ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

ΟΔΗΓΟΣ
για τη Συμμόρφωση των Επιχειρήσεων

με τον **Ν. 5160/2024**
και την Οδηγία **NIS2**

Οκτώβριος 2025

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΓΑ ΛΟΓΙΑ ΓΙΑ ΤΟΝ ΟΔΗΓΟ

Η Οδηγία NIS2 αποτελεί το νέο, ενιαίο νομικό πλαίσιο για την κυβερνοασφάλεια στην ΕΕ και ο Οδηγός του ΣΕΒ έχει σκοπό να βοηθήσει τις ελληνικές επιχειρήσεις να προσαρμοστούν ομαλά, μέσα από πρακτικά βήματα, στο νέο ευρωπαϊκό κανονιστικό πλαίσιο.

Η ενίσχυση της κυβερνο-ανθεκτικότητας των επιχειρήσεων είναι καίριας σημασίας σε ένα ψηφιακό περιβάλλον που προσφέρει ευκαιρίες για οικονομική ανάπτυξη και βελτίωση της ανταγωνιστικότητας αλλά περιλαμβάνει και απειλές, διαρκώς αυξανόμενης πολυπλοκότητας, για πληροφοριακά συστήματα, δίκτυα και εργαζομένους.

Η NIS2 αναμένεται να επηρεάσει πάνω από 100.000 επιχειρήσεις και φορείς μεγάλου και μεσαίου μεγέθους στην ΕΕ και πάνω από 2.000 στην Ελλάδα. Μέσα από την ευθυγράμμιση με την Οδηγία NIS2 οι επιχειρήσεις μπορούν να βελτιώσουν τη διαχείριση κινδύνων, να διασφαλίσουν την επιχειρησιακή συνέχεια σε περίπτωση κυβερνοεπίθεσης και να προστατεύσουν εργαζόμενους, συνεργάτες και περιουσιακά τους στοιχεία.

Η κυβερνοασφάλεια ανάγεται πλέον, από καθαρά τεχνικό ζήτημα, σε στρατηγική και νομική προτεραιότητα για μεσαίες και μεγάλου μεγέθους επιχειρήσεις, ενώ ο επαναπροσδιορισμός των πολιτικών και η εναρμόνιση των πρακτικών

κυβερνοασφάλειας στην ΕΕ δεν δημιουργεί ένα επιπλέον διοικητικό βάρος, αλλά καθιερώνει ένα κοινό μέτωπο άμυνας που βελτιώνει τη θωράκιση των επιχειρήσεων απέναντι σε κάθε είδους ψηφιακές απειλές.

Ο Οδηγός προτείνει 10 κρίσιμα βήματα που πρέπει να υλοποιήσουν οι επιχειρήσεις, όσον αφορά τον στρατηγικό σχεδιασμό, αλλά και τις διαδικασίες πρόληψης, διαχείρισης και ανάκαμψης από περιστατικά, προκειμένου να διασφαλίσουν μια ομαλή συμμόρφωση με τις απαιτήσεις της NIS2.

Ο Οδηγός Συμμόρφωσης με την Οδηγία NIS2 αναπτύχθηκε με πρωτοβουλία της Επιτροπής Τεχνολογίας και Ψηφιακού Μετασχηματισμού του ΣΕΒ, με την ειδικότερη συνδρομή των **ABB, Coca-Cola Τρία Έψιλον, Grant Thornton, Metro, Mind the Hack, Siemens, SysteCom, Uni Systems** και **Ομίλου ΟΤΕ**. Επίσης, αξιοποιεί πληροφορίες και υλικό από την Εθνική Αρχή Κυβερνοασφάλειας.

ΜΕΓΑΣ ΧΟΡΗΓΟΣ

Digital Academy

EUROBANK

ΧΟΡΗΓΟΙ

accenture

Coca-Cola Τρία Έψιλον

ELVIAL ADVANCED ALUMINIUM SOLUTIONS

Grant Thornton

COSMOTE

Α. ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΤΗΣ ΟΔΗΓΙΑΣ NIS2

Τι είναι η Οδηγία NIS2;

Η Οδηγία NIS2 (Network and Information Security Directive – (ΕΕ) 2022/2555) αποτελεί το νέο, **ενιαίο νομικό πλαίσιο για τη διατήρηση της κυβερνοασφάλειας σε 18 κρίσιμους κλάδους στην ΕΕ.**

Η Ελλάδα, έχει ενσωματώσει την Οδηγία NIS2 στην εθνική της νομοθεσία, με τον Ν. 5160/2024 (Α 195). Κατ' εξουσιοδότηση του ανωτέρω νόμου, έχει εκδοθεί η ΚΥΑ 1689/6.5.2025 (Β 2186), στην οποία καθορίζεται το Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας των βασικών και σημαντικών οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής του Ν. 5160/2024.

Ποιοι είναι οι στόχοι και τα οφέλη;

- Ενίσχυση της κυβερνο-ανθεκτικότητας ενός ευρέος φάσματος επιχειρήσεων της ΕΕ, με την εφαρμογή μέτρων και πρωτοκόλλων ασφαλείας για την προστασία από τις κυβερνοαπειλές.
- Εναρμόνιση των πρακτικών κυβερνοασφάλειας σε ολόκληρη την ΕΕ, καθιερώνοντας ένα κοινό μέτωπο άμυνας έναντι κάθε είδους απειλών.
- Ενδυνάμωση της συνολικής ετοιμότητας και ικανότητας αντιμετώπισης περιστατικών.

Γιατί είναι σημαντικό να υπάρχει ένα ενιαίο πλαίσιο αντιμετώπισης κυβερνοαπειλών;
Μόνο το **29%** των ευρωπαϊκών επιχειρήσεων έχουν καθορίσει ή αναθεωρήσει την πολιτική κυβερνοασφάλειάς τους τα τελευταία 2 χρόνια, τη στιγμή που οι κυβερνοεπιθέσεις στην ΕΕ αυξάνονται με σημαντικούς ρυθμούς (+24% το 2024).

Οι επιχειρήσεις που ευθυγραμμίζονται με την NIS2 αποκομίζουν οφέλη όπως:

- Βελτιωμένη διαχείριση κινδύνων και προστασία από αυτούς
- Διασφάλιση επιχειρησιακής συνέχειας σε περίπτωση κυβερνοεπίθεσης
- Προστασία περιουσιακών στοιχείων, διαδικασιών, εργαζομένων και δικτύου συνεργατών
- Βελτίωση εικόνας και φήμης
- Καλλιέργεια οριζόντιας κουλτούρας κυβερνοασφάλειας
- Επίτευξη ανταγωνιστικού πλεονεκτήματος
- Μείωση του νομικού κινδύνου επιβολής σημαντικών διοικητικών κυρώσεων

Τα τελευταία 5 χρόνια **η επιτυχής συμμόρφωση σχετίζεται με σχεδόν διπλάσια μείωση των περιστατικών παραβιάσεων.**
4 φορές μικρότερη η πιθανότητα περιστατικού παραβίασης στις επιχειρήσεις που έχουν συμμορφωθεί, σε σύγκριση με αυτές που δεν είναι συμμορφωμένες.

Τι συνεπάγεται για τις επιχειρήσεις;

- Υιοθέτηση νέων διαδικασιών με στόχο την ενσωμάτωση της κυβερνοασφάλειας στις βασικές λειτουργίες της επιχείρησης, κάτι που αφορά σε όλα τα τμήματα και το προσωπικό.
- Μεγαλύτερες επενδύσεις σε συστήματα κυβερνοασφάλειας, εκπαίδευση και διαδικασίες διαχείρισης κινδύνων.
- Αναθεώρηση στρατηγικών προμηθειών και σχέσεων με προμηθευτές, καθώς οι επιχειρήσεις πρέπει να παρακολουθούν τις αλυσίδες εφοδιασμού για πιθανές αδυναμίες στην κυβερνοασφάλεια.
- Εστίαση σε συστήματα εντοπισμού περιστατικών και μηχανισμούς εσωτερικής ενημέρωσης και άμεσης υποβολής αναφορών.
- Συνεχής ενημέρωση της Διοίκησης ώστε να κατανοεί τους κινδύνους κυβερνοασφάλειας, να εγκρίνει πολιτικές και να παρακολουθεί ενεργά τη συμμόρφωση.

Η κυβερνοασφάλεια ανάγεται πλέον, από καθαρά τεχνικό ζήτημα, σε στρατηγική και νομική προτεραιότητα για μεσαίου και μεγάλου μεγέθους επιχειρήσεις.

01 ΝΕΟΙ ΡΟΛΟΙ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ

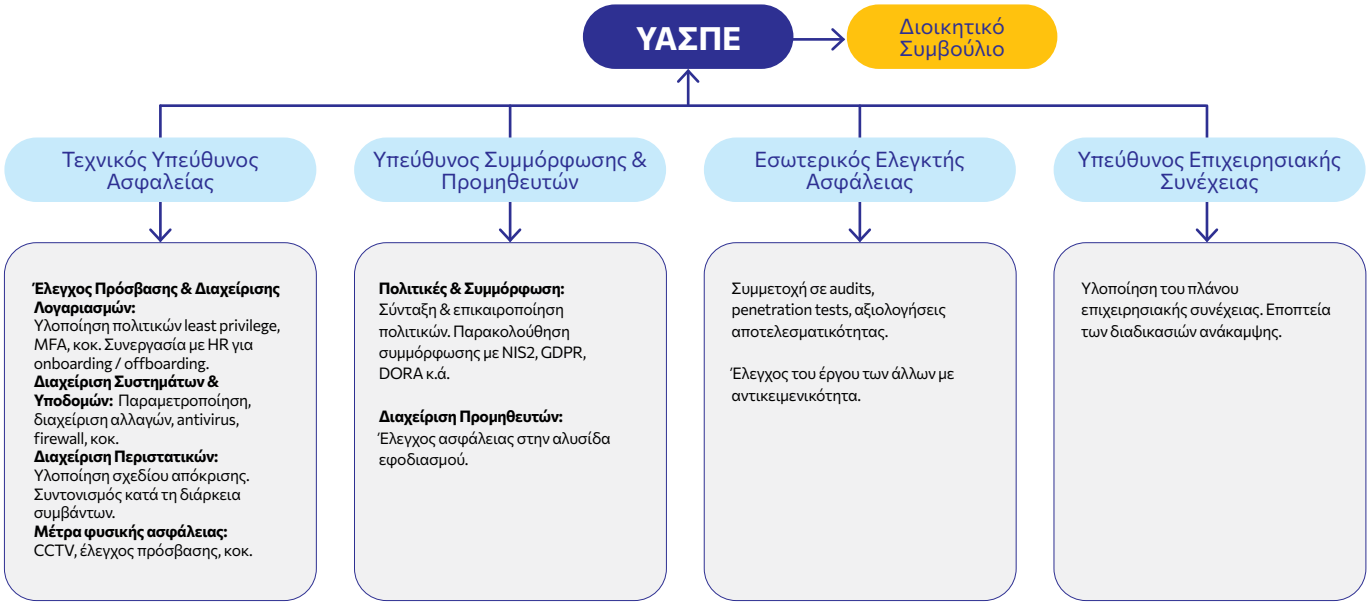
Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών (ΥΑΣΠΕ):
Η επιχείρηση πρέπει να ορίσει ένα στέλεχος (πχ τον Chief Information Security Officer – CISO) ως ΥΑΣΠΕ. Ο συγκεκριμένος ρόλος:

- Έχει ευθύνη για την ασφάλεια των συστημάτων και πληροφοριών, ενώ εποπτεύει και συντονίζει την εφαρμογή της πολιτικής κυβερνοασφάλειας και όλων των σχετικών μέτρων.
- Επικοινωνεί με την Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ) για κάθε θέμα συμμόρφωσης, διεξαγωγής ελέγχων, κοκ.
- Παρακολουθεί και συντονίζει τη συμμόρφωση με τις απαιτήσεις της NIS2.
- Πρέπει να διαθέτει εμπειρία σε διαχείριση και αντιμετώπιση κινδύνων στον κυβερνοχώρο.
- Συμμετέχει στις συνεδριάσεις της Διοίκησης και ενημερώνει για θέματα ασφάλειας.

Η παράλειψη ορισμού ΥΑΣΠΕ από τις υπόχρεες επιχειρήσεις συνιστά σοβαρή παράλειψη συμμόρφωσης και αντιμετωπίζεται ανάλογα από τις Αρχές.

Λεπτομέρειες για τα προσόντα, τα ασυμβίβαστα, τα καθήκοντα και τις υποχρεώσεις των ΥΑΣΠΕ, βλ. ΚΥΑ1899/2025/Β4250/5.8.2025.

Ομάδα Κυβερνοασφάλειας:
Πρόκειται για διατομεακό όργανο με επικεφαλής τον Υπεύθυνο Ασφάλειας, επανδρωμένο με στελέχη των τμημάτων πληροφορικής, διαχείρισης κινδύνου, νομικών υποθέσεων, προστασίας δεδομένων προσωπικού χαρακτήρα, κοκ. Η σύνθεσή της εξαρτάται από το μέγεθος, τις ανάγκες και λειτουργίες της επιχείρησης. Ενδεικτικά:



Η Ομάδα Κυβερνοασφάλειας δεν είναι αποκλειστικά τεχνική. Το αντικείμενό της είναι στρατηγικού, τεχνικού, αλλά και νομικού χαρακτήρα. Πρέπει να απαρτίζεται από στελέχη που κατανοούν κινδύνους και διαδικασίες, και από τμήματα τα οποία «τρέχουν» διαδικασίες ή τηρούν δεδομένα που εγείρουν απαιτήσεις προστασίας.

Αρμοδιότητες:
- Παρακολούθηση στρατηγικής, υποστήριξη του Υπεύθυνου Ασφάλειας, εισήγηση πολιτικών και μέτρων
- Σύνταξη, αξιολόγηση και επικαιροποίηση γενικών και θεματικών πολιτικών ασφάλειας
- Εκπόνηση εκτίμησης επικινδυνότητας, πλάνου αντιμετώπισης, ανάλυσης επιχειρηματικών επιπτώσεων
- Ανίχνευση, απόκριση, ανάκαμψη από περιστατικά
- Συντονισμός ανεξάρτητων και τεχνικών ελέγχων / penetration tests
- Παρακολούθηση συμμόρφωσης με το κανονιστικό πλαίσιο
- Παροχή αναφορών, μετρήσεων, εισηγήσεων για αποφάσεις

Διοικητικό Συμβούλιο:
Επιβλέπει τη διακυβέρνηση και συμμόρφωση με τον Ν. 5160/2024 και την Οδηγία NIS2, με προσωπική ευθύνη των μελών. Εγκρίνει τη στρατηγική κυβερνοασφάλειας, πολιτικές, ελέγχους και διορθωτικά μέτρα, εγκρίνει τη σύνθεση και λειτουργία της Ομάδας Κυβερνοασφάλειας, κατανέμει τους αντίστοιχους πόρους, κοκ.

02 ΑΠΑΡΑΙΤΗΤΑ ΣΥΣΤΗΜΑΤΑ & ΥΠΟΔΟΜΕΣ

- **Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών** (Information Security Management System-ISMS): Πλαίσιο πολιτικών, διαδικασιών και μέτρων που διασφαλίζει την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριών.
- **Σύστημα Διαχείρισης Συμμόρφωσης & Ελέγχων:** Τεκμηρίωση, αξιολόγηση συμμόρφωσης και σχεδιασμός / παρακολούθηση πολιτικών.
- **Πλατφόρμα Εκπαίδευσης & Awareness:** Οργάνωση, παρακολούθηση και τεκμηρίωση εκπαιδεύσεων και ασκήσεων προσωπικού σε θέματα ασφάλειας.
- **Σύστημα Διαχείρισης Περιουσιακών Στοιχείων:** Καταγραφή, ταξινόμηση και εποπτεία όλου του πληροφοριακού, τεχνολογικού και μηχανολογικού εξοπλισμού.
- **Σύστημα Ταξινόμησης και Προστασίας Δεδομένων:** Καθορισμός επιπέδων ευαισθησίας και κρισιμότητας κάθε δεδομένου ή στοιχείου.
- **Σύστημα Ελέγχου Τερματικών Συσκευών:** Κεντρική διαχείριση, παρακολούθηση και ασφάλεια όλων των τερματικών συσκευών.
- **Σύστημα Καταγραφής και Παρακολούθησης Προμηθευτών:** Οργάνωση και ταξινόμηση τουλάχιστον των άμεσων προμηθευτών και παρεχόμενων υπηρεσιών.
- **Σύστημα Διαχείρισης Πρόσβασης & Ταυτοποίησης:** Έλεγχος προσβάσεων, αυθεντικοποίηση χρηστών και διαχείριση προνομιακών λογαριασμών.
- **Πλατφόρμα Διαχείρισης Ευπαθειών και Απειλών:** Εντοπισμός ευπαθειών, συλλογή πληροφοριών για απειλές, εκτίμηση κινδύνων.

- **Εργαλεία Διαχείρισης Ρυθμίσεων:** Καταγραφή, εφαρμογή, έλεγχος και αυτοματοποίηση ρυθμίσεων σε συστήματα, λογισμικά και δίκτυα.
- **Σύστημα Διαχείρισης Αλλαγών:** Οργάνωση, έγκριση, παρακολούθηση και τεκμηρίωση αλλαγών στα πληροφοριακά συστήματα.
- **Σύστημα Καταγραφής και Απόκρισης σε Περιστατικά:** Υλοποίηση Σχεδίου Αντιμετώπισης Περιστατικών, με τεκμηρίωση και παρακολούθηση περιστατικών και ενεργειών απόκρισης.
- **Πλαίσιο Επιχειρησιακής Συνέχειας και Ανάκαμψης:** Τεκμηρίωση και εφαρμογή σχεδίου επιχειρησιακής συνέχειας και disaster recovery.

03 ΔΡΑΣΕΙΣ ΕΚΠΑΙΔΕΥΣΗΣ & ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗΣ

Η ευθυγράμμιση με τον Ν. 5160/2024 και την Οδηγία NIS2 προϋποθέτει την **καλλιέργεια κουλτούρας** για την κυβερνοασφάλεια στο σύνολο του προσωπικού, μέσα από σειρά εκπαιδευτικών δράσεων με διάρθρωση περιεχομένου ανάλογα με τη διοικητική βαθμίδα και ρόλο των καταρτιζομένων:

- Τακτικά σεμινάρια και ενημερώσεις για όλο το προσωπικό (ιδίως για θέματα phishing, χρήσης / αλλαγής κωδικών πρόσβασης, χρήσης συστημάτων και εφαρμογών, απομακρυσμένης εργασίας).
- Ειδικευμένη εκπαίδευση για εργαζόμενους και στελέχη με κρίσιμους ρόλους και ενεργή συμμετοχή σε διαδικασίες διαχείρισης κινδύνων (IT officers, security officers, legal experts, κοκ).
- Τακτικές ασκήσεις κυβερνοασφάλειας.

Η εκπαίδευση πρέπει να τεκμηριώνεται και ενσωματώνεται στον κύκλο αξιολόγησης προσωπικού.

32% μόνο των ελληνικών επιχειρήσεων καταρτίζουν το προσωπικό τους σε θέματα κυβερνοασφάλειας, έναντι 60% στην ΕΕ.

Ποιες επιχειρήσεις αφορά;

Όλες τις επιχειρήσεις παροχής υπηρεσιών και παραγωγής αγαθών, των οποίων η διατάραξη της ασφάλειας ενδέχεται να έχει σημαντικό αρνητικό αντίκτυπο στην οικονομία ή/και στην κοινωνία, εφόσον πληρούν συγκεκριμένα κριτήρια μεγέθους.

Η NIS2 θα επηρεάσει πάνω από 100.000 επιχειρήσεις και φορείς μεγάλου και μεσαίου μεγέθους στην ΕΕ και πάνω από 2.000 στην Ελλάδα.

Ι. Βασικές οντότητες

- **Χώρα δραστηριοποίησης: Ελλάδα**
- **Μέγεθος: Μεγάλες**

(>250 εργαζόμενοι ή ετήσιος κύκλος εργασιών >€50 εκ. και ισολογισμός >€43 εκ.)

- **Λειτουργούν σε Τομείς Υψηλής Κρισιμότητας:**

- **Ειδικές περιπτώσεις:** Ανεξαρτήτως μεγέθους, βασικές οντότητες θεωρούνται:

- οι εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης,
- τα μητρώα ονομάτων τομέα ανώτατου επιπέδου (TLD),
- οι πάροχοι υπηρεσιών συστήματος ονομάτων τομέα (DNS),
- οι επιχειρήσεις που δραστηριοποιούνται σε **Τομείς Υψηλής Κρισιμότητας ή Άλλους Κρίσιμους Τομείς** και οι οποίες προσδιορίζονται από την Εθνική Αρχή Κυβερνοασφάλειας ως βασικές οντότητες διότι κρίνεται ότι διαδραματίζουν ιδιαίτερα νευραλγικό ρόλο στην οικονομική και κοινωνική ζωή (πχ επιχείρηση που είναι ο μοναδικός πάροχος στη χώρα ουσιώδους για την διατήρηση κρίσιμων κοινωνικών ή οικονομικών δραστηριοτήτων υπηρεσίας),
- οι μεσαίου και μεγάλου μεγέθους πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών.

ΙΙ. Σημαντικές οντότητες

Χαρακτηρίζονται από μικρότερο βαθμό κρισιμότητας έναντι των βασικών, παραμένοντας ωστόσο ζωτικής σημασίας.

- **Χώρα δραστηριοποίησης: Ελλάδα**

- **Λειτουργούν σε Άλλους Κρίσιμους Τομείς και είναι μεσαίες ή μεγάλες:**

Ταχυδρομικές υπηρεσίες, υπηρεσίες ταχυμεταφορών

Παρασκευή, παραγωγή και διανομή χημικών προϊόντων

Παραγωγή, μεταποίηση και διανομή τροφίμων

Κατασκευή ηλεκτρολογικού, ηλεκτρονικού και μηχανολογικού εξοπλισμού

Πάροχοι ψηφιακών υπηρεσιών

Διαχείριση αποβλήτων

Έρευνα

- **Λειτουργούν σε Τομείς Υψηλής Κρισιμότητας, αλλά είναι μεσαίες**

(ή μικρές εφόσον εμπίπτουν στις κατηγορίες που εντάσσονται στο πεδίο εφαρμογής του Ν. 5160/2024 και της NIS 2 ανεξαρτήτως μεγέθους – βλ. άρθρο 3 του Ν. 5160/2024).

Για πλήρη κατάταξη των οντοτήτων σε βασικές και σημαντικές βάσει μεγέθους και τομέα, περιλαμβανομένων των εξαιρέσεων, βλ. άρθρα 3 και 4 και Παράρτημα Ι και ΙΙ του Ν. 5160/2024.

Πώς διαπιστώνει μια επιχείρηση ότι εμπίπτει στον Ν. 5160/2024 και την Οδηγία NIS2;

Κάθε επιχείρηση, προκειμένου να ελέγξει αν εντάσσεται στο νέο καθεστώς NIS2, μπορεί να χρησιμοποιήσει το εργαλείο ελέγχου υπαγωγής της ΕΑΚ.

ΤΕΣΤ ΥΠΑΓΩΓΗΣ

Αν η επιχείρηση υπάγεται, εγγράφεται υποχρεωτικά στην Ψηφιακή Πλατφόρμα Εγγραφής Οντοτήτων της ΕΑΚ. Για πληροφορίες για τα στοιχεία που υποβάλλονται, βλ. ΚΥΑ1381/2025/Β463/10.2.2025 και την τροποποίηση ΚΥΑ 4241/2025/Β4241/4.8.2025.

- Η προθεσμία εγγραφής για τις υπόχρεες επιχειρήσεις έληξε στις 30 Σεπτεμβρίου 2025.

Ποιες είναι οι ευθύνες της Διοίκησης και οι κυρώσεις;

Η NIS2 δίνει έμφαση στις **υποχρεώσεις** και τη **λογοδοσία** της Ανώτατης Διοίκησης. Πλέον, η συμμόρφωση στις απαιτήσεις του νόμου προϋποθέτει την ενεργή συμμετοχή των διοικούντων.

Η προσαρμογή στον Ν. 5160/2024 και την Οδηγία NIS2 απαιτεί από τη Διοίκηση στρατηγική προσέγγιση και ενεργό συμμετοχή στο σχεδιασμό, υλοποίηση, επίβλεψη και αξιολόγηση των μέτρων συμμόρφωσης. Σε καμία περίπτωση, δεν αφορά αποκλειστικά τεχνικά ζητήματα πληροφορικής.

Τα μέλη ΔΣ:

Έχουν νομική υποχρέωση να εγκρίνουν και να επιβλέπουν την εφαρμογή των μέτρων διαχείρισης κινδύνων.

Εκπαιδεύονται ώστε να αποκτήσουν γνώσεις και δεξιότητες για να μπορούν να εντοπίζουν κινδύνους και να αξιολογούν πρακτικές διαχείρισης αυτών, αλλά και παρέχουν όμοια κατάρτιση στους εργαζομένους σε ετήσια βάση.

Σε σοβαρές περιπτώσεις παραβιάσεων, μπορούν να θεωρηθούν προσωπικά υπεύθυνα, έχοντας ανάλογες κυρώσεις.

Οι βασικές οντότητες υπόκεινται σε πλήρες εποπτικό καθεστώς, δηλαδή σε υποχρεωτικούς περιοδικούς ή έκτακτους ελέγχους χωρίς να έχει συμβεί περιστατικό, αλλά και μετά την εκδήλωσή του (ex-ante και ex-post έλεγχοι). Οι σημαντικές οντότητες υπόκεινται σε απλοποιημένο εποπτικό καθεστώς, δηλαδή μόνο όταν έχει συμβεί περιστατικό (ex-post έλεγχοι).

Παράβαση	**Πιθανές συνέπειες**
Μη καταγραφή ή αναφορά συμβάντος. Μη ύπαρξη ή ανεπαρκής εφαρμογή μέτρων. Παρεμπόδιση ελέγχου ή παροχή ψευδών στοιχείων.	Μέτρα επιβολής από ΕΑΚ (προειδοποιήσεις, δεσμευτικές οδηγίες, διορθωτικές εντολές και, σε περίπτωση μη συμμόρφωσης, αναστολή πιστοποίησης παρεχόμενων υπηρεσιών, απαγόρευση άσκησης διευθυντικού δικαιώματος). Διοικητικό πρόστιμο.
Μη εκτίμηση ή μη τεκμηρίωση εκτίμησης κινδύνων. Παράβαση από πλευράς Διοίκησης της έγκρισης μέτρων διαχείρισης κινδύνων και επίβλεψης της εφαρμογής τους. Μη παρακολούθηση εκπαίδευσης κυβερνοασφάλειας και μη παροχή σχετικής εκπαίδευσης στους υπαλλήλους. Παράβαση επιβληθέντων από την ΕΑΚ μέτρων κατά την άσκηση των εποπτικών της καθηκόντων (σύμφωνα με την παρ. 4 α έως η και την παρ. 5 του άρθρου 24 και το άρθρο 25).	Ευθύνη ανώτατης διοίκησης. Μέτρα επιβολής από ΕΑΚ (προειδοποιήσεις, δεσμευτικές οδηγίες, διορθωτικές εντολές και, σε περίπτωση μη συμμόρφωσης, αναστολή πιστοποίησης παρεχόμενων υπηρεσιών, απαγόρευση άσκησης διευθυντικού δικαιώματος). Διοικητικό πρόστιμο.

Στο 34% των ευρωπαϊκών επιχειρήσεων η Διοίκηση ακόμα δεν έχει ενεργή εμπλοκή σε θέματα εφαρμογής της NIS2.

Επιβολή διοικητικών προστίμων από την Εθνική Αρχή Κυβερνοασφάλειας

Περιπτώσεις παραβιάσεων: ανεπαρκή μέτρα διαχείρισης κινδύνων, μη ενημέρωση ή καθυστέρηση ενημέρωσης σε περίπτωση σημαντικού περιστατικού

Σε βασικές οντότητες:
πρόστιμο έως **€10 εκ.** ή έως **2%** του παγκόσμιου κύκλου εργασιών του προηγούμενου έτους (όποιο είναι υψηλότερο)

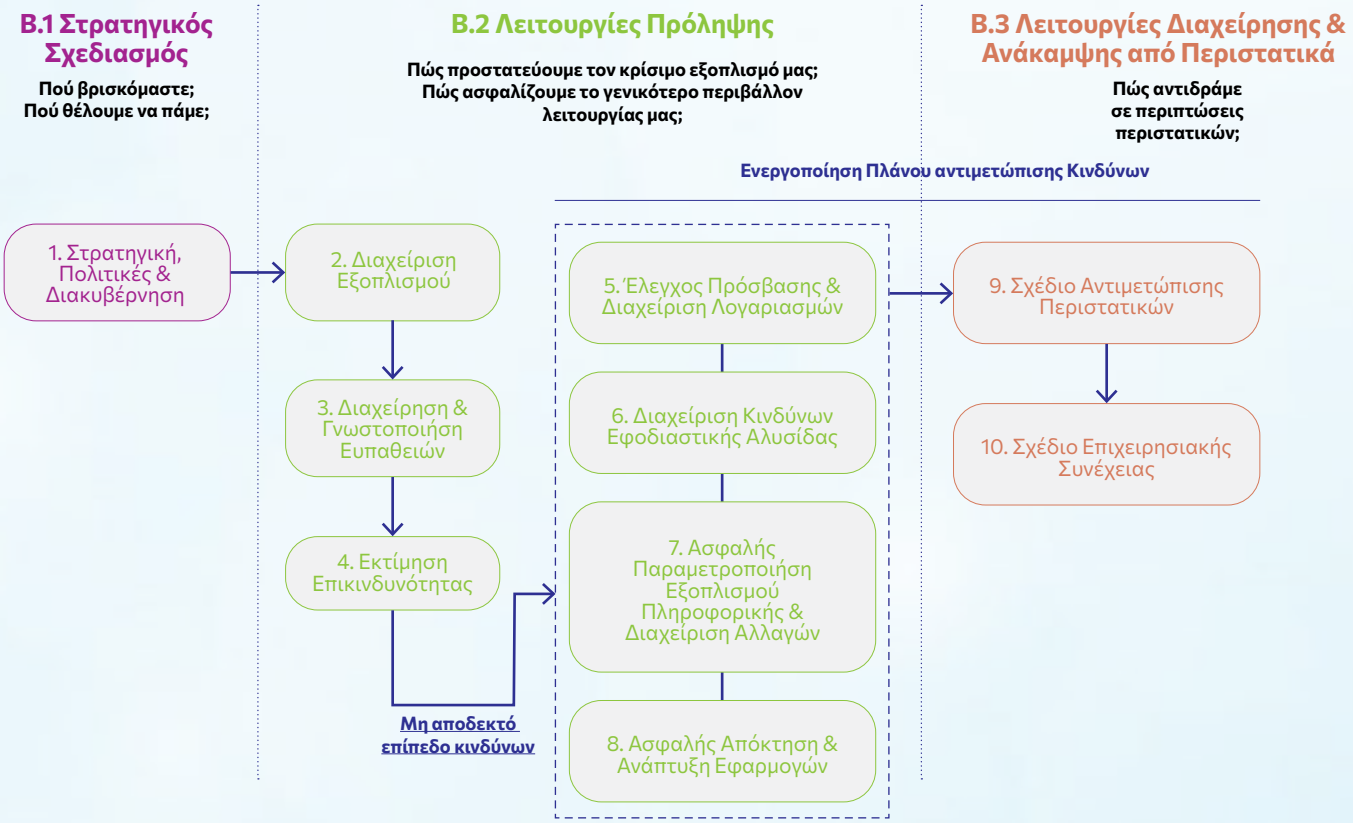
Σε σημαντικές οντότητες:
πρόστιμο έως **€7 εκ.** ή έως **1,4%** του παγκόσμιου κύκλου εργασιών του προηγούμενου έτους (όποιο είναι υψηλότερο) γασιών του προηγούμενου έτους (όποιο είναι υψηλότερο)

Για περισσότερες λεπτομέρειες σχετικά με τον Ν. 5160/2024 και τη NIS2, βλ. τον σχετικό Οδηγό Αναφοράς της ΕΑΚ.

Πηγές:
Εθνική Αρχή Κυβερνοασφάλειας, ΣΕΒ, Υπουργείο Ψηφιακής Διακυβέρνησης, European Commission, European Cyber Security Organisation, Eurostat, EY, National Cyber Security Center of Ireland, Thales Group

Β.
ΑΝΑΛΥΣΗ ΔΙΑΔΙΚΑΣΙΩΝ, ΑΡΜΟΔΙΟΤΗΤΩΝ, ΕΡΓΑΛΕΙΩΝ & ΤΕΚΜΗΡΙΩΣΗΣ

ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΔΙΑΔΙΚΑΣΙΩΝ ΠΡΟΛΗΨΗΣ & ΑΝΑΚΑΜΨΗΣ



B.1
ΣΤΡΑΤΗΓΙΚΟΣ ΣΧΕΔΙΑΣΜΟΣ

ΔΙΑΔΙΚΑΣΙΑ **No1**

Στρατηγικός Σχεδιασμός
(Στρατηγική, Πολιτικές, Διακυβέρνηση)

ΣΚΟΠΟΣ

Η αναγωγή της κυβερνοασφάλειας σε θεμελιώδες και συστηματικό μέρος της εταιρικής διακυβέρνησης, υπό την άμεση εποπτεία της Διοίκησης, μέσα από ένα ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων.

Το Πρόγραμμα Διαχείρισης Κινδύνων περιλαμβάνει αφενός τη στρατηγική κυβερνοασφάλειας (όραμα και κατεύθυνση), και αφετέρου τον τρόπο και τα μέσα υλοποίησης της στρατηγικής (πολιτικές, διαδικασίες, ρόλοι & αρμοδιότητες, τεχνικά, οργανωτικά & επιχειρησιακά μέτρα, αξιολόγηση & βελτίωση).

ΒΗΜΑΤΑ

1. Ανάθεση ευθύνης έγκρισης, εποπτείας και λογοδοσίας για το πρόγραμμα στο ανώτατο όργανο Διοίκησης:
Διοικητικό Συμβούλιο ή Γενικός Διευθυντής.

2. Ανάπτυξη στρατηγικής κυβερνοασφάλειας:
Ευθυγράμμιση με τους επιχειρηματικούς στόχους και την ευρύτερη στρατηγική κινδύνων της επιχείρησης.

Τα θεμελιώδη ερωτήματα που πρέπει να απαντάει η στρατηγική κυβερνοασφάλειας: Τι πρέπει να προστατεύσουμε; Από τι κινδυνεύουμε; Πού θέλουμε να πάμε; Πώς θα φτάσουμε εκεί; Πώς θα ξέρουμε ότι πετύχαμε;

3. Σχεδίαση και τεκμηρίωση πολιτικών και διαδικασιών:
- Εκπόνηση γενικής πολιτικής ασφάλειας πληροφοριών και θεματικών πολιτικών (πχ ελέγχου πρόσβασης, διαχείρισης περιστατικών, αντιγράφων ασφαλείας, κ.α.).
- Ορισμός διαδικασιών για την εφαρμογή και παρακολούθηση των πολιτικών.

4. Ορισμός ρόλων και αρμοδιοτήτων:
- Ανάθεση καθηκόντων σε συγκεκριμένα στελέχη.
- Καθορισμός συγκεκριμένων ευθυνών για κάθε ρόλο.

5. Παροχή πόρων και υποστήριξης:
- Δέσμευση οικονομικών, τεχνικών και ανθρώπινων πόρων για την εφαρμογή του προγράμματος.
- Ανάθεση προϋπολογισμού για τεχνολογίες, εργαλεία, εκπαίδευση, προσωπικό.

6. Εκπαίδευση και ευαισθητοποίηση όλων των εργαζομένων, του τεχνικού προσωπικού και της Διοίκησης.

7. Τεκμηρίωση και αρχειοθέτηση:
- Καταγραφή όλων των ενεργειών, πολιτικών, αποφάσεων και εκπαιδεύσεων.
- Δημιουργία φακέλου συμμόρφωσης, με όλα τα απαραίτητα τεκμήρια και αποδεικτικά στοιχεία υλοποίησης.

8. Παρακολούθηση και αξιολόγηση:
- Καθιέρωση διαδικασίας για περιοδική αξιολόγηση της αποτελεσματικότητας του προγράμματος. Επικαιροποίηση πολιτικών και μέτρων όπου χρειάζεται.

9. Συνεχής βελτίωση:
- Ανάλυση εμπειριών, περιστατικών και διεθνών εξελίξεων.
- Ενσωμάτωση ανατροφοδότησης και ελέγχων.

Για βιομηχανικές επιχειρήσεις, συνίσταται η χρήση του προτύπου ISA/IEC 62443 που παρέχει μια δομημένη προσέγγιση για την ασφάλεια του βιομηχανικού αυτοματισμού και ΟΤ.

Επιχειρήσεις με ΟΤ υποδομές:
Ο σχεδιασμός του συνόλου των πολιτικών, διαδικασιών και ρόλων προσαρμόζεται στις απαιτήσεις ασφαλείας του ΟΤ περιβάλλοντος. Απαιτείται συντονισμός με το γενικότερο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών που εφαρμόζει η επιχείρηση. Επίσης:
- **Εκτίμηση επιπέδου προστασίας** (cybersecurity assessment) που παρέχει το υφιστάμενο ΟΤ περιβάλλον σε σχέση με τις απαιτήσεις του ISA/IEC 62443.
- **Πρόγραμμα διαχείρισης αναβαθμίσεων** (patch management) που μειώνουν τα τρωτά σημεία, βάσει των προδιαγραφών λειτουργίας και ασφαλείας του ΟΤ.
- **Καθορισμός απαιτήσεων ασφαλείας** για τους παρόχους υπηρεσιών (πχ integrators, συντηρητές).

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

Οι διαδικασίες καλύπτουν:

- Όλα τα μέλη του Ανώτατου Οργάνου Διοίκησης (πχ ΔΣ).
- Όλες τις μονάδες / τμήματα της επιχείρησης που επηρεάζονται από την ασφάλεια πληροφοριών.
- Όλες τις υποδομές, συμπεριλαμβανομένων των ΟΤ συστημάτων.
- Όλο το προσωπικό που σχετίζεται άμεσα ή έμμεσα με κρίσιμες λειτουργίες.
- Όλα τα μέρη από τα οποία υπάρχει εξάρτηση για την ασφάλεια των υπηρεσιών (πχ προμηθευτές).

ΕΥΘΥΝΗ

Στρατηγικό επίπεδο

Διοίκηση:

- Εγκρίνει το πρόγραμμα διαχείρισης κινδύνων κυβερνοασφάλειας.
- Διασφαλίζει την ύπαρξη απαραίτητων πόρων για υλοποίηση και μέτρα.
- Διασφαλίζει την ενημέρωση του προσωπικού για τις πολιτικές και υποχρεώσεις.
- Εξασφαλίζει την τήρηση τεκμηρίωσης (τεχνική, διοικητική, νομική).
- Παρακολουθεί προγράμματα εκπαίδευσης και τα διασφαλίζει για όλο το προσωπικό.

Επιχειρησιακό επίπεδο

Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών:

- Εποπτεύει την εφαρμογή του προγράμματος.
- Συντονίζει μέτρα και πολιτικές.
- Ενημερώνει τη Διοίκηση για κινδύνους ή μη συμμόρφωση.

Μέλη Ομάδας Κυβερνοασφάλειας
(με ρόλους που κατανέμονται βάσει των αναγκών και του μεγέθους της οντότητας).

Εκτελεστικό επίπεδο

Προσωπικό:

- Υποχρεούται να γνωρίζει και να τηρεί τις πολιτικές και διαδικασίες ασφάλειας.
- Εκπαιδεύεται σε θέματα κυβερνοασφάλειας.
- Συμβάλλει στην καθημερινή εφαρμογή των μέτρων.

ΕΡΓΑΛΕΙΑ ΚΑΙ ΕΓΓΡΑΦΑ

Εργαλείο / Λειτουργία	Περιγραφή
Σύστημα Διαχείρισης Συμμόρφωσης & Ελέγχων (GRC platform - Governance, Risk & Compliance)	Διαχείριση, παρακολούθηση και τεκμηρίωση διακυβέρνησης, διαχείρισης κινδύνων και συμμόρφωσης με κανονιστικά πλαίσια, πρότυπα και νόμους.
Εργαλείο καταγραφής αποφάσεων Διοίκησης	Πρακτικά ΔΣ, έγγραφα επικύρωσης πολιτικών.
Σύστημα εκπαίδευσης προσωπικού (LMS)	Παρακολούθηση, τεκμηρίωση και reporting για awareness.
Εργαλεία project management	Παρακολούθηση υλοποίησης του προγράμματος και ενεργειών.
Σύστημα παρακολούθησης risk management	Εφαρμογή πλάνου μέτρων, προτεραιοτήτων και ελέγχων.

Τεκμηρίωση & Αναφορές	Περιγραφή
Γενική Πολιτική Ασφάλειας Πληροφοριών & Συστημάτων	Ορισμός στρατηγικής και βασικών αρχών.
Κανονισμός Ρόλων & Αρμοδιοτήτων	Τεκμηριώνει ποιος κάνει τι.
Πλάνο εκπαίδευσης προσωπικού	Αναλυτικό πρόγραμμα επιμόρφωσης για την ασφάλεια.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

- **Άμεση:**
  Έναρξη προγράμματος.
- **3-6 μήνες από την έναρξη του προγράμματος:**
  Ολοκλήρωση και τεκμηρίωση, το αργότερο πριν τον πρώτο έλεγχο ή αυτοαξιολόγηση.
- **Ετήσια:**
  Προγραμματισμένη επανεξέταση.
- **Ad hoc:**
  Επανεξέταση μετά από σοβαρό περιστατικό, σημαντικές οργανωτικές αλλαγές και αλλαγές στο διεθνές ή κανονιστικό περιβάλλον.

B.2
ΔΙΑΔΙΚΑΣΙΕΣ ΚΑΙ ΒΗΜΑΤΑ ΠΡΟΛΗΨΗΣ

Όλα τα επόμενα βήματα εντάσσονται στην ευρύτερη διαδικασία Διαχείρισης Κινδύνων. Πριν την έναρξή της, συνίσταται η υιοθέτηση διεθνούς προτύπου που παρέχει συγκεκριμένες κατευθύνσεις και εργαλεία (πχ ISO 27005, NIST SP 800-30 ή IEC 62443).

ΔΙΑΔΙΚΑΣΙΑ No2

Διαχείριση Εξοπλισμού
(Asset Management)

ΣΚΟΠΟΣ

Η καταγραφή και παρακολούθηση του τεχνολογικού και πληροφοριακού εξοπλισμού που χρησιμοποιεί η επιχείρηση, καθώς και η ανάθεση ευθυνών διαχείρισης και συντήρησής του. Το βήμα αυτό επιτρέπει στην οντότητα να γνωρίζει τι έχει και πόσο σημαντικό είναι.

ΒΗΜΑΤΑ

1. Περιοδική χαρτογράφηση των εξοπλισμού πληροφορικής.

2. Ορισμός υπεύθυνου διαχείρισης και συντήρησης (ιδιοκτήτης - owner) για κάθε στοιχείο. Ο ρόλος των υπεύθυνων είναι σημαντικός, καθώς:

- Βοηθούν στη διαδικασία καταγραφής και ταξινόμησης του εξοπλισμού.
- Παρέχουν χρήσιμες πληροφορίες στο επόμενο βήμα εκτίμησης κινδύνων και επιπτώσεων από περιστατικά.
- Συμμετέχουν στην επιλογή κατάλληλων μέτρων προστασίας για κάθε στοιχείο, ελέγχουν την εφαρμογή τους και αξιολογούν την αποτελεσματικότητά τους.

3. Ταξινόμηση του εξοπλισμού σε διακριτά επίπεδα με βάση τις απαιτήσεις προστασίας, την ευαισθησία, την κρισιμότητα και την επιχειρησιακή τους αξία. Κάθε επίπεδο προστασίας θα επηρεάσει σε επόμενο στάδιο την επιλογή των μέτρων.

Το Asset Management διασφαλίζει τον εντοπισμό και παρακολούθηση συστημάτων, ψηφιακών υποδομών και των ρυθμίσεών τους (configurations), αποτελώντας προϋπόθεση για μια ακριβή εκτίμηση κινδύνου.

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

Η διαδικασία καλύπτει όλα τα στοιχεία πληροφορικής και τεχνολογίας, ανεξάρτητα από την τοποθεσία (on-premise ή cloud περιβάλλον) ή μορφή τους (φυσική ή εικονική). Πχ:

- **Υλικό (hardware):** σταθμοί εργασίας, διακομιστές, φορητές συσκευές, αφαιρούμενα μέσα αποθήκευσης, κοκ.
- **Λογισμικό (software):** λειτουργικά συστήματα, εφαρμογές, ειδικά εργαλεία, κοκ.
- **Υπηρεσίες πληροφορικής:** cloud, SaaS, υποδομές IT.
- **Συστήματα και δεδομένα,** ανεξαρτήτως τοποθεσίας ή τεχνολογικής πλατφόρμας.
- **OT:** SCADA, βιομηχανικά συστήματα, κοκ.

Η διαδικασία αφορά όλη τη διάρκεια ζωής του εξοπλισμού, από την προμήθεια, την ενεργή χρήση, τη μεταφορά, την αποθήκευση έως και την ασφαλή απόσυρση ή διαγραφή του.

ΕΥΘΥΝΗ

Διοίκηση:
Έγκριση, εφαρμογή και εποπτεία του προγράμματος διαχείρισης εξοπλισμού.

Ιδιοκτήτες εξοπλισμού:
Καλή λειτουργία και συντήρηση κάθε στοιχείου, ενημέρωση του καταλόγου με ακριβείς καταγραφές, τήρηση και εφαρμογή μέτρων ασφάλειας του εξοπλισμού ευθύνης τους.

ΕΡΓΑΛΕΙΑ ΚΑΙ ΕΓΓΡΑΦΑ

Εργαλείο / Λειτουργία	Περιγραφή
Σύστημα Διαχείρισης Περιουσιακών Στοιχείων	Καταγραφή, ταξινόμηση και εποπτεία όλου του πληροφοριακού / τεχνολογικού εξοπλισμού, λογισμικών, cloud υπηρεσιών και συστημάτων OT στη διάρκεια του κύκλου ζωής τους (απόκτηση–χρήση–απόρριψη).
Σύστημα Ταξινόμησης και Προστασίας Δεδομένων	Καθορισμός επιπέδων ευαισθησίας / κρισιμότητας κάθε δεδομένου ή στοιχείου.
Διαχειριστής αφαιρούμενων μέσων (USB device control)	Έλεγχος εξωτερικών μέσων αποθήκευσης.
Σύστημα Ελέγχου Τερματικών Συσκευών	Κεντρική διαχείριση, παρακολούθηση και ασφάλεια όλων των τερματικών συσκευών.

Τεκμηρίωση & Αναφορές	Περιγραφή
Πολιτική Διαχείρισης Εξοπλισμού και Δεδομένων	Περιγραφή επιπέδων ταξινόμησης (π.χ. Δημόσιο, Εμπιστευτικό, Κρίσιμο), κριτηρίων και διαδικασίας αντιστοίχισης στοιχείων εξοπλισμού με επίπεδα προστασίας.
Πολιτική Ορθής Χρήσης Εξοπλισμού και Δεδομένων	Καθορίζει τι επιτρέπεται και τι όχι, υποχρεώσεις χρηστών, παραδείγματα κατάχρησης, διαδικασία επιστροφής / απενεργοποίησης του εξοπλισμού.
Πολιτική Διαχείρισης Αφαιρούμενων Μέσων Αποθήκευσης	Καθορίζει τύπους επιτρεπτών μέσων (π.χ. κρυπτογραφημένα USB), διαδικασία έγκρισης χρήσης, διαδικασία καταγραφής / logging.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

- **Ετήσια:**
Προγραμματισμένος εντοπισμός και ταξινόμηση.
- **Ad hoc:**
Μετά από προσθήκη νέου εξοπλισμού στο σύστημα (πχ cloud, OT), οργανωτικές αλλαγές (πχ αναδιάρθρωση IT), σοβαρό περιστατικό, αναθεώρηση πολιτικών, εξωτερικούς ή εσωτερικούς ελέγχους, εκτίμηση κινδύνων (η ταξινόμηση συχνά τροφοδοτείται από τα αποτελέσματα της εκτίμησης κινδύνων).

ΔΙΑΔΙΚΑΣΙΑ No3

Διαχείριση και Γνωστοποίηση Ευπαθειών (Vulnerability Management)

ΣΚΟΠΟΣ

Ο έγκαιρος εντοπισμός και η αντιμετώπιση ευπαθειών, πριν τις εκμεταλλευθούν κακόβουλοι δρώντες.

ΒΗΜΑΤΑ

1. Παρακολούθηση και Συλλογή Πληροφοριών:
- Ανίχνευση νέων ευπαθειών μέσω προμηθευτών λογισμικού / υλικού, βάσεων δεδομένων CVE/CVSS, Threat intelligence feeds, κοκ.
- Καταγραφή σε μητρώο παρακολούθησης ευπαθειών.

2. Εντοπισμός (Scanning) στα συστήματα:
- Εκτέλεση αυτοματοποιημένων σαρώσεων ευπαθειών.
- Επιβεβαίωση ευπάθειας στο περιβάλλον της επιχείρησης (πχ μη αναβαθμισμένα συστήματα, έλλειψη κρυπτογράφησης, ανίσχυροι κωδικοί, ανεπαρκείς έλεγχοι πρόσβασης, ανοιχτές θύρες).
- Καταγραφή asset, IP, λειτουργικού συστήματος, affected version.

3. Αξιολόγηση & Προτεραιοποίηση:
- Εκτίμηση σοβαρότητας (πχ CVSS score).
- Ανάλυση πιθανών επιπτώσεων (impact assessment).
- Προσδιορισμός κρίσιμων υποδομών που επηρεάζονται.
- Κατηγοριοποίηση: Υψηλού κινδύνου → άμεση δράση, Μέσου κινδύνου → προγραμματισμένη δράση, Χαμηλού κινδύνου→ τεκμηρίωση / παρακολούθηση

4. Απόφαση Αντιμετώπισης:
- Επιλογή ενέργειας: Εφαρμογή patch / update, Παράκαμψη, Αποδοχή κινδύνου (σε ειδικές περιπτώσεις και με ειδική τεκμηρίωση).
- Ανάθεση αρμοδιοτήτων σε τεχνικό προσωπικό.

5. Διορθωτικές Ενέργειες (Remediation):
- Εγκατάσταση ενημερώσεων ασφαλείας (patching).
- Επανεκκίνηση ή περιορισμός προσβάσεων (όπου χρειάζεται).
- Παρακολούθηση του αποτελέσματος (verification scan).

6. Τεκμηρίωση & Γνωστοποίηση (αν απαιτείται):

- Ενημέρωση των εσωτερικών stakeholders.
- Γνωστοποίηση της ευπάθειας (zero-day) στην Εθνική Αρχή Κυβερνοασφάλειας όταν προβλέπεται από τον νόμο ή η ευπάθεια επηρεάζει κρίσιμες υποδομές.
- Τήρηση αρχείου ενεργειών και καταγραφή στο μητρώο ευπαθειών.

7. Ανασκόπηση & Βελτίωση

- Ανασκόπηση της διαδικασίας χειρισμού της ευπάθειας.
- Lessons learned (τι λειτούργησε / τι όχι).
- Επικαιροποίηση πολιτικής, εργαλείων, ρόλων και χρόνων απόκρισης.

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

- Οι διαδικασίες καλύπτουν το σύνολο των συστημάτων IT και OT, εφαρμογών, συσκευών και υπηρεσιών ΤΠΕ που χρησιμοποιεί η επιχείρηση και μπορεί να είναι ευάλωτα σε τεχνικές ευπάθειες.
- Αφορούν κάθε τύπο τεχνικής ευπάθειας (ευπάθειες στο λογισμικό ή firmware, λανθασμένες ρυθμίσεις, ανοιχτές θύρες / πρωτόκολλα, κοκ) και όλα τα στάδια διαχείρισης ευπάθειας (ανακάλυψη, τεκμηρίωση, αξιολόγηση, προτεραιοποίηση, διόρθωση, γνωστοποίηση).

ΕΥΘΥΝΗ

Διοίκηση: Εφαρμογή πολιτικής και διαδικασιών διαχείρισης ευπαθειών. Έγκριση διαδικασιών και διασφάλιση παροχής πόρων.

Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών: Κεντρική εποπτεία της πολιτικής διαχείρισης ευπαθειών. Καθορισμός της διαδικασίας γνωστοποίησης στις αρμόδιες αρχές (όταν απαιτείται).

IT / System Administrators: Εντοπισμός, τεχνική αξιολόγηση και εφαρμογή διορθώσεων (patching) σε συστήματα, εφαρμογές και εξοπλισμό. Τακτική εκτέλεση vulnerability scans.

Νομικός Σύμβουλος / DPO: Αξιολόγηση υποχρέωσης γνωστοποίησης σε ρυθμιστικές αρχές.

Τρίτοι / Προμηθευτές (εφόσον εμπλέκονται): Υποχρέωση -μέσω συμβάσεων- γνωστοποίησης ευπαθειών σε συστήματα / υπηρεσίες που παρέχουν και συνεργασία για την αντιμετώπισή τους.

ΕΡΓΑΛΕΙΑ ΚΑΙ ΕΓΓΡΑΦΑ

Εργαλεία	Περιγραφή
Πλατφόρμα Διαχείρισης Ευπαθειών και Απειλών	Εντοπισμός ευπαθειών, συλλογή πληροφοριών για απειλές, εκτίμηση κινδύνων.
Vulnerability Scanning Tools	Σαρώσεις συστημάτων για εντοπισμό γνωστών ευπαθειών.
Σύστημα Διαχείρισης Ενημερώσεων Ασφαλείας	Οργάνωση, εγκατάσταση και παρακολούθηση ενημερώσεων ασφαλείας.
CVSS Scoring Tools	Αξιολόγηση σοβαρότητας ευπαθειών με βάση τον διεθνή δείκτη CVSS.
Asset Inventory / CMDB	Καταγραφή όλων των συστημάτων / υπηρεσιών που μπορεί να επηρεαστούν από ευπάθειες.
Ticketing System / IR Tool	Διαχείριση και παρακολούθηση ενεργειών αντιμετώπισης.

Τεκμηρίωση & Αναφορές	Περιγραφή
Δελτίο Γνωστοποίησης Ευπάθειας προς την Αρχή	Πρότυπο αρχείο που αποστέλλεται στην Εθνική Αρχή Κυβερνοασφάλειας.
Εσωτερικές αναφορές αποκατάστασης / διορθωτικών μέτρων	Τεκμηρίωση της αντιμετώπισης και ανάκαμψης.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

Κάθε μήνα / τρίμηνο για IT ή Σε παράθυρα συντήρησης για OT:
Σάρωση ευπαθειών.
Κάθε μήνα / μετά από σημαντικά updates:
Αναθεώρηση διαχείρισης των patches.
Τουλάχιστον ανά τρίμηνο ή ανά κύκλο ελέγχου:
Επανεξέταση μητρώου ευπαθειών.
Ετήσια / μετά από σημαντικές αλλαγές:
Ανασκόπηση διαδικασιών διαχείρισης ευπαθειών.
Ad hoc:
Σάρωση ευπαθειών μετά από εξωτερικά ερεθίσματα ή απειλές (πχ εμφάνιση νέας κρίσιμης ευπάθειας, έκδοση προειδοποίησης από την Εθνική Αρχή Κυβερνοασφάλειας, εγκατάσταση νέων συστημάτων, κοκ).

ΔΙΑΔΙΚΑΣΙΑ No4

Εκτίμηση Επικινδυνότητας
(Risk Assessment)

ΣΚΟΠΟΣ

Η πρόβλεψη, αξιολόγηση, παρακολούθηση και αντιμετώπιση των κινδύνων κυβερνοασφάλειας, πριν εξελιχθούν σε περιστατικά που θα πλήξουν τις λειτουργίες και την ασφάλεια των δεδομένων. Πρόκειται για κομβικής σημασίας βήμα, καθώς τα ευρήματα της αξιολόγησης αποτελούν θεμέλιο για τα μέτρα που θα εφαρμοστούν ακολούθως.

ΒΗΜΑΤΑ

1. Ανάλυση & υπολογισμός κινδύνων:
- Δημιουργία σεναρίων κινδύνων μέσα από το συνδυασμό εξοπλισμού, απειλών και ευπαθειών.
- Για κάθε σενάριο:
  - Εκτίμηση πιθανότητας επιτυχούς περιστατικού (πχ χαμηλή, μεσαία, υψηλή).
  - Εκτίμηση επιπτώσεων (σε λειτουργίες, οικονομικά μεγέθη, φήμη).

2. Προτεραιοποίηση κινδύνων:
- Ποσοτικοποίηση κάθε κινδύνου με σκορ (πχ μέσω χρήσης risk matrix).
- Ταξινόμηση κινδύνων ανά επίπεδο σημαντικότητας.
- Ορισμός αποδεκτών επιπέδων κινδύνου (χαμηλότερης σημαντικότητας) και των κινδύνων που χρήζουν αντιμετώπισης.

3. Αντιμετώπιση κινδύνων:
- Ανάπτυξη πλάνου αντιμετώπισης των αναγνωρισμένων κινδύνων (Risk Treatment Plan), το οποίο προσδιορίζει ποια τεχνικά, οργανωτικά και επιχειρησιακά μέτρα θα υιοθετηθούν.
- Ανάθεση αρμοδιοτήτων / ευθυνών για κάθε μέτρο.

70% των κυβερνοεπιθέσεων σε ΟΤ προκαλούν διακοπή λειτουργίας από **4** έως **24** ώρες.

Επιχειρήσεις με ΟΤ υποδομές: Προσέγγιση με διαχωρισμό των συστημάτων σε Ζώνες και Διαύλους και δύο εκτιμήσεις κινδύνου. Αναλυτικά:

- **Διαχείριση στοιχείων** (asset management): Καταγραφή όλων των φυσικών και λογικών στοιχείων που απαρτίζουν το ΟΤ (πχ PLC, SCADA, HVAC, αισθητήρες, λογισμικό, δίκτυα, κοκ), καθώς και των ροών δεδομένων και επικοινωνίας μεταξύ τους.
- **Επιλογή του συστήματος ενδιαφέροντος,** στο οποίο θα γίνει εκτίμηση κινδύνου. Πλήρης καθορισμός της περιμέτρου και των στοιχείων του συστήματος.
- **Αρχική εκτίμηση κινδύνου** (ως ανωτέρω).
- **Διαχωρισμός** του συστήματος σε **Ζώνες** (Zones) και **Διαύλους Επικοινωνίας** (Conduits) βάσει συγκεκριμένων κριτηρίων. Πχ ομαδοποίηση σε κάθε Ζώνη φυσικών ή λογικών στοιχείων που εντάσσονται στην ίδια κατηγορία κινδύνου ή εμφανίζουν κοινά χαρακτηριστικά (πχ κρισιμότητα, λειτουργία, φυσική / λογική τοποθεσία, ασύρματες συσκευές, κοκ).
- **Προσδιορισμός Στοχευμένου Επιπέδου Ασφαλείας** (Target Security Level) για κάθε Ζώνη ή Δίαυλο (εκφράζει τον απαιτούμενο / επιθυμητό βαθμό προστασίας), βάσει παραμέτρων όπως κρισιμότητα του συστήματος, επιπτώσεις στην ασφάλεια, ρυθμιστικές απαιτήσεις, κοκ.
- **Σύγκριση** της αρχικής εκτίμησης με τα επιθυμητά επίπεδα κινδύνου. Εντοπισμός των κινδύνων για τους οποίους απαιτούνται επιπλέον μέτρα αντιμετώπισης.
- **Λεπτομερής εκτίμηση κινδύνου** βάσει των αποτελεσμάτων της πρώτης εκτίμησης.
- **Καθορισμός και εφαρμογή οργανωτικών και τεχνικών μέτρων ασφαλείας** για κάθε Επίπεδο (έλεγχος πρόσβασης, αυθεντικοποίηση, διαχείριση αναβαθμίσεων, φυσική προστασία, προστασία από malware, data backup & restore, κοκ).

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

- Σε ολόκληρη την πληροφοριακή / τεχνική υποδομή (συστήματα IT και OT, εφαρμογές, δίκτυα, βάσεις δεδομένων, endpoint devices).
- Σε όλους τους τύπους κινδύνων κυβερνοασφάλειας (ανθρώπινα σφάλματα, τεχνικές αστοχίες, επιθέσεις, διασυνδέσεις με προμηθευτές / συνεργάτες, κοκ).

ΕΥΘΥΝΗ

Διοίκηση:
Αποδοχή κινδύνων και έγκριση του πλάνου αντιμετώπισης.

Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών:
Οργάνωση, συντονισμός και υλοποίηση της εκτίμησης κινδύνου, σε συνεργασία με τις τεχνικές και επιχειρησιακές ομάδες.

Τεχνικές και επιχειρησιακές ομάδες (πχ πληροφορικής, λειτουργιών, κοκ):
Παροχή δεδομένων και τεχνικών πληροφοριών για την αναγνώριση κινδύνων. Εφαρμογή τεχνικών και οργανωτικών μέτρων που αποφασίζονται στο risk treatment plan. Επικαιροποίηση στοιχείων εξοπλισμού και υποδομών (asset owners).

Εσωτερικός Ελεγκτής:
Διαμόρφωση ή υποστήριξη της μεθοδολογίας risk assessment, έλεγχος της τήρησής της.

Υπεύθυνος Συμμόρφωσης & Προμηθευτών:
Ευθυγράμμιση της διαδικασίας με ρυθμιστικά πλαίσια (NIS2, GDPR, ISO 27005 κ.λπ.).

ΕΡΓΑΛΕΙΑ ΚΑΙ ΕΓΓΡΑΦΑ

Εργαλείο / Λειτουργία	Περιγραφή
Λογισμικά εκτίμησης κινδύνου	Αυτοματοποίηση και τεκμηρίωση της διαδικασίας εκτίμησης κινδύνου με τρόπο μεθοδικό, επαναλήψιμο και ευθυγραμμισμένο με διεθνή πρότυπα (πχ ISO 27005, NIST SP 800-30).
Πλατφόρμες GRC	Διαχείριση, παρακολούθηση και τεκμηρίωση διακυβέρνησης, διαχείρισης κινδύνων και συμμόρφωσης με κανονιστικά πλαίσια, πρότυπα και νόμους.
Vulnerability scanners	Αναζήτηση και τεκμηρίωση ευπαθειών.
Εργαλεία Ανάλυσης Επιχειρηματικών Επιπτώσεων (Business Impact Analysis - BIA)	Εντοπισμός κρίσιμων υπηρεσιών και συστημάτων και εκτίμηση συνεπειών από ενδεχόμενη διακοπή (σύνδεση με τη διαδικασία επιχειρησιακής συνέχειας).
Σύστημα Διαχείρισης Περιουσιακών Στοιχείων Πληροφορικής	Αυτοματοποιημένη καταγραφή, εντοπισμός, ταξινόμηση και παρακολούθηση των IT/OT assets (σύνδεση με τη διαδικασία διαχείρισης στοιχείων).

ΕΡΓΑΛΕΙΑ ΚΑΙ ΕΓΓΡΑΦΑ

Τεκμηρίωση & Αναφορές	Περιγραφή
Πλάνο Αντιμετώπισης Κινδύνων	Τεκμηρίωση μέτρων που θα ληφθούν, ποιος είναι υπεύθυνος, και χρονοδιάγραμμα υλοποίησης.
Αναφορά Ανάλυσης Επιχειρηματικών Επιπτώσεων	Περιγραφή επιπτώσεων πιθανών κινδύνων στη λειτουργία της επιχείρησης.
Έκθεση Εκτίμησης Κινδύνων	Καταγραφή απειλών, ευπαθειών, επιπτώσεων, πιθανοτήτων ανά σύστημα ή υπηρεσία.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

- **Περιοδικά (πχ ετήσια):**
Αξιολόγηση και αναθεώρηση.
- **Ad hoc:**
Αξιολόγηση και αναθεώρηση μετά από περιστατικά και σημαντικές αλλαγές σε επιχειρησιακές λειτουργίες και ρυθμιστικό περιβάλλον. Σύνδεση με σχέδια αντιμετώπισης περιστατικών (incident response plans).

ΔΙΑΔΙΚΑΣΙΑ No5

Έλεγχος Πρόσβασης & Διαχείριση Λογαριασμών

(Access Control & Identity Management)

ΣΚΟΠΟΣ

Η ανάπτυξη πλαισίου ασφαλούς διαχείρισης λογαριασμών και προσβάσεων, το οποίο προλαμβάνει παραβιάσεις, περιορίζει τα προνόμια βάσει ρόλων και καταγράφει ποιος έχει πρόσβαση, πού και γιατί.

ΒΗΜΑΤΑ

1. Καθορισμός Πολιτικής Ελέγχου Πρόσβασης.
Τεκμηριωμένη πολιτική που ορίζει:
- Αρχή ελαχιστοποίησης προνομίων (least privilege),
- Χρήση πολυπαραγοντικής αυθεντικοποίησης (MFA),
- Διαχωρισμό ρόλων (Segregation of Duties - SoD),
- Επιτρεπτά επίπεδα πρόσβασης ανά ρόλο.

2. Δημιουργία / Τροποποίηση Πρόσβασης (Onboarding – Access Provisioning):
- Καταχώριση αιτήματος από αρμόδιο προϊστάμενο.
- Αξιολόγηση και έγκριση του αιτήματος (πχ μέσω φόρμας ή εργαλείου IAM).
- Δημιουργία λογαριασμού με κατάλληλο ρόλο και προνόμια.
- Ενεργοποίηση MFA όπου απαιτείται.

3. Χρήση πρόσβασης με περιορισμό και καταγραφή:
- Ο χρήστης αποκτά πρόσβαση μόνο στα απαραίτητα συστήματα / δεδομένα.
- Όλες οι προσβάσεις και ενέργειες καταγράφονται μέσω logs.
- Οι υπηρεσιακοί και προνομιούχοι λογαριασμοί (πχ admin) προστατεύονται με PAM.

4. Αναθεώρηση / Επανεξέταση Πρόσβασης (Access Review):
- Περιοδικός έλεγχος όλων των ενεργών λογαριασμών.
- Διασταύρωση προσβάσεων με τρέχοντες ρόλους.
- Αφαίρεση μη τεκμηριωμένων ή παρωχημένων δικαιωμάτων.
- Επικαιροποίηση ρόλων αν υπάρχουν αλλαγές καθηκόντων.

5. Τερματισμός Πρόσβασης (Offboarding / Revocation):
- Αυτόματη ή άμεση απενεργοποίηση λογαριασμών όταν ο χρήστης αποχωρεί, αλλάζει ρόλο, λήγει σύμβαση ή ανάθεση τρίτου.
- Καταγραφή ενέργειας και ενημέρωση των διαχειριστών.

6. Παρακολούθηση και Έλεγχος (Audit & Monitoring):
- Συνεχής παρακολούθηση της χρήσης των λογαριασμών (πχ μέσω SIEM).
- Ανίχνευση ανωμαλιών / κατάχρησης (πχ πρόσβαση εκτός ωραρίου, privilege escalation).
- Έρευνα περιστατικών και λήψη διορθωτικών μέτρων.

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

- Οι διαδικασίες καλύπτουν το σύνολο των προσβάσεων (σε φυσικά και λογικά συστήματα, ευαίσθητα δεδομένα, κρίσιμες λειτουργίες και υποδομές), ανεξαρτήτως αν παρέχονται σε εσωτερικό ή εξωτερικό προσωπικό (μόνιμοι και εποχικοί υπάλληλοι, πάροχοι ΤΠΕ, προμηθευτές, σύμβουλοι, κοκ).

- Επίσης, καλύπτουν όλο τον κύκλο ζωής πρόσβασης και εφαρμόζονται σε όλα τα τμήματα, λειτουργίες και συστήματα της επιχείρησης.

ΕΥΘΥΝΗ

Διοικητική επίβλεψη:
Διοίκηση: Έγκριση και εφαρμογή των πολιτικών ελέγχου πρόσβασης.

Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών:
Εποπτεία εφαρμογής των πολιτικών ασφάλειας, συμπεριλαμβανομένης της πρόσβασης. Συμμετοχή σε αναθεώρηση και επικαιροποίηση των διαδικασιών.

DPO ή Υπεύθυνος Συμμόρφωσης & Προμηθευτών:
Εξασφάλιση ευθυγράμμισης της διαχείρισης πρόσβασης με το GDPR και τις αρχές ελαχιστοποίησης πρόσβασης και αναλογικότητας.

Τεχνική εφαρμογή:
Τεχνικός Υπεύθυνος Ασφαλείας ή Διαχειριστές Συστημάτων & Δικτύων (IT Administrators):
Δημιουργία, τροποποίηση και απενεργοποίηση λογαριασμών. Ρυθμίσεις ελέγχου πρόσβασης (πχ MFA). Τεχνική επιβολή πολιτικών πρόσβασης.

Καθημερινή συμμόρφωση:
Υπεύθυνοι κάθε τμήματος / προϊστάμενοι:
Έγκριση και αιτιολόγηση πρόσβασης του προσωπικού τους, ανάλογα με τις ανάγκες εργασίας.

Υπάλληλοι / Τελικοί χρήστες:
Τήρηση πολιτικών πρόσβασης. Προστασία διαπιστευτηρίων και αναφορά παραβιάσεων.

ΕΡΓΑΛΕΙΑ ΚΑΙ ΕΓΓΡΑΦΑ

Εργαλεία	Περιγραφή
Σύστημα Διαχείρισης Πρόσβασης & Ταυτοποίησης	Έλεγχος προσβάσεων, αυθεντικοποίηση χρηστών και διαχείριση προνομιακών λογαριασμών.
Role-Based Access Control (RBAC)	Εκχώρηση δικαιωμάτων ανά ρόλο εργασίας, με αρχή ελάχιστου προνομίου.
Multi-Factor Authentication (MFA)	Υποχρεωτική αυθεντικοποίηση για χρήστες σε κρίσιμα συστήματα.
LDAP / Active Directory / Azure AD	Διαχείριση λογαριασμών και ομάδων χρηστών.
Log management / SIEM	Καταγραφή και παρακολούθηση ενεργειών χρηστών.
Privileged Access Management (PAM)	Έλεγχος πρόσβασης σε κρίσιμα/διαχειριστικά συστήματα.
Self-Service Access Request Tool	Αιτήματα και έγκριση προσβάσεων με καταγραφή.
Διαχειριστής Κωδικών (Password Vault)	Ασφαλής αποθήκευση και πολιτική χρήσης κωδικών.

Τεκμηρίωση & Αναφορές	Περιγραφή
Πολιτική Ελέγχου Πρόσβασης	Καθορισμός κανόνων πρόσβασης, ρόλων, διαδικασιών έγκρισης, ελάχιστου προνομίου, MFA κ.ά.
Πίνακας Ρόλων Χρηστών (User Role Matrix)	Ποιος ρόλος έχει πρόσβαση πού, με τι δικαιώματα.
Αρχείο Παραχώρησης Πρόσβασης / Ιστορικό	Τεκμηρίωση ποιος έλαβε πρόσβαση, πότε και με ποια έγκριση.
Αναφορές Επιθεώρησης Προσβάσεων (Access Review Reports)	Περιοδικοί έλεγχοι προσβάσεων για επικαιροποίηση / αφαίρεση περιττών δικαιωμάτων.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

Διαρκής:
Έγκριση νέων προσβάσεων (onboarding). Περιοδική χρήση MFA και πολιτικών αυθεντικοποίησης. Καταγραφή και παρακολούθηση ενεργειών χρηστών (log & audit). Αφαίρεση προσβάσεων μετά από αποχώρηση ή αλλαγή ρόλου (offboarding).
Κάθε 6 ή 12 μήνες:
Έλεγχος και επικαιροποίηση προσβάσεων.
Ετήσια / αλλαγή λειτουργιών και συστημάτων:
Αναθεώρηση πολιτικής ελέγχου πρόσβασης. Έλεγχος συμμόρφωσης MFA & διαχειριστικών λογαριασμών.
Περιοδικά ή μετά από εσωτερικούς ελέγχους:
Αναθεώρηση ρόλων και πολιτικών Role-Based Access Control.
Ad hoc:
Μετά από σοβαρό περιστατικό (πχ παραβίαση λογαριασμού), αλλαγή οργανωτικών ή τεχνολογικών δομών (πχ νέα συστήματα, συγχωνεύσεις), εντοπισμό υπερβολικών ή μη εγκεκριμένων προσβάσεων, αίτημα από ελεγκτικές ή ρυθμιστικές αρχές.

ΔΙΑΔΙΚΑΣΙΑ **No6**

Διαχείριση Κινδύνων Εφοδιαστικής Αλυσίδας (Supply Chain Risk Management)

ΣΚΟΠΟΣ

Η πρόληψη και ο μετριασμός των κινδύνων κυβερνοασφάλειας που προέρχονται από προμηθευτές, παρόχους υπηρεσιών και τρίτους συνεργάτες, οι οποίοι ενδέχεται να χρησιμοποιούν διαφορετικά συστήματα και πρωτόκολλα ασφαλείας.

54% **των μεγάλων επιχειρήσεων θεωρούν τα τρωτά σημεία της εφοδιαστικής αλυσίδας ως τον κυριότερο κίνδυνο κυβερνοασφάλειας.**

ΒΗΜΑΤΑ

Βάσει της πολιτικής και διαδικασιών που αφορούν τη σχέση της επιχείρησης με προμηθευτές και τρίτους:

1. Αναγνώριση και καταγραφή των προμηθευτών και των παρόχων υπηρεσιών ΤΠΕ. Καταγραφή σε Μητρώο Προμηθευτών όλων των τρίτων που έχουν πρόσβαση σε συστήματα ή δεδομένα της επιχείρησης και παρέχουν κρίσιμες υπηρεσίες (πχ cloud, SaaS, IT υποστήριξη, outsourcing).

2.Εκτίμηση κινδύνου ανά προμηθευτή.
Για κάθε προμηθευτή αξιολογούνται:

- η φύση της υπηρεσίας (π.χ. υποδομές, λογισμικό, συντήρηση),
- το επίπεδο πρόσβασης σε κρίσιμα συστήματα ή δεδομένα,
- η πιθανότητα και ο αντίκτυπος ενός περιστατικού που προέρχεται από αυτόν.

Συνίσταται η χρήση **κριτηρίων αξιολόγησης,** ώστε να εκτιμηθεί το επίπεδο κυβερνοασφάλειας κάθε προμηθευτή. Βάσει αυτών, η επιχείρηση μπορεί να υιοθετήσει ένα **ελάχιστα αποδεκτό επίπεδο κυβερνοασφάλειας** για τους προμηθευτές της (πχ να συνεργάζεται μόνο με όσους είναι ευθυγραμμισμένοι με NIS2).

Η αξιολόγηση του επιπέδου κυβερνοασφάλειας βασίζεται σε πρακτικές όπως τυποποιημένα ερωτηματολόγια (βλ. παρακάτω παράδειγμα), πιστοποιήσεις που τεκμηριώνουν την εφαρμογή τεχνικών / οργανωτικών μέτρων σύμφωνα με τα πρότυπα της NIS2, παροχή αντιγράφων από πολιτικές ασφάλειας ή εσωτερικές διαδικασίες του προμηθευτή, κ.α.

Παράδειγμα Ερωτηματολογίου Αξιολόγησης Επιπέδου Κυβερνοασφάλειας

Κατηγορία	Ενδεικτικό ερώτημα
Διακυβέρνηση	Υπάρχει CISO ή Ομάδα Κυβερνοασφάλειας;
Διαχείριση κινδύνου	Γίνεται τακτική παρακολούθηση για πιθανές τρωτότητες και επακόλουθη διόρθωσή τους;
Έλεγχοι ασφαλείας	Γίνεται κρυπτογράφηση ευαίσθητων δεδομένων; Χρησιμοποιούνται firewalls, backups, κοκ;
Συμμόρφωση και Πιστοποίηση	Υπάρχει συμμόρφωση με νομοθετικά πλαίσια όπως NIS2 και GDPR; Εφαρμόζεται ISO27001, NIST, κοκ;
Έλεγχοι και ασκήσεις	Γίνονται τακτικά penetration tests;
Διαχείριση περιστατικών	Υπάρχει σχέδιο διαχείρισης περιστατικών; Πόσο σύντομες είναι οι ενημερώσεις σε περίπτωση περιστατικού;
Επιχειρησιακή συνέχεια	Υπάρχει σχέδιο ανάκαμψης μετά από περιστατικό;

3. Τεκμηρίωση και ενσωμάτωση απαιτήσεων ασφάλειας στις συμβάσεις, που μπορούν να περιλαμβάνουν:

- ελάχιστες τεχνικές απαιτήσεις (πχ κρυπτογράφηση, MFA),
- υποχρέωση γνωστοποίησης περιστατικών (incident notification),
- υποχρέωση συνεχούς συμμόρφωσης με NIS2, GDPR, κ.ά.

Μια σύμβαση ενδέχεται να επιτρέπει σε μια επιχείρηση να ζητάει αναφορές ελέγχου ή αποτελέσματα προηγούμενων ελέγχων από τον προμηθευτή, ή ακόμα και να διενεργεί επιτόπιους ελέγχους.

Είναι αναγκαία η χρήση συμβατικών ρητρών σε MoUs, ή η κατάρτιση **Συμφωνιών Επιπέδου Υπηρεσιών** (Service Level Agreements - SLA), που διασφαλίζουν ότι οι πρακτικές κυβερνοασφάλειας που ακολουθεί ο προμηθευτής, καθώς και το επίπεδο κυβερνοασφάλειας των συστημάτων και υπηρεσιών που παρέχει, ανταποκρίνονται στο επίπεδο αποδοχής κινδύνου της επιχείρησης και στις απαιτήσεις της νομοθεσίας.

Εργαλεία όπως οι **Συμφωνίες Επιπέδου Υπηρεσιών** βοηθούν την επιχείρηση να μειώσει την έκθεσή της σε κινδύνους και να επιδείξει κανονιστική συμμόρφωση, δεσμεύοντας νομικά τους συνεργαζόμενους τρίτους στη διατήρηση ενός αποδεκτού επιπέδου κυβερνοασφάλειας.

4. Εποπτεία και παρακολούθηση της ασφάλειας των προμηθευτών. Διαχρονική εφαρμογή μηχανισμών εποπτείας, ελέγχου και επανεκτίμησης (πχ SLAs, τακτικές αναφορές συμμόρφωσης, δικαίωμα ελέγχου, παρακολούθηση KPIs όπως Μέσος Χρόνος Εντοπισμού & Μέσος Χρόνος Απόκρισης σε Περιστατικά, % συμμόρφωσης με SLA), που διασφαλίζουν ότι ο προμηθευτής:

- εφαρμόζει στην πράξη τα συμφωνηθέντα μέτρα ασφαλείας,
- υποβάλλεται σε επαναξιολόγηση ανά τακτά χρονικά διαστήματα ή όταν αλλάξει κάτι ουσιώδες στη συνεργασία.

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

Η διαδικασία εφαρμόζεται οριζόντια σε:

- Προμηθευτές τεχνολογικών συστημάτων και λύσεων (πχ cloud providers, λύσεις Saas, πάροχοι διαχειριζόμενων υπηρεσιών, IT outsourcing).
- Παρόχους υπηρεσιών με πρόσβαση σε συστήματα / δεδομένα της επιχείρησης (πχ λογιστικά ή νομικά γραφεία με πρόσβαση σε πληροφορίες, εξωτερικοί συνεργάτες που διαχειρίζονται πληροφοριακά συστήματα, data centers / hosting providers).
- Υπεργολάβους και εξωτερικούς συνεργάτες (πχ εργολάβοι έργων IT/OT που αποκτούν πρόσβαση σε υποδομές).

ΕΥΘΥΝΗ

Διοίκηση:
Έγκριση πολιτικής και διαδικασιών διαχείρισης κινδύνων από την εφοδιαστική αλυσίδα.

Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών:
Συντονισμός διαδικασίας αξιολόγησης κινδύνου προμηθευτών. Διασφάλιση εφαρμογής τεχνικών και οργανωτικών μέτρων.

Υπεύθυνος Συμμόρφωσης & Προμηθευτών:
Καθορισμός πολιτικών και προτύπων για τον χειρισμό προμηθευτών (πχ τυποποιημένοι όροι ασφάλειας, due diligence). Παρακολούθηση συμμόρφωσης τρίτων μερών με τις συμβατικές και κανονιστικές υποχρεώσεις.

Τμήμα Προμηθειών / Νομικό Τμήμα:
Εφαρμογή συμβατικών απαιτήσεων ασφαλείας στις συμφωνίες. Εξασφάλιση ότι οι αξιολογήσεις κινδύνου λαμβάνονται υπόψη πριν τη σύναψη / ανανέωση συνεργασίας.

Εσωτερικός Ελεγκτής:
Επαλήθευση εφαρμογής της διαδικασίας. Περιοδικός έλεγχος της αποτελεσματικότητας των μέτρων. Εισήγηση διορθωτικών ενεργειών σε περιπτώσεις μη συμμόρφωσης.

ΕΡΓΑΛΕΙΑ ΚΑΙ ΕΓΓΡΑΦΑ

Εργαλεία	Περιγραφή
Σύστημα καταγραφής και παρακολούθησης προμηθευτών (Supplier Registry Tool)	Οργάνωση και δυναμική ταξινόμηση των προμηθευτών και των παρεχόμενων υπηρεσιών.
Πλατφόρμα αξιολόγησης προμηθευτών (Vendor Risk Assessment Tool)	Συλλογή πληροφοριών, αξιολογήσεων και αυτοαξιολογήσεων κυβερνοασφάλειας.
Τυποποιημένα ερωτηματολόγια	Χρήση πριν από προμήθεια ή ανάθεση για αξιολόγηση κυβερνοασφάλειας τρίτων.
Checklists συμβατότητας με απαιτήσεις ασφάλειας	Για εσωτερικούς και εξωτερικούς ελέγχους συμμόρφωσης προμηθευτών.
Σύστημα παρακολούθησης / ενημέρωσης για κυβερνοαπειλές (Threat Intelligence)	Για εκτίμηση κινδύνων ανά προμηθευτή (ιδίως για βασικές οντότητες).

Τεκμηρίωση & Αναφορές	Περιγραφή
Πολιτική Διαχείρισης Προμηθευτών και Παρόχων ΤΠΕ	Καθορισμός συνολικής προσέγγισης της οντότητας στη διαχείριση των σχετικών κινδύνων.
Πολιτική Διαχείρισης Συμβολαίων ΤΠΕ	Ορισμός συμβατικών διαδικασιών, ρητρών ασφάλειας και μηχανισμών ελέγχου και επιβολής.
Διαδικασία Αξιολόγησης και Επιλογής Προμηθευτών	Καθορισμός κριτηρίων επιλογής (κυβερνοασφάλεια, πιστοποιήσεις, κοκ).
Κατάλογος Απαιτήσεων Κυβερνοασφάλειας	Τεχνικές και οργανωτικές απαιτήσεις που πρέπει να πληρούν οι προμηθευτές και τα προϊόντα τους.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

Περιοδικά (πχ ετήσια):
Επανάληψη της αρχικής αξιολόγησης κινδύνου και μέτρων συμμόρφωσης.
Ad hoc:
Επαναξιολόγηση μετά από περιστατικά που σχετίζονται με παροχή προϊόντων και υπηρεσιών ΤΠΕ, εμφάνιση νέων απειλών, αλλαγή τεχνολογίας (πχ μετάβαση σε cloud), αλλαγή τύπου δεδομένων (πχ πρόσβαση σε προσωπικά/ευαίσθητα δεδομένα), αλλαγή στο ιδιοκτησιακό καθεστώς του προμηθευτή.

ΔΙΑΔΙΚΑΣΙΑ **No7**

Ασφαλής Παραμετροποίηση Εξοπλισμού Πληροφορικής & Διαχείριση Αλλαγών

(Secure Configuration & Change Management)

ΣΚΟΠΟΣ

Η διαμόρφωση ενός σταθερού, ελεγχόμενου και κυβερνοασφαλούς τεχνικού περιβάλλοντος και η προστασία από σφάλματα και τρωτά σημεία λόγω αλλαγών.

Η ασφαλής παραμετροποίηση καθορίζει «πώς πρέπει να είναι ασφαλές» το σύστημα, ενώ η διαχείριση αλλαγών καθορίζει «πώς αλλάζει» το σύστημα χωρίς να χάσει αυτή την ασφάλεια.

ΒΗΜΑΤΑ

Ασφαλής παραμετροποίηση:

1. Καταγραφή όλων των συστημάτων / συσκευών που υπόκεινται σε παραμετροποίηση. Κατηγοριοποίηση ανάλογα με κρισιμότητα, λειτουργία και κίνδυνο.

2. Καθορισμός Πολιτικής Παραμετροποίησης: Τήρηση προτύπων ασφαλείας (π.χ. CIS, ISO). Εφαρμογή αρχών “least privilege” & “least functionality”.

3. Εκτέλεση Παραμετροποίησης: Απενεργοποίηση μη απαραίτητων λειτουργιών, ports, accounts. Εφαρμογή ισχυρών πολιτικών ασφάλειας (πχ password policies, logging, firewall rules).

4. Έλεγχος Συμμόρφωσης: Χρήση εργαλείων για έλεγχο συμφωνίας των ρυθμίσεων με την πολιτική. Τεκμηρίωση αποκλίσεων.

5. Διορθωτικές Ενέργειες: Αποκατάσταση αποκλίσεων ή μη συμμορφώσεων.

6. Τεκμηρίωση: Τήρηση πλήρους αρχείου για κάθε σύστημα: ημερομηνία παραμετροποίησης, υπεύθυνος, status.

7. Επαναληπτικοί Έλεγχοι: Περιοδική ανασκόπηση (πχ ανά 6μηνο ή όταν αλλάζει η υποδομή).

Διαχείριση αλλαγών:

1. Καταγραφή Αιτήματος Αλλαγής (Request for Change - RFC): Τεκμηρίωση αιτίας, περιγραφής, εμπλεκόμενων συστημάτων, κρίσιμων παραμέτρων.

2. Κατηγοριοποίηση & Προτεραιοποίηση ανάλογα με τον κίνδυνο, την επίδραση και την πολυπλοκότητα.

3. Αξιολόγηση Αντικτύπου: Ανάλυση κινδύνων για ασφάλεια, διαθεσιμότητα, συνέπεια. Έλεγχος συμβατότητας με παραμετροποίηση.

4. Έγκριση από κατάλληλους ρόλους (Υπεύθυνο Ασφάλειας, IT manager, Διοίκηση).

5. Προγραμματισμός & Πλάνο Υλοποίησης: Ορισμός ημερομηνίας / ώρας, σχεδιασμός rollback, ενημέρωση εμπλεκομένων.

6. Δοκιμές σε ασφαλές περιβάλλον (πχ staging ή sandbox).

7. Εκτέλεση της αλλαγής: Υλοποίηση από εξουσιοδοτημένο προσωπικό, καταγραφή ενεργειών.

8. Παρακολούθηση & Επιβεβαίωση Επιτυχίας

9. Τεκμηρίωση αποτελέσματος, απόκλισης, επιπτώσεων και lessons learned.

10. Αρχειοθέτηση στο Μητρώο Αλλαγών: Καταγραφή στο κεντρικό change log με ημερομηνία, αποτέλεσμα, υπεύθυνο.

Μετά από κάθε αλλαγή πρέπει να ελέγχεται αν παραμένουν οι ασφαλείς παραμετροποιήσεις.

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

- Ασφαλής παραμετροποίηση: Στο σύνολο του υλικού, λογισμικού, υπηρεσιών και δικτύων.
- Διαχείριση αλλαγών: Σε κάθε αλλαγή που
  - επηρεάζει πληροφοριακά συστήματα, δικτυακές υποδομές ή λογισμικά,
  - σχετίζεται με επισκευές, αναβαθμίσεις, ρυθμίσεις ή συντήρηση,
  - αλλάζει τον τρόπο που λειτουργεί ή αλληλεπιδρά ένα σύστημα,
  - ενδέχεται να επηρεάσει τη διαθεσιμότητα, ακεραιότητα ή εμπιστευτικότητα των πληροφοριών.

ΕΥΘΥΝΗ

Διοίκηση:
Έγκριση και μέριμνα εφαρμογής των διαδικασιών.

Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών:
Σχεδίαση, υλοποίηση και παρακολούθηση των διαδικασιών ασφαλούς παραμετροποίησης. Συνεργασία με τον Τεχνικό Υπεύθυνο Ασφαλείας και τις τεχνικές ομάδες για την επιλογή εργαλείων και μεθόδων.

Τεχνικός Υπεύθυνος Ασφαλείας ή Τεχνικές Ομάδες:
Εκτέλεση τεχνικών ρυθμίσεων. Χρήση εργαλείων παραμετροποίησης και συμμόρφωσης.

Ελεγκτής Ασφάλειας:
Έλεγχος συμμόρφωσης και αποτελεσματικότητας μέτρων.

ΕΡΓΑΛΕΙΑ ΚΑΙ ΕΓΓΡΑΦΑ

Εργαλεία	Περιγραφή
Εργαλεία Διαχείρισης Ρυθμίσεων	Καταγραφή, εφαρμογή, έλεγχος και αυτοματοποίηση ρυθμίσεων σε συστήματα, λογισμικά και δίκτυα.
Asset inventory tools	Καταγραφή και κατηγοριοποίηση συστημάτων, κοκ.
Vulnerability scanners	Αναζήτηση και τεκμηρίωση ευπαθειών.
Benchmarking scripts	Σύγκριση με πρότυπα ασφαλείας.
Σύστημα Διαχείρισης Αλλαγών	Οργάνωση, έγκριση, παρακολούθηση και τεκμηρίωση αλλαγών στα πληροφοριακά συστήματα.
Version Control Systems	Αλλαγές σε κώδικα ή αρχεία ρυθμίσεων.
Δοκιμαστικά περιβάλλοντα	Αξιολόγηση αλλαγών πριν την εφαρμογή τους.
Εργαλεία παρακολούθησης	Παρακολούθηση σε πραγματικό χρόνο της κατάστασης και λειτουργίας των πληροφοριακών συστημάτων μετά από κάποια αλλαγή, και άμεση ειδοποίηση σε περίπτωση δυσλειτουργίας ή αποκλίσεων.

ΕΡΓΑΛΕΙΑ ΚΑΙ ΕΓΓΡΑΦΑ

Τεκμηρίωση & Αναφορές	Περιγραφή
Πολιτική ασφαλούς παραμετροποίησης	Ορισμός πρότυπων ρυθμίσεων ανά τύπο συστήματος (πχ Windows servers, routers).
Κατάλογος παραμετροποιήσεων	Αναλυτική τεκμηρίωση για όλες τις ρυθμίσεις ασφαλείας (πχ log retention, password policy).
Έκθεση συμμόρφωσης με πρότυπα (πχ CIS)	Τεκμηρίωση της αξιολόγησης συστημάτων ως προς βέλτιστες πρακτικές.
Αναφορές επιθεώρησης παραμετροποίησης	Περιοδικές αναφορές από ελέγχους.
Πολιτική διαχείρισης αλλαγών	Καθορισμός πλαισίου αλλαγών (τύποι, έγκριση, τεκμηρίωση, rollback).
Αξιολόγηση αντικτύπου	Τεκμηρίωση πιθανών επιπτώσεων της αλλαγής (πχ σε ασφάλεια ή διαθεσιμότητα).
Έκθεση αποδοχής αλλαγής	Καταγραφή του αποτελέσματος και αν χρειάστηκε rollback.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

Ασφαλής παραμετροποίηση:
- **Άμεσα** (κατά την αρχική εγκατάσταση συστήματος / υπηρεσίας)
- **Άμεσα ή σε προκαθορισμένο διάστημα** (μετά από αλλαγές ή ενημερώσεις)
- **Εύλογο διάστημα** (πχ 30 ημέρες ή νωρίτερα για κρίσιμα συστήματα) με τον εντοπισμό νέας ευπάθειας ή απειλής
- **Κάθε 6-12 μήνες** (σύμφωνα με την πολιτική ασφάλειας της επιχείρησης)

Διαχείριση αλλαγών:
- **Μηνιαία ή ανά τρίμηνο:** Ομαδοποίηση σε κύκλους αλλαγών (πχ ενημερώσεις λειτουργικών συστημάτων).
- **Ad hoc:** Προγραμματισμένη (πχ αναβάθμιση) ή επείγουσα αλλαγή (πχ για λόγους ασφάλειας).

ΔΙΑΔΙΚΑΣΙΑ No8

Ασφαλής Απόκτηση & Ανάπτυξη Εφαρμογών (Secure Software Acquisition & Development Lifecycle)

ΣΚΟΠΟΣ

Η ενσωμάτωση της ασφάλειας σε όλη τη διάρκεια του κύκλου ζωής των εφαρμογών – από το στάδιο του σχεδιασμού έως και την παραγωγική λειτουργία.

ΒΗΜΑΤΑ

1. Καθορισμός απαιτήσεων ασφαλείας, ήδη από το στάδιο ανάλυσης και σχεδιασμού. Λαμβάνονται υπόψη η κρισιμότητα της εφαρμογής, το είδος των δεδομένων που επεξεργάζεται και οι πιθανοί κίνδυνοι κυβερνοασφάλειας.

2. Εφαρμογή αρχών ασφαλούς σχεδιασμού: «Ασφάλειας από το Σχεδιασμό» (Security by Design), «Ασφάλειας εξ ορισμού» (Security by Default), «Ελάχιστων προνομίων» (Least Privilege) και «Μηδενικής εμπιστοσύνης» (Zero Trust).

3. Ανάπτυξη με πρακτικές ασφαλούς κώδικα. Τήρηση οδηγιών, αποφυγή ευπαθειών, εκπαίδευση προγραμματιστών σε θέματα ασφαλούς ανάπτυξης.

4. Δοκιμές και έλεγχοι ασφαλείας: Ανάλυση πηγαίου κώδικα, έλεγχος της εφαρμογής κατά την εκτέλεση, επιθετικός έλεγχος για εντοπισμό ευπαθειών. Οι έλεγχοι γίνονται σε όλα τα στάδια, και οπωσδήποτε πριν την παραγωγή.

5. Διαχωρισμός περιβαλλόντων: Αυστηρός διαχωρισμός ανάπτυξης, δοκιμών και παραγωγής. Εφαρμογή ελέγχων πρόσβασης και περιορισμένων δικαιωμάτων σε κάθε περιβάλλον.

6. Διαχείριση εξαρτήσεων και λογισμικού τρίτων: Αξιολόγηση και τακτική ενημέρωση βιβλιοθηκών / πακέτων που χρησιμοποιούνται. Έλεγχος για γνωστές ευπάθειες.

7. Τεκμηρίωση και παρακολούθηση: Καταγραφή όλων των ενεργειών, ελέγχων, αποφάσεων και ευρημάτων. Διατήρηση audit trail για λόγους συμμόρφωσης και αναφοράς.

8. Προετοιμασία για παραγωγική λειτουργία: Ολοκλήρωση δοκιμών ασφάλειας. Εφαρμογή διαδικασιών “go-live security checklist”. Εξασφάλιση ότι έχουν ενσωματωθεί όλοι οι έλεγχοι.

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

Σε κάθε εφαρμογή που:

- Αναπτύσσεται εσωτερικά από την οντότητα.
- Αποκτάται από τρίτους (αγορασμένο λογισμικό ή software as a service).
- Ενσωματώνεται σε κρίσιμα επιχειρησιακά συστήματα, πχ ERP, SCADA, πλατφόρμες ηλεκτρονικής διακυβέρνησης.
- Επεξεργάζεται ή αποθηκεύει ευαίσθητα δεδομένα.
- Επηρεάζει τη συνέχεια των υπηρεσιών ή την ακεραιότητα των πληροφοριακών συστημάτων.

ΕΥΘΥΝΗ

Διοίκηση:
Τελική ευθύνη για τις εν λόγω διαδικασίες.

Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών:
Επιχειρησιακή ευθύνη για την εφαρμογή μέτρων ασφαλούς απόκτησης και ανάπτυξης εφαρμογών.

Τεχνικός Υπεύθυνος Ασφαλείας ή Ομάδα ανάπτυξης / απόκτησης λογισμικού:
Εφαρμογή στην πράξη των απαιτήσεων συγγραφής ασφαλούς κώδικα, τήρησης αρχών ασφαλούς σχεδιασμού, κοκ.

Υπεύθυνος Συμμόρφωσης & Προμηθευτών ή Ομάδα προμηθειών και νομικής υποστήριξης:
Ενσωμάτωση ρητρών και απαιτήσεων ασφαλείας σε συμβάσεις λογισμικού που αποκτάται από τρίτους.

Προσωπικό που εμπλέκεται στον κύκλο ζωής εφαρμογών:
Γνώση και εφαρμογή των πολιτικών ασφαλείας, ιδίως όταν εμπλέκεται σε έργα πληροφορικής ή λήψη αποφάσεων που επηρεάζουν το λογισμικό.

ΕΡΓΑΛΕΙΑ ΚΑΙ ΕΓΓΡΑΦΑ

Εργαλεία	Περιγραφή
Εργαλεία ανάλυσης και ελέγχου ασφάλειας	SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing), SCA (Software Composition Analysis), Vulnerability scanners για περιβάλλοντα ανάπτυξης και παραγωγής.
Εργαλεία DevOps / DevSecOps	CI/CD pipelines με ενσωμάτωση ελέγχων ασφαλείας, Container security tools.
Εργαλεία παρακολούθησης και τεκμηρίωσης	Version control, Ticketing / issue tracking, Wiki / knowledge base, Log management.

Τεκμηρίωση & Αναφορές	Περιγραφή
Πρακτικές ασφαλούς ανάπτυξης εφαρμογών	Καθορισμός σκοπού και πεδίου εφαρμογής, ρόλων και υπευθυνοτήτων, εφαρμοζόμενων αρχών, υποχρεωτικών διαδικασιών, ελάχιστων προτύπων ασφάλειας, κοκ.
Τεχνική τεκμηρίωση	Τεκμηρίωση αρχιτεκτονικής εφαρμογών, κατάλογος εξαρτήσεων / βιβλιοθηκών (Software Bill of Materials – SBOM), αποτελέσματα SAST / DAST / pen test και αναφορές ευπαθειών, πλάνα αποκατάστασης ευρημάτων, κοκ.
Τεκμηρίωση συμμόρφωσης	Πρακτικά αξιολογήσεων / συναντήσεων ασφαλείας, τεκμηρίωση κριτηρίων εγκρίσεων λογισμικού πριν την παραγωγή, έγγραφα εκπαιδεύσεων προσωπικού για ασφαλή ανάπτυξη.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

Δεν ορίζεται με συγκεκριμένα ημερολογιακά όρια, αλλά ρυθμίζεται με βάση το πλαίσιο του κύκλου ζωής της εφαρμογής:

Κατά τον σχεδιασμό και πριν την υλοποίηση:
Καθορισμός απαιτήσεων ασφαλείας, εφαρμογή αρχών.

Σε όλη τη διάρκεια της ανάπτυξης:
Εφαρμογή πρακτικών ασφαλούς συγγραφής κώδικα. Συνεχής δοκιμή και αξιολόγηση του κώδικα με στατικές και δυναμικές μεθόδους.

Πριν από τη μετάβαση σε παραγωγική λειτουργία:
Υλοποίηση τελικών δοκιμών ασφάλειας. Επιβεβαίωση ότι έχουν εφαρμοστεί όλα τα μέτρα ασφαλείας.

Διαρκώς, για τα περιβάλλοντα ανάπτυξης / δοκιμής / παραγωγής:
Διαχωρισμός περιβαλλόντων. Πρέπει να ισχύει μόνιμα και να ελέγχεται περιοδικά.

B.3
ΔΙΑΔΙΚΑΣΙΕΣ ΚΑΙ ΒΗΜΑΤΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΠΕΡΙΣΤΑΤΙΚΑ

ΔΙΑΔΙΚΑΣΙΑ No9

Διαχείριση Περιστατικών Κυβερνοασφάλειας (Σχέδιο Αντιμετώπισης Περιστατικών – Incident Response Plan)

Το Σχέδιο Αντιμετώπισης Περιστατικών αφορά το σχεδιασμό ενεργειών προετοιμασίας για την αντιμετώπιση περιστατικού, καθώς και ενεργειών διαχείρισης και ανάκαμψης από αυτό.

ΣΚΟΠΟΣ

Η έγκαιρη και αποτελεσματική απόκριση στα περιστατικά ώστε να ελαχιστοποιηθούν οι επιπτώσεις τους στις λειτουργίες, τα οικονομικά μεγέθη και τη φήμη της επιχείρησης.

ΒΗΜΑΤΑ

ΠΡΙΝ το περιστατικό (Προετοιμασία):

1. Εκπόνηση πολιτικής και πλάνου διαχείρισης περιστατικών.
Η πολιτική καθορίζει «τι» και «πώς»:
- Σκοπός – πεδίο εφαρμογής
- Καθορισμός ρόλων και ομάδων (π.χ. υπεύθυνος διαχείρισης περιστατικών).
- Ορισμός διαδικασιών
- Σύνδεση με άλλα σχέδια (πχ επιχειρησιακή συνέχεια, ανάκαμψη από καταστροφές)

Το πλάνο περιγράφει το «πώς» εκτελείται στην πράξη η απόκριση:
- Φάσεις απόκρισης
- Διαδικασία αναγνώρισης και καταγραφής
- Ενεργοποίηση Ομάδας Απόκρισης
- Επικοινωνία με εσωτερικά και εξωτερικά μέρη
- Τεχνικές ενέργειες απόκρισης
- Διαδικασία ανάκαμψης και επαναφοράς

2. Εκπαίδευση, δοκιμές (π.χ. ασκήσεις προσομοίωσης).

3. Δημιουργία εργαλείων αναφοράς και λογισμικού παρακολούθησης.

ΚΑΤΑ ΤΗ ΔΙΑΡΚΕΙΑ του περιστατικού (Απόκριση):

4. Ανίχνευση και επιβεβαίωση του περιστατικού.
5. Ανάλυση αιτίας και αξιολόγηση του εύρους/αντίκτυπου.
6. Ενεργοποίηση πλάνου απόκρισης και ενημέρωση αρμοδίων.
7. Εφαρμογή τεχνικών και οργανωτικών μέτρων περιορισμού της εξάπλωσης.

ΜΕΤΑ το περιστατικό (Αποκατάσταση):

8. Ανάκαμψη συστημάτων και δεδομένων, επαναφορά λειτουργιών.
9. Αναφορά στην Εθνική Αρχή Κυβερνοασφάλειας.
10. Αξιολόγηση της απόκρισης και αναθεώρηση του πλάνου.
11. Καταγραφή του περιστατικού στο ιστορικό (incident log).

Η επιχείρηση, σε περίπτωση σημαντικού περιστατικού, υποχρεούται να ενημερώσει άμεσα την Εθνική Αρχή Κυβερνοασφάλειας βάσει χρονοδιαγράμματος. Ένα περιστατικό θεωρείται σημαντικό αν έχει προκαλέσει ή μπορεί να προκαλέσει:

- **Σοβαρή διατάραξη στη λειτουργία ή οικονομική ζημιά στην επιχείρηση.**
- **Σημαντική υλική ή μη ζημιά σε άλλα φυσικά ή νομικά πρόσωπα.**

Χρονοδιάγραμμα κοινοποίησης περιστατικών στην Εθνική Αρχή Κυβερνοασφάλειας

Πότε υποβάλλονται αναφορές	Τι περιέχουν οι αναφορές
Έγκαιρη προειδοποίηση εντός 24 ωρών από τη στιγμή που αντιλήφθηκαν το περιστατικό	• Προκαταρκτική αξιολόγηση (είδος περιστατικού, πιθανός αντίκτυπος).
Κοινοποίηση περιστατικού εντός 72 ωρών από τη στιγμή που αντιλήφθηκαν το περιστατικό	• Πλήρη αναφορά με επικαιροποίηση πληροφοριών. • Αρχική αξιολόγηση (σοβαρότητα, αντίκτυπος, ενδείξεις παραβίασης, κοκ).
Ενδιάμεση έκθεση, αν αιτηθεί από την Εθνική Αρχή Κυβερνοασφάλειας	• Επικαιροποίηση της κατάστασης.
Τελική έκθεση το αργότερο σε 1 μήνα μετά την υποβολή της κοινοποίησης	• Λεπτομερή περιγραφή του περιστατικού (σοβαρότητα, αντίκτυπος, κοκ). • Είδος απειλής ή βασική αιτία που ενδεχομένως προκάλεσε το περιστατικό. • Μέτρα αντιμετώπισης που εφαρμόζονται.

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

- Οι διαδικασίες αφορούν το σύνολο των περιστατικών που σχετίζονται με την ασφάλεια των συστημάτων δικτύου και πληροφοριών της επιχείρησης. Εφαρμόζονται σε όλα τα πληροφοριακά συστήματα, τα δίκτυα, τις υποδομές ΤΠΕ και τις υπηρεσίες που χρησιμοποιούνται για την εκτέλεση λειτουργιών ή την παροχή υπηρεσιών.

Οι διαδικασίες πρέπει να καλύπτουν όλο τον κύκλο ζωής ενός περιστατικού, από την ανίχνευση έως την τελική ανάκαμψη.

ΕΥΘΥΝΗ

Διοίκηση:
Έγκριση της πολιτικής διαχείρισης περιστατικών. Παροχή των αναγκαίων πόρων και υποστήριξης. Λογοδοσία για πλημμελή εφαρμογή των μέτρων. Συμμετοχή στην ενημέρωση (reporting) σοβαρών περιστατικών.

Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών:
Συνεργασία με τον Υπεύθυνο Διαχείρισης Περιστατικών (αν είναι διαφορετικά πρόσωπα). Απευθείας αναφορά στη Διοίκηση για θέματα κυβερνοασφάλειας. Κοινοποίηση σημαντικών περιστατικών στην Εθνική Αρχή Κυβερνοασφάλειας εντός των προθεσμιών.

Τεχνικός Υπεύθυνος Ασφαλείας:
Διαχείριση και συντονισμός της απόκρισης σε περιστατικά. Αναλυτικά:
- Συντονισμός ενεργειών κατά την ανίχνευση, ανάλυση, απόκριση και ανάκαμψη.
- Συνεργασία με εσωτερικές ομάδες και την Εθνική Αρχή Κυβερνοασφάλειας.
- Τεκμηρίωση και αξιολόγηση αποτελεσματικότητας των ενεργειών.

Μπορεί να ταυτίζεται με τον Υπεύθυνο Ασφάλειας αν η επιχείρηση είναι μικρή ή δεν διαθέτει εξειδικευμένο προσωπικό.

Εσωτερικός Σύνδεσμος Εποπτείας (όταν υπάρχει εξωτερικός ανάδοχος):
Αν η διαχείριση περιστατικών έχει ανατεθεί σε εξωτερικό συνεργάτη, η επιχείρηση ορίζει υπάλληλο-σύνδεσμο, ο ρόλος του οποίου είναι:
- Η επίβλεψη και εποπτεία των ενεργειών του εξωτερικού αναδόχου.
- Η διασφάλιση της πλήρους συμμόρφωσης του παρόχου με την πολιτική και τις διαδικασίες της επιχείρησης.

Ομάδα Διαχείρισης Περιστατικών (Incident Response Team):
Εκτέλεση εντολών και διαδικασιών ανίχνευσης, απομόνωσης, αποκατάστασης και επαναφοράς συστημάτων. Η σύστασή της δεν είναι υποχρεωτική. Οι συμμετέχοντες παρακολουθούν εκπαίδευση και ενεργούν σύμφωνα με τα σενάρια της πολιτικής. Ο αριθμός τους εξαρτάται από το μέγεθος της επιχείρησης, τον βαθμό πολυπλοκότητας της τεχνολογικής υποδομής, τη διαχείριση ευαίσθητων δεδομένων, κοκ.

Τυπική δομή Ομάδας Διαχείρισης Περιστατικών		
Ρόλος	**Τμήμα προέλευσης**	**Κύριες αρμοδιότητες**
Υπεύθυνος Ασφάλειας	IT	Εποπτεία των ενεργειών διαχείρισης.
Τεχνικός Υπεύθυνος Ασφαλείας (ή Συντονιστής Απόκρισης)	IT	Συντονισμός ενεργειών ανίχνευσης, ανάλυσης, απόκρισης και ανάκαμψης.
Τεχνικός Αναλυτής	IT	Εντοπισμός αιτίας, ανάλυση logs, περιορισμός περιστατικού.
SOC Analyst	IT	Ανίχνευση και απόκριση σε περιστατικά.
Νομικός Συνεργάτης	Νομικό Τμήμα / Τμήμα Συμμόρφωσης / DPO	Εκτίμηση υποχρεώσεων αναφοράς.
Εκπρόσωπος Επικοινωνίας	Επικοινωνία / Μάρκετινγκ	Σχέδιο επικοινωνίας με Εθνική Αρχή Κυβερνοασφάλειας και κοινό.
Εκπρόσωπος Διοίκησης	ΔΣ	Απόφαση για κρίσιμες ενέργειες. Ενεργοποίηση πλάνου επιχειρησιακής συνέχειας.

ΕΡΓΑΛΕΙΑ ΚΑΙ ΕΓΓΡΑΦΑ

Εργαλείο / Λειτουργία	**Περιγραφή**
SIEM (Security Information and Event Management)	Κεντρική συλλογή, ανάλυση και συσχέτιση logs από συστήματα, δίκτυα και εφαρμογές.
EDR/XDR (Endpoint / Extended Detection & Response)	Ανίχνευση και αποκλεισμός κακόβουλης δραστηριότητας σε τελικές συσκευές.
IDS/IPS (Intrusion Detection / Prevention System)	Παρακολούθηση και αποκλεισμός ύποπτης δραστηριότητας σε δίκτυα.
Ticketing / IR platform	Σύστημα διαχείρισης περιστατικών.
Αυτόματες ειδοποιήσεις (alerts)	Πχ μέσω email / SMS ή dashboard σε SOC / NOC.
Backup / DR system	Εργαλεία ανάκαμψης και επαναφοράς (recovery).
Log management tools	Ασφαλής αποθήκευση αρχείων καταγραφής, χρονική σήμανση (timestamp), integrity protection.
Threat intelligence feeds	Πηγές κυβερνοαπειλών για συσχέτιση περιστατικών.

ΕΡΓΑΛΕΙΑ ΚΑΙ ΕΓΓΡΑΦΑ

Τεκμηρίωση & Έγγραφα	Περιγραφή
Πολιτική Διαχείρισης Περιστατικών Κυβερνοασφάλειας	Περιγραφή ρόλων, διαδικασιών, τύπων περιστατικών, κριτηρίων σοβαρότητας.
Σχέδιο Απόκρισης σε Περιστατικά (IR Plan)	Αναλυτικό εγχειρίδιο με βήμα-βήμα ενέργειες για κάθε τύπο περιστατικού.
Έντυπα / φόρμες αναφοράς περιστατικών	Εσωτερικές φόρμες για προσωπικό ή help-desk. Εξωτερικές φόρμες για Εθνική Αρχή Κυβερνοασφάλειας (έγκαιρη προειδοποίηση, κοινοποίηση, ενδιάμεση και τελική έκθεση).
Τελικό δελτίο (Post-Incident Review Report)	Αξιολόγηση της απόκρισης, μαθησιακά σημεία, διορθωτικά μέτρα.
Ετήσιο πλάνο δοκιμών IR	Πρόγραμμα δοκιμών, πχ tabletop, simulation, red team.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

Ad hoc:
Εκτέλεση Σχεδίου Απόκρισης κάθε φορά που ανιχνεύεται περιστατικό. Αξιολόγηση και επικαιροποίηση μετά από σοβαρά περιστατικά και αλλαγές σε επιχειρηματικές λειτουργίες και περιβάλλον των κυβερνοαπειλών.

ΔΙΑΔΙΚΑΣΙΑ No10

Επιχειρησιακή Συνέχεια & Διαχείριση Κρίσεων (Business Continuity Plan & Crisis Management Plan)

Το Σχέδιο Επιχειρησιακής Συνέχειας αφορά προετοιμασία και προδραστικές ενέργειες, που επιτρέπουν τη γρήγορη ανάκαμψη της επιχείρησης σε περίπτωση έκτακτων συνθηκών που θέτουν σε κίνδυνο τη συνέχειά της.

ΣΚΟΠΟΣ

Η διασφάλιση της ελάχιστης λειτουργικότητας των κρίσιμων υπηρεσιών της επιχείρησης, ακόμα και μετά από σοβαρή διακοπή, κυβερνοεπίθεση ή τεχνική καταστροφή, με κατάρτιση σχεδίων ενεργοποίησης και ανάκαμψης και ενίσχυση της ανθεκτικότητας των συστημάτων.

ΒΗΜΑΤΑ

ΠΡΙΝ το περιστατικό (Προετοιμασία):

1. Ανάλυση Επιχειρησιακών Επιπτώσεων (Business Impact Analysis - BIA): Συμβάλλει στην κατανόηση των κρίσιμων λειτουργιών της επιχείρησης.

- Εντοπισμός κρίσιμων υπηρεσιών και συστημάτων.
- Εκτίμηση συνεπειών από ενδεχόμενη διακοπή.
- Ορισμός δεικτών αποκατάστασης: RTO (Recovery Time Objective), RPO (Recovery Point Objective).

2. Κατάρτιση Πλάνου Επιχειρησιακής Συνέχειας: Προετοιμασία για την αντιμετώπιση διαταραχής ή καταστροφής.

- Προσδιορισμός ρόλων, υπευθύνων και σημείων επαφής.
- Προκαθορισμένα κριτήρια ενεργοποίησης του πλάνου.
- Περιγραφή ακολουθίας ενεργειών για ανάκαμψη κρίσιμων λειτουργιών.
- Καθορισμός απαραίτητων πόρων (ανθρώπινοι, τεχνικοί, επικοινωνιακοί).

3. Ανάπτυξη Σχεδίου Διαχείρισης Κρίσεων: Συντονισμός αντίδρασης σε κρίσεις μεγάλης κλίμακας.

- Καθορισμός επικοινωνιακής στρατηγικής.
- Ενημέρωση αρμόδιων αρχών και του κοινού.
- Διευθέτηση ευθυνών και εντολών κλιμάκωσης.

ΜΕΤΑ το περιστατικό (Αντίδραση):

4. Ενεργοποίηση Πλάνου Επιχειρησιακής Συνέχειας: Εφαρμογή σχεδίου σε περίπτωση πραγματικού περιστατικού.
- Εκκίνηση διαδικασιών επιχειρησιακής συνέχειας.
- Ενεργοποίηση Ομάδας Επιχειρησιακής Συνέχειας / Διαχείρισης Κρίσεων.
- Εφαρμογή σχεδίου ανάκαμψης για κρίσιμες λειτουργίες.

5. Ανάκαμψη & Επαναφορά: Επιστροφή στην κανονική λειτουργία.
- Επαναφορά υπηρεσιών και συστημάτων σύμφωνα με τις προτεραιότητες.
- Συντονισμός εσωτερικής λειτουργίας και εξυπηρέτησης πελατών.
- Καταγραφή περιστατικού και ενεργειών ανάκαμψης.

6. Ανασκόπηση και Βελτίωση: Αποτίμηση της ανταπόκρισης και διόρθωση αδυναμιών.
- Καταγραφή “lessons learned”.
- Επικαιροποίηση Ανάλυσης (1), Πλάνου (2) και Σχεδίου (3) με βάση τα ευρήματα.
- Ενημέρωση πολιτικών, διαδικασιών και εκπαιδευτικών υλικών.

ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

Οι διαδικασίες αφορούν το σύνολο των κρίσιμων λειτουργιών, υπηρεσιών, συστημάτων και πληροφοριακών υποδομών της επιχείρησης. Ενεργοποιούνται σε κάθε περιστατικό ή απειλή που μπορεί να προκαλέσει διακοπή λειτουργίας, αδυναμία παροχής υπηρεσιών και κίνδυνο για τη δημόσια ασφάλεια, οικονομία και εμπιστοσύνη των πολιτών.

ΕΥΘΥΝΗ

Διοίκηση:
Εφαρμογή και αποτελεσματικότητα των διαδικασιών. Έγκριση πλάνου επιχειρησιακής συνέχειας και εξασφάλιση των απαραίτητων πόρων (ανθρώπινοι, τεχνικοί, οικονομικοί) για την εφαρμογή του.

Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών:
Συνεργασία με τον Υπεύθυνο Επιχειρησιακής Συνέχειας. Εξασφάλιση λειτουργίας των πληροφοριακών συστημάτων.

Υπεύθυνος Επιχειρησιακής Συνέχειας:
Υλοποίηση πλάνου επιχειρησιακής συνέχειας και εποπτεία των διαδικασιών ανάκαμψης.

Ομάδα Επιχειρησιακής Συνέχειας & Διαχείρισης Κρίσεων:
Επαναφορά κρίσιμων λειτουργιών βάσει του σχεδίου. Στρατηγικός και επικοινωνιακός συντονισμός. Η σύστασή της δεν είναι υποχρεωτική. Ο αριθμός των συμμετεχόντων εξαρτάται από το μέγεθος της επιχείρησης, τον βαθμό πολυπλοκότητας της τεχνολογικής υποδομής, τη διαχείριση ευαίσθητων δεδομένων, κοκ.

Τυπική δομή Ομάδας Διαχείρισης Περιστατικών		
Ρόλος	**Τμήμα προέλευσης**	**Κύριες αρμοδιότητες**
Υπεύθυνος Ασφάλειας (*)	IT / OT	Εποπτεία των ενεργειών. Εξασφάλιση ακεραιότητας και λειτουργίας συστημάτων IT/OT, τεχνικές ενέργειες.
Υπεύθυνος Επιχειρησιακής Συνέχειας (BCM Officer)	Διοίκηση / Διαχείριση κινδύνου	Συντονισμός πλάνου, επικαιροποίηση, ενεργοποίηση σε κρίση, εποπτεία ανάκαμψης.
Υπεύθυνος Πληροφορικής (IT Manager)	IT	Επαναφορά υποδομών, εφαρμογών και βάσεων δεδομένων, τεχνική υποστήριξη.
Υπεύθυνος Ανθρώπινου Δυναμικού	HR	Συντονισμός προσβασιμότητας προσωπικού, επικοινωνία με εργαζομένους.
Υπεύθυνος Επικοινωνίας / Δημόσιων Σχέσεων	Επικοινωνία / Μάρκετινγκ	Σύνταξη και διανομή εγκεκριμένων μηνυμάτων σε κοινό, ΜΜΕ και Εθνική Αρχή Κυβερνοασφάλειας.
Νομικός Σύμβουλος / Υπεύθυνος Συμμόρφωσης	Νομικό Τμήμα / Τμήμα Συμμόρφωσης	Έλεγχος νομικών υποχρεώσεων, σχέσεις με ρυθμιστικές αρχές, γνωμοδοτήσεις.
Υπεύθυνος Κτηριακών Υποδομών / Λειτουργιών	Τεχνικές Υπηρεσίες / Facility Management	Εποπτεία φυσικής προσβασιμότητας, εναλλακτικές εγκαταστάσεις.
Εκπρόσωπος Διοίκησης	ΔΣ	Εγκρίνει ενεργοποίηση πλάνου, αποφασίζει για κλιμάκωση και στρατηγικές κινήσεις.
Υπεύθυνος Υποστήριξης Πελατών / Υπηρεσιών	Εξυπηρέτηση Πελατών / Operations	Ενημέρωση πελατών, προσωρινή λειτουργία κρίσιμων υπηρεσιών.
Data Protection Officer (DPO)	Νομικό Τμήμα / Τμήμα Συμμόρφωσης	Συντονισμός θεμάτων προσωπικών δεδομένων κατά τη διάρκεια κρίσεων (GDPR).
* Στις περισσότερες περιπτώσεις προέρχεται από το τμήμα IT. Σε επιχειρήσεις με κρίσιμα βιομηχανικά συστήματα, μπορεί να προέρχεται ή να πλαισιώνεται από τον χώρο του OT, και να έχει την ευθύνη για την ασφάλεια, ακεραιότητα και διαθεσιμότητα των OT συστημάτων (πχ PLCs, SCADA, DCS).		

ΕΡΓΑΛΕΙΑ ΚΑΙ ΕΓΓΡΑΦΑ

Εργαλείο / Λειτουργία	Περιγραφή
Σύστημα Διαχείρισης Επιχειρησιακής Συνέχειας (Business Continuity Management System - BCMS)	Τεκμηρίωση και εφαρμογή σχεδίου επιχειρησιακής συνέχειας και disaster recovery.
Σύστημα Backup και Ανάκαμψης (Backup & Recovery)	Λήψη αντιγράφων ασφαλείας, επαναφορά δεδομένων και συστημάτων σε περίπτωση καταστροφής.
Υποδομή Ανάκαμψης από Καταστροφή	Εφεδρική υποδομή (πχ DR site, εναλλακτικά data centers ή cloud).
Εργαλεία επικοινωνίας έκτακτης ανάγκης	Επικοινωνία με προσωπικό, Διοίκηση, εξωτερικούς φορείς (πχ SMS alerting, emergency calling trees, encrypted email).
Συστήματα παρακολούθησης IT υποδομών	Ανίχνευση βλαβών, προσδιορισμός κρίσιμων εξαρτήσεων, έγκαιρη ενεργοποίηση σχεδίου.
Καταγραφή και διαχείριση περιστατικών (Incident Log)	Χρονική τεκμηρίωση ενεργειών κατά τη διάρκεια κρίσης.
Εσωτερική πλατφόρμα ενημέρωσης (πχ. intranet)	Επικοινωνία, οδηγίες, checklists και πρότυπα.

Τεκμηρίωση & Έγγραφα	Περιγραφή
Σχέδιο Επιχειρησιακής Συνέχειας	Αναλυτικό σχέδιο ενεργειών για κρίσιμες υπηρεσίες, ρόλους, επαφές, καταγραφή ενεργειών, κλιμάκωση.
Σχέδιο Διαχείρισης Κρίσεων / Επικοινωνίας	Ρόλοι και διαδικασίες επικοινωνίας εντός και εκτός οντότητας (πχ προς αρχές, ΜΜΕ, πελάτες).
Αναφορά Ανάλυσης Επιχειρησιακών Επιπτώσεων	Εντοπισμός κρίσιμων λειτουργιών, καθορισμός RTO/RPO, ιεράρχηση προτεραιοτήτων ανάκαμψης.
Έντυπα καταγραφής περιστατικών και ενεργειών	Templates για real-time documentation.
Πρόγραμμα Δοκιμών (Testing & Exercises Plan)	Ετήσιο πλάνο ασκήσεων (πχ tabletop, simulation, drill).
Αποτίμηση άσκησης / κρίσης (Post-exercise / crisis report)	Lessons learned, κενά, βελτιώσεις.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

Ανά εξάμηνο / ετήσια:
Αξιολόγηση και αναθεώρηση Σχεδίου Επιχειρησιακής Συνέχειας / Διαχείρισης Κρίσεων.

Ad hoc:
Εκτέλεση, αξιολόγηση και αναθεώρηση μετά από:

- σοβαρό περιστατικό κυβερνοασφάλειας ή άλλο γεγονός που προκαλεί ή ενδέχεται να προκαλέσει σημαντικές επιπτώσεις,
- σημαντικές οργανωτικές αλλαγές,
- μεταβολές στο περιβάλλον απειλών,
- δοκιμές και ασκήσεις ετοιμότητας (πχ tabletop, simulation drills).

Πηγές:
Εθνική Αρχή Κυβερνοασφάλειας, ΣΕΒ, International Electrotechnical Commission, International Organization for Standardization, International Society of Automation, National Institute of Standards and Technology, VDC Research, World Economic Forum

Γ.
ΣΥΧΝΕΣ ΕΡΩΤΗΣΕΙΣ

1. Αν μια επιχείρηση εφαρμόζει ISO27001, συνεπάγεται ότι είναι συμμορφωμένη με τον Ν. 5160/2024 και την Οδηγία NIS2;
Όχι πλήρως. Η εφαρμογή του προτύπου ISO27001 μεταφράζεται σε κάλυψη μεγάλου μέρους των απαιτήσεων του Ν. 5160/2024 και της Οδηγίας και ένα αρκετά καλό επίπεδο συμμόρφωσης, όμως χρειάζεται περαιτέρω εξειδίκευση. Ακόμα και στην περίπτωση αυτή, συνίσταται αξιολόγηση κενών ώστε να διαπιστωθεί ποιες διαδικασίες πρέπει να ενσωματωθούν στο ISMS που ήδη εφαρμόζεται. Για παράδειγμα, αν η επιχείρηση εφαρμόζει πολιτική απόκρισης σε περιστατικά, απαιτείται προσαρμογή στο χρονοδιάγραμμα κοινοποίησης περιστατικών που ορίζουν ο Ν. 5160/2024 και η NIS2.

Επιπλέον, για τη συμμόρφωση μιας επιχείρησης με τις νομικές απαιτήσεις, ανάλογα με τις επιχειρηματικές της δραστηριότητες, είναι πολύ πιθανό να απαιτείται ένας συνδυασμός μέτρων, που υπάρχουν σε περισσότερα πρότυπα.

2. Ο Ν. 5160/2024 και η NIS2 απαιτούν από τις επιχειρήσεις την εφαρμογή συγκεκριμένων προτύπων και τεχνικών προδιαγραφών που σχετίζονται με την κυβερνοασφάλεια;
Ο Ν. 5160/2024 και η NIS2 απλώς ενθαρρύνουν τη χρήση τους. Δεν υπαγορεύουν ρητά την υιοθέτηση κάποιου συγκεκριμένου προτύπου (πχ ISO27001 ή NIST).

3. Μπορούν επιχειρήσεις μικρού μεγέθους να εντάσσονται στο πεδίο εφαρμογής του Ν. 5160/2024 και της NIS2;
Ναι, αν είναι πάροχοι υπηρεσιών συστήματος ονομάτων τομέα (DNS), υπηρεσιών εμπιστοσύνης, δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, μητρώα ονομάτων τομέα ανώτατου επιπέδου (TLD), καθώς και αν παρέχουν υπηρεσίες υψηλής σημασίας για την οικονομία ή και την κοινωνία, εφόσον, στην τελευταία περίπτωση, προσδιορισθούν από την Εθνική Αρχή Κυβερνοασφάλειας ως τέτοιες.

Επίσης, αν μια μικρή επιχείρηση αποτελεί μέρος της εφοδιαστικής αλυσίδας μιας οντότητας που εντάσσεται στο πεδίο εφαρμογής του Ν. 5160/2024 και της NIS2, ενδέχεται να λάβει αίτημα από την τελευταία να εφαρμόσει μέτρα που προβλέπονται στον Ν. 5160/2024 και τη NIS2, ώστε να μην υπάρχουν κενά ασφαλείας.

4. Τι πρέπει να γνωρίζει μια επιχείρηση που λειτουργεί συγχρόνως και σε άλλες χώρες της ΕΕ;
Κάποιες χώρες έχουν διαφορετικό εφαρμοστικό πλαίσιο όσον αφορά στην ενσωμάτωση της NIS2, αλλά χωρίς σημαντικές αποκλίσεις. Η επιχείρηση πρέπει να ερευνήσει τις απαιτήσεις και κανονισμούς κάθε Αρχής, ώστε να διαπιστώσει τυχόν διαφορές από το ελληνικό πλαίσιο (πχ κατηγοριοποίηση οντοτήτων, πεδίο εφαρμογής, εφαρμογή συγκεκριμένων προτύπων, κοκ) που ενδέχεται να προκαλέσουν κάποιο βαθμό δυσχέρειας στη συμμόρφωση. Η γνώση αυτών των μικρών αποκλίσεων διευκολύνει την πλήρη συμμόρφωση και εκτός συνόρων.

5. Αν μια επιχείρηση που λειτουργεί συγχρόνως και σε άλλες χώρες της ΕΕ, δέχεται κυβερνοεπίθεση που επηρεάζει τις λειτουργίες της διασυνοριακά, ποιους πρέπει να ενημερώσει;
Ενημερώνει κατά πρώτον την Εθνική Αρχή Κυβερνοασφάλειας, επισημαίνοντας το διασυνοριακό αντίκτυπο, καθώς και τις αντίστοιχες Αρχές των χωρών στις οποίες δέχεται συνέπειες. Στην περίπτωση αυτή, πρέπει να γνωρίζει ενδεχόμενες διαφορές στο χρονοδιάγραμμα των γνωστοποιήσεων των Αρχών (πχ κάποιες χώρες έχουν ορίσει χρονικό όριο μικρότερο των 24 ωρών για την πρώτη κοινοποίηση).

6. Η Εθνική Αρχή Κυβερνοασφάλειας μπορεί να ελέγξει μια επιχείρηση ακόμα και αν δεν έχει προκύψει περιστατικό;
Ναι, αν είναι βασική οντότητα. Αντιθέτως, οι έλεγχοι στις σημαντικές οντότητες γίνονται όταν η Εθνική Αρχή Κυβερνοασφάλειας έχει ενδείξεις ή πληροφορίες ότι η οντότητα δε συμμορφώνεται με τις υποχρεώσεις λήψης μέτρων ή αναφοράς περιστατικών, ιδίως δε κατόπιν εκδήλωσης περιστατικού. Σε κάθε περίπτωση, τα εποπτικά μέτρα περιλαμβάνουν επιθεωρήσεις εντός ή εκτός των εγκαταστάσεων, ελέγχους και αιτήματα παροχής πληροφοριών, πρόσβασης σε δεδομένα, κοκ.

7. Πώς μπορεί μια επιχείρηση να είναι προετοιμασμένη σε ενδεχόμενο έλεγχο της Εθνικής Αρχής Κυβερνοασφάλειας;
Η επιχείρηση έχει το βάρος απόδειξης της συμμόρφωσής της και απαιτείται να τηρεί κατάλληλη τεκμηρίωση και αποδεικτικά στοιχεία υλοποίησης των πολιτικών ασφάλειάς της. Πρέπει να διεξάγει τακτικά εσωτερικούς ελέγχους και ασκήσεις προσομοίωσης άμεσης απόκρισης σε περιστατικά. Επιπλέον, να τηρεί ενημερωμένα αρχεία με αποτελέσματα των εκτιμήσεων κινδύνου, πολιτικές ασφαλείας, ιστορικό περιστατικών, εκτιμήσεις αξιολόγησης κινδύνου από προμηθευτές, και εκπαιδευτικές δράσεις.

8. Πώς «χτίζει» μια βιομηχανική επιχείρηση ένα κυβερνοασφαλές ΟΤ περιβάλλον, εντάσσοντάς το στη NIS2;
Οι πρακτικές IT συνήθως δεν επαρκούν για την κυβερνοασφάλεια του ΟΤ περιβάλλοντος, λόγω διαφορετικών προτεραιοτήτων και απαιτήσεων προστασίας μεταξύ των δύο μερών. Οι κίνδυνοι στο ΟΤ εντείνονται κυρίως από τεχνικά χαρακτηριστικά (υψηλή κατανομή και ετερογένεια των συστημάτων, περίπλοκες διαδικασίες, ανεπαρκής ορατότητα) και οργανωτικές δυσχέρειες (προβληματική συνεργασία μεταξύ των ομάδων IT και ΟΤ).

Επομένως, η επιχείρηση πρέπει αρχικά να κατανοήσει τόσο τις οργανωτικές όσο και τις τεχνικές διαφορές σε σχέση με το IT, και στη συνέχεια να συγκλίνει τα δύο μέρη προσαρμόζοντας τις πολιτικές και λύσεις κυβερνοασφάλειας στο ΟΤ περιβάλλον. Στο πλαίσιο αυτό, συνίσταται η χρήση του προτύπου ISA/IEC 62443.

ΜΙΚΡΟ ΛΕΞΙΚΟ

Επιχειρησιακή Τεχνολογία (Operational Technology - OT) είναι το υλικό και λογισμικό που χρησιμοποιούνται για την αλλαγή, την παρακολούθηση ή τον έλεγχο φυσικών συσκευών, διαδικασιών και περιστατικών σε μια επιχείρηση ή οργανισμό. Ενδεικτικά: Programmable Logic Controllers (PLC), Human-Machine Interface (HMI), Supervisory Control and Data Acquisition (SCADA), ρυθμιστές στροφών κινητήρων, όργανα μέτρησης, κτλ.

Κυβερνοαπειλή (Cyber threat) αποτελεί οποιαδήποτε δυνητικά κακόβουλη δραστηριότητα ή συνθήκη, που σκοπεύει, μέσω ενός ψηφιακού συστήματος, να επιδράσει αρνητικά στις λειτουργίες ενός οργανισμού, στα περιουσιακά του στοιχεία, σε πρόσωπα, άλλους οργανισμούς ή τη χώρα, εξαιτίας:
• μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες,
• καταστροφής, δημοσιοποίησης ή αλλοίωσης και φθοράς πληροφοριών,
• άρνησης παροχής υπηρεσιών στους χρήστες του συστήματος.

Κυβερνοασφάλεια (Cyber security) είναι ένας συνδυασμός τεχνολογιών, διαδικασιών και πρακτικών που είναι σχεδιασμένες για να προστατεύουν δίκτυα, συσκευές, προγράμματα, δεδομένα και υλικά και άυλα περιουσιακά στοιχεία από εξωτερικές απειλές, επιθέσεις, φθορές ή μη εξουσιοδοτημένη πρόσβαση. Δεδομένης της αυξανόμενης διασύνδεσης των συστημάτων IT και OT, ο όρος πλέον δεν αφορά μόνο την ασφάλεια των πληροφοριακών συστημάτων, αλλά τη συνολική ψηφιακή ασφάλεια ενός οργανισμού.

Κυβερνοϋγιεινή (Cyber hygiene) είναι πρακτικές και καθημερινά βήματα / ενέργειες που εφαρμόζουν οργανισμοί και φυσικά πρόσωπα για να διασφαλίσουν την καλή λειτουργία και online ασφάλεια των συστημάτων και υπολογιστών τους. Ενδεικτικά, περιλαμβάνει: τακτικές ενημερώσεις του λογισμικού (updates), ισχυρούς κωδικούς, τακτικά backups των δεδομένων, εγκατάσταση λογισμικών προστασίας (antivirus, antimalware, κοκ), διαδικασίες κρυπτογράφησης (encryption), διαμερισματοποίηση του εταιρικού δικτύου, κοκ.

Περιστατικό (Incident) είναι 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.

Σύστημα Διαχείρισης Αλλαγών (Patch Management System) είναι ένα τεχνικό και οργανωτικό σύστημα που επιτρέπει σε έναν οργανισμό να εντοπίζει, αξιολογεί, δοκιμάζει, εγκρίνει και εγκαθιστά αλλαγές ή ενημερώσεις λογισμικού σε λειτουργικά συστήματα, εφαρμογές και υποδομές πληροφορικής, με ασφαλή και ελεγχόμενο τρόπο.

Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System) είναι ένα σύνολο πολιτικών, διαδικασιών και ελεγκτικών μηχανισμών (controls) που σχεδιάζονται με σκοπό την προστασία των πληροφοριακών συστημάτων και τη διαχείριση των κινδύνων ασφαλείας σε έναν οργανισμό.

Σύστημα Διαχείρισης Περιουσιακών Στοιχείων Πληροφορικής (IT Asset Management System) είναι ένα σύνολο πολιτικών, διαδικασιών και εργαλείων που χρησιμοποιούνται για την καταγραφή, παρακολούθηση, διαχείριση και βελτιστοποίηση όλων των περιουσιακών στοιχείων πληροφορικής ενός οργανισμού καθ' όλη τη διάρκεια του κύκλου ζωής τους.

Σύστημα Διαχείρισης Πρόσβασης & Ταυτοποίησης (Identity and Access Management System) είναι ένα οργανωμένο σύνολο διαδικασιών, τεχνολογιών και πολιτικών που επιτρέπει σε έναν οργανισμό να διαχειρίζεται τις ταυτότητες των χρηστών και να ελέγχει την πρόσβασή τους σε πληροφοριακά συστήματα, δεδομένα και εφαρμογές, με ασφαλή και ελεγχόμενο τρόπο.

Σύστημα Ελέγχου Τερματικών Συσκευών (Endpoint Detection and Control System) είναι μια λύση λογισμικού και πολιτικών που επιτρέπει σε έναν οργανισμό να παρακολουθεί, διαχειρίζεται και προστατεύει τις τερματικές συσκευές του από απειλές και μη εξουσιοδοτημένες ενέργειες.

Σύστημα Καταγραφής και Απόκρισης σε Περιστατικά (Incident Detection and Response System ή Incident Management System) είναι ένα οργανωμένο τεχνικό και διαδικαστικό πλαίσιο που επιτρέπει σε έναν οργανισμό να εντοπίζει, καταγράφει, διαχειρίζεται και αντιμετωπίζει περιστατικά ασφάλειας, όπως επιθέσεις, παραβιάσεις, κακόβουλες ενέργειες ή δυσλειτουργίες.

Σύστημα Καταγραφής και Παρακολούθησης Προμηθευτών (Supplier or Third-Party Risk Management System) είναι ένα τεχνικό και οργανωτικό σύστημα που επιτρέπει σε έναν οργανισμό να καταγράφει, αξιολογεί, παρακολουθεί και διαχειρίζεται τους κινδύνους που σχετίζονται με τους προμηθευτές, υπεργολάβους ή άλλους εξωτερικούς συνεργάτες του – ειδικά σε ό,τι αφορά την ασφάλεια πληροφοριών, τη συμμόρφωση και τη διαθεσιμότητα κρίσιμων υπηρεσιών.

Σύστημα Ταξινόμησης και Προστασίας Δεδομένων (Data Classification and Protection System) είναι ένα οργανωμένο σύνολο πολιτικών, διαδικασιών και τεχνολογικών μέσων που επιτρέπει σε έναν οργανισμό να ταξινομεί τα δεδομένα του με βάση την ευαισθησία και τη σημασία τους, και να εφαρμόζει τα κατάλληλα μέτρα προστασίας ανάλογα με την κατηγορία στην οποία ανήκουν.

ΠΗΓΕΣ

Εθνική Αρχή Κυβερνοασφάλειας
ΣΕΒ
Υπουργείο Ψηφιακής Διακυβέρνησης
European Commission
European Cyber Security Organisation
Eurostat
EY
International Electrotechnical Commission
International Organization for Standardization
International Society of Automation
National Cyber Security Centre of Ireland
National Institute of Standards and Technology
Thales Group
VDC Research
World Economic Forum

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

ΣΕΒ σύνδεσμος επιχειρήσεων και βιομηχανιών

Τομέας Τεχνολογίας & Ψηφιακού Μετασχηματισμού

www.sev.org.gr

E. **innovation@sev.org.gr**
T. 211 5006 165

SEV Hellenic Federation of Enterprises
ΣΕΒ σύνδεσμος επιχειρήσεων και βιομηχανιών
SEV_Fed
SEVFed