

Focus **Digital resilience**

Από την Κυβερνοασφάλεια στην Ψηφιακή Ανθεκτικότητα

Η Ψηφιακή Εμπιστοσύνη (Digital Trust) στο επίκεντρο του νέου ρυθμιστικού πλαισίου (νομοθετικές πράξεις ΕΕ NIS2, CERD, DORA)

Το συνολικό κόστος του κυβερνο-εγκλήματος παγκοσμίως ήταν περίπου στα **\$8.44 τρις το 2022** και εκτιμάται πως θα υπερβεί τα **\$10.5 τρις ετησίως το 2025**, σύμφωνα με αναφορές έγκυρων αναλυτών. Παρομοίως, η Gartner (Gartner analysts) προβλέπει ότι μέσα στα επόμενα δύο χρόνια το 45% των επιχειρήσεων παγκοσμίως θα επηρεαστούν με κάποιον τρόπο από κυβερνοεπίθεση στην εφοδιαστική τους αλυσίδα.

Η Ψηφιακή Ανθεκτικότητα (Digital Resilience), δεν εξαντλείται στην Κυβερνοασφάλεια με την έννοια των προληπτικών και κατασταλτικών μέτρων προστασίας των συστημάτων δικτύου και πληροφοριών αλλά και των χρηστών και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων, αλλά εστιάζει στη συνολική ικανότητα της επιχείρησης να διαμορφώνει, να εξασφαλίζει και να επανεξετάζει την επιχειρησιακή ακεραιότητα και αξιοπιστία της, διασφαλίζοντας, άμεσα ή έμμεσα μέσω της χρήσης υπηρεσιών που προσφέρονται από τρίτους, το πλήρες φάσμα των ικανοτήτων Τεχνολογίας Πληροφορικής και Επικοινωνιών (ΤΠΕ) που απαιτούνται, ώστε να ανταποκρίνεται στην ασφάλεια των συστημάτων που χρησιμοποιεί και τα οποία υποστηρίζουν τη συνεχή παροχή υπηρεσιών και την ποιότητά τους, μεταξύ άλλων και καθ' όλη τη διάρκεια διαταραχών.

Με άλλα λόγια, είναι η ικανότητα ενός οργανισμού να διατηρεί απρόσκοπτα τις βασικές του λειτουργίες παρά τις απειλές που υφίσταται σε σχέση με τη διακοπή ή τη διαταραχή της ομαλής λειτουργίας των ψηφιακών του συστημάτων, των διαδικασιών / διεργασιών ή υποδομών του οι οποίες βασίζονται σε ΤΠΕ (Digital Risk).

Το νέο Κανονιστικό Πλαίσιο

Το νέο Ρυθμιστικό Πλαίσιο της Ευρωπαϊκής Ένωσης για την ψηφιακή επιχειρησιακή ανθεκτικότητα έχει ήδη τεθεί σε εφαρμογή και, κατά συνέπεια, οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής έχουν πλέον υποχρέωση συμμόρφωσης με τις προβλεπόμενες κανονιστικές απαιτήσεις. Συγκεκριμένα, η θέσπιση των παρακάτω νομοθετικών πράξεων της ΕΕ έχει επιφέρει αρκετές νέες και σημαντικές υποχρεώσεις για τις επιχειρήσεις σε σχέση με την Κυβερνοασφάλεια και την Ψηφιακή Ανθεκτικότητα:

- Η οδηγία της Ευρωπαϊκής Ένωσης **NIS 2** (οδηγία (ΕΕ) 2022/2555 - Network Information Security 2), επικαιροποιώντας τη σχετική προηγούμενη οδηγία NIS 1, αναφορικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοσφάλειας σε ολόκληρη την Ένωση επεκτείνει τόσο το πεδίο εφαρμογής της όσο και τις απαιτήσεις αναφορικά με την προστασία της ασφάλειας και τη θωράκιση της λειτουργίας των εταιρειών που παρέχουν υπηρεσίες κρίσιμων υποδομών.
Η ενσωμάτωση της οδηγίας (ΕΕ) NIS2 στην εθνική νομοθεσία έχει ήδη υλοποιηθεί με τη ψήφιση του Ν. 5160/27-11-2024 (Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 NIS 2).
- Η οδηγία της Ευρωπαϊκής Ένωσης **CERD** (οδηγία (ΕΕ) 2022/2557 “The Critical Entities Resilience Directive”) για την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ του Συμβουλίου.
- Ο κανονισμός (ΕΕ) **DORA** για τη Ψηφιακή Επιχειρησιακή Ανθεκτικότητα (Κανονισμός (ΕΕ) 2022/2554 - Digital Operational Resilience Act) του χρηματοπιστωτικού τομέα στοχεύει στη βελτίωση της ασφάλειας, στην ενίσχυση της επιχειρησιακής ανθεκτικότητας και την αποτροπή διαταραχών που οφείλονται στα συστήματα του χρηματοπιστωτικού τομέα επιτάσσοντας αυστηρή διακυβέρνηση, διαχείριση κινδύνου, και πρακτικές ασφάλειας Τεχνολογίας Πληροφορικής και Επικοινωνιών (ΤΠΕ). Θεωρείται τομεακή νομική πράξη της Ένωσης σε σχέση με την οδηγία (ΕΕ) NIS2 όσον αφορά τις οντότητες του χρηματοπιστωτικού τομέα.

Ο κανονισμός (ΕΕ) **DORA** τέθηκε σε ισχύ στις 16 Ιανουαρίου 2023 και εφαρμόζεται από τις 17 Ιανουαρίου 2025.

Ποιους αφορά

Το νέο κανονιστικό πλαίσιο για την Κυβερνοασφάλεια και την Ψηφιακή Ανθεκτικότητα διευρύνει (βάσει NIS 2) το πεδίο εφαρμογής σε τομείς υψηλής κρισιμότητας (Προσάρτημα I) και άλλους κρίσιμους τομείς (Προσάρτημα II) για την κοινωνική και οικονομική ζωή της χώρας, εισάγοντας, παράλληλα, έναν κανόνα ανώτατου μεγέθους (“size cap”) σε σχέση με την εφαρμογή.

(δείτε πίνακες παρακάτω)





Ταχυδρομικές υπηρεσίες
και υπηρεσίες
Ταχυμεταφορών



Παραγωγή,
μεταποίηση και
διανομή
Τροφίμων



Διαχείριση
Αποβλήτων



Ψηφιακοί
πάροχοι



Κατασκευαστικός
Τομέας



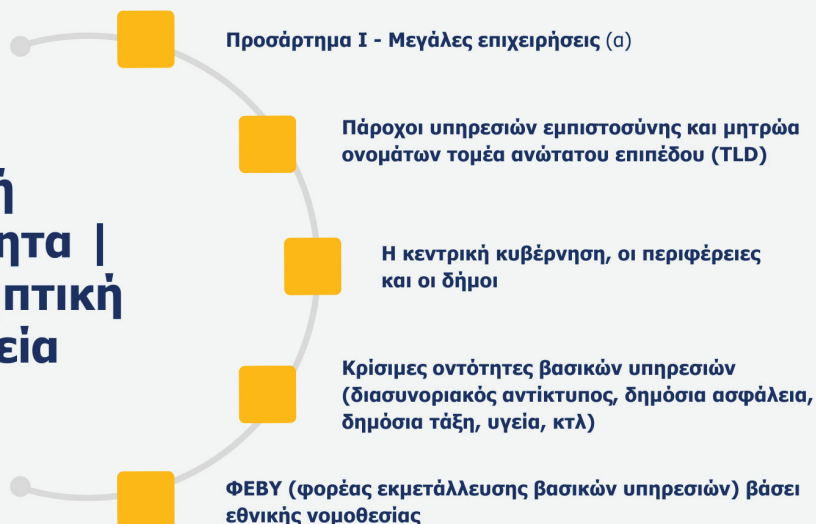
Παρασκευή, παραγωγή
και διανομή χημικών
προϊόντων

Στις υποκείμενες οντότητες συμπεριλαμβάνονται ανεξαρτήτως μεγέθους:

- Πάροχοι δημοσίων δικτύων ηλεκτρονικών επικοινωνιών
- Πάροχοι υπηρεσιών εμπιστοσύνης και μητρώα ονομάτων τομέα ανώτατου επιπέδου
- Άλλες κρίσιμες οντότητες βασικών υπηρεσιών (βάσει διασυνοριακού αντικτύπου, δημόσιας ασφάλειας, δημόσιας τάξης / υγείας κλπ.)
- Η κεντρική κυβέρνηση, οι περιφέρειες και οι δήμοι της χώρας

Πίνακες - Κανόνας ανώτατου μεγέθους σε σχέση με την εφαρμογή

Βασική Οντότητα | Προληπτική Εποπτεία



Σημαντική Οντότητα | Κατασταλτική Εποπτεία



Προσάρτημα Ι
Μεσαίες Επιχειρήσεις (β)

Προσάρτημα ΙΙ
Μεσαίες & Μεγάλες
Επιχειρήσεις

**Βάσει εθνικής
νομοθεσίας (γ)**

Επεξήγηση:

(α) Μεγάλες επιχειρήσεις:

> €50εκ. ετήσιος κύκλος εργασιών | 250+ εργαζόμενοι

(β) Μεσαίες επιχειρήσεις:

> €10εκ. ετήσιος κύκλος εργασιών | 50+ εργαζόμενοι

(γ) Βάσει εθνικής νομοθεσίας:

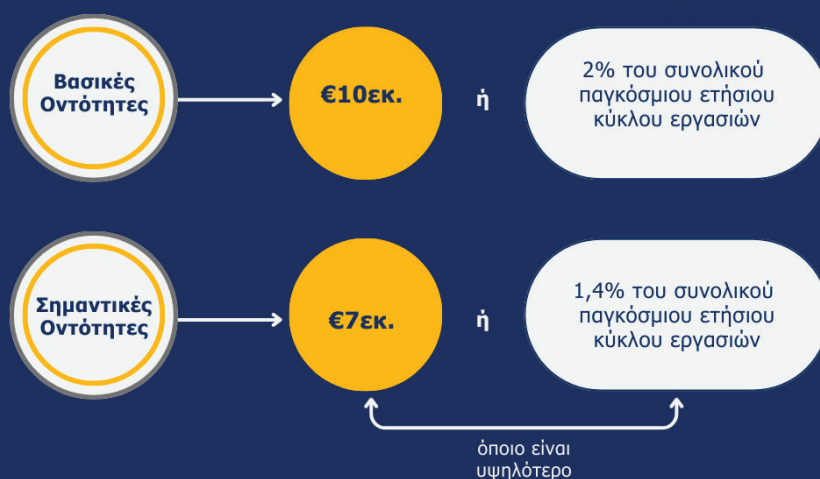
ανεξαρτήτως μεγέθους | επιλογή βάσει προφίλ κινδύνου

Ο Κανονισμός DORA έχει εφαρμογή σε ένα ευρύ φάσμα οντοτήτων του χρηματοπιστωτικού τομέα (πιστωτικά ιδρύματα, ιδρύματα πληρωμών, κεντρικοί αντισυμβαλλόμενοι, τόποι συναλλαγών, ασφαλιστικές και αντασφαλιστικές επιχειρήσεις, οργανισμοί αξιολόγησης πιστοληπτικής ικανότητας, κ.λπ.) και σε τρίτους παρόχους υπηρεσιών τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ) (συμπεριλαμβανομένων μεταξύ άλλων παρόχων υπηρεσιών υπολογιστικού νέφους, λογισμικού, υπηρεσίες ανάλυσης δεδομένων και πάροχοι υπηρεσιών data center).

Διοικητικά Πρόστιμα & Άλλες Συνέπειες

Εσωτερικός αντίκτυπος βάσει συμμόρφωσης

Διοικητικά πρόστιμα (ύψος κατ' ανώτατο όριο)



Άλλες Διοικητικές Κυρώσεις:

- Προσωρινή αναστολή στην άσκηση διευθυντικών καθηκόντων σε επίπεδο διευθύνοντος συμβούλου ή νόμιμου εκπροσώπου
- Αναστολή παροχής υπηρεσιών

Εξωτερικός αντίκτυπος



Προκλήσεις

- Κατανόηση του κανονιστικού πλαισίου – προκύπτει ανάγκη συμμόρφωσης;
- Άμεσες ενέργειες έναρξης έργου για τη συμμόρφωση – άμεσα αποτελέσματα (Quick Wins)
- Εταιρική Λογοδοσία, Διακυβέρνηση & Διαφάνεια - Ευαισθητοποίηση της διοίκησης
- Συμμετοχή όλων των ενδεδειγμένων, ενδιαφερομένων μερών (right stakeholders)
- Εκτίμηση / διαχείριση κινδύνων – Στρατηγικός Σχεδιασμός
- Ταχέως εξελισσόμενες απειλές – Εξισορρόπηση μεταξύ ασφάλειας και χρηστικότητας / απόδοσης
- Συσχέτιση με άλλες υφιστάμενες και μελλοντικές κανονιστικές απαιτήσεις
- Ολιστική προσέγγιση - αξιοποίηση των πρωτοβουλιών ήδη σε εξέλιξη (“Test once and comply to many”)
- Ενθάρρυνση της ανταλλαγής πληροφοριών για κυβερνοαπειλές
- Ασφάλεια της αλυσίδας εφοδιασμού – Κίνδυνοι ΤΠΕ τρίτων παρόχων - Αναγνώριση / αξιολόγηση κινδύνων τρίτων παρόχων υπηρεσιών ΤΠΕ
- Δοκιμές ανθεκτικότητας σε τακτική βάση
- Ανάπτυξη κουλτούρας κυβερνοασφάλειας και ψηφιακής επιχειρησιακής ανθεκτικότητας
- Υιοθέτηση της αρχής “Security by Design”

Προσέγγιση και υποστηρικτικές υπηρεσίες της ΣΟΛ Crowe για τη συμμόρφωση



- Ανάλυση Αποκλίσεων (Gap Analysis) – Αξιολόγηση ετοιμότητας και προετοιμασία για τη συμμόρφωση με DORA και NIS2
- Επισκόπηση και σχεδιασμός πλαισίου Διαχείρισης Κινδύνων ΤΠΕ και Ασφάλειας
- Αξιολόγηση κινδύνων ΤΠΕ και Ασφάλειας
- Στρατηγικός Σχεδιασμός και Διακυβέρνηση Κυβερνοασφάλειας - Ολιστική Προσέγγιση συμμόρφωσης με απαιτήσεις κανονιστικών πλαισίων αλλά και προτύπων
- Ανάπτυξη και υποστήριξη υλοποίησης Επιχειρησιακού Προγράμματος για την Κυβερνοασφάλεια και την Ψηφιακή Επιχειρησιακή Ανθεκτικότητα - Μετασχηματισμός Κινδύνων Ασφάλειας
- Αξιολόγηση / Διαχείριση κινδύνων τρίτων παρόχων ΤΠΕ
- Ανάπτυξη Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) – Προετοιμασία πιστοποίησης (ISO/IEC 27001)
- Σχεδιασμός και Υλοποίηση Πολιτικών - Διαδικασιών και Δικλίδων Ασφάλειας
- Τεχνολογίες GRC και Βελτιστοποίηση Δικλίδων
- Εκθέσεις Διασφάλισης για υπηρεσίες τρίτων παρόχων (βάσει προτύπων διασφάλισης ISAE3000, ISAE3402, SOC1, SOC2/3 κλπ.)
- Υποστήριξη Εσωτερικού Ελέγχου σε σχέση με την οργάνωση και διεξαγωγή ελέγχων συμμόρφωσης
- Κυβερνο-άμυνα (Τεχνικές αξιολογήσεις, ανάλυση ευπαθειών – VA, δοκιμές παρεϊσδυσης – PenTest, κοινωνική μηχανική, αρχιτεκτονική ασφάλειας, ασφάλεια συστημάτων SAP κλπ.)
- Εξωπορισμός υπηρεσιών Υπεύθυνου Ασφάλειας (v.CISO - CISOaaS)

Επικοινωνήστε μαζί μας

Για περισσότερες πληροφορίες, μπορείτε να επικοινωνήσετε με:

Συμεών Καλαματιανός

Επικεφαλής Υπηρεσιών Τεχνολογίας και Ψηφιακής Διασφάλισης

ΣΟΛ Crowe Συμβουλευτική

T: 210 7256900

E: skalamatianos@solcrowe.gr



Συνεργαζόμενοι Ορκωτοί
Λογιστές Α.Ε.

Ελεγκτικές Υπηρεσίες

Φωκ. Νέγρη 3
112 57, Αθήνα
T: 210 8691100
F: 210 8617328 - 210 8618016
E: solcrowe@solcrowe.gr

ΣΟΛ Συμβουλευτική Α.Ε.

Συμβουλευτικές Υπηρεσίες

Καρνεάδου 25-29
106 75, Αθήνα
T: 210 7256900
F: 210 7234583
E: advisory@solcrowe.gr

www.solcrowe.gr

