ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης

NIS2

Η ΟΔΗΓΙΑ NIS2 ΣΤΗΝ ΕΛΛΑΔΑ

Πίνακας Περιεχομένων

«Το παρόν φυλλάδιο προετοιμάστηκε υπό την καθοδήγηση της Εθνικής Αρχής Κυβερνοασφάλειας/Γενική Διεύθυνση Επιτελικού Σχεδιασμού/Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας, με την υποστήριξη της Expertise France και μέσω χρηματοδότησης της Γενικής Διεύθυνσης Μεταρρυθμίσεων (DG REFORM) της Ευρωπαϊκής Επιτροπής»

Εισαγωγή

Η Οδηγία NIS2 (ΕΕ 2022/2555) αποτελεί τη βασική νομοθεσία της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια, εστιάζοντας στην προστασία κρίσιμων υποδομών (βασικών και σημαντικών οντοτήτων). Καθορίζει νομικά μέτρα για την ενίσχυση της ασφάλειάς τους, διασφαλίζοντας ένα αυξημένο επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση.

Οι κανόνες της ΕΕ για την κυβερνοασφάλεια, που θεσπίστηκαν το 2016[1] επικαιροποιήθηκαν με την Οδηγία NIS2, η οποία δημοσιεύτηκε το 2022. Η Οδηγία NIS2 εκσυγχρονίζει το υφιστάμενο νομικό πλαίσιο, προσαρμόζοντάς το στις αυξημένες απαιτήσεις ψηφιοποίησης και στο συνεχώς εξελισσόμενο τοπίο απειλών στον κυβερνοχώρο.

Ο στόχος της Οδηγίας NIS2, εξακολουθεί να είναι:
Η θέσπιση μέτρων που αποσκοπούν στην επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση, με σκοπό τη βελτίωση της λειτουργίας της εσωτερικής αγοράς.

Για το σκοπό αυτό η Οδηγία NIS2 καθορίζει:

| Α |
Υποχρεώσεις Διακυβέρνησης Κρατών Μελών

- εθνικές στρατηγικές κυβερνοασφάλειας
- αρχές διαχείρισης κυβερνοκρίσεων
- ενιαία σημεία επαφής για την κυβερνοασφάλεια
- ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT)
- διενέργεια εποπτείας και μηχανισμός επιβολής σε σχέση με τις απαιτήσεις

| Β |
Υποχρεώσεις οργανισμών

- μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας
- ενίσχυση της λογοδοσίας της ανώτατης διοίκησης
- διευκόλυνση εποπτείας από τις αρμόδιες αρχές

και

- υποχρεώσεις υποβολής αναφορών

| Γ |
Υποχρεώσεις για την υποστήριξη και την ανταλλαγή πληροφοριών

- κανόνες και υποχρεώσεις σχετικά με την ανταλλαγή πληροφοριών για την κυβερνοασφάλεια

Η Οδηγία NIS2, βασίζεται στις απαιτήσεις και προβλέψεις της αρχικής οδηγίας NIS1 και

- **επεκτείνει το πεδίο εφαρμογής** των κανόνων κυβερνοασφάλειας σε νέους τομείς και οντότητες,
- **εισάγει επιπλέον υποχρεώσεις** σχετικά με την γνωστοποίηση περιστατικών κυβερνοασφάλειας, περιλαμβανομένων αυστηρών προθεσμιών και πολλαπλών σταδίων, εντός των οποίων πρέπει να ενημερώνεται η αρμόδια CSIRT
- **διευκρινίζει και ενισχύει τα ελάχιστα οριζόντια μέτρα** διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας,
- **προβλέπει** διάφορα είδη εποπτείας και ελέγχων και
- **βελτιώνει** περαιτέρω την ανθεκτικότητα και τις ικανότητες αντιμετώπισης συμβάντων των δημόσιων και ιδιωτικών οντοτήτων, των αρμόδιων αρχών και της ΕΕ στο σύνολό της.

1. Με την Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του συμβουλίου της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, η οποία μεταφέρθηκε στην εθνική έννομη τάξη με το ν. 4577/2018.

ΤΟΜΕΙΣ & ΟΝΤΟΤΗΤΕΣ ΕΝΤΟΣ ΤΗΣ ΟΔΗΓΙΑΣ NIS2 ΚΑΙ ΤΟΥ Ν. 5160/2024

Οι κρίσιμες υποδομές, επιχειρήσεις, φορείς και οργανισμοί που εμπίπτουν στο πεδίο εφαρμογής του ν. 5160/2024 και της Οδηγίας NIS2 αναφέρονται ως "οντότητες". Για τις οντότητες αυτές, η διατάραξη της ασφάλειας των υπηρεσιών που παρέχουν, εκτιμάται ότι μπορεί να έχει σημαντικό αρνητικό αντίκτυπο στην εσωτερική αγορά ή την λειτουργία του κράτους.

Τέτοιες οντότητες θεωρούνται όσες δραστηριοποιούνται σε συγκεκριμένους τομείς και κατά κανόνα πληρούν συγκεκριμένα κριτήρια μεγέθους αναφορικά με τον αριθμό του απασχολούμενου προσωπικού ή τον κύκλο εργασιών τους.

Συγκεκριμένα, εντός πεδίου εφαρμογής της Οδηγίας NIS2, βρίσκονται δημόσιοι ή ιδιωτικοί οργανισμοί οι οποίοι:

Α. παρέχουν τις υπηρεσίες τους ή ασκούν τις δραστηριότητές τους εντός της Ένωσης ΚΑΙ
Β. δραστηριοποιούνται στους ακόλουθους τομείς

Βασικές Οντότητες

Ενέργεια	Υγεία	Διαχείριση υπηρεσιών ΤΠΕ (μεταξύ επιχειρήσεων)
Μεταφορές	Πόσιμο νερό	Οντότητες δημόσιας διοίκησης
Τράπεζες	Λύματα	Διάστημα
Υποδομές χρηματοπιστωτικών αγορών	Ψηφιακές υποδομές	

Σημαντικές Οντότητες

Ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών	Παραγωγή, μεταποίηση και διανομή τροφίμων	Έρευνα
Διαχείριση αποβλήτων	Κατασκευαστικός τομέας	
Παρασκευή, παραγωγή και διανομή χημικών προϊόντων	Ψηφιακοί πάροχοι	

ΚΑΙ

Γ. Χαρακτηρίζονται -κατ' ελάχιστο- ως μεσαίες επιχειρήσεις σύμφωνα με το άρθρο 2 του παραρτήματος της σύστασης 2003/361/ΕΚ

Διάγραμμα: Ορισμός των ΜμΕ, σύμφωνα με τη σύσταση 2003/361/ΕΚ.

Κατηγορία Επιχείρησης	Αριθμός απασχολούμενων		Ετήσιος κύκλος εργασιών	<ή>	Ετήσιος συνολικός Ισολογισμός
Μεσαία	<250	ΚΑΙ	≤ € 50 εκατ.	<ή>	≤ € 43 εκατ.
Μικρή	<50		≤ € 10 εκατ.	<ή>	≤ € 10 εκατ.
Πολύ Μικρή	<10		≤ € 2 εκατ.	<ή>	≤ € 2 εκατ.

Αριθμός απασχολούμενων και οικονομικά όρια που προσδιορίζουν τις κατηγορίες επιχειρήσεων

1. Η κατηγορία των **πολύ μικρών**, **μικρών** και **μεσαίων επιχειρήσεων** (ΜμΕ) αποτελείται από επιχειρήσεις που **απασχολούν λιγότερους από 250 εργαζομένους** και των οποίων ο **ετήσιος κύκλος εργασιών δεν υπερβαίνει** τα **50 εκατ**. ευρώ ή το **σύνολο του ετήσιου ισολογισμού** δεν υπερβαίνει τα **43 εκατ. ευρώ**.

2. Στην κατηγορία των ΜμΕ, ως **μικρή επιχείρηση** ορίζεται η επιχείρηση η οποία **απασχολεί λιγότερους από 50 εργαζομένους** και της οποίας ο **ετήσιος κύκλος εργασιών** ή το **σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα 10 εκατ. ευρώ**.

3. Στην κατηγορία των ΜμΕ, ως **πολύ μικρή επιχείρηση** ορίζεται η επιχείρηση η οποία **απασχολεί λιγότερους από δέκα εργαζομένους** και της οποίας ο **ετήσιος κύκλος εργασιών** ή το **σύνολο του ετήσιου ισολογισμού** δεν υπερβαίνει τα **2 εκατ. ευρώ**.)

Ανεξαρτήτως μεγέθους, στο πεδίο εφαρμογής εντάσσονται:

| Α | Οντότητες που παρέχουν υπηρεσίες

i) δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών
ii) εμπιστοσύνης
iii) μητρώου ονομάτων τομέα ανωτάτου επιπέδου, και πάροχοι υπηρεσιών συστήματος ονομάτων τομέα

| Β | Οργανισμοί που είναι ο μοναδικός πάροχος στη χώρα υπηρεσίας που είναι ουσιώδης για τη διατήρηση κρίσιμων κοινωνικών ή οικονομικών δραστηριοτήτων

| Γ | Οργανισμοί, η διατάραξη της υπηρεσίας που παρέχουν θα μπορούσε να έχει σημαντικό αντίκτυπο στη δημόσια ασφάλεια, στη δημόσια τάξη ή στη δημόσια υγεία

| Δ | Οργανισμοί, η διατάραξη της υπηρεσίας που παρέχουν θα μπορούσε να προκαλέσει σημαντικό συστημικό κίνδυνο, περιλαμβανομένων των τομέων στους οποίους η διατάραξη αυτή θα μπορούσε να έχει διασυνοριακό αντίκτυπο

| Ε | Οργανισμοί που είναι κρίσιμοι λόγω της ιδιαίτερης σημασίας τους σε εθνικό ή περιφερειακό επίπεδο για τον συγκεκριμένο τομέα ή είδος υπηρεσίας ή για άλλους αλληλοεξαρτώμενους τομείς στη χώρα

| ΣΤ | Φορείς δημόσιας διοίκησης:

i) της κεντρικής κυβέρνησης, όπως αυτή ορίζεται με το άρθρο 14 παράγραφος 1 περίπτωση γ΄ του ν. 4270/2014,

ii) σε περιφερειακό επίπεδο, ως δευτεροβάθμιος ή πρωτοβάθμιος Οργανισμός Τοπικής Αυτοδιοίκησης (Περιφέρειες και Δήμοι).

| Η | Οντότητες που χαρακτηρίζονται ως κρίσιμες οντότητες δυνάμει της Οδηγίας (ΕΕ) 2022/2557

| Θ | Οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα

ΝΕΕΣ ΡΥΘΜΙΣΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ NIS2: ΣΕ ΣΧΕΣΗ ΜΕ ΤΟ ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Σχετικά με τους τομείς Δραστηριότητας

Στο πεδίο εφαρμογής της Οδηγίας NIS2 έχουν ενταχθεί περισσότεροι τομείς δραστηριότητας σε σχέση με την Οδηγία NIS1.

Στο ακόλουθο γράφημα αποτυπώνονται τόσο οι τομείς δραστηριότητας που περιλαμβάνονταν στην NIS1, όσο και οι νέοι τομείς οι οποίοι προστίθενται στην NIS2.

ΤΟΜΕΙΣ ΥΨΗΛΗΣ ΚΡΙΣΙΜΟΤΗΤΑΣ

ΤΟΜΕΑΣ	ΥΠΟΤΟΜΕΑΣ	ΕΙΔΟΣ ΥΠΗΡΕΣΙΑΣ
Ενέργεια	Ηλεκτρική Ενέργεια	Προμήθεια
		Διανομή
		Μεταφορά
		Παραγωγή
		Διαχείριση
		Συμμετέχοντες στην αγορά (υπηρεσίες συγκέντρωσης, απόκρισης ζήτησης ή αποθήκευσης ενέργειας)
		Διαχείριση σημείου επαναφόρτισης
	Τηλεθέρμανση και τηλεψύξη	Διαχείριση
	Πετρέλαιο	Μεταφορά
		Διύλιση / Επεξεργασία / Αποθήκευση / Παραγωγή
		Κεντρικοί φορείς διατήρησης αποθεμάτων
	Αέριο	Προμήθεια
		Διανομή
		Μεταφορά
		Αποθήκευση
		Υγροποιημένο Φυσικό Αέριο (ΥΦΑ)
		Διύλιση και Επεξεργασία
	Υδρογόνο	Παραγωγή, Αποθήκευση και Μεταφορά

ΤΟΜΕΑΣ	ΥΠΟΤΟΜΕΑΣ	ΕΙΔΟΣ ΥΠΗΡΕΣΙΑΣ
Μεταφορές	Εναέριες	Αερομεταφορές
		Διαχείριση αερολιμένα και βοηθητικών εγκαταστάσεων εντός αερολιμένα
		Διαχείριση εναέριας κυκλοφορίας
	Σιδηροδρομικές	Διαχείριση υποδομής
		Μεταφορά επιβατών και εμπορευμάτων
	Πλωτές	Εσωτερικές μεταφορές επιβατών και εμπορευμάτων
		Διαχείριση λιμένων και εκμετάλλευση έργων εξοπλισμού εντός λιμένων
		Διαχείριση κυκλοφορίας πλοίων (VTS)
	Οδικές	Έλεγχος και Διαχείριση Κυκλοφορίας
		Συστήματα Ευφυών Μεταφορών (ITS)
Τράπεζες		Πιστωτικά ιδρύματα
Υποδομές χρηματοπιστωτικών αγορών		Εκμετάλλευση τόπων διαπραγμάτευσης
		Κεντρικοί Αντισυμβαλλόμενοι (CCPs) – Εκκαθάριση Προϊόντων
Υγεία		Παροχή Υγειονομικής Περίθαλψης
		Εργαστήρια αναφοράς σύμφωνα με το άρθρο 15 του κανονισμού (ΕΕ) 2022/2371
		Δραστηριότητες έρευνας και ανάπτυξης για φάρμακα
		Παρασκευή βασικών φαρμακευτικών προϊόντων και φαρμακευτικών σκευασμάτων (τομέας Γ κλάδος 21 της NACE αναθ. 2)
		Κατασκευή ιατροτεχνολογικών προϊόντων που θεωρούνται κρίσιμης σημασίας κατά τη διάρκεια κατάστασης έκτακτης ανάγκης (άρθρο 22 του κανονισμού (ΕΕ) 2022/123)
Πόσιμο νερό		Προμήθεια και διανομή πόσιμου νερού
Λύματα		Συλλογή, διάθεση ή επεξεργασία αστικών, οικιακών ή βιομηχανικών λυμάτων
Ψηφιακές υποδομές		Πάροχοι σημείων ανταλλαγής κίνησης διαδικτύου
		Πάροχοι υπηρεσιών συστήματος ονομάτων τομέα (DNS), εξαιρουμένων των διαχειριστών των εξυπηρετητών ονομάτων ρίζας
		Μητρώα ονομάτων τομέα ανώτατου επιπέδου (TLD)
		Πάροχοι υπηρεσιών υπολογιστικού νέφους
		Πάροχοι υπηρεσιών κέντρου δεδομένων
		Πάροχοι δικτύων διανομής περιεχομένου
		Πάροχοι υπηρεσιών εμπιστοσύνης·
		Πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών
		Πάροχοι δημόσια διαθέσιμων υπηρεσιών ηλεκτρονικών επικοινωνιών
Διαχείριση υπηρεσιών ΤΠΕ (μεταξύ επιχειρήσεων)		Πάροχοι διαχειριζόμενων υπηρεσιών
		Πάροχοι διαχειριζόμενων υπηρεσιών ασφαλείας
Οντότητες δημόσιας διοίκησης		Οντότητες δημόσιας διοίκησης όπως ορίζονται σύμφωνα με το άρθρο 14 παράγραφος 1 περίπτωση γ΄ του ν. 4270/2014
		Πρωτοβάθμιοι Ο.Τ.Α.
		Δευτεροβάθμιοι Ο.Τ.Α.
Διάστημα		Φορείς εκμετάλλευσης επίγειας υποδομής, ιδιοκτησίας, διαχείρισης και εκμετάλλευσης, οι οποίοι υποστηρίζουν την παροχή διαστημικών υπηρεσιών

ΑΛΛΟΙ ΚΡΙΣΙΜΟΙ ΤΟΜΕΙΣ

ΤΟΜΕΑΣ	ΥΠΟΤΟΜΕΑΣ	ΕΙΔΟΣ ΥΠΗΡΕΣΙΑΣ
Ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών		Ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών
Διαχείριση αποβλήτων		Διαχείριση αποβλήτων ως κύρια οικονομική δραστηριότητα
Παρασκευή, παραγωγή και διανομή χημικών προϊόντων		Παρασκευή ουσιών και διανομή ουσιών ή μειγμάτων όπως προβλέπεται από τον Κανονισμό (ΕΚ) 1907/2006
Παραγωγή, μεταποίηση και διανομή τροφίμων		Χονδρική διανομή και βιομηχανική παραγωγή και μεταποίηση τροφίμων.
Κατασκευαστικός τομέας	**Κατασκευή ιατροτεχνολογικών προϊόντων και κατασκευή in vitro διαγνωστικών ιατροτεχνολογικών προϊόντων**	Κατασκευή ιατροτεχνολογικών προϊόντων και κατασκευή in vitro διαγνωστικών ιατροτεχνολογικών προϊόντων
	Κατασκευή προϊόντων υπολογιστών, ηλεκτρονικών και οπτικών προϊόντων	Κατασκευή ηλεκτρονικών υπολογιστών, ηλεκτρονικών και οπτικών προϊόντων (NACE αναθ. 2 Γ / κλάδος 26)
	Κατασκευή ηλεκτρολογικού εξοπλισμού	(NACE αναθ. 2 Γ / κλάδος 27)
	Κατασκευή μηχανημάτων και ειδών εξοπλισμού π.δ.κ.α.	Κατασκευή μηχανημάτων και ειδών εξοπλισμού π.δ.κ.α. (NACE αναθ. 2 Γ / κλάδος 28)
	Κατασκευή μηχανοκίνητων οχημάτων, ρυμουλκούμενων και ημιρυμουλκούμενων οχημάτων	Κατασκευή μηχανοκίνητων οχημάτων, ρυμουλκούμενων και ημιρυμουλκούμενων οχημάτων (NACE αναθ. 2 Γ / κλάδος 29)
	Κατασκευή λοιπού εξοπλισμού μεταφορών	Κατασκευή λοιπού εξοπλισμού μεταφορών (NACE αναθ. 2 Γ / κλάδος 30)
Ψηφιακοί πάροχοι		Πάροχοι επιγραμμικών / διαδικτυακών αγορών
		Πάροχοι επιγραμμικών / διαδικτυακών μηχανών αναζήτησης
		Πάροχοι πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης
Έρευνα		Έρευνα

Τομείς δραστηριότητας που περιλαμβάνονταν στην Οδηγία NIS1

Νέοι τομείς δραστηριότητας που προστίθενται στην Οδηγία NIS2

ΝΕΕΣ ΡΥΘΜΙΣΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ NIS2: ΣΕ ΣΧΕΣΗ ΜΕ ΣΥΓΚΕΚΡΙΜΕΝΟΥΣ ΤΟΜΕΙΣ

Στο πλαίσιο του **άρθρου 4 της Οδηγίας NIS2**, προβλέπονται εξαιρέσεις στην εφαρμογή της, για **οντότητες οι οποίες αν και πληρούν τα γενικά κριτήρια** και υπάγονται στους τομείς όπως αναφέρθηκαν παραπάνω, **υπόκεινται ταυτόχρονα σε τομεακές νομικές πράξεις της Ένωσης**, οι οποίες επιβάλουν τουλάχιστον ισοδύναμες απαιτήσεις σχετικά με:

α) μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας **και**

β) άμεση πρόσβαση στις κοινοποιήσεις περιστατικών από τις CSIRT, τις αρμόδιες αρχές ή τα ενιαία σημεία επαφής και τις απαιτήσεις για την κοινοποίηση σημαντικών περιστατικών.

Κατά την τρέχουσα συγκυρία, παράδειγμα τομεακής νομικής πράξης της Ένωσης που εμπίπτει στην παραπάνω κατηγορία είναι ο Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (Digital Operational Resilience Act - DORA)[2].

Ο Κανονισμός DORA, ΕΦΑΡΜΟΖΕΤΑΙ στις ακόλουθες οντότητες:

α) πιστωτικά ιδρύματα
β) ιδρύματα πληρωμών, συμπεριλαμβανομένων των ιδρυμάτων πληρωμών που εξαιρούνται σύμφωνα με την Οδηγία (ΕΕ) 2015/2366
γ) παρόχους υπηρεσιών πληροφοριών λογαριασμού
δ) ιδρύματα ηλεκτρονικού χρήματος, συμπεριλαμβανομένων των ιδρυμάτων ηλεκτρονικού χρήματος που εξαιρούνται σύμφωνα με την οδηγία 2009/110/ΕΚ
ε) επιχειρήσεις επενδύσεων
στ) παρόχους υπηρεσιών κρυπτοστοιχείων που έχουν λάβει άδεια βάσει του κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τις αγορές κρυπτοστοιχείων και την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1093/2010 και (ΕΕ) αριθ. 1095/2010 και των οδηγιών 2013/36/ΕΕ και (ΕΕ) 2019/1937 («κανονισμός σχετικά με τις αγορές κρυπτοστοιχείων») και τους εκδότες ψηφιακών μαρκών με εγγύηση περιουσιακών στοιχείων
ζ) κεντρικά αποθετήρια τίτλων
η) κεντρικούς αντισυμβαλλομένους
θ) τόπους διαπραγμάτευσης
ι) αρχεία καταγραφής συναλλαγών
ια) διαχειριστές οργανισμών εναλλακτικών επενδύσεων
ιβ) εταιρείες διαχείρισης
ιγ) παρόχους υπηρεσιών αναφοράς δεδομένων
ιδ) ασφαλιστικές και αντασφαλιστικές επιχειρήσεις
ιε) ασφαλιστικούς διαμεσολαβητές, αντασφαλιστικούς διαμεσολαβητές και ασφαλιστικούς διαμεσολαβητές που ασκούν ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση
ιστ) ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών
ιζ) οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας
ιη) διαχειριστές δεικτών αναφοράς κρίσιμης σημασίας
ιθ) παρόχους υπηρεσιών συμμετοχικής χρηματοδότησης
κ) αρχεία καταγραφής τιτλοποιήσεων και τρίτους παρόχους υπηρεσιών ΤΠΕ.

2. https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32022R2554

Ενώ ΔΕΝ ΕΜΠΙΠΤΟΥΝ στο πεδίο εφαρμογής του Κανονισμού DORA οι ακόλουθες οντότητες:

α) διαχειριστές οργανισμών εναλλακτικών επενδύσεων, όπως αναφέρονται στο άρθρο 3 παράγραφος 2 της Οδηγίας 2011/61/ΕΕ

β) ασφαλιστικές και αντασφαλιστικές επιχειρήσεις, όπως αναφέρονται στο άρθρο 4 της Οδηγίας 2009/138/ΕΚ

γ) ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών που διαχειρίζονται συνταξιοδοτικά συστήματα τα οποία συνολικά δεν έχουν περισσότερα από 15 μέλη

δ) φυσικά ή νομικά πρόσωπα που εξαιρούνται σύμφωνα με τα άρθρα 2 και 3 της Οδηγίας 2014/65/ΕΕ

ε) ασφαλιστικοί διαμεσολαβητές, αντασφαλιστικοί διαμεσολαβητές και ασφαλιστικοί διαμεσολαβητές που ασκούν ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση που είναι πολύ μικρές επιχειρήσεις ή μικρές ή μεσαίες επιχειρήσεις

στ) γραφεία ταχυδρομικών επιταγών, όπως αναφέρονται στο άρθρο 2 παράγραφος 5 σημείο 3) της Οδηγίας 2013/36/ΕΕ.

ΝΕΕΣ ΡΥΘΜΙΣΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ NIS2: ΣΕ ΣΧΕΣΗ ΜΕ ΤΗΝ ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΤΩΝ ΟΝΤΟΤΗΤΩΝ

ΟΔΗΓΙΑ NIS1

Η Οδηγία NIS1, διαχώριζε τις οντότητες σε δύο βασικές κατηγορίες:

Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ) και
Πάροχους Ψηφιακών Υπηρεσιών (ΠΨΥ).

Συγκεκριμένα, σύμφωνα με τον Νόμο 4577/2018, που μετέφερε την Οδηγία NIS1 στην ελληνική νομοθεσία «**Φορέας εκμετάλλευσης βασικών υπηρεσιών**» νοείται η δημόσια ή ιδιωτική οντότητα που

- ανήκει στους τομείς δραστηριότητας Ενέργειας, Μεταφορών, Τραπεζών, Υποδομών χρηματοπιστωτικών αγορών, Υγείας, Προμήθειας και διανομής πόσιμου νερού και Ψηφιακής υποδομής.
- καλύπτει τα ακόλουθα κριτήρια

α) ο φορέας παρέχει υπηρεσία ουσιώδη για τη διατήρηση κρίσιμων κοινωνικών ή και οικονομικών δραστηριοτήτων,

β) η παροχή της υπηρεσίας αυτής στηρίζεται σε συστήματα δικτύου και πληροφοριών και

γ) υπάρχει δυνατότητα πρόκλησης σοβαρής διατάραξης της παροχής της εν λόγω υπηρεσίας, κατά τα οριζόμενα στο άρθρο 5, από τυχόν συμβάν κυβερνοασφάλειας

Ενώ

«**Πάροχος ψηφιακών υπηρεσιών**» νοείται το νομικό πρόσωπο που παρέχει ψηφιακή υπηρεσία όπως είναι οι υπηρεσίες επιγραμμικής αγοράς (online marketplace), επιγραμμική μηχανή αναζήτησης (online search engine) και νεφοϋπολογιστικής (cloud services).

ΟΔΗΓΙΑ NIS2

Στο πλαίσιο της διεύρυνσης του πεδίου εφαρμογής της οδηγίας, πλέον αναγνωρίζονται δύο κατηγορίες οντοτήτων που είναι εντός πεδίου εφαρμογής της Οδηγίας NIS2.

Βασικές Οντότητες

Α. Πρόκειται για οντότητες που καλύπτουν τις προϋποθέσεις μεγέθους και δραστηριοποίησης εντός της ελληνικής επικράτειας δηλαδή χαρακτηρίζονται **ως μεγάλες** επιχειρήσεις και **ασκούν δραστηριότητες** στους ακόλουθους τομείς:


Ενέργεια


Μεταφορές


Τράπεζες


Υποδομές χρηματοπιστωτικών αγορών


Υγεία


Πόσιμο νερό


Λύματα


Ψηφιακές υποδομές


Διαχείριση υπηρεσιών ΤΠΕ (μεταξύ επιχειρήσεων)


Διάστημα

Β. Ανεξαρτήτως μεγέθους, βασικές οντότητες αποτελούν οι:

β) πάροχοι υπηρεσιών εμπιστοσύνης και μητρώα ονομάτων τομέα ανωτάτου επιπέδου, καθώς και πάροχοι υπηρεσιών συστήματος ονομάτων τομέα (DNS)·

γ) πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών που χαρακτηρίζονται ως μεσαίες επιχειρήσεις, δυνάμει του παραρτήματος της Σύστασης της Επιτροπής 2003/361/ΕΚ·

δ) οντότητες δημόσιας διοίκησης που εντάσσονται στους φορείς της κεντρικής κυβέρνησης·

ε) οποιεσδήποτε άλλες οντότητες των τύπων που αναφέρονται στο παράρτημα Ι ή ΙΙ του ν. 5160/2024, οι οποίες προσδιορίζονται ως βασικές οντότητες λόγω της κρισιμότητάς τους·

στ) οντότητες που προσδιορίζονται ως κρίσιμες οντότητες βάσει της Οδηγίας (ΕΕ) 2022/2557·

ζ) οντότητες που αναγνωρίστηκαν, σύμφωνα με το ν. 4577/2018, ως φορείς εκμετάλλευσης βασικών υπηρεσιών.

Σημαντικές Οντότητες

Το σύνολο των οντοτήτων των τομέων που αναφέρονται στο παράρτημα Ι ή ΙΙ του ν. 5160/2024, οι οποίες δεν χαρακτηρίζονται ως βασικές οντότητες, θεωρούνται σημαντικές οντότητες.

Δηλαδή:

Α. Οι οντότητες που ανήκουν στους τομείς

Και

Β. όσες οντότητες δραστηριοποιούνται στους τομείς του Παραρτήματος Ι του ν. 5160/2024, αλλά δεν πληρούν την προϋπόθεση του μεγέθους δηλαδή δεν αποτελούν "μεγάλες επιχειρήσεις".

ΝΕΕΣ ΡΥΘΜΙΣΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ NIS2: ΑΛΛΕΣ ΔΙΑΦΟΡΕΣ

Άλλες διαφορές μεταξύ των Οδηγιών NIS1 και NIS2 αφορούν τα θέματα των **μέτρων ασφάλειας**, της **εποπτείας**, των **κυρώσεων** και των **ευθυνών**.

Συγκεκριμένα, για τα **μέτρα ασφάλειας**

Η **υπουργική απόφαση 1027/2019**, προέβλεπε την επιλογή και εφαρμογή αποτελεσματικών, αποδοτικών, κατάλληλων, αναλογικών, συγκεκριμένων και περιεκτικών μέτρων καλύπτοντας κατ' ελάχιστο τις ακόλουθες περιοχές:

- Ενιαία Πολιτική Ασφαλείας
- Επιχειρησιακό περιβάλλον
- Διαχείριση πόρων / πάγιων στοιχείων
- Αποτίμηση διακινδύνευσης
- Στρατηγική διαχείρισης διακινδύνευσης
- Διαχείριση διακινδύνευσης αλυσίδας εφοδιασμού
- Αυτοαξιολόγηση – Βελτίωση
- Διαχείριση ταυτότητας και έλεγχος πρόσβασης
- Φυσική και περιβαλλοντική ασφάλεια
- Ασφάλεια συστημάτων και εφαρμογών
- Ασφάλεια δεδομένων
- Αντίγραφα ασφαλείας
- Τεχνολογίες ασφάλειας
- Δοκιμές συστημάτων
- Διαχείριση Αλλαγών
- Ευαισθητοποίηση και κατάρτιση
- Ανίχνευση απειλών
- Διαχείριση Περιστατικών
- Επιχειρησιακή συνέχεια
- Ανάκαμψη από καταστροφές

Ενώ επίσης, ο κάθε οργανισμός όφειλε να ορίσει συγκεκριμένο εργαζόμενο ως Υπεύθυνο Ασφάλειας Πληροφοριών και Δικτύων.

Σύμφωνα με το **ν. 5160/2024** με τον οποίο μεταφέρθηκε η Οδηγία NIS2 στην ελληνική έννομη τάξη, τα μέτρα βασίζονται σε ολιστική προσέγγιση του κινδύνου που αποσκοπεί στην προστασία των συστημάτων δικτύου και πληροφοριακών συστημάτων και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από περιστατικά, δίνοντας έμφαση τουλάχιστον στα ακόλουθα:

α) πολιτικές και διαδικασίες για την ανάλυση κινδύνου και την ασφάλεια των πληροφοριακών συστημάτων, ενίσχυση της λογοδοσίας του ανώτατου οργάνου διοίκησης κάθε οντότητας για την εφαρμογή των σχετικών απαιτήσεων,
β) διαχείριση περιστατικών,
ω) επιχειρησιακή συνέχεια, όπως διαχείριση αντιγράφων ασφαλείας και αποκατάσταση έπειτα από καταστροφή, καθώς και διαχείριση των κρίσεων,
δ) ασφάλεια της αλυσίδας εφοδιασμού, συμπεριλαμβανομένων των σχετικών με την ασφάλεια πτυχών που αφορούν τις σχέσεις μεταξύ κάθε οντότητας και των άμεσων προμηθευτών ή παρόχων υπηρεσιών της,
ε) ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση συστημάτων δικτύου και πληροφοριακών συστημάτων, συμπεριλαμβανομένων του χειρισμού και της γνωστοποίησης ευπαθειών,
στ) πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας,
ζ) βασικές πρακτικές κυβερνοϋγιεινής και κατάρτιση στην κυβερνοασφάλεια,
η) πολιτικές και διαδικασίες σχετικά με τη χρήση κρυπτογραφίας και, κατά περίπτωση, κρυπτογράφησης, σε συνεργασία με την εθνική αρχή CRYPTO, όπου απαιτείται,
θ) ασφάλεια ανθρώπινων πόρων, πολιτικές ελέγχου πρόσβασης και διαχείριση πάγιων στοιχείων,
ι) χρήση λύσεων πολυπαραγοντικής επαλήθευσης ταυτότητας ή συνεχούς επαλήθευσης ταυτότητας, ασφαλών φωνητικών επικοινωνιών, επικοινωνιών βίντεο και κειμένου και ασφαλών συστημάτων επικοινωνιών έκτακτης ανάγκης εντός της οντότητας, κατά περίπτωση.

Επιπλέον, τίθενται συγκεκριμένες υποχρεώσεις για την απόδοση ρόλων και ευθυνών εντός κάθε οντότητας για τα θέματα κυβερνοασφάλειας. Οι οντότητες οφείλουν να:

α) Ορίζουν ένα αρμόδιο στέλεχός τους, ανάλογων προσόντων και εμπειρογνωμοσύνης**, ως Υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.),**

β) Τηρούν ενιαία πολιτική κυβερνοασφάλειας, στην οποία συμπεριλαμβάνεται το σύνολο των επιμέρους μέτρων, πολιτικών και διαδικασιών που αφορούν στα ελάχιστα τεχνικά και οργανωτικά μέτρα συμμόρφωσης. Σε περίπτωση τήρησης από τον φορέα επιμέρους καταγεγραμμένων πολιτικών και διαδικασιών, η ενιαία πολιτική κυβερνοασφάλειας παραπέμπει για τις επιμέρους λεπτομέρειες στις πολιτικές και διαδικασίες αυτές.

γ) Τηρούν συνολική καταγραφή των υλικών και άυλων πληροφοριακών και επικοινωνιακών αγαθών, τα οποία ιεραρχούνται βάσει της κρισιμότητάς τους.

ΓΙΑ ΤΗΝ ΕΠΟΠΤΕΙΑ

Σύμφωνα με την Οδηγία **NIS1** δινόταν η δυνατότητα στις εθνικές αρχές να καθορίσουν τον τρόπο άσκησης της εποπτείας σε εθνικό επίπεδο.

Η Οδηγία **NIS2**, προβλέπει ex-ante & ex-post εποπτεία για τις βασικές οντότητες και ex-post για τις σημαντικές οντότητες. Περισσότερες πληροφορίες σχετικά με την εποπτεία, μπορείτε να βρείτε στην ενότητα «Εποπτεία».

Για τις **κυρώσεις**

Σύμφωνα με την υπουργική απόφαση 1027/2019, μπορούσε να επιβληθεί:

α) Σύσταση προς τον Οργανισμό ή τον νόμιμο εκπρόσωπό του, σε περίπτωση που, κατόπιν διενέργειας ελέγχου συμβάντος ασφαλείας, αναγνωριστεί ότι δεν τηρούνται τα απαιτούμενα από το νόμο μέτρα ασφαλείας.

β) Επίπληξη προς τον Οργανισμό ή τον νόμιμο εκπρόσωπό τους, σε περίπτωση που κατόπιν διενέργειας ελέγχου συμβάντος ασφαλείας, αναγνωριστεί ότι παρά την πρότερη σύσταση της αρχής δεν συμμορφώθηκαν με τις υποδείξεις της ΕΑΚ.

γ) Στην περίπτωση μη συμμόρφωσης του Οργανισμού με την διαδικασία σύστασης ή επίπληξης, επιβάλλεται διοικητικό πρόστιμο στον Οργανισμό σύμφωνα με τις διατάξεις του άρθρου 15 του ν. 4577/2018 (Α΄ 199).

Ν. 5160/2024 ΓΙΑ ΤΗΝ ΜΕΤΑΦΟΡΑ ΤΗΣ ΟΔΗΓΙΑΣ NIS2

Παραβίαση των άρθρων 15 ή 16 » **πρόστιμο έως 10.000.000€**
(βασικές οντότητες)

ή κατ' ανώτατο όριο δύο τοις εκατό (2%) του κατά το προηγούμενο οικονομικό έτος συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκει η σημαντική οντότητα, ανάλογα με το ποιο είναι υψηλότερο.

Παραβίαση των άρθρων 15 ή 16 » **πρόστιμο έως 7.000.000€**
(σημαντικές οντότητες)

ή κατ' ανώτατο όριο ένα κόμμα τέσσερα τοις εκατό (1,4%) του κατά το προηγούμενο οικονομικό έτος συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκει η σημαντική οντότητα, ανάλογα με το ποιο είναι υψηλότερο.

Κλιμάκωση διοικητικών προστίμων » **πρόστιμο έως 1.000.000€**

για παράδειγμα: για την παράβαση εκ μέρους βασικών οντοτήτων δεσμευτικών οδηγιών και κατευθύνσεων, μεταξύ άλλων όσον αφορά τα μέτρα που είναι αναγκαία για την πρόληψη ή την αποκατάσταση περιστατικού επιβάλλεται πρόστιμο ύψους κατ' ανώτατο όριο ενός εκατομμυρίου (1.000.000) ευρώ ενώ για την παράβαση εκ μέρους σημαντικών οντοτήτων δεσμευτικών οδηγιών ή εντολών για την αποκατάσταση διαπιστωμένων ελλείψεων, κατ' ανώτατο όριο επτακοσίων χιλιάδων (700.000) ευρώ.

Διοικητικά πρόστιμα σε οντότητες δημόσιας διοίκησης » **πρόστιμο 20.000€-500.000€**

Παραβίαση παρ. 1 του άρθρου 14 » **πρόστιμο έως 200.000€**

Παραβίαση παρ. 2 του άρθρου 14 » **πρόστιμο έως 100.000€**

Παραβίαση του άρθρου 19 » **πρόστιμο έως 200.000€**

Παραβίαση του άρθρου 20 » **πρόστιμο έως 800.000€**

Παραβίαση παρ. 3 του άρθρου 21 » **πρόστιμο έως 100.000€**

Παραβίαση παρ. 2 και 4 του άρθρου 24 » **πρόστιμο έως 500.000€**

Παραβίαση παρ. 2 του άρθρου 25 » **πρόστιμο έως 350.000€**

Παραβίαση παρ. 6 του άρθρου 15 » **πρόστιμο έως 300.000€**

ΜΕΤΑΦΟΡΑ ΤΗΣ ΟΔΗΓΙΑΣ NIS2 ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΕΝΝΟΜΗ ΤΑΞΗ

Σύμφωνα με την Οδηγία NIS2, τα μέτρα που προβλέπονται σε αυτήν εφαρμόζονται από τις 18 Οκτωβρίου 2024. Η Ελλάδα συγκαταλέγεται μεταξύ των πρώτων κρατών μελών της Ε.Ε. που μετέφερε την Οδηγία NIS2 στο εθνικό της δίκαιο, με το ν. 5160/2024.

Το αντικείμενο του ν. 5160/2024 είναι:

α) ο καθορισμός του εθνικού συστήματος διακυβέρνησης, η εισαγωγή ρυθμίσεων για την Εθνική Στρατηγική Κυβερνοασφάλειας, ο ορισμός αρμόδιας αρχής για την κυβερνοασφάλεια και τη διαχείριση κυβερνοκρίσεων, ο ορισμός ενιαίου σημείου επαφής για την κυβερνοασφάλεια και ομάδων απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών [Computer Security Incident Response Team (CSIRT)],

β) ο καθορισμός των ελάχιστων, οριζόντιων μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και η επιβολή υποχρεώσεων υποβολής αναφορών για τις οντότητες που υπάγονται στο πεδίο εφαρμογής του νόμου,

γ) η πρόβλεψη κανόνων και υποχρεώσεων σχετικά με την συνεργασία και την ανταλλαγή πληροφοριών για την κυβερνοασφάλεια και

δ) η θέσπιση διατάξεων για την εν γένει εποπτεία και επιβολή μέτρων και κυρώσεων για την εφαρμογή του νόμου, έτσι ώστε να επιτυγχάνεται υψηλό επίπεδο κυβερνοασφάλειας στην Ελλάδα στο πλαίσιο του νόμου, των κανόνων και των στόχων της Οδηγίας NIS2.

Με την δημοσίευση του ν. 5160/2024 στην Εφημερίδα της Κυβέρνησης καταργούνται

α) τα άρθρα 148, περί ασφάλειας δικτύων και υπηρεσιών, και 149, περί εφαρμογής και επιβολής, του ν. 4727/2020 (Α' 184) και

β) τα άρθρα 1 έως 16 του ν. 4577/2018 (Α΄ 199), περί ενσωμάτωσης στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση.

Σε συνέχεια της ψήφισης του ν. 5160/2024, ακολουθεί η έκδοση σειράς αποφάσεων για την εξειδίκευση του περιεχομένου του και την αποτελεσματική εφαρμογή των προβλέψεών του.

ΣΗΜΑΝΤΙΚΟΤΕΡΕΣ ΑΠΟΦΑΣΕΙΣ

Αποφάσεις του Υπουργού Ψηφιακής Διακυβέρνησης

- Νέα Εθνική Στρατηγική Κυβερνοασφάλειας
- Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας (ΕΠΑΚ)
- Καθορισμός προσόντων, καθηκόντων, ασυμβιβάστων και υποχρεώσεων των Υπεύθυνων Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.)

Αποφάσεις του Διοικητή ΕΑΚ

- Εθνικό Σχέδιο Διαχείρισης Περιστατικών Μεγάλης κλίμακας και Κρίσεων στον Κυβερνοχώρο
- Εξειδίκευση ΕΠΑΚ (για βασικές και για σημαντικές οντότητες)
- Κανονισμός Ελέγχου και Εποπτείας της ΕΑΚ
- Πρότυπη Πολιτική Κυβερνοασφάλειας για βασικές και σημαντικές οντότητες
- Προϋποθέσεις χαρακτηρισμού ενός περιστατικού κυβερνοασφάλειας ως σημαντικού

ΕΥΘΥΝΕΣ ΚΑΙ ΡΟΛΟΣ ΤΗΣ ΑΝΩΤΑΤΗΣ ΔΙΟΙΚΗΣΗΣ

Η αποτελεσματική εφαρμογή και συμμόρφωση προς τις απαιτήσεις του ν. 5160/2024, απαιτεί την ενεργή συμμετοχή της ανώτατης διοίκησης του οργανισμού.

Ορισμός:

Με τον όρο ανώτατη διοίκηση, νοείται κάθε φυσικό πρόσωπο που, σύμφωνα με τις ισχύουσες νομοθετικές διατάξεις, είναι, κατά περίπτωση, υπεύθυνο ή ενεργεί ως νόμιμος εκπρόσωπος της οντότητας με βάση την εξουσία εκπροσώπησής της ή έχει την αρμοδιότητα να λαμβάνει αποφάσεις εξ ονόματός της ή να ασκεί τον έλεγχό της.

Η ανώτατη διοίκηση διατηρεί την ευθύνη για την επιλογή και εφαρμογή των μέτρων διαχείρισης κινδύνου, για την ενημέρωση σε σχέση με πιθανά περιστατικά ασφάλειας και την παροχή της πληροφόρησης που απαιτείται προς την Εθνική Αρχή Κυβερνοασφάλειας και τα λοιπά εμπλεκόμενα μέρη.

Τα μέλη της ανώτατης διοίκησης των βασικών και σημαντικών οντοτήτων οφείλουν να παρακολουθούν εκπαίδευση, η οποία θα τους δίνει γνώσεις και ικανότητες απαραίτητες για την αξιολόγηση, λήψη και παρακολούθηση των σχετικών τους αποφάσεων.

Αυτό δεν σημαίνει ότι τα μέλη της ανώτατης διοίκησης πρέπει να είναι ειδικοί στο χώρο της κυβερνοασφάλειας, αλλά ότι θα έχουν ικανές γνώσεις ώστε να μπορούν να συμμετέχουν στις απαραίτητες συζητήσεις, και να λαμβάνουν ενημερωμένες αποφάσεις.

Σύμφωνα με το ν. 5160/2024, προβλέπεται ότι με κοινή απόφαση των Υπουργών Ψηφιακής Διακυβέρνησης, Παιδείας, Θρησκευμάτων και Αθλητισμού και Εργασίας και Κοινωνικής Ασφάλισης που εκδίδεται μετά από πρόταση του Διοικητή της Εθνικής Αρχής Κυβερνοασφάλειας, καθορίζονται οι διαδικασίες, η διάρκεια εκπαίδευσης, τα προσόντα των εκπαιδευτών, το εκπαιδευτικό υλικό και κάθε άλλη λεπτομέρεια.

Επίσης, η ανώτατη διοίκηση των υπόχρεων οργανισμών οφείλει να προσφέρει παρόμοια κατάρτιση στους υπαλλήλους τους σε τακτική βάση, προκειμένου να αποκτούν επαρκείς γνώσεις και δεξιότητες που θα τους επιτρέπουν να εντοπίζουν τους κινδύνους καθώς και να αξιολογούν τις πρακτικές διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τον αντίκτυπό τους στις υπηρεσίες που παρέχει ο οργανισμός.

Αξίζει να σημειωθεί ότι σε περίπτωση που τα μέτρα επιβολής που θεσπίζονται από την Εθνική Αρχή Κυβερνοασφάλειας δεν είναι αποτελεσματικά ή ο οργανισμός δεν ανταποκριθεί αποτελεσματικά εντός προκαθορισμένου χρονικού διαστήματος, ο Διοικητής της Εθνικής Αρχής Κυβερνοασφάλειας δύναται με ειδικώς αιτιολογημένη απόφασή του να απαγορεύει προσωρινά σε κάθε φυσικό πρόσωπο που είναι υπεύθυνο για την άσκηση διευθυντικών καθηκόντων σε επίπεδο διευθύνοντος συμβούλου ή νόμιμου εκπροσώπου στη βασική οντότητα να ασκεί διευθυντικά καθήκοντα στην εν λόγω οντότητα.

Οι προσωρινές αναστολές ή απαγορεύσεις που επιβάλλονται εφαρμόζονται μόνο έως ότου η οικεία οντότητα λάβει τα αναγκαία μέτρα για να διορθώσει τις ελλείψεις ή να συμμορφωθεί με τις απαιτήσεις της ως άνω αρμόδιας αρχής για τις οποίες εφαρμόστηκαν τέτοια μέτρα επιβολής.

Η ανώτατη διοίκηση των υπόχρεων οργανισμών,

- ✓ **εγκρίνει** τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που λαμβάνουν οι εν λόγω οντότητες
- ✓ **επιβλέπει** την εφαρμογή τους και
- ✓ **λογοδοτεί** για την εκ μέρους των οντοτήτων παραβίαση των υποχρεώσεων

Ενώ επιπλέον, οφείλει να ορίσει υπάλληλο της οντότητας ως Υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών, με τα ακόλουθα καθήκοντα:

- ✓ **Αποτελεί το σημείο επαφής** και συνεργάζεται με την Εθνική Αρχή Κυβερνοασφάλειας και το αρμόδιο CSIRT.
- ✓ **Συντονίζει και επιβλέπει** τη συμμόρφωση της οντότητας, ως προς την τήρηση των υποχρεώσεων που απορρέουν την σχετική νομοθεσία και του ενωσιακού ή του εθνικού δικαίου 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.
- ✓ Τη **σύνταξη της αναφοράς αυτοαξιολόγησης** του Οργανισμού που αποστέλλεται στην Εθνική Αρχή Κυβερνοσφάλειας, καθώς και τις σχετικές άλλες απαιτήσεις όπως ζητούνται.
- ✓ **Παρίσταται 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.

Ο ρόλος του στην οργανωτική δομή του Οργανισμού πρέπει να είναι ανεξάρτητος και να μην έγκειται σε σύγκρουση συμφερόντων με άλλους εργασιακούς ρόλους που τυχόν κατέχει. Κάθε Οργανισμός οφείλει αμελλητί να κοινοποιεί στην Εθνική Αρχή Κυβερνοασφάλειας τα στοιχεία επικοινωνίας του εκάστοτε Υπευθύνου που έχει οριστεί.

ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΩΝ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Οι υπόχρεοι οργανισμοί οφείλουν να λαμβάνουν κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά στην ασφάλεια συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν για τις δραστηριότητές τους ή για την παροχή των υπηρεσιών τους, καθώς και για την πρόληψη ή ελαχιστοποίηση των επιπτώσεων των περιστατικών στους αποδέκτες των υπηρεσιών τους ή σε άλλες υπηρεσίες και Οργανισμούς.

Στην επιλογή των μέτρων αυτών θα πρέπει να λαμβάνονται υπόψη

- Οι ελάχιστες απαιτήσεις της νομοθεσίας, των σχετικών αποφάσεων και συστάσεων της Εθνικής Αρχής Κυβερνοασφάλειας,
- οι κατευθύνσεις που παρέχονται από τις εφαρμοστικές πράξεις της Ευρωπαϊκής Επιτροπής,
- τα πιο σύγχρονα κατά περίπτωση, σχετικά εθνικά, ευρωπαϊκά και διεθνή πρότυπα,
- το κόστος εφαρμογής,
- η αρχή της αναλογικότητας,
- το μέγεθος του οργανισμού,
- πιθανότητα εμφάνισης περιστατικών και η σοβαρότητά τους, συμπεριλαμβανομένων των κοινωνικών και οικονομικών επιπτώσεών τους,
- ο βαθμός έκθεσης του οργανισμού σε κινδύνους,
- τα αποτελέσματα των συντονισμένων εκτιμήσεων κινδύνου των κρίσιμων αλυσίδων εφοδιασμού που διενεργούνται σύμφωνα με την Οδηγία NIS2 και
- οι ευπάθειες που χαρακτηρίζουν κάθε άμεσο προμηθευτή και πάροχο υπηρεσιών και η συνολική ποιότητα των προϊόντων και των πρακτικών κυβερνοασφάλειας των προμηθευτών και των παρόχων υπηρεσιών τους.

Τα μέτρα βασίζονται σε ολιστική προσέγγιση του κινδύνου που αποσκοπεί στην προστασία των συστημάτων δικτύου και πληροφοριών και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από περιστατικά κυβερνοασφάλειας και περιλαμβάνουν τουλάχιστον τα ακόλουθα:

α) πολιτικές για την ανάλυση κινδύνου και την ασφάλεια των πληροφοριακών συστημάτων·

β) διαχείριση περιστατικών

γ) επιχειρησιακή συνέχεια, όπως τήρηση αντικράφων ασφαλείας και αποκατάσταση έπειτα από καταστροφή, και διαχείριση των κρίσεων

δ) ασφάλεια της αλυσίδας εφοδιασμού, συμπεριλαμβανομένων των σχετικών με την ασφάλεια πτυχών που αφορούν τις σχέσεις μεταξύ κάθε οντότητας και των άμεσων προμηθευτών ή παρόχων υπηρεσιών της·

ε) ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένου του χειρισμού και της γνωστοποίησης ευπαθειών

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

ζ) βασικές πρακτικές κυβερνοϋγιεινής και κατάρτιση στην κυβερνοασφάλεια

η) πολιτικές και διαδικασίες σχετικά με τη χρήση κρυπτογραφίας και, κατά περίπτωση, κρυπτογράφησης

θ) ασφάλεια ανθρώπινων πόρων, πολιτικές ελέγχου πρόσβασης και διαχείριση πάγιων στοιχείων

ι) χρήση λύσεων πολυπαραγοντικής επαλήθευσης ταυτότητας ή συνεχούς επαλήθευσης ταυτότητας, ασφαλών φωνητικών επικοινωνιών, επικοινωνιών βίντεο και κειμένου και ασφαλών συστημάτων επικοινωνιών έκτακτης ανάγκης εντός της οντότητας, κατά περίπτωση.

ΑΥΤΟΑΞΙΟΛΟΓΗΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Η εθνική αρχή κυβερνοασφάλειας, έχει εκδώσει και δημοσιεύσει, Οδηγό αυτοαξιολόγησης της κυβερνοασφάλειας οργανισμών (CYBERSECURITY SELF ASSESSMENT TOOL).

Ο Οδηγός αποτελεί ένα μηχανισμό με τον οποίο οι οργανισμοί μπορούν να διενεργήσουν αυτοαξιολόγηση του επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών τους.

Ο Οδηγός περιέχει συνολικά 236 σημεία ελέγχου χωρισμένα σε 19 θεματικές ενότητες, οι οποίες είναι οι εξής:

1. Διοίκηση κυβερνοασφάλειας και διαχείριση επικινδυνότητας
2. Καταγραφή υλικού και λογισμικού
3. Ασφαλής παραμετροποίηση εξοπλισμού και εφαρμογών
4. Έλεγχος εκτέλεσης προγραμμάτων και υπηρεσιών
5. Διαχείριση λογαριασμών και έλεγχος πρόσβασης
6. Αυθεντικοποίηση χρηστών
7. Ασφάλεια δικτύων
8. Προστασία από κακόβουλο λογισμικό
9. Τήρηση και ανάλυση αρχείων καταγραφής συμβάντων (event logs)
10. Ασφάλεια διαδικτυακών εφαρμογών
11. Απομακρυσμένη εργασία
12. Χρήση κρυπτογραφίας
13. Εκπαίδευση και ευαισθητοποίηση σε θέματα κυβερνοασφάλειας
14. Διαχείριση κινδύνων στην εφοδιαστική αλυσίδα
15. Υλοποίηση τεχνικών ελέγχων κυβερνοασφάλειας
16. Μέτρα φυσικής ασφάλειας εγκαταστάσεων
17. Λήψη αντιγράφων ασφαλείας (backup)
18. Αντιμετώπιση περιστατικών κυβερνοασφάλειας
19. Διασφάλιση επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή

Ο Οδηγός μπορεί να χρησιμοποιηθεί:

- ✓ **από τις υπόχρεες οντότητες για να κατανοήσουν τις απαιτήσεις** σε σχέση με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας,

- ✓ **από τις υπόχρεες οντότητες για να αξιολογήσουν το βαθμό υλοποίησης των μέτρων** διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας,

- ✓ **ως υποστηρικτικό εργαλείο** κατά τη διενέργεια των ελέγχων ασφάλειας και επιθεωρήσεων,

- ✓ **από οποιοδήποτε άλλο οργανισμό** (ακόμα και εκτός πεδίου εφαρμογής του ν. 5160/2024) προκειμένου να εντοπίσει, σε ποιο σημείο βρίσκεται σε σχέση με βέλτιστες πρακτικές στον τομέα της κυβερνοασφάλειας.

ΠΕΡΙΣΤΑΤΙΚΑ ΑΣΦΑΛΕΙΑΣ

Ως περιστατικό νοείται κάθε συμβάν που θέτει σε κίνδυνο τη διαθεσιμότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω συστημάτων δικτύου και πληροφοριακών συστημάτων.

Ένα περιστατικό θεωρείται σημαντικό αν:

α) έχει προκαλέσει ή μπορεί να προκαλέσει σοβαρή λειτουργική διατάραξη των υπηρεσιών ή οικονομική ζημία για την οικεία οντότητα,

β) έχει επηρεάσει ή μπορεί να επηρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία.

Παράδειγμα:

Σημαντικά περιστατικά όσον αφορά στους παρόχους υπηρεσιών κέντρων δεδομένων (Data Centre)

Όσον αφορά στους παρόχους υπηρεσιών κέντρου δεδομένων, ένα περιστατικό θεωρείται σημαντικό όταν πληροί ένα ή περισσότερα από τα ακόλουθα κριτήρια:

| Α |
μια υπηρεσία κέντρου δεδομένων που διαχειρίζεται ο πάροχος είναι πλήρως μη διαθέσιμη

| Β |
η διαθεσιμότητα μιας υπηρεσίας κέντρου δεδομένων που διαχειρίζεται ο πάροχος είναι περιορισμένη για διάρκεια μεγαλύτερη της μίας ώρας

| Γ |
διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή μιας υπηρεσίας κέντρου δεδομένων ως αποτέλεσμα μιας ύποπτα κακόβουλης ενέργειας

| Δ |
διακυβεύεται η φυσική πρόσβαση σε κέντρο δεδομένων που διαχειρίζεται ο πάροχος.

ΑΝΑΦΟΡΑ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Κάθε περιστατικό που έχει σημαντικό αντίκτυπο στην παροχή των υπηρεσιών των βασικών και σημαντικών οντοτήτων, πρέπει να κοινοποιείται άμεσα στην Εθνική Αρχή Κυβερνοασφάλειας.

Η κοινοποίηση αυτή, πρέπει να γίνεται από τις οντότητες ως εξής:

Α

Έγκαιρη προειδοποίηση:

χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός είκοσι τεσσάρων (24) ωρών από τη στιγμή που αντιλήφθηκαν το σημαντικό περιστατικό, η οποία, κατά περίπτωση, αναφέρει αν υπάρχει υποψία ότι το σημαντικό περιστατικό προκλήθηκε από παράνομες ή κακόβουλες ενέργειες ή θα μπορούσε να έχει διασυνοριακό αντίκτυπο.

Β

Κοινοποίηση περιστατικού:

χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός εβδομήντα δύο (72) ωρών από τη στιγμή που αντιλήφθηκαν το σημαντικό περιστατικό, η οποία, κατά περίπτωση, επικαιροποιεί τις πληροφορίες και, επιπλέον, περιλαμβάνει μια αρχική αξιολόγηση του σημαντικού περιστατικού, μεταξύ άλλων της σοβαρότητας και των επιπτώσεών του, καθώς και, εφόσον υπάρχουν, τις ενδείξεις της παραβίασης.

Γ

Ενδιάμεση έκθεση:

κατόπιν αιτήματος της Εθνικής Αρχής Κυβερνοασφάλειας, σχετικά με τις επικαιροποιήσεις της κατάστασης.

Δ

Τελική έκθεση:

το αργότερο εντός ενός (1) μήνα μετά από την υποβολή της κοινοποίησης περιστατικού ή το "κλείσιμο" του περιστατικού.

ΕΠΟΠΤΕΙΑ

Η Εθνική Αρχή Κυβερνοασφάλειας είναι η αρμόδια αρχή εποπτείας και ελέγχου για τη συμμόρφωση με τις διατάξεις του του ν. 5160/2024 και ασκεί εποπτεία και έλεγχο σύμφωνα με τα άρθρα 23, 24 και 25 του ίδιου νόμου.

Οι βασικές οντότητες υπόκεινται σε πλήρες εκ των προτέρων και εκ των υστέρων καθεστώς εποπτείας, ενώ οι σημαντικές οντότητες υπόκεινται σε απλοποιημένο, μόνο εκ των υστέρων, εποπτικό καθεστώς.

Εκ των προτέρων (**ex ante**) εποπτικό καθεστώς εννοείται ο έλεγχος και εποπτεία που πραγματοποιείται περιοδικά ή εκτάκτως, χωρίς να έχει λάβει χώρα περιστατικό κυβερνοασφάλειας. Εκ των υστέρων (**ex post**) εποπτικό καθεστώς, εννοείται ο έλεγχος και εποπτεία που πραγματοποιείται μετά την εκδήλωση περιστατικού. Κατά τους ελέγχους (**ex post και ex ante**), παρέχονται αποδεικτικά στοιχεία, ενδείξεις ή πληροφορίες από την οικεία οντότητα από τα οποία αποδεικνύεται η συμμόρφωσή της με τις απαιτήσεις, ιδίως των άρθρων 15 και 16 του ν. 5160/2024. (αρχή της λογοδοσίας)

ΒΑΣΙΚΕΣ ΟΝΤΟΤΗΤΕΣ	ΣΗΜΑΝΤΙΚΕΣ ΟΝΤΟΤΗΤΕΣ
επιτόπιες επιθεωρήσεις και εποπτεία εκτός των εγκαταστάσεων, συμπεριλαμβανομένων δειγματοληπτικών ελέγχων, που διεξάγονται από τους επιθεωρητές	επιτόπιες επιθεωρήσεις και κατασταλτική εποπτεία εντός και εκτός των εγκαταστάσεων
τακτικοί και στοχευμένοι έλεγχοι ασφάλειας που διενεργούνται από την Εθνική Αρχή Κυβερνοασφάλειας,	στοχευμένοι έλεγχοι ασφάλειας που διενεργούνται από την Εθνική Αρχή Κυβερνοασφάλειας
έκτακτοι ειδικοί έλεγχοι	σαρώσεις ασφαλείας βάσει αντικειμενικών, αμερόληπτων, δίκαιων και διαφανών κριτηρίων αξιολόγησης του κινδύνου
σαρώσεις ασφαλείας βάσει αντικειμενικών, αμερόληπτων, δίκαιων και διαφανών κριτηρίων αξιολόγησης του κινδύνου	αιτήματα παροχής αναγκαίων πληροφοριών για την αξιολόγηση των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που λαμβάνει η οικεία οντότητα
αιτήματα παροχής αναγκαίων πληροφοριών για την εκ των υστέρων αξιολόγηση των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που λαμβάνει η οικεία οντότητα	αιτήματα για πρόσβαση σε δεδομένα, έγγραφα ή πληροφορίες που είναι αναγκαίες για την εκτέλεση των εποπτικών καθηκόντων
αιτήματα πρόσβασης σε δεδομένα, έγγραφα και πληροφορίες που απαιτούνται για την εκτέλεση των εποπτικών καθηκόντων	αιτήματα για αποδεικτικά στοιχεία που αφορούν στην εφαρμογή των πολιτικών κυβερνοασφάλειας
αιτήματα για αποδεικτικά στοιχεία που αφορούν στην εφαρμογή των πολιτικών κυβερνοασφάλειας	

ΚΥΡΩΣΕΙΣ

Η Εθνική Αρχή Κυβερνοασφάλειας είναι η αρμόδια αρχή εποπτείας και ελέγχου για τη συμμόρφωση με τις υποχρεώσεις του ν. 5160/2024, διαθέτοντας όλα τα αναγκαία μέσα.

| Α |
εκδίδει προειδοποιήσεις σχετικά με παραβιάσεις από τις οικείες οντότητες

| Β |
εκδίδει δεσμευτικές οδηγίες και κατευθύνσεις, μεταξύ άλλων όσον αφορά στα μέτρα που είναι αναγκαία για την πρόληψη ή την αποκατάσταση περιστατικού, και τάσσει προθεσμίες για την εφαρμογή των εν λόγω μέτρων και για την υποβολή εκθέσεων σχετικά με την εφαρμογή τους, ή εντέλλει τις οικείες οντότητες να αποκαταστήσουν τις ελλείψεις ή τις παραβιάσεις που εντοπίστηκαν

| Γ |
εντέλλει τις οικείες οντότητες να παύσουν συμπεριφορά που παραβιάζει τις απαιτήσεις και να απόσχουν από την επανάληψη της εν λόγω συμπεριφοράς

| Δ |
εντέλλει τις οικείες οντότητες να διασφαλίσουν ότι τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας εναρμονίζονται με το άρθρο 15 ή να εκπληρώσουν τις υποχρεώσεις υποβολής εκθέσεων που ορίζονται στο άρθρο 16, με συγκεκριμένο τρόπο και εντός ορισμένου χρονικού διαστήματος

| Ε |
εντέλλει τις οικείες οντότητες να ενημερώσουν τα φυσικά ή νομικά πρόσωπα, σε σχέση με τα οποία παρέχουν υπηρεσίες ή ασκούν δραστηριότητες που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή, σχετικά με τη φύση της απειλής, καθώς και σχετικά με τυχόν μέτρα προστασίας ή αποκατάστασης που μπορούν να λάβουν τα εν λόγω φυσικά ή νομικά πρόσωπα για την αντιμετώπιση της εν λόγω απειλής

| ΣΤ |
εντέλλει τις οικείες οντότητες να εφαρμόσουν τις συστάσεις που διατυπώθηκαν ως αποτέλεσμα ελέγχου ασφάλειας εντός εύλογης προθεσμίας

| Ζ |*
ορίζει αρμόδιο επιβλέποντα με σαφώς καθορισμένα καθήκοντα για καθορισμένο χρονικό διάστημα, προκειμένου να επιβλέπει τη συμμόρφωση των οικείων οντοτήτων με τα άρθρα 15 και 16

* Ισχύει για βασικές οντότητες.

| Η |
εντέλλει τις οικείες οντότητες να δημοσιοποιούν στοιχεία των παραβιάσεων με συγκεκριμένο τρόπο και διαδικασία

| Θ |
επιπλέον των λοιπών μέτρων, επιβάλλει διοικητικά πρόστιμα

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης

NIS2: Η Οδηγία NIS2 στην Ελλάδα

2024

Επικοινωνία

email: nis2info@cyber.gov.gr

EXPERTISE FRANCE
GROUPE AFD

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης