ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ

Μαρούσι, 07-10-2024
ΑΠ 1128/24

ΑΠΟΦΑΣΗ

Έγκριση της «Πολιτικής Προμήθειας και Ανάπτυξης Συστημάτων»

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),

Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

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 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 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) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2),

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*

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

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,
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 1069/13/27-03-2023 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Ασφάλειας Τελικού Χρήστη"*»,
8. Την ΑΠ 1078/23/17-07-2023 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Προστασίας Προσωπικών Δεδομένων"*»,
9. Την ΑΠ 1115/11/10-06-2024 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Πληροφοριακών Πόρων"*»,
10. Την ΑΠ 1125/17/16-09-2024 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα"*»,
11. Την ΑΠ 1109/13/15-4-2024 Απόφαση της ΕΕΤΤ «*Επικύρωση του Εγχειριδίου Διαδικασιών της ΕΕΤΤ*»,
12. Την Εισήγηση αριθ. 37901/01-10-2024 της αρμόδιας Υπηρεσίας της ΕΕΤΤ,

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

Επειδή :

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

1. Η ΕΕΤΤ διαχειρίζεται, σε τακτική βάση, αιτήματα για νέα πληροφοριακά συστήματα και εφαρμογές, προκειμένου να υποστηρίζει αποτελεσματικά τις επιχειρησιακές λειτουργίες της.
2. Η πλειοψηφία, αν όχι το σύνολο, των πληροφοριακών συστημάτων και εφαρμογών που προμηθεύεται ή αναπτύσσει η ΕΕΤΤ επιδρούν σε πληροφορίες. Για το λόγο αυτό, κρίνεται σκόπιμη η υιοθέτηση μιας πολιτικής που θα καλύπτει τις πτυχές ασφάλειας πληροφοριών που σχετίζονται με την ανάπτυξη πληροφοριακών συστημάτων με ίδια μέσα, την ανάθεση της ανάπτυξης και διαχείρισης σε εξειδικευμένο εξωτερικό συνεργάτη, την προμήθεια εμπορικών συστημάτων / έτοιμων πακέτων λογισμικού και την ένταξη των παραπάνω σε λειτουργία και συντήρηση.
3. Σκοπός της πολιτικής αυτής θα είναι ο καθορισμός των αρχών και κανόνων για την αξιολόγηση, προμήθεια, ανάπτυξη, εγκατάσταση και ένταξη σε λειτουργία νέων πληροφοριακών συστημάτων και εφαρμογών που ικανοποιούν τους επιχειρησιακούς στόχους της ΕΕΤΤ διασφαλίζοντας τη συμμόρφωση με το σχετικό νομοθετικό και κανονιστικό πλαίσιο και τα πρότυπα ασφαλείας.

Αποφασίζει :

1. **Εγκρίνει** την «*Πολιτική Προμήθειας και Ανάπτυξης Συστημάτων*», η οποία έχει ως εξής:

« ***Πολιτική Προμήθειας και Ανάπτυξης Συστημάτων***

Έκδοση: 1η

Τελευταία Ημερομηνία Ενημέρωσης: Σεπτέμβριος 2024

1. Σκοπός και πεδίο εφαρμογής

Στόχος της παρούσας πολιτικής είναι ο καθορισμός των βασικών απαιτήσεων ασφάλειας που πρέπει να πληρούνται, προκειμένου να διασφαλιστεί ότι:

- *Η ασφάλεια των πληροφοριών ενσωματώνεται στις νέες εφαρμογές και τα πληροφοριακά συστήματα από το αρχικό κιόλας στάδιο καθορισμού των απαιτήσεων αλλά και καθ' όλη τη διάρκεια του κύκλου ζωής τους.*

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

- *Αποτρέπεται η απώλεια, η τροποποίηση ή η κακή χρήση των δεδομένων και του πηγαίου κώδικα στα συστήματα.*
- *Τα πληροφοριακά συστήματα λειτουργούν κατάλληλα, μέσω επίσημων διαδικασιών, σε όλη τη διάρκεια του κύκλου ζωής τους.*
- *Τα πληροφοριακά συστήματα αξιολογούνται συνεχώς με βάση τις προδιαγραφές και τις απαιτήσεις ασφάλειας.*
- *Τα πληροφοριακά συστήματα, όταν δεν χρησιμοποιούνται πλέον, αποσύρονται με εφαρμογή όλων των κατάλληλων μέτρων ασφάλειας.*

Η πολιτική ισχύει για τα στελέχη της ΕΕΤΤ, τους προμηθευτές, συμβούλους, αναδόχους κτλ. των οποίων τα εργασιακά καθήκοντα σχετίζονται με τον κύκλο ζωής των πληροφοριακών συστημάτων της και καλύπτει τις ακόλουθες δραστηριότητες που σχετίζονται με την προμήθεια, ανάπτυξη, υλοποίηση και διαχείριση συστημάτων:

- *Εσωτερική ανάπτυξη (δηλαδή ανάπτυξη με ίδια μέσα)*
- *Προμήθεια εμπορικών λύσεων / έτοιμων πακέτων λογισμικού*
- *Ανάθεση της ανάπτυξης και διαχείρισης σε εξειδικευμένο εξωτερικό συνεργάτη (outsourcing)*
- *Λειτουργία και συντήρηση των πληροφοριακών συστημάτων με ίδια μέσα ή μέσω αναδόχων.*

Η παρούσα πολιτική ενεργοποιείται στις εξής περιπτώσεις:

- *όταν η δραστηριότητα συνεπάγεται την ένταξη σε λειτουργία ενός υπολογιστικού συστήματος ή την ανάπτυξη ενός νέου πληροφοριακού συστήματος ή εφαρμογής ή module*
- *όταν η δραστηριότητα περιλαμβάνει την προμήθεια ενός υπολογιστικού συστήματος, την οποία χειρίζεται το Τμήμα Προμηθειών και Διοικητικής Μέριμνας, η Διεύθυνση Ψηφιακής Διακυβέρνησης ή άλλη αρμόδια οργανική μονάδα, επιτροπή ή ομάδα της ΕΕΤΤ.*

Σε αντιδιαστολή με τις δύο παραπάνω περιπτώσεις που αναφέρονται σε νέα συστήματα, οι αλλαγές σε υφιστάμενα πληροφοριακά συστήματα της ΕΕΤΤ δεν εμπίπτουν στην παρούσα πολιτική αλλά στην Πολιτική Διαχείρισης Αλλαγών της ΕΕΤΤ.

2. Διαδικασία διαχείρισης αιτημάτων για νέα συστήματα / εφαρμογές και ασφάλεια πληροφοριών

2.1 Διαδικασία διαχείρισης αιτημάτων για νέα συστήματα / εφαρμογές

Η ΕΕΤΤ διαθέτει και χρησιμοποιεί μια τυπική, δομημένη και τεκμηριωμένη διαδικασία διαχείρισης αιτημάτων για νέα πληροφοριακά συστήματα / εφαρμογές. Η διαδικασία αυτή περιλαμβάνει, κυρίως, τα ακόλουθα βήματα:

- *Υποβολή αιτήματος νέου συστήματος / εφαρμογής από στέλεχος της ΕΕΤΤ στη Διεύθυνση Ψηφιακής Διακυβέρνησης. Η υποβολή του αιτήματος αποτελεί το έναυσμα της διαδικασίας.*
- *Έλεγχος του αιτήματος από τον αρμόδιο Προϊστάμενο αναφορικά με την σκοπιμότητα / αναγκαιότητα του προτεινόμενου συστήματος / εφαρμογής σε συνάρτηση με τους επιχειρησιακούς στόχους και τις υπηρεσιακές ανάγκες της ΕΕΤΤ.*
- *Εφόσον το σύστημα / η εφαρμογή κριθεί αναγκαίο/α, το αίτημα ανατίθεται σε αρμόδιο χειριστή.*

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

- *Ο αρμόδιος χειριστής ελέγχει τις λεπτομέρειες του αιτήματος και μεριμνά για τη διενέργεια ανάλυσης κόστους-οφέλους, ειδικά στα σημαντικότερα συστήματα. Ενδεικτικά, λαμβάνονται υπόψη, μεταξύ άλλων, η αύξηση της απόδοσης, η μείωση του λειτουργικού κόστους, η βελτίωση της εικόνας της ΕΕΤΤ, καθώς επίσης, η δυνατότητα υλοποίησης, υποστήριξης και συντήρησης από πλευράς ανθρώπινου δυναμικού και λοιπών πόρων.*
- *Εφόσον η υλοποίηση του συστήματος / εφαρμογής κριθεί σκόπιμο/η από την ανάλυση κόστους-οφέλους, τότε εξετάζεται εάν θα υλοποιηθεί με ίδια μέσα ή θα ανατεθεί σε ανάδοχο.*
- *Στην περίπτωση που αποφασιστεί η ανάπτυξη με ίδια μέσα, τότε:*
    - *Ορίζονται στελέχη / ομάδα έργου, καταρτίζεται χρονοδιάγραμμα με τα παραδοτέα και ακολουθείται κατάλληλη μεθοδολογία ανάπτυξης συστημάτων. Καθορίζεται το σχέδιο επικοινωνίας των εμπλεκομένων μερών και ενημέρωσης της Διοίκησης. Αναλύονται οι απαιτήσεις, εκτιμάται όγκος δεδομένων και πλήθος συναλλαγών, ελέγχονται νέες / βελτιωμένες λύσεις πληροφορικής, εξετάζονται θέματα απορρήτου, ασφάλειας και κανονιστικών απαιτήσεων.*
    - *Σχεδιάζεται μαζί με τον αιτούντα τόσο η ίδια η εφαρμογή όσο και η συνεργασία της με υφιστάμενα συστήματα. Η σχεδίαση εγκρίνεται από τους αρμόδιους Προϊστάμενους και ανάλογα με την περίπτωση από τρίτους, όπως τον Υπεύθυνο Ασφάλειας Πληροφοριών (CISO), τον Υπεύθυνο Προστασίας Δεδομένων (DPO) κτλ.*
    - *Ακολουθούν, κατάλληλα, η υλοποίηση της εφαρμογής, οι δοκιμές και η διασφάλιση ποιότητας, η εκπαίδευση, η μετάπτωση δεδομένων από υφιστάμενα συστήματα στη νέα εφαρμογή και εφόσον κριθεί, η δοκιμαστική / πιλοτική λειτουργία.*
    - *Η νέα εφαρμογή εντάσσεται σε παραγωγική λειτουργία, δρομολογείται η παρακολούθηση και συντήρησή της και έτσι ολοκληρώνεται η διαδικασία.*
- *Στην περίπτωση που αποφασιστεί η ανάθεση σε ανάδοχο, τότε:*
    - *Διαμορφώνονται οι τεχνικές προδιαγραφές σε συνεργασία με τον αιτούντα. Οι τεχνικές προδιαγραφές εγκρίνονται από τους αρμόδιους Προϊστάμενους και ανά περίπτωση από τρίτους, όπως από τον Υπεύθυνο Ασφάλειας Πληροφοριών (CISO), τον Υπεύθυνο Προστασίας Δεδομένων (DPO) κτλ. Σκοπός είναι η προμήθεια αγαθών και υπηρεσιών που ικανοποιούν τις συγκεκριμένες επιχειρησιακές ανάγκες της ΕΕΤΤ και τα πρότυπα ασφαλείας και ιδιωτικότητας και παραλαμβάνονται στη σωστή ποιότητα, ποσότητα, τιμή και στον προγραμματισμένο χρόνο.*
    - *Ακολουθεί η διαδικασία της προμήθειας, που περιλαμβάνει αναζήτηση και επιλογή προμηθευτή, ανάθεση, σύναψη σύμβασης, παρακολούθηση και παραλαβή, σύμφωνα με το σχετικό νομοθετικό πλαίσιο περί δημοσίων συμβάσεων και η διαδικασία ολοκληρώνεται.*

Κύριοι υπεύθυνοι για την παραπάνω διαδικασία είναι η Διεύθυνση Ψηφιακής Διακυβέρνησης και η αρμόδια επιτροπή ή ομάδα, που συνεργάζονται στενά με τον υπηρεσιακό ιδιοκτήτη του συστήματος και τους τελικούς χρήστες ή άλλα εμπλεκόμενα μέρη.

2.2 Ανάλυση απαιτήσεων και καθορισμός προδιαγραφών συστημάτων

Τα πληροφοριακά συστήματα που προμηθεύεται ή αναπτύσσει η ΕΕΤΤ πρέπει να ανταποκρίνονται στις επιχειρησιακές ανάγκες και απαιτήσεις της. Για το σκοπό αυτό, σε κάθε περίπτωση, η ΕΕΤΤ ορίζει με σαφήνεια και λεπτομέρεια τις προδιαγραφές των νέων

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

συστημάτων ως προς τη λειτουργικότητα και τα χαρακτηριστικά τους, τις υπηρεσίες και τις πληροφορίες που θα παρέχουν, την αρχιτεκτονική, τις τεχνολογίες υλοποίησης, τις απαιτήσεις διαλειτουργικότητας και ανταλλαγής δεδομένων με άλλα συστήματα, την παροχή ανοικτών δεδομένων, την ευχρηστία και φιλικότητα προς το χρήστη, την προσβασιμότητα, την επεκτασιμότητα και προσαρμοστικότητα στις μεταβαλλόμενες επιχειρησιακές ανάγκες, την ασφαλή λειτουργία που αναλύεται παρακάτω, κτλ.

Παράλληλα, η ΕΕΤΤ ορίζει την επιθυμητή οργάνωση του έργου της εγκατάστασης / υλοποίησης κάθε νέου συστήματος, το χρονοδιάγραμμα, τις φάσεις, τα παραδοτέα και τα ορόσημα, καθώς και τις απαιτούμενες υπηρεσίες υποστήριξης, εγγύησης, συντήρησης κτλ.

2.3 Ανάλυση ή αξιολόγηση κινδύνων

Τα πληροφοριακά συστήματα πρέπει να προστατεύονται από πρόσβαση ή τροποποίηση χωρίς εξουσιοδότηση, απώλεια της διαθεσιμότητάς τους ή απώλεια δεδομένων και άλλες απειλές, με τη χρήση κατάλληλων τεχνικών και οργανωτικών μέτρων ασφαλείας. Τέτοια μέτρα μπορεί ενδεικτικά να περιλαμβάνουν τον καθορισμό των ρυθμίσεων ασφάλειας (παραμέτρων) του συστήματος, τη διαμόρφωση της δομής των απαραίτητων αρχείων καταγραφής (audit trails και logs) κτλ.

Πριν την προμήθεια ή ανάπτυξη του πληροφοριακού συστήματος και συγκεκριμένα πριν την οριστικοποίηση των προδιαγραφών ασφαλούς λειτουργίας του διενεργείται ανάλυση κινδύνων. Μέσω της ανάλυσης κινδύνων εντοπίζονται οι κίνδυνοι που δυνητικά αντιμετωπίζει το σύστημα, η πιθανότητα εμφάνισής τους και οι συνέπειές τους και εκτιμώνται οι απαιτήσεις ασφαλούς λειτουργίας του. Έτσι προσδιορίζονται τα μέτρα ασφάλειας που πρέπει να εφαρμόζονται για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητάς του, σύμφωνα με όσα προβλέπει η Πολιτική Ασφαλείας της ΕΕΤΤ.

2.4 Απαιτήσεις και προδιαγραφές ως προς την ασφάλεια

Η ΕΕΤΤ ενσωματώνει απαιτήσεις και προδιαγραφές ασφάλειας πληροφοριών κατά την προκήρυξη, αξιολόγηση και προμήθεια συστημάτων, την ανάπτυξη με ίδια μέσα, την ανάθεση της ανάπτυξης σε τρίτους ή τις αναθεωρήσεις / αναβαθμίσεις των πληροφοριακών συστημάτων της. Οι συγκεκριμένες απαιτήσεις ασφάλειας διαφέρουν ανά σύστημα, διότι εξαρτώνται και επηρεάζονται από τα ειδικότερα χαρακτηριστικά του κάθε συστήματος, τους συγκεκριμένους επιχειρησιακούς στόχους του, τους τύπους δεδομένων που επεξεργάζεται (π.χ. προσωπικά δεδομένα), το επίπεδο ταξινόμησής του (κρίσιμο ή ευαίσθητο ή μη κρίσιμο σύμφωνα με τα οριζόμενα στην Πολιτική Διαχείρισης Πληροφοριακών Πόρων), τα αποτελέσματα της ανάλυσης κινδύνων όπως αναφέρθηκε παραπάνω, καθώς και το περιβάλλον στο οποίο το σύστημα θα εγκατασταθεί (π.χ. παραγωγής, ανάπτυξης, δοκιμών).

Επομένως, ανάλογα με τους παραπάνω παράγοντες, ένα νέο σύστημα ενδέχεται να προβλέπει προδιαγραφές για μηχανισμούς ελέγχου της πρόσβασης, τεχνικές κρυπτογράφησης ή άλλες μεθόδους προστασίας των δεδομένων, προστασία των συστημάτων μέσω λειτουργιών ελέγχου και καταγραφής (auditing και logging functions), κτλ. Για παράδειγμα, στο σχεδιασμό εφαρμογών που αποθηκεύουν ή μεταδίδουν εμπιστευτικές πληροφορίες, πρέπει να προβλέπονται αυξημένα μέτρα ασφάλειας για τον περιορισμό της πρόσβασης. Στόχος σε κάθε περίπτωση είναι η ασφάλεια των πληροφοριακών συστημάτων σε επίπεδο ανάλογο με την κρισιμότητά τους και η προστασία έναντι των αυξανόμενων κινδύνων από κυβερνοεπιθέσεις (Cyberesiliency).

Τονίζεται ότι η ασφάλεια των πληροφοριών λαμβάνεται υπόψη καθ' όλη τη διάρκεια του κύκλου ζωής ενός πληροφοριακού συστήματος, είτε αυτό αναπτύσσεται είτε προμηθεύεται, δηλαδή κατά την εκκίνηση του έργου ανάπτυξής του, την ανάλυση απαιτήσεων, το σχεδιασμό του συστήματος και την ανάπτυξη του λογισμικού ή αντίστοιχα, τον καθορισμό των τεχνικών προδιαγραφών, την επιλογή και αξιολόγηση των τρίτων μερών, την προμήθεια, καθώς επίσης, στις φάσεις της δοκιμής, της εγκατάστασης και της συντήρησης.

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

2.5 Απαιτήσεις επιχειρησιακής συνέχειας

Στα κρίσιμα ή ευαίσθητα συστήματα πληροφοριών πρέπει να λαμβάνονται υπόψη και να εφαρμόζονται οι απαιτήσεις επιχειρησιακής συνέχειας (business continuity), δηλαδή οι δυνατότητες συνέχισης της λειτουργίας κατά την διάρκεια και μετά από μια καταστροφή και η δυνατότητα ανάκαμψης το συντομότερο δυνατόν.

3. Νομικά ζητήματα και συμφωνίες με τρίτα μέρη

3.1 Συμμόρφωση με το νομοθετικό και κανονιστικό πλαίσιο

Η προμήθεια ή η ανάπτυξη ενός πληροφοριακού συστήματος στην ΕΕΤΤ συμμορφώνεται στις υφιστάμενες νομοθετικές και κανονιστικές απαιτήσεις. Κατ' επέκταση, η αρχή "προστασίας των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού" ("privacy by design and by default"), όπως ορίζεται στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR), πρέπει να εφαρμόζεται σε όλα τα νέα συστήματα που σχεδιάζονται από ή/και για την ΕΕΤΤ. Επομένως, πρέπει να εφαρμόζονται μέτρα, στα αρχικά στάδια του σχεδιασμού των συστημάτων, που διασφαλίζουν τις αρχές ιδιωτικού απορρήτου και συμμόρφωσης με τον GDPR ήδη από την αρχή («προστασία δεδομένων ήδη από τον σχεδιασμό»). Επίσης, εξ ορισμού τα συστήματα θα επεξεργάζονται τα προσωπικά δεδομένα με το υψηλότερο επίπεδο προστασίας της ιδιωτικής ζωής, χωρίς να απαιτείται κάποια επιπλέον ρύθμιση / διαμόρφωσή τους («προστασία δεδομένων εξ ορισμού»). Για παράδειγμα, το κάθε σύστημα πρέπει να συλλέγει και να επεξεργάζεται μόνο τα απολύτως απαραίτητα προσωπικά δεδομένα για τους σκοπούς που εξυπηρετεί («ελαχιστοποίηση των δεδομένων»). Πρέπει να τηρεί ακριβή δεδομένα και να παρέχει τη δυνατότητα επικαιροποίησης και διόρθωσής τους, όταν χρειάζεται. Πρέπει να περιορίζει τη χρονική περίοδο αποθήκευσης στην ελάχιστη που απαιτείται για την επίτευξη των σκοπών του. Παράλληλα, θα λαμβάνει τα κατάλληλα μέτρα ώστε να προστατεύεται από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, κτλ.

Περαιτέρω, σύμφωνα με το νομοθετικό και κανονιστικό πλαίσιο περί προσωπικών δεδομένων, τα πληροφοριακά συστήματα της ΕΕΤΤ πρέπει να περιλαμβάνουν κατάλληλους μηχανισμούς ενημέρωσης των χρηστών και λήψης της συγκατάθεσής τους ή αντιθέτως άρσης της για την επεξεργασία των προσωπικών δεδομένων τους, να διευκολύνουν την ικανοποίηση των δικαιωμάτων των υποκειμένων (πρόσβαση, διόρθωση, διαγραφή, φορητότητα, περιορισμό της επεξεργασίας, εναντίωση), να παρέχουν εύχρηστη εκκαθάριση των δεδομένων μετά τη λήξη της περιόδου διατήρησης, να υποστηρίζουν τη λογοδοσία τεκμηριώνοντας τη συμμόρφωσή τους με το νομοθετικό και κανονιστικό πλαίσιο περί προστασίας προσωπικών δεδομένων.

Πριν την ένταξη των συστημάτων σε παραγωγική λειτουργία, πρέπει να εκπονείται η μελέτη ταξινόμησης των δεδομένων (data classification), σύμφωνα με τα οριζόμενα στην Πολιτική Διαχείρισης Πληροφοριακών Πόρων. Η μελέτη εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων (ΕΑΠΔ ή αλλιώς DPIA) πρέπει να εκπονείται στις περιπτώσεις που απαιτείται σύμφωνα με τον GDPR.

Στις online εφαρμογές πρέπει να συντάσσονται και να αναρτώνται, σύμφωνα με τις απαιτήσεις της σχετικής νομοθεσίας, η δήλωση προστασίας προσωπικών δεδομένων που αποτελεί την πολιτική εμπιστευτικότητας των προσωπικών δεδομένων που εφαρμόζει η ΕΕΤΤ, η δήλωση προσβασιμότητας, οι ρυθμίσεις και η πολιτική cookies κτλ.

Κατά τα οριζόμενα στο νομοθετικό και κανονιστικό πλαίσιο περί κυβερνοασφάλειας, η ΕΕΤΤ πρέπει περιοδικά να εκπονεί ανάλυση κινδύνων των πληροφοριακών συστημάτων και δικτύων της και να αντιμετωπίζει αποτελεσματικά τους κινδύνους λαμβάνοντας τα κατάλληλα μέτρα ασφάλειας που θα είναι ανάλογα προς τους κινδύνους αυτούς. Η Διοίκηση θα πρέπει να είναι ιδιαιτέρως ευαισθητοποιημένη στα θέματα της ασφάλειας, να εγκρίνει και να παρακολουθεί την ανάλυση και διαχείριση κινδύνων. Το ανθρώπινο δυναμικό θα πρέπει να εκπαιδεύεται σε διαρκή βάση στις πολιτικές και διαδικασίες ασφαλείας που διαθέτει και εφαρμόζει η ΕΕΤΤ. Σύμφωνα με αυτές, η ΕΕΤΤ ταξινομεί τους πληροφοριακούς πόρους της

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

ανάλογα με την κρισιμότητα και ευαισθησία τους. Διαχειρίζεται και ελέγχει τακτικά την πρόσβαση στα δεδομένα και τα δικαιώματα των χρηστών και επιβεβαιώνει ότι μόνο εξουσιοδοτημένο προσωπικό έχει πρόσβαση στην ευαίσθητη πληροφορία. Για το σκοπό αυτό, διαχειρίζεται κατάλληλα τα τρίτα μέρη με τα οποία συνεργάζεται και εκπαιδεύει το προσωπικό της. Χρησιμοποιεί τεχνικές προστασίας των δεδομένων, όπως κρυπτογράφηση, όπου απαιτείται. Διατηρεί ενημερωμένα και ασφαλή αντίγραφα ασφαλείας κρίσιμων δεδομένων και συστημάτων, για να μπορεί να τα ανακτήσει και να αποκαταστήσει τη λειτουργία της εφόσον απαιτηθεί. Διαθέτει διαδικασία και πολιτική διαχείρισης συμβάντων ασφαλείας, συμπεριλαμβανομένης της ενημέρωσης των αρμόδιων φορέων σε περίπτωση περιστατικού. Διατηρεί αρχεία των δραστηριοτήτων και των μέτρων ασφαλείας, για να μπορεί να τεκμηριώσει τη συμμόρφωση της με το νομοθετικό και κανονιστικό πλαίσιο σε αναφορές της ή τυχόν ελέγχους.

Οι πολιτικές και τα μέτρα ασφαλείας της ΕΕΤΤ θα πρέπει, περιοδικά, να ανασκοπούνται, να δοκιμάζονται, να αξιολογούνται ως προς την αποτελεσματικότητά τους και να αναθεωρούνται εφόσον απαιτείται.

3.2 Συμφωνίες με τρίτα μέρη

Στην περίπτωση επιλογής τρίτων μερών, όπως προμηθευτών, αναδόχων, συμβούλων, κλπ., η επιλογή αυτή συμμορφώνεται με τη νομοθεσία περί δημοσίων συμβάσεων.

Από τεχνικής άποψης, κατά την επιλογή, θα πρέπει να αξιολογούνται η αξιοπιστία των συστημάτων, η καταλληλότητα και ωριμότητα των τεχνολογιών, οι παρεχόμενες υπηρεσίες (υποστήριξης, εκπαίδευσης, τεκμηρίωσης, εγγύησης, συντήρησης κτλ.), η πολιτική ασφάλειας και το σχέδιο συνέχειας εργασιών και ανάκαμψης από καταστροφή των υποψηφίων.

Οι προκηρύξεις των διαγωνισμών και οι συναπτόμενες συμβάσεις πρέπει να ενσωματώνουν τις απαιτήσεις της ΕΕΤΤ τόσο στη λήψη των συμφωνηθέντων αγαθών / υπηρεσιών όσο και στη διασφάλιση των πληροφοριών και της ιδιωτικότητας. Πιο συγκεκριμένα, σύμφωνα με τις πολιτικές της ΕΕΤΤ, οι προκηρύξεις και οι συμβάσεις για την προμήθεια ή ανάπτυξη συστημάτων πρέπει, μεταξύ άλλων, να περιγράφουν αναλυτικά και με σαφήνεια:

- *τη συμμόρφωση των συστημάτων με τα ισχύοντα πρότυπα ασφάλειας και ιδιωτικότητας και με τις απαιτήσεις του νομοθετικού και κανονιστικού πλαισίου που αναφέρθηκαν παραπάνω*
- *τη συμμόρφωση με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, ιδίως με το άρθρο 28 «Εκτελών την επεξεργασία», ειδικά στην περίπτωση που το τρίτο μέρος λειτουργεί ως εκτελών επεξεργασία προσωπικών δεδομένων για λογαριασμό της ΕΕΤΤ*
- *τη συμμόρφωση του τρίτου μέρους με τις πολιτικές ασφαλείας της ΕΕΤΤ, π.χ. αναφορικά με την εξουσιοδοτημένη πρόσβαση, την ασφάλεια τελικού χρήστη, την προστασία προσωπικών δεδομένων, την αποδεκτή χρήση των πληροφοριακών αγαθών, τη διαχείριση συμβάντων ασφαλείας κτλ.*
- *τα θέματα που αφορούν τη μεθοδολογία (π.χ. μεθοδολογία ανάπτυξης πληροφοριακού συστήματος) και τις υπηρεσίες που θα παρέχουν τα τρίτα μέρη κατά την υλοποίηση του έργου, ιδίως αναφορικά με τυχόν ιδιαίτερες απαιτήσεις που ενδεχομένως έχει η ΕΕΤΤ για ένα κρίσιμο ή ευαίσθητο σύστημα, όπως να εκτελεστεί δοκιμή διείσδυσης (penetration testing), δηλαδή προσομοίωση επίθεσης και εισβολής στο σύστημα, με σκοπό την επιβεβαίωση της ασφάλειάς του πριν την οριστική παραλαβή*
- *την ασφάλεια των διασυνδέσεων μεταξύ της ΕΕΤΤ και του τρίτου μέρους*
- *τα οργανωτικά και τεχνικά μέτρα ασφάλειας που λαμβάνει το τρίτο μέρος και τις πιστοποιήσεις στην ασφάλεια πληροφοριών που κατέχει*
- *το σχέδιο συνέχισης εργασιών και ανάκαμψης από καταστροφή του τρίτου μέρους*

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

- *το συμφωνηθέν επίπεδο παροχής υπηρεσιών (Service Level Agreement - SLA)*
- *τα δικαιώματα ιδιοκτησίας και πνευματικών δικαιωμάτων και τα θέματα αδειοδότησης (βλ. επίσης παρακάτω)*
- *την συνεχή επιβεβαίωση από μέρους του τρίτου μέρους της επάρκειας και ακεραιότητας του προσωπικού του*
- *τη δυνατότητα και τους όρους ανάθεσης υπηρεσιών / υποχρεώσεων από το τρίτο μέρος σε υπεργολάβους και τις απαιτήσεις ασφάλειας πληροφοριών στις οποίες αυτοί υπάγονται*
- *τη διασφάλιση της εμπιστευτικότητας από το προσωπικό και τους υπεργολάβους του τρίτου μέρους*
- *την διαδικασία άμεσης αναφοράς στην ΕΕΤΤ των αδυναμιών ασφαλείας και των συμβάντων ασφαλείας που πιθανόν να εντοπίσει το τρίτο μέρος*
- *τις διαδικασίες διαχείρισης αλλαγών του συστήματος τις οποίες υιοθετούν τα δύο μέρη*
- *το σχέδιο επικοινωνίας των δύο μερών (είδος, συχνότητα αναφορών / αρχείων κτλ.)*
- *τις διαδικασίες ολοκλήρωσης ή λύσης της σύμβασης (για παράδειγμα βλ. παρακάτω συμφωνίες μεσεγγύησης πηγαίου κώδικα)*
- *τα θέματα επιστροφής υλικού, λογισμικού, πληροφοριών και δεδομένων που ανήκουν στην ΕΕΤΤ μετά την ολοκλήρωση ή λύση της σύμβασης, καθώς και διαγραφής τυχόν αντιγράφων*
- *τη δυνατότητα διενέργειας ελέγχων του αναδόχου από την ΕΕΤΤ ή από τρίτους για λογαριασμό της ΕΕΤΤ και την παροχή των απαραίτητων πληροφοριών από τον ανάδοχο προς διευκόλυνση αυτών των ελέγχων*
- *τη συνδρομή του τρίτου μέρους προς την ΕΕΤΤ στην διασφάλιση της συμμόρφωσης προς τις υποχρεώσεις που απορρέουν από το νομοθετικό και κανονιστικό πλαίσιο περί προσωπικών δεδομένων και κυβερνοασφάλειας, λαμβάνοντας υπόψη τις πληροφορίες που το τρίτο μέρος διαθέτει στο πλαίσιο εκτέλεσης των συμβατικών του υποχρεώσεων*
- *τις κυρώσεις για τη μη συμμόρφωση του τρίτου μέρους με το πλαίσιο ασφάλειας πληροφοριών της ΕΕΤΤ και γενικότερα*
- *τις κυρώσεις για τις περιπτώσεις παραβίασης των συμφωνηθέντων.*

Κατά τη διάρκεια της σύμβασης, η συνεργασία της ΕΕΤΤ με το τρίτο μέρος διέπεται από τις σχετικές πολιτικές διαχείρισης τρίτων μερών της ΕΕΤΤ.

3.3 Άδειες χρήσης και εργαλεία λογισμικού

Το λογισμικό, τα εργαλεία ανάπτυξης εφαρμογών, καθώς και η αντίστοιχη τεκμηρίωση πρέπει να χρησιμοποιούνται σύμφωνα με τις σχετικές συμβάσεις και τη νομοθεσία περί πνευματικής ιδιοκτησίας.

3.4 Συμφωνίες μεσεγγύησης πηγαίου κώδικα

Η ΕΕΤΤ πρέπει να εξετάζει το ενδεχόμενο σύναψης συμφωνιών μεσεγγύησης λογισμικού (software escrow) με τους εξωτερικούς συνεργάτες που της παρέχουν λύσεις λογισμικού.

Στη συμφωνία πρέπει να ορίζονται οι ενέργειες που πρέπει να υλοποιηθούν για την απελευθέρωση του πηγαίου κώδικα λογισμικού σε περιπτώσεις, στις οποίες ο αρχικός κάτοχος των πνευματικών δικαιωμάτων δεν είναι σε θέση να συντηρήσει και να αναβαθμίσει το λογισμικό, όπως έχει δεσμευτεί στη συμφωνία παραχώρησης άδειας χρήσης λογισμικού. Σε τέτοιου είδους περιπτώσεις, ο πηγαίος κώδικας του λογισμικού πρέπει να φυλάσσεται σε λογαριασμό ανεξάρτητου μεσεγγυητή, ο οποίος φροντίζει για τη συντήρηση του λογισμικού.

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

Με τον τρόπο αυτό, προστατεύεται η επένδυση της ΕΕΤΤ σε επιχειρησιακά κρίσιμες εφαρμογές λογισμικού.

4. Αρμοδιότητες ανάπτυξης και συντήρησης

4.1 Διαχωρισμός στα περιβάλλοντα

Τα περιβάλλοντα λειτουργίας των πληροφοριακών συστημάτων διαχωρίζονται κατ' ελάχιστον σε περιβάλλοντα ανάπτυξης / δοκιμής και σε περιβάλλοντα παραγωγής. Η ανάπτυξη και η δοκιμή συστημάτων και εφαρμογών δεν πρέπει να διεξάγεται στο περιβάλλον παραγωγής.

4.2 Διαχωρισμός καθηκόντων

Όπου είναι εφικτό, υπάρχει διαχωρισμός των καθηκόντων και των δικαιωμάτων πρόσβασης μεταξύ του προσωπικού που ασχολείται στα περιβάλλοντα ανάπτυξης / δοκιμών και εκείνου που εργάζεται στο περιβάλλον παραγωγής. Εκτός εάν υπάρχει συγκεκριμένος λόγος, ένας προγραμματιστής ή μηχανικός λογισμικού δεν πρέπει να έχει δικαιώματα διαχειριστή ή δικαιώματα τροποποίησης στο περιβάλλον παραγωγής.

Σε περίπτωση που κάποιος υπάλληλος της ΕΕΤΤ ή εξωτερικός συνεργάτης απαιτήσει πρόσβαση σε κάποιο σύστημα για οποιοδήποτε λόγο (π.χ. κάποιος εξωτερικός συνεργάτης για την αντιμετώπιση ενός προβλήματος), ακολουθείται η τυπική διαδικασία διαχείρισης πρόσβασης χρηστών.

4.3 Αρχή των ελάχιστων προνομίων

Η αρχή των ελάχιστων προνομίων εφαρμόζεται σε όλους τους μηχανικούς λογισμικού και προγραμματιστές, ώστε ο καθένας από αυτούς να διατηρεί τα ελάχιστα προνόμια πρόσβασης στον πηγαίο κώδικα των συστημάτων και εφαρμογών, προκειμένου να ελαχιστοποιούνται οι πιθανές αρνητικές συνέπειες από κάποια ενέργειά του.

4.4 Διαχείριση αλλαγών

Η διαχείριση αλλαγών και ρυθμίσεων στον πηγαίο κώδικα συμμορφώνεται με την Πολιτική Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα της ΕΕΤΤ.

5. Ανάπτυξη και διαχείριση πηγαίου κώδικα πληροφοριακών συστημάτων / εφαρμογών

4.1 Αξιοποίηση μεθοδολογιών ανάπτυξης πληροφοριακών συστημάτων

Οι εφαρμογές που αναπτύσσονται εσωτερικά στην ΕΕΤΤ ή αναπτύσσονται από αναδόχους ακολουθούν έναν τυποποιημένο κύκλο ζωής εφαρμογών. Οι μεθοδολογίες ανάπτυξης πληροφοριακών συστημάτων περιλαμβάνουν την ανάλυση απαιτήσεων και τον καθορισμό προδιαγραφών, την τεχνική ανάλυση και το σχεδιασμό του συστήματος, την υλοποίηση, τις δοκιμές του, την αποδοχή του, την εκπαίδευση, τη μεταφορά στην παραγωγή και τη λειτουργία του. Η μετάβαση από τη μία φάση στην άλλη προϋποθέτει την ανασκόπηση και έγκριση των αποτελεσμάτων της προηγούμενης.

Στις σύγχρονες ευέλικτες μεθοδολογίες ανάπτυξης πληροφοριακών συστημάτων, που χρησιμοποιεί η ΕΕΤΤ, οι απαιτήσεις και οι λύσεις εξελίσσονται μέσω της συνεργασίας των στελεχών των οργανικών μονάδων που έχουν την επιχειρησιακή ιδιοκτησία του συστήματος και θα είναι οι τελικοί χρήστες του και της Διεύθυνσης Ψηφιακής Διακυβέρνησης. Τα πρώτα στελέχη εισφέρουν την τεχνογνωσία και την εμπειρία που έχουν αποκομίσει ασκώντας την αρμοδιότητα την οποία θα υποστηρίξει το νέο σύστημα, ενώ τα δεύτερα μετουσιώνουν τις λειτουργικές και τεχνικές απαιτήσεις σε πληροφοριακό σύστημα. Η συνεργασία μεταξύ τους πρέπει να είναι πολύ στενή και διαρκής. Προωθείται ο γρήγορος και σταδιακός σχεδιασμός, η

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

ταχεία ανάπτυξη, η έγκαιρη παράδοση του συστήματος στους χρήστες με στόχο την ανάδρασή τους, η ταχεία και ευέλικτη ανταπόκριση στις διορθώσεις και βελτιώσεις.

4.2 Ανάπτυξη ασφαλούς κώδικα

Προκειμένου να αποφευχθούν προβλήματα ασφάλειας από ευπάθειες του πηγαίου κώδικα, κατά την ανάπτυξη λογισμικού πρέπει να εφαρμόζονται πρότυπα ασφαλούς ανάπτυξης λογισμικού. Αυτό αφορά τόσο την εσωτερική ανάπτυξη με ίδια μέσα όσο και την ανάπτυξη που ανατίθεται σε αναδόχους.

Ειδικότερα, όταν πρόκειται για διαβίβαση, αποθήκευση και/ή επεξεργασία προσωπικών, εμπιστευτικών ή κρίσιμων για την ΕΕΤΤ δεδομένων, πρέπει να ακολουθούνται βέλτιστες πρακτικές (οδηγίες για ασφαλή κωδικοποίηση) και η ασφάλεια να λαμβάνεται πάντοτε υπόψη κατά τις φάσεις της ανάλυσης, του σχεδιασμού και δοκιμής των εφαρμογών.

Γενικότερα, η χρήση προτύπων, εργαλείων και μεθοδολογιών κατά την ανάπτυξη αποβλέπει επιπλέον στην κατά το δυνατόν ομοιογένεια των πληροφοριακών συστημάτων που αναπτύσσονται, η οποία αποτελεί ζητούμενο καθώς διευκολύνει την υποστήριξή τους.

Το προσωπικό της ΕΕΤΤ που αναπτύσσει κώδικα λογισμικού λαμβάνει επαρκή εκπαίδευση στην ανάπτυξη ασφαλούς κώδικα για το συγκεκριμένο περιβάλλον ανάπτυξης της ΕΕΤΤ.

4.3 Χρήση εργαλείων ανάπτυξης σε περιβάλλοντα παραγωγής

Η χρήση εργαλείων ανάπτυξης λογισμικού σε περιβάλλοντα παραγωγής απαγορεύεται.

4.4 Προστασία πηγαίου κώδικα

Η πρόσβαση στον πηγαίο κώδικα των εφαρμογών δίνεται μετά από εξουσιοδότηση, σύμφωνα με τις σχετικές πολιτικές και αρχές ασφαλείας.

4.5 Πηγαίος κώδικας σε παραγωγικό περιβάλλον

Ο πηγαίος κώδικας δεν αποθηκεύεται στο παραγωγικό περιβάλλον.

Ο πηγαίος κώδικας των υπό ανάπτυξη εφαρμογών αποθηκεύεται ξεχωριστά από τον πηγαίο κώδικα των εφαρμογών που λειτουργούν σε περιβάλλον παραγωγής.

4.6 Προστασία από κακόβουλο κώδικα

Πρέπει να διενεργούνται κατάλληλοι έλεγχοι κατά τις φάσεις ανάπτυξης και συντήρησης της εφαρμογής προκειμένου να εντοπιστεί κακόβουλος κώδικας (π.χ. μέσω εργαλείων source code review).

4.7 Εκδόσεις πηγαίου κώδικα

Πρέπει να χρησιμοποιούνται κατάλληλοι μηχανισμοί ελέγχου των εκδόσεων του πηγαίου κώδικα των εφαρμογών (version control).

4.8 Επικύρωση κώδικα

Οι μέθοδοι επικύρωσης του κώδικα πρέπει να χρησιμοποιούνται κατά τη διάρκεια του κύκλου ζωής ενός συστήματος, προκειμένου να διασφαλίζεται ότι ο ανεπτυγμένος κώδικας διαθέτει όλα τα χαρακτηριστικά ασφαλείας αλλά και τη λειτουργικότητα που καθορίζεται από τις προδιαγραφές του λογισμικού.

4.9 Χρήση maintenance hooks / backdoors

Απαγορεύεται η ενσωμάτωση/χρήση backdoors (maintenance hooks) στο λογισμικό από τους προγραμματιστές ή τις ομάδες υποστήριξης, ως μέθοδος που επιτρέπει την άμεση πρόσβαση και διευκόλυνσή τους για την εκτέλεση εργασιών συντήρησης ή διαχείρισης, διότι μπορούν να αναχθούν σε κίνδυνο ασφαλείας εάν ανακαλυφθούν από κακόβουλους εισβολείς που θα τα

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

εκμεταλλευτούν για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στο λογισμικό ή στα συστήματα. Γενικότερα, απαγορεύεται κάθε παράκαμψη των μηχανισμών ασφάλειας.

6. Έλεγχος, προστασία και κάλυψη δεδομένων (data masking)

4.1 Έλεγχος επικύρωσης εισόδου, εξόδου και αποτελεσμάτων επεξεργασίας

Κάθε εφαρμογή πρέπει να διαθέτει μηχανισμούς για τον έλεγχο της εγκυρότητας και της ακεραιότητας των εισαγόμενων δεδομένων, όπου αυτό είναι εφικτό.

Τα αποτελέσματα της επεξεργασίας των δεδομένων από τα πληροφοριακά συστήματα πρέπει να ελέγχονται ώστε να επαληθεύεται η ακρίβειά τους, όπου αυτό είναι εφικτό.

Τα αποτελέσματα των επεξεργαζόμενων δεδομένων πρέπει να ελέγχονται ώστε να επαληθεύεται η ακρίβεια τους, όπου αυτό είναι εφικτό, με βάση τις υπηρεσιακές ανάγκες και απαιτήσεις της ΕΕΤΤ.

4.2 Απαιτήσεις κάλυψης δεδομένων

Προκειμένου να αποφευχθεί η πιθανή διαρροή δεδομένων, πρέπει να εφαρμόζεται κάλυψη (masking) ή ανωνυμοποίηση των δεδομένων, κατά το δυνατόν, όταν δεδομένα του περιβάλλοντος παραγωγής αντιγράφονται σε περιβάλλον ανάπτυξης / δοκιμών.

Οι τεχνικές κάλυψης δεδομένων πρέπει να διασφαλίζουν ότι τα πρωτότυπα δεδομένα καλύπτονται πάντα όταν μεταφέρονται μεταξύ διαφορετικών πληροφοριακών συστημάτων και ότι δεν μπορούν να εξαχθούν από την καλυμμένη (masked) τιμή.

7. Δοκιμές και αποδοχή πληροφοριακών συστημάτων / εφαρμογών

4.1 Δοκιμές ασφαλείας

Το λογισμικό που αναπτύσσει ή προμηθεύεται η ΕΕΤΤ, καθώς και οι ενημερώσεις ή αναθεωρήσεις του, ελέγχεται πλήρως στο περιβάλλον δοκιμών και γίνεται αποδεκτό πριν από την εγκατάσταση στο περιβάλλον παραγωγής.

Θα πρέπει να γίνονται εκτεταμένες, τεκμηριωμένες και ολοκληρωμένες δοκιμές. Οι δοκιμές ασφαλείας ελέγχουν ότι το σύστημα περιλαμβάνει τις δικλείδες ασφαλείας που προδιαγράφηκαν κατά τον σχεδιασμό του. Οι δοκιμές αντοχής διενεργούνται σε συνθήκες επεξεργασίας αυξημένου όγκου δεδομένων και προσομοιώνουν ακραίες καταστάσεις. Οι δοκιμές διαλειτουργικότητας επιβεβαιώνουν τη διαλειτουργικότητα του συστήματος με άλλα συστήματα. Απαραίτητες είναι και οι δοκιμές για τον έλεγχο της δυνατότητας επαναφοράς του συστήματος σε περιπτώσεις βλάβης του λογισμικού ή του εξοπλισμού, κτλ.

Στις εμπορικές λύσεις / έτοιμα πακέτα λογισμικού τα οποία έχουν αναπτυχθεί εξωτερικά και τα οποία προμηθεύεται η ΕΕΤΤ, συνιστάται οι τυχόν προσαρμογές (customizations) που υλοποιούνται ειδικά για την ΕΕΤΤ, να περιορίζονται μόνο στις αναγκαίες, όσο αυτό είναι δυνατόν, προκειμένου να μην αλλοιώνεται η φυσιογνωμία των συστημάτων και να είναι εύκολη η αναβάθμιση και συντήρησή τους. Όλες αυτές οι προσαρμογές και τροποποιήσεις ελέγχονται μεθοδικά και αυστηρά πριν από την ένταξή τους σε παραγωγική λειτουργία.

Σε όλες τις περιπτώσεις, ο έλεγχος / η δοκιμή ασφαλείας που θα διενεργηθεί πριν από την εγκατάσταση του πληροφοριακού συστήματος, ενδείκνυται, ανάλογα και με την ταξινόμηση (κρισιμότητα / ευαισθησία) του συστήματος, να ανατίθεται σε μία ανεξάρτητη οντότητα (ανεξάρτητη ως προς την οντότητα υλοποίησης του συστήματος), προερχόμενη είτε από στελέχη της ΕΕΤΤ είτε ακόμη και από εξωτερικούς συνεργάτες.

Μεταξύ των άλλων δοκιμών ασφαλείας, στα κρίσιμα ή ευαίσθητα συστήματα θα πρέπει να εξετάζεται η υλοποίηση penetration testing από εξειδικευμένες εταιρείες για την επιβεβαίωση της ασφάλειας του συστήματος στις ενδεχόμενες επιθέσεις κακόβουλων εισβολέων.

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

4.2 Διατήρηση των αποτελεσμάτων των δοκιμών

Τα αποτελέσματα των δοκιμών διατηρούνται σύμφωνα με τις σχετικές πολιτικές.

4.3 Προστασία δεδομένων δοκιμών

Τα δεδομένα που χρησιμοποιούνται για τις δοκιμές των εφαρμογών προστατεύονται σύμφωνα με το επίπεδο ταξινόμησής τους.

4.4 Καθορισμός κριτηρίων αποδοχής

Για την αποδοχή των πληροφοριακών συστημάτων διενεργούνται ολοκληρωμένες δοκιμές με όσο το δυνατόν πιο πιστή προσομοίωση των συνθηκών της παραγωγικής λειτουργίας.

Τα κριτήρια αποδοχής των συστημάτων παρέχονται από τον υπηρεσιακό ιδιοκτήτη του συστήματος και εγκρίνονται από τον Υπεύθυνο Ασφάλειας Πληροφοριών (CISO). Περιλαμβάνουν λειτουργικές και τεχνικές απαιτήσεις της εφαρμογής, απαιτήσεις απόδοσης και χωρητικότητας, ταξινόμηση δεδομένων, προδιαγραφές υλικού εάν υπάρχουν, κτλ.

4.5 Αποδοχή πληροφοριακών συστημάτων

Οι δοκιμές αποδοχής (acceptance tests) εκτελούνται με τρόπο ώστε να εξασφαλίζεται ότι τα πληροφοριακά συστήματα πληρούν τα καθορισμένα κριτήρια αποδοχής. Όλα τα κριτήρια αυτά πρέπει να πληρούνται πριν το οποιοδήποτε σύστημα ή εφαρμογή εγκατασταθεί σε περιβάλλον παραγωγής.

Στην περίπτωση που το νέο σύστημα αντικαθιστά παλαιότερο, συνιστάται να εξετάζεται η περίπτωση τα δύο συστήματα για ένα χρονικό διάστημα να λειτουργήσουν παράλληλα με τα ίδια δεδομένα και να αντιπαραβάλλονται τα αποτελέσματά τους.

8. Εκπαίδευση διαχειριστών και χειριστών

Οι διαχειριστές και οι χειριστές των πληροφοριακών συστημάτων πρέπει να είναι κατάλληλα εκπαιδευμένοι, ώστε να είναι σε θέση να διαχειριστούν / χρησιμοποιήσουν τα αντίστοιχα πληροφοριακά συστήματα και να αξιοποιήσουν πλήρως τις δυνατότητές τους.

9. Τεκμηρίωση πληροφοριακών συστημάτων/εφαρμογών

Κάθε πληροφοριακό σύστημα που αποκτάται από τρίτο μέρος ή αναπτύσσεται εσωτερικά στην ΕΕΤΤ, πρέπει να συνοδεύεται από πλήρη και ενημερωμένα εγχειρίδια (τεχνικά εγχειρίδια, εγχειρίδια διαχείρισης, χρήσης, λειτουργίας κτλ). Τα εγχειρίδια της τεκμηρίωσης θα πρέπει να έχουν ενιαία μορφή και δομή, όσο αυτό είναι δυνατόν. Οι ιδιοκτήτες των πληροφοριακών συστημάτων είναι υπεύθυνοι για την ανάπτυξη και τήρηση ολοκληρωμένων εγχειριδίων.

Τα εγχειρίδια των πληροφοριακών συστημάτων ταξινομούνται τουλάχιστον στο ίδιο επίπεδο ταξινόμησης με τα συστήματα στα οποία αναφέρονται. Οι ιδιοκτήτες των πληροφοριακών συστημάτων είναι υπεύθυνοι για τον προσδιορισμό του επιπέδου ταξινόμησης, σύμφωνα με την Πολιτική Διαχείρισης Πληροφοριακών Πόρων της ΕΕΤΤ.

10. Εγκατάσταση πληροφοριακών συστημάτων / εφαρμογών

4.1 Έγκριση για μετάβαση στο περιβάλλον παραγωγής

Για να πραγματοποιηθεί η μετάβαση ενός πληροφοριακού συστήματος ή μιας εφαρμογής στο περιβάλλον παραγωγής, πρέπει να υπάρχει σχετική εισήγηση από την αρμόδια επιτροπή ή ομάδα.

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

4.2 Μετάβαση στο περιβάλλον παραγωγής

Η μετάβαση ενός πληροφοριακού συστήματος ή μιας εφαρμογής στο περιβάλλον παραγωγής εκτελείται μόνο από εξουσιοδοτημένο προσωπικό.

Για τη μετάβαση επιλέγεται χρονική περίοδος που δεν εκτελούνται άλλες σημαντικές εργασίες και προβλέπεται δυνατότητα επαναφοράς στην αρχική κατάσταση, σε περίπτωση προβλήματος.

Τυχόν δεδομένα και λογαριασμοί δοκιμών διαγράφονται προτού το περιβάλλον παραγωγής αρχίσει να λειτουργεί ενεργά.

11. Λειτουργία και συντήρηση των πληροφοριακών συστημάτων

4.1 Λειτουργία των πληροφοριακών συστημάτων

Η λειτουργία πληροφοριακών συστημάτων αναφέρεται στο σύνολο των διαδικασιών που απαιτούνται για την καθημερινή λειτουργία τους με ασφάλεια και αξιοπιστία και περιλαμβάνει, μεταξύ άλλων, επαρκή έλεγχο και παρακολούθηση (αλλαγών, εκδόσεων, διορθώσεων ασφαλείας / patches, απόδοσης, συνέχειας εργασιών κτλ.), συντήρηση και υποστήριξη των συστημάτων με βάση τις προδιαγραφές τους και τις ανάγκες που προκύπτουν και σύμφωνα με τις σχετικές πολιτικές και διαδικασίες της ΕΕΤΤ.

4.2 Τεχνική υποστήριξη συστημάτων από τρίτα μέρη

Οι περιπτώσεις στις οποίες απαιτείται υποστήριξη των συστημάτων της ΕΕΤΤ από τρίτα μέρη πρέπει να είναι σαφώς καθορισμένες, καθώς επίσης ο τρόπος υποστήριξης από αυτά πρέπει να είναι αυστηρά προδιαγεγραμμένος και με συγκεκριμένα χρονικά περιθώρια ανταπόκρισής τους. Οι περιπτώσεις απομακρυσμένης πρόσβασης αναδόχου στα συστήματα της ΕΕΤΤ για την επίλυση εκτάκτων προβλημάτων πρέπει να είναι περιορισμένες, να αντιμετωπίζονται με ιδιαίτερη προσοχή και σε κάθε περίπτωση να υπάρχει καταγραφή (logging) των ενεργειών του.

4.3 Ισχυροποίηση του επιπέδου ασφαλείας (security hardening)

Τα πληροφοριακά συστήματα πρέπει να έχουν ενεργοποιημένες μόνο τις λειτουργίες που απαιτούνται για την εκπλήρωση του υπηρεσιακού σκοπού τους.

Μη απαραίτητα χαρακτηριστικά του λογισμικού, τόσο του περιβάλλοντος (π.χ. λειτουργικό σύστημα, RDBMS, κ.ο.κ.), όσο και της εφαρμογής, πρέπει να απενεργοποιούνται στο πλαίσιο ισχυροποίησης του επιπέδου ασφαλείας (Security Hardening) του συστήματος, ακολουθώντας τα τεχνικά πρότυπα ασφαλείας της ΕΕΤΤ.

Όλοι οι διαχειριστές / ιδιοκτήτες των πληροφοριακών συστημάτων και εφαρμογών πρέπει να γνωρίζουν τις ρυθμίσεις των παραμέτρων ασφαλείας για τα συστήματα ή τις εφαρμογές που τους αφορούν.

4.4 Απενεργοποίηση χαρακτηριστικών και λειτουργιών που δεν χρησιμοποιούνται

Τα χαρακτηριστικά και οι λειτουργίες των πληροφοριακών συστημάτων που δεν χρησιμοποιούνται, πρέπει να απενεργοποιούνται, όπου αυτό είναι εφικτό.

4.5 Παραμετροποίηση ρυθμίσεων ασφαλείας των πληροφοριακών συστημάτων

Οι ρυθμίσεις ασφαλείας των πληροφοριακών συστημάτων διαμορφώνονται σύμφωνα με τα αποτελέσματα της ανάλυσης κινδύνων.

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

4.6 Περιορισμός σχέσεων εμπιστοσύνης μεταξύ των πληροφοριακών συστημάτων

Η ισχυροποίηση του επιπέδου ασφάλειας των πληροφοριακών συστημάτων πρέπει να περιορίζει τη διασύνδεση / σχέση μεταξύ των πληροφοριακών συστημάτων στον ελάχιστο δυνατό βαθμό.

4.7 Απομόνωση εφαρμογών και υπηρεσιών

Όλα τα πληροφοριακά συστήματα πρέπει να αναπτύσσονται σύμφωνα με την αρχή: «μία κύρια λειτουργία ανά διακομιστή» ("one primary function per server"), έτσι ώστε να διασφαλίζεται ότι λειτουργίες με διαφορετικά επίπεδα ασφαλείας δεν θα φιλοξενηθούν στον ίδιο διακομιστή.

Αυτή η αρχή πρέπει, επίσης, να ισχύει όταν χρησιμοποιούνται «εικονικές τεχνολογίες» (virtualization technologies). Συγκεκριμένα, πρέπει να επαληθεύεται ότι εφαρμόζεται μόνο μία κύρια λειτουργία ανά εικονικό σύστημα και ότι η εικονική υποδομή είναι επαρκώς προστατευμένη.

4.8 Απενεργοποίηση προκαθορισμένων/ειδικών λογαριασμών

Οι προκαθορισμένοι λογαριασμοί εφαρμογών ή βάσεων δεδομένων, τα αναγνωριστικά χρήστη και οι κωδικοί πρόσβασης πρέπει να αφαιρούνται ως μέρος της διαδικασίας ισχυροποίησης του επιπέδου ασφάλειας, όπου αυτό είναι εφικτό.

4.9 Κεντρική διαχείριση συστήματος

Η διαχείριση των πληροφοριακών συστημάτων μέσω του δικτύου πρέπει να πραγματοποιείται από συστήματα που αποτελούν μέρος μιας κεντρικής υποδομής διαχείρισης, όπου αυτό είναι εφικτό.

Τα εν λόγω συστήματα διαχείρισης πρέπει να βρίσκονται σε ένα ξεχωριστό, απομονωμένο και προστατευμένο υποδίκτυο που εξυπηρετεί μόνο αυτόν το σκοπό.

4.1 Καταγραφή ελέγχου

Για λόγους ασφαλείας, όλα τα πληροφοριακά συστήματα της ΕΕΤΤ (εφόσον είναι εφικτό) πρέπει να παρέχουν τη δυνατότητα εξαγωγής αρχείων καταγραφής (log files, audit trails).

4.2 Δημιουργία αντιγράφων ασφαλείας

Για όλα τα ευαίσθητα και κρίσιμα πληροφοριακά συστήματα της ΕΕΤΤ, κατ' ελάχιστον, λαμβάνονται αντίγραφα ασφαλείας τα οποία αποθηκεύονται σε προστατευμένες περιοχές, σύμφωνα με τις σχετικές πολιτικές και διαδικασίες.

4.3 Παρακολούθηση λειτουργίας των συστημάτων παραγωγής

Όλα τα κρίσιμα και / ή ευαίσθητα πληροφοριακά συστήματα επιβλέπονται σύμφωνα με τις σχετικές πολιτικές της ΕΕΤΤ, με σκοπό τον έγκαιρο εντοπισμό προβλημάτων και για σκοπούς διαχείρισης της χωρητικότητάς τους.

4.4 Αναφορά σφαλμάτων από χρήστες

Όλοι οι χρήστες είναι υποχρεωμένοι να αναφέρουν στα αρμόδια στελέχη της Διεύθυνσης Ψηφιακής Διακυβέρνησης πιθανά προβλήματα σχετικά με τη λειτουργία των πληροφοριακών συστημάτων που υποπίπτουν στην αντίληψή τους.

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

12. Έλεγχος των ευπαθειών των πληροφοριακών συστημάτων

4.5 Εσωτερικοί έλεγχοι

Οι διαδικασίες ανάπτυξης / προμήθειας ενός συστήματος ή εξωτερικής ανάθεσης για τη δημιουργία ενός συστήματος συμπεριλαμβάνονται στο πεδίο εφαρμογής των εσωτερικών ελέγχων που πραγματοποιεί η ΕΕΤΤ.

4.6 Προσδιορισμός των ευπαθειών των πληροφοριακών συστημάτων

Η ΕΕΤΤ λαμβάνει προληπτικά μέτρα για τον εντοπισμό και την ελαχιστοποίηση των τρωτών σημείων / ευπαθειών των συστημάτων της, σύμφωνα με τις σχετικές πολιτικές, προτού τα εκμεταλλευτούν κακόβουλες οντότητες.

Μεταξύ άλλων, πρέπει να διενεργεί σε τακτική βάση, μέσω εξειδικευμένων εταιρειών, penetration tests, δηλαδή δοκιμαστικές απόπειρες παραβίασης της ασφάλειας των συστημάτων και δικτύων της, βάσει καθορισμένων σεναρίων, με στόχο την αξιολόγηση της επάρκειας της ασφάλειάς τους.

4.7 Αποκατάσταση των ευπαθειών των πληροφοριακών συστημάτων

Η ΕΕΤΤ αξιολογεί όλες τις ευπάθειες που εντοπίζονται στα πληροφοριακά συστήματά της και εφαρμόζει τα κατάλληλα σχέδια αποκατάστασης ή επιδιόρθωσης, όπως για παράδειγμα περιοδικές ενημερώσεις λογισμικού (updates). Εάν μια εφαρμογή δεν υποστηρίζεται πλέον από τον προμηθευτή, τον προγραμματιστή ή κάποιο άλλο τρίτο μέρος, τότε πρέπει να αξιολογείται προς αντικατάσταση.

13. Παύση λειτουργίας πληροφοριακών συστημάτων

Η παύση της λειτουργίας και η απόσυρση των πληροφοριακών συστημάτων της ΕΕΤΤ εκτελείται σύμφωνα με τα οριζόμενα στην Πολιτική Διαχείρισης Πληροφοριακών Πόρων. Διασφαλίζεται η αποτελεσματική συνέχεια των εργασιών.

14. Πρόσθετα θέματα ασφάλειας εφαρμογών δικτύου

4.1 Κίνδυνοι ασφάλειας εφαρμογών δικτύου

Δεδομένου ότι το επίπεδο εφαρμογής δικτύου είναι ιδιαίτερα υψηλού κινδύνου και μπορεί να γίνει στόχος τόσο εσωτερικών όσο και εξωτερικών απειλών, πρέπει να χρησιμοποιείται κατάλληλη διαδικασία ανάπτυξης λογισμικού για οποιαδήποτε εφαρμογή δικτύου μεταδίδει, επεξεργάζεται ή αποθηκεύει προσωπικά δεδομένα.

4.2 Προστασία εφαρμογών

Η λειτουργικότητα που παρέχεται από τις εφαρμογές ή οι πληροφορίες που αυτές διαχειρίζονται, δεν πρέπει να εκτίθενται άσκοπα.

4.3 Μηχανισμοί ασφαλούς αποτυχίας (fail safe)

Κάθε εφαρμογή πρέπει αυτόματα να ενεργοποιεί το μηχανισμό ασφαλούς αποτυχίας μόλις ανιχνεύσει ύποπτη δραστηριότητα, ώστε να προστατευτούν τα δεδομένα που επεξεργάζεται από πιθανή διαρροή ή αλλοίωση.

4.4 Διαχείριση και παρακολούθηση των συνεδριών (sessions)

Κάθε εφαρμογή πρέπει να γνωρίζει οποιαδήποτε στιγμή ποιος χρήστης είναι συνδεδεμένος, τι ενέργειες επιχειρεί να εκτελέσει και να ελέγχει αν πρέπει να του χορηγηθεί πρόσβαση ή όχι.

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

4.5 Απόκρυψη πληροφοριών

Οι προγραμματιστές πρέπει να διασφαλίζουν ότι οι εφαρμογές δεν αποκαλύπτουν άσκοπα πληροφορίες ή μηνύματα εντοπισμού σφαλμάτων από λάθος.

4.6 Προστασία αποστολής ευαίσθητων δεδομένων

Η αποστολή ευαίσθητων δεδομένων πρέπει να πραγματοποιείται μέσω προστατευμένων καναλιών, σύμφωνα με τις σχετικές πολιτικές.

4.7 Firewalls εφαρμογών/Reverse proxies

Πρέπει να χρησιμοποιούνται, όπου είναι εφικτό, firewalls εφαρμογών και/ή reverse proxies, ώστε να ελέγχεται η κυκλοφορία δεδομένων σε εφαρμογές δικτύου και να αποφεύγονται πιθανές επιθέσεις, όπως SQL injection, buffer overflows, cross site scripting κτλ.

4.8 Συστήματα προστασίας βάσεων δεδομένων

Οι βάσεις δεδομένων πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση.

»

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.
3. **Ορίζει** ότι η *«Πολιτική Προμήθειας και Ανάπτυξης Συστημάτων»* συνδέεται άρρηκτα με τις υπό στοιχείο 4΄, 5΄, 6΄, 7΄, 8΄, 9΄, 10΄ ως άνω πολιτικές ασφαλείας της ΕΕΤΤ και πρέπει να εφαρμόζεται υποχρεωτικά και απαρέγκλιτα από το προσωπικό της του οποίου οι δραστηριότητες εργασίας σχετίζονται με τον κύκλο ζωής των πληροφοριακών συστημάτων.
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 Προμήθειας και Ανάπτυξης Συστημάτων»*.
    - Τροποποιεί την *«Πολιτική Προμήθειας και Ανάπτυξης Συστημάτων»*, όποτε αυτό απαιτείται, για να ευθυγραμμίζεται με τις τρέχουσες ανάγκες και εξελίξεις.

Ο ΠΡΟΕΔΡΟΣ

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

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