
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
**ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ**

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων


# Ανάλυση της Οδηγίας NIS και η εφαρμογή της και η εξέλιξη με την πρόταση Οδηγίας NIS2

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του


Δρίβα Δ. Σπυρίδων


**Επιβλέπων :** Ευαγγελία Μήτρου

**Μέλη εξεταστικής επιτροπής:** Μ. Καρύδα, Γ. Στεργιόπουλος

Σάμος, Ιούνιος 2022

Η σελίδα αυτή είναι σκόπιμα λευκή.

# Ευχαριστίες

Θα ήθελα να ευχαριστήσω την επιβλέποντα καθηγήτρια κ. Ευαγγέλια Μήτρου για τα εποικοδομητικά σχόλια και της συμβουλές της. Επίσης, θέλω να ευχαριστήσω την οικογένεια, τους φίλους μου αλλά και τους συμφοιτητές που γνώρισα κατά την διάρκεια των σπουδών μου για την υπομονή, την κατανόηση και την στήριξή τους κατά τη διάρκεια των μεταπτυχιακών σπουδών μου και την συγγραφή της παρούσας διπλωματικής εργασίας



Δρίβα Δ. Σπυρίδων

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

# Πίνακας περιεχομένων

# Ακρωνύμια

| | |
|---|---|
| ΓΕΕΘΑ | Γενικό Επιτελείο Εθνικής Άμυνας |
| ΕΕ | Ευρωπαϊκή Ένωση |
| Κ-Μ | Κράτος – μέλος |
| Ν. | Νόμος |
| Π.Δ. | Προεδρικό Διάταγμα |
| ΠΨΥ | Πάροχοι Ψηφιακών Υπηρεσιών |
| Υ.Α. | Υπουργική Απόφαση |
| ΦΕΒΥ | Φορέας Εκμετάλλευσης Βασικών Υπηρεσιών |
| NIS | Network and Information Systems |
| ISP | Internet Service Providers |
| CSIRT | Computer Security Incident Response Team |
| ΤΠΕ | Τεχνολογίες Πληροφορίων και Επικοινωνίας |

# Περίληψη

Η παρούσα εργασία έχει ένα τριπλό στόχο. Καταρχάς, να παρουσιάσει την Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τα μέτρα για υψηλό κοινό επίπεδο ασφαλείας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση. Στη συνέχεια, να παρουσιάσει τον τρόπο με τον οποίο ενσωματώθηκε στην ελληνική έννομη τάξη. Και τέλος αφού γίνει η αποτίμηση της εφαρμογής της, να παρουσιάσει τη νέα Πρόταση της Ευρωπαϊκής Επιτροπής σχετικά με την αναθεώρηση της ισχύουσας Οδηγίας, με σκοπό τη διόρθωση των σφαλμάτων που εμπειρικά διαπιστώθηκαν και κυρίως τη βέλτιστη προστασία των κρατών-μελών της Ευρωπαϊκής Ένωσης από τους κινδύνους του Διαδικτύου.

# 1

# *Εισαγωγή*

## *1.1. Αντικείμενο Εργασίας*

Είναι αδιαμφισβήτητο ότι η ψηφιακή εποχή έχει δημιουργήσει ένα νέο κόσμο, άυλο και παράλληλο με τον δικό μας, πραγματικό κόσμο. Η ανωνυμία και η κατάργηση κάθε εδαφικού περιορισμού δημιουργούν ποικίλους κινδύνους τόσο για τη διεθνή όσο και για την εσωτερική ασφάλεια των κρατών. Οι κυβερνοεπιθέσεις είναι εύκολο να οργανωθούν και δύσκολο να εντοπιστούν. Υποκείμενα της απειλής μπορεί να είναι άλλα κράτη, μη κυβερνητικοί δρώντες, ακόμη και ένας απλός πολίτης.

Σαφώς, όπως σε όλους του τομείς της κοινωνικής ζωής, έτσι και σε αυτόν του Διαδικτύου, δε θα μπορούσε να λείπει και από αυτή τη νέα εξέλιξη η νομοθετική ρύθμιση, ώστε να δοθούν κατευθύνσεις και οδηγίες για την ασφάλεια των δικτύων και να αποφευχθεί ο κίνδυνος

ενός νέου τύπου τρομοκρατίας, αυτού της κυβερνοτρομοκρατίας. Για το σκοπό αυτό αναπτύχθηκαν στρατηγικές κυβερνοασφάλειας που παρέχουν προστασία έναντι των απειλών ασφάλειας και διασφαλίζουν την οικονομική και κοινωνική ευημερία. Ο στόχος των στρατηγικών αυτών είναι να ενισχύσουν την κυβερνητική συνεργασία, να ορίσουν αρμοδιότητες και ρόλους σε φορείς όσον αφορά τη δίωξη του ηλεκτρονικού εγκλήματος, αλλά και τη συνεργασία των φορέων, ιδίως των παρόχων υπηρεσιών Διαδικτύου, ιδιωτικών και δημόσιων, αλλά και τη διεθνή συνεργασία.

Η παρούσα εργασία έχει ως στόχο την αποτύπωση, ανάλυση και κριτική της Οδηγίας (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (στο εξής: η Οδηγία), με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ευρώπη. Η ΕΕ δε θα μπορούσε να μη λάβει πρωτοβουλίες προκειμένου να προασπιστεί τα δικαιώματα των πολιτών της και να διασφαλίσει ένα επίπεδο ασφάλειας και ευημερίας στο εσωτερικό της. Σε επόμενη ενότητα θα αναλύσουμε τις σκέψεις και τις ενέργειες που έχουν γίνει μέχρι σήμερα προκειμένου η Οδηγία NIS να επικαιροποιηθεί και να ψηφιστεί μία νέα, η NIS 2.

Η Οδηγία που είναι ευρέως γνωστή ως NIS, από τα αρχικά Network and Information Systems είναι ο πρώτος νόμος της ΕΕ για την Κυβερνοασφάλεια. Εκδόθηκε τον Ιούλιο του 2016, και τα κ-μ θα έπρεπε μέχρι τις οκτώ (8) Μαΐου 2018[1] να την έχουν ενσωματώσει στην εθνική τους έννομη τάξη. Η NIS συνέβαλε για πρώτη φορά στο να επιτευχθεί ένα κοινό και υψηλό επίπεδο ασφάλειας των συστημάτων δικτύου και

[1] Άρθρο 26 της Οδηγίας

πληροφοριών στην ΕΕ. Πώς έγινε αυτό, με τη θέσπιση μέτρων ασφαλείας και συνέχειας για τα συστήματα δικτύου και πληροφοριών που υποστηρίζουν την παροχή υπηρεσιών με σοβαρό αντίκτυπο στην ομαλή και εύρυθμη λειτουργία της αγοράς.

## *1.2. Προϊστορία- Τι οδήγησε στην υιοθέτησή της*

Η εξέλιξη αυτή ήταν απότοκος της συνειδητοποίησης του ζωτικού ρόλου της ασφάλειας των δικτύων για την κοινωνία μας εν γένει και για τις οικονομικές και κοινωνικές δραστηριότητες. Η συνειδητοποίηση άργησε γιατί μέχρι και πρόσφατα, επικρατούσε στην κοινή γνώμη η άποψη ότι στο Διαδίκτυο, παρά τα κοινότυπα περί «λαμπρού» πεδίου, δεν μπορούν να γίνουν «σοβαρές δουλειές». Στην Ελλάδα η δημόσια συζήτηση περιστρέφεται κυρίως γύρω από θέματα όπως η παιδική πορνογραφία και η οικονομική απάτη, δε φτάνει όμως σε μεγάλο βαθμό στην ευθύνη που έχουν οι πάροχοι υπηρεσιών για την προστασία των πολιτών από κυβερνοαπειλές.

Στην Ελλάδα συγκεκριμένα παρατηρείται ότι οι ενδιάμεσοι πάροχοι υπηρεσιών πρόσβασης στο Διαδίκτυο, ερμηνεύουν κατά το δοκούν τις ισχύουσες υποχρεώσεις τους, εκμεταλλευόμενοι την ασάφεια των κειμένων και τη χαλαρή επιτήρηση από την πληθώρα ανεξάρτητων αρχών. Αυτό αποδείχθηκε και από την αδιαφορία τους όταν το 2006 στην Ελλάδα παρουσιάστηκαν τα πρώτα δείγματα απάτης στα συστήματα υπολογιστών των τραπεζών και σε χρηματοπιστωτικούς οργανισμούς[2], αλλά και όταν το 2009 αντιμετώπισαν με αμηχανία τις

[2] Γ. Γιαννόπουλος, Η ευθύνη των παρόχων υπηρεσιών στο Internet, Νομική Βιβλιοθήκη, 2013, σελ.1

αντικρουόμενες επιταγές διαφορετικών αρχών (ΑΔΑΕ και Εισαγγελία ΑΠ) αναφορικά με την άρση ή μη του απορρήτου[3].

Το πρόβλημα έγινε ακόμη πιο έντονο τα τελευταία χρόνια, λόγω της δραματικής αύξησης των παραγόντων που δραστηριοποιούνται στο Διαδίκτυο. Είναι αυτοί που χαρακτηρίζονται ως ενδιάμεσοι πάροχοι υπηρεσιών, όπως τα κοινωνικά δίκτυα (Facebook, Instagram, Tik Tok), τα blogs, οι μηχανές αναζήτησης (google), οι ιστοσελίδες διεξαγωγής παιχνιδιών. Γρήγορα παρουσιάστηκαν τα πρώτα περιστατικά παράνομου και επιζήμιου περιεχομένου και η νομική κοινότητα (και όχι μόνο) βρέθηκε αντιμέτωπη με τα εξής ερωτήματα: ποια η ευθύνη αυτών των παρόχων και πώς θα ρυθμιστεί και θα ασφαλιστεί ο νέος διαδικτυακός κόσμος.

Οι κυβερνοεπιθέσεις ολοένα αυξάνονται και αλλάζουν μορφή. Εκδηλώνονται ως προσπάθεια υποκλοπής προσωπικών δεδομένων με εξαπάτηση των συναλλαζομένων (phishing) ή μέσω παράνομης πρόσβασης στα συστήματα των υπολογιστών ή κακόβουλης επιβάρυνσης του συστήματος, ώστε να προκύπτει αδυναμία παροχής υπηρεσιών (denial of service). Τελευταία παρατηρείται μόλυνση του λογισμικού με την απλή αποστολή ενός μηνύματος ηλεκτρονικού ταχυδρομείου, όπου ο χάκερ επισυνάπτει ένα σύνδεσμο. Ο ανυποψίαστος ή αφηρημένος λήπτης του μηνύματος μπορεί σε λίγα δευτερόλεπτα να παραχωρήσει πρόσβαση σε προσωπικά του στοιχεία ή ακόμη χειρότερα για το κοινωνικό σύνολο, να επιτρέψει την πρόσβαση σε δεδομένα κρατικά. Ο Κυβερνοχώρος είναι ένα περίπλοκο

[3] Γ. Γιαννόπουλος, Η ευθύνη των παρόχων υπηρεσιών στο Internet, Νομική Βιβλιοθήκη, 2013, Πρόλογος, σελ. IX

περιβάλλον, με αδιευκρίνιστο μέγεθος, όπου ο έλεγχος και η προστασία είναι αρκετά περίπλοκη υπόθεση. Αναφύεται λοιπόν η ανάγκη ύπαρξης κάποιας ρυθμιστικής και ελεγκτικής αρχής.

Οι κύριοι πάροχοι υπηρεσιών πρόσβασης στο Διαδίκτυο (Internet Service Providers- ISP) στην Ελλάδα είναι περίπου πέντε (5). Ωστόσο δε διαφαίνεται μεγάλη προθυμία των παρόχων να συνεργαστούν με ενδιαφερόμενους οργανισμούς προκειμένου να αντιμετωπιστεί η απάτη στο Διαδίκτυο. Το κύριο εμπόδιο που βλέπουν οι φορείς είναι ότι αδυνατούν με σύννομο τρόπο να εξακριβώσουν το χρήστη που κρύβεται πίσω από την παράνομη συμπεριφορά, καθώς θα προσέκρουε στη νομοθεσία για τα προσωπικά δεδομένα και την προστασία του απορρήτου ενέργειες που θα βοηθούσαν στην ταυτοποίηση του υπόπτου , όπως η διακοπή πρόσβασης σε ιστοσελίδα, η αποκάλυψη διευθύνσεων ανεπιθύμητης αλληλογραφίας ή οποιαδήποτε άλλη παροχή.

Στόχος της Οδηγίας είναι να εξασφαλίσει ότι τα κ-μ είναι έτοιμα και προετοιμασμένα να αντιμετωπίσουν τις επιθέσεις στον Κυβερνοχώρο, μέσω εθνικών αρχών, ομάδων απόκρισης για συμβάντα ασφαλείας των υπολογιστών και με την υιοθέτηση εθνικών στρατηγικών για την ασφάλεια στον Κυβερνοχώρο. Παρακάτω θα αναλύσουμε πως αυτοί οι στόχοι υλοποιήθηκαν στην Ελλάδα. Στο προοίμιο της Οδηγίας τονίζεται συχνά η ανάγκη προστασίας της εσωτερικής αγοράς της ΕΕ.

Σε δημόσια διαβούλευση[4] που διεξήγαγε η Ευρωπαϊκή Επιτροπή για το ηλεκτρονικό εμπόριο προσπάθησε να αναλύσει τα αίτια που είχαν καθηλώσει τις ηλεκτρονικές συναλλαγές στο 2% του συνόλου των λιανικών πωλήσεων. Στην Ελλάδα συγκεκριμένα στο όχι και τόσο μακρινό 2012 τα αποτελέσματα της έρευνας ήταν απογοητευτικά. Το 2010 το μέγεθος της διαδικτυακής οικονομίας ήταν 2,7 δις ευρώ, δηλαδή το 1,2% του ΑΕΠ, ποσοστό χαμηλότερο από το μέσο όρο της Ε.Ε. των 27, που ανέρχεται σε 3,8%. Από το ποσό αυτό η καταναλωτική δαπάνη συνέβαλε με 2,3 δις ευρώ στο ελληνικό ΑΕΠ και οι Έλληνες καταναλωτές ξόδεψαν 1,1 δις ευρώ για πρόσβαση στο Διαδίκτυο. Στο ηλεκτρονικό εμπόριο αντιστοιχεί 0,7 δις ευρώ της καταναλωτικής δαπάνης, με κύριο αντικείμενο τις ηλεκτρονικές κρατήσεις και αγορές που σχετίζονται με τον τουρισμό (περίπου 300 εκατομμύρια ευρώ), καθώς και την αγορά ηλεκτρονικών ειδών (περίπου 270 εκατομμύρια ευρώ)[5].

Τότε λοιπόν υπήρχε το όραμα της δημιουργίας ενός κυβερνοκόσμου ασφαλούς, τον οποίο οι πολίτες θα εμπιστεύονταν για όλο και περισσότερες καθημερινές τους ανάγκες. Οι εξελίξεις έτρεξαν με ραγδαίο ρυθμό, τα τελευταία δύο χρόνια της Πανδημίας Covid- 19. Έλαβαν χώρα μέσα σ' ένα χρόνο αλλαγές οι οποίες κανονικά θα χρειάζονταν περίπου 5- 10 χρόνια για να γίνουν. Ζήσαμε και ζούμε τον λεγόμενο ψηφιακό μετασχηματισμό, ακόμα και των μικρών επιχειρήσεων. Ακόμη δημιουργήθηκαν νέα μοντέλα στην αγορά, όπου η

[4] Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC)

[5] Έκθεση: Παράγων Ίντερνετ: Το Διαδίκτυο ως μοχλός ανάπτυξης, Boston Consulting Group, https://www.euro2day.gr/

φυσική παρουσία και το διαδίκτυο έπρεπε να συνεργαστούν, όπως το «click away» και το «click in shop».

Το ηλεκτρονικό εμπόριο στην Ελλάδα παρουσίασε ποσοστό ανάπτυξης +7 %. Πλέον το 85 % των καταναλωτών κάνει το 80 % των αγορών του διαδικτυακά. Το online grocery αναπτύχθηκε κατά +262 % σε σχέση με το 2012, ενώ το Online φαρμακείο κατά +18%[6]. Σύμφωνα με έρευνα[7] ο πρώτος λόγος που πλέον οι καταναλωτές εμπιστεύονται τις ηλεκτρονικές αγορές είναι κατά 43 % η ασφάλεια και η εμπιστοσύνη που τους προσφέρουν οι πάροχοι αναφορικά με τη διαδικασία πληρωμής.

Άλλωστε δεν πρέπει να παροράται ότι αυτή αποτελεί βασικό πυλώνα του ενωσιακού κεκτημένου.

Οι κίνδυνοι από τις απειλές του διαδικτύου είναι πολλαπλοί και μπορούν να προκαλέσουν βλάβες και δυσλειτουργίες στα συστήματα και σημαντική οικονομική ζημία στην ΕΕ. Ειδικά αν η εμπιστοσύνη των χρηστών υπονομευτεί. Πέρα όμως από την εσωτερική αγορά και η κυκλοφορία υπηρεσιών και προσώπων μπορεί να διαταραχθούν και να πληγούν ανεπανόρθωτα. Η προστασία του κυβερνοχώρου είναι από κάθε οπτική ουσιώδης για την ομαλή λειτουργία της ΕΕ.

[6] (πηγή eRetail Audit by Convert Group) https://convertgroup.com/insight/greek-egrocery-2020/?fbclid=IwAR2imoe0X8WlZRPqnJI8RP6wteDiDYG3C7ZI12mrQjnsuo3mw6CepLXtOd8

[7] Έρευνα του ELTRUN, https://digitalsteps.gr/ilektroniko-emporio-ellada/

## *1.3. Μεθοδολογία ανάπτυξης θέματος*

Η παρούσα εργασία πραγματεύεται με αναλυτικό τρόπο τη σημασία της Οδηγίας (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 6ης Ιουλίου 2016 για τη λήψη μέτρων για ένα υψηλό κοινό επίπεδο ασφαλείας των συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση.

Αρχικά ερευνήθηκε το ιστορικό πριν την υιοθέτηση της εν λόγω ευρωπαϊκής νομοθετικής πράξης και των λόγων που οδήγησαν την Επιτροπή στην αρχική της πρόταση. Κατόπιν επιχειρήθηκε μία ανάλυση με τις σημαντικότερες προβλέψεις της Οδηγίας και στο επόμενο υποκεφάλαιο αναλύθηκε πως αυτή ενσωματώθηκε στην Ελλάδα. Ειδικότερα, τις νομοθετικές πράξεις που λήφθηκαν για να συμμορφωθεί η χώρα μας με την Οδηγία, τις αρμόδιες αρχές που συστάθηκαν για να εξυπηρετήσουν αυτού στους σκοπούς και μία αποτίμηση της μέχρι σήμερα εφαρμογής της.

Η αποτίμηση αυτή δίνει με λογικό άλμα τη συνέχεια στο κεφάλαιο όπου αναλύονται οι λόγοι για τους οποίους η Επιτροπή οδηγήθηκε σε νέα Πρόταση σχετικά με τα μέτρα που εξασφαλίζουν ένα υψηλό και κοινό επίπεδο ασφάλειας του δικτύου και των πληροφοριών στην ΕΕ.

Στο επόμενο κεφάλαιο παρουσιάζεται το σχέδιο της νέας Οδηγίας (NIS II) η οποία θα έρθει να αντικαταστήσει την ισχύουσα, όπως αυτό

προκύπτει από την πρόταση της Επιτροπής προς το Ευρωκοινοβούλιο και το Συμβούλιο της ΕΕ, κατά τη συνήθη νομοθετική διαδικασία[8].

Εκεί και σύμφωνα με τα λίγα δεδομένα που έχουμε μέχρι τη στιγμή που γράφεται αυτή η εργασία, δεδομένου ότι όχι μόνο δεν έχει ψηφιστεί ακόμη αλλά και το σημαντικότερο, δεν έχει εφαρμοστεί από τα κ-μ, για να υπάρχει ολοκληρωμένη εικόνα, γίνεται ανάλυση των νέων προτάσεων και όπου κρίνεται σκόπιμο με συγκριτική ματιά ως προς την ισχύουσα Οδηγία, αιτιολογώντας ακριβώς και το λόγο της νέας πρόβλεψης. Γίνεται λόγος για την επέκταση του πεδίου εφαρμογής της οδηγίας, την ενίσχυση των προϋποθέσεων ασφαλείας για τις επιχειρήσεις και των ακριβώς προβλέψεων για τη διαδικασία που θα πρέπει να ακολουθείται στην αναφορά του συμβάντος καθώς και για την ενίσχυση των μηχανισμών επιβολής.

[8] Άρθρο 294 της ΣΛΕΕ

# 2

# *Ορισμοί – Έννοιες*

Στην παρούσα εργασία χρησιμοποιείται πληθώρα λέξεων με πρώτο συνθετικό το «κυβερνο-», όπως κυβερνοεπίθεση, κυβερνοασφάλεια, κυβερνοχώρος, κυβερνοτρομοκρατία. Είναι λέξεις της καθημερινότητας, που με το πρώτο συνθετικό μεταφέρονται στο χώρο του διαδικτύου, σ' αυτό το νοητό κόσμο που δημιουργείται με τους ηλεκτρονικούς υπολογιστές. Άλλωστε ο Κυβερνοχώρος είναι η αλληλεπίδραση των ανθρώπων μέσω του δικτύου, ανεξάρτητα από τη φυσική γεωγραφία.

Η **Κυβερνοτρομοκρατία** είναι η ξαφνική επίθεση μέσω του διαδικτύου κατά εθνικών ηλεκτρονικών υποδομών με σκοπό την απενεργοποίησή τους, την υποκλοπή ή την καταστροφή των δεδομένων τους.

**Κυβερνοασφάλεια** είναι η προσπάθεια προστασίας των δικτύων, των ηλεκτρονικών συσκευών μας που έχουν πρόσβαση στο διαδίκτυο και των δεδομένων που υπάρχουν εκεί. Για το σκοπό αυτό αναπτύχθηκαν διάφορες στρατηγικές για την καταπολέμηση του ηλεκτρονικού εγκλήματος, τη συνεργασία δημόσιων και ιδιωτικών φορέων, κρατών μελών της ΕΕ αλλά και διεθνώς. Ενδεικτικά, φορείς που

ηγούνται της κυβερνοπροστασίας είναι η Εθνική Αρχή Κυβερνοασφάλειας[9], η ομάδα CSIRT, ο ENISA και το Ευρωπαϊκό Κέντρο Ικανοτήτων.

Στην αναθεωρημένη πρόταση της Επιτροπής για την NIS II αποτυπώνεται και η έννοια της Κυβερνοασφάλειας. Στο άρ.4 παρ.3[10] παραπέμπει στον Κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[11], σύμφωνα με το άρ. 2 του οποίου «**κυβερνοασφάλεια**[12] είναι οι δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων».

Στο Ν. 4577/2018 η ασφάλεια των συστημάτων δικτύου και πληροφοριών ορίζεται ως η ικανότητα συστημάτων δικτύου και πληροφοριών να ανθίστανται με δεδομένο βαθμό αξιοπιστίας σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται , μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών

[9] Άρ. 43 επ. ΠΔ 40/2020.

[10] https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0017.02/DOC_1&format=PDF

[11] Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA (Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια) και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (ΕΕ L 151 της 7.6.2019, σ. 15).

[12] Άρθρο 2 παρ.1 του Κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου

υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών[13].

Στον ίδιο Κανονισμό παραπέμπει η Πρόταση και για τον ορισμό της **Κυβερνοαπειλής,** η οποία είναι «κάθε πιθανή περίσταση, πιθανό συμβάν ή πιθανή ενέργεια που θα μπορούσε να καταστρέψει, να διαταράξει ή να επιδράσει κατ' άλλον τρόπο δυσμενώς στα συστήματα δικτύου και πληροφοριών, στους χρήστες των εν λόγω συστημάτων και σε άλλα πρόσωπα»[14].

Η απουσία των δύο παραπάνω ορισμών, της Κυβερνοασφάλειας και Κυβερνοαπειλής, από τον NIS, οδήγησε στη μη δημιουργία της απαιτούμενης «κουλτούρας και νοοτροπίας» στα κ-μ ότι η ασφάλεια του διαδικτύου είναι δική τους ευθύνη[15]. Πλέον με τη συμπερίληψη των ορισμών γίνεται ξεκάθαρο ότι πρωταρχικός στόχος είναι η διασφάλιση της ανθεκτικότητας του Κυβερνοχώρου μέσω των απαιτήσεων Κυβερνοασφάλειας που οφείλουν τα κ-μ να τηρούν.

Κρίνεται σκόπιμο να παρατεθούν στο παρόν Κεφάλαιο και κάποιοι ορισμοί κοινών διαδικτυακών αδικημάτων, αυτών δηλαδή που μας οδηγούν στη συνεχή εγρήγορση για την πρόληψη και αντιμετώπισή τους. Ενδεικτικά αναφέρουμε την **παράνομη πρόσβαση** (illegal access), την εκ προθέσεως και χωρίς δικαίωμα πρόσβαση στο σύστημα ενός υπολογιστή παραβιάζοντας μέτρα ασφαλείας και η **παράνομη υποκλοπή δεδομένων** (illegal interception) η, μετά την τέλεση

[13] Άρθρο 3 παρ. 2 Ν. 4577/18

[14] Άρθρο 2 παρ.8 του Κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου

[15] Αιτιολογική Έκθεση της Οδηγίας

παράνομης πρόσβασης, απόκτηση μη δημόσιων δεδομένων με τεχνικά μέσα και την κακόβουλη περαιτέρω χρήση τους. Η **επέμβαση στο σύστημα** (system interference) είναι η εκ προθέσεως σοβαρή παρεμπόδιση της λειτουργίας ενός ηλεκτρονικού συστήματος και η **επέμβαση σε δεδομένα** (data interference), η χωρίς δικαίωμα και εκ προθέσεως πρόσβαση, καταστροφή, αλλοίωση , απόκρυψη ή και διαφοροποίηση δεδομένων. Τέλος, **η κακή χρήση συσκευών** (misuse of devices), είναι η με πρόθεση και χωρίς δικαίωμα παραγωγή, πώληση, διαβίβαση ή διάθεση κωδικών ή άλλων δεδομένων προκειμένου να συντελεστεί ένα από τα ανωτέρω αδικήματα[16].

**Εθνική Αρχή Κυβερνοασφάλειας** έχει οριστεί στην Ελλάδα η Γενική Διεύθυνση Κυβερνοασφάλειας[17] του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης ως αρμόδια εποπτική αρχή. Έχει ως αρμοδιότητα να χαράσσει την πολιτική Κυβερνοασφάλειας για τις κρίσιμες υποδομές του δημόσιου και ιδιωτικού τομέα, να ορίσει τους κανόνες και τις απαιτήσεις ασφαλείας για τις οντότητες που υπάγονται στο πεδίο εφαρμογής της Οδηγίας NIS και να διασφαλίζει την τήρηση του επιπέδου αυτού, να συνεργάζεται με συναρμόδιους φορείς σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο και να προάγει την επιστημονική έρευνα και την εκπαίδευση – επιμόρφωση στα θέματα κυβερνοασφάλειας.

[16] Άρθρα 2-6 της Σύμβασης της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο

[17] Βάσει του Ν. 4577/2018 (Α΄199), ο οποίος ενσωματώνει στην ελληνική έννομη τάξη το πλαίσιο των διατάξεων της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου, σχετικά με μέτρα για το υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, την NIS.

Μεταξύ των φορέων που συνίσταται να συνεργάζεται η Γενική Διεύθυνση Κυβερνοασφάλειας είναι και η συνεργασία με την αρμόδια **CSIRT** (Computer Security Incident Response Team), με σκοπό την από κοινού τήρηση των υποχρεώσεων της χώρας. Η CSIRT είναι η Αρμόδια Ομάδα Απόκρισης για την παρακολούθηση συμβάντων που αφορούν την ασφάλεια των υπολογιστών και έχει στην ευθύνη της:

Α) τη διαχείριση και αντιμετώπιση κινδύνων και συμβάντων με βάση συγκεκριμένη διαδικασία

Β) την ανάλυση των κινδύνων και την επίγνωση της κατάστασης

Γ) τη συμμετοχή της στο δίκτυο CSIRT

Δ) την προώθηση της χρήσης τυποποιημένων πρακτικών για τη διαχείριση ενός περιστατικού και

Ε) τη συνεργασία με ιδιωτικούς φορείς

Στην Ελλάδα το ρόλο αυτό διαδραματίζει η **Διεύθυνση Κυβερνοάμυνας** του ΓΕΕΘΑ[18]. Διαθέτει τεχνική επάρκεια και εμπειρογνωμοσύνη για να στηρίξει τους φορείς στο χειρισμό τυχόν συμβάντων. Οι φορείς έχουν υποχρέωση να κοινοποιούν και στη CSIRT τα κρίσιμα περιστατικά ασφαλείας. Ωστόσο ο ρόλος της είναι καθαρά γνωμοδοτικός και όχι εποπτικός, όπως της Γενικής Διεύθυνσης Κυβερνοασφάλειας.

Η Διεύθυνση Κυβερνοάμυνας καλύπτει τομείς όπως η ενέργεια, οι μεταφορές, χρηματοπιστωτικές αγορές, οι τράπεζες, η υγεία, η προμήθεια πόσιμου νερού, ψηφιακές υποδομές και υπηρεσίες , όπως οι

[18] Υ.Α. υπ’ αριθμ. 1027/2019 (Β’ 3739).

Online αγορές, οι Online μηχανές αναζήτησης και οι υπηρεσίες νεφοϋπολογιστικής (cloud).

Ο **ENISA** είναι ο ευρωπαϊκός Οργανισμός για την ασφάλεια των δικτύων και της πληροφορικής και συγκεκριμένα για την επίτευξη ενός κοινού επιπέδου κυβερνοασφάλειας στην Ευρώπη. Ιδρύθηκε το 2004 και έκτοτε αγωνίζεται για την ενίσχυση της εμπιστοσύνης στην ψηφιακή οικονομία, την τόνωση της ανθεκτικότητας των υποδομών της ΕΕ και τη διατήρηση της ψηφιακής ασφάλειας για τους πολίτες.

**ΦΕΒΥ**[19]: Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, σύμφωνα με το άρ. 4 της Οδηγίας θεωρούνται «οι δημόσιες ή ιδιωτικές οντότητες», οι οποίες καταγράφονται αναλυτικά στο Παράρτημα ΙΙ και «πληρούν τα κριτήρια που ορίζονται στο άρ. 5 παρ.2 της Οδηγίας. Ενδεικτικά οι ΦΕΒΥ εμπίπτουν στους τομείς της ενέργειας, των μεταφορών, των τραπεζικών και χρηματοπιστωτικών υπηρεσιών, της υγείας, του πόσιμου νερού και της ψηφιακής υποδομής. Στο Παράρτημα αναγράφονται και οι υποτομείς των ανωτέρω κατηγοριών[20]. Ο κατάλογος αυτός δεν είναι εξαντλητικός και οι χώρες έχουν ενσωματώσει διαφορετικούς κλάδους. Επί παραδείγματι[21], η δημόσια διοίκηση έχει ενταχθεί από χώρες όπως η Κύπρος, η Μάλτα, η Αυστρία, η Λιθουανία, η Ισπανία, η Κροατία και η Ελβετία, ενώ η παιδεία έχει ενταχθεί από τη Γαλλία. Τα διαστημικά και ερευνητικά κέντρα έχουν ενταχθεί από την Ισπανία. Βλέπουμε ότι η ελευθερία οδηγεί σε ανομοιομορφία μεταξύ των κ-μ και αυτό θα ήταν

[19] Οδηγία παρ. 14

[20] Οδηγία παρ. 50, Παράρτημα ΙΙ

[21] Nicolas Van Tieghem, Nicolas Lfebvre, "While preparing the NIS 2, update of the European Overview of NIS transposition by the Member States…toward convergence?», Riskinsight

καλό να εξαλειφθεί και να ενταχθούν ρητά, σε μελλοντική τροποποίηση, και άλλοι τομείς, οι οποίοι όμως θα είναι ίδιοι για όλα τα κ-μ. Ενδεικτικά, θα μπορούσε να προστεθεί η δημόσια διοίκηση, οι ταχυδρομικές υπηρεσίες, η πολιτική προστασία, η προστασία του περιβάλλοντος, ο τομέας των τροφίμων και η βιομηχανία.

**ΠΨΥ**[22]: Πάροχοι Ψηφιακών Υπηρεσιών. Είναι η δεύτερη κατηγορία που εντάσσεται στο πεδίο εφαρμογής της Οδηγίας. Σύμφωνα με το άρ. 4 της Οδηγίας, ΠΨΥ θεωρούνται «τα νομικά πρόσωπα που παρέχουν ψηφιακές υπηρεσίες». Συμπεριλαμβάνουν τις υπηρεσίες επιγραμμικής αγοράς (online marketplaces), μηχανής αναζήτησης (online search engines) και νεφοϋπολογιστικής (cloud computing). Σε αντίθεση με τους ΦΕΒΥ, οι ΠΨΥ δεν προσδιορίζονται από τα κ-μ, αλλά εντάσσονται όλοι αυτόματα, λόγω του διασυνοριακού τους χαρακτήρα.

Αναλυτικότερα, **επιγραμμική αγορά** ορίζεται «η ψηφιακή υπηρεσία που επιτρέπει σε καταναλωτές και/ή εμπόρους να συνάπτουν επιγραμμικές συμβάσεις πώλησης ή παροχής υπηρεσιών με εμπόρους είτε στον ιστοχώρο της επιγραμμικής αγοράς είτε σε ιστοχώρο εμπόρου που χρησιμοποιεί υπηρεσίες υπολογιστικής παρεχόμενες από επιγραμμική αγορά»[23].

Ως **επιγραμμική μηχανή αναζήτησης** ορίζεται η «ψηφιακή υπηρεσία που επιτρέπει στους χρήστες να εκτελούν αναζητήσεις καταρχήν σε όλους τους ιστοχώρους ή σε ιστοχώρους συγκεκριμένης γλώσσας βάσει ερωτήματος για οποιοδήποτε θέμα, με τη μορφή λέξης κλειδιού, φράσης ή άλλων δεδομένων, και επιστρέφει ως αποτέλεσμα

[22] Άρθρο 5 της Οδηγίας συν σημείωση 50 ???

[23] Άρθρο 4 της Οδηγίας

συνδέσμους όπου μπορεί κανείς να βρει πληροφορίες σχετικές με το περιεχόμενο που έχει ζητηθεί»[24]. Τέλος, ως **υπηρεσία νεφοϋπολογιστική** ορίζεται «η ψηφιακή υπηρεσία που επιτρέπει την πρόσβαση σε κλιμακοθετήσιμο και ελαστικό σύνολο κοινόχρηστων υπολογιστικών πόρων»[25].

Ορισμένα παραδείγματα από την καθημερινότητα για να γίνουν πιο εύληπτοι οι εξειδικευμένοι όροι είναι τα ακόλουθα: ηλεκτρονικές αγορές μέσω ιστοσελίδων, όπως είναι το SHEIN, Aliexpress είναι παραδείγματα επιγραμμικών αγορών, όπως επίσης και το Netflix. Επιγραμμική μηχανή αναζήτησης είναι το Google και η Amazon. Και νεφοϋπολογιστική υπηρεσία είναι ο πρόσθετος χώρος αποθήκευσης που αγοράζουμε, όπως το iCloud στα iPhones.

Σύμφωνα με την αιτιολογική σκέψη 53 της NIS «σε περίπτωση παρόχων ψηφιακών υπηρεσιών, οι απαιτήσεις αυτές δεν θα πρέπει να εφαρμόζονται στις μικρές ή στις πολύ μικρές επιχειρήσεις». Ως **μικρή επιχείρηση** ορίζεται «η επιχείρηση που απασχολεί λιγότερους από 50 εργαζόμενους και της οποίας ο ετήσιος κύκλος εργασιών ή το σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα δέκα εκατομμύρια ευρώ»[26]. Ως **πολύ μικρή επιχείρηση** θεωρείται «η επιχείρηση που απασχολεί λιγότερους από δέκα εργαζόμενους και της οποίας ο ετήσιος κύκλος εργασιών ή το σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα δύο

[24] Άρθρο 4 της Οδηγίας

[25] Άρθρο 4 της Οδηγίας

[26] Σύσταση Ευρωπαϊκής Επιτροπής «Σύσταση της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών και μεσαίων επιχειρήσεων, ημερομηνίας 6/5/2003, υπ' αριθμ. 2003/361/ΕΚ, άρ.2 παρ. 2.

εκατομμύρια ευρώ»[27]. Για τις μικρές επιχειρήσεις, η συμμόρφωση προς τις ευρωπαϊκές επιταγές, όπως προκύπτουν από την NIS, ενδέχεται να αποτελέσουν δυσανάλογο οικονομικό βάρος γι' αυτές[28]. Σημειώνεται ωστόσο ότι μια ενιαία εφαρμογή κανόνων ασφαλείας μπορεί να δημιουργήσουν προβλήματα στο μέλλον.

[27] Σύσταση Ευρωπαϊκής Επιτροπής «Σύσταση της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών και μεσαίων επιχειρήσεων, ημερομηνίας 6/5/2003, υπ' αριθμ. 2003/361/ΕΚ, άρ.2 παρ. 2.

[28] Maria Theres Holzleitner, Johannes Reicht, "European provisions for cybersecurity in the smart grid an overview of th NIS- directive", Elektrotechnik Und Informationstechnik, Vol 134, No.1, 2017, p. 15

# 3

# *Οδηγία NIS*

## *3.1. Τι προβλέπει*

Η Οδηγία NIS θεσπίζει μέτρα για την επίτευξη ενός υψηλού κοινού επιπέδου ασφαλείας συστημάτων δικτύου και πληροφοριών εντός της Ένωσης και πιο συγκεκριμένα: α) προβλέπει τις υποχρεώσεις να θεσπιστεί εθνική στρατηγική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών από όλα τα κ-μ, β) δημιουργεί ομάδα συνεργασίας με σκοπό την υποστήριξη και διευκόλυνση της στρατηγικής συνεργασίας και ανταλλαγής πληροφοριών μεταξύ των κ-μ, καθώς και την ανάπτυξη εμπιστοσύνης και αξιοπιστίας μεταξύ τους, γ) δημιουργεί δίκτυο ομάδων απόκρισης συμβάντων που αφορούν την ασφάλεια των υπολογιστών (δίκτυο CSIRT), προκειμένου να συμβάλει στην ανάπτυξη της αξιοπιστίας και εμπιστοσύνης μεταξύ των κ-μ και να προωθήσει την ταχεία και αποτελεσματική επιχειρησιακή συνεργασία, δ) θεσπίζει απαιτήσεις ασφαλείας και κοινοποίησης για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και για τους παρόχους ψηφιακών υπηρεσιών, ε) προβλέπει τις υποχρεώσεις των κ-μ να ορίζουν εθνικές αρμόδιες αρχές ,

ενιαία κέντρα επαφής και CSIRT με καθήκοντα σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών.

Η Οδηγία 2016/1148 θεσπίζει μέτρα ελάχιστης εναρμόνισης, σύμφωνα με το άρθρο 3. Συνεπώς τα κ-μ μπορούν να θεσπίζουν ή να διατηρούν διατάξεις με σκοπό την επίτευξη υψηλότερου επιπέδου κυβερνοασφάλειας. Ωστόσο, σύμφωνα με το άρθρο 16 παρ.10 δεν μπορούν να επιβάλλουν οποιεσδήποτε περαιτέρω απαιτήσεις ασφάλειας ή κοινοποίησης στους παρόχους ψηφιακών υπηρεσιών.

Βάσει της Οδηγίας, τα κ-μ είναι υποχρεωμένα να ορίσουν μία ή περισσότερες εθνικές αρμόδιες αρχές και να ορίσουν σημείο επαφής , σε περίπτωση που υπάρχουν περισσότερες από μία αρμόδιες αρχές. Ακόμη πρέπει να προσδιορίσουν τους βασικούς παρόχους υπηρεσιών σε τομείς όπως η ενέργεια, οι μεταφορές, η χρηματοδότηση, οι τράπεζες, η υγεία, η ύδρευση και η ψηφιακή υποδομή, τομείς δηλαδή στους οποίους η επίθεση θα μπορούσε να διαταράξει μία βασική υπηρεσία της κοινωνίας και των πολιτών.

Αναλυτικότερα, οι βασικές διατάξεις της Οδηγίας αφορούν:

- Τον καθορισμό των υποχρεώσεων των κ-μ όσον αφορά το επίπεδο ασφαλείας που πρέπει να τηρείται για την πρόληψη, το χειρισμό και την απόκριση σε κινδύνους που επηρεάζουν τα συστήματα
- Τη συνεργασία μεταξύ των κ-μ ώστε να διασφαλίζεται η ενιαία εφαρμογή των κανόνων και η ενιαία αντιμετώπιση, όπου χρειάζεται , συντονισμένα και αποτελεσματικά, σε περίπτωση διασυνοριακής κυβερνοεπίθεσης
- Πέρα από τις υποχρεώσεις που απορρέουν για την εθνική αρχή ασφάλειας, αντίστοιχες υποχρεώσεις πηγάζουν και για τους φορείς

παροχής ουσιωδών υπηρεσιών, ψηφιακών υπηρεσιών και τη δημόσια διοίκηση

- Συγκρότηση ειδικών μονάδων έκτακτων αναγκών για την αντιμετώπιση ζητημάτων
- Και την παρακολούθηση της εφαρμογής όλων αυτών από ειδική εθνική αρχή

Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ)[29], αναφέρεται ότι, σύμφωνα με το άρ. 4 της Οδηγίας, όπως αναλύθηκε σε παραπάνω κεφάλαιο, ορίζονται «οι δημόσιες ή ιδιωτικές οντότητες», οι οποίες καταγράφονται αναλυτικά στο Παράρτημα ΙΙ και «πληρούν τα κριτήρια που ορίζονται στο άρ. 5 παρ.2 της Οδηγίας. Ενδεικτικά οι ΦΕΒΥ εμπίπτουν στους τομείς της ενέργειας, των μεταφορών, των τραπεζικών και χρηματοπιστωτικών υπηρεσιών, της υγείας, του πόσιμου νερού και της ψηφιακής υποδομής. Στο Παράρτημα αναγράφονται και οι υποτομείς των ανωτέρω κατηγοριών[30].

Τα κριτήρια που θα πρέπει να κατέχει μία οντότητα ιδιωτική ή δημόσια για να πληροί της προϋποθέσεις ένταξης στο Παράρτημα ΙΙ , είναι, σύμφωνα με το άρθρο 5 παρ. 2 της Οδηγίας : «α) να παρέχει υπηρεσία ουσιώδη για τη διατήρηση κρίσιμων κοινωνικών ή- και οικονομικών δραστηριοτήτων, β) η παροχή αυτής της υπηρεσίας να στηρίζεται σε συστήματα δικτύου και πληροφοριών και γ) τυχόν συμβάν στη λειτουργία του συστήματος δικτύου και πληροφοριών» να μπορεί

[29] Οδηγία παρ. 14

[30] Οδηγία παρ. 50, Παράρτημα ΙΙ

να προκαλέσει σοβαρή διατάραξη της παροχής της εν λόγω υπηρεσίας»[31].

Σύμφωνα με το άρθρο 6 της Οδηγίας αυτό που προσδιορίζει τη σοβαρότητα της διατάραξης είναι «ο αριθμός των χρηστών που εξαρτώνται από την υπηρεσία που παρέχεται από την οικεία οντότητα, η εξάρτηση άλλων τομέων που αναφέρονται στο παράρτημα ΙΙ από την υπηρεσία που παρέχεται από την εν λόγω οντότητα, ο αντίκτυπος που θα μπορούσαν να έχουν τα συμβάντα, από άποψη βαθμού και διάρκειας, σε οικονομικές και κοινωνικές δραστηριότητες ή στη δημόσια ασφάλεια, το μερίδιο αγοράς της εν λόγω οντότητας, το γεωγραφικό εύρος της περιοχής που θα μπορούσε να επηρεαστεί από ένα συμβάν και η σημασία του φορέα για τη διατήρηση επαρκούς επιπέδου της υπηρεσίας, λαμβανομένων υπόψη των διαθέσιμων εναλλακτικών μέσων για την παροχή της εν λόγω υπηρεσίας»[32].

Τα τρία αυτά κριτήρια θα πρέπει να σωρεύονται σε μια οντότητα για να χαρακτηριστεί αυτή ως ΦΕΒΥ[33]. Άρα δεν εμπίπτουν αυτοδικαίως όλοι οι φορείς του Παραρτήματος ΙΙ στο πεδίο εφαρμογής της Οδηγίας. Εναπόκειται στο κ-μ να αποφασίσει εάν προσφέρει «ουσιώδη παροχή». Το κάθε κ-μ ανέλαβε την υποχρέωση με περιθώριο έξι μηνών (ως 9 Νοεμβρίου 2018), από την προθεσμία ενσωμάτωσης της Οδηγίας, να καταρτίσουν κατάλογο αναγνωρισμένων φορέων εκμετάλλευσης βασικών υπηρεσιών. Αυτό σημαίνει ότι αν κάποιος φορέας δεν

[31] Άρθρο 5 της Οδηγίας

[32] Άρθρο 6 της Οδηγίας

[33] Dimitra Markopoulou, Vangelis Papakonstantinou , Paul de Hert "The new EU cybersecurity framework The NIS Directive , ENISA' S role and thw General Data Protection Regulation", Computer law & Security review, Issue 6, 2019, pp. 3-6

πληρούσε ένα από τα τρία στοιχεία δεν θα εντάσσονταν στον κατάλογο και θα έπρεπε να περιμένει για δύο έτη, χρονικό διάστημα κατά το οποίο ο κατάλογος ανανεώνεται και εντάσσονται νέες οντότητες[34]. Προληπτικά λοιπόν διάφορα κράτη, δημιούργησαν έναν εκτενή κατάλογο φορέων για να αποφύγουν τυχόν κυρώσεις λόγω έλλειψης συμμόρφωσης, διόλου απίθανο δεδομένης της ασάφειας των κριτηρίων του άρ. 5 παρ.2.

Οι Πάροχοι Ψηφιακών Υπηρεσιών [35] είναι η δεύτερη κατηγορία που εντάσσεται στο πεδίο εφαρμογής της Οδηγίας. Σύμφωνα με το άρ. 4 της Οδηγίας, ΠΨΥ θεωρούνται «τα νομικά πρόσωπα που παρέχουν ψηφιακές υπηρεσίες». Συμπεριλαμβάνουν τις υπηρεσίες επιγραμμικής αγοράς (online marketplaces), μηχανής αναζήτησης (online search engines) και νεφοϋπολογιστικής (cloud computing). Σε αντίθεση με τους ΦΕΒΥ, οι ΠΨΥ δεν προσδιορίζονται από τα κ-μ , αλλά εντάσσονται όλοι αυτόματα, λόγω του διασυνοριακού τους χαρακτήρα.

Ας δούμε τώρα τι υποχρεώσεις υπέχουν οι ΦΕΒΥ και ΠΨΥ στο πλαίσιο εφαρμογής της Οδηγίας NIS:

- Οφείλουν να ορίσουν Υπεύθυνο Ασφάλειας Πληροφοριών και Δικτύων, ως σημείο επαφής με τις αρμόδιες αρχές και με ρόλο την επίβλεψη και το συντονισμό των ενεργειών συμμόρφωσης
- Οφείλουν να χαράξουν και να αποδείξουν μια πολιτική με σαφώς καθορισμένους στόχους ασφάλειας και επιχειρησιακής συνέχεια στο πνεύμα της Εθνικής Στρατηγικής Κυβερνοασφάλειας

[34] Dimitra Markopoulou, Vangelis Papakonstantinou , Paul de Hert “The new EU cybersecurity framework The NIS Directive , ENISA’ S role and thw General Data Protection Regulation”, Computer law & Security review, Issue 6, 2019, pp. 3-6

[35] Άρθρο 5 της Οδηγίας

- Να πραγματοποιούν μελέτες εκτίμησης των κινδύνων ασφαλείας και να λαμβάνουν τα κατάλληλα μέτρα στα συστήματα που υποστηρίζουν τις δραστηριότητές τους
- Να ενημερώνουν χωρίς καθυστέρηση και εμπεριστατωμένα την Εθνική Αρχή Κυβερνοασφάλειας και στην εθνική CSIRT για τα συμβάντα που εμφανίστηκαν και που τυχόν είχαν σοβαρό αντίκτυπο στην εύρυθμη λειτουργία των υπηρεσιών τους.
- Να αυτοαξιολογούνται και να υποβάλλουν σχετική αναφορά με ταυτόχρονη αποτύπωση των ενεργειών, του πλάνου δηλαδή που έχουν για τη διόρθωση των αδυναμιών ασφαλείας και ως προς την αξιοποίηση των ευκαιριών βελτίωσης.
- Ενημέρωση όλων των εργαζομένων σχετικά με τα πρωτόκολλα ασφαλείας των συστημάτων δικτύου και πληροφορικής

Σύμφωνα με το άρ. 14 παρ. 1 της Οδηγίας, οι φορείς εκμετάλλευσης Βασικών υπηρεσιών οφείλουν να «λάβουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα, λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες», με στόχο τη διαχείριση των κινδύνων[36]. Επιπρόσθετα, θα πρέπει « να λαμβάνουν κατάλληλα μέτρα για την αποτροπή και ελαχιστοποίηση του αντίκτυπου των συμβάντων , για τη διασφάλιση της συνέχειάς του»[37]. Με δύο λόγια λοιπόν οφείλουν να διαχειρίζονται τους κινδύνους και να εξασφαλίζουν τη συνέχεια στη λειτουργία των υπηρεσιών τους, ελαχιστοποιώντας τις συνέπειες τυχόν κυβερνοεπίθεσης. Κύριο μέλημα λοιπόν είναι να μη διακόψουν τη λειτουργία τους, γιατί πιθανή διακοπή, ανεξαρτήτως του πως θα

[36] Άρ. 14 της Οδηγίας

[37] Άρ. 14 της Οδηγίας

εκδηλωθεί, εκτιμάται ότι θα έχει αντίκτυπο στην εσωτερική αγορά της Ένωσης[38].

Σημειωτέον ότι χρησιμοποιούνται στο κείμενο της Οδηγίας λέξεις γενικές, όπως «κατάλληλα» και «αναλογικά», χωρίς να ερμηνεύονται, γεγονός που αφήνει τα κ-μ να ερμηνεύουν τα ίδια τι συνιστά αναλογικό και κατάλληλο μέτρο τη δεδομένη στιγμή. Η Οδηγία αφήνει στην υποκειμενική κρίση των παρόχων να εκτιμήσουν κάθε φορά την κατάσταση και να λάβουν μέτρα, το κόστος των οποίων θα πρέπει να είναι ανάλογο των ενδεχόμενων κινδύνων[39]. Απ' αυτή την άποψη ορθά η Οδηγία αποφεύγει να επιβάλλει διοικητικά και οικονομικά βάρη στους φορείς, διότι ενδέχεται να ήταν δυσανάλογα. Θα πρέπει η κάθε περίπτωση να εξετάζεται μεμονωμένα και να εκτιμάται ο κίνδυνος σε συνάρτηση με το κόστος ώστε να ευοδωθούν οι στόχοι της Οδηγίας[40].

Είναι σαφές ότι οι φορείς καλούνται να αναπτύξουν ένα ολοκληρωμένο σύστημα ασφαλείας των υπηρεσιών τους. Σύμφωνα με το άρθρο 19 της Οδηγίας, και προς αυτή την κατεύθυνση, οι φορείς ενθαρρύνονται να χρησιμοποιήσουν ευρωπαϊκά ή διεθνώς αποδεκτών προτύπων και προδιαγραφών ασφαλείας, όπως είναι για παράδειγμα τα πρότυπα ISO/IEC 27001:2018, ISO 22301:2018, ISA/IEC 62443-4-2 και

[38] Dimitra Markopoulou, Vangelis Papakonstantinou , Paul de Hert "The new EU cybersecurity framework The NIS Directive , ENISA' S role and thw General Data Protection Regulation", Computer law & Security review, Issue 6, 2019, pp.3-6

[39] Johan David Michels, Ian Walden, "Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?" , European Law Review, 2020, Vol. 45, Issue 1, p.25

[40] Johan David Michels, Ian Walden, "Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?" European Law Review, 2020, Vol. 45, Issue 1, p. 35- 36.

NIST SP 800-82, τα οποία αποτελούν ένα πολύτιμο οδηγό για τις επιχειρήσεις.

Το ερώτημα που προκύπτει αβίαστα είναι πως θα διαπιστωθεί ότι ελήφθησαν πράγματι τα κατάλληλα και αναλογικά μέτρα σε κάθε περίπτωση και σαφώς επανερχόμαστε και στο ζήτημα της ομοιόμορφης εφαρμογής και της κοινής προσέγγισης των κινδύνων από τα κ-μ. Θυμίζουμε ότι σκοπός της Οδηγίας είναι η ομοιόμορφη αντιμετώπιση των κινδύνων και των περιστατικών κυβερνοεπίθεσης, διότι οι πρακτικές που εφαρμόζονταν μέχρι και πριν την εφαρμογή της Οδηγίας, δεν ήταν αρκετές ούτε αποτελεσματικές.

Γι’ αυτό το λόγο είναι σημαντική η αποσαφήνιση των όρων. Είναι κομβικής σημασίας για την ορθή εφαρμογή των κατευθυντήριων από την Οδηγία γραμμών, για να μην αποκλίνουν τα κ-μ στις πρακτικές που εφαρμόζουν, όπως άλλωστε συνέβαινε πριν την Οδηγία. Θα μπορούσε το κείμενο της Οδηγίας να θέτει κάποιες ελάχιστες απαιτήσεις, εάν όχι ορισμούς[41].

Ακόμη στο άρθρο 14 σημειώνεται και η υποχρέωση των φορέων για κοινοποίηση των περιστατικών. Συγκεκριμένα «θα πρέπει να κοινοποιούν χωρίς αδικαιολόγητη καθυστέρηση στην αρμόδια αρχή ή στην CSIRT συμβάντα με σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών που παρέχουν. Οι κοινοποιήσεις περιλαμβάνουν πληροφορίες που επιτρέπουν στην αρμόδια αρχή ή στην ομάδα απόκρισης να προσδιορίσει τυχόν διασυνοριακό αντίκτυπο του

[41] Dimitra Markopoulou, Vangelis Papakonstantinou , Paul de Hert “The new EU cybersecurity framework The NIS Directive , ENISA’ S role and thw General Data Protection Regulation”, Computer law & Security review, Issue 6, 2019, pp. 3-6

συμβάντος. Η κοινοποίηση δεν συνεπάγεται αυξημένη ευθύνη για τον κοινοποιούνται»[42]. Κρατάμε ότι κοινοποιούνται τα συμβάντα με «σοβαρό αντίκτυπο», άρα δεν απαιτείται η κοινοποίηση κάθε συμβάντος παρά μόνο ό, τι κρίνεται σοβαρό από τον ίδιο το φορέα εκμετάλλευσης.

Για τον προσδιορισμό της σοβαρότητας ή όχι του αντικτύπου ενός συμβάντος αναφέρονται συγκεκριμένες παράμετροι που θα πρέπει να ληφθούν υπόψη[43]. Συγκεκριμένα, να λαμβάνεται υπόψη «ο αριθμός των χρηστών που επηρεάζονται από τη διάταξη της βασικής υπηρεσίας , η διάρκεια του συμβάντος και το γεωγραφικό εύρος της περιοχής που επηρεάζονται από το συμβάν»[44]. Τα στοιχεία αυτά θα πρέπει να συνεκτιμώνται κάθε φορά σωρευτικά για τη διαπίστωση του κατά πόσο η διατάραξη είναι όντως σοβαρή ή όχι[45]. Η λύση στο πρόβλημα του μη ορισμού και περιορισμού των εννοιών θα ήταν κατά τη γνώμη του γράφοντος η παραπομπή μιας υπόθεσης στο Δικαστήριο της Ευρωπαϊκής Ένωσης ή η αναθεώρηση της Οδηγίας.

Όσον αφορά τους παρόχους ψηφιακών υπηρεσιών, αυτοί θα πρέπει να «λάβουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα, λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες», με σκοπό πάντα τη διαχείριση των κινδύνων[46]. Θα πρέπει

[42] Άρθρο 14 της Οδηγίας.

[43] Άρθρο 14 παρ.4 της Οδηγίας.

[44] Άρθρο 14 της Οδηγίας

[45] Dimitra Markopoulou, Vangelis Papakonstantinou , Paul de Hert "The new EU cybersecurity framework The NIS Directive , ENISA' S role and thw General Data Protection Regulation", Computer law & Security review, Issue 6, 2019, pp. 3-6

[46] Άρθρο 16 της Οδηγίας

να συνεκτιμούν « α) την ασφάλεια των συστημάτων και των εγκαταστάσεων, β) τη διαχείριση των συμβάντων , γ) τη διαχείριση της υπηρεσιακής συνέχειας, δ) την παρακολούθηση, τις επιθεωρήσεις και τις δοκιμές , ε) τη συμμόρφωση με διεθνή πρότυπα»[47].

Υπογραμμίζεται η «συνεκτίμηση των κινδύνων», που σημαίνει ότι ο πάροχος οφείλει όλα τα ανωτέρω να λάβει υπόψιν του σωρευτικά[48].

Ακόμη αναφέρεται ότι οι πάροχοι πρέπει να λάβουν «κατάλληλα μέτρα για την αποτροπή και ελαχιστοποίηση του αντίκτυπου των συμβάντων , για τη διασφάλιση της συνέχειας του»[49]. Επομένως οφείλουν και να διαχειριστούν τον κίνδυνο αλλά και να εξασφαλίσουν τη συνέχεια των υπηρεσιών τους, ελαχιστοποιώντας και εκμηδενίζοντας την απειλή.

Δε θα μπορούσε να λείπει και στους παρόχους η υποχρέωση κοινοποίησης των συμβάντων. Ειδικότερα, «οι πάροχοι ψηφιακών υπηρεσιών κοινοποιούν στην αρμόδια αρχή ή στην CSIRT χωρίς αδικαιολόγητη καθυστέρηση κάθε συμβάν που έχει σημαντικό αντίκτυπο στην παροχή της υπηρεσίας που προσφέρουν εντός της Ένωσης, όπως αναφέρεται στο Παράρτημα ΙΙΙ. Οι κοινοποιήσεις περιλαμβάνουν πληροφορίες που επιτρέπουν στην αρμόδια αρχή ή την CSIRT να προσδιορίσουν τη σοβαρότητα τυχόν διασυνοριακού

[47] Άρθρο 16 της Οδηγίας

[48] Dimitra Markopoulou, Vangelis Papakonstantinou , Paul de Hert “The new EU cybersecurity framework The NIS Directive , ENISA’ S role and thw General Data Protection Regulation”, Computer law & Security review, Issue 6, 2019, pp. 3-6

[49] Άρθρο 16 παρ.2 της Οδηγίας

αντίκτυπου. Η κοινοποίηση δεν συνεπάγεται αυξημένη ευθύνη για τον κοινοποιούντα»[50].

Για τον προσδιορισμό ενός συμβάντος ως σημαντικού λαμβάνεται υπόψη «α) ο αριθμός των χρηστών που επηρεάζονται από το συμβάν, ιδίως των χρηστών που εξαρτώνται από την υπηρεσία για την παροχή των δικών τους υπηρεσιών, β) η διάρκεια του συμβάντος, γ) το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν , δ) η έκταση της διατάραξης της λειτουργίας της υπηρεσίας, ε) η έκταση του αντίκτυπου στις οικονομικές και κοινωνικές δραστηριότητας»[51]. Και εδώ όλες οι συνισταμένες πρέπει να συνυπολογίζονται.

Εκ των ανωτέρω συνάγεται ότι τόσο οι πάροχοι εκμετάλλευσης βασικών υπηρεσιών όσο και οι φορείς βασικών υπηρεσιών έχουν υποχρέωση κοινοποίησης του κινδύνου όταν υπάρχει «σημαντικός αντίκτυπος συμβάντος» και «σοβαρός αντίκτυπος συμβάντος», αντίστοιχα. Και παρόλο που η Οδηγία θέτει κάποιες παραμέτρους, ωστόσο οι έννοιες δεν παύουν να παραμένουν αόριστες[52].

Οι απαιτήσεις που προβλέπονται για τους παρόχους βασικών υπηρεσιών κρίνονται αρκετά ήπιες, ιδίως αν λάβουμε υπόψη ότι «η υποχρέωση κοινοποίησης συμβάντος εφαρμόζεται μόνο σε περίπτωση που ο πάροχος ψηφιακών υπηρεσιών έχει πρόσβαση στις πληροφορίες

[50] Άρθρο 16 της Οδηγίας

[51] Άρθρο 16 της Οδηγίας

[52] Dimitra Markopoulou, Vangelis Papakonstantinou , Paul de Hert "The new EU cybersecurity framework The NIS Directive , ENISA' S role and thw General Data Protection Regulation", Computer law & Security review, Issue 6, 2019, pp. 3-6

που απαιτούνται για να εκτιμηθεί ο αντίκτυπος συμβάντος έναντι των παραμέτρων που αναφέρονται στο πρώτο εδάφιο»[53].

Η ανομοιομορφία λοιπόν δημιουργεί ένα ακόμη πρόβλημα, καθώς ορισμένα κ-μ μπορεί να παραλείπουν να κοινοποιούν περιστατικά που δεν κρίνουν σοβαρά και σημαντικά ενώ άλλα την ίδια στιγμή να επιβάλλουν κυρώσεις λόγω παράλειψης[54].

[53] Dimitra Markopoulou, Vangelis Papakonstantinou , Paul de Hert "The new EU cybersecurity framework The NIS Directive , ENISA' S role and thw General Data Protection Regulation", Computer law & Security review, Issue 6, 2019, pp. 3-6

[54] Nicolas Van Tieghem, Nicolas Lfebvre, "While preparing the NIS 2, update of the European Overview of NIS transposition by the Member States…toward convergence?», Riskinsight

## *3.2. Πως εφαρμόστηκε στην Ελλάδα η Οδηγία NIS*

Η Οδηγία ενσωματώθηκε στην ελληνική έννομη τάξη με το Ν. 4577/2018 και περαιτέρω εξειδίκευση των θεμάτων εφαρμογής έλαβε χώρα με την Υπουργική Απόφαση 1027/2019 (3739, τ. Β΄).

Οι απαιτήσεις ασφάλειας και κοινοποίησης που προβλέπονται στο νόμο αφορούν αποκλειστικά τους φορείς εκμετάλλευσης βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών σε κρίσιμους τομείς. Οι εν λόγω απαιτήσεις δεν βρίσκουν εφαρμογή στις επιχειρήσεις που παρέχουν δημόσια δίκτυα ή δημόσιες υπηρεσίες ηλεκτρονικών επικοινωνιών και έχουν ειδικά ή αποκλειστικά δικαιώματα παροχής υπηρεσιών σε άλλες αγορές πλην των αγορών δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, στην Ελλάδα ή σε άλλο κ-μ της ΕΕ ή σε παρόχους υπηρεσιών εμπιστοσύνης που εμπίπτουν στο άρθρο 19 του Κανονισμού (ΕΕ) 910/2014 (άρ.1 παρ.2) .

Παράλληλα ισχύει και το π.δ. 39/2011 με το οποίο θεσπίζεται μία διαδικασία προσδιορισμού των ευρωπαϊκών υποδομών ζωτικής σημασίας και αξιολόγησης της ανάγκης προστασίας των υποδομών αυτών, καθώς και οι διατάξεις που αφορούν την παιδική πορνογραφία και του ν.4360/2016 περί ευρωπαϊκής εντολής προστασίας (άρ.1 παρ.3). Στην παρ.4 προβλέπονται περιορισμοί στην ανταλλαγή πληροφοριών με την Επιτροπή αναφορικά με απόρρητες πληροφορίες , όπως είναι αυτές που εμπίπτουν στο επιχειρηματικό απόρρητο. Αξίζει να σημειωθεί ότι πρόσφατα κατατέθηκε πρόταση οδηγίας σχετικά με την ανθεκτικότητα

των κρίσιμων οντοτήτων[55], η οποία δε βρίσκει εφαρμογή στους τομείς που καλύπτει η Οδηγία NIS I.

Ο νόμος βρίσκει εφαρμογή σε συστήματα δικτύου και πληροφοριών. Ως δίκτυο ηλεκτρονικών επικοινωνιών ορίζεται :

α) ένα δίκτυο ηλεκτρονικών επικοινωνιών, σύμφωνα με το άρ.100 Ενότητα Α, αριθμ.9 του ν.4727/2020 που αντικατέστησε την αντίστοιχη διάταξη του άρ.2 περ. ιζ΄ της Ενότητας Α του ν.4070/2012, τα συστήματα μετάδοσης, είτε βασίζονται σε χωρητικότητα μόνιμων υποδομών ή κεντρικής διαχείρισης είτε όχι, και , κατά περίπτωση, ο εξοπλισμός μεταγωγής ή δρομολόγησης και οι λοιποί πόροι, περιλαμβανομένων μη ενεργών στοιχείων δικτύου, που επιτρέπουν τη μεταφορά σημάτων μέσω καλωδίου, ραδιοσημάτων, οπτικού ή άλλου ηλεκτρομαγνητικού μέσου, περιλαμβανομένων των δορυφορικών δικτύων, των σταθερών (μεταγωγής δεδομένων μέσω κυκλωμάτων και πακετομεταγωγής, περιλαμβανομένου του διαδικτύου) και κινητών δικτύων των συστημάτων ηλεκτρικών καλωδίων, εφόσον χρησιμοποιούνται για τη μετάδοση σημάτων , των δικτύων που χρησιμοποιούνται για ραδιοτηλεοπτικές εκπομπές καθώς και των δικτύων καλωδιακής τηλεόρασης, ασχέτως του τύπου των μεταφερόμενων πληροφοριών,

β) κάθε συσκευή ή ομάδα διασυνδεδεμένων ή συσχετιζομένων συσκευών από τις οποίες μία ή περισσότερες εκτελούν, βάσει προγράμματος, αυτόματη επεξεργασία ψηφιακών δεδομένων και

γ) ψηφιακά δεδομένα που αποθηκεύονται, υποβάλλονται σε επεξεργασία, ανακτώνται ή μεταδίδονται από στοιχεία που καλύπτονται

[55] COM (2020) 820 final

στις περιπτώσεις α' και β' για τους σκοπούς της λειτουργίας, της χρήσης, της προστασίας και της συντήρησής τους[56].

Όσον αφορά τους ΦΕΒΥ, ο ν. 4577/2018 προβλέπει, σε εφαρμογή του άρ.5 της Οδηγίας, ότι αρμόδια για τον προσδιορισμό των φορέων εκμετάλλευσης των βασικών υπηρεσιών είναι η Εθνική Αρχή Κυβερνοασφάλειας, η οποία τους προσδιορίζει , ανά τομέα και υποτομέα και ο ορισμός αυτός γίνεται με απόφαση του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης (άρθρο 4).

Ο ν. 4557/2018 προβλέπει σε εφαρμογή του άρθρου 5 της οδηγίας ότι αρμόδια για τον προσδιορισμό των φορέων εκμετάλλευσης των βασικών υπηρεσιών είναι η εθνική αρχή κυβερνοασφάλειας, η οποία τους προσδιορίζει ανά τομέα και υποτομέα και ο ορισμός αυτός γίνεται με απόφαση του Υπουργού Ψηφιακής Πολιτικής , Τηλεπικοινωνιών και Ενημέρωσης, σύμφωνα με το άρθρο 4.

Η ως άνω αρχή, βάσει του άρθρου 5, καθορίζει σε συνεργασία με τις ανά τομέα βασικής υπηρεσίας, αρμόδιες ρυθμιστικές ή εποπτικές αρχές και λοιπούς εμπλεκόμενους εθνικούς φορείς, καθορίζει τα κριτήρια προσδιορισμού ενός συμβάντος ως σοβαρής διατάραξης.

Περαιτέρω πρέπει να σημειωθεί ότι η μεθοδολογία προσδιορισμού των ΦΕΒΥ καθώς και η μεθοδολογία αξιολόγησης και ελέγχου, σύμφωνα με τις προβλέψεις της Οδηγίας 2016/1148/ΕΕ, του Εκτελεστικού Κανονισμού (ΕΕ) 2018/151 της Επιτροπής της 30ης

[56] Ι. Ιγγλεζάκης, Δίκαιο Πληροφορικής, Εκδόσεις Σάκκουλα, 2021, σελ. 453

Ιανουαρίου 2018 και του ν. 4577/2018, αναλύεται στην Υπ. Απόφαση αριθμ. 1027/2019 (άρ.16)[57].

Με την ως άνω υπουργική απόφαση του Υπουργού Επικρατείας ρυθμίστηκαν θέματα εφαρμογής και διαδικασιών του ν. 4577/2018. Σκοπός της ΥΑ είναι η έκδοση των βασικών απαιτήσεων ασφαλείας συστημάτων δικτύου και πληροφοριών, της διαδικασίας παροχής πληροφοριών και κοινοποίησης συμβάντων ασφάλειας στις αρμόδιες αρχές, η μεθοδολογία προσδιορισμού των ΦΕΒΥ καθώς και η μεθοδολογία αξιολόγησης και ελέγχου, σύμφωνα με τις προβλέψεις της Οδηγίας.

Στο άρθρο 3 της ΥΑ θεσπίζεται ο καθορισμός ενιαίας πολιτικής ασφάλειας από την Εθνική Αρχή Κυβερνοασφάλειας, δηλαδή η τήρηση ενός ενιαίου ελάχιστου βασικού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών. Κάθε οργανισμός πρέπει να θεσπίζει, να υλοποιεί και να διατηρεί Πολιτική Ασφάλειας σχετική με την ασφάλεια συστημάτων δικτύου και πληροφοριών, η οποία οφείλει να καλύπτει τουλάχιστον όσα ορίζει η ενιαία πολιτική ασφάλειας, τα κύρια σημεία της οποίας περιγράφονται στη διάταξη αυτή.

Βασικοί στόχοι της Πολιτικής Ασφάλειας είναι:

- Η διασφάλιση της εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας των δεδομένων, συστημάτων, υπηρεσιών έναντι εκούσιων ή ακούσιων απειλών

[57] Θέματα εφαρμογής και διαδικασιών του ν. 4577/2018 (Α 199), ΦΕΚ 3739/Β/8-10-2019

- Η ικανοποίηση των νομικών και κανονιστικών απαιτήσεων σχετικά με την ασφάλεια και προστασία των δεδομένων
- Η επιχειρησιακή συνέχεια των βασικών υπηρεσιών του Οργανισμού έναντι περιστατικών κυβερνοεπιθέσεων
- Η ενημέρωση και η εκπαίδευση όλων των υπαλλήλων και λοιπών εμπλεκομένων τρίτων σχετικά με την παροχή των βασικών υπηρεσιών του Οργανισμού
- Η άμεση κοινοποίηση και διαχείριση περιστατικών ή αδυναμιών ασφαλείας.

Αρμοδιότητα για την επίβλεψη της εφαρμογής της Πολιτικής Ασφαλείας έχουν:

- Η Διοίκηση του Οργανισμού, η οποία εγκρίνει , αναθεωρεί και είναι αρμόδια για αποτελεσματική και αποδοτική εφαρμογή της Πολιτικής Ασφάλειας.
- Ο Υπεύθυνος Ασφάλειας Πληροφοριών και Δικτύων, όπως περιγράφεται στο άρθρο 6 της παρούσας, ο οποίος επιβλέπει και συντονίζει την εφαρμογή αυτής της πολιτικής μέσω χρήσης κατάλληλων προτύπων, διαδικασιών και διεθνών πρακτικών και λειτουργεί ως σημείο επαφής με τους αρμόδιους φορείς
- όλο το προσωπικό και οι συμβεβλημένοι προμηθευτές, οι οποίοι ακολουθούν τις διαδικασίες για την τήρηση της πολιτικής ασφάλειας πληροφοριών.

Παρακάτω στο άρθρο 4 περιγράφονται οι βασικές απαιτήσεις ασφαλείας. Η πρώτη κατηγορία απαιτήσεων είναι η «Αναγνώριση» που περιλαμβάνει απαιτήσεις σχετικά με το επιχειρησιακό περιβάλλον, τη διαχείριση πόρων, την αποτίμηση της διακινδύνευσης, τη στρατηγική

διακινδύνευσης, τη διαχείριση διακινδύνευσης αλυσίδας εφοδιασμού και την αυτοαξιολόγηση-βελτίωση. Η δεύτερη κατηγορία , η «Προστασία» περιλαμβάνει πολιτικές, διεργασίες και διαδικασίες προστασίας βασικών υπηρεσιών, τη διαχείριση ταυτότητας και έλεγχο πρόσβασης, τη φυσική και περιβαλλοντική ασφάλεια, την ασφάλεια συστημάτων και εφαρμογών, την ασφάλεια δεδομένων, τα αντίγραφα ασφαλείας , τις τεχνολογίες ασφάλειας, τις δοκιμές συστημάτων, τη διαχείριση αλλαγών και την ευαισθητοποίηση και κατάρτιση. Τέλος η «Αντιμετώπιση» περιλαμβάνει την ανίχνευση απειλών, την επιχειρησιακή συνέχεια και την ανάκαμψη από καταστροφές.

Το άρθρο 5 αναφέρεται στην επιλογή των μέτρων ασφαλείας, τα οποία θα πρέπει να είναι αποτελεσματικά, αποδοτικά, κατάλληλα, αναλογικά, αξιόπιστα και περιεκτικά.

Περαιτέρω, με το άρθρο 6 ορίζεται η υποχρέωση κάθε οργανισμού που εμπίπτει στην κατηγορία των ΦΕΒΥ να ορίσει συγκεκριμένο εργαζόμενό του ως υπεύθυνο ασφαλείας πληροφοριών και δικτύων του, ο οποίος πρέπει να διαθέτει ανεξαρτησία και να μην έρχεται σε σύγκρουση συμφερόντων με άλλους εργασιακούς ρόλους που τυχόν κατέχει. Κάθε οργανισμός οφείλει αμελλητί να κοινοποιεί στην Εθνική Αρχή Κυβερνοασφάλειας τα στοιχεία επικοινωνίας του Υπευθύνου που έχει οριστεί.

Αναλυτικότερα σχετικά με τον Υπεύθυνο Ασφαλείας σημειώνεται ότι αποτελεί το σημείο επαφής των φορέων με την Εθνική Αρχή Κυβερνοασφάλειας και το αρμόδιο CSIRT, με τις οποίες έχει καθήκον να συνεργάζεται. Έχει το ρόλο του συντονιστή και επιβλέπει τον Οργανισμό ως προς τις υποχρεώσεις που απορρέουν από τον ν. 4577/2018 (Α` 199),

από την υπουργική απόφαση και από άλλες διατάξεις της Ευρωπαϊκής Ένωσης ή της Εθνικής Αρχής Κυβερνοασφάλειας σχετικά με την Ασφάλεια Συστημάτων Δικτύων και Πληροφοριών. Εποπτεύει την υλοποίηση της Ενιαίας Πολιτικής Ασφάλειας και την ικανοποίηση των βασικών απαιτήσεων ασφάλειας, την εκπαίδευση και ευαισθητοποίηση των υπαλλήλων του Οργανισμού σε θέματα ασφάλειας πληροφοριών και δικτύων καθώς, και τη σύνταξη της αναφοράς αυτοαξιολόγησης του Οργανισμού που αποστέλλεται στην Εθνική Αρχή Κυβερνοσφάλειας. Είναι παρόν στους ελέγχους που πραγματοποιεί η Ομάδα Επιθεώρησης Ελέγχου, όπως αυτή ορίζεται από την Εθνική Αρχή Κυβερνοσφάλειας, και της παρέχει όλα τα κατάλληλα μέσα για να διευκολύνει το έργο της.

Επιθυμητά προσόντα του Υπεύθυνου Ασφάλειας Πληροφοριών και Δικτύων είναι να διαθέτει προπτυχιακό ή Μεταπτυχιακό τίτλο ετήσιας τουλάχιστον διάρκειας σε συναφές γνωστικό αντικείμενο, εμπειρία στον τομέα της ασφάλειας πληροφοριών και δικτύων τουλάχιστον 5 ετών. Να διαθέτει πιστοποιημένη γνώση μεθοδολογιών, διαδικασιών, τεχνικών, εργαλείων και προτύπων ασφάλειας πληροφοριών και ψηφιακών συστημάτων και να γνωρίζει τις επιχειρηματικές διαδικασίες του Οργανισμού.

### *3.2.1. Εθνική Αρχή Κυβερνοασφάλειας*

Για την Ελλάδα, ως Εθνική Αρχή Κυβερνοασφάλειας έχει οριστεί η Γενική Διεύθυνση Κυβερνοασφάλειας[58] του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης ως αρμόδια εποπτική αρχή. Έχει ως αρμοδιότητα να χαράσσει την πολιτική Κυβερνοασφάλειας για τις κρίσιμες υποδομές του δημόσιου και ιδιωτικού τομέα, να ορίσει τους κανόνες και τις απαιτήσεις ασφαλείας για τις οντότητες που υπάγονται στο πεδίο εφαρμογής της Οδηγίας NIS και να διασφαλίζει την τήρηση του επιπέδου αυτού, παρακολουθώντας την εφαρμογή του Ν.4577/2018. Να συνεργάζεται με συναρμόδιους φορείς σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο και να προάγει την επιστημονική έρευνα και την εκπαίδευση – επιμόρφωση στα θέματα κυβερνοασφάλειας.

Στο πλαίσιο της συνεργασίας με άλλους φορείς έχει το ρόλο του συντονισμού μεταξύ των φορέων που δραστηριοποιούνται στον τομέα της ασφάλειας στον Κυβερνοχώρο, τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα. Ενδεικτικά αναφέρουμε τη Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ, του άρθρου 8 παρ. 1, με σκοπό την αμοιβαία και από κοινού τήρηση των υποχρεώσεων της χώρας στο πλαίσιο του νόμου. Να διαβουλεύεται και να συνεργάζεται με τις Αρμόδιες Εθνικές Αρχές επιβολής του νόμου την Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), το Κέντρο Μελετών Ασφαλείας και την Αρχή Προστασίας

[58] Βάσει του άρθρου 6 του Ν. 4577/2018 (Α΄199), ο οποίος ενσωματώνει στην ελληνική έννομη τάξη το πλαίσιο των διατάξεων της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου, σχετικά με μέτρα για το υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, την NIS.

Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), καθώς και με τις λοιπές αρμόδιες ρυθμιστικές ή εποπτικές αρχές και τους λοιπούς εμπλεκόμενους φορείς αναφορικά με τα θέματα που άπτονται της εφαρμογής του νόμου.

Ακόμη πολύ σημαντική είναι η συνεργασία με τις Αρμόδιες Αρχές των λοιπών κρατών- μελών , στο πλαίσιο των μηχανισμών συνεργασίας, όπως αυτοί προσδιορίζονται από τα άρθρα 11 και 12 της Οδηγίας.

Οφείλει να συμμετέχει στην ομάδα συνεργασίας του άρθρου 11 της Οδηγίας, ορίζει τους εθνικούς αντιπροσώπους της χώρας σ' αυτήν και ενημερώνει τους λοιπούς εμπλεκόμενους εθνικούς φορείς αναφορικά με τις εργασίες και τις αποφάσεις που λαμβάνονται στο πλαίσιο αυτής.

Συνεργάζεται με σχετικούς για θέματα κυβερνοασφάλειας και προστασίας κρίσιμων υποδομών διεθνείς οργανισμούς και όργανα ή υπηρεσίες της ΕΕ ή άλλων κρατών και συμμετέχει στις αντίστοιχες συναντήσεις συναφών με τα ανωτέρω επιτροπών και ομάδων εργασίας.

Πολύ σημαντικός είναι ο ρόλος της ως εποπτεύουσα αρχή, η οποία οφείλει να αξιολογεί τα μέτρα που λαμβάνουν οι ΦΕΒΥ και ΠΨΥ για τη διαχείριση των διαδικτυακών κινδύνων ασφάλειας και τη αποτροπή ή έστω ελαχιστοποίηση του αντικτύπου που θα έχει ένα τέτοιο περιστατικό στην επαγγελματική τους συνέχεια.

Για να μπορέσει να ανταποκριθεί στις ως άνω αρμοδιότητες της έχουν ανατεθεί οι ακόλουθες εξουσίες:

- να της παρέχεται επαρκής πληροφόρηση σχετικά με το επίπεδο ασφαλείας που τηρεί ο κάθε φορέας και την αυτή καθεαυτή εφαρμογή των πολιτικών της.
- Διενέργεια ελέγχων, τακτικών και έκτακτων, συμμόρφωσης. Στο πλαίσιο αυτών των ελέγχων μπορεί να ζητήσει πρόσβαση σε υλικό, εγκαταστάσεις, δεδομένα, να διενεργήσει επιτόπιους ελέγχους, να λάβει ένορκες βεβαιώσεις.
- Σε περίπτωση διαπίστωσης ανεπάρκειας στο επίπεδο ασφαλείας, δύναται να εκδίδει οδηγίες, δεσμευτικές ως προς τον φορέα, για την αποκατάσταση των ελλείψεων.

Στην Ελληνική έννομη τάξη, η Εθνική Αρχή Κυβερνοασφάλειας, στο πλαίσιο της Δράσης 1.Α.2: «Ανάπτυξη πλαισίου προαγωγής της αριστείας στον τομέα της κυβερνοασφάλειας (cybersecurity excellence management framework)», έχει προχωρήσει στη σύνταξη Εγχειριδίου Κυβερνοασφάλειας[59] (handbook), το οποίο αποτελεί έναν χρήσιμο οδηγό σε τεχνικά και οργανωτικά μέτρα για την προστασία και ανθεκτικότητα των πληροφοριακών συστημάτων του Δημόσιου Τομέα της χώρας, αλλά και του Ιδιωτικού και συγκεκριμένα των μικρών και μεσαίων επιχειρήσεων. Αποτελείται από δεκαοκτώ ενότητες, όπου η καθεμία θεματική αναπτύσσει ξεχωριστή δέσμη μέτρων προστασίας, τους κινδύνους από τη μη τήρηση των μέτρων αλλά και εξειδικευμένα

[59] Εγχειρίδιο Κυβερνοασφάλειας- Cybersecurity Handbook, ΕΘνική Αρχή Κυβερνοασφάλειας, https://mindigital.gr/wp-content/uploads/2021/06/%CE%95%CE%B3%CF%87%CE%B5%CE%B9%CF%81%CE%AF%CE%B4%CE%B9%CE%BF-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf

μέτρα προστασίας (sub- controls) για συγκεκριμένους τύπους συστημάτων και συγκεκριμένες λειτουργίες.

Με αυτό τον τρόπο η εθνική αρχή επεδίωξε να βελτιώσει την ικανότητα των εθνικών οντοτήτων να ανθίστανται στις απειλές, να προστατεύουν τα κρίσιμα συστήματα , τις υπηρεσίες που αυτά παρέχουν, τα προσωπικά δεδομένα που εμπεριέχουν, τηρούν και τυχόν επεξεργάζονται, με τις λιγότερες δυνατές απώλειες. Στόχος συνεχές είναι να δημιουργηθεί ένα ασφαλές περιβάλλον Διαδικτύου που θα τονώσει την εμπιστοσύνη των πολιτών και θα τους οδηγήσει στη χρήση των νέων ψηφιακών προϊόντων και υπηρεσιών. Όλα αυτά οδηγούν σαφώς στην τόνωση και ανάπτυξη της εθνικής οικονομίας.

Πρόσφατα δημοσιεύθηκε η Εθνική Στρατηγική Κυβερνοασφάλειας για την περίοδο 2020-2025, με την οποία επικαιροποιήθηκε ο στρατηγικός σχεδιασμός για την κυβερνοασφάλεια της χώρας, προκειμένου να αντιμετωπιστούν οι νέες προκλήσεις από τις σημαντικές τεχνολογικές εξελίξεις , όπως είναι τα δίκτυα 5G, η τεχνητή νοημοσύνη και το διαδίκτυο των πραγμάτων , σε συνδυασμό με την αυξανόμενη χρήση των ΤΠΕ εν μέσω της πανδημίας του covid-19[60].

[60] ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020 -2025- Εθνική Στρατηγική Κυβερνοασφάλειας, https://mindigital.gr/wp-content/uploads/2020/12/%CE%95%CE%B8%CE%BD%CE%B9%CE%BA%CE%B7%CC%81-%CE%A3%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%B7%CC%81-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CC%81%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf

Η Εθνική Στρατηγική Κυβερνοασφάλειας περιλαμβάνει τα ακόλουθα σημεία:

- Περιλαμβάνει του στόχους και τις προτεραιότητες της εθνική στρατηγικής για την ασφάλεια συστημάτων δικτύου και πληροφοριών
- Διαμοιρασμό ρόλων και καθηκόντων κάθε φορέα στο πλαίσιο της επίτευξης των στόχων και των προτεραιοτήτων της εθνικής στρατηγικής για την ασφάλεια συστημάτων δικτύου και πληροφοριών
- Μέτρα ετοιμότητας , ανταπόκρισης και αποκατάστασης
- Τρόπους συνεργασίας ιδιωτικού και δημόσιου τομέα
- Κατάρτιση καταλόγου φορέων που εμπλέκονται στην υλοποίηση της εθνικής στρατηγικής ασφάλειας των συστημάτων δικτύου και πληροφοριών
- Αναφορά των σχεδίων έρευνας και ανάπτυξης σχετικά με την στρατηγική ασφαλείας συστημάτων δικτύου και πληροφοριών
- Προσδιορισμός των κινδύνων και σχέδιο εκτίμησης αυτών
- Προγράμματα εκπαίδευσης, κατάρτισης και ευαισθητοποίησης σε σχέση με την εθνική στρατηγική κυβερνοασφάλειας

Στις 16.12.2020 δημοσιεύθηκε και η νέα στρατηγική Κυβερνοασφάλειας της ΕΕ και οι νέοι κανόνες για την ενίσχυση της ανθεκτικότητας των φυσικών και ψηφιακών κρίσιμων οντοτήτων[61]. Στόχος της νέας στρατηγικής είναι να ενισχύσει την συλλογική ανθεκτικότητα της Ευρώπης έναντι των κυβερνοαπειλών και να

[61] New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

διασφαλίσει ότι όλοι οι πολίτες και οι επιχειρήσεις θα μπορούν να επωφεληθούν πλήρως από αξιόπιστες υπηρεσίες και αξιόπιστα ψηφιακά εργαλεία, όπως και να προστατεύονται από τις κυβερνοαπειλές.

### *3.2.2. Διεύθυνση Κυβερνοάμυνας*

Μεταξύ των φορέων που συνίσταται να συνεργάζεται η Γενική Διεύθυνση Κυβερνοασφάλειας είναι και η συνεργασία με την αρμόδια CSIRT (Computer Security Incident Response Team), με σκοπό την από κοινού τήρηση των υποχρεώσεων της χώρας. Η CSIRT καλύπτει τους τομείς του Παραρτήματος Ι και τις υπηρεσίες του Παραρτήματος ΙΙ και είναι η Αρμόδια Ομάδα Απόκρισης για την παρακολούθηση συμβάντων που αφορούν την ασφάλεια των υπολογιστών και έχει στην ευθύνη της[62]:

Α) Την παρακολούθηση των συμβάντων σε εθνικό επίπεδο

Β) Την παροχή προειδοποιήσεων και ανακοινώσεων

Γ) Την παρέμβαση, διαχείριση και αντιμετώπιση κινδύνων και συμβάντων με βάση συγκεκριμένη διαδικασία

Δ) την ανάλυση των κινδύνων και την επίγνωση της κατάστασης

Ε) τη συμμετοχή της στο δίκτυο CSIRT

[62] Άρθρο 12 της Οδηγίας

ΣΤ) την προώθηση της χρήσης τυποποιημένων πρακτικών για τη διαχείριση ενός περιστατικού και

Ζ) τη συνεργασία με τις αρχές των άλλων κρατών μελών στο πλαίσιο του δικτύου SCIRT αλλά και με ιδιωτικούς φορείς

Στην Ελλάδα το ρόλο αυτό διαδραματίζει η Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ[63]. Διαθέτει τεχνική επάρκεια και εμπειρογνωμοσύνη για να στηρίξει τους φορείς στο χειρισμό τυχόν συμβάντων. Οι φορείς έχουν υποχρέωση να κοινοποιούν και στη CSIRT τα κρίσιμα περιστατικά ασφαλείας. Ωστόσο ο ρόλος της είναι καθαρά γνωμοδοτικός και όχι εποπτικός, όπως της Γενικής Διεύθυνσης Κυβερνοασφάλειας.

Η Διεύθυνση Κυβερνοάμυνας καλύπτει τομείς όπως η ενέργεια, οι μεταφορές, χρηματοπιστωτικές αγορές, οι τράπεζες, η υγεία, η προμήθεια πόσιμου νερού, ψηφιακές υποδομές και υπηρεσίες , όπως οι Online αγορές, οι Online μηχανές αναζήτησης και οι υπηρεσίες νεφοϋπολογιστικής (cloud).

### *3.2.3. Κυρώσεις*

Στο άρθρο 15 της Οδηγίας προβλέπονται κυρώσεις σε περίπτωση μη εφαρμογής του νόμου. Ο Υπουργός Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης μπορεί , ύστερα από εισήγηση της

[63] Άρθρο 8 του Ν. 4577/2018

Εθνικής Αρχής Κυβερνοασφάλειας να επιβάλλει κυρώσεις σε φυσικό ή νομικό πρόσωπο σε περίπτωση παραβίασης των διατάξεων του ν. 4577/2018, δηλαδή σε περίπτωση που οι υπόχρεοι δεν κοινοποιούν ή κοινοποιούν με καθυστέρηση συμβάντα με σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών του, όπως επίσης και στην περίπτωση που δεν λαμβάνονται κατάλληλα και αναλογικά, τεχνικά και οργανωτικά, προληπτικά μέτρα για τη διαχείριση των κινδύνων όσων αφορά την ασφάλεια των δικτύων και των συστημάτων πληροφοριών που χρησιμοποιεί ο υπόχρεος φορέας και τέλος , όταν ένα φυσικό ή νομικό πρόσωπο δεν παρέχει ή παρέχει με αδικαιολόγητη καθυστέρηση οποιαδήποτε σχετική πληροφορία που ζητείται κατά τη διενέργεια ελέγχου ή τη διερεύνηση περιστατικού.

Στην Ελλάδα, σε περίπτωση μη συμμόρφωσης με την Οδηγία NIS , η Εθνική Αρχή Κυβερνοασφάλειας δύναται να κάνει συστάσεις, επίπληξη αλλά και να επιβάλλει πρόστιμα, πάντα με γραπτή και αιτιολογημένη απόφαση. Το είδος και το μέγεθος αυτών των κυρώσεων εξαρτάται από το μέγεθος της παράβασης και την τυχόν υποτροπή- επανάληψη των παραβιάσεων. Στην περίπτωση αυτή βέβαια , η οικονομική κύρωση, πέρα από την πιθανή οικονομική ζημία, έχει διόλου ευκαταφρόνητες συνέπειες στη φήμη και την αξιοπιστία του φορέα που δε συμμορφώνεται. Το ευρύ κοινό ενημερώνεται σχετικά από την ιστοσελίδα της Εθνικής Αρχής Κυβερνοασφάλειας.

Σε περίπτωση υποτροπής το πρόστιμο μπορεί να αγγίξει το ποσό των 200.000 ευρώ εάν, κατ’ εξακολούθηση ένας φορέας:

- Παραλείπει να κοινοποιήσει ή κοινοποιεί με μεγάλη καθυστέρηση περιστατικά τα οποία έχουν αντίκτυπο στην ομαλή λειτουργία του.

- Δεν λαμβάνει κατάλληλα μέτρα, τεχνικά, οργανωτικά και προληπτικά για τη διαχείριση των κινδύνων
- Στον έλεγχο που διενεργείται από την εποπτεύουσα αρχή, καθυστερεί ή αρνείται την παροχή πληροφοριών που της ζητούνται.

Όσον αφορά στους φορείς πρέπει να επισημανθεί ο αποδοτικός χαρακτήρας που πρέπει να έχουν τα μέτρα που θα λάβουν, δηλαδή το κόστος των προληπτικών μέτρων που θα λάβουν πρέπει να είναι μικρότερο από το κόστος που θα προκαλούσε πιθανή διάρρηξη των συστημάτων τους[64]. Τα μέτρα που θα λάβουν ακόμη κι αν είναι δαπανηρά, αυτό η ζημία αντισταθμίζεται από το επαρκές κίνητρο της αποφυγής πλήξης της εμπορικής τους φήμης σε περιστατικό κυβερνοεπίθεσης. Έτσι θα διαφυλάξουν τα ιδιωτικά τους συμφέροντα και θα διασφαλίσουν αποτελεσματικά της απαιτήσεις κυβερνοασφάλειας. Χωρίς βέβαια να είναι δεδομένο ότι το υψηλό κόστος ενός συστήματος ασφαλείας είναι δίχως άλλο και αποτελεσματικό[65].

[64] Johan David Michels, Ian Walden, "Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?" European Law Review, 2020, Vol. 45, Issue 1, p.28-29.

[65] Johan David Michels, Ian Walden, "Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?" European Law Review, 2020, Vol. 45, Issue 1, p.28-29.

## *3.3. Απολογισμός της εφαρμογής της*

Κοιτώντας με κριτική ματιά τις κατευθύνσεις της Οδηγίας διαπιστώνουμε ότι πάρα πολλοί όροι είναι γενικοί και αδιευκρίνιστοι. Ο όρος ουσιώδης υπηρεσία (για τους ΦΕΒΥ) είναι γενικός και δεν επεξηγείται επαρκώς. Αυτό δίνει τη δυνατότητα στα κ-μ να αποφασίσουν τα ίδια τι κρίνουν ως ουσιώδες και τι όχι στην επικράτειά τους[66]. Στην κοινή λογική, ουσιώδης παροχή θεωρείται αυτή που σε περίπτωση διατάραξης μπορεί να προκαλέσει σοβαρές επιπτώσεις σε κοινωνικό και οικονομικό επίπεδο και στις αντίστοιχες δραστηριότητες. Επαφίεται στα κ-μ να αξιολογήσουν την κρισιμότητα και το ρόλο του κάθε ΦΕΒΥ για την κοινωνία τους. Διαδικασία εγγενώς υποκειμενική[67]. Στο πλαίσιο όμως της ευρωπαϊκής ενοποίησης και της άσκησης νομοθετικής εξουσίας από την ΕΕ, κρίνεται προτιμότερο οι οδηγίες να είναι σαφείς και να εμπεριέχουν περισσότερα αντικειμενικά κριτήρια. Αφήνουν μεν τα κ-μ να είναι ελεύθερα ως προς τον τρόπο ενσωμάτωσής τους στο εσωτερικό δίκαιο, αλλά ως προς το περιεχόμενο είναι προτιμότερο να υπάρχουν αυστηρά όρια και ξεκάθαρη νομοθέτηση.

Μία ακόμη κριτική ματιά στις απαιτήσεις ασφαλείας και κοινοποίησης μας οδηγεί στο συμπέρασμα ότι για τους παρόχους

[66] Maria There Holzieitner, Johannes Reichl, "Legal Problems for the protection of smart Grids from cyber threats", European Energy Journal, Vol 6, Issue 3, 2016, pp. 53-55.

[67] Maria There Holzieitner, Johannes Reichl, "Legal Problems for the protection of smart Grids from cyber threats", European Energy Journal, Vol 6, Issue 3, 2016, pp.54/55

ψηφιακών υπηρεσιών παρέχεται μεγαλύτερη ευελιξία για να ενεργούν ελεύθερα, πράγμα που αποτυπώνεται και στις ακόλουθες αιτιολογικές σκέψεις της Οδηγίας.

Σύμφωνα με την αιτιολογική σκέψη 49 «οι απαιτήσεις ασφάλειας για τους παρόχους ψηφιακών υπηρεσιών θα πρέπει να είναι λιγότερο αυστηρές»[68]. Ομοίως «η παρούσα οδηγία θα πρέπει να ακολουθήσει διαφοροποιημένη προσέγγιση όσον αφορά το επίπεδο εναρμόνισης για τις δύο αυτές ομάδες οντοτήτων. Όσον αφορά τους φορείς εκμετάλλευσης βασικών υπηρεσιών, τα κράτη μέλη θα πρέπει να έχουν τη δυνατότητα να προσδιορίζουν τους σχετικούς φορείς και να επιβάλλουν αυστηρότερες απαιτήσεις από αυτές που προβλέπονται στην παρούσα οδηγία»[69]. Και ακόμη ότι «οι πάροχοι ψηφιακών υπηρεσιών θα πρέπει να υπόκεινται σε ήπιες και αντενεργές εκ των υστέρων εποπτικές δραστηριότητες, δικαιολογούμενες από τη φύση των υπηρεσιών και των δραστηριοτήτων τους»[70]. Ως εκ τούτου συνάγεται ότι η διαφορετική προσέγγιση του νομοθέτη οφείλεται στη διαφορετική φύση των υπηρεσιών και δραστηριοτήτων που παρέχουν.

Για να έχουν αντίκρισμα όλες αυτές οι προβλέψεις, σαφώς πρέπει να προβλέπονται και αντίστοιχες κυρώσεις σε περίπτωση μη συμμόρφωσης. Το άρθρο 21 της Οδηγίας προβλέπει ότι «οι προβλεπόμενες κυρώσεις είναι αποτελεσματικές, αναλογικές και αποτρεπτικές»[71].

[68] Αιτιολογική σκέψη 49 της Οδηγίας

[69] Αιτιολογική σκέψη 57 της Οδηγίας

[70] Αιτιολογική σκέψη 60 της Οδηγίας

[71] Άρθρο 21 της Οδηγίας

Άλλος ένας τομέας πρόσφορος για ποικιλομορφία ως προς την ενσωμάτωση της Οδηγίας από τα κ-μ είναι αυτός των κυρώσεων. Υπάρχουν κράτη, όπως το Βέλγιο και η Κύπρος που φτάνουν μέχρι την ποινή της φυλάκισης για αδικήματα που απορρέουν από μη συμμόρφωση στις υποχρεώσεις της NIS. Αλλά και στα κράτη που προβλέπεται μόνο χρηματική ποινή, υπάρχει μεγάλη διακύμανση. Τέλος υπάρχουν και κράτη, όπως η Φινλανδία που δεν έχουν προβλέψει κυρώσεις[72].

Αποτιμώντας την Οδηγία NIS, υπογραμμίζουμε ότι η μη συμμόρφωση με αυτή, αποτελεί ξεκάθαρα απειλή. Τα οφέλη από το επαρκές επίπεδο προστασίας συνοψίζεται στα παρακάτω:

- Προστασία και ετοιμότητα απέναντι σε κυβερνοαπειλές που μέσα σε ελάχιστο χρόνο μπορούν να επηρεάσουν δυσμενώς και πιθανώς ανεπιστρεπτί την παροχή βασικών τους υπηρεσιών.

- Αποφυγή κυρώσεων και προστίμων, όχι μόνο σε επίπεδο ασφάλειας αλλά και όλων των παρελκομένων, πχ GDPR

- Δημιουργία μιας αξιόπιστης εικόνας για την εταιρία που κερδίζει την εμπιστοσύνη

- και ελαχιστοποίηση των συμβάντων που δύνανται να προκαλέσουν βλάβη

[72] Nicolas Van Tieghem, Nicolas Lfebvre, "While preparing the NIS 2, update of the European Overview of NIS transposition by the Member States…toward convergence? »

Μία νέα ή αναθεωρημένη Οδηγία θα μπορούσε να προβλέψει ένα σύστημα ευθύνης για τους φορείς που λόγω αμέλειας δεν φρόντισαν να λάβουν τα κατάλληλα μέτρα για να διασφαλίσουν το δημόσιο συμφέρον. Αυτό θα είχε ως αποτέλεσμα, οι φορείς πέραν της τυπικής υιοθέτησης μέτρων ασφαλείας, να συνυπολογίζουν την καταλληλότητα αυτών ως προς τις συνέπειές τους εν γένει στο κοινωνικό σύνολο[73].

[73] Johan David Michels, Ian Walden, "Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?" , European Law Review, 2020, Vol. 45, Issue 1, p.28-29.

# 4

# *Τι οδήγησε στην ανάγκη αναθεώρησής της*

Η αυξανόμενη ψηφιοποίηση των καθημερινών υπηρεσιών και διασύνδεση πολιτών και υπηρεσιών μέσω ψηφιακών πλατφορμών έχει εξελιχθεί παράλληλα με τους κινδύνους της κυβερνοασφάλειας. Για το λόγο αυτό τα υφιστάμενα μέτρα πρέπει να επικαιροποιηθούν. Είναι ανάγκη να καλυφθούν περισσότεροι τομείς, μικροί και μεσαίοι, ανάλογα με την κρισιμότητά τους για την κοινωνία και την οικονομία.

Στόχος της αναθεωρημένης Οδηγίας είναι να ενισχυθούν οι απαιτήσεις ασφαλείας που επιβάλλονται στις εταιρίες, να αντιμετωπιστούν τα ζητήματα ασφάλειας στις εφοδιαστικές αλυσίδες και στους προμηθευτές, να εξορθολογιστούν οι διάφορες υποχρεώσεις, π.χ. υποβολή εκθέσεων, να εποπτεύει αυστηρότερα τις εθνικές αρχές, να αυστηροποιήσει τις απαιτήσεις και να εναρμονίσει το καθεστώς κυρώσεων.

Η επόμενη γενιά δικτύων 5G αλλά και οι μελλοντικές γενιές ενθαρρύνει τη νέα στρατηγική της ΕΕ και ωθεί τα κ-μ να αξιοποιούν και να εφαρμόζουν την υπάρχουσα ήδη εργαλειοθήκη της ΕΕ για το 5G. Σύμφωνα με έκθεση[74] που δημοσιεύθηκε πρόσφατα, τα περισσότερα κ-

[74] https://www.consilium.europa.eu/el/

μ εφαρμόζουν τα συνιστώμενα από την Επιτροπή για την κυβερνοασφάλεια των δικτύων 5G μέτρα.

Η κ. Μαργκρέιτε Βεστεϊγιερ, Αντιπρόεδρος της εκτελεστικής επιτροπής για την Ευρώπη Έτοιμη για την Ψηφιακή Εποχή, δήλωσε: « Η Ευρώπη έχει δεσμευτεί για τον ψηφιακό μετασχηματισμό της κοινωνίας και της οικονομίας μας. Επομένως θα πρέπει να τον στηρίξουμε με πρωτοφανή επίπεδα επενδύσεων. Αν και ο ψηφιακός μετασχηματισμός επιταχύνεται ,μπορεί να επιτύχει μόνο εάν οι πολίτες και ι επιχειρήσεις έχουν τη βεβαιότητα ότι τα συνδεδεμένα προϊόντα και υπηρεσίες στα οποία βασίζονται είναι ασφαλή»[75].

Ο Ύπατος εκπρόσωπος κ. Ζοζέφ Μπορέλ δήλωσε: «Η διεθνής ασφάλεια και σταθερότητα εξαρτώνται περισσότερο από ποτέ από έναν παγκόσμιο , ανοικτό , σταθερό και ασφαλή κυβερνοχώρο όπου θα γίνονται σεβαστά το κράτος δικαίου, τα ανθρώπινα δικαιώματα, οι ελευθερίες και η δημοκρατία. Με τη σημερινή στρατηγική, η ΕΕ εντείνει τις προσπάθειές της για να προστατεύσει τις κυβερνήσεις , τους πολίτες και τις επιχειρήσεις της από παγκόσμιες κυβερνοαπειλές και να αναλάβει ηγετικό ρόλο στον κυβερνοχώρο , διασφαλίζοντας ότι μπορούν όλοι να αποκομίσουν οφέλη του διαδικτύου και της χρήσης των τεχνολογιών»[76].

Ο Τιερί Μπρετόν, Επίτροπος Εσωτερικής Αγοράς δήλωσε: « Οι κυβερνοαπειλές εξελίσσονται γρήγορα, είναι όλο πιο σύνθετες και προσαρμόσιμες. Για να διασφαλίσουμε την προστασία των πολιτών και των υποδομών μας, πρέπει να προετοιμαστούμε για τις μελλοντικές

[75] https://www.consilium.europa.eu/el/

[76] https://www.consilium.europa.eu/el/

εξελίξεις: μία ανθεκτική και αυτόνομη ευρωπαϊκή κυβερνο-ασπίδα θα μας επιτρέψει να αξιοποιήσουμε την εμπειρογνωσία και τις γνώσεις μας για να εντοπίσουμε και να αντιδράσουμε ταχύτερα, να περιορίσουμε τις ενδεχόμενες βλάβες και να αυξήσουμε την ανθεκτικότητά μας. Επενδύοντας στην Κυβερνοασφάλεια επενδύουμε σε υγιή μελλοντικά διαδικτυακά περιβάλλοντα και στη στρατηγική μας αυτονομία»[77].

Η κ. Ίλβα Γιούανσον , Επίτροπος Εσωτερικών Υποθέσεων, δήλωσε ότι[78]: « Τα νοσοκομεία, τα αποχετευτικά συστήματα ή οι υποδομές μεταφορών είναι τόσο ισχυρά όσο οι πιο αδύναμοι κρίκοι τους. Οι διαταραχές σε ένα μέρος της Ένωσης απειλούν την παροχή βασικών υπηρεσιών σε άλλα μέρη της . Για να διασφαλιστεί η ομαλή λειτουργία της εσωτερικής αγοράς και τα μέσα βιοπορισμού όσων ζουν στην Ευρώπη, οι βασικές υποδομές μας πρέπει να είναι ανθεκτικές απέναντι σε κινδύνους όπως οι φυσικές καταστροφές , οι τρομοκρατικές επιθέσεις, τα ατυχήματα, οι πανδημίες σαν αυτή που βιώνουμε σήμερα».

Η ανησυχία και η έρευνα πάνω σ’ αυτό το θέμα είναι συνεχής. Η ομάδα εργασίας που έχει συσταθεί δυνάμει της Οδηγίας έχει αναγνωρίσει ακόμη και την κυβερνοασφάλεια των εκλογών ως κοινή πρόκληση. Ζήτημα θεμελιώδες για τη δημοκρατία μας. Ο ομάδα αυτή έχει χαρτογραφήσει  τις υφιστάμενες εθνικές πρωτοβουλίες για την κυβερνοασφάλεια των συστημάτων δικτύων και πληροφοριών που χρησιμοποιούνται για τη διεξαγωγή εκλογών. Έχει προσδιορίσει τους κινδύνους και τις ανεπάρκειες του συστήματος που θα μπορούσαν να

[77] https://www.consilium.europa.eu/el/

[78] https://www.consilium.europa.eu/el/

επηρεάσουν τις επόμενες εκλογές για το Ευρωπαϊκό Κοινοβούλιο και έχει καταρτίσει επιτομή για την κυβερνοασφάλεια των τεχνολογιών που χρησιμοποιούνται στις εκλογές, που περιλαμβάνει τεχνικά και οργανωτικά μέτρα , βάσει εμπειριών και βέλτιστων πρακτικών.

Είναι κοινή πεποίθηση συνεπώς ότι το υπάρχον και ισχύον νομικό πλαίσιο δεν είναι επαρκές, δεν καλύπτει τις ανάγκες της σύγχρονης ζωής. Η Ελλάδα συμπληρωματικά προς το υπό εξέταση νομικό πλαίσιο, κύρωσε τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Πρόσθετου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση ρατσιστικών και ξενοφοβικών πράξεων που διαπράττονται μέσω ηλεκτρονικών υπολογιστών- δικτύων. Προχώρησε ακόμη και στην ενσωμάτωση της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης πλαισίου 2005/222/ΔΕΥ του Συμβουλίου.

# 5

# *Τι αλλάζει με την νέα Οδηγία NIS 2*

Το Φεβρουάριο του 2019, η Επιτροπή ανακοίνωσε[79] την αναθεώρησης της Οδηγίας προκειμένου να καταστεί η ΕΕ έτοιμη για την ψηφιακή εποχή. Επόμενος στόχος της Ευρωπαϊκής Ένωσης είναι η δημιουργία ενός επόμενο και αναβαθμισμένου επιπέδου κυβερνοασφάλειας.

Είναι αδιαμφισβήτητος ο ηγετικός ρόλος της Ένωσης σε πρωτοβουλίες που στοχεύουν στην ενίσχυση και προαγωγή ανθρώπινων δικαιωμάτων, ελευθεριών και δημοκρατικών αξιών. Στο πλαίσιο αυτό εντάσσεται και η πρωτοβουλία για την ενίσχυση των διεθνών κανόνων και προτύπων ενός ασφαλούς παγκόσμιου κυβερνοχώρου.

Η νέα στρατηγική στοχεύει στην ενίσχυση της ανθεκτικότητας της Ευρώπης συλλογικά απέναντι στις κυβερνοαπειλές και στη διασφάλιση ότι τόσο οι πολίτες όσο και οι διάφορες επιχειρήσεις θα μπορέσουν να επωφεληθούν από αξιόπιστα ψηφιακά εργαλεία και αξιόπιστες

79 https://ec.europa.eu/info/sites/info/files/file_import/2019-european-semester-country-report-greece_el.pdf

διαδικτυακές υπηρεσίες. Το νέο ψηφιακό μέλλον της Ευρώπης, έτσι όπως παρουσιάστηκε από την Επιτροπή και τον ύπατο εκπρόσωπο της Ένωσης για θέματα εξωτερική πολιτικής και πολιτικής ασφαλείας, υπάρχει βούληση να διαμορφωθεί έτσι ώστε όλοι οι εξυπηρετούμενοι πολίτες να έχουν τη βεβαιότητα ότι προστατεύονται από κυβερνοαπειλές.

Με την πρόταση της Επιτροπής[80], την 16 Δεκεμβρίου 2020 «σχετικά με τα μέτρα για ένα υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και την κατάργηση της Οδηγίας (ΕΕ) 2016/1148» αναμένονται δραστικές και θεμελιώδεις αλλαγές , οι οποίες μεταξύ άλλων θα επηρεάσουν τον τρόπο που ασκείται η δημόσια πολιτική της Κυβερνοασφάλειας στα κ-μ.

Στην αιτιολογική έκθεση της Οδηγίας αναφέρεται η ανάγκη μιας νέας ρύθμισης που θα προβλέπει έναν αποτελεσματικό και καθολικό μηχανισμό συνεργασίας στον Κυβερνοχώρο. Η εν λόγω πρόταση εξηγεί τους λόγους που οδήγησαν σε αναθεώρηση και τους οποίους και η παρούσα εργασία ανέλυσε παραπάνω και αναγνωρίζει αδιαμφισβήτητα την NIS I ως ένα σημαντικό επίτευγμα για την εσωτερική αγορά της Ένωσης, καθώς συνέβαλε στην θέσπιση εθνικών στρατηγικών κυβερνοασφάλειας στα κ-μ, στην ενίσχυση της συνεργασίας τους και στην θωράκιση επτά φορέων εκμετάλλευσης βασικών υπηρεσιών και τριών παρόχων ψηφιακών υπηρεσιών.

[80] Πρόταση Οδηγίας NIS 2.0 https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:52020PC0823

## *5.1. Διεύρυνση πεδίου εφαρμογής*

Με τη νέα Οδηγία σκοπείται αρχικά να διευρυνθεί το πεδίο εφαρμογής της Οδηγίας[81]. Μεγάλη της αδυναμία αποδείχθηκε , ενόψει της αυξημένης ψηφιοποίησης, το περιορισμένο πεδίο εφαρμογής της[82]. Στην πρόταση υπογραμμίζεται ότι δεν εντάσσονται στο πεδίο εφαρμογής της όλοι οι ψηφιοποιημένοι τομείς της εσωτερικής αγοράς. Αυτό έχει ως αποτέλεσμα να εκτίθενται σε κινδύνους σημαντικοί τομείς, που παραμένουν αρρύθμιστοι κι έτσι διακυβεύουν την εύρυθμη λειτουργία και συνέχεια της εσωτερικής αγοράς[83].

Η έκθεση προτείνει[84] να καταργηθεί η διάκριση σε Φορείς εκμετάλλευσης Βασικών Υπηρεσιών και Παρόχους Ψηφιακών Υπηρεσιών, λόγω της ασάφειας των εννοιών αυτών[85].

Ο προτεινόμενος διαχωρισμός των οντοτήτων είναι σε βασικούς και σημαντικούς.

[81] Αιτιολογική έκθεση Πρότασης

[82] Grazyna Szpor, "The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland", Review of European and Comparative Law, Vol 46, Issue 3, 2021, pp. 226-235.

[83] Αιτιολογική Έκθεση

[84] Αιτιολογική Έκθεση

[85] Ildiko Angeli, Eszter Sieber- Fazakas, "Automotive Sector Within the Scope of Planned NIS II Cybersecurity Rules", Budapest Business Journal, 2021, Vol. 29, Issue 10, p,13.

Οι βασικές οντότητες αναλύονται στο Παράρτημα Ι[86] της Πρότασης και περιλαμβάνουν δημόσιους ή ιδιωτικούς φορείς που δραστηριοποιούνται στον τομέα της ενέργειας, των μεταφορών, των τραπεζών, στις υποδομές χρηματοπιστωτικών αγορών, την υγεία, το πόσιμο νερό, τα λύματα, τις ψηφιακές υποδομές , τη δημόσια διοίκηση αλλά και το διάστημα.

Οι οντότητες που χαρακτηρίζονται ως σημαντικές παρατίθενται στο Παράρτημα ΙΙ[87] και θεωρούνται οι υπηρεσίες ταχυμεταφορών και ταχυδρομείου, υπηρεσίες διαχείρισης αποβλήτων, παραγωγής και διανομής χρημάτων, κατασκευαστικές εταιρίες και ψηφιακοί πάροχοι.

Βλέπουμε αντικατάσταση των γενικών εννοιών ΦΕΒΥ και ΠΨΥ με τις έννοιες βασικές και σημαντικές. Σαφώς και οι νέες έννοιες είναι επίσης γενικές, αλλά δε θα τις χαρακτηρίζαμε τόσο ασαφείς. Συγκεκριμένα, βασικές οντότητες είναι αυτές που απαιτούνται για τη λειτουργία της εσωτερικής αγοράς και που σε περίπτωση διατάραξής τους, να παραλύσει ο τομέας. Ενώ σημαντικές οι οντότητες οι οποίες δεν έχουν την ίδια βαρύτητα με τα βασικές, αλλά διευκολύνουν την εύρυθμη λειτουργία της εσωτερικής αγοράς. Διασαφηνίζονται συνεπώς οι έννοιες αν τις ερμηνεύσουμε από τη σκοπιά του ρόλου που διαδραματίζουν εντός της Ένωσης.

Στο άρθρο 4 της πρότασης[88] εισάγεται κι μία νέα οντότητα. «Κάθε φυσικό ή νομικό πρόσωπο που έχει συσταθεί και αναγνωρίζεται ως τέτοιο σύμφωνα με το εθνικό δίκαιο του τόπου εγκατάστασής του, τα

[86] Άρθρο 2 της Πρότασης

[87] Άρθρο 4 της Πρότασης

[88] Άρθρο 4 της Πρότασης

οποίο μπορεί , ενεργώντας εξ ιδίου ονόματος, να ασκεί δικαιώματα και να αναλαμβάνει υποχρεώσεις».

Κάνοντας τον παραλληλισμό με την NIS , θα λέγαμε ότι οι ΦΕΒΥ μετονομάστηκαν σε βασικές οντότητες και οι ΠΨΥ σε σημαντικές, οπότε δεν αλλάζει κάτι ως τη δυσκολία στη διαδικασία κατηγοριοποίησής των.

Ωστόσο, παρατηρούνται δύο στοχευμένες αλλαγές. Πρώτον , η διεύρυνση των τομέων και η ένταξη σε αυτούς και των φυσικών προσώπων. Συγκεκριμένα, οι βασικοί τομείς αυξάνονται από επτά στους δέκα και οι σημαντικοί από τρεις σε οκτώ!

Αναλυτικότερα, στο Παράρτημα Ι πέραν των [……] , έχουν προστεθεί οι ψηφιακές υποδομές , η δημόσια διοίκηση και το διάστημα. Η δημόσια διοίκηση είχε ενταχθεί ήδη από κάποιες χώρες (Ισπανία, Κύπρος), , ενώ η Ισπανία είχε εντάξει και το διάστημα, πέρα από τους επτά τομείς που ήδη προβλέπονται στην NIS. Προτείνονται και οι ψηφιακές υποδομές λόγω της μεγάλης αλληλεξάρτησης με την οικονομία της Ένωσης[89].

Και στο Παράρτημα ΙΙ, ενσωματώνονται οι ταχυδρομικές υπηρεσίες, οι υπηρεσίες ταχυμεταφορών, η διαχείριση αποβλήτων , η παραγωγή και διανομή χρημάτων και ο κατασκευαστικός τομέας.

Οι νέες προσθήκες αποτυπώνουν[90] την επιθυμία της Επιτροπής να αμβλυνθούνε οι διαφορετικές πρακτικές των κ-μ και την αυξημένη ψηφιοποίηση της εποχής μας. Αν και είναι ακόμη νωρίς, θα μπορούσαμε

[89] Αιτιολογική έκθεση

[90] Thomas Siever “Proposal for a NIS Directive 2.0: Companies covered by the extended scope of application and their obligations”, International Cybersecurity Law Review, 2021, pp. 224-225.

να πούμε ότι οι στόχοι που θέτει η Επιτροπή φαίνεται να επιδιώκονται πιο αποτελεσματικά από την εν θέματι, επικαιροποιημένη έκδοση.

Η δεύτερη σημαντική αλλαγή είναι ότι εισάγεται ένα ενιαίο κριτήριο προσδιορισμού των οντοτήτων , για να κριθεί εάν εμπίπτουν ή όχι στο πεδίο εφαρμογής της NIS II. Οι οντότητες που δεν πληρούν το κριτήριο αυτό, δεν εντάσσονται «αυτόματα» στο πεδίο εφαρμογής της NIS II ακόμη κι αν ανήκουν σε έναν από τους τομείς των Παραρτημάτων I και II[91]. Αυτό σύμφωνα με την Πρόταση[92] είναι η εφαρμογή του κανόνα του κατώτατου ορίου μεγέθους, σύμφωνα με το οποίο όλες οι μεσαίες και μεγάλες επιχειρήσεις, όπως ορίζονται στη σύσταση της Επιτροπής [93], «οι οποίες δραστηριοποιούνται εντός των τομέων ή παρέχουν το είδος των υπηρεσιών που καλύπτονται από την παρούσα οδηγία, εμπίπτουν στο πεδίο εφαρμογής της. Τα κράτη μέλη δεν θα πρέπει να υποχρεούνται να καταρτίσουν κατάλογο των οντοτήτων οι οποίες πληρούν αυτό το γενικά εφαρμοστέο κριτήριο που αφορά το μέγεθος».

Επομένως, οι οντότητες που θεωρούνται «μικρές» ή «πολύ μικρές» ακόμη κι αν εντάσσονται στα Παραρτήματα Της αναθεωρημένης οδηγίας, αποκλείονται από την εφαρμογή της[94].

[91] Thomas Siever “Proposal for a NIS Directive 2.0: Companies covered by the extended scope of application and their obligations”, International Cybersecurity Law Review, 2021, pp. 224-225.

[92] Άρθρο 2 παρ. 1 της Πρότασης

[93] 2003/361/ΕΚ Σύσταση της Επιτροπής

[94] Christoph Haid, Felix Schneider “Cybersecurity on the rise: The NIS Directive 2.0”, Schonherr, https://www.schoenherr.eu/content/cybersecurity-on-the-rise-the-nis-directive-2-0/

Στην NIS I , σύμφωνα με το άρθρο 5, τα κ-μ είναι επιφορτισμένα με το καθήκον του προσδιορισμού των οντοτήτων που υπάγονται στους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών. Αυτή η πρόβλεψη καθυστέρησε την εφαρμογή της οδηγίας κατά έξι μήνες (09 Νοεμβρίου 2018), εκθέτοντας σε κινδύνους και απειλές τόσο τα κ–μ όσο και την εσωτερική αγορά. Η νέα πρόταση δεν έχει αντίστοιχη πρόβλεψη[95]. Το ίδιο το μέγεθος της οντότητας πρέπει από μόνο του να είναι καθοριστικό για το αν εμπίπτει ή όχι στο πεδίο εφαρμογής.

Στόχος όμως είναι να μη μείνουμε στις μεσαίες και μεγάλες επιχειρήσεις, αλλά να ενταχθούν στο πεδίο εφαρμογής και οι μικρές επιχειρήσεις, οι οποίες πληρούν «ορισμένα κριτήρια, τα οποία υποδηλώνουν ότι αυτές διαδραματίζουν σημαντικό ρόλο στις οικονομίες ή τις κοινωνίες των κρατών – μελών ή σε συγκεκριμένους τομείς ή είδη υπηρεσιών»[96].

Σύμφωνα με το άρθρο 2 παρ. 2 της Πρότασης, ανεξαρτήτως μεγέθους, μία οντότητα εντάσσεται στο πεδίο εφαρμογής της NIS II, εάν:

- «α) οι υπηρεσίες παρέχονται από μία από τις ακόλουθες οντότητες: i) δημόσια δίκτυα ηλεκτρονικών επικοινωνιών ή διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών που αναφέρονται στο παράρτημα I σημείο 8· ii) παρόχους υπηρεσιών εμπιστοσύνης που αναφέρονται στο παράρτημα I σημείο 8· iii) μητρώα ονομάτων τομέα ανωτάτου επιπέδου και παρόχου

[95] Thomas Siever “Proposal for a NIS Directive 2.0: Companies covered by the extended scope of application and their obligations”, International Cybersecurity Law Review, 2021, pp. 225-226.

[96] Πρόταση Προοίμιο παρ. 9, 10

υπηρεσιών του συστήματος ονομάτων τομέα (DNS) που αναφέρονται στο παράρτημα I σημείο 8·

- β) η οντότητα είναι φορέας δημόσιας διοίκησης όπως ορίζεται στο άρθρο 4 σημείο 23·
- γ) η οντότητα είναι ο μοναδικός πάροχος υπηρεσίας σε κράτος μέλος·
- δ) η ενδεχόμενη διατάραξη της υπηρεσίας που παρέχει η οντότητα θα μπορούσε να έχει επιπτώσεις στη δημόσια ασφάλεια, στη δημόσια προστασία ή στη δημόσια υγεία·
- ε) ενδεχόμενη διατάραξη της υπηρεσίας που παρέχεται από την οντότητα θα μπορούσε να προκαλέσει συστημικούς κινδύνους, ιδίως για τους τομείς στους οποίους η διαταραχή αυτή θα μπορούσε να έχει διασυνοριακό αντίκτυπο· 28 Σύσταση 2003/361/ΕΚ της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων (ΕΕ L 124 της 20.5.2003, σ. 36). EL 37 EL
- στ) η οντότητα είναι κρίσιμη λόγω της ιδιαίτερης σημασίας της σε περιφερειακό ή εθνικό επίπεδο για τον συγκεκριμένο τομέα ή είδος υπηρεσίας ή για άλλους αλληλοεξαρτώμενους τομείς στο κράτος μέλος·
- ζ) η οντότητα χαρακτηρίζεται ως κρίσιμη οντότητα σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου29 [οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων] ή ως οντότητα ισοδύναμη με κρίσιμη οντότητα, σύμφωνα με το άρθρο 7 της εν λόγω οδηγίας»[97].

[97] Άρθρο 2 παρ. 2 της Πρότασης

Τα κράτη μέλη θα πρέπει να καταρτίσουν κατάλογο των εν λόγω οντοτήτων που εντάσσονται στις επιφυλάξεις και να τον υποβάλουν στην Επιτροπή, εντός έξι μηνών από την προθεσμία ενσωμάτωσης της Οδηγίας. Ανά διετία ο κατάλογος αναθεωρείται. Η Επιτροπή αναλαμβάνει να εκδίδει κατευθυντήριες γραμμές σχετικά με την εφαρμογή των κριτηρίων που ισχύουν για τις πολύ μικρές και τις μικρές επιχειρήσεις, για να διευκολύνει τα κ-μ και για να αποφευχθεί το ενδεχόμενο ανομοιομορφίας.

Αδιαμφισβήτητα, το πεδίο εφαρμογής της NIS II επεκτείνεται σημαντικά, οδηγώντας σε σημαντική αύξηση των οντοτήτων που καλύπτονται από το πεδίο εφαρμογής της. Αναμένεται πενταπλάσια αύξηση των οντοτήτων που θα εντάσσονται σε αυτήν. Έτσι βελτιώνεται η ανθεκτικότητα σχεδόν σε όλους τους τομείς που επηρεάζουν άμεσα ή έμμεσα την εσωτερική αγορά της Ένωσης[98].

## *5.2. Μέτρα διαχείρισης κινδύνου*

Στην αναθεωρημένη έκδοση της NIS βλέπουμε ότι ο νομοθέτης απαιτεί από τις βασικές και σημαντικές οντότητες τις ίδιες απαιτήσεις ασφαλείας. Στο άρθρο 18 αναφέρεται ότι: «Τα κράτη μέλη εξασφαλίζουν ότι οι βασικές και σημαντικές οντότητες λαμβάνουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων

[98] Thomas Siever "Proposal for a NIS Directive 2.0: Companies covered by the extended scope of application and their obligations", International Cybersecurity Law Review, 2021, pp. 226- 227.

όσον αφορά την ασφάλεια δικτυακών και πληροφοριακών συστημάτων που χρησιμοποιούν οι εν λόγω οντότητες κατά την παροχή των υπηρεσιών τους. Λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες, τα μέτρα αυτά διασφαλίζουν επίπεδο ασφάλειας δικτυακών και πληροφοριακών συστημάτων ανάλογο προς τον εκάστοτε κίνδυνο»[99].

Βλέπουμε ότι απαιτεί αναλογικά τεχνικά και οργανωτικά μέσα, όπως ακριβώς και τα άρθρα 14 και 16 της NIS I. Ωστόσο , στην παράγραφο 2 αποτυπώνονται τα μέτρα που θα πρέπει «τουλάχιστον» να ληφθούν. Έτσι έχουμε έναν οδικό χάρτη για τα μέτρα που κατ' ελάχιστον πρέπει να ληφθούν από τις οντότητες των κ-μ.

Η αναφορά στις πλέον πρόσφατες τεχνικές δυνατότητες απαιτεί από τις οντότητες μία συνεχή ενημέρωση και εγρήγορση ως προς τις τεχνολογικές εξελίξεις, με προσαρμοσμένες και καινοτόμες απαντήσεις.

Αναλυτικά τα μέτρα που θα πρέπει τουλάχιστον να λαμβάνονται είναι τα ακόλουθα:

«α) πολιτικές ανάλυσης κινδύνων και ασφάλειας του πληροφοριακού συστήματος·

β) χειρισμός περιστατικών (πρόληψη, ανίχνευση και αντιμετώπιση περιστατικών)·

γ) συνέχιση των δραστηριοτήτων και διαχείριση των κρίσεων·

δ) η ασφάλεια της αλυσίδας εφοδιασμού, συμπεριλαμβανομένων των σχετικών με την ασφάλεια πτυχών που αφορούν τις σχέσεις μεταξύ

[99] Άρθρο 18 της Πρότασης

της κάθε οντότητας και των προμηθευτών της ή των παρόχων υπηρεσιών, όπως οι πάροχοι υπηρεσιών αποθήκευσης και επεξεργασίας δεδομένων ή υπηρεσιών διαχείρισης ασφάλειας·

ε) η ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση δικτυακών και πληροφοριακών συστημάτων, συμπεριλαμβανομένου του χειρισμού και της γνωστοποίησης τρωτών σημείων·

στ) πολιτικές και διαδικασίες (δοκιμές και έλεγχοι) για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας·

ζ) η χρήση της κρυπτογράφησης και της κρυπτοθέτησης»[100].

Σημειώνεται ότι στην ισχύουσα Οδηγία NIS I, δε γίνεται καθόλου αναφορά σε ενδεδειγμένα μέτρα με σκοπό τη διαχείριση του κινδύνου. Συνεπώς αξιολογείται θετικά η απαρίθμηση ορισμένων, ενδεικτικών μέτρων τα οποία σωρευτικά και καθολικά επιβάλλει η Επιτροπή τόσο για την πρόληψη όσο και την καταστολή των διαδικτυακών απειλών. Έτσι διασφαλίζεται η ομοιομορφία στα κ-μ και ένα επίπεδο ωριμότητας αναφορικά με την αντιμετώπιση των απειλών[101].

Επαφίεται στα κ-μ «χωρίς αδικαιολόγητη καθυστέρηση» να διασφαλίσουν τη συμμόρφωση στα ως άνω μέτρα των οντοτήτων της περιοχής ευθύνης τους και αν χρειαστεί να λάβουν «τα αναγκαία διορθωτικά μέτρα» για να το πετύχουν. Αναμένεται μετά την Ψήφιση της

[100] Άρθρο 18 παρ. 2 της Πρότασης

[101] Thomas Siever "Proposal for a NIS Directive 2.0: Companies covered by the extended scope of application and their obligations", International Cybersecurity Law Review, 2021, pp. 229-230.

νέας Οδηγίας να δούμε ποια μέτρα επέλεξαν τα κ-μ να υιοθετήσουν κατά τη διαδικασία ενσωμάτωσης.

Προκειμένου να αποδειχθεί η συμμόρφωση των οντοτήτων στις παραπάνω υποχρεώσεις, τα κ-μ ,σύμφωνα με το άρ. 21 της Πρότασης μπορούν «να απαιτούν από βασικές και σημαντικές οντότητες να πιστοποιούν ορισμένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ στο πλαίσιο συγκεκριμένων ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας που εγκρίνονται σύμφωνα με το άρθρο 49 του κανονισμού (ΕΕ) 2019/881»[102].

Συνεχίζοντας, στην παράγραφο 2 του άρ. 21, η Επιτροπή θέτει πλαίσιο στην ευθύνη των οντοτήτων μέσω ασφαλιστικών δικλείδων κατά τη συμμόρφωσή τους με τις απαιτήσεις της Οδηγίας. Συγκεκριμένα αναφέρεται ότι μέσω εξουσιοδοτικών πράξεων «από ποιες κατηγορίες βασικών οντοτήτων θα απαιτείται η λήψη πιστοποιητικού και δυνάμει ποιων συγκεκριμένα ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας»[103].

Πέραν της διαχείριση των κινδύνων πολύ σημαντικό είναι και η κοινοποίηση των περιστατικών και από τις δύο οντότητες[104]. Οι κοινές υποχρεώσεις για την αναφορά των περιστατικών θεσπίζονται στο άρθρο 20, σύμφωνα με το οποίο «οι βασικές και σημαντικές οντότητες κοινοποιούν, χωρίς αδικαιολόγητη καθυστέρηση, στις αρμόδιες αρχές ή

[102] Άρθρο 21 της Πρότασης

[103] Άρθρο 21 παρ. 2 της Πρότασης

[104] Christoph Haid, Felix Schneider “Cybersecurity on the rise: The NIS Directive 2.0”, Schonherr, https://www.schoenherr.eu/content/cybersecurity-on-the-rise-the-nis-directive-2-0/

στην CSIRT, σύμφωνα με τις παραγράφους 3 και 4, κάθε περιστατικό που έχει σημαντικό αντίκτυπο στην παροχή των υπηρεσιών τους»[105].

Στην παρ.3 του ίδιου άρθρου προσδιορίζεται η έννοια του σημαντικού περιστατικού, το οποίο είναι ένα συμβάν που είτε προκάλεσε ή μπορεί να προκαλέσει σημαντική διαταραχή στη λειτουργία ή να έχει οικονομική ζημία για την οντότητα είτε έχει επηρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας ζημία υλική ή μη.

Πολύ σημαντικό είναι ότι η Πρόταση αποτυπώνει ακριβώς το σχέδιο δράσης που πρέπει να αναλάβει η οντότητα για να ενημερώσει. Η επιτροπή επιθυμεί τη λογοδοσία των οντοτήτων για τον τρόπο χειρισμού συγκεκριμένων συμβάντων[106]. Αρχικά οι οντότητα πρέπει «χωρίς αδικαιολόγητη καθυστέρηση» και συγκεκριμένα εντός 24 ωρών από τη στιγμή που έχει γίνει αντιληπτό το συμβάν να ενημερώσει «αν το περιστατικό προκλήθηκε από παράνομη ή κακόβουλη ενέργεια»[107]. Κατόπιν υποβάλλουν μία ενδιάμεση έκθεση αν το ζητήσει η αρμόδια αρχή ή η SCIRT και τέλος μία τελική έκθεση, η οποία περιλαμβάνει τρεις βασικές πληροφορίες:

«i) λεπτομερή περιγραφή του περιστατικού, της σοβαρότητάς του και των επιπτώσεών του·

ii) το είδος της απειλής ή τη βασική αιτία που ενδεχομένως προκάλεσε το περιστατικό·

[105] Άρθρο 20 της Πρότασης

[106] Thomas Siever "Proposal for a NIS Directive 2.0: Companies covered by the extended scope of application and their obligations", International Cybersecurity Law Review, 2021, pp. 227-228.

[107] Άρθρο 20 της Πρότασης

iii) εφαρμοζόμενα και εν εξελίξει μέτρα μετριασμού»[108].

Τέλος, αρκετά ρηξικέλευθη κρίνεται η πρόβλεψη του άρθρου 27, σύμφωνα με την οποία δίνεται η δυνατότητα σε φορείς εκτος πλαισίου εφαρμογής της Οδηγίας, να ενημερώνου, εθελοντικά, για «σημαντικά συμβάντα, κυβερνοαπειλές ή παρ' ολίγον περιστατικά». Αυτό θα συμβάλει την επαναξιολόγηση τυχόν περιστατικών που δεν έχουν ήδη συμπεριληφθεί αλλά και στην ενίσχυση του «οπλοστασίου» και των «εργαλείων» για την αντιμετώπιση του φαινομένου.[109]

[108] Άρθρο 20 παρ. 4γ της Πρότασης

[109] Thomas Siever "Proposal for a NIS Directive 2.0: Companies covered by the extended scope of application and their obligations", International Cybersecurity Law Review, 2021, pp.229-230.

## *5.3. Γιατί νέα Οδηγία και όχι Κανονισμός*

Σύμφωνα με το άρθρο 18 δίνεται η δυνατότητα στην Επιτροπή να εκδίδει εκτελεστικές πράξεις για να καθορίσει τεχνικές και μεθοδολογικές προδιαγραφές των ανωτέρω (α-ζ) στοιχείων- μέτρων που πρέπει να λαμβάνουν οι οντότητες. Αλλά το μεγαλύτερο ενδιαφέρον παρουσιάζει η επόμενη παράγραφος[110] η οποία δίνει τη δυνατότητα στην Επιτροπή να εκδίδει πράξεις «για τη συμπλήρωση των στοιχείων που ορίζονται στην παράγραφο 2, ώστε να λαμβάνονται υπόψη νέες κυβερνοαπειλές, τεχνολογικές εξελίξεις ή τομεακές ιδιαιτερότητες». Με αυτό τον τρόπο, η Επιτροπή μπορεί να μετεξελίσσει συνεχώς και να αναπροσαρμόζει τα μέτρα ασφαλείας των κ-μ στις νέες καινοτόμες διαδικτυακές εξελίξεις, χωρίς να χρειάζεται πάλι η χρονοβόρα διαδικασία της νομοθετικής πρωτοβουλίας και τροποποίησης.

Ο ερευνητής των εν λόγω Οδηγιών σίγουρα έχει αναρωτηθεί γιατί η ΕΕ επιμένει στο μοτίβο της Οδηγίας και δεν υιοθετεί έναν Κανονισμό, όπως αντίστοιχα έκανε με τον Κανονισμό για τη προστασία των προσωπικών δεδομένων GDPR. Δεδομένου μάλιστα ότι μία από τις πολλές αδυναμίες της NIS I ήταν η μη άμεση και καθολική εφαρμογή της από τα κ-μ. Η ίδια η αιτιολογική έκθεση της Πρότασης δίνει απάντηση σε αυτό το ερώτημα και συγκεκριμένα αναφέρει ότι: στόχος της Οδηγίας ΙΙ είναι «να παράσχει στα κράτη μέλη την απαιτούμενη ευελιξία ώστε να λαμβάνουν υπόψη τις εθνικές ιδιαιτερότητες (όπως η δυνατότητα εντοπισμού πρόσθετων βασικών ή σημαντικών οντοτήτων που υπερβαίνουν το βασικό σενάριο που καθορίζεται στη νομική πράξη). Ως

[110] Άρθρο 18 παρ.6 της Πρότασης

εκ τούτου, το μελλοντικό νομικό μέσο θα πρέπει να είναι οδηγία, δεδομένου αυτός ο νομικός τύπος επιτρέπει τη στοχευμένη βελτίωση της εναρμόνισης, αλλά και έναν ορισμένο βαθμό ευελιξίας για τις αρμόδιες αρχές»[111].

[111] Αιτιολογική Έκθεση Πρότασης

## *5.4.* ***Κυρώσεις***

Ο τρόπος εποπτείας των βασικών και σημαντικών οντοτήτων προτείνεται από την Επιτροπή να διαφοροποιηθεί. Η εποπτεία των βασικών οντοτήτων αναλύεται στο άρθρο 29 της Πρότασης και δύναται να διενεργηθεί τόσο εκ των προτέρων[112] όσο και εκ των υστέρων[113] μιας κυβερνοαπειλής. Τα μέτρα που μπορούν να ληφθούν εκ των προτέρων ενδεικτικά είναι η διενέργεια τακτικών ελέγχων, επιτόπιων επιθεωρήσεων και η πρόσβαση σε δεδομένα, έγγραφα και πληροφορίες. Εκ των υστέρων μπορούν να εκδίδουν προειδοποιήσεις (σε περίπτωση μη συμμόρφωσης), οδηγίες (σε περίπτωση εσφαλμένης συμμόρφωσης), να διατάσσουν παύση συμπεριφοράς και μη επανάληψη αυτής στο μέλλον, να ζητούν ενημέρωση σχετικά με την αποκατάσταση και αντιμετώπιση, να δημοσιοποιούν κατονομαστικά το συμβάν και να επιβάλλουν πρόστιμο.

Σε περίπτωση που τα μέτρα επιβολής αποδειχθούν αναποτελεσματικά, το κ-μ μπορεί να θέσει μία προθεσμία[114] στην οντότητα για να αποκαταστήσει την έλλειψη και να συμμορφωθεί. Αν η προθεσμία παρέλθη άπρακτη, τότε το κ-μ μπορεί να υπεισέλθει σε κυρώσεις. Δεδομένου ότι η επιβολή κυρώσεων είναι το έσχατο μέτρο, η Επιτροπή θέτει στην Πρότασή της[115] τα κριτήρια που θα πρέπει να λάβουν υπόψιν τους οι αρχές πριν την επιβολή των δυσβάσταχτων

[112] Άρθρο 29 παρ.2 της Πρότασης

[113] Άρθρο 29 παρ.4 της Πρότασης

[114] Άρθρο 29 παρ. 5 της Πρότασης

[115] Άρθρο 29 παρ. 7 της Πρότασης

μέτρων. Αυτά , σύμφωνα με το άρθρο 29 της Πρότασης είναι τα ακόλουθα:

«α) η σοβαρότητα της παράβασης και η σημασία των διατάξεων που παραβιάστηκαν. Στις παραβάσεις που θα πρέπει να θεωρούνται σοβαρές συγκαταλέγονται: επανειλημμένες παραβιάσεις, παράλειψη κοινοποίησης ή αποκατάστασης περιστατικών με αποτέλεσμα τη σημαντική διατάραξη, αδυναμία αποκατάστασης ελλείψεων σύμφωνα με δεσμευτικές οδηγίες των αρμόδιων αρχών, παρεμπόδιση των ελέγχων ή των δραστηριοτήτων παρακολούθησης που διατάσσονται από την αρμόδια αρχή μετά τη διαπίστωση παράβασης, παροχή ψευδών ή χονδροειδώς διαστρεβλωμένων πληροφοριών σε σχέση με τις απαιτήσεις διαχείρισης κινδύνου ή τις υποχρεώσεις αναφοράς περιστατικών που ορίζονται στα άρθρα 18 και 20.

β) η διάρκεια της παράβασης, συμπεριλαμβανομένου του στοιχείου των επανειλημμένων παραβάσεων·

γ) η πραγματική ζημία που προκλήθηκε ή οι απώλειες που προέκυψαν ή οι δυνητικές ζημίες ή απώλειες που θα μπορούσαν να έχουν προκληθεί, στον βαθμό που μπορούν να προσδιοριστούν. Κατά την αξιολόγηση αυτής της πτυχής, λαμβάνονται υπόψη, μεταξύ άλλων, οι πραγματικές ή δυνητικές χρηματοοικονομικές ή οικονομικές απώλειες, οι επιπτώσεις σε άλλες υπηρεσίες, ο αριθμός των χρηστών που επηρεάζονται ή ενδέχεται να επηρεαστούν·

δ) το αν η παράβαση διαπράχθηκε εκ προθέσεως ή εξ αμελείας·

ε) μέτρα που λαμβάνει η οντότητα για την πρόληψη ή τον μετριασμό της ζημίας ή/και των απωλειών·

στ) η τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης·

ζ) ο βαθμός συνεργασίας του υπαίτιου φυσικού ή νομικού προσώπου (ή προσώπων) με τις αρμόδιες αρχές»[116].

Αντίθετα, η εποπτεία των σημαντικών φορέων γίνεται μόνο εκ των υστέρων[117]. Τα μέτρα που μπορούν να λάβουν τα κ-μ στο πλαίσιο εποπτείας των σημαντικών φορέων αναγράφονται στο άρθρο 30 παρ. 4 της Πρότασης και ενδεικτικά αναφέρουμε να εκδίδουν ειδοποιήσεις, οδηγίες προς συμμόρφωση, να ζητούν παύση συμπεριφοράς , να κάνουν δημοσίως γνωστή την οντότητα που δε συμμορφώνεται αλλά και να επιβάλλουν κυρώσεις (πρόστιμο). Τα κριτήρια που θα πρέπει να λάβουν υπόψιν τους οι αρμόδιες αρχές πριν την επιβολή κυρώσεων, είναι τα ίδια (α-ζ) που αναλύθηκαν ανωτέρω για τους βασικούς φορείς[118].

Ως εκ τούτου, συνάγεται ότι οι βασικές οντότητες υπόκεινται σε έναν πλήρη έλεγχο ενώ οι σημαντικές οντότητες σε έναν πιο ήπιο έλεγχο. Η διαφοροποίηση έγκειται σαφώς στο γεγονός ότι η αποδιοργάνωση των βασικών οντοτήτων μπορεί να κλονίσει την εσωτερική αγορά της Ένωσης, ενώ στις σημαντικές οντότητες δεν θα έχει τον ίδιο αντίκτυπο[119].

[116] Άρθρο 29 της Πρότασης

[117] Thomas Siever "Proposal for a NIS Directive 2.0: Companies covered by the extended scope of application and their obligations", International Cybersecurity Law Review, 2021, pp. 228-229.

[118] Άρθρο 30 παρ. 5 της Πρότασης

[119] Thomas Siever "Proposal for a NIS Directive 2.0: Companies covered by the extended scope of application and their obligations", International Cybersecurity Law Review, 2021, pp. 228-229.

Ρηξικέλευθη ρύθμιση, όσον αφορά την επιβολή κυρώσεων είναι αυτή που προβλέπεται στο άρθρο 29 παρ. 6, ήτοι ότι «κάθε φυσικό πρόσωπο που είναι υπεύθυνο ή ενεργεί ως αντιπρόσωπος βασικής οντότητας με βάση την εξουσία εκπροσώπησής της, την αρμοδιότητα να λαμβάνει αποφάσεις εξ ονόματός της ή να ασκεί τον έλεγχό της, έχει τις εξουσίες να διασφαλίζει τη συμμόρφωσή της με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία. Τα κράτη μέλη μεριμνούν ώστε τα εν λόγω φυσικά πρόσωπα να μπορούν να θεωρηθούν υπεύθυνα για παράβαση των καθηκόντων τους όσον αφορά την τήρηση των υποχρεώσεων που ορίζονται στην παρούσα οδηγία»[120].

Για να γίνει κατανοητό περί ποιών φυσικών προσώπων γίνεται ο λόγος θα πρέπει να διαβάσουμε την ανωτέρω παράγραφο συνδυαστικά με το άρθρο 29 παρ. 5β[121].

Στο άρθρο 29 αναφέρεται ότι οι αρμόδιες αρχές «να επιβάλουν ή να ζητήσουν από τα αρμόδια όργανα ή δικαστήρια να επιβάλουν, σύμφωνα με την εθνική νομοθεσία, προσωρινή απαγόρευση κατά οποιουδήποτε προσώπου ασκεί διευθυντικά καθήκοντα σε επίπεδο γενικού διευθυντή ή νομικού εκπροσώπου στην εν λόγω βασική οντότητα, καθώς και οποιουδήποτε άλλου φυσικού προσώπου θεωρείται υπαίτιο για την παράβαση, να ασκούν διευθυντικά καθήκοντα στην εν λόγω οντότητα»[122].

[120] Άρθρο 30 παρ.6 της Πρότασης

[121] Thomas Siever “Proposal for a NIS Directive 2.0: Companies covered by the extended scope of application and their obligations”, International Cybersecurity Law Review, 2021, p. 229

[122] Άρθρο 29 παρ.5 υποπαράγραφος β της Πρότασης

Ερμηνεύοντας συνδυαστικά αυτές τις δύο διατάξεις συνάγεται ότι ευθύνες λόγω μη συμμόρφωσης μπορούν να αποδοθούν και σε όποιο πρόσωπο ασκεί διευθυντικά καθήκοντα αλλά και σε οποιονδήποτε κριθεί υπεύθυνος για την παράλειψη ή παραβίαση[123].

Η Επιτροπή αναφέρει στην αιτιολογική έκθεση ότι το σύστημα κυρώσεων που προβλέφθηκε με την NIS I είναι αναποτελεσματικό. Συγκεκριμένα προβλέπει ότι « τα κ-μ είναι υπεύθυνα να επιβάλλουν κυρώσεις , οι οποίες πρέπει να είναι αποτελεσματικές , αναλογικές και αποτρεπτικές»[124]. Η ασάφεια του καθεστώτος κυρώσεων έδωσε ευρεία διακριτική ευχέρεια στα κ-μ[125]. Τα κ-μ δείχνουν απροθυμία να επιβάλλουν κυρώσεις στις οντότητες που δε συμμορφώνονται στις απαιτήσεις ασφαλείας και κοινοποίησης των συμβάντων[126]. Με αυτή τη στάση τους τα κ-μ δεν αποτρέπουν τις αδρανείς συμπεριφορές και αυτές γίνονται αποδεκτές. Το γεγονός αυτό όμως σαφώς και υπονομεύει την επιδίωξη των στόχων της Οδηγίας και γι’ αυτό υπάρχει πρόταση για αλλαγή του πλαισίου.

Στην πρόταση της Επιτροπής υπάρχει ρητή και σαφής πρόβλεψη για το καθεστώς των κυρώσεων, η οποία σύμφωνα με κάποιους ερευνητές ομοιάζει αρκετά με την αντίστοιχη πρόβλεψη που υπάρχει

[123] Thomas Siever “Proposal for a NIS Directive 2.0: Companies covered by the extended scope of application and their obligations”, International Cybersecurity Law Review, 2021, p. 229

[124] Άρθρο 21 της NIS

[125] Nicolas Van Tieghem, Nicolas Lfebvre, “While preparing the NIS 2, update of the European Overview of NIS transposition by the Member States…toward convergence?», Riskinsight

[126] Αιτιολογική Έκθεση Πρότασης

στον Κανονισμό GDPR (Άρθρο 83)[127]. Συγκεκριμένα στο άρθρο 31 παράγραφος 4 προβλέπεται ότι «Τα κράτη μέλη διασφαλίζουν ότι οι παραβάσεις των υποχρεώσεων που προβλέπονται στο άρθρο 18 ή στο άρθρο 20 υπόκεινται, σύμφωνα με τις παραγράφους 2 και 3 του παρόντος άρθρου, σε διοικητικά πρόστιμα κατ' ανώτατο όριο ύψους τουλάχιστον 10 000 000 EUR ή έως 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκει η βασική ή σημαντική οντότητα κατά το προηγούμενο οικονομικό έτος, ανάλογα με το ποιο ποσό είναι υψηλότερο»[128].

Καθορίζεται πλέον ρητά το είδος και το ύψος των κυρώσεων που θα πρέπει να επιβάλλουν τα κ-μ με στόχο την ομοιομορφία και την αποφυγή περιπτώσεων όπου για την ίδια παράβαση άλλο κράτος δεν επιβάλλει καμία κύρωση και άλλο φτάνει μέχρι την ποινή φυλάκισης, όπως έχει προβλέψει το Βέλγιο και η Κύπρος.[129]

## *5.5. Πρόβλεψη για GDPR*

Στην ισχύουσα Οδηγία παρατηρείται νομοθετικό κενό ως προς την προστασία των φυσικών προσώπων και των προσωπικών δεδομένων

[127] Thomas Siever "Proposal for a NIS Directive 2.0: Companies covered by the extended scope of application and their obligations", International Cybersecurity Law Review, 2021, p. 229

[128] Άρθρο 31 παρ. 4 της Πρότασης

[129] Nicolas Van Tieghem, Nicolas Lfebvre, "While preparing the NIS 2, update of the European Overview of NIS transposition by the Member States…toward convergence?», Riskinsight

τους[130]. Δεν υπάρχει καμία αναφορά στις περιπτώσεις πρόκλησης ζημίας «υλικής ή άυλης» (όπως διατυπώνεται στη νέα Οδηγία) σε φυσικά πρόσωπα.

Στο άρθρο 32 της Πρότασης προβλέπεται ότι «εάν οι αρμόδιες αρχές έχουν ενδείξεις ότι η παράβαση από βασική ή σημαντική οντότητα των υποχρεώσεων που ορίζονται στα άρθρα 18 και 20 συνεπάγεται παραβίαση δεδομένων προσωπικού χαρακτήρα, όπως ορίζεται στο άρθρο 4 παράγραφος 12 του κανονισμού (ΕΕ) αριθ. 2016/679, η οποία κοινοποιείται σύμφωνα με το άρθρο 33 του εν λόγω κανονισμού, ενημερώνουν τις εποπτικές αρχές που είναι αρμόδιες σύμφωνα με τα άρθρα 55 και 56 του εν λόγω κανονισμού εντός εύλογου χρονικού διαστήματος»[131].

Θα πρέπει λοιπόν οι αρμόδιες αρχές που έχει ορίσει το κάθε κ-μ να συνεργάζεται με τις αρμόδιες για την προστασία δεδομένων προσωπικού χαρακτήρα αρχές. Σύμφωνα με το άρθρο 33 του Κανονισμού GDPR, η κοινοποίηση θα πρέπει να λαμβάνει χώρα «εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα»[132].

Από τη στιγμή της κοινοποίησης αναλαμβάνουν δράση οι αρμόδιες κατά τον Κανονισμό GDPR αρχές, για να διαφυλάξουν τα προσωπικά δεδομένα των φυσικών προσώπων που κινδυνεύουν.

[130] Sandra Schmitz- Berndt, Fabian Anheier, "Synergies in Cybersecurity Incident Reporting- The NIS Cooperation Group Publication 04/20 in Context", European Data protection Law Review, 2021, Vol 7 Issue 1, p.101

[131] Άρθρο 32 παρ.1 της Πρότασης

[132] Άρθρο 33 του Κανονισμού

Στην επόμενη παράγραφο αναφέρεται ότι «Εάν οι εποπτικές αρχές που είναι αρμόδιες σύμφωνα με τα άρθρα 55 και 56 του κανονισμού (ΕΕ) 2016/679 αποφασίσουν να ασκήσουν τις εξουσίες τους σύμφωνα με το άρθρο 58 στοιχείο θ) του εν λόγω κανονισμού και να επιβάλουν διοικητικό πρόστιμο, οι αρμόδιες αρχές δεν επιβάλλουν διοικητικό πρόστιμο για την ίδια παράβαση δυνάμει του άρθρου 31 της παρούσας οδηγίας. Οι αρμόδιες αρχές μπορούν, ωστόσο, να εφαρμόζουν τα μέτρα επιβολής ή να ασκούν τις εξουσίες επιβολής κυρώσεων που προβλέπονται στο άρθρο 29 παράγραφος 4 στοιχεία α) έως θ), στο άρθρο 29 παράγραφος 5 και στο άρθρο 30 παράγραφος 4 στοιχεία α) έως η) της παρούσας οδηγίας»[133].

Συνεπώς λαμβάνουν μεν χώρα δύο ξεχωριστές και παράλληλες διαδικασίες , αλλά η εποπτική αρχή κυβερνοασφάλειας του κ-μ χάνει την εξουσία και το μοχλό πίεσης της επιβολής προστίμου. Αυτό εξηγείται από τη γενική αρχή του δικαίου ότι δεν μπορούν να συντρέξουν δύο διοικητικά πρόστιμα για την ίδια παράβαση.

Η παραπομπή της παράβασης στις αρχές των προσωπικών δεδομένων σημαίνει ότι οι κυρώσεις της οντότητας δύναται να είναι ανάλογες με αυτές του Κανονισμού GDPR. Σημειωτέον ότι οι κυρώσεις που προβλέπονται στο άρθρο 83 του εν λόγω Κανονισμού είναι πολύ υψηλότερες από αυτές της Οδηγίας NIS II αφού μπορεί να φτάσουν και τα 20 εκατομμύρια ευρώ.

Όλα αυτά προβλέφθηκαν διότι σε μία πιθανή κυβερνοεπίθεση και υποκλοπή των δεδομένων μιας οντότητας με στοιχεία φυσικών

[133] Άρθρο 32 παρ.2 της Πρότασης

προσώπων (ιατρικά δεδομένα, τραπεζικό απόρρητο), τα οποία μπορούν περαιτέρω να τα χρησιμοποιήσουν για αλλότριους και κακόβουλους σκοπούς.

## 5.6. *Πυλώνες δράσης και Κοινή Μονάδα Κυβερνοχώρου*

Η πρόταση της Επιτροπής στοχεύει σε λήψη μέτρων αναφορικά με τρεις πυλώνες δράσης της Ένωσης και συγκεκριμένα στον τομέα της τεχνολογικής κυριαρχίας, της επιχειρησιακής ικανότητας πρόληψης-αντιμετώπισης και την ανάπτυξη ενός παγκόσμιου και ανοιχτού κυβερνοχώρου. Αναλυτικότερα:

Προτείνεται η μεταρρύθμιση των υπαρχόντων συστημάτων ασφαλείας του δικτύου και των πληροφοριών, ούτως ώστε οι διάφορες δημόσιες και ιδιωτικές δομές κρίσιμης σημασίας να αυξήσουν την κυβερνοανθεκτικότητά τους. Δομές όπως, νοσοκομεία, σχολεία, ερευνητικά κέντρα, εγκαταστάσεις κατασκευής ιατρικών και φαρμακευτικών προϊόντων, ενεργειακά και τηλεπικοινωνιακά δίκτυα καθώς και δομές δημόσιας διοίκησης είναι ζωτικής σημασίας και πρέπει να τα προστατέψουμε στο περιβάλλον των όλο και πιο περίπλοκων απειλών που αναπτύσσονται.

Η Επιτροπή προτείνει[134] τη δημιουργία ενός δικτύου, τύπου κέντρο επιχειρήσεων ασφαλείας, για ολόκληρη την Ένωση. Μία Κοινή Μονάδα Κυβερνοχώρου. Το νέο συλλογικό όργανο θα έχει ως σκοπό την

[134] https://ec.europa.eu/commission/presscorner/detail/el/ip_21_3088

ενίσχυση της ήδη υπάρχουσας συνεργασίας μεταξύ των κρατών- μελών και συγκεκριμένα των φορέων που έχουν ως αρμοδιότητα την πρόληψη, αποτροπή και αντιμετώπιση των κυβερνοεπιθέσεων. Αυτό που θα καταφέρει ουσιαστικά να αναβαθμίσει το επίπεδο ασφαλείας είναι η δυνατότητα έγκαιρου εντοπισμού των ενδείξεων κυβερνοεπίθεσης αλλά και η ανάπτυξη προορατικής δράσης, πριν ακόμα προκληθεί βλάβη. Σαφώς απαιτείται μηχανισμός Τεχνητής Νοημοσύνης για να καταστούν δυνατές αυτές οι λειτουργίες.

Ο Ύπατος Εκπρόσωπος[135] από την πλευρά του υποβάλλει προτάσεις για την ενίσχυση της εργαλειοθήκης για τη διπλωματία στον κυβερνοχώρο, για την αποτελεσματική πρόληψη και αποθάρρυνση των κακόβουλων δραστηριοτήτων ειδικά εάν αυτές επηρεάζουν ζωτική σημασίας τομείς, όπως εφοδιασμό και δημοκρατία.

Στη δράση προτείνεται και η συνεργασία με τον Ευρωπαϊκό Οργανισμό Άμυνας και η αξιοποίηση του Ευρωπαϊκού Ταμείου Άμυνας, καθώς δεν πρέπει να παροράται ότι οι κυβερνοεπιθέσεις αποτελούν ένα νέο είδος πολέμου που μπορεί να αποβούν επιζήμιες για την εκάστοτε εθνική ασφάλεια. Η διάρρηξη της κυβερνοασφάλειας ενός κράτους αποδεικνύει ή έστω δημιουργεί την εντύπωση της τρωτότητας και υπολειτουργικότητας. Αρκεί κανείς να σκεφτεί ότι η ενεργοποίηση της εθνικής άμυνας και της ασφάλειας μιας χώρας στηρίζεται εξολοκλήρου σε διαδικτυακά μέσα (επικοινωνία, επιστράτευση, συντονισμός) και εάν ένας πυλώνας νεκρώσει από κυβερνοεπίθεση, δεν έχει αναπτυχθεί εναλλακτικός τρόπος υποστήριξης αυτών των τομέων, παρά μόνο οι

[135] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM:high_representative_cfsp

προσπάθειες αντιμετώπισης και άμεσης επίλυσης του προβλήματος. Αντίστοιχα σε περίπτωση φυσικής καταστροφής η κυβερνοεπίθεση σε καίριες δομές, όπως είναι η ενημέρωση των πολιτών ή η διάδραση δύο δημόσιων φορέων μπορεί να αποβεί καταστροφική.

Η Ένωση και σε αυτόν τον τομέα δεν περιορίζεται στο έδαφος της και αναπτύσσει μια εξωεδαφική δράση παρακινώντας τους διεθνείς εταίρους για την παγκόσμια συνεργασία και την ενίσχυση της διεθνούς ασφάλειας και σταθερότητας στον κυβερνοχώρο. Θα προσπαθήσει να προωθήσει το όραμά της εντατικοποιώντας τους κυβερνοδιαλόγους με τρίτες χώρες, διεθνείς και περιφερειακούς οργανισμούς για την ανάπτυξη των εξωτερικών ικανοτήτων της στον Κυβερνοχώρο.

Η Ευρωπαϊκή Ένωση έχει την εξαιρετικά μοναδική ευκαιρία να συνδυάσει τον προϋπολογισμό της με τους προϋπολογισμούς των κρατών μελών για να ενισχύσει τις βιομηχανικές και τεχνολογικές ικανότητές της στον τομέα της κυβερνοασφάλειας. Όσον αφορά το επόμενο μακροπρόθεσμο προϋπολογισμό της, έχει δεσμευτεί να στηρίξει το νέο όραμα για ενισχυμένη κυβερνοασφάλεια, μέσω των προγραμμάτων «Ψηφιακή Ευρώπη» και «Ορίζων Ευρώπη». Αντίστοιχα, τα κράτη μέλη ενθαρρύνονται να προϋπολογίσουν ισόποσες επενδύσεις, ώστε να φτάσουν συνδυαστικά στα 4,5 δισεκατομμύρια.

# 6

# *Συμπεράσματα- Επίλογος*

Ο νομοθέτης πρέπει πάντα να ακολουθεί τις εξελίξεις της κοινωνικής ζωής, στις οποίες εντάσσονται και οι εξελίξεις της τεχνολογίας, για να αντιμετωπίζονται οριζοντίως οι νέες προκλήσεις. Παρατηρείται βέβαια μία εύλογη καθυστέρηση στην ανάληψη νομοθετικής πρωτοβουλίας και δράσης. Για την υιοθέτηση της NIS I , οι συζητήσεις ξεκίνησαν το 2013, ψηφίστηκε μετά από τρία χρόνια και μετά από άλλα δύο όφειλαν τα κ-μ να έχουν συμμορφωθεί. Όλο αυτό το χρονικό διάστημα οι πολίτες και η πολιτεία ήταν ευάλωτοι και εκτεθειμένοι σε κινδύνους και σε απειλές.

Δεν μπορούμε να μην αναγνωρίσουμε ότι με την NIS έγινε μία πρώτη προσπάθεια. Από την εφαρμογή της όμως διαπιστώθηκαν αρκετές αδυναμίες. Οι φορείς που εντάσσονται στο πεδίο εφαρμογής της εξαρτώνται σε μεγάλο βαθμό από τις υποκειμενικές επιλογές του κάθε κ-μ. Παρέχει ευρεία διακριτική ευχέρεια στα κ-μ για καίρια ζητήματα τα οποία θα μπορούσε να ρυθμίσει η ίδια. Και εμπεριέχει αρκετές ασαφείς και γενικόλογες έννοιες, οι οποίες όχι μόνο καθιστούν απίθανη την ομοιόμορφη και ευθυγραμμισμένη εφαρμογή της από τα κ-

μ αλλά και συμβάλλουν στη μη αποτελεσματική συνύπαρξη της με τον Κανονισμό GDPR. Η μη αναφορά στον εν λόγω Κανονισμό αποδεικνύει τα κενά που αφήνει η Οδηγία ως προς τη συνεργασία των αρμόδιων φορέων για την αντιμετώπιση των Κυβερνοαπειλών.

Η Επιτροπή και ο Ύπατος Εκπρόσωπος έχουν δεσμευτεί να υποβάλλουν κατά τακτά χρονικά διαστήματα εκθέσεις σχετικά με την πρόοδο που σημειώνεται στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της ΕΕ αλλά και στα κ-μ, ενθαρρύνοντας τους ανωτέρω φορείς να συμμετάσχουν στη διαδικασία. Στόχος βάσιμος είναι τους προσεχείς μήνες να εφαρμόζεται η νέα στρατηγική για την Κυβερνοασφάλεια. Επαφίεται στο Συμβούλιο και το Ευρωκοινοβούλιο, ως τα κατεξοχήν νομοθετικά όργανα στην ενωσιακή έννομη τάξη, να εξετάσουν και να εγκρίνουν την επικείμενη Οδηγία NIS 2 και κατόπιν τα κ-μ να μεταφέρουν εντός εύλογου χρονικού πλαισίου τις σχετικές διατάξεις στην εθνική τους έννομη τάξη. Σαφώς, το έργο της Επιτροπής δε σταματά στην αρχική πρόταση νομοθετικής πρωτοβουλίας, αλλά αναλαμβάνει και το έργο περιοδικής επανεξέτασής της, υποβάλλοντας αντίστοιχες εκθέσεις.

Λαμβάνοντας υπόψη τις εγγενείς αδυναμίες της Οδηγίας, η Επιτροπή προτείνει την κατάργηση της διάκρισης των οντοτήτων σε Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και σε Παρόχους Ψηφιακών Υπηρεσιών. Αντ' αυτού εισηγείται τη διάκριση σε βασικές και σημαντικές οντότητες, ανάλογα με τη σημασία τους για τη λειτουργία της εσωτερικής αγοράς. Επεκτείνει το πεδίο εφαρμογής και σε άλλους τομείς και υποτομείς, εντάσσει και τις μικρές και πολύ μικρές οντότητες, επεκτείνοντας σημαντικά το πεδίο εφαρμογής της Οδηγίας. Κατ' αυτό

τον τρόπο θα εμπλακεί στη διαδικασία ένα πολύ σημαντικό μέρος της εσωτερικής οικονομίας της Ένωσης. Πολύ σημαντικό είναι ακόμη ότι διευρύνει την έννοια του περιστατικού και περιλαμβάνει και τις συνέπειες σε φυσικά πρόσωπα. Έτσι θα λέγαμε ότι επιτυγχάνεται η σύνδεση με τον Κανονισμό GDPR. Εισάγει όμως και ευθύνες για τα φυσικά πρόσωπα, λόγω μη συμμόρφωσης σε απαιτήσεις ασφάλειας και κοινοποίησης περιστατικών. Τέλος, επιβάλλει εποπτικά μέτρα σχετικά με τις απαιτήσεις ασφάλειας και κοινοποίησης περιστατικών, αναγνωρίζοντας την υπερβολική διακριτική ευχέρεια που δόθηκε με την NIS I.

Κατόπιν όλων των ανωτέρω, καταλήγουμε στο συμπέρασμα ότι υπάρχουν βάσιμες ελπίδες για την έτι περαιτέρω θωράκιση του Κυβερνοκόσμου και των δικαιωμάτων και ελευθεριών που γεννώνται μέσω αυτού για τους Ευρωπαίους Πολίτες.

# *Βιβλιογραφία*

## *Ελληνική*


- -Γ. Γιαννόπουλος, Η ευθύνη των παρόχων υπηρεσιών στο Internet, Νομική Βιβλιοθήκη, 2013
- Ι. Ιγγλεζάκης, Δίκαιο Πληροφορικής, Εκδόσεις Σάκκουλα, 2021


## *Ξενόγλωσση*


- Nicolas Van Tieghem, Nicolas Lfebvre, “While preparing the NIS 2, update of the European Overview of NIS transposition by the Member States…toward convergence?», Riskinsight
- Maria Theres Holzleitner, Johannes Reicht, “European provisions for cybersecurity in the smart grid an overview of th NIS- directive”, Elektrotechnik Und Informationstechnik, Vol 134, No.1, 2017
- Dimitra Markopoulou, Vangelis Papakonstantinou , Paul de Hert “The new EU cybersecurity framework The NIS Directive , ENISA’ S role and thw General Data Protection Regulation”, Computer law & Security review, Issue 6, 2019
- Johan David Michels, Ian Walden, “Beyond “Complacency and Panic”: Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?” , European Law Review, 2020, Vol. 45, Issue 1

- Maria There Holzieitner, Johannes Reichl, “Legal Problems for the protection of smart Grids from cyber threats”, European Energy Journal, Vol 6, Issue 3, 2016
- Grazyna Szpor, “The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland”, Review of European and Comparative Law, Vol 46, Issue 3, 2021
- Ildiko Angeli, Eszter Sieber- Fazakas, “Automotive Sector Within the Scope of Planned NIS II Cybersecurity Rules”, Budapest Business Journal, 2021, Vol. 29, Issue 10
- Thomas Siever “Proposal for a NIS Directive 2.0: Companies covered by the extended scope of application and their obligations”, International Cybersecurity Law Review, 2021
- Christoph Haid, Felix Schneider “Cybersecurity on the rise: The NIS Directive 2.0”, Schonherr
- Sandra Schmitz- Berndt, Fabian Anheier, “Synergies in Cybersecurity Incident Reporting- The NIS Cooperation Group Publication 04/20 in Context”, European Data protection Law Review, 2021, Vol 7 Issue 1,

## *Ιστοσελίδες*

- https://www.schoenherr.eu/content/cybersecurity-on-the-rise-the-nis-directive-2-0/
- https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0017.02/DOC_1&format=PDF

- https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32016L1148
- https://lawdb.intrasoftnet.com/
- https://mindigital.gr
- https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:52020PC0823
- https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391
- https://mindigital.gr/wp-content/uploads/2021/06/%CE%95%CE%B3%CF%87%CE%B5%CE%B9%CF%81%CE%AF%CE%B4%CE%B9%CE%BF-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf
- https://ec.europa.eu/commission/presscorner/detail/el/ip_21_3088