης στις κείμενες διατάξεις, διαστάσεις και πορεία του κυβερνοεγκλήματος στη χώρα, σε διεθνές και ευρωπαϊκό επίπεδο) με τις κατά περίπτωση αρμόδιες Υπηρεσίες (π.χ. Δίωξη Ηλεκτρονικού Εγκλήματος, Υπουργείο Δικαιοσύνης, Υπουργείο Εξωτερικών). Περαιτέρω, σημαντική δράση συνιστά η χαρτογράφηση του υφιστάμενου θεσμικού πλαισίου και κυρωτικών διατάξεων, ως βάση για τη διενέργεια αξιολόγησης της πορείας εφαρμογής αυτού, περιλαμβανομένου του επιπέδου αποτροπής,

αλλά και την πραγματοποίηση παρεμβάσεων ενίσχυσης του κυρωτικού πλαισίου σε συνεργασία με τους κατά περίπτωση αρμόδιους φορείς.

9.3 Ειδικος Στοχος 3.Γ.: Προαγωγη της ασφαλειας δεδομενων σε συνδυασμο με την προστασια της ιδιωτικοτητας

Η Στρατηγική ευθυγραμμίζεται με τις απαιτήσεις των κανονισμών και της κείμενης νομοθεσίας για την προστασία των εν λόγω δεδομένων, μέσω της, μεταξύ άλλων, ενσωμάτωσης αρχών προστασίας δεδομένων (data protection by design) στις βασικές απαιτήσεις και αρχές κυβερνοασφάλειας και της συνεργασίας με αρμόδιους φορείς (π.χ. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα – ΑΠΔΠΧ). Καίρια δράση εν προκειμένω συνιστά ο συντονισμός των διαδικασιών αναφοράς περιστατικών με τους εμπλεκόμενους φορείς, μέσω της ανάπτυξη θεσμικής συνεργασίας/μικτής ομάδας συνεργασίας με ΑΠΔΠΧ και ΑΔΑΕ στο πλαίσιο της προστασίας της ιδιωτικότητας. Συγχρόνως, σημαντικό πλαίσιο παρέμβασης συνιστά η συλλογή, ανάλυση και τεκμηρίωση δεδομένων κυβερνοεπιθέσεων που ενέχουν παραβίαση της ιδιωτικότητας, με σκοπό την απόκτηση ολοκληρωμένης εικόνας για τα εν λόγω περιστατικά, καθώς και την πραγματοποίηση περαιτέρω δράσεων για την αντιμετώπισή τους.

9.4 Εμβληματικες δραστηριοτητες

ΣΤΟΧΟΙ	ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	ΟΡΟΣΗΜΑ
3.Α. Βελτιστοποίηση μεθόδων, τεχνικών και εργαλείων ανάλυσης, απόκρισης και κοινοποίησης συμβάντων	**3.Α.1.** Δημιουργία Κέντρου Παρακολούθησης Κρίσιμων Υποδομών Security Operations Center – SOC	**Q4 2022 – συνεχής δραστηριότητα**
	3.Α.2. Δημιουργία Cyber hotline	**Q2 2023– συνεχής δραστηριότητα**
	3.Α.3. Ορισμός πλαισίου διαχείρισης συμβάντων ασφάλειας	**Q2 2022**
	3.Α.4. Κατάρτιση και διαχείριση μητρώου συμβάντων (επίσημα ή/και ανώνυμα), συμπεριλαμβανομένων όλων των πληροφοριών που αφορούσαν το συμβάν, ενέργειες που έλαβαν χώρα, αποτελέσματα, lessons learned.	**Q4 2023 – συνεχής δραστηριότητα**
	3.Α.5. Λειτουργία συστήματος προστασίας κυβερνητικών ιστοτόπων	**Q4 2021 – συνεχής δραστηριότητα**
	3.Α.6. Πρόγραμμα παρακολούθησης και αξιολόγησης επιπέδου ασφάλειας ελληνικού κυβερνοχώρου (threat intelligence tool)	**Q1 2022 – συνεχής δραστηριότητα**
	3.Α.7. Εγκατάσταση και παραμετροποίηση open source εργαλείου συστήματος αυτόματης ειδοποίησης για την διαθεσιμότητα των ιστοτόπων και των δικτυακών συσκευών	**Q4 2022 – συνεχής δραστηριότητα**
		Q4 2022 – συνεχής δραστηριότητα

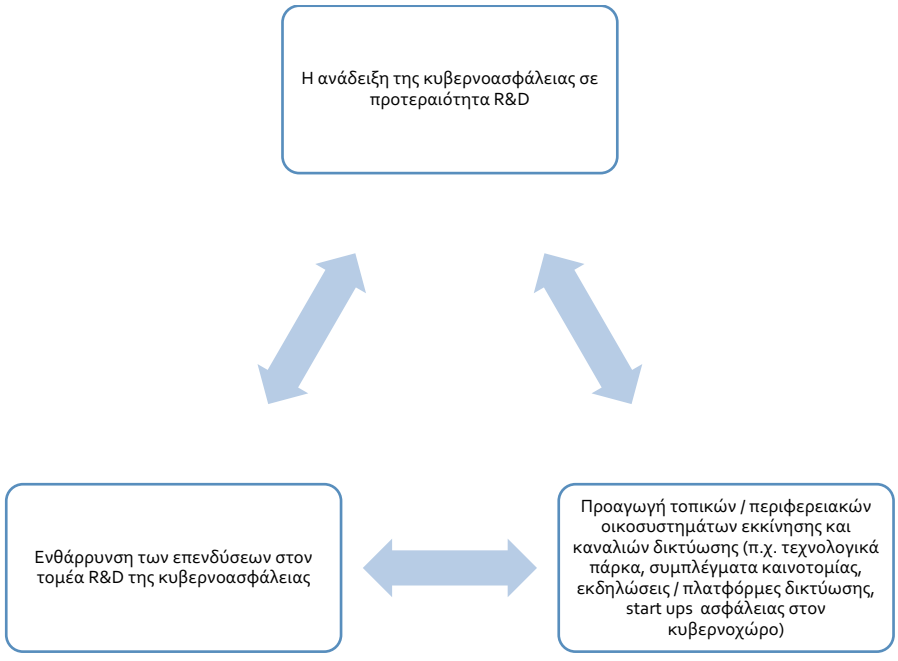
	3.Α.8. Εγκατάσταση open source πλατφόρμας για vulnerability assessment και διενέργεια ελέγχων Τρωτότητας (Penetration tests)	
	3.Α.9. Εγκατάσταση και παραμετροποίηση εργαλείου log file & malware analysis	**Q4 2022 – συνεχής δραστηριότητα**
	3.Α.10. Εγκατάσταση και παραμετροποίηση open source εργαλείου για ανταλλαγή δεικτών IOCs με άλλους οργανισμούς κυβερνοασφάλειας (Εθνικό CERT, CERT/ΔΙΚΥΒ, CERT ΕΔΗΤΕ, FORTHcert)	**Q4 2023 – συνεχής δραστηριότητα**
	3.Α.11. Συγκρότηση κεντρικού συντονιστικού μηχανισμού για τη διαχείριση αναφορών στο πλαίσιο του GDPR, NISD, art. 13a, eIDAS	**Q2 2023– συνεχής δραστηριότητα**
	3.Α.12. Εκπόνηση ετήσιων δελτίων και landscape reports για περιστατικά κυβερνοεπιθέσεων	**Q4 2024 – συνεχής δραστηριότητα**
	3.Α.13. Λειτουργία εργαστηρίου για ανάλυση log files και κυβερνοπεριστατικών	**Q4 2024 – συνεχής δραστηριότητα**
3.Β. Ενδυνάμωση μηχανισμών αποτροπής και βελτιστοποίηση της επιχειρησιακής συνεργασίας	**3.Β.1.** Ανάπτυξη δικτύου ενισχυμένης συνεργασίας για την καταπολέμηση του κυβερνοεγκλήματος	**Q4 2021 – συνεχής δραστηριότητα**
	3.Β.2. Επεξεργασία συνολικής πρότασης για το κυρωτικό πλαίσιο της δημόσιας πολιτικής κυβερνοασφάλειας	**Q2 2024**
	3.Β.3. Δημιουργία και αξιοποίηση σύγχρονων εργαλείων και τεχνικών για την πάταξη του κυβερνοεγκλήματος	**Q1 2021 – Q4 2025**
3.Γ. Κυβερνοασφάλεια και προστασία της ιδιωτικότητας	**3.Γ.1.** Ανάπτυξη θεσμικής συνεργασίας/μικτής ομάδας συνεργασίας με ΑΠΔΠΧ και ΑΔΑΕ στο πλαίσιο της προστασίας της ιδιωτικότητας	**Q4 2021 – συνεχής δραστηριότητα**
	3.Γ.2. Ανάπτυξη και παρακολούθηση πλατφόρμας καταγραφής δεδομένων κυβερνοεπιθέσεων που ενέχουν παραβίαση της ιδιωτικότητας	**Q2 2024**

10 ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ 4. ΕΝΑ ΣΥΓΧΡΟΝΟ ΕΠΕΝΔΥΤΙΚΟ ΠΕΡΙΒΑΛΛΟΝ ΜΕ ΕΜΦΑΣΗ ΣΤΗΝ ΠΡΟΑΓΩΓΗ ΤΗΣ ΈΡΕΥΝΑΣ ΚΑΙ ΑΝΑΠΤΥΞΗΣ

10.1 Ειδικος Στοχος 4.Α.: Προαγωγη της Έρευνας και Αναπτυξης

Ένας από τους σημαντικότερους τομείς ενίσχυσης του εθνικού επιπέδου κυβερνοασφάλειας είναι η υποστήριξη από το κράτος της έρευνας και ανάπτυξης τόσο σε ακαδημαϊκό όσο και σε ιδιωτικό επίπεδο. Οι εν λόγω πρωτοβουλίες μπορεί να αφορούν τη συμμετοχή Φορέων (δημόσιοι ή/και ιδιωτικοί) σε ευρωπαϊκούς διαγωνισμούς με στόχο την ανάπτυξη κρίσιμων νέων τεχνολογιών και μέτρων κυβερνοασφάλειας, είτε την ενίσχυση δράσεων ιδιωτικών Φορέων στον τομέα της εφαρμοσμένης έρευνας, ή ακόμα και την αναμόρφωση προγραμμάτων σπουδών ώστε να καλυφθούν θέματα κυβερνοασφάλειας (π.χ. ενίσχυση μεταπτυχιακών προγραμμάτων, σεμινάρια, πιστοποιήσεις, κλπ.).

Η Αρχή θα αποτελέσει το σημείο επαφής μεταξύ όλων των εμπλεκόμενων Φορέων, ώστε, λαμβάνοντας υπόψη τις κατάλληλες πληροφορίες και κατανοώντας σε βάθος το διαρκώς μεταβαλλόμενο περιβάλλον ΤΠΕ, να παρέχει τις κατευθυντήριες γραμμές για στοχευμένες δράσεις με σαφή χρονοδιαγράμματα και αναμενόμενα αποτελέσματα. Συγκεκριμένα, στο πλαίσιο του παρόντος στόχου επιμέρους δράσεις συνιστούν:



Εικόνα 15 Προαγωγή της Έρευνας και της Ανάπτυξης (R&D) στον τομέα της κυβερνοασφάλειας

Οι ανωτέρω παρεμβάσεις πρόκειται να συστηματοποιηθούν στο πλαίσιο της εκπόνησης μιας μεσομακροπρόθεσμης R&D αντζέντας με θεματικές που προωθούν την εφαρμογή της στρατηγικής κυβερνοασφάλειας και τη δικτύωση για την ανάπτυξη καινοτομιών στον τομέα της κυβερνοασφάλειας (π.χ. τεχνολογικά πάρκα, συμπλέγματα καινοτομίας κ.λπ.). Υπό το εν λόγω πρίσμα, καίριος παράγοντας είναι η ανάπτυξη ενισχυμένης συνεργασίας με ακαδημαϊκούς και ερευνητικούς φορείς.

10.2 Ειδικος Στοχος 4.Β.: Παροχη κινητρων στον ιδιωτικο τομεα για επενδυσεις σε μετρα ασφαλειας

Η επιτυχής υλοποίηση της Στρατηγικής στηρίζεται στην επένδυση των Φορέων σε οργανωτικά, τεχνικά και άλλα μέτρα κυβερνοασφάλειας. Ως άμεση απόρροια της αξιολόγησης κινδύνων κυβερνοσφάλειας, οι Φορείς θα πρέπει να υλοποιήσουν τα απαιτούμενα μέτρα για τη διασφάλιση των επιχειρησιακών τους λειτουργιών σύμφωνα με τις βασικές απαιτήσεις και αρχές κυβερνοασφάλειας. Η Στρατηγική ορίζει κίνητρα για τους Φορείς ώστε να τους κινητοποιήσει προς την εφαρμογή κατάλληλων δράσεων, ενισχύοντας έτσι το προφίλ τους και συνδράμοντας στην επιτυχή αντιμετώπιση περιστατικών. Υπό το πρίσμα αυτό, καίριες δράσεις συνιστούν:

- Η χαρτογράφηση των διαθέσιμων χρηματοδοτικών πόρων και η ενδυνάμωση του συστήματος αξιοποίησής τους.
- Η παροχή στοχευμένων κινήτρων (π.χ. φορολογικών, χρηματοπιστωτικών κ.λπ.).
- Η ανάπτυξη καινοτόμων εργαλείων ενδυνάμωσης της κυβερνοασφάλειας φορέων.

Για την αποτελεσματική χρηματοδότηση των εν λόγω παρεμβάσεων προκρίνεται η δημιουργία μιας εργαλειοθήκης (toolkit) κινήτρων σε συνεργασία με τους κατά περίπτωση αρμόδιους φορείς, με στόχο την παρακίνηση των επιχειρήσεων στην επένδυση μέτρων κυβερνοασφάλειας. Στο πλαίσιο της εν λόγω εργαλειοθήκης μπορούν να συμπεριληφθούν δημοσιονομικά και οικονομικά κίνητρα, όπως π.χ. μειωμένη φορολόγηση, επιχορηγήσεις κ.α. Περαιτέρω, η ανάπτυξη και αξιοποίηση καινοτόμων μηχανισμών χρηματοδότησης αλλά και μηχανισμών βελτιστοποίησης - επιτάχυνσης και απλοποίησης διαδικασιών για τη χρηματοδότηση δράσεων κυβερνοασφάλειας, πρόκειται να συμβάλλει καίρια στην πάταξη της γραφειοκρατίας και την αποτελεσματικότερη κατανομή των πόρων προς όφελος των Φορέων.

10.3 Ειδικος Στοχος 4.Γ.: Αξιοποιηση Συμπραξεων Δημοσιου και Ιδιωτικου τομεα (Σ.Δ.Ι.Τ.)

Η αγαστή συνεργασία μεταξύ του Δημόσιου και Ιδιωτικού τομέα αποτελεί κρίσιμο παράγοντα επιτυχίας της Εθνικής Στρατηγικής Κυβερνοασφάλειας, μιας και διαπιστευμένες επιχειρήσεις θα μπορούν να παράσχουν, κατά το δοκούν, υπηρεσίες μέσω Συμπράξεων Δημοσίου και Ιδιωτικού Τομέα (Σ.Δ.Ι.Τ.). Στο πλαίσιο αυτό κρίσιμη ενέργεια συνιστά η σύνταξη μητρώου με ιδιωτικούς φορείς, οι οποίοι, εφόσον πληρούν συγκεκριμένες προϋποθέσεις (διαπίστευση) θα συμπράξουν, με φορείς του δημοσίου, με

σκοπό την παροχή εξιδεικευμένων υπηρεσιών προς όφελος της ψηφιακής διακυβέρνησης. Ενδεικτικά:

- Παροχή συμβουλευτικών υπηρεσιών ασφάλειας.
- Παροχή υπηρεσιών διασύνδεσης και προστασίας από επιθέσεις DoS/DDoS.
- Παροχή υπηρεσιών τεχνικών ελέγχων ασφάλειας.
- Παροχή υπηρεσιών threat intelligence.
- Εγκατάσταση και λειτουργία εξοπλισμού ή/και λογισμικού ασφάλειας.

Το μητρώο μπορεί να περιλαμβάνει πληροφορίες όπως:

- Αντιστοίχιση φορέων με τις υπηρεσίες που ενδέχεται να ζητηθούν από την Αρχή, είτε για εσωτερικούς σκοπούς, είτε για λογαριασμό των εποπτευόμενων φορέων.
- Ένδειξη κόστους ανά επίπεδο στελέχους.
- Τρόπος έκδοσης εντολών αγοράς (work orders) ή μίνι-διακηρύξεων για συγκεκριμένα αντικείμενα.
- Επίπεδα παροχής απόκρισης Φορέα και υπηρεσιών (SLA).
- Ενδεικτικοί όροι συναλλαγών, τιμολόγησης, ρήτρες, κλπ.

Επιπροσθέτως, προτείνεται η διαπίστευση των εν λόγω φορέων, μέσω κριτηρίων που θα αφορούν ενδεικτικά:

- Εμπειρία παρόχου και στελεχών του.
- Πιστοποιήσεις.
- Παρουσία στην Ελληνική αγορά.
- Έργα σε Ευρωπαϊκούς οργανισμούς.

10.4 ΕΜΒΛΗΜΑΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

ΣΤΟΧΟΙ	ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	ΟΡΟΣΗΜΑ
4.Α. Προαγωγή της Έρευνας και Ανάπτυξης	**4.Α.1.**Εκπόνηση μεσομακροπρόθεσμης R&D αντζέντας με θεματικές που προωθούν την εφαρμογή της στρατηγικής κυβερνοασφάλειας.	**Q1 2022 – συνεχής δραστηριότητα**
	4.Α.2. Προαγωγή δικτύωσης για την εφαρμογή καινοτομιών στον τομέα της κυβερνοασφάλειας (τεχνολογικά πάρκα, συμπλέγματα καινοτομίας κ.λπ.)	**Q2 2023 – συνεχής δραστηριότητα**
	4.Α.3. Ανάπτυξη ενισχυμένης συνεργασίας με ακαδημαϊκούς και ερευνητικούς φορείς σε θέματα κυβερνοασφάλειας	**Q2 2022 - συνεχής δραστηριότητα**

4.Β. Παροχή επενδυτικών κινήτρων	**4.Β.1.** Δημιουργία εργαλειοθήκης (toolkit) για την παρακίνηση των επιχειρήσεων στην επένδυση μέτρων κυβερνοασφάλειας με χρησιμοποίηση δημοσιονομικών και οικονομικών κινήτρων όπως π.χ. μειωμένη φορολόγηση, επιχορηγήσεις κ.α.	**Q2 2022 - συνεχής δραστηριότητα**
	4.Β.2. Ανάπτυξη καινοτόμων μηχανισμών χρηματοδότησης	**Q2 2022 - συνεχής δραστηριότητα**
4.Γ. Αξιοποίηση Συμπράξεων Δημόσιου και Ιδιωτικού τομέα (ΣΔΙΤ)	**4.Γ.1.** Εκπόνηση απαιτήσεων για παρόχους υπηρεσιών κυβερνοασφάλειας	**Q3 2022**
	4.Γ.2. Έναρξη προγραμματικής συνεργασίας με την Ειδική Γραμματεία ΣΔΙΤ	**Q4 2021**
	4.Γ.3. Κατάρτιση μητρώου συμπραττουσών εταιριών	**Q4 2022**

11 ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ 5. ΑΝΑΠΤΥΞΗ ΙΚΑΝΟΤΗΤΩΝ (CAPACITY BUILDING), ΠΡΟΑΓΩΓΗ ΤΗΣ ΕΝΗΜΕΡΩΣΗΣ ΚΑΙ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗΣ

11.1 Ειδικος Στοχος 5.Α.: Βελτιωση ικανοτητων μεσω οργανωσης καταλληλων ασκησεων

Βασικό στόχο της Στρατηγικής αποτελεί η δημιουργία πλαισίου διαρκούς εκπαίδευσης και αξιολόγησης της ετοιμότητας των Φορέων στο να αποκριθούν σε συμβάντα κυβερνοασφάλειας. Προς αυτή την κατεύθυνση, η Αρχή, σε συνεργασία με Εθνικούς και Ευρωπαϊκούς φορείς, θα καθορίσει το περιεχόμενο και το ρυθμό διενέργειας ασκήσεων κυβερνοασφάλειας, ώστε να εξομοιώσει, στο μέτρο που αυτό είναι δυνατό, απειλές που ενδέχεται να επηρεάσουν τις λειτουργίες της Δημόσιας Διοίκησης και των λοιπών εμπλεκόμενων Φορέων. 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. Για την εκτέλεση των ασκήσεων δύναται να χρησιμοποιηθούν συγκεκριμένες ηλεκτρονικές (online) πλατφόρμες που παρέχουν δυνατότητες καθορισμού σεναρίων, ορισμού ομάδων (επιτιθέμενοι, αμυνόμενοι), παρακολούθησης της εξέλιξης της άσκησης, καταγραφής δεξιοτήτων ανά ομάδα και μέλος αυτής, καθώς και συνεργασίας με πληθώρα φορέων από κρίσιμους, για τη Δημόσια Διοίκηση, τομείς. Ταυτόχρονα, η Αρχή θα συμμετέχει ενεργά σε ασκήσεις όπως η Cyber Europe που διοργανώνεται από τον Ευρωπαϊκό Οργανισμό Ασφάλειας Πληροφοριών και Δικτύων (ENISA) ή η Locked Shields που διοργανώνεται από το ΝΑΤΟ ή ο ΠΑΝΟΠΤΗΣ που διοργανώνεται από το ελληνικό κράτος.

11.1.1 Ανάπτυξη και χρήση πλατφόρμας "cyber range"

Καθώς οι ασκήσεις κυβερνοασφάλειας σε Εθνικό επίπεδο είναι δύσκολο να οργανωθούν, ενώ απαιτούν σημαντικά κονδύλια για τη διοργάνωση και επιτυχή ολοκλήρωσή τους, η Αρχή προτείνεται να προβεί σε ανάπτυξη ή χρήση πλατφόρμας cyber range. Οι εν λόγω πλατφόρμες είναι διαδικτυακές (online platforms) και αποσκοπούν στη δημιουργία περιβάλλοντος το οποίο εξομοιώνει πραγματικά δίκτυα, επιτιθέμενους και χρήστες, μέσα από ένα πλαίσιο προσομοίωσης το οποίο απαντάται σε διαδικτυακά παίγνια. Ουσιαστικά, οι πλατφόρμες cyber range χρησιμοποιούνται ως ακολούθως:

— Ο επικεφαλής των ασκήσεων (π.χ. η Εθνική Αρχή Κυβερνοασφάλειας) ορίζει το περιβάλλον για το οποίο θα λάβει χώρα μια άσκηση, ενώ ομαδοποιεί τους χρήστες (π.χ. στελέχη Φορέων) σε κόκκινη ομάδα (επιτιθέμενοι) και μπλε ομάδα (αμυνόμενοι). Ταυτόχρονα, θέτει τους στόχους και ορίζει το χρονικό διάστημα μέσα στο οποίο θα πρέπει να έχει ολοκληρωθεί η άσκηση.

— Κάθε ομάδα έχει ένα σενάριο το οποίο θα πρέπει να ακολουθήσει, με πληθώρα εργαλείων να είναι διαθέσιμα, όπως penetration testing tools, forensic tools κ.λπ.

— Ο επικεφαλής γνωρίζει τη λύση για κάθε πιθανό σενάριο, ανά ομάδα, και μπορεί να παράσχει σύντομες πληροφορίες (tips) στα μέλη της, τα οποία όμως μπορεί να καταναλώνουν πόντους (εφόσον το έχει ορίσει ο επικεφαλής) προκειμένου να αποκτήσουν πρόσβαση σε μέρος της λύσης της άσκησης. Όσο μειώνονται οι πόντοι μιας ομάδας, τόσο «μειώνεται η αξιολόγησή» της έναντι της «αντίπαλης».

— Ο επικεφαλής παρακολουθεί την πορεία των μελών των ομάδων και είναι σε θέση να κατανοήσει τυχόν κενά που υπάρχουν αναφορικά με δεξιότητες, χρόνους απόκρισης, κλπ., ώστε να παραχθούν οι κατάλληλες αναφορές που θα χρησιμοποιηθούν για την περαιτέρω εκπαίδευση μελών Φορέων.

— Τα μέλη των ομάδων συνεργάζονται, ανταλλάσσουν ιδέες, δοκιμάζουν νέες πρακτικές και εργαλεία, ενώ κατανοούν το επίπεδο δεξιοτήτων τους σε πληθώρα σεναρίων τα οποία, δυνητικά, αποτελούν πραγματικά σενάρια απειλών.

Κατά συνέπεια, η ανάπτυξη ή η χρήση υπάρχουσας πλατφόρμας (από εξειδικευμένους παρόχους), θα βοηθήσει στο να δημιουργηθεί το κατάλληλο περιβάλλον για την τεχνική εκπαίδευση των στελεχών Φορέων, διατηρώντας τη συνεχή επαγρύπνησή τους έναντι κυβερνοαπειλών που μπορεί να θέσουν σε κίνδυνο την επιχειρησιακή τους λειτουργία και παροχή υπηρεσιών.

11.2 Ειδικος Στοχος 5.Β.: Αξιοποιηση συγχρονων μεθοδων και εργαλειων καταρτισης και εκπαιδευσης

Ιδιαίτερη έμφαση δίδεται στην προετοιμασία των μελλοντικών στελεχών των Φορέων στον τομέα της κυβερνοασφάλειας, για το οποίο απαιτείται έμπρακτη υποστήριξη και από τα ιδρύματα ανώτερης και ανώτατης εκπαίδευσης. Άρρηκτα συνδεδεμένη με την ενίσχυση της έρευνας και ανάπτυξης και της συνεργασίας μεταξύ

Φορέων, είναι η δημιουργία κατάλληλων κινήτρων ώστε οι νεότερες γενιές να έρθουν σε άμεση επαφή με την κυβερνοασφάλεια και να μπορούν να την επιλέξουν ως αντικείμενο σπουδών ή εξειδίκευσης. Απώτερος στόχος αποτελεί η εγκαθίδρυση πλαισίου κυβερνο-υγιεινής και η δημιουργία θετικής κουλτούρας προς την κυβερνοασφάλεια.

Ειδικότερα, στις εμβληματικές δραστηριότητες του εν λόγω ειδικού στόχου συγκαταλέγονται, μεταξύ άλλων:

11.2.1 Σχέδιο Δράσης για την Εκπαίδευση και την Ευαισθητοποίηση

Η ανάπτυξη ικανοτήτων, η συστηματική και διαρκής εκπαίδευση, αλλά και η ευαισθητοποίηση και διατήρηση ενός υψηλού επιπέδου ενημερότητας όλων των συμμετεχόντων στο Εθνικό Οικοσύστημα Κυβερνοσφάλειας, αποτελούν βασικά στοιχεία για την εξασφάλιση της εγρήγορσης έναντι των απειλών και της αποτελεσματικής ανταπόκρισης στα περιστατικά ασφάλειας.

Καθοριστικής σημασίας για την επιτυχή έκβαση των δράσεων του παρόντα στρατηγικού στόχου, αποτελεί η ανάπτυξη σχεδίου εκπαίδευσης συμβατό και εναρμονισμένο με τις ανάγκες του Οικοσυστήματος. Στο σχέδιο πρέπει να τίθενται συγκεκριμένοι στόχοι σχετικά με την εκπαίδευση και ενημέρωση των διαφορετικών ομάδων ενδιαφερομένων και να ιχνογραφείται ο οδικός χάρτης για την επίτευξη τους.

Ένα **Σχέδιο Δράσης για την Εκπαίδευση και την Ευαισθητοποίηση**, πρέπει να περιλαμβάνει την ανάλυση της υφιστάμενης κατάστασης (παγιωμένες δράσεις και εμπλεκόμενοι, καταγραφή της κουλτούρας για την κυβερνοασφάλεια, ο ρόλος των ακαδημαϊκών ιδρυμάτων, κ.τ.λ.), με σκοπό την ανάδειξη των ελλείψεων του Οικοσυστήματος. Το σχέδιο πρέπει να συμπληρωθεί με στοχευμένες δράσεις και δραστηριότητες. Κρίνεται απαραίτητη η διάκριση των σχετικών δραστηριοτήτων, ανάλογα με το κοινό στο οποίο απευθύνονται (επαγγελματίες κυβερνοασφάλειας, στελέχη ή επιτελικά στελέχη επιχειρήσεων, πολίτες κ.τ.λ.).

Το Σχέδιο Δράσης για την Εκπαίδευση και την Ευαισθητοποίηση, πλαισιώνει τους υπόλοιπους ειδικούς στόχους, παρέχοντας κατευθυντήριες γραμμές για την βελτίωση της κουλτούρας, της αντίληψης αλλά και της τεχνογνωσίας που απαιτείται για ένα υψηλό επίπεδο ασφάλειας των πληροφοριών. Επίσης, πρέπει να υποστηρίζεται από μηχανισμούς για την παρακολούθηση και τη μέτρηση της επίτευξης των σχετικών στόχων.

11.2.2 Πλαίσιο αναβάθμισης Τεχνογνωσίας και Ικανοτήτων Επαγγελματιών

Βασικό στόχο της Στρατηγικής, αποτελεί η δημιουργία πλαισίου διαρκούς εκπαίδευσης και ετοιμότητας των Φορέων στο να αποκριθούν σε συμβάντα κυβερνοασφάλειας. Προς αυτή την κατεύθυνση, οι αρμόδιοι φορείς πρέπει να καθορίσουν συγκεκριμένες δράσεις και παρεμβάσεις, που να αφορούν στους παρακάτω πυλώνες.

- Ακαδημαϊκή Εκπαίδευση

Ιδιαίτερη έμφαση δίδεται στην προετοιμασία των μελλοντικών στελεχών των Φορέων στον τομέα της κυβερνοασφάλειας, για την οποία βασικό ρόλο διαδραματίζουν τα ακαδημαϊκά ιδρύματα, τόσο με την δημιουργία κατάλληλων προπτυχιακών και

μεταπτυχιακών προγραμμάτων σπουδών, όσο και με την δημιουργία κατάλληλων κινήτρων για την προσέλκυση σπουδαστών στους σχετικούς κλάδους σπουδών.

Σχετικές δράσεις είναι: α) η αποτίμηση της κάλυψης των ελάχιστων ικανοτήτων που απαιτεί το υφιστάμενο τοπίο απειλών (threat landscape) και β) ο καθορισμός στοχευμένων δράσεων για την προσέλκυση σπουδαστών.

- Επαγγελματική Κατάρτιση

Εξίσου σημαντική θεωρείται η τακτική επικαιροποίηση των γνώσεων και δεξιοτήτων των επαγγελματιών, καθώς οι τεχνολογικές εξελίξεις αλλά και απειλές, μεταβάλλονται συνεχώς.

Σχετικές δράσεις είναι: α) ο καθορισμός κινήτρων για τις δημόσιες και ιδιωτικές επιχειρήσεις και στους επαγγελματίες αυτών, για συμμετοχή των τελευταίων σε δράσεις κατάρτισης και β) η δημιουργία εξειδικευμένων προγραμμάτων κατάρτισης

- Δια-βίου Μάθηση

Προγράμματα σπουδών που να υποστηρίζουν επαγγελματίες σχετικών επαγγελματικών κλάδων και ειδικοτήτων, ώστε να ενημερωθούν και να εκπαιδευτούν σε κατάλληλους τομείς της κυβερνοασφάλειας, εμπλουτίζοντας έτσι το διαθέσιμο ανθρώπινο δυναμικό.

Σχετικές δράσεις είναι: α) η καταγραφή και ανάλυση του υφιστάμενου πλαισίου δια-βίου μάθησης και β) η δημιουργία προτάσεων για παρεμβάσεις σχετικές με την προσέλκυση επαγγελματιών διαφορετικών κλάδων.

Ειδικά για τις δράσεις που σχετίζονται με την ακαδημαϊκή εκπαίδευση, κρίνεται σκόπιμο να σχεδιαστούν επαγγελματικά προφίλ για τους διάφορους ρόλους στον τομέα της κυβερνοασφάλειας. Ο σαφής ορισμός ρόλων, εμπεριέχει περιγραφή προσόντων, καθηκόντων, που δρουν βοηθητικά σε οποιαδήποτε δράση κατάρτισης και εκπαίδευσης. Επίσης, παρέχεται σαφής επαγγελματικός προσανατολισμός στους ενδιαφερόμενους νέους.

Ειδικά για τις δράσεις ανάπτυξης ικανοτήτων, ιδιαίτερα αποτελεσματικός μηχανισμός ανάπτυξης δεξιοτήτων αποτελεί η διενέργεια ασκήσεων κυβερνοασφάλειας, που εξομοιώνουν περιστατικά ασφάλειας βάσει προκαθορισμένων σεναρίων. Οι εν λόγω ασκήσεις εξυπηρετούν με πολλούς τρόπους του συμμετέχοντες: α) αξιολόγηση της ετοιμότητας και των σχεδίων έκτακτης ανάγκης, β) καλλιέργεια της ανταλλαγής πληροφοριών και γνώσεων και της συνεργασίας, γ) δοκιμή και ανάπτυξη δεξιοτήτων.

11.2.3 Δημιουργία υλικού

Έχοντας κατανοήσει και ορίσει τις ομάδες – target groups που η κάθε εκπαιδευτική δράση θα έχει ως στόχο, η Αρχή προτείνεται να προχωρήσει στη δημιουργία του κατάλληλου υλικού. Τονίζεται η ανάγκη συμμετοχής και άλλων αρχών, όπως ο ENISA, η ΑΠΔΠΧ, η ΕΕΤΤ, η Δ/νση Ηλεκτρονικού Εγκλήματος Ελληνικής Αστυνομίας, ιδιωτικοί φορείς, κλπ.

Το υλικό αφορά, μεταξύ άλλων:

- Ενημέρωση στελεχών – παρουσίαση: Θα εξηγεί στα στελέχη Φορέων τις βασικές αρχές της νέας κουλτούρας, τις νέες επιθυμητές συμπεριφορές καθώς και τυχόν θέματα που μπορεί να προκύψουν για τον εκάστοτε Φορέα από τη μη εφαρμογή των νέων κανόνων και διαδικασιών από τους εργαζομένους. Η εν λόγω παρουσίαση θα μπορεί να χρησιμοποιηθεί κατά τη διάρκεια ένταξης νέων στελεχών.
- Ανάπτυξη ενημερωτικού υλικού – φυλλάδια και αφίσες: Για θέματα όπως: Κακόβουλο λογισμικό, Κοινωνική μηχανική και phishing, Προστασία προσωπικών δεδομένων, study visits, Κινητές συσκευές, Χρήση ηλεκτρονικού ταχυδρομείου, Επίσκεψη σε ιστότοπους, Προστασία εξοπλισμού κατά τη διάρκεια των διακοπών, κλπ.
- Ανάπτυξη ενημερωτικών ηλεκτρονικών μηνυμάτων / e-mails με συμβουλές (tips): Θα στέλνονται στα στελέχη σε συγκεκριμένες χρονικές περιόδους όπου η συχνότητα των περιστατικών για διαρροές ή κλοπές δεδομένων είναι πιο αυξημένη και με προειδοποιήσεις αναφορικά με ιούς ή άλλους κινδύνους (π.χ. Οκτώβριος – cyber security, Νοέμβριος Black Friday, περίοδος Χριστουγέννων-Πρωτοχρονιάς, περίοδοι εκπτώσεων, Πάσχα, καλοκαιρινές διακοπές, τριήμερα).
- Ανάπτυξη προγραμμάτων e-learning: Θα περιλαμβάνουν τεστ στο οποίο τα Στελέχη θα καλούνται να επιβεβαιώσουν ότι κατανοούν τους κανόνες και τις συμπεριφορές που επιβάλλει η νέα κουλτούρα ασφάλειας πληροφοριών. Το πρόγραμμα θα καλύπτει τις ακόλουθες ενδεικτικές θεματικές ενότητες: Προστασία δεδομένων Φορέα, Προστασία προσωπικών δεδομένων, Ορθή χρήση συστημάτων, Ορθή χρήση κωδικών ασφάλειας, Ορθή χρήση εταιρικού ηλεκτρονικού ταχυδρομείου, Κινητές συσκευές και μονάδες αποθήκευσης, Κοινωνική μηχανική, Αναφορά συμβάντων ασφάλειας, Καλές πρακτικές, Φυσική ασφάλεια, κλπ.
- Ανάπτυξη εκπαιδευτικού προγράμματος για στελέχη Διευθύνσεων ή Τμημάτος Πληροφορικής (διαχειριστές συστημάτων, developers, κλπ.).
- Εκπαίδευση εκπαιδευτών – στελεχών των Φορέων που θα αναλάβουν στη συνέχεια την υλοποίηση εκπαιδεύσεων σε θέματα διαχείρισης & προστασίας δεδομένων.
- Frequently asked questions (FAQ): Καθορισμός πιθανών ερωτήσεων και σχετικές απαντήσεις (θα μπορούν να αναρτηθούν σε ιστότοπους, κλπ.).
- Hotline όπου Φορείς (ΦΕΒΥ και ΠΨΥ) θα μπορούν να απευθύνονται για διευκρινήσεις, απορίες ή άλλα θέματα που άπτονται της ασφάλειας πληροφοριών (διαδικασία, ερωτήματα, escalation points, περιγραφή ρόλου κλπ).
- Online alerting application: Εγκατάσταση και χρήση εργαλείου ψηφιακής εφαρμογής η οποία αποσκοπεί στο να ενισχύει τα εκπαιδευτικά μηνύματα στους χρήστες, υπενθυμίζοντάς τους μέσω μηνυμάτων στο κινητό τη σημασία της ασφάλειας και προστασίας των δεδομένων, βοηθώντας με τον τρόπο αυτό στην εδραίωση των επιθυμητών συμπεριφορών.

11.2.4 Σεμινάρια

Ιδιαίτερη βαρύτητα θα δοθεί σε εκπαιδευτικά σεμινάρια Υπεύθυνων Ασφάλειας και Δικτύων τα οποία θα διοργανώσει η Αρχή.

11.3 Ειδικος Στοχος 5.Γ.: Διαρκης ενημερωση Φορεων και πολιτων αναφορικα με θεματα κυβερνοασφαλειας

Η επιτυχής υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας, εξαρτάται και από τη δημιουργία θετικής κουλτούρας ασφάλειας σε εθνικό επίπεδο. Η διαρκής ενημέρωση του γενικού πληθυσμού αποτελεί έναν από τους κρισιμότερους παράγοντες επιτυχίας της Στρατηγικής, και, ως εκ τούτου, πρέπει να αξιολογηθούν οι υφιστάμενες δράσεις ευαισθητοποίησης και ενημέρωσης (ως απόρροια του Σχεδίου Δράσης για την Εκπαίδευση και την Ευαισθητοποίηση) και να καθοριστούν οι περιοχές που χρήζουν περαιτέρω δραστηριοποίησης.

Σε συνεργασία με τους εμπλεκόμενους εθνικούς οργανισμούς, προτείνεται να δημιουργηθεί ένα **Εθνικό Πρόγραμμα Ευαισθητοποίησης για την Κυβερνοασφάλεια**, με σκοπό την πλήρη κάλυψη όλων των ηλικιακών και κοινωνικών ομάδων πολιτών, με κατάλληλο και σύγχρονο υλικό ενημέρωσης.

Απώτερος στόχος αποτελεί η εγκαθίδρυση ενός πλαισίου κυβερνο-υγιεινής και η εγκαθίδρυση μια εθνικής κουλτούρας ευαισθητοποίησης ως προς την προαγωγή της κυβερνοασφάλειας.

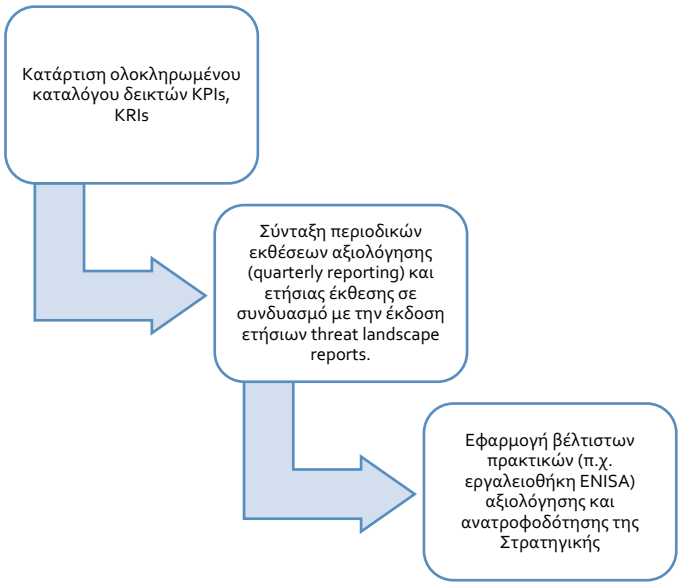
11.4 Εμβληματικες δραστηριοτητες

ΣΤΟΧΟΙ	ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	ΟΡΟΣΗΜΑ
5.Α. Βελτίωση ικανοτήτων μέσω οργάνωσης κατάλληλων ασκήσεων	**5.Α.1**. Εκπόνηση του Εθνικού Προγράμματος Ασκήσεων Κυβερνοασφάλειας	**Q1 2022 - συνεχής δραστηριότητα**
	5.Α.2. Ανάπτυξη ικανότητας και διαδικασιών "lessons learnt"	**Q1 2022 - συνεχής δραστηριότητα**
	5.Α.3. Αξιοποίηση πλατφόρμας τύπου "cyber range" για την εκπαίδευση των διαχειριστών (ασφάλειας, δικτύων, συστημάτων, εφαρμογών, βάσεων δεδομένων, κλπ.) της Αρχής και των Φορέων	**Q1 2022 - συνεχής δραστηριότητα**
5.Β. Αξιοποίηση σύγχρονων μεθόδων και εργαλείων κατάρτισης και εκπαίδευσης	**5.Β.1.** Κατάρτιση ενημερωτικού και εκπαιδευτικού υλικού (γενικό και ανά κατηγορία Φορέα)	**Συνεχής δραστηριότητα**
	5.Β.2. Εκπόνηση Σχεδίου Δράσης για την Εκπαίδευση και την Ευαισθητοποίηση	**Q1 2022**
	5.Β.3. Πλαίσιο αναβάθμισης Τεχνογνωσίας και Ικανοτήτων Επαγγελματιών	**Q4 2024 – Συνεχής δραστηριότητα**

5.Γ. Διαρκής ενημέρωση Φορέων και πολιτών σε θέματα κυβερνοασφάλειας	**5.Γ.1**. Εκπόνηση του Εθνικού Προγράμματος Ευαισθητοποίησης για την Κυβερνοασφάλεια	**Q4 2023 – Συνεχής δραστηριότητα**
	5.Γ.2. Διαμόρφωση πλαισίου επικοινωνιακής διαχείρισης περιστατικών	**Q1 2022 - συνεχής δραστηριότητα**

12 ΑΞΙΟΛΟΓΗΣΗ ΚΑΙ ΑΝΑΤΡΟΦΟΔΟΤΗΣΗ

Η υλοποίηση των στρατηγικών στόχων της Εθνικής Στρατηγικής Κυβερνοασφάλειας παρακολουθείται από την Εθνική Αρχή Κυβερνοασφάλειας, με σκοπό την αξιολόγηση και την ανατροφοδότηση της Στρατηγικής. Ειδικότερα, στο πλαίσιο αξιολόγησης και ανατροφοδότησης της Στρατηγικής θα οργανωθεί ένα ολοκληρωμένο σύστημα παρακολούθησης και αξιολόγησης της πορείας εφαρμογής της Στρατηγικής μέσω της ανάπτυξης κατάλληλων δεικτών μέτρησης (KPIs, KRIs), έκδοσης περιοδικών εκθέσεων και ετήσιας έκθεσης δράσεων και αποτελεσμάτων (παράλληλα με την έκδοση threat landscape report), αλλά και αξιοποίησης εργαλείων και βέλτιστων πρακτικών (π.χ. ENISA):



Εικόνα 16 Πλαίσιο αξιολόγησης και ανατροφοδότησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας

Λαμβάνοντας δε υπόψη την ανάγκη διαμόρφωσης ενός πιο μακροπρόθεσμου ορίζοντα στην υλοποίηση των περιγραφόμενων πρωτοβουλιών και δράσεων, προκρίνεται η παρούσα στρατηγική να επικαιροποιείται ανά πέντε έτη.

13 ΠΙΝΑΚΑΣ ΕΜΒΛΗΜΑΤΙΚΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ

ΣΤΡΑΤΗΓΙΚΟΙ ΣΤΟΧΟΙ	ΕΙΔΙΚΟΙ ΣΤΟΧΟΙ	ΕΜΒΛΗΜΑΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ	KPIs	ΟΡΟΣΗΜΑ
1. Ένα λειτουργικό σύστημα διακυβέρνησης	1.Α. Βελτιστοποίηση του πλαισίου οργάνωσης και λειτουργίας δομών και διαδικασιών	**1.Α.1.** Ανάπτυξη ολοκληρωμένου συστήματος διαχείρισης κυβερνοασφάλειας για φορείς του δημοσίου	Ε.Α.Κ.,φορείς κεντρικής δημόσιας διοίκησης, Εθνικό CERT, CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ	1.Α.1.Κ.1. Αριθμός Υ.Α.Π.Δ. /Αριθμός φορέων Κ.Δ.Δ. 1.Α.1.Κ.2. Αριθμός φορέων που αξιολογήθηκαν	**Q2 2021**
		1.Α.2. Ανάπτυξη πλαισίου προαγωγής της αριστείας στον τομέα της κυβερνοασφάλειας (cybersecurity excellence management framework)	Ε.Α.Κ.	1.Α.2.Κ.1. Αριθμός φορέων που πιστοποιήθηκαν 1.Α.2.Κ.2. Προσδιορισμός συνολικού δείκτη επίδοσης	**Q3 2022 – συνεχής δραστηριότητα**
		1.Α.3. Εκπόνηση τομεακών σχεδίων δράσης (π.χ. Energy, Healthcare, Transport, Finance, Telco, Maritime κ.λπ.)	Ε.Α.Κ., τομεακά Υπουργεία, Φ.Ε.Β.Υ./ Π.Ψ.Υ., CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ, Εθνικό CERT	1.Α.3.Κ.1. Αριθμός σχεδίων που εκπονήθηκαν/Αριθμός τομέων	**Q4 2024**
		1.Α.4. Ενδυνάμωση μηχανισμών ανταλλαγής πληροφοριών (information sharing)	Ε.Α.Κ., οικείοι φορείς	1.Α.4.Κ.1. Αριθμός φορέων δικτύου ανταλλαγής πληροφοριών	**Q2 2022**

	1.Β. Αποτελεσματικός σχεδιασμός αποτίμησης επικινδυνότητας και διαχείρισης έκτακτης ανάγκης.	**1.Β.1.** Ανάπτυξη μεθοδολογίας ανάλυσης δεδομένων και μητρώου καταγραφής απειλών	Ε.Α.Κ., φορείς Κεντικής Δημόσιας Διοίκησης, Φ.Ε.Β.Υ./ Π.Ψ.Υ., CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ, Εθνικό CERT, ΚΕΜΕΑ	1.Β.1.Κ.1. Σύνολο δεδομένων συστήματο	**Q4 2021**
		1.Β.2. Εθνικός σχεδιασμός αποτίμησης επικινδυνότητας	Ε.Α.Κ., φορείς Κεντικής Δημόσιας Διοίκησης, Φ.Ε.Β.Υ./ Π.Ψ.Υ., CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ, Εθνικό CERT, ΚΕΜΕΑ	1.Β.2.Κ.1. Ολοκλήρωση σχεδιασμού	**Q4 2021 – συνεχής αξιολόγηση και επικαιροποίηση**
		1.Β.3. Εθνικός σχεδιασμός έκτακτης ανάγκης	Ε.Α.Κ., φορείς Κεντικής Δημόσιας Διοίκησης, Φ.Ε.Β.Υ./ Π.Ψ.Υ., CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ, Εθνικό CERT, ΚΕΜΕΑ	1.Β.3.Κ.1. Ολοκλήρωση σχεδιασμού	**Q4 2021 – συνεχής αξιολόγηση και επικαιροποίηση**
	1.Γ. Ενδυνάμωση συνεργασιών σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο	**1.Γ.1.** Ενίσχυση της Ελληνικής παρουσίας και συμμετοχής σε διεθνείς συμμαχίες για θέματα κυβερνοασφάλειας.	Ε.Α.Κ., ΥΠΕΞ, Εθνικό CERT	1.Γ.1.Κ.1. Αριθμός συνεργασιών/ συμμαχιών	**Συνεχής δραστηριότητα**
		1.Γ.2. Υποστήριξη των συνεργασιών με τρίτα κράτη για μεταφορά τεχνογνωσίας από και προς αυτές με στόχο την ενίσχυση του κοινά υψηλού επιπέδου ασφάλειας και την αποδοτικότερη αντιμετώπιση των διασυνοριακών απειλών.	Ε.Α.Κ., ΥΠΕΞ, Εθνικό CERT	1.Γ.2.Κ.1. Αριθμός συνεργασιών 1.Γ.2.Κ.2. Αριθμός σχετικών δράσεων	**Συνεχής δραστηριότητα**
		1.Γ.3. Δημιουργία μεθόδου καθορισμού των προσδοκώμενων συνεργασιών	Ε.Α.Κ., ΥΠΕΞ, Εθνικό CERT	1.Γ.3.Κ.1. Αριθμός συμφώνων συνεργασίας	**Q4 2021 – Συνεχής δραστηριότητα**

		για θέματα κυβερνοασφάλειας και σύναψη συμφώνων συνεργασίας με τρίτες χώρες.			
		1.Γ.4. Δημιουργία μοντέλου διαχείρισης ώστε μέσω της συνεργασίας να επιτυγχάνεται πρόοδος στην περαιτέρω ανάπτυξη του εθνικού επιπέδου ασφάλειας, ικανοτήτων και ευαισθητοποίησης	Ε.Α.Κ., ΥΠΕΞ, Εθνικό CERT	1.Γ.4.Κ.1. Κατάταξη σε διεθνείς δείκτες	**Q4 2021 – Συνεχής δραστηριότητα**
2. Θωράκιση κρίσιμων υποδομών, ασφάλεια και νέες τεχνολογίες	2.Α. Κατανόηση των τεχνολογικών εξελίξεων και του τρόπου που επηρεάζουν την ψηφιακή διακυβέρνηση.	**2.Α.1.** Εφαρμογή ολοκληρωμένου πλαισίου κυβερνοασφάλειας για τα δίκτυα 5G	Ε.Α.Κ, Α.Δ.Α.Ε., Ε.Ε.Τ.Τ., ΥΠΕΞ, Εθνικό CERT	2.Α.1.Κ.1. Θέσπιση πλαισίου	**Q4 2021 - συνεχής δραστηριότητα**
		2.Α.2. Εφαρμογή πλαισίου μέτρων και δράσεων για την Τεχνητή Νοημοσύνη	Ε.Α.Κ. , Εθνικό CERT	2,Α,2,Κ.1. Έκδοση πλαισίου	**Q4 2021 – συνεχής δραστηριότητα**
		2.Α.3. Εφαρμογή πλαισίου μέτρων και δράσεων για το Internet of Things (IoT)	Ε.Α.Κ. , Εθνικό CERT	2.Α.3.Κ.1. Έκδοση πλαισίου	**Q4 2021 – συνεχής δραστηριότητα**
		2.Α.4. Ανάπτυξη ενισχυμένης συνεργασίας με ακαδημαϊκούς και ερευνητικούς φορείς πάνω στις νέες τεχνολογίες	Ε.Α.Κ., επιστημονικοί - ερευνητικοί φορείς, Γ.Γ.Ε.Τ. , Εθνικό CERT	2.Α.4.Κ.1. Αριθμός συνερασιών που υλοποιούνται	**Q4 2021 – συνεχής δραστηριότητα**
	2.Β.Αναβάθμιση της προστασίας κρίσιμων υποδομών	**2.Β.1.** Καθορισμός και επικαιροποίηση καταλόγου κρίσιμων υποδομών	Ε.Α.Κ.	2.Β.1.Κ.1. Έκδοση καταλόγου	**Q4 2022**
		2.Β.2. Ανάπτυξη και εφαρμογή ενιαίου συντονιστικού πλαισίου για τους CISO	Ε.Α.Κ., Φ.Ε.Β.Υ. / Π.Ψ.Υ.	2.Β.2.Κ.1. Έκδοση πλαισίου	**Q1 2022**

		2.Β.3.Ανάπτυξη πρακτικών ανίχνευσης, ποσοτικοποίησης, προτεραιοποίησης, έγκαιρης προειδοποίησης και διαχείρισης κινδύνων για κρίσιμες υποδομές	Ε.Α.Κ., Φ.Ε.Β.Υ. / Π.Ψ.Υ., CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ, Εθνικό CERT	2.Β.3.Κ.1. Έκδοση αποτίμησης επικινδυνότητας	**Q4 2022**
		2.Β.4. Εκπόνηση threat landscape reports	Ε.Α.Κ., φορείς Κεντικής Δημόσιας Διοίκησης, Φ.Ε.Β.Υ./ Π.Ψ.Υ., CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ, Εθνικό CERT, ΚΕΜΕΑ	.Β.4.Κ.1. Αριθμός εκθέσεων/έτος	**Q4 2025**
	2.Γ.Θωράκιση συστημάτων και εφαρμογών μέσω ενισχυμένων απαιτήσεων ασφαλείας	**2.Γ.1**.Ανάπτυξη και διαχείριση μητρώου υποδομών (hardware), λογισμικού (software) και άυλων πληροφοριακών αγαθών σε κρίσιμους τομείς (δημόσιο, κρίσιμες υποδομές)	Ε.Α.Κ.	2.Γ.1.Κ.1. Αριθμός υποδομών μητρώου	**Q4 2021 – συνεχής δραστηριότητα**
		2.Γ.2. Κατηγοριοποίηση φορέων για τον προσδιορισμό ενισχυμένων απαιτήσεων ασφαλείας	Ε.Α.Κ.	2.Γ.2.Κ.1. Αριθμός φορέων που κατηγοριοποιήθηκαν	**Q2 2023**
		2.Γ.3. Έκδοση ενισχυμένων απαιτήσεων ασφαλείας (οριζόντια και τομεακά) λαμβάνοντας υπόψη τα διεθνή και ευρωπαϊκά standards και πλαίσια πιστοποίησης	Ε.Α.Κ., φορείς Κεντικής Δημόσιας Διοίκησης, Φ.Ε.Β.Υ./ Π.Ψ.Υ., CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ, Εθνικό CERT, ΚΕΜΕΑ	2.Γ.3.Κ.1. Έκδοση απαιτήσεων ασφαλείας	**Συνεχής δραστηριότητα**
		2.Γ.4. Έκδοση ειδικών απαιτήσεων ασφάλειας σε έργα ΤΠΕ	Ε.Α.Κ.	2.Γ.4.Κ.1. Έκδοση ειδικών απαιτήσεων	**Q4 2022 - συνεχής δραστηριότητα**
		2.Γ.5. Ανάπτυξη συστήματος ελέγχων (audit) εφαρμογής των απαιτήσεων ασφάλειας	Ε.Α.Κ.	2.Γ.5.Κ.1. Έλεγχοι/έτος 2.Γ.5.Κ.2. Φορείς που ελέγχονται/έτος	**Q4 2021 – συνεχής δραστηριότητα**

		2.Γ.6. Ανάπτυξη ολοκληρωμένου συστήματος αξιολόγησης επιπέδου ωριμότητας φορέων	Ε.Α.Κ.	2.Γ.6.Κ.1. Φορείς που αξιολογήθηκαν	**Q4 2021 – συνεχής δραστηριότητα**
3. Βελτιστοποίηση διαχείρισης περιστατικών, καταπολέμηση του κυβερνοεγκλήματος και προστασία της ιδιωτικότητας	3.Α. Βελτιστοποίηση μεθόδων, τεχνικών και εργαλείων ανάλυσης, απόκρισης και κοινοποίησης συμβάντων	**3.Α.1.** Δημιουργία Κέντρου Παρακολούθησης Κρίσιμων Υποδομών Security Operations Center – SOC)	Ε.Α.Κ., Εθνικό CERT	3.Α.1.Κ.1. Αριθμός περιστατικών διαχείρισης/έτος	**Q4 2022 – συνεχής δραστηριότητα**
		3.Α.2. Δημιουργία Cyber hotline	Ε.Α.Κ., Εθνικό CERT	3.Α.2.Κ.1. Αριθμός κλήσεων	**Q2 2023– συνεχής δραστηριότητα**
		3.Α.3. Ορισμός πλαισίου διαχείρισης συμβάντων ασφάλειας	Ε.Α.Κ., Εθνικό CERT, CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ, ΚΕΜΕΑ, .Α.Δ.Α.Ε, Α.Π.Δ.Π.Χ.	3.Α.3.Κ.1. Έκδοση πλαισίου	**Q2 2022**
		3.Α.4. Κατάρτιση και διαχείριση μητρώου συμβάντων (επίσημα ή/και ανώνυμα), συμπεριλαμβανομένων όλων των πληροφοριών που αφορούσαν το συμβάν, ενέργειες που έλαβαν χώρα, αποτελέσματα, lessons learned.	Ε.Α.Κ., Εθνικό CERT, CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ, ΚΕΜΕΑ, .Α.Δ.Α.Ε, Α.Π.Δ.Π.Χ.	3.Α.4.Κ.1. Συμβάντα και δεδομένα που εγγράφονται στο μητρώο/μήνα	**Q4 2023 – συνεχής δραστηριότητα**
		3.Α.5. Λειτουργία συστήματος προστασίας κυβερνητικών ιστοτόπων	Ε.Α.Κ., Εθνικό CERT	3.Α.5.Κ.1. Αριθμός Ιστοτόπων που προστατεύονται	**Q4 2021 – συνεχής δραστηριότητα**
		3.Α.6. Πρόγραμμα παρακολούθησης και αξιολόγησης επιπέδου ασφάλειας ελληνικού κυβερνοχώρου (threat intelligence tool)	Ε.Α.Κ. , Εθνικό CERT	3.Α.6.Κ.1.Υλοποιηση συστήματος 3.Α.6.Κ.2. Σύνολο απειλών που καταγράφονται 3.Α.6.Κ.3. Αριθμός ενταγμένων φορέων/συσκευών	**Q1 2022 – συνεχής δραστηριότητα**

		3.Α.7. Εγκατάσταση και παραμετροποίηση open source εργαλείου συστήματος αυτόματης ειδοποίησης για την διαθεσιμότητα των ιστοτόπων και των δικτυακών συσκευών	Ε.Α.Κ., Εθνικό CERT	3.Α.7.Κ.1.Υλοποιηση συστήματος 3.Α.7.Κ.2. Σύνολο απειλών που καταγράφονται 3.Α.7.Κ.3. Αριθμός ενταγμένων φορέων/συσκευών	**Q4 2022 – συνεχής δραστηριότητα**
		3.Α.8. Εγκατάσταση open source πλατφόρμας για vulnerability assessment και διενέργεια ελέγχων Τρωτότητας (Penetration tests)	Ε.Α.Κ., Εθνικό CERT	3.Α.8.Κ.1.Υλοποιηση συστήματος 3.Α.8.Κ.2. Σύνολο απειλών που καταγράφονται 3.Α.8.Κ.3. Αριθμός ενταγμένων φορέων/συσκευών	**Q4 2022 – συνεχής δραστηριότητα**
		3.Α.9. Εγκατάσταση και παραμετροποίηση εργαλείου log file & malware analysis	Ε.Α.Κ., Εθνικό CERT	3.Α.9.Κ.1.Υλοποιηση συστήματος 3.Α.9.Κ.2. Σύνολο απειλών που καταγράφονται 3.Α.9.Κ.3. Αριθμός ενταγμένων φορέων/συσκευών	**Q4 2022 – συνεχής δραστηριότητα**
		3.Α.10. Εγκατάσταση και παραμετροποίηση open source εργαλείου για ανταλλαγή δεικτών IOCs με άλλους οργανισμούς	Ε.Α.Κ., Εθνικό CERT, CERT/ΔΙΚΥΒ, CERT ΕΔΗΤΕ, FORTHcert	3.Α.10.Κ.1. Σύνολο δεικτών που ανταλλάχθηκαν/μήνα	**Q4 2023 – συνεχής δραστηριότητα**

		κυβερνοασφάλειας (Εθνικό CERT, CERT/ΔΙΚΥΒ, CERT ΕΔΗΤΕ, FORTHcert)			
		3.Α.11. Συγκρότηση κεντρικού συντονιστικού μηχανισμού για τη διαχείριση αναφορών στο πλαίσιο του GDPR, NISD, art. 13a, eIDAS	Ε.Α.Κ., Εθνικό CERT, CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ, ΚΕΜΕΑ, .Α.Δ.Α.Ε, Α.Π.Δ.Π.Χ.	3.Α.11.Κ.1. Σύνολο περιστατικών που εντάχθηκαν στο μηχανισμό/έτος	**Q2 2023– συνεχής δραστηριότητα**
		3.Α.12. Εκπόνηση ετήσιων δελτίων και landscape reports για περιστατικά κυβερνοεπιθέσεων	Ε.Α.Κ., Εθνικό CERT, CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ, ΚΕΜΕΑ	3.Α.12.Κ.1. Σύνολο εκθέσεων/έτος	**Q4 2024 – συνεχής δραστηριότητα**
		3.Α.13. Λειτουργία εργαστηρίου για ανάλυση log files και κυβερνοπεριστατικών	Ε.Α.Κ., Εθνικό CERT	3.Α.13.Κ.1. Υλοποίηση εργαστηρίου	**Q4 2024 – συνεχής δραστηριότητα**
	3.Β. Ενδυνάμωση μηχανισμών αποτροπής και βελτιστοποίηση της επιχειρησιακής συνεργασίας	**3.Β.1.** Ανάπτυξη δικτύου ενισχυμένης συνεργασίας για την καταπολέμηση του κυβερνοεγκλήματος	Ε.Α.Κ., Υπουργείο Δικαιοσύνης, Δ.Η.Ε., ΥΠΕΞ	3.Β.1.Κ.1. Συναντήσεις /μήνα	**Q4 2021 – συνεχής δραστηριότητα**
		3.Β.2. Επεξεργασία συνολικής πρότασης για το κυρωτικό πλαίσιο της δημόσιας πολιτικής κυβερνοασφάλειας	Ε.Α.Κ.	3.Β.2.Κ.1. Σύνολο παραβάσεων/ έτος	**Q2 2024**
		3.Β.3. Δημιουργία και αξιοποίηση σύγχρονων εργαλείων και τεχνικών για την πάταξη του κυβερνοεγκλήματος	Ε.Α.Κ., Υπουργείο Δικαιοσύνης, Δ.Η.Ε., ΥΠΕΞ	3.Β.3.Κ..1. Σύνολο παραβάσεων/έτος	**Q1 2021 – Q4 2025**
	3.Γ. Κυβερνοασφάλεια και προστασία της ιδιωτικότητας	**3.Γ.1.** Ανάπτυξη θεσμικής συνεργασίας/μικτής ομάδας συνεργασίας με ΑΠΔΠΧ και ΑΔΑΕ στο πλαίσιο της προστασίας της ιδιωτικότητας	Ε.Α.Κ., Α.Δ.Α.Ε., Α.Π.Δ.Π.Χ.	3.Γ.1.Κ.1. Συνεδριάσεις ομάδας κατ' έτος	**Q4 2021 – συνεχής δραστηριότητα**
		3.Γ.2. Ανάπτυξη και παρακολούθηση πλατφόρμας καταγραφής δεδομένων	Ε.Α.Κ., Α.Δ.Α.Ε., Α.Π.Δ.Π.Χ.	3.Γ.2.Κ.1. Δεδομένα που καταχωρήθηκαν στην πλατφόρμα	**Q2 2024**

		κυβερνοεπιθέσεων που ενέχουν παραβίαση της ιδιωτικότητας			
4. Ένα σύγχρονο επενδυτικό περιβάλλον με έμφαση στην προαγωγή της Έρευνας και Ανάπτυξης	4.Α. Προαγωγή της Έρευνας και Ανάπτυξης	**4.Α.1.**Εκπόνηση και εφαρμογή μεσομακροπρόθεσμης R&D αντζέντας με θεματικές που προωθούν την εφαρμογή της στρατηγικής κυβερνοασφάλειας.	Ε.Α.Κ., Υπουργείο Παιδείας, Υπουργείο Ανάπτυξης και Επενδύσεων, επιστημονικοί - ερευνητικοί φορείς, , ΚΕΤΥΑΚ/ΕΥΠ	4.Α.1.Κ.1. Έκδοση ατζέντας	**Q1 2022 – συνεχής δραστηριότητα**
		4.Α.2. Προαγωγή δικτύωσης για την εφαρμογή καινοτομιών στον τομέα της κυβερνοασφάλειας (τεχνολογικά πάρκα, συμπλέγματα καινοτομίας κ.λπ.)	Ε.Α.Κ., Υπουργείο Παιδείας, Υπουργείο Ανάπτυξης και Επενδύσεων, επιστημονικοί - ερευνητικοί φορείς, ΚΕΤΥΑΚ/ΕΥΠ	4.Α.2.Κ.1. Αριθμός τεχν. πάρκων, συμπλεγμάτων κ.λπ.	**Q2 2023 – συνεχής δραστηριότητα**
		4.Α.3. Ανάπτυξη ενισχυμένης συνεργασίας με ακαδημαϊκούς και ερευνητικούς φορείς σε θέματα κυβερνοασφάλειας	Ε.Α.Κ., Υπουργείο Παιδείας, Υπουργείο Ανάπτυξης και Επενδύσεων, επιστημονικοί - ερευνητικοί φορείς, ΚΕΤΥΑΚ/ΕΥΠ	4.Α.3.Κ.1. Συνεργασίες/έτος	**Q2 2022 - συνεχής δραστηριότητα**
	4.Β. Παροχή επενδυτικών κινήτρων	**4.Β.1.** Δημιουργία εργαλειοθήκης (toolkit) για την παρακίνηση των επιχειρήσεων στην επένδυση μέτρων κυβερνοασφάλειας με χρησιμοποίηση δημοσιονομικών και οικονομικών κινήτρων όπως π.χ. μειωμένη φορολόγηση, επιχορηγήσεις κ.α.	Ε.Α.Κ., Υπουργείο Ανάπτυξης και Επενδύσεων, Υπουργείο Οικονομικών	4.Β.1.Κ.1. Αριθμός φορέων που χρηματοδοτήθηκαν	**Q2 2022 - συνεχής δραστηριότητα**
		4.Β.2. Ανάπτυξη καινοτόμων μηχανισμών χρηματοδότησης	Ε.Α.Κ., επιστημονικοί - ερευνητικοί φορείς, Γ.Γ.Ε.Τ.	4.Β.2.Κ.1. Αριθμός φορέων που χρηματοδοτήθηκαν	**Q2 2022 - συνεχής δραστηριότητα**

	4.Γ. Αξιοποίηση Συμπράξεων Δημόσιου και Ιδιωτικού τομέα (ΣΔΙΤ)	**4.Γ.1.** Εκπόνηση απαιτήσεων για παρόχους υπηρεσιών κυβερνοασφάλειας	Ε.Α.Κ., Υπουργείο Ανάπτυξης και Επενδύσεων, Υπουργείο Οικονομικών	4.Γ.1.Κ.1. Έκδοση απαιτήσεων	**Q3 2022**
		4.Γ.2. Έναρξη προγραμματικής συνεργασίας με την Ειδική Γραμματεία ΣΔΙΤ	Ε.Α.Κ., Υπουργείο Ανάπτυξης και Επενδύσεων, Υπουργείο Οικονομικών	4.Γ.2.Κ.1. Συναντήσεις/έτος	**Q4 2021**
		4.Γ.3. Κατάρτιση μητρώου συμπραττουσών εταιριών	Ε.Α.Κ., Υπουργείο Ανάπτυξης και Επενδύσεων, Υπουργείο Οικονομικών	4.Γ.3.Κ.1. Εταιρίες που εγγράφονται στο μητρώο	**Q4 2022**
5. Ανάπτυξη ικανοτήτων (capacity building), προαγωγή της ενημέρωσης και ευαισθητοποίησης	5.Α. Βελτίωση ικανοτήτων μέσω οργάνωσης κατάλληλων ασκήσεων	**5.Α.1**. Ανάπτυξη ολοκληρωμένου προγράμματος διενέργειας ασκήσεων	Ε.Α.Κ., κατά περίπτωση εμπλεκόμενοι φορείς	5.Α.1.Κ.1. Σύνολο ασκήσεων/έτος 5.Α.1.Κ.2. Σύνολο εκπαιδευόμενων/έτος	**Q1 2022 - συνεχής δραστηριότητα**
		5.Α.2. Ανάπτυξη ικανότητας και διαδικασιών "lessons learnt"	Ε.Α.Κ.	5.Α.2.Κ.1. Σύνολο εγγραφών στο αποθετήριο ασκήσεων	**Q1 2022 - συνεχής δραστηριότητα**
		5.Α.3. Αξιοποίηση πλατφόρμας τύπου "cyber range" για την εκπαίδευση των διαχειριστών (ασφάλειας, δικτύων, συστημάτων, εφαρμογών, βάσεων δεδομένων, κλπ.) της Αρχής και των Φορέων	Ε.Α.Κ.	5.Α.3.Κ.1. Σύνολο ασκήσεων/έτος 5.Α.3.Κ.2. Σύνολο εκπαιδευόμενων/έτο	**Q1 2022 - συνεχής δραστηριότητα**
	5.Β. Αξιοποίηση σύγχρονων μεθόδων και εργαλείων	**5.Β.1.** Κατάρτιση ενημερωτικού και εκπαιδευτικού υλικού (γενικό και ανά κατηγορία Φορέα)	Ε.Α.Κ., φορείς παροχής εκπαίδευσης	5.Β.1.Κ.1 Αριθμός υλικού που διανεμήθηκε	**Συνεχής δραστηριότητα**

	κατάρτισης και εκπαίδευσης	**5.Β.2.** Εκπόνηση Σχεδίου Δράσης για την Εκπαίδευση και την Ευαισθητοποίηση	Ε.Α.Κ.	5.Β.2.Κ.1. Εκπόνηση Σχεδίου Δράσης	**Q1 2022**
		5.Β.3. Πλαίσιο αναβάθμισης Τεχνογνωσίας και Ικανοτήτων Επαγγελματιών	Ε.Α.Κ., φορείς παροχής εκπαίδευσης	5.Β.3.Κ.1. Εκπόνηση μελέτης, δημοσίευση 5.Β.3.Κ.2 Αριθμός δράσεων για προσέλκυση 5.Β.3.Κ.3. Αριθμός συμμετεχόντων	**Q4 2024 – Συνεχής δραστηριότητα**
	5.Γ. Διαρκής ενημέρωση Φορέων και πολιτών αναφορικά με θέματα κυβερνοασφάλειας	**5.Γ.1.** Εκπόνηση του Εθνικού Προγράμματος Ευαισθητοποίησης για την Κυβερνοασφάλεια	Ε.Α.Κ., εμπλεκόμενοι οικοσυστήματος	5.Γ.1.Κ.1. Αριθμός δράσεων 5.Γ.1.Κ.2. Εκπόνηση Προγράμματος	**Q4 2023 – Συνεχής δραστηριότητα**
		5.Γ.2. Διαμόρφωση πλαισίου επικοινωνιακής διαχείρισης περιστατικών	Ε.Α.Κ.	5.Γ.2.Κ.1. Αριθμός περιστατικών που διαχειρίστηκαν επικοινωνιακά	**Q1 2022 - συνεχής δραστηριότητα**

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Νοέμβριος 2020