ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ

Μαρούσι, 29-09-2025

ΑΠ 1168/14

ΑΠΟΦΑΣΗ

Έγκριση της «Πολιτικής Παρακολούθησης Ασφάλειας 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),

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*

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

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 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),

1.11 της Υ.Α. 1899/27-06-2025 *«Καθορισμός προσόντων, καθηκόντων, ασυμβιβάστων και υποχρεώσεων των Υπεύθυνων Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών»* (ΦΕΚ 4250/Β΄/05-08-2025),

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

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

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 1078/23/17-07-2023 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Προστασίας Προσωπικών Δεδομένων"*»,
8. Την ΑΠ 1089/32/30-10-2023 Απόφαση της ΕΕΤΤ «*Έγκριση της «Πολιτικής Διατήρησης Πληροφοριών»*»,
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 1128/24/07-10-2024 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Προμήθειας και Ανάπτυξης Συστημάτων"*»,
12. Την ΑΠ 1138/24/23-12-2024 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Τρίτων Μερών"*»,
13. Την ΑΠ 1161/13/21-07-2025 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διενέργειας Ελέγχων Ασφάλειας Πληροφοριών"*»,

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

14. Την ΑΠ 1109/13/15-4-2024 Απόφαση της ΕΕΤΤ «*Επικύρωση του Εγχειριδίου Διαδικασιών της ΕΕΤΤ*»,
15. 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),
16. Το γεγονός ότι από τις διατάξεις της παρούσας Απόφασης δεν προκαλείται δαπάνη σε βάρος του κρατικού προϋπολογισμού ούτε του προϋπολογισμού της ΕΕΤΤ,
17. Την Εισήγηση αριθ. 38629/Φ600/23-09-2025 της αρμόδιας Υπηρεσίας της ΕΕΤΤ,

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

Επειδή :

1. Η παρακολούθηση της χρήσης και απόδοσης των συστημάτων πληροφορικής ενός οργανισμού (IT systems monitoring), συμπεριλαμβανομένου του υλικού, του λογισμικού και των δικτύων του, περιλαμβάνει εργασίες, όπως ενδεικτικά η παρακολούθηση και ανάλυση πληροφοριών που τα συστήματα καταγράφουν για τη λειτουργία τους, τις βλάβες και τα σφάλματα, τις ενέργειες των χρηστών, τα περιστατικά ασφαλείας κ.λπ.
2. Η συστηματική παρακολούθηση της χρήσης και απόδοσης των συστημάτων πληροφορικής είναι κρίσιμη και αναγκαία για την προληπτική διαχείριση των κινδύνων που τα απειλούν, τον έγκαιρο εντοπισμό συμβάντων, τη διατήρηση της ασφάλειας, τη διασφάλιση της συμμόρφωσης με τις νομικές, κανονιστικές υποχρεώσεις και τις πολιτικές, καθώς και τη βελτιστοποίηση της απόδοσής τους.

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

3. Η παρακολούθηση των συστημάτων της ΕΕΤΤ πρέπει υποχρεωτικά να ακολουθεί πρότυπα, κανόνες, βέλτιστες πρακτικές και να συμμορφώνεται με το νομοθετικό και κανονιστικό πλαίσιο, όπως ενδεικτικά τη νομοθεσία περί προστασίας δεδομένων προσωπικού χαρακτήρα. Παράλληλα, οι χρήστες των πληροφοριακών συστημάτων της ΕΕΤΤ πρέπει να είναι ενήμεροι για τους σκοπούς, τους τρόπους και τους κανόνες παρακολούθησης των συστημάτων.
4. Για τους λόγους αυτούς, κρίνεται σκόπιμη η σύνταξη και γνωστοποίηση στο προσωπικό της ΕΕΤΤ και στους λοιπούς χρήστες των συστημάτων της, μιας περιεκτικής πολιτικής η οποία θα περιγράφει τους κανόνες, τις διαδικασίες και τις κατευθυντήριες γραμμές για την παρακολούθηση ασφάλειας των συστημάτων της ΕΕΤΤ σε συστηματική βάση. Η καταγεγραμμένη αυτή πολιτική πρέπει να είναι εύκολα προσβάσιμη από το σύνολο του προσωπικού.

Αποφασίζει :

1. **Εγκρίνει** την «*Πολιτική Παρακολούθησης Ασφάλειας Συστημάτων*», *η οποία* έχει ως εξής:

« Πολιτική Παρακολούθησης Ασφάλειας Συστημάτων

Έκδοση: 1η

Τελευταία Ημερομηνία Ενημέρωσης: Σεπτέμβριος 2025

1. Σκοπός και πεδίο εφαρμογής

Σκοπός της παρούσας πολιτικής είναι η δημιουργία ενός πλαισίου παρακολούθησης των συστημάτων πληροφορικής της ΕΕΤΤ (IT systems monitoring), προκειμένου να:

- *ανιχνεύονται και αντιμετωπίζονται εγκαίρως, βλάβες, δυσλειτουργίες, προσπάθειες μη εξουσιοδοτημένης δραστηριότητας, συμβάντα ασφάλειας και παραβιάσεις προσωπικών δεδομένων*
- *εντοπίζεται και εμποδίζεται η εκούσια ή ακούσια λανθασμένη χρήση των συστημάτων*
- *διατηρείται η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα συστημάτων και δεδομένων*

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

- *διασφαλίζεται η συμμόρφωση με τη νομοθεσία, τους κανονισμούς και τις πολιτικές της ΕΕΤΤ (π.χ. ως προς την προστασία προσωπικών δεδομένων, την ασφάλεια και χρήση της πληροφορίας)*
- *διευκολύνονται οι έρευνες περιστατικών, η αντιμετώπιση προβλημάτων και η λογοδοσία*
- *παρακολουθούνται οι μετρήσεις απόδοσης των συστημάτων και βελτιστοποιούνται οι επιδόσεις τους.*

Η παρακολούθηση των συστημάτων αυξάνει την ασφάλεια και αποτελεσματικότητά τους, μειώνει τις διακοπές λειτουργίας και τα λειτουργικά κόστη και βελτιώνει τη λήψη αποφάσεων. Επομένως, είναι αμοιβαία επωφελής τόσο για την ΕΕΤΤ όσο και για το προσωπικό της και γενικότερα για τους χρήστες των πληροφοριακών συστημάτων της.

Η παρακολούθηση των συστημάτων μπορεί να περιλαμβάνει ενδεικτικά την παρακολούθηση αρχείων καταγραφής[1] (log files) για σφάλματα, προειδοποιήσεις και ύποπτη δράση, την ανάλυση της κίνησης δικτύου για την ανίχνευση ασυνήθιστης δραστηριότητας ή πιθανών απειλών ασφαλείας, την παρακολούθηση των συνδέσεων χρηστών, χρήσης των εφαρμογών και πρόσβασης δεδομένων για τον εντοπισμό πιθανής κακής χρήσης ή κινδύνων ασφαλείας, καθώς και τη μέτρηση της χρήσης πόρων συστήματος (κεντρική μονάδα επεξεργασίας, μνήμη, χώρος στο δίσκο) για τη διασφάλιση βέλτιστης απόδοσης και τον εντοπισμό πιθανών προβλημάτων.

Το πεδίο εφαρμογής της παρούσας πολιτικής περιλαμβάνει ανθρώπους, διαδικασίες, τεχνολογία. Αφορά, δε, όλο το προσωπικό της ΕΕΤΤ και τους χρήστες των συστημάτων της χωρίς εξαιρέσεις.

2. Βασικές Έννοιες και Αρχές της παρακολούθησης ασφαλείας των συστημάτων

2.1 Αρχές δεοντολογίας και διασφαλίσεις

Η παρακολούθηση ασφάλειας των συστημάτων πληροφορικής της ΕΕΤΤ διενεργείται αποκλειστικά και μόνο από εξουσιοδοτημένο, για το σκοπό αυτό, προσωπικό, που είναι είτε εργαζόμενοι της ΕΕΤΤ (ειδικότερα της Διεύθυνσης Ψηφιακής Διακυβέρνησης) είτε τους έχει ανατεθεί με γραπτή σύμβαση να ενεργούν ως εκτελούντες για λογαριασμό της ΕΕΤΤ. Αποτελεί πειθαρχικό παράπτωμα η συμμετοχή οποιουδήποτε σε δραστηριότητες παρακολούθησης συστημάτων χωρίς την κατάλληλη άδεια ή η παρακολούθηση εκτός των τομέων ευθύνης του.

Το εξουσιοδοτημένο προσωπικό εκτελεί τα καθήκοντά του αναφορικά με την παρακολούθηση των συστημάτων σύμφωνα με το νομοθετικό και κανονιστικό πλαίσιο και τις σχετικές πολιτικές της ΕΕΤΤ. Ειδικότερα:

- *Σέβεται και διασφαλίζει τα προσωπικά δεδομένα και την ιδιωτικότητα των άλλων ανά πάσα στιγμή*
- *Δεν χρησιμοποιεί ή αποκαλύπτει πληροφορίες που συλλέγονται κατά τη διαδικασία παρακολούθησης της ασφάλειας για σκοπούς διαφορετικούς από εκείνους για τους οποίους εγκρίθηκε αυτή η διαδικασία*
- *Προστατεύει τις πληροφορίες που συλλέγονται από οποιαδήποτε πιθανή μη εξουσιοδοτημένη πρόσβαση*

[1] *Τα αρχεία καταγραφής (log files) είναι αρχεία που αποθηκεύουν πληροφορίες για συμβάντα, ενέργειες, σφάλματα και άλλες δραστηριότητες σε έναν υπολογιστή, ένα σύστημα ή μια συσκευή. Χρησιμοποιούνται για την παρακολούθηση της απόδοσης, την αντιμετώπιση προβλημάτων, την ανίχνευση απειλών και την παροχή ιστορικού χρήσης.*

- *Καταστρέφει τις πληροφορίες που συλλέγονται, καθώς και τις σχετικές αναφορές που συντάσσονται, σύμφωνα με τις πολιτικές και προθεσμίες διατήρησης της ΕΕΤΤ (βλ. την Πολιτική Διατήρησης Πληροφοριών).*

2.2 Ενημέρωση και ευθύνες των χρηστών των συστημάτων

Οι χρήστες των πληροφοριακών συστημάτων είναι ενήμεροι ότι η ΕΕΤΤ διατηρεί το δικαίωμα παρακολούθησης της πρόσβασης στα συστήματά της, αποκλειστικά από εξουσιοδοτημένο προσωπικό, προκειμένου να διασφαλίζει την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητά τους. Η ΕΕΤΤ ενημερώνει, με κάθε πρόσφορο τρόπο, τους χρήστες σχετικά με τους σκοπούς και τους τρόπους της παρακολούθησης της ασφάλειας, καθώς και για τους τρόπους χρήσης των καταγραφέντων δεδομένων παρακολούθησης.

Η παρούσα πολιτική είναι εύκολα προσβάσιμη για τους χρήστες των συστημάτων της ΕΕΤΤ, οι οποίοι είναι υποχρεωμένοι να την γνωρίζουν και συναινούν με αυτήν για το σκοπό της ασφάλειας των πληροφοριακών πόρων. Παράλληλα, αντιλαμβάνονται τις δικές τους ευθύνες και υποχρεώσεις για χρήση των συστημάτων σύμφωνα με τις πολιτικές της ΕΕΤΤ (βλ. ενδεικτικά την Πολιτική Αποδεκτής Χρήσης των Πληροφοριακών Αγαθών της ΕΕΤΤ, την Πολιτική Ασφάλειας Τελικού Χρήστη, καθώς και την Πολιτική Τηλεργασίας και Φορητών Συσκευών).

Η παρακολούθηση ασφάλειας των συστημάτων διενεργείται σύμφωνα με τους κανόνες της παρούσας πολιτικής ως μία διαφανής διαδικασία. Μόνη επιτρεπτή εξαίρεση ως προς τη διατήρηση της διαφάνειας κατά την παρακολούθηση των συστημάτων, αποτελεί η διερεύνηση ύποπτης εγκληματικής δραστηριότητας κατά την οποία δεν απαιτείται ενημέρωση του χρήστη η οποία θα δυσχέραινε την έρευνα.

2.3 Αντικείμενο της παρακολούθησης ασφάλειας

Όλα τα συστήματα που παρέχουν υπηρεσίες δικτύου ή εφαρμογές ενδέχεται να παρακολουθούνται, δηλαδή τα δίκτυα, οι υπολογιστές των χρηστών, οι διακομιστές (servers) που είναι εγκατεστημένοι στην ΕΕΤΤ, οι εφαρμογές, οι βάσεις δεδομένων, καθώς επίσης τα συστήματα που φιλοξενούνται στην Κυβερνητική Υπηρεσία Υπολογιστικού Νέφους (G-Cloud) που διαχειρίζεται η Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης (ΓΓΠΣΨΔ) του Υπουργείου Ψηφιακής Διακυβέρνησης. Η επιλογή των συστημάτων που παρακολουθούνται εξαρτάται από την κρισιμότητά τους (σύμφωνα με την Πολιτική Διαχείρισης Πληροφοριακών Πόρων) και την εκτίμηση της επικινδυνότητάς τους.

Η εποπτεία των συστημάτων για λόγους ασφαλείας ενδέχεται να στοχεύει μεταξύ άλλων σε (η λίστα δεν είναι εξαντλητική και η σειρά είναι τυχαία):

- *ασυνήθιστη κίνηση δικτύου,*
- *στατιστικά στοιχεία δικτύου, όπως στατιστικά καταστάσεων σφάλματος,*
- *μη αδειοδοτημένο λογισμικό,*
- *ενεργές διεργασίες που χρησιμοποιούν την Κεντρική Μονάδα Επεξεργασίας (CPU),*
- *ασυνήθιστη δραστηριότητα αποθήκευσης και χρήσης αρχείων (π.χ. διερεύνηση τύπων και μεγεθών αρχείων),*
- *μη αναμενόμενες καταγραφές στα αρχεία καταγραφής,*
- *επιτυχημένες και ανεπιτυχείς προσπάθειες πρόσβασης (λογαριασμός χρήστη, απομακρυσμένη διεύθυνση IP, σήμανση ημερομηνίας/ώρας, διάρκεια συνεδρίας),*
- *συμπεριφορές διαχειριστών και χρηστών που δεν συμμορφώνονται με τις πολιτικές της ΕΕΤΤ,*
- *λοιπές ύποπτες καταστάσεις.*

Η παραπάνω λίστα είναι ενδεικτική και προσαρμόζεται σύμφωνα με τις εκάστοτε ανάγκες.

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

Επισημαίνεται ότι η παρακολούθηση ασφαλείας των συστημάτων που διενεργεί η ΕΕΤΤ έχει ως σκοπό και αντικείμενο την ευρύτερη επιτήρηση των συστημάτων πληροφορικής για προστασία από απειλές και σε καμία περίπτωση δεν στοχεύει στην ατομική παρακολούθηση των κινήσεων και δραστηριοτήτων ενός ή περισσότερων συγκεκριμένων φυσικών προσώπων. Όμως στο πλαίσιο της επιτήρησης αυτής, τα συστήματα της ΕΕΤΤ διεξάγουν με αυτόματο τρόπο, καταγραφές της συμπεριφοράς των χρηστών, οι οποίες, εφόσον χρειαστεί, μπορούν να αξιοποιηθούν για τη διερεύνηση περιστατικού ασφαλείας ή παράνομης δραστηριότητας ή παραβίασης ταυτότητας κτλ.

2.4 Διεργασία Παρακολούθησης της Ασφάλειας, Καταγραφή και Έλεγχος (logging και auditing)

Η διεργασία παρακολούθησης της ασφάλειας των συστημάτων περιλαμβάνει συλλογή, αποθήκευση και ανάλυση δεδομένων παρακολούθησης και στη συνέχεια, ανάληψη κατάλληλης δράσης με σκοπό τη διόρθωση / βελτίωση.

Η ΕΕΤΤ πρέπει να διαθέτει και εφαρμόζει διεργασία επίβλεψης του επιπέδου ασφαλείας των συστημάτων μέσω συνεχούς παρακολούθησης και περιοδικής αναθεώρησης των αρχείων καταγραφής συστημάτων, μέτρησης της χρήσης των πόρων συστήματος, καθώς και παρακολούθησης μηνυμάτων, ειδοποιήσεων και συναγερμών έκτακτης ανάγκης που ειδοποιούν για συμβάντα και σφάλματα (βλ. επίσης τις ενότητες 3 και 4 παρακάτω για περισσότερες λεπτομέρειες επί των σχετικών διαδικασιών της ΕΕΤΤ).

Ως προς τη συλλογή των δεδομένων παρακολούθησης, η ΕΕΤΤ διατηρεί επίσημα αρχεία που περιλαμβάνουν καταγραφές (logs) σχετικές με τη δραστηριότητα των συστημάτων και τις εκτελούμενες διεργασίες, καθώς και τη δραστηριότητα των χρηστών. Αυτά τα αρχεία διαμορφώνονται, λαμβάνονται, διατηρούνται και αποθηκεύονται σύμφωνα με τις εκάστοτε υπηρεσιακές ανάγκες και συμμορφώνονται στις νομικές / κανονιστικές υποχρεώσεις.

Τα υπό εξέταση αρχεία ενδέχεται να περιλαμβάνουν αρχεία καταγραφής (η λίστα είναι ενδεικτική των δυνητικών καταγραφών):

- *περιμετρικών συσκευών ασφαλείας (firewalls)[2]*
- *υποδομών προστασίας (ενάντια σε κακόβουλο λογισμικό)*
- *υποδομής απομακρυσμένης πρόσβασης*
- *συστημάτων / εφαρμογών*
- *πρόσβασης χρήστη*
- *σφαλμάτων συστήματος / εφαρμογής*
- *αντιγραφής και ανάκτησης δεδομένων*
- *φυσικής πρόσβασης*

Η επιλογή και παρακολούθηση αυτών των αρχείων καταγραφής εξαρτώνται από τις υπηρεσιακές και νομικές / κανονιστικές απαιτήσεις. Σε κάθε περίπτωση, πρέπει να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα, σύμφωνα με την ισχύουσα νομοθεσία.

Σε συνέχεια της συλλογής των δεδομένων, ο σκοπός της ανάλυσης των εν λόγω αρχείων καταγραφής είναι να αναζητηθούν ύποπτα μοτίβα, ασυνήθιστες συμπεριφορές, σφάλματα, προβλήματα επιδόσεων, περιστατικά κ.λπ. που θα διευκολύνουν την ανίχνευση παραβιάσεων ασφαλείας και λοιπών προβλημάτων λειτουργίας των συστημάτων και θα καθοδηγήσουν στην αντιμετώπισή τους.

[2] *Η περιμετρική συσκευή ασφαλείας ή αλλιώς τείχος προστασίας (firewall) λειτουργεί ως ένα προστατευτικό φράγμα που ελέγχει και φιλτράρει την εισερχόμενη και εξερχόμενη κυκλοφορία δεδομένων σε ένα δίκτυο, επιτρέποντας ή αποκλείοντας την πρόσβαση με βάση προκαθορισμένους κανόνες ασφαλείας.*

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 Εργαλεία και Τεχνολογίες Παρακολούθησης της Ασφάλειας

Για την παρακολούθηση της λειτουργίας και ασφάλειας των συστημάτων δεν επαρκεί μόνο η υιοθέτηση πολιτικών και λήψη μέτρων. Απαιτείται επιπλέον η προμήθεια και εφαρμογή κατάλληλων τεχνολογιών και εξειδικευμένων εργαλείων τα οποία προωθούν την συγκεντρωτική, αυτοματοποιημένη και συνεχή επιτήρηση των συστημάτων και έτσι διευκολύνουν στο έργο τους τα στελέχη που έχουν επιφορτιστεί με αυτήν. Οι οπτικοί πίνακες ελέγχου (dashboards) που διαθέτουν αυτά τα συστήματα βοηθούν τους χειριστές τους να αντιλαμβάνονται γρήγορα την εύρυθμη λειτουργία των συστημάτων και να εντοπίζουν τάσεις ή προβλήματα.

Η αξιοποίηση τέτοιων συστημάτων παρακολούθησης ασφαλείας προϋποθέτει τον καθορισμό των κρίσιμων παραμέτρων λειτουργίας, απόδοσης και ασφάλειας που κρίνεται ότι πρέπει να παρακολουθούνται για τον εντοπισμό μη αποδεκτών καταστάσεων και πιθανών απειλών και τον ορισμό κατάλληλων ορίων πέραν των οποίων αποστέλλονται αυτόματες ειδοποιήσεις και συναγερμοί έκτακτης ανάγκης, για να ενημερώνονται άμεσα όσοι έχουν την ευθύνη της αντιμετώπισης των κρίσιμων ζητημάτων ασφαλείας.

Περισσότερες λεπτομέρειες επί των συστημάτων παρακολούθησης που χρησιμοποιεί η ΕΕΤΤ αναφέρονται παρακάτω στην ενότητα 4.1.

3. Καταγραφή Συμβάντων Ασφαλείας

3.1 Ενεργοποίηση Καταγραφής Συμβάντων Ασφαλείας

Η καταγραφή συμβάντων ασφαλείας για τα συστήματα της ΕΕΤΤ πρέπει να υλοποιείται σύμφωνα με τις καλές πρακτικές και συμμορφώνεται με τις απαιτήσεις του ισχύοντος νομοθετικού και κανονιστικού πλαισίου, όπως περί προστασίας δεδομένων προσωπικού χαρακτήρα (βλ. την Πολιτική Προστασίας Προσωπικών Δεδομένων). Επίσης, πρέπει να εφαρμόζεται σύμφωνα με τα επίπεδα ταξινόμησης των συστημάτων (βλ. την Πολιτική Διαχείρισης Πληροφοριακών Πόρων), διότι κρίσιμα ή ευαίσθητα συστήματα έχουν αυξημένες ανάγκες καταγραφής συμβάντων ασφαλείας σε αντιδιαστολή προς τα υπόλοιπα συστήματα.

Τα αρχεία καταγραφής πρέπει να διαμορφώνονται με κατάλληλο τρόπο, ώστε να συμπεριλαμβάνουν χρήσιμες λεπτομέρειες, σύμφωνα με τις ιδιαίτερες ανάγκες και απαιτήσεις της ΕΕΤΤ. Ενδεικτικά, τέτοιες πληροφορίες θα μπορούσαν να είναι η ημερομηνία και ώρα των συμβάντων, η ώρα που οι χρήστες συνδέονται και αποσυνδέονται από το σύστημα, τα αναγνωριστικά χρήστη, οι αλλαγές κωδικού πρόσβασης, η ημερομηνία και ώρα που το σύστημα ενεργοποιείται και απενεργοποιείται, οι τροποποιήσεις ρυθμίσεων ασφαλείας κ.λπ.

Η ποσότητα και ο τύπος των συμβάντων που καταγράφονται δεν πρέπει να επηρεάζουν την φυσιολογική λειτουργία του συστήματος.

3.2 Κανονικοποίηση Καταγραφών

Όπου είναι εφικτό, η ΕΕΤΤ επιδιώκει μια διαδικασία κανονικοποίησης των καταγραφών, ώστε τα αρχεία καταγραφής που λαμβάνονται από διάφορες πηγές να μπορούν να μεταφερθούν σε μια κοινή μορφή. Με αυτόν τον τρόπο, όλα τα αρχεία καταγραφής μπορούν να τροφοδοτηθούν σε μια κεντρική λύση διαχείρισης αρχείων καταγραφής για περαιτέρω επεξεργασία (κατάταξη, συμπίεση, κλπ.).

3.3 Ελάχιστες Απαιτήσεις για Καταγραφή Συμβάντων Ασφαλείας σε Επίπεδο Δικτύου

Για συσκευές δικτύου, οι αποτυχημένες προσπάθειες πρόσβασης και άλλες δραστηριότητες που σχετίζονται με την ασφάλεια των συσκευών πρέπει να καταγράφονται, όπου είναι εφικτό.

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

3.4 Ελάχιστες Απαιτήσεις για Καταγραφή Συμβάντων Ασφαλείας σε Επίπεδο Συστήματος

Οι ανεπιτυχείς προσπάθειες πρόσβασης σε πόρους συστήματος και άλλες δραστηριότητες που σχετίζονται με την ασφάλεια στο σύστημα πρέπει να καταγράφονται, όπου είναι εφικτό, ιδίως στα κρίσιμα ή ευαίσθητα συστήματα.

3.5 Ελάχιστες Απαιτήσεις για την Καταγραφή Συμβάντων Ασφαλείας σε Επίπεδο Εφαρμογών

Σε επίπεδο εφαρμογής, οι προσπάθειες χρήστη να αποκτήσει πρόσβαση στο σύστημα (σε περιπτώσεις όπου η διαδικασία αναγνώρισης και η διαδικασία αυθεντικοποίησης λαμβάνει χώρα σε επίπεδο εφαρμογής) και οι προσπάθειες να αποκτήσει πρόσβαση στα δεδομένα και τους πόρους της εφαρμογής πρέπει να καταγράφονται από τις εφαρμογές, όπου αυτό είναι εφικτό, ιδίως στις κρίσιμες ή ευαίσθητες εφαρμογές. Η καταγραφή διασφαλίζει ότι ο χρήστης δεν μπορεί να αρνηθεί ότι πραγματοποίησε τη συναλλαγή που του αποδίδεται (non-repudiation), οπότε διευκολύνεται η λογοδοσία.

3.6 Καταγραφή Συμβάντων και Λογαριασμοί με Αυξημένα Δικαιώματα

Οι δραστηριότητες των διαχειριστών σε εφαρμογές, βάσεις δεδομένων, συστήματα και συσκευές δικτύου, δηλαδή οι προνομιακές λειτουργίες πρέπει να καταγράφονται, εφόσον είναι εφικτό. Αυτά τα αρχεία καταγραφής προστατεύονται και πρέπει να υποβάλλονται σε τακτικούς ελέγχους.

3.7 Καταγραφή Συμβάντων και Διαχειριστών σε Συστήματα Παρακολούθησης Ασφαλείας

Οι μηχανισμοί καταγραφής συμβάντων ασφαλείας πρέπει να καταγράφουν τις λειτουργίες στα συστήματα ασφαλείας και παρακολούθησης (όπως πρόσβαση διαχειριστή, αλλαγές στη διαμόρφωσή τους κ.λπ.), όπου αυτό είναι εφικτό.

3.8 Απαγόρευση Καταγραφής Κωδικών Πρόσβασης

Οι μηχανισμοί παρακολούθησης δεν πρέπει να καταγράφουν τους κωδικούς πρόσβασης (passwords) που χρησιμοποιούν οι χρήστες για την πρόσβαση σε συστήματα ή εφαρμογές.

3.9 Συγχρονισμός Ρολογιού Συστήματος

Πρέπει να χρησιμοποιείται τεχνολογία συγχρονισμού ώρας, προκειμένου να συγχρονίζονται όλα τα κρίσιμα ρολόγια συστήματος και να διασφαλίζεται σταθερή ώρα όλων των συστημάτων πληροφορικής και των σχετικών αρχείων καταγραφής.

4. Συστήματα Ασφάλειας και Διαχείριση Συμβάντων

4.1 Συστήματα Παρακολούθησης Ασφαλείας που χρησιμοποιεί η ΕΕΤΤ

Η ΕΕΤΤ χρησιμοποιεί ένα ενιαίο σύστημα παρακολούθησης προστασίας από ιούς (antivirus monitoring system) χρηστών και firewall, το οποίο εντοπίζει και αποτρέπει απειλές σε πραγματικό χρόνο. Ειδοποιεί για απειλές σε επίπεδο δικτύου και υπολογιστών των χρηστών. Ανάλογα με τη σοβαρότητα της απειλής, μπορεί να απομονώσει αυτόματα τον υπολογιστή του χρήστη και να ειδοποιήσει σχετικά τον αρμόδιο διαχειριστή της Διεύθυνσης Ψηφιακής Διακυβέρνησης. Από την ίδια πλατφόρμα παρέχεται δυνατότητα πρόσβασης στα αρχεία καταγραφής (logs) των firewalls. Επίσης, στην ίδια πλατφόρμα υπάρχει η πληροφορία για τους χρήστες της ΕΕΤΤ οι οποίοι εργάζονται απομακρυσμένα και είναι συνδεδεμένοι στο δίκτυο της ΕΕΤΤ μέσω εικονικού ιδιωτικού δικτύου (Virtual Private Network - VPN)[3].

[3] *Το VPN ή αλλιώς το Εικονικό Ιδιωτικό Δίκτυο είναι μια τεχνολογία που επιτρέπει τη δημιουργία μιας ασφαλούς και κρυπτογραφημένης σύνδεσης μεταξύ της συσκευής του χρήστη και του Διαδικτύου. Αυτό σημαίνει ότι όλα τα*

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

Στους κρίσιμους διακομιστές (servers) της ΕΕΤΤ (όπως για παράδειγμα στους Active Directory Servers[4]) έχει εγκατασταθεί σύστημα antivirus το οποίο παρακολουθεί, καταγράφει και αποτρέπει απειλές. Είναι συνδεδεμένο με σύστημα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (Security Information and Event Management – SIEM) στο οποίο καταγράφονται τα συμβάντα (events) των servers. Παρακολουθεί και διερευνά ύποπτη δραστηριότητα, επιθέσεις και άλλα περιστατικά ασφαλείας στους servers και συμβάλει στον περιορισμό και την αποκατάσταση κυβερνοεπιθέσεων σε πραγματικό χρόνο. Παράλληλα, η ΕΕΤΤ διατηρεί κι ένα δεύτερο εργαλείο για τη συγκέντρωση, αποθήκευση και ανάλυση δεδομένων καταγραφής από τους servers της το οποίο συμβάλει στην αντιμετώπιση προβλημάτων, την ασφάλεια, τη συμμόρφωση και τη βελτιστοποίηση της απόδοσης των συστημάτων της.

Επίσης, η ΕΕΤΤ χρησιμοποιεί ένα σύστημα το οποίο παρακολουθεί αυτόματα το Μητρώο Πληροφοριακών Πόρων (Asset Management) με τους servers και το δικτυακό εξοπλισμό της, παρέχοντας αναλυτικές πληροφορίες για αυτά. Επιπλέον, διαθέτει τη δυνατότητα να παρατηρεί και μετρά τη διαθεσιμότητα και απόδοση των servers και του δικτυακού εξοπλισμού ώστε να επιβεβαιώνει ότι παραμένουν προσβάσιμα και λειτουργικά στους χρήστες.

Τα πληροφοριακά συστήματα της ΕΕΤΤ που φιλοξενούνται στην Κυβερνητική Υπηρεσία Υπολογιστικού Νέφους (G-Cloud) παρακολουθούνται μέσω ενός προηγμένου συστήματος διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM). Το σύστημα αυτό αξιοποιεί σύγχρονες τεχνολογίες για να εντοπίσει, διερευνήσει και αντιμετωπίσει τις απειλές ασφαλείας των συστημάτων και τις παραβιάσεις των πολιτικών. Παρέχει μια κεντρική πλατφόρμα για τη συλλογή και ανάλυση των αρχείων καταγραφής (logs), συσχετίζει δεδομένα από πολλαπλές πηγές (όπως server logs, firewall logs) και ενσωματώνει προηγμένες δυνατότητες ανίχνευσης απειλών μέσω του εντοπισμού ύποπτων μοτίβων και ασυνήθιστων συμπεριφορών. Η ΓΓΠΣΨΔ έχει δώσει πρόσβαση στην ΕΕΤΤ στο σύστημα αυτό και έτσι οι αρμόδιοι διαχειριστές της παρακολουθούν την υγεία των συστημάτων της που φιλοξενούνται στο G-Cloud, servers και λοιπών πόρων (π.χ. firewalls, application gateways). Το SIEM αποστέλλει στην ΕΕΤΤ μηνύματα σε πραγματικό χρόνο για περιστατικά ασφαλείας και αποθηκεύει events για τον εξοπλισμό.

Τα παραπάνω συστήματα παρακολούθησης ασφαλείας δημιουργούν αναφορές σχετικά με την απόδοσή τους, καθώς και τα σχετικά αρχεία καταγραφής. Προστατεύονται επαρκώς από μη εξουσιοδοτημένη πρόσβαση ενώ οι αλλαγές διαμόρφωσής τους επιτρέπονται μόνο από τους καθορισμένους εξουσιοδοτημένους διαχειριστές. Επίσης, παρέχουν ασφαλή διατήρηση των δεδομένων μέσω μηχανισμών κρυπτογράφησης[5]. Έτσι διασφαλίζουν ότι οι πληροφορίες που αποθηκεύονται ή μεταδίδονται παραμένουν εμπιστευτικές και προστατευμένες από μη εξουσιοδοτημένη πρόσβαση. Αυτό σημαίνει ότι ακόμα και αν κάποιος υποκλέψει τα δεδομένα δεν έχει τη δυνατότητα να τα διαβάσει.

4.2 Διαδικασίες Επίβλεψης των Συστημάτων Παρακολούθησης Ασφαλείας που χρησιμοποιεί η ΕΕΤΤ

Καθώς τα συστήματα της ΕΕΤΤ εξελίσσονται, πρέπει να εξελίσσονται και οι πρακτικές παρακολούθησής τους. Ενδεικτικά πρέπει να προσαρμόζονται τα εργαλεία, τα όρια και οι στρατηγικές ειδοποίησης, όπως απαιτείται. Αρμόδιο προσωπικό της Διεύθυνσης Ψηφιακής

δεδομένα που στέλνει και λαμβάνει μέσω αυτού του δικτύου προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και κατασκοπεία. Το VPN λειτουργεί δρομολογώντας τα δεδομένα στο Διαδίκτυο μέσω ενός VPN διακομιστή (server) που παρέχει στη συσκευή του χρήστη μια νέα διεύθυνση IP, αποκρύπτοντας έτσι την πραγματική τοποθεσία και την ταυτότητά του. Για λόγους ασφαλείας, οποιαδήποτε πρόσβαση στα εσωτερικά πληροφοριακά συστήματα της ΕΕΤΤ γίνεται μόνο μέσω σύνδεσης VPN. Επίσης, όταν οι εργαζόμενοι τηλεργάζονται πρέπει να συνδέονται στο VPN της ΕΕΤΤ, καθώς αυξάνει την ασφάλεια κατά την τηλεργασία.

[4] *Active Directory Server είναι ο διακομιστής που εκτελεί την υπηρεσία καταλόγου για τη διαχείριση χρηστών, υπολογιστών, ομάδων, πολιτικών και άλλων πόρων σε ένα δίκτυο βασισμένο σε Windows Server.*

[5] *Η κρυπτογράφηση είναι μια διαδικασία μετατροπής δεδομένων σε μια μη αναγνώσιμη μορφή, έτσι ώστε μόνο ο εξουσιοδοτημένος παραλήπτης να μπορεί να την αποκρυπτογραφήσει και να τη διαβάσει.*

Διακυβέρνησης ασχολείται με την κατάλληλη ρύθμιση των συστημάτων παρακολούθησης ασφαλείας που χρησιμοποιεί η ΕΕΤΤ.

Εφόσον τα συστήματα ασφαλείας είναι επαρκώς εγκατεστημένα και παραμετροποιημένα, τότε σε καθημερινή βάση τα αρμόδια στελέχη έχουν την ευθύνη να παρακολουθούν τα μηνύματα ειδοποίησης που αποστέλλουν τα συστήματα αυτά με αυτόματο τρόπο. Αλλιώς τα στελέχη πρέπει να εισέρχονται σε κάθε σύστημα ασφαλείας για να εντοπίζουν τυχόν χρήσιμη πληροφορία παρακολούθησης και τυχόν προβλήματα. Για παράδειγμα, ανασκοπούν τους dashboards των SIEM συστημάτων, οι οποίοι παρουσιάζουν σε κατανοητές οπτικές προβολές, τα συγκεντρωτικά δεδομένα και μετρήσεις, προκειμένου να κατανοήσουν και αναλύσουν την τρέχουσα κατάσταση των υπό παρακολούθηση συστημάτων.

4.3 Χειροκίνητη Επιθεώρηση με χρήση Δείγματος Αρχείου Καταγραφής Συμβάντων Ασφαλείας

Η παρακολούθηση ασφαλείας συστημάτων που έχουν ταξινομηθεί ως μη κρίσιμα και μη ευαίσθητα ενδέχεται να διενεργείται με τη χρήση χειροκίνητων επιθεωρήσεων / ελέγχων και όχι αυτόματα με τη χρήση συστημάτων ασφαλείας. Έτσι, σε περιπτώσεις που δεν χρησιμοποιούνται αυτοματοποιημένα συστήματα, τα αρχεία καταγραφής συμβάντων ασφαλείας μπορούν να υποβάλλονται σε δειγματοληψία και να ελέγχονται χειροκίνητα από διαχειριστές ή ελεγκτές, χρησιμοποιώντας ευρέως αποδεκτές μεθόδους δειγματοληψίας.

4.4 Αναφορά Συμβάντων Ασφαλείας

Όλα τα ύποπτα συμβάντα ασφαλείας ή τα πιθανά περιστατικά που αναδεικνύει η παρακολούθηση πρέπει να γνωστοποιούνται αμέσως στον Υπεύθυνο Ασφάλειας Πληροφοριακών Συστημάτων. Περισσότερες λεπτομέρειες για τη συγκεκριμένη διαδικασία διαχείρισης περιστατικών περιγράφονται στην Πολιτική Διαχείρισης Συμβάντων Ασφαλείας Πληροφοριών.

4.5 Παρακολούθηση Συστήματος μετά από Συμβάν Ασφαλείας

Τα πληροφοριακά συστήματα που έχουν υποστεί βλάβη από συμβάν ασφαλείας, πρέπει να παρακολουθούνται συνεχώς για ένα επαρκές χρονικό διάστημα (π.χ. 2 μήνες) μετά την ανάκτηση της λειτουργίας τους στο παραγωγικό περιβάλλον.

5. Διαχείριση και Προστασία Αρχείων Καταγραφής και σχετικών Αναφορών

5.1 Ταξινόμηση Αρχείων Καταγραφής και σχετικών αναφορών

Τα αρχεία καταγραφής συμβάντων ασφαλείας πρέπει να έχουν το κατάλληλο επίπεδο ταξινόμησης όσον αφορά την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των αποθηκευμένων πληροφοριών. Ειδικότερα, πρέπει να έχουν τουλάχιστον το ίδιο επίπεδο διαβάθμισης με το πληροφοριακό σύστημα από το οποίο προέρχονται (βλ. περισσότερες λεπτομέρειες αναφορικά με την ταξινόμηση των πληροφοριακών συστημάτων και εφαρμογών στην Πολιτική Διαχείρισης Πληροφοριακών Πόρων).

Ομοίως οι αναφορές που συντάσσονται με τα αποτελέσματα της παρακολούθησης πρέπει να έχουν το κατάλληλο επίπεδο ταξινόμησης όσον αφορά την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των παρεχόμενων πληροφοριών.

5.2 Προστασία Αρχείων Καταγραφής

Τα αρχεία καταγραφής προστατεύονται από μη εξουσιοδοτημένη χρήση ή αλλοίωση. Η πρόσβαση στα αρχεία καταγραφής παρέχεται μόνο κατόπιν ρητής εξουσιοδότησης και περιορίζεται σε εκείνους που την χρειάζονται για να εκτελέσουν τα υπηρεσιακά καθήκοντά τους, όπως στο προσωπικό που είναι υπεύθυνο για την ανάλυση, αξιολόγηση και αντιμετώπιση των καταγεγραμμένων συμβάντων.

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

Οι πληροφορίες σχετικά με τις δραστηριότητες χρηστών που εμπεριέχονται στα αρχεία καταγραφής, δεν πρέπει να γνωστοποιούνται σε τρίτους, εκτός εάν:

- *υπάρχει σαφής υποχρέωση για την ΕΕΤΤ (π.χ. λόγω αιτήματος δημοσίων αρχών στο πλαίσιο έρευνας που διενεργούν για το γενικό συμφέρον)*
- *η ΕΕΤΤ εκτιμά ότι είναι απαραίτητο να αποκαλύψει τέτοιες πληροφορίες, σύμφωνα με την ισχύουσα νομοθεσία*

Σε κάθε περίπτωση, απαγορεύεται η δημιουργία αντιγράφων και η αποθήκευση καταγεγραμμένων συμβάντων σε προσωπικά μέσα αποθήκευσης.

5.3 Αλλαγές Καταγραφής Ελέγχου και Λογαριασμοί με Αυξημένα Δικαιώματα

Οι διαχειριστές εφαρμογών, βάσεων δεδομένων, συστημάτων και / ή δικτύων δεν επιτρέπεται να διαγράφουν ή να απενεργοποιούν τα αρχεία καταγραφής, ακόμη και εκείνα των δικών τους δραστηριοτήτων.

Μηχανισμοί παρακολούθησης της ακεραιότητας των αρχείων ή εντοπισμού αλλαγών στα αρχεία καταγραφής μπορούν να χρησιμοποιούνται, όπου είναι εφικτό, για να διασφαλίζεται ότι τα υπάρχοντα δεδομένα καταγραφής δεν δύναται να αλλάξουν χωρίς τη δημιουργία ειδοποιήσεων. Η συχνή παρακολούθηση / επισκόπηση των αρχείων καταγραφής συμβάλει στη διατήρηση της λογοδοσίας των προνομιακών χρηστών με αυξημένα δικαιώματα.

5.4 Παρακολούθηση Χωρητικότητας Αποθήκευσης των Αρχείων Καταγραφής

Η χωρητικότητα αποθήκευσης (και οι σχετικές ρυθμίσεις διαμόρφωσης) των συστημάτων που φιλοξενούν τα αρχεία καταγραφής συμβάντων ασφαλείας, πρέπει να παρακολουθούνται περιοδικά, προκειμένου να διασφαλίζεται η επάρκεια των μέσων αποθήκευσης και να αποφεύγονται δυσλειτουργίες των συστημάτων ή / και απώλεια της δυνατότητας καταγραφής συμβάντων ασφαλείας.

5.5 Δημιουργία Αντιγράφων Αρχείων Καταγραφής

Τα αρχεία καταγραφής περιλαμβάνονται στα αντίγραφα ασφαλείας (back-ups) των συστημάτων. Οι απαιτήσεις δημιουργίας αντιγράφων ασφαλείας για τα αρχεία καταγραφής καθορίζονται σύμφωνα με την κρισιμότητα των πληροφοριακών συστημάτων. Η συχνότητα των αντιγράφων ασφαλείας των αρχείων καταγραφής ακολουθεί τους κανόνες της Πολιτικής Ασφαλείας της ΕΕΤΤ, ιδίως τις οδηγίες για τη λήψη και διαχείριση αντιγράφων ασφαλείας που περιγράφονται στην Πολιτική Διατήρησης Πληροφοριών. Σε κάθε περίπτωση, απαγορεύεται η δημιουργία αντιγράφων αρχείων καταγραφής σε προσωπικά μέσα αποθήκευσης.

5.6 Διατήρηση και Διαγραφή Αρχείων Καταγραφής

Η διατήρηση και διαγραφή των αρχείων καταγραφής ακολουθούν τους κανόνες που περιγράφονται στην Πολιτική Διατήρησης Πληροφοριών.

Ομοίως οι αναφορές που συντάσσονται με τα αποτελέσματα της παρακολούθησης διατηρούνται και καταστρέφονται σύμφωνα με τις σχετικές πολιτικές και προθεσμίες της ΕΕΤΤ.

Περισσότερες λεπτομέρειες αναφορικά με τη διατήρηση, προστασία και διαγραφή / καταστροφή των αρχείων καταγραφής και όλων των πληροφοριών και αναφορών παρακολούθησης συστημάτων αναφέρονται στην Πολιτική Διατήρησης Πληροφοριών.

6. Αλλαγές στην Πολιτική Παρακολούθησης Ασφάλειας Συστημάτων

Η ΕΕΤΤ αξιολογεί και επικαιροποιεί σε περιοδική βάση το σύνολο των πολιτικών και διαδικασιών που αφορούν στην παρακολούθηση ασφάλειας συστημάτων, ιδίως όταν λαμβάνουν χώρα σημαντικές αλλαγές στις λειτουργίες και υπηρεσιακές ανάγκες της, στις

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

κανονιστικές υποχρεώσεις και τεχνολογικές εξελίξεις ή προκύπτουν μεταβολές στο περιβάλλον των κυβερνοαπειλών.

»

2. **Εντέλλεται** την κοινοποίηση της παρούσας Απόφασης στο προσωπικό της ΕΕΤΤ μέσω μηνύματος ηλεκτρονικού ταχυδρομείου και την ανάρτησή της στη Γνωσιακή Πύλη (portal) προκειμένου να είναι εύκολα προσβάσιμη.
3. **Ορίζει** ότι η «*Πολιτική Παρακολούθησης Ασφάλειας Συστημάτων» πρέπει* να εφαρμόζεται υποχρεωτικά και απαρέγκλιτα από το 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 Παρακολούθησης Ασφάλειας Συστημάτων»*.
    - Τροποποιεί την *«Πολιτική Παρακολούθησης Ασφάλειας Συστημάτων»*, 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