Όνομα Οργανισμού

Πολιτική Ασφάλειας Δικτύου

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Ασφάλειας Δικτύου |
| **Δημιουργός:** |  |
| **Έκδοση:** | 1.0 |
| **Ημερομηνία Έκδοσης:** | ηη/μμ/χχχχ |
| **Εμπιστευτικότητα:** |  |
| **Ιδιοκτήτης:** |  |

Διανομή

| Ρόλος | Όνομα | Οργανισμός | Τοποθεσία | Αριθμός Αντιτύπων |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Καταγραφή Τροποποιήσεων

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Κατάσταση Έκδοσης | Έκδοση | Ημερομηνία | Ενέργειες από | Περιγραφή |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Αναφορές

|  |  |  |
| --- | --- | --- |
| **Αρ.** |  | **Αναφορά Εγγράφου** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

Υποστηρικτικό Υλικό

|  |  |
| --- | --- |
| **Αρ.** | **Αναφορά** |
| 1 |  |
| 2 |  |
| 3 |  |

Ειδικό Λεξιλόγιο

Οι όροι και συντμήσεις ορίζονται πιο κάτω:

| Όροι και συντμήσεις | Περιγραφή |
| --- | --- |
|  |  |
|  |  |
|  |  |

Πίνακας Περιεχομένων

[1. Εισαγωγή 4](#_Toc184731885)

[1.2 Σκοπός 4](#_Toc184731886)

[2. Πεδίο Εφαρμογής 4](#_Toc184731887)

[3. Πολιτική Ασφάλειας Δικτύου 4](#_Toc184731888)

[3.1. Ασφάλεια Δικτύου 4](#_Toc184731889)

[3.2. Ρόλοι και Ευθύνες 5](#_Toc184731890)

[3.2.1. Διαχειριστής της δικτυακής υποδομής 5](#_Toc184731891)

[4. Ανάλυση Κινδύνων 6](#_Toc184731892)

[5. Αρχιτεκτονική δικτύου 7](#_Toc184731893)

[6. Σχέδιο δικτύου - Αρχιτεκτονική 8](#_Toc184731894)

[7. Γενικές Απαιτήσεις για την ασφάλεια του δικτύου 9](#_Toc184731895)

[8. Διαχωρισμός και τμηματοποίηση του δικτύου 11](#_Toc184731896)

[9. Περιμετρική Ασφάλεια Δικτύου 11](#_Toc184731897)

[10. Απομακρυσμένη Ασφάλεια Δικτύου 12](#_Toc184731898)

[11. Προστασία από άρνηση παροχής υπηρεσιών 13](#_Toc184731902)

[12. Ασφαλή πρωτόκολλα επικοινωνίας/Κρυπτογράφηση 13](#_Toc184731903)

[13. Ανίχνευση και πρόληψη εισβολών και άλλων απειλών 14](#_Toc184731904)

[14. Αναθεώρηση 16](#_Toc184731905)

[15. Αναφορές 17](#_Toc184731906)

[Παράρτημα Α – Διάγραμμα Δικτύου [Όνομα Οργανισμού] 19](#_Toc184731907)

# Εισαγωγή

# Σκοπός

Το παρόν έγγραφο καθορίζει την Πολιτική Ασφάλειας Δικτύου του [Όνομα Οργανισμού] με σκοπό να καθοριστούν τα απαραίτητα οργανωτικά και τεχνικά μέτρα προς προστασία και υπεράσπιση των πληροφοριακών συστημάτων και πληροφοριών του [Όνομα Οργανισμού]. Στόχος της Πολιτικής είναι η διαφύλαξη της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των συστημάτων και πληροφοριών του [Όνομα Οργανισμού] καθώς και η συμμόρφωση του με τις σχετικές απαιτήσεις του Κανονισμού Κ.Δ.Π 389/2020 σε σχέση με την ασφάλεια δικτύου.

# Πεδίο Εφαρμογής

Η παρούσα Πολιτική Ασφάλειας Δικτύου εφαρμόζεται σε όλα τα δίκτυα του [Όνομα Οργανισμού], συμπεριλαμβανομένων των δικτύων που διαχειρίζονται τρίτα μέρη.

Βάσει της Απόφασης Κ.Δ.Π 245/2045 δίκτυα ενός Οργανισμού δύναται να είναι τα ξεχωριστά και λογικά τμηματοποιημένα δίκτυα υπολογιστών της συνολικής δικτυακής υποδομής ενός οργανισμού όπως:

* Φυσικά δίκτυα: συλλογή υπολογιστικών συσκευών που συνδέονται μεταξύ τους με κάποιο μέσο μετάδοσης π.χ. LAN (Local Area Networks), WAN (Wide Area Networks) και των MAN (Metropolitan Area Networks).
* Λογικά δίκτυα: εικονικά τμήματα εντός ενός φυσικού δικτύου, τα οποία δημιουργούνται με τη χρήση VLANs (Virtual Local Area Networks).
* Υποδικτύωση (Subnets): αναφέρεται στην πρακτική της διαίρεσης ενός δικτύου σε δύο ή μικρότερα δίκτυα.
* Zώνες δικτύου (network zones), τμήματα εντός ενός δικτύου που ορίζονται από διαφορετικές πολιτικές ασφαλείας, όπως DMZ (Demilitarized Zone).
* Απομακρυσμένα δίκτυα: Δίκτυα που επεκτείνουν τη συνδεσιμότητα του κυρίως δικτύου π.χ VPN.
* Ασύρματα δίκτυα: δίκτυα τα οποία παρέχουν συνδεσιμότητα μέσω ασύρματων πρωτοκόλλων (Wi-Fi).
* Δίκτυα επιχειρησιακής τεχνολογίας (OT): δίκτυα που υποστηρίζουν βιομηχανικά συστήματα ελέγχου (ICS) και άλλες επιχειρησιακές τεχνολογίες.

# Πολιτική Ασφάλειας Δικτύου

# Ασφάλεια Δικτύου

Η Δικτυακή υποδομή του [Όνομα Οργανισμού] πρέπει να προστατεύεται τόσο από τις εξωτερικές όσο και από τις εσωτερικές απειλές, προκειμένου να διασφαλίζεται η διαθεσιμότητα, η ακεραιότητα και η εμπιστευτικότητα των πληροφοριών του [Όνομα Οργανισμού].

Ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόζει και διατηρεί επαρκή μέτρα για να διασφαλίζεται ένα εύλογο επίπεδο εφεδρείας και υψηλής διαθεσιμότητας, ιδίως για τα συστήματα, τις υπηρεσίες και τις εφαρμογές ζωτικής σημασίας που επεξεργάζονται διαβαθμισμένες ή/και επιχειρησιακές πληροφορίες σύμφωνα με την απαίτηση NS6 της Απόφασης Κ.Δ.Π 389/2020.

# Ρόλοι και Ευθύνες

Το προσωπικό του [Όνομα Οργανισμού] πρέπει να γνωρίζει τους ρόλους και τις αρμοδιότητες του σε σχέση με την εν λόγω Πολιτική. Αυτές, καθώς επίσης και οποιαδήποτε συγκεκριμένη ευθύνη για την προστασία των ιδιαίτερων στοιχείων, ή την εκτέλεση των ιδιαίτερων διαδικασιών ή δραστηριοτήτων, όπως είναι η προστασία των δεδομένων, πρέπει απαραίτητα να προσδιοριστούν και να ανατεθούν σε χρήστες με τις απαραίτητες γνώσεις και δεξιότητες. Αυτές θα πρέπει να περιλαμβάνονται στις περιγραφές εργασίας του προσωπικού του [Όνομα Οργανισμού].

# Διαχειριστής της δικτυακής υποδομής

Όλα τα συστήματα δικτύου και δικτυακής ασφάλειας πρέπει να τυγχάνουν διαχείρισης από τον [Όνομα Οργανισμού] εξασφαλίζοντας τον ορθό διαχωρισμό καθηκόντων.

Ο διαχειριστής της δικτυακής υποδομής θα πρέπει να δημιουργήσει, να υλοποιήσει και να συντηρεί:

Σχέδιο Υλοποίησης Ασφαλούς Δικτύου. Το σχέδιο αυτό πρέπει να περιέχει:

* + πρότυπα και οδηγίες.
  + διαδικασίες για τη διαμόρφωση (αρχιτεκτονική) του δικτύου.
  + διαδικασίες για τη διαχείριση και πρόσβαση του δικτύου.
* Εγχειρίδιο Λειτουργίας Δικτύου. Το εγχειρίδιο αυτό πρέπει να περιέχει:
  + συνοπτικό διάγραμμα του δικτύου πληροφοριακών συστημάτων.
  + οδηγίες/ρυθμίσεις εγκατάστασης δικτυακού εξοπλισμού.
  + διαδικασίες για τη διαχείριση και πρόσβαση του δικτύου.
  + κατάλογο με τις κυριότερες εφαρμογές, σύντομη περιγραφή της λειτουργίας που επιτελεί η κάθε μια.
  + διαδικασίες για την παρακολούθηση του δικτύου.
  + κίνηση δικτύου φιλτράρετε σε επιθυμητό επίπεδο.
  + διαχωρισμό δικτύων [NS2].
  + εγχειρίδιο Άμεσης Αντιμετώπισης Περιστατικών Ασφαλείας
  + διαδικασίες που διασφαλίζουν την επιχειρησιακή συνέχεια (βλέπε *Πολιτική Επιχειρησιακής Συνέχειας*).
  + διαδικασίες αντικατάστασης εξοπλισμού και διαχείρισης αλλαγών
  + διαδικασίες δοκιμών δικτύου

Επιπρόσθετα, θα πρέπει να καθορίσει πρόγραμμα εκτέλεσης δοκιμών ασφάλειας όπως δοκιμές διείσδυσης (penetration testing), έλεγχοι ασφαλείας και εκτιμήσεις τρωτότητας (vulnerability management) του δικτύου. Αυτοί οι έλεγχοι θα πρέπει να διεξάγονται σε τακτά χρονικά διαστήματα (τουλάχιστον σε ετήσια βάση).

# Ανάλυση Κινδύνων

Οι κίνδυνοι που διατρέχουν οι δικτυακοί πόροι του [Όνομα Οργανισμού] θα πρέπει να αξιολογούνται σε τακτά χρονικά διαστήματα στα πλαίσια της Μεθοδολογίας Διαχείρισης Κινδύνου. Κατά τον σχεδιασμό των κανόνων και μηχανισμών ασφαλείας, λαμβάνονται υπόψη τα αποτελέσματα της αξιολόγησης κινδύνου, καθώς και οι συγκεκριμένες απειλές και κίνδυνοι που σχετίζονται με τον [Όνομα Οργανισμού].

Οι συσκευές δικτύου (routers, switches, εξυπηρετητές, firewall, συστήματα ανίχνευσης και προστασίας εισβολών, συστήματα ηλεκτρονικού ταχυδρομείου κλπ.) πρέπει να προσδιοριστούν με το κατάλληλο επίπεδο κινδύνου ανάλογα με τη κρισιμότητα τους. Στη συνέχεια, για την κάθε συσκευή θα πρέπει να προσδιοριστούν ρόλοι και προνόμια χρηστών που χρησιμοποιούν αυτές τις συσκευές.

# Αρχιτεκτονική δικτύου

Σύμφωνα με την Απόφαση Κ.Δ.Π. 389/2020, ο [Όνομα Οργανισμού] έχει σχεδιάσει και υλοποιήσει μια αρχιτεκτονική δικτύου για την εξασφάλιση του επιθυμητού επιπέδου ασφαλείας δικτύου, λαμβάνοντας υπόψη τις πρακτικές και τα μέτρα που αναφέρονται στα [NS2] – [NS7]. Κατά το σχεδιασμό της αρχιτεκτονικής δικτύου θα πρέπει να λαμβάνονται υπόψη οι ακόλουθες κατευθυντήριες αρχές:

* Το δίκτυο έχει σχεδιαστεί για υψηλή απόδοση και αξιοπιστία, προσαρμόζοντας τις ανάγκες της επιχείρησης. Τα σημεία αστοχίας να ελαχιστοποιούνται για τη διασφάλιση υψηλής διαθεσιμότητας μέσω μιας πολυεπίπεδης αρχιτεκτονικής άμυνας (“defense in depth”) .
* Στο δίκτυο έχουν υιοθετηθεί μηχανισμοί υψηλής διαθεσιμότητας (High Availability). Έχει διασφαλιστεί ότι η οποιαδήποτε διακοπή του δικτύου δεν θα υπερβαίνει τον μέγιστο αποδεκτό χρόνο διακοπής των πληροφοριακών συστημάτων ή/ και υπηρεσιών του [Όνομα Οργανισμού].
* Στο δίκτυο υπάρχει η δυνατότητα αναβάθμισης και επέκτασης (scalability).
* Εφεδρικοί μηχανισμοί και μέτρα διαθεσιμότητας εφαρμόζονται για τα κρίσιμα δίκτυα.
* Κατά το σχεδιασμό, λαμβάνεται υπόψη το απαιτούμενο επίπεδο ευελιξίας για μελλοντικές απαιτήσεις.
* Η τεκμηρίωση του σχεδιασμού δικτύου θα πρέπει να επαναλαμβάνεται τακτικά για ενημέρωση.
* Το δίκτυο έχει καταμεριστεί σε απομονωμένους λογικούς δικτυακούς τομείς με βάση τη λειτουργικότητα. Ο καταμερισμός του δικτύου σε απομονωμένους λογικούς τομείς πρέπει να βασιστεί στα ακόλουθα:
  + 1. Ιδεατά τοπικά δίκτυα (VLans): Καταμερισμός σε ομάδες υπηρεσιών πληροφορικής, χρηστών και πληροφοριακών συστημάτων.
    2. Οι εξυπηρετητές διαφορετικού τύπου/φύσεως (όπως application, database, webserver κ.τ.λ.) πρέπει να διαχωρίζονται σε ξεχωριστές ζώνες δικτύου.
* Οι ζώνες DMZ εφαρμόζονται για δημοσίευση επιχειρησιακών υπηρεσιών. Οποιεσδήποτε διαδικτυακές υπηρεσίες του [Όνομα Οργανισμού] έχουν τοποθετηθεί σε ζώνη DMZ (Demilitarized Zone)
* Λαμβάνεται υπόψη κατά τον σχεδιασμό η απομόνωση ευαίσθητων συστημάτων και πληροφοριών (π.χ. συστήματα που επεξεργάζονται εμπιστευτικά δεδομένα απομονώνονται) από το υπόλοιπο δίκτυο.
* Οι αλλαγές στο δίκτυο συμβαδίζουν με την υπάρχουσα αρχιτεκτονική και τεκμηρίωση.
* Έχουν εφαρμοστεί συστήματα ταξινόμησης και επισήμανσης με βάση τις διεθνείς βέλτιστες πρακτικές, όπως το πρωτόκολλο «Traffic Light Protocol». Τουλάχιστον, ο Οργανισμός εφαρμόζει διάκριση μεταξύ των δημόσιων, ιδιωτικών και διαβαθμισμένων πληροφοριών.

# Σχέδιο δικτύου - Αρχιτεκτονική

Η δικτυακή αρχιτεκτονική του [Όνομα Οργανισμού] απεικονίζεται σε ένα διάγραμμα δικτύου που παρέχει λεπτομερείς πληροφορίες για τα διάφορα επίπεδα της αρχιτεκτονικής, τα στοιχεία που περιλαμβάνει κάθε επίπεδο, τα βασικά χαρακτηριστικά τους, τα πιθανά σημεία αστοχίας και τα σημεία όπου είναι ενεργοποιημένη η παρακολούθηση.

Τα διαγράμματα του [Όνομα Οργανισμού] χαρακτηρίζονται και αναλόγως διαχειρίζονται ως πληροφορίες του υψηλότερου επιπέδου διαβάθμισης πληροφοριών (όπως αναφέρεται στο [DS2]) σύμφωνα με την εμπιστευτικότητα τους.

Η πρόσβαση στα διαγράμματα δικτύου ελέγχεται και περιορίζεται σε εξουσιοδοτημένο προσωπικό.

Για περαιτέρω πληροφορίες σχετικά με το διάγραμμα δικτύου του [Όνομα Οργανισμού] , ανατρέξτε στο Παράρτημα Α της παρούσας Πολιτικής.

* + Ιδεατά τοπικά δίκτυα προστατεύονται από εσωτερικά firewalls και η πλοήγηση σε αυτά είναι φιλτραρισμένη.
  + Απομακρυσμένη Πρόσβαση (remote access).
  + Σύνδεση Τρίτων Μερών.

# Γενικές Απαιτήσεις για την ασφάλεια του δικτύου

* Όλος ο εξοπλισμός διαμορφώνεται σύμφωνα με τις βέλτιστες πρακτικές διαμόρφωσης (Hardening) του εκάστοτε κατασκευαστή.
* Το δίκτυο ελέγχεται και προστατεύεται. Η σύνδεση μη εξουσιοδοτημένων πληροφοριακών συστημάτων και χρηστών στο δίκτυο του [Όνομα Οργανισμού] παρεμποδίζεται με τα απαραίτητα τεχνικά μέτρα. Συστήνεται η χρήση τεχνολογίας ελέγχου δικτυακής πρόσβασης τύπου ΝΑC (Network Access Control)
* Οι ηλεκτρονικοί υπολογιστές, ελέγχονται εάν πληρούν τις προϋποθέσεις/κριτήρια ασφάλειας πριν συνδεθούν στο δίκτυο. Απαγορεύεται η σύνδεση μη εξουσιοδοτημένου εξοπλισμού στο δίκτυο.
* Όλος ο εξοπλισμός ο οποίος είναι συνδεδεμένος στο δίκτυο του [Όνομα Οργανισμού] είναι συγχρονισμένος σε κεντρικό σύστημα πρωτοκόλλου ώρας δικτύου (ntp) για τον ομοιόμορφο καθορισμό της ώρας / ημερομηνίας.
* Η πρόσβαση σε οποιοδήποτε πληροφοριακό σύστημα του δικτύου ελέγχεται.
* Οι διαχειριστικές ενέργειες (administrative tasks) διενεργούνται αποκλειστικά και μόνο μέσω των κατάλληλων διαχειριστικών συστημάτων και εργαλείων που έχουν οριστεί για αυτό το σκοπό.
* Η δημιουργία και η χρήση κοινών λογαριασμών για χρήση σε πληροφοριακό σύστημα του δικτύου αποφεύγεται.
* Μόνο εξουσιοδοτημένος χρήστης μπορεί να κάνει αλλαγές σε ρυθμίσεις, παραμέτρους, διευθύνσεις IP σε πληροφοριακό σύστημα δικτύου ή ηλεκτρονικό υπολογιστή.
* Η πρόσβαση με δικαιώματα διαχειριστή στις δικτυακές συσκευές πραγματοποιείται αυστηρά μέσω μηχανισμών αυθεντικοποίηση πολλαπλών παραγόντων (MFA).
* Απαγορεύεται η χρησιμοποίηση μη εξουσιοδοτημένου λογισμικού.
* Τα πληροφοριακά συστήματα και οι υπολογιστές έχουν εγκατεστημένο και ενημερωμένο λογισμικό αντιμετώπισης κακόβουλων λογισμικών πριν συνδεθούν στο δίκτυο.
* Τα πληροφοριακά συστήματα και οι υπολογιστές έχουν τις τελευταίες ενημερώσεις και αναβαθμίσεις (updates, patches) πριν συνδεθούν στο δίκτυο του [Όνομα Οργανισμού]
* Η καταγραφή ενεργειών (logs) των πληροφοριακών συστημάτων δικτύου και άλλων κρίσιμων συστημάτων καταγράφονται και συλλέγονται σε κεντρικό σύστημα ανάλυσης δεδομένων. Οι καταγραφές ενεργειών (logs) ελέγχονται σε τακτά χρονικά διαστήματα. Όσον αφορά τις καταγραφές ενεργειών (logs) των domain controllers, firewalls IDS, routers/switches και άλλων υψηλής σημασίας/ κρισιμότητας συστημάτων, ελέγχονται όπου είναι δυνατό σε καθημερινή βάση.
* Όπου χρειάζεται απομακρυσμένη πρόσβαση (εντός δικτύου) σε πληροφοριακά συστήματα γίνεται με ασφαλή πρωτόκολλα όπως ssh, https.
* Ο οργανισμός έχει θεσπίσει ασφαλή πρωτόκολλα για τη διευκόλυνση της διακίνησης πληροφοριών μεταξύ σημείων δικτύου, εφαρμογών και συστημάτων για την διασφάλιση της εμπιστευτικότητας και ακεραιότητας των πληροφοριών.
* Περιττά πρωτόκολλα και υπηρεσίες απενεργοποιούνται και αποκόπτονται σε επίπεδο δικτύου.
* Ασύρματα δίκτυα απενεργοποιούνται , εκτός στο guest Vlan που δεν είναι συνδεδεμένο με το εταιρικό δίκτυο του [Όνομα Οργανισμού]
* Ο [Όνομα Οργανισμού] έχει αναγνωρίσει τον εξοπλισμό που εκτελεί δραστηριότητες ασφάλειας σε κάθε επίπεδο και έχει εφαρμόσει πολιτικές και κανόνες ασφαλείας υιοθετώντας αρνητική λογική και υπηρεσίες που δεν χρειάζονται (περιττές) είναι απενεργοποιημένες.
* Flood Guards πρέπει να χρησιμοποιούνται προκειμένου να αποτρέπουν τις διαδικτυακές επιθέσεις άρνησης Υπηρεσιών (Distributed Denial of Service Attacks -DDoS).
* Ο [Όνομα Οργανισμού] διατηρεί κατάλληλο διαχωρισμό και τμηματοποίηση του δικτύου, προκειμένου να διασφαλιστεί - λογικός ή/και φυσικός (όπου αυτό είναι εφικτό) - διαχωρισμός των δικτύων πληροφοριών σύμφωνα με τη παράγραφο 12 της παρούσας Πολιτικής.
* Η υπηρεσία port security πρέπει να είναι ενεργοποιημένη σε όλα τα switches, ενώ οι μη χρησιμοποιούμενες θύρες πρέπει να απενεργοποιούνται.
* Στους routers, τα interfaces και τα πρωτόκολλα δρομολόγησης είναι απενεργοποιημένα εκτός αν λαμβάνονται άλλα αντισταθμιστικά μέτρα (compensating controls).
* Οι αλλαγές που πραγματοποιούνται στον εξοπλισμό της περιμέτρου ακολουθούν τη πολιτική Διαχείρισης Αλλαγών και Διαμόρφωσης
* Ο [Όνομα Οργανισμού] έχει εγκαταστήσει host-based firewalls ή εργαλεία port filtering, τα οποία εφαρμόζουν κανόνες που απορρίπτουν όλη την κίνηση, εκτός από τις υπηρεσίες, τα πρωτόκολλα και τις θύρες που έχουν ρητά εξουσιοδοτηθεί.
* Το IPv6 όταν δεν χρησιμοποιείται, απενεργοποιείται.

# Διαχωρισμός και τμηματοποίηση του δικτύου

Ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόσει και διατηρήσει κατάλληλο διαχωρισμό και τμηματοποίηση του δικτύου, προκειμένου να διασφαλιστεί ο λογικός (μέσω λογικών δικτύων) ή/και φυσικός (μέσω φυσικών μέσων, όπως ξεχωριστά φυσικά δίκτυα) - διαχωρισμός των δικτύων πληροφοριών. Κατά τον σχεδιασμό, την εφαρμογή και τη διατήρηση των μέτρων διαχωρισμού και τμηματοποίησης του δικτύου, ο οργανισμός λαμβάνει υπόψη τους διάφορους τομείς λειτουργικής δραστηριότητας του οργανισμού, τη φύση και την έκταση των δεδομένων που υποβάλλονται σε επεξεργασία στο πλαίσιο συγκεκριμένων επιχειρηματικών δραστηριοτήτων, προκειμένου να διασφαλίζεται επαρκής διαχωρισμός.

* Η προστασία των κρίσιμων συστημάτων είναι πολυεπίπεδη.
* Το εσωτερικό δίκτυο του [Όνομα Οργανισμού] είναι διαχωρισμένο και τμηματοποιημένο λαμβάνοντας υπόψιν την κρισιμότητα, το επίπεδο διαβάθμισης των δεδομένων που υποβάλλονται σε επεξεργασία και την λειτουργία των πόρων του [Όνομα Οργανισμού].
* Τα κρίσιμα συστήματα τοποθετούνται σε διακριτά υποδίκτυα από τα υπόλοιπα συστήματα, γίνεται φιλτράρισμα της δικτυακής κίνησης (traffic filtering) και περιορίζεται η ροή της πληροφορίας μεταξύ των υποδικτύων στην απολύτως απαραίτητη για τις επιχειρησιακές ανάγκες του [Όνομα Οργανισμού].
* Κατά το σχεδιασμό της αρχιτεκτονικής του δικτύου έχει υιοθετηθεί ο διαχωρισμός και η τμηματοποίηση του δικτύου του [Όνομα Οργανισμού] με τη χρήση εικονικών δικτύων (VLAN), λαμβάνοντας υπόψη την κρισιμότητα των δεδομένων και άλλα κριτήρια που ο [Όνομα Οργανισμού] κρίνει ως απαραίτητα σύμφωνα με την απαίτηση NS2 της Απόφασης Κ.Δ.Π 389/2020. Όπου είναι δυνατό, υλοποιείται φυσικός διαχωρισμός.
* Οι τομείς έρευνας και ανάπτυξης, διοίκησης, κεντρικής υποδομής πληροφοριών και των δημόσια διαθέσιμων (στο διαδίκτυο) εφαρμογών και συστημάτων είναι διαχωρισμένοι σε διαφορετικές δικτυακές ζώνες.
* Ο [Όνομα Οργανισμού] διενεργεί τακτικούς ελέγχους και δοκιμές για την επιβεβαίωση υλοποίησης των σχετικών κανόνων και της ύπαρξης διαχωρισμού σε όλα τα επίπεδα.
* Υλοποιείται διαχωρισμός ανάμεσα στις λειτουργίες ασφάλειας από τις υπόλοιπες με την δημιουργία περιβάλλοντος απομόνωσης (isolation boundary).

# Περιμετρική Ασφάλεια Δικτύου

Σύμφωνα με την Απόφαση Κ.Δ.Π. 389/2020 ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόσει και διατηρήσει μέτρα ασφάλειας δικτύου με σκοπό την προστασία της περιμέτρου του δικτύου από εξωτερικές απειλές λαμβάνοντας υπόψη ότι η ασφάλεια περιμέτρου αποτελεί ένα μόνο συγκεκριμένο επίπεδο σε μια πολυεπίπεδη αρχιτεκτονική άμυνας. Για την προστασία από επιθέσεις στο δίκτυο, ο οργανισμός λαμβάνει υπόψη τις ειδικές για τον οργανισμό, απειλές και τις ειδικές για τον τομέα, απειλές και κινδύνους για το δίκτυο. Συγκεκριμένα ο Οργανισμός έχει θεσπίσει τα πιο κάτω:

* Ο [Όνομα Οργανισμού] έχει εγκατεστημένο firewall το οποίο να λειτουργεί ως σημείο διεπαφής ανάμεσα στο τοπικό δίκτυο και το εξωτερικό δίκτυο. Η συνολική δικτυακή κίνηση, είτε εισερχόμενη είτε εξερχόμενη, διέρχεται και ελέγχεται από το firewall.
* Ο [Όνομα Οργανισμού] επιτρέπει συνδέσεις προς εξωτερικά δίκτυα ή συστήματα μόνο μέσω των διαχειριζόμενων διεπαφών των στοιχείων που έχουν αναγνωριστεί στη λογική περίμετρο, σύμφωνα με την υλοποιημένη αρχιτεκτονική.
* Ο εξοπλισμός περιμέτρου είναι διαμορφωμένος ώστε ως προεπιλεγμένη ενέργεια να πραγματοποιεί απόρριψη οποιασδήποτε μη εγκεκριμένης δικτυακής κίνησης, μέσω της χρήσης κανόνα “Deny All / Deny By Default” και να επιτρέπει την επικοινωνία μόνο μέσω σαφώς καθορισμένων κανόνων.
* Ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόζει και διατηρεί μέτρα ασφάλειας δικτύου (π.χ. Firewall, Συστήματα Εντοπισμού και Πρόληψης Εισβολών (IDS/IPS), διαχωρισμός δικτύου σε υποδίκτυα, χρήση VPN, κ.α.) με σκοπό την προστασία της περιμέτρου του δικτύου από εξωτερικές απειλές και τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που βρίσκονται στο εσωτερικό δίκτυο.
* Ελεγχόμενη πρόσβαση και παρακολούθηση των ενεργειών και τήρηση αρχείων καταγραφής.

# Απομακρυσμένη Ασφάλεια Δικτύου

Ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόζει και διατηρεί μέτρα ασφάλειας δικτύου με σκοπό την διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που βρίσκονται στο εσωτερικό δίκτυο από εξωτερικές προσβάσεις.

Σε κάθε περίπτωση στοιχεία τα οποία χρειάζεται να είναι προσβάσιμα από το εξωτερικό δίκτυο, είναι διαχωρισμένα από το εσωτερικό δίκτυο. Οι συνδέσεις σε εξωτερικά δίκτυα ή συστήματα γίνονται μόνο από τις διαχειριζόμενες διεπαφές των στοιχείων που έχουν αναγνωριστεί στην λογική περίμετρο (σύμφωνα με την υλοποιημένη αρχιτεκτονική).

Όλη η δικτυακή κίνηση του [Όνομα Οργανισμού] , από και προς το διαδίκτυο, διέρχεται από αυθεντικοποιημένο διακομιστή μεσολάβησης επιπέδου εφαρμογής, ο οποίος έχει ρυθμιστεί να αποτρέπει μη εξουσιοδοτημένες συνδέσεις.

Για την πραγματοποίηση απομακρυσμένης πρόσβασης χρησιμοποιείται VPN (Virtual Private Network) και ενσωματώνεται με την υποδομή ΑΑΑ (Authentication, Authorization, and Accounting) του [Όνομα Οργανισμού] .

Για την πραγματοποίηση απομακρυσμένης πρόσβασης στο εσωτερικό δίκτυο του [Όνομα Οργανισμού] χρησιμοποιείται VPN (Virtual Private Network), αυθεντικοποίηση δύο παραγόντων (2-factor authentication) και σύγχρονοι αλγόριθμοι κρυπτογράφησης.



# Προστασία από άρνηση παροχής υπηρεσιών

Ο [Όνομα Οργανισμού] διασφαλίζει την προστασία των οργανωτικών πόρων από επιθέσεις άρνησης παροχής υπηρεσιών, και ότι δεν επηρεάζονται οι νόμιμες δραστηριότητες παροχής υπηρεσιών. Θεσπίζει, εφαρμόζει και διατηρεί επαρκή προστασία από άρνηση παροχής υπηρεσιών και διανεμημένη άρνηση παροχής υπηρεσιών, προκειμένου να διασφαλίζεται η έγκαιρη και ποιοτική παροχή της υπηρεσίας σε εξουσιοδοτημένους και επικυρωμένους χρήστες και να διατηρείται σταθερό επίπεδο παραγωγικότητας.

Κατά τον σχεδιασμό των σχετικών μέτρων προστασίας, ο οργανισμός λαμβάνει υπόψη τα ακόλουθα:

* Οι πόροι που είναι προσβάσιμοι από εξωτερικά δίκτυα είναι διαχωρισμένοι από το υπόλοιπο δίκτυο του [Όνομα Οργανισμού] .
* Για κάθε ένα από τα κρίσιμα στοιχεία ενεργητικού, έχουν αναγνωρισθεί και καταγραφεί οι τρόποι με τους οποίους μπορεί να υπερφορτωθεί, καθώς και τα όρια (σε bandwidth, επεξεργαστική ισχύ και αποθηκευτικό χώρο) πέρα από τα οποία η διαθεσιμότητα του στοιχείου είναι επισφαλής.
* Η υποδομή του [Όνομα Οργανισμού] είναι κατάλληλα διαμορφωμένη ώστε να διασφαλίζεται η διαθεσιμότητα των πόρων του και η προστασία έναντι επιθέσεων άρνησης παροχής υπηρεσιών.
* Ο [Όνομα Οργανισμού] εφαρμόζει τη χρήση του domain registrar locking, προκειμένου να εμποδίζει ενδεχόμενα συμβάντα άρνησης παροχής υπηρεσιών λόγω μη εξουσιοδοτημένης διαγραφής, μεταφοράς ή αλλοίωσης της εγγραφής του domain του.
* Τα συστήματα παρακολούθησης της διαθεσιμότητας των κρίσιμων υπηρεσιών του [Όνομα Οργανισμού] ανιχνεύουν πιθανές επιθέσεις άρνησης παροχής υπηρεσιών και να στέλνουν ειδοποίηση σε πραγματικό χρόνο.
* Ο [Όνομα Οργανισμού] διαθέτει τουλάχιστον δύο (2) εξυπηρετητές DNS, οι οποίοι είναι φυσικά και λογικά προστατευμένοι και βρίσκονται σε διαφορετικές τοποθεσίες.
* Ο [Όνομα Οργανισμού] δεν επιτρέπει την χρήση source routing.

# Ασφαλή πρωτόκολλα επικοινωνίας/Κρυπτογράφηση

Με στόχο να διασφαλιστούν τα κατάλληλα πρωτοκόλλα επικοινωνίας μεταξύ των πόρων του δικτύου ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόζει και διατηρεί ασφαλή πρωτόκολλα για τη διευκόλυνση της διακίνησης πληροφοριών μεταξύ σημείων δικτύου, εφαρμογών και συστημάτων, προκειμένου να διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των πληροφοριών κατά τη μεταφορά τους, και να αποτρέπονται επιθέσεις και απειλές στο δίκτυο, όπως για παράδειγμα υποκλοπές επικοινωνιών. Ο οργανισμός λαμβάνει υπόψη μέτρα ασφάλειας που υποστηρίζονται από κρυπτογραφικά μέσα, όπως αυτά ορίζονται στο μέτρο [AM5] ανάλογα πάντα με το επιδιωκόμενο επίπεδο τεχνολογίας. Πιο συγκεκριμένα:

* Για ανταλλαγή πληροφοριών υψηλής κρισιμότητας, ο [Όνομα Οργανισμού] χρησιμοποιεί σύγχρονα πρωτόκολλα επικοινωνίας που υποστηρίζουν ισχυρή κρυπτογράφηση (π.χ. Hypertext Transfer Protocol Secure (HTTPS), Internet Protocol security (IPsec), Transport Layer Security (TLS) / Secure Sockets Layer (SSL)). Σε περιπτώσεις που χρησιμοποιούνται πρωτόκολλα επικοινωνίας που δεν υποστηρίζουν ισχυρή κρυπτογράφηση, οι επικοινωνίες υλοποιούνται σε συνδυασμό με δεύτερο μέτρο ασφάλειας (π.χ. SSH, SSL ή Internet Protocol Security (IPsec)).
* Τα δίκτυα του [Όνομα Οργανισμού] χρησιμοποιούν τα πιο πρόσφατα και ασφαλή πρωτόκολλα, όπως το SFTP ή το HTTPS, για την ασφαλή μεταφορά δεδομένων.
* Τα δίκτυα του [Όνομα Οργανισμού] χρησιμοποιούν ασφαλή πρωτόκολλα δρομολόγησης (secure routing protocols) ή στατικές διαδρομές (static routes) για την προστασία της εσωτερικής τους δομής.
* Ο [Όνομα Οργανισμού] επανεξετάζει και να αναλύει τους πόρους και τα στοιχεία ενεργητικού του ώστε να καθορίσει ποια πρωτόκολλα, θύρες και υπηρεσίες είναι απαραίτητα για την ορθή και αποτελεσματική λειτουργία τους. Οτιδήποτε δεν κρίνεται απαραίτητο απενεργοποιείται (π.χ. Bluetooth, FTP, peer-to-peer κ.α.)
* Ο [Όνομα Οργανισμού] διασφαλίζει ότι η ανταλλαγή πληροφοριών μέσω APIs πραγματοποιείται με κατάλληλο σχεδιασμό, παραμετροποίηση, υλοποίηση και λειτουργία, ώστε να πληροί τα καθορισμένα επίπεδα ασφάλειας, εφαρμόζοντας βέλτιστες διεθνείς πρακτικές (π.χ. API OWASP Top Ten).
* Ο [Όνομα Οργανισμού] εξασφαλίζει την εμπιστευτικότητα των δεδομένων είτε με κρυπτογράφηση σε επίπεδο καναλιού είτε με κρυπτογράφηση σε επίπεδο δεδομένων όταν γίνεται μεταφορά σε διαφορετικά δίκτυα, ακόμα και στο εσωτερικό του δίκτυο με στόχο να προστατευθούν από ανεπιθύμητη πρόσβαση, ακόμα και αν πέσουν σε λάθος χέρια.
* Ο [Όνομα Οργανισμός] διασφαλίζει ότι απενεργοποιούνται κατ’ ελάχιστο τα εξής:

α) Η εισερχόμενη και εξερχόμενη επικοινωνία προς το εξωτερικό δίκτυο στις θύρες TCP 445 (SMB), UDP 137 (NetBIOS Name Resolution), UDP 138 (NetBIOS Datagram Service) και TCP 139 (NetBIOS Session Service).

β) Οι εισερχόμενες συνδέσεις SMB στην TCP θύρα 445 σε συστήματα που δεν φιλοξενούν κοινόχρηστο περιεχόμενο (shares).

γ) Οι εκδόσεις SMBv1 και SMBv2 στο εσωτερικό δίκτυο.

* Η χρήση πρωτοκόλλων μεταφοράς, όπως SMB και SNTP, επιτρέπεται μόνο όταν είναι απολύτως αναγκαία και έπειτα από τη δέουσα ανάλυση και παραμετροποίησή τους.

# Ανίχνευση και πρόληψη εισβολών και άλλων απειλών

Ο [Όνομα Οργανισμού] στα πλαίσια μετριασμού του κινδύνου από απόπειρα εξωτερικής εισβολής υλοποιεί συστήματα ανίχνευσης εισβολών (IDS) και τα συστήματα πρόληψης εισβολών (IPS) εντός DMZ για την ανάλυση της πληροφορίας που ανταλλάσσεται με το εξωτερικό δίκτυο, για πιο άμεσο εντοπισμό σχετικών επιθέσεων μέσω της χρήσης υπογραφών, ανάλυσης κυκλοφορίας ή άλλων μηχανισμών.

Επιπρόσθετα στα πλαίσια σχεδιασμού των διαδικασιών ανίχνευσης και πρόληψης εισβολών, ο οργανισμός πρέπει να εξετάσει το ενδεχόμενο αυτόματης ενεργοποίησης άμεσων μηχανισμών για λήψη κατάλληλων ενεργειών για την αντιμετώπιση συμβάντων σύμφωνα με την απαίτηση EIM2 της Απόφασης Κ.Δ.Π 389/2020.

Εφεδρικά αντίγραφα ασφαλείας των αρχείων διαμόρφωσης πρέπει να λαμβάνονται σύμφωνα με την πολιτική Επιχειρησιακής Συνέχειας του [Όνομα Οργανισμού] και έκτακτα πριν από κάθε αλλαγή. Το ιστορικό των αντιγράφων αυτών διατηρείται για εύλογο χρονικό διάστημα.

# Αναθεώρηση

Τα έγγραφα σχετικά με την Ασφάλεια Δικτύου θα πρέπει να επανεξετάζονται και να αναθεωρούνται τουλάχιστον ετησίως ή σε περίπτωση σημαντικών αλλαγών στο περιβάλλον του [Όνομα Οργανισμού] (π.χ. όσον αφορά την οργανωτική δομή, τις επιχειρηματικές δραστηριότητες και τις τάσεις της αγοράς, τις νομικές, κανονιστικές απαιτήσεις και τις απαιτήσεις συμμόρφωσης, την εφαρμογή νέων συστημάτων, τους νέους κινδύνους, τις αναδυόμενες απειλές κλπ.).

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Ασφάλεια Δικτύου | NS1 | Ασφάλεια Περιμέτρου | Να διασφαλιστεί ότι η διεπαφή του τοπικού δικτύου με το εξωτερικό δίκτυο προστατεύεται από επιθέσεις, απειλές και άλλες εκούσιες ή ακούσιες ενέργειες με δυνητικά αρνητικές επιπτώσεις. |
| Ασφάλεια Δικτύου | NS2 | Διαχωρισμός και τμηματοποίηση του δικτύου | Να εξασφαλιστεί ο διαχωρισμός του λογικού δικτύου, σύμφωνα με τις επιχειρηματικές λειτουργίες, και να απόφευχθεί η εξάπλωση κακόβουλων στοιχείων. |
| Ασφάλεια Δικτύου | NS3 | Προστασία από άρνηση παροχής υπηρεσιών | Να διασφαλιστεί η προστασία των οργανωτικών πόρων από επιθέσεις άρνησης παροχής υπηρεσιών, και ότι δεν επηρεάζονται οι νόμιμες δραστηριότητες παροχής υπηρεσιών. |
| Ασφάλεια Δικτύου | NS4 | Ασφαλή πρωτόκολλα επικοινωνίας | Να διασφαλιστούν κατάλληλα πρωτοκόλλα επικοινωνίας προκειμένου να επιτευχθεί ασφαλής επικοινωνία μεταξύ των πόρων του δικτύου. |
| Ασφάλεια Δικτύου | NS5 | Έλεγχος πρόσβασης στο δίκτυο | Να εξασφαλιστεί ότι η πρόσβαση στο λογικό δίκτυο από εξωτερικά και εσωτερικά συστήματα ασφαλίζεται κατάλληλα, ώστε μόνο τα εξουσιοδοτημένα πρόσωπα να μπορούν να έχουν πρόσβαση σε οργανωτικούς πόρους. |
| Ασφάλεια Δικτύου | NS7 | Ανίχνευση και πρόληψη εισβολών | Να διασφαλιστεί η ανίχνευση και η πρόληψη από εξωτερικές απόπειρες εισβολής και επιθέσεις ασφάλειας. |

# Παράρτημα Α – Διάγραμμα Δικτύου [Όνομα Οργανισμού]

*Το παρών διάγραμμα είναι εικονικό. Παρακαλείστε να το αλλάξετε με αυτό που αντικατοπτρίζει τον Οργανισμό σας.*

