ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ & ΕΠΙΚΟΙΝΩΝΙΩΝ

Στρατηγική της Κυβερνοασφάλειας στην ΕΕ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Δήμητρας Μπρεχού

Επιβλέπουσα Καθηγήτρια : Μήτρου Λίλιαν

Μέλη εξεταστικής επιτροπής:

Αθήνα, Ιούνιος 2022

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Ολοκληρώνοντας την παρούσα Διπλωματική Εργασία, θα ήθελα να ευχαριστήσω θερμά την κα Λίλιαν Μήτρου, επιβλέπουσα καθηγήτρια, για την καθοδήγηση και την πολύτιμη βοήθεια της.

Επίσης, ευχαριστώ όλους όσους με βοήθησαν, με τον τρόπο τους και τις ιδέες τους στην ολοκλήρωση αυτής της Διπλωματικής.

Και φυσικά, θα ήθελα να ευχαριστήσω την οικογένειά μου και κυρίως τον σύζυγό μου για την υπομονή και την στήριξη του σε όλη την προσπάθεια μου.

Δήμητρας Μπρεχού
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Περιεχόμενα

Λίστα Σχημάτων

Ακρωνύμια

ΑΔΑΕ	Αρχή Διασφάλισης Απορρήτου Επικοινωνιών
ΑΔΠ	Ασφάλεια Δικτύων και Πληροφοριών
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
ΔΔΑ	Διεύθυνση Δημόσιας Ασφάλειας
ΔΔΑΣ	Διεύθυνση Διεθνούς Αστυνομικής Συνεργασίας
ΔΙΔΗΕ	Διεύθυνση Δίωξης Οικονομικού Εγκλήματος
ΕΕ	Ευρωπαϊκή Ένωση
ΕΕΕΠ	Επιτροπή Εποπτείας & Ελέγχου Παιγνίων
ΕΕΤΤ	Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
ΚΠΣ	Κεντρικό Πληροφορικό Σύστημα
ΟΠΙ	Οργανισμός Πνευματικής Ιδιοκτησίας
ΤΠΕ	Τεχνολογίες Πληροφοριών & Επικοινωνιών

Περίληψη

Ελλάδα 2022: Ζούμε σε μια εποχή στην οποία είμαστε πιο εξαρτημένοι ηλεκτρονικά από κάθε άλλη φορά.

Όλα γύρω μας έχουν σχεδιαστεί με τρόπο που μας επιτρέπει να εκπαιδευόμαστε, να εργαζόμαστε, να ενημερωνόμαστε, να κάνουμε αγορές και να επικοινωνούμε ηλεκτρονικά. Το γεγονός αυτό, εκτός από τα θετικά και τα αρνητικά που περιλαμβάνει, διατρέχει και έναν πολύ σοβαρό κίνδυνο: τον κίνδυνο της κυβερνοεπίθεσης, η οποία μπορεί να συμβεί όπου υπάρχει διασύνδεση, οποιαδήποτε στιγμή.

Η παρούσα Διπλωματική Εργασία επιχειρεί να αναλύσει την κατάσταση που επικρατεί στον κυβερνοχώρο, να παρουσιάσει όλες τις στρατηγικές κυβερνοασφάλειας που έχουν υιοθετηθεί από την Ευρωπαϊκή Ένωση και να προτείνει τρόπους ενίσχυσης της κυβερνοασφάλειας για την αντιμετώπιση των επιθέσεων αυτών.

Λέξεις Κλειδιά: *κυβερνοασφάλεια, κυβερνοεπίθεση, κυβερνοαπειλή, κυβερνοάμυνα*

Abstract

Greece 2022: We live in an era in which we are more electronically dependent than ever.

Everything around us is designed in a way that allows us to be educated, to work, to be informed, to shop and to communicate electronically. This fact, apart from its advantages and disadvantages, entails a very serious risk: the risk of cyber-attack, which can occur where there is an interconnection, at any time.

This Thesis attempts to analyze the situation in cyberspace, to present all the strategic cybersecurity adopted by the European Union and suggest ways in order to deal with these attacks.

Keywords: *cyber security, cyber-attack, cyber threat, cyber defense*

1

Εισαγωγή

1.1 Αναγνώριση κυβερνοαπειλής

Διανύουμε την τρίτη δεκαετία του 21ου αιώνα και βλέπουμε καθημερινά ότι οι αλλαγές στον τρόπο που ζούμε είναι καταιγιστικές. Τέταρτη βιομηχανική επανάσταση, διαδίκτυο των πραγμάτων, υπολογιστικό νέφος, τεχνητή νοημοσύνη και μηχανική μάθηση, είναι μόνο μερικές από τις τεχνολογίες που έχουν έρθει για να αλλάξουν μόνιμα τον τρόπο τόσο της προσωπικής, όσο και της επαγγελματικής μας ζωής.

Οι δικτυακές υποδομές εξελίσσονται για να είναι σε θέση να υποστηρίξουν αυτή τη νέα τάξη πραγμάτων. Μαζί με αυτές εξελίσσονται και οι απειλές τις οποίες έχουμε να αντιμετωπίσουμε. Η παραδοσιακή προσέγγιση της ασφάλειας δεν είναι πλέον αρκετή.

Ένα πολύ σημαντικό χαρακτηριστικό του εγκλήματος είναι να μπορούμε να αναγνωρίζουμε την απειλή. Στον κυβερνοχώρο αυτό δεν συμβαίνει. Δεν γνωρίζουμε αν απειλείται ο υπολογιστής, από τι απειλείται και πόσες επιθέσεις δέχεται ανά δευτερόλεπτο. Επομένως, για να μπορούμε να προσπεράσουμε αυτές τις απειλές, μπορούμε να χρησιμοποιήσουμε νέες τεχνολογίες, όπως είναι η τεχνητή νοημοσύνη, το machine learning και άλλες διαδικασίες, όπου η μηχανή σκέφτεται πλέον πολύ πιο γρήγορα με ανθρώπινη «διάσταση», δηλαδή να μπορεί να αντιληφθεί τι είναι αυτό που ανιχνεύει και να το αντιμετωπίσει. Το πιο σημαντικό, όμως, είναι η ανάγκη για διαρκή εκπαίδευση και μετεκπαίδευση όλων των χρηστών. Πρέπει να επενδύσουμε στο ανθρώπινο δυναμικό. Στην αλυσίδα της ασφάλειας, ο ανθρώπινος παράγοντας είναι ο πιο σημαντικός κρίκος.

1.2 Αντικείμενο διπλωματικής-

Στο πλαίσιο ανάπτυξης της παρούσας διπλωματικής εργασίας επεξηγούνται οι έννοιες του κυβερνοεγκλήματος και της κυβερνοασφάλειας και παρουσιάζονται οι αρμόδιες Αρχές, Φορείς και Οργανισμοί και οι αρμοδιότητες τους.

Αναλύονται εκτενώς οι κατηγορίες και οι παράγοντες απειλών, και τονίζεται η ανάγκη για ενίσχυση των υποδομών ασφάλειας των Οργανισμών, παράλληλα με τη συνεχή εκπαίδευση των χρηστών.

Παρουσιάζονται σημαντικά γεγονότα που αποτελούν σταθμούς για το έργο και τις ενέργειες της Ευρωπαϊκής Επιτροπής σχετικά με την Ασφάλεια στον Κυβερνοχώρο, στις Διατάξεις και Ανακοινώσεις της ΕΕ σχετικά με τις στρατηγικές κυβερνοασφάλειας.

1.3 Δομή της διπλωματικής

Η διπλωματική εργασία αποτελείται από έξι κεφάλαια. Στο 1ο Κεφάλαιο γίνεται μία σύντομη εισαγωγή για το αντικείμενο της διπλωματικής εργασίας και για τον στόχο της. Στο Κεφάλαιο 2 αναλύεται η παρούσα κατάσταση και παρουσιάζονται οι βασικές έννοιες του κυβερνοεγκλήματος και της κυβερνοασφάλειας. Στο Κεφάλαιο 3 περιγράφονται οι κυριότερες κατηγορίες απειλών και οι παράγοντες απειλών. Το Κεφάλαιο 4 παρουσιάζει τις πιο σημαντικές Διατάξεις/Ανακοινώσεις της ΕΕ σχετικά με την στρατηγικές κυβερνοασφάλειας. Στο Κεφάλαιο 5 παρουσιάζονται οι Αρμόδιες Αρχές, Φορείς και Οργανισμοί στην ΕΕ και στην Ελλάδα. Τέλος, στο Κεφάλαιο 6 παρατίθενται σύντομα συμπεράσματα, καθώς και προτάσεις βελτίωσης της κυβερνοασφάλειας.

2

Ανάλυση Κατάστασης

2.1 Ορισμοί

2.1.1 Κυβερνοέγκλημα -Cybercrime – Τι είναι το Κυβερνοέγκλημα?

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής και η ευρύτατη χρήση του Διαδικτύου έχουν επιφέρει επαναστατικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων, στην παραγωγική διαδικασία, στις συναλλαγές, στην εκπαίδευση, στη διασκέδαση, ακόμα και στον τρόπο σκέψης του σύγχρονου ανθρώπου. Μαζί με αυτές τις αλλαγές, οι οποίες κατά κανόνα βελτιώνουν την ποιότητα της ζωής μας, υπεισέρχονται και οι παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας. Οι νέες αυτές μορφές εγκληματικότητας θεσμοθετούνται με τον όρο «Ηλεκτρονικό Έγκλημα». Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση. Ως «Ηλεκτρονικό Έγκλημα», λοιπόν, θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία.

2.2.2. Κυβερνοασφάλεια –Cyber Security

Σύμφωνα με τον Κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, ο όρος «Κυβερνοασφάλεια» περιλαμβάνει όλες τις δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων.[1]

Καλύπτει το σύνολο των διασφαλίσεων και μέτρων που υιοθετούνται για την προστασία των συστημάτων πληροφοριών έναντι μη εξουσιοδοτημένης πρόσβασης και επιθέσεων, με στόχο την εξασφάλιση των βασικών αρχών της ασφάλειας πληροφοριακών συστημάτων, δηλαδή της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων.[1]

Είναι η διαδικασία κατά την οποία εμπλέκονται 3 βασικοί παράγοντες:

- **Τεχνολογία/Εργαλεία/Software:** Η τεχνολογία είναι απαραίτητη έτσι ώστε να παρέχει τα κατάλληλα εργαλεία στους Οργανισμούς και τους ιδιώτες.
  Οι βασικές οντότητες που πρέπει να προστατευτούν μέσω των τεχνολογικών εργαλείων είναι: Τερματικά, Έξυπνες συσκευές και Routers, το δίκτυο στο σύνολο του αλλά και το Cloud.
  Απαιτούνται προχωρημένα εργαλεία όπως Firewalls, προστασία από Malware, Antivirus, Cloud Backup, email security λύσεις.
- **Διαδικασίες:** Οι Οργανισμοί είναι υποχρεωμένοι να μελετούν και να εφαρμόζουν πολιτικές ασφάλειας πληροφοριακών συστημάτων, καθορίζοντας σχέδιο με το οποίο θα αντιμετωπίζουν οι χρήστες τις επιτυχημένες ή αποτυχημένες απόπειρες κυβερνοεπιθέσεων.
- **Οι άνθρωποι / Χρήστες:** Είναι σημαντικό οι Χρήστες να κατανοήσουν και να ακολουθήσουν βασικές αρχές ασφάλειας, όπως η σωστή διαχείριση των passwords. Θα πρέπει να υπάρχει μέριμνα για συχνή και κατάλληλη ενημέρωση για να είναι σε θέση να αναγνωρίζουν τις κυβερνοαπειλές.
  Όποια εργαλεία και να χρησιμοποιηθούν, αν ο τελικός χρήστης δεν έχει γνώση για την εποπτεία των διαδικασιών και των εργαλείων ή δεν μπορεί να αναγνωρίσει τις κυβερνοαπειλές, είναι ο «αδύναμος κρίκος» στην αλυσίδα της κυβερνοασφάλειας.[2]

Χρηματοδότηση και δαπάνες

Η στρατηγική για την κυβερνοασφάλεια δεν χρηματοδοτείται από ειδικό προϋπολογισμό. Σε ενωσιακό επίπεδο, οι δαπάνες για την κυβερνοασφάλεια καλύπτονται από τον γενικό προϋπολογισμό της ΕΕ καθώς και από συγχρηματοδότηση των κρατών μελών.

Κατά την περίοδο 2014-2018, η Επιτροπή διέθεσε τουλάχιστον 1,4 δισεκατομμύρια ευρώ για την εφαρμογή της στρατηγικής, το μεγαλύτερο μέρος των οποίων διατέθηκε για το πρόγραμμα «Ορίζων 2020».[3] Η χρηματοδότηση του προγράμματος «Ορίζων 2020» διοχετεύεται κυρίως στο πλαίσιο των κοινωνικών προκλήσεων «Ασφαλείς κοινωνίες» και «Υπεροχή στις ευρείας εφαρμογής και βιομηχανικές τεχνολογίες». Εντοπίσαμε 279 έργα σχετικά με την κυβερνοασφάλεια τα οποία είχαν αποτελέσει αντικείμενο σύμβασης έως τα

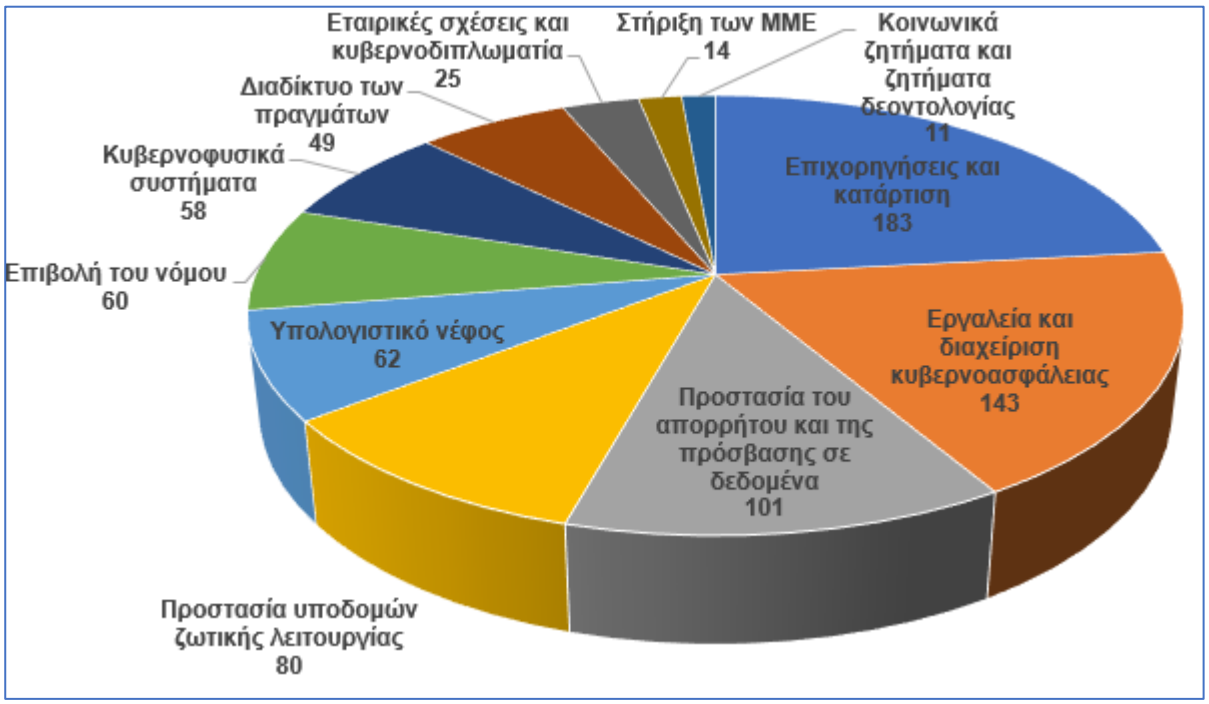
[1] https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EL.pdf

[2] https://tictac.gr/cyber-security-ti-einai/

[3] Το πρόγραμμα «Ορίζων 2020» είναι το πρόγραμμα της ΕΕ ύψους 80 δισεκατομμυρίων ευρώ για την έρευνα και την καινοτομία που στηρίζει την Ένωση καινοτομίας, στόχος της οποίας είναι η διασφάλιση της παγκόσμιας ανταγωνιστικότητας της ΕΕ

τέλη Σεπτεμβρίου του 2018, με συνολική χρηματοδότηση από την ΕΕ ύψους 786 εκατομμυρίων ευρώ.[4]

Στο παρακάτω γράφημα παρουσιάζεται η τυπολογία των έργων αυτών με την αντίστοιχη χρηματοδότηση της ΕΕ.



Εικόνα 1: Ερευνητικά έργα στον τομέα της κυβερνοασφάλειας για τα οποία υπεγράφησαν συμβάσεις στο πλαίσιο του προγράμματος «Ορίζων 2020» (σε εκατομμύρια ευρώ)

Για την περίοδο 2021-2027, έχει προβλεφθεί για την κυβερνοασφάλεια το ποσό των 2 δισεκατομμυρίων ευρώ, στο πλαίσιο του προτεινόμενου νέου προγράμματος «Ψηφιακή Ευρώπη»[2]. Στόχος είναι η ενίσχυση του τομέα της κυβερνοασφάλειας στην ΕΕ και της κοινωνικής προστασίας συνολικά, μεταξύ άλλων, συμβάλλοντας στην εφαρμογή της οδηγίας NIS, την οποία θα αναλύσουμε σε επόμενο κεφάλαιο. Το δίκτυο κέντρων ικανοτήτων στον τομέα της κυβερνοασφάλειας και το ερευνητικό κέντρο ικανοτήτων που προτείνεται να δημιουργηθούν με στόχο την υιοθέτηση μιας πιο εξορθολογισμένης προσέγγισης, αναμένεται να αποτελέσουν τον κύριο μηχανισμό εκτέλεσης των ενωσιακών δαπανών στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη».

[4]https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EL.pdf

3

Κατηγορίες & Παράγοντες Απειλών

3.1 Κατηγορίες Απειλών

Σύμφωνα με τα αποτελέσματα έρευνας που διεξήγαγε η McConnell International σε 52 χώρες, με τίτλο «Cyber Crime... and Punishment?»[5] κατατάσσει τα αδικήματα που διαπράττονται στον Κυβερνοχώρο στις παρακάτω οχτώ κατηγορίες:

- Παρεμπόδιση (κυβερνο)κυκλοφορίας
- Υποκλοπή και Τροποποίηση δεδομένων
- Εισβολή και Σαμποτάζ σε δίκτυο
- Μη εξουσιοδοτημένη πρόσβαση
- Διασπορά ιών
- Υπόθαλψη αδικημάτων
- Πλαστογραφία
- Απάτη

Στην Ελλάδα συγκεκριμένα έχουν εξιχνιαστεί οι εξής μορφές κυβερνοεγκλημάτων από το τμήμα ηλεκτρονικού εγκλήματος:

- Απάτες μέσω Διαδικτύου
- Παιδική πορνογραφία
- Cracking και hacking
- Διακίνηση-πειρατεία λογισμικού
- Πιστωτικές κάρτες
- Διακίνηση ναρκωτικών
- Έγκλημα στα chat rooms

Ακολουθεί μία επισκόπηση των κορυφαίων κυβερνοαπειλών τα τελευταία χρόνια (2017-2021), σύμφωνα με τα στοιχεία που έχει συγκεντρώσει ο ENISA στις ετήσιες μελέτες.

[5] https://uh.edu/tech/cisre/resources/ia-resources/_files/7033/Week12/cybercrime.pdf

2017

Πιο συγκεκριμένα, στην ετήσια μελέτη του ENISA, σύμφωνα με τα στοιχεία που έχει συγκεντρώσει ο οργανισμός, το 2017 στην Ευρωπαϊκή Ένωση παρατηρηθήκαν επιθέσεις οι οποίες είχαν διάφορους στόχους. Στην παρακάτω εικόνα συνοψίζονται οι 15 κορυφαίες κυβερνοαπειλές και τάσεις του 2017 σε σύγκριση με το 2016:

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware	→	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Denial of service	↑	4. Phishing	↑	↑
5. Botnets	↑	5. Spam	↑	↑
6. Phishing	→	6. Denial of service	↑	↓
7. Spam	↓	7. Ransomware	↑	↑
8. Ransomware	→	8. Botnets	↑	↓
9. Insider threat	→	9. Insider threat	→	→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss	→	→
11. Exploit kits	↑	11. Data breaches	↑	↑
12. Data breaches	↑	12. Identity theft	↑	↑
13. Identity theft	↓	13. Information leakage	↑	↑
14. Information leakage	↑	14. Exploit kits	↓	↓
15. Cyber espionage	↓	15. Cyber espionage	↑	→

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

Εικόνα 2: ENISA - Threat Landscape Report 2017, 15 Top Cyberthreats and Trends[3]

Παρατηρούμε ότι στις 3 πρώτες θέσεις βρίσκονται σταθερά οι επιθέσεις Malware (κακόβουλου λογισμικού), οι Web based επιθέσεις (διαδικτυακές) και οι Web application επιθέσεις (σε διαδικτυακές εφαρμογές).

Ακολουθούν οι επιθέσεις Phishing και Spam οι οποίες έχουν αυξητικές τάσεις και οι υπόλοιπες επιθέσεις από την 6η έως την 15η θέση οι οποίες εναλλάσσονται.

2018

Στην ετήσια αναφορά του ENISA για το 2018, παρατηρούμε ότι στις 4 πρώτες θέσεις βρίσκονται σταθερά οι επιθέσεις Malware, οι Web basedεπιθέσεις, οι Web application επιθέσεις και οι επιθέσεις Phishing.

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

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

Εικόνα 3: ENISA - Threat Landscape Report 2018, 15 Top Cyberthreats and Trends[4]

Αξίζει να σημειώσουμε ότι οι επιθέσεις Ransomware έχουν πτωτική τάση και από την 7η θέση έπεσαν στην 14η. Επίσης παρατηρούμε ότι οι Exploit Kits επιθέσεις οι οποίες το 2017 είχαν πτωτική τάση, το 2018 δεν υπάρχουν στην λίστα, ενώ κάνει την εμφάνιση του ένα νέο είδος επίθεσης, το cryptojacking attack (επίθεση κρυπτογράφησης).

2019

Το 2019 ο ENISA παρουσίασε μία αξιολόγηση απειλών για την πέμπτη γενιά δικτύων κινητής τηλεφωνίας (5G).

Εικόνα 4: ENISA (2019)– Threat Landscape for 5G Networks[5]

Πρόκειται για μία πρώτη προσπάθεια του ENISA να προσδιορίσει την έκθεση στοιχείων 5G σε κυβερνοαπειλές, και να επιστήσει την προσοχή όλων των σχετικών ενδιαφερομένων στις παρακάτω συστάσεις:

- Διαμοιρασμός της υπάρχουσας γνώσης 5G στις κοινότητες των ενδιαφερομένων
- «Χτίσιμο» γεφυρών μεταξύ όλων των ενδιαφερομένων
- Συμμετοχή σε συζητήσεις σε επίπεδο ΕΕ για θέματα 5G
- Συμβολή στη συλλογή/διάδοση γνώσεων
- Διάδοση του υπάρχοντος υλικού 5G
- Ενημέρωση για δραστηριότητες 5G που πραγματοποιούνται στο πλαίσιο των αρμοδιοτήτων τους
- Παροχή διαθέσιμης εμπειρογνωμοσύνης και ανθρώπινου δυναμικού
- Βελτίωση/τροποποίηση του υπάρχοντος υλικού ανάλογα με τον ρυθμό των εξελίξεων στο 5G

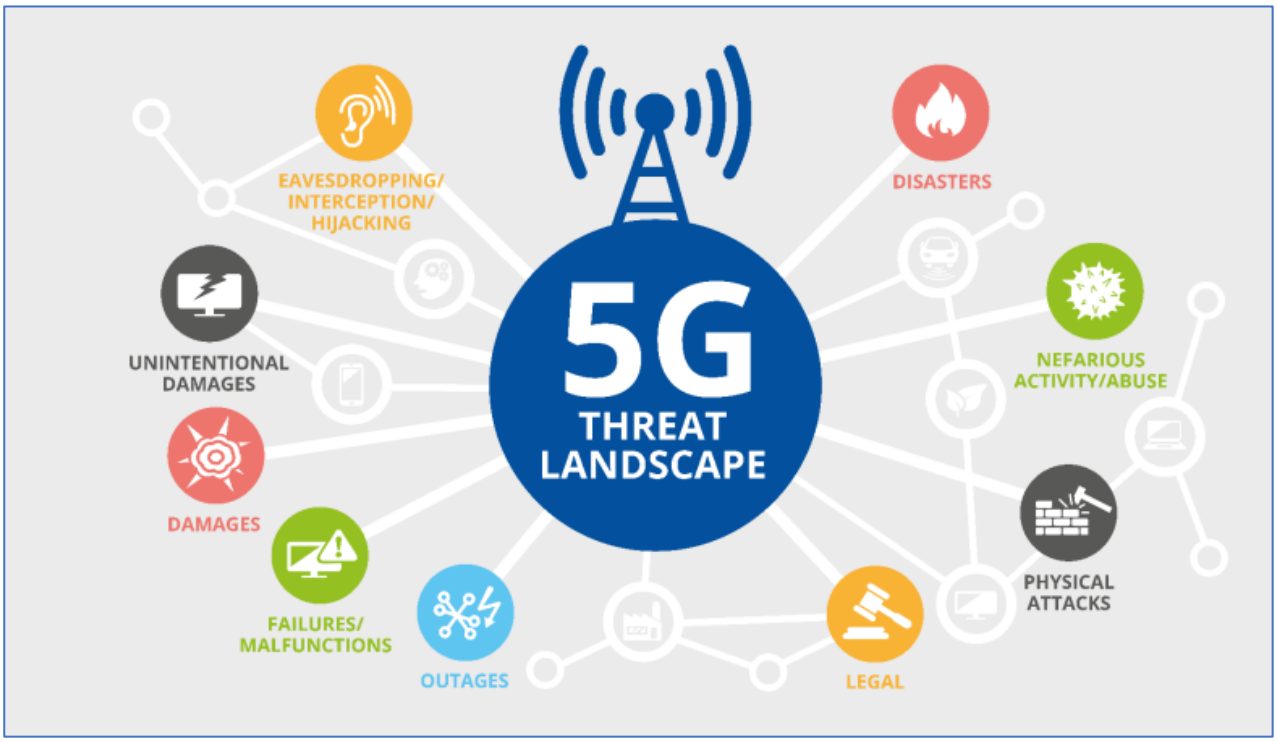
Ως συμπέρασμα, ο ENISA αναφέρει ότι θα είναι σημαντικό να χρησιμοποιηθεί αυτό το υλικό σε διάφορες δραστηριότητες των ενδιαφερομένων, να προσδιοριστούν οι τρέχουσες και μελλοντικές εξελίξεις και να γίνει προσπάθεια να συμπεριληφθούν οι εξελίξεις αυτές σε μελλοντικές εκδόσεις της παρούσας έκθεσης.

Μια τέτοια εξέλιξη θα επιταχύνει την υιοθέτηση απαιτήσεων ασφάλειας και ασφαλών πρακτικών 5G και θα δημιουργήσει ανταγωνιστικά πλεονεκτήματα σε ολόκληρο τον χώρο της ΕΕ.

Ο ENISA θα συνεχίσει να εμπλέκεται σε δραστηριότητες κυβερνοασφάλειας του 5G. Ο συντονισμός με δραστηριότητες σε επίπεδο ΕΕ θα είναι το κλειδί για την επιτυχία αυτής της προσπάθειας.

2020

Το 2020 ο ENISA παρουσίασε μία αναθεωρημένη αξιολόγηση απειλών για την πέμπτη γενιά δικτύων κινητής τηλεφωνίας (5G).



Εικόνα 5: ENISA (2020)– Threat Landscape for 5G Networks[6]

Ουσιαστικά, δεν έχει κάποια αξιόλογη τροποποίηση σχετικά με το 5G, παρά μόνο να επαναλάβει την σημασία και σπουδαιότητα της ασφάλειας απέναντι στις ευπάθειες της πέμπτης γενιάς δικτύων κινητής τηλεφωνίας.

Παράλληλα, ο ENISA παρουσίασε τις 15 κορυφαίες κυβερνοαπειλές και τάσεις για το 2020.

Εικόνα 6: ENISA - Threat Landscape Report 2020, 15 Top Cyberthreats and Trends

2021

Στην ετήσια αναφορά του ENISA για το 2021 (Απρίλιος 2020 έως Ιούλιος 2021) γίνεται ξεκάθαρο για το ποιες είναι οι κυριότερες απειλές που εντοπίστηκαν:

1. Ransomware
2. Malware
3. Cryptojacking
4. E-mail related threats
5. Threats against data
6. Threats against availability and integrity
7. Disinformation – misinformation
8. Non-malicious threats
9. Supply-chain attacks

Κορυφαίες Τάσεις

Για καθεμία από τις απειλές που έχουν εντοπιστεί, συζητούνται τεχνικές επίθεσης, αξιοσημείωτα περιστατικά και τάσεις μαζί με τα προτεινόμενα μέτρα αντιμετώπισης. Όσον αφορά τις τάσεις, κατά την περίοδο αναφοράς επισημαίνουμε τα ακόλουθα:

- **Το Ransomware** έχει αξιολογηθεί ως η **κυριότερη απειλή για το 2020-2021**.
- Οι **κυβερνητικοί οργανισμοί έχουν βελτιώσει τις ικανότητες τους** τόσο σε εθνικό όσο και σε διεθνές επίπεδο.
- **Οι κυβερνοεγκληματίες παρακινούνται όλο και περισσότερο από τη δημιουργία εσόδων** από τις δραστηριότητές τους όπως το ransomware. **Η πληρωμή σε κρυπτονομίσματα** παραμένει η πιο κοινή μέθοδος πληρωμής
- **Η πτωτική τάση του malware attack** που παρατηρήθηκε το 2020 συνεχίζεται και το 2021.
- Ο όγκος των **cryptojacking infections** σημείωσε **υψηλό ρεκόρ** το πρώτο τρίμηνο του 2021, σε σχέση με τα τελευταία χρόνια. Το **οικονομικό κέρδος** που σχετίζεται με το cryptojacking παρότρυνε τους κυβερνοεγκληματίες να πραγματοποιήσουν αυτές τις επιθέσεις.
- **Ο COVID-19 εξακολουθεί να είναι το κυρίαρχο δέλεαρ στις καμπάνιες** για e-mail επιθέσεις.
- Υπήρξε μια α**ύξηση στις παραβιάσεις δεδομένων που σχετίζονται με τον τομέα της υγείας.**
- **Οι παραδοσιακές εκστρατείες DDoS (Distributed Denial of Service)** το 2021 είναι πιο στοχευμένες. Το **IoT (Internet of Things),** σε συνδυασμό με τα **δίκτυα κινητής τηλεφωνίας,** έχει ως αποτέλεσμα ένα νέο κύμα επιθέσεων DDoS.
- Το 2020 και το 2021 παρατηρούμε μια **έξαρση στα μη κακόβουλα περιστατικά**, καθώς η πανδημία του COVID-19 έγινε αφορμή για **ανθρώπινα λάθη** και **λανθασμένες ρυθμίσεις συστήματος**, μέχρι το σημείο που οι περισσότερες παραβιάσεις το 2020 οφείλονταν σε σφάλματα.

Εικόνα 7: ENISA - Threat Landscape 2021 - Prime Threats[7]

Ακολουθεί αναλυτική επεξήγηση των κορυφαίων απειλών-

3.1.1 Malware (Κακόβουλο λογισμικό)

Λογισμικό σχεδιασμένο ειδικά για πρόκληση ζημιάς ή απόκτησης μη εξουσιοδοτημένης πρόσβασης σε ένα σύστημα υπολογιστή. Περιλαμβάνει ιούς (viruses), worms, trojan horses.[8]

3.1.2. Web-based attacks (Διαδικτυακές επιθέσεις)

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

3.1.3 Phishing

Κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου ή τηλεφωνικές συνδιαλλαγές, οι οποίες αποσκοπούν στην παραπλάνηση των χρηστών και στην αποκάλυψη εμπιστευτικών πληροφοριών.

3.1.4 Web applications attacks (Επιθέσεις σε διαδικτυακές εφαρμογές)

Οι διαδικτυακές εφαρμογές, λόγω της καθολικής χρήσης τους στην προσφορά περιεχομένου, αποτελούν στόχο πολλαπλών ειδών επιθέσεων, με κυριότερες τα cross-site scripting (XSS), SQL injection κ.α.

3.1.5 Spam (Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου)

Αυτές οι επιθέσεις περιλαμβάνουν την αποστολή ανεπιθύμητης αλληλογραφίας σε χρήστες. Η αλληλογραφία αυτή χαρακτηρίζεται από το πολύ μικρό κόστος αποστολής των μηνυμάτων, την ενόχληση που προκαλεί στους χρήστες, αλλά και την πιθανή μετεξέλιξη των μηνυμάτων σε απειλή phishing.

3.1.6 Dos Attacks (Επιθέσεις άρνησης υπηρεσίας - Denial of Service)

Επιθέσεις κατά τις οποίες μια υπηρεσία δέχεται ξαφνικά μεγάλο όγκο διαδικτυακής κίνησης, με σκοπό να καταστεί αδύνατο από τα συστήματα να εξυπηρετήσουν νόμιμα αιτήματα. Ουσιαστικά, εκμεταλλεύονται την πεπερασμένη χωρητικότητα συστημάτων και δικτύων, με στόχο να καταστήσουν αδύνατη την παροχή υπηρεσιών (απώλεια διαθεσιμότητας).

3.1.7 Identity theft (Υποκλοπή ταυτότητας)

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

3.1.8 Data breach (Παραβίαση προσωπικών δεδομένων)

Επιθέσεις οι οποίες αποσκοπούν στη διαρροή, αλλοίωση ή μη διαθεσιμότητα προσωπικών δεδομένων. Σύμφωνα με τον Κανονισμό της Ε.Ε. 2016/679[9], τέτοιου είδους επιθέσεις θεωρούνται παραβιάσεις δεδομένων προσωπικού χαρακτήρα οι οποίες χρήζουν άμεσης αντιμετώπισης.

3.1.9 Insider theft (Εσωτερικές απειλές)

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

3.1.10 Botnets

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

3.1.11 Physical manipulation, damage, theft and loss (Φυσικές απειλές)

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

3.1.12 Information leakage (Διαρροή δεδομένων)

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

3.1.13 Ransomware (Λογισμικό λύτρων)

Το Ransomware ανήκει στην κατηγορία του malware, όμως εξετάζεται χωριστά λόγω της ιδιαιτερότητάς του. Πρόκειται για ένα είδος κακόβουλου λογισμικού που συνήθως

χρησιμοποιείται για εκβιασμούς. Αυτό που κάνει είναι να κρυπτογραφεί τα δεδομένα του πληροφοριακού συστήματος, για την αποκρυπτογράφηση των οποίων ο επιτιθέμενος απαιτεί λύτρα (συνήθως σε μορφή κρυπτονομίσματος).

Σύμφωνα με ειδικούς, όταν μια επιχείρηση, μια κυβερνητική υπηρεσία ή οποιοσδήποτε άλλος οργανισμός χτυπηθεί από ransomware και επιλέγει να πληρώσει λύτρα στον εισβολέα της με αντάλλαγμα ένα κλειδί αποκρυπτογράφησης ή κάποια άλλη υπόσχεση, πληρώνει κατά μέσο όρο 140.000 δολάρια.[10]

3.1.14 Cyber-espionage (Ηλεκτρονική κατασκοπεία)

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

3.1.15 Cryptojacking

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

3.2 Παράγοντες Απειλών

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

3.2.1 Κυβερνοεγκληματίες (Cybercriminals)

Όπως αναφέραμε και παραπάνω, ο όρος «κυβερνοέγκλημα» (cybercrime) χρησιμοποιείται για να χαρακτηρίσει κάθε κακόβουλη ενέργεια η οποία αποσκοπεί στο να επιφέρει αντίκτυπο στις επιχειρησιακές λειτουργίες ενός οργανισμού. Κατά συνέπεια, οι κυβερνοεγκληματίες, ως παράγοντες απειλών, είναι ομάδες ή μεμονωμένα φυσικά πρόσωπα που χρησιμοποιούν την τεχνολογία (ΤΠΕ) για την τέλεση κακόβουλων ενεργειών.

Οι κυβερνοεγκληματίες συχνά εμπλέκονται σε παράνομες δοσοληψίες στο επονομαζόμενο Dark Web, όπου προβαίνουν σε αγοροπωλησία κακόβουλων εφαρμογών ή πληροφοριών για πιθανούς στόχους.

Το κυβερνοέγκλημα είναι πιθανόν να περιλαμβάνει:

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

3.2.2 Τρίτα κράτη

Η κατηγορία αυτή περιλαμβάνει ομάδες οι οποίες είτε ανήκουν, είτε χρηματοδοτούνται από κράτη και ουσιαστικά αποσκοπούν στο να εξαπολύσουν επιθέσεις που θα επιφέρουν μεγάλο αντίκτυπο στην παροχή βασικών / ουσιωδών υπηρεσιών από Φορείς. Τέτοιου είδους επιθέσεις έχουν ως κύριο στόχο τη διακοπή υπηρεσιών (π.χ. μέσω επιθέσεων άρνησης υπηρεσίας – DoS/DDoS) ή μη εξουσιοδοτημένης πρόσβασης σε διαβαθμισμένα δεδομένα. Ιδιαίτερη μνεία πρέπει να γίνει σε περιπτώσεις κυβερνοκατασκοπείας, όπου διακρίνεται, τα τελευταία έτη, έξαρση επιθέσεων σε Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (Φ.Ε.Β.Υ.)

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

Είναι συχνό φαινόμενο, ομάδες του κυβερνοχώρου να επιτίθενται σε φορείς Δημόσιας Διοίκησης στο όνομα ενός τρίτου κράτους. Οι επιθέσεις αυτές, που κατά βάση αποσκοπούν σε αλλοίωση ιστοσελίδων ή/και προσωρινή άρνηση υπηρεσιών, πρέπει να αντιμετωπίζονται αφενός με σοβαρότητα, αφετέρου όμως στο πλαίσιο ακτιβιστικών ενεργειών και όχι ως απόρροια ενεργειών τρίτων κρατών.

3.2.3 Ακτιβιστές

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

3.2.4 Εσωτερικές απειλές

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

3.3 Πανδημία COVID-19

Με βάση τις εκτιμήσεις των ειδικών, το πρώτο κρούσμα στην Ευρώπη καταγράφηκε στην Ισπανία στις 12 Ιανουαρίου 2020 και το πρώτο στις ΗΠΑ στις 16 Ιανουαρίου 2020. Η συνέχεια είναι γνωστή, με τον ιό να εξαπλώνεται παγκοσμίως με ταχύτατους ρυθμούς.

Το 2020 ήταν μια ιδιαίτερη χρονιά με τον COVID-19 να αποτελεί παγκόσμια κρίση: κοινωνική αποστασιοποίηση, αυτοαπομόνωση, απαγόρευση κυκλοφορίας. Η παγκόσμια πανδημία έκανε αυτούς τους όρους να αποτελούν μέρος της καθημερινότητάς μας.

Η αναγκαιότητα για επιχειρησιακή συνέχεια, τόσο στο κράτος όσο και στον ιδιωτικό τομέα, υποχρέωσε δημόσιους οργανισμούς, φορείς και ιδιωτικές εταιρείες να προσαρμοστούν γρήγορα και να μετασχηματίσουν τις δραστηριότητές τους. Κατάφεραν σε πολύ γρήγορο χρονικό διάστημα να χρησιμοποιήσουν ηλεκτρονικές υπηρεσίες και υποδομές, οι οποίες τις περισσότερες φορές δημιουργήθηκαν άμεσα. Υπήρξε μία ταχύτατη προσαρμογή που είχε εξαιρετικά αποτελέσματα, τόσο μέσα από ηλεκτρονικές υπηρεσίες, αφού πλέον ζούμε στην εποχή της ηλεκτρονικής διακυβέρνησης, όσο και σε εργαλεία τηλεκπαίδευσης και τηλεργασίας. Αυτός ο μετασχηματισμός ευνόησε στην δημιουργία υποδομών που δεν υπήρχαν.

Αυτές οι αλλαγές δημιούργησαν ένα νέο τοπίο προκλήσεων για το 2021 σχετικά με την ασφάλεια, καθώς οι απειλές γίνονται πιο σύνθετες και η ανάγκη για προστασία ακόμη μεγαλύτερη. Η έκθεση της Europol για το σοβαρό και οργανωμένο έγκλημα στον κυβερνοχώρο για το 2020 ανέδειξε ότι αυτή η ανάγκη προσαρμογής στα νέα δεδομένα εκτόξευσε και κάποια αδικήματα στον κυβερνοχώρο. Ενώ υπήρξε αύξηση σε όλα τα αδικήματα στον κυβερνοχώρο, παρατηρούνται 3 μεγάλες κατηγορίες που είχαν ιδιαίτερη αύξηση παγκοσμίως:

- Ransomware attacks: όπως αναφέραμε και παραπάνω, αυτό το είδος επίθεσης έχει αξιολογηθεί ως η κυριότερη απειλή για το 2020-2021
- Online Child Abuse: Δυστυχώς υπήρξε αύξηση και στην κακοποίηση παιδιών και πορνογραφία ανηλίκων. Ο περιορισμός του να ταξιδέψει κάποιος οδήγησε στην αύξηση του φαινόμενου του να παράγεται τέτοιο υλικό και να το παρακολουθούν live stream σε ζωντανή μετάδοση. Η online αναμετάδοση της κακοποίησης παιδιών συνεχίζει να αυξάνεται, γίνεται ακόμη πιο διαδεδομένη κατά την διάρκεια της

πανδημίας, όταν οι ταξιδιωτικοί περιορισμοί εμπόδισαν τους παραβάτες να κακοποιούν τα παιδιά με φυσικό τρόπο. #IOCTA2020

- Payment Fraud: η απάτη με αντικατάσταση SIM είναι μία από τις νέες τάσεις. Οι εγκληματίες αντικαθιστούν ψευδώς τις κάρτες SIM των θυμάτων με αυτές που έχουν στην κατοχή τους για να υποκλέψουν κωδικούς πρόσβασης και να παρακάμψουν τον έλεγχο ταυτότητας δύο παραγόντων.

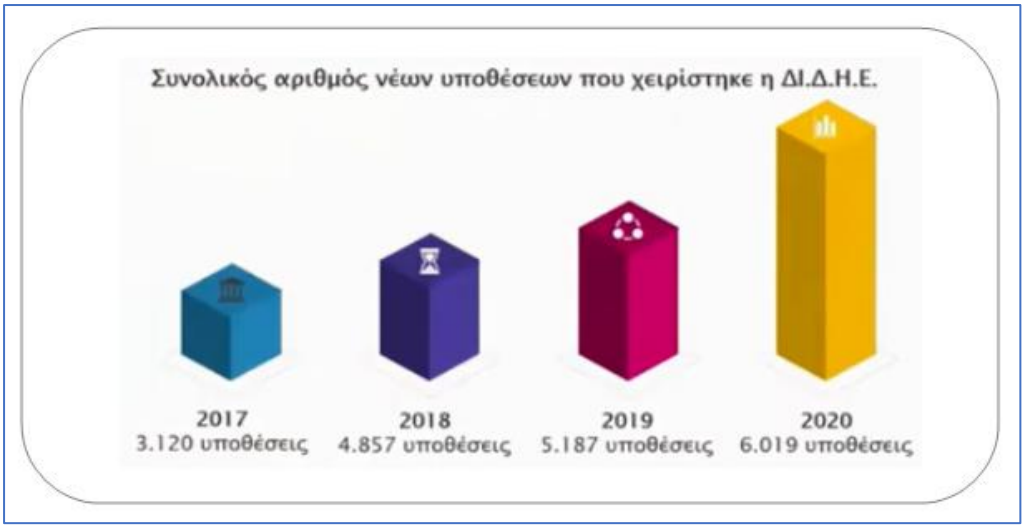
Επιπλέον, η πανδημία δημιούργησε νέο χώρο για τους κυβερνοεγκληματίες. Έτσι, πολλοί οργανισμοί ενίσχυσαν τους μηχανισμούς ασφάλειας και προχώρησαν σε πρωτοβουλίες γρήγορου ψηφιακού μετασχηματισμού.

Η εκτεταμένη μετάβαση στην εξ αποστάσεως εργασία είχε αποτέλεσμα την εμφάνιση τρωτών σημείων που ήταν καλά κρυμμένα, τα οποία φυσικά θα συνεχίσουν να επηρεάζουν τις επιχειρήσεις τους επόμενους μήνες. Οι εργασιακές μας συνήθειες και οι συμπεριφορές μας αλλάζουν μόνιμα από τον Covid. Επίσης, καθώς η πανδημία επηρεάζει τα ανθρώπινα συναισθήματα, οι εσωτερικές απειλές ενισχύονται περαιτέρω, δημιουργώντας σημαντικές ευκαιρίες για τους κυβερνοεγκληματίες. Οι κυβερνοεγκληματίες προσαρμόστηκαν πολύ γρήγορα εκμεταλλευόμενοι το άγχος, την ταχύτητα και σε αρκετές περιπτώσεις την άγνοια.

Το πρόβλημα είναι ότι δεν δόθηκε η έμφαση που πρέπει στην δημιουργία υποδομών ασφάλειας. Οι πολιτικές ασφάλειας, σε έναν δημόσιο Οργανισμό ή σε μια ιδιωτική εταιρεία, δεν πρέπει να αντιμετωπίζονται ως ένα απλό κείμενο. Το προσωπικό θα πρέπει να εκπαιδευτεί και να εκπαιδεύεται συνεχώς, ώστε να τηρεί απόλυτα όλες αυτές τις διαδικασίες που προβλέπονται και ουσιαστικά, μέσα από αυτό, ο σωστά εκπαιδευμένος χρήστης να καταφέρει να συμμετέχει στην αλυσίδα της ασφάλειας ισότιμα με την τεχνολογία.

Πολλά περιστατικά δεν καταγράφονται, καθώς οι επιθέσεις είναι αναβαθμισμένες και συμβαίνει συχνά την ώρα της επίθεσης, το γεγονός να μην γίνει αντιληπτό, ή να γίνει αντιληπτό όταν θα είναι πολύ αργά. Αν οι κυβερνοεγκληματίες αποσκοπούν στο να αποσπάσουν πληροφορίες όπως είναι ζητήματα βιομηχανικής κατασκοπίας για παράδειγμα, θα μπουν, θα υποκλέψουν τα στοιχεία που θέλουν και θα αποχωρήσουν καθαρίζοντας όλα τα ψηφιακά τους ίχνη και δεν αφήνουν κανένα αξιοποιήσιμο στοιχεία ώστε να μπορέσει κάποιος να τους ανακαλύψει.

Ένα ενδιαφέρον στοιχείο που μας ανακοίνωσε η ΔΙΔΗΕ είναι ότι από το 2017 έως το 2020 διπλασιάστηκαν οι υποθέσεις που χειρίστηκαν.



Εικόνα 8: Συνολικός αριθμός νέων υποθέσεων ΔΙΔΗΕ

Ο άνθρωπος ως παράγοντας απειλής

Σύμφωνα με παγκόσμια έρευνα που διεξήγαγε η Check Point μαζί με την Dimensional Research με στόχο να αποκαλύψει τις κύριες προκλήσεις και προτεραιότητες ασφάλειας των οργανισμών καθώς βαδίζαμε προς το 2021 και φυσικά επηρεαζόμενες από την πανδημία, προέκυψε ότι η κύρια πρόκληση είναι η ασφάλεια των εργαζομένων που δουλεύουν απομακρυσμένα με ποσοστό 47%, ακολουθούμενοι από την προστασία από επιθέσεις phishing και social engineering με ποσοστό 42%. Παράλληλα, βλέπουμε ότι το phishing ήταν ο πιο κοινός τύπος κυβερνο-εγκλήματος το 2020 σύμφωνα με την έκθεση της Verizon. Σχετικά με έρευνα για την παραβίαση δεδομένων για το 2020, το phishing προέκυψε ως ο τρόπος με τον οποίο ξεκινάει μεγάλη πλειονότητα των παραβιάσεων δεδομένων. Το 75% των οργανισμών σε όλο τον κόσμο υπέστησαν κάποιο είδος phishing επίθεσης μέσα στο 2020, με το 96% των επιθέσεων phishing να πραγματοποιούνται μέσω email.

Βλέπουμε λοιπόν πως οι κοινωνικές επιθέσεις έχουν την πρώτη θέση, γεγονός το οποίο σημαίνει ότι ο ανθρώπινος παράγοντας διαδραματίζει σημαντικά το τοπίο απειλών για έναν οργανισμό. Η αλήθεια είναι πως οι οργανισμοί μπορούν να λάβουν όλες τις πιθανές προφυλάξεις και να εφαρμόσουν μέτρα ασφάλειας για να ελαχιστοποιήσουν τον κίνδυνο που μπορεί να επιφέρουν οι κυβερνοαπειλές, αλλά στο τέλος της ημέρας το μόνο που χρειάζεται είναι ένα απλό ανθρώπινο λάθος για να τεθούν τα πάντα σε κίνδυνο. Επίσης, οι άνθρωποι τείνουν να πιστεύουν ότι οι μηχανισμοί ασφάλειας και όλες οι τεχνολογίες που υιοθετεί ένας οργανισμός είναι αρκετά για να τους προστατεύσουν από πιθανούς κινδύνους. Η τεχνολογία δεν είναι αρκετή για να κρατήσει ασφαλή έναν οργανισμό. Πρέπει να λαμβάνεται πάντα υπόψη ο ανθρώπινος παράγοντας.

Ένα από τα πιο ανησυχητικά ευρήματα του Cyber Threats Report 2020 της Netwrix[11] ήταν ότι περισσότεροι από τους μισούς ερωτηθέντες (58%) δήλωσαν ότι οι εργαζόμενοι αγνοούν τις πολιτικές και τις οδηγίες σχετικά με την ασφάλεια πληροφοριών.

Μελέτη της CyberArc η οποία διεξήχθη ανάμεσα σε 3.000 remote workers το 2020 σχετικά με τις συνήθειες που επικρατούσαν κατά την απομακρυσμένη εργασία αποκάλυψε τα εξής αποτελέσματα:

- Το 77% των εργαζομένων χρησιμοποιεί μη ασφαλείς προσωπικές συσκευές που δεν είναι κεντρικά διαχειρίσιμες, τις λεγόμενες Bring Your Own Devices (BYOD), για να έχουν πρόσβαση στα εταιρικά δεδομένα και τα συστήματα.
- Το 93%, δηλαδή σχεδόν όλοι, χρησιμοποιεί τα ίδια passwords σε πολλές εφαρμογές και συσκευές.
- Το 29% παραδέχτηκε ότι αφήνει άλλα μέλη της οικογένειας να χρησιμοποιούν την εταιρική τους συσκευή για δραστηριότητες που σχετίζονται με το σχολείο, τα παιχνίδια και τις ηλεκτρονικές αγορές.

Σύμφωνα με μια έρευνα που έγινε από το Πανεπιστήμιο του Stanford και την εταιρία Tessian, 9 στα 10 περιστατικά (88%) των παραβιάσεων δεδομένων προκαλούνται από ανθρώπινο σφάλμα.[6]

[6] https://cisomag.eccouncil.org/psychology-of-human-error-could-help-businesses-prevent-security-breaches/

4

Διατάξεις - Ανακοινώσεις της ΕΕ σχετικά με την Κυβερνοασφάλεια

Ακολουθούν κάποια σημαντικά γεγονότα που αποτελούν σταθμούς για το έργο και τις ενέργειες της Ευρωπαϊκής Επιτροπής σχετικά με την Ασφάλεια στον Κυβερνοχώρο.

2001

Ήδη από το 2001, η ΕΕ είχε αντιληφθεί την σημασία της ασφάλειας και την βασική προτεραιότητα που έχει, καθώς οι επικοινωνίες και οι πληροφορίες έχουν αποβεί βασικός παράγοντας στην οικονομική και κοινωνική εξέλιξη[12]. Τα δίκτυα και συστήματα πληροφοριών υποστηρίζουν υπηρεσίες και μεταφέρουν δεδομένα σε βαθμό που μερικά χρόνια πριν ήταν αδιανόητο.

- Στις 6 Ιουνίου 2001 η Ευρωπαϊκή Επιτροπή εξέδωσε ανακοίνωση σχετικά με την Ασφάλεια Δικτύων και Πληροφοριών, με την οποία ανακοίνωσε την ανάπτυξη συνολικής στρατηγικής για την ασφάλεια των ηλεκτρονικών δικτύων καθώς και πρακτικές δράσεις για την εφαρμογή της.

- Στις 23 Νοεμβρίου 2001, με την **Σύμβαση της Βουδαπέστης για το έγκλημα στο κυβερνοχώρο**[13], θεσπίστηκαν επίσημα για πρώτη φορά μέτρα κατά του κυβερνοεγκλήματος, τα οποία κάθε Κράτος Μέλος της ΕΕ υποχρεούται να τηρήσει. Γίνεται διάκριση σε:
  - Εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και συστημάτων υπολογιστών, όπως παράνομη πρόσβαση στο σύστημα υπολογιστή, υποκλοπή δεδομένων, παρεμβολές σε δεδομένα και σε συστήματα υπολογιστών, κακή χρήση συσκευών.
  - Εγκλήματα σχετικά με υπολογιστές, όπως πλαστογραφία και απάτη σχετικά με υπολογιστές.
  - Εγκλήματα σχετικά με το περιεχόμενο, όπως παιδική πορνογραφία
  - Εγκλήματα σχετικά με παραβιάσεις συγγραφικών και συγγενικών δικαιωμάτων

Η Σύμβαση εισήγαγε διατάξεις σχετικά με τη διασυνοριακή συνεργασία και ορισμένες τεχνικές έρευνας σχετικά με τα ηλεκτρονικά αποδεικτικά στοιχεία ("e-evidence").[7] Περισσότερες πληροφορίες για τη Σύμβαση παρατίθενται στο Παράρτημα Α.

2002

Στις 12 Ιουλίου 2002 το Ευρωπαϊκό Κοινοβούλιο εξέδωσε οδηγία σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.[14]

Έβαλε τις βάσεις για την Ασφάλεια και το Απόρρητο των Επικοινωνιών και απαιτεί από όλα τα κράτη μέλη να θεσπίσουν μέτρα ασφάλειας για την προστασία των προσωπικών δεδομένων. Ανάμεσα στα μέτρα αυτά, θα πρέπει τα συστήματα για την παροχή ηλεκτρονικών επικοινωνιακών δικτύων και υπηρεσιών να σχεδιάζονται με τέτοιον τρόπο ώστε η ποσότητα των απαιτούμενων δεδομένων προσωπικού χαρακτήρα να περιορίζεται στο ελάχιστο δυνατό.

2006

- Στις 31 Μαΐου 2006 η Ευρωπαϊκή Επιτροπή παρουσίασε την **Στρατηγική για ασφαλή κοινωνία της πληροφορίας** – «διάλογος, πνεύμα συνεργασίας και ενίσχυση των ικανοτήτων».[15] Στην στρατηγική επανεξέτασε την τρέχουσα κατάσταση όσον αφορά τις απειλές κατά της κοινωνίας της πληροφορίας και παρουσίασε μια επικαιροποιημένη πολιτική στρατηγική, τονίζοντας τον θετικό αντίκτυπο της τεχνολογικής ποικιλομορφίας στην ασφάλεια, καθώς και τη σημασία του ανοίγματος και της διαλειτουργικότητας.

- Στις 15 Νοεμβρίου 2006 η Επιτροπή εξέδωσε ανακοίνωση σχετικά με την καταπολέμηση των ανεπίκλητων ηλεκτρονικών μηνυμάτων (spam emails),[8] του κατασκοπευτικού και του κακόβουλου λογισμικού.[16] Τονίζει το πρόβλημα που έχει προκύψει την πενταετία 2001-2005. Σύμφωνα με πηγές του κλάδου, το 2001 τα spam emails ανέρχονταν στο 7% της παγκόσμιας κίνησης ηλεκτρονικού ταχυδρομείου και το 2006 ανέρχονται πλέον σε ποσοστό περίπου 50-80% του συνόλου των μηνυμάτων που απευθύνονται σε τελικούς χρήστες. Μεγάλο ποσοστό

[7] Ηλεκτρονικά αποδεικτικά στοιχεία ονομάζουμε τα ψηφιακά δεδομένα που χρησιμοποιούνται για τη διερεύνηση και τη δίωξη ποινικών αδικημάτων. Στα στοιχεία αυτά περιλαμβάνονται (α) τα μηνύματα ηλεκτρονικού ταχυδρομείου, (β) τα γραπτά μηνύματα (SMS) ή το περιεχόμενο από εφαρμογές ανταλλαγής μηνυμάτων, (γ) το οπτικοακουστικό περιεχόμενο και (δ) οι πληροφορίες για τον ηλεκτρονικό λογαριασμό ενός χρήστη. Τέτοιου είδους δεδομένα μπορούν να χρησιμοποιηθούν για την ταυτοποίηση ενός προσώπου ή για την συγκέντρωση περισσότερων πληροφοριών σχετικά με τις δραστηριότητές του. Στην ψηφιακή εποχή, οι εγκληματίες χρησιμοποιούν όλο και περισσότερο τεχνολογικές υπηρεσίες και εργαλεία για τον σχεδιασμό και τη διάπραξη εγκλημάτων. Συνεπώς, τα ηλεκτρονικά αποδεικτικά στοιχεία αποκτούν εξαιρετικά σημαντικό ρόλο στην καταπολέμηση του εγκλήματος.

[8] Το spam αναφέρεται στην αποστολή ανεπίκλητων επικοινωνιών (μηνυμάτων), π.χ. μέσω email, για εμπορικούς σκοπούς. Τα spam emails μπορούν, ωστόσο, να περιέχουν επίσης κακόβουλο και κατασκοπευτικό λογισμικό.

αποτελεί η χρήση “phishing” emails που παρασύρουν τους τελικούς χρήστες να αποκαλύψουν ευαίσθητα δεδομένα τους, μιμούμενα δικτυακούς τόπους υποτιθέμενων γνήσιων εταιριών.

Η ανακοίνωση της Επιτροπής συνέβαλε στην αύξηση της ευαισθητοποίησης απέναντι στα spam emails, σε εθνικό και διεθνές επίπεδο, σε ολόκληρο τον πλανήτη. Σε επίπεδο ΕΕ, το πρόγραμμα **Safer Internet plus programme**[9] προωθεί την ασφαλέστερη χρήση του Ίντερνετ και των νέων επιγραμμικών τεχνολογιών, ιδίως για τα παιδιά, ως μέρους μιας συνεκτικής προσέγγισης που προτείνει η Ευρωπαϊκή Ένωση. Τα κράτη μέλη δρομολόγησαν ή υποστήριξαν εκστρατείες ευαισθητοποίησης των χρηστών σχετικά με το πρόβλημα των spam emails και τους τρόπους αντιμετώπισής του. Οι πάροχοι υπηρεσιών Ίντερνετ ανέλαβαν την ευθύνη συμβουλευτικών υπηρεσιών και τεχνικής βοήθειας στους πελάτες τους σχετικά με τρόπους προστασίας απέναντι σε κατασκοπευτικό λογισμικό και σε ιούς.

2007

Στις 1 Ιουνίου 2007 η Ευρωπαϊκή Επιτροπή εξέδωσε ανακοίνωση σχετικά με την αξιολόγηση του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA).[17] Στόχος της εξωτερικής αξιολόγησης ήταν η αποτίμηση των αποτελεσμάτων του Οργανισμού ως προς την εκπλήρωση των στόχων και των καθηκόντων του, καθώς και τις εργασιακές του πρακτικές.

Στο πλαίσιο της αξιολόγησης εξετάσθηκαν οι δυνατότητες αντίκτυπου σε εθνικό και διεθνές επίπεδο, καθώς και τα αντληθέντα διδάγματα που είναι χρήσιμα για την εκπόνηση του προγράμματος εργασίας και τον πιθανό αναπροσανατολισμό του πεδίου δραστηριότητας του Οργανισμού.

Στον πίνακα που ακολουθεί παρουσιάζεται η ανάλυση SWOT[10] σύμφωνα με την έκθεση αξιολόγησης της ομάδας εμπειρογνωμόνων.

[9] https://www.efta.int/eea/eu-programmes/safer-internet-plus
[10] SWOT -> Strengths, Weaknesses, Opportunities & Threats Analysis

Πίνακας 'SWOT' (Ανάλυση πλεονεκτημάτων, αδυναμιών, ευκαιριών και απειλών) της έκθεσης αξιολόγησης της εξωτερικής ομάδας εμπειρογνωμόνων, σ. 72

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΑΔΥΝΑΜΙΕΣ
• Εντολή των κρατών μελών και της Επιτροπής • Καλή εκκίνηση για την οικοδόμηση σχέσεων • Ικανότητες του προσωπικού	• Έλλειψη οράματος, εστίασης και ευελιξίας • Εύθραυστη σχέση μεταξύ διοικητικού συμβουλίου και Οργανισμού • Προβληματική τοποθέτηση της έδρας για προσλήψεις και δικτύωση • Έλλειψη κρίσιμης μάζας του προσωπικού λειτουργίας • Καμπύλη μάθησης σε αρχικό στάδιο
ΕΥΚΑΙΡΙΕΣ	**ΑΠΕΙΛΕΣ**
• Ενίσχυση της σημασίας της ασφάλειας στην ΕΕ • Μοναδική θέση για την αντιμετώπιση των αναγκών συντονισμού σε θέματα ασφάλειας • Αναζήτηση ομολόγου στην ΕΕ από παγκόσμιες συμμαχίες • Δρομολόγηση νέων έργων μείζονος σημασίας στον τομέα της ασφάλειας • Ανάδειξη σε σημείο αναφοράς για όλα τα κράτη μέλη	• Εάν δεν βελτιωθεί η αποτελεσματικότητα, ταχεία αποδυνάμωση και απώλεια φήμης • Υψηλός ρυθμός αντικατάστασης προσωπικού που έχει ως αποτέλεσμα την αποδυνάμωσή του • Αντιφατικές προσδοκίες εκ μέρους των κρατών μελών και μεταξύ κρατών μελών και ενδιαφερομένων • Εσφαλμένη αντίληψη του ρόλου και των σκοπών του από τους εξωτερικούς ενδιαφερομένους

Εικόνα 9: SWOT Analysis

2009

Στις 18 Δεκεμβρίου 2009 το Ευρωπαϊκό Συμβούλιο εξέδωσε Ψήφισμα για ευρωπαϊκή συνεργατική προσέγγιση[18] όσον αφορά την ασφάλεια δικτύων και πληροφοριών.

Τονίζει ότι μια διευρυμένη και ολιστική ευρωπαϊκή στρατηγική για την ασφάλεια δικτύων και πληροφοριών, με σαφώς καθορισμένους ρόλους της Ευρωπαϊκής Επιτροπής, των κρατών μελών και του ENISA, είναι ζωτικής σημασίας για την αντιμετώπιση των τρεχουσών και των μελλοντικών προκλήσεων. Παράλληλα, καλεί τα Κράτη Μέλη, την Ευρωπαϊκή Επιτροπή, τον ENISA και τους ενδιαφερόμενους φορείς να εντατικοποιήσουν τις ενέργειες τους και, σε πλαίσιο συνεργασίας μεταξύ τους, να οργανώσουν δράσεις και να συσταθούν ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) στα κράτη μέλη που δεν διαθέτουν ακόμα τη δυνατότητα αυτή, ενισχύοντας τη συνεργασία μεταξύ εθνικών CERT σε ευρωπαϊκό επίπεδο.

2010

- Στο ψηφιακό θεματολόγιο για την Ευρώπη[19], το οποίο εγκρίθηκε τον Μάιο του 2010, και στα σχετικά συμπεράσματα του Συμβουλίου[20] η Επιτροπή κρούει τον κώδωνα του κινδύνου για την αύξηση του ηλεκτρονικού εγκλήματος και επισημαίνει την απειλή για την αξιοπιστία των δικτύων. Τονίζει ότι η εμπιστοσύνη και η ασφάλεια αποτελούν απαραίτητες προϋποθέσεις για την ευρεία αφομοίωση των ΤΠΕ από τους χρήστες και, ως εκ τούτου, για την επίτευξη των στόχων της διάστασης της στρατηγικής «Ευρώπη 2020» που αφορά την «έξυπνη ανάπτυξη»[21].

  Συγκεκριμένα, στο κεφάλαιο «Εμπιστοσύνη και Ασφάλεια», το Ψηφιακό θεματολόγιο φέρνει ως παράδειγμα ότι για την αντιμετώπιση της σεξουαλικής εκμετάλλευσης και της παιδικής πορνογραφίας μπορούν να δημιουργηθούν πλατφόρμες συναγερμού σε εθνικό και ενωσιακό επίπεδο, παράλληλα με μέτρα διαγραφής και παρεμπόδισης εμφάνισης του βλαβερού περιεχομένου.

  Μέσα από εκπαιδευτικές δραστηριότητες και εκστρατείες ευαισθητοποίησης, η ΕΕ και τα κράτη μέλη μπορούν να εντείνουν τις προσπάθειές τους για την παροχή πληροφοριών και την εκπαίδευση παιδιών και οικογενειών σχετικά με την διαδικτυακή ασφάλεια, π.χ. μέσω του προγράμματος για ασφαλέστερη χρήση του διαδικτύου (Safer Internet).[11]

  Παράλληλα αναφέρεται ότι σε επιχειρησιακό επίπεδο πρέπει να επιδιωχθεί διεθνής συντονισμός δράσεων για την ασφάλεια πληροφοριών, και πρέπει να αναληφθεί κοινή δράση για την καταπολέμηση του ηλεκτρονικού εγκλήματος, με υποστήριξη του ανανεωμένου Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA).

  Τέλος, η Επιτροπή ενημερώνει συνοπτικά για τις σχετικές δράσεις που πρόκειται να γίνουν μέχρι τέλος του έτους καθώς και μελλοντικές στο αμέσως επόμενο διάστημα.

[11] https://www.saferinternet.gr/index.php?objId=Category82&parentobjId=Page15

ΔΡΑΣΕΙΣ

Η Επιτροπή πρόκειται:

- **Βασική δράση 6:** να υποβάλει το 2010 μέτρα που αποσκοπούν σε **ενισχυμένη και υψηλού επιπέδου πολιτική ασφάλειας δικτύων και πληροφοριών**, περιλαμβανομένων νομοθετικών πρωτοβουλιών, όπως ενός εκσυγχρονισμένου ευρωπαϊκού οργανισμού για την ασφάλεια δικτύων και πληροφοριών (ENISA), και μέτρα που παρέχουν τη δυνατότητα ταχύτερης αντίδρασης σε περίπτωση επιθέσεων στον κυβερνοχώρο, συμπεριλαμβανομένου CERT για τα θεσμικά όργανα της ΕΕ,

- **Βασική δράση 7**: να υποβάλει έως το 2010 μέτρα, συμπεριλαμβανομένων νομοθετικών πρωτοβουλιών, για την **καταπολέμηση επιθέσεων στον κυβερνοχώρο εναντίον συστημάτων πληροφοριών**, καθώς και συναφείς κανόνες δικαιοδοσίας στον κυβερνοχώρο σε ευρωπαϊκό και διεθνές επίπεδο, έως το 2013.

- **Άλλες δράσεις:**

    - δημιουργία, έως το 2012, **ευρωπαϊκής πλατφόρμας για εγκλήματα στον κυβερνοχώρο**,

    - έως το 2012, εξέταση της σκοπιμότητας δημιουργίας **ευρωπαϊκού κέντρου για εγκλήματα στον κυβερνοχώρο**,

Εικόνα 10: Σχετικές Δράσεις της Επιτροπής για τα μέτρα που θα ληφθούν για την Ασφάλεια Δικτύων & Πληροφοριών και αντιμετώπιση του Κυβερνοεγκλήματος

- Στις 22 Νοεμβρίου 2010, η Επιτροπή ανακοίνωσε την «Στρατηγική εσωτερικής ασφάλειας της ΕΕ στην πράξη: πέντε βήματα για μια ασφαλέστερη Ευρώπη»[22] με την οποία προτείνει πέντε στρατηγικούς στόχους και συγκεκριμένες δράσεις για τα έτη 2011-2014 οι οποίες, σε συνδυασμό με τις προσπάθειες και τις πρωτοβουλίες που έχουν ήδη αναληφθεί, θα βοηθήσουν την ΕΕ να γίνει περισσότερο ασφαλής.

  Η υλοποίηση της «Στρατηγικής εσωτερικής ασφάλειας στην πράξη» αποτελεί κοινή ευθύνη των οργάνων, των κρατών μελών και των οργανισμών της ΕΕ.

  Ανάμεσα στους στόχους βρίσκεται και η «**Αύξηση των επιπέδων ασφάλειας των πολιτών και των επιχειρήσεων στον κυβερνοχώρο**» (Στόχος 3). Όπως αναφέρεται στην παρούσα στρατηγική, το έγκλημα στον κυβερνοχώρο αποτελεί παγκόσμιο φαινόμενο που βλάπτει σημαντικά την εσωτερική αγορά της ΕΕ. Μολονότι η δομή του Διαδικτύου καθεαυτή δεν γνωρίζει σύνορα, η δικαιοδοσία για τη δίωξη του εγκλήματος στον κυβερνοχώρο εξακολουθεί να σταματά στα εθνικά σύνορα. Τα κράτη μέλη πρέπει να συντονίσουν τις προσπάθειές τους σε επίπεδο ΕΕ. Παρόλο που το τμήμα δίωξης εγκλήματος υψηλής τεχνολογίας της Europol διαδραματίζει ήδη σημαντικό συντονιστικό ρόλο για την επιβολή του νόμου, χρειάζεται να αναληφθεί περαιτέρω δράση.

  Οι δράσεις που προτείνονται είναι:

- **Δημιουργία ικανοτήτων των αρχών επιβολής του νόμου και των δικαστικών αρχών.**
  Έως το 2013, η ΕΕ θα δημιουργήσει ένα κέντρο για το έγκλημα στον κυβερνοχώρο, μέσω του οποίου τα κράτη μέλη και τα όργανα της ΕΕ θα είναι σε θέση να δημιουργούν επιχειρησιακές και αναλυτικές ικανότητες για τη διενέργεια ερευνών. Το κέντρο θα βελτιώσει την αξιολόγηση και την παρακολούθηση των υφιστάμενων προληπτικών και ερευνητικών μέτρων, θα υποστηρίξει την ανάπτυξη προγραμμάτων κατάρτισης και ευαισθητοποίησης για τις αρχές επιβολής του νόμου και τις δικαστικές αρχές, θα καθιερώσει συνεργασία με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) και διεπαφή με ένα δίκτυο εθνικών/κυβερνητικών ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT).
- **Συνεργασία με τη βιομηχανία για την παροχή δυνατοτήτων και για την προστασία των πολιτών.**
  Όλα τα κράτη μέλη πρέπει να λάβουν μέτρα ώστε οι πολίτες να μπορούν εύκολα να καταγγέλλουν τα εγκλήματα στον κυβερνοχώρο. Οι πληροφορίες αυτές, αφού αξιολογηθούν, θα πρέπει να εισάγονται στην εθνική και, εάν κρίνεται σκόπιμο, στην ευρωπαϊκή πλατφόρμα έγκαιρης προειδοποίησης για το έγκλημα στον κυβερνοχώρο. Με βάση το πολύτιμο έργο που πραγματοποιήθηκε στο πλαίσιο του προγράμματος «Ασφαλέστερο Διαδίκτυο», τα κράτη μέλη πρέπει επίσης να λάβουν μέτρα για να διευκολύνουν την παροχή οδηγιών στους πολίτες σχετικά με τις απειλές στον κυβερνοχώρο και με τα μέτρα προφύλαξης που πρέπει να λαμβάνουν. Οι οδηγίες αυτές πρέπει να περιλαμβάνουν τους τρόπους με τους οποίους οι πολίτες μπορούν να προστατεύουν την ιδιωτική τους ζωή στο Διαδίκτυο, να εντοπίζουν και να καταγγέλλουν την άγρα παιδιών μέσω του Διαδικτύου, να εξοπλίζουν τους υπολογιστές τους με βασικό αντι-ιικό λογισμικό και με τείχη προστασίας (firewalls), να διαχειρίζονται τους προσωπικούς κωδικούς τους και να αναγνωρίζουν το ηλεκτρονικό «ψάρεμα» (phishing) και άλλες επιθέσεις.
- **Βελτίωση της δυνατότητας αντιμετώπισης επιθέσεων στον κυβερνοχώρο.**
  Πρέπει να ληφθούν συγκεκριμένα μέτρα για τη βελτίωση της πρόληψης, του εντοπισμού και της ταχείας αντίδρασης σε περίπτωση επιθέσεων ή πρόκλησης διαταραχών στον κυβερνοχώρο. Πρώτον, έως το 2012 όλα τα κράτη μέλη, καθώς και τα ίδια τα θεσμικά όργανα της ΕΕ, πρέπει να διαθέτουν μια αποτελεσματική ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT). Είναι σημαντικό να συνεργάζονται όλες οι CERT - μόλις δημιουργηθούν - με τις αρχές επιβολής του νόμου για την πρόληψη και την αντιμετώπιση. Δεύτερον, έως το 2012 τα κράτη μέλη πρέπει να διαδικτυώσουν τις εθνικές / δημόσιες CERT τους με σκοπό να αυξηθεί η ετοιμότητα της Ευρώπης. Η δραστηριότητα αυτή θα είναι επίσης αποφασιστικής σημασίας προκειμένου να αναπτυχθεί, με την υποστήριξη της Επιτροπής και του ENISA, έως το 2012 το ευρωπαϊκό σύστημα συναγερμού και ανταλλαγής πληροφοριών (EISAS), και να δημιουργηθεί δίκτυο σημείων επαφής μεταξύ των αρμόδιων φορέων και των κρατών μελών. Τρίτον, τα κράτη μέλη μαζί με τον ENISA πρέπει να καταρτίσουν εθνικά σχέδια έκτακτης ανάγκης και να πραγματοποιούν τακτικά ασκήσεις σε εθνικό και ευρωπαϊκό επίπεδο για την αντιμετώπιση τέτοιων περιστατικών

και για την αποκατάσταση μετά από καταστροφές. Ο ENISA θα παρέχει υποστήριξη στις δράσεις αυτές με σκοπό την αύξηση του επιπέδου των CERT στην Ευρώπη.

2013

Στις 7 Φεβρουαρίου 2013 η Ευρωπαϊκή Επιτροπή εξέδωσε οδηγία σχετικά με μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση.[23]

Πρόκειται για την πρώτη Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο και καθορίζει στρατηγικούς στόχους και συγκεκριμένες δράσεις για την επίτευξη ανθεκτικότητας, τη μείωση του ηλεκτρονικού εγκλήματος και την επεξεργασία πολιτικής και ανάπτυξη ικανοτήτων για την άμυνα στον κυβερνοχώρο.

Οι στόχοι της προτεινόμενης οδηγίας είναι οι ακόλουθοι:

1. Όλα τα κράτη μέλη υποχρεούνται να εξασφαλίσουν ότι έχει τεθεί σε εφαρμογή ένα ελάχιστο επίπεδο εθνικών ικανοτήτων, με τον καθορισμό αρχών αρμόδιων για την NIS, τη σύσταση ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) και με τη θέσπιση εθνικών στρατηγικών ΑΔΠ και εθνικών σχεδίων συνεργασίας για την ασφάλεια δικτύων και πληροφοριών.
2. Οι αρμόδιες εθνικές αρχές πρέπει να συνεργάζονται σε ένα δίκτυο που θα εξασφαλίζει ασφαλή και αποτελεσματικό συντονισμό, συμπεριλαμβανομένης της συντονισμένης ανταλλαγής πληροφοριών, καθώς και ανίχνευση και απόκριση σε επίπεδο ΕΕ. Μέσω του δικτύου αυτού, τα κράτη μέλη αναμένεται ότι θα ανταλλάσσουν πληροφορίες και θα συνεργάζονται για την αντιμετώπιση απειλών και συμβάντων σε βάρος της ΑΔΠ, με βάση το ευρωπαϊκό σχέδιο συνεργασίας για την ασφάλεια δικτύων και πληροφοριών.
3. Με βάση το υπόδειγμα της οδηγίας πλαίσιο για τις ηλεκτρονικές επικοινωνίες, η πρόταση αποσκοπεί να εξασφαλίσει την ανάπτυξη κλίματος διαχείρισης κινδύνων και την ανταλλαγή πληροφοριών μεταξύ του ιδιωτικού και του δημόσιου τομέα.

Συγκεκριμένα, στο άρθρο 5 της οδηγίας, κάθε κράτος μέλος θεσπίζει εθνική στρατηγική για την Ασφάλεια Δικτύων και Πληροφοριών (ΑΔΠ) που καθορίζει τους στρατηγικούς στόχους και συγκεκριμένα μέτρα, πολιτικής και ρυθμιστικά, για να επιτευχθεί και να διατηρηθεί υψηλό επίπεδο ασφάλειας δικτύων και πληροφοριών.
Επίσης στο άρθρο 6 αναφέρει ότι κάθε κράτος μέλος ορίζει μια εθνική αρμόδια αρχή σχετικά με την ασφάλεια των συστημάτων δικτύων και πληροφοριών.

2014

Στο νομοθετικό ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 13ης Μαρτίου 2014 σχετικά με την πρόταση οδηγίας που εξέδωσε η Ευρωπαϊκή Επιτροπή τον Φεβρουάριο 2013, διαπιστώνεται ότι αυξάνεται το μέγεθος, η συχνότητα και ο αντίκτυπος συμβάντων

ασφάλειας με και συνιστά μείζονα απειλή για τη λειτουργία των δικτύων και των συστημάτων πληροφοριών, τα οποία μπορούν να αποτελέσουν εύκολο στόχο σκόπιμων επιζήμιων ενεργειών που έχουν σκοπό την πρόκληση βλαβών ή την διακοπή της λειτουργία τους. Μερικές από τις πιο σημαντικές τροπολογίες όσον αφορά την ασφάλεια των συστημάτων είναι οι ακόλουθες:

- **Τροπολογία 3**: Δεδομένου ότι οι κοινές αιτίες συστημικής αστοχίας παραμένουν ακούσιες, όπως φυσικοί παράγοντες ή ανθρώπινο λάθος, οι υποδομές θα πρέπει να είναι ανθεκτικές τόσο σε σκόπιμες όσο και σε ακούσιες διαταραχές, και οι φορείς εκμετάλλευσης κρίσιμης υποδομής θα πρέπει να σχεδιάζουν τα συστήματα με γνώμονα την ανθεκτικότητα.
- **Τροπολογία 8**: Θα πρέπει να εφαρμοστούν ελάχιστα κοινά πρότυπα με βάση κατάλληλες συστάσεις των ομάδων συντονισμού για την ασφάλεια στον κυβερνοχώρο (CSGC).
- **Τροπολογία 10**: Κάθε κράτος μέλος θα πρέπει να πληροί κοινά πρότυπα όσον αφορά το μορφότυπο και την ανταλλαξιμότητα των δεδομένων που θα πρέπει να ανταλλάσσονται και να αξιολογούνται. Τα κράτη μέλη θα πρέπει να μπορούν να ζητούν τη συνδρομή του ενωσιακού Οργανισμού Ασφάλειας Δικτύων και Πληροφοριών («ENISA») για την ανάπτυξη των εθνικών τους στρατηγικών ΑΔΠ, βάσει ενός ελάχιστου κοινού προτύπου στρατηγικής ΑΔΠ.
- **Τροπολογία 42**: Κάθε χρήση των δεδομένων προσωπικού χαρακτήρα περιορίζεται στο απολύτως αναγκαίο για τους σκοπούς της παρούσας οδηγίας, τα δε δεδομένα αυτά πρέπει να είναι σε όσο το δυνατόν μεγαλύτερο βαθμό, αν όχι εντελώς, ανώνυμα.

Παράλληλα, με ειδικές τροπολογίες (**Τροπολογίες 44 - 46**), ο όρος «Ηλεκτρονικά Δεδομένα» αντικαθίσταται από τον όρο «Ψηφιακά Δεδομένα» και στον ορισμό της «Ασφάλειας» περιλαμβάνονται και τα κατάλληλα τεχνικά μέσα, λύσεις και επιχειρησιακές διαδικασίες που διασφαλίζουν τις απαιτήσεις ασφάλειας οι οποίες ορίζονται στην παρούσα οδηγία.[24]

2016

- Στις 5 Ιουλίου 2016 η Ευρωπαϊκή Επιτροπή εξέδωσε ανακοίνωση σχετικά με την ενίσχυση του συστήματος κυβερνοανθεκτικότητας της Ευρώπης και προώθηση ανταγωνιστικού και καινοτόμου κλάδου ασφάλειας στον κυβερνοχώρο,[25] στην οποία ανακοινώθηκαν περαιτέρω μέτρα για την αναβάθμιση της συνεργασίας και ανταλλαγής πληροφοριών και γνώσεων και την ενίσχυση της ανθεκτικότητας και της ετοιμότητας της ΕΕ.

  Τα συγκεκριμένα μέτρα και οι ανακοινώσεις ενισχύθηκαν με τα συμπεράσματα του Συμβουλίου του 2016, με τα οποία αναγνωρίστηκε ότι «οι απειλές και τα ευάλωτα σημεία στον κυβερνοχώρο εξακολουθούν να αυξάνονται και να εντείνονται, πράγμα που θα απαιτήσει συνεχή και στενότερη συνεργασία, ιδίως στο πλαίσιο της αντιμετώπισης διασυνοριακών συμβάντων ασφάλειας στον κυβερνοχώρο μεγάλης κλίμακας». Στα συμπεράσματα επιβεβαιώθηκε ότι ο κανονισμός ENISA αποτελεί μία από «τις βασικές συνιστώσες ενός πλαισίου της ΕΕ για την ανθεκτικότητα στον κυβερνοχώρο»[26] και η Επιτροπή κλήθηκε να λάβει περαιτέρω μέτρα για την αντιμετώπιση του ζητήματος της πιστοποίησης σε ευρωπαϊκό επίπεδο.

- Το ίδιο έτος (19 Ιουλίου) το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της ΕΕ εξέδωσε την **οδηγία NIS**[27] (Network and Information Systems), η οποία θα αρχίσει να εφαρμόζεται από τον Μάιο του 2018 και στοχεύει στην υιοθέτηση μέτρων από όλα τα κράτη μέλη της Ε.Ε προκειμένου να επιτευχθεί ένα υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου. Η οδηγία επιβάλει στους παρόχους ψηφιακών υπηρεσιών να προσδιορίσουν και να λάβουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων και την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων που επηρεάζουν την ασφάλεια. Ταυτόχρονα, θα πρέπει να κοινοποιούν στην αρμόδια αρχή ή την CSIRT χωρίς αδικαιολόγητη καθυστέρηση κάθε συμβάν που έχει σημαντικό αντίκτυπο.[28]

  Επίσης, η οδηγία επιβάλει ιδιαίτερες υποχρεώσεις στα κράτη μέλη. Τα κράτη μέλη θα πρέπει να καταστρώσουν μια **εθνική στρατηγική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών** και να ορίσουν ένα **εθνικό ενιαίο κέντρο επαφής** για την ασφάλεια των συστημάτων δικτύου και πληροφοριών («ενιαίο κέντρο επαφής»). Στο πλαίσιο της οδηγίας προβλέπεται επίσης η ίδρυση ενός **δικτύου - national CSIRTs**, γνωστών επίσης ως «ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική» (Computer Emergency Response Teams - CERT) και η σύσταση και λειτουργία μιας «**Ομάδας Συνεργασίας**» αποτελούμενη από εκπροσώπους των κρατών μελών, της Επιτροπής και του ENISA για την υποστήριξη και διευκόλυνση της στρατηγικής συνεργασίας καθώς και της ανταλλαγής πληροφοριών, και την καλλιέργεια πνεύματος αξιοπιστίας και εμπιστοσύνης.

  Να παρατηρήσουμε ότι ακόμη δεν υπάρχει επίσημη εθνική στρατηγική για την κυβερνοασφάλεια, υπάρχουν, όμως, πολλοί διαφορετικοί δημόσιοι αλλά και ιδιωτικοί φορείς που ασχολούνται θεσμικά στο πλαίσιο των αρμοδιοτήτων τους με την αντιμετώπιση του κυβερνοεγκλήματος.

- Παράλληλα, ο γενικός κανονισμός για την προστασία των δεδομένων (ΓΚΠΔ) τέθηκε σε ισχύ το 2016 και σε εφαρμογή από τον Μάιο του 2018. Στόχο έχει την προστασία των δεδομένων προσωπικού χαρακτήρα των Ευρωπαίων πολιτών, μέσω του καθορισμού κανόνων για την επεξεργασία και τη διάδοσή τους. Παρέχει στα υποκείμενα των δεδομένων ορισμένα δικαιώματα και συνεπάγεται υποχρεώσεις για τους υπεύθυνους επεξεργασίας δεδομένων (τους παρόχους ψηφιακών υπηρεσιών) σχετικά με τη χρήση και τη διαβίβαση πληροφοριών. Επιπλέον, επιβάλλει απαιτήσεις κοινοποίησης σε περίπτωση παραβίασης και προβλέπει πρόστιμα για ορισμένες περιπτώσεις.

  Στην επόμενη εικόνα επεξηγείται πώς η **οδηγία NIS** και ο **ΓΚΠΔ** αλληλοσυμπληρώνονται στις επιδιώξεις τους για την ενίσχυση της κυβερνοασφάλειας και τη διασφάλιση της προστασίας των δεδομένων.

Εικόνα 11: Πώς αλληλοσυμπληρώνονται ο κανονισμός ΓΚΠΔ και η οδηγία NIS[12]

2017

- Στις 10 Μαρτίου 2017 η Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή (ΕΟΚΕ), της οποίας πρόεδρος κατά το έτος αυτό ήταν η Ελλάδα, εξέδωσε ανακοίνωση σχετικά με την ενίσχυση του συστήματος κυβερνοανθεκτικότητας της Ευρώπης και προώθηση ανταγωνιστικού και καινοτόμου κλάδου ασφάλειας στον κυβερνοχώρο.[29]

  Τα μέτρα που προτείνει η Επιτροπή κάνουν χρήση των διατάξεων της οδηγίας ΑΔΠ για την ενίσχυση της συνεργασίας στον τομέα της ασφάλειας στον κυβερνοχώρο, την ανταλλαγή πληροφοριών, την κατάρτιση και την οργάνωση ασφαλείας σε ολόκληρη την Ένωση. Επίσης, προτείνει μέτρα που θα διευκολύνουν την ανάπτυξη ενός ισχυρού ευρωπαϊκού κλάδου για την ασφάλεια στον κυβερνοχώρο μέσω απαιτήσεων σχετικών με την κατάρτιση, τις επενδύσεις και την ενιαία αγορά, καθώς και μέσω της δημιουργίας μιας νέας σύμπραξης δημοσίου-ιδιωτικού τομέα σχετικά με την ασφάλεια στον κυβερνοχώρο.

  Στην ανακοίνωση αναφέρεται ότι η ΕΟΚΕ έχει εντυπωσιαστεί από τις ικανότητες που έχει αναπτύξει ο ENISA με την πάροδο του χρόνου και πιστεύει ότι θα μπορούσε να συμβάλει ακόμη περισσότερο στη θωράκιση και στην ασφάλεια της ΕΕ στον κυβερνοχώρο. Η επιχειρησιακή εντολή του ENISA θα πρέπει να ενισχυθεί προκειμένου να σημειωθεί αποτελεσματικότερη αύξηση της ευαισθητοποίησης και της απόκρισης σχετικά με τις επιθέσεις στον κυβερνοχώρο σε ολόκληρη την Ένωση. Θα μπορούσε λοιπόν να επεκταθεί ο ρόλος του, προκειμένου να αυξηθεί η αξία που παράγει για την ΕΕ, τα κράτη μέλη, τους πολίτες και τις επιχειρήσεις. Επίσης, ο ENISA θα πρέπει να καταστεί πιο άμεσα υπεύθυνος

[12] Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια (2019), σελ 19

για την προώθηση προγραμμάτων εκπαίδευσης και ευαισθητοποίησης ειδικά εστιασμένων στους πολίτες και στις ΜΜΕ.

- Στις 4 Οκτωβρίου 2017 η Ευρωπαϊκή Επιτροπή παρουσίασε Κανονισμό του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου σχετικά με τον ENISA, τον «οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο», και την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013, σχετικά με την πιστοποίηση της ασφάλειας στον κυβερνοχώρο στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών («πράξη για την ασφάλεια στον κυβερνοχώρο»).[30]

  Στον Κανονισμό η Επιτροπή συνειδητοποιεί, ξεκάθαρα πλέον, τις αυξημένες προκλήσεις που αντιμετωπίζει η Ένωση στον τομέα της ασφάλειας στον κυβερνοχώρο, και φαίνεται έκδηλη η ανάγκη για ολοκληρωμένη σειρά μέτρων που βασίζονται σε προηγούμενες δράσεις της Ένωσης και ευνοούν τους αλληλοενισχυόμενους στόχους.[13] [Εκτίμηση No. 4]

  Επίσης γίνεται αναφορά στην αποτελεσματικότητα και αποδοτικότητα του ENISA, των μέτρων ασφάλειας που έχουν ήδη ληφθεί το χρονικό διάστημα 2013-2016 προτείνοντας, παράλληλα, νέους στόχους και νέες στοχευμένες δράσεις για την κυβερνοασφάλεια και κυβερνοενθεκτικότητα.

2018

- Στις 16 Αυγούστου 2018 η Ευρωπαϊκή Επιτροπή εξέδωσε ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά με την άμεση ισχύ του γενικού κανονισμού για την προστασία δεδομένων από την 25η Μαΐου 2018.
  Η ανακοίνωση επιγραμματικά:
  - ανακεφαλαιώνει τις κύριες καινοτομίες και τις ευκαιρίες που διανοίγονται από τη νέα νομοθεσία της ΕΕ για την προστασία των δεδομένων
  - καταγράφει τις προπαρασκευαστικές εργασίες που έχουν πραγματοποιηθεί μέχρι στιγμής σε επίπεδο ΕΕ
  - περιγράφει τι θα πρέπει ακόμη να κάνουν η Ευρωπαϊκή Επιτροπή, οι εθνικές αρχές προστασίας δεδομένων και οι εθνικές διοικήσεις, ώστε η προετοιμασία να ολοκληρωθεί επιτυχώς
  - παραθέτει τα μέτρα που σκοπεύει να λάβει η Επιτροπή κατά τους προσεχείς μήνες.

[13] Σε αυτά περιλαμβάνεται η ανάγκη περαιτέρω αύξησης των ικανοτήτων και της ετοιμότητας των κρατών μελών και των επιχειρήσεων, καθώς και η ανάγκη βελτίωσης της συνεργασίας και του συντονισμού σε όλα τα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ. Επιπλέον, δεδομένης της διασυνοριακής φύσης των απειλών στον κυβερνοχώρο, υπάρχει ανάγκη αύξησης των ικανοτήτων σε επίπεδο Ένωσης που θα μπορούσαν να συμπληρώσουν τη δράση των κρατών μελών, ιδίως στην περίπτωση των μεγάλης κλίμακας διασυνοριακών συμβάντων και κρίσεων στον κυβερνοχώρο.

- Στις 13 Ιουνίου 2018 το Ευρωπαϊκό Κοινοβούλιο εξέδωσε Ψήφισμα σχετικά με την άμυνα στον κυβερνοχώρο (2018/2004(INI)).[31] Στο πλαίσιο ανάπτυξης ικανοτήτων για την κυβερνοάμυνα και την κυβερνοαποτροπή, τα κράτη μέλη παροτρύνονται να αυξήσουν τους οικονομικούς και ανθρώπινους πόρους, ιδίως σε εμπειρογνώμονες κυβερνοϊατροδικαστικής, προκειμένου να βελτιωθεί η εξακρίβωση της προέλευσης των κυβερνοεπιθέσεων, κάνοντας λόγο ότι η συνεργασία αυτή θα πρέπει να υλοποιηθεί επίσης μέσω της ενίσχυσης του ENISA.

  Αναγνωρίζει τις προόδους που σημειώνονται σε τομείς όπως η νανοτεχνολογία, η τεχνητή νοημοσύνη, τα μαζικά δεδομένα, τα απόβλητα ηλεκτρικού και ηλεκτρονικού εξοπλισμού και η προηγμένη ρομποτική, παροτρύνει τα κράτη μέλη και την ΕΕ να δώσουν ιδιαίτερη προσοχή στην πιθανή εκμετάλλευση των εν λόγω περιοχών από εχθρικούς κρατικούς παράγοντες και από ομάδες του οργανωμένου εγκλήματος, ζητεί την ανάπτυξη κατάρτισης και δυνατοτήτων που να αποβλέπουν στην προστασία από την εμφάνιση περίπλοκων εγκληματικών σχεδίων, όπως οι πολύπλοκες απάτες ταυτότητας και η παραποίηση αγαθών.

  Τονίζει την ανάγκη μεγαλύτερης ορολογικής σαφήνειας σχετικά με την κυβερνοασφάλεια, καθώς και εμπεριστατωμένης και ολοκληρωμένης προσέγγισης και κοινών προσπαθειών για την αντιμετώπιση κυβερνοαπειλών και υβριδικών απειλών, την ανίχνευση και την εξάλειψη εξτρεμιστικών και εγκληματικών καταφυγίων στο διαδίκτυο μέσω της ενίσχυσης και της αύξησης της ανταλλαγής πληροφοριών μεταξύ της ΕΕ και οργανισμών της ΕΕ όπως η Ευρωπόλ, η Eurojust, ο ΕΟΑ και ο ENISA.

  Υπογραμμίζει τον αυξανόμενο ρόλο της τεχνητής νοημοσύνης τόσο στα κυβερνοαδικήματα όσο και στην κυβερνοάμυνα, καλεί την ΕΕ και τα κράτη μέλη να δώσουν ιδιαίτερη σημασία σε αυτόν τον τομέα, τόσο κατά την έρευνα όσο και κατά την πρακτική ανάπτυξη των δυνατοτήτων κυβερνοάμυνάς τους.

  Τέλος, τονίζει με έμφαση ότι με την ανάπτυξη μη επανδρωμένων οχημάτων αέρος, οπλισμένων ή μη, θα πρέπει να ληφθούν πρόσθετα μέτρα για τη μείωση των πιθανών κυβερνοευπαθειών τους.

2019

Στις 17 Απριλίου 2019 το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο εξέδωσε κανονισμό σχετικά με τον ENISA 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) [32]

Οι στόχοι που αναφέρονται στον κανονισμό είναι ότι ο ENISA:

1. αποτελεί κέντρο εμπειρογνωσίας σε θέματα κυβερνοασφάλειας χάρη στην ανεξαρτησία του, την επιστημονική και τεχνική ποιότητα των συμβουλών και της επικουρίας που παρέχει, τις πληροφορίες που παρέχει, τη διαφάνεια των επιχειρησιακών διαδικασιών του, τις μεθόδους λειτουργίας και την επιμέλεια με την οποία εκτελεί τα καθήκοντά του.
2. 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.

3. στηρίζει την ανάπτυξη ικανοτήτων και την ετοιμότητα στην Ένωση, επικουρώντας τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, καθώς και τα κράτη μέλη και τους ιδιωτικούς και δημόσιους συμφεροντούχους, με σκοπό 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.
4. προάγει τη συνεργασία, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών, και τον συντονισμό σε ενωσιακό επίπεδο ανάμεσα στα κράτη μέλη, τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και στους σχετικούς ιδιωτικούς και δημόσιους συμφεροντούχους σε θέματα που σχετίζονται με την κυβερνοασφάλεια.
5. συμβάλλει στην αύξηση των ικανοτήτων κυβερνοασφάλειας σε επίπεδο Ένωσης προκειμένου να στηρίζει τις ενέργειες των κρατών μελών όσον αφορά την πρόληψη και την αντιμετώπιση κυβερνοαπειλών, ιδίως σε περίπτωση διασυνοριακών συμβάντων.
6. προάγει τη χρήση της ευρωπαϊκής πιστοποίησης της κυβερνοασφάλειας προκειμένου να αποφευχθεί ο κατακερματισμός της εσωτερικής αγοράς. Ο ENISA συμβάλλει στη θέσπιση και τη διατήρηση ενός ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας σύμφωνα με τον τίτλο III του παρόντος κανονισμού, προκειμένου να αυξηθεί η διαφάνεια της κυβερνοασφάλειας των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ και, επομένως, να ενισχυθεί η εμπιστοσύνη στην ψηφιακή εσωτερική αγορά και η ανταγωνιστικότητά της.
7. προάγει ένα υψηλό επίπεδο ευαισθητοποίησης ως προς την κυβερνοασφάλεια, συμπεριλαμβανομένης της κυβερνο-υγιεινής μεταξύ πολιτών, οργανισμών και επιχειρήσεων.

Πιο συγκεκριμένα, στο άρθρο 51, αναφέρονται οι στόχοι ασφάλειας για τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας.

Ένα ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας σχεδιάζεται κατά τέτοιο τρόπο ώστε να επιτυγχάνει, κατά περίπτωση, τουλάχιστον τους ακόλουθους στόχους ασφάλειας:

- την προστασία δεδομένων που έχουν αποθηκευτεί, διαβιβαστεί ή αποτελέσει με άλλον τρόπο αντικείμενο επεξεργασίας από τυχαία ή μη εγκεκριμένη αποθήκευση, επεξεργασία, πρόσβαση ή αποκάλυψη, κατά τη διάρκεια ολόκληρου του κύκλου ζωής του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ ή της διαδικασίας ΤΠΕ,
- ότι εγκεκριμένα άτομα, προγράμματα ή μηχανήματα μπορούν να έχουν πρόσβαση σε δεδομένα, υπηρεσίες ή λειτουργίες που καλύπτονται από το δικαίωμα πρόσβασης που τους παρέχεται,
- τον εντοπισμό και την τεκμηρίωση γνωστών εξαρτήσεων και τρωτών σημείων, 7.6.2019 EL Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης L 151/55
- την καταγραφή των δεδομένων, υπηρεσιών ή λειτουργιών στα οποία πραγματοποιήθηκε πρόσβαση, τα οποία χρησιμοποιήθηκαν ή αποτέλεσαν με άλλον τρόπο αντικείμενο επεξεργασίας, καθώς και του πότε και από ποιον,
- τη δυνατότητα να ελέγχεται σε ποια δεδομένα, υπηρεσίες ή λειτουργίες πραγματοποιήθηκε πρόσβαση, ποια χρησιμοποιήθηκαν ή αποτέλεσαν με άλλον τρόπο αντικείμενο επεξεργασίας, πότε και από ποιον,
- την επαλήθευση ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ δεν έχουν γνωστά τρωτά σημεία,

- την έγκαιρη αποκατάσταση της διαθεσιμότητας και της πρόσβασης σε δεδομένα, υπηρεσίες και λειτουργίες σε περίπτωση φυσικού ή τεχνικού συμβάντος,
- ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ προστατεύονται εξ ορισμού και από τον σχεδιασμό τους,
- ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ παρέχονται με επικαιροποιημένο λογισμικό και υλισμικό που δεν περιέχουν γνωστά στο κοινό τρωτά σημεία, και προβλέπονται μηχανισμοί για ασφαλείς επικαιροποιήσεις.

2020

Στις 16 Δεκεμβρίου 2020 το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο εξέδωσε Οδηγία σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148[33]

Η παρούσα πρόταση έχει ως βάση και καταργεί την οδηγία (ΕΕ) 2016/1148 για την ασφάλεια των συστημάτων δικτύου και πληροφοριών (οδηγία NIS), η οποία αποτελεί την πρώτη νομοθετική πράξη της ΕΕ για την κυβερνοασφάλεια και προβλέπει νομικά μέτρα για την ενίσχυση του συνολικού επιπέδου κυβερνοασφάλειας στην Ένωση.

Πρόκειται, ουσιαστικά, για μια νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια, η οποία δίνει στην ΕΕ τη δυνατότητα να ενισχύσει τον ηγετικό της ρόλο όσον αφορά τους διεθνείς κανόνες και τα διεθνή πρότυπα στον κυβερνοχώρο.[34]

Επιπλέον, η Επιτροπή υποβάλλει προτάσεις για την αντιμετώπιση τόσο της κυβερνοανθεκτικότητας όσο και της φυσικής ανθεκτικότητας των κρίσιμων οντοτήτων και δικτύων: μια οδηγία σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση[35] (**αναθεωρημένη οδηγία NIS ή «NIS 2»**) και μια νέα οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων.[36]

Ο λόγος κατάργησης της οδηγίας NIS είναι το γεγονός ότι, παρόλο που έχει σημειωθεί σημαντική πρόοδος όσον αφορά την αύξηση του επιπέδου ανθεκτικότητας της κυβερνοασφάλειας της Ένωσης, το πεδίο εφαρμογής της οδηγίας είναι υπερβολικά περιορισμένο όσον αφορά τους τομείς που καλύπτει. Αυτό συμβαίνει κυρίως λόγω της αυξημένης ψηφιοποίησης κατά τα τελευταία έτη και του υψηλότερου βαθμού διασύνδεσης, καθώς και το ότι του πεδίο εφαρμογής της οδηγίας NIS δεν καλύπτει πλέον όλους τους ψηφιοποιημένους τομείς που παρέχουν βασικές υπηρεσίες στην οικονομία και την κοινωνία στο σύνολό της.

Λαμβάνοντας υπόψη την αυξημένη ψηφιοποίηση της εσωτερικής αγοράς τα τελευταία χρόνια και το εξελισσόμενο τοπίο των απειλών για την κυβερνοασφάλεια, η πρόταση επιχειρεί να εκσυγχρονίσει το υφιστάμενο νομικό πλαίσιο. Και οι δύο αυτές εξελίξεις έχουν επιταχυνθεί περαιτέρω μετά την έναρξη της κρίσης της COVID-19. Η πανδημία της COVID-19 κατέδειξε την τρωτότητα των ολοένα και πιο αλληλεξαρτώμενων κοινωνιών μας απέναντι σε κινδύνους χαμηλής πιθανότητας. Καταλήγουμε στο συμπέρασμα ότι η ανθεκτικότητα της κυβερνοασφάλειας στην Ένωση δεν μπορεί να είναι αποτελεσματική αν δεν ακολουθείται μια ομοιογενής προσέγγιση από όλα τα κράτη-μέλη.

Οι γενικοί στόχοι της αναθεώρησης είναι:

- Αύξηση του επιπέδου κυβερνοανθεκτικότητας ενός ολοκληρωμένου συνόλου επιχειρήσεων που δραστηριοποιούνται στην Ευρωπαϊκή Ένωση σε όλους τους σχετικούς τομείς,
- Μείωση των ασυνεπειών στην ανθεκτικότητα εντός της εσωτερικής αγοράς στους τομείς που καλύπτονται ήδη από την οδηγία και
- Βελτίωση του επιπέδου κοινής επίγνωσης της κατάστασης και η συλλογική ικανότητα προετοιμασίας και αντίδρασης.

Οι ειδικοί στόχοι είναι:

- Διασφάλιση ότι οι οντότητες σε όλους τους τομείς που εξαρτώνται από δικτυακά και πληροφοριακά συστήματα και παρέχουν βασικές υπηρεσίες στην οικονομία και την κοινωνία συνολικά υποχρεούνται να λαμβάνουν μέτρα κυβερνοασφάλειας και να αναφέρουν περιστατικά με σκοπό την αύξηση του συνολικού επιπέδου κυβερνοανθεκτικότητας σε ολόκληρη την εσωτερική αγορά.
- Διασφάλιση ότι όλες οι οντότητες οι οποίες δραστηριοποιούνται σε τομείς που καλύπτονται από το νομικό πλαίσιο NIS και οι οποίες είναι παρόμοιου μεγέθους και έχουν συγκρίσιμο ρόλο υπόκεινται στο ίδιο ρυθμιστικό καθεστώς (είτε εμπίπτουν στο πεδίο εφαρμογής είτε όχι), ανεξάρτητα από τη δικαιοδοσία στην οποία υπάγονται εντός της ΕΕ.
- Διασφάλιση ότι οι αρμόδιες αρχές εφαρμόζουν αποτελεσματικότερα τους κανόνες που ορίζονται από τη νομική πράξη μέσω εναρμονισμένων μέτρων εποπτείας και επιβολής και να διασφαλιστεί συγκρίσιμο επίπεδο μεταξύ κρατών μελών όσον αφορά τους πόρους που διατίθενται στις αρμόδιες αρχές και θα τους παρέχουν τη δυνατότητα να εκπληρώνουν τα βασικά καθήκοντα τα οποία ορίζονται από το πλαίσιο NIS.
- Διασφάλιση της ανταλλαγής βασικών πληροφοριών μεταξύ κρατών μελών με την επιβολή στις αρμόδιες αρχές σαφών υποχρεώσεων ανταλλαγής πληροφοριών και συνεργασίας όταν πρόκειται για κυβερνοαπειλές και περιστατικά, καθώς και με την ανάπτυξη ενωσιακής κοινής επιχειρησιακής ικανότητας για την αντιμετώπιση κρίσεων.

2021

- Στις 20 Μαΐου 2021 το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο εξέδωσε Κανονισμό για τη σύσταση του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού.[37]

  Η διαδικασία επιλογής της έδρας του Ευρωπαϊκού Βιομηχανικού, Τεχνολογικού και Ερευνητικού Κέντρου Αρμοδιότητας στον τομέα της Κυβερνοασφάλειας (ECCC) άρχισε στις 28 Οκτωβρίου 2020. Για την απόφαση απαιτείτο κοινή συμφωνία των κρατών μελών. Τα κράτη μέλη ψήφισαν για την έδρα του ECCC στις 9 Δεκεμβρίου 2020, στο περιθώριο της Επιτροπής των Μονίμων Αντιπροσώπων των κυβερνήσεων των κρατών μελών στην Ευρωπαϊκή Ένωση

(ΕΜΑ). Η τοποθεσία που επιλέχθηκε για το Κέντρο είναι το Βουκουρέστι της Ρουμανίας.[14]

Ο ρόλος του Κέντρου Αρμοδιότητας είναι να συμβάλει στην ενίσχυση της ασφάλειας των συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένου του διαδικτύου και άλλων υποδομών κρίσιμης σημασίας για τη λειτουργία της κοινωνίας, όπως οι μεταφορές, η υγεία, η ενέργεια, οι ψηφιακές υποδομές, το νερό, οι χρηματοπιστωτικές αγορές και τα τραπεζικά συστήματα.

Ανάμεσα στις πολύ σημαντικές εκτιμήσεις του Κοινοβουλίου, θα σταθούμε στο γεγονός ότι, παρόλο που η πλειονότητα του πληθυσμού της Ένωσης συνδέεται στο διαδίκτυο και η καθημερινή ζωή των ανθρώπων και των οικονομιών εξαρτάται ολοένα και περισσότερο από τις ψηφιακές τεχνολογίες, η Ένωση εξακολουθεί να μην διαθέτει επαρκείς τεχνολογικές και βιομηχανικές ικανότητες και δυνατότητες που θα της επιτρέπουν να προστατεύει αυτόνομα την οικονομία και τις κρίσιμης σημασίας υποδομές, καθώς το επίπεδο στρατηγικού και διαχρονικού συντονισμού και συνεργασίας μεταξύ βιομηχανιών, ερευνητικών κοινοτήτων στον τομέα της κυβερνοασφάλειας και κυβερνήσεων κρίνεται ανεπαρκές.

Μία από τις προκλήσεις που καλείται να αντιμετωπίσει το Κέντρο Αρμοδιότητας είναι ότι, λόγω της ταχέως μεταβαλλόμενης φύσης των κυβερνοαπειλών και της κυβερνοασφάλειας, θα πρέπει να είναι σε θέση να προσαρμόζεται γρήγορα και συνεχώς στις νέες εξελίξεις στον τομέα αυτό. Συνεπώς, το Κέντρο Αρμοδιότητας, το δίκτυο και η κοινότητα θα πρέπει να διαθέτουν επαρκή ευελιξία ώστε να εξασφαλίζεται η απαιτούμενη ικανότητα ανταπόκρισης σε τέτοιες εξελίξεις.

Οι ειδικοί στόχοι του Κέντρου Αρμοδιότητας είναι:

- η ενίσχυση των ικανοτήτων, δυνατοτήτων, γνώσεων και υποδομής κυβερνοασφάλειας προς όφελος της βιομηχανίας, ιδίως των ΜΜΕ, των ερευνητικών κοινοτήτων, του δημόσιου τομέα και της κοινωνίας των πολιτών, κατά περίπτωση
- η προώθηση της ανθεκτικότητας στον τομέα της κυβερνοασφάλειας και η υιοθέτηση βέλτιστων πρακτικών κυβερνοασφάλειας,
- εφαρμογή της αρχής της ασφάλειας από το στάδιο του σχεδιασμού και η πιστοποίηση της ασφάλειας των ψηφιακών προϊόντων και υπηρεσιών με τρόπο που συμπληρώνει τις προσπάθειες άλλων δημόσιων οντοτήτων
- η συμβολή στη δημιουργία ενός ισχυρού ευρωπαϊκού οικοσυστήματος κυβερνοασφάλειας, στο οποίο θα συμμετέχουν όλοι οι ενδιαφερόμενοι φορείς.

- Στις 23 Ιουνίου 2021 η Ευρωπαϊκή Επιτροπή εξέδωσε Έκθεση σχετικά με την εφαρμογή της στρατηγικής κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία.[38] Σύμφωνα με την Έκθεση, η ανθεκτικότητα, η επιχειρησιακή ικανότητα και ο ανοικτός χαρακτήρας του κυβερνοχώρου είναι πιο σημαντικά από ποτέ. Μετά την πανδημία, η κυβερνοασφάλεια είναι απαραίτητη για την ανάπτυξη ευφυέστερης και πιο πράσινης τεχνολογίας στον κόσμο.

  Ένα σοβαρό στοιχείο που αναφέρεται είναι ότι, όσον αφορά τις κυβερνοαπειλές, η ΕΕ δεν διαθέτει συλλογική επίγνωση της κατάστασης. Αυτό οφείλεται στο γεγονός ότι οι εθνικές αρχές δεν συλλέγουν και δεν ανταλλάσσουν συστηματικά πληροφορίες, όπως αυτές που διατίθενται από τον ιδιωτικό τομέα, οι

[14] https://www.consilium.europa.eu/el/policies/cybersecurity/seat-selection-cybersecurity-centre/

οποίες θα μπορούσαν να συμβάλουν στην αξιολόγηση της κατάστασης κυβερνοασφάλειας στην ΕΕ. Τα κράτη μέλη αναφέρουν μόνο ένα μικρό ποσοστό των περιστατικών και η ανταλλαγή πληροφοριών δεν είναι ούτε συστηματική ούτε ολοκληρωμένη. Οι κυβερνοεπιθέσεις μπορεί να αποτελούν μία μόνο πτυχή συντονισμένων κακόβουλων επιθέσεων κατά των ευρωπαϊκών κοινωνιών.

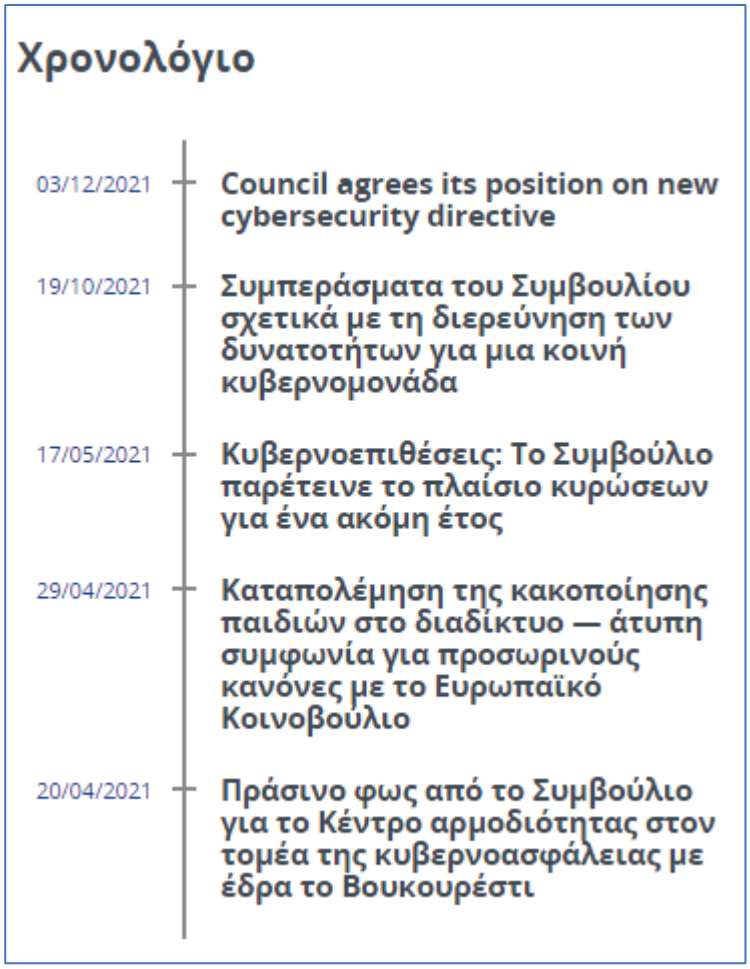
Συνεπώς, η βελτίωση της κυβερνοασφάλειας είναι απαραίτητη προκειμένου οι πολίτες να εμπιστεύονται, να χρησιμοποιούν και να ωφελούνται από την καινοτομία, τη συνδεσιμότητα και την αυτοματοποίηση, καθώς και για να διασφαλίζονται τα θεμελιώδη δικαιώματα και ελευθερίες, συμπεριλαμβανομένων των δικαιωμάτων στην ιδιωτική ζωή και στην προστασία των δεδομένων προσωπικού χαρακτήρα.

Η Επιτροπή προτείνει να δημιουργηθεί δίκτυο κέντρων επιχειρήσεων ασφάλειας σε ολόκληρη την Ένωση, το οποίο θα λειτουργεί ως πραγματική ασπίδα κυβερνοασφάλειας για την ΕΕ, παρέχοντας ένα στέρεο πλέγμα παρατηρητηρίων, ικανών να εντοπίζουν δυνητικές απειλές πριν προκληθούν ζημίες μεγάλης κλίμακας. Στόχος θα είναι η σταδιακή σύνδεση όσο το δυνατόν περισσότερων κέντρων σε ολόκληρη την ΕΕ για τη δημιουργία συλλογικών γνώσεων και την ανταλλαγή βέλτιστων πρακτικών. Προϋπόθεση, φυσικά, είναι τα κράτη μέλη να ενθαρρύνονται να συνεπενδύσουν σε αυτό το έργο, ανταλλάσσοντας και συσχετίζοντας αποτελεσματικότερα τα σήματα που εντοπίζονται, δημιουργώντας υψηλής ποιότητας πληροφορίες σχετικά με απειλές, τις οποίες θα κοινοποιούν στα ISAC και στις εθνικές αρχές, καθιστώντας έτσι δυνατή την πληρέστερη επίγνωση της κατάστασης.

Παράλληλα, η διασφάλιση της κυβερνοασφάλειας του 5G είναι μια συνεχής διαδικασία που θα συνοδεύει τη σταδιακή ανάπτυξη του 5G και την εφαρμογή της εργαλειοθήκης της ΕΕ για το 5G. Τα περισσότερα κράτη μέλη έχουν ήδη θεσπίσει, ή θα θεσπίσουν σύντομα, πλαίσια για την επιβολή κατάλληλων περιορισμών στους προμηθευτές 5G, όπως έχει θεσπιστεί στην εργαλειοθήκη ΕΕ και την ενίσχυση των μέτρων προστασίας.[39]

Να σημειώσουμε ότι έχει δημιουργηθεί ειδική σελίδα που παρουσιάζεται η δράση της ΕΕ για την αντιμετώπιση των προκλήσεων στον τομέα της κυβερνοασφάλειας.[40] Στη σελίδα αυτή παρουσιάζονται οι δραστηριότητες που υλοποιεί η ΕΕ με σκοπό:

- να ενισχύσει την κυβερνοανθεκτικότητα
- να καταπολεμήσει το κυβερνοέγκλημα
- να ενισχύσει την κυβερνοδιπλωματία
- να ενδυναμώσει την κυβερνοάμυνα
- να τονώσει την έρευνα και την καινοτομία
- να προστατεύσει τις υποδομές ζωτικής σημασίας



Εικόνα 12: Χρονολόγιο - Κυβερνοασφάλεια

5

Αρμόδιες Αρχές - Φορείς - Οργανισμοί

5.1 Αρμόδιες Αρχές στην ΕΕ

5.1.1 ENISA

Πρόκειται για τον οργανισμό της Ευρωπαϊκής Ένωσης που έχει ως αποστολή να μεριμνά για την πρόληψη και την αντιμετώπιση προβλημάτων ασφάλειας δικτύων και πληροφοριών. Ιδρύθηκε το 2004 με αρχική έδρα στο Ηράκλειο, ενώ από το 2019 (11/9/2019) η έδρα μεταφέρθηκε στην Αθήνα και στο Ηράκλειο διατηρείται ως γραφείο παραρτήματος ENISA.

Ο ENISA[15] είναι ένα ευρωπαϊκό κέντρο εμπειρογνωσίας για την ασφάλεια στον κυβερνοχώρο. Βοηθά την ΕΕ και τα κράτη μέλη της να εξοπλίζονται και να προετοιμάζονται καλύτερα ώστε να προλαμβάνουν, να εντοπίζουν και να αντιμετωπίζουν προβλήματα που αφορούν την ασφάλεια των πληροφοριών.[16]

Οι αρμοδιότητες του ENISA είναι να:

- επικουρεί και να παρέχει συμβουλές σχετικά με τη χάραξη και την επανεξέταση της πολιτικής και του δικαίου της Ένωσης στον τομέα της κυβερνοασφάλειας και σχετικά με πρωτοβουλίες πολιτικής και δικαίου ανά τομέα εφόσον εμπλέκονται ζητήματα που αφορούν την κυβερνοασφάλεια, ιδίως με την παροχή της οικείας ανεξάρτητης γνωμοδότησης και ανάλυσης, καθώς και με τη διενέργεια προπαρασκευαστικών εργασιών,

[15] https://www.enisa.europa.eu/about-enisa/about/el

[16] https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/enisa_el#%CF%83%CF%8D%CE%BD%CF%84%CE%BF%CE%BC%CE%B7-%CF%80%CE%B1%CF%81%CE%BF%CF%85%CF%83%CE%AF%CE%B1%CF%83%CE%B7

- επικουρεί τα κράτη μέλη για τη συνεπή εφαρμογή της πολιτικής και του δικαίου της Ένωσης σχετικά με την κυβερνοασφάλεια, ιδίως σε σχέση με την οδηγία (ΕΕ) 2016/1148, μεταξύ άλλων με την έκδοση γνωμοδοτήσεων, κατευθυντήριες γραμμές, 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 για το θέμα αυτό,
- επικουρεί τα κράτη μέλη και τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης στην ανάπτυξη και την προώθηση πολιτικών κυβερνοασφάλειας που συνδέονται με την υποστήριξη της γενικής διαθεσιμότητας ή της ακεραιότητας του δημόσιου πυρήνα του ανοιχτού διαδικτύου,
- συμβάλλει στο έργο της ομάδας συνεργασίας δυνάμει του άρθρου 11 της οδηγίας (ΕΕ) 2016/1148, παρέχοντας την εμπειρογνωμοσύνη και τη συνδρομή του,
- στηρίζει:
    - τη χάραξη και την εφαρμογή της ενωσιακής πολιτικής στον τομέα της ηλεκτρονικής ταυτότητας και των υπηρεσιών εμπιστοσύνης, κυρίως με την παροχή συμβουλών και την έκδοση τεχνικών κατευθυντήριων γραμμών, καθώς και με τη διευκόλυνση της ανταλλαγής βέλτιστων πρακτικών μεταξύ αρμόδιων αρχών,
    - την προαγωγή ενισχυμένου επιπέδου ασφάλειας των ηλεκτρονικών επικοινωνιών, μεταξύ άλλων με την παροχή συμβουλών και εμπειρογνωμοσύνης, καθώς και με τη διευκόλυνση της ανταλλαγής βέλτιστων πρακτικών μεταξύ αρμόδιων αρχών,
    - τα κράτη μέλη στην εφαρμογή των ειδικών πτυχών κυβερνοασφάλειας της πολιτικής και του δικαίου της Ένωσης σχετικά με την προστασία των δεδομένων και της ιδιωτικής ζωής, παρέχοντας συμβουλευτική γνώμη στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων κατόπιν αιτήματος,
- στηρίζει την τακτική επανεξέταση των δραστηριοτήτων πολιτικής της Ένωσης με την εκπόνηση ετήσιας έκθεσης σχετικά με την κατάσταση εφαρμογής του αντίστοιχου νομικού πλαισίου όσον αφορά:
    - πληροφορίες για τις κοινοποιήσεις συμβάντων των κρατών μελών που υποβάλλουν τα ενιαία κέντρα επαφής στην ομάδα συνεργασίας δυνάμει του άρθρου 10 παράγραφος 3 της οδηγίας (ΕΕ) 2016/1148,
    - περιλήψεις των κοινοποιήσεων παραβίασης της ασφάλειας ή απώλειας της ακεραιότητας που λαμβάνονται από παρόχους υπηρεσιών εμπιστοσύνης και που υποβάλλουν τα εποπτικά όργανα στον ENISA, δυνάμει του άρθρου 19 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (23),
    - τις κοινοποιήσεις συμβάντων σχετικών με την ασφάλεια που διαβιβάζουν οι πάροχοι δημόσιων ηλεκτρονικών δικτύων επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, τις οποίες υποβάλλουν οι αρμόδιες αρχές στον Οργανισμό, δυνάμει του άρθρου 40 της οδηγίας (ΕΕ) 2018/1972.

Μία από τις σημαντικές δράσεις του ENISA είναι ο συντονισμός της εκστρατείας ευαισθητοποίησης για την κυβερνοασφάλεια. Τα τελευταία χρόνια, ο Οκτώβριος κάθε χρόνο έχει καθιερωθεί ως «Ευρωπαϊκός Μήνας Κυβερνοασφάλειας» (ECSM)[17]. Σε όλη την Ευρώπη, και πέραν αυτής, διοργανώνονται διαδικτυακές δραστηριότητες, συμπεριλαμβανομένων προγραμμάτων κατάρτισης, συνεδρίων, κουίζ[18], παρουσιάσεων και εθνικών εκστρατειών, με σκοπό την ενίσχυση της ευαισθητοποίησης σχετικά με τους κινδύνους κυβερνοασφάλειας και την ανταλλαγή επικαιροποιημένων κατευθυντήριων γραμμών και συμβουλών για τον μετριασμό των εν λόγω κινδύνων.

Ειδικά το 2021, η εκστρατεία ECSM[19] ασχολήθηκε με την αντιμετώπιση ζητημάτων ασφάλειας που αφορούν την ψηφιοποίηση της καθημερινής ζωής, η οποία επιταχύνθηκε λόγω της πανδημίας COVID-19.[20] Η εκστρατεία του 2021, η οποία ενθαρρύνει τους πολίτες να **«σκέφτονται πριν κάνουν κλικ»**, παρουσιάζει δύο θεματικές σχετικά με την κυβερνοασφάλεια με σκοπό να βοηθήσει τους πολίτες της ΕΕ να αναγνωρίζουν τις κυβερνοαπειλές και να προετοιμάζονται για αυτές.

1. Η πρώτη θεματική επικεντρώνεται στην πρωτοβουλία **«Προστατέψου από κυβερνοαπειλές στο σπίτι»** και παρέχει συμβουλές σχετικά με το πώς μπορούμε να παραμείνουμε ασφαλείς στον κυβερνοχώρο κατά την πραγματοποίηση διαδικτυακών συναλλαγών, την επικοινωνία, την εργασία ή τις σπουδές μέσω διαδικτύου. Θα παρέχονται συμβουλές καλής κυβερνο-υγιεινής[21] όσον αφορά τις καθημερινές δραστηριότητες στο διαδίκτυο.
2. Η δεύτερη θεματική παρέχει κατευθυντήριες γραμμές **«πρώτων βοηθειών»** σχετικά με τις ενέργειες που πρέπει να γίνουν σε περίπτωση κυβερνοσυμβάντος. Στόχος αυτής της θεματικής είναι να ενθαρρύνει τους πολίτες να έχουν αυξημένη εγρήγορση σχετικά με τις πιο κοινές κυβερνοαπειλές και να τους παρέχει συμβουλές σχετικά με τον τρόπο αντίδρασης σε περίπτωση που πέσουν θύματα απάτης στις διαδικτυακές αγορές, σε περίπτωση που έχει διακυβευτεί η ασφάλεια της πιστωτικής κάρτας και/ή του τραπεζικού λογαριασμού τους και έχει παραβιαστεί ο λογαριασμός τους στα μέσα κοινωνικής δικτύωσης. Οι πραγματικές ιστορίες των θυμάτων κοινοποιούνται υπό μορφή συνεντεύξεων και βίντεο.

5.1.2 CERT-EU

Η CERT-EU[22] ιδρύθηκε το 2011 στις Βρυξέλλες με κύριο ρόλο να συμβάλλει στην ενίσχυση της ασφάλειας των υποδομών ΤΠΕ όλων των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ.

[17] Ο επίσημος ιστότοπος της εκστρατείας ECSM είναι cybersecuritymonth.eu
[18] https://cybersecuritymonth.eu/quiz
[19] Ένατος Ευρωπαϊκός Μήνας Κυβερνοασφάλειας
[20] https://www.enisa.europa.eu/news/ecsm-2021-pr/cnect-2021-00359-02-00-el-tra-00.pdf
[21] Στον κυβερνοχώρο, υπάρχει η Cyber Hygiene ή αλλιώς Κυβερνο-υγιεινή, κατά την οποία λαμβάνονται καθημερινά κάποια μέτρα που εξασφαλίζουν την υγιεινή των συσκευών μας. Η κυβερνο-υγιεινή έχει να κάνει με το να εκπαιδεύσετε τον εαυτό σας να σκέφτεται την ηλεκτρονική συσκευή σαν ένα ζωτικό μέρος του εαυτού του, πραγματοποιώντας όλους τους απαραίτητους ελέγχους και εξασφαλίζοντας την προστασία της συσκευής, είτε είναι κινητή, είτε σταθερή.
[22] https://cert.europa.eu/cert/plainedition/en/cert_about.html

Αποτελείται από ομάδα εμπειρογνωμόνων σε θέματα ασφάλειας ΤΠ από τα θεσμικά όργανα και τους οργανισμούς της ΕΕ.[23] Συλλέγει, διαχειρίζεται, αναλύει και ανταλλάσσει πληροφορίες με τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ σχετικά με απειλές, τρωτά σημεία και συμβάντα που σχετίζονται με μη διαβαθμισμένες υποδομές ΤΠΕ. Συντονίζει επίσης την αντιμετώπιση συμβάντων σε διοργανικό και θεσμικό επίπεδο, για παράδειγμα παρέχοντας ή συντονίζοντας την παροχή εξειδικευμένης επιχειρησιακής συνδρομής

Στην Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση (Οδηγία NIS),[41] αναφέρεται η υποχρέωση κάθε κράτους μέλους να καταρτίσει Ομάδα αντιμετώπισης έκτακτων αναγκών (CERT) που είναι υπεύθυνη για τον χειρισμό συμβάντων και κινδύνων σύμφωνα με επακριβώς καθορισμένη διαδικασία, η οποία πρέπει να συμμορφώνεται με τις απαιτήσεις που αναφέρονται παρακάτω.

Απαιτήσεις για τη CERT:

- Η CERT εξασφαλίζει ευρεία διαθεσιμότητα των υπηρεσιών επικοινωνιών της αποφεύγοντας μονοσημειακές αστοχίες και προσφέρει διάφορους τρόπους για εισερχόμενη και εξερχόμενη επικοινωνία με τρίτους. Επιπλέον, οι δίαυλοι επικοινωνίας πρέπει να είναι σαφώς προσδιορισμένοι και ευρύτερα γνωστοί στην κοινότητα και στους εταίρους της συνεργασίας.
- Η CERT εφαρμόζει και διαχειρίζεται μέτρα ασφάλειας για να διασφαλίσει την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και την αυθεντικότητα των πληροφοριών που λαμβάνει και χειρίζεται.
- Τα γραφεία της CERT και τα υποστηρικτικά συστήματα πληροφοριών εγκαθίστανται σε ασφαλείς χώρους.
- Συστήνεται σύστημα ποιότητας διαχείρισης υπηρεσιών για την παρακολούθηση των επιδόσεων της CERT και για την εξασφάλιση διαρκούς διαδικασίας βελτίωσης. Βασίζεται σε σαφώς καθορισμένα κριτήρια μέτρησης που περιλαμβάνουν επίσημα επίπεδα παρεχόμενων υπηρεσιών και βασικούς δείκτες επιδόσεων.

Στα καθήκοντα της CERT περιλαμβάνονται τα εξής:

- Παρακολούθηση συμβάντων σε εθνικό επίπεδο.
- Παροχή έγκαιρης προειδοποίησης, ειδοποιήσεων επαγρύπνησης, ανακοινώσεων και διάδοσης των πληροφοριών σε ενδιαφερόμενους φορείς σχετικά με κινδύνους και συμβάντα.
- Απόκριση σε συμβάντα.
- Παροχή δυναμικής ανάλυσης κινδύνου και συμβάντων και επίγνωση της κατάστασης.
- Ανάπτυξη ευρείας ευαισθητοποίησης του κοινού σχετικά με τους κινδύνους που συνδέονται με δραστηριότητες στο διαδίκτυο.
- Διοργάνωση εκστρατειών ευαισθητοποίησης για την ασφάλεια δικτύων και πληροφοριών (NIS).

[23] https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/cert-eu_el

Στην αναθεωρημένη Οδηγία NIS ή «NIS 2», η οποία αφορά μια νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια, ενισχύεται ο ρόλος της Ομάδας Συνεργασίας NIS στη λήψη αποφάσεων και στην ενίσχυση της συνεργασίας μεταξύ των κρατών μελών. Τα κράτη μέλη θα εξακολουθήσουν να υποχρεούνται να υιοθετήσουν μια εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο και να ορίσουν μία ή περισσότερες εθνικές αρμόδιες αρχές για την εποπτεία της συμμόρφωσης με την οδηγία. Επίσης, θα πρέπει να ορίσουν CSIRT[24] για το χειρισμό ειδοποιήσεων συμβάντων και μεμονωμένα σημεία επαφής (SPOC) που θα λειτουργούν ως σημείο σύνδεσης με άλλα κράτη μέλη.

5.2 Αρμόδιες Αρχές στην Ελλάδα

5.2.1 Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

Με το Π.Δ. 178/2014[42] προβλέφθηκε η ίδρυση και η διάρθρωση της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα την Αθήνα και αντίστοιχα της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα τη Θεσσαλονίκη.

Η αποστολή της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος συμπεριλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος είναι αυτοτελής κεντρική Υπηρεσία και υπάγεται απευθείας στον κ. Αρχηγό της Ελληνικής Αστυνομίας.

Η ΔΙΔΗΕ απαρτίζεται από τμήματα, καθένα από τα οποία έχει τις ακόλουθες αρμοδιότητες:

Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών

- χειρισμός θεμάτων προσωπικού, διαχείριση του χρηματικού και υλικού, γραμματειακή, διοικητική και τεχνική υποστήριξη και γενικά εξυπηρέτηση των λειτουργικών αναγκών της Υπηρεσίας,
- συλλογή, μελέτη, ανάλυση, αξιολόγηση, τυχόν συσχέτιση και επεξεργασία πληροφοριών, στοιχείων και δεδομένων σχετικών με την αποστολή της Υπηρεσίας και την προώθηση των επεξεργασμένων στοιχείων στα αρμόδια Τμήματα της Διεύθυνσης για επιχειρησιακή αξιοποίηση, κατά λόγο αρμοδιότητας,
- μέριμνα για τη διαρκή εξειδικευμένη εκπαίδευση και μετεκπαίδευση του προσωπικού της Διεύθυνσης σε θέματα καταπολέμησης του ηλεκτρονικού εγκλήματος, μέσω της κατάρτισης και υλοποίησης εκπαιδευτικών προγραμμάτων, σύμφωνα με τις σχετικές ανάγκες των επιχειρησιακών Τμημάτων και σε συνεργασία με τη Διεύθυνση Εκπαίδευσης και Ανάπτυξης Ανθρωπίνων Πόρων του Αρχηγείου, καθώς και με άλλες αρμόδιες υπηρεσίες ή φορείς της Χώρας και άλλων χωρών μέσω της Διεύθυνσης Διεθνούς Αστυνομικής Συνεργασίας του Αρχηγείου.

Στο Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών λειτουργεί Κέντρο Επιχειρήσεων, το οποίο εξασφαλίζει το συντονισμό και την επικοινωνία του προσωπικού

[24] CSIRT -> Computer Security Incident Response Team (Ομάδα Αντιμετώπισης Συμβάντων της Ασφάλειας Υπολογιστών)

της Υπηρεσίας κατά τη διάρκεια της επιχειρησιακής του δράσης. Στο κέντρο επιχειρήσεων λειτουργούν, σε 24ωρη βάση, τηλεφωνικό κέντρο με ειδική γραμμή καταγγελιών, καθώς και ηλεκτρονική διεύθυνση (e−mail) για την επικοινωνία των πολιτών με την Υπηρεσία.

Τμήμα Καινοτόμων Δράσεων και Στρατηγικής

- κατάρτιση προγραμμάτων ενημέρωσης πολιτών και φορέων για θέματα διαδικτύου και ηλεκτρονικών εγκλημάτων. μέσω της υλοποίησης διαφόρων δράσεων όπως συνέδρια, ημερίδες, και τηλεδιασκέψεις, καθώς και η οργάνωση άλλων καινοτόμων δράσεων στο τομέα καταπολέμησης του ηλεκτρονικού εγκλήματος,
- χάραξη θεμάτων στρατηγικού σχεδιασμού, αναφορικά με το κυβερνοέγκλημα,
- προβολή και δημοσιοποίηση του κοινωνικού έργου της Υπηρεσίας μέσω της δημιουργίας και διαχείρισης προφίλ σε ιστοσελίδες κοινωνικής δικτύωσης (Twitter, Facebook κ.λπ.) προς το σκοπό, αποκλειστικά της επικοινωνίας, ενημέρωσης και ευαισθητοποίησης των πολιτών σε θέματα ηλεκτρονικών απειλών και κινδύνων,
- παρακολούθηση των εξελίξεων σε θέματα ηλεκτρονικού εγκλήματος, τόσο σε εσωτερικό όσο και σε διεθνές επίπεδο, η εκπόνηση σχετικής ετήσιας μελέτης με συναγωγή συμπερασμάτων για την εγκληματικότητα επί των αδικημάτων αυτών στη Χώρα και η υποβολή συγκεκριμένων αιτιολογημένων προτάσεων για την αντιμετώπισή τους και
- καταγραφή δράσεων και στατιστικών στοιχείων αναφορικά με το ηλεκτρονικό έγκλημα και η τήρηση αυτών.

Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων

- χειρισμός υποθέσεων παράνομης διείσδυσης σε υπολογιστικά συστήματα και κλοπής, καταστροφής ή παράνομης διακίνησης λογισμικού υλικού, ψηφιακών δεδομένων και οπτικοακουστικών έργων που τελούνται σε ολόκληρη τη Χώρα,
- παροχή συνδρομής σε άλλες αρμόδιες υπηρεσίες που διερευνούν τις υποθέσεις αυτές, κατά την ισχύουσα νομοθεσία και
- παροχή αναγκαίας τεχνικής συνδρομής στα άλλα Τμήματα της Υπηρεσίας, τη διενέργεια ψηφιακής και διαδικτυακής έρευνας με τη χρήση σύγχρονου τεχνολογικού εξοπλισμού και την ψηφιακή και διαδικτυακή ανάλυση ψηφιακών δεδομένων, αρχείων και άλλων μέσων και ευρημάτων σε περιπτώσεις διερεύνησης σοβαρών υποθέσεων αρμοδιότητάς τους.

Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης

- εξιχνίαση και δίωξη των εγκλημάτων που διαπράττονται κατά των ανηλίκων με τη χρήση του διαδικτύου και των άλλων μέσων ηλεκτρονικής ή ψηφιακής επικοινωνίας και αποθήκευσης,
- διερεύνηση υποθέσεων διαδικτυακής ή ηλεκτρονικής παρενόχλησης (cyber bullying) και ρατσισμού,
- παροχή συνδρομής στις αρμόδιες κρατικές Υπηρεσίες για την αποτροπή αυτοκτονιών που αναγγέλλονται μέσω διαδικτύου, καθώς και στις Υπηρεσίες που διερευνούν υποθέσεις για εγκλήματα που τελούνται στο διαδίκτυο σύμφωνα με την ισχύουσα νομοθεσία.

Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων

- καταπολέμηση, σε συνεργασία με τη Διεύθυνση Οικονομικής Αστυνομίας και τις άλλες αρμόδιες εθνικές, ευρωπαϊκές και αλλοδαπές υπηρεσίες και αρχές, οικονομικών εγκλημάτων και ιδίως εγκλημάτων που τελέστηκαν σε διαδικτυακό περιβάλλον με τη χρήση ηλεκτρονικών μέσων και νέων τεχνολογιών, σε βάρος των οικονομικών συμφερόντων του δημοσίου και της εθνικής οικονομίας γενικότερα ή εμφανίζουν τα χαρακτηριστικά του οργανωμένου οικονομικού εγκλήματος και η διερεύνησή τους απαιτεί εξειδικευμένη τεχνογνωσία.
- συνεχής έρευνα του διαδικτύου και των άλλων μέσων ηλεκτρονικής επικοινωνίας και ψηφιακής αποθήκευσης, για την ανακάλυψη, εξιχνίαση και δίωξη των εγκληματικών πράξεων αρμοδιότητάς του που διαπράττονται σ' αυτά ή μέσω αυτών σε ολόκληρη τη Χώρα, εφόσον για την διερεύνησή τους απαιτείται εξειδικευμένη τεχνική ή ψηφιακή έρευνα.

5.2.2 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι συνταγματικά κατοχυρωμένη ανεξάρτητη δημόσια Αρχή, η οποία έχει ως αποστολή της την εποπτεία της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων, του ν. 4624/2019, του ν. 3471/2006 και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά.

5.2.3 Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

Με το άρθρο 1 του νόμου 3115/2003[43] συστάθηκε, σύμφωνα με την παράγραφο 2 του άρθρου 19 του Συντάγματος, η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών - ΑΔΑΕ. *Η ΑΔΑΕ* έχει σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης

ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών

Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από τον νόμο.

Οι κύριες αρμοδιότητες της ΑΔΑΕ είναι:

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

5.2.4 Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) είναι Ανεξάρτητη Διοικητική Αρχή. Αποτελεί τον Εθνικό Ρυθμιστή που ρυθμίζει, εποπτεύει και ελέγχει:

- την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρίες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου και
- την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρίες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς.

Επιπλέον, η ΕΕΤΤ αποτελεί την αρχή ανταγωνισμού στις ανωτέρω αγορές της αρμοδιότητας της και διαθέτει όλες τις εξουσίες και τα δικαιώματα της Επιτροπής Ανταγωνισμού κατά την εφαρμογή της νομοθεσίας του ελεύθερου ανταγωνισμού στις εν λόγω αγορές.[25]

[25] Ν.3959/2011 (Α' 93), άρθρα 101/102 ΣΛΕΕ και Κανονισμός 1/2003 ΕΚ του Συμβουλίου. Η εφαρμογή της νομοθεσίας περί ελεύθερου ανταγωνισμού από την ΕΕΤΤ στις αγορές της αποκλειστικής της αρμοδιότητας προβλεπόταν από τον νόμο Ν.2867/2000, τον μετέπειτα νόμο Ν.3431/2006, τον Ν.4070/2012 (ΦΕΚ 82Α/2012) και πλέον με τον ισχύοντα νόμο Ν.4727/2020 (ΦΕΚ 184Α/2020).

Η Αρχή ιδρύθηκε το 1992 με το Ν.2075/1992 υπό την επωνυμία Εθνική Επιτροπή Τηλεπικοινωνιών (ΕΕΤ), καθώς οι αρμοδιότητές της αρχικά επικεντρώνονταν στην εποπτεία της απελευθερωμένης αγοράς των τηλεπικοινωνιών. Η λειτουργία της ξεκίνησε το καλοκαίρι του 1995. Με την ψήφιση του Ν.2668/1998, ο οποίος καθόριζε τον τρόπο οργάνωσης και λειτουργίας της αγοράς των ταχυδρομικών υπηρεσιών, ανατέθηκε στην ΕΕΤ η επιπρόσθετη ευθύνη για την εποπτεία και ρύθμιση της αγοράς των ταχυδρομικών υπηρεσιών και η Αρχή μετονομάστηκε σε Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ).

Με το Ν.2867/2000 ενισχύθηκε ο ρυθμιστικός, εποπτικός και ελεγκτικός ρόλος της ΕΕΤΤ, ενώ με το Ν.3431/2006 περί ηλεκτρονικών επικοινωνιών που ενσωμάτωσε νεότερες ευρωπαϊκές ρυθμίσεις, καθορίστηκε το πλαίσιο παροχής δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών και συναφών ευκολιών εντός της ελληνικής επικράτειας και διευρύνθηκαν οι αρμοδιότητές της.

5.2.5 Εθνική Αρχή Κυβερνοασφάλειας - CSIRTs / CERTs[26]

Η Γενική Διεύθυνση Κυβερνοασφάλειας υπάγεται στη Γενική Γραμματεία Τηλεπικοινωνιών & Ταχυδρομείων του υπουργείου Ψηφιακής Διακυβέρνησης και καταρτίζει την Εθνική Στρατηγική Κυβερνοασφάλειας, στην οποία καθορίζονται οι στρατηγικοί στόχοι, οι προτεραιότητες και τα μέτρα πολιτικής και κανονιστικής ρύθμισης, με σκοπό την εξασφάλιση υψηλού επιπέδου ασφάλειας για τα συστήματα τηλεπικοινωνιών και πληροφορικής σε εθνικό επίπεδο.
Η Γενική Διεύθυνση Κυβερνοασφάλειας:

- Διατυπώνει την πολιτική ασφάλειας συστημάτων ΤΠΕ για το δημόσιο τομέα και προωθεί την εφαρμογή της[44]
- Ορίζει απαιτήσεις και κανόνες 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
- Συνεργάζεται με τις αρμόδιες Ανεξάρτητες και Ρυθμιστικές Αρχές, τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών και ακαδημαϊκούς φορείς για την υιοθέτηση ενιαίων πολιτικών ασφαλείας στο πλαίσιο της δημόσιας διοίκησης
- Συνεργάζεται με την Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων και την Τεχνικής Φύσεως Αρχή Ασφάλειας Πληροφοριών της Εθνικής Υπηρεσίας Πληροφοριών, καθώς επίσης και με τα CERTs που δραστηριοποιούνται στην Ελλάδα για θέματα αρμοδιότητας του Τμήματος
- Προωθεί δράσεις εκπαίδευσης και ενημέρωσης του προσωπικού που διαχειρίζεται και υποστηρίζει κρίσιμα συστήματα και υποδομές του Δημοσίου.

Η Ελληνική Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT) δημιουργήθηκε σύμφωνα με το άρθρο 8 - Νόμος 4577/2018, καθώς η Ελλάδα, σαν κράτος μέλος της ΕΕ, είχε την υποχρέωση να καταρτίσει μία αρμόδια Ομάδα αντιμετώπισης έκτακτων αναγκών.
Η αρμόδια CSIRT:

[26] CERT -> Computer Emergency Response Team

- εξασφαλίζει υψηλό επίπεδο διαθεσιμότητας των υπηρεσιών επικοινωνιών της, αποφεύγοντας μοναδικά σημεία αστοχίας και διαθέτει διάφορους τρόπους για εισερχόμενη και εξερχόμενη επικοινωνία με τρίτους ανά πάσα στιγμή. Επιπλέον, οι δίαυλοι επικοινωνίας είναι σαφώς προσδιορισμένοι και ευρύτερα γνωστοί στα μέλη της περιοχής ευθύνης και τους συνεργαζόμενους εταίρους,
- τα γραφεία της και τα υποστηρικτικά συστήματα πληροφοριών εγκαθίστανται σε ασφαλείς χώρους,
- συμμετέχει σε διεθνή δίκτυα συνεργασίας

Αναφορικά με τη συνέχεια της επιχειρησιακής δραστηριότητάς της, η αρμόδια CSIRT:

- είναι εφοδιασμένη με κατάλληλο σύστημα διαχείρισης και δρομολόγησης αιτημάτων, προκειμένου να διευκολύνεται η παράδοση καθηκόντων,
- είναι επαρκώς στελεχωμένη ώστε να εξασφαλίζεται η διαθεσιμότητα ανά πάσα στιγμή,
- βασίζεται σε υποδομή, η συνέχεια της οποίας είναι διασφαλισμένη. Για τον σκοπό αυτό, διατίθενται πλεονάζοντα συστήματα και εφεδρικοί χώροι εργασίας,

6

Συμπεράσματα – Προτάσεις Βελτίωσης της Κυβερνοασφάλειας

6.1 Συμπεράσματα

Στο πλαίσιο ανάπτυξης της παρούσας διπλωματικής εργασίας επεξηγήθηκαν οι ορισμοί του κυβερνοεγκλήματος και της κυβερνοασφάλειας και παρουσιάστηκαν με συντομία οι αρμόδιες Αρχές, Φορείς και Οργανισμοί και οι αρμοδιότητες τους.

Αναλύθηκαν λεπτομερώς οι κατηγορίες και οι παράγοντες απειλών, και τονίστηκε η ανάγκη για ενίσχυση των υποδομών ασφάλειας των Οργανισμών, παράλληλα με τη συνεχή εκπαίδευση των χρηστών.

Παρουσιάστηκαν σημαντικά γεγονότα - σταθμοί για το έργο και τις ενέργειες της Ευρωπαϊκής Επιτροπής σχετικά με την Ασφάλεια στον Κυβερνοχώρο, στις Διατάξεις και Ανακοινώσεις της ΕΕ σχετικά με τις στρατηγικές κυβερνοασφάλειας.

Τα συμπεράσματα που μπορούμε να βγάλουμε είναι, καταρχήν, ότι όλοι έχουμε αντιληφθεί την σημασία και την υιοθέτηση στρατηγικών ασφάλειας σε όλα τα επίπεδα δημιουργίας των πληροφοριακών συστημάτων. Αυτό σημαίνει ότι οι απαιτήσεις ασφάλειας θα πρέπει να προβλέπονται από το στάδιο του σχεδιασμού των εφαρμογών. Παράλληλα, είναι εξίσου σημαντική η συμβολή των χρηστών των πληροφοριακών συστημάτων στην αποτροπή μίας επίθεσης, συνεπώς θα πρέπει να γίνεται συνεχής εκπαίδευση στα θέματα ασφάλειας που αφορούν τον Οργανισμό ή την επιχείρηση.

6.2 Προτάσεις Βελτίωσης της Κυβερνοασφάλειας

Από την ανάλυση που έγινε στο πλαίσιο ανάπτυξης της παρούσας διπλωματικής εργασίας, έχουν ξεκαθαρίσει δύο πράγματα.

Το πρώτο είναι το γεγονός ότι όλοι έχουμε κατανοήσει την σημασία της εφαρμογής μιας ενιαίας στρατηγικής κυβερνοασφάλειας από όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης, ανεξάρτητα από την εθνική στρατηγική που έχει το κάθε κράτος. Αυτό θα βοηθήσει τα κράτη να ζητούν τη συνδρομή των «συμμάχων» κρατών για να αντιμετωπιστούν άμεσα οι κυβερνοεπιθέσεις. Επιπλέον, η ύπαρξη κοινής ενωσιακής στρατηγικής κυβερνοασφάλειας δίνει το αίσθημα ότι σε κάθε περίπτωση, κανένα κράτος δεν θα μείνει αβοήθητο.

Το δεύτερο είναι κάτι με το οποίο πρέπει όλοι να συμφωνήσουμε. Για να είναι πραγματικά αποτελεσματικά τα προγράμματα ανθεκτικότητας στον κυβερνοχώρο πρέπει να εξισορροπούν τις τεχνολογικές δυνατότητες με μια βιώσιμη αλλαγή στην συμπεριφορά των εργαζομένων. Ο κίνδυνος στον κυβερνοχώρο είναι πολλά περισσότερα από ένα τεχνολογικό ζήτημα. Η ανθρώπινη συμπεριφορά στον χώρο εργασίας είναι μια άμεση εκδήλωση της εταιρικής κουλτούρας, των κοινών γνώσεων, των πεποιθήσεων και των κανόνων που ορίζουν έναν οργανισμό.

Ο κορυφαίος κίνδυνος στον κυβερνοχώρο είναι η ανεπαρκής κατανόηση και η συμπεριφορά των εργαζομένων σχετικά με τους κινδύνους στον κυβερνοχώρο. Η απλή ευαισθητοποίηση σχετικά με την ασφάλεια σπάνια οδηγεί σε διαρκή αλλαγή συμπεριφοράς από μόνη της, που σημαίνει ότι οι οργανισμοί πρέπει να αναπτύξουν έναν ισχυρό ανθρωποκεντρικό πρόγραμμα ασφάλειας για να μειώσουν τον αριθμό περιστατικών ασφάλειας, που σχετίζονται με μη ασφαλείς συμπεριφορές.

Θα πρέπει να ενισχυθούν οι δράσεις εκπαίδευσης των υπαλλήλων και να υλοποιούνται σε τακτά διαστήματα εκπαιδευτικά προγράμματα με σκοπό τη βελτίωση της γνώσης και την ευαισθητοποίηση του προσωπικού σε θέματα κυβερνοασφάλειας. Δεν φτάνει να υπάρχουν πολιτικές ασφάλειας σε έναν Οργανισμό, αν ο εργαζόμενος δεν εκπαιδευτεί με κάθε τρόπο και να είναι σε θέση να αντιληφθεί και να αντιμετωπίσει ή να αποτρέψει μία κυβερνοαπειλή. Τότε μόνο θα μπορούμε να μετατρέψουμε τον άνθρωπο από τον πιο «αδύναμο κρίκο» στην αλυσίδα της κυβερνοασφάλειας στον πιο «ισχυρό κρίκο» και το πιο σημαντικό στοιχείο κάθε οργανισμού.

Παράρτημα Ι - Σύνοψη της Σύμβασης του Συμβουλίου της Ευρώπης για το Έγκλημα στον Κυβερνοχώρο

Η Σύμβαση, στο 1ο άρθρο του πρώτου Κεφαλαίου, περιλαμβάνει συγκεκριμένους ορισμούς για τον προσδιορισμό ορισμένων εννοιών τεχνικής φύσης από τις οποίες συναρτάται η εφαρμογή της και ειδικότερα των εννοιών: «σύστημα υπολογιστή», «δεδομένα κίνησης» και «πάροχος υπηρεσιών».

Στη συνέχεια, οροθετείται η έννοια του κυβερνοεγκλήματος και προσδιορίζονται τα συγκεκριμένα αδικήματα κατά τρόπο που να διασφαλίζεται η ιδιαιτερότητα κάθε εσωτερικής έννομης τάξης.

Με τα άρθρα 2 έως 6 τιμωρούνται τα αδικήματα που στρέφονται κατά των δικτύων πληροφοριών και επιβάλλεται στα Συμβαλλόμενα Μέρη η υποχρέωση να χαρακτηρίσουν ως αξιόποινες τις πράξεις που αποσκοπούν στην από πρόθεση πρόκλησης βλάβης στα δίκτυα, την ακεραιότητα, τη διαθεσιμότητα των δεδομένων ή των συστημάτων πληροφορικής και ειδικότερα την παράνομη πρόσβαση (άρθρο 2), την υποκλοπή (άρθρο 3), την παρεμβολή σε δεδομένα (άρθρο 4) και τις παρεμβολές σε συστήματα (άρθρο 5).

Το άρθρο 6 αποβλέπει στην απαγόρευση τόσο της κατασκευής όσο και της διανομής ή της διάθεσης προγραμμάτων υπολογιστών, καθώς και της διακίνησης συνθηματικών λέξεων ή κωδικών πρόσβασης.

Με τα άρθρα 7 και 8 προβλέπεται η υποχρέωση των Συμβαλλόμενων Μερών να καταστήσουν αξιόποινες την πλαστογραφία και την απάτη μέσω υπολογιστή.

Με το άρθρο 9 επιβάλλεται στα Συμβαλλόμενα Μέρη η υποχρέωση να καταστήσουν αξιόποινες συμπεριφορές που σχετίζονται με το υλικό σεξουαλικής κακοποίησης ανηλίκων. Το πεδίο εφαρμογής της τελευταίας διάταξης είναι ιδιαιτέρως ευρύ, δεδομένου ότι καλύπτεται η απαγόρευση της παραγωγής, διάδοσης, η τηλεφόρτωση ή η απλή κατοχή υλικού περιλαμβανόμενης και της οπτικής αναπαραγωγής προσώπων ηλικίας κάτω των 18 ετών (ή κάτω των 16 ετών για τα Συμβαλλόμενα Μέρη που έχουν ορίσει το όριο αυτό), ενηλίκων που εμφανίζονται ως ανήλικοι καθώς και κάθε εικονικής αναπαράστασης ανηλίκων που επιδίδονται σε σεξουαλικές πράξεις.

Με τη διάταξη του άρθρου 10 αντιμετωπίζονται εγκλήματα σχετικά με τα δικαιώματα πνευματικής ιδιοκτησίας, εφόσον αυτά διαπράττονται για εμπορικούς σκοπούς, αποβλέπουν δηλαδή στην επίτευξη κέρδους.

Οι διατάξεις των άρθρων 11 έως και 13 της Σύμβασης ρυθμίζουν ζητήματα ευθύνης και ποινικών κυρώσεων, με τη θέσπιση ορισμένων γενικής φύσης Αρχών που επαναλαμβάνουν, κατά βάση, τις κλασικές ρήτρες που περιέχουν οι Ευρωπαϊκές Συμβάσεις που αφορούν σε θέματα ποινικού δικαίου.

Πέρα της ποινικής ευθύνης των φυσικών προσώπων, προβλέπεται ακόμη η επιβολή κυρώσεων και σε βάρος νομικών προσώπων, οι οποίες μπορεί να είναι ποινικής, διοικητικής ή αστικής φύσης.

Με βάση τον πλήρη σεβασμό των θεμελιωδών Δικαιωμάτων του Ανθρώπου, επιδιώκεται, με τις διατάξεις των άρθρων 14 έως και 21 της Σύμβασης, η βελτίωση των δυνατοτήτων των Συμβαλλόμενων Μερών να διεξάγουν στα δίκτυα έρευνες σε πραγματικό χρόνο ("in real time") ανεξαρτήτως του είδους των διαπραττόμενων εγκλημάτων και να συλλέγουν τις αναγκαίες για τη στοιχειοθέτησή τους ηλεκτρονικές αποδείξεις, πριν αυτές χαθούν οριστικά. Η διαρκής και μυστική παρακολούθηση των δικτύων δεν είναι επιτρεπτή.

Τα άρθρα 16 έως και 18 της Σύμβασης αφορούν στη διατήρηση, κοινοποίηση, διάδοση και γνωστοποίηση των δεδομένων. Αποβλέπουν, επίσης, στην προσαρμογή των μέσω έρευνας στον προσωρινό χαρακτήρα που εμφανίζουν τα δεδομένα στα δίκτυα, παρέχοντας την αναγκαία νομοθετική πρόβλεψη για την διενέργεια των επειγουσών ενεργειών εκ μέρους των διωκτικών αρχών, με σκοπό την παρεμπόδιση της εξαφάνισης ή της απάλειψης δεδομένων, τα οποία είναι απαραίτητα για την διεξαγωγή της έρευνας. Τα Συμβαλλόμενα Μέρη οφείλουν να λάβουν τα απαραίτητα μέτρα για να εξασφαλίσουν την κατεπείγουσα διατήρηση από τους παρόχους όλων των τύπων δεδομένων που έχουν αποθηκευθεί από αυτούς (άρθρο 16) αλλά και επαρκούς ποσότητας δεδομένων κίνησης που να καθιστούν δυνατό τον εντοπισμό των παρόχων υπηρεσιών, αλλά και της διαδρομής μέσω της οποίας έλαβε χώρα ορισμένη επικοινωνία (άρθρο 17) και την παράδοση στις αρμόδιες Αρχές του συνόλου των δεδομένων που έχουν παγώσει.

Το άρθρο 19 προβλέπει την έρευνα και την πρόσβαση σε υπολογιστή (παρ. 1) ή σε δίκτυα υπολογιστών εφόσον αυτά παραμένουν εντός της επικράτειας (παρ. 2) (έρευνα από απόσταση ή τηλε-έρευνα) και δέσμευση δεδομένων (παρ. 3).

Το άρθρο 20 ρυθμίζει τη συλλογή και αποθήκευση σε πραγματικό χρόνο, δηλαδή κατά τη μετάδοση, των δεδομένων κίνησης που μπορεί να γίνονται απευθείας από τις διωκτικές αρχές ή από τους παρόχους υπηρεσιών του διαδικτύου, σύμφωνα με τις τεχνικές τους δυνατότητες.

Το άρθρο 21 ρυθμίζει την συλλογή και καταγραφή δεδομένων περιεχομένου σε πραγματικό χρόνο, προκειμένου για σοβαρά εγκλήματα που προσδιορίζονται από την εσωτερική νομοθεσία.

Το τρίτο τμήμα του δεύτερου κεφαλαίου της Σύμβασης αφορά στη δικαιοδοσία. Αρχικά κάθε Συμβαλλόμενο Μέρος έχει δικαιοδοσία αν η παράβαση έλαβε χώρα εντός της επικράτειάς του, εφόσον αυτή είναι ποινικά κολάσιμη στον τόπου που διαπράχθηκε ή αν διαπράχθηκε εκτός της εδαφικής δικαιοδοσίας ενός Κράτους. Περαιτέρω, με το τρίτο κεφάλαιο της Σύμβασης επιχειρείται η προσαρμογή των κλασικών κανόνων των Συμβάσεων του 1957 και 1959 που αφορούν την έκδοση και την δικαστική συνδρομή και παρέχεται η αναγκαία νομοθετική πρόβλεψη για τη διευκόλυνση της συνεργασίας με όλα τα Κράτη και ιδίως αυτά που βρίσκονται εκτός της Ευρωπαϊκής Ηπείρου, που δεν έχουν κυρώσει τις προαναφερθείσες Συμβάσεις (άρθρο 23).

Το άρθρο 24 περιλαμβάνει ορισμένους κανόνες σχετικά με την έκδοση για τα προβλεπόμενα από τη Σύμβαση αδικήματα, για την εφαρμογή των οποίων πρέπει να προβλέπεται η επιβολή ποινής τουλάχιστον ενός έτους.

Το άρθρο 25 καθορίζει τις γενικές αρχές που διέπουν την αμοιβαία συνδρομή, καθορίζονται οι διαδικασίες παροχής συνδρομής σε περιπτώσεις που δεν υπάρχει σχετική Σύμβαση ή Συμφωνία. Οι προϋποθέσεις παροχής συνδρομής και οι σχετικές διαδικασίες έχουν απλοποιηθεί, οι λόγοι άρνησης παροχής συνδρομής έχουν περιορισθεί και η εκτέλεση των σχετικών μέτρων έχει επιταχυνθεί (άρθρο 27).

Θεσπίζονται ακόμη κανόνες με τους οποίους επιδιώκεται η απλοποίηση της αυθόρμητης παροχής πληροφοριών (άρθρο 26).

Σε ό,τι αφορά στην ανταλλαγή πληροφοριών και ιδίως δεδομένων προσωπικού χαρακτήρα μεταξύ των διαφόρων Κρατών που κάνουν χρήση της δικαστικής συνδρομής και ιδίως των τρίτων χωρών που δε διαθέτουν εσωτερική νομοθεσία που να παρέχει ικανοποιητικό επίπεδο προστασίας των προσωπικών δεδομένων, το άρθρο 28 περιλαμβάνει ορισμένους στοιχειώδεις κανόνες σχετικά με την ανταλλαγή πληροφοριών με τα Κράτη αυτά. Αυτό οφείλεται στο γεγονός ότι το προστατευτικό καθεστώς των προσωπικών δεδομένων που προβλέπεται τόσο από την εν ευρεία έννοια ευρωπαϊκή έννομη τάξη, όσο και από το Κοινοτικό Δίκαιο, δεν εφαρμόζεται από όλα τα υπογράφοντα την παρούσα Σύμβαση Κράτη, τα οποία δεν είναι όλα Κράτη-Μέλη της ΕΕ.

Με τις διατάξεις των άρθρων 29 έως και 34 ρυθμίζονται από δικονομική άποψη τα ζητήματα της ταχείας διατήρησης των δεδομένων (άρθρο 29), της αποκάλυψης των δεδομένων (άρθρο 29), της αποκάλυψης των δεδομένων (άρθρο 30), των ερευνών και κατασχέσεων αποθηκευμένων δεδομένων (άρθρα 31 και 32) και τα της υποκλοπής δεδομένων κίνησης και περιεχομένου (άρθρα 33 και 34). Προβλέπεται, ειδικότερα, η δυνατότητα διασυνοριακής πρόσβασης σε δεδομένα χωρίς την τήρηση της διαδικασίας παροχής δικαστικής συνδρομής σε δύο μόνο περιπτώσεις (άρθρο 32): σε δεδομένα στα οποία έχει πρόσβαση το κοινό (“ανοιχτά δεδομένα”) και σε δεδομένα στα οποία το Συμβαλλόμενο Μέρος απέκτησε πρόσβαση ή έλαβε μέσω ενός συστήματος υπολογιστή που βρίσκεται στην Επικράτειά του και για τα οποία έχει λάβει τη νόμιμη και εκούσια συγκατάθεση του προσώπου που έχει το νόμιμο δικαίωμα να τα διαθέσει σε αυτό μέσω του συστήματος υπολογιστή.

Το άρθρο 35 προβλέπει τη δημιουργία ενός δικτύου σημείων διαρκούς επαφής για τη διευκόλυνση της ταχείας επεξεργασίας των αιτημάτων συνδρομής που προέρχονται από την αλλοδαπή,

Το τέταρτο κεφάλαιο της Σύμβασης περιλαμβάνει τις τελικές διατάξεις, ρυθμίζει ζητήματα σχετικά με την υπογραφή, την έναρξη ισχύος της (άρθρο 36), την προσχώρηση (άρθρο 37), την καταγγελία (άρθρο 47), το εδαφικό πεδίο εφαρμογής (άρθρο 38), τις δηλώσεις και τις επιφυλάξεις (άρθρα 40, 42 και 43), τις τροποποιήσεις (άρθρο 44) και τα θέματα επίλυσης τυχόν αναφυόμενων διαφορών από την ερμηνεία και την εφαρμογή της.

Τέλος, το άρθρο 46 προβλέπει τη διενέργεια απολογισμού σχετικά με τα αποτελέσματα από την εφαρμογή της και την δυνατότητα διατύπωσης προτάσεων για την τροποποίησή της μετά την πάροδο τριετίας από τη θέση σε ισχύ της Σύμβασης.

Βιβλιογραφία

- Γεώργιος Γέρμανος, Νικόλαος Γεωργίου (2021) - Κυβερνοέγκλημα, Ιδιωτική Έκδοση
- Γεώργιος Γέρμανος (2018) – Cyber Safety, Ιδιωτική Έκδοση

[1] Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου σχετικά με τον ENISA
[2] Κανονισμός COM(2018) 434 final του Ευρωπαϊκού Κοινοβουλίου για τη θέσπιση του προγράμματος Ψηφιακή Ευρώπη για την περίοδο 2021-2027
[3] ENISA Threat Landscape Report 2017
[4] ENISA Threat Landscape Report 2018
[5] ENISA THREAT LANDSCAPE FOR 5G NETWORKS - Threat assessment for 5G Networks
[6] ENISA THREAT LANDSCAPE FOR 5G NETWORKS - Threat assessment for 5G Networks (updated)
[7] ENISA THREAT LANDSCAPE 2021

[8] Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025

[9] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)
[10] https://www.inforisktoday.com/ransomware-average-ransom-payment-stays-steady-at-140000-a-17773
[11] netwrix: 2020_Cyber_Threats_Report
[12] COM(2001)298 Ανακοίνωση από την Ευρωπαϊκή Επιτροπή σχετικά με την Ασφάλεια δικτύων και πληροφοριών
[13] Ν. 4411/2016: Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο (Lawspot)
[14] Οδηγία 2002/58 του Ευρωπαϊκού Κοινοβουλίου σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)
[15] COM(2006) 251 Ανακοίνωση από την Ευρωπαϊκή Επιτροπή σχετικά με την Στρατηγική για ασφαλή κοινωνία της πληροφορίας – «διάλογος, πνεύμα συνεργασίας και ενίσχυση των ικανοτήτων»
[16] COM(2006) 688 Ανακοίνωση από την Ευρωπαϊκή Επιτροπή σχετικά με την καταπολέμηση των ανεπίκλητων ηλεκτρονικών μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού
[17] COM(2007) 285 Ανακοίνωση από την Ευρωπαϊκή Επιτροπή σχετικά με την αξιολόγηση του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)
[18] 2009/C 321/01 Ψήφισμα του Συμβουλίου για μια ευρωπαϊκή συνεργατική προσέγγιση όσον αφορά την ασφάλεια δικτύων και πληροφοριών
[19] COM (2010) 245 - Digital Agenda for Europe
[20] Συμπεράσματα του Συμβουλίου της 31ης Μαΐου 2010 σχετικά με το Ψηφιακό θεματολόγιο για την Ευρώπη (10130/10)
[21] COM(2010) 2020 και συμπεράσματα του Ευρωπαϊκού Συμβουλίου της 25/26 Μαρτίου 2010 (EUCO 7/10).
[22] COM(2010) 673 Ανακοίνωση από την Ευρωπαϊκή Επιτροπή: Η στρατηγική εσωτερικής ασφάλειας της ΕΕ στην πράξη: πέντε βήματα για μια ασφαλέστερη Ευρώπη
[23] Οδηγία COM(2013) 48 του Ευρωπαϊκού Κοινοβουλίου σχετικά με μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση
[24] Νομοθετικό ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 13ης Μαρτίου 2014 σχετικά με την πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορά μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση (COM(2013)0048 — C7-0035/2013 — – σελ.11

[25] COM(2016) 410 Ανακοίνωση από την Ευρωπαϊκή Επιτροπή σχετικά με την ενίσχυση του συστήματος κυβερνοανθεκτικότητας της Ευρώπης και προώθηση ανταγωνιστικού και καινοτόμου κλάδου ασφάλειας στον κυβερνοχώρο
[26] Συμπεράσματα του Συμβουλίου σχετικά με την ενίσχυση του ευρωπαϊκού συστήματος
[27] Οδηγία 2016/1148 του Ευρωπαϊκού Κοινοβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση
[28] IT Professional Security (19-7-2017) - Βαγενά Ευαγγελία NIS - Η νέα οδηγία για την κυβερνοασφάλεια
[29] Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής με θέμα «Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών: Ενίσχυση του συστήματος κυβερνοανθεκτικότητας της Ευρώπης και προώθηση ανταγωνιστικού και καινοτόμου κλάδου ασφάλειας στον κυβερνοχώρο»
[30] Κανονισμός COM(2017) 477 του Ευρωπαϊκού Κοινοβουλίου σχετικά με τον ENISA, τον «οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο», και την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013, καθώς και σχετικά με την πιστοποίηση της ασφάλειας στον κυβερνοχώρο στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών («πράξη για την ασφάλεια στον κυβερνοχώρο»)
[31] 2020/C 28/06 Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 13ης Ιουνίου 2018 σχετικά με την άμυνα στον κυβερνοχώρο (2018/2004(INI))
[32] Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου σχετικά με τον ENISA 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
[33] Οδηγία COM(2020) 823 του Ευρωπαϊκού Κοινοβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148
[34] Ευρωπαϊκή Επιτροπή - Νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια και νέοι κανόνες για την ενίσχυση της ανθεκτικότητας των φυσικών και ψηφιακών κρίσιμων οντοτήτων
[35] Ευρωπαϊκή Επιτροπή (European Commission) - Proposal for directive on measures for high common level of cybersecurity across the Union
[36] Αναστασόπουλος Δημήτρης (Πηγή: ec.europa.eu) Νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια
[37] Κανονισμός (ΕΕ) 2021/887 του Ευρωπαϊκού Κοινοβουλίου για τη σύσταση του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού
[38] 2021/0166 (NLE) Ανακοίνωση από την Ευρωπαϊκή Επιτροπή- Έκθεση σχετικά με την εφαρμογή της στρατηγικής κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία
[39] Ευρωπαϊκή Επιτροπή - Ασφάλεια των δικτύων 5G: έκθεση των κρατών μελών σχετικά με την πρόοδο που έχει σημειωθεί ως προς την εφαρμογή της εργαλειοθήκης της ΕΕ και την ενίσχυση των μέτρων προστασίας
[40] Ευρωπαϊκό Συμβούλιο - Κυβερνοασφάλεια: Πώς αντιμετωπίζει η ΕΕ τις κυβερνοαπειλές
[41] Οδηγία COM(2013) 48 του Ευρωπαϊκού Κοινοβουλίου σχετικά με μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση
[42] Προεδρικό Διάταγμα 178/2014 - ΦΕΚ 281/Α/31-12-2014
[43] Νόμος 3115/2003 : Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
[44] Εθνική Αρχή Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης - Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας - Τμήμα Απαιτήσεων και Αρχιτεκτονικής Ασφάλειας: Εγχειρίδιο Κυβερνοασφάλειας