ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

Οδηγός ΣΕΒ για Επιχειρήσεις

Συμμόρφωση των Επιχειρήσεων με τον Ν. 5160/2024 και την Οδηγία NIS2

Τομέας Τεχνολογίας & Ψηφιακού Μετασχηματισμού

ΨΗΦΙΑΚΟΣ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

Οδηγία NIS2

Ενιαίο νομικό πλαίσιο για τη διατήρηση της κυβερνοασφάλειας σε 18 κρίσιμους κλάδους στην ΕΕ

Στόχοι

- Ενίσχυση της κυβερνο-ανθεκτικότητας ενός ευρέος φάσματος επιχειρήσεων της ΕΕ
- Εναρμόνιση των πρακτικών κυβερνοασφάλειας σε ολόκληρη την ΕΕ (κοινό μέτωπο άμυνας)
- Ενδυνάμωση της συνολικής ετοιμότητας και ικανότητας αντιμετώπισης περιστατικών

Γιατί είναι σημαντική η NIS2;

- **29%** των ευρωπαϊκών επιχειρήσεων έχουν καθορίσει ή αναθεωρήσει την πολιτική κυβερνοασφάλειάς τους τα τελευταία 2 χρόνια
- Σημαντική αύξηση των κυβερνοεπιθέσεων στην ΕΕ (+24% το 2024)

ΨΗΦΙΑΚΟΣ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

Οφέλη συμμόρφωσης

- 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

Η επιτυχής συμμόρφωση σχετίζεται με:

Σχεδόν **διπλάσια μείωση** των περιστατικών παραβιάσεων

4 φορές μικρότερη πιθανότητα περιστατικού παραβίασης

ΨΗΦΙΑΚΟΣ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

Ποιες επιχειρήσεις αφορά;

Βασικές οντότητες

Μεγάλες, Τομείς Υψηλής Κρισιμότητας

- Ενέργεια
- Υγεία
- Μεταφορές
- Πόσιμο νερό
- Τράπεζες
- Λύματα
- Υποδομές χρημ/κών αγορών
- Διαχείριση υπηρεσιών ΤΠΕ (B2B)
- Ψηφιακές υποδομές
- Διάστημα

Ειδικές περιπτώσεις ανεξαρτήτως μεγέθους

Σημαντικές οντότητες

Μεσαίες ή μεγάλες, Άλλοι Κρίσιμοι Τομείς

- Ταχυδρομικές υπηρεσίες, ταχυμεταφορές
- Κατασκευή ηλεκτρολογικού, ηλεκτρονικού & μηχανολ. εξοπλισμού
- Διαχείριση αποβλήτων
- Παρασκευή, παραγωγή και διανομή χημικών προϊόντων
- Ψηφιακοί πάροχοι
- Παραγωγή, μεταποίηση και διανομή τροφίμων
- Έρευνα

Μεσαίες ή μικρές, Τομείς Υψηλής Κρισιμότητας

ΨΗΦΙΑΚΟΣ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

Τι συνεπάγεται για τις επιχειρήσεις;

Α. Καθορισμός νέων ρόλων και αρμοδιοτήτων

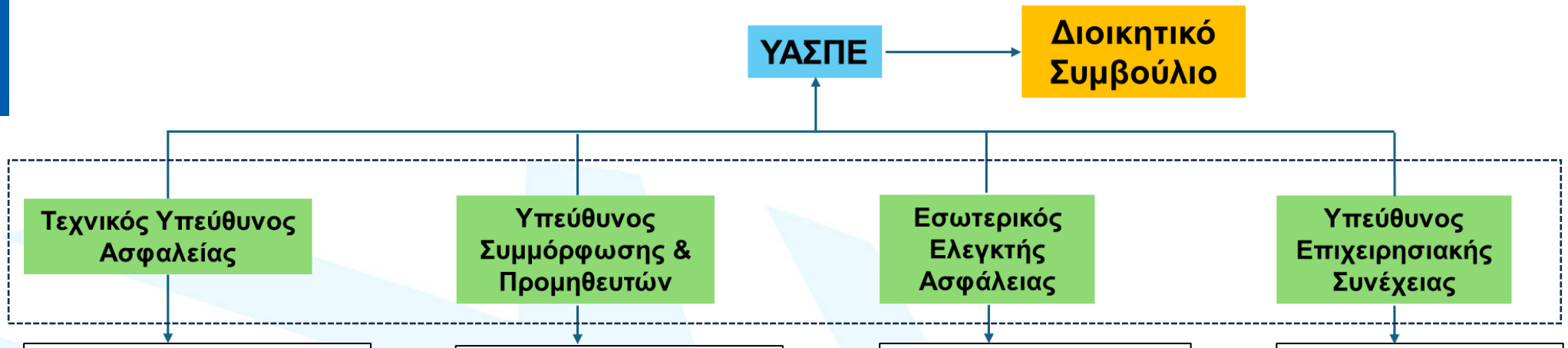
Β. Υιοθέτηση νέων διαδικασιών με στόχο την ενσωμάτωση της κυβερνοασφάλειας

Γ. Μεγαλύτερες επενδύσεις σε συστήματα κυβερνοασφάλειας

Δ. Εκπαίδευση, ευαισθητοποίηση - Συνεχής ενημέρωση της διοίκησης

Η κυβερνοασφάλεια ανάγεται πλέον, από καθαρά τεχνικό ζήτημα, σε στρατηγική και νομική προτεραιότητα για τις μεσαίες και μεγάλες επιχειρήσεις

Α. Νέοι ρόλοι και αρμοδιότητες



Έλεγχος Πρόσβασης & Διαχείρισης Λογαριασμών:
- Υλοποίηση πολιτικών least privilege, MFA, κοκ. Συνεργασία με HR για onboarding / offboarding.

Διαχείριση Συστημάτων & Υποδομών:
- Παραμετροποίηση, διαχείριση αλλαγών, antivirus, firewall, κοκ.

Διαχείριση Περιστατικών:
- Υλοποίηση σχεδίου απόκρισης. Συντονισμός κατά τη διάρκεια συμβάντων.

Μέτρα φυσικής ασφάλειας:
- CCTV, έλεγχος πρόσβασης, κοκ.

Πολιτικές & Συμμόρφωση:
- Σύνταξη & επικαιροποίηση πολιτικών. Παρακολούθηση συμμόρφωσης με NIS2, GDPR, DORA κ.ά.

Διαχείριση Προμηθευτών:
- Έλεγχος ασφάλειας στην αλυσίδα εφοδιασμού.

- Συμμετοχή σε audits, penetration tests, αξιολογήσεις αποτελεσματικότητας.
- Έλεγχος του έργου των άλλων με αντικειμενικότητα.

- Υλοποίηση του πλάνου επιχειρησιακής συνέχειας. Εποπτεία των διαδικασιών ανάκαμψης.

- Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών (ΥΑΣΠΕ)
- Ομάδα Κυβερνοασφάλειας
- Διοικητικό Συμβούλιο

ΨΗΦΙΑΚΟΣ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

Β. 10 κρίσιμες διαδικασίες για συμμόρφωση με τη NIS2

Β.1 Στρατηγικός Σχεδιασμός

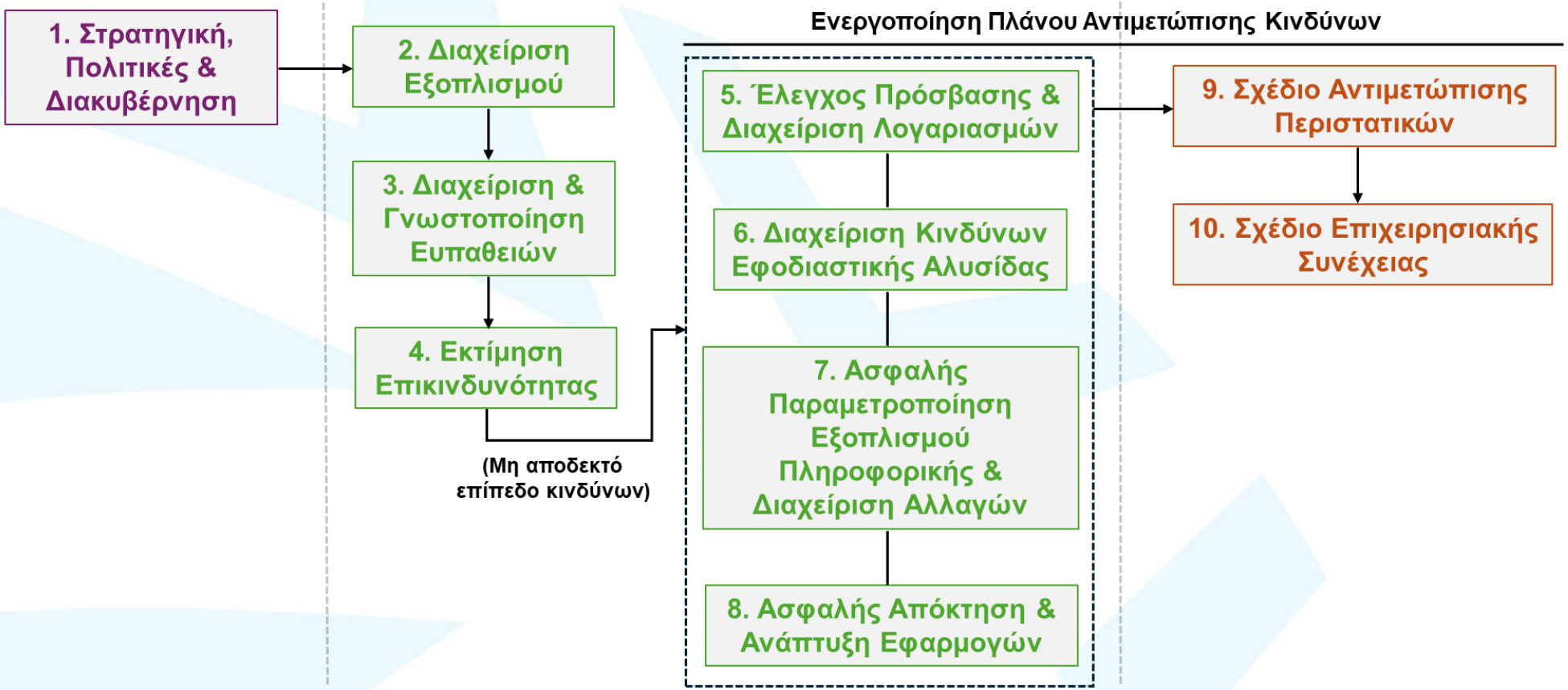
Πού βρισκόμαστε; Πού θέλουμε να πάμε

Β.2 Λειτουργίες Πρόληψης

Πώς προστατεύουμε τον κρίσιμο εξοπλισμό μας; Πώς ασφαλίζουμε το γενικότερο περιβάλλον λειτουργίας μας;

Β.3 Λειτουργίες Διαχείρισης & Ανάκαμψης από Περιστατικά

Πώς αντιδράμε σε περιπτώσεις περιστατικών;



Β.1 - Στρατηγικός Σχεδιασμός

1. Στρατηγική, πολιτικές & διακυβέρνηση

- Η κυβερνοασφάλεια ενσωματώνεται στη διακυβέρνηση της επιχείρησης μέσα από ένα ολοκληρωμένο **Πρόγραμμα Διαχείρισης Κινδύνων**.
- Περιλαμβάνονται: Στρατηγική + Μέσα υλοποίησης (καθορισμός πολιτικών, διαδικασιών, ρόλων & αρμοδιοτήτων, πόρων, μέτρων υλοποίησης)
- Η διοίκηση εγκρίνει και εποπτεύει το πρόγραμμα, ενώ ο ΥΑΣΠΕ εποπτεύει την εφαρμογή και ενημερώνει τη διοίκηση.
- Συνίσταται η χρήση προτύπων όπως το ISA/IEC 62443 για βιομηχανικές επιχειρήσεις με ΟΤ υποδομές

Β.2 - Διαδικασίες και βήματα πρόληψης

Εσωτερικές επιχειρησιακές λειτουργίες

2. **Διαχείριση Εξοπλισμού**: Καταγραφή, ταξινόμηση και ανάθεση ευθυνών διαχείρισης και συντήρησης για όλα τα IT/OT περιουσιακά στοιχεία, ανεξαρτήτως τοποθεσίας ή μορφής.
3. **Διαχείριση και Γνωστοποίηση Ευπαθειών**: Συνεχής ανίχνευση, αξιολόγηση, προτεραιοποίηση και διόρθωση ευπαθειών, με τεκμηρίωση και γνωστοποίηση σε αρμόδιες αρχές όπου απαιτείται.
4. **Εκτίμηση Επικινδυνότητας**: Ανάλυση σεναρίων κινδύνου, ποσοτικοποίηση, προτεραιοποίηση και ανάπτυξη πλάνου αντιμετώπισης. Έμφαση σε ΟΤ υποδομές με διαχωρισμό σε ζώνες και διαύλους.
5. **Έλεγχος Πρόσβασης & Διαχείριση Λογαριασμών**: Υιοθέτηση πολιτικής ελεγχόμενης πρόσβασης, δημιουργία πρόσβασης, περιοδικές αναθεωρήσεις προσβάσεων, άμεση απενεργοποίηση λογαριασμών μετά από αλλαγές ή αποχωρήσεις.
6. **Ασφαλής Παραμετροποίηση Εξοπλισμού Πληροφορικής & Διαχείριση Αλλαγών**: Καθορισμός διαδικασιών ασφαλούς παραμετροποίησης, διαχείριση αιτημάτων αλλαγών με αξιολόγηση κινδύνου και τεκμηρίωση.
7. **Ασφαλής Απόκτηση & Ανάπτυξη Εφαρμογών**: Ενσωμάτωση ασφάλειας σε όλη τη διάρκεια ζωής των εφαρμογών, από σχεδιασμό έως παραγωγή, με αρχές πχ Security by Design, Zero Trust, και τακτικούς ελέγχους.

Επιχειρησιακές λειτουργίες που αφορούν το εξωτερικό περιβάλλον

8. Διαχείριση Κινδύνων Εφοδιαστικής Αλυσίδας:

- Καταγραφή, αξιολόγηση κινδύνων και παρακολούθηση προμηθευτών και τρίτων συνεργατών.
- Χρήση συμβατικών ρητρών με απαιτήσεις ασφάλειας, που διασφαλίζουν την εφαρμογή μέτρων κυβερνοασφάλειας και δυνατότητα ελέγχου.

Β.3 - Διαχείριση και ανάκαμψη από περιστατικά

9. **Διαχείριση Περιστατικών Κυβερνοασφάλειας**: Εκπόνηση σχεδίου απόκρισης που καλύπτει προετοιμασία, ανίχνευση, απόκριση και αποκατάσταση, με υποχρέωση άμεσης ενημέρωσης της Εθνικής Αρχής Κυβερνοασφάλειας εντός συγκεκριμένων προθεσμιών.
10. **Επιχειρησιακή Συνέχεια & Διαχείριση Κρίσεων**: Ανάλυση επιχειρησιακών επιπτώσεων (με εντοπισμό κρίσιμων συστημάτων, εκτίμηση συνεπειών και ορισμό δεικτών αποκατάστασης), κατάρτιση πλάνου επιχειρησιακής συνέχειας και διαχείρισης κρίσεων, συντονισμός ανάκαμψης μετά το περιστατικό. Περιλαμβάνει ρόλους, επικοινωνιακή στρατηγική και τακτικές δοκιμές.

ΨΗΦΙΑΚΟΣ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

Γ. Επενδύσεις σε συστήματα & υποδομές

- Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS)
- Σύστημα Διαχείρισης Συμμόρφωσης & Ελέγχων
- Σύστημα Διαχείρισης Περιουσιακών Στοιχείων
- Σύστημα Ελέγχου Τερματικών Συσκευών
- Σύστημα Καταγραφής και Παρακολούθησης Προμηθευτών
- Σύστημα Διαχείρισης Πρόσβασης & Ταυτοποίησης
- Πλατφόρμα Διαχείρισης Ευπαθειών και Απειλών
- κοκ

Δ. Εκπαίδευση, ευαισθητοποίηση, ενημέρωση της διοίκησης

- Τακτικά σεμινάρια και ενημερώσεις για όλο το προσωπικό
- Ειδικευμένη εκπαίδευση για εργαζόμενους και στελέχη με κρίσιμους ρόλους
- Τακτικές ασκήσεις κυβερνοασφάλειας
- Ενημέρωση της διοίκησης από τον ΥΑΣΠΕ