ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ

Μαρούσι, 21-07-2025

ΑΠ: 1161/13

ΑΠΟΦΑΣΗ

Έγκριση της «Πολιτικής Διενέργειας Ελέγχων Ασφάλειας Πληροφοριών»

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ),

Έχοντας υπόψη:

1. Τις διατάξεις:

1.1 του Ν. 4070/2012 «*Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις*» (ΦΕΚ 82/Α/2012), όπως ισχύει τροποποιηθείς,

1.2 του Ν. 4053/2012 «*Ρύθμιση λειτουργίας της ταχυδρομικής αγοράς, θεμάτων ηλεκτρονικών επικοινωνιών και άλλες διατάξεις*» (ΦΕΚ 44/Α/2012), όπως ισχύει τροποποιηθείς,

1.3 του Ν. 4727/2020 «*Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) – Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις.*» (ΦΕΚ 184/Α/2020),

1.4 του Κανονισμού (ΕΕ) αριθ. 679/2016 της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων ή ΓΚΠΔ),

1.5 του Ν. 4624/2019 «*Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις*» (ΦΕΚ 137/Α/2019),

1.6 του Ν. 4577/2018 «*Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις*», (ΦΕΚ 199/ Α' /03-12-2018), όπως ισχύει,

1.7 του Ν. 4961/2022 «*Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της*

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

ψηφιακής διακυβέρνησης και άλλες διατάξεις», (ΦΕΚ 146/Α'/27-7-2022),

1.8 του Ν. 5002/2022 «*Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών*», (ΦΕΚ 228/Α΄/2022),

1.9 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),

1.10 της ΚΥΑ υπ' αρ. 1689/30-4-2025 «*Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων*» (ΦΕΚ 2186/Β΄/6-5-2025),

2. Την ΑΠ 996/08/22-06-2021 Απόφαση της ΕΕΤΤ «*Έγκριση Οργανισμού της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων*» (ΦΕΚ 3367/Β΄/2021),

3. Την ΑΠ 1004/40/30-8-2021 Απόφαση της ΕΕΤΤ «*Κανονισμός Λειτουργίας της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)*» (ΦΕΚ 4660/Β΄/8-10-2021), όπως ισχύει τροποποιηθείσα με την ΑΠ 1062/18/24-01-2023 (ΦΕΚ 947/Β΄/2023),

4. Την εγκεκριμένη από τον Πρόεδρο της ΕΕΤΤ «*Πολιτική Ασφαλείας της ΕΕΤΤ, έκδοση 1.0*» με αριθ. πρωτ. 278/1-6-2018, όπως ισχύει μετά την αναθεώρησή της με την ΑΠ 1157/33/16-6-2025 Απόφαση της ΕΕΤΤ «*Έγκριση της εφαρμογής της αναθεωρημένης «Πολιτικής Ασφαλείας» της ΕΕΤΤ*»,

5. Την ΑΠ 989/25/26-04-2021 Απόφαση της ΕΕΤΤ «*Έγκριση της εφαρμογής της αναθεωρημένης "Πολιτικής Αποδεκτής Χρήσης των Πληροφοριακών Αγαθών της ΕΕΤΤ"*»,

6. Την ΑΠ 1048/13/24-10-2022 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Συμβάντων Ασφαλείας Πληροφοριών"*»,

7. Την ΑΠ 1115/11/10-06-2024 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Πληροφοριακών Πόρων"*»,

8. Την ΑΠ 1125/17/16-09-2024 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα"*»,

9. Την ΑΠ 1128/24/07-10-2024 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Προμήθειας και Ανάπτυξης Συστημάτων"*»,

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

10. Την ΑΠ 1138/24/23-12-2024 Απόφαση της ΕΕΤΤ *«Έγκριση της "Πολιτικής Διαχείρισης Τρίτων Μερών"»*,
11. Την ΑΠ 1109/13/15-4-2024 Απόφαση της ΕΕΤΤ «*Επικύρωση του Εγχειριδίου Διαδικασιών της ΕΕΤΤ*»,
12. Την ΑΠ 1142/21/10-02-2025 Απόφαση της ΕΕΤΤ «*Προσθήκη νέας οργανικής μονάδας και τροποποίηση της Διεύθυνσης Τηλεπικοινωνιών του Οργανισμού της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων όπως αυτός έχει εγκριθεί με την υπό στοιχεία ΑΠ ΕΕΤΤ 996/08/22.6.2021 απόφαση*» (ΦΕΚ 1280/Β΄/2025),
13. Το γεγονός ότι από τις διατάξεις της παρούσας Απόφασης δεν προκαλείται δαπάνη σε βάρος του κρατικού προϋπολογισμού ούτε του προϋπολογισμού της ΕΕΤΤ,
14. Την Εισήγηση αριθ. 38515/Φ600/16-07-2025 της αρμόδιας Υπηρεσίας της ΕΕΤΤ,

και ύστερα από προφορική εισήγηση του Προέδρου της ΕΕΤΤ (Καθηγητή Κωνσταντίνου Μασσέλου),

Επειδή :

1. Η διενέργεια ελέγχων ασφαλείας πληροφοριών είναι μια θεμελιώδης διεργασία για την προάσπιση της ασφάλειας των πληροφοριών σε έναν οργανισμό και τη μείωση των κινδύνων που την απειλούν. Περιλαμβάνει την εξέταση και αξιολόγηση πολιτικών, διαδικασιών, συμπεριφοράς ανθρώπινου δυναμικού και τεχνολογιών, τον εντοπισμό των προβληματικών σημείων και των προς βελτίωση περιοχών και έτσι επιφέρει την εφαρμογή διορθωτικών μέτρων και τη συμμόρφωση με τις κανονιστικές υποχρεώσεις και τα πρότυπα ασφαλείας.
2. Για τους παραπάνω λόγους, κρίνεται σκόπιμη η σύνταξη και γνωστοποίηση στο προσωπικό της ΕΕΤΤ μιας πολιτικής η οποία θα εξειδικεύει το πλαίσιο διενέργειας ελέγχων και δοκιμών ασφάλειας πληροφοριών σε περιοδική βάση.

Αποφασίζει :

1. **Εγκρίνει** την «*Πολιτική Διενέργειας Ελέγχων Ασφάλειας Πληροφοριών*», η οποία έχει ως εξής:

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

« *Πολιτική Διενέργειας Ελέγχων Ασφάλειας Πληροφοριών*

Έκδοση: 1η

Τελευταία Ημερομηνία Ενημέρωσης: Ιούλιος 2025

1. Σκοπός και πεδίο εφαρμογής

Οι έλεγχοι ασφάλειας πληροφοριών αξιολογούν την κατάσταση ασφάλειας των πληροφοριών ενός Οργανισμού σε μια δεδομένη χρονική στιγμή. Ελέγχουν πολιτικές, διαδικασίες, πληροφοριακά συστήματα και συμπεριφορές του ανθρώπινου δυναμικού σε σχέση με τις κανονιστικές υποχρεώσεις, το πρότυπα ασφάλειας, τις βέλτιστες πρακτικές. Εντοπίζουν ευπάθειες και πιθανούς κινδύνους και προτείνουν μέτρα και διορθωτικές ενέργειες για την ενίσχυση της προστασίας δεδομένων και υποδομών έναντι εξωτερικών και εσωτερικών απειλών. Με τους τρόπους αυτούς οι έλεγχοι ασφάλειας πληροφοριών είναι απαραίτητοι για τη διασφάλιση της διαθεσιμότητας των πληροφοριακών συστημάτων, της ακεραιότητας και εμπιστευτικότητας των δεδομένων, την αντιμετώπιση των κινδύνων ασφαλείας. Επομένως, διαδραματίζουν έναν κρίσιμο ρόλο στην προάσπιση της ασφάλειας πληροφοριών.

Σκοπός της παρούσας πολιτικής είναι η δημιουργία ενός πλαισίου διενέργειας ελέγχων και δοκιμών ασφάλειας, μέσω του οποίου η ΕΕΤΤ θα είναι σε θέση να:

- *Διατηρεί ένα επαρκές επίπεδο ωριμότητας στην ασφάλεια πληροφοριών*
- *Αξιολογεί περιοδικά το επίπεδο ασφάλειας των πληροφοριακών πόρων της μέσω των κατάλληλων τεχνικών ελέγχων (όπως δοκιμών παρείσδυσης).*

Η παρούσα πολιτική ισχύει για τους χρήστες των οποίων τα καθήκοντα σχετίζονται με τον κύκλο ζωής των πληροφοριακών συστημάτων της ΕΕΤΤ και καλύπτει θέματα σχετικά με τη διενέργεια:

- *ελέγχων / αξιολογήσεων ασφάλειας*
- *δοκιμών παρείσδυσης (penetration tests).*

Το πεδίο εφαρμογής της παρούσας πολιτικής περιλαμβάνει ανθρώπινο δυναμικό, διαδικασίες και τεχνολογίες.

2. Διαδικασία διενέργειας ελέγχων ασφάλειας

Η υλοποίηση της παρούσας πολιτικής διέπεται από μια τυποποιημένη και καταγεγραμμένη διαδικασία ελέγχου ασφάλειας, η οποία ευθυγραμμίζεται, σε γενικές γραμμές, με τις αρχές και διαδικασίες εσωτερικού ελέγχου.

Όλοι οι έλεγχοι συμμόρφωσης με την Πολιτική Ασφάλειας της ΕΕΤΤ, οι αξιολογήσεις ευπαθειών, μέτρων και μηχανισμών ασφαλείας, οι τεχνικοί έλεγχοι ασφαλείας κ.λπ. πρέπει να διενεργούνται σύμφωνα με την διαδικασία ελέγχων ασφάλειας της ΕΕΤΤ. Κύρια βήματα αυτής της διαδικασίας αποτελούν η λήψη απόφασης για την έγκριση του ελέγχου, ο σχεδιασμός του, η διενέργεια, η σύνταξη έκθεσης με τα ευρήματα, η ενημέρωση των αρμόδιων στελεχών και της Διοίκησης της ΕΕΤΤ και στη συνέχεια, η επίβλεψη εφαρμογής των διορθωτικών ενεργειών και μέτρων.

3. Σχεδιασμός ελέγχων ασφάλειας

3.1 Σχεδιασμός-προγραμματισμός ελέγχων και ενεργοποίηση της διαδικασίας

Δεδομένου ότι το ζητούμενο είναι η διαρκής εποπτεία της ασφάλειας, πρέπει να διαμορφωθεί και να υιοθετηθεί ένα ετήσιο Σχέδιο Ελέγχου Ασφάλειας. Εκτός από τους προγραμματισμένους ελέγχους αυτού του σχεδίου, η διαδικασία ελέγχου ασφάλειας πρέπει να ακολουθείται επίσης:

- *μετά από σημαντικές αλλαγές στα πληροφοριακά συστήματα (βλ. την Πολιτική Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα),*
- *μετά από σημαντικές αλλαγές στις λειτουργίες της ΕΕΤΤ,*

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

- *μετά την ολοκλήρωση της διαδικασίας αντιμετώπισης περιστατικού ασφαλείας (βλ. την Πολιτική Διαχείρισης Συμβάντων Ασφαλείας Πληροφοριών),*
- *μετά από σχετικό αίτημα κάποιας υπηρεσιακής μονάδας,*
- *μετά την ολοκλήρωση της ανάλυσης κινδύνου (βλ. πολιτικές αξιολόγησης κινδύνων της ΕΕΤΤ),*
- *εφόσον μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών,*
- *όταν προκύπτει κάποια συγκεκριμένη ανάγκη ή ζήτημα που κρίνεται ότι πρέπει να αντιμετωπιστεί μέσω του ελέγχου.*

Στη φάση του σχεδιασμού του κάθε ελέγχου περιλαμβάνονται ο καθορισμός του εύρους, των στόχων, των κριτηρίων του ελέγχου, του χρονοδιαγράμματος υλοποίησης, της ομάδας και των πόρων που θα χρησιμοποιηθούν.

3.2 Έγκριση και εξουσιοδότηση των ελέγχων ασφάλειας

Πριν την έναρξη του ελέγχου ασφάλειας, απαιτείται έγκριση και σχετικές εξουσιοδοτήσεις. Μη εξουσιοδοτημένοι έλεγχοι ασφάλειας στα συστήματα ή τις εγκαταστάσεις της ΕΕΤΤ απαγορεύονται αυστηρά.

3.3 Προσδιορισμός του πεδίου εφαρμογής του ελέγχου

Οι έλεγχοι στην ασφάλεια περιλαμβάνουν το σύνολο των παραμέτρων διαχείρισης ασφάλειας πληροφοριών, συμπεριλαμβανομένων των πολιτικών, διαδικασιών, τεχνολογιών και της συμπεριφοράς του ανθρώπινου δυναμικού. Ενδεικτικά παραδείγματα κρίσιμων πεδίων προς έλεγχο μπορεί να είναι παλαιά συστήματα, δικαιώματα πρόσβασης, θέματα αντιμετώπισης περιστατικών και σχεδίου επιχειρησιακής συνέχειας, προστασίας προσωπικών δεδομένων, κυβερνοασφάλειας τρίτων μερών, κ.λπ.

Το πεδίο εφαρμογής του κάθε ελέγχου ασφάλειας καθορίζεται κατά τη φάση του σχεδιασμού του. Για τον καθορισμό του πεδίου εφαρμογής πρέπει να λαμβάνονται υπόψη παράμετροι όπως οι πληροφοριακοί πόροι που πρόκειται να αξιολογηθούν, η ταξινόμηση και η πολυπλοκότητά τους (βλ. την Πολιτική Διαχείρισης Πληροφοριακών Πόρων), καθώς επίσης η ανάλυση κινδύνων και οι ιδιαίτερες πτυχές του συμβάντος που ενδέχεται να προκάλεσε τον έλεγχο ασφάλειας.

3.4 Καθορισμός τύπου του ελέγχου ασφάλειας

Οι έλεγχοι ασφάλειας πληροφοριών μπορεί να περιλαμβάνουν:

- *έλεγχο της συμμόρφωσης των μέτρων ασφαλείας με τις νομοθετικές και κανονιστικές υποχρεώσεις (όπως ενδεικτικά τη νομοθεσία περί κυβερνοασφάλειας, προστασίας δεδομένων προσωπικού χαρακτήρα, ιδιωτικότητας των επικοινωνιών, υπηρεσιών εμπιστοσύνης (π.χ. ηλεκτρονικών υπογραφών), δικαιωμάτων πνευματικής ιδιοκτησίας, εκκαθάρισης αρχείων, το δημοσιοϋπαλληλικό κώδικα κ.λπ.), καθώς και τα πρότυπα ασφάλειας,*
- *εντοπισμό ευπαθειών σε υποδομές, δίκτυα, πληροφοριακά συστήματα, εφαρμογές (όπως απαρχαιωμένο λογισμικό, αδύναμα συνθηματικά κ.λπ.),*
- *έλεγχο ότι η διαμόρφωση των συστημάτων προστατεύει την ασφάλεια και τη συμμόρφωση με τα πρότυπα ασφαλείας,*
- *δοκιμές παρείσδυσης που προσομοιώνουν μια κυβερνοεπίθεση στα συστήματα και δίκτυα και επιχειρούν να εκμεταλλευτούν τις ευπάθειές τους,*
- *αξιολόγηση του συνολικού κινδύνου ασφάλειας, εντοπίζοντας πιθανούς κινδύνους που προκύπτουν από ευπάθειες, την πιθανότητα εμφάνισης και τις συνέπειές τους,*
- *εντοπισμό ελλείψεων και κενών στην εκπαίδευση και ευαισθητοποίηση του ανθρώπινου δυναμικού ως προς την ασφάλεια πληροφοριών ή*
- *συνδυασμούς των παραπάνω.*

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

Προκειμένου να καθοριστεί ο τύπος του ελέγχου, κατά τη φάση του σχεδιασμού του, δηλαδή εάν θα είναι εσωτερικός έλεγχος που σημαίνει διενεργούμενος εσωτερικά από στελέχη της ΕΕΤΤ ή εξωτερικός που διενεργείται από εξωτερικό ανάδοχο, πρέπει να λαμβάνονται υπόψη τα ακόλουθα:

- *Η ανάγκη εσωτερικής ή εξωτερικής αξιολόγησης της ασφάλειας.*
- *Η ανάγκη ανάθεσης της αξιολόγησης της ασφάλειας (εξ' ολοκλήρου ή μέρους αυτής) σε εξωτερικό συνεργάτη.*
- *Το επίπεδο των πόρων και των ικανοτήτων που απαιτούνται για την αξιολόγηση ασφάλειας.*
- *Θέματα / προβλήματα προγραμματισμού (όπως ζητήματα διαθεσιμότητας των ανθρώπινων πόρων, ιεράρχησης προτεραιοτήτων, κ.λπ.).*

3.5 Πρόσθετες απαιτήσεις ελέγχου της ασφάλειας

Επιπλέον θέματα που πρέπει, επίσης, να αντιμετωπιστούν πριν από έναν έλεγχο ασφάλειας και περιλαμβάνονται στο σχεδιασμό, είναι τα ακόλουθα:

- *Η ανάγκη σχεδιασμού κατάλληλων τεχνικών για τη διασφάλιση αποτελεσματικής αξιολόγησης της ασφάλειας.*
- *Η αξιολόγηση, επιλογή, σύναψη σύμβασης και συμφωνίας εμπιστευτικότητας με τρίτο μέρος, όταν οι αξιολογήσεις ασφάλειας ανατίθενται σε εξωτερικούς συνεργάτες (βλ. την Πολιτική Διαχείρισης Τρίτων Μερών).*
- *Το είδος των εκθέσεων αξιολόγησης ασφάλειας.*
- *Η ανάγκη υιοθέτησης πρόσθετων μεθόδων και εργαλείων για τη συλλογή των ευρημάτων του ελέγχου.*
- *Η διασφάλιση ότι ο έλεγχος δεν θα διακόψει ή επηρεάσει σημαντικά τη λειτουργία των υπό έλεγχο πληροφοριακών συστημάτων, υποδομών ή υπηρεσιακών δραστηριοτήτων.*

3.6 Ανεξαρτησία των ελέγχων ασφάλειας

Ο έλεγχος ασφαλείας πρέπει να έχει επαρκή ανεξαρτησία από εκείνους που απαιτείται να ελέγξει, έτσι ώστε να επιτελεί και να θεωρείται ότι επιτελεί το έργο του χωρίς παρεμβάσεις. Επίσης, αναγκαίο είναι να αποφεύγεται η σύγκρουση συμφερόντων, δηλαδή η κατάσταση εκείνη στην οποία ο ελεγκτής έχει ένα ανταγωνιστικό επαγγελματικό ή προσωπικό συμφέρον.

Επομένως, η ΕΕΤΤ δεν πρέπει να αναθέτει τους ελέγχους ασφάλειας των πληροφοριακών συστημάτων της σε τρίτα μέρη ή σε υπαλλήλους / οργανικές μονάδες της που είχαν σημαντικό ρόλο στην εφαρμογή ή τη λειτουργία τους, εφόσον αυτό είναι πρακτικά εφικτό. Σε αντίθετη περίπτωση πρέπει να εφαρμόζονται κατάλληλα μέτρα για την ελαχιστοποίηση των κινδύνων.
Η επιλογή τρίτων μερών για τη διενέργεια ελέγχων ασφάλειας πρέπει να βασίζεται σε παράγοντες, όπως:

- *Η εμπειρία του εξωτερικού συνεργάτη.*
- *Η επάρκεια και η ικανότητα του εξωτερικού συνεργάτη.*
- *Η μεθοδολογία που πρόκειται να ακολουθηθεί (εάν είναι διεθνώς αποδεκτή κτλ.).*
- *Η ανεξαρτησία και αντικειμενικότητα του τρίτου μέρους.*

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

3.7 Ορισμός ρόλων και αρμοδιοτήτων

Κατά το σχεδιασμό των ελέγχων, πρέπει να ορίζονται οι απαραίτητοι ρόλοι και αρμοδιότητες που σχετίζονται με τη διαχείριση των ελέγχων ασφάλειας, ανάλογα με την κάθε περίπτωση. Τη συνολική ευθύνη φέρει ο Υπεύθυνος Ασφάλειας Πληροφοριακών Συστημάτων.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

4. Διενέργεια ελέγχων ασφάλειας

4.1 Διενέργεια ελέγχων συμμόρφωσης με το πλαίσιο ασφάλειας πληροφοριών

Οι έλεγχοι συμμόρφωσης με την Πολιτική Ασφάλειας της ΕΕΤΤ πρέπει να διενεργούνται εστιάζοντας στους υφιστάμενους μηχανισμούς ασφάλειας που έχουν υλοποιηθεί. Μπορεί να περιλαμβάνουν θεματικές περιοχές ελέγχου, όπως η εσωτερική οργάνωση και διοίκηση, η διαχείριση κινδύνων, οι πολιτικές ασφάλειας πληροφοριών, η συμμόρφωση των διαδικασιών ασφαλείας με τις κανονιστικές υποχρεώσεις και τα πρότυπα, η αντιμετώπιση εκτάκτων καταστάσεων, η διαχείριση συμβάντων ασφαλείας, η επαναφορά από καταστροφή, η επιχειρησιακή συνέχεια κ.λπ.

Στόχος των ελέγχων αυτών είναι να εκτιμηθεί η συμμόρφωση των δραστηριοτήτων, χρηστών και εμπλεκομένων, η αποτελεσματικότητα της Πολιτικής Ασφάλειας σε σχέση με διεθνώς αποδεκτά πρότυπα και αρχές και η εξακρίβωση ότι το ισχύον πλαίσιο τροποποιείται, όποτε απαιτείται, αναλόγως των οργανωτικών και τεχνολογικών αλλαγών που υφίσταται η ΕΕΤΤ.

Ανάλογα με το αντικείμενο του ελέγχου, αυτός μπορεί να περιλαμβάνει επιτόπια επιθεώρηση, συνεντεύξεις με μέλη της Διοίκησης και εργαζόμενους, συλλογή στοιχείων, εξέταση πολιτικών, διαδικασιών, αρχείων τεκμηρίωσης, αναφορών συμβάντων, ανάλυση της πληροφορίας που συγκεντρώθηκε, αξιολόγηση συμμόρφωσης, κ.λπ., προκειμένου να εντοπιστούν προβληματικές περιοχές και δυνατότητες βελτίωσης.

4.2 Διενέργεια ελέγχων αναφορικά με το ανθρώπινο δυναμικό

Οι εργαζόμενοι διαδραματίζουν έναν κρίσιμο ρόλο στην ασφάλεια πληροφοριών και οι παραβιάσεις ασφαλείας συχνά οφείλονται σε ανθρώπινο λάθος. Για το λόγο αυτό, πρέπει να ελέγχεται το πλαίσιο διαχείρισης ανθρώπινου δυναμικού που είναι σημαντικό για την ασφάλεια πληροφοριών, *μέσω της υλοποίησης διαδικασιών:*

- *ελέγχου της αποτελεσματικότητας των σχετικών με την ασφάλεια ρόλων και αρμοδιοτήτων που έχει ορίσει η ΕΕΤΤ*
- *ελέγχων καταλληλότητας του υποψήφιου προσωπικού (π.χ. επαλήθευση του ιστορικού του), κατά τη διαδικασία της πρόσληψης*
- *επιβεβαίωσης της διαρκούς καταλληλότητας του προσωπικού που αναλαμβάνει ρόλους και αρμοδιότητες που σχετίζονται με την κυβερνοασφάλεια, όσον αφορά στις ικανότητες, την αξιοπιστία, την ακεραιότητα και την αμεροληψία*
- *εντοπισμού ελλείψεων και κενών στην εκπαίδευση και ευαισθητοποίηση του ανθρώπινου δυναμικού ως προς την ασφάλεια πληροφοριών*
- *ελέγχου της συμμόρφωσης των καθημερινών δραστηριοτήτων των εργαζομένων με την Πολιτική Ασφάλειας (τόσο τη γενική πολιτική όσο και τις επιμέρους θεματικές πολιτικές ασφάλειας)*
- *πειθαρχικού ελέγχου για τη διάπραξη παραβίασης των οριζόμενων στην Πολιτική Ασφαλείας και ελέγχου ότι ανακαλούνται τα δικαιώματα πρόσβασης στα πληροφοριακά συστήματα της ΕΕΤΤ για τους εργαζόμενους που είναι άμεσα εμπλεκόμενοι σε περιπτώσεις σοβαρών περιστατικών ασφαλείας και έχουν τεθεί σε αναστολή άσκησης των καθηκόντων τους*
- *ελέγχου ανάκλησης προνομίων και επιστροφής πληροφοριών και περιουσιακών στοιχείων στην ΕΕΤΤ μετά τη λήξη της εργασιακής σχέσης του εργαζόμενου.*

4.3 Διενέργεια τεχνικών ελέγχων ασφάλειας

Οι τεχνικοί έλεγχοι ασφάλειας στα πληροφοριακά συστήματα και στις υποδομές της ΕΕΤΤ (π.χ. δίκτυα, εφαρμογές, βάσεις δεδομένων) πρέπει να διενεργούνται προκειμένου να πραγματοποιηθούν οι κατάλληλες δοκιμές, να διασφαλιστεί η τεχνική συμμόρφωση με την Πολιτική Ασφάλειας της ΕΕΤΤ και να αναδειχθούν πιθανά τρωτά σημεία και ενδεχόμενοι κίνδυνοι ασφαλείας για τα οποία θα πρέπει να ληφθούν κατάλληλα διορθωτικά μέτρα.

Οι έλεγχοι ασφάλειας πρέπει να σχεδιάζονται και να διενεργούνται χωρίς να επηρεάζεται η λειτουργικότητα του υπό έλεγχο πληροφοριακού συστήματος ή υποδομής.

Πριν από κάθε έλεγχο, πρέπει να διασφαλίζεται ότι παρέχονται στους ελεγκτές μόνο τα απαραίτητα δικαιώματα πρόσβασης στους πληροφοριακούς πόρους που πρόκειται να ελέγξουν. Η ΕΕΤΤ πρέπει πάντα να επιβλέπει τη διενέργεια των ελέγχων ασφάλειας.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

Στις περιπτώσεις που κρίνεται απαραίτητο, πριν από τη διενέργεια ελέγχων ή την εφαρμογή σχεδίων αποκατάστασης που αφορούν ενημερώσεις / διορθωτικές ενέργειες σε διακομιστές που βρίσκονται σε παραγωγικό περιβάλλον, πρέπει να λαμβάνονται αντίγραφα ασφαλείας όλων των κρίσιμων και / ή ευαίσθητων πληροφοριακών συστημάτων.

Οι τεχνικοί έλεγχοι ασφάλειας πρέπει να συμπεριλαμβάνουν την επιθεώρηση των αρχείων καταγραφής (logs) που δημιουργούνται από τα συστήματα δικτύου και πληροφοριών της ΕΕΤΤ (διακομιστές, δικτυακές συσκευές, συσκευές χρηστών, πληροφοριακά συστήματα και εφαρμογές), με σκοπό την ανίχνευση ασυνήθιστων ή/και ύποπτων δραστηριοτήτων.

4.4 Η αρμοδιότητα των ελεγκτών και ο υποστηρικτικός ρόλος του προσωπικού

Πρέπει να διασφαλίζεται ότι οι έλεγχοι διενεργούνται από προσωπικό που διαθέτει τις γνώσεις, ικανότητες και απαιτούμενα προσόντα αναφορικά με τις λειτουργίες της ΕΕΤΤ, τις κανονιστικές υποχρεώσεις κτλ.

Το προσωπικό της ΕΕΤΤ που σχετίζεται με τα υπό έλεγχο πληροφοριακά συστήματα και υποδομές πρέπει να παρέχει οποιαδήποτε συνδρομή ζητηθεί από τους ελεγκτές, βάσει του σχεδίου ελέγχου.

4.5 Επίβλεψη ελέγχων ασφάλειας που διενεργούνται από τρίτα μέρη

Η ΕΕΤΤ πρέπει να διασφαλίζει ότι οι έλεγχοι ασφάλειας που διενεργούνται από τρίτα μέρη στα πληροφοριακά συστήματα, εποπτεύονται πάντα από το αρμόδιο προσωπικό. Επιπλέον, το αρμόδιο αυτό προσωπικό πρέπει να διασφαλίζει ότι οι απαραίτητοι πόροι καθώς και τα σχετικά δικαιώματα πρόσβασης είναι διαθέσιμα στους εξωτερικούς ελεγκτές και ότι ο έλεγχος διενεργείται από εξειδικευμένο προσωπικό που ενεργεί με αντικειμενικότητα και με βάση εγκεκριμένα πρότυπα και διαδικασίες.

Σε κάθε περίπτωση, κατά το σχεδιασμό και τη διενέργεια ελέγχων ασφάλειας, οι εξωτερικοί συνεργάτες πρέπει να συνοδεύονται συνεχώς από κάποιον υπάλληλο που λειτουργεί ως εκπρόσωπος της ΕΕΤΤ.

4.6 Αντικειμενικότητα των ελεγκτών

Οι ελεγκτές δεν πρέπει να επηρεάζονται από προσωπικούς ή εξωτερικούς παράγοντες αλλά να παραμένουν αμερόληπτοι κατά τη διενέργεια των ελέγχων, διαμορφώνοντας τις απόψεις και τα συμπεράσματά τους βασιζόμενοι σε αντικειμενικά στοιχεία.

Η ΕΕΤΤ διατηρεί το δικαίωμα να ελέγχει την αντικειμενικότητα των ελεγκτών.

Σε κάθε περίπτωση, είτε εσωτερικοί είτε εξωτερικοί, με τη στάση και συμπεριφορά τους, οι ελεγκτές πρέπει να διασφαλίζουν την ποιότητα και να μεγιστοποιούν την αξία του ελέγχου.

4.7 Επαγγελματισμός και δέουσα επιμέλεια των ελεγκτών

Πρέπει να επιδεικνύεται επαγγελματισμός και δέουσα επιμέλεια κατά τη διενέργεια των ελέγχων ασφάλειας και κατά την προετοιμασία των εκθέσεων και αναφορών των ελέγχων.

Η επίδειξη επαγγελματισμού προϋποθέτει την ορθή κρίση κατά τον καθορισμό του πεδίου ελέγχου, την επιλογή της μεθοδολογίας και την επιλογή σεναρίων δοκιμών και διαδικασιών για τον έλεγχο.

Η ίδια ορθή κρίση πρέπει να αποδειχθεί κατά τη διενέργεια των ελέγχων, την αξιολόγηση των αποτελεσμάτων και τη σύνταξη εκθέσεων με τα πορίσματα του ελέγχου.

Οι ελεγκτές πρέπει να συμμορφώνονται με τις απαιτήσεις της ΕΕΤΤ όπως ορίζονται στα πρότυπα διενέργειας και υποβολής εκθέσεων ελέγχου. Εάν χρειάζεται να εφαρμοστούν πιο εξειδικευμένες τεχνικές κατά τη διάρκεια των ελέγχων ασφάλειας, οι ελεγκτές πρέπει να τις ορίσουν παράλληλα.

4.8 Πρόσβαση των ελεγκτών στους πληροφοριακούς πόρους

Για τη διενέργεια ελέγχων ασφάλειας, πρέπει να χορηγούνται στους ελεγκτές μόνο τα απαιτούμενα δικαιώματα πρόσβασης στα πληροφοριακά συστήματα και τις πληροφορίες της ΕΕΤΤ και μόνο μετά από σχετική έγκριση από τα αρμόδια μέρη (π.χ. από τους ιδιοκτήτες της πληροφορίας).

Μετά την ολοκλήρωση του ελέγχου, όλα τα ειδικά δικαιώματα πρόσβασης που χορηγήθηκαν, πρέπει να διαγραφούν ή να απενεργοποιηθούν. Η διαγραφή ή η απενεργοποίηση των δικαιωμάτων πρόσβασης πρέπει να επιβεβαιωθεί από τα αρμόδια μέρη.

Σε περίπτωση που δεν επιτραπεί η παροχή προνομίων σε έναν ελεγκτή, τότε ο έλεγχος συνεχίζεται μέσω της πρόσβασης του διαχειριστή, ο οποίος ακολουθεί τις οδηγίες του ελεγκτή, παρόντος του τελευταίου.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

4.9 Διακοπές επιχειρησιακής λειτουργίας

Σε οποιαδήποτε φάση του ελέγχου, από το σχεδιασμό του έως την ολοκλήρωσή του, δεν πρέπει να προκαλούνται διακοπές στις υπηρεσιακές δραστηριότητες της ΕΕΤΤ. Εάν παρόλα αυτά κάποια διακοπή θεωρείται απαραίτητη, θα πρέπει να εγκριθεί και να λάβει χώρα κατά τη διάρκεια εγκεκριμένου χρονικού διαστήματος με τον ελάχιστο αντίκτυπο στις υπηρεσιακές δραστηριότητες.

5. Χρήση των εργαλείων τεχνικού ελέγχου ασφάλειας

5.1 Προστασία των εργαλείων τεχνικού ελέγχου ασφάλειας

Η πρόσβαση στα εργαλεία ελέγχου ασφάλειας, όπως εξειδικευμένο λογισμικό ή συσκευές, πρέπει να περιορίζεται και να χορηγείται μόνο σε εξουσιοδοτημένους χρήστες. Εάν είναι εφικτό, τα εργαλεία αυτά πρέπει να φυλάσσονται χωριστά από τα περιβάλλοντα παραγωγής και ανάπτυξης.

5.2 Λεπτομερής διαμόρφωση των εργαλείων ελέγχου τεχνικής ασφάλειας

Τα εργαλεία ελέγχου τεχνικής ασφάλειας πρέπει να είναι επαρκώς διαμορφωμένα, πριν από τη χρήση τους, προκειμένου να απενεργοποιηθούν οι λειτουργίες που δεν είναι απαραίτητες για τη διεξαγωγή του ελέγχου. Κάτι τέτοιο ελαχιστοποιεί τυχόν δυσμενείς επιπτώσεις στα συστήματα που θα μπορούσαν να επηρεάσουν την επιχειρησιακή τους συνέχεια.

5.3 Καταγραφή μέτρων των τεχνικών ελέγχων ασφάλειας

Όλα τα μέτρα που λαμβάνονται κατά τη διάρκεια των τεχνικών ελέγχων ασφάλειας πρέπει να καταγράφονται από τους ελεγκτές, ώστε να διευκολύνεται η αναπαραγωγή και ο έλεγχος των μέτρων που έχουν ληφθεί.

6. Διαχείριση και έκθεση των ευρημάτων του ελέγχου

6.1 Έγγραφα τεκμηρίωσης των ευρημάτων ελέγχου ασφάλειας

Αφού ολοκληρωθούν οι έλεγχοι ασφάλειας, όλα τα ευρήματα πρέπει να τεκμηριωθούν λεπτομερώς σε γραπτή μορφή.

6.2 Επάρκεια των εκθέσεων και αναφορών του ελέγχου

Η έκθεση ενός ελέγχου πρέπει να περιλαμβάνει το σκοπό, τους στόχους, το πεδίο του ελέγχου, τις περιγραφές των πληροφοριακών συστημάτων και της υπό έλεγχο υποδομής, την πηγή των συλλεγόμενων πληροφοριών, τη μεθοδολογία που χρησιμοποιήθηκε (και τα σχετικά κριτήρια δειγματοληψίας), τα σενάρια δοκιμών και τα αποτελέσματά τους, τις διαπιστώσεις (εντοπισμένοι κίνδυνοι, έλλειψη συμμόρφωσης, ευπάθειες κτλ.) και τις συστάσεις του ελέγχου, καθώς και απόδειξη ότι το έργο και η τεκμηρίωση που έχουν παραχθεί έχουν γίνει αποδεκτά από τα αρμόδια στελέχη της ΕΕΤΤ.

6.3 Ταξινόμηση των ευρημάτων του ελέγχου ασφάλειας

Όλα τα ευρήματα των ελέγχων ασφάλειας ταξινομούνται ως κρίσιμα, σύμφωνα με τους όρους που καθορίζονται στην Πολιτική Διαχείρισης Πληροφοριακών Πόρων. Επομένως, οποιαδήποτε γνωστοποίηση των πορισμάτων του ελέγχου από υπαλλήλους ή τρίτα μέρη χωρίς την κατάλληλη έγκριση απαγορεύεται αυστηρά.

Τα πορίσματα γνωστοποιούνται μόνο στη Διοίκηση, στον Υπεύθυνο Ασφάλειας Πληροφοριών και στα στελέχη που πρέπει να τα γνωρίζουν λόγω αρμοδιοτήτων.

6.4 Εφαρμογή των συστάσεων του ελέγχου ασφάλειας

Με την ολοκλήρωση των ελέγχων ασφάλειας πρέπει οι οργανικές μονάδες της ΕΕΤΤ που συμμετείχαν στον έλεγχο, να αναλύσουν τον άμεσο και έμμεσο αντίκτυπο που προκύπτει από τις συστάσεις. Εφόσον από τα αποτελέσματα του ελέγχου προκύψει ανεπαρκής υλοποίηση των απαραίτητων τεχνικών, οργανωτικών και επιχειρησιακών μέτρων ασφάλειας, η ΕΕΤΤ εκκινεί διαδικασίες διορθωτικών ενεργειών.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

6.5 Σχέδιο απόκρισης στα ευρήματα και επίβλεψη της εφαρμογής του

Ανάλογα με τα πορίσματα του ελέγχου, ενδέχεται να χρειάζεται η ΕΕΤΤ να αναπτύξει ένα λεπτομερές σχέδιο αντιμετώπισης όλων των ζητημάτων που ανέδειξε ο έλεγχος. Για την ανάπτυξή του πρέπει να ληφθούν υπόψη τα ακόλουθα:

- *Επανεξέταση των ευρημάτων του ελέγχου, διόρθωση τυχόν ανακριβειών και παροχή διευκρινίσεων σε απορίες ή ανησυχίες σχετικά με τα ευρήματα.*
- *Ιεράρχηση των ευρημάτων του ελέγχου, αναλόγως του υπηρεσιακού αντικτύπου.*
- *Αντιστοίχιση ευρημάτων με τις κατάλληλες οργανωτικές και / ή τεχνικές διορθωτικές ενέργειες.*
- *Ανάπτυξη χρονοδιαγράμματος με σκοπό την έγκαιρη αντιμετώπιση όλων των ζητημάτων ασφάλειας.*
- *Σαφής προσδιορισμός των διορθωτικών ενεργειών που επελέγησαν.*

Ακολουθεί η υλοποίηση του συμφωνημένου σχεδίου με τα προτεινόμενα μέτρα και η επίβλεψη της εφαρμογής του, η συγκέντρωση και αξιολόγηση στοιχείων για την πρόοδο και την αποτελεσματικότητα των διορθωτικών ενεργειών και η υποβολή σχετικών αναφορών στη Διοίκηση και τον Υπεύθυνο Ασφάλειας Πληροφοριών, όταν απαιτείται.

6.6 Τήρηση αρχείου των ελέγχων ασφάλειας

Τα αρχεία ελέγχου ασφάλειας των πληροφοριακών συστημάτων της ΕΕΤΤ πρέπει να φυλάσσονται με εμπιστευτικότητα, ως αποδεικτικά συμμόρφωσης με την Πολιτική Ασφάλειας της ΕΕΤΤ.

6.7 Περιοδικότητα διενέργειας των ελέγχων ασφάλειας

Οι έλεγχοι ασφάλειας πρέπει να διενεργούνται ανά τακτά χρονικά διαστήματα, ιδανικά σε ετήσια βάση, με στόχο την επίλυση των προβληματικών περιοχών και τη συνεχή βελτίωση. Οποιεσδήποτε οργανωτικές ή επιχειρησιακές αλλαγές, τεχνολογικές εξελίξεις, προηγούμενα ευρήματα ελέγχων και μεταβολές στα αποδεκτά επίπεδα κινδύνου που θέτει η ΕΕΤΤ, πρέπει να λαμβάνονται υπόψη πριν από τη διενέργεια ενός ανεξάρτητου ελέγχου ασφάλειας.

Η συχνότητα των ελέγχων αυτών πρέπει να καθορίζεται ανάλογα με το επίπεδο κινδύνου και την ταξινόμηση του υπό έλεγχο πληροφοριακού συστήματος ή υποδομής. Τα πληροφοριακά συστήματα και οι υποδομές που αντιμετωπίζουν μεγαλύτερους κινδύνους πρέπει να ελέγχονται πιο συχνά και πιο προσεκτικά συγκριτικά με άλλα. Το ίδιο ισχύει και για τα συστήματα και τις εφαρμογές που ταξινομούνται ως κρίσιμα ή ευαίσθητα (βλ. την Πολιτική Διαχείρισης Πληροφοριακών Πόρων), αντίστοιχα.

7. Δοκιμές παρείσδυσης (penetration tests)

7.1 Συμμόρφωση με τις πολιτικές

Όλες οι εσωτερικές ή / και εξωτερικές δοκιμές παρείσδυσης που εκτελούνται είτε από την ΕΕΤΤ είτε από εξωτερικά μέρη στόχο έχουν προσομοιώνοντας επίθεση από κακόβουλο εισβολέα και εκμεταλλευόμενοι κενά ασφαλείας, να αποκαλύπτουν τις αδυναμίες των συστημάτων. Οι δοκιμές παρείσδυσης συμμορφώνονται με τις σχετικές πολιτικές και διαδικασίες της ΕΕΤΤ.

7.2 Δομή και χαρακτηριστικά των δοκιμών παρείσδυσης

Κάθε δοκιμή παρείσδυσης, είτε εσωτερική είτε εξωτερική, πρέπει να:

- *Προσδιορίζει την κρισιμότητα κάθε ευπάθειας με βάση τον ενδεχόμενο αντίκτυπο.*
- *Προσδιορίζει τον τύπο και την πολυπλοκότητα της απειλής που μπορεί να εκμεταλλευτεί την κάθε ευπάθεια.*
- *Προσδιορίζει το ρόλο της ευπάθειας σε περίπτωση επίθεσης.*
- *Παρουσιάζει αποτελέσματα που μπορούν να χρησιμοποιηθούν για:*
    - *Να προωθήσουν νέα πρότυπα ασφάλειας, μεθόδους υλοποίησης και μελλοντικές σχεδιαστικές απαιτήσεις για συγκεκριμένα συστήματα, έτσι ώστε να μειωθούν τα κενά ασφάλειας και να αποφευχθούν μελλοντικά ζητήματα ασφάλειας.*

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

- *Να υποστηρίξουν τις διορθωτικές ενέργειες.*

7.3 Πεδίο εφαρμογής δοκιμών παρείσδυσης

Στις ακόλουθες ομάδες πληροφοριακών πόρων πρέπει να εκτελούνται τακτικά εσωτερικές και / ή εξωτερικές δοκιμές παρείσδυσης:

- *Ενσύρματα και ασύρματα δίκτυα (συμπεριλαμβανομένων των πρωτοκόλλων επικοινωνίας και των σημείων ασύρματης πρόσβασης)*
- *Συστήματα (συμπεριλαμβανομένων διακομιστών, δικτυακών συσκευών, συστημάτων ασφάλειας, φορητών υπολογιστών, εκτυπωτών, εξοπλισμού τηλεδιάσκεψης, αποθήκευσης δεδομένων, εφεδρικών συσκευών, συσκευών load balancing, κτλ.)*
- *Servers*
- *Clients*
- *Εφαρμογές, συμπεριλαμβανομένων των εφαρμογών διαδικτύου (web applications)*

Η εκτέλεση των δοκιμών παρείσδυσης πρέπει να εκτελείται εσωτερικά ή εξωτερικά ανάλογα με τις υπηρεσιακές απαιτήσεις.

Μετά από κάθε δοκιμή, τα εμπλεκόμενα μέρη πρέπει να συντάσσουν μια σύντομη έκθεση που να περιγράφει τα αποτελέσματα της δοκιμής και τις διορθωτικές ενέργειες που μπορούν να εφαρμοστούν.

7.4 Εκτέλεση δοκιμών παρείσδυσης από τρίτα μέρη

Πριν από την εκτέλεση εσωτερικής ή εξωτερικής δοκιμής παρείσδυσης από τρίτα μέρη στα πληροφοριακά συστήματα της ΕΕΤΤ, πρέπει να εφαρμοστούν τα εξής:

- *Εισήγηση προς την Ολομέλεια για έγκριση του εύρους των δοκιμών παρείσδυσης.*
- *Αξιολόγηση και επιλογή των εξωτερικών συνεργατών.*
- *Σύναψη σύμβασης με τον εξωτερικό συνεργάτη που θα συμπεριλαμβάνει τις σχετικές απαιτήσεις ασφάλειας της ΕΕΤΤ (βλ. και την Πολιτική Διαχείρισης Τρίτων Μερών).*
- *Συμφωνία Εμπιστευτικότητας με τον εξωτερικό συνεργάτη (Non-Disclosure Agreement).*
- *Κατά τα λοιπά, οι γενικοί κανόνες που αναφέρθηκαν για τη διενέργεια ελέγχων ασφαλείας πληροφοριών.*

Στα κρίσιμα ή ευαίσθητα υπό παραλαβή συστήματα, προτείνεται η ΕΕΤΤ να εξετάζει κατά την προκήρυξη και ανάθεση του έργου υλοποίησης του συστήματος σε τρίτα μέρη, μήπως συμπεριλαμβάνει την ειδική απαίτηση εκτέλεσης δοκιμής παρείσδυσης. Έτσι θα προσομοιώνεται η επίθεση και εισβολή στο σύστημα και θα επιβεβαιώνεται η ασφάλειά του για πρώτη φορά πριν την οριστική παραλαβή του.

8. Αλλαγές στην Πολιτική Διενέργειας Ελέγχων Ασφάλειας Πληροφοριών

Η ΕΕΤΤ αξιολογεί και επικαιροποιεί σε περιοδική βάση το σύνολο των πολιτικών και διαδικασιών που αφορούν στη διενέργεια ελέγχων ασφαλείας, ιδίως όταν λαμβάνουν χώρα σημαντικές αλλαγές στις λειτουργίες της ή στις τεχνολογικές εξελίξεις ή προκύπτουν μεταβολές στο περιβάλλον των κυβερνοαπειλών.

»

2. **Εντέλλεται** την κοινοποίηση της παρούσας Απόφασης στο προσωπικό της ΕΕΤΤ μέσω ανάρτησής της στη Γνωσιακή Πύλη (portal) και αποστολής της με μήνυμα ηλεκτρονικού ταχυδρομείου.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

3. **Ορίζει** ότι η «*Πολιτική Διενέργειας Ελέγχων Ασφάλειας Πληροφοριών*» πρέπει να εφαρμόζεται υποχρεωτικά και απαρέγκλιτα από το αρμόδιο προσωπικό της ΕΕΤΤ.
4. **Εξουσιοδοτεί** τον Πρόεδρο της ΕΕΤΤ όπως:
    - Προβεί σε κάθε διαδικαστική ενέργεια ή έκδοση πράξης, που θα διευκολύνει την έγκαιρη και πλήρη ολοκλήρωση κάθε δράσης που αφορά στην εφαρμογή της *«Πολιτικής Διενέργειας Ελέγχων Ασφάλειας Πληροφοριών»*.

Τροποποιεί την *«Πολιτική Διενέργειας Ελέγχων Ασφάλειας Πληροφοριών»*, όποτε αυτό απαιτείται.

Ο ΠΡΟΕΔΡΟΣ

ΚΑΘΗΓΗΤΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ ΜΑΣΣΕΛΟΣ

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr