ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

ΣΧΟΛΗ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ, ΕΠΙΚΟΙΝΩΝΙΑΣ ΚΑΙ ΠΟΛΙΤΙΣΜΟΥ

ΤΜΗΜΑ ΔΙΕΘΝΩΝ, ΕΥΡΩΠΑΪΚΩΝ & ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ

Ευρωπαϊκό Ποινικό Δίκαιο και Πολιτική

"Ασφάλεια στον Κυβερνοχώρο: Ευρω-ενωσιακό Κανονιστικό Πλαίσιο, Στρατηγική και Διαμόρφωση Πολιτικής"

Cyber Security: EU Regulatory Framework, Strategy and Policy Formation"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Νικολέτα Ε. Χρηστάτου

Αθήνα, 2023

Τριμελής Επιτροπή

Αργύρης Πασσάς, Επίτιμος Καθηγητής, Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών (Επιβλέπων)

Βασίλειος Χατζόπουλος, Καθηγητής, Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών

Όλγα Τσόλκα, Επίκουρη Καθηγήτρια, Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών

Περιεχόμενα

Περίληψη

Η παρούσα διπλωματική εργασία στοχεύει να αξιολογήσει τις τρέχουσες απειλές κατά του κυβερνοχώρου και να αναδείξει τη συμβολή της Ευρωπαϊκής Ένωσης στη δημιουργία ενός ασφαλούς ψηφιακού περιβάλλοντος. Εξετάζει το ρυθμιστικό πλαίσιο της ΕΕ, τη χάραξη στρατηγικής και τη διαμόρφωση πολιτικής στον τομέα της κυβερνοασφάλειας, με ιδιαίτερη έμφαση στον αντίκτυπο και την εφαρμογή τους στην Ελλάδα.

Η αυξανόμενη εξάρτηση φυσικών προσώπων, φορέων, οντοτήτων και κρατών στον κυβερνοχώρο, μια τάση που συνεχίζει να βαθαίνει με την πάροδο του χρόνου. Ενώ η ενοποίηση του κυβερνοχώρου προσφέρει ευκολία και αποτελεσματικότητα, εκθέτει επίσης τις κοινωνίες σε διάφορους κινδύνους. Μέσω της παρούσας μελέτης επιδιώκεται η εμβάθυνση στην απάντηση της Ευρωπαϊκής Ένωσης σε αυτές τις προκλήσεις, παρακολουθώντας την εξέλιξη της νομοθεσίας της για την κυβερνοασφάλεια. Ως σημεία-κλειδιά στην πορεία αυτή χαρακτηρίζονται ο Κανονισμός 881/2019 και οι οδηγίες 2016/1148 (NIS 1)[1] και 2555/2022 (NIS 2[2]).

Ο Κανονισμός 881/2019 γνωστός και ως Νόμος για την Ασφάλεια στον Κυβερνοχώρο, αντιπροσωπεύει ένα σημαντικό βήμα για την ενοποίηση της προσέγγισης της Ένωσης για την ενίσχυση της ασφάλειας στον κυβερνοχώρο. Κεντρικά σημεία του αποτέλεσαν η ενίσχυση του ENISA, η εναρμόνιση των προτύπων κυβερνοασφάλειας των κρατών μελών, καθώς και η εξουσιοδότηση που παρείχε στα κράτη μέλη να ιδρύσουν Εθνικές Αρχές Πιστοποίησης Κυβερνοασφάλειας (NCCA), συμβάλλοντας ούτως σημαντικα στην οικοδόμηση της εμπιστοσύνης του κοινού στην ψηφιακή αγορά. Παράλληλα, η μετάβαση από την Οδηγία 2016/1148 (NIS 1)[3] στην Οδηγία 2555/2022 (NIS 2) σηματοδοτεί μια σημαντική εξέλιξη στο τοπίο της κυβερνοασφάλειας της Ένωσης, με το NIS 2 να έχει ιδιαίτερη επιρροή στη διαμόρφωση της πραγματικότητας της κυβερνοασφάλειας σε ενωσιακό επίπεδο εν γένει αλλά και στην Ελλάδα ειδικότερα.

Με την παρούσα μελέτη υπογραμμίζεται η περίπλοκη σχέση μεταξύ της διαμόρφωσης πολιτικής και της στρατηγικής στο ζήτημα της κυβερνοασφάλειας. Αν και διαφέρουν ως προς τις λειτουργίες τους, αυτές οι διαδικασίες είναι στενά αλληλένδετες και ζωτικής σημασίας

[1] Ενσωμάτωση με Ν. 4577/2018 (ΦΕΚ Α' 199/03.12.2018)
[2] Επεται η ενσωμάτωση
[3] Ενσωμάτωση με Ν. 4577/2018 (ΦΕΚ Α' 199/03.12.2018)

για την αποτελεσματική διακυβέρνηση και την ασφάλεια του κυβερνοχώρου. Μέσα από την ανάλυση των διαφορετικών πτυχών της διαμόρφωσης πολιτικής και της στρατηγικής, επισημαίνονται οι προκλήσεις και οι πολυπλοκότητες που συνεπάγεται η προσπάθεια ισχυροποίησης της ενωσιακής θέσης στον κυβερνοχώρο, τονίζοντας την ανάγκη για ισχυρές και δυναμικές απαντήσεις πολιτικής από πλευράς Ευρωπαϊκής Ένωσης.

Μέσα από την ανάλυση των ανωτέρω, αναδύεται μια νέα παλέτα ερωτημάτων, όπως το ζήτημα αν η αποτελεσματικότητα των στρατηγικών κυβερνοασφάλειας των κρατών μελών σήμερα μπορεί να παραμείνει η ίδια όταν στην πραγματικότητα ο κυβερνοχώρος κατακλύζεται από νέες τεχνολογίες όπως η τεχνητή νοημοσύνη και το blockchain, οι συνέπειες των οποίων είναι ακόμα ένα αχαρτογράφητο πεδίο.

Λέξεις-κλειδιά

Κυβερνοχώρος, Κυβερνοασφάλεια, Τεχνολογίες Πληροφορικής και Επικοινωνιών, Ενωσιακή Στρατηγική για την Κυβερνοασφάλεια

Abstract

This thesis aims to assess current cyber threats and highlight the European Union's contribution to creating a secure digital environment. It examines the EU regulatory framework, strategy-making and policy-making in the field of cybersecurity, with a particular focus on their impact and implementation in Greece.

The growing dependence of individuals, agencies, entities and states on cyberspace, a trend that continues to deepen over time. While cyber consolidation offers convenience and efficiency, it also exposes societies to various risks. This study seeks to deepen into the European Union's response to these challenges by monitoring the evolution of its cybersecurity legislation. Regulation 881/2019 and directives 2016/1148 (NIS 1) and 2555/2022 (NIS 2) are characterized as key points along this path.

Regulation 881/2019 also known as the Cybersecurity Act represents an important step in unifying the Union's approach to strengthening cyber security. Its central points were the strengthening of ENISA, the harmonization of Member States' cybersecurity standards, as well as the authorization given to Member States to establish National Cybersecurity Certification Authorities (NCCA), thus contributing significantly to building public confidence in the digital market. At the same time, the transition from Directive 2016/1148 (NIS 1) to Directive 2555/2022 (NIS 2) marks an important development in the Union's cybersecurity landscape, with NIS 2 having a particular influence in shaping the cybersecurity reality in the Union level in general but also in Greece in particular.

This study highlights the complex relationship between policy-making and strategy in the issue of cybersecurity. Although they differ in their functions, these processes are closely interrelated and vital to effective cyber governance and security. Through the analysis of different aspects of policy-making and strategy, the challenges and complexities involved in trying to strengthen the Union's position in cyberspace are highlighted, highlighting the need for strong and dynamic policy responses from the European Union.

Through the analysis of the above, a new palette of questions emerges, such as the question of whether the effectiveness of Member States' cybersecurity strategies today can remain the same when in fact cyberspace is flooded by new technologies such as artificial intelligence and blockchain, the consequences of which is still an uncharted field.

Keywords

Cyberspace, Cybersecurity, Information and Communication Technologies, Union Cybersecurity Strategy

Εισαγωγή

Το έτος 1999, ο δεκαπεντάχρονος μαθητής J. Jonathan James, από το Pinecrest της Φλόριντα, κατάφερε να εγκαταστήσει μια κερκόπορτα[4] σε στρατιωτικούς διακομιστές των ΗΠΑ και να αποκτήσει πρόσβαση στον πηγαίο κώδικα του Διεθνούς Διαστημικού Σταθμού (ISS). Ο δεκαπεντάχρονος James, αρχικά εντόπισε μια ευπάθεια σε κυβερνητικό διακομιστή στην περιφέρεια της Βιρτζίνια, εκμεταλλευόμενος τον οποίο εισήχθη στα συστήματα της Ομοσπονδιακής Κυβέρνησης των ΗΠΑ, παρεμποδίζοντας χιλιάδες μηνύματα μεταξύ των υπαλλήλων της Defense Threat Reduction Agency (DTRA)[5]. Για όλο το χρονικό διάστημα μεταξύ του Αυγούστου και Οκτωβρίου του 1999, ο James είχε πρόσβαση στους υπολογιστές της Defense Threat Reduction Agency (DTRA), ενός τμήματος του Υπουργείου Άμυνας που είναι υπεύθυνο για την ανάλυση πιθανών απειλών για τις Ηνωμένες Πολιτείες. Στη συνέχεια, αφού πραγματοποίησε επιθέσεις σε άλλους κυβερνητικούς υπολογιστές, συμπεριλαμβανομένων εκείνων που χειρίζετο η NASA στο Marshall Space Flight Center στην Αλαμπάμα, βρήκε τον πηγαίο κώδικα στο λογισμικό που εκτελεί τις κρίσιμες μονάδες του Διεθνούς Διαστημικού Σταθμού, όπως ο έλεγχος θερμοκρασίας και υγρασίας στους χώρους διαμονής του. Στην πραγματικότητα, ένας έφηβος, ερασιτέχνης hacker, αχρήστευσε τους υπολογιστές της NASA για 21 μέρες.

Σήμερα, σχεδόν 30 χρόνια μετά, παρατηρείται μια πρωτοφανής αύξηση της λειτουργικής εξάρτησης, της πλειονότητας ίσως των πτυχών, της καθημερινότητας μας από ηλεκτρονικής φύσεως συστήματα, όπως για παράδειγμα συναλλαγές με πιστωτικά ιδρύματα, θέματα διοικητικής φύσεως ή η υγειονομική περίθαλψη. Μάλιστα η περίοδος που διανύουμε έχει χαρακτηριστεί ως η "Τέταρτη Βιομηχανική Επανάσταση" (άλλως γνωστή και ως 4ΒΕ ή και Βιομηχανία 4.0) [6], καθώς σηματοδοτεί μια μεταμορφωτική εποχή

---

[4] Back door (κερκόπορτα/πίσω πόρτα), ή trap door (καταπακτή), είναι μια κρυφή είσοδος σε μια υπολογιστική συσκευή ή στο λογισμικό, που παρακάμπτει τα μέτρα ασφαλείας, όπως τα logins και την προστασία με τον κωδικό πρόσβασης. Κάποιοι ισχυρίζονται ότι οι κατασκευαστές (λογισμικού/υλικού) έχουν συνεργαστεί με τις υπηρεσίες πληροφοριών της κυβέρνησης (των ΗΠΑ και άλλων χωρών) για την κατασκευή κερκόπορτων στα προϊόντα τους. Τα Malware σχεδιάζονται, συχνά, για να εκμεταλλευτούν αυτές τις πίσω πόρτες ή τις ευπάθειες στα συστήματα Η/Υ.

[5] Η Defense Threat Reduction Agency (Υπηρεσία Μείωσης Αμυντικών Απειλών) είναι ο πνευματικός, τεχνικός και επιχειρησιακός ηγέτης για το Υπουργείο Άμυνας των ΗΠΑ (DoD) και τη Στρατηγική Διοίκηση των ΗΠΑ στην προσπάθεια καταπολέμησης βιολογικών, χημικών και πυρηνικών απειλών.

[6] Ξεκινώντας στα τέλη του 18ου αιώνα, η πρώτη βιομηχανική επανάσταση εισήγαγε τη μηχανοποίηση που κινούνταν με νερό και ατμό. Οι επακόλουθες βιομηχανικές επαναστάσεις είδαν την άνοδο της μαζικής παραγωγής μέσω του ηλεκτρισμού και της γραμμής συναρμολόγησης (δεύτερη επανάσταση) και την εμφάνιση της μηχανογράφησης και του αυτοματισμού (τρίτη επανάσταση) στα μέσα του 20ού αιώνα.

κατά την οποία οι παραδοσιακές βιομηχανίες υφίστανται βαθιές αλλαγές, ωθούμενη από την ενσωμάτωση ψηφιακών τεχνολογιών αιχμής, γνώσεων που βασίζονται σε δεδομένα και προηγμένους αυτοματισμούς. Χτισμένη στα θεμέλια που έθεσαν οι προηγούμενες βιομηχανικές επαναστάσεις, η τέταρτη βιομηχανική επανάσταση χαρακτηρίζεται από τη σύγκλιση διαφορετικών τεχνολογιών, όπως η τεχνητή νοημοσύνη, το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT)[7], η ρομποτική, η τρισδιάστατη εκτύπωση, το blockchain και τα προηγμένα υλικά. Η ψηφιοποίηση διαδραματίζει κεντρικό ρόλο, χρησιμοποιώντας τις ψηφιακές τεχνολογίες για να φέρει επανάσταση σε διαδικασίες, προϊόντα και υπηρεσίες. Ο αυτοματισμός, με γνώμονα τη ρομποτική και την τεχνητή νοημοσύνη, επικρατεί ολοένα και περισσότερο, αυτοματοποιώντας εργασίες και διαδικασίες λήψης αποφάσεων. Η διασυνδεσιμότητα επιτυγχάνεται μέσω του Διαδικτύου των Πραγμάτων (Internet of Things - IoT), επιτρέποντας απρόσκοπτες συνδέσεις μεταξύ συσκευών και συστημάτων για ανταλλαγή δεδομένων και συνεργασία σε πραγματικό χρόνο. Τα μεγάλα δεδομένα και τα αναλυτικά στοιχεία αξιοποιούν μεγάλα σύνολα δεδομένων για να αντλήσουν πολύτιμες πληροφορίες, ενημερώνοντας τις διαδικασίες λήψης αποφάσεων. Οι τεχνολογίες επαυξημένης πραγματικότητας (AR) και εικονικής πραγματικότητας (VR) ενισχύουν τις αλληλεπιδράσεις ανθρώπου-μηχανής και παρέχουν καθηλωτικές εμπειρίες. Οι βιομηχανίες σε όλο το φάσμα, συμπεριλαμβανομένης της μεταποίησης, της υγειονομικής περίθαλψης, των οικονομικών και των μεταφορών, αναδιαμορφώνονται από την Τέταρτη Βιομηχανική Επανάσταση. Ο αντίκτυπός της εκτείνεται πέρα από συγκεκριμένους τομείς, επηρεάζοντας την παγκόσμια οικονομία, τις αγορές εργασίας και τις κοινωνικές δομές.

Με βάση τις ριζικές αλλαγές που έχει επιφέρει η Τέταρτη Βιομηχανική Επανάσταση, αναπόφευκτα αναδιαμορφώνεται εντόνως και το τοπίο της διακυβέρνησης της Ευρωπαϊκής Ένωσης σε διάφορους τομείς. Εφόσον οι ψηφιακές τεχνολογίες συνεχίζουν να προοδεύουν, η Ένωση επεξεργάζεται με τη σειρά της πολιτικές για την πλοήγηση των μετασχηματιστικών επιπτώσεων της Τέταρτης Βιομηχανικής

[7] Το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) αναφέρεται στο δίκτυο φυσικών αντικειμένων ή «πραγμάτων» που είναι ενσωματωμένα με αισθητήρες, λογισμικό και άλλες τεχνολογίες με σκοπό τη σύνδεση και την ανταλλαγή δεδομένων με άλλες συσκευές και συστήματα μέσω του Διαδικτύου. Αυτά τα αντικείμενα κυμαίνονται από συνηθισμένα είδη οικιακής χρήσης έως εξελιγμένα βιομηχανικά εργαλεία.

Επανάστασης[8]. Πρωτοβουλίες όπως η ψηφιακή ενιαία αγορά[9] υπογραμμίζουν τη δέσμευση της Ένωσης για την προώθηση ενός εναρμονισμένου ψηφιακού περιβάλλοντος, την προώθηση της καινοτομίας και τη διευκόλυνση της απρόσκοπτης ροής δεδομένων στην περιοχή.

Αναγνωρίζοντας την ανάγκη για προσαρμοστικά ρυθμιστικά πλαίσια, η Ένωση επανεξετάζει και αναπτύσσει κανονισμούς που ευθυγραμμίζονται με τις σύγχρονες τεχνολογίες. Τομείς όπως η προστασία δεδομένων, η ασφάλεια στον κυβερνοχώρο, η τεχνητή νοημοσύνη και το Διαδίκτυο των Πραγμάτων αποτελούν κεντρικά σημεία του ενδιαφέροντός της. Οι προσπάθειες εξεύρεσης μια βιώσιμης ισορροπίας μεταξύ της δυνατότητας καινοτομίας και της διασφάλισης της προστασίας των πολιτών είναι εμφανείς στην προσέγγιση της Ένωσης για την έξυπνη ρύθμιση, με στόχο τη δημιουργία ενός περιβάλλοντος που υποστηρίζει τις τεχνολογικές εξελίξεις, ενώ παράλληλα αντιμετωπίζει πιθανούς κινδύνους.

Η ανθεκτικότητα στην κυβερνοασφάλεια συνιστά μια υψίστης σημασίας προτεραιότητα για την Ένωση, ενόψει των αυξανόμενων ψηφιακών απειλών. Ενδεικτικό είναι ότι σε έρευνα του Ευρωβαρόμετρου που δημοσιεύτηκε το 2013 στην οποία συμμετείχαν πάνω από 27.000 άτομα προερχόμενα από όλα τα κράτη μέλη, αν και το 70% των χρηστών του Διαδικτύου στην ΕΕ εμπιστεύονταν την ικανότητά τους να χρησιμοποιούν το Διαδίκτυο για αγορές ή τραπεζικές συναλλαγές, μόνο το 50% εξ αυτών επέλεγε τελικά να το χρησιμοποιήσει, προκειμένου να αποφευχθεί το ενδεχόμενο να πέσει θύμα ηλεκτρονικού εγκλήματος. Οι δύο κύριες ανησυχίες σχετικά με τέτοιου είδους διαδικτυακές δραστηριότητες φάνηκε να σχετίζονται με την κακή χρήση των προσωπικών δεδομένων (37% των ερωτηθέντων) και την ασφάλεια των πληρωμών μέσω του διαδικτύου (35%).

Η παρούσα μελέτη έχει ως σκοπό, αφού αποτυπώσει την υφιστάμενη κατάσταση σε επίπεδο απειλών κατά του κυβερνοχώρου, να αναδείξει τη συνεισφορά της Ένωσης σε επίπεδο Ευρω-Ενωσιακού κανονιστικού πλαισίου, χάραξης στρατηγικής και διαμόρφωσης

[8] Schwab, K. (2016). "The Fourth Industrial Revolution." World Economic Forum

[9] Η ψηφιακή ενιαία αγορά της ΕΕ (DSM) είναι μια στρατηγική που ξεκίνησε η Ευρωπαϊκή Ένωση (ΕΕ) για τη δημιουργία μιας ενοποιημένης ψηφιακής αγοράς που επιτρέπει την ελεύθερη κυκλοφορία ψηφιακών αγαθών, υπηρεσιών και δεδομένων μεταξύ των κρατών μελών. Στόχος της ψηφιακής ενιαίας αγοράς είναι να εξαλειφθούν τα εμπόδια στις διασυνοριακές διαδικτυακές δραστηριότητες εντός της ΕΕ, προωθώντας μια απρόσκοπτη και ολοκληρωμένη ψηφιακή οικονομία.

πολιτικής, αναφορικά με την επίτευξη ενός ασφαλούς κυβερνοχώρου.

1. Απειλές κατά της ασφάλειας στον Κυβερνοχώρο

1.1.Περιεχόμενο της έννοιας του Κυβερνοχώρου

"*Κυβερνοχώρος. Μια συναινετική παραίσθηση που βιώνουν καθημερινά δισεκατομμύρια νόμιμοι χειριστές, σε κάθε έθνος, από παιδιά που διδάσκονται μαθηματικές έννοιες... Μια γραφική αναπαράσταση δεδομένων που έχουν αφαιρεθεί από τις τράπεζες κάθε υπολογιστή στο ανθρώπινο σύστημα. Αδιανόητη πολυπλοκότητα. Γραμμές φωτός κυμαινόταν στον μη χώρο του μυαλού, τα σμήνη και οι αστερισμοί των δεδομένων. Όπως τα φώτα της πόλης, υποχωρούν..."*[10]. Αυτό το απόσπασμα από το μυθιστόρημα "Neuromancer" του William Gibson χαρακτηρίζει γλαφυρά την δυσκολία ακριβούς προσδιορισμού της έννοιας του κυβερνοχώρου[11]. Μετά το πέρας σχεδόν 4 δεκαετιών από το χρονικό σημείο που ο πρωτοπόρος Gibson μας χάρισε αυτή την τόσο ζωντανή και μεταφορική απεικόνιση περί της δυστοπίας του εικονικού τοπίου, αν και η έννοια “Κυβερνοχώρος” (Cyberspace) πλέον συνιστά αναπόσπαστο κομμάτι της καθημερινότητας του μέσου πολίτη, εργαζομένου, φοιτητή ή μαθητή, ιδιαίτερα κατά την μετά την πανδημία εποχή και παρά το αδιαμφισβήτητο της διάχυτης ενσωμάτωσης της ψηφιακής τεχνολογίας σε πληθώρα πτυχών της ζωής μας, η αποσαφήνιση της έννοιας του “Κυβερνοχώρου” δεν ακολούθησε την ίδια αλματώδη πορεία. Μέχρι και σήμερα υπάρχουν αντικρουόμενες απόψεις για το περιεχόμενο και την ακριβή σημασία του.

Σε μια προσπάθεια διατύπωσης του περιεχομένου της έννοιας, μπορεί να λεχθεί ότι ο “Κυβερνοχώρος” αναφέρεται στο εικονικό περιβάλλον που δημιουργείται από διασυνδεδεμένα συστήματα υπολογιστών και τις πληροφορίες που ανταλλάσσουν. Πρόκειται δηλαδή για έναν εννοιολογικό χώρο που υπάρχει στη σφαίρα των δικτύων υπολογιστών, και ο οποίος περιλαμβάνει το διαδίκτυο και άλλα διασυνδεδεμένα δίκτυα. Στον κυβερνοχώρο, τα άτομα μπορούν να συμμετέχουν σε διάφορες δραστηριότητες, όπως επικοινωνία, ανταλλαγή δεδομένων και διαδικτυακές αλληλεπιδράσεις. Ο όρος χρησιμοποιείται συχνά για να περιγράψει τον ψηφιακό τομέα όπου λαμβάνει χώρα η

[10] Gibson, W.. *Neuromancer*. New York: Ace Books, 1984

[11] Amy Novak, *Virtual Poltergeists and Memory: The Question of Ahistorcism in William Gibson's Neuromoncer (1984)*, Journal of the Fantastic in the Arts Vol. 11, No. 4 (44),2001, pp. 395-414

ηλεκτρονική επικοινωνία και η ανταλλαγή πληροφοριών, υπερβαίνοντας τα φυσικά όρια. Ο κυβερνοχώρος περιλαμβάνει ιστότοπους, διαδικτυακές πλατφόρμες, ψηφιακά κανάλια επικοινωνίας και την τεράστια γκάμα ψηφιακού περιεχομένου και υπηρεσιών προσβάσιμων μέσω του Διαδικτύου.

1.2. Απειλές για την ασφάλεια στον κυβερνοχώρο

Η αυξανόμενη εξάρτηση των πολιτών, αλλά και των κρατών, από τον κυβερνοχώρο, είναι πολύπλευρη και "βαθαίνει" όσο περνάει ο καιρός περισσότερο. Ωστόσο, ενώ η ενσωμάτωση του κυβερνοχώρου στη ζωή μας έχει αναμφισβήτητα επιφέρει ευκολία και αποτελεσματικότητα, έχει επίσης εκθέσει τα άτομα, τις κοινωνίες και τα ίδια τα κράτη σε πιθανούς κινδύνους, ανοίγοντας έτσι τον ασκό του αιόλου αναφορικά με κακόβουλες ενέργειες και απειλές, επηρεάζοντας μάλιστα ένα ευρύτατο φάσμα τομέων. Ορισμένοι από τους τρόπους που απειλείται η ασφάλεια των ψηφιακών συστημάτων είναι το κακόβουλο λογισμικό, το phishing, οι παραβιάσεις δεδομένων, η μη εξουσιοδοτημένη πρόσβαση, η κλοπή ταυτότητας,οι παραβιάσεις δεδομένων και οι διαδικτυακές απάτες.

1.2.1. Κακόβουλο Λογισμικό (Malware)

Ως κακόβουλο λογισμικό (Malware), νοείται κάθε τύπος λογισμικού που έχει σχεδιαστεί ειδικά για να βλάψει ή να εκμεταλλεύεται συστήματα υπολογιστών, δίκτυα ή χρήστες. Το κακόβουλο λογισμικό συνιστά μια ευρεία έννοια που περιλαμβάνει διάφορους τύπους κακόβουλων προγραμμάτων, το καθένα με τις δικές του λειτουργίες και σκοπούς, τα σημαντικότερα από τα οποία είναι τα ακόλουθα:

Οι ιοί (Viruses), οι οποίοι αποτελούν τύπο κακόβουλου λογισμικού, είναι προγράμματα που μπορούν να αναπαραχθούν με την προσάρτησή τους σε άλλα προγράμματα. Συχνά εξαπλώνονται μέσω μολυσμένων αρχείων και μπορεί να προκαλέσουν βλάβη στα αρχεία, το λογισμικό ή ακόμα και το υλικό του υπολογιστή. Άλλο είδος κακόβουλου λογισμικού συνιστούν οι Δούρειοι Ίπποι (Trojans), οι οποίοι είναι παραπλανητικά προγράμματα που μεταμφιέζονται ως νόμιμο λογισμικό. Μόλις εγκατασταθούν, μπορούν να παρέχουν μη εξουσιοδοτημένη πρόσβαση σε έναν υπολογιστή, επιτρέποντας σε κακόβουλους παράγοντες να κλέψουν ευαίσθητες πληροφορίες ή να πραγματοποιήσουν άλλες επιβλαβείς δραστηριότητες. Από την άλλη πλευρά, το Ransomware είναι τύπος κακόβουλου λογισμικού που κρυπτογραφεί τα αρχεία ενός χρήστη, καθιστώντας τα απρόσιτα. Στη συνέχεια, ο εισβολέας απαιτεί λύτρα, συνήθως σε

κρυπτονομίσματα[12][13], σε αντάλλαγμα για το κλειδί αποκρυπτογράφησης. Το κακόβουλο λογισμικό spyware, έχει σχεδιαστεί για να παρακολουθεί κρυφά και να συλλέγει πληροφορίες σχετικά με τις δραστηριότητες ενός χρήστη. Αυτό μπορεί να περιλαμβάνει πατήματα πλήκτρων, συνήθειες περιήγησης στον ιστό και προσωπικές πληροφορίες, οι οποίες στη συνέχεια αποστέλλονται στον εισβολέα. Το Adware, εμφανίζει ανεπιθύμητες διαφημίσεις στη συσκευή ενός χρήστη. Αν και δεν είναι εγγενώς επιβλαβές όπως ορισμένοι άλλοι τύποι κακόβουλου λογισμικού, το adware μπορεί να είναι παρεμβατικό και να επηρεάσει αρνητικά την εμπειρία του χρήστη. Τα σκουλήκια (worms)[14] είναι αυτοαναπαραγόμενα προγράμματα που μπορούν να εξαπλωθούν σε δίκτυα και υπολογιστές χωρίς την ανάγκη παρέμβασης του χρήστη. Συχνά εκμεταλλεύονται τα τρωτά σημεία ασφαλείας για να διαδοθούν. Τα botnet συνιστούν δίκτυα παραβιασμένων υπολογιστών (γνωστών ως bot) που ελέγχονται από έναν κεντρικό διακομιστή. Μπορούν να χρησιμοποιηθούν για διάφορες κακόβουλες δραστηριότητες, όπως η έναρξη συντονισμένων επιθέσεων σε ιστότοπους ή η αποστολή ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Τα Rootkit έχουν σχεδιαστεί για να αποκρύπτουν την παρουσία κακόβουλου λογισμικού σε ένα σύστημα ανατρέποντας ή αποφεύγοντας τους μηχανισμούς ασφαλείας του λειτουργικού συστήματος. Συχνά παρέχουν μη εξουσιοδοτημένη πρόσβαση σε υπολογιστή ή δίκτυο.

1.2.2. Ηλεκτρονικό Ψάρεμα (Phishing)

Το Ηλεκτρονικό Ψάρεμα (Phishing), αποτελεί τύπο κακόβουλου λογισμικού στα πλαίσια του οποίου οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου ή ιστότοπους για να εξαπατήσουν τα άτομα ώστε να παρέχουν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης ή στοιχεία πιστωτικών καρτών. Μπορεί να επηρεάσει σημαντικά τις τράπεζες και τη νομισματική πολιτική θέτοντας διάφορες απειλές για τα χρηματοπιστωτικά ιδρύματα, τους πελάτες τους και το συνολικό οικονομικό τοπίο.

Οι επιθέσεις ηλεκτρονικού ψαρέματος συχνά στοχεύουν στο να εξαπατήσουν άτομα

---

[12] Τα κρυπτονομίσματα, είναι ψηφιακές ή εικονικές μορφές νομισμάτων που χρησιμοποιούν κρυπτογραφία για ασφάλεια. Αυτό τα καθιστά αποκεντρωμένα και γενικά απρόσβλητα στον κυβερνητικό έλεγχο ή χειραγώγηση, σε αντίθεση με τα παραδοσιακά νομίσματα που εκδίδονται από την κυβέρνηση.

[13] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[14] Robert McMill, *Siemens: Stuxnet worm hit industrial systems*, 2010

ώστε να παρέχουν ευαίσθητες οικονομικές πληροφορίες, όπως διαπιστευτήρια σύνδεσης και στοιχεία πιστωτικής κάρτας. Μόλις αποκτηθούν, οι εγκληματίες του κυβερνοχώρου μπορούν να συμμετάσχουν σε μη εξουσιοδοτημένες συναλλαγές, οδηγώντας σε οικονομικές απώλειες τόσο τους πελάτες όσο και τις τράπεζες. Παράλληλα, οι επιθέσεις ηλεκτρονικού ψαρέματος μπορεί να έχουν ως αποτέλεσμα την κλοπή προσωπικών πληροφοριών, οι οποίες δύνανται να χρησιμοποιηθούν για τη δημιουργία ψευδών ταυτοτήτων. Αυτό, με τη σειρά του, μπορεί να οδηγήσει σε δόλια ανοίγματα λογαριασμών, αιτήσεις δανείου και άλλες οικονομικές δραστηριότητες. Οι επιτυχημένες προσπάθειες ηλεκτρονικού ψαρέματος μπορούν να οδηγήσουν και σε παραβιάσεις δεδομένων, εκθέτοντας ευαίσθητες πληροφορίες πελατών. Αυτό όχι μόνο βλάπτει τα άτομα που επηρεάζονται, αλλά μπορεί επίσης να βλάψει τη φήμη της τράπεζας και να διαβρώσει την εμπιστοσύνη των πελατών. Ακόμη, οι επιθέσεις ηλεκτρονικού ψαρέματος έχουν συχνά ως στόχο τραπεζικούς υπαλλήλους, προσπαθώντας να αποκτήσουν πρόσβαση σε εσωτερικά συστήματα και ευαίσθητα οικονομικά δεδομένα. Στις περιπτώσεις που οι επιθέσεις αποδεικνύονται επιτυχείς, οι επιτιθέμενοι ενδέχεται να παραβιάσουν λογαριασμούς, να χειραγωγήσουν οικονομικά αρχεία ή να πραγματοποιήσουν μη εξουσιοδοτημένες συναλλαγές. Τέλος, μπορεί από ανάλογες επιθέσεις να προκληθούν και λειτουργικές διαταραχές, όπως για παράδειγμα πρόκληση λειτουργικών διακοπών με τη διάδοση κακόβουλου λογισμικού ή ransomware στο δίκτυο μιας τράπεζας. Αυτό μπορεί να οδηγήσει σε διακοπές του συστήματος, καθυστερήσεις στις χρηματοοικονομικές συναλλαγές και αυξημένο λειτουργικό κόστος για το ίδρυμα.

Το ηλεκτρονικό ψάρεμα (phishing) μπορεί να εμφανιστεί είτε ως ηλεκτρονικό ψάρεμα μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (email phishing) , είτε ως ηλεκτρονικό ψάρεμα (spear phishing). Τα παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου επιδιώκουν να παραπλανήσουν τους παραλήπτες ώστε να αποκαλύψουν ευαίσθητες πληροφορίες ή να κάνουν κλικ σε κακόβουλους συνδέσμους. Το spear phishing έχει διαφορετική μορφή, καθώς στα πλαίσια αυτού λαμβάνουν χώρα στοχευμένες επιθέσεις phishing που επικεντρώνονται σε συγκεκριμένα άτομα ή οργανισμούς. Το τελευταίο θεωρείται ιδιαίτερα επικίνδυνο, καθώς όταν αντικείμενο της επίθεσης συνιστούν Τραπεζικά Ιδρύματα ή Κρατικές υπηρεσίες, τυχόν ευδοκίμηση τους μπορεί να επιφέρει ολέθριες συνέπειες - μεταξύ άλλων - οικονομικές, αλλά και σε επίπεδο ασφαλείας.

1.2.3. Κυβερνο-φυσικές επιθέσεις (Cyber-physical attacks)

Οι κρίσιμες υποδομές, όπως τα δίκτυα ηλεκτρικής ενέργειας ή τα συστήματα μεταφοράς, μπορεί να είναι ευάλωτα σε κυβερνο-φυσικές επιθέσεις που θα μπορούσαν να έχουν συνέπειες στον πραγματικό κόσμο. Οι κυβερνοφυσικές επιθέσεις, γνωστές και ως επιθέσεις κυβερνοφυσικού συστήματος (CPS), αναφέρονται σε έναν τύπο απειλής για την ασφάλεια που στοχεύει στην ενοποίηση μεταξύ συστημάτων που βασίζονται σε υπολογιστές και του φυσικού κόσμου. Με άλλα λόγια, αυτές οι επιθέσεις εκμεταλλεύονται τρωτά σημεία στα διασυνδεδεμένα συστήματα που συνδυάζουν λογισμικό, υλικό και φυσικά στοιχεία. Τα κυβερνοφυσικά συστήματα είναι διαδεδομένα σε διάφορους τομείς ζωτικής σημασίας υποδομών, συμπεριλαμβανομένης της μεταποίησης, της ενέργειας, των μεταφορών, της υγειονομικής περίθαλψης και των ηλεκτρονικών συστημάτων των πόλεων.

1.2.4. Ανησυχίες γεωπολιτικής και εθνικής ασφάλειας

Έχει λεχθεί ότι «*Ο κυβερνοχώρος είναι πλέον ένας τομέας επιχειρήσεων ίσος με αυτούς της ξηράς, της θάλασσας, του αέρα και του διαστήματος*[15]». Η αύξηση των απειλών ασφάλειας στον κυβερνοχώρο σε έναν υπερσυνδεδεμένο κόσμο, δεν θα μπορούσε να αφήσει ανεπηρέαστους τους τομείς της γεωπολιτικής σταθερότητας και της εθνικής ασφάλειας[16]. Οι κυβερνοεπιθέσεις σε κρίσιμες υποδομές μπορούν να προκαλέσουν εκτεταμένη αναστάτωση, υπογραμμίζοντας την ευπάθεια των βασικών υπηρεσιών σε ψηφιακές απειλές. Η κυβερνοκατασκοπεία έχει γίνει στρατηγικό εργαλείο για τα έθνη, θολώνοντας τις παραδοσιακές γραμμές μεταξύ πολιτικών και στρατιωτικών στόχων και περιπλέκοντας το τοπίο της εθνικής ασφάλειας, ενώ ο κυβερνοπόλεμος επεκτείνει τον αντίκτυπό του μέσω εκστρατειών παραπληροφόρησης που μπορούν να αποσταθεροποιήσουν τις κυβερνήσεις και να επηρεάσουν τις δημοκρατικές διαδικασίες[17]. Οι οικονομικές επιπτώσεις τέτοιων απειλών είναι βαθιές, με επιθέσεις στα χρηματοπιστωτικά συστήματα να οδηγούν δυνητικά σε διαταραχές του παγκόσμιου εμπορίου και των επενδύσεων. Επιπλέον, η στόχευση στρατιωτικών συστημάτων επικοινωνίας και ελέγχου υπογραμμίζει την περίπλοκη φύση του σύγχρονου πολέμου.

Καθώς αυτές οι απειλές εξελίσσονται, όχι μόνο επιβαρύνουν τις διεθνείς σχέσεις

---

[15] Jens Stoltenberg, NATO Secretary General, NATO's Cyber Defense Pledge Conference, Rome, November 2022.
[16] Research Division NATO Defence College, *Strategic Shifts and NATO's New Strategic Concept*, Rome, σελ. 25
[17] Jason N. Smolanoff, Live from Davos – Cyber in 2023: Geopolitical and Economic Risks, January, 2023

αλλά και αμφισβητούν τα υπάρχοντα νομικά πλαίσια, καθιστώντας μια ενιαία παγκόσμια απάντηση στην επίθεση στον κυβερνοχώρο μια πολύπλοκη αλλά ζωτικής σημασίας προσπάθεια. Σε αυτό το σενάριο, η αναγνώριση και η αντιμετώπιση της πολύπλευρης φύσης των απειλών για την ασφάλεια στον κυβερνοχώρο καθίσταται ζωτικής σημασίας για τη διατήρηση της παγκόσμιας σταθερότητας και τη διασφάλιση των εθνικών συμφερόντων στην ψηφιακή εποχή.

1.2.4.1. Κυβερνοκατασκοπεία (cyber spying)

Η Κυβερνοκατασκοπεία αναφέρεται στη χρήση ψηφιακών τεχνικών και τεχνολογιών για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε εμπιστευτικές πληροφορίες ή πνευματική ιδιοκτησία από άτομα, οργανισμούς ή κυβερνήσεις. Ο πρωταρχικός στόχος της κατασκοπείας στον κυβερνοχώρο είναι η συλλογή ευαίσθητων πληροφοριών, όπως εμπορικά μυστικά, στρατιωτικά σχέδια, πολιτικές στρατηγικές ή άλλα διαβαθμισμένα δεδομένα, για στρατηγικό, οικονομικό, πολιτικό ή στρατιωτικό πλεονέκτημα. Οι δραστηριότητες κατασκοπείας στον κυβερνοχώρο μπορούν να διεξαχθούν τόσο από κρατικές οντότητες, όπως κυβερνήσεις ή μυστικές υπηρεσίες πληροφοριών, όσο και από μη κρατικούς φορείς, όπως εγκληματικές ή τρομοκρατικές οργανώσεις.

Ορισμένα από τα βασικά χαρακτηριστικά της κυβερνοκατασκοπείας[18] συνιστούν τόσο η διενέργεια μυστικών επιχειρήσεων, κατά τις οποίες καταβάλλεται προσπάθεια εκ μέρους των δραστών να παραμείνουν απαρατήρητοι, με ταυτόχρονη πρόσβαση και διείσδυση σε ευαίσθητες πληροφορίες, όσο και η χρήση προηγμένων τεχνικών όπως κακόβουλο λογισμικό, phishing και άλλες μέθοδοι κυβερνοεπιθέσεων, με σκοπό τη διείσδυση σε συστήματα και δίκτυα-στόχους. Μάλιστα, ορισμένες εκστρατείες κατασκοπείας στον κυβερνοχώρο διεξάγονται για εκτεταμένες περιόδους, με τους εισβολείς να διατηρούν επίμονη πρόσβαση σε συστήματα-στόχους προκειμένου να επιτύχουν την διαρκή και αδιάκοπη συλλογή πληροφοριών.

Ο εντοπισμός της πηγής μιας επίθεσης κατασκοπείας στον κυβερνοχώρο κατά κανόνα αποτελεί μια ιδιαίτερα απαιτητική διαδικασία, τόσο σε επίπεδο ειδίκευσης και ικανοτήτων, όσο και σε επίπεδο τεχνολογικών πόρων και ανθρώπινου δυναμικού. Οι επιτιθέμενοι συχνά χρησιμοποιούν διάφορες μεθόδους για να συσκοτίσουν την ταυτότητά τους, καθιστώντας δυσχερέστατο τον προσδιορισμό του ποιος βρίσκεται πίσω από την

[18] Richard Bejtlich, Don't Underestimate Cyber Spies, Foreign Affairs, 2013

κατασκοπεία. Επιπρόσθετα, ένα από τα βασικά χαρακτηριστικά της κυβερνοκατασκοπείας, είναι ο μη περιορισμός της από γεωγραφικά όρια. Οι επιτιθέμενοι μπορούν να δραστηριοποιηθούν από οπουδήποτε στον κόσμο, καθιστώντας πρόκληση για τις στοχευμένες οντότητες να αμυνθούν αποτελεσματικά από τέτοιες απειλές.:

Παρόλα αυτά, το διακύβευμα είναι εξαιρετικά μεγάλο, καθώς οι στόχοι της κυβερνοκατασκοπείας μπορεί να περιλαμβάνουν κυβερνητικές υπηρεσίες, στρατιωτικούς οργανισμούς, αμυντικούς εργολάβους, εταιρείες, ερευνητικά ιδρύματα και άτομα με πρόσβαση σε πολύτιμες πληροφορίες. Καθίσταται κατ΄αυτόν τον τρόπο σαφές ότι η δυνατότητα κακόβουλης πρόσβασης σε άκρως απόρρητες κρατικές πληροφορίες ενδέχεται να οδηγήσει σε γεωπολιτική πανωλεθρία.

1.2.4.2. Κυβερνοπόλεμος (Cyber Warfare)

Παρόμοια με την κατασκοπεία στον κυβερνοχώρο, η απόδοση επιθέσεων στον κυβερνοχώρο σε ένα πλαίσιο κυβερνοπολέμου[19] συνιστά μια επιπρόσθετη πρόκληση ασφαλείας. Ο Κυβερνοπόλεμος, αναφέρεται στη χρήση ψηφιακών μέσων, όπως δίκτυα υπολογιστών, λογισμικό και άλλες τεχνολογίες πληροφοριών και επικοινωνιών, για τη διεξαγωγή πολέμου στην εικονική σφαίρα. Σε αντίθεση με τον παραδοσιακό πόλεμο που περιλαμβάνει φυσικές μάχες και καταστροφή, ο κυβερνοπόλεμος περιλαμβάνει επιθέσεις σε συστήματα υπολογιστών, δίκτυα και υποδομές ενός έθνους με στόχο την πρόκληση διακοπής, βλάβης ή απόκτησης στρατηγικού πλεονεκτήματος.

Μια από τις βασικές πτυχές του κυβερνοπολέμου συνιστά η συχνή διασύνδεση και εμπλοκή κρατών ή κρατικών οντοτήτων, τόσο σε επιθετικές όσο και σε αμυντικές επιχειρήσεις στον κυβερνοχώρο. Οι κυβερνήσεις κατά κανόνα επιδιώκουν την ανάπτυξη εξειδικευμένων στρατιωτικών μονάδων ή την σύμπραξη και συνεργασία με ειδικούς του κυβερνοχώρου αναφορικά με τη διεξαγωγή κυβερνοεπιθέσεων προς επίτευξη στρατηγικών σκοπών.

Οι συνήθεις στόχοι του κυβερνοπολέμου περιλαμβάνουν στρατιωτικά συστήματα, κρίσιμες υποδομές, όπως δίκτυα ηλεκτρικής ενέργειας, δίκτυα μεταφορών και χρηματοοικονομικά συστήματα, κυβερνητικά ιδρύματα και δίκτυα επικοινωνίας, με στόχο

[19] F. Allhoff, A. Henschke, B.J. Strawser, *Binary Bullets: The Ethics of Cyberwarfare*, Oxford University Press, 2016, σελ. 89

τη διατάραξη ή απενεργοποίηση αυτών των συστημάτων προς επίτευξη στρατιωτικού ή γεωπολιτικού πλεονεκτήματος. Παραταύτα, ο κυβερνοπόλεμος μπορεί να οδηγήσει και σε πλήξη παράπλευρων συστημάτων, επηρεάζοντας ούτως όχι μόνο στρατιωτικούς ή κυβερνητικούς στόχους αλλά και μη στρατιωτικές υποδομές ζωτικής σημασίας, οι οποίες δύνανται να επιφέρουν εκτεταμένες συνέπειες για τον γενικό πληθυσμό.

1.3. Κυβερνοασφάλεια (Cybersecurity)

Στον αντίποδα των ανωτέρω, οι διάφοροι ιδιωτικοί και δημόσιοι φορείς, συμπεριλαμβανομένων και των ίδιων των κρατών, επιδιώκουν να προστατευτούν από κακόβουλα πλήγματα μέσω της ανάπτυξης πολιτικών ασφαλείας. Στο σημείο αυτό εισάγεται η έννοια της κυβερνοασφάλειας (Cybersecurity)[20] η οποία αναφέρεται αμιγώς στην ανάπτυξη πρακτικών προστασίας συστημάτων υπολογιστών, δικτύων και δεδομένων από κλοπή, ζημιά ή μη εξουσιοδοτημένη πρόσβαση. Περιλαμβάνει διάφορα μέτρα, τεχνολογίες και διαδικασίες για την προστασία των περιουσιακών στοιχείων της τεχνολογίας των πληροφοριών και την πρόληψη των απειλών στον κυβερνοχώρο.

Ως καίρια σημεία της χαρακτηρίζονται, μεταξύ άλλων, η ασφάλεια δικτύων, η ασφάλεια τελικού σημείου και εφαρμογών, η προστασία δεδομένων, η διαχείριση ταυτότητας και πρόσβασης, και η διαχείριση ευπάθειας και συμμόρφωση σε μοντέλα ασφάλειας.

---

[20] Στον τομέα της ψηφιακής ασφάλειας, χρησιμοποιούνται συχνά οι όροι «κυβερνοασφάλεια (cybersecurity)» και «κυβερνοάμυνα (cyberdefense)», ο καθένας εκ των οποίων έχει ξεχωριστή εστίαση και εμβέλεια. Η κυβερνοασφάλεια είναι η ευρύτερη έννοια, η οποία περιλαμβάνει ένα σύνολο μέτρων και πρακτικών που έχουν σχεδιαστεί για την προστασία συστημάτων υπολογιστών, δικτύων και δεδομένων από μη εξουσιοδοτημένη πρόσβαση, κλοπή ή ζημιά. Δίνει έμφαση στη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των ψηφιακών πληροφοριών, χρησιμοποιώντας εργαλεία όπως λογισμικό προστασίας από ιούς, τείχη προστασίας, κρυπτογράφηση και εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια.Από την άλλη πλευρά, η κυβερνοάμυνα είναι ένα υποσύνολο της κυβερνοασφάλειας με πιο στρατηγικό προσανατολισμό. Αναφέρεται συγκεκριμένα στις ολοκληρωμένες στρατηγικές και δραστηριότητες που αναλαμβάνονται για την προστασία ενός έθνους, ενός οργανισμού ή ενός δικτύου από απειλές στον κυβερνοχώρο. Ενώ η κυβερνοασφάλεια αφορά την προστασία των ψηφιακών πληροφοριών, η κυβερνοάμυνα εκτείνεται πέρα από αυτό και περιλαμβάνει προληπτικά μέτρα που στοχεύουν στην αποτροπή, τον εντοπισμό, την απόκριση και την ανάκαμψη από επιθέσεις στον κυβερνοχώρο. Ουσιαστικά, η κυβερνοασφάλεια αποτελεί το θεμελιώδες στρώμα προστασίας, που ασχολείται με τη διαφύλαξη των ψηφιακών περιουσιακών στοιχείων σε πιο αναλυτικό επίπεδο. Η κυβερνοάμυνα, ωστόσο, είναι μια ευρύτερη και πιο περιεκτική έννοια που ενσωματώνει μέτρα κυβερνοασφάλειας αλλά επεκτείνεται περαιτέρω στον στρατηγικό σχεδιασμό και την εκτέλεση ολοκληρωμένων στρατηγικών ασφάλειας. Περιλαμβάνει πτυχές όπως η ανάπτυξη πολιτικής, ο σχεδιασμός αντιμετώπισης περιστατικών, οι πληροφορίες για τις απειλές και η συνεργασία με τις αρχές επιβολής του νόμου και διεθνείς εταίρους. Μαζί, η κυβερνοασφάλεια και η κυβερνοάμυνα διαδραματίζουν κρίσιμους ρόλους στη διατήρηση της ανθεκτικότητας και της ασφάλειας των ψηφιακών περιβαλλόντων σε έναν όλο και πιο διασυνδεδεμένο κόσμο.

2. Ευρω-Ενωσιακό Κανονιστικό Πλαίσιο

2.1. Η κανονιστική διαδρομή της Ένωσης στο ζήτημα νομοθέτησης για την ασφάλεια στον Κυβερνοχώρο - μια συνοπτική αναδρομή ρυθμίσεων

Η Ευρωπαϊκή Ένωση φαίνεται να έχει αντιληφθεί τους κινδύνους που ελλοχεύει η διείσδυση των ψηφιακών δικτύων στις διάφορες πτυχές της καθημερινότητας. Επίσημα, ξεκίνησε να ασχολείται με το ζήτημα της κυβερνοασφάλειας μόλις το 2000, ενώ το 2002 εξέδωσε μια σειρά οδηγιών, με την 2002/21/ΕΚ να αναδεικνύεται ως η σημαντικότερη από αυτές, καθώς αναφερόταν σε ένα κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, καθορίζοντας τα καθήκοντα των εθνικών ρυθμιστικών αρχών, μεταξύ των οποίων περιλαμβάνονταν η αμοιβαία συνεργασία και η συνεργασία με την Επιτροπή με διαφανή τρόπο, προκειμένου να διασφαλιστεί η ανάπτυξη συνεκτικής ρυθμιστικής πρακτικής, η συμβολή στη διασφάλιση υψηλού επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής, καθώς και η κατοχύρωση της ακεραιότητας και της ασφάλειας των δικτύων δημοσίων επικοινωνιών.

Ωστόσο, η πρώτη ουσιαστική εξέλιξη στο σχεδιασμό στρατηγικής για την προστασία από τους κινδύνους του Κυβερνοχώρου, επήλθε με τον Κανονισμό 460/2004. Με τον εν λόγω κανονισμό, ιδρύθηκε ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), αντικείμενο του οποίου ήταν η ενίσχυση της ανάπτυξης των εθνικών στρατηγικών κυβερνοασφάλειας, και η παροχή συμβουλευτικής και λύσεων, προκειμένου τα κράτη να βελτιώσουν την αμυντική δυναμική τους έναντι των κινδύνων, αλλά και η εφαρμογή της πολιτικής και του νομικού πλαισίου της Ένωσης σε θέματα ασφάλειας δικτύου και πληροφοριών.

Το 2006 η Επιτροπή εξέδωσε την COM(2006)251 Στρατηγική για ασφαλή κοινωνία της πληροφορίας, ενώ από το 2009 και μετά, έχει επίσης εκδώσει ένα σχέδιο δράσης και μια ανακοίνωση σχετικά με την προστασία υποδομών πληροφοριών ζωτικής σημασίας (COM(2009)149, που εγκρίθηκε με το ψήφισμα του Συμβουλίου 2009/C 321/01 και COM(2011)163, το οποίο ενέκρινε το Συμβούλιο με τα συμπεράσματά του (10299/11).

Το 2016 ο εκδόθηκε ο κανονισμός 2016/679[21], με αντικείμενο την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και

[21] Νόμος 4624/2019 (ΦΕΚ Α' 137/ 29.8.2019)

για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Ο εν λόγω κανονισμός επικεντρώθηκε στο ζήτημα της προστασίας από την αθέμιτη επεξεργασία προσωπικών δεδομένων, θέτοντας προϋποθέσεις και αναδεικνύοντας την έννοια της συγκατάθεσης των προσώπων στην επεξεργασία των δεδομένων τους, αναγκαία προϋπόθεση της οποίας συνιστά η διαφανής ενημέρωση του υποκειμένου των δεδομένων για την άσκηση των δικαιωμάτων του. Παράλληλα ο εν λόγω κανονισμός όριζε ότι όλα τα κράτη μέλη όφειλαν να διασφαλίζουν την παρακολούθηση της εφαρμογής του μέσω της λειτουργίας ανεξάρτητων δημοσίων αρχών. Οι εποπτικές αυτές αρχές είχαν μεταξύ άλλων την εξουσία επιβολής διοικητικών προστίμων για παραβάσεις συγκεκριμένων διατάξεων του.

Το ίδιο έτος, μια πιο σχετική με το ζήτημα της κυβερνοασφάλειας ρύθμιση, η οδηγία (ΕΕ) 2016/1148[22][23], έθεσε τα θεμέλια για την ανάπτυξη ικανοτήτων κυβερνοασφάλειας σε ολόκληρη την Ένωση, αποσκοπώντας ούτως στον μετριασμό των κινδύνων που απειλούσαν συστήματα δικτύου και πληροφοριών, καθώς και στη διασφάλιση της συνέχειας των υπηρεσιών αυτών κατά την αντιμετώπιση περιστατικών. Η ανωτέρω οδηγία συνέβαλε σε σημαντικό βαθμό στην αύξηση του επιπέδου κυβερνοανθεκτικότητας της Ένωσης. Η επανεξέταση της εν λόγω οδηγίας[24] οδήγησε στο συμπέρασμα ότι αυτή *"λειτούργησε ως καταλύτης για τη θεσμική και κανονιστική προσέγγιση της κυβερνοασφάλειας στην Ένωση καθώς προετοίμασε το έδαφος για μια σημαντική αλλαγή νοοτροπίας. Με την οδηγία διασφαλίστηκε η ολοκλήρωση των εθνικών πλαισίων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών με τη θέσπιση εθνικών στρατηγικών για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, τη θέσπιση εθνικών ικανοτήτων και με την εφαρμογή ρυθμιστικών μέτρων τα οποία καλύπτουν βασικές υποδομές και οντότητες που προσδιορίζονται από κάθε κράτος μέλος. Η οδηγία (ΕΕ) 2016/1148 συνέβαλε επίσης στη συνεργασία σε επίπεδο Ένωσης μέσω της σύστασης της ομάδας συνεργασίας και του δικτύου εθνικών ομάδων αντιμετώπισης περιστατικών ασφάλειας υπολογιστών*".

Σήμερα, ακρογωνιαίο λίθο του ευρω-ενωσιακού κανονιστικού πλαισίου αναφορικά με το ζήτημα της κυβερνοασφάλειας συνιστά ο κανονισμός 881/2019, ο οποίος ρυθμίζει τα

[22] Ενσωμάτωση με Ν. 4577/2018 (ΦΕΚ Α' 199/03.12.2018)
[23] Αντικαταστάθηκε από την οδηγία 2555/2022
[24] Βλ. σκέψη 2 αιτιολογικής έκθεσης οδηγίας 2555/2022 (απόσπασμα)

σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) ζητήματα, ενώ ορίζει κατευθυντήριες γραμμές αφορώσες την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών.

2.2. Ο Κανονισμός 881/2019 (Cybersecurity Act)

Η σταδιακή αύξηση της εξάρτησης από τον ψηφιακό παράγοντα σε συνδυασμό με την κυριάρχηση ενός ολοένα και πιο σύνθετου τοπίου κυβερνοαπειλών, οδήγησε αναπόφευκτα στην αναγκαιότητα σχεδίασης μιας ενιαίας και ισχυρής ενωσιακής προσέγγισης κυβερνοασφάλειας, την ενσάρκωση της οποίας αποτέλεσε ο Κανονισμός 881/2019, που έμεινε γνωστός ως Cybersecurity Act. Αν και Cybersecurity Ac ψηφίστηκε μερικούς μήνες πριν την έκρηξη της πανδημίας, χρονικό σημείο κατά το οποίο εκτοξεύτηκε ο παράγοντας ψηφιοποίησης σε τομείς όπως η εκπαίδευση, η εργασία αλλά και η δημόσια διοίκηση, αναδεικνύοντας ούτως τους ήδη αυξημένους κινδύνους που αντιμετώπιζε η Ένωση στον τομέα της κυβερνοασφάλειας, στόχος του εν λόγω κανονισμού ήταν ακριβώς η ενίσχυση της ασφάλειας για τον Κυβερνοχώρο μέσω της πιστοποίησης για την κυβερνοασφάλεια στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και την αναδιάρθρωση του «Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια» (ENISA).

Σύμφωνα με την αιτιολογική έκθεση του κανονισμού, ο τελευταίος επιδιώκει να θέσει μια σειρά μέτρων βασιζόμενων σε προηγμένες δράσεις της Ένωσης, μέσω των οποίων θα ευνοούνται ορισμένοι αλληλοενισχυόμενοι στόχοι, μεταξύ των οποίων η αύξηση των ικανοτήτων αντιμετώπισης και ετοιμότητας των κρατών μελών, καθώς και των επιχειρήσεων, αλλά και η σημασία της διατήρησης και περαιτέρω ενίσχυσης των εθνικών ικανοτήτων αντιμετώπισης κινδύνων από κυβερνοαπειλές μικρής ή μεγάλης κλίμακας. Άλλο σημαντικό ζήτημα που συμπεριλαμβάνεται στους στόχους που επιδιώκει να ενισχύσει ο κανονισμός συνιστά η βελτίωση της συνεργασίας, της ανταλλαγής πληροφοριών και του συντονισμού στα κράτη μέλη και στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης[25].

Μια ακόμα παλέτα στόχων που θέτει ο εν λόγω κανονισμός, αφορά στην αύξηση της ευαισθητοποίησης των πολιτών, των οργανισμών και των επιχειρήσεων σε ζητήματα κυβερνοασφάλειας, τονίζοντας ότι: «*Η κυβερνοασφάλεια δεν είναι μόνο ζήτημα τεχνολογίας, αλλά ζήτημα όπου σημαντικό ρόλο κατέχει η ανθρώπινη συμπεριφορά*». Έτσι,

[25] βλ. Σκέψη 6 της αιτιολογικής έκθεσης του Κανονισμού 881/2019

εισάγεται στο σημείο αυτό[26] η έννοια της «κυβερνοϋγιεινής», η οποία αφορά στην τακτική εφαρμογή απλών, προστατευτικών μέτρων από τους χρήστες, είτε αυτοί είναι πολίτες, οργανισμοί ή επιχειρήσεις, τα οποία θα έχουν στόχο την πρόληψη έκθεσης σε κινδύνους από κυβερνοαπειλές.

Ωστόσο, την ευθύνη για την ασφάλεια στον κυβερνοχώρο δεν δύνανται να φέρουν μόνο οι χρήστες. Ο κανονισμός λαμβάνει υπόψη τον ζωτικό ρόλο τον φορέων διαμόρφωσης Οι επιχειρήσεις, οι οργανισμοί και ο δημόσιος τομέας θα πρέπει να διαμορφώνουν τα προϊόντα, τις υπηρεσίες και τις διαδικασίες Τεχνολογιών Πληροφορικής & Επικοινωνιών (ΤΠΕ)[27] που σχεδιάζουν κατά τρόπο που να διασφαλίζει υψηλότερο επίπεδο ασφάλειας, προκειμένου να μειώνεται η επιβάρυνση των χρηστών με την ανάγκη εξειδικευμένης ρύθμισης για την επίτευξη του βέλτιστου επιπέδου ασφαλείας.

Βασικούς πυλώνες του Cybersecurity Act αποτέλεσαν η ενίσχυση του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), η καθιέρωση ενός ολοκληρωμένου πλαισίου πιστοποίησης κυβερνοασφάλειας σε ενωσιακό επίπεδο, η εναρμόνιση των προτύπων κυβερνοασφάλειας των κρατών μελών, η οικοδόμηση της εμπιστοσύνης των πολιτών στην ψηφιακή αγορά και η ενίσχυση του ανταγωνιστικού πλεονεκτήματος των επιχειρήσεων της Ευρωπαϊκής Ένωσης στην παγκόσμια αγορά.

2.2.1. Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA)

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, (εφεξής αναφερόμενος ως ENISA) είναι ο οργανισμός της Ένωσης που έχει ως αντικείμενο την διασφάλιση υψηλού και αποτελεσματικού επιπέδου ασφάλειας των δικτύων και των πληροφοριών εντός του πλαισίου της Ένωσης, καθώς και την επίτευξη στόχων με σκοπό την ανάπτυξη και ενίσχυση μιας αντίληψης για την ασφάλεια των δικτύων και των πληροφοριών προς όφελος των πολιτών, των καταναλωτών, των επιχειρήσεων και των οργανισμών του δημόσιου τομέα. Ιδρύθηκε το 2004 με τον κανονισμό 460/2004, αρχικά για περιορισμένο χρονικό διάστημα, με στόχο να λάβει χώρα αξιολόγηση του έργου του και βάσει αυτής να

[26] Βλ. Σκέψη 8 της αιτιολογικής έκθεσης του Κανονισμού 881/2019

[27] (Information and communication technologies - ICT): ένα ποικίλο σύνολο τεχνολογικών εργαλείων και πόρων που χρησιμοποιούνται για τη μετάδοση, αποθήκευση, δημιουργία, κοινή χρήση ή ανταλλαγή πληροφοριών. Αυτά τα τεχνολογικά εργαλεία και πόροι περιλαμβάνουν υπολογιστές, το Διαδίκτυο (ιστοσελίδες, ιστολόγια και email), τεχνολογίες ζωντανής μετάδοσης (ραδιόφωνο, τηλεόραση και μετάδοση μέσω web), τεχνολογίες ηχογραφημένης μετάδοσης (podcasting, συσκευές αναπαραγωγής ήχου και βίντεο και συσκευές αποθήκευσης) και τηλεφωνία (σταθερή ή κινητή, δορυφόρος, visio/video-conferencing, κ.λπ.).

καθοριστεί εάν θα πρέπει να παραταθεί η διάρκεια λειτουργίας του.Έκτοτε, η θητεία του παρατάθηκε μέσα από μια σειρά έκδοσης διαδοχικών Κανονισμών[28], μέχρι το 2019 που έγινε μόνιμο στοιχείο στο τοπίο της ασφάλειας του κυβερνοχώρου της Ένωσης με τον Cybersecurity Act.

2.2.1.1. Ο ENISA πριν τον Cybersecurity Act

Καθώς η ταχύτητα της τεχνολογικής εξέλιξης και η περιπλοκότητα του αντικειμένου δεν επέτρεπαν στην Επιτροπή και τα κράτη μέλη, μεμονωμένα, να παρακολουθούν τα πρότυπα κατά τις απαιτήσεις της κοινοτικής νομοθεσίας, δημιουργήθηκε με τον κανονισμό 460/2004 ένας Οργανισμός, ο ENISA, ώστε να παρακολουθεί τα τεχνικά πρότυπα των διεθνών οργανισμών, καθώς επίσης και τα de facto πρότυπα που εκπονούνταν σε παγκόσμιο επίπεδο και χρησιμοποιούνταν από τα κράτη μέλη. Παράλληλα, Ο ENISA, ήταν θεσμικά ανεξάρτητος, ενώ είχε υποχρέωση σε ανεξάρτητη έκφραση των συμπερασμάτων, προσανατολισμών και συμβουλών του σχετικά με θέματα που άπτονταν της εμβέλειας και των στόχων του. Το πλαίσιο λειτουργίας του καθοριζόταν αποκλειστικά με σημείο εκκίνησης τις εθνικές και κοινοτικές προσπάθειες, καθιστώντας ούτως απαραίτητη την στενή συνεργασία του με τα κράτη μέλη, ενώ με δεδομένο το ότι τα ηλεκτρονικά δίκτυα ανήκουν, σε μεγάλο βαθμό, σε ιδιωτικά συμφέροντα,ήταν απαραίτητη και η συνεργασία του με τον ιδιωτικό τομέα.

Αξίζει να σημειωθεί ότι ο ENISA δεν είχε παρεμβατικό ή ιδιαίτερα αποφασιστικό χαρακτήρα, καθώς όφειλε να θέτει στόχους και να ασκεί τα καθήκοντά του χωρίς να παρεμβαίνει στις αρμοδιότητες των εθνικών ρυθμιστικών αρχών[29], των ευρωπαϊκών οργανισμών τυποποίησης και της μόνιμης επιτροπής που συστάθηκε με την οδηγία 98/34/ΕΚ[30], καθώς και των εποπτικών αρχών των κρατών μελών που είχαν ως αντικείμενο την προστασία των ατόμων όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ελεύθερη διακίνηση των δεδομένων αυτών. Σε κάθε περίπτωση, η

[28] Ο κανονισμός 1007/2008 παρέτεινε τη θητεία του ENISA έως τον Μάρτιο του 2012. Ο κανονισμός 580/2011 παρέτεινε περαιτέρω τη θητεία του ENISA έως τις 13 Σεπτεμβρίου 2013. Τέλος ο κανονισμός 526/2013 παρέτεινε τη θητεία του ENISA έως τις 19 Ιουνίου 2020.

[29] Όπως αυτές ορίζονταν στις οδηγίες που αφορούσαν τα δίκτυα και τις υπηρεσίες ηλεκτρονικών επικοινωνιών, καθώς και στην ομάδα των ευρωπαϊκών ρυθμιστικών αρχών για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, που είχαν συσταθεί με την απόφαση 2002/627/ΕΚ της Επιτροπής και στην επιτροπή επικοινωνιών που αναφερόταν στην οδηγία 2002/21/ΕΚ.

[30] Η μόνιμη Επιτροπή της οδηγίας 98/34/ΕΚ είχε ως αντικείμενο την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών

στοχοθεσία και λειτουργία του δεν έπρεπε να θίγουν δραστηριότητες εμπίπτουσες στους τομείς της δημόσιας ασφάλειας, της εθνικής άμυνας, της ασφάλειας του κράτους, της οικονομικής ευημερίας του κράτους, καθώς και τις κρατικές δραστηριότητες στον τομέα του ποινικού δικαίου.

Ήδη από την αρχική μορφή του ο ENISA είχε ως στόχο την ενίσχυση της ικανότητας της Ένωσης και των κρατών μελών να προλαμβάνουν, να αντιμετωπίζουν και να ανταποκρίνονται στα προβλήματα ασφάλειας δικτύων και πληροφοριών. Για το σκοπό αυτό, ο ENISA παρείχε συνδρομή και συμβουλές στην Επιτροπή και στα κράτη μέλη αναφορικά με ζητήματα αφορώντα στην ασφάλεια δικτύων και πληροφοριών, ενώ όφειλε, μέσω των ειδικών γνώσεων που διέθετε, να προωθεί την ευρεία συνεργασία μεταξύ παραγόντων του δημόσιου και του ιδιωτικού τομέα. Ακόμα, όταν του ζητείτο, συνέδραμε την Επιτροπή, στις τεχνικές προπαρασκευαστικές εργασίες ενημέρωσης και ανάπτυξης της κοινοτικής νομοθεσίας στον τομέα της ασφάλειας δικτύων και πληροφοριών.

Ήδη από την ίδρυση του ENISA, κεντρικό άξονα των καθηκόντων του αποτέλεσε η ανάλυση υφιστάμενων και μελλοντικών κινδύνων που αφορούσαν την κυβερνοασφάλεια. Συγκεκριμένα, στα πλαίσια των αρμοδιοτήτων του, συνέλεγε πληροφορίες για την ανάλυση των υφιστάμενων, μελλοντικών και άμεσων κινδύνων, και ιδιαίτερα κινδύνων οι οποίοι θα μπορούσαν να έχουν επιπτώσεις στην ανθεκτικότητα και τη διαθεσιμότητα των δικτύων ηλεκτρονικών επικοινωνιών, καθώς και στην αυθεντικότητα, ακεραιότητα και εμπιστευτικότητα των πληροφοριών, οι οποίες είναι προσβάσιμες ή μεταφέρονται μέσω των εν λόγω δικτύων, και διαβίβαση των αποτελεσμάτων της ανάλυσης στα κράτη μέλη και την Επιτροπή. Στο πλαίσιο αυτό, ο ENISA παρείχε συμβουλές και συνδρομή στο Ευρωπαϊκό Κοινοβούλιο, σε ευρωπαϊκούς φορείς ή σε αρμόδιους εθνικούς φορείς που όριζαν τα κράτη μέλη, μόνο όταν του το ζητούσαν, χωρίς όμως να δύναται να προβαίνει σε επιβολή επιπρόσθετων υποχρεώσεων στον ιδιωτικό τομέα ή στα κράτη μέλη. Στα πλαίσια των καθηκόντων του, ο Οργανισμός προωθούσε δραστηριότητες εκτίμησης κινδύνων, διαλειτουργικών λύσεων διαχείρισης κινδύνων και μελετών σχετικά με λύσεις διαχείρισης της πρόληψης εντός των οργανισμών τόσο του δημόσιου, όσο και του ιδιωτικού τομέα.

Κεντρικό άξονα των καθηκόντων του ENISA αποτέλεσε επίσης η ενίσχυση της συνεργασίας μεταξύ των διαφόρων παραγόντων που δραστηριοποιούνταν στον τομέα της ασφάλειας δικτύων και πληροφοριών, μεταξύ άλλων με τη διοργάνωση τακτικών

διαβουλεύσεων με τη βιομηχανία, τα πανεπιστήμια και άλλους συναφείς κλάδους, ενώ έγιναν προσπάθειες δόμησης δικτύου επικοινωνίας για κοινοτικούς φορείς, φορείς του δημόσιου τομέα που είχαν ορίσει τα κράτη μέλη, φορείς του ιδιωτικού τομέα και οργανώσεις καταναλωτών. Παράλληλα επιχειρήθηκε διευκόλυνση της συνεργασίας μεταξύ της Επιτροπής και των κρατών μελών αναφορικά με την ανάπτυξη κοινών μεθοδολογιών πρόληψης, αντιμετώπισης και ανταπόκρισης σε ζητήματα ασφάλειας δικτύων και πληροφοριών, με τον ίδιο τον ENSIA να παράσχει συνδρομή κατά τη διεξαγωγή του διαλόγου τους. Με δεδομένο δε ότι οι απειλές κατά της ασφάλειας στον Κυβερνοχώρο δεν γνωρίζουν σύνορα, ο ENISA απολάμβανε σημαίνοντα ρόλο στις κοινοτικές προσπάθειες για ανάπτυξη συνεργασίας με τρίτες χώρες και, κατά περίπτωση, με διεθνείς οργανισμούς, με στόχο την προώθηση μιας κοινής, σφαιρικής προσέγγισης σε θέματα ασφάλειας δικτύων και πληροφοριών.

Για την αποτελεσματική εκτέλεση των καθηκόντων του, ήτοι την ανάλυση υφιστάμενων και μελλοντικών κινδύνων, την ενίσχυση της συνεργασίας μεταξύ των διαφόρων παραγόντων που δραστηριοποιούνταν στον τομέα της ασφάλειας δικτύων και πληροφοριών και την παροχή συμβουλών στην Επιτροπή και στα κράτη μέλη όταν αυτό του ζητούνταν, ο ENSIA όφειλε να λαμβάνει έγκαιρη, αντικειμενική και συγκεντρωτική πληροφόρηση αναφορικά με ζητήματα ασφάλειας δικτύων και πληροφοριών για όλους τους χρήστες. Προς εκπλήρωση των καθηκόντων πληροφόρησης που του είχαν ανατεθεί, ο εν λόγω οργανισμός όφειλε να παρακολουθεί την εξέλιξη των προτύπων για προϊόντα και υπηρεσίες σε ότι αφορούσε την ασφάλεια των δικτύων και των πληροφοριών.

Σύμφωνα με τον κανονισμό 460/2004 τα θεσμικά όργανα του ENISA αποτελούνταν από το διοικητικό συμβούλιο, τον εκτελεστικό διευθυντή και τη μόνιμη ομάδα ενδιαφερομένων. Το πλαίσιο σύστασης και λειτουργίας τους εξασφάλιζε τη θεσμική ανεξαρτησία του Οργανισμού.

Το διοικητικό συμβούλιο αποτελούνταν από έναν εκπρόσωπο προερχόμενο από κάθε κράτος μέλος, τρεις εκπροσώπους που διορίζονταν από την Επιτροπή, καθώς και τρεις εκπροσώπους που προτείνονταν από την Επιτροπή και διορίζονταν από το Συμβούλιο, χωρίς δικαίωμα ψήφου, καθένας από τους οποίους προερχόταν από τον βιομηχανικό κλάδο των τεχνολογιών, των πληροφοριών και των επικοινωνιών, από ενώσεις καταναλωτών, καθώς και πανεπιστημιακούς εμπειρογνώμονες σε θέματα ασφάλειας δικτύων και πληροφοριών.

Τα μέλη του διοικητικού συμβουλίου διορίζονταν με βάση το βαθμό της πείρας και της εξειδίκευσής τους στον τομέα της ασφάλειας δικτύων και πληροφοριών και εξέλεγαν, από τα μέλη του, τον πρόεδρο και τον αναπληρωτή. Η θητεία τους ήταν για δυόμισι έτη και μπορούσε να ανανεωθεί. Στα πλαίσια των αρμοδιοτήτων του διοικητικού συμβουλίου ενέπιπταν η έγκριση του εσωτερικού του κανονισμού και εσωτερικών κανόνων λειτουργίας κατόπιν πρότασης της Επιτροπής, οι οποίοι στη συνέχεια δημοσιοποιούνταν. Οι αποφάσεις του λαμβάνονταν με την πλειοψηφία των μελών του που διέθεταν δικαίωμα ψήφου, εκτός αν για ορισμένο ζήτημα προβλεπόταν ειδική διάταξη[31].

Ο Οργανισμός διοικείτο από τον εκτελεστικό του διευθυντή, ο οποίος κατά την άσκηση των καθηκόντων του απολάμβανε ανεξαρτησίας και διορίζετο για 5 έτη από το διοικητικό συμβούλιο, βάσει καταλόγου υποψηφίων που πρότεινε η Επιτροπή, μετά από την διενέργεια γενικού διαγωνισμού, και δημοσίευση της πρόσκλησης για εκδήλωση ενδιαφέροντος στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Η επιλογή του προσώπου του εκτελεστικού διευθυντή λάμβανε χώρα επί τη βάσει των προσόντων του, τις διοικητικές και διαχειριστικές του ικανότητες, καθώς και την επάρκεια και πείρα του στον τομέα της ασφάλειας δικτύων και πληροφοριών. Το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο είχαν τη δυνατότητα να ζητούν οποτεδήποτε ακρόαση με τον εκτελεστικό διευθυντή για οποιοδήποτε θέμα αφορούσε τις δραστηριότητες του Οργανισμού. Τον εκτελεστικό διευθυντή μπορούσε να παύσει από τα καθήκοντά του μόνο το διοικητικό συμβούλιο του ENISA. Στα καθήκοντα του εκτελεστικού διευθυντή περιλαμβάνονταν, μεταξύ άλλων, η καθημερινή διοίκηση του ENISA και η εκπόνηση προτάσεων για τα προγράμματα εργασίας του, η εκτέλεση των προγραμμάτων εργασίας και των αποφάσεων που είχαν εγκριθεί από το διοικητικό συμβούλιο, η διασφάλιση ότι ο οργανισμός ασκούσε τα καθήκοντά του σύμφωνα με τις απαιτήσεις εκείνων που χρησιμοποιούσαν τις υπηρεσίες του, η κατάρτιση σχεδίου κατάστασης προβλεπόμενων εσόδων και δαπανών του Οργανισμού και η εκτέλεση του προϋπολογισμού του, η ανάπτυξη και διατήρηση επαφών τόσο με το Ευρωπαϊκό Κοινοβούλιο και τις σχετικές επιτροπές, όσο και με την επιχειρηματική κοινότητα και τις ενώσεις των καταναλωτών, ενώ προέδρευε και της μόνιμης επιτροπής ενδιαφερομένων. Σε

[31] Παραδείγματα περιπτώσεων όπου απαιτείτο πλειοψηφία δύο τρίτων όλων των μελών που διέθεταν δικαίωμα ψήφου συνιστούσαν η έγκριση του εσωτερικού κανονισμού του Δοικητικού Συμβουλίου, των εσωτερικών κανόνων λειτουργίας του Οργανισμού, του προϋπολογισμού, του ετήσιου προγράμματος εργασιών, καθώς και ο διορισμός και η παύση του εκτελεστικού διευθυντή.

ετήσια βάση υπέβαλλε στο διοικητικό συμβούλιο προς έγκριση το σχέδιο γενικής έκθεσης[32] η οποία κάλυπτε όλες τις δραστηριότητες του Οργανισμού κατά το προηγούμενο έτος, και το σχέδιο προγράμματος εργασίας[33]. Είχε δε τη δυνατότητα σύστασης, ad hoc ομάδων εργασίας απαρτιζόμενες από εμπειρογνώμονες[34], με σκοπό την ενασχόληση ιδίως με τεχνικά και επιστημονικά ζητήματα.

Το τρίτο όργανο του ENISA, η Μόνιμη Ομάδα Ενδιαφερομένων, συγκροτούνταν από τον εκτελεστικό διευθυντή, ο οποίος και προέδρευε. Απαρτίζονταν από εμπειρογνώμονες που εκπροσωπούσαν ενδιαφερόμενους, όπως τον βιομηχανικό κλάδο των τεχνολογιών, των πληροφοριών και των επικοινωνιών, ενώσεις καταναλωτών, και πανεπιστημιακούς εμπειρογνώμονες σε θέματα ασφάλειας δικτύων και πληροφοριών. Τα διαδικαστικά ζητήματα αναφορικά με τη λειτουργία της Μόνιμης Ομάδας Ενδιαφερομένων, καθορίζονταν από τους εσωτερικούς κανόνες λειτουργίας του Οργανισμού, οι οποίοι ήταν δημοσιοποιημένοι. Στα πλαίσια άσκησης των καθηκόντων της, η Μόνιμη Ομάδα Ενδιαφερομένων, συμβούλευε τον εκτελεστικό διευθυντή κατά την άσκηση των καθηκόντων του.

Οι αιτήσεις για παροχή συμβουλών και συνδρομής που εμπίπτουν στην εμβέλεια, τους στόχους και τα καθήκοντα του Οργανισμού απευθύνονται στον εκτελεστικό διευθυντή και συνοδεύονται από τεκμηρίωση με την οποία επεξηγείται το θέμα περί του οποίου πρόκειται. Ο εκτελεστικός διευθυντής ενημερώνει την Επιτροπή σχετικά με τις αιτήσεις που παραλαμβάνει, ενώ ο Οργανισμός δύναται να αρνηθεί την παροχή συμβουλών μόνο με σχετική αιτιολόγηση. Αιτήσεις για παροχή συμβουλών και συνδρομής είχαν τη δυνατότητα να υποβάλλουν το Ευρωπαϊκό Κοινοβούλιο, η Επιτροπή, καθώς και συγκεκριμένοι φορείς που ορίζονταν από τα κράτη μέλη.

Ήδη από τη γέννηση του ENISA, κατέστη σαφές ότι η ορθή και απρόσκοπτη λειτουργία του, θα συνιστούσε σε μεγάλο βαθμό συνάρτηση των σχέσεων εμπιστοσύνης που θα ανέπτυσσε τόσο με δημόσιους όσο και με ιδιωτικούς φορείς. Για το λόγο αυτό

---

[32] Κατόπιν έγκρισης του διοικητικού συμβουλίου, διαβίβαζε τη γενική έκθεση του Οργανισμού στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Επιτροπή, το Ελεγκτικό Συνέδριο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, και την δημοσίευε.

[33] Ο εκτελεστικός διευθυντής, έπειτα από έγκριση του διοικητικού συμβουλίου, διαβίβαζε το πρόγραμμα εργασίας στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Επιτροπή και τα κράτη μέλη, και το δημοσίευε.

[34] Τα μέλη του διοικητικού συμβουλίου συμμετείχαν στις ad hoc ομάδες εργασίας. Εκπρόσωποι της Επιτροπής δικαιούνται να παρίστανται στις συνεδριάσεις τους.

απολάμβανε θεσμικής ανεξαρτησίας, ενώ διέπονταν από καθεστώς διαφάνειας. Προκειμένου να ενισχυθεί το στοιχείο της διαφάνειας και να εξασφαλιστεί η ανεξάρτητη λειτουργία του Οργανισμού, τηρούνταν ορισμένες διατυπώσεις. Μια από τις εν λόγω διατυπώσεις αφορούσε στην υποχρέωση, εκ μέρους του εκτελεστικού διευθυντή και των υπαλλήλων που αποσπώνταν προσωρινά από τα κράτη μέλη, υποβολής γραπτών δηλώσεων[35], στις οποίες να γνωστοποιείται ότι δεν εξυπηρετούν οιαδήποτε άμεσα ή έμμεσα συμφέροντα, δυνάμενα να επηρεάσουν την ανεξαρτησία τους. Αντίστοιχη, προφορική όμως, δήλωση έκαναν και οι εξωτερικοί εμπειρογνώμονες που συμμετείχαν σε ad hoc ομάδες εργασίας, κατά την έναρξη κάθε συνεδρίασης. Παράλληλα, στην ενίσχυση του επιπέδου διαφάνειας του οργανισμού συνέβαλε η παροχή στο κοινό πληροφοριών αναφορικά με τα αποτελέσματα των εργασιών του.

2.2.1.2. Ο ENISA μετά τον Cybersecurity Act

Στα 15 περίπου έτη λειτουργίας του ENISA από τη στιγμή της δημιουργίας του μέχρι την έναρξη λειτουργίας του Cybersecurity Act (Κανονισμός 881/2019), ο ρόλος του ENISA διαφοροποιήθηκε έντονα. Η αλλαγή αυτή εκφράζεται μέσα από την διαφοροποίηση της θεσμικής υπόστασης του ENISA, από έναν οργανισμό που ιδρύθηκε δοκιμαστικά και η ύπαρξη του οποίου απαιτούσε την ανανέωση λειτουργίας του για ορισμένο χρονικό διάστημα, σε μόνιμο οργανισμό με αυξημένους πόρους και ευρύτερη εντολή. Ο νέος ρόλος που επιφύλασσε ο Cybersecurity Act στον ENISA, περιλαμβάνει την ανάπτυξη πλαισίων πιστοποίησης κυβερνοασφάλειας, την παροχή καθοδήγησης και εμπειρογνωμοσύνης σε θέματα κυβερνοασφάλειας και την παροχή βοήθειας στα κράτη μέλη αναφορικά με την εφαρμογή πολιτικών για την ασφάλεια στον κυβερνοχώρο.

Ως κεντρικός σκοπός του "Νέου ENISA" τίθεται η επίτευξη ενός υψηλού, κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση, μεταξύ άλλων υποστηρίζοντας ενεργά τα κράτη μέλη, τα όργανα και οργανισμούς της Ένωσης για τη βελτίωση της κυβερνοασφάλειας. Ο ENISA πλέον ενεργεί ως σημείο αναφοράς για την παροχή συμβουλών και εμπειρογνωμοσύνης σχετικά με την κυβερνοασφάλεια για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, καθώς και άλλους σχετικούς συμφεροντούχους στην Ένωση. Παράλληλα μέσω της δράσης του, συμβάλλει στη μείωση του κατακερματισμού της εσωτερικής αγοράς, ενεργώντας ανεξάρτητα και αναπτύσσοντας τους δικούς του

[35] Συγκεκριμένα επρόκειτο για γραπτή δήλωση δεσμεύσεων και γραπτή δήλωση συμφερόντων.

αναγκαίους πόρους, συμπεριλαμβανομένων τεχνικών και ανθρώπινων ικανοτήτων και δεξιοτήτων, για να εκτελεί τα καθήκοντα που του ανατίθενται δυνάμει του παρόντος κανονισμού.

Σε επίπεδο στοχοθεσίας, παρατηρείται επίσης διεύρυνση. Ο ENISA πλέον συνιστά κεντρικό άξονα εμπειρογνωσίας σε θέματα κυβερνοασφάλειας. Η θέση του αυτή ενισχύεται από την ανεξαρτησία την οποία απολαμβάνει, την επιστημονική και τεχνική ποιότητα των συμβουλών και της επικουρίας που παρέχει, τις πληροφορίες που διαθέτει, τη διαφάνεια των επιχειρησιακών διαδικασιών του, τις μεθόδους λειτουργίας και την επιμέλεια με την οποία εκτελεί τα καθήκοντά του. Εξακολουθεί να επικουρεί τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και τα κράτη μέλη, στην ανάπτυξη και την εφαρμογή πολιτικών της Ένωσης που σχετίζονται με την κυβερνοασφάλεια, συμπεριλαμβανομένων των τομεακών πολιτικών για την κυβερνοασφάλεια, ενώ στηρίζει την ανάπτυξη ικανοτήτων και ετοιμότητας αντιμετώπισης περιστατικών σε επίπεδο Ένωσης. Μέσω της συνεργασίας του με τα όργανα και τους οργανισμούς της Ένωσης, τα κράτη μέλη και τους ιδιωτικούς και δημόσιους συμφεροντούχους, επιδιώκει την ενίσχυση της προστασίας των συστημάτων δικτύου και πληροφοριών τους, την ανάπτυξη και τη βελτίωση της κυβερνοανθεκτικότητας και της ικανότητας ανταπόκρισης και την ανάπτυξη δεξιοτήτων και ικανοτήτων στο πεδίο της κυβερνοασφάλειας. Παράλληλα προάγει τη συνεργασία, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών, και τον συντονισμό σε ενωσιακό επίπεδο, συμβάλλει στην αύξηση των ικανοτήτων κυβερνοασφάλειας σε επίπεδο Ένωσης προκειμένου να εξασφαλίζεται αποτελεσματικότερη πρόληψη όσον αφορά την πρόληψη και την αντιμετώπιση κυβερνοαπειλών. Επιπρόσθετα συμβάλλει στη θέσπιση και τη διατήρηση ενός ευρωπαϊκού πλαισίου πιστοποίησης αναφορικά με την κυβερνοασφάλεια που έχει ως στόχο την ενίσχυση της κυβερνοασφάλειας των προϊόντων, υπηρεσιών και διαδικασιών τεχνολογιών πληροφορικής και υπηρεσιών. Απώτερο στόχο συνιστά η ενίσχυση της εμπιστοσύνης στην ψηφιακή εσωτερική αγορά και την διατήρηση της ανταγωνιστικότητά της. Τέλος, εξακολουθεί να συνιστά κεντρικό ζήτημα η ευαισθητοποίηση ως προς το ζήτημα της προστασίας από τους κινδύνους του κυβερνοχώρου, καθώς και η καθιέρωση διαδικασιών κυβερνοϋγιεινής και κυβερνογραμματισμού μεταξύ πολιτών, οργανισμών και επιχειρήσεων.

Ο ENISA, στα πλαίσια του νέου, διευρυμένου ρόλου του, συμβάλλει στη χάραξη και

την εφαρμογή της πολιτικής και του δικαίου της Ένωσης αναφορικά με το ζήτημα της κυβερνοασφάλειας με πληθώρα τρόπων, μεταξύ των οποίων παρέχοντας ανεξάρτητη γνωμοδότηση, ανάλυση, υποστήριξη και συμβουλές σχετικά με τη χάραξη και την επανεξέταση της πολιτικής και του δικαίου της Ένωσης αναφορικά με τον οικείο κλάδο. Όταν αυτό κρίνεται απαραίτητο δύναται να διενεργεί προπαρασκευαστικές πράξεις και εργασίες σχετικά με πρωτοβουλίες πολιτικής και δικαίου, εφόσον εμπλέκονται και ζητήματα που αφορούν την κυβερνοασφάλεια. Εκτός της χάραξης πολιτικής, επικουρεί τα κράτη μέλη στο πεδίο της συνεπούς εφαρμογής της πολιτικής και του κανονιστικού πλαισίου της Ένωσης σχετικά με την κυβερνοασφάλεια[36], μεταξύ άλλων με την έκδοση γνωμοδοτήσεων, κατευθυντήριων γραμμών, την παροχή συμβουλών και βέλτιστων πρακτικών σχετικά με ζητήματα όπως διαχείριση κινδύνων, κοινοποίηση συμβάντων και ανταλλαγή πληροφοριών, καθώς και διευκολύνοντας την ανταλλαγή βέλτιστων πρακτικών μεταξύ αρμόδιων αρχών αναφορικά με το ζήτημα επικοινωνίας και ενημέρωσης.

Η χάραξη και εφαρμογή της ενωσιακής πολιτικής στον τομέα της ηλεκτρονικής ταυτότητας και των υπηρεσιών εμπιστοσύνης, ενισχύεται μέσω του ενισχυμένου ρόλου του ENSIA, μέσω της παροχής συμβουλών, της έκδοσης τεχνικών κατευθυντήριων γραμμών, και της διευκόλυνσης στην ανταλλαγή βέλτιστων πρακτικών μεταξύ των διαφόρων αρχών. Παράλληλα παρέχει υποστήριξη στα κράτη μέλη σε επίπεδο εφαρμογής ειδικών πτυχών κυβερνοασφάλειας της πολιτικής και του δικαίου της Ένωσης, ιδιαιτέρως στο πεδίο της προστασίας των δεδομένων και της ιδιωτικής ζωής των πολιτών και συμβάλει στην διαρκή βελτίωση του συστήματος μέσω της εκπόνησης ετήσιας έκθεσης αναφορικά με τη συνάρτηση των δραστηριοτήτων πολιτικής της Ένωσης σε σχέση με την κατάσταση εφαρμογής του αντίστοιχου νομικού πλαισίου στο πεδίο πληροφόρησης και κοινοποίησης συμβάντων από πλευράς των κρατών μελών που υποβάλλονται από τα ενιαία κέντρα επαφής στην ομάδα συνεργασίας. Λαμβάνονται επίσης υπόψη οι περιλήψεις των κοινοποιήσεων παραβίασης της ασφάλειας ή απώλειας της ακεραιότητας που αποστέλλονται από παρόχους υπηρεσιών εμπιστοσύνης και που υποβάλλονται από τα εποπτικά όργανα στον ENISA[37], καθώς και οι σχετικές με συμβάντα αφορώντα την ασφάλεια κοινοποιήσεις που υποβάλλονται από τις αρμόδιες αρχές στον ENISA, προερχόμενες από

[36] Ιδίως σε σχέση με την οδηγία (ΕΕ) 2016/1148

[37] Δυνάμει του άρθρου 19 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

παρόχους δημοσίων ηλεκτρονικών δικτύων επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών[38].

Ο ρόλος του ENISA σε επίπεδο ανάπτυξης ικανοτήτων εντοπισμού, αντιμετώπισης και πρόληψης κινδύνων είναι κατά βάση επικουρικός και συνίσταται στην παροχή γνώσεων και εμπειρογνωμοσύνης, ενώ όταν του ζητείται ενισχύει τα κράτη μέλη στην ανάπτυξη εθνικών στρατηγικών ασφάλειας των συστημάτων δικτύου και πληροφοριών τους[39], και προάγει τη διάδοση των εν λόγω στρατηγικών, παρακολουθώντας την πρόοδο εφαρμογής τους, με σκοπό τον εντοπισμό, τη βελτίωση κατανόηση και αναπαραγωγή των βέλτιστων πρακτικών. Ανά τακτά χρονικά διαστήματα, ο ENISA διοργανώνει ασκήσεις κυβερνοασφάλειας σε επίπεδο Ένωσης με σκοπό τον εντοπισμό τυχόν ευάλωτων σημείων σε επίπεδο αντιμετώπισης ενδεχόμενων απειλών και σε δεύτερο χρόνο, τη διατύπωση συστάσεων πολιτικής, ανάλογα τα στοιχεία που συλλέχθηκαν κατά τη διενέργεια της άσκησης και επί τη βάσει της διαδικασίας αξιολόγησης. Ο ENISA επικουρεί έμμεσα ή άμεσα και τις εθνικές CSIRT, είτε μέσω της υποβοήθησης στην δημιουργία τους σε εθνικό επίπεδο[40], είτε ενισχύοντας τις εθνικές και ενωσιακές CSIRT με στόχο την αύξηση του επιπέδου ικανότητάς τους, μεταξύ άλλων μέσω της προώθησης του διαλόγου και της ανταλλαγής πληροφοριών. Στόχος είναι η εξασφάλιση ότι όλα τα CSIRT διαθέτουν ένα κοινό σύνολο ελάχιστων ικανοτήτων και λειτουργούν με βάση τις βέλτιστες πρακτικές. Τέλος, παρέχεται η δυνατότητα ενίσχυσης δημόσιων οργανισμών μέσω της κατάρτισης σχετικά με την κυβερνοασφάλεια, ενώ γίνονται από τον ENSIA προσπάθειες ενίσχυσης των διόδων επικοινωνίας μεταξύ των ενδιαφερόμενων φορέων, μέσω της θέσπισης και εφαρμογής πολιτικών δημοσιοποίησης τρωτών σημείων σε εθελοντική βάση, προς βελτίωση των ικανοτήτων πρόληψης, εντοπισμού, ανάλυσης και αντιμετώπισης κυβερνοαπειλών και συμβάντων. Εν γένει ο ENISA στηρίζει την ανταλλαγή πληροφοριών με την παροχή βέλτιστων πρακτικών και καθοδήγησης για τα διαθέσιμα εργαλεία, τις διαδικασίες, καθώς και για τον τρόπο αντιμετώπισης των ρυθμιστικών ζητημάτων που σχετίζονται με την άμεση και ασφαλή μετάδοση πληροφόρησης για ύπαρξη ενδεχόμενων απειλών ή συμβάντων.

[38] Δυνάμει του άρθρου 40 της οδηγίας (ΕΕ) 2018/1972.
[39] Δυνάμει του άρθρου 7 παράγραφος 2 της οδηγίας (ΕΕ) 2016/1148
[40] Δυνάμει του άρθρου 9 παράγραφος 5 της οδηγίας (ΕΕ) 2016/1148

2.2.2. Οι Εθνικές Αρχές Πιστοποίησης της Κυβερνοασφάλειας (National Cybersecurity Certification Authorities - NCCAs)

Στο πλαίσιο προσπάθειας τυποποίησης αποτελεσματικής και ενιαίας προσέγγισης στον τομέα της κυβερνοασφάλειας, ο Cybersecurity Act θέσπισε υποχρέωση των κρατών μελών να ορίσουν μία ή περισσότερες Εθνικές Αρχές Πιστοποίησης της Κυβερνοασφάλειας (National Cybersecurity Certification Authorities - NCCAs). Για λόγους διαφάνειας, επρόκειτο για αρχές θεσμικά και διοικητικά ανεξάρτητες σε σχέση με τις επιβλεπόμενες οντότητες, η ταυτότητα των οποίων γνωστοποιείται στην Επιτροπή.

Κάθε μια από τις ανωτέρω αρχές είναι υπεύθυνη για την επίβλεψη των συστημάτων πιστοποίησης κυβερνοασφάλειας του κράτους μέλους προέλευσής της, προκειμένου να διασφαλίζεται η σωστή και σύμφωνη με τα ενωσιακά πρότυπα εκτέλεση των διαδικασιών πιστοποίησης. Παράλληλα, έχουν επιφορτιστεί με την επιβολή των διατάξεων του ενωσιακού πλαισίου πιστοποίησης σε ζητήματα κυβερνοασφάλειας, που πραγματοποιείται μέσω της παρακολούθησης του επιπέδου της συμμόρφωσης προϊόντων, υπηρεσιών και διαδικασιών ΤΠΕ με τα καθιερωμένα συστήματα πιστοποίησης, ενώ ενεργούν και μερική εποπτεία της αγοράς, μέσω του ελέγχου περί συμμόρφωσης με τις ανωτέρω πιστοποιήσεις των προσφερόμενων προϊόντων, υπηρεσιών και διαδικασιών και τη λήψη μέτρων κατά οντοτήτων που εμμένουν σε μη συμμόρφωση.

Επιπρόσθετα, οι Εθνικές Αρχές Πιστοποίησης της Κυβερνοασφάλειας ενεργούν ως το εθνικό σημείο επαφής για θέματα που σχετίζονται με την εφαρμογή αυτών των συστημάτων πιστοποίησης, και συνεργάζονται σε επίπεδο ανταλλαγής πληροφοριών με αρχές άλλων κρατών μελών, με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) και άλλους σχετικούς φορείς. Τέλος, σε περιπτώσεις μη συμμόρφωσης, έχουν την εξουσία να λαμβάνουν κατάλληλα μέτρα επιβολής, μεταξύ των οποίων έκδοση προειδοποιήσεων, επιβολή προστίμων κ.α.

Μέσα από την λειτουργία τους έχει φανεί ότι οι Εθνικές Αρχές Πιστοποίησης της Κυβερνοασφάλειας διαδραματίζουν βασικό ρόλο στην εναρμόνιση των προτύπων κυβερνοασφάλειας σε ενωσιακό επίπεδο, συμβάλλοντας ενεργά στην δημιουργία ενός κοινού ελάχιστου επιπέδου προστασίας για όλα τα κράτη μέλη. Παράλληλα, μέσω της επιβολής υιοθέτηση κοινών ενωσιακών πιστοποιήσεων, συμβάλλουν στην οικοδόμηση εμπιστοσύνης στην ψηφιακή αγορά, ενισχύοντας ούτως τη συνολική ασφάλεια στον

κυβερνοχώρο.

2.3. Οι οδηγίες NIS 1 και NIS 2

Στο σύγχρονο, ταχύτατα εξελισσόμενο τοπίο της κυβερνοασφάλειας, οι Οδηγίες για τα Δίκτυα και τα Συστήματα Πληροφοριακών Συστημάτων (NIS) της Ευρωπαϊκής Ένωσης - NIS 1 (Οδηγία 1148/2016)[41] και NIS 2 (Οδηγία 2555/2022) - θεωρούνται κεντρικά ρυθμιστικά πλαίσια. Η NIS 1, που εισήχθη το 2016, σηματοδότησε την πρώτη ολοκληρωμένη ενωσιακή προσπάθεια για θέσπιση ενός σύγχρονου κανονιστικού πλαισίου για την ασφάλεια στον κυβερνοχώρο. Έθεσε τα θεμέλια καθορισμού των βασικών απαιτήσεων ασφάλειας και κοινοποίησης για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών, με στόχο την ενίσχυση του συνολικού επιπέδου ασφάλειας στον κυβερνοχώρο σε ενωσιακό επίπεδο. Ωστόσο, το ήπιο πλαίσιο εφαρμογής και η ερμηνευτική ευελιξία του NIS 1 οδήγησαν σε μη ομοιόμορφη εφαρμογή του από τα κράτη μέλη, υπογραμμίζοντας την ανάγκη μιας πιο ενοποιημένης προσέγγισης.

Ανταποκρινόμενη σε αυτή την ανάγκη, εισήχθη η Οδηγία NIS 2, μια ολοκληρωμένη αναθεώρηση της προκατόχου της. Επεκτείνοντας το πεδίο εφαρμογής για να συμπεριλάβει ένα ευρύτερο φάσμα τομέων και εισάγοντας πιο αυστηρές απαιτήσεις συμμόρφωσης, η οδηγία NIS 2 αντικατοπτρίζει μια εντατική εστίαση στην ασφάλεια στον κυβερνοχώρο. Κατηγοριοποιεί τις οντότητες ως «βασικές» ή «σημαντικές», καθεμία από τις οποίες υπόκειται σε συγκεκριμένα μέτρα εποπτείας και συμμόρφωσης. Αυτή η ταξινόμηση, μαζί έναν συνδυασμό αυστηροποίησης υποχρεώσεων αναφοράς και εποπτείας, σε συνδυασμό με τη θέσπιση σημαντικών κυρώσεων σε περιπτώσεις μη συμμόρφωσης, αντικατοπτρίζουν την ωρίμανση της Ευρω-ενωσιακής δέσμευσης για ενίσχυση του επιπέδου ασφάλειας στον κυβερνοχώρο.

2.3.1. Η NIS 1 (Οδηγία 1148/2016)

Η Οδηγία 2016/1148 (εφεξής NIS 1)[42], η οποία ίσχυε μέχρι το 2022 που αντικαταστάθηκε από την Οδηγία 2555/2022 (εφεξής NIS 2), αποσκοπούσε στην ανάπτυξη του επιπέδου και ικανοτήτων κυβερνοασφάλειας σε όλο το εύρος της Ένωσης, με κύριο

[41] Ενσωμάτωση με Ν. 4577/2018 (ΦΕΚ Α' 199/03.12.2018)

[42] Ενσωμάτωση με Ν. 4577/2018 (ΦΕΚ Α' 199/03.12.2018)

γνώμονα το μετριασμό των απειλών που στρέφονται κατά των συστημάτων δικτύου και πληροφοριών, τα οποία χρησιμοποιούνται για την παροχή βασικών υπηρεσιών σε σημαντικούς τομείς και στη διασφάλιση της συνέχειας των υπηρεσιών αυτών κατά την αντιμετώπιση περιστατικών. Κατά τα ανωτέρω η οδηγία 1148/2016 είχε ως στόχο την ενίσχυση του επιπέδου ασφαλείας, προκειμένου να εξασφαλιστεί απρόσκοπτη και αποτελεσματική λειτουργία της οικονομίας και της κοινωνίας της Ένωσης. Κατά το χρονικό διάστημα λειτουργίας της εν λόγω οδηγίας, σημειώθηκε σημαντική πρόοδος στην αύξηση του επιπέδου κυβερνοανθεκτικότητας της Ένωσης, ενώ λειτούργησε ως καταλύτης για τη θεσμική και κανονιστική προσέγγιση της κυβερνοασφάλειας στην Ένωση, με δεδομένο ότι προετοίμασε το έδαφος για μια σημαντική αλλαγή νοοτροπίας.

Μέσω της θέσπισης εθνικών στρατηγικών για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, της θέσπισης εθνικών ικανοτήτων, αλλά και με την εφαρμογή ρυθμιστικών μέτρων τα οποία είχαν ως αντικείμενο την κάλυψη βασικών υποδομών (ΚΥ) (Critical Infrastructures – CI)[43] και οντοτήτων, όπως αυτά προσδιορίζονταν από κάθε κράτος μέλος, η οδηγία 1148/2016 συνέβαλε αποφασιστικά στην εξ υπαρχής δημιουργία ή και ολοκλήρωση εθνικών πλαισίων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών. Η ύπαρξη και ενίσχυση των εθνικών πλαισίων για την προστασία των συστημάτων στον κυβερνοχώρο έχει εξ΄αντικειμένου, διπλή σημασία. Από τη μια πλευρά δομείται μια προστατευτική βάση σε εθνικό επίπεδο, η οποία έχει ως σκοπό την προστασία των κύριων εθνικών υποδομών και οντοτήτων, ενώ από την άλλη ενισχύεται σε συλλογικό επίπεδο η συνολική ασφάλεια σε επίπεδο Ένωσης, στοιχείο απαραίτητο για την ολοκλήρωσή της ως χώρου ελευθερίας, ασφάλειας και δικαιοσύνης. Παράλληλα μέσω της σύστασης της ομάδας συνεργασίας και του δικτύου εθνικών ομάδων αντιμετώπισης περιστατικών ασφάλειας υπολογιστών, η οδηγία 1148/2016 συνέβαλε επίσης στην ανάπτυξη δομών και συστήματος συνεργασίας σε επίπεδο Ένωσης, συνδέοντας με αυτό τον τρόπο άμεσα την ασφάλεια των κρατών μελών με την Ενωσιακή ασφάλεια.

Παρά τα επιτεύγματα αυτά, η επανεξέταση της οδηγίας 1148/2016 κατέδειξε εγγενείς αδυναμίες της, οι οποίες έθεταν εμπόδια στην αποτελεσματική αντιμετώπιση των

[43] Κρίσιμη Υποδομή (ΚΥ) (Critical Infrastructure – CI) ή Υποδομή Ζωτικής Σημασίας (ΥΖΣ) ορίζεται ένα αγαθό, σύστημα ή υποσύστημα που είναι απαραίτητο για τη διατήρηση των ζωτικών λειτουργιών της κοινωνίας, την υγεία, τη φυσική προστασία (safety), την ασφάλεια (security), την οικονομική και την κοινωνική ευημερία των ανθρώπων»

τρεχουσών και ταχύτατα αναδυόμενων προκλήσεων κυβερνοασφάλειας. Η νομική βάση της εν λόγω οδηγίας ήταν το άρθρο 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), στόχος του οποίου είναι η εγκαθίδρυση και η λειτουργία της εσωτερικής αγοράς με την ενίσχυση των μέτρων για την προσέγγιση των εθνικών κανόνων. Μέσω της λειτουργίας της οδηγίας αναδείχθηκε η σημασία της εγκαθίδρυσης κοινών, ή τουλάχιστον συναφών, για τα κράτη μέλη απαιτήσεων κυβερνοασφάλειας, με σκοπό τόσο την αύξηση της αποτελεσματικότητας όσο και τη μείωση του κόστους. Ο λόγος που κρίθηκε απαραίτητη μια σύγκλιση των νομικών πλαισίων για την ασφάλεια, έγκειται στο ότι οι απαιτήσεις κυβερνοασφάλειας που επιβάλλονταν μεταξύ των κρατών μελών ως προς το είδος των απαιτήσεων, τον βαθμό λεπτομέρειάς τους και τη μέθοδο εποπτείας στις παρέχουσες υπηρεσίες ή ασκούντες οικονομικά σημαντικές δραστηριότητες οντότητες είχαν σημαντικές διαφορές μεταξύ τους. Οι διαφορές αυτές συνεπάγονταν πρόσθετο κόστος και προκαλούσαν δυσκολίες στις οντότητες που δραστηριοποιούνταν διασυνοριακά στον τομέα προσφοράς αγαθών ή υπηρεσιών. Ενίοτε οι απαιτήσεις που επιβάλλονταν από ένα κράτος μέλος όχι απλά διέφεραν, αλλά έρχονταν και σε αντίθεση με τις απαιτήσεις που επιβάλλονταν σε άλλο κράτος μέλος, με αποτέλεσμα να επηρεάζονται σημαντικά οι εν λόγω διασυνοριακές δραστηριότητες. Επιπλέον, η πιθανότητα ανεπαρκούς σχεδιασμού ή εφαρμογής των απαιτήσεων κυβερνοασφάλειας σε ένα κράτος μέλος είναι πιθανό να έχει επιπτώσεις στο επίπεδο κυβερνοασφάλειας άλλων κρατών μελών, ιδίως λαμβανομένης υπόψη της έντασης των διασυνοριακών συναλλαγών.

Σε μια προσπάθεια απολογισμού, θα μπορούσε να λεχθεί ότι κατά την εφαρμογή της οδηγίας 1148/2016 εμφανίστηκαν έντονες αποκλίσεις από τα κράτη μέλη, μεταξύ άλλων όσον αφορά το πεδίο εφαρμογής της, η οριοθέτηση του οποίου ε[αφίετο σε μεγάλο βαθμό στη διακριτική ευχέρεια των κρατών μελών. Με δεδομένο μάλιστα ότι παρείχε ευρύτατη διακριτική ευχέρεια στα κράτη μέλη όσον αφορά την εφαρμογή των υποχρεώσεων τους σχετικά με την ασφάλεια και την αναφορά των περιστατικών που ορίζονταν στην εν λόγω οδηγία, οι υποχρεώσεις αυτές εκπληρώθηκαν με πολύ διαφορετικούς τρόπους σε εθνικό επίπεδο. Παρόμοιες αποκλίσεις υπάρχουν στην εφαρμογή των σχετικών με την εποπτεία και την επιβολή των διατάξεων της ανωτέρω οδηγίας.

2.3.2. Η NIS 2 (Οδηγία 2555/2022)

Η, σχετικά πρόσφατη, Οδηγία 2555/2022[44], διαφοροποιήθηκε σε σχέση με την `Οδηγία 1148/2016 την οποία και διαδέχθηκε καταργώντας την, σε έξι κεντρικούς άξονες, και συγκεκριμένα θέτοντας: α) διευρυμένο πεδίο εφαρμογής της προγενέστερης, β) ενισχυμένες απαιτήσεις ασφαλείας γ) διατάξεις για ενίσχυση της συνεργασίας σε Ευρω-ενωσιακό επίπεδο, δ) αυστηρότερα χρονοδιαγράμματα σε επίπεδο αναφοράς περιστατικών, ε) υψηλότερες κυρώσεις και πρόστιμα σε περίπτωση μη συμμόρφωσης εκ μέρους των οντοτήτων, ενώ στ) προς αποφυγή αστοχιών της προϊσχύσασα οδηγίας, τίθενται με την παρούσα οδηγία υποχρεώσεις εποπτείας και λογοδοσίας του αρμόδιο εποπτικού διοικητικού οργάνου, αλλά και υποχρέωση επιβολής των διατάξεων της. Επιπρόσθετα, σε επίπεδο χάραξης στρατηγικής για την αντιμετώπιση των απειλών κατά της κυβερνοασφάλειας, η NIS 2, προβλέπει υποχρέωση εκ μέρους των κρατών μελών για σχεδιασμό και έγκριση εθνικών στρατηγικών κυβερνοασφάλειας. Η NIS 2 τέθηκε σε ισχύ στις 16 Ιανουαρίου του 2023, ενώ δίνεται χρονικό περιθώριο στα τα κράτη μέλη να θεσπίζουν και να δημοσιεύσουν τα απαραίτητα προς συμμόρφωση με τις διατάξεις της εν λόγω οδηγίας μέτρα, έως τις 17 Οκτωβρίου 2024. Από την επομένη της λήξης της ως άνω προθεσμίας, ήτοι από τις 18 Οκτωβρίου 2024, θεωρείται ότι καταργείται η προγενέστερη Οδηγία NIS 1, και τίθενται σε εφαρμογή θα εφαρμόζονται τα μέτρα αυτά.

2.3.2.1. Διεύρυνση του πεδίου εφαρμογής

Αναφορικά με τη διεύρυνση του πεδίου εφαρμογής, σημειώνεται ότι ενώ η οδηγία NIS 1 προέβλεπε τη λήψη μέτρων για την αύξηση του επιπέδου κυβερνοασφάλειας σε επτά μόνο τομείς, ήτοι στους τομείς της ενέργειας, των μεταφορών, των συστημάτων που σχετίζονται με παροχή τραπεζικών υπηρεσιών και τη λειτουργία των χρηματοπιστωτικών αγορών, του πόσιμου νερού, την υγειονομική περίθαλψη και τις ψηφιακές υποδομές, η οδηγία NIS 2 διευρύνει σημαντικά το πεδίο εφαρμογής της, λαμβάνοντας υπόψη τις εξελίξεις στο ζήτημα τόσο της αυξανόμενης εξάρτησης από τον τομέα Τεχνολογιών Πληροφορικής και Επικοινωνιών, όσο και την αλληλοσύνδεση της επίτευξης ενός υψηλού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση με την δημιουργία δομών συνεργασίας δημόσιων και ιδιωτικών οντοτήτων τόσο σε εθνικό επίπεδο όσο και μεταξύ των κρατών μελών, με βασικό πάντοτε γνώμονα την ανάπτυξη και βελτίωση της λειτουργίας της

[44] Έπεται η ενσωμάτωσή του

εσωτερικής αγοράς.

Η ανωτέρω διεύρυνση του πεδίου εφαρμογής λαμβάνει χώρα μέσω της προσθήκης νέων τομέων, ανάλογα με τον βαθμό ψηφιοποίησης και διασύνδεσής τους και τον βαθμό κρισιμότητας τους για την οικονομία και την κοινωνία. Για λόγους σαφήνειας και διευκόλυνσης της ομοιόμορφης εφαρμογής της, η Οδηγία NIS 2 εισάγει έναν σαφή κανόνα διαλογής των σημαντικών οντοτήτων, προχωρώντας κατά τρόπον

τινά σε μια κατάταξη τους, σε δημόσιες[45] ή ιδιωτικές, με βάσει τα χαρακτηριστικά τους, όπως το μέγεθος[46] ή το αντικείμενό τους, και τη σημασία τους. από πλευράς μεγέθους οντοτήτων, συμπεριλαμβάνοντας κατά τον τρόπο αυτό στο πεδίο εφαρμογής της όλες τις μεσαίου και μεγάλου μεγέθους επιχειρήσεις σε επιλεγμένους τομείς, αποκλείοντας ούτως καταρχήν τις μικρότερες. Κατ' ουσίαν ο εντοπισμός μικρότερων οντοτήτων με υψηλό προφίλ κινδύνου ασφάλειας, που θα πρέπει επίσης να καλύπτονται από τις υποχρεώσεις της NIS 2, επαφίεται στη διακριτική ευχέρεια των κρατών μελών.

Είναι χαρακτηριστικό και ενδεικτικό των στόχων της NIS 2, το γεγονός ότι οι διατάξεις της εφαρμόζονται, σε συγκεκριμένες περιπτώσεις, και για οντότητες ανεξαρτήτως του μεγέθους τους. Εισάγεται έτσι επιπροσθέτως και ένα, κατά τρόπον τινά, ποιοτικό κριτήριο, με βάση το οποίο επιλέγονται οι οντότητες που χρήζουν προστασίας. Στις ανωτέρω οντότητες περιλαμβάνονται, μεταξύ άλλων και οι παρέχουσες υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό, ή υπηρεσίες παρόχων εμπιστοσύνης (Trust Services

---

[45] βλ. περ. στ της παρ. 2 του αρ. 2, «*Μια οντότητα είναι φορέας δημόσιας διοίκησης: i) της κεντρικής κυβέρνησης όπως ορίζεται από κράτος μέλος σύμφωνα με το εθνικό δίκαιο· ii) σε περιφερειακό επίπεδο, όπως ορίζεται από κράτος μέλος σύμφωνα με το εθνικό δίκαιο, ο οποίος, μετά από αξιολόγηση βάσει κινδύνου, παρέχει υπηρεσίες των οποίων η διατάραξη θα μπορούσε να έχει σημαντικό αντίκτυπο σε κρίσιμες κοινωνικές ή οικονομικές δραστηριότητες».*

Ακόμα, κατά το αρ. 6 περ. 35 *«"Οντότητα δημόσιας διοίκησης": η οντότητα που αναγνωρίζεται ως τέτοια σε κράτος μέλος σύμφωνα με το εθνικό δίκαιο, μη συμπεριλαμβανομένων των δικαστηρίων, των κοινοβουλίων ή των κεντρικών τραπεζών, η οποία πληροί τα ακόλουθα κριτήρια: α) έχει συσταθεί με σκοπό την κάλυψη αναγκών γενικού συμφέροντος και δεν έχει βιομηχανικό ή εμπορικό χαρακτήρα· β) έχει νομική προσωπικότητα ή δικαιούται εκ του νόμου να ενεργεί για λογαριασμό άλλης οντότητας με νομική προσωπικότητα· γ) χρηματοδοτείται κατά το μεγαλύτερο μέρος από το κράτος, τις περιφερειακές αρχές ή άλλους οργανισμούς δημοσίου δικαίου, υπόκειται σε έλεγχο διαχείρισης από τις εν λόγω αρχές ή οργανισμούς ή έχει διοικητικό, διευθυντικό ή εποπτικό συμβούλιο, του οποίου περισσότερα από τα μισά μέλη διορίζονται από το κράτος, τις περιφερειακές αρχές ή άλλους οργανισμούς δημοσίου δικαίου· δ) έχει την εξουσία να απευθύνει σε φυσικά ή νομικά πρόσωπα διοικητικές ή κανονιστικές αποφάσεις που επηρεάζουν τα δικαιώματά τους στη διασυνοριακή κυκλοφορία προσώπων, αγαθών, υπηρεσιών ή κεφαλαίων·»*

[46] Για παράδειγμα γίνονται αναφορές για μεσαίες επιχειρήσεις, ή επιχειρήσεις που υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις

Provider)[47], αν και δεν ανήκουν στο δημόσιο συνιστούν τον μοναδικό πάροχο, σε ένα κράτος μέλος, υπηρεσίας που είναι ουσιώδης για τη διατήρηση κρίσιμων κοινωνικών ή οικονομικών δραστηριοτήτων. Ακόμα, ανεξαρτήτως του μεγέθους τους καταλαμβάνονται από τις διατάξεις του NIS 2 και οντότητες αυξημένης λειτουργικής σημασίας, η διατάραξη των οποίων ενδέχεται να επιφέρει σημαντικό διασυνοριακό αντίκτυπο, ή αντίκτυπο στη δημόσια τάξη και ασφάλεια ή στη δημόσια υγεία[48]. Στην ίδια αξιολογική κλίμακα, οντοτήτων επί των οποίων εφαρμόζονται οι διατάξεις της ανωτέρω οδηγίας ανεξαρτήτως του μεγέθους τους, υπάγονται και οι «Κρίσιμες οντότητες[49]» όπως αυτές ορίζονται στην οδηγία 2022/2557, καθώς και οντότητες που παρέχουν υπηρεσίες καταχώρησης ονομάτων τομέα[50].

Από το πεδίο εφαρμογής της NIS 2 εξαιρούνται οντότητες δημόσιας διοίκησης που δραστηριοποιούνται στους τομείς της εθνικής ασφάλειας, της δημόσιας τάξης, της άμυνας ή της επιβολής του νόμου, συμπεριλαμβανομένων της πρόληψης, της διακρίβωσης, της διαπίστωσης και της δίωξης ποινικών αδικημάτων. Παράλληλα, τα κράτη μέλη μπορούν να εξαιρούν από την εφαρμογή της NIS 2 συγκεκριμένες οντότητες, ενώ για άλλες δύνανται να αποφασίσουν αν θα συμπεριληφθούν στο πεδίο εφαρμογής της ή όχι[51].

2.3.2.2. Ενισχυμένες απαιτήσεις ασφαλείας

Η NIS 2 διακρίνεται για την ενίσχυση των απαιτήσεων ασφαλείας που προβλέπει. η οποία σε μεγάλο βαθμό επιτυγχάνεται τόσο σε επίπεδο πρόληψης, μέσω της θέσπισης

---

[47] Σύμφωνα με τον κανονισμό 910/2014, ο πάροχος υπηρεσιών εμπιστοσύνης (Trust Services Provider - TSP) είναι ένα φυσικό ή νομικό πρόσωπο που παρέχει μία ή περισσότερες υπηρεσίες καταπιστεύματος είτε ως ειδικευμένη είτε ως μη ειδικευμένη υπηρεσία εμπιστοσύνης προμηθευτής. Συνεπώς, ένας πάροχος υπηρεσιών εμ[ιστοσύνης παρέχει σωρευτικά ή υπαλλακτικά υπηρεσίες α) δημιουργίας, επαλήθευσης και επικύρωσης ηλεκτρονικών υπογραφών, σφραγίδων ή σφραγίδων χρόνου, ηλεκτρονικών καταχωρημένων υπηρεσιών παράδοσης και πιστοποιητικών που σχετίζονται με αυτές τις υπηρεσίες, β) δημιουργία, επαλήθευση και επικύρωση πιστοποιητικών που χρησιμοποιούνται για τον έλεγχο ταυτότητας ιστότοπου, και γ) διατήρηση ηλεκτρονικών υπογραφών, σφραγίδων ή πιστοποιητικών που σχετίζονται με αυτές τις υπηρεσίες. Οι TSP πρέπει, λόγω του αντικειμένου τους συνιστούν υψηλού κινδύνου τομείς, που χρήζουν αυξημένης προστασίας.

[48] https://nis2directive.eu/health/

[49] «Κρίσιμη οντότητα»: Ως κρίσιμες νοούνται οι οντότητες που παρέχουν βασικές υπηρεσίες καίριας σημασίας για τη διατήρηση νευραλγικών λειτουργιών της κοινωνίας, των οικονομικών δραστηριοτήτων, της δημόσιας υγείας και ασφάλειας, και του περιβάλλοντος. Οι κρίσιμες οντότητες είναι αναγκαίο να διαθέτουν ικανότητες στους τομείς της πρόληψης, της προστασίας, της αντίδρασης, της αντιμετώπισης και της ανάκαμψης έναντι υβριδικών επιθέσεων, φυσικών καταστροφών, τρομοκρατικών απειλών και καταστάσεων έκτακτης ανάγκης στον τομέα της δημόσιας υγείας

[50] βλ NIS 2 αρ. 6 περ. 22 «*Οντότητα που παρέχει υπηρεσίες καταχώρησης ονομάτων τομέα»: καταχωρητής ή αντιπρόσωπος που ενεργεί για λογαριασμό καταχωρητών, όπως πάροχος υπηρεσιών καταχώρισης δεδομένων προσωπικού χαρακτήρα ή πληρεξούσιος ή μεταπωλητής*.

[51] Σε αυτές περιλαμβάνονται οι οντότητες που ασκούν δημόσια διοίκηση σε τοπικό επίπεδο και εκπαιδευτικά ιδρύματα, ιδίως όταν διεξάγουν κρίσιμες ερευνητικές δραστηριότητες.

Πολιτικών και Διαδικασιών Ανάλυσης Κινδύνου και Ασφάλειας Πληροφοριακών Συστημάτων, όσο και σε επίπεδο διαχείρισης συμβάντων και διαχείρισης επιχειρησιακής συνέχειας (Business Continuity Management)[52]. Στα πλαίσια της τελευταίας συμπεριλαμβάνονται και η Διαχείριση Αντιγράφων Ασφαλείας, η Αποκατάσταση Καταστροφών[53] και η Διαχείριση Κρίσεων. Προς επίτευξη των ανωτέρω, δημιουργείται υποχρέωση εκ μέρους των κρατών μελών ορισμού ή σύστασης αρχών διαχείρισης κυβερνοκρίσεων, ήτοι μίας ή περισσότερων αρμόδιων αρχών, οι οποίες θα έχουν ως αντικείμενο ενασχόλησής τους τη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας. Προκειμένου να διευκολύνεται η λειτουργία των εν λόγω αρχών τα κράτη μέλη οφείλουν να εξασφαλίζουν επάρκεια πόρων για την αποτελεσματική και αποδοτική εκτέλεση των καθηκόντων που τους ανατίθενται, καθώς και ένα συνεκτικό πλαίσιο ώστε να διευκολύνεται η γενική εθνική διαχείριση κρίσεων. Παράλληλα, επαφίεται μεν στα κράτη μέλη η θέσπιση ενός εθνικού σχεδίου αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, πλην όμως η NIS 2 καθορίζει εξαντλητικά τους στόχους και το αντικείμενο ρύθμισής τους[54].

Στο πεδίο αντιμετώπισης συμβάντων και ενδεχόμενων απειλών, εγκαθιδρύεται υποχρέωση εκ μέρους των κρατών μελών να ορίσουν ή να συστήσουν μία ή περισσότερες CSIRT (Computer Security Incident Response Teams). Οι CSIRT είναι εξειδικευμένες ομάδες αντιμετώπισης περιστατικών ασφαλείας, υπεύθυνες για τη διαχείριση και την ανταπόκριση σε συμβάντα ασφάλειας υπολογιστών. Αυτά τα περιστατικά μπορεί να περιλαμβάνουν απειλές για την ασφάλεια στον κυβερνοχώρο, επιθέσεις ή παραβιάσεις που επηρεάζουν τα συστήματα και τα δίκτυα τεχνολογίας πληροφοριών ενός οργανισμού. Μετά τον εντοπισμό

---

[52] Η Διαχείριση Επιχειρηματικής Συνέχειας (Business Continuity Management), αφορά στην ολιστική διαδικασία διαχείρισης που προσδιορίζει πιθανές απειλές για έναν οργανισμό και τις επιπτώσεις στις επιχειρηματικές δραστηριότητες που αυτές οι απειλές, εάν πραγματοποιηθούν, θα μπορούσαν να προκαλέσουν και η οποία παρέχει ένα πλαίσιο για την οικοδόμηση οργανωτικής ανθεκτικότητας με την ικανότητα μιας αποτελεσματικής απάντησης που προστατεύει τα συμφέροντα των βασικών ενδιαφερομένων. δραστηριότητες φήμης, επωνυμίας και δημιουργίας αξίας

[53] https://setterwalls.se/artikel/preparing-for-the-nis-2-directive-impacts-on-the-health-sector/

[54] βλ. αρ. 9 παρ. 4: «*Το εν λόγω σχέδιο πρέπει να καθορίζει ιδίως: α) τους στόχους των εθνικών μέτρων και δραστηριοτήτων ετοιμότητας· β) τα καθήκοντα και τις αρμοδιότητες των αρχών διαχείρισης κυβερνοκρίσεων· γ) τις διαδικασίες διαχείρισης κυβερνοκρίσεων, συμπεριλαμβανομένης της ενσωμάτωσής τους στο γενικό εθνικό πλαίσιο διαχείρισης κρίσεων και στους διαύλους ανταλλαγής πληροφοριών· δ) τα εθνικά μέτρα ετοιμότητας, συμπεριλαμβανομένων ασκήσεων και δραστηριοτήτων κατάρτισης· ε) τα σχετικά ενδιαφερόμενα μέρη δημόσιου και ιδιωτικού τομέα και τις σχετικές υποδομές· στ) τις εθνικές διαδικασίες και ρυθμίσεις μεταξύ των αρμόδιων εθνικών αρχών και φορέων για να διασφαλίζεται η αποτελεσματική συμμετοχή και η παροχή υποστήριξης εκ μέρους του κράτους μέλους στη συντονισμένη διαχείριση περιστατικών μεγάλης κλίμακας και κρίσεων στον τομέα της κυβερνοασφάλειας σε επίπεδο Ένωσης*».

και την επαλήθευση ενός συμβάντος, το επόμενο βήμα είναι η ανταπόκριση, η ένταση της οποίας ποικίλλει ανάλογα με τη σοβαρότητα του συμβάντος. Το πεδίο προστασίας των CSIRT καθορίζεται από τα κράτη μέλη, ωστόσο πρέπει να καλύπτουν υποχρεωτικά τους τομείς και τις οντότητες που περιλαμβάνονται στα παραρτήματα[55] I (Τομείς Υψηλής Κρισιμότητας) [56] και II (Άλλοι Κρίσιμοι Τομείς)[57].

Προκειμένου δε να εξασφαλίζεται ένα ποιοτικό δίκτυο αντιμετώπισης συμβάντων, διευκρινίζεται ότι τα κράτη μέλη μπορούν να ζητούν τη συνδρομή του ENISA για την ανάπτυξη των CSIRT τους, ενώ προβλέπονται ειδικές διατάξεις αναφορικά με τις απαιτήσεις και τις τεχνικές ικανότητες τους, την ευθύνη για την εφαρμογή των οποιων φέρουν τα κράτη μέλη.

Στα πλαίσια ενίσχυσης των απαιτήσεων ασφαλείας της Ένωσης, επαφίεται στα κράτη μέλη να εξασφαλίζουν ότι οι βασικές και σημαντικες τους οντότητες λαμβάνουν κατάλληλα, και σύμφωνα με τα ευρωπαϊκά και διεθνή πρότυπα, μέτρα για την αντιμετώπιση περιστατικών και κρίσεων σχετιζόμενων με την κυβερνοασφάλεια. Σημαντικές πτυχές των προτύπων ασφαλείας που οφείλουν να υιοθετούν οι οντότητες, συνιστά οι υποχρέωσή τους να εφαρμόζουν πολιτικές για την ανάλυση κινδύνων, ανάπτυξη της ικανότητας αποκατάστασης μετά από επιτυχημένες επιθέσεις, βασικές πρακτικές κυβερνοϋγιεινής και βασική θεωρητική και τεχνική κατάρτιση των χρηστών τους αναφορικά με την κυβερνοασφάλεια, πολιτικές και διαδικασίες σχετικά με τη χρήση κρυπτογραφίας και, κατά περίπτωση, κρυπτογράφησης, αλλά και ασφάλεια ανθρώπινων πόρων, μέσω της

[55] Βλ. Ανακοίνωση Ευρωπαϊκής Επιτροπής (2023/C 324/01)

[56] Στο παράρτημα I περιλαμβάνονται οι τομείς υψηλής κρισιμότητας. Σε αυτούς περιλαμβάνονται οι τομείς που αφορούν την Ενέργεια (όπως ηλεκτρική ενέργεια, επιχειρήσεις ηλεκτρικής ενέργειας, διαχειριστές συστήματος διανομής, διαχειριστές συστήματος μεταφοράς, παραγωγοί, ορισθέντες διαχειριστές αγοράς ηλεκτρικής ενέργειας, συμμετέχοντες στην αγορά οι οποίοι παρέχουν υπηρεσίες συγκέντρωσης, απόκρισης ζήτησης ή αποθήκευσης ενέργειας κ.α., Πετρέλαιο, Αέριο). Μεταφορές (οδικές, εναέριες, αερομεταφορείς, φορείς διαχείρισης αερολιμένα, σιδηροδρομικές μεταφορές και σιδηροδρομικές επιχειρήσεις, πλωτές κ.α.) Υγεία, Πόσιμο νερό, Λύματα, Ψηφιακές υποδομές (Πάροχοι σημείων ανταλλαγής κίνησης διαδικτύου, Πάροχοι υπηρεσιών συστήματος ονομάτων τομέα (DNS), Μητρώα ονομάτων τομέα ανώτατου επιπέδου (TLD), Πάροχοι υπηρεσιών υπολογιστικού νέφους, Πάροχοι υπηρεσιών κέντρων δεδομένων, Πάροχοι δικτύων διανομής περιεχομένου, Πάροχοι υπηρεσιών εμπιστοσύνης, Πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών, Πάροχοι δημόσια διαθέσιμων υπηρεσιών ηλεκτρονικών επικοινωνιών, Διαχείριση υπηρεσιών ΤΠΕ (μεταξύ επιχειρήσεων), Πάροχοι διαχειριζόμενων υπηρεσιών, Πάροχοι διαχειριζόμενων υπηρεσιών ασφαλείας), Οντότητες δημόσιας διοίκησης, Διάστημα.

[57] Στο Παράρτημα II περιλαμβάνονται άλλοι κρίσιμοι τομείς, όπως Ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών, Διαχείριση αποβλήτων, Χημικά προϊόντα, Παραγωγή μεταποίηση και διανομή τροφίμων, Κατασκευαστικός τομέας, Ψηφιακοί πάροχοι (πάροχοι επιγραμμικών αγορών, πάροχοι επιγραμμικών μηχανών αναζήτησης, πάροχοι πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης), Οργανισμοί έρευνας.

διαμόρφωσης πολιτικών ελέγχου πρόσβασης, προς μείωση του ρόλου του ανθρώπινου παράγοντα σε περιπτώσεις ανάπτυξης κυβερνοαπειλών. Ειδική μνεία γίνεται στις κρίσιμες αλυσίδες εφοδιασμού, οι οποίες αναφέρονται στο διασυνδεδεμένο δίκτυο πόρων, υπηρεσιών και τεχνολογίας που είναι ζωτικής σημασίας για την παραγωγή και την παράδοση κρίσιμων αγαθών και υπηρεσιών. Κατά κανόνα αφορούν σε τομείς όπως η ενέργεια, οι μεταφορές, οι τράπεζες, η υγεία και οι ψηφιακές υποδομές. Η Οδηγία NIS 2 αναγνωρίζει ότι οι διακοπές σε αυτές τις αλυσίδες εφοδιασμού μπορεί να έχουν σημαντικές επιπτώσεις στην εθνική ασφάλεια, την οικονομική σταθερότητα και τη δημόσια ασφάλεια. Ως εκ τούτου, η οδηγία στοχεύει να ενισχύσει τα μέτρα ασφαλείας και τις υποχρεώσεις αναφοράς συμβάντων όχι μόνο των οργανισμών που εμπλέκονται άμεσα σε αυτούς τους κρίσιμους τομείς αλλά και εκείνων που αποτελούν αναπόσπαστο μέρος των αλυσίδων εφοδιασμού τους. Αυτή η προσέγγιση βοηθά στη διασφάλιση μιας ολοκληρωμένης και ισχυρής θέσης κυβερνοασφάλειας που εκτείνεται σε ολόκληρο το δίκτυο ανεφοδιασμού, μετριάζοντας τον κίνδυνο κυβερνοεπιθέσεων και άλλων διαταραχών που θα μπορούσαν να έχουν εκτεταμένες συνέπειες.

Τα κράτη μέλη μπορούν να θέτουν, αναφορικά με ορισμένες βασικές και σημαντικές οντότητες, απαιτήσεις, ώστε τα προϊόντα, οι υπηρεσίες και οι διαδικασίες ΤΠΕ που παράγουν ή χρησιμοποιούνται από αυτές να πιστοποιούνται στο πλαίσιο ευρωπαϊκών συστημάτων πιστοποίησης κυβερνοασφάλειας, ενώ ταυτόχρονα μπορούν να ενθαρρύνουν τις βασικές και σημαντικές οντότητες να χρησιμοποιούν αναγνωρισμένες υπηρεσίες εμπιστοσύνης. Στις περιπτώσεις όπου κανένα από τα υφιστάμενα διαθέσιμα ευρωπαϊκά συστήματα πιστοποίησης κυβερνοασφάλειας δεν κρίνεται κατάλληλο, η Επιτροπή δύναται να αναθέσει στον ENISA να καταρτίσει υποψήφιο σύστημα.

2.3.2.3. Χειρισμός και αποκάλυψη ευπαθειών

Συνιστά αδιαμφισβήτητο γεγονός ότι η αποτελεσματικότερη πολιτική αντιμετώπισης απειλών κατά της κυβερνοασφάλειας, αφορά συμβάντα για τα οποία δεν μάθαμε τίποτα. Είναι σαφές ότι η αποτελεσματική προστασία έναντι του αόρατου ψηφιακού κινδύνου, επαφίεται σε μεγάλο βαθμό στην δυνατότητα έγκαιρης αποκάλυψης ευπαθειών και την κατάλληλη διαχείρισή τους.

Προκειμένου να εξασφαλιστεί ο μεγαλύτερος δυνατός βαθμός εντοπισμού τους, η NIS 2 προβλέπει δυνατότητα των CSIRT να διενεργούν προληπτική μη παρεμβατική

σάρωση των δημοσίως προσβάσιμων συστημάτων δικτύου και πληροφοριών βασικών και σημαντικών οντοτήτων, προς τον εντοπισμό ευπαθειών ή επισφαλώς διαμορφωμένων συστημάτων δικτύου και πληροφοριών και ενημέρωση των οικείων οντοτήτων. Παράλληλα, κάθε κράτος μέλος αναθέτει σε μία από τις CSIRT του συντονιστικό ρόλο για τους σκοπούς της συντονισμένης γνωστοποίησης ευπαθειών, προκειμένου να ενεργεί ως αξιόπιστος διαμεσολαβητής, διευκολύνοντας, όπου απαιτείται, την αλληλεπίδραση μεταξύ του φυσικού ή νομικού προσώπου που αναφέρει την ευπάθεια και του κατασκευαστή ή του παρόχου των δυνητικά ευπαθών προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ, κατόπιν αιτήματος ενός εκ των μερών. Τα καθήκοντα της CSIRT στην οποία έχει ανατεθεί συντονιστικός ρόλος περιλαμβάνουν τον προσδιορισμό των οικείων οντοτήτων και την επικοινωνία με αυτές, την παροχή συνδρομής στα φυσικά ή νομικά πρόσωπα που αναφέρουν ευπάθειες, και τη διαπραγμάτευση χρονοδιαγραμμάτων γνωστοποίησης και τη διαχείριση ευπαθειών που επηρεάζουν πλείονες οντότητες. Προκειμένου να διευκολύνεται η αναφορά ευπαθειών, πρέπει να διασφαλίζεται ότι υφίσταται η δυνατότητα αν, ευπάθειες στην CSIRT στην οποία έχει ανατεθεί ο συντονισμός. Η CSIRT στην οποία έχει ανατεθεί ο συντονισμός διασφαλίζει ότι εκτελούνται επιμελείς ενέργειες παρακολούθησης όσον αφορά την αναφερθείσα τρωτότητα και διασφαλίζει την ανωνυμία του φυσικού ή νομικού προσώπου που αναφέρει την τρωτότητα. Στις περιπτώσεις όπου μια αναφερόμενη ευπάθεια θα μπορούσε να έχει σημαντικό αντίκτυπο σε οντότητες σε περισσότερα του ενός κράτη μέλη, η CSIRT στην οποία έχει ανατεθεί ο συντονισμός σε κάθε ενδιαφερόμενο κράτος μέλος συνεργάζεται, κατά περίπτωση, με άλλες CSIRT στις οποίες έχει ανατεθεί συντονιστικός ρόλος στο πλαίσιο του δικτύου CSIRT.

Ο ENISA αναπτύσσει και διατηρεί, ευρωπαϊκή βάση δεδομένων ευπαθειών, η οποία παρέχεται σε όλα τα ενδιαφερόμενα και περιλαμβάνει πληροφορίες που περιγράφουν την ευπάθεια, τα επηρεαζόμενα από αυτή προϊόντα και υπηρεσίες και τη διαθεσιμότητα διορθωτικών προγραμμάτων ή, ελλείψει διορθωτικών προγραμμάτων, υλικό καθοδήγησης που απευθύνεται στους χρήστες στους οποίους εμφανίζεται η ευπάθεια. Για τον σκοπό αυτό, ο ENISA καταρτίζει και διατηρεί τα κατάλληλα συστήματα πληροφοριών, πολιτικές και διαδικασίες και θεσπίζει τα αναγκαία τεχνικά και οργανωτικά μέτρα για τη διαφύλαξη της ασφάλειας και της ακεραιότητας της ευρωπαϊκής βάσης δεδομένων ευπαθειών, με σκοπό ιδίως να δοθεί η δυνατότητα σε όλο το εύρος των οντοτήτων, να δημοσιοποιούν και να

καταχωρίζουν, σε εθελοντική βάση, δημόσια γνωστές ευπάθειες.

Ένα μεγάλο πεδίο που εγκαινιάζει ο NIS 2 προς την κατεύθυνση της βελτίωσης των ικανοτήτων έγκαιρης αποκάλυψης ευπαθειών και της κατάλληλης διαχείρισής τους, συνιστά η διαμόρφωση πολιτικών και διαδικασιών για την αξιολόγηση της πραγματικής κατάστασης, δηλαδή του επιπέδου ασφαλείας σε συνάρτηση με τους υφιστάμενους κινδύνους, και της αποτελεσματικότητας των υφιστάμενων μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας, συνοδευόμενα συχνά από προτάσεις βελτίωσης τους. Στα πλαίσια αυτά, ανά δύο έτη εκδίδεται από τον ENISA, σε συνεργασία με την Επιτροπή και την Ομάδα Συνεργασίας, έκθεση σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση. Η εν λόγω έκθεση, η οποία υποβάλλεται και στο Ευρωπαϊκό Κοινοβούλιο, αναφέρεται όχι μόνο σε αξιολόγηση των κινδύνων και των ικανοτήτων διαχείρισης, αλλά και σε ζητήματα όπως το επίπεδο ευαισθητοποίησης των πολιτών και των οντοτήτων σε θέματα κυβερνοασφάλειας και κυβερνοϋγιεινής.

2.3.2.4. Διατάξεις για ενίσχυση της συνεργασίας

Αντιλαμβανόμενη ότι η συνεργατική προσέγγιση είναι ζωτικής σημασίας για την αντιμετώπιση της περίπλοκης και εξελισσόμενης φύσης των απειλών στον κυβερνοχώρο, η NIS 2 έδωσε έμφαση στην ενίσχυση της συνεργασίας. Σημαντικό βήμα προόδου συνιστά το γεγονός ότι η συνεργασία σε θέματα κυβερνοασφάλειας δεν αντιμετωπίζεται από την NIS 2 ως αμιγώς ενωσιακό ζήτημα. Αντίθετα, υπάρχει πρόβλεψη για την ενίσχυση του επιπέδου συνεργασίας σε τρία επίπεδα, σε εθνικό, ενωσιακό και διεθνές.

Σε εθνικό επίπεδο, η συνεργασία αφορά στη δημιουργία διόδων επικοινωνίας μεταξύ των εθνικών αρμόδιων αρχών, το ενιαίο σημείο επαφής και τις CSIRT, εφόσον υφίστανται περισσότερες από μια στο ίδιο κράτος μέλος. Ένας από τους σημαντικότερους σκοπούς, η επίτευξη του οποίου επιδιώκεται μέσω της ενίσχυσης της συνεργασίας μεταξύ των εμπλεκόμενων αρχών και οντοτήτων, συνίσταται στην αναφορά σοβαρών περιστατικών κυβερνοασφάλειας ή παρ' ολίγον περιστατικών, τα οποία γνωστοποιούνται και στα ενιαία σημεία επαφής τους. Οι κρίσιμες οντότητες[58], καθώς και οι οντότητες που εμπλέκονται με τα σχετιζόμενα με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης ζητήματα[59],

[58] βλ. Οδηγία 2557/2022
[59] βλ. Κανονισμος 910/2014

την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα[60] και τις ηλεκτρονικές επικοινωνίες[61] οφείλουν να ανταλλάσσουν σχετικές πληροφορίες σε τακτική βάση αναφορικά με ζητήματα αφορώντα την κυβερνοασφάλεια και κυβερνοαπειλές.

Σε ενωσιακό επίπεδο, η συνεργασία επιτυγχάνεται μέσω της σύστασης Ομάδας Εργασίας καθώς και της δημιουργίας δικτύου εθνικών CSIRT με σκοπό τη συμβολή στην ανάπτυξη εμπιστοσύνης και την προώθηση ταχείας και αποτελεσματικής επιχειρησιακής συνεργασίας μεταξύ των κρατών μελών. Οι CSIRT με τη σειρά τους συνάπτουν σχέσεις συνεργασίας με τα σχετικά ενδιαφερόμενα μέρη του ιδιωτικού τομέα, με σκοπό την αύξηση του επιπέδου προστασίας στον Κυβερνοχώρο. Παράλληλα, θεμέλιο λίθο στον τομέα της ενωσιακής συνεργασίας συνιστά η σύσταση του Ευρωπαϊκού δικτύου Οργανώσεων Διασύνδεσης για Κρίσεις στον Κυβερνοχώρο (European cyber crisis liaison organisation network - EU-CyCLONe), με σκοπό την ενίσχυση της συντονισμένης διαχείρισης περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας σε επιχειρησιακό επίπεδο και την διασφάλιση της τακτικής ανταλλαγής σχετικών πληροφοριών μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης. Μεταξύ των καθηκόντων του EU-CyCLONe περιλαμβάνονται η αναγνώριση της υφιστάμενης κατάστασης αναφορικά με περιστατικά και κρίσεις μεγάλης κλίμακας, η βελτίωση της ικανότητας αντιμετώπισής τους, η αξιολόγηση των συνεπειών και του αντικτύπου τους και η υποβολή προτάσεων για πιθανά μέτρα μετριασμού. Επιπρόσθετα, το EU-CyCLONe συμβάλει στην διαμόρφωση πολιτικής και συντονισμού του εθνικού σχεδίου αντιμετώπισης των κρατών μελών. Η συνεργασία του EU-CyCLONe με άλλες ομάδες είναι αρκετά διευρυμένη, καθώς υποβάλλει τακτικά εκθέσεις στην Ομάδα Συνεργασίας αναφορικά υφιστάμενα περιστατικά ή νεοεμφανιζομενες τάσεις και τον ενδεχόμενο αντίκτυπό τους, συνεργάζεται με το δίκτυο CSIRT, και συνεργάζεται και και με τα κράτη μέλη όταν αυτό είναι απαραίτητο.

Η NISS II, στο αρ. 17 προβλέπει ευθέως τη δυνατότητα ενεργειών συνεργασίας σε διεθνές επίπεδο, ορίζεται ότι η Ένωση μπορεί, κατά περίπτωση, δύναται να συνάπτει διεθνείς συμφωνίες σύμφωνα με το άρθρο 218 ΣΛΕΕ με τρίτες χώρες ή διεθνείς οργανισμούς, που επιτρέπουν και οργανώνουν τη συμμετοχή τους σε ορισμένες δραστηριότητες της ομάδας συνεργασίας, του δικτύου CSIRT και του EU-CyCLONe. Οι εν

[60] βλ. Κανονισμός 2554/2022
[61] βλ. Οδηγία 1972/2018

λόγω συμφωνίες είναι απαραίτητο να συμμορφώνονται με το δίκαιο της Ένωσης για την προστασία των δεδομένων.

2.3.2.5. Αυστηροποίηση χρονοδιαγραμμάτων σε επίπεδο αναφοράς περιστατικών

Η NIS 2, εκτός από τη δημιουργία ενός πλαισίου συνεργασίας, το οποίο περιλαμβάνει οντότητες, αρχές και κράτη μέλη, θέτει και αυστηρές υποχρεώσεις αναφοράς περιστατικών μεταξύ των ανωτέρω. Κατά ταύτα, επαφίεται στα κράτη μέλη η διασφάλιση κοινοποίησης σημαντικών περιστατικών[62], από πλευράς των βασικών και σημαντικών οντοτήτων. Η κοινοποίηση αυτή λαμβάνει χώρα, χωρίς αδικαιολόγητη καθυστέρηση, προς την CSIRT ή άλλη αρμόδια αρχή του του κράτους μέλους. Σε ορισμένες περιπτώσεις, όταν έχει εντοπιστεί σημαντικό περιστατικό, αυτό πρέπει να κοινοποιείται και στους χρήστες, ή κατά περίπτωση τους πιθανούς αποδέκτες για σημαντική κυβερνοαπειλή. Σε περίπτωση που το κοινοποιούμενο σημαντικό περιστατικό είναι διασυνοριακού ή διατομεακού τύπου, πρέπει να διασφαλίζεται ότι τα ενιαία σημεία επαφής τους λαμβάνουν εγκαίρως τις σχετικές πληροφορίες που κοινοποιούνται. Μάλιστα οι ανωτέρω κοινοποιήσεις που γίνονται προς την CSIRT ή άλλη αρμόδια αρχή, ακολουθούν αυστηρά χρονοδιαγράμματα, ήτοι εντός 24 ωρών από όταν έγινε αντιληπτό το περιστατικό πρέπει να έχει γίνει κοινοποίηση των πρώτων στοιχείων του περιστατικού ή της υποψίας για την ύπαρξη αυτού, ενώ εντός 72 ωρών από τη στιγμή που έγινε αντιληπτό το σημαντικό περιστατικό πρέπει να λάβει χώρα κοινοποίηση του περιστατικού με επικαιροποίηση των πληροφοριών, αναφορά της εξέλιξης του συμβάντος και αξιολόγηση της σοβαρότητας και των ενδεχόμενων συνεπειών του. Η αρχή που έλαβε την αρχική κοινοποίηση, οφείλει με τη σειρά της να παρέχει στην κοινοποιούσα οντότητα, αμελλητί και ει δυνατόν εντός 24 ωρών από τη λήψη της έγκαιρης προειδοποίησης απάντηση και, κατόπιν αιτήματος της οντότητας, καθοδήγηση ή επιχειρησιακές συμβουλές σχετικά με τη διαχείριση της εμφανισθείσας απειλής. Όταν δε υπάρχουν υπόνοιες και για ποινικού χαρακτήρα περιστατικό, η CSIRT ή η αρμόδια αρχή παρέχει επίσης καθοδήγηση σχετικά με την αναφορά του σημαντικού περιστατικού στις αρχές επιβολής του νόμου. Σε περίπτωση που το περιστατικό που προέκυψε είναι ενδιαφέροντος περισσοτέρων κρατών μελών, λαμβάνει χώρα ενημέρωση τόσο των

[62] Κατά το αρ. 23 παρ. 3 του NIS 2: «Ένα περιστατικό θεωρείται σημαντικό εάν: α) έχει προκαλέσει ή μπορεί να προκαλέσει σοβαρή λειτουργική διατάραξη των υπηρεσιών ή οικονομική ζημία για την οικεία οντότητα· β) έχει επηρεάσει ή μπορεί να επηρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία».

επηρεαζομένων κρατών, όσο και του ENISA, προκειμένου να λάβουν μέτρα εγκαίρως.

Η θέσπιση και εφαρμογή κανόνων για την κοινοποίηση περιστατικών από πλευράς των βασικών και σημαντικών οντοτήτων, αν και σε μεγάλο βαθμό συνιστά υποχρέωση των κρατών μελών, δεν επαφίεται αποκλειστικά σε αυτά. Αντίθετα, δίνεται η δυνατότητα στην Επιτροπή να εκδίδει εκτελεστικές πράξεις για τον περαιτέρω προσδιορισμό και την τυποποίηση ορισμένων στοιχείων της κοινοποίησης περιστατικών, όπως το είδος των πληροφοριών, ο μορφότυπος και η διαδικασία κοινοποίησης των περιστατικών. Μάλιστα σε ορισμένες περιπτώσεις[63], δίνεται η δυνατότητα στην Επιτροπή να εκδίδει ειδικότερες εκτελεστικές πράξεις για τον περαιτέρω προσδιορισμό των περιπτώσεων στις οποίες ένα περιστατικό θεωρείται σημαντικό.

2.3.2.6. Επιβολή κυρώσεων και προστίμων κατά μη συμμορφούμενων οντοτήτων

Κρίσιμο στοιχείο της παρούσας οδηγίας συνιστά η θέσπιση αυστηρών κυρώσεων και προστίμων για οντότητες που δεν συμμορφώνονται με τις διατάξεις της. Η θέσπιση κυρώσεων σε περιπτώσεις μη συμμόρφωσης, υπογραμμίζει τη δέσμευση της Ένωσης για ισχυρή παρουσία της σε ζητήματα προστασίας και αυστηροποίηση του μοντέλου ασφάλειας στον κυβερνοχώρο. Η NIS 2 εισάγει ένα σύστημα κυρώσεων δύο επιπέδων σε περιπτώσεις μη συμμόρφωσης, διακρίνοντας μεταξύ «ουσιωδών» και «σημαντικών» οντοτήτων.

Ως ουσιώδεις οντότητες, νοούνται οι ζωτικής σημασίας οντότητες για τομείς όπως οι μεταφορές, τα οικονομικά, η ενέργεια, το νερό, η υγεία, η δημόσια διοίκηση και οι ψηφιακές υποδομές. Όπως είναι αναμενόμενο, οι βασικές οντότητες αντιμετωπίζουν σημαντικά πρόστιμα. Οι κυρώσεις δύναται να φτάσουν έως και τα 10 εκατομμύρια ευρώ ή το 2% των παγκόσμιων ετήσιων εσόδων τους, όποιο είναι υψηλότερο. Αυτό αντανακλά την κρίσιμη φύση των υπηρεσιών τους και τον πιθανό αντίκτυπο των αποτυχιών τους στον κυβερνοχώρο σε ευρύτερη κλίμακα.

Οι σημαντικές οντότητες, αφορούν οντότητες με αντικείμενο ενασχόλησης σχετικό με τομείς όπως τα τρόφιμα, οι ψηφιακοί πάροχοι, τα χημικά προϊόντα, οι ταχυδρομικές υπηρεσίες, η διαχείριση απορριμμάτων και η έρευνα. Τα πρόστιμα για αυτές τις οντότητες

[63]βλ. αρ. 23 παρ. 11 του NISS II: Η δυνατότητα αυτή δίνεται αναφορικά με τους: «*Παρόχους υπηρεσιών DNS, τα μητρώα ονομάτων TLD, τους παρόχους υπηρεσιών υπολογιστικού νέφους, τους παρόχους υπηρεσιών κέντρων δεδομένων, τους παρόχους δικτύων διανομής περιεχομένου, τους παρόχους διαχειριζόμενων υπηρεσιών, τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας, καθώς και τους παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών υπηρεσιών κοινωνικής δικτύωσης*».

ορίζονται κατ' ανώτατο όριο στα 7 εκατ. ευρώ ή στο 1,4% των παγκόσμιων ετήσιων εσόδων τους, όποιο είναι μεγαλύτερο. Αν και είναι χαμηλότερα από εκείνα για βασικές οντότητες, αυτά τα πρόστιμα εξακολουθούν να αποτελούν σημαντικό αποτρεπτικό παράγοντα κατά της μη συμμόρφωσης εκ μέρους των εμπλεκομένων οντοτήτων.

Εκτός όμως από τις οικονομικές κυρώσεις, η NIS 2 προβλέπει και μη χρηματικά αποτρεπτικά μέτρα, ήτοι εντολές συμμόρφωσης, δεσμευτικές οδηγίες, εντολές εφαρμογής ελέγχου ασφαλείας και εντολές ειδοποίησης απειλών στους χρήστες των οντοτήτων. Για πρώτη φορά, μέσω της NIS 2 εισάγεται επίσης δυνατότητα προσωπικής λογοδοσίας προσώπων που ανήκουν στην ανώτατη διοίκηση των οντοτήτων. Συγκεκριμένα, δύναται σε περιπτώσεις βαριάς αμέλειας μετά από περιστατικό στον κυβερνοχώρο, να θεωρηθούν προσωπικά υπεύθυνοι οι διευθυντές, και να επιβληθούν εναντίον τους κυρώσεις. Μεταξύ των κυρώσεων περιλαμβάνονται η δημοσίευση των στοιχείων τους και, σε περιπτωση επανειλημμένων παραβιάσεων, προσωρινή απαγόρευση απασχόλησης σε διευθυντικές θέσεις[64].

2.3.2.7. Υποχρεώσεις εποπτείας και λογοδοσίας

Ένα κεντρικό στοιχείο που διαχωρίζει σε μεγάλο βαθμό την NIS 2 από άλλα κανονιστικά πλαίσια που αφορούν στην ενίσχυση ασφάλειας στον κυβερνοχώρο, είναι η ενσωμάτωση διαφόρων μέτρων εποπτείας και λογοδοσίας με σκοπό τη διασφάλιση της συμμόρφωσης των κρατών μελών και των οντοτήτων μεγάλης σημασίας.

Σε επίπεδο εθνικών εποπτικών αρχών, η NIS 2 θέτει υποχρέωση των κρατών μελών να ορίσουν εθνικές εποπτικές αρχές υπεύθυνες για την παρακολούθηση της εφαρμογής της Οδηγίας. Αυτές οι αρχές διαδραματίζουν κεντρικό ρόλο στη διασφάλιση της συμμόρφωσης, τη διενέργεια τακτικών ελέγχων και την αξιολόγηση των μέτρων κυβερνοασφάλειας των οντοτήτων.

Αναφορικά με τα μέτρα λογοδοσίας, είναι σημαντικό να σημειωθεί ότι η NIS 2 καθιστά την ανώτατη διοίκηση υπεύθυνη για τη διασφάλιση επαρκών μέτρων κυβερνοασφάλειας. Αυτό περιλαμβάνει υποχρεωτικές αξιολογήσεις κινδύνου και εφαρμογή στρατηγικών μετριασμού του κινδύνου. Για παράδειγμα, ένας πάροχος υγειονομικής περίθαλψης, ως βασική οντότητα, πρέπει να αποδείξει ότι υφίσταται εποπτεία της διοίκησης σε σχέση με την εφαρμογή αποτελεσματικών αμυντικών μέτρων για την ασφάλεια στον

[64] https://nis2directive.eu/nis2-fines/

κυβερνοχώρο, ειδικά σε ότι αφορά τα ευαίσθητα δεδομένα ασθενών[65]. Όπως μάλιστα έχει αναλυθεί ανωτέρω, σε περιπτώσεις βαριάς αμέλειας προβλέπεται και ενδεχόμενο κλήσης των ανώτατων στελεχών σε προσωπική λογοδοσία, ενώ σε κάποιες περιπτώσεις, για λόγους προστασίας των αποδεκτών και ενίσχυσης της διαφάνειας, επιτρέπεται η δημόσια αποκάλυψη περιστατικών μη συμμόρφωσης.

3. Στρατηγική και Διαμόρφωση Πολιτικής

Η σχέση μεταξύ διαμόρφωσης πολιτικής[66] και στρατηγικής έχει περίπλοκο και πολύπλευρο χαρακτήρα. Ως διαδικασίες, διαδραματίζουν αμφότερες κρίσιμους ρόλους στον σχεδιασμό και τη λήψη αποφάσεων των οργανισμών, των κυβερνήσεων και διαφόρων φορέων, χωρίς φυσικά η Ευρωπαϊκή Ένωση να αποτελεί εξαίρεση. Παρά το γεγονός ότι υπηρετούν διακριτούς στόχους και έχουν διαφορετική λειτουργία, συνδέονται μεταξύ τους αναπόσπαστα και συχνά αλληλοσυμπληρώνονται, διαμορφώνοντας σημαντικά η μια την πορεία της άλλης, μέσω της συνεχούς αλληλοτροφοδότησης πληροφοριών, εμπειριών και συμπερασμάτων τους. Κατά συνέπεια οι στρατηγικές πρωτοβουλίες μπορούν να ενημερώσουν και να οδηγήσουν σε προσαρμογές στις πολιτικές, ενώ αντίστοιχα, οι αλλαγές στις πολιτικές μπορεί να απαιτήσουν επανεκτίμηση και τροποποίηση των στρατηγικών.

Η διαμόρφωση στρατηγικής[67] έχει κατά κανόνα γενικότερο χαρακτήρα, καθώς σχεδιάζεται σε αδρές γραμμές για να μπορεί να εφαρμοστεί σε ένα ευρύ φάσμα καταστάσεων, μέσω της ανάπτυξης γενικών κατευθυντήριων γραμμών που σκοπούν στην σταδιακή διαμόρφωση πολιτικών. Η διαμόρφωση πολιτικών, έχει έναν πιο ειδικό χαρακτήρα, συνιστά μια διαδικασία επιλογής της βέλτιστης πορείας δράσης μέσω του καθορισμού συγκεκριμένων, μετρήσιμων στόχων και τον σχεδιασμό των απαραίτητων για την επίτευξη τους ενεργειών. Μέσω της διαμόρφωσης πολιτικής επιδιώκεται ο σχεδιασμός μιας πορείας που θα ακολουθηθεί προκειμένου να επιτευχθεί μια ορισμένη μελλοντική κατάσταση.

3.1. Διαμόρφωση πολιτικής

Η διαμόρφωση πολιτικής, όπως αναλύθηκε ανωτέρω, αναφέρεται στη διαδικασία

---

[65] T. V. Canneyt, L. Vanderdonckt, N. Shah, The NIS 2 Directive – implications for the healthcare sector and manufacturers of medical devices, Fieldfisker, March, 2023

[66] E. Araral, S. Fritzen, M. Howlett, M. Ramesh, X. Wu, *Routledge Handbook of Public Policy*, Routledge, London. 2012, σελ. 17

[67] Lawrence Freedman, *Strategy: A History,* Oxford University Press, 2016, σελ. 69

επιλογής της βέλτιστης πορείας δράσης μέσω του καθορισμού συγκεκριμένων, μετρήσιμων στόχων και τον σχεδιασμό των απαραίτητων για την επίτευξη τους ενεργειών για έναν συγκεκριμένο τομέα, όπως η ασφάλεια στον κυβερνοχώρο. Αυτή η διαδικασία συχνά περιλαμβάνει τον εντοπισμό ζητημάτων, τον καθορισμό στόχων και την ανάπτυξη ευρέων πλαισίων δράσης και συνεργασίας. Η πολιτική της Ένωσης για την ασφάλεια στον κυβερνοχώρο τα τελευταία χρόνια έχει διαμορφωθεί από τις αναδυόμενες ψηφιακές προκλήσεις και την ανάγκη για μια ενοποιημένη ευρωπαϊκή προσέγγιση. Αρχικά, δόθηκε έμφαση στην κατανόηση του τοπίου των απειλών στον κυβερνοχώρο και στην προώθηση της συνεργασίας μεταξύ των κρατών μελών. Σταδιακά, αυτό εξελίχθηκε σε πιο συγκεκριμένα πλαίσια πολιτικής, όπως η Στρατηγική της 'Ενωσης για την Κυβερνοασφάλεια το 2013, η οποία σκιαγράφησε μια συνολική προσέγγιση για την προστασία των ζωτικών υποδομών και τη βελτίωση της συνολικής ανθεκτικότητας στον κυβερνοχώρο.

Η ενωσιακή πολιτική διαμορφώνεται σταδιακά μέσα από μια σειρά παραγόντων, μεταξύ των οποίων και τα αποτελέσματα από τις αξιολογήσεις των φορέων και των εφαρμοζόμενων διαδικασιών. Ένα τέτοιο παράδειγμα αποτελεί η οδηγία NIS 2, η οποία προβλέπει την εφαρμογή πολιτικών και διαδικασιών αξιολόγησης της πραγματικής κατάστασης, δηλαδή του επιπέδου ασφαλείας σε συνάρτηση με τους υφιστάμενους κινδύνους, και της αποτελεσματικότητας των υφιστάμενων μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας, συνοδευόμενα συχνά από προτάσεις βελτίωσης τους. Στα πλαίσια αυτά, ανά δύο έτη εκδίδεται από τον ENISA, σε συνεργασία με την Επιτροπή και την Ομάδα Συνεργασίας, έκθεση σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση, η οποία υποβάλλεται και στην Επιτροπή. Αυτού του είδους η συλλογή και σύγκριση πληροφοριών και εμπειριών, σε συνδυασμό με τις γενικότερες γεωπολιτικές και οικονομικές εξελίξεις και τις εξελίξεις στον τομέα Τεχνολογίας Πληροφοριών και Επικοινωνίας, επηρεάζουν σε μεγάλο βαθμό στην διαμόρφωση της πολιτικής στον τομέα της Κυβερνοασφάλειας.

2.2. Η Ενωσιακή Στρατηγική για την Ασφάλεια στον Κυβερνοχώρο

Το ζήτημα του καθορισμού μιας ενιαίας ευρωπαϊκής στρατηγικής για την ενίσχυση της κυβερνοασφάλειας, μέχρι τις αρχές της προηγούμενης δεκαετίας δεν απασχολούσε ιδιαίτερα ως έννοια. Μέχρι το 2013 που εγκρίθηκε η Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο (EU Cyber Security Strategy - EUCSS), το όλο ζήτημα συνιστούσε μια υποενότητα του ευρύτερου πλαισίου της

ασφάλειας δικτύων και πληροφοριών[68]. Σε μεγάλο βαθμό, είχε απασχολήσει κυρίως ως μέσο για τη δημιουργία ενός ασφαλούς ψηφιακού περιβάλλοντος, με έμφαση στην προστασία των συστημάτων πληροφοριών και στη διασφάλιση του απορρήτου των δεδομένων, ιδιαίτερα μετά τη θέσπιση της Οδηγίας για την Προστασία Δεδομένων το 1995[69]. Στις αρχές της δεκαετίας του 2000, άρχισε να γίνεται αντιληπτή η σημασία της ενίσχυσης της ασφάλειας δικτύων και πληροφοριών σε επίπεδο Ένωσης. Για το λόγο αυτό στη συνέχεια εκδόθηκαν μια σειρά από οδηγίες και κανονισμούς με αντικείμενο την προστασία δεδομένων και την ασφάλεια των ηλεκτρονικών επικοινωνιών. Παρά το γεγονός ότι δημιουργήθηκε ο ENISA ήδη από το 2004, με περιορισμένες βέβαια τότε δυνατότητες και αρμοδιότητες, είναι σαφές ότι το ζήτημα της Κυβερνοασφάλειας απασχολούσε την Ένωση αποσπασματικά, και δεν υφίστατο κάποια συντονισμένη στρατηγική για την αντιμετώπιση των ψηφιακών απειλών.

Η επίσημη καθιέρωση της κυβερνοασφάλειας ως σημαίνοντα τομέα που χρήζει αυτοτελούς συστηματικής αντιμετώπισης σε ενωσιακό επίπεδο, μέσω της χάραξης στρατηγικής, επήλθε με τη δημοσίευση της Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο (EU Cyber Security Strategy - EUCSS) τον φεβρουάριο του 2013. Η πρώτη αυτή δημοσιευμένη Στρατηγική της Ευρωπαϊκής Ένωσης, το όραμα της οποίας καθρευτιζε ο ίδιος ο τίτλος της «*Ένας ανοιχτός, ασφαλής και προστατευμένος κυβερνοχώρος*», έθεσε τις βάσεις για μια συνολική ενωσιακή προσέγγιση στον τομέα ενίσχυσης της ασφάλειας στον κυβερνοχώρο, εστιάζοντας κατά κύριο λόγο στους βασικούς τομείς της επίτευξης ανθεκτικότητας στον κυβερνοχώρο, του περιορισμού εγκληματικής δράσης στον κυβερνοχώρο, την ανάπτυξη των αμυντικών δυνατοτήτων, την ανάπτυξη των βιομηχανικών και τεχνολογικών πόρων με στόχο την ενίσχυση της ασφάλειας στον κυβερνοχώρο, και τη θεμελίωση συνεκτικής ενωσιακής πολιτικής στους ανωτέρω τομείς. Η καθιέρωση της κυβερνοασφάλειας ως αυτοτελούς, επίσημου τομέα πολιτικής, αναμφίβολα σηματοδότησε την ανάγκη για συντονισμένη προσέγγιση της ψηφιακής ασφάλειας, μέσω της χάραξης στρατηγικής.

Η πρώτη αυτή ενωσιακή στρατηγική για την κυβερνοασφάλεια του 2013 άφησε το αποτύπωμά της στον τρόπο προσέγγισης της ψηφιακής ασφάλειας από πλευράς

[68] George Christou, *The EU's Approach to Cyber Security*, EUSC Policy paper series, 2014, σελ. 5
[69] βλ. Οδηγία 95/46/ΕΚ

Ευρωπαϊκής Ένωσης. Καθιέρωσε ένα ολοκληρωμένο πλαίσιο για την αντιμετώπιση των απειλών στον κυβερνοχώρο, τονίζοντας την ανάγκη για συνεργασία, ανθεκτικότητα και καινοτομία στην ασφάλεια στον κυβερνοχώρο. Η επιρροή της στρατηγικής επεκτάθηκε σε νομοθετικές εξελίξεις όπως η Οδηγία NIS και ο Γενικός Κανονισμός για την Προστασία Δεδομένων (General Data Protection Regulation - GDPR)[70], που τέθηκε σε εφαρμογή στις 25 Μαΐου 2018, σηματοδοτεί ένα ορόσημο στη σφαίρα της νομοθεσίας περί προστασίας δεδομένων και απορρήτου, ενισχύοντας τα πρότυπα κυβερνοασφάλειας και προστασίας δεδομένων σε όλα τα κράτη μέλη. Παράλληλα έθεσε τη βάση για την επίτευξη συνεργασίας μεταξύ δημόσιου και ιδιωτικού τομέα, αλλά και ενίσχυση της ενωσιακής και διεθνούς συνεργασίας, ενισχύοντας τη συνολική θέση της Ένωσης στον τομέα της κυβερνοασφάλειας σε ένα παγκόσμιο συνδεδεμένο ψηφιακό τοπίο.

Παρά το γεγονός ότι αποτέλεσε ένα κομβικό βήμα προς την κατεύθυνση ενοποιημένων προσπαθειών κυβερνοασφάλειας στην ΕΕ, αντιμετώπισε σημαντικές προκλήσεις. Η διακύμανση στην εφαρμογή του μεταξύ των κρατών μελών, λόγω των διαφορετικών επιπέδων ωριμότητας στον κυβερνοχώρο και της διαθεσιμότητας πόρων, οδήγησε στη δημιουργία ενός ενωσιακού ψηφιδωτού αποτελούμενο από διαφορετικές - και συχνά μη δεκτικές συνεργασίας - ρυθμίσεις και πρότυπα. Παράλληλα, οι ταχύτατες τεχνολογικές αλλαγές και οι συνεχώς αναδυόμενες απειλές στον κυβερνοχώρο, κατέστησαν αναγκαία την θέσπιση νέων στρατηγικών στόχων, προσαρμοσμένων στα νέα δεδομένα.

Τα ανωτέρω, σε συνδυασμό την συνεχώς αυξανόμενη σύνδεση κρίσιμων και βασικών υπηρεσιών του ιδιωτικού βίου και του κατασκευαστικού τομέα με τη λειτουργία του διαδικτύου, την αμφισβήτηση της ιδέας ενός ανοιχτού παγκόσμιου Διαδικτύου, και τη επικράτηση μιας λογικής ότι ο κυβερνοχώρος είναι ο τόπος ενός γεωπολιτικού διαγωνισμού και για το λόγο αυτό πρέπει να δομηθεί ένα διεθνές πλαίσιο καθορισμού κανόνων, έθεσαν την πρώτη βάση περί ανάγκης διαφοροποίησης της κατεύθυνσης. Με την εμπειρία της πανδημίας και την εξάρτηση - ή μάλλον την επιτάχυνση της εξάρτησης - που αυτή επέφερε από τα συστήματα Τεχνολογιών Πληροφορικής και Επικοινωνιών, οδήγησαν το 2020 σε πρόταση της Ευρωπαϊκής Επιτροπής και της Ύπατης Εκπροσώπου της Ένωσης για Θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας για μια νέα

[70] βλ. Κανονισμός 2016/679.

στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο, η οποία αφορά στην ενίσχυση του επιπέδου ασφαλείας αναφορικά με βασικές υπηρεσίες, όπως τα νοσοκομεία, τα ενεργειακά δίκτυα και οι σιδηρόδρομοι, καθώς και του αυξανόμενου αριθμού εξαρτώμενων από Τεχνολογίες Πληροφορικής και Επικοινωνιών οικιών, επαγγελματικών χώρων και σημείων παραγωγής.

Η στρατηγική αυτή[71] επιδιώκει την θεμελίωση ενός συστήματος αποτελεσματικής αξιοποίησης και ενίσχυσης των υπαρχόντων εργαλείων και τους πόρους που διαθέτει η Ένωση, προκειμένου να επιτευχθεί τεχνολογική κυριαρχία και στρατηγική αυτονομία, δίνοντας παράλληλα ιδιαίτερα μεγάλη βάση στην ενίσχυση της συνεργασίας της Ένωσης με εταίρους σε όλο τον κόσμο που συμμερίζονται τις αξίες μας για τη δημοκρατία, το κράτος δικαίου και τα ανθρώπινα δικαιώματα. Μάλιστα, η στρατηγική αυτονομία επιδιώκεται να θεμελιωθεί στην ανθεκτικότητα όλων των συνδεδεμένων υπηρεσιών και προϊόντων. Παράλληλα προβλέπεται στενότερη συνεργασία των τεσσάρων κυβερνοκοινοτήτων, ήτοι όσων συνδέονται με την εσωτερική αγορά, με την επιβολή του νόμου, τη διπλωματία και την άμυνα.

Στο επίκεντρο της νέας στρατηγικής βρίσκεται η οικοδόμηση συλλογικών ικανοτήτων για την αντιμετώπιση σημαντικών κυβερνοεπιθέσεων η ενίσχυση του στοιχείου της συνεργασίας για τη διασφάλιση της διεθνούς ασφάλειας και σταθερότητας στον κυβερνοχώρο. Προτείνεται μάλιστα και μια Κοινή Κυβερνομονάδα, με στόχο την συγκέντρωση πόρων και εμπειρογνωμοσύνης για την αποτελεσματική πρόληψη, αποτροπή και αντιμετώπιση μαζικών περιστατικών και κρίσεων στον κυβερνοχώρο. Μέσω της σύστασης μιας Κοινής Κυβερνομονάδας επιδιώκεται μια προσπάθεια συντονισμού μεμονωμένων δρώντων[72] που λειτουργούν αυτόνομα, και συχνά χωρίς συνεννόηση μεταξύ τους, προς μια κοινή κατεύθυνση αποτελεσματικότερης συνεργασίας. Η επίτευξη αυτής της αποτελεσματικότερης συνεργασίας επιδιώκεται μέσω της διάθεσης μιας εικονικής και φυσικής πλατφόρμας συνεργασίας, μέσω της οποίας τα αρμόδια θεσμικά και λοιπά όργανα και οι οργανισμοί της Ευρωπαϊκής Ένωσης μαζί με τα κράτη μέλη θα δημιουργήσουν σταδιακά μια ευρωπαϊκή πλατφόρμα

[71] Κοινή ανακοίνωση για τη Στρατηγική κυβερνοασφάλειας της ΕΕ για την Ψηφιακή Δεκαετία, 2020

[72] Σε αυτούς περιλαμβάνονται μεταξύ άλλων κοινότητες κυβερνοασφάλειας, συμπεριλαμβανομένων των μη στρατιωτικών κοινοτήτων, των κοινοτήτων επιβολής του νόμου, των διπλωματικών κοινοτήτων και των κοινοτήτων κυβερνοάμυνας, καθώς και οι εταίροι του ιδιωτικού τομέα, πολύ συχνά λειτουργούν χωρίς συνεννόηση μεταξύ τους. Με την Κοινή Κυβερνομονάδα,

αλληλεγγύης και αμοιβαίας συνδρομής για την αντιμετώπιση απειλών στρεφόμενων κατά βασικών οντοτήτων και κυβερνοεπιθέσεις μεγάλης κλίμακας[73].

Στις 18 Απριλίου 2023, η Ευρωπαϊκή Επιτροπή πρότεινε ένα νέο κανονιστικό πλαίσιο για την αλληλεγγύη στον κυβερνοχώρο, προκειμένου να ενισχυθούν η ετοιμότητα, ο εντοπισμός και η ικανότητα απόκρισης σε συμβάντα κυβερνοασφάλειας σε ολόκληρη την Ένωση. Η πρόταση περιλαμβάνει τη δημιουργία μιας Ευρωπαϊκής Ασπίδας Κυβερνοασφάλειας, αποτελούμενη από Επιχειρησιακά Κέντρα Ασφάλειας διασυνδεδεμένα σε ολόκληρη την Ένωση, καθώς και ενός ολοκληρωμένου Μηχανισμού Έκτακτης Ανάγκης για την Κυβερνοασφάλεια για τη ισχυροποίησης της θέσεις της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο .

Η Ευρωπαϊκή Ασπίδα Κυβερνοασφάλειας (European Cyber Shield) θα αποτελείται από Επιχειρησιακά Κέντρα Ασφάλειας (Security Operations Centers - SOC) σε ολόκληρη την ΕΕ, συγκεντρωμένα σε πλατφόρμες Υπηρεσιακών Κέντρων Ασφαλείας κρατών μελών, οι οποίες θα δημιουργηθούν με την υποστήριξη του Προγράμματος Ψηφιακής Ευρώπης (Digital Europe Programme - DEP) για να συμπληρώσουν την εθνική χρηματοδότηση. Μεταξύ των καθηκόντων της Ευρωπαϊκής Ασπίδας Κυβερνοασφάλειας συμπεριλαμβάνονται η βελτίωση του εντοπισμού, της ανάλυσης και της απάντησης σε απειλές στον κυβερνοχώρο. Προβλέπεται ότι τα Υπηρεσιακά Κέντρα Ασφαλείας θα χρησιμοποιούν προηγμένη τεχνολογία, μεταξύ των οποίων η Τεχνητή Νοημοσύνη (Artificial Intelligence - AI) και η ανάλυση δεδομένων, για τον εντοπισμό και την κοινή αποστολή ειδοποίησης αναφορικά με ενδεχόμενες με τέτοιες απειλές.

Ένα άλλο μεγάλο κεφάλαιο που εμπλέκεται με τη χάραξη της ενωσιακής στρατηγικής για την αντιμετώπιση των κυβερνοαπειλών είναι η στρατηγική για την αντιμετώπισή τους από το ΝΑΤΟ. Ο Ρωσο-ουκρανικός πόλεμος ενέτεινε την ανάγκη συνεργασίας προς επίτευξη αποτελεσματικής προστασίας από τις συνεχείς κυβερνοεπιθέσεις αυταρχικών κρατών, οι οποίες εντείνονται με την πόλωση και την αύξηση του ανταγωνισμού μεταξύ των δυνάμεων. Με αντικείμενο ακριβώς την εντατικοποίηση της συνεργασίας των δύο οργανισμών συναντήθηκαν στις αρχές του Σεπτέμβρη του 2023 ανώτατοι αξιωματούχοι τους. Η συνέργεια μεταξύ των στρατηγικών

[73] Ένωση Ελλήνων Νομικών, *Κυβερνοασφάλεια της ΕΕ: Η Επιτροπή προτείνει τη δημιουργία μιας Κοινής Κυβερνομονάδας*, e-Θέμις, Ιούνιος, 2023

προσεγγίσεων του ΝΑΤΟ και της Ένωσης για την ασφάλεια στον κυβερνοχώρο δεν είναι μόνο αντανάκλαση κοινών ανησυχιών αλλά και στρατηγική αναγκαιότητα για την αντιμετώπιση ψηφιακών απειλών που δεν γνωρίζουν σύνορα. Η συνεργασία των δύο οργανισμών δεν είναι ένα πρόσφατο φαινόμενο. Η συνεργασία τους στον τομέα της κυβερνοασφάλειας έχει σφραγιστεί από κοινές δηλώσεις ήδη από τα έτη 2016 και 2018. Στα πλαίσια της συνεργασίας τους λαμβάνει χώρα ανταλλαγή πληροφοριών, κοινές ασκήσεις και συντονισμένες απαντήσεις σε περιστατικά στον κυβερνοχώρο. Η δέσμευση δεν είναι μόνο στρατηγική αλλά και επιχειρησιακή, με το ΝΑΤΟ και την Ευρωπαϊκή Ένωση να συντονίζονται σε πραγματικό χρόνο για να ανταποκριθούν σε απειλές στον κυβερνοχώρο, αξιοποιώντας αμφότεροι τις δυνάμεις και τους πόρους του άλλου. Η σύγκλιση των στρατηγικών τους δεν αφορά μόνο την προστασία δικτύων και πληροφοριών, αντικατοπτρίζει και μια προσπάθεια διαφύλαξης των αξιών και των κοινωνικών κανόνων που εκπροσωπούν αυτοί οι οργανισμοί.

4. Ο Ελληνικός Μηχανισμός για την Κυβερνοασφάλεια

4.1. Το Ισχύον Κανονιστικό Πλαίσιο

Η διαμόρφωση του μηχανισμού Κυβερνοασφάλειας της Ελλάδας σε μεγάλο βαθμό έχει υφανθεί μέσα από μια σειρά νομοθετημάτων. Κεντρικό ρόλο διαδραματίζει μέχρι σήμερα ο νόμος 4577/2018, με τον οποίο ενσωματώθηκε στην ελληνική έννομη τάξη η Οδηγία NIS 1[74] σε συνδυασμό με την Υπουργική Απόφαση 1027/2019, η οποία εξειδίκευσε σειρά ζητημάτων εφαρμογής και διαδικασιών του Ν. 4577/2018. Η Οδηγία NIS 2 δεν έχει ακόμα ενσωματωθεί στην Ελλάδα. Η χώρα μας έχει καταληκτική ημερομηνία για την ενσωμάτωση την 17η Οκτώβρη του 2024. Τότε η εν λόγω οδηγία θα πρέπει να έχει υιοθετηθεί δια νόμου από τα κράτη μέλη της Ευρωπαϊκής Ένωσης, ενώ η εφαρμογή της και οι συνέπειες σε περίπτωση μη συμμόρφωσης έχουν σημείο εκκίνησης την επομένη, ήτοι την 18η Οκτωβριου του 2024[75].

Παράλληλα, σημαντικό εθνικό κανονιστικό όχημα για την Κυβερνοασφάλεια συνιστά ο Νόμος 4727/2020[76] για την Ψηφιακή Διακυβέρνηση, σκοπός του οποίου είναι

[74] L.Maglaras, G. Drivas, K. Noou, S. Rallis, NIS directive: The case of Greece, EAI Endorsed Transactions on Security and Safety, 2018

[75] https://www.itsecuritypro.gr/nis2-amp-industry-4-0-dyo-antirropes-dynameis-gia-to-ot-security/

[76] Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972 και άλλες διατάξεις

η ολοκληρωμένη ρύθμιση ζητημάτων που άπτονται της ψηφιακής διακυβέρνησης και ιδίως εκείνων που σχετίζονται με τη χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνίας (ΤΠΕ) από τους φορείς του δημόσιου τομέα για τις ανάγκες της λειτουργίας τους, καθώς και την υποστήριξη της άσκησης των αρμοδιοτήτων και των συναλλαγών τους με φυσικά ή νομικά πρόσωπα ή νομικές οντότητες[77]. Στον ανωτέρω νόμο προβλέπεται τόσο η αποτύπωση της ψηφιακής στρατηγικής στη Βίβλο Ψηφιακού Μετασχηματισμού[78], όσο και η ανάγκη εναρμόνισής της με τα έργα Τεχνολογιών Πληροφορικής και Επικοινωνίας (ΤΠΕ). Παράλληλα θεσπίζεται υποχρέωση κάθε Υπουργείου να ορίζει, με απόφαση του αρμοδίου Υπουργού, Υπηρεσία Ψηφιακής Διακυβέρνησης, οποιουδήποτε διοικητικού επιπέδου, με αποστολή τον συντονισμό όλων των δράσεων ψηφιακού μετασχηματισμού του Υπουργείου και των εποπτευόμενων από αυτό φορέων. Επίσης, καριερώθηκε προσωπικός αριθμός (Π.Α.) ως αριθμός υποχρεωτικής επαλήθευσης της ταυτότητας των φυσικών προσώπων στις συναλλαγές τους με τους φορείς του δημόσιου τομέα, και ρυθμίστηκε εξαντλητικά το ζήτημα

4.2. Η Εθνική Στρατηγική Κυβερνοασφάλειας για το 2020 – 2025

Τον Δεκέμβριο του 2020, εγκρίθηκε με Υπουργική Απόφαση η Εθνική Στρατηγική για την Κυβερνοασφάλεια για το 2020 – 2025[79], μέσω της οποίας διατυπώθηκε το όραμα για: «*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.*[80]»

Βασικοί άξονες της νέας στρατηγικής θεωρηθηκαν η οικοδόμηση ενός σύγχρονου ψηφιακού περιβάλλοντος που να επιτρέπει τη διαρκή εισροή και ανάπτυξη των νέων τεχνολογιών και καινοτομιών, καθώς και η επίτευξη ενός υψηλού επιπέδου

---

[77] Βλ. αρθρ. 1 παρ. 1. Ν. 4727/2020

[78] Η Βίβλος Ψηφιακού Μετασχηματισμού καθορίζει τις βασικές αρχές, το πλαίσιο και τις κατευθύνσεις για τον ψηφιακό μετασχηματισμό της χώρας, καθώς και τις ειδικότερες αρχές που διέπουν κάθε οριζόντια ή τομεακή πρωτοβουλία προς τον σκοπό αυτό και ενσωματώνει την καταγραφή όλων των σχετικών διαδικασιών και δράσεων που υλοποιούν τον ψηφιακό μετασχηματισμό

[79] https://www.cyberwiser.eu/greece-gr

[80] Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025

κυβερνοασφάλειας, που να καλύπτει όλο το φάσμα των πληροφοριακών υποδομών, εφαρμογών και υπηρεσιών, προσαρμοσμένο στις διαρκώς μεταβαλλόμενες προκλήσεις και απαιτήσεις του χώρου. Παρά τη σημασία της επίτευξης αποτελεσματικής προστασίας, η νέα στρατηγική δίνει έμφαση στην προστασία των θεμελιωδών δικαιωμάτων, τόσο σε επίπεδο προσωπικών δεδομένων, αλλά και σε επίπεδο διαφύλαξης της ιδιωτικότητας, ανάπτυξης της προσωπικότητας, και ισότητας στη συμμετοχή της ψηφιακής κοινωνίας. Τέλος, εντοπίζεται ως κεντρικό ζήτημα η ανάπτυξη κουλτούρας ασφαλούς χρήσης μέσα από την οικοδόμηση ψηφιακής παιδείας, προκειμένου να ενισχυθεί εκ θεμελίων η εμπιστοσύνη των αποδεκτών στην ψηφιακή διακυβέρνηση.

4.3. Οι κεντρικοί φορείς που εμπλέκονται στο ζήτημα της κυβερνοασφάλειας

Το εθνικό σχέδιο Κυβερνοάμυνας έχει δομηθεί πάνω σε τρεις κεντρικούς πυλώνες. Ο πρώτος πυλώνας αφορά την τοποθέτηση σε ρόλο στρατηγικού σχεδιασμού, συντονισμού και εποπτείας, της Εθνικής Αρχής Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης, ο δεύτερος την θέσπιση της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων της Ε.Υ.Π., ως εθνικό φορέα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων σε ενωσιακό επίπεδο, η οποία συνιστά το εθνικό CERT (Computer Emergency Response Team), και ο τρίτος την Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ ως αρμόδια αρχή προληπτικής και κατασταλτικής απόκρισης για περιστατικά που αφορούν κυβερνοασφάλεια (Computer Security Incident Response Team - CSIRT). Η τελευταία αναλαμβάνει τη διαχείριση περιστατικών σύμφωνα με ορισμένη διαδικασία και έχει ως κεντρική προτεραιότητα την προστασία των κρίσιμων για τη λειτουργία του κράτος φορέων. Αντίστοιχα κάθε κρίσιμος για τη λειτουργία του κράτους φορέας προβλέπεται να διαθέτει Ομάδα Προστασίας (Security Operations Center, SOC), προκειμένου να γίνονται αντιληπτές έγκαιρα και να αντιμετωπίζονται αποτελεσματικά οι κυβερνοαπειλές.

4.3.1. Η Εθνική Αρχή Κυβερνοασφάλειας (National Cybersecurity Authority)

Η Εθνική Αρχή Κυβερνοασφάλειας (National Cybersecurity Authority)[81], υπάγεται στο Υπουργείο Ψηφιακής Διακυβέρνησης[82]. Στα πλαίσια των αρμοδιοτήτων της η

[81] https://mindigital.gr/dioikisi/kyvernoasfaleia
[82] Greece Cyber Security Strategy, International Trade Administration U.S. Department of Commerce

ανωτέρω αρχή διαχειρίζεται την Εθνική Στρατηγική για την Κυβερνοασφάλεια, καθορίζει τις βασικές απαιτήσεις ασφάλειας που αποτελούν αναπόσπαστο μέρος κάθε έργου ΤΠΕ του δημοσίου και ενσωματώνονται σε αυτά από τη φάση της σχεδίασης, ως απαραίτητη προϋπόθεση των αρχών του ενιαίου σχεδιασμού και διαχειρίζεται το σχετικό θεσμικό πλαίσιο. Παράλληλα της έχει ανατεθεί η συλλογή πολιτικών ασφαλείας και τήρηση σχετικού μητρώου, η συλλογή και επεξεργασία σχεδίων αποκατάστασης και η επεξεργασία των πολιτικών και διαδικασιών ασφαλείας για την πρόληψη και αντιμετώπιση περιστατικών ασφαλείας. Στα πλαίσια επίτευξης των στρατηγικών στόχων που έχουν τεθεί από την Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025, Εθνική Αρχή Κυβερνοασφάλειας συνεργάζεται μεταξύ άλλων με τις αρμόδιες Ανεξάρτητες και Ρυθμιστικές Αρχές, συναφείς ακαδημαϊκούς φορείς, και με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών, με σκοπό την υιοθέτηση ενιαίων πολιτικών ασφαλείας στο πλαίσιο της δημόσιας διοίκησης. Για τους ίδιους λόγους αναπτύσσει σχέσεις συνεργασίας και με την Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων και με τα CSIRTs[83] που δραστηριοποιούνται στην Ελλάδα για θέματα που εμπίπτουν στην αρμοδιότητά της. Τέλος, δραστηριοποιείται στο πεδίο καλλιέργειας ψηφιακής παιδείας μέσω της προώθησης δράσεων εκπαίδευσης και ενημέρωσης του προσωπικού που διαχειρίζεται και υποστηρίζει κρίσιμα συστήματα και υποδομές του Δημοσίου.

4.3.2. Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT) (Ε.Υ.Π.)

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT - Computer Emergency Response Team), η οποία υπάγεται στη Διεύθυνση Κυβερνοχώρου της Εθνικής Υπηρεσίας Πληροφοριών (ΕΥΠ), είναι αρμόδια για την αντιμετώπιση και την προστασία κυρίως του Δημόσιου τομέα και των κρίσιμων υποδομών[84], όπου για την εκπλήρωση της αποστολής της, η ΕΥΠ ασκεί τις αρμοδιότητες της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων, η οποία μεριμνά για την πρόληψη και τη στατική και την ενεργητική αντιμετώπιση ηλεκτρονικών επιθέσεων κατά δικτύων επικοινωνιών, εγκαταστάσεων αποθήκευσης πληροφοριών και συστημάτων πληροφορικής. Αποστολή της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων η μέριμνα για πρόληψη, έγκαιρη προειδοποίηση και την αντιμετώπιση κυβερνοεπιθέσεων

[83] National Cyber Security Authority – Ministry of Digital Governance (NCSA)

[84] Όπως ορίζεται στην παρ. 8 του άρθρου 4 του ν. 3649/2008

εναντίον της κοινότητας αρμοδιότητάς της. Στην κοινότητα αρμοδιότητας της υπάγονται κυρίως οι δημόσιοι φορείς της χώρας που δεν εμπίπτουν στην αρμοδιότητα της Διεύθυνσης Κυβερνοάμυνας του ΓΕΕΘΑ (CSIRT), ήτοι υποστηρίζει πρωτευόντως την Προεδρία της Κυβέρνησης, τα Υπουργεία και τους εποπτευόμενους φορείς τους, με εξαίρεση το Υπουργείο Εθνικής Άμυνας.

4.3.3. Υπουργείο Ψηφιακής Διακυβέρνησης

Το Υπουργείο Ψηφιακής Διακυβέρνησης συντονίζει δραστηριότητες με άλλα υπουργεία, κυβερνητικούς οργανισμούς και φορείς για να εξασφαλίσει διαλειτουργικότητα σε διάφορα επίπεδα, όπως συσκευές, δίκτυα, αποθετήρια δεδομένων, υπηρεσίες και πολλά άλλα. Ο στόχος του υπουργείου είναι να συμβάλει στη δημιουργία της ψηφιακής αγοράς χωρίς αποκλεισμούς σε ενωσιακό επίπεδο.

4.3.4. Η Διεύθυνση Κυβερνοάμυνας (ΓΕΕΘΑ/ΔΙΚΕΚΥΒ)

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[85] και την επιχειρησιακή ολοκλήρωση. Αποστολή της ανωτέρω Υπηρεσίας συνιστά η μείωση του κινδύνου εθνικών προκλήσεων στον τομέα της ασφάλειας του κυβερνοχώρου και των επικοινωνιών.

4.3.5. Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος[86] της ΕΛ.ΑΣ, είναι αυτοτελής κεντρική Υπηρεσία που υπάγεται απευθείας στον Αρχηγό της Ελληνικής Αστυνομίας, και έχει ως αποστολή την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που λαμβάνουν χώρα στον Κυβερνοχώρο ή άλλα μέσα ηλεκτρονικής επικοινωνίας. Μεταξύ άλλων διαθέτει 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. Η Διεύθυνση Δίωξης Ηλεκτρονικού

[85] Με τον ν. 4577/2018 ενσωματώθηκε στην ελληνική έννομη τάξη η Οδηγία 1148/2016

[86] Η ίδρυση και η διάρθρωση της προβλέφθηκε με το π.δ. 178/2014 (Α’ 281)

Εγκλήματος, η οποία έχει κυρίως κατασταλτικές ή προανακριτικές αρμοδιότητες, συνεπικουρεί έμπρακτα το έργο των ανωτέρω αρχών, και ιδιαίτερα της Εθνικής Αρχής Κυβερνοασφάλειας και της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων.

4.3.6. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) αποτελεί μια 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[87]. Στα πλαίσια άσκησης των αρμοδιοτήτων που της ανατίθενται, η Α.Π.Δ.Π.Χ. είναι επιφορτισμένη με την παρακολούθηση της εφαρμογής των διατάξεων του Κανονισμού 679/2016, γνωστός και ως Γενικός Κανονισμός Προστασίας Δεδομένων, 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. Μέσα από τη συνεργασία που αναπτύσει με τα κράτη μέλη και την Επιτροπή, συμβάλλει στη συνεκτική εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων[88] σε ολόκληρη την Ένωση.

Στα πλαίσια των αρμοδιοτήτων της[89] και προς επίτευξη των ανωτέρω στόχων, έχει ανατεθεί στην Α.Π.Δ.Π.Χ., η παρακολούθηση για την ορθότητα της εφαρμογής και επιβολή του Γενικού Κανονισμού Προστασίας Δεδομένων, η προώθηση δράσεων για ευαισθητοποίηση του κοινού στα ζητήματα προστασίας προσωπικών δεδομένων. Ειδική μέριμνα αναπτύσσεται προς πληροφόρηση όσων εκτελούν επεξεργασία προσωπικών δεδομένων αναφορικά με το εύρος των υποχρεώσεών τους δυνάμει του Γενικού Κανονισμού Προστασίας Δεδομένων, με αυξημένη προσοχή αναφορικά με δραστηριότητες που απευθύνονται ειδικά σε παιδιά. Παράλληλα συμβουλεύει το εθνικό κοινοβούλιο, την κυβέρνηση και άλλα όργανα και οργανισμούς για νομοθετικά και διοικητικά μέτρα που σχετίζονται με την προστασία των προσωπικών δεδομένων, ενώ κατόπιν αιτήματος παρέχει πληροφορίες και στα υποκείμενα των δεδομένων σχετικά με την άσκηση των δικαιωμάτων τους. Ειδικότερα σε επίπεδο εποπτείας διενεργεί έρευνες

[87] https://www.dpa.gr/
[88] βλ. αρθρ. 51 παρ. 2 του Κανονισμού 679/2016
[89] https://www.dpa.gr/el/arxi/armodiotites

σχετικά με την εφαρμογή του ανωτέρω κανονισμού, χειρίζεται τις υποβληθείσες για παράβαση των διατάξεων του καταγγελίες, και διαθέτει διορθωτικές, συμβουλευτικές και αδειοδοτικές εξουσίες και εξουσίες ελέγχου. Παράλληλα έχει αναπτύξει ένα διευρυμένο επίπεδο συνεργασίας με άλλες εποπτικές αρχές μέσω ανταλλαγής πληροφοριών και παροχής αμοιβαίας συνδρομής, ενώ συμβάλλει και στις δραστηριότητες του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων[90].

4.3.7. Η Εθνική Επιτροπή Τηλεπικοινωνικών και Ταχυδρομείων (Ε.Ε.Τ.Τ.)

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) είναι Ανεξάρτητη Διοικητική Αρχή. Αποτελεί τον Εθνικό Ρυθμιστή με αντικείμενο τη ρύθμιση, την εποπτεία και τον έλεγχο της αγοράς ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρείες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου και την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρείες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς.

Έχει τεθεί σε εφαρμογή η Πράξη, «Η Οργανωτική και Λειτουργική Προσαρμογή της ΕΕΤΤ στις νέες εξελίξεις και απαιτήσεις των αγορών ηλεκτρονικών επικοινωνιών και ταχυδρομικών υπηρεσιών - (ΟΛΠ)»[91], στα πλαίσια του οποίου υλοποιείται ένα υποέργο επιχειρησιακού και οργανωτικού ανασχεδιασμού της Ε.Ε.Τ.Τ. , με σκοπό την μετάβασή της σε ένα σύγχρονο μοντέλο διοικητικών και οργανωτικών δομών που θα ανταποκρίνεται στις απαιτητικές ανάγκες των αγορών ηλεκτρονικών επικοινωνιών και ταχυδρομικών υπηρεσιών.

4.3.8. Η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (Α.Δ.Α.Ε.)

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.)[92], είναι Ανεξάρτητη Αρχή που απολαύει διοικητικής αυτοτέλειας, η οποία υπόκειται σε κοινοβουλευτικό έλεγχο κατά τον τρόπο και τη διαδικασία που κάθε φορά προβλέπεται από τον Κανονισμό της Βουλής. Αποστολή της είναι η προστασία του απορρήτου των επιστολών, η ελεύθερη ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο

---

[90] Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ)

[91] https://www.eett.gr/eett/praxeis-sygchrimatodotoymenes-apo-tin-eyropaiki-enosi/organotiki-kai-leitoyrgiki-prosarmogi-tis-eett-stis-nees-exelixeis-kai-apaitiseis-ton-agoron-ilektronikon-epikoinonion-kai-tachydromikon-ypiresion/

[92] http://www.adae.gr/i-adae/paroysiasi/

καθώς και η ασφάλεια των δικτύων και πληροφοριών.

Στα πλαίσια των αρμοδιοτήτων της, η Α.Δ.Α.Ε. διενεργεί τακτικούς και έκτακτους ελέγχους σε εγκαταστάσεις δημόσιων υπηρεσιών ή και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες, προκειμένου να διασφαλίζεται ότι τηρούνται οι διατάξεις περί άρσης απορρήτου. Προβλέπεται μάλιστα η δυνατότητα επιβολής διοικητικών κυρώσεων, σε περίπτωση που διαπιστώνεται παραβίαση της κείμενης νομοθεσίας περί απορρήτου των επικοινωνιών.

4.3.9. Το Κέντρο Μελετών Ασφαλείας Κ.Ε.Μ.Ε.Α.

Το ΚΕ.ΜΕ.Α. συνιστά έναν επιστημονικό, ερευνητικό και συμβουλευτικό φορέα 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. Η συμβολή του ΚΕ.ΜΕ.Α στο ζήτημα της Κυβερνοασφάλειας πραγματοποιείται μέσω της δημιουργίας και λειτουργίας ενωσιακών, κατά βάση, ερευνητικών προγραμμάτων με αντικείμενο την ενίσχυση του επιπέδου ασφάλειας στον Κυβερνοχώρο. Ένα από τα πιο σημαντικά ερευνητικά προγράμματα αυτού του τύπου που βρίσκονται αυτή τη στιγμή σε λειτουργία είναι το πρόγραμμα Cyber-Trust, το οποίο στοχεύει στην ανάπτυξη μιας καινοτόμου συστήματος συλλογής και ανίχνευσης απειλών στον κυβερνοχώρο, καθώς και ενός συστήματος διεξαγωγής διεπιστημονικής έρευνας υψηλής ποιότητας σε βασικούς τομείς, με απώτερο σκοπό την αντιμετώπιση των μεγάλων ψηφιακών προκλήσεων.

5. Συμπέρασμα

Καθώς οι κοινωνίες διαπλέκονται όλο και περισσότερο με τον κυβερνοχώρο, αντιμετωπίζουν μια διπλή πραγματικότητα: ενώ η ψηφιακή ολοκλήρωση προσφέρει πρωτοφανή αποτελεσματικότητα και συνδεσιμότητα, η εξάρτησή τους από τον κυβερνοχώρο τις εκθέτει ταυτόχρονα σε ποικίλες και πολύπλοκες απειλές. Με αυτό τον τρόπο καθίσταται όλο και πιο επείγουσα η ανάγκη για προηγμένες, προσαρμόσιμες και προληπτικές στρατηγικές ασφάλειας στον κυβερνοχώρο.

Η λεπτομερής διερεύνηση από τη μελέτη σημαντικών του ενωσιακού κανονιστικού πλαισίου, βασικούς πυλώνες του οποίου συνιστούν ο κανονισμός 881/2019 και οι οδηγίες

NIS 1 και NIS 2, υπογραμμίζει τη δέσμευση της Ένωσης για μια συνεκτική και ενισχυμένη στρατηγική ψηφιακής ασφάλειας. Η ενδυνάμωση του ENISA και η σύσταση Εθνικών Αρχών Πιστοποίησης Κυβερνοασφάλειας (NCCA) είναι καθοριστικά βήματα προς την ενίσχυση της εμπιστοσύνης του κοινού στην ψηφιακή αγορά και την ενίσχυση της ανθεκτικότητας των υποδομών στον κυβερνοχώρο. Στην Ελλάδα, η προσαρμογή αυτών των οδηγιών διαμορφώνει το τοπίο της κυβερνοασφάλειας, αντικατοπτρίζοντας την περίπλοκη ισορροπία μεταξύ της ευθυγράμμισης με ευρύτερες ενωσιακές στρατηγικές και της αντιμετώπισης των ιδιαιτεροτήτων των εθνικών απαιτήσεων.

Μελετώντας την πορεία της διαμόρφωσης ενωσιακής πολιτικής και των αναπροσαρμογών της στρατηγικής, αναδεικνύεται έντονα η ανάγκη και τάση για ανάπτυξη συνεργασιών της Ένωσης με όλων των ειδών τους φορείς, με τους οποίους μοιράζεται ίδιες αξίες και αρχές ή με όσους διαπλέκεται για σκοπούς εμπορικούς, οικονομικούς ή και άλλους. Χαρακτηριστικό παράδειγμα αυτής της τάσης συνιστά η ανάπτυξη συνεργασίας σε επιχειρησιακό και στρατηγικό επίπεδο μεταξύ των πλαισίων πολιτικής της Ένωσης και της ομάδας κυβερνοασφάλειας του ΝΑΤΟ, το οποίο προσφέρει μια ισχυρή πλατφόρμα για την αντιμετώπιση των απειλών στον κυβερνοχώρο, αξιοποιώντας κοινή τεχνογνωσία και πόρους. Αυτή η συνεργασία δεν είναι μόνο καίριας σημασίας για την ενίσχυση των μέτρων κυβερνοασφάλειας αλλά και για την ενίσχυση μιας ενιαίας στάσης έναντι των απειλών στον κυβερνοχώρο.

Κοιτάζοντας πέρα από την Ευρωπαϊκή Ένωση, η προοπτική συνεργασίας με τις Ηνωμένες Πολιτείες στον τομέα της κυβερνοασφάλειας θα μπορούσε να αναδειχθεί ως μια πιθανή στρατηγική συμμαχία. Μια τέτοια συνεργασία θα μπορούσε να προσφέρει αμοιβαία οφέλη, συνδυάζοντας τα δυνατά σημεία των κανονιστικών πλαισίων της Ένωσης με την τεχνολογική ικανότητα των ΗΠΑ, διευκολύνοντας κατ΄αυτό τον τρόπο την ανάπτυξη πιο εξελιγμένων λύσεων στον κυβερνοχώρο και την ενίσχυση της ανθεκτικότητας της άμυνας έναντι των παγκόσμιων απειλών στον κυβερνοχώρο. Όλα αυτά υπό το πρίσμα ενός μεταβαλλόμενου κυβερνοχώρου, με αδυναμία υπολογισμού της τρέχουσας αποτελεσματικότητας των στρατηγικών κυβερνοασφάλειας, η οποία έγκειται στην αδιάκοπη εξέλιξη των τεχνολογιών, όπως η τεχνολογία της τεχνητής νοημοσύνης (AI), και των απειλών που αυτές συνεπιφέρουν, ορισμένες από τις οποίες ενδεχομένως ξεπερνούν τη σφαίρα της επιστημονικής φαντασίας.

Βιβλιογραφία

E. Araral, S. Fritzen, M. Howlett, M. Ramesh, X. Wu, *Routledge Handbook of Public Policy*, Routledge, London. 2012

F. Allhoff, A. Henschke, B.J. Strawser, *Binary Bullets: The Ethics of Cyberwarfare*, Oxford University Press, 2016, σελ. 89

George Christou, *The EU's Approach to Cyber Security*, EUSC Policy paper series, 2014

Lawrence Freedman, *Strategy: A History,* Oxford University Press, 2016

Research Division NATO Defence College, *Strategic Shifts and NATO's New Strategic Concept*, Rome

Robert McMill, Siemens: Stuxnet worm hit industrial systems, 2010

Schwab, K. (2016). "The Fourth Industrial Revolution." World Economic Forum

Αρθρογραφία

Ένωση Ελλήνων Νομικών, Κυβερνοασφάλεια της ΕΕ: Η Επιτροπή προτείνει τη δημιουργία μιας Κοινής Κυβερνομονάδας, e-Θέμις, Ιούνιος, 2023

Amy Novak, *Virtual Poltergeists and Memory: The Question of Ahistorcism in William Gibson's Neuromoncer(1984)*, Journal of the Fantastic in the Arts Vol. 11, No. 4 (44),2001

L.Maglaras, G. Drivas, K. Noou, S. Rallis, NIS directive: The case of Greece, EAI Endorsed Transactions on Security and Safety, 2018

Richard Bejtlich, Don't Underestimate Cyber Spies, Foreign Affairs, 2013

T. V. Canneyt, L. Vanderdonckt, N. Shah, The NIS 2 Directive – implications for the healthcare sector and manufacturers of medical devices, Fieldfisker, March, 2023

Ενωσιακό Κανονιστικό Πλαίσιο

Οδηγία 2002/21/ΕΚ, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία πλαίσιο)

Κανονισμός (ΕΚ) αριθ. 460/2004, της 10ης Μαρτίου 2004, για τη δημιουργία του οργανισμού για την ασφάλεια Δικτύων και Πληροφοριών

Κανονισμός (ΕΕ) αριθ. 910/2014, της 23ης Ιουλίου 2014, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ

Κανονισμός (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών

Οδηγία (ΕΕ) 2016/1148, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση

Οδηγία (ΕΕ) 2018/1972 της 11ης Δεκεμβρίου 2018 για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών

Κανονισμός (ΕΕ) 2019/881, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια)

Κανονισμός (ΕΕ) 2022/2554 «σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα» ('DORA')

Οδηγία (ΕΕ) 2022/2555, της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2)

Οδηγία (ΕΕ) 2022/2557 της 14ης Δεκεμβρίου 2022 για την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ του Συμβουλίου

Άλλα Επίσημα Κείμενα της Ένωσης

Στρατηγική για ασφαλή κοινωνία της πληροφορίας – «διάλογος, πνεύμα συνεργασίας και ενίσχυση των ικανοτήτων» {SEC(2006) 656}

Έκθεση σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορά τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)) (COM(2010)0521 – C7-0302/2010 – 2010/0275(COD)) Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας Εισηγητής: Giles Chichester

Κοινή ανακοίνωση για τη Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο, 2013

Κοινή ανακοίνωση για τη Στρατηγική κυβερνοασφάλειας της ΕΕ για την Ψηφιακή Δεκαετία, 2020

Διαδικτυακοί Σύνδεσμοι

Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025
https://mindigital.gr/wp-content/uploads/2020/12/%CE%95%CE%98%CE%9D%CE%99%CE%9A%CE%97-%CE%A3%CE%A4%CE%A1%CE%91%CE%A4%CE%97%CE%93%CE%99%CE%9A%CE%97-%CE%9A%CE%A5%CE%92%CE%95%CE%A1%CE%9D%CE%9F%CE%91%CE%A3%CE%A6%CE%91%CE%9B%CE%95%CE%99%CE%91%CE%A3-2020-2025.pdf

Ένωση Ελλήνων Νομικών, Κυβερνοασφάλεια της ΕΕ: Η Επιτροπή προτείνει τη δημιουργία μιας Κοινής Κυβερνομονάδας, e-Θέμις, Ιούνιος, 2023
https://www.ethemis.gr/2021/06/24/%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1-%CF%84%CE%B7%CF%82-%CE%B5%CE%B5-%CE%B7-%CE%B5%CF%80%CE%B9%CF%84%CF%81%CE%BF%CF%80%CE%AE-%CF%80%CF%81%CE%BF%CF%84%CE%B5%CE%AF%CE%BD%CE%B5%CE%B9-%CF%84%CE%B7-%CE%B4%CE%B7%CE%BC%CE%B9%CE%BF%CF%85%CF%81%CE%B3%CE%AF%CE%B1-%CE%BC%CE%B9%CE%B1%CF%82-%CE%BA%CE%BF%CE%B9%CE%BD%CE%AE%CF%82-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%BC%CE%BF%CE%BD%CE%AC%CE%B4%CE%B1%CF%82.html

Εθνική Αρχή Κυβερνοασφάλειας
https://mindigital.gr/dioikisi/kyvernoasfaleia

Εθνική Αρχή Κυβερνοασφάλειας – Υπουργείο Ψηφιακής Διακυβέρνησης (NCSA)
https://www.concordia-h2020.eu/consortium/national-cyber-authority-ncsa/

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ)
https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board-edpb_el

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.)
https://www.dpa.gr/
https://www.dpa.gr/el/arxi/armodiotites

Η επίδραση της Οδηγίας NIS2 σε φορείς που σχετίζονται με τον τομέα της υγείας
https://nis2directive.eu/health/

Η Οργανωτική και Λειτουργική Προσαρμογή της ΕΕΤΤ στις νέες εξελίξεις και απαιτήσεις

των αγορών ηλεκτρονικών επικοινωνιών και ταχυδρομικών υπηρεσιών - (ΟΛΠ
https://www.eett.gr/eett/praxeis-sygchrimatodotoymenes-apo-tin-eyropaiki-enosi/organotiki-kai-leitoyrgiki-prosarmogi-tis-eett-stis-nees-exelixeis-kai-apaitiseis-ton-agoron-ilektronikon-epikoinonion-kai-tachydromikon-ypiresion/

Κυρώσεις της NIS 2 σε περιπτώσεις μη συμμόρφωσης
https://nis2directive.eu/nis2-fines/

NIS2 & Industry 4.0: Δύο αντίρροπες δυνάμεις για το OT Security
https://www.itsecuritypro.gr/nis2-amp-industry-4-0-dyo-antirropes-dynameis-gia-to-ot-security/

Στρατηγική για την κυβερνοασφάλεια 2006
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF

Τεχνολογίες Πληροφορικής & Επικοινωνιών (ΤΠΕ)
https://learningportal.iiep.unesco.org/en/glossary/information-and-communication-technologies-ict

Ψηφιακή ενιαία αγορά
https://www.europarl.europa.eu/factsheets/el/sheet/43/%CE%B7-%CF%80%CE%B1%CE%BD%CF%84%CE%B1%CF%87%CE%BF%CF%85-%CF%80%CE%B1%CF%81%CE%BF%CF%85%CF%83%CE%B1-%CF%88%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%B7-%CE%B5%CE%BD%CE%B9%CE%B1%CE%B9%CE%B1-%CE%B1%CE%B3%CE%BF%CF%81%CE%B1

Cyberwiser eu, Greece
https://www.cyberwiser.eu/greece-gr

Defense Threat Reduction Agency
https://www.dtra.mil/

Greece Cyber Security Strategy, International Trade Administration U.S. Department of Commerce
https://www.trade.gov/market-intelligence/greece-cyber-security-strategy

Jason N. Smolanoff, Live from Davos – Cyber in 2023: Geopolitical and Economic Risks, January, 2023

https://www.kroll.com/en/insights/publications/cyber/2023-geopolitical-and-economic-risks-davos

National Cyber Security Authority – Ministry of Digital Governance (NCSA)
https://www.concordia-h2020.eu/consortium/national-cyber-authority-ncsa/

Preparing for the NIS 2 Directive: Impacts on the health sector
https://setterwalls.se/artikel/preparing-for-the-nis-2-directive-impacts-on-the-health-sector/

Robert McMill, Siemens: Stuxnet worm hit industrial systems, 2010
https://www.computerworld.com/article/2515570/siemens--stuxnet-worm-hit-industrial-systems.html

T. V. Canneyt, L. Vanderdonckt, N. Shah, The NIS 2 Directive – implications for the healthcare sector and manufacturers of medical devices, Fieldfisker, March, 2023
https://www.fieldfisher.com/en/insights/the-nis-2-directive-implications-for-the-healthcare-sector-and-manufacturers-of-medical-devices