ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

Αρχή Ψηφιακής Ασφάλειας

ΣΥΝΟΠΤΙΚΟΣ ΟΔΗΓΟΣ ΑΝΑΦΟΡΙΚΑ ΜΕ ΤΗΝ ΟΔΗΓΙΑ NIS2

2024

dsa.cy

ΕΙΣΑΓΩΓΗ
NIS 2

Η Οδηγία (ΕΕ) 2022/2555, γνωστή και ως Οδηγία NIS2 επιδιώκει να ενισχύσει περαιτέρω το έργο που ξεκίνησε η Οδηγία NIS αναφορικά με τη δημιουργία ενός υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ευρωπαϊκή Ένωση.

Η Οδηγία NIS2 δημιουργεί υποχρεώσεις στα κράτη-μέλη καθώς και σε συγκεκριμένες οντότητες που δραστηριοποιούνται σε κρίσιμους τομείς όπως αυτοί ορίζονται στα παραρτήματα της Οδηγίας NIS2.

Ευχαριστούμε θερμά το NCSC της Ιρλανδίας για την παραχώρηση άδειας χρήσης του “NIS2 Reference Guide”

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ
Αρχή Ψηφιακής Ασφάλειας

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

Η ΟΔΗΓΙΑ **NIS 2** ΕΣΤΙΑΖΕΙ ΣΕ ΤΡΕΙΣ ΒΑΣΙΚΟΥΣ ΠΥΛΩΝΕΣ

ΥΠΟΧΡΕΩΣΕΙΣ ΚΡΑΤΩΝ ΜΕΛΩΝ

- Εθνικές Αρχές
- Εθνικές Στρατηγικές
- Συντονισμένη Γνωστοποίηση Ευπαθειών (CVD - Coordinated Vulnerability Disclosure)
- Πλαίσιο για τη Διαχείριση Κρίσεων

ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ

- Λογοδοσία της Ανώτατης Διοίκησης για μη συμμόρφωση
- Οι Βασικές και οι Σημαντικές Οντότητες οφείλουν να λαμβάνουν Μέτρα Ασφάλειας
- Οι Οντότητες οφείλουν να κοινοποιούν περιστατικά εντός συγκεκριμένου χρονικού πλαισίου

ΣΥΝΕΡΓΑΣΙΑ ΚΑΙ ΑΝΤΑΛΛΑΓΗ ΠΛΗΡΟΦΟΡΙΩΝ

- Ομάδα Συνεργασίας
- Δίκτυο CSIRTs – Computer Security Incident Response Teams
- CyCLONe – Cyber Crisis Liaison Organisations Network
- CVD και Ευρωπαϊκή Βάση Δεδομένων Ευπαθειών
- Αξιολογήσεις από Ομότιμους (Peer Reviews)
- Διετής Έκθεση του ENISA για την Κυβερνοασφάλεια

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

ΑΛΛΑΓΕΣ ΣΤΗΝ ΟΔΗΓΙΑ

NIS 2

1. Περισσότεροι Τομείς
2. Περισσότερες Οντότητες
3. Νέες Μέθοδοι Επιλογής Και Εγγραφής
4. Νέες Προθεσμίες Κοινοποίησης Περιστατικών
5. Πρόσθετες Απαιτήσεις

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. Βασικές και Σημαντικές Οντότητες
2. Τομείς στο Πεδίο Εφαρμογής
3. Κοινοποίηση Περιστατικών
4. Μέτρα Διαχείρισης Κινδύνων Κυβερνοασφάλειας
5. Βασικές και Σημαντικές Οντότητες – Εποπτεία
6. Εφαρμογή και Κυρώσεις
7. Ευθύνες της Διοίκησης

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

1.

ΒΑΣΙΚΕΣ ΚΑΙ ΣΗΜΑΝΤΙΚΕΣ ΟΝΤΟΤΗΤΕΣ

ΟΙ ΟΝΤΟΤΗΤΕΣ ΚΑΤΗΓΟΡΙΟΠΟΙΟΥΝΤΑΙ ΣΕ «ΒΑΣΙΚΕΣ» Ή «ΣΗΜΑΝΤΙΚΕΣ» ΒΑΣΕΙ ΚΡΙΤΗΡΙΩΝ ΟΠΩΣ ΤΟ ΜΕΓΕΘΟΣ, Ο ΤΟΜΕΑΣ ΚΑΙ Η ΚΡΙΣΙΜΟΤΗΤΑ.

Σημειώσεις:

• Οι Οντότητες που ορίζονται ως Κρίσιμες οντότητες βάσει της Οδηγίας (ΕΕ) 2022/2557 (Οδηγία CER) θα θεωρούνται αυτομάτως ως Βασικές Οντότητες κάτω από την Οδηγία NIS2.

• Όπου τομεακές νομικές πράξεις κρίνονται τουλάχιστον ισάξιες με την Οδηγία NIS2, δύναται να ισχύει το lex specialis.

• Στους πίνακες που ακολουθούν, υπάρχουν μερικές εξαιρέσεις για μικρές οντότητες των οποίων η διατάραξη μπορεί να επιφέρει σημαντικό αντίκτυπο στην κοινωνία, η συστημικό κίνδυνο, ή κρίνονται κρίσιμες για κάποιο λόγο. Για τέτοιες περιπτώσεις, θα ισχύουν οι ανάλογες εξαιρέσεις (βλ. κείμενο Οδηγίας NIS2 – Άρθρο 2 – για περισσότερες λεπτομέρειες).

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

1. ΒΑΣΙΚΕΣ & ΣΗΜΑΝΤΙΚΕΣ ΟΝΤΟΤΗΤΕΣ

ΠΑΡΑΡΤΗΜΑ Ι: ΤΟΜΕΙΣ ΥΨΗΛΗΣ ΚΡΙΣΙΜΟΤΗΤΑΣ

ΤΟΜΕΑΣ	ΥΠΟΤΟΜΕΑΣ	ΜΕΓΑΛΕΣ ΟΝΤΟΤΗΤΕΣ >= 250 εργαζόμενοι ή περισσότερο από €50 Εκατ. κύκλο εργασιών	ΜΕΣΑΙΕΣ ΟΝΤΟΤΗΤΕΣ 50-249 εργαζόμενοι ή περισσότερο από €10 εκατ. κύκλο εργασιών	ΜΙΚΡΕΣ & ΠΟΛΥ ΜΙΚΡΕΣ ΟΝΤΟΤΗΤΕΣ < 50 εργαζόμενοι ή λιγότερο από €10 εκατ. κύκλο εργασιών
Ενέργεια	Ηλεκτρική ενέργεια, τηλεθέρμανση και τηλεψύξη, φυσικό αέριο, υδρογόνο, πετρέλαιο. Συμπεριλαμβανομένων των παρόχων υπηρεσιών επαναφόρτισης σε τελικούς χρήστες.	Βασικές	Σημαντικές	Εκτός πεδίου εφαρμογής
Μεταφορές	Αερομεταφορές (εμπορικές, αερολιμένες, έλεγχος εναέριας κυκλοφορίας), σιδηροδρομικές μεταφορές (υποδομές και επιχειρήσεις), πλωτές μεταφορές (εταιρείες μεταφορών, λιμάνια, υπηρεσίες εξυπηρέτησης κυκλοφορίας πλοίων (VTS)), οδικές μεταφορές. *Ειδική κατηγορία: Δημόσιες μεταφορές: μόνο εάν ορίζονται στην Οδηγία (ΕΕ) 2022/2557 (CER Directive)	Βασικές	Σημαντικές	Εκτός πεδίου εφαρμογής
Τράπεζες	Πιστωτικά ιδρύματα (προσοχή: ο Κανονισμός DORA αποτελεί lex specialis)	Βασικές	Σημαντικές	Εκτός πεδίου εφαρμογής
Υποδομές Χρηματοπιστωτικών Αγορών	Τόποι διαπραγμάτευσης, κεντρικοί αντισυμβαλλόμενοι (προσοχή: ο Κανονισμός DORA αποτελεί lex specialis)	Βασικές	Σημαντικές	Εκτός πεδίου εφαρμογής

*Ενδέχεται να υπάρξουν διαφοροποιήσεις στον πίνακα κατά τη διεξαγωγή του έργου αξιολόγησης κρισιμότητας

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

1. ΒΑΣΙΚΕΣ & ΣΗΜΑΝΤΙΚΕΣ ΟΝΤΟΤΗΤΕΣ

ΤΟΜΕΑΣ	ΥΠΟΤΟΜΕΑΣ	ΜΕΓΑΛΕΣ ΟΝΤΟΤΗΤΕΣ >= 250 εργαζόμενοι ή περισσότερο από €50 Εκατ. κύκλο εργασιών	ΜΕΣΑΙΕΣ ΟΝΤΟΤΗΤΕΣ 50-249 εργαζόμενοι ή περισσότερο από €10 εκατ. κύκλο εργασιών	ΜΙΚΡΕΣ & ΠΟΛΥ ΜΙΚΡΕΣ ΟΝΤΟΤΗΤΕΣ < 50 εργαζόμενοι ή λιγότερο από €10 εκατ. κύκλο εργασιών
Υγεία	Πάροχοι υγειονομικής περίθαλψης, εργαστήρια αναφοράς της ΕΕ, έρευνα και ανάπτυξη για φάρμακα, παρασκευή βασικών φαρμακευτικών προϊόντων και παρασκευασμάτων, κατασκευή ιατροτεχνολογικών προϊόντων κρίσιμης σημασίας κατά τη διάρκεια έκτακτης ανάγκης στον τομέα της δημόσιας υγείας.	Βασικές	Σημαντικές	Εκτός πεδίου εφαρμογής
Πόσιμο Νερό	Προμηθευτές και διανομείς νερού ανθρώπινης κατανάλωσης	Βασικές	Σημαντικές	Εκτός πεδίου εφαρμογής
Λύματα	Επιχειρήσεις συλλογής, διάθεσης ή επεξεργασίας αστικών, οικιακών ή βιομηχανικών λυμάτων (Μόνο εάν αποτελεί ουσιώδες μέρος της γενικής δραστηριότητάς τους)	Βασικές	Σημαντικές	Εκτός πεδίου εφαρμογής

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

1. ΒΑΣΙΚΕΣ & ΣΗΜΑΝΤΙΚΕΣ ΟΝΤΟΤΗΤΕΣ

ΤΟΜΕΑΣ	ΥΠΟΤΟΜΕΑΣ	ΜΕΓΑΛΕΣ ΟΝΤΟΤΗΤΕΣ >= 250 εργαζόμενοι ή περισσότερο από €50 Εκατ. κύκλο εργασιών	ΜΕΣΑΙΕΣ ΟΝΤΟΤΗΤΕΣ 50-249 εργαζόμενοι ή περισσότερο από €10 εκατ. κύκλο εργασιών	ΜΙΚΡΕΣ & ΠΟΛΥ ΜΙΚΡΕΣ ΟΝΤΟΤΗΤΕΣ < 50 εργαζόμενοι ή λιγότερο από €10 εκατ. κύκλο εργασιών
Ψηφιακές υποδομές	Παρόχοι υπηρεσιών εμπιστοσύνης (qualified)	Βασικές	Βασικές	Βασικές
	Πάροχοι υπηρεσιών DNS (εξαιρουμένων των διαχειριστών των εξυπηρετητών ονομάτων ρίζας)	Βασικές	Βασικές	Βασικές
	Μητρώα ονομάτων τομέα ανώτατου επιπέδου - TLD	Βασικές	Βασικές	Βασικές
	Πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών	Βασικές	Βασικές	Σημαντικές
	Πάροχοι υπηρεσιών εμπιστοσύνης (non-qualified)	Βασικές	Σημαντικές	Σημαντικές
	Πάροχοι υπηρεσιών υπολογιστικού νέφους	Βασικές	Σημαντικές	Εκτός πεδίου εφαρμογής
	Πάροχοι υπηρεσιών κέντρου δεδομένων	Βασικές	Σημαντικές	Εκτός πεδίου εφαρμογής
	Πάροχοι σημείων ανταλλαγής κίνησης διαδικτύου	Βασικές	Σημαντικές	Εκτός πεδίου εφαρμογής
	Πάροχοι δικτύων διανομής περιεχομένου	Βασικές	Σημαντικές	Εκτός πεδίου εφαρμογής

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

1. ΒΑΣΙΚΕΣ & ΣΗΜΑΝΤΙΚΕΣ ΟΝΤΟΤΗΤΕΣ

ΤΟΜΕΑΣ	ΥΠΟΤΟΜΕΑΣ	ΜΕΓΑΛΕΣ ΟΝΤΟΤΗΤΕΣ >= 250 εργαζόμενοι ή περισσότερο από 50 Εκατ. κύκλο εργασιών	ΜΕΣΑΙΕΣ ΟΝΤΟΤΗΤΕΣ 50-249 εργαζόμενοι ή περισσότερο από 10 εκατ. κύκλο εργασιών	ΜΙΚΡΕΣ & ΠΟΛΥ ΜΙΚΡΕΣ ΟΝΤΟΤΗΤΕΣ < 50 εργαζόμενοι ή λιγότερο από €10 εκατ. κύκλο εργασιών
Διαχείριση υπηρεσιών ΤΠΕ (μεταξύ επιχειρήσεων B2B)	Πάροχοι διαχειριζόμενων υπηρεσιών	Βασικές	Σημαντικές	Εκτός πεδίου εφαρμογής
	Πάροχοι διαχειριζόμενων υπηρεσιών ασφαλείας	Βασικές	Σημαντικές	Εκτός πεδίου εφαρμογής
Οντότητες δημόσιας διοίκησης	Οντότητες δημόσιας διοίκησης της κεντρικής κυβέρνησης (με δυνατότητα εξαίρεσης των δικαστικών αρχών, των κοινοβουλίων, των κεντρικών τραπεζών, της άμυνας, της εθνικής ή δημόσιας ασφάλειας)	Βασικές	Βασικές	Βασικές
	Τοπική αυτοδιοίκηση	Σημαντικές	Σημαντικές	Σημαντικές
Διάστημα	Φορείς εκμετάλλευσης επίγειας υποδομής, ιδιοκτησίας, διαχείρισης και εκμετάλλευσης από κράτη μέλη ή ιδιωτικούς φορείς, οι οποίοι υποστηρίζουν την παροχή διαστημικών υπηρεσιών, εξαιρουμένων των παρόχων δημόσιων δικτύων ηλεκτρονικών επικοινωνιών	Βασικές	Σημαντικές	Εκτός πεδίου εφαρμογής

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

ΠΑΡΑΡΤΗΜΑ ΙΙ: ΑΛΛΟΙ ΚΡΙΣΙΜΟΙ ΤΟΜΕΙΣ

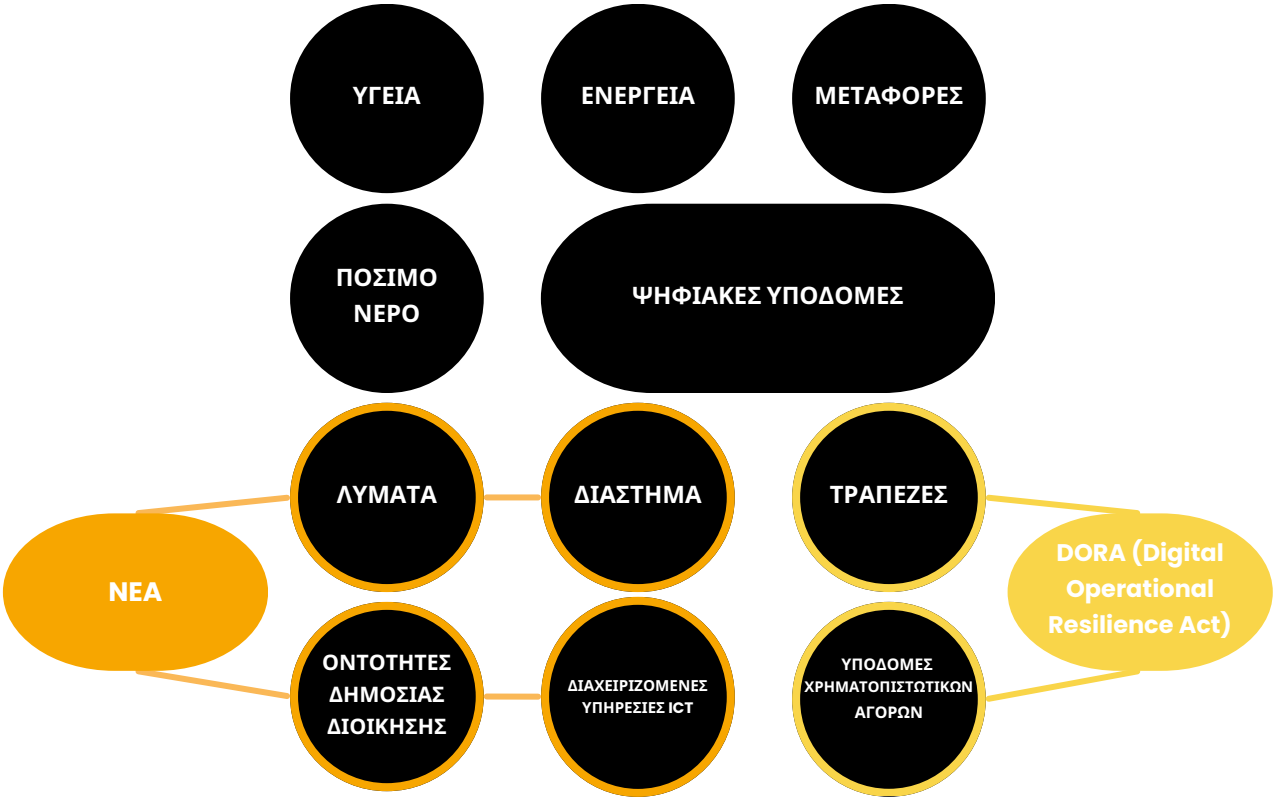
ΤΟΜΕΑΣ	**ΥΠΟΤΟΜΕΑΣ**	**ΜΕΓΑΛΕΣ ΟΝΤΟΤΗΤΕΣ** >= 250 εργαζόμενοι ή περισσότερο από €50 Εκατ. κύκλο εργασιών	**ΜΕΣΑΙΕΣ ΟΝΤΟΤΗΤΕΣ** 50-249 εργαζόμενοι ή περισσότερο από €10 εκατ. κύκλο εργασιών	**ΜΙΚΡΕΣ & ΠΟΛΥ ΜΙΚΡΕΣ ΟΝΤΟΤΗΤΕΣ** < 50 εργαζόμενοι ή λιγότερο από €10 εκατ. κύκλο εργασιών
Ταχυδρομικες Υπηρεσίες και Υπηρεσίες ταχυμεταφορών		Σημαντικές	Σημαντικές	Εκτός πεδίου εφαρμογής
Διαχείριση αποβλήτων	**Μόνο αν πρόκειται για κύρια οικονομική δραστηριότητα*	Σημαντικές	Σημαντικές	Εκτός πεδίου εφαρμογής
Χημικά	Κατασκευή, παραγωγή, διανομή	Σημαντικές	Σημαντικές	Εκτός πεδίου εφαρμογής
Τρόφιμα	Χονδρική παραγωγή και βιομηχανική παραγωγή και μεταποίηση	Σημαντικές	Σημαντικές	Εκτός πεδίου εφαρμογής
Κατασκευές (manufacturing)	Ιατροτεχνολογικά προϊόντα (in vitro diagnostic), υπολογιστές, ηλεκτρονικά και οπτικά προϊόντα, ηλεκτρικός εξοπλισμός, μηχανήματα, μηχανοκίνητα οχήματα, ρυμουλκούμενα και ημιρυμουλκούμενα, καθώς και άλλο εξοπλισμό μεταφορών (NACE C 26-30).	Σημαντικές	Σημαντικές	Εκτός πεδίου εφαρμογής
Ψηφιακοί Πάροχοι	Διαδικτυακές αγορές, μηχανές αναζήτησης, πλατφόρμες κοινωνικής δικτύωσης	Σημαντικές	Σημαντικές	Εκτός πεδίου εφαρμογής
Έρευνα	Ερευνητικοί οργανισμοί (εξαιρούνται τα εκπαιδευτικά ιδρύματα) (Προαιρετικό για τα κράτη μέλη: εκπαιδευτικά ιδρύματα)	Σημαντικές	Σημαντικές	Εκτός πεδίου εφαρμογής
Οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα		Όλα τα μεγέθη, αλλά βάσει των κριτηρίων της Οδηγίας NIS2.		

2.

ΤΟΜΕΙΣ ΣΤΟ ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η Οδηγία NIS2 θα εφαρμοστεί σε ένα ευρύτερο και εκτενέστερο σύνολο οντοτήτων από τις κατηγορίες οντοτήτων που καλύπτονται σήμερα από την Οδηγία NIS. Η Οδηγία NIS2 περιλαμβάνει νέους τομείς, ενώ παράλληλα διευρύνει τα κριτήρια για τη συμπερίληψη οντοτήτων, οι οποίες κατηγοριοποιούνται ως βασικές ή σημαντικές, εντός υφιστάμενων τομέων. Οι τομείς χωρίζονται σε δύο ομάδες: «Τομείς υψηλής κρισιμότητας» και «Άλλοι κρίσιμοι τομείς».

ΠΑΡΑΡΤΗΜΑ Ι - ΤΟΜΕΙΣ ΥΨΗΛΗΣ ΚΡΙΣΙΜΟΤΗΤΑΣ



2. ΤΟΜΕΙΣ ΣΤΟ ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

ΠΑΡΑΡΤΗΜΑ II -
ΑΛΛΟΙ ΚΡΙΣΙΜΟΙ ΤΟΜΕΙΣ

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

3. ΚΟΙΝΟΠΟΙΗΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ

Η Οδηγία NIS2 επιβάλλει στις βασικές και σημαντικές οντότητες υποχρεώσεις κοινοποίησης περιστατικών σε στάδια, για περιστατικά που έχουν «σημαντικό αντίκτυπο» στην παροχή των υπηρεσιών τους. Οι κοινοποιήσεις αυτές πρέπει να γίνονται στη σχετική αρμόδια αρχή ή στο Εθνικό CSIRT (Computer Security Incident Response Team).

6 h

ΕΓΚΑΙΡΗ ΠΡΟΕΙΔΟΠΟΙΗΣΗ (EARLY WARNING)

Αρχική κοινοποίηση, μόνο με βασικές πληροφορίες. Αποτελεί ύποπτη και κακόβουλη πράξη με πιθανές διασυνοριακές επιπτώσεις

72 h

ΚΟΙΝΟΠΟΙΗΣΗ ΠΕΡΙΣΤΑΤΙΚΟΥ

Αξιολόγηση του περιστατικού, της σοβαρότητας και του αντίκτυπου, καθώς και των ενδείξεων της παραβίασης (Indicators of Compromise).

όπως απαιτείται

ΕΝΔΙΑΜΕΣΗ ΕΚΘΕΣΗ ΠΡΟΟΔΟΥ

Κατόπιν αιτήματος του εθνικού CSIRT ή της αρμόδιας αρχής.

1 μήνας

ΤΕΛΙΚΗ ΕΚΘΕΣΗ

Η τελική έκθεση πρέπει να υποβληθεί το αργότερο ένα μήνα μετά την κοινοποίηση του συμβάντος.

Κατά περίπτωση, οι οντότητες ενημερώνουν τους αποδέκτες των υπηρεσιών τους για σημαντικά περιστατικά. Όταν αυτό είναι προς το δημόσιο συμφέρον, το Εθνικό CSIRT ή η αρμόδια αρχή μπορεί να ενημερώσει το κοινό για το περιστατικό ή μπορεί να απαιτήσει από την οντότητα να το πράξει.

4.
ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Οι βασικές και σημαντικές οντότητες πρέπει να λαμβάνουν κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων που διατρέχουν τα συστήματα στα οποία στηρίζονται οι υπηρεσίες τους και να αποτρέπουν ή να ελαχιστοποιούν τον αντίκτυπο των περιστατικών στις δικές τους και σε άλλες υπηρεσίες.

Τα μέτρα αυτά βασίζονται σε μια ολιστική προσέγγιση του κινδύνου (all-hazards approach) που αποσκοπεί στην προστασία των δικτύων και των συστημάτων πληροφοριών και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από συμβάντα, και πρέπει να περιλαμβάνουν τουλάχιστον τα εξής:

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

4. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

1. Πολιτικές για την ανάλυση κινδύνων & ασφάλεια πληροφοριακών συστημάτων
2. Διαχείριση περιστατικών
3. Μέτρα επιχειρησιακής συνέχειας (εφεδρικά αντίγραφα ασφαλείας, ανάκαμψη από καταστροφές, διαχείριση κρίσεων)
4. Ασφάλεια της αλυσίδας εφοδιασμού
5. Ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση συστημάτων, συμπεριλαμβανομένου του χειρισμού και της γνωστοποίησης ευπαθειών
6. Πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης των κινδύνων κυβερνοασφάλειας
7. Βασικές πρακτικές κυβερνο-υγιεινής και κατάρτισης στην κυβερνοασφάλεια
8. Πολιτικές και διαδικασίες για την κατάλληλη χρήση της κρυπτογραφίας και της κρυπτογράφησης
9. Ασφάλεια ανθρώπινου δυναμικού, πολιτικές ελέγχου πρόσβασης και διαχείριση πάγιων στοιχείων
10. Χρήση ταυτοποίησης πολλαπλών παραγόντων, ασφαλούς επικοινωνίας φωνής/βίντεο/κειμένου και ασφαλούς επικοινωνίας έκτακτης ανάγκης

4. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Όλα τα μέτρα πρέπει να είναι:	**Η Ευρωπαϊκή Επιτροπή μπορεί:**
• Ανάλογα με τον κίνδυνο, το μέγεθος, το κόστος, τον αντίκτυπο και τη σοβαρότητα των περιστατικών. • Να λαμβάνουν υπόψη την τελευταία εξέλιξη της τεχνολογίας και, κατά περίπτωση, τα σχετικά ευρωπαϊκά και διεθνή πρότυπα	• Να διενεργεί εκτιμήσεις κινδύνου για κρίσιμες υπηρεσίες, συστήματα ή αλυσίδες εφοδιασμού ΤΠΕ. • Να επιβάλλει υποχρεώσεις πιστοποίησης (με κατ' εξουσιοδότηση πράξεις). • Να εκδίδει εκτελεστικές πράξεις που καθορίζουν τεχνικές απαιτήσεις.

5. ΒΑΣΙΚΕΣ ΚΑΙ ΣΗΜΑΝΤΙΚΕΣ ΟΝΤΟΤΗΤΕΣ – ΕΠΟΠΤΕΙΑ

Η προηγούμενη κατηγοριοποίηση των «φορέων εκμετάλλευσης βασικών υπηρεσιών»(ΦΕΒΥ) / των «φορέων κρίσιμων υποδομών πληροφοριών») (ΦΚΥΠ) και των «παρόχων ψηφιακών υπηρεσιών» (ΠΨΥ) στην αρχική Οδηγία NIS αντικαθίσταται από την κατηγοριοποίηση μεταξύ «βασικών» και «σημαντικών» οντοτήτων.

Δεν υπάρχει πλέον κατηγοριοποίηση των ΦΕΒΥ/ΦΚΥΠ και ΠΨΥ

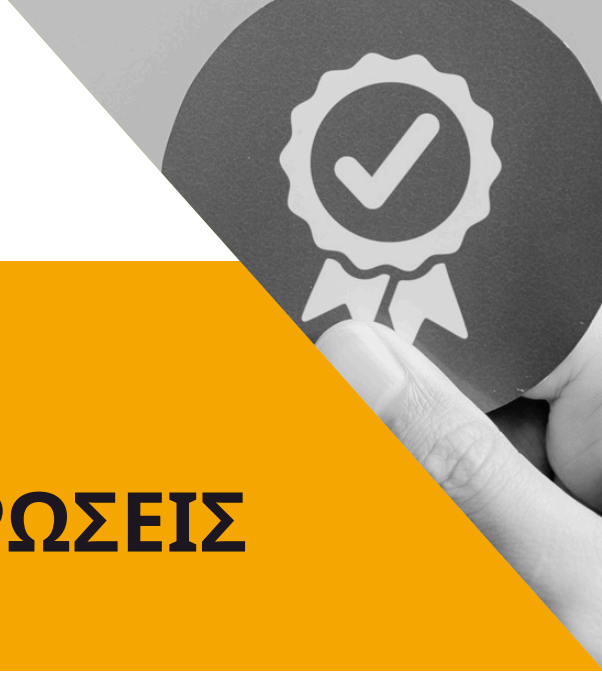
ΒΑΣΙΚΕΣ ΟΝΤΟΤΗΤΕΣ

- Εποπτεία εκ των προτέρων και εκ των υστέρων
- Επιτόπιες επιθεωρήσεις και μη-επιτόπια εποπτεία
- Τακτικοί και στοχευμένοι έλεγχοι ασφαλείας
- Σαρώσεις Ασφαλείας
- Αιτήματα παροχής πληροφοριών
- Αιτήματα για πληροφορίες που είναι αναγκαίες για την αξιολόγηση των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας που έχει λάβει η ενδιαφερόμενη οντότητα.
- Ελέγχοι Ad hoc, π.χ. μετά από ένα σημαντικό περιστατικό.

ΣΗΜΑΝΤΙΚΕΣ ΟΝΤΟΤΗΤΕΣ

- Εποπτεία εκ των υστέρων
- Επιτόπιες επιθεωρήσεις και εκ των υστέρων μη-επιτόπια εποπτεία
- Στοχευμένοι έλεγχοι ασφαλείας
- Σαρώσεις Ασφαλείας
- Αιτήματα παροχής πληροφοριών
- Αιτήματα για πληροφορίες που είναι αναγκαίες για την εκ των υστέρων αξιολόγηση των μέτρων διαχείρισης των κινδύνων κυβερνοασφάλειας που έχει λάβει η ενδιαφερόμενη οντότητα.

Οι αρμόδιες αρχές μπορούν να υιοθετήσουν μια προσέγγιση με βάση τον κίνδυνο για την ιεράρχηση των εποπτικών καθηκόντων.



6.
ΕΦΑΡΜΟΓΗ ΚΑΙ ΚΥΡΩΣΕΙΣ

Η Οδηγία NIS2 παρέχει στις εθνικές αρχές έναν ελάχιστο κατάλογο εξουσιών επιβολής για τη μη συμμόρφωση, συμπεριλαμβανομένων:

Α	Έκδοση προειδοποιήσεων για μη συμμόρφωση
Β	Έκδοση δεσμευτικών οδηγιών
Γ	Να απαιτεί παύση μη συμμορφούμενης συμπεριφοράς
Δ	Να απαιτεί να συμμορφωθούν με τα μέτρα διαχείρισης κινδύνου ή με τις υποχρεώσεις υποβολής κοινοποιήσεων με συγκεκριμένο τρόπο και εντός συγκεκριμένης προθεσμίας
Ε	Να απαιτεί την ενημέρωση του φυσικού ή νομικού προσώπου ή των φυσικών ή νομικών προσώπων στα οποία παρέχουν υπηρεσίες ή δραστηριότητες που ενδέχεται να επηρεάζονται από σημαντική κυβερνοαπειλή
ΣΤ	Να απαιτεί την εφαρμογή των συστάσεων που παρέχονται ως αποτέλεσμα ενός ελέγχου ασφαλείας εντός εύλογης προθεσμίας
Ζ	Ορισμός υπευθύνου παρακολούθησης με σαφώς καθορισμένα καθήκοντα για μια καθορισμένη χρονική περίοδο για την επίβλεψη της συμμόρφωσης
Η	Να απαιτεί δημοσιοποίηση των πτυχών της μη συμμόρφωσης
Θ	Επιβολή διοικητικών προστίμων
Ι	Η πιστοποίηση ή η εξουσιοδότηση βασικών οντοτήτων σχετικά με την υπηρεσία μπορεί να ανασταλεί εάν δεν τηρηθεί η προθεσμία για τη λήψη μέτρων.
ΙΑ	Στους υπεύθυνους για την άσκηση διοικητικών καθηκόντων σε επίπεδο διευθύνοντος συμβούλου ή νόμιμου εκπροσώπου, μπορεί να απαγορευτεί προσωρινά η άσκηση διοικητικών καθηκόντων (ισχύει μόνο για βασικές οντότητες, όχι για σημαντικές οντότητες).

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

6. ΕΦΑΡΜΟΓΗ ΚΑΙ ΚΥΡΩΣΕΙΣ

Η Οδηγία NIS2 προβλέπει την επιβολή διοικητικών προστίμων για παραβάσεις.

Μέγιστο ποσό **τουλάχιστον €10.000.000** ή έως και 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία η **βασική οντότητα** ανήκει κατά το προηγούμενο οικονομικό έτος, ανάλογα με το ποιο είναι υψηλότερο.

Μέγιστο ποσό **τουλάχιστον €7.000.000** ή έως και 1.4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία η **σημαντική οντότητα** ανήκει κατά το προηγούμενο οικονομικό έτος, ανάλογα με το ποιο είναι υψηλότερο.

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

7. ΕΥΘΥΝΕΣ ΤΗΣ ΔΙΟΙΚΗΣΗΣ

Η ανώτατη διοίκηση έχει την τελική ευθύνη για τη διαχείριση των κινδύνων κυβερνοασφάλειας σε βασικές και σημαντικές οντότητες. Η μη συμμόρφωση της διοίκησης με τις απαιτήσεις της Οδηγίας NIS2 θα μπορούσε να έχει σοβαρές συνέπειες, συμπεριλαμβανομένης της ευθύνης, των προσωρινών απαγορεύσεων και των διοικητικών προστίμων, όπως προβλέπεται στην εναρμονιστική Εθνική νομοθεσία.

Η ανώτατη διοίκηση των βασικών και σημαντικών οντοτήτων πρέπει να:

Εγκρίνει την επάρκεια των μέτρων διαχείρισης των κινδύνων κυβερνοασφάλειας που λαμβάνει η οντότητα.

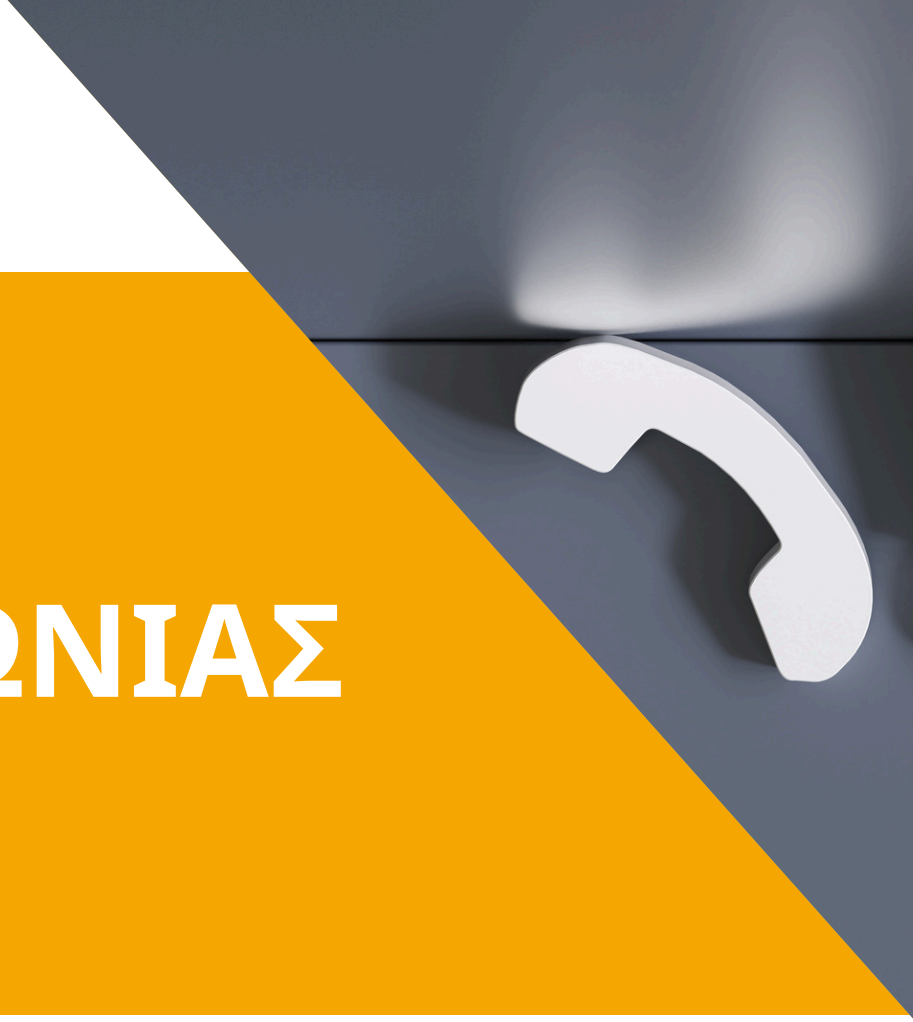
Επίβλεπει την εφαρμογή των μέτρων διαχείρισης κινδύνων.

Παρακολουθεί εκπαιδεύσεις προκειμένου να αποκτήσει επαρκείς γνώσεις και δεξιότητες για τον εντοπισμό κινδύνων και την αξιολόγηση των πρακτικών διαχείρισης κινδύνων κυβερνοασφάλειας και των επιπτώσεών τους στις υπηρεσίες που παρέχει η οντότητα.

Παρέχει παρόμοια κατάρτιση στους υπαλλήλους της σε τακτική βάση.

Αναλαμβάνει ευθύνη για μη συμμόρφωση.

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ
Αρχή Ψηφιακής Ασφάλειας



ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ

+357 22 693000

WWW.DSA.CY

CONTACT@DSA.EE.CY

ΑΝΔΡΕΑ ΧΑΛΙΟΥ 1
2408 ΕΓΚΩΜΗ
ΛΕΥΚΩΣΙΑ, ΚΥΠΡΟΣ