ΕΦΗΜΕΡΙΔΑ
ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ
ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

6 Μαΐου 2025 | ΤΕΥΧΟΣ ΔΕΥΤΕΡΟ | Αρ. Φύλλου **2186**

ΑΠΟΦΑΣΕΙΣ

Αριθμ. 1689

Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων.

**ΟΙ ΥΠΟΥΡΓΟΙ
ΕΘΝΙΚΗΣ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΟΙΚΟΝΟΜΙΚΩΝ - ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ**

Έχοντας υπόψη:

1. Τις διατάξεις:

α. Του ν. 5160/2024 «Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του Κανονισμού (ΕΕ) 910/2014 και της Οδηγίας (ΕΕ) 2018/1972, και την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS 2) και άλλες διατάξεις» (Α' 195), και ιδίως της παρ. 2 του άρθρου 15 και της περ. α' της παρ. 13 του άρθρου 30,

β. του ν. 5086/2024 «Εθνική Αρχή Κυβερνοασφάλειας και άλλες διατάξεις» (Α' 23),

γ. της Οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του Κανονισμού (ΕΕ) αριθμ. 910/2010 και της Οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 (L 333/80),

δ. του Εκτελεστικού Κανονισμού (ΕΕ) 2024/2690 της Επιτροπής της 17ης Οκτωβρίου 2024 για τη θέσπιση κανόνων εφαρμογής της Οδηγίας (ΕΕ) 2022/2555 όσον αφορά τις τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τον περαιτέρω προσδιορισμό των περιπτώσεων στις οποίες ένα περιστατικό θεωρείται σημαντικό όσον αφορά τους παρόχους υπηρεσιών DNS, τα μητρώα ονομάτων TLD, τους παρόχους υπηρεσιών υπολογιστικού νέφους, τους παρόχους υπηρεσιών κέντρων δεδομένων, τους παρόχους δικτύων διανομής περιεχομένου, τους παρόχους διαχειριζόμενων υπηρεσιών, τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας, τους παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών υπηρεσιών κοινωνικής δικτύωσης και τους παρόχους υπηρεσιών εμπιστοσύνης (L/18.10.2024),

ε. του ν. 4270/2014 «Αρχές δημοσιονομικής διαχείρισης και εποπτείας (ενσωμάτωση της Οδηγίας 2011/85/ΕΕ) - δημόσιο λογιστικό και άλλες διατάξεις» (Α' 143) και ειδικότερα της περ. ιβ' του άρθρου 20,

στ. του π.δ. 79/2023 «Διορισμός Υπουργών, Αναπληρωτών Υπουργών και Υφυπουργών» (Α' 131),

ζ. του π.δ. 82/2023 «Μετονομασία Υπουργείου - Σύσταση και μετονομασία Γενικών Γραμματειών - Μεταφορά αρμοδιοτήτων, υπηρεσιακών μονάδων και θέσεων προσωπικού - Τροποποίηση και συμπλήρωση του π.δ. 77/2023 (Α' 130) - Μεταβατικές διατάξεις» (Α' 139),

η. του π.δ. 40/2020 «Οργανισμός του Υπουργείου Ψηφιακής Διακυβέρνησης» (Α' 85), και

θ. του π.δ. 81/2019 «Σύσταση, συγχώνευση, μετονομασία και κατάργηση Υπουργείων και καθορισμός αρμοδιοτήτων τους - Μεταφορά υπηρεσιών και αρμοδιοτήτων μεταξύ Υπουργείων» (Α' 119).

2. Την υπό στοιχεία 102928/ΕΞ 2023/10.07.2023 κοινή απόφαση του Πρωθυπουργού και του Υπουργού Οικονομικών «Ανάθεση αρμοδιοτήτων στον Υφυπουργό Οικονομικών, Αθανάσιο Πετραλιά» (Β' 4441).

3. Την υπό στοιχεία 11685/ΕΞ 2025/08.04.2025 εισήγηση της Υποδιοικήτριας της Εθνικής Αρχής Κυβερνοασφάλειας.

4. Την ανάγκη καθορισμού του εθνικού πλαισίου απαιτήσεων κυβερνοασφάλειας που εφαρμόζεται από τις βασικές και σημαντικές οντότητες του άρθρου 4 του ν. 5160/2024.

5. Την υπό στοιχεία 2530 ΕΞ/24.01.2025 εισήγηση δημοσιονομικών επιπτώσεων της Διεύθυνσης Προϋπολογισμού και Δημοσιονομικών Αναφορών της Γενικής Διεύθυνσης Οικονομικών και Διοικητικών Υπηρεσιών του Υπουργείου Ψηφιακής Διακυβέρνησης από την οποία προκύπτει ότι από την έκδοση της παρούσας απόφασης προκαλείται δαπάνη στις περιπτώσεις των δημοσίων οντοτήτων, των τύπων που αναφέρονται στο Παράρτημα Ι και ΙΙ του ν. 5160/2024 (Α' 195) που είναι φορείς Γενικής Κυβέρνησης, υπάγονται στον κρατικό προϋπολογισμό, και

κατά συνέπεια στο Μ.Π.Δ.Σ., και η οποία θα καλυφθεί από τους οικείους προϋπολογισμούς τους το ύψος των οποίων δεν δύναται να υπολογιστεί εκ των προτέρων αφού κυμαίνεται ανάλογα με τον βαθμό υλοποίησης των μέτρων.

6. Το γεγονός ότι οι διατάξεις της παρούσας δεν αφορούν σε διοικητική διαδικασία για την οποία υπάρχει υποχρέωση καταχώρισης στο ΕΜΔΔ - ΜΙΤΟΣ, αποφασίζουμε:

Άρθρο 1
Σκοπός

Σκοπός της παρούσας είναι ο καθορισμός του εθνικού πλαισίου απαιτήσεων κυβερνοασφάλειας, το οποίο περιλαμβάνει τα τεχνικά, επιχειρησιακά και οργανωτικά μέτρα διαχείρισης των κινδύνων κυβερνοασφάλειας της παρ. 2 του άρθρου 15 του ν. 5160/2024. Οι απαιτήσεις και τα μέτρα της παρούσας λαμβάνονται από τις βασικές και σημαντικές οντότητες του άρθρου 4 του ως άνω νόμου, προκειμένου να διαχειρίζονται τους κινδύνους που αφορούν στην ασφάλεια των συστημάτων δικτύου και πληροφοριών που οι εν λόγω οντότητες χρησιμοποιούν για τις δραστηριότητές τους ή για την παροχή των υπηρεσιών τους, καθώς και να προλαμβάνουν ή να ελαχιστοποιούν τις επιπτώσεις συμβάντων ασφάλειας στις ίδιες τις οντότητες, στους αποδέκτες των υπηρεσιών τους, καθώς και σε άλλες υπηρεσίες και οργανισμούς.

Άρθρο 2
Γενικές διατάξεις εθνικού πλαισίου απαιτήσεων κυβερνοασφάλειας

1. Οι απαιτήσεις και τα μέτρα διαχείρισης των κινδύνων κυβερνοασφάλειας της παρούσας βασίζονται σε ολιστική προσέγγιση του κινδύνου (all hazards approach), που αποσκοπεί στην προστασία των συστημάτων δικτύου και πληροφοριών και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από περιστατικά, εξασφαλίζοντας επίπεδο ασφάλειας ανάλογο προς τον εκάστοτε κίνδυνο.

2. Οι απαιτήσεις και τα μέτρα της παρούσας απόφασης τελούν υπό την επιφύλαξη των οριζομένων στις εκτελεστικές πράξεις, που εκδίδονται από την Ευρωπαϊκή Επιτροπή σύμφωνα με την παρ. 5 του άρθρου 21 της Οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του Κανονισμού (ΕΕ) αριθμ. 910/2010 και της Οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 (L 333/80).

Άρθρο 3
Γενικές αρχές εφαρμογής

1. Τα μέτρα της παρούσας εφαρμόζονται με βάση την αρχή της αναλογικότητας (proportionality principle). Για τον βαθμό και το επίπεδο εξειδίκευσης της εφαρμογής τους και για τις αντίστοιχες τεχνολογίες υλοποίησης λαμβάνονται υπόψη:

α. Το μέγεθος και η πολυπλοκότητα των επιχειρησιακών λειτουργιών της οντότητας,

β. το είδος και η κρισιμότητα των δεδομένων που η οντότητα επεξεργάζεται,

γ. ο βαθμός έκθεσης της οντότητας σε κινδύνους,

δ. η πιθανότητα εμφάνισης περιστατικών και η σοβαρότητά τους,

ε. οι κοινωνικές και οικονομικές επιπτώσεις από την εμφάνιση περιστατικών,

στ. το κόστος υλοποίησης του μέτρου σε σχέση με τα προσδοκώμενα οφέλη.

2. Οι σημαντικές οντότητες της παρ. 2 του άρθρου 4 του ν. 5160/2024 δύνανται να εφαρμόσουν επιπλέον μέτρα που απευθύνονται μόνο σε βασικές οντότητες της παρ. 1 του ν. 5160/2024, λαμβάνοντας υπόψη τα αποτελέσματα της διαδικασίας εκτίμησης κινδύνων (risk assessment).

3. Για τον σκοπό της τεκμηρίωσης εφαρμογής των μέτρων διαχείρισης των κινδύνων κυβερνοασφάλειας της παρούσας (αρχή της λογοδοσίας) ιδίως, κατά τη διενέργεια των ελέγχων και επιθεωρήσεων που προβλέπονται στα άρθρα 24 και 25 του ν. 5160/2024, λαμβάνονται υπόψη:

α. Στοιχεία τεκμηρίωσης που η οντότητα τηρεί στην υποδομή της και αφορούν σε έγγραφα ψηφιακής ή φυσικής μορφής (όπως, πολιτικές ασφάλειας και διαδικασίες, πρακτικά διοικητικού συμβουλίου, οικονομικά στοιχεία, συμβάσεις, βεβαιώσεις εκπαίδευσης, διαγράμματα δικτύου, πλάνα επιχειρησιακής συνέχειας, έγγραφα περιοδικής αξιολόγησης μέτρων και διαδικασιών, αναφορές ελέγχων ασφάλειας, μηνύματα ηλεκτρονικού ταχυδρομείου). Τα τηρούμενα αποδεικτικά στοιχεία πρέπει να είναι επαρκή για την τεκμηρίωση συμμόρφωσης με τις οικείες υποχρεώσεις.

β. Στοιχεία τεκμηρίωσης που προκύπτουν μέσω της φυσικής παρατήρησης κατάλληλου δείγματος πληροφοριακών συστημάτων και εξέτασης των εφαρμοσμένων μέτρων ασφάλειας και διαδικασιών (ενδεικτικά, τεχνολογίες ασφάλειας δικτύων, μέτρα ασφάλειας σε συσκευές τελικού χρήστη και διακομιστές, κατανομή δικαιωμάτων πρόσβασης, μέτρα φυσικής ασφάλειας).

γ. Στοιχεία τεκμηρίωσης που προκύπτουν μέσω συνεντεύξεων με κατάλληλο δείγμα μελών της διοίκησης και εργαζομένων της οντότητας.

Άρθρο 4
Υποχρεώσεις και ευθύνη των ανωτάτων οργάνων διοίκησης

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα διαμορφώνει και υλοποιεί, με ευθύνη του κατά περίπτωση ανώτατου οργάνου διοίκησης, ολοκληρωμένο πρόγραμμα διαχείρισης των κινδύνων κυβερνοασφάλειας, που αποτελείται από πολιτικές, διαδικασίες, ανάθεση ρόλων, αρμοδιοτήτων και ευθυνών, καθώς και από ένα σύνολο τεχνικών, οργανωτικών και επιχειρησιακών μέτρων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών.

β. Το ανώτατο όργανο διοίκησης της οντότητας:

βα. εγκρίνει το πρόγραμμα διαχείρισης των κινδύνων κυβερνοασφάλειας και λαμβάνει μέριμνα για τη συνολική υλοποίηση, επίβλεψη, περιοδική αξιολόγηση και συνεχή βελτίωσή του.

ββ. διασφαλίζει ότι παρέχονται οι απαραίτητοι πόροι για την υλοποίηση του προγράμματος διαχείρισης των κινδύνων κυβερνοασφάλειας και για τη λήψη των κατάλληλων και αναλογικών τεχνικών, επιχειρησιακών και οργανωτικών μέτρων διαχείρισης των εν λόγω κινδύνων.

βγ. διασφαλίζει ότι το σύνολο του προσωπικού ενημερώνεται για τις υποχρεώσεις και τις ευθύνες του όσον αφορά στην τήρηση και εφαρμογή της πολιτικής ασφάλειας, των θεματικών πολιτικών ασφάλειας και των συναφών διαδικασιών της οντότητας.

βδ. διασφαλίζει ότι η οικεία οντότητα τηρεί τα στοιχεία της περ. α’ της παρ. 3 του άρθρου 3 της παρούσας και λογοδοτεί, σύμφωνα με την παρ. 1 του άρθρου 14 του ν. 5160/2024 (Α’ 195), για την τυχόν πλημμελή εφαρμογή του προγράμματος διαχείρισης των κινδύνων κυβερνοασφάλειας και για τη μη λήψη των κατάλληλων και αναλογικών τεχνικών, επιχειρησιακών και οργανωτικών μέτρων διαχείρισης των εν λόγω κινδύνων.

βε. παρακολουθεί σε περιοδική βάση πρόγραμμα εκπαίδευσης για θέματα κυβερνοασφάλειας και διασφαλίζει ότι παρέχεται αντίστοιχο πρόγραμμα και στο προσωπικό της.

Άρθρο 5
Πλαίσιο διαχείρισης κινδύνων

1. Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα αναπτύσσει και τηρεί κατάλληλο πλαίσιο για τη διαχείριση των κινδύνων κυβερνοασφάλειας, το οποίο ευθυγραμμίζεται με τη συνολική στρατηγική διαχείρισης των επιχειρηματικών κινδύνων της ή των κινδύνων που προκύπτουν κατά την άσκηση των αρμοδιοτήτων της, εφόσον πρόκειται για οντότητα της περ. στ’ της παρ. 2 του άρθρου 3 του ν. 5160/2024. Για τη διαμόρφωση του εν λόγω πλαισίου λαμβάνονται υπόψη και οι σχέσεις της οντότητας με τρίτα μέρη, καθώς και με προμηθευτές και παρόχους υπηρεσιών.

β. Η οντότητα διενεργεί, σε περιοδική βάση και με αναλογικό τρόπο, εκτίμηση κινδύνων (risk assessment), εφαρμόζοντας διαδικασίες αναγνώρισης, ανάλυσης και αξιολόγησης των κινδύνων που απειλούν την ασφάλεια των συστημάτων δικτύου και πληροφοριών της. Για την υλοποίηση των εν λόγω διαδικασιών, εφαρμόζονται μεθοδολογίες που βασίζονται σε διεθνή πρότυπα ή/και βέλτιστες πρακτικές.

γ. Η οντότητα αναπτύσσει, υλοποιεί και επιβλέπει κατάλληλο πλάνο αντιμετώπισης των κινδύνων (risk treatment plan). Για την επιλογή και προτεραιοποίηση των τεχνικών, οργανωτικών και επιχειρησιακών μέτρων αντιμετώπισης των κινδύνων λαμβάνονται υπόψη:

γα. τα αποτελέσματα της διαδικασίας εκτίμησης κινδύνων (risk assessment),

γβ. τα αποτελέσματα της διαδικασίας αξιολόγησης της αποτελεσματικότητας των μέτρων διαχείρισης των κινδύνων κυβερνοασφάλειας σύμφωνα με την περ. α’ της παρ. 1 του άρθρου 18 της παρούσας,

γγ. το κόστος υλοποίησης σε σχέση με το προσδοκώμενο όφελος,

γδ. το σχήμα ταξινόμησης των αγαθών και των δεδομένων σύμφωνα με την παρ. β’ του άρθρου 11 της παρούσας,

γε. τα αποτελέσματα της ανάλυσης επιχειρηματικών επιπτώσεων σύμφωνα με την περ. β’ της παρ. 1 του άρθρου 25 της παρούσας.

δ. Τα αποτελέσματα της εκτίμησης κινδύνων (risk assessment) και το πλάνο αντιμετώπισης κινδύνων αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας ή εφόσον έχει μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.

2. Οι βασικές οντότητες, επιπλέον των μέτρων της παρ. 1, διενεργούν, σε περιοδική βάση και με αναλογικό τρόπο, εμπεριστατωμένες διαδικασίες εκτίμησης κινδύνων (risk assessment), λαμβάνοντας υπόψη πληροφορίες που αφορούν σε κυβερνοαπειλές (cyber threat intelligence) από αξιόπιστες και τεχνικά εξειδικευμένες πηγές, καθώς και τα αποτελέσματα πλήρους αξιολόγησης των ευπαθειών στα συστήματα δικτύου και πληροφοριών τους.

Άρθρο 6
Πολιτικές και διαδικασίες ασφάλειας πληροφοριών

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα εκπονεί γραπτή γενική πολιτική ασφάλειας πληροφοριών, η οποία εγκρίνεται από το ανώτατο όργανο διοίκησης και καθορίζει την προσέγγιση της οντότητας για τη διαχείριση της ασφάλειας των συστημάτων δικτύου και πληροφοριών της.

β. Η οντότητα εκπονεί γραπτές θεματικές πολιτικές ασφάλειας που καλύπτουν ειδικές πτυχές κυβερνοασφάλειας αυτής, όσον αφορά ανθρώπινο δυναμικό, διαδικασίες και τεχνολογίες. Οι θεματικές πολιτικές εγκρίνονται από το ανώτατο όργανο διοίκησης. Οι ελάχιστες θεματικές πολιτικές που απαιτούνται είναι οι ακόλουθες:

βα. Πολιτική ελέγχου πρόσβασης

ββ. Πολιτική διαχείρισης αγαθών

βγ. Πολιτική ορθής χρήσης αγαθών και δεδομένων

βδ. Πολιτική αφαιρούμενων μέσων αποθήκευσης

βε. Πολιτική διαχείρισης περιστατικών κυβερνοασφάλειας

βστ. Πολιτική ασφάλειας εφοδιαστικής αλυσίδας

βζ. Πολιτική ασφάλειας δικτύων

βη. Πολιτική διενέργειας ελέγχων κυβερνοασφάλειας

βθ. Πολιτική αντιγράφων ασφαλείας

βι. Πολιτική κρυπτογράφησης δεδομένων και επικοινωνιών

βια. Πολιτική φυσικής και περιβαλλοντικής ασφάλειας.

Επιπλέον των παραπάνω, η οντότητα δύναται, ανάλογα με τις ανάγκες της, να εκπονεί επιπρόσθετες θεματικές πολιτικές ασφάλειας.

γ. Η γενική πολιτική ασφάλειας και οι θεματικές πολιτικές αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά

κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας.

Άρθρο 7
Ρόλοι, αρμοδιότητες και εξουσίες

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα ορίζει αρμοδιότητες και εξουσίες όσον αφορά στην κυβερνοασφάλεια, τις οποίες αναθέτει σε ρόλους, οι οποίοι κατανέμονται σύμφωνα με τις επιχειρηματικές της ανάγκες ή τις αρμοδιότητές της, εφόσον πρόκειται για οντότητα της περ. στ’ της παρ. 2 του άρθρου 3 του ν. 5160/2024. Ανάλογα με το μέγεθος της οντότητας και την κρισιμότητά της, πέραν της υποχρέωσης ορισμού στελέχους τους ως Υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.), δύνανται να ορίζονται επιπρόσθετοι ρόλοι ή καθήκοντα επιπλέον των υφιστάμενων.

β. Ο Υ.Α.Σ.Π.Ε. αναφέρεται απ’ ευθείας στο ανώτατο όργανο διοίκησης της οντότητας για θέματα που σχετίζονται με την κυβερνοασφάλεια.

γ. Οι ρόλοι, αρμοδιότητες και εξουσίες αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται από το ανώτατο όργανο διοίκησης σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας.

Άρθρο 8
Ανεξάρτητος έλεγχος ασφάλειας πληροφοριών

Οι βασικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα υλοποιεί, σε περιοδική βάση, ανεξάρτητους ελέγχους (independent audits) του συνόλου των παραμέτρων του προγράμματος διαχείρισης ασφάλειας πληροφοριών της, συμπεριλαμβανομένων του προσωπικού, των πολιτικών, των διαδικασιών και των τεχνολογιών που χρησιμοποιεί. Οι ως άνω έλεγχοι δύνανται να διενεργούνται από εσωτερικούς ή εξωτερικούς ελεγκτές.

β. Η οντότητα διασφαλίζει και εγγυάται την αμεροληψία των προσώπων που διενεργούν τους ανεξάρτητους ελέγχους ασφάλειας πληροφοριών.

γ. Εφόσον από τα αποτελέσματα του ανεξάρτητου ελέγχου προκύψει ανεπαρκής υλοποίηση των απαραίτητων τεχνικών, οργανωτικών και επιχειρησιακών μέτρων κυβερνοασφάλειας, το ανώτατο όργανο διοίκησης της οντότητας εκκινεί διαδικασίες διορθωτικών ενεργειών.

δ. Οι ανεξάρτητοι έλεγχοι διενεργούνται σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας ή εφόσον έχει μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.

Άρθρο 9
Διαδικασίες παρακολούθησης της συμμόρφωσης

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα υλοποιεί διαδικασίες παρακολούθησης και αξιολόγησης της συμμόρφωσής της με τις κανονιστικές της υποχρεώσεις που σχετίζονται με την κυβερνοασφάλεια. Αναφορά με τα αποτελέσματα της παρακολούθησης της συμμόρφωσης υποβάλλεται περιοδικά στο ανώτατο όργανο διοίκησης.

β. Σε περίπτωση μη συμμόρφωσης της οντότητας με τις κανονιστικές της υποχρεώσεις, το ανώτατο όργανο διοίκησής της εκκινεί διαδικασίες διορθωτικών ενεργειών.

γ. Οι διαδικασίες παρακολούθησης και αξιολόγησης της συμμόρφωσης διενεργούνται σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα μεταβολές στο σχετικό κανονιστικό πλαίσιο ή σημαντικές αλλαγές στις λειτουργίες της οντότητας.

Άρθρο 10
Ασφάλεια ανθρώπινου δυναμικού

1. Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα υλοποιεί διαδικασίες ελέγχων καταλληλότητας του υποψηφίου προσωπικού.

β. Η οντότητα ορίζει και κοινοποιεί στο αρμόδιο προσωπικό τις ευθύνες και τα καθήκοντα που παραμένουν σε ισχύ μετά τη λήξη της σχέσης εργασίας ή τυχόν αλλαγής της κατάστασης απασχόλησης.

γ. Η οντότητα ορίζει και υλοποιεί διαδικασίες πειθαρχικού ελέγχου για το προσωπικό που έχει διαπράξει παραβίαση των οριζόμενων στη γενική πολιτική και στις θεματικές πολιτικές ασφάλειας της οντότητας.

2. Οι βασικές οντότητες, επιπλέον των μέτρων της παρ. 1, εφαρμόζουν διαδικασίες ελέγχων επαλήθευσης του ιστορικού του υποψηφίου προσωπικού (background checks), καθώς και, κατά περίπτωση, ζητήματα αμεροληψίας και ακεραιότητας. Το εν λόγω μέτρο αφορά στο υποψήφιο προσωπικό που αναλαμβάνει ρόλους και αρμοδιότητες που σχετίζονται με την κυβερνοασφάλεια, με σκοπό την επιβεβαίωση της διαρκούς καταλληλότητάς του όσον αφορά στις ικανότητες και στην αξιοπιστία του.

Άρθρο 11
Διαχείριση υλικού και λογισμικού

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα τηρεί ακριβή και ενημερωμένο κατάλογο με τα αγαθά πληροφορικής (υλικό, λογισμικό, συστήματα, κατηγορίες δεδομένων, υπηρεσίες κ.α.) που φιλοξενούνται στις εγκαταστάσεις της και σε περιβάλλοντα νεφοϋπολογιστικής (cloud). Στον εν λόγω κατάλογο περιλαμβάνονται και τα αγαθά επιχειρησιακής τεχνολογίας (operational technology), εφόσον υπάρχουν. Για κάθε αγαθό, η οντότητα ορίζει έναν ιδιοκτήτη (owner), υπεύθυνο για τη συνολική διαχείριση και συντήρησή του.

β. Η οντότητα ταξινομεί τα δεδομένα και αγαθά που διαχειρίζεται σε διακριτά επίπεδα, με βάση τις απαιτήσεις εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητάς τους. Η αντιστοίχιση κάθε αγαθού και συνόλου δεδομένων με ένα επίπεδο ταξινόμησης γίνεται ανάλογα με την ευαισθησία, κρισιμότητα και επιχειρηματική τους αξία.

γ. Η οντότητα εκπονεί γραπτή πολιτική και οδηγίες για την ορθή χρήση των αγαθών και των δεδομένων καθ’

όλη τη διάρκεια του κύκλου ζωής τους (προμήθεια, χρήση, αποθήκευση, μεταφορά και ασφαλή απομάκρυνση/διαγραφή).

δ. Η οντότητα εκπονεί γραπτή πολιτική για την ασφαλή διαχείριση των αφαιρούμενων μέσων αποθήκευσης, σύμφωνα με το σχήμα ταξινόμησης των αγαθών και των δεδομένων.

Άρθρο 12
Διαχείριση κινδύνων από τις σχέσεις με προμηθευτές και παρόχους υπηρεσιών Τ.Π.Ε.

1. Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα εκπονεί πολιτική και διαδικασίες που αφορούν στις σχέσεις της με προμηθευτές και παρόχους υπηρεσιών Τ.Π.Ε., με σκοπό τη διαχείριση των κινδύνων που σχετίζονται με τη χρήση από την οντότητα προϊόντων και υπηρεσιών τους.

β. Η οντότητα καταρτίζει και τηρεί ενημερωμένο κατάλογο με τους άμεσους προμηθευτές και παρόχους υπηρεσιών Τ.Π.Ε., (ενδεικτικά, παραγωγοί/κατασκευαστές προϊόντων υλικού και λογισμικού, πάροχοι υπηρεσιών νεφοϋπολογιστικής, πάροχοι διαχειριζόμενων υπηρεσιών, πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας), ο οποίος περιλαμβάνει κατ’ ελάχιστον σημεία επαφής, καθώς και τα προϊόντα και υπηρεσίες Τ.Π.Ε. που κάθε προμηθευτής παρέχει. Ο εν λόγω κατάλογος περιλαμβάνει και την ταξινόμηση των προμηθευτών και παρόχων υπηρεσιών Τ.Π.Ε. σε επίπεδα κρισιμότητας.

γ. Η οντότητα υλοποιεί διαδικασίες για τη διαχείριση των κινδύνων που σχετίζονται με την απόκτηση εξοπλισμού και την παροχή υπηρεσιών Τ.Π.Ε. από άμεσους προμηθευτές και παρόχους υπηρεσιών, αντίστοιχα, καθ’ όλη τη διάρκεια του κύκλου ζωής τους. Οι εν λόγω διαδικασίες αφορούν και στη χρήση από την οντότητα πόρων νεφοϋπολογιστικής από παρόχους υπηρεσιών νεφοϋπολογιστικής. Οι ως άνω διαδικασίες περιλαμβάνουν κατ’ ελάχιστον:

γα. τους τρόπους αξιολόγησης και τα κριτήρια επιλογής των άμεσων προμηθευτών και παρόχων υπηρεσιών Τ.Π.Ε. (όπως, το συνολικό επίπεδο κυβερνοασφάλειάς τους, λαμβάνοντας υπόψη τεχνικές και, κατά περίπτωση, μη τεχνικές παραμέτρους, πιστοποιήσεις, δυνατότητα διενέργειας ελέγχων κυβερνοασφάλειας εκ μέρους της οντότητας, ανάλυση αγοράς, αξιολογήσεις πελατών).

γβ. τον καθορισμό των απαιτήσεων κυβερνοασφάλειας που οι άμεσοι προμηθευτές και πάροχοι υπηρεσιών Τ.Π.Ε. πρέπει, κατά περίπτωση, να εφαρμόζουν στην υποδομή τους και στις τεχνολογίες πληροφορικής και επικοινωνιών που χρησιμοποιούν,

γγ. τον καθορισμό των απαιτήσεων κυβερνοασφάλειας που τα προς απόκτηση προϊόντα, συστήματα και υπηρεσίες Τ.Π.Ε. πρέπει, κατά περίπτωση, να πληρούν.

δ. Η οντότητα διασφαλίζει ότι στις συμβάσεις προμηθειών και παροχής υπηρεσιών Τ.Π.Ε. περιλαμβάνονται κατ’ ελάχιστον:

δα. οι απαιτήσεις κυβερνοασφάλειας που τα προϊόντα και υπηρεσίες Τ.Π.Ε. πρέπει, κατά περίπτωση, να πληρούν,

δβ. η περιγραφή των συστημάτων και δεδομένων της οντότητας στα οποία ο άμεσος προμηθευτής ή πάροχος υπηρεσιών Τ.Π.Ε. τυχόν αποκτά πρόσβαση κατά τη διάρκεια της σύμβασης,

δγ. το δικαίωμα της διενέργειας ελέγχου εκ μέρους της οντότητας ή το δικαίωμα να ζητηθούν αναφορές και αποτελέσματα παρελθόντων ελέγχων ή άλλων στοιχείων αξιολόγησης,

δδ. οι υποχρεώσεις που αφορούν στην ασφαλή λήξη της σύμβασης, στις οποίες περιλαμβάνονται, κατ’ ελάχιστον, η διαγραφή δικαιωμάτων πρόσβασης, η ασφαλής διαγραφή δεδομένων και οι απαιτήσεις εμπιστευτικότητας.

ε. Η οντότητα αξιολογεί και επικαιροποιεί σε περιοδική βάση το σύνολο των πολιτικών και διαδικασιών που αφορούν στις σχέσεις της με προμηθευτές και παρόχους υπηρεσιών Τ.Π.Ε., λαμβάνοντας υπόψη αλλαγές στις πρακτικές των προμηθευτών ή μετά από περιστατικό κυβερνοασφάλειας που σχετίζεται με παροχή προϊόντων και υπηρεσιών Τ.Π.Ε..

2. Οι βασικές οντότητες, επιπλέον των μέτρων της παρ. 1, εφαρμόζουν τα παρακάτω:

α. καθορίζουν και επιβάλλουν ενισχυμένες απαιτήσεις κυβερνοασφάλειας για τους κρίσιμους προμηθευτές και παρόχους υπηρεσιών Τ.Π.Ε.. Ως κρίσιμοι προμηθευτές και πάροχοι υπηρεσιών Τ.Π.Ε. νοούνται εκείνοι των οποίων συγκεκριμένα προϊόντα, συστατικά, τεχνολογίες και υπηρεσίες θεωρούνται κρίσιμα λόγω της απαραίτητης φύσης τους για την υποστήριξη της παροχής της κύριας δραστηριότητας της οντότητας και των δυνητικών επιπτώσεων στην εθνική ασφάλεια, στη δημόσια ασφάλεια, στη δημόσια υγεία και στην οικονομική σταθερότητα.

β. επεκτείνουν, εφόσον απαιτείται, τις διαδικασίες διαχείρισης κινδύνων στο σύνολο της εφοδιαστικής τους αλυσίδας, καθορίζοντας απαιτήσεις κυβερνοασφάλειας και σε υπεργολάβους των αναδόχων προμηθευτών και παρόχων υπηρεσιών Τ.Π.Ε..

Άρθρο 13
Διαχείριση λογαριασμών και έλεγχος πρόσβασης

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα εκπονεί πολιτική και διαδικασίες που αφορούν στο λογικό έλεγχο πρόσβασης (logical access control) στα συστήματα δικτύου και πληροφοριών της, με βάση τις επιχειρηματικές της ανάγκες ή τις αρμοδιότητές της, εφόσον πρόκειται για οντότητα της περ. στ’ της παρ. 2 του άρθρου 3 του ν. 5160/2024, καθώς και τις απαιτήσεις ασφάλειας. Οι ως άνω πολιτικές και διαδικασίες αφορούν στο προσωπικό της οντότητας και σε προσωπικό άλλων οντοτήτων, όπως είναι προμηθευτές και πάροχοι υπηρεσιών Τ.Π.Ε..

β. Η οντότητα χορηγεί μοναδική ταυτότητα (identity) σε κάθε χρήστη και σύστημα που αποκτά πρόσβαση στα συστήματα δικτύου και πληροφοριών της, με σκοπό τη διασφάλιση λογοδοσίας για ενέργειες που εκτελούνται με τη συγκεκριμένη ταυτότητα.

γ. Η οντότητα χορηγεί και ανακαλεί δικαιώματα πρόσβασης στα συστήματα δικτύου και πληροφοριών της

με βάση τις αρχές των ελάχιστων προνομίων (least privilege), της ανάγκης γνώσης (need to know) και του διαχωρισμού καθηκόντων (separation of duties).

δ. Η οντότητα διασφαλίζει ότι η χορήγηση «προνομιούχων» (privileged) λογαριασμών και δικαιωμάτων διαχείρισης περιορίζονται στον απόλυτα απαραίτητο βαθμό, με βάση την κρισιμότητα των επιχειρηματικών λειτουργιών της ή των αρμοδιοτήτων της, κατά περίπτωση, καθώς και το σχήμα ταξινόμησης των αγαθών και των δεδομένων.

ε. Η οντότητα διασφαλίζει ότι στις περιπτώσεις μεταβολής ή διακοπής της απασχόλησης του προσωπικού, τα δικαιώματα πρόσβασης τροποποιούνται ανάλογα.

στ. Η οντότητα διασφαλίζει ότι εφαρμόζονται ισχυρές μέθοδοι και τεχνολογίες ασφαλούς αυθεντικοποίησης, ανάλογες με την ταξινόμηση της κρισιμότητας των αγαθών και των δεδομένων. Οι μέθοδοι αυθεντικοποίησης μπορεί να περιλαμβάνουν ισχυρά συνθηματικά, ψηφιακά πιστοποιητικά, έξυπνες κάρτες, συσκευές ή βιομετρικά μέσα.

ζ. Η οντότητα διασφαλίζει ότι εφαρμόζονται μέθοδοι και τεχνολογίες πολυπαραγοντικής αυθεντικοποίησης (multi-factor authentication) για την πρόσβαση στις τεχνολογίες πληροφορικής και επικοινωνιών της, όπου απαιτείται με βάση την ταξινόμηση της κρισιμότητας των αγαθών και των δεδομένων.

η. Η οντότητα αξιολογεί και επικαιροποιεί σε περιοδική βάση το σύνολο των πολιτικών και διαδικασιών που αφορούν στον έλεγχο πρόσβασης, ιδίως όταν λαμβάνουν χώρα σημαντικές αλλαγές στις λειτουργίες της οντότητας ή σοβαρά περιστατικά κυβερνοασφάλειας.

Άρθρο 14
Ασφαλής παραμετροποίηση υλικού, λογισμικού, υπηρεσιών και δικτύων

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα αναπτύσσει διαδικασίες και εργαλεία για την επιβολή ρυθμίσεων και παραμετροποιήσεων του υλικού, του λογισμικού, των υπηρεσιών και του δικτύου της, συμπεριλαμβανομένων των ρυθμίσεων και παραμετροποιήσεων ασφάλειας.

β. Η οντότητα υλοποιεί διαδικασίες ασφαλούς παραμετροποίησης (secure configuration) για το σύνολο του υλικού, του λογισμικού, των υπηρεσιών και του δικτύου της. Στις εν λόγω διαδικασίες δύνανται να χρησιμοποιηθούν προκαθορισμένα πρότυπα κατασκευαστών ή ανεξάρτητων ερευνητικών οργανισμών, καθώς και να εφαρμοστούν γενικές αρχές κυβερνοασφάλειας, όπως είναι η αρχή της «ελάχιστης λειτουργικότητας» (“least functionality”) και η αρχή των «ελάχιστων προνομίων» (“least privilege”).

γ. Η οντότητα διασφαλίζει ότι τα προεπιλεγμένα συνθηματικά (default passwords) τροποποιούνται κατά την εγκατάσταση κάθε νέου προϊόντος, συστήματος ή εφαρμογής.

δ. Οι διαδικασίες ασφαλούς παραμετροποίησης αξιολογούνται και επικαιροποιούνται σε περιοδική βάση, όταν νέες απειλές και ευπάθειες γίνονται γνωστές ή όταν εισάγονται νέες εκδόσεις υλικού ή λογισμικού.

Άρθρο 15
Αρχές ασφαλούς ανάπτυξης εφαρμογών

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα ορίζει τις απαιτήσεις ασφάλειας των εφαρμογών που αποκτά ή αναπτύσσει, ήδη από το στάδιο του σχεδιασμού και των προδιαγραφών, με βάση την κρισιμότητα των εφαρμογών και τους κινδύνους που σχετίζονται με τη λειτουργία τους.

β. Η οντότητα διασφαλίζει ότι υλοποιούνται αρχές συγγραφής ασφαλούς κώδικα και ασφαλούς αρχιτεκτονικής για τις εφαρμογές που αποκτά ή αναπτύσσει, όπως οι αρχές της «ασφάλειας από το σχεδιασμό» (“security by design”), της «ασφάλειας εξ ορισμού» (“security by default”), των «ελάχιστων προνομίων» (“least privilege”), καθώς και της «μηδενικής εμπιστοσύνης» (“zero-trust”).

γ. Η οντότητα διασφαλίζει ότι τα περιβάλλοντα ανάπτυξης, δοκιμών και παραγωγής των εφαρμογών που αποκτά ή αναπτύσσει είναι διαχωρισμένα μεταξύ τους και προστατευμένα με κατάλληλα μέτρα ασφάλειας (ενδεικτικά, διαχωρισμός δικτύων, ασφαλής διαμόρφωση συστημάτων, έλεγχος πρόσβασης).

δ. Η οντότητα διασφαλίζει ότι υλοποιούνται διαδικασίες διενέργειας δοκιμών και τεχνικών ελέγχων ασφάλειας σε διάφορα στάδια ανάπτυξης των εφαρμογών που αποκτά ή αναπτύσσει, και, σε κάθε περίπτωση, προ της θέσης τους σε παραγωγική λειτουργία.

Άρθρο 16
Διαχείριση αλλαγών

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα εφαρμόζει διαδικασίες για τη διαχείριση των αλλαγών στα συστήματα δικτύου και πληροφοριών της. Οι εν λόγω διαδικασίες αφορούν και σε θέματα επισκευών και συντήρησης και περιλαμβάνουν κατ’ ελάχιστον:

αα. την αξιολόγηση του πιθανού αντικτύπου των αλλαγών,

αβ. τον ορισμό κριτηρίων για την κατηγοριοποίηση και προτεραιοποίηση των αλλαγών,

αγ. την υλοποίηση των αλλαγών με βάση συγκεκριμένο πλάνο,

αδ. την πραγματοποίηση δοκιμών για τις αλλαγές, καθώς και την αποδοχή των δοκιμών.

β. Οι διαδικασίες διαχείρισης αλλαγών αξιολογούνται και επικαιροποιούνται σε περιοδική βάση, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας.

Άρθρο 17
Διαχείριση και γνωστοποίηση ευπαθειών

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα ορίζει και εφαρμόζει διαδικασίες και ρόλους που αφορούν στον εντοπισμό, αξιολόγηση και αντιμετώπιση των τεχνικών ευπαθειών στα συστήματα δικτύου και πληροφοριών της.

β. Η οντότητα λαμβάνει και επεξεργάζεται, σε τακτική βάση, πληροφορίες που αφορούν σε τεχνικές ευπάθειες τεχνολογιών πληροφορικής και επικοινωνιών μέσω κατάλληλων πηγών, όπως είναι αρμόδιες αρχές, ερευνητικοί οργανισμοί, προμηθευτές και πάροχοι υπηρεσιών, καθώς και αρμόδιες ομάδες απόκρισης σε περιστατικά κυβερνοασφάλειας (CSIRTs).

γ. Η οντότητα εγκαθιστά τις ενημερώσεις ασφάλειας (security patches) στα συστήματα δικτύου και πληροφοριών της εντός εύλογου χρονικού διαστήματος αφότου αυτές καταστούν διαθέσιμες. Το εν λόγω μέτρο αφορά ιδίως σε κρίσιμα συστήματα με δημόσια IP διεύθυνση στο διαδίκτυο. Κατ’ εξαίρεση, η οντότητα δύναται να μην εγκαθιστά τις ενημερώσεις ασφάλειας, όταν τα μειονεκτήματα της εφαρμογής τους υπερτερούν έναντι των πλεονεκτημάτων στην ασφάλεια πληροφοριών. Στην περίπτωση αυτή, η οντότητα εφαρμόζει κατάλληλα αντισταθμιστικά μέτρα προστασίας και τηρεί πλήρη τεκμηρίωση για κάθε τέτοια απόφαση.

δ. Η οντότητα διενεργεί δοκιμές των ενημερώσεων ασφάλειας σε ελεγχόμενο περιβάλλον, προτού αυτές εγκατασταθούν σε συστήματα που βρίσκονται σε παραγωγική λειτουργία, εφόσον απαιτείται με βάση το σχήμα ταξινόμησης των αγαθών και των δεδομένων.

ε. Η οντότητα διενεργεί σε περιοδική βάση σαρώσεις ευπαθειών (vulnerability scanning) στα συστήματα δικτύου και πληροφοριών της μέσω αυτοματοποιημένων εργαλείων, τα αποτελέσματα των οποίων καταγράφονται σε αναλυτική αναφορά.

στ. Η οντότητα αποκαθιστά τις ευπάθειες που έχουν ανιχνευθεί στα συστήματα δικτύου και πληροφοριών της εντός εύλογου χρονικού διαστήματος, με βάση συγκεκριμένο πλάνο προτεραιοποίησης, λαμβάνοντας υπόψη τη σοβαρότητα των ευπαθειών, τις δυνητικές επιπτώσεις τους, καθώς και την ταξινόμηση της κρισιμότητας των αγαθών και των δεδομένων. Η οντότητα τηρεί πλήρη τεκμηρίωση για τους λόγους που συγκεκριμένες εντοπισμένες ευπάθειες δεν απαιτούν αποκατάσταση.

ζ. Η οντότητα ορίζει και υλοποιεί διαδικασία για τη γνωστοποίηση μη δημόσια γνωστών ευπαθειών (zero-day vulnerabilities) που αφορούν στα συστήματα δικτύου και πληροφοριών της προς το αρμόδιο CSIRT (Computer Security Incident Response Team), προς τον σκοπό της συντονισμένης γνωστοποίησης ευπαθειών σύμφωνα με το άρθρο 12 του ν. 5160/2024.

Άρθρο 18
Αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας

1. Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα εκπονεί πολιτική και διαδικασίες που αφορούν στη διενέργεια ελέγχων κυβερνοασφάλειας στα συστήματα δικτύου και πληροφοριών της, για το σκοπό της αξιολόγησης της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας που έχουν υλοποιηθεί σε αυτά. Οι εν λόγω διαδικασίες περιλαμβάνουν το πεδίο εφαρμογής, τη συχνότητα και το είδος των ελέγχων ασφάλειας.

β. Η οντότητα διενεργεί σε περιοδική βάση, τουλάχιστον μία φορά ετησίως ή κατόπιν σοβαρού περιστατικού κυβερνοασφάλειας, εξωτερικούς ελέγχους παρείσδυσης (external penetration tests) στα συστήματα δικτύου και πληροφοριών της.

γ. Η οντότητα υλοποιεί διαδικασίες αποκατάστασης των ελλείψεων που διαπιστώνονται στους εξωτερικούς ελέγχους παρείσδυσης, καθώς και διαδικασίες επικύρωσης των διορθωτικών μέτρων, με βάση συγκεκριμένο πλάνο προτεραιοποίησης, λαμβάνοντας υπόψη την κρισιμότητα των ευρημάτων.

δ. Η οντότητα διενεργεί σε ετήσια βάση ή κατόπιν σοβαρού περιστατικού κυβερνοασφάλειας, αυτοαξιολόγηση της ασφάλειας των συστημάτων δικτύου και πληροφοριών της, με χρήση κατάλληλου Οδηγού που εκδίδει και αναθεωρεί η Εθνική Αρχή Κυβερνοασφάλειας. Τα αποτελέσματά της αποστέλλονται στην Εθνική Αρχή Κυβερνοασφάλειας, συνοδευόμενα από πλάνο διορθωτικών ενεργειών.

2. Οι βασικές οντότητες, επιπλέον των μέτρων της παρ. 1, εφαρμόζουν τα ακόλουθα:

α. Η οντότητα διενεργεί σε περιοδική βάση, τουλάχιστον μία φορά ετησίως ή κατόπιν σοβαρού περιστατικού κυβερνοασφάλειας, εσωτερικούς ελέγχους παρείσδυσης (internal penetration tests) στα συστήματα δικτύου και πληροφοριών της, με βάση το σχήμα ταξινόμησης των αγαθών και των δεδομένων.

β. Η οντότητα υλοποιεί διαδικασίες αποκατάστασης των ελλείψεων που διαπιστώνονται στους εσωτερικούς ελέγχους παρείσδυσης, καθώς και διαδικασίες επικύρωσης των διορθωτικών μέτρων, με βάση σαφές πλάνο προτεραιοποίησης, λαμβάνοντας υπόψη την κρισιμότητα των ευρημάτων.

Άρθρο 19
Ασφάλεια δικτύων

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα εκπονεί γραπτή πολιτική και διαδικασίες που αφορούν στην προστασία των δικτύων και δικτυακών συσκευών της από παραβίαση.

β. Η οντότητα υλοποιεί τείχη προστασίας (firewalls) που περιορίζουν και φιλτράρουν τις δικτυακές συνδέσεις, για την προστασία του δικτύου της από μη εξουσιοδοτημένη πρόσβαση. Ανάλογα με το επίπεδο επικινδυνότητας και την κρισιμότητα των επιμέρους υποδικτύων ή ζωνών, η οντότητα υλοποιεί επιπρόσθετα προηγμένες τεχνολογίες, όπως intrusion detection/prevention systems (IDS/IPS) ή web application firewalls (WAF).

γ. Η οντότητα εφαρμόζει κανόνες που αφορούν στην ασφαλή σύνδεση, στις απαιτήσεις αυθεντικοποίησης και στις διαδικασίες εξουσιοδότησης, για τον έλεγχο της πρόσβασης στο δίκτυο και στις δικτυακές της υπηρεσίες.

δ. Η οντότητα εφαρμόζει κανόνες και τεχνολογίες για την αποτροπή σύνδεσης μη εξουσιοδοτημένων συσκευών στο εσωτερικό της δίκτυο.

ε. Η οντότητα διαχωρίζει το δίκτυό της σε διακριτά υποδίκτυα ή ζώνες (network segmentation), με βάση

το βαθμό κρισιμότητας και ευαισθησίας των επιχειρηματικών λειτουργιών της και τα αποτελέσματα της αξιολόγησης κινδύνων.

στ. Η οντότητα εφαρμόζει φιλτράρισμα της δικτυακής κίνησης μεταξύ των διακριτών υποδικτύων, με βάση τις απαιτήσεις ασφάλειας κάθε ζώνης.

ζ. Η οντότητα υλοποιεί ισχυρά μέτρα ελέγχου πρόσβασης και αυθεντικοποίησης για τις απομακρυσμένες συνδέσεις χρηστών στο δίκτυό της, συμπεριλαμβανομένων των προμηθευτών και παρόχων υπηρεσιών Τ.Π.Ε..

η. Η οντότητα περιορίζει τις ανοικτές δικτυακές θύρες, τα πρωτόκολλα και τις δικτυακές υπηρεσίες της στον απολύτως απαραίτητο βαθμό, με βάση τις επιχειρηματικές της λειτουργίες.

θ. Η οντότητα υλοποιεί βέλτιστες πρακτικές όσον αφορά στην ασφάλεια του DNS (Domain Name System) και στην ασφαλή δρομολόγηση της δικτυακής κίνησης από και προς το δίκτυό της.

ι. Η οντότητα υλοποιεί μέτρα προστασίας έναντι απειλών στη διαθεσιμότητα των κρίσιμων υπηρεσιών της, με σκοπό τη διασφάλιση της συνεχούς και αδιάλειπτης λειτουργίας τους.

ια. Οι πολιτικές και διαδικασίες που αφορούν στην ασφάλεια δικτύων αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας ή εφόσον έχει μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.

Άρθρο 20
Προστασία από κακόβουλο λογισμικό

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα υλοποιεί, σε σταθμούς εργασίας, διακομιστές και δικτυακές συσκευές, τεχνολογίες που ανιχνεύουν και εξουδετερώνουν κακόβουλο λογισμικό. Οι ενημερώσεις των ως άνω τεχνολογιών εγκαθίστανται με αυτοματοποιημένο τρόπο.

β. Η οντότητα υλοποιεί κανόνες και τεχνολογίες που ελέγχουν την εκτέλεση εφαρμογών και ανιχνεύουν μη εξουσιοδοτημένους τύπους λογισμικού σε σταθμούς εργασίας, διακομιστές και δικτυακές συσκευές.

γ. Η οντότητα υλοποιεί τεχνολογίες που φιλτράρουν και εξετάζουν τα μηνύματα ηλεκτρονικού ταχυδρομείου, για τον εντοπισμό και την απόρριψη κακόβουλων ή ανεπιθύμητων μηνυμάτων.

δ. Η οντότητα μεριμνεί για τη χρήση μόνο υποστηριζόμενων φυλλομετρητών (web browsers) σε σταθμούς εργασίας χρηστών, για την τακτική ενημέρωσή τους, καθώς και για τον περιορισμό της εγκατάστασης σε αυτούς περιττών ή μη εξουσιοδοτημένων επεκτάσεων (extensions) τρίτων παρόχων.

ε. Η οντότητα υλοποιεί τεχνολογίες φιλτραρίσματος που εμποδίζουν τη σύνδεση των συστημάτων δικτύου και πληροφοριών της με γνωστά κακόβουλα ονόματα χώρου (domains) και ιστοτόπους.

Άρθρο 21
Εκπαίδευση και ευαισθητοποίηση σε θέματα κυβερνοασφάλειας

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα διενεργεί, σε περιοδική βάση, προγράμματα εκπαίδευσης και ευαισθητοποίησης για το σύνολο του προσωπικού, καθώς και μελών του κατά περίπτωση ανώτατου οργάνου διοίκησης, σε θέματα κυβερνοασφάλειας. Τα ως άνω προγράμματα παρέχουν βασικές πρακτικές κυβερνοϋγιεινής στους χρήστες και περιλαμβάνουν τουλάχιστον:

αα. την ασφαλή χρήση του ηλεκτρονικού ταχυδρομείου και τους τρόπους αντιμετώπισης μηνυμάτων εξαπάτησης και κοινωνικής μηχανικής,

αβ. τη δημιουργία και διαχείριση ισχυρών κωδικών πρόσβασης,

αγ. τη χρήση μεθόδων πολυπαραγοντικής αυθεντικοποίησης (multi-factor authentication),

αδ. τους τρόπους ασφαλούς πλοήγησης στο διαδίκτυο,

αε. τις βασικές ρυθμίσεις ασφάλειας στο οικιακό δίκτυο του χρήστη, με σκοπό τη διενέργεια τηλεργασίας και απομακρυσμένης πρόσβασης με ασφαλή τρόπο,

αστ. τους τρόπους λήψης αντιγράφων ασφαλείας,

αζ. τους τρόπους αναγνώρισης δυνητικών συμβάντων κυβερνοασφάλειας και αναφοράς τους στο αρμόδιο προσωπικό.

β. Η οντότητα διενεργεί, σε περιοδική βάση, προγράμματα εκπαίδευσης σε θέματα κυβερνοασφάλειας για συγκεκριμένες κατηγορίες εργαζομένων, με βάση τον τεχνικά εξειδικευμένο ρόλο και τις αρμοδιότητές τους στη διαχείριση των συστημάτων δικτύου και πληροφοριών της οντότητας. Τα ως άνω προγράμματα περιλαμβάνουν τουλάχιστον:

βα. λεπτομερείς οδηγίες για την ασφαλή παραμετροποίηση και λειτουργία συσκευών, συστημάτων, εφαρμογών, υπηρεσιών και δικτύων,

ββ. ανάλυση γνωστών απειλών και κινδύνων κυβερνοασφάλειας,

βγ. εκπαίδευση στη διαχείριση και αποτελεσματική απόκριση σε περιστατικά κυβερνοασφάλειας.

γ. Τα προγράμματα εκπαίδευσης και ευαισθητοποίησης στην κυβερνοασφάλεια αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται, λαμβάνοντας υπόψη αλλαγές σε κανονιστικές απαιτήσεις, μεταβολές στο τρέχον διεθνές περιβάλλον κυβερνοαπειλών, καθώς και τις τεχνολογικές εξελίξεις.

Άρθρο 22
Χρήση κρυπτογραφίας

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα εκπονεί γραπτή πολιτική και διαδικασίες που αφορούν στην κρυπτογραφία, με σκοπό τη διασφάλιση της εμπιστευτικότητας, αυθεντικότητας και ακεραιότητας των δεδομένων της, σε συμφωνία με το σχήμα ταξινόμησης των αγαθών και των δεδομένων, καθώς και τα αποτελέσματα της αποτίμησης επικινδυνότητας.

β. Η οντότητα διασφαλίζει ότι τα δεδομένα που έχουν ταξινομηθεί ως αυξημένης κρισιμότητας και είναι απο-

θηκευμένα σε υπολογιστές τελικού χρήστη, διακομιστές, αφαιρούμενα μέσα, εφαρμογές και βάσεις δεδομένων κρυπτογραφούνται (encryption at rest).

γ. Η οντότητα διασφαλίζει ότι τα δεδομένα που έχουν ταξινομηθεί ως αυξημένης κρισιμότητας κρυπτογραφούνται κατά τη μεταφορά τους μέσω δικτύου (encryption in transit).

δ. Η οντότητα υλοποιεί διαδικασίες που αφορούν στην κρυπτογραφία και καλύπτουν:

δα. τους τρόπους κρυπτογράφησης και το είδος των πρωτοκόλλων και αλγορίθμων, σε αναλογία με το απαιτούμενο επίπεδο προστασίας και το σχήμα ταξινόμησης των αγαθών και των δεδομένων,

δβ. την προσέγγιση στη διαχείριση των κρυπτογραφικών κλειδιών και ψηφιακών πιστοποιητικών, συμπεριλαμβανομένων των μεθόδων δημιουργίας, διανομής, αποθήκευσης, αλλαγής και ανάκλησής τους.

ε. Οι διαδικασίες που αφορούν στην κρυπτογραφία αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται σε περιοδική βάση, λαμβάνοντας υπόψη τις εξελίξεις στις μεθόδους και τεχνολογίες κρυπτογράφησης.

Άρθρο 23
Φυσική και περιβαλλοντική ασφάλεια

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα εκπονεί γραπτή πολιτική και διαδικασίες που αφορούν στον φυσικό έλεγχο πρόσβασης (physical access control) στην υποδομή της και στους χώρους που φιλοξενούν πληροφοριακά της συστήματα, καθώς και στην προστασία τους από φυσικούς και περιβαλλοντικούς κινδύνους.

β. Η οντότητα υλοποιεί επαρκή μέτρα φυσικής ασφάλειας και επίβλεψης στην περίμετρο των εγκαταστάσεών της, καθώς και, όπου απαιτείται, εσωτερικές διακριτές ζώνες προστασίας ανάλογες με τις απαιτήσεις ασφάλειας κάθε ζώνης.

γ. Η φυσική πρόσβαση στους χώρους που φιλοξενούν κρίσιμα πληροφοριακά συστήματα της οντότητας περιορίζεται σε εξουσιοδοτημένο προσωπικό και με την εφαρμογή κατάλληλων μεθόδων ταυτοποίησης, καταγραφής και επίβλεψης.

δ. Η οντότητα υλοποιεί επαρκή μέτρα προστασίας από φυσικούς και περιβαλλοντικούς κινδύνους, ιδίως όσον αφορά στις περιπτώσεις πυρκαγιάς, πλημμύρας και εγκληματικής δραστηριότητας.

ε. Η οντότητα υλοποιεί επαρκή μέτρα προστασίας και επίβλεψης των μηχανισμών και μέσων υποστήριξης της συνεχούς λειτουργίας των πληροφοριακών της συστημάτων, ιδίως όσον αφορά στα μέσα παροχής ηλεκτρισμού, νερού, εξαερισμού και κλιματισμού, από συμβάντα αστοχίας ή σοβαρής διατάραξης της λειτουργίας τους.

στ. Η πολιτική και οι διαδικασίες φυσικής και περιβαλλοντικής ασφάλειας αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά φυσικής και περιβαλλοντικής ασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας.

Άρθρο 24
Διαχείριση περιστατικών κυβερνοασφάλειας

Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα αναπτύσσει γραπτή πολιτική διαχείρισης περιστατικών κυβερνοασφάλειας, η οποία περιλαμβάνει:

αα. καθορισμό ρόλων και διαδικασιών για την αναφορά περιστατικών σε αρμόδιες αρχές,

αβ. λεπτομερές πλάνο για την ανίχνευση, ανάλυση και απόκριση σε περιστατικά κυβερνοασφάλειας, καθώς και ανάκαμψης και επαναφοράς των συστημάτων σε ορθή λειτουργία.

β. Η οντότητα ορίζει τουλάχιστον έναν υπάλληλο από το προσωπικό της που διαχειρίζεται και συντονίζει τη διαδικασία απόκρισης σε περιστατικά κυβερνοασφάλειας. Εάν το έργο της διαχείρισης περιστατικών έχει ανατεθεί σε εξωτερικό ανάδοχο, η οντότητα ορίζει τουλάχιστον έναν υπάλληλο από το προσωπικό της με ρόλο επίβλεψης της διαδικασίας.

γ. Η οντότητα παραμετροποιεί τα συστήματα δικτύου και πληροφοριών της (διακομιστές, δικτυακές συσκευές, συσκευές χρηστών, συστήματα και εφαρμογές) ώστε να καταγράφουν δραστηριότητες που σχετίζονται με αυτά (event logging). Η εν λόγω καταγραφή αφορά ιδίως δραστηριότητες που σχετίζονται με ευαίσθητα δεδομένα και λογαριασμούς αυξημένων προνομίων.

δ. Η οντότητα διασφαλίζει ότι οι καταγραφές συμβάντων συλλέγονται και τηρούνται για προκαθορισμένη χρονική περίοδο με επαρκή μέσα προστασίας από μη εξουσιοδοτημένη πρόσβαση και παραποίηση.

ε. Η οντότητα διασφαλίζει ότι τα αρχεία καταγραφής συμβάντων ελέγχονται σε τακτική βάση με σκοπό την ανίχνευση ασυνήθιστων ή/και ύποπτων δραστηριοτήτων. Στις περιπτώσεις που η παρακολούθηση και ο έλεγχος των συμβάντων γίνονται με αυτοματοποιημένο τρόπο, η οντότητα καθορίζει κατάλληλα όρια και συνθήκες για την ενεργοποίηση ειδοποιήσεων, έτσι ώστε να ανιχνεύονται έγκαιρα πιθανά περιστατικά κυβερνοασφάλειας.

στ. Η πολιτική και οι διαδικασίες απόκρισης σε περιστατικά κυβερνοασφάλειας αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας ή εφόσον έχει μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.

Άρθρο 25
Επιχειρησιακή συνέχεια και διαχείριση κρίσεων

1. Οι βασικές και σημαντικές οντότητες εφαρμόζουν τα ακόλουθα:

α. Η οντότητα καταρτίζει και τηρεί λεπτομερές πλάνο διασφάλισης επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή, βασισμένο στα αποτελέσματα της διαδικασίας αποτίμησης κινδύνων. Το εν λόγω πλάνο περιλαμβάνει τουλάχιστον τα ακόλουθα:

αα. σκοπό και πεδίο εφαρμογής,

αβ. ρόλους και αρμοδιότητες,

αγ. σημεία επαφής και κανάλια επικοινωνίας,

αδ. συνθήκες για την ενεργοποίηση του πλάνου,

αε. τη σειρά των δραστηριοτήτων ανάκαμψης για συγκεκριμένες λειτουργίες,

αστ. τους απαιτούμενους πόρους για την ορθή εκτέλεση του πλάνου.

β. Η οντότητα διενεργεί διαδικασία ανάλυσης επιχειρηματικών επιπτώσεων (business impact analysis) με σκοπό την αναγνώριση και αξιολόγηση δυνητικών επιπτώσεων λόγω επέλευσης σοβαρών διαταράξεων στις επιχειρηματικές της λειτουργίες. Με βάση τα αποτελέσματα της εν λόγω διαδικασίας, η οντότητα αναπτύσσει απαιτήσεις επιχειρησιακής συνέχειας για τα συστήματα δικτύου και πληροφοριών της.

γ. Το πλάνο διασφάλισης επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή αξιολογείται και, κατά περίπτωση, επικαιροποιείται σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας ή εφόσον έχει μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.

δ. Η οντότητα εκπονεί γραπτή πολιτική και διαδικασίες που αφορούν στη λήψη και ασφαλή διαχείριση των αντιγράφων ασφαλείας (backups) συστημάτων, εφαρμογών και δεδομένων.

ε. Η οντότητα λαμβάνει και τηρεί αντίγραφα ασφαλείας συστημάτων, εφαρμογών και δεδομένων με αυτοματοποιημένο τρόπο, λαμβάνοντας υπόψη την ταξινόμηση της κρισιμότητάς τους και την πολιτική αντιγράφων ασφαλείας.

στ. Η οντότητα υλοποιεί κατάλληλα μέτρα για τον έλεγχο της φυσικής και λογικής πρόσβασης στα αντίγραφα ασφαλείας, σε αντιστοιχία με το σχήμα ταξινόμησης των αγαθών και των δεδομένων.

ζ. Η οντότητα διενεργεί σε περιοδική βάση δοκιμή επαναφοράς (restoration) επιλεγμένου δείγματος των αντιγράφων ασφαλείας.

2. Οι βασικές οντότητες, επιπλέον των μέτρων της παρ. 1, εφαρμόζουν τα ακόλουθα:

α. Η οντότητα καταρτίζει και τηρεί διαδικασίες για τη διαχείριση κρίσεων σε περιπτώσεις ιδιαίτερα σοβαρών περιστατικών. Οι εν λόγω διαδικασίες ρυθμίζουν τουλάχιστον τα παρακάτω:

αα. τον καθορισμό ρόλων και ευθυνών για συγκεκριμένα τμήματα του προσωπικού,

αβ. τον καθορισμό των κατάλληλων καναλιών επικοινωνίας με τις αρμόδιες αρχές και οργανισμούς, ιδιαίτερα όσον αφορά στις υποχρεωτικές επικοινωνίες βάσει των νόμιμων ή των συμβατικών υποχρεώσεων της οντότητας, καθώς και επικοινωνιών με το κοινό,

αγ. την εφαρμογή των κατάλληλων μέτρων διατήρησης της ασφάλειας των συστημάτων δικτύου και πληροφοριών σε περιπτώσεις κρίσεων.

β. Οι διαδικασίες διαχείρισης κρίσεων αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας ή εφόσον έχει μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.

Άρθρο 26
Έναρξη ισχύος

Η ισχύς της παρούσας απόφασης άρχεται από τη δημοσίευσή της στην Εφημερίδα της Κυβερνήσεως.

Η απόφαση αυτή να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Αθήνα, 30 Απριλίου 2025

Οι Υπουργοί

Υφυπουργός
Εθνικής Οικονομίας
και Οικονομικών
ΑΘΑΝΑΣΙΟΣ
ΠΕΤΡΑΛΙΑΣ

Ψηφιακής Διακυβέρνησης
ΔΗΜΗΤΡΙΟΣ
ΠΑΠΑΣΤΕΡΓΙΟΥ

ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ

Το Εθνικό Τυπογραφείο αποτελεί δημόσια υπηρεσία υπαγόμενη στην Προεδρία της Κυβέρνησης και έχει την ευθύνη τόσο για τη σύνταξη, διαχείριση, εκτύπωση και κυκλοφορία των Φύλλων της Εφημερίδας της Κυβερνήσεως (ΦΕΚ), όσο και για την κάλυψη των εκτυπωτικών - εκδοτικών αναγκών του δημοσίου και του ευρύτερου δημόσιου τομέα (ν. 3469/2006/Α΄ 131 και π.δ. 29/2018/Α΄58).

1. ΦΥΛΛΟ ΤΗΣ ΕΦΗΜΕΡΙΔΑΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ (ΦΕΚ)

• Τα **ΦΕΚ σε ηλεκτρονική μορφή** διατίθενται δωρεάν στο **www.et.gr**, την επίσημη ιστοσελίδα του Εθνικού Τυπογραφείου. Όσα ΦΕΚ δεν έχουν ψηφιοποιηθεί και καταχωριστεί στην ανωτέρω ιστοσελίδα, ψηφιοποιούνται και αποστέλλονται επίσης δωρεάν με την υποβολή αιτήματος στην ηλεκτρονική διεύθυνση feksales@et.gr.

• Τα **ΦΕΚ σε έντυπη μορφή** διατίθενται σε μεμονωμένα φύλλα είτε απευθείας από το Τμήμα Πωλήσεων και Συνδρομητών, είτε ταχυδρομικά με την αποστολή αιτήματος παραγγελίας στην ηλεκτρονική διεύθυνση feksales@et.gr.

- Το κόστος ενός ασπρόμαυρου ΦΕΚ από 1 έως 16 σελίδες είναι 1,00 €, αλλά για κάθε επιπλέον οκτασέλιδο (ή μέρος αυτού) προσαυξάνεται κατά 0,20 €. Το κόστος ενός έγχρωμου ΦΕΚ από 1 έως 16 σελίδες είναι 1,50 €, αλλά για κάθε επιπλέον οκτασέλιδο (ή μέρος αυτού) προσαυξάνεται κατά 0,30 €.
- Το τεύχος Α.Σ.Ε.Π. διατίθεται δωρεάν.
- Υπάρχει δυνατότητα ετήσιας συνδρομής οποιουδήποτε τεύχους σε έντυπη μορφή μέσω του Τμήματος Πωλήσεων και Συνδρομητών.

• **Τρόποι αποστολής κειμένων προς δημοσίευση:**

Α. Αποστολή των εγγράφων προς δημοσίευση στο ΦΕΚ στην ηλεκτρονική διεύθυνση **https://eservices.et.gr**. Σχετικές εγκύκλιοι και οδηγίες στην ηλεκτρονική διεύθυνση του Εθνικού Τυπογραφείου (**www.et.gr**) στη διαδρομή **Ανακοινώσεις** → **Εγκύκλιοι**.

Β. Κατ’ εξαίρεση, όσοι πολίτες δεν διαθέτουν προηγμένη ψηφιακή υπογραφή μπορούν είτε να αποστέλλουν ταχυδρομικά, είτε να καταθέτουν με εκπρόσωπό τους κείμενα προς δημοσίευση εκτυπωμένα σε χαρτί στο Τμήμα Παραλαβής και Καταχώρισης Δημοσιευμάτων.

• Πληροφορίες, σχετικά με την αποστολή/κατάθεση εγγράφων προς δημοσίευση, την ημερήσια κυκλοφορία των Φ.Ε.Κ., με την πώληση των τευχών και με τους ισχύοντες τιμοκαταλόγους για όλες τις υπηρεσίες μας, περιλαμβάνονται στον ιστότοπο (www.et.gr). Επίσης μέσω του ιστότοπου δίδονται πληροφορίες σχετικά με την πορεία δημοσίευσης των εγγράφων, με βάση τον Κωδικό Αριθμό Δημοσιεύματος (ΚΑΔ). Πρόκειται για τον αριθμό που εκδίδει το Εθνικό Τυπογραφείο για όλα τα κείμενα που πληρούν τις προϋποθέσεις δημοσίευσης.

2. ΕΚΤΥΠΩΤΙΚΕΣ - ΕΚΔΟΤΙΚΕΣ ΑΝΑΓΚΕΣ ΤΟΥ ΔΗΜΟΣΙΟΥ

Το Εθνικό Τυπογραφείο ανταποκρινόμενο σε αιτήματα υπηρεσιών και φορέων του δημοσίου αναλαμβάνει να σχεδιάσει και να εκτυπώσει έντυπα, φυλλάδια, βιβλία, αφίσες, μπλοκ, μηχανογραφικά έντυπα, φακέλους για κάθε χρήση, κ.ά.

Επίσης σχεδιάζει ψηφιακές εκδόσεις, λογότυπα και παράγει οπτικοακουστικό υλικό.

Ταχυδρομική Διεύθυνση: **Καποδιστρίου 34, 10432 Αθήνα**

ΤΗΛΕΦΩΝΙΚΟ ΚΕΝΤΡΟ: 210 5279000

Ιστότοπος: **www.et.gr**

Πληροφορίες σχετικά με την λειτουργία του ιστότοπου: **helpdesk.et@et.gr**

Αποστολή εγγράφων προς δημοσίευση στο ΦΕΚ στην ηλεκτρονική διεύθυνση **https://eservices.et.gr**

ΕΞΥΠΗΡΕΤΗΣΗ ΚΟΙΝΟΥ

Πωλήσεις - Συνδρομές: (Ισόγειο, τηλ. 210 5279178 - 180)
Πληροφορίες: (Ισόγειο, Γραφείο 3 και τηλεφ. κέντρο 210 5279000)
Παραλαβή Δημοσιευτέας Ύλης: (Ισόγειο, τηλ. 210 5279167, 210 5279139)

Ωράριο για το κοινό: Δευτέρα έως και Παρασκευή: 8:00 - 13:30

02021860605250012