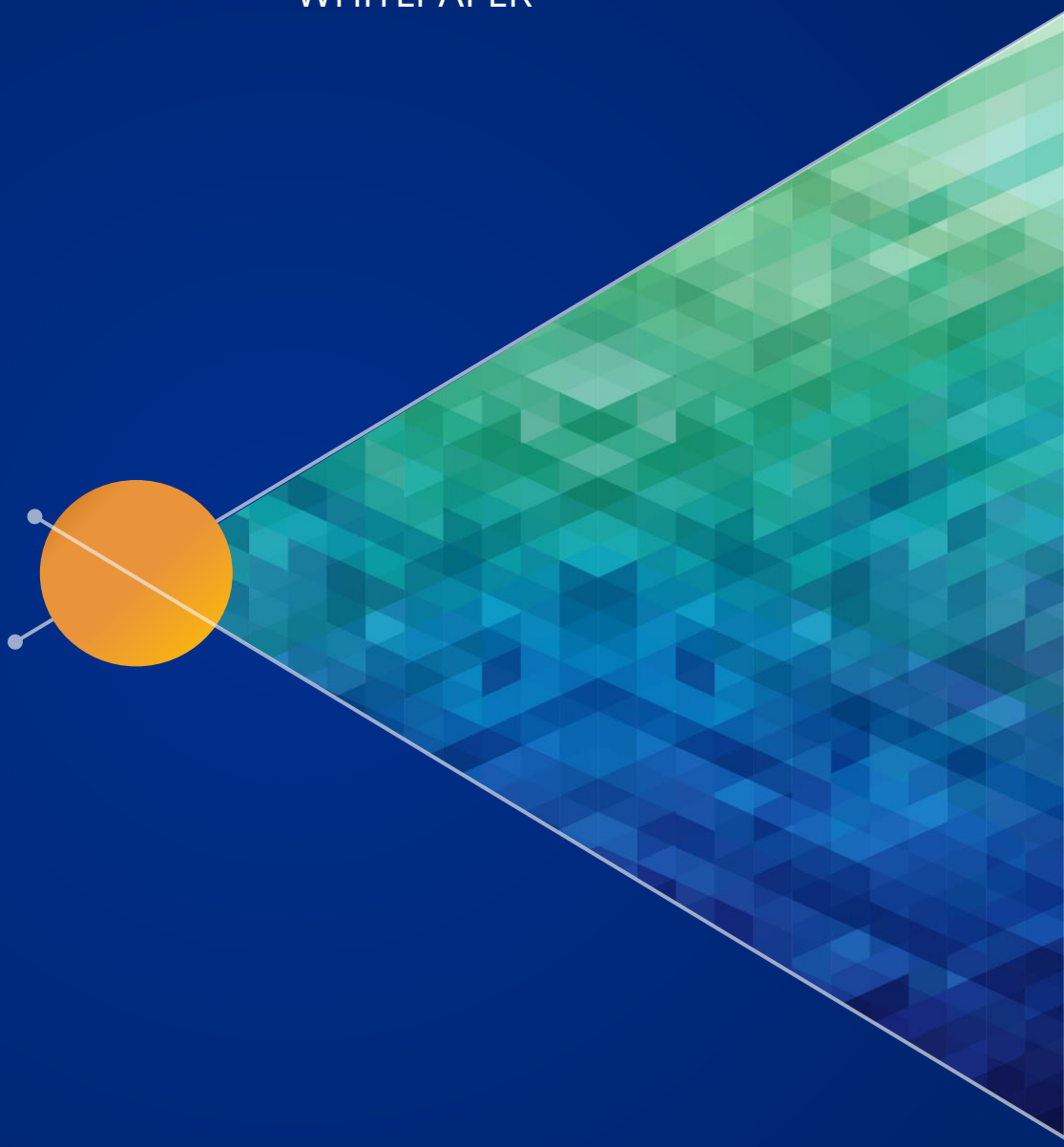
EU

NIS Directive

WHITEPAPER



spearIT
InfoSec · Compliance

ΠΕΡΙΕΧΟΜΕΝΑ

ΟΔΗΓΙΑ EU 2016/1148

NIS DIRECTIVE

ΜΑΪΟΥ
10

Υποχρεωτική εφαρμογή σε εθνικό επίπεδο από την 10η Μαΐου 2018.

Στόχος της είναι η επίτευξη υψηλού ενιαίου επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών στην ΕΕ

Θεσπίζει απαιτήσεις ασφάλειας και κοινοποίησης για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και για τους παρόχους ψηφιακών

Ενσωμάτωση στην ελληνική νομοθεσία με τον N.4577/2018 και την ΥΑ 1027/2019

Η Ευρωπαϊκή Επιτροπή παρουσίασε την Ευρωπαϊκή Οδηγία Ασφάλειας Δικτύου και Πληροφοριών (EU NIS Directive), ως μέρος της γενικότερης ευρωπαϊκής στρατηγικής για την κυβερνοασφάλεια.

Είναι ο πρώτος κανονισμός κυβερνοασφάλειας σε ευρωπαϊκό επίπεδο και στόχο έχει την ενίσχυση της κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση.

Υιοθετήθηκε το 2016 και καθώς αποτελεί οδηγία της Ευρωπαϊκής Ένωσης, κάθε κράτος – μέλος θα πρέπει να υιοθετεί αντίστοιχη νομοθεσία σε εθνικό επίπεδο, σε αντιστοιχία με την αρχική οδηγία.

Η προθεσμία για την εφαρμογή της σε εθνικό επίπεδο από τα κράτη – μέλη είναι η 9η Μαΐου 2018.

Ορισμένες δυνατότητες κυβερνοασφάλειας πρέπει να υπάρχουν σε **εθνικό επίπεδο**, π.χ. να υπάρχει μια εθνική ομάδα CSIRT, να εκτελούνται ασκήσεις κυβερνο-ετοιμότητας κ.α.

Διασυνοριακή συνεργασία μεταξύ χωρών της ΕΕ με όργανα όπως π.χ. το επιχειρησιακό δίκτυο CSIRT της ΕΕ, η στρατηγική ομάδα συνεργασίας του NIS κ.α.

Η ασφάλεια του κυβερνοχώρου των **κρίσιμων** φορέων της αγοράς στη χώρα κάθε κράτους-μέλους πρέπει να εποπτεύεται: τομέας ενέργειας, μεταφορών, ύδατος, υγείας και χρηματοδότησης, σημεία ανταλλαγής μέσω διαδικτύου, συστήματα ονομάτων τομέα κ.λπ.

Μάθετε περισσότερα για την **Εθνική Στρατηγική Κυβερνοασφάλειας** της Ελλάδας, **εδώ.**

ΕΘΝΙΚΟ ΠΛΑΙΣΙΟ ΕΦΑΡΜΟΓΗΣ

Ν.4577/2018 & ΥΑ 1027/2019

Σκοπός της έκδοσης του **Νόμου 4577/2018** είναι:

- η ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ (NIS Directive) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016 (ΕΕ L 194), με την οποία θεσπίζονται μέτρα για την επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών.

Σκοπός της έκδοσης της **ΥΑ 1027** είναι ο καθορισμός:

- **των βασικών απαιτήσεων ασφαλείας συστημάτων δικτύου και πληροφοριών**
- **της διαδικασίας παροχής πληροφοριών κοινοποίησης συμβάντων ασφάλειας στις αρμόδιες Αρχές**
- **της μεθοδολογίας προσδιορισμού των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών (Φ.Ε.Β.Υ.)**
- **της μεθοδολογίας αξιολόγησης και ελέγχου**

Οργανισμοί σχετικοί με τους παρακάτω τομείς θα πρέπει να προχωρήσουν άμεσα σε **πλάνο συμμόρφωσης** με την Οδηγία και το εθνικό πλαίσιο εφαρμογής της:

Ενέργειας
(προμήθεια, διανομή, μεταφορά, διύλιση, διαχείριση συστημάτων)

Πόσιμου Νερού
(προμήθεια, διανομή)

Μεταφορών
(αεροπορικών, σιδηροδρομικών, πλωτών, οδικών)

Υγείας

Τραπεζών

Ψηφιακών Υποδομών
(DNS, gTLDs, IPX)

Οι **Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ)** έχουν υποχρέωση:

- Να ορίσουν Υπεύθυνο Ασφαλείας Πληροφοριών και Δικτύων και να κοινοποιηθούν τα στοιχεία του στην Εθνική Αρχή Κυβερνοασφάλειας
- Να ορίσουν ενιαία πολιτική ασφαλείας
- Να συντάξουν εγχειρίδιο ασφάλειας πληροφοριών.
- Να πραγματοποιήσουν αποτίμηση κινδύνων
- Να συντάξουν αναφορά αυτοαξιολόγησης και να κοινοποιηθεί στην ΕΑΚ**, εντός 6 μηνών από την ημερομηνία έκδοσης του Οδηγού Αυτοαξιολόγησης** από την Εθνική Αρχή Κυβερνοασφάλειας
- Να κοινοποιούν σε ετήσια βάση τα αποτελέσματα αυτοαξιολόγησης στην Εθνική Αρχή Κυβερνοασφάλειας
- Να ακολουθήσουν κατάλληλα τα 3 στάδια εφαρμογής (Αναγνώριση – Προστασία – Αντιμετώπιση)
- Να επικαιροποιήσουν συμβάσεις με προμηθευτές (SLA)

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Είναι η **εθνική**, αρμόδια αρχή για την **ασφάλεια των συστημάτων δικτύου και πληροφοριών**.

Αντιστοιχεί στην **Διεύθυνση Κυβερνοασφάλειας της Γενικής Γραμματείας Ψηφιακής Πολιτικής του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης**.

Ορίζει τις απαιτήσεις για την εφαρμογή μιας **Ενιαίας Πολιτικής Ασφάλειας**, σύμφωνα με το NIS Directive.

Παρακολουθεί την εφαρμογή του **Ν.4577/2018**.

Δρα ως **εθνικό ενιαίο κέντρο επαφής** για την ασφάλεια των συστημάτων δικτύου και πληροφοριών για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών των κρατών-μελών.

Συμβάλλει στην **ανταλλαγή εμπειρίας και γνώσης** με λοιπές ευρωπαϊκές αρχές/οργανισμούς κυβερνοασφάλειας, συμμετέχοντας σε συναντήσεις/ομάδες συνεργασίες.

ΕΝΙΑΙΑ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

Η Εθνική Αρχή Κυβερνοασφάλειας ορίζει τις απαιτήσεις για την εφαρμογή μιας **Ενιαίας Πολιτικής Ασφάλειας** σε κάθε οργανισμό που εμπίπτει στην κατηγορία των **Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ)**.

Κάθε οργανισμός **θεσπίζει**, **υλοποιεί** και **διατηρεί** επίκαιρη και καταγεγραμμένη Πολιτική Ασφαλείας σχετική με την ασφάλεια των συστημάτων δικτύου και πληροφοριών του.

Αρμόδιοι εφαρμογής:

Διοίκηση Οργανισμού

Υπεύθυνος Ασφάλειας Πληροφοριών και Δικτύων

Προσωπικό και συμβεβλημένοι προμηθευτές

ΣΤΟΧΟΙ
ΕΝΙΑΙΑΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Διασφάλιση εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας δεδομένων έναντι απειλών.

Ικανοποίηση των νομικών και κανονιστικών απαιτήσεων σχετικών με την ασφάλεια και προστασία δεδομένων.

Επιχειρησιακή συνέχεια των βασικών υπηρεσιών του Οργανισμού έναντι περιστατικών κυβερνοεπιθέσεων.

Άμεση κοινοποίηση και διαχείριση περιστατικών ή αδυναμιών ασφαλείας.

Ενημέρωση και εκπαίδευση των υπαλλήλων και εμπλεκομένων τρίτων σχετικά με την παροχή των βασικών υπηρεσιών του Οργανισμού.

ΣΤΑΔΙΑ ΕΦΑΡΜΟΓΗΣ

Η εφαρμογή των 3 σταδίων είναι μια επαναληπτική διαδικασία. Ακολουθώντας τον κύκλο **ΑΝΑΓΝΩΡΙΣΗ – ΠΡΟΣΤΑΣΙΑ – ΑΝΤΙΜΕΤΩΠΙΣΗ**, ένας οργανισμός πετυχαίνει:

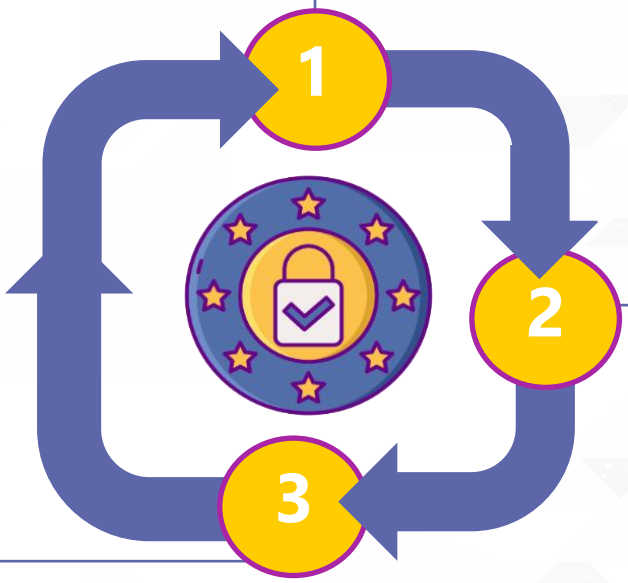
- να έχει **συνεχή παρακολούθηση** του επιπέδου ασφαλείας και ρίσκων του
- **συνεχή βελτίωση** επιχειρησιακά, οργανωτικά και τεχνικά, στο κομμάτι της κυβερνοασφάλειας

ΑΝΑΓΝΩΡΙΣΗ

Κατανόηση του επιχειρηματικού πλαισίου, των πόρων που υποστηρίζουν τις βασικές υπηρεσίες και την σχετική διακινδύνευση για την ασφάλεια των συστημάτων δικτύου και πληροφοριών.

Ενέργειες για να διασφαλιστούν όλοι οι πόροι που υποστηρίζουν τις βασικές υπηρεσίες του Οργανισμού.

ΠΡΟΣΤΑΣΙΑ



ΑΝΤΙΜΕΤΩΠΙΣΗ

Αφορά στην διαχείριση και κοινοποίηση συμβάντων ασφάλειας.

Αποτελεί το σημείο επαφής με την ΕΑΚ και το αρμόδιο CSIRT.

Εποπτεύει την υλοποίηση της ΕΠ και την ικανοποίηση των βασικών απαιτήσεων ασφάλειας.

Συντονίζει και επιβλέπει τον Οργανισμό ως προς τις υποχρεώσεις του ν. 4577/2018, ΥΑ 1027/2019 κ.α.

Εκπαιδεύει και ευαισθητοποιεί τους υπαλλήλους του Οργανισμού σε θέματα ασφάλειας πληροφοριών και δικτύων .

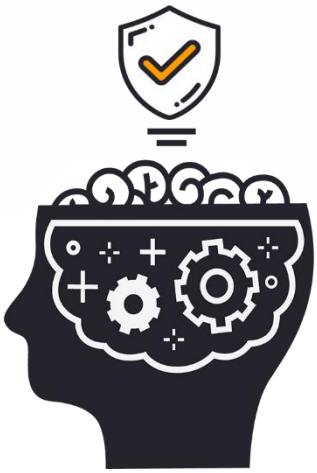
Παρίσταται στους ελέγχους που πραγματοποιεί η Ομάδα Επιθεώρησης Ελέγχου και παρέχει τα κατάλληλα μέσα για να διευκολύνει το έργο της.

Συντάσσει την ετήσια αναφοράς αυτοαξιολόγησης του Οργανισμού που αποστέλλεται στην ΕΑΚ.

Προτείνεται ο ρόλος του να είναι **ανεξάρτητος** και να μην έγκειται σε σύγκρουση συμφερόντων με άλλους εργασιακούς ρόλους που τυχόν κατέχει.

Κάθε Οργανισμός **οφείλει**:

- να ορίσει συγκεκριμένο εργαζόμενο του ως **ΥΑΠΔ**
- να κοινοποιεί στην ΕΑΚ τα στοιχεία επικοινωνίας του ΥΑΠΔ, **το αργότερο μέχρι τις 08/12/2019**



ΥΑΠΔ

Υπεύθυνος Ασφάλειας Πληροφοριών και Δικτύων

Επιθυμητά προσόντα:

- Προπτυχιακό/μεταπτυχιακό τίτλο ετήσιας τουλάχιστον διάρκειας σε συναφές γνωστικό αντικείμενο.
- 5+ Εμπειρογνωσία στον τομέα της ασφάλειας πληροφοριών και δικτύων τουλάχιστον 5 ετών.
- Πιστοποιημένη γνώση μεθοδολογιών, διαδικασιών, τεχνικών, εργαλείων και προτύπων ασφάλειας πληροφοριών και ψηφιακών συστημάτων.
- Γνώση των επιχειρηματικών διαδικασιών του Οργανισμού.

ΠΡΟΚΛΗΣΕΙΣ ΣΤΗ ΣΥΜΜΟΡΦΩΣΗ ΚΑΤΑ NIS DIRECTIVE

1. **Αναγνώριση και αλληλοσυσχέτιση κρίσιμων πόρων και δικτύων.**
2. **Συντονισμός διαδικασίας αναγνώρισης, ανάλυσης και διαχείρισης ρίσκων.**
3. **Διαχείριση συμβάσεων και SLA με προμηθευτές και εξωτερικούς συνεργάτες.**
4. **Κοινοποίηση συμβάντων ασφαλείας και σύνταξη αναφορών προς την Εθνική Αρχή Κυβερνοασφάλειας.**
5. **Σχεδιασμός και υλοποίηση αποτελεσματικού μηχανισμού εντοπισμού και ανταπόκρισης συμβάντων ασφαλείας.**

ΥΠΗΡΕΣΙΕΣ ΣΥΜΜΟΡΦΩΣΗΣ

Η **SpearIT**, έχοντας μια ομάδα έμπειρων και πιστοποιημένων επαγγελματιών cybersecurity, παρέχει ένα ολιστικό πακέτο συμμόρφωσης – συνεχούς παρακολούθησης με κανονισμούς & πρότυπα κυβερνοασφάλειας, ευθυγραμμισμένο πλέον και κατά **EU NIS Directive**.

ΠΑΡΟΧΕΣ

- **Εκπαίδευση ΥΑΠΔ και security awareness προσωπικού**
- **Σύνταξη και Συντήρηση Τεκμηρίωσης**
  Ενιαία Πολιτική Ασφάλειας & σχετικά Εγχειρίδια
- **Διαχείριση Ρίσκου**
  Ορισμός πλαισίου διαχείρισης διακινδυνεύσεων
  Αποτύπωση και αξιολόγησης διακινδυνεύσεων
  Προτάσεις αντιμετώπισης διακινδυνεύσεων
- **Διενέργεια Αυτοαξιολόγησης και Σύνταξη Αναφοράς Αυτοαξιολόγησης**
- **Τεχνικών Συμβουλών**
  Σε θέματα υλοποίησης τεχνικών και οργανωτικών μέτρων, π.χ. DR/BC, data protection, cryptography, incident handling.
- **Τεχνικών Ελέγχων Ασφαλείας**
  Ανίχνευση ευπαθειών, δοκιμές διείσδυσης σε Πληροφοριακά Συστήματα
- **Υπεύθυνου Ασφάλειας Πληροφοριών και Δικτύων (CISO as-a-Service)**
  Προηγμένη υποστήριξη εσωτερικού ΥΑΠΔ και προσωπικού
  Συμβουλευτική διαχείρισης περιστατικών ασφαλείας

Μιλήστε με έναν εκπρόσωπό μας στο
www.spearit.net

SPEARIT

Egnatia 154 st,

Thessaloniki, 54636

GREECE

p: +30 2311 320 270

w: spearit.net

e: info@spearit.net