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](#_Toc158630581)

[2. Αποστολή 4](#_Toc158630582)

[2.1. Πεδίο Εφαρμογής 4](#_Toc158630583)

[3. Σκοπός 4](#_Toc158630584)

[4. Ευθύνες Προσωπικού 4](#_Toc158630585)

[5. Πολιτική Ασφάλειας Δικτύου 4](#_Toc158630586)

[5.1. Ασφάλεια Δικτύου 4](#_Toc158630587)

[5.2. Ρόλοι και Ευθύνες 5](#_Toc158630588)

[5.3. Διαχειριστής της δικτυακής υποδομής 5](#_Toc158630589)

[5.4. Ανάλυση Κινδύνων 5](#_Toc158630590)

[5.5. Απαιτήσεις για την ασφάλεια του δικτύου 6](#_Toc158630591)

[5.6. Αρχιτεκτονική δικτύου 7](#_Toc158630592)

[5.6.1 Σχέδιο δικτύου - Αρχιτεκτονική 8](#_Toc158630593)

[5.7. Εσωτερική Ασφάλεια Δικτύου 9](#_Toc158630594)

[5.8. Περιμετρική Ασφάλεια Δικτύου 10](#_Toc158630595)

[5.8.1 Πρωτόκολλα Ασφάλειας Δικτύου 10](#_Toc158630599)

[5.8.2 Κρυπτογράφηση 11](#_Toc158630600)

[5.8.3 Απειλές 11](#_Toc158630601)

[5.8.4 Στοιχεία Ενεργητικού 13](#_Toc158630602)

[Παράρτημα Α – Διάγραμμα Δικτύου [Όνομα Οργανισμού] 14](#_Toc158630603)

# Εισαγωγή

Το έγγραφο αυτό καθορίζει την Πολιτική Ασφάλειας Δικτύου του [Όνομα Οργανισμού].

# Αποστολή

Η αποστολή του [Όνομα Οργανισμού] σε σχέση με την ασφάλεια δικτύου είναι η συμμόρφωση του με τις σχετικές απαιτήσεις του Κανονισμού Κ.Δ.Π 389/2020, για την εκπλήρωση της ευρύτερης αποστολής του Οργανισμού που είναι [Αποστολή Οργανισμού].

# Πεδίο Εφαρμογής

Η εν λόγω Πολιτική εφαρμόζεται σε όλες τις επιχειρησιακές μονάδες του [Όνομα Οργανισμού], που έχουν άμεση ή έμμεση σχέση με συστήματα ή πληροφορίες.

Η Πολιτική συμπεριλαμβάνει όλα τα συστήματα και πληροφορίες του [Όνομα Οργανισμού].

Ο [Όνομα Οργανισμού] πρέπει να υιοθετεί πρόγραμμα ελέγχου Ασφάλειας Πληροφοριών που να στοχεύει στον εντοπισμό μη συμμόρφωσης με το θεσμικό πλαίσιο και την Πολιτική Ασφάλειας Πληροφοριών. Το πρόγραμμά αυτό πρέπει να είναι σε ετήσια βάση και οι έλεγχοι της ασφάλειας των συστημάτων πρέπει να διενεργούνται τόσο από τις Μονάδες Ελέγχου του [Όνομα Οργανισμού] αλλά και από ανεξάρτητους οργανισμούς.

# Σκοπός

Ο σκοπός της Πολιτικής είναι να προστατεύει και να υπερασπίζεται τα πληροφοριακά συστήματα και πληροφορίες του [Όνομα Οργανισμού]. Στόχος της Πολιτικής είναι η διαφύλαξη της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των συστημάτων και πληροφοριών του [Όνομα Οργανισμού].

# Ευθύνες Προσωπικού

Το προσωπικό του [Όνομα Οργανισμού] πρέπει να γνωρίζει τους ρόλους και τις ευθύνες 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 περιλαμβάνονται στις περιγραφές εργασίας του προσωπικού του [Όνομα Οργανισμού].

# 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].

# Ρόλοι και Ευθύνες

Ρόλοι και ευθύνες πρέπει να προσδιοριστούν και να ανατεθούν στους χρήστες των πληροφοριακών συστημάτων.

# Διαχειριστής της δικτυακής υποδομής

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

Ως 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.
  + διαχωρισμός 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, δοκιμές διείσδυσης, έλεγχοι ασφαλείας και εκτιμήσεις τρωτότητας του δικτύου πρέπει να διεξάγονται σε τακτά χρονικά διαστήματα (τουλάχιστον ετησίως).

# Ανάλυση Κινδύνων

Οι Κίνδυνοι που διατρέχουν οι δικτυακοί πόροι του [Όνομα Οργανισμού] πρέπει να αξιολογούνται σε τακτά χρονικά διαστήματα. Μέσα από την εν λόγω διαδικασία οι κίνδυνοι πρέπει να εντοπιστούν και να καταταχθούν στις 5 ακόλουθες κατηγορίες:

* Πολύ Χαμηλός Κίνδυνος
* Χαμηλός Κίνδυνος
* Μέτριος Κίνδυνος
* Υψηλός Κίνδυνος
* Κρίσιμος Κίνδυνος

Οι συσκευές δικτύου (όπως ασφαλή πρωτόκολλα δρομολόγησης, switches, εξυπηρετητές, firewall, συστήματα ανίχνευσης και προστασίας εισβολών, συστήματα ηλεκτρονικού ταχυδρομείου κλπ.) πρέπει να προσδιοριστούν/αντιστοιχιστούν με το κατάλληλο επίπεδο κινδύνου. Στη συνέχεια, για την κάθε συσκευή πρέπει να προσδιοριστούν ρόλοι και προνόμια χρηστών που χρησιμοποιούν αυτές τις συσκευές. Για περισσότερες πληροφορίες σχετικά με την ανάλυση κινδύνων, ανατρέξτε στην Μεθοδολογία Διαχείρισης Κινδύνων.

# Απαιτήσεις για την ασφάλεια του δικτύου

* Όλος ο εξοπλισμός πρέπει να διαμορφώνεται σύμφωνα με τις βέλτιστες πρακτικές διαμόρφωσης (Hardening) του κατασκευαστή
* Το δίκτυο πρέπει να ελέγχεται και να προστατεύεται. Η σύνδεση μη εξουσιοδοτημένων πληροφοριακών συστημάτων και χρηστών στο δίκτυο του [Όνομα Οργανισμού] πρέπει να παρεμποδίζεται. Πρέπει να χρησιμοποιούνται τεχνολογίες ΝΑC (Network Access Control)
* Οι ηλεκτρονικοί υπολογιστές, πρέπει να ελέγχονται αν πληρούν τις προϋποθέσεις/κριτήρια ασφάλειας πριν συνδεθούν στο δίκτυο.
* Όλος ο εξοπλισμός ο οποίος είναι συνδεδεμένος στο δίκτυο του [Όνομα Οργανισμού] πρέπει να είναι συγχρονισμένος σε κεντρικό σύστημα Πρωτοκόλλου ώρας δικτύου (ntp) για τον ομοιόμορφο καθορισμό της ώρας / ημερομηνίας.
* Η πρόσβαση σε οποιοδήποτε πληροφοριακό σύστημα του δικτύου πρέπει να ελέγχεται.
* Η δημιουργία και η χρήση κοινών λογαριασμών σε πληροφοριακό σύστημα πρέπει να αποφεύγεται. Σε τέτοια περίπτωση το πληροφοριακό σύστημα πρέπει να υποστηρίζεται με λογισμικό το οποίο έχει την δυνατότητα εξακρίβωσης ταυτότητας κοινού λογαριασμού. Για παράδειγμα Observe IT, CyberArk, Microsoft PAM.
* Μόνο εξουσιοδοτημένος χρήστης πρέπει να μπορεί να κάνει αλλαγές σε ρυθμίσεις, παραμέτρους, διευθύνσεις IP σε πληροφοριακό σύστημα δικτύου ή ηλεκτρονικό υπολογιστή.
* Απαγορεύεται η σύνδεση μη εξουσιοδοτημένου εξοπλισμού στο δίκτυο.
* Απαγορεύεται η χρησιμοποίηση μη εξουσιοδοτημένου λογισμικού.
* Τα πληροφοριακά συστήματα και οι υπολογιστές πρέπει να έχουν εγκατεστημένο και ενημερωμένο λογισμικό αντιμετώπισης κακόβουλων λογισμικών πριν συνδεθούν στο δίκτυο.
* Τα πληροφοριακά συστήματα και οι υπολογιστές πρέπει να έχουν τις τελευταίες ενημερώσεις και αναβαθμίσεις (updates, patches) πριν συνδεθούν στο δίκτυο.
* Τα ημερολόγια (logs) των πληροφοριακών συστημάτων πρέπει να καταγράφονται σε κεντρικό σύστημα συλλογής και ανάλυσης δεδομένων. Τα ημερολόγια πρέπει να ελέγχονται σε τακτά χρονικά διαστήματα. Όσον αφορά τα ημερολόγια των domain controllers, firewalls IDS, routers/switches και άλλων υψηλής σημασίας/ κρισιμότητας συστημάτων, αυτά πρέπει να ελέγχονται καθημερινά
* Όπου χρειάζεται απομακρυσμένη πρόσβαση (εντός δικτύου) σε πληροφοριακά συστήματα πρέπει να 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 διασφάλισή της εμπιστευτικότητας και ακεραιότητας των πληροφοριών.
* Περιττά πρωτόκολλα και υπηρεσίες πρέπει να απενεργοποιούνται και να αποκόπτονται σε επίπεδο δικτύου.
* Ασύρματα δίκτυα πρέπει να απενεργοποιηθούν, εκτός στο guest Vlan που δεν πρέπει να 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.
* Ελεγχόμενη πρόσβαση και παρακολούθηση των ενεργειών και τήρηση αρχείων καταγραφής.
* Συνδέσεις σε εξωτερικά δίκτυα ή συστήματα να γίνονται μόνο από τις διαχειριζόμενες διεπαφές των στοιχείων που έχουν αναγνωριστεί
* Ο [Όνομα Οργανισμού] πρέπει να έχει firewall το οποίο να λειτουργεί ως σημείο διεπαφης ανάμεσα στο τοπικό δίκτυο και το εξωτερικό δίκτυο
* 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

# Αρχιτεκτονική δικτύου

Σύμφωνα με τον Κανονισμό 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]. Συγκεκριμένα περιλαμβάνονται:

1. Διαχωρισμός και τμηματοποίηση του δικτύου:

Να εξασφαλιστεί ο διαχωρισμός του λογικού δικτύου, σύμφωνα με τις επιχειρηματικές λειτουργίες, και να αποφευχθεί η εξάπλωση κακόβουλων στοιχείων.

1. 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.

1. Ασφαλή πρωτόκολλα επικοινωνίας:

Να διασφαλιστούν κατάλληλα πρωτοκόλλα επικοινωνίας προκειμένου να επιτευχθεί ασφαλής επικοινωνία μεταξύ των πόρων του δικτύου.

1. 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.

1. Εφεδρεία και υψηλή διαθεσιμότητα:

Να εξασφαλιστεί η διαθεσιμότητα πληροφοριών και δικτύων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρικού εξοπλισμού, συστημάτων και συνδέσεων υψηλής διαθεσιμότητας.

1. Ανίχνευση και πρόληψη εισβολών:

Να διασφαλιστεί η ανίχνευση και η πρόληψη από εξωτερικές απόπειρες εισβολής και επιθέσεις ασφάλειας.

## Σχέδιο δικτύου - Αρχιτεκτονική

Το σχέδιο δικτύου για τον [Όνομα Οργανισμού] περιλαμβάνει τις εξής κατευθυντήριες αρχές:

1. Το δίκτυο θα πρέπει να σχεδιαστεί για υψηλή απόδοση και αξιοπιστία, προσαρμόζοντας τις ανάγκες της επιχείρησης.
2. Τα διαγράμματα και οι διαμορφώσεις δικτύου θα πρέπει να τεκμηριώνονται και να συντηρούνται με ασφάλεια. Τα διαγράμματα θα διαχειρίζονται ως πληροφορία του υψηλότερου επιπέδου διαβάθμισης πληροφοριών (όπως αναφέρεται στο [DS2]), σύμφωνα με την εμπιστευτικότητα και την ευαισθησία τους. Εξετάζεται το ενδεχομένο εφαρμογής συστημάτων ταξινόμησης και επισήμανσης με βάση τις διεθνείς βέλτιστες πρακτικές, όπως το πρωτόκολλο «Traffic Light Protocol». Τουλάχιστον, ο Οργανισμός θα πρέπει να εφαρμόζει διάκριση μεταξύ των δημόσιων, ιδιωτικών και διαβαθμισμένων πληροφοριών.
3. Η τεκμηρίωση του σχεδιασμού δικτύου θα πρέπει να επαναλαμβάνεται τακτικά για ενημέρωση.
4. Οι αλλαγές στο δίκτυο πρέπει να συμβαδίζουν με την υπάρχουσα αρχιτεκτονική και τεκμηρίωση.
5. Η πρόσβαση στα διαγράμματα δικτύου πρέπει να ελέγχεται και να περιορίζεται σε εξουσιοδοτημένο προσωπικό.
6. Κατά το σχεδιασμό, λαμβάνεται υπόψη το απαιτούμενο επίπεδο ευελιξίας για μελλοντικές απαιτήσεις.
7. Η ασφαλής αρχιτεκτονική δικτύου προσαρμόζεται σε διάφορα στοιχεία ασφάλειας.
8. Τα σημεία αστοχίας ελαχιστοποιούνται για τη διασφάλιση υψηλής διαθεσιμότητας.
9. Εφεδρικοί μηχανισμοί και μέτρα διαθεσιμότητας εφαρμόζονται για κρίσιμα δίκτυα.
10. Το δίκτυο χωρίζεται σε λογικές περιμέτρους με βάση τη λειτουργικότητα.
11. Οι ζώνες DMZ εφαρμόζονται για δημοσίευση επιχειρησιακών υπηρεσιών.
12. Απομόνωση ευαίσθητων συστημάτων λαμβάνεται υπόψη κατά τον σχεδιασμό.
13. Συστήματα που επεξεργάζονται εμπιστευτικά δεδομένα απομονώνονται.
14. Δημόσιες υπηρεσίες τοποθετούνται σε ζώνες DMZ.
15. Ο [Όνομα Οργανισμού] εφαρμόζει μια ασφαλή αρχιτεκτονική δικτύου που περιλαμβάνει ένα firewall ως σημείο διεπαφής μεταξύ του τοπικού δικτύου και του εξωτερικού δικτύου. Το firewall λειτουργεί ως προστατευτικό φράγμα, ελέγχοντας την εισερχόμενη και εξερχόμενη κυκλοφορία δεδομένων, επιτρέποντας μόνο τη διέλευση επιτρεπόμενης κυκλοφορίας, ενώ αποκλείει ανεπιθύμητη ή επικίνδυνη επικοινωνία. Αυτό επιτυγχάνεται με την εφαρμογή κανόνων ασφαλείας που περιορίζουν την πρόσβαση και προστατεύουν το εσωτερικό δίκτυο από ανεπιθύμητη πρόσβαση και επιθέσεις.

* Στο δίκτυο πρέπει να υπάρχει πρόνοια αναβάθμισης και επέκτασης (scalability).
* Ο [Όνομα Οργανισμού] θα πρέπει να υλοποιήσει μια αρχιτεκτονική δικτύου για την εξασφάλιση του επιθυμητού επιπέδου ασφαλείας δικτύου για τον οργανισμό λαμβάνοντας υπόψη τις πρακτικές και τα μέτρα που αναφέρονται στα [NS2] – [NS7] του ΚΔΠ 389/2020.
* Στο δίκτυο πρέπει να υπάρχουν μηχανισμοί υψηλής διαθεσιμότητας (High Availability). Πρέπει να διασφαλίζεται ότι η οποιαδήποτε διακοπή του δικτύου δεν θα υπερβαίνει τον μέγιστο αποδεκτό χρόνο διακοπής των πληροφοριακών συστημάτων ή/ και υπηρεσιών του [Όνομα Οργανισμού].
* Το IPv6 όταν δεν χρησιμοποιείται συνιστάται να απενεργοποιείται.
* Το δίκτυο πρέπει να καταμεριστεί σε απομονωμένους λογικούς δικτυακούς τομείς . Ο καταμερισμός του δικτύου σε απομονωμένους λογικούς τομείς πρέπει να βασιστεί στα ακόλουθα:
  + Ιδεατά τοπικά δίκτυα (VLans): Καταμερισμός σε ομάδες υπηρεσιών πληροφορικής, χρηστών και πληροφοριακών συστημάτων
    - Οι εξυπηρετητές διαφορετικού τύπου/φύσεως (όπως application, database, webserver κ.τ.λ.) πρέπει να διαχωρίζονται σε ξεχωριστές ζώνες δικτύου.
  + Ιδεατά τοπικά δίκτυα πρέπει ναι προστατεύονται από εσωτερικά firewalls και η πλοήγηση σε αυτά να είναι φιλτραρισμένη.
  + Απομακρυσμένη Πρόσβαση (remote access).
  + Σύνδεση Τρίτων Μερών.
  + DMZ (Demilitarized Zone): Οποιεσδήποτε διαδικτυακές υπηρεσίες του [Όνομα Οργανισμού] πρέπει να τοποθετηθούν σε ζώνη DMZ.

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

# Εσωτερική 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.

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

* Διαχωρισμός των Στοιχείων: Τα δεδομένα ή οι πόροι που πρέπει να είναι προσβάσιμα από το εξωτερικό δίκτυο θα πρέπει να είναι χωρισμένα και ανεξάρτητα από τα εσωτερικά στοιχεία.
* Διαχειριζόμενες Διεπαφές: Οι συνδέσεις προς εξωτερικά δίκτυα ή συστήματα θα πρέπει να πραγματοποιούνται μόνο μέσω των διαχειριζόμενων διεπαφών των στοιχείων που έχουν αναγνωριστεί στη λογική περίμετρο. Αυτό εξασφαλίζει έλεγχο και ασφάλεια στις επικοινωνίες προς το εξωτερικό.

Με αυτόν τον τρόπο, διατηρείται η ασφάλεια και ο έλεγχος κατά την πρόσβαση από το εξωτερικό δίκτυο, προστατεύοντας το εσωτερικό δίκτυο από ανεπιθύμητη πρόσβαση ή επιθέσεις

# Περιμετρική Ασφάλεια Δικτύου

Σύμφωνα με τον Κανονισμό 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 και τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που βρίσκονται στο εσωτερικό δίκτυο. Θα πρέπει να λαμβάνει 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.

Ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόσει και διατηρήσει κατάλληλο διαχωρισμό και τμηματοποίηση του δικτύου, προκειμένου να διασφαλιστεί – 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. Έχει εξετάσει το ενδεχόμενο να υιοθετήσει εικονική τοπική δικτύωση (VLAN) κατά το σχεδιασμό του διαχωρισμού και της αρχιτεκτονικής του δικτύου σε τμήματα και τον διαχωρισμό των τομέων έρευνας και ανάπτυξης, της διοίκησης, της κεντρικής υποδομής πληροφοριών και των δημόσια διαθέσιμων (στο διαδίκτυο) εφαρμογών και συστημάτων. [NS2].



## 5.8.1 Πρωτόκολλα Ασφάλειας Δικτύου

Άρνηση υπηρεσιών: Ο [Όνομα Οργανισμού] πρέπει να διασφαλίσει 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 θα πρέπει να εξετάσει την ενσωμάτωση ικανοτήτων για τον εντοπισμό νόμιμων χρηστών και εφαρμογών έναντι κακόβουλων προσπαθειών πρόσβασης σε πόρους.

Επιπλέον για να διασφαλίσει την εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα των πληροφοριών υιοθετεί κατάλληλες κρυπτογραφικές λύσεις κατά την αποθήκευση, τη χρήση και τη μεταφορά δεδομένων. Η πολιτική κρυπτογράφησης θα πρέπει να λαμβάνει υπόψη την εφαρμογή κρυπτογραφικών μέτρων σε όλα τα στάδια του κύκλου ζωής των πληροφοριών και να εξετάζει εφαρμογές, συστήματα, εξοπλισμό δικτύου και διαύλους επικοινωνίας [ΑΜ5].

Κατά την ανταλλαγή πληροφοριών όπως κωδικοί πρόσβασης, η χρήση πρωτοκόλλων ασφαλείας, όπως το HTTPS για τον έλεγχο της ασφάλειας των διαδικτυακών επικοινωνιών, και μεθόδων επικοινωνίας που υποστηρίζουν την κρυπτογράφηση είναι κρίσιμη. Σε περιπτώσεις, λοιπόν, όπου κάποια πρωτόκολλα δεν παρέχουν επαρκή κρυπτογράφηση, προτείνεται η χρήση άλλων πρωτοκόλλων σε συνδυασμό με ένα δεύτερο επίπεδο ασφάλειας. Για παράδειγμα, όταν χρησιμοποιείται telnet, virtual network computing (VNC) ή remote desktop protocol (RDP), προτείνεται να γίνεται αυτό μέσω πρωτοκόλλων όπως το SSL ή το Internet Protocol Security (IPsec).

Συγκεκριμένα, αυτό σημαίνει ότι οι ευαίσθητες πληροφορίες που μεταδίδονται μέσω των προαναφερθέντων πρωτοκόλλων θα πρέπει να προστατεύονται με διπλό επίπεδο ασφάλειας. Η πρώτη στρώση είναι η ίδια η κρυπτογράφηση που παρέχεται από τα πρωτόκολλα SSL ή IPsec. Η δεύτερη στρώση είναι το πρωτόκολλο που χρησιμοποιείται για τη μεταφορά των πληροφοριών, όπως το telnet ή το RDP, το οποίο επίσης λειτουργεί εντός του πεδίου της κρυπτογράφησης. Αυτό ενισχύει την ασφάλεια της επικοινωνίας και προστατεύει τις ευαίσθητες πληροφορίες από ανεπιθύμητη πρόσβαση ή παρακολούθηση.

## 5.8.2 Κρυπτογράφηση

Τα δεδομένα που πρόκειται να μεταφερθούν με φυσικά μέσα, πρώτα κρυπτογραφούνται κατάλληλα και μετά αποστέλλονται για να προστατευθούν από ανεπιθύμητη πρόσβαση. Αυτό εξασφαλίζει ότι, αν πέσουν σε λάθος χέρια, δεν θα είναι ευανάγνωστα.

Τα κλειδιά κρυπτογράφησης, τα οποία απαιτούνται για την αποκρυπτογράφηση των δεδομένων, μεταφέρονται χωριστά, με άλλο μέσο (ή τρόπο) χωρίς επισήμανση της χρήσης τους. Για σύγχρονη μεταφορά να χρησιμοποιούνται πρωτόκολλα όπως είναι οι πιο πρόσφατες σταθερές εκδόσεις πρωτοκόλλων όπως είναι το SFTP (Secure File Transfer Protocol) ή HTTPS (Hypertext Transfer Protocol Secure).

## 5.8.3 Απειλές

Ο [Όνομα Οργανισμού] θα πρέπει να θεσπίζει, 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. Ο οργανισμός πρέπει εξασφαλίζει εφεδρεία και υψηλή διαθεσιμότητα σε όλα τα επίπεδα τεχνολογίας, μεταξύ άλλων, αποθήκευσης, επικοινωνίας και επεξεργασίας [NS6].

Ο [Όνομα Οργανισμού] οφείλει να υλοποιεί συστήματα ανίχνευσης εισβολών (IDS) και τα συστήματα πρόληψης εισβολών (IPS) για τον μετριασμό του κινδύνου απόπειρας εξωτερικής εισβολής. Εξετάζει το ενδεχόμενο δημιουργίας κονσόλας διαχείρισης για την παρακολούθηση του δικτύου με στόχο την καταχώρηση όλων των αποπειρών εισβολής για περαιτέρω ανάλυση. Στα πλαίσια σχεδιασμού των διαδικασιών ανίχνευσης και πρόληψης εισβολών, ο οργανισμός πρέπει να εξετάσει το ενδεχόμενο αυτόματης ενεργοποίησης μοχλών για την αντιμετώπιση συμβάντων [EIM2].

Σε περίπτωση που έχει αναγνωριστεί μη τυπική (anomalous) συμπεριφορά, ο οργανισμός πρέπει να ενεργοποιεί την διαδικασία ανταπόκρισης περιστατικών ασφαλείας και να απομονώνει τα σχετικά στοιχεία μέχρι να διερευνηθεί πλήρως η κατάσταση. Στόχος είναι να διασφαλίζει ότι οι φορείς είναι σε θέση να ανταποκρίνονται σε συμβάντα και περιστατικά που ενδέχεται να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα ή την αυθεντικότητα πληροφοριών. Συνεπάγεται την υιοθέτηση της επιχειρησιακής ανθεκτικότητας και μέτρων επιχειρησιακής συνέχειας και αποκατάστασης των καταστροφών, καθώς και την αποκατάσταση των κανονικών δραστηριοτήτων.

Ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόζει και διατηρεί μέτρα ασφάλειας δικτύου με σκοπό την προστασία της περιμέτρου του δικτύου από εξωτερικές απειλές με την υλοποιήσει πολυεπίπεδης αρχιτεκτονικής άμυνας όπου η ασφάλεια περιμέτρου αποτελεί ένα μόνο συγκεκριμένο επίπεδο.

* **Flood Guards:** Flood Guards πρέπει να χρησιμοποιούνται προκειμένου να αποτρέπουν τις διαδικτυακές επιθέσεις άρνησης Υπηρεσιών (Distributed Denial of Service Attacks -DDoS).
* **IPsec:** IPsec είναι ένα σύνολο κανόνων επικοινωνίας ή πρωτοκόλλων και πρέπει να χρησιμοποιείται για τη ρύθμιση ασφαλών συνδέσεων μέσω δικτύου
* **SSL:** Το SSL, είναι ένα πρωτόκολλο ασφαλείας διαδικτύου που βασίζεται σε κρυπτογράφηση και πρέπει να χρησιμοποιείται για τον σκοπό της διασφάλισης του απορρήτου, του ελέγχου ταυτότητας και της ακεραιότητας των δεδομένων στις επικοινωνίες του Διαδικτύου.
* **Firewall**: Firewalls πρέπει να χρησιμοποιούνται για να αποτρέπουν την μη εξουσιοδοτημένη πρόσβαση στο δίκτυο ή/και σε μη εξουσιοδοτημένους δικτυακούς χώρους ή/και σε μη εξουσιοδοτημένα πρωτόκολλα και υπηρεσίες.
* **Web Application Firewalls**: Web Application Firewalls πρέπει να χρησιμοποιούνται για να αποτρέπουν την μη εξουσιοδοτημένη πρόσβαση στις εφαρμογές WEB που προσφέρει ο [Όνομα Οργανισμού].
* **IPS/IDS**: Πρέπει να τοποθετηθούν αισθητήρες (IDS/IPS) σε συγκεκριμένα μέρη του δικτύου για να αποτρέπουν πιθανόν επιθέσεις στο δίκτυο (είτε εσωτερικές είτε εξωτερικές).
* **Data Loss Prevention**: Σύστημα πρόληψης απώλειας δεδομένων το οποίο ανιχνεύει και αποτρέπει μη εξουσιοδοτημένες μεταφορές δεδομένων πρέπει να τοποθετηθεί σε όλα τα μέρη του δικτύου που έχουν έξοδο από αυτό (π.χ. Internet, Email, VPN connection, Endpoints).
* **Sandbox**: Σύστημα τύπου Sandbox (ελεγχόμενο περιβάλλον) το οποίο ανιχνεύει και αποτρέπει κακόβουλα λογισμικά, πρέπει να τοποθετηθεί σε όλα τα μέρη του δικτύου που έχουν είσοδο σε αυτό (π.χ. Internet, Email, Endpoints).
* **Spam** **Filters, Email** **Antivirus**: Πρέπει να χρησιμοποιούνται συστήματα για την ασφάλεια του ηλεκτρονικού ταχυδρομείου (όπως «Spam Filters»). Επίσης τα ηλεκτρονικά μηνύματα πρέπει να σαρώνονται με λογισμικό αντιμετώπισης κακόβουλων λογισμικών.
* **Web** **Filtering**: Πρέπει να χρησιμοποιούνται συστήματα για την ασφάλεια της χρήσης διαδικτύου (Web Filtering).**Antivirus**: Πρέπει να χρησιμοποιείται κεντρικό σύστημα αντιμετώπισης ιών και κακόβουλων λογισμικών.

## 5.8.4 Στοιχεία Ενεργητικού

Σύμφωνα με τον Κανονισμό Κ.Δ.Π. 389/2020, ο [Όνομα Οργανισμού] πρέπει να ορίσει δυνατότητες παρακολούθησης των στοιχείων ενεργητικού, ώστε να είναι σε θέση να εντοπίζει ανωμαλίες σε σχέση με κανονικές συνθήκες (π.χ. τοποθεσία, χρήση) και/ή τη λειτουργία των στοιχείων αυτών. Ο [Όνομα Οργανισμού] θα πρέπει να αναφέρει στην πολιτική αποδεκτής χρήσης, τι συνιστά αποδεκτή χρήση και/ή λειτουργία των στοιχείων ενεργητικού. Να εξετάσει την συμπερίληψη της περιγραφής της αποδεκτής χρήσης, της λειτουργίας και της τοποθεσίας των στοιχείων στον κατάλογο των στοιχείων ενεργητικού, προκειμένου να υπάρχει πλήρης απογραφή των στοιχείων αυτών. Όταν εντοπίζονται ανωμαλίες, θα πρέπει να ενεργοποιούνται οι διαδικασίες διαχείρισης συμβάντων και περιστατικών [ΑΜ3].

Τα κρίσιμα συστήματα πρέπει να τοποθετούνται σε διαχωρισμένα δίκτυα ή υποδίκτυα ώστε να εφαρμόζονται επιπλέον μέτρα προστασίας. Η εφαρμογή αυτών των μέτρων περιλαμβάνει τη χρήση τεχνικών για τον περιορισμό της πρόσβασης σε αυτά τα συστήματα μόνο σε εξουσιοδοτημένους χρήστες. Σε αυτό βοηθάει να καταρτιστεί κατάλογος στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού [RS2] και να εξασφαλιστεί ότι τα δεδομένα ταξινομούνται και επισημαίνονται κατά τρόπο ώστε να αντικατοπτρίζεται η ευαισθησία τους ώστε να εξασφαλίζεται η κατάλληλη επεξεργασία τους [DS2].

# Παράρτημα Α – Διάγραμμα Δικτύου [Όνομα Οργανισμού]

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

