ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΣΥΓΓΡΑΦΕΙΣ:

Φακιόλας Γεώργιος 321/2019231

Μανωλάκος Κωνταντίνος 321/2019127

Σωματόπουλος Στυλιανός 321/2021061

ΕΡΓΑΣΙΑ ΕΑΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2023-24

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ

Το παρόν σχέδιο ασφαλείας, πρόκειται για μία βιομηχανική μονάδα παραγωγής καλλυντικών και αρωμάτων για την αποτελεσματική της λειτουργία, την καταγραφή και την εξυπηρέτηση των πελατών της στο πλαίσιο της εξέτασης του εργαστηρίου του μαθήματος «Ασφάλεια Πληροφοριακών & Επικοινωνιακών Συστημάτων του τμήματος Μ.Π.Ε.Σ.

1.1. Περιγραφή Εργασίας

Σε αυτό το σχέδιο, χρειάζεται να υλοποιήσουμε ένα Πληροφοριακό Σύστημα μία βιομηχανική μονάδα παραγωγής καλλυντικών και αρωμάτων για την αποτελεσματική της λειτουργία, την καταγραφή και την εξυπηρέτηση των πελατών της. Βασίζεται στις διαδικτυακές τεχνολογίες επικοινωνιών και νέας γενιάς συσκευών επεξεργασίας και αποθήκευσης πληροφοριών για την απομακρυσμένη υλοποίηση βασικών λειτουργιών όπως πώληση προϊόντων, τιμολόγησης των πελατών της κτλ. Η εταιρεία που θα μελετήσουμε μπορεί να πραγματοποιήσει πώληση τόσο στα γραφεία της (από κοντά) όσο και απομακρυσμένα μέσω διαδικτύου. Στην παρούσα εργασία καλούμαστε να εκπονήσουμε **μία ολοκληρωμένη πρόταση ενός σχεδίου ασφαλείας** μιας εταιρείας που επεξεργάζεται εκ των πραγμάτων προσωπικά δεδομένα, χωρίς να υπάρχει γνώση σε θέματα ασφάλειας δικτύων και πληροφοριακών συστημάτων. Στο πλαίσιο της εργασίας θα ασχοληθούμε αποκλειστικά με την προστασία του εξοπλισμού της εταιρείας (εύρος προστασίας συστημάτων) Η συγκεκριμένη εργασία απαρτίζεται από 2 μέρη, το **Α** και το **Β**. Η **Α** φάση περιλαμβάνει την ανάλυση συστήματος με τη χρήση καρτών. Σε αυτή τη φάση μας έχει ζητηθεί να χρησιμοποιήσουμε τη μέθοδο των καρτών ασφάλειας, οι οποίες δημιουργήθηκαν από το Πανεπιστήμιο της Ουάσιγκτον. Πρόκειται για μία προσέγγιση η οποία επικεντρώνεται στη δημιουργικότητα και τον καταιγισμό ιδεών. Αυτή η μέθοδος χρησιμοποιεί μια τράπουλα 42 καρτών προς διευκόλυνση ανακάλυψης απειλών και επιπτώσεων, που ταξινομούνται σε τέσσερις βασικές κατηγορίες: **Human Impact** [9 κάρτες], Κίνητρα του Επιτιθέμενου/**Adversary's Motivations** [13 κάρτες], Πόροι του επιτιθέμενου/**Adversary's Resources** [11 κάρτες] και Μέθοδοι του Επιτιθέμενου/**Adversary's Methods** [9 κάρτες]. Στόχος της φάσης αυτής είναι η ανάλυση των τεσσάρων αυτών βασικών παραγόντων που δύναται να επηρεάσουν το επίπεδο ασφάλειας της υπό εξέταση υποδομής (ΠΣ της βιομηχανικής μονάδας) σε σχέση με τις βασικές συνιστώσες της, κάνοντας χρήση των 42 καρτών. Σκοπός είναι ο προσδιορισμός και η αποτίμηση των σοβαρών απειλών αλλά και η εξεύρεση των πιο πολύπλοκων επιθέσεων που μπορούν να πλήξουν το συγκεκριμένο ολοκληρωμένο σύστημα (θα το αναλύσουμε ακριβώς μετά την ενότητα 1 και πριν την ενότητα 2). Η **Β** φάση είναι όλες οι ενότητες 2 , 3 , 4 , 5.

1.2. Δομή παραδοτέου

Ενότητα 1η : Εισαγωγικά στοιχεία για την εκπόνηση της εργασίας μας, και μια σύντομη περιγραφή του περιεχομένου και της δομής της.
Α: Ανάλυση συστήματος με τη χρήση καρτών.
Β: Μεθοδολογία FMEA (Failure Modes and Effects Analysis) και Σχέδιο Ασφαλείας.
Ενότητα 2η : Περιγραφή για την μεθοδολογία που θα ακολουθήσουμε για το σχέδιο ασφαλείας μας. Παρουσίαση του Πληροφοριακού Συστήματος και των επιμέρους στοιχείων του, που μας ενδιαφέρουν να αναλύσουμε, ώστε να επιφέρουμε κατάλληλα αντίμετρα για την ασφαλέστερη λειτουργία του.
Ενότητα 3η : Αποτίμηση των αγαθών και εγκαταστάσεων του ΠΣ που μελετήσαμε, ταξινομημένα βάσει επικινδυνότητας. Αποτύπωση απειλών και ευπαθειών που εντοπίστηκαν από την μελέτη αυτών. Ένας πίνακας αποτίμησης των επιπτώσεων (Impact Assessment), βάσει του προτύπου που ακολουθούμε.
Ενότητα 4η : Αποτύπωση των μέτρων ασφαλείας που προτείνουμε και η ανάλυσή τους σε κατηγορίες.
Ενότητα 5η : Παρουσίαση των πιο κρίσιμων αποτελεσμάτων που αντλήσαμε από την ολοκληρωμένη ανάλυση επικινδυνότητας που πραγματοποιήθηκε.

Α. ΑΝΑΛΥΣΗ ΣΥΣΤΗΜΑΤΟΣ ΜΕ ΤΗ ΧΡΗΣΗ ΚΑΡΤΩΝ

Αρχικά, υπάρχουν τέσσερις κατηγορίες καρτών: Ο ανθρώπινος αντίκτυπος (human impact), τα κίνητρα του επιτιθέμενου (adversary's motivations), οι πόροι του επιτιθέμενου (adversary's resources) καθώς και οι μέθοδοι του επιτιθέμενου (adversary's methods).

- Οι κάρτες «Ανθρώπινος αντίκτυπος» περιγράφουν τον πιθανό αντίκτυπο μιας παραβίασης της ασφάλειας σε ανθρώπους, όπως
- Οι κάρτες «Κίνητρα του επιτιθέμενου» περιγράφουν τους λόγους για τους οποίους κάποιος μπορεί να θέλει να επιτεθεί στο σύστημα.
- Οι κάρτες «Πόροι του επιτιθέμενου» περιγράφουν τους πόρους που μπορεί να διαθέτει ένας επιτιθέμενος.
- Οι κάρτες «Μέθοδοι του επιτιθέμενου» περιγράφουν τους τρόπους με τους οποίους ένας επιτιθέμενος μπορεί να προσπαθήσει να παραβιάσει το σύστημα.

Παρακάτω, θα αναλύσουμε την κάθε ενότητα, κι θα παραθέσουμε ποιες σύμφωνα με τη γνώμη μας, είναι οι κάρτες που πιστεύουμε ότι ταιριάζουν καλύτερα με το σενάριό μας.

- Αρχικά, ας εξετάσουμε τις κάρτες «**ανθρώπινος αντίκτυπος**» (human impact). Θα μπορούσαμε να εξετάσουμε τον πιθανό αντίκτυπο μιας παραβίασης της ασφάλειας στους εργαζόμενους και τους πελάτες, τον αντίκτυπο στη φήμη της εταιρείας, αλλά και τους πόρους που μπορούν να σπαταληθούν. Για παράδειγμα, μια παραβίαση θα μπορούσε να έχει ως αποτέλεσμα την απώλεια εμπιστευτικών πληροφοριών για τους πελάτες (Personal Data), οικονομικές απώλειες λόγω απάτης ή κλοπής (Financial Wellbeing), ζημιά στη φήμη της εταιρείας (Societal Wellbeing), διαταραχή της λειτουργίας της (Emotional Wellbeing) ή σπατάλη φυσικών πόρων για την παραγωγή προϊόντων (The Biosphere).

Παραβίαση & Απώλεια των δεδομένων των πελατών ή των εργαζομένων (Personal Data) & Οικονομικές απώλειες λόγω απάτης ή κλοπής (Financial Wellbeing): Η μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών/εργαζομένων, όπως προσωπικές πληροφορίες και στοιχεία συναλλαγών, μπορεί να οδηγήσει σε κλοπή ταυτότητας και οικονομική απώλεια για τους εμπλεκόμενους πελάτες/εργαζόμενους.

Κλοπή πνευματικής ιδιοκτησίας (Societal Wellbeing): Η κλοπή πνευματικής ιδιοκτησίας, όπως συνταγές καλλυντικών και αρωμάτων και διπλώματα ευρεσιτεχνίας, μπορεί να βλάψει τη φήμη της εταιρείας και την να επηρεάσει αρνητικά και το προσωπικό που εργάστηκε πάνω στην κλεμμένη πνευματική ιδιοκτησία.

Διαταραχή της λειτουργίας (Emotional Wellbeing): Μια παραβίαση της ασφάλειας μπορεί να προκαλέσει λειτουργικές διαταραχές, οδηγώντας σε διακοπή λειτουργίας του συστήματος και απώλεια παραγωγικότητας για το προσωπικό και τη διεύθυνση της εταιρείας.

Οικονομικές απώλειες λόγω απάτης ή κλοπής (Financial Wellbeing): Η οικονομική απώλεια δεν αφορά μόνο τους πελάτες/εργαζόμενους αλλά και την ίδια την εταιρεία καθώς μπορεί να μπει η περιουσία της στο στόχαστρο των επιτιθέμενων, με αποτέλεσμα να χάσει χρήματα είτε από κλοπή είτε από κάποια απάτη εις βάρος της.

Σπατάλη φυσικών πόρων (The Biosphere) & Οικονομικές απώλειες (Financial Wellbeing): Μία επιτηδευμένη και υπέρμετρη λανθασμένη παραγγελία λόγω επέμβασης στις συνναλαγές της εταιρείας από κάποιον επιτιθέμενο, μπορεί να οδηγήσει σε σπατάλη φυσικών πόρων για την παραγωγή των προϊόντων και κατά συνέπεια οικονομική απώλεια για την εταιρεία.

- Στην συνέχεια, ας εξετάσουμε τις κάρτες με **«τα κίνητρα του επιτιθέμενου»** (adversary's motivations). Θα μπορούσαμε να εξετάσουμε τα κίνητρα των πιθανών επιτιθέμενων, όπως είναι για παράδειγμα το οικονομικό κέρδος (Money), , η εκδίκηση – ένας κακόβουλος εσωτερικός χρήστης (Malice or Revenge) ή απλώς η περιέργεια (Curiosity or Boredom) ή η επιθυμία του επιτιθέμενου για επίθεση (Desire or Obsession).

Οικονομικό κέρδος (Money): Οι επιτιθέμενοι μπορεί να έχουν ως κίνητρο το πιθανό οικονομικό κέρδος από την πώληση κλεμμένων δεδομένων ή τη χρήση κλεμμένων δεδομένων για τη διάπραξη οικονομικής απάτης.

Εκδίκηση - ένας κακόβουλος εσωτερικός χρήστης (Malice of Revenge): Δυσαρεστημένοι πρώην εργαζόμενοι μπορεί να επιδιώξουν να βλάψουν την εταιρεία εξαπολύοντας επίθεση. Ακόμα, ένας κακόβουλος εσωτερικός χρήστης, μπορεί να έχει κίνητρο να βλάψει το σύστημα πληροφοριών της εταιρείας, λόγω προσωπικής μνησικακίας ή για οικονομικό όφελος.

Περιέργεια του επιτιθέμενου για επίθεση (Curiosity or Boredom): Ορισμένοι επιτιθέμενοι μπορεί να θέλουν να πειραματιστούν για το τι μπορεί να προκαλέσει μια επίθεση στην εταιρεία από περιέργεια.

Επιθυμία του επιτιθέμενου για επίθεση (Desire or Obsession): Ορισμένοι επιτιθέμενοι μπορεί να παρακινούνται απλώς από την πρόκληση της παραβίασης του συστήματος πληροφοριών της εταιρείας ή από τη συγκίνηση της πρόκλησης διαταραχών ή ζημιών.

- Έπειτα, ας εξετάσουμε τις κάρτες των «πόρων του επιτιθέμενου» (adversary's resources). Θα μπορούσαμε να εξετάσουμε τους πόρους που μπορεί να διαθέτει ένας επιτιθέμενος, όπως τεχνική εμπειρογνωμοσύνη (Expertise), οικονομικούς πόρους (Money), η πρόσβαση σε εμπιστευτικές πληροφορίες (Inside Capabilities & Inside Knowledge), ο χρόνος (Time) ή τα εργαλεία (Tools).

Τεχνική εμπειρογνωμοσύνη (Expertise): Οι επιτιθέμενοι με τεχνική εμπειρογνωμοσύνη μπορούν να εκμεταλλευτούν τα τρωτά σημεία των συστημάτων της εταιρείας για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση ή να προκαλέσουν ζημιά.

Οικονομικοί πόροι (Money): Επιτιθέμενοι με οικονομικούς πόρους μπορούν να τους χρησιμοποιήσουν για να χρηματοδοτήσουν πιο σύνθετες επιθέσεις, όπως η αγορά exploits μηδενικής ημέρας ή η πρόσληψη εξειδικευμένων επιτιθέμενων.

Πρόσβαση σε εμπιστευτικές πληροφορίες (Inside Capabilities & Inside Knowledge): Οι εισβολείς με πρόσβαση σε ευαίσθητες πληροφορίες μπορούν να κλέψουν δεδομένα ή να προκαλέσουν ζημιά στα συστήματα της εταιρείας από το εσωτερικό.

Χρόνος (Time): Ένας επιτιθέμενος με σημαντικούς χρονικούς πόρους μπορεί να είναι σε θέση να πραγματοποιήσει μια πιο ενδελεχή και επίμονη επίθεση στο σύστημα πληροφοριών .

Εργαλεία για την επίτευξη του στόχου (Tools): Ο επιτιθέμενος μπορεί να χρησιμοποιήσει διάφορα εργαλεία για να επιτεθεί στο σύστημα της εταιρείας, όπως κακόβουλο λογισμικό (malware), phishing, εκμετάλλευση ευπαθειών και social engineering. Αναλυτικότερα:

Κακόβουλο Λογισμικό (Malware): Ο επιτιθέμενος μπορεί να δημιουργήσει και να εισαγάγει κακόβουλο λογισμικό στο πληροφοριακό σύστημα, όπως ιούς, τρόιανους ή ransomware, τα οποία μπορούν να προκαλέσουν διακοπές λειτουργίας ή ακόμα και να κλέψουν εμπιστευτικά δεδομένα.

Phishing: Μέσω αποστολής κακόβουλων email ή μηνυμάτων, ο επιτιθέμενος μπορεί να προσπαθήσει να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης ή διαπιστευτήρια χρηστών.

Εκμετάλλευση Ευπάθειών: Ο επιτιθέμενος μπορεί να αναζητήσει ευπάθειες στο λογισμικό ή το δίκτυο της εταιρείας και να τις εκμεταλλευτεί για να κερδίσει πρόσβαση ή να προκαλέσει ζημιά.

Social Engineering: Με τη χρήση κοινωνικών μηχανικών τεχνικών, ο επιτιθέμενος μπορεί να παρασύρει εργαζόμενους της εταιρείας να αποκαλύψουν ευαίσθητες πληροφορίες ή να εκτελέσουν κακόβουλες ενέργειες.

- Τέλος, ας εξετάσουμε τις κάρτες των **«μεθόδων του επιτιθέμενου»**. Θα μπορούσαμε να εξετάσουμε τους τρόπους με τους οποίους ένας επιτιθέμενος μπορεί να προσπαθήσει να παραβιάσει το σύστημα όπως το phishing (Manipulation or Coercion), η εκμετάλλευση ευπαθειών (Technological Attack) ή και με φυσικές επιθέσεις (Physical Attack).

Phishing (Manipulation or Coercion): Μέσω αποστολής κακόβουλων email ή μηνυμάτων, ο επιτιθέμενος μπορεί να προσπαθήσει να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης ή διαπιστευτήρια χρηστών.

Εκμετάλλευση Ευπάθειών (Technological Attack): Ο επιτιθέμενος μπορεί να αναζητήσει ευπάθειες στο λογισμικό ή το δίκτυο της εταιρείας και να τις εκμεταλλευτεί για να κερδίσει πρόσβαση ή να προκαλέσει ζημιά.

Φυσικές επιθέσεις (Physical Attack): Ο επιτιθέμενος μπορεί να προκαλέσει φυσική ζημιά ή να καταστρέψει το σύστημα πληροφοριών της εταιρείας με σκοπό να διακόψει τις λειτουργίες ή να προκαλέσει άλλου είδους ζημιά.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας της βιομηχανικής μονάδας παραγωγής καλλυντικών και αρωμάτων χρησιμοποιήθηκε παραμετροποιημένη μέθοδος του ISO27001K[1]. Επιλέχθηκε για τη συγκεκριμένη εργασία για τους εξής λόγους:

- Αποτελεί πρότυπη μέθοδο και έχει αναπτυχθεί με σκοπό να εφαρμοστεί στην εκπαίδευση.
- Συνοδεύεται από αυτοματοποιημένο excel *(tool)* που υποστηρίζει όλα τα στάδια της εφαρμογής.
- Καλύπτει όλες τις συνιστώσες της ασφάλειας των πληροφοριακών συστημάτων, περιλαμβανομένων του τεχνικού παράγοντα, των θεμάτων διαδικασιών και προσωπικού, της φυσικής ασφάλειας, της ασφάλειας δικτύων κλπ.

Στάδιο	Βήματα
1. Προσδιορισμός και αποτίμηση αγαθών *(identification and valuation of assets)*	*Βήμα 1*: Περιγραφή πληροφοριακών συστημάτων και εγκαταστάσεων *Βήμα 2:* Αποτίμηση αγαθών πληροφοριακών συστημάτων και εγκαταστάσεων *Βήμα 3:* Επιβεβαίωση και επικύρωση αποτίμησης
2. Ανάλυση επικινδυνότητας *(risk analysis)*	*Βήμα 1:* Προσδιορισμός απειλών που αφορούν κάθε Αγαθό (asset) *Βήμα 2:* Εκτίμηση απειλών (threat assessment) και αδυναμιών (vulnerability assessment) *Βήμα 3:* Υπολογισμός επικινδυνότητας συνδυασμών Αγαθό-Απειλή-Αδυναμία *Βήμα 4:* Επιβεβαίωση και επικύρωση βαθμού επικινδυνότητας
3. Διαχείριση επικινδυνότητας *(risk management)*	*Βήμα 1:* Προσδιορισμός προτεινόμενων αντιμέτρων *Βήμα 2:* Σχέδιο ασφάλειας πληροφοριακών συστημάτων και εγκαταστάσεων

Πίνακας 1: *Στάδια και βήματα της Ανάλυσης και Διαχείρισης επικινδυνότητας*

2.1. Περιγραφή Πληροφοριακού Συστήματος (ΠΣ) υπό έλεγχο

Στην ενότητα αυτή, καταγράφονται τα υφιστάμενα πληροφοριακά συστήματα της βιομηχανίας καλλυντικών και αρωμάτων, τα οποία με το πέρας της μελέτης θα επικαιροποιηθούν, αναβαθμιστούν ή σε κάποιες περιπτώσεις αντικατασταθούν.

[1] http://www.iso27001security.com/html/toolkit.html

2.1.1. Υλικός εξοπλισμός (hardware)

Inventory ID	ΟΝΟΜΑΣΙΑ ΑΓΑΘΟΥ	ΤΥΠΟΣ ΑΓΑΘΟΥ
CI-A-1008	LAPTOP1	Workstation
CI-A-1009	PC5	Workstation
CI-A-1010	CRM SERVER	Server
CI-A-1011	RADIUS/SNMP SERVER	Server
CI-A-1012	ROUTER2	Router
CI-A-1013	VOIP-PHONE1	IP Phone
CI-A-1014	FIREWALL	Firewall
CI-A-1015	ROUTER3	Router
CI-A-1016	WIRELESS-LAN-CONTROLLER1	Wireless Controller
CI-A-1017	TABLET-PC1	Tablet
CI-A-1018	EMAIL SERVER	Server
CI-A-1019	PC4	Workstation
CI-A-1020	PC6	Workstation
CI-A-1021	PRINTER1	Printer
CI-A-1022	EDGE-ROUTER	Router
CI-A-1023	DNS/DHCP SERVER	Server
CI-A-1024	HRM SERVER	Server
CI-A-1025	SW-FLOOR4.1	Switch
CI-A-1026	ROUTER1	Router
CI-A-1027	SW-FLOOR4.2	Switch
CI-A-1028	ROUTER4	Router
CI-A-1029	WEB APPLICATION SERVER	Server
CI-A-1030	PC3	Workstation
CI-A-1031	PC1	Workstation
CI-A-1032	PC2	Workstation
CI-A-1033	DOMAIN CONTROLLER/FILE SERVER	Server

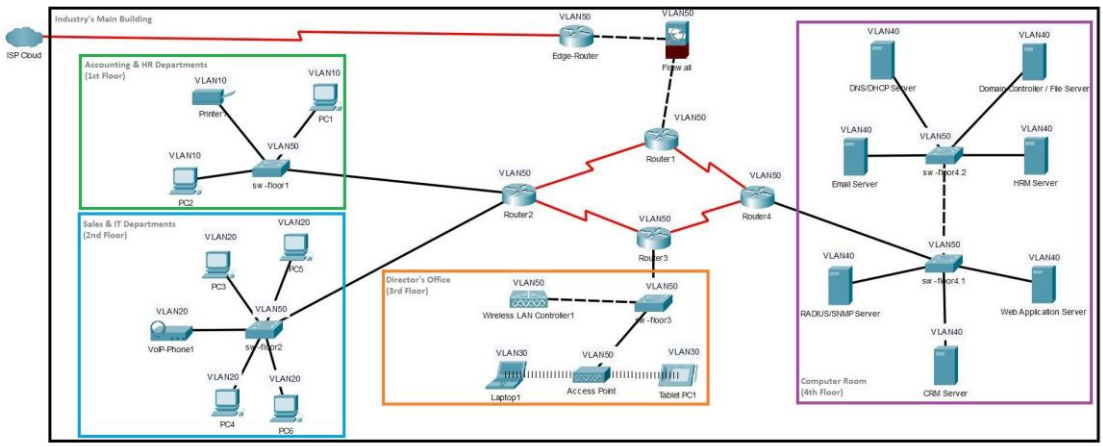
CI-A-1034	SW-FLOOR2	Switch
CI-A-1035	ACCESS POINT	Access Point
CI-A-1036	SW-FLOOR1	Switch
CI-A-1037	SW-FLOOR3	Switch

2.1.2. Λογισμικό και εφαρμογές

Inventory ID	**ΟΝΟΜΑΣΙΑ ΑΓΑΘΟΥ**	**ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ**
CI-A-1008	LAPTOP1	Windows 11 Home
CI-A-1009	PC5	Windows 11 Home
CI-A-1010	CRM SERVER	Windows Server 2008
CI-A-1011	RADIUS/SNMP SERVER	Ubuntu 16.04.7 LTS
CI-A-1012	ROUTER2	Cisco proprietary software
CI-A-1013	VOIP-PHONE1	Cisco proprietary software
CI-A-1014	FIREWALL	FortiGate proprietary software
CI-A-1015	ROUTER3	Cisco proprietary software
CI-A-1016	WIRELESS-LAN-CONTROLLER1	Cisco proprietary software
CI-A-1017	TABLET-PC1	Android 9 Pie (API 28)
CI-A-1018	EMAIL SERVER	Ubuntu 16.04.7 LTS
CI-A-1019	PC4	Windows 7
CI-A-1020	PC6	Windows 7
CI-A-1021	PRINTER1	Epson proprietary software
CI-A-1022	EDGE-ROUTER	Cisco proprietary software
CI-A-1023	DNS/DHCP SERVER	Ubuntu 12.04.5 LTS
CI-A-1024	HRM SERVER	Windows Server 2008
CI-A-1025	SW-FLOOR4.1	Cisco proprietary software
CI-A-1026	ROUTER1	Cisco proprietary software
CI-A-1027	SW-FLOOR4.2	Cisco proprietary software
CI-A-1028	ROUTER4	Cisco proprietary software

CI-A-1029	WEB APPLICATION SERVER	Ubuntu 16.04.7 LTS
CI-A-1030	PC3	Windows 11 Home
CI-A-1031	PC1	Windows XP
CI-A-1032	PC2	Windows XP
CI-A-1033	DOMAIN CONTROLLER/FILE SERVER	Windows Server 2008
CI-A-1034	SW-FLOOR2	Cisco proprietary software
CI-A-1035	ACCESS POINT	Cisco proprietary software
CI-A-1036	SW-FLOOR1	Cisco proprietary software
CI-A-1037	SW-FLOOR3	Cisco proprietary software
CI-A-1042	Wired phone1 (Δικό μας αγαθό)	Fanvil proprietary software

2.1.3. Δίκτυο



Περιγραφή του δικτύου της βιομηχανίας:
Στο δίκτυο της βιομηχανίας διακρίνουμε το ISP, που είναι ο πάροχος υπηρεσιών Διαδικτύου και συνδέεται με τον Edge Router, το Firewall και ένα κεντρικό Router (Router1) στον οποίο συνδέονται οι υπόλοιποι Routers (Router2, Router3 & Router4).
Επιπλέον, διακρίνουμε 4 switches, για τη σύνδεση των παρακάτω 4 τμημάτων της βιομηχανίας:
Accounting & HR Departments (1st floor): Σε αυτό το switch (sw -floor1 -> σύνδεση με Router2) είναι συνδεδεμένα PC (PC1 & PC2) και ένας εκτυπωτής (Printer 1).
Sales & IT Departments (2nd floor): Σε αυτό το switch (sw -floor2 -> σύνδεση με Router2), είναι συνδεδεμένα 4 PC (PC3, PC4, PC5 & PC6) και ένα VoIP (Phone1).
Director's (3rd floor): Σε αυτό το switch (sw -floor3 -> σύνδεση με Router3) είναι συνδεδεμένα ένας WLAN Controller (Wireless LAN Controller 1) και ένα Access Point

που επιτρέπει τη σύνδεση ενός Laptop (Laptop1) και ενός Tablet (Tablet PC1) ασύρματα στο δίκτυο.

Computer Room (4th floor): Σε αυτό το switch(sw -floor4.1 -> σύνδεση με Router4), είναι συνδεδεμένα ένας RADIUS/SNMP server (για τη διαχείριση και την παρακολούθηση των συσκευών και των χρηστών), ένας CRM server (για τη διαχείριση των πληροφοριών πελατών και των διαδικασιών επικοινωνίας με αυτούς), ένας Web Application Server (για την εκτέλεση και τη διαχείριση διαδικτυακών εφαρμογών δηλαδή για την επεξεργασία των αιτημάτων από τους χρήστες και την παρουσίαση του περιεχομένου στον περιηγητή τους) και ένα ακόμα switch (sw -floor4.2). Αυτό το switch συνδέεται με έναν Email Server (για τον χειρισμό των μηνυμάτων ηλεκτρονικού ταχυδρομείου που αποστέλλονται και λαμβάνονται από τους χρήστες που έχουν λογαριασμούς ηλεκτρονικού ταχυδρομείου στο δίκτυο της βιομηχανίας), έναν DNS/DHCP Server (παρέχει υπηρεσίες συστήματος ονομάτων τομέα (DNS) και δυναμικού πρωτοκόλλου διαμόρφωσης κεντρικών υπολογιστών (DHCP) στους χρήστες που είναι συνδεδεμένοι στο δίκτυο της βιομηχανίας), έναν Domain Controller/File Server (σύστημα που χρησιμεύει ως κεντρικό αποθετήριο για σημαντικά αρχεία και δεδομένα και διαχειρίζεται επίσης λογαριασμούς χρηστών και πόρους δικτύου) και έναν HRM Server (για τη διαχείριση των ανθρώπινων πόρων της βιομηχανίας).

2.1.4. Δεδομένα

Inventory ID	ΟΝΟΜΑΣΙΑ ΑΓΑΘΟΥ	ΠΕΡΙΓΡΑΦΗ	ΤΟΠΟΘΕΣΙΑ
CI-A-1000	Industry Customer Data	Στοιχεία Πελατών Βιομηχανίας	Database Server
CI-A-1001	Industry Employee Data	Στοιχεία Εργαζομένων Βιομηχανίας	Database Server
CI-A-1038	Industry Product Data (δικό μας δεδομένο)	Στοιχεία Προϊόντων Βιομηχανίας	Database Server
CI-A-1039	Industry Supplier Data (δικό μας δεδομένο)	Στοιχεία Προμηθευτή Βιομηχανίας	Database Server

2.1.5. Διαδικασίες

Inventory ID	ΟΝΟΜΑΣΙΑ ΑΓΑΘΟΥ	ΠΕΡΙΓΡΑΦΗ	ΤΟΠΟΘΕΣΙΑ
CI-A-1002	Create New Customer	Δημιουργία νέου πελάτη	Sales & IT Departments (2nd Floor)
CI-A-1003	Create New Order (Local)	Δημιουργία νέας παραγγελίας (διά ζώσης)	Sales & IT Departments (2nd Floor)
CI-A-1004	Create New Order (Remotely)	Δημιουργία νέας παραγγελίας (εξ αποστάσεως)	Field Sales through smartphone
CI-A-1005	Customer Support	Εξυπηρέτηση πελατών	Accounting & HR Departments (1st Floor)
CI-A-1040	Staff shift hours (δική μας διαδικασία)	Προγραμματισμός του εβδομαδιαίου προγράμματος εργασίας του προσωπικού.	Accounting & HR Departments (1st floor)

CI-A-1041	Staff Payments (δική μας διαδικασία)	Πληρωμή προσωπικού	Accounting & HR Departments (1st Floor)

3. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ

Σε αυτό το σημείο, θα κάνουμε μια αποτίμηση όλων των αγαθών και των εγκαταστάσεων του ΠΣ που μελετούμε, ταξινομημένα, από το πιο σημαντικό, στο λιγότερο σημαντικό. Θα πραγματοποιήσουμε αποτύπωση απειλών και ευπαθειών που εντοπίστηκαν από την μελέτη αυτών. Θα συμπριλάβουμε και έναν πίνακα αποτίμησης των επιπτώσεων (Impact Assessment), βάσει του προτύπου ασφαλείας που ακολουθούμε.

3.1. Αγαθά που εντοπίστηκαν

ΥΛΙΚΟ	ΔΙΑΔΙΚΑΣΙΕΣ	ΛΟΓΙΣΜΙΚΟ	ΠΕΡΙΓΡΑΦΗ	RPN
FIREWALL		FortiGate proprietary software	monitors incoming and outgoing network traffic	**500**
WEB APPLICATION SERVER		Ubuntu 16.04.7 LTS	serves as the middleware between web clients and back-end databases or other data sources.	**486**
ACCESS POINT		Cisco proprietary software	Wireless Connectivity	**405**
Domain Controller / File Server		Windows Server 2008	1)Verifies users on computer network. 2)Stores industry data (high value non personal data)	**400**
TABLET-PC1		Android 9 Pie (API 28)	Director's tablet	**343**
EMAIL SERVER		Ubuntu 16.04.7 LTS	Manages email communication	**336**
SW-FLOOR4.1 & 4.2		Cisco proprietary software	facilitates the exchange of data packets between these devices	**320**
SW-FLOOR3		Cisco proprietary software	facilitates the exchange of data packets between these devices	**320**
Industry Employee Data			Employees information	**336**
PC4&PC6		Windows 7	Sales, System and Network administration	**294**
Industry Customer Data			Customer's information	**294**
Laptop1		Windows 11 Home	Director's laptop	**288**
RADIUS/SNMP		Ubuntu 16.04.7	User's and Device's	**280**

SERVER		LTS	Management and Monitoring	
ROUTERs		Cisco proprietary software	Network Security	**280**
DNS/DHCP SERVER		Ubuntu 12.04.5 LTS	Assigns IP addresses and resolves domain names	**280**
WIRELESS-LAN-CONTROLLER1		Cisco proprietary software	manages and controls multiple access points (APs) and wireless clients	**270**
	Create New Customer	Cisco proprietary software	The system allows a new customer to register to the system	**216**
	Create New Order (Remotely)		Order registration	**216**
	Staff Payments		Planning the employees' payments	**216**
PC1&PC2			Accounting and human resources administration	**210**
SW-FLOOR2			facilitates the exchange of data packets between these devices	**210**
PC3&PC5		Windows 11 Home	Sales, System and Network administration	**210**
CRM SERVER		Windows Server 2008	Customers' information and communication management	**192**
	Customer Support		Provides help to customers	**180**
HRM SERVER		Windows Server 2008	streamlines HR operations and support the effective management of the workforce	**175**
VOIP-PHONE1		Cisco proprietary software	transmission of voice and multimedia content over the internet or IP networks	**160**
SW-FLOOR1		Cisco proprietary software	facilitates the exchange of data packets between these devices	**150**
	Staff shift hours		Planning the weekly work schedule of the staff	**112**
Edge-Router		Cisco proprietary software	packet filtering, routing packages	**128**
	Create New Order (Local)		Order registration	**100**
Industry Product			Product's	**96**

Data			information	
Industry Supplier Data			Supplier's information	**63**
PRINTER1		Epson proprietary software	Printing	**54**
Wired phone 1		Fanvil proprietary software	Secretary's wired phone	**40**

3.2. Απειλές που εντοπίστηκαν

ΑΓΑΘΟ	**ΑΠΕΙΛΗ**
LAPTOP1	Malware, Phishing Attacks, Man-in-the-Middle (MitM) Attacks, Unsecured Wi-Fi Networks, Data Theft or Loss, Weak Passwords, Physical Security Breaches
PC3&PC5	Malware, Phishing Attacks, Man-in-the-Middle (MitM) Attacks, Unsecured Wi-Fi Networks, Data Theft or Loss, Weak Passwords, Physical Security Breaches
CRM SERVER	Unpatched Software, Weak Authentication Mechanisms, SQL Injection, Cross-Site Scripting (XSS), Insecure Configuration
RADIUS/SNMP SERVER	Brute Force Attacks, Credential Phishing, Credential Theft, Man-in-the-Middle (MitM) Attacks
VOIP-PHONE1	Eavesdropping on Conversations, Interception of Call Signaling, Compromise of VoIP Endpoints, Insider Threats, Man-in-the-Middle (MitM) Attacks, Corporate Espionage and Data Theft
FIREWALL	Packet Fragmentation, Protocol Tunneling, IP Address Spoofing, Port Obfuscation, Application Layer Attacks, Covert Channels
WIRELESS-LAN-CONTROLLER1	Unauthorized Access, Man-in-the-Middle (MitM) Attacks, Denial of Service (DoS) Attacks, Rogue Access Points, Wireless Intrusion, Data Interception and Theft, Firmware Tampering, Insider Threats
TABLET-PC1	Malware, App Store Risks, Phishing Attacks, Unsecured Wi-Fi Networks, Data Theft or Loss, Unpatched Software, Physical Security Breaches, Physical Tampering
EMAIL SERVER	Phishing Attacks, Malware, Spam and Unsolicited Emails, Email Spoofing, Data Breaches, Denial of Service (DoS) Attacks, Brute Force Attacks, Man-in-the-Middle (MitM) Attacks
PC4&PC6	Malware, Phishing Attacks, Man-in-the-Middle (MitM) Attacks, Unsecured Wi-Fi Networks, Data Theft or Loss, Weak Passwords, Unpatched Software, Physical Security Breaches
PRINTER1	Unauthorized Access, Data Leakage, Malware Infection, Print Job Manipulation, Physical Security Breaches, Denial-of-Service (DoS) Attacks, Firmware Vulnerabilities
EDGE-ROUTER	Denial of Service (DoS) Attacks, Distributed Denial of Service (DDoS) Attacks, Routing Protocol Attacks, Brute Force Attacks, Credential Theft, Misconfiguration, Zero-Day Exploits, Firmware Vulnerabilities, Man-in-the-Middle (MitM) Attacks

DNS/DHCP SERVER	DNS Spoofing/Cache Poisoning, DNS Amplification Attacks, DNS Tunneling, Denial of Service (DoS) Attacks, DNSSEC Vulnerabilities, DNS Hijacking, DHCP Spoofing/DoS Attacks, Rogue DHCP Servers, Unauthorized Access, Data Breaches
HRM SERVER	Unauthorized Access, Data Breaches, Ransomware Attacks, Data Corruption or Loss, Insider Threats, Denial of Service (DoS) Attacks
SWITCHES	Denial of Service (DoS) Attacks, ARP Spoofing/ARP Poisoning, MAC Address Spoofing, VLAN Hopping, Spanning Tree Protocol (STP) Manipulation, Port Security Attacks, Firmware Exploitation, Insider Threats
ROUTERS	Unauthorized Access, Brute Force Attacks, Denial of Service (DoS) Attacks, Distributed Denial of Service (DDoS) Attacks, Firmware Vulnerabilities, DNS Hijacking, Man-in-the-Middle (MitM) Attacks, Packet Sniffing, Routing Protocol Attacks, Physical Security Breaches
WEB APPLICATION SERVER	Denial of Service (DoS) Attacks, Distributed Denial of Service (DDoS) Attacks, Injection Attacks, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Brute Force Attacks
PC1&PC2	Malware, Phishing Attacks, Man-in-the-Middle (MitM) Attacks, Unsecured Wi-Fi Networks, Data Theft or Loss, Weak Passwords, Unpatched Software, Physical Security Breaches
DOMAIN CONTROLLER/FILE SERVER	Unauthorized Access, Brute Force Attacks, Insider Threats, Data Breaches, Malware, Data Loss or Corruption, Weak Security Controls, Physical Security Breaches, Software Vulnerabilities, Network Attacks
ACCESS POINT	Unauthorized Access, Man-in-the-Middle (MitM) Attacks, Rogue Access Points, Evil Twin Attacks, Denial of Service (DoS) Attacks
Wired phone (Δικό μας αγαθό)	Eavesdropping, Phreaking, Social Engineering, Denial of Service (DoS) Attacks, Caller ID Spoofing, VoIP Vulnerabilities, Physical Security Breaches, Telephony Denial of Service (TDoS) Attacks, Voicemail Hacking, Regulatory Compliance Risks
Create New Customer	Insider Threats
Create New Order (Local)	Insider Threats
Create New Order (Remotely)	Insider Threats
Customer Support	Cybersecurity Threats
Staff shift hours (δική μας διαδικασία)	Insider Threats
Staff Payments (δική μας διαδικασία)	Insider Threats

3.3. Ευπάθειες που εντοπίστηκαν

ΑΓΑΘΟ	**ΕΥΠΑΘΕΙΑ**
LAPTOP1	ThinkCentre M710 με Windows 11 Pro (συνιστάται η τελευταία ενημέρωση αν δεν έχει γίνει), προτείνεται χρήση και εγκατάσταση Ubuntu)
PC3&PC5	ThinkCentre M710 με Windows 11 Pro (συνιστάται η τελευταία ενημέρωση αν δεν έχει

	γίνει), προτείνεται χρήση και εγκατάσταση Ubuntu)
CRM SERVER	Unwanted Code Execution (συνιστάται η κρυπτογράφηση για την προστασία των ευαίσθητων δεδομένων πελατών)
RADIUS/SNMP SERVER	Cryptographic Key Disclosure (συνιστάται η κρυπτογράφηση των κλειδιών)
VOIP-PHONE1	Aggressive Packet Moving Attack (συνισάται η ενημέρωση των συστημάτων με τις τελευταίες ενημερώσεις)
FIREWALL	FortiGate proprietary software SSL VPN Ευπάθειες (CVE-2018-13379 (FG-IR-18-384)– Πρόκειται για μια ευπάθεια διέλευσης διαδρομής στην πύλη web FortiOS SSL VPN που θα μπορούσε ενδεχομένως να επιτρέψει σε έναν εισβολέα χωρίς έλεγχο ταυτοποίησης να κατεβάσει αρχεία μέσω ειδικά δημιουργημένων αιτημάτων πόρων HTTP.
WIRELESS-LAN-CONTROLLER1	Malicious Firmware Control Attack (συνιστάται η ενημέρωση του Firmware)
TABLET-PC1	Android (πρέπει να υπάρχει η τελευταία έκδοση αυτου του λογισμικού)
EMAIL SERVER	HP ProLiant ML150 με Ubuntu 16.04.7 LTS (συνιστάται η εγκατάσταση της τελευταίας έκδοσης Ubuntu 22.04 LTS)
PC4&PC6	ThinkCentre M710 με Windows 11 Pro (συνιστάται η τελευταία ενημέρωση αν δεν έχει γίνει), προτείνεται χρήση και εγκατάσταση Ubuntu)
PRINTER1	Epson proprietary software (πρέπει να υπάρχει η τελευταία έκδοση αυτου του λογισμικού)
EDGE-ROUTER	Cisco proprietary software (πρέπει να υπάρχει η τελευταία έκδοση αυτου του λογισμικού)
DNS/DHCP SERVER	Data Disclosure Attack (συνιστάται η αποκρυπτογράφηση επικοινωνίας & η ενημέρωση λογισμικού)
HRM SERVER	Sensitive Data Disclosure Attack (συνιστάται η ενημέρωση κρυπτογράφηση και η ενημέρωση λογισμικού)
SWITCHES	Malicious Input Data Attack (συνιστάται η ενημέρωση λογισμικού και η χρήση εργαλείων παρακολούθησης για κακόβουλες δαστηριότητες στο switch)
ROUTERS	Cisco proprietary software (πρέπει να υπάρχει η τελευταία έκδοση αυτου του λογισμικού)
WEB APPLICATION SERVER	Malicious Input Data Attack (συνιστάται η ενημέρωση λογισμικού)
PC1&PC2	ThinkCentre M710 με Windows 11 Pro (συνιστάται η τελευταία ενημέρωση αν δεν έχει γίνει), προτείνεται χρήση και εγκατάσταση Ubuntu)
DOMAIN CONTROLLER/FILE SERVER	Windows Server 2008 (δεν έχουν εγκατασταθεί οι τελευταίες ενημερώσεις)
ACCESS POINT	Security Key Disclosure Attack & Denial of Service - DoS Attack (συνιστάται η χρήση ισχυρών κλειδιών

	ασφαλείας και η ενημέρωση λογισμικού)
Wired phone1 (Δικό μας αγαθό)	Eavesdropping Attack (συνιστάται η κρυπτογράφηση των κλήσεων και η επαλήθευση της ασφάλειας του δικτύου)
Create New Customer	Πιθανή διαρροή δεδομένων του πελάτη
Create New Order (Local)	Πιθανή διαρροή δεδομένων της παραγγελίας και του πελάτη
Create New Order (Remotely)	Πιθανή διαρροή δεδομένων της παραγγελίας και του πελάτη
Customer Support	Πιθανή διαρροή δεδομένων του πελάτη
Staff shift hours (δική μας διαδικασία)	Πιθανή διαρροή δεδομένων της βιομηχανίας και των εργαζομένων της
Staff Payments (δική μας διαδικασία)	Πιθανή διαρροή δεδομένων της βιομηχανίας και των εργαζομένων της

3.4. Αποτελέσματα αποτίμησης

	Απώλεια διαθεσιμότητας								Απώλεια ακεραιότητας					Αποκάλυψη			Αστοχίες και λάθη στην τηλεπικοινωνιακή μετάδοση							
Αγαθά των ΠΣ	3 ώρες	12 ώρες	1 μέρα	2 μέρες	1 εβδομάδα	2 εβδομάδες	1 μήνας	Ολική καταστροφή	Μερική απώλεια	Σκόπιμη αλλοίωση	Λάθη μικρής κλίμακας	Λάθη μεγάλης Κλίμακας	Εσωτερικούς	Παρόχους Υπηρεσιών	Εξωτερικούς	Επανάληψη μηνυμάτων	Αποτυχία αποστολέα	Αποτυχία παραλήπτη	Άρνηση αποστολής ή παραλαβής	Παραβολή λανθασμένων μηνυμάτων	Λανθασμένη δρομολόγηση	Παρακολούθηση πόντης	Μη παράδοση	Απώλεια ασκόλουθίας μηνυμάτων
LAPTOP1	3	5	8	8	9	9	9	9	8	8	5	8	4	5	8	6	4	5	7	7	8	8	8	8
PC3&PC5	1	2	3	5	6	7	7	7	5	6	3	6	2	4	6	5	4	5	5	5	6	6	6	6
CRM SERVER	3	4	7	8	8	8	8	8	6	6	3	7	4	6	7	4	4	4	6	6	7	7	7	7
RADIUS/SNMP SERVER	3	4	7	8	8	8	8	8	6	6	3	7	4	6	7	4	4	4	6	6	7	7	7	7
ROUTERs	4	7	8	8	8	8	8	8	6	7	4	8	4	6	7	5	6	6	7	7	8	8	8	8
VOIP-PHONE1	1	2	3	4	4	4	4	4	3	3	1	3	1	2	3	3	3	3	3	3	4	4	4	4
FIREWALL	9	10	10	10	10	10	10	10	9	8	5	9	5	6	8	7	7	7	8	8	9	9	9	9
WIRELESS-LAN-CONTROLLER1	6	7	9	9	9	9	9	9	6	7	4	8	4	5	8	7	7	7	8	8	8	8	8	8
TABLET-PC1	5	6	7	7	7	7	7	7	5	6	4	6	4	6	7	6	6	6	6	6	7	7	7	7
EMAIL SERVER	4	6	7	8	8	8	8	8	6	6	5	7	5	6	7	6	6	6	6	7	7	7	7	7
PC4&PC6	4	5	6	7	7	7	7	7	5	5	4	6	3	5	6	5	6	6	6	7	7	7	7	7
PRINTER1	1	2	2	3	3	3	3	3	2	2	1	2	1	2	3	2	2	2	2	3	3	3	3	3
EDGE-ROUTER	6	7	8	8	8	8	8	8	6	6	4	7	4	5	7	7	7	7	7	8	8	8	8	8

DNS/DHCP SERVER	6	7	8	8	8	8	8	8	6	6	5	7	4	6	7	6	7	7	7	7	8	8	8	8
HRM SERVER	5	6	7	7	7	7	7	7	5	6	4	6	4	5	6	5	6	6	6	6	7	7	7	7
SW-FLOOR4.1&4.2	7	7	8	8	8	8	8	8	6	7	5	7	4	5	7	6	7	7	7	7	8	8	8	8
WEB APPLICATION SERVER	7	8	9	9	9	9	9	9	7	8	6	8	5	8	8	7	8	8	8	8	9	9	9	9
PC1&PC2	4	4	5	6	6	6	6	6	4	4	3	6	4	5	6	5	5	5	5	5	6	6	6	6
DOMAIN CONTROLLER/FIL E SERVER	8	9	10	10	10	10	10	10	8	8	7	9	6	7	7	7	7	8	8	8	9	9	9	9
SW-FLOOR2	5	6	7	7	7	7	7	7	5	6	4	6	4	5	6	6	6	6	6	6	7	7	7	7
ACCESS POINT	7	9	9	9	9	9	9	9	7	7	6	8	4	5	7	7	7	7	7	7	8	8	8	8
SW-FLOOR1	5	5	6	6	6	6	6	6	4	5	4	5	3	5	5	5	5	5	5	5	6	6	6	6
SW-FLOOR3	6	7	8	8	8	8	8	8	6	6	5	7	4	5	7	6	6	6	6	6	7	7	7	7
Wired phone1 (Δικό μας αγαθό)	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
Industry Customer Data	4	5	6	6	7	7	7	7	5	5	3	6	4	5	6	3	3	3	3	5	6	6	6	6
Industry Employee Data	4	5	6	6	7	7	7	7	5	5	3	6	4	5	6	3	3	3	3	5	6	6	6	6
Industry Product Data (δικό μας δεδομένο)	2	2	3	3	4	4	4	4	2	2	2	4	1	2	3	2	2	2	3	3	3	3	3	3
Industry Supplier Data	1	1	2	2	3	3	3	3	1	1	1	3	1	1	2	1	1	1	2	2	2	2	2	2

(δικό μας δεδομένο)																								
Create New Customer	4	4	5	5	6	6	6	6	4	3	3	6	2	5	5	5	5	5	5	5	6	6	6	6
Create New Order (Local)	3	4	5	5	5	5	5	5	3	4	3	4	2	4	4	4	4	4	4	4	5	5	5	5
Create New Order (Remotely)	4	5	6	6	6	6	6	6	4	5	4	5	2	5	5	5	5	5	5	5	6	6	6	6
Customer Support	4	4	5	5	6	6	6	6	4	3	3	6	2	5	5	5	6	6	5	5	6	6	6	6
Staff shift hours (δική μας διαδικασία)	2	2	3	3	4	4	4	4	3	3	2	3	2	3	3	3	3	3	3	3	4	4	4	4
Staff Payments (δική μας διαδικασία)	4	4	5	5	6	6	6	5	4	4	3	5	3	5	5	5	5	5	5	5	6	6	6	6

Από την συμπλήρωση του πίνακα του impact assessment διακρίνουμε ότι:
Σημαντικό αντίκτυπο θα επιφέρει η απώλεια προσωπικών δεδομένων των πελατών, καθώς και των υπαλλήλων, ο οποίος σε περίπτωση απώλειας διαθεσιμότητας-απώλειας ακεραιότητας-απώλειας εμπιστευτικότητας (CIA) ή δυσλειτουργίας μπορεί επηρεάσει άμεσα την προστασία των προσωπικών δεδομένων των φυσικών προσώπων. Οι συσκευές αυτές είναι οι εξής: Laptop1, PCs, CRM Server, Web Application Server, tablet-PC1, Email Server.

Έπειτα, οι συσκευές που μπορούν να διακόψουν τη σωστή λειτουργία της βιομηχανίας (με σημαντικότατο αντίκτυπο), σε περίπτωση απώλειας των CIA ή δυσλειτουργίας, είναι οι εξής: Firewall , Edge-Router , Routers , DNS/DHCP Server , Domain Controller / File Server, Access Point, Wireless LAN Controller Server. Τέλος είναι όλα τα υπόλοιπα αγαθά που έχουν περισσότερο οικονομικό, οργανωτικό, νομικό αντίκτυπο για τη βιομηχανία.

4. ΠΡΟΤΕΙΝΟΜΕΝΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

Τα προτεινόμενα Μέτρα Προστασίας εντάσσονται σε έντεκα (11) γενικές κατηγορίες:

Α1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

Α2. Ταυτοποίηση και αυθεντικοποίηση

Α3. Έλεγχος προσπέλασης και χρήσης πόρων

Α4. Διαχείριση εμπιστευτικών δεδομένων

Α5. Προστασία από τη χρήση υπηρεσιών από τρίτους

Α6. Προστασία λογισμικού

Α7. Διαχείριση ασφάλειας δικτύου

Α8. Προστασία από ιομορφικό λογισμικό

Α9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

Α10. Ασφάλεια εξοπλισμού

Α11. Φυσική ασφάλεια κτιριακής εγκατάστασης

Τα μέτρα έχουν εφαρμογή στο ΠΣ της βιομηχανίας καλλυντικών και αρωμάτων.

4.1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

- **Κατάχρηση υπερβολικών δικαιωμάτων**: Περιορισμός των δικαιωμάτων πρόσβασης στα δεδομένα με βάση το ανάγκες των χρηστών και των ρόλων τους.
- **Μη κατάλληλα διαμορφωμένοι κανόνες:** Αναθεώρηση και ενημέρωση των κανόνων ασφαλείας και πολιτικών της εταιρείας για να εξασφαλιστεί ότι είναι επαρκώς διαμορφωμένοι και εφαρμόζονται σωστά.
- **Μη κρυπτογραφημένη βάση δεδομένων:** Εφαρμογή της κρυπτογράφησης δεδομένων σε επίπεδο βάσης δεδομένων για προστασία των ευαίσθητων πληροφοριών.
- **Κακή αντιμετώπιση εσωτερικής απειλής:** Η υιοθέτηση μιας προληπτικής προσέγγισης, με τη χρήση λογισμικού ανίχνευσης απειλών και παραβάσεων, μπορεί να βοηθήσει στην ανίχνευση ανωμαλιών και στην αντίδραση πριν από την εμφάνιση προβλημάτων.
- **Αδύναμος κωδικός πρόσβασης**: Επιβολή πολιτικών για ισχυρούς κωδικούς πρόσβασης και εκπαίδευση των χρηστών για την επιλογή και τη διαχείριση ασφαλών κωδικών.
- **Κακή διαχείριση προνομίων:** Η εφαρμογή αρχών του λιγότερου προνομίου, όπως τον περιορισμό της πρόσβασης με την αρχή του χωρισμού των καθηκόντων (principle of least privilege), μπορεί να

αποτρέψει την κατάχρηση προνομίων από εσωτερικούς ή εξωτερικούς παράγοντες.

- **Αποκλεισμός των υπηρεσιών (DoS) επιθέσεις:** Η χρήση λύσεων όπως οι firewalls, οι intrusion detection και οι ανιχνευτές κακόβουλου λογισμικού μπορεί να βοηθήσει στον εντοπισμό και τον αποκλεισμό αυτών των επιθέσεων.
- **Ανεπαρκής ασφάλεια δεδομένων:** Η διαμόρφωση της πρόσβασης στα δεδομένα με τη χρήση τεχνολογιών όπως η διαχείριση ταυτοποίησης και πρόσβασης (IAM), καθώς και η εφαρμογή της αρχής του χωρισμού των καθηκόντων, μπορεί να βοηθήσει στην προστασία των δεδομένων από εσωτερικές απειλές.
- **Κρυφάκουσμα συνομιλιών και παρέμβαση τηλεφωνημάτων:** Επιλογή εφαρμογών επικοινωνίας που προσφέρουν ενσωματωμένη κρυπτογράφηση για τις κλήσεις και τα μηνύματα. Ορισμένες εφαρμογές ακόμα προσφέρουν ειδικά χαρακτηριστικά για ανωνυμία και ασφάλεια στις επικοινωνίες.

4.2. Ταυτοποίηση και αυθεντικοποίηση

- **Μη κατάλληλα διαμορφωμένοι κανόνες:** Αναθεώρηση και ενημέρωση των κανόνων ασφαλείας και πολιτικών της εταιρείας για να εξασφαλιστεί ότι είναι επαρκώς διαμορφωμένοι και εφαρμόζονται σωστά.
- **Κατάχρηση υπερβολικών δικαιωμάτων:** Περιορισμός των δικαιωμάτων πρόσβασης στα δεδομένα με βάση τις ανάγκες των χρηστών και των ρόλων τους.
- Αδύναμοι μηχανισμοί πιστοποίησης και μη ασφαλείς κανάλια επικοινωνίας: Εφαρμογή ασφαλών μηχανισμών πιστοποίησης όπως πολύπλοκοι κωδικοί και πολυπαραμετρική πιστοποίηση (π.χ. παραγόμενοι κωδικοί), και χρήση κρυπτογράφησης για την ασφαλή μετάδοση δεδομένων μέσω ασφαλών καναλιών επικοινωνίας.
- **Απάτη διαπιστευτηρίων (Credential Phishing):** Εκπαίδευση των χρηστών για την αναγνώριση απάτης διαπιστευτηρίων, χρήση διπλού παράθυρου ελέγχου, εφαρμογή της πολυπαραμετρικής πιστοποίησης και χρήση πιστοποιητικών SSL.
- **Μη εξουσιοδοτημένη πρόσβαση:** Εφαρμογή αυστηρών πολιτικών πρόσβασης, περιορισμός της πρόσβασης σε ανάγκες με βάση τον ρόλο του χρήστη και την χρήση πολιτικών πρόσβασης βάσει της αρχής του ελάχιστου δικαιώματος.
- **Αποκλεισμός των υπηρεσιών (DoS) επιθέσεις:** Η χρήση λύσεων όπως οι firewalls, οι intrusion detection και οι ανιχνευτές κακόβουλου

λογισμικού μπορεί να βοηθήσει στον εντοπισμό και τον αποκλεισμό αυτών των επιθέσεων.

- **Μη πλήρης αυθεντικοποίηση αποστολέα πακέτου:** Εφαρμογή μηχανισμών αυθεντικοποίησης στο επίπεδο των πακέτων δεδομένων στο δίκτυο. Αυτό μπορεί να περιλαμβάνει τη χρήση μηχανισμών όπως Digital Signatures ή HMAC (Hash-based Message Authentication Code) για να εξασφαλίσετε ότι τα πακέτα δεδομένων προέρχονται από εξουσιοδοτημένους αποστολείς και δεν έχουν τροποποιηθεί κατά τη μετάδοση τους.
- **Πρόσβαση στο δίκτυο από μη εξουσιοδοτημένους χρήστες:** Εφαρμογή τεχνολογιών ελέγχου πρόσβασης, όπως IEEE 802.1X, που απαιτούν αυθεντικοποίηση χρήστη πριν από την παροχή πρόσβασης στο δίκτυο. Αυτό επιτρέπει την επαλήθευση ταυτότητας και την αντιστοίχιση των δικαιωμάτων πρόσβασης με τους χρήστες που πραγματοποιούν πρόσβαση στο δίκτυο.

4.3. Έλεγχος προσπέλασης και χρήσης πόρων

- **Κατάχρηση υπερβολικών δικαιωμάτων**: Περιορισμός των δικαιωμάτων πρόσβασης στα δεδομένα με βάση το ανάγκες των χρηστών και των ρόλων τους.
- **Μη κατάλληλα διαμορφωμένοι κανόνες:** Αναθεώρηση και ενημέρωση των κανόνων ασφαλείας και πολιτικών της εταιρείας για να εξασφαλιστεί ότι είναι επαρκώς διαμορφωμένοι και εφαρμόζονται σωστά.
- **Μη εξουσιοδοτημένη πρόσβαση:** Εφαρμογή αυστηρών πολιτικών πρόσβασης, περιορισμός της πρόσβασης σε ανάγκες με βάση τον ρόλο του χρήστη και την χρήση πολιτικών πρόσβασης βάσει της αρχής του ελάχιστου δικαιώματος.
- **Μη κρυπτογραφημένη βάση δεδομένων:** Εφαρμογή της κρυπτογράφησης δεδομένων σε επίπεδο βάσης δεδομένων για προστασία των ευαίσθητων πληροφοριών.
- **Κακή αντιμετώπιση εσωτερικής απειλής:** Η υιοθέτηση μιας προληπτικής προσέγγισης, με τη χρήση λογισμικού ανίχνευσης απειλών και παραβάσεων, μπορεί να βοηθήσει στην ανίχνευση ανωμαλιών και στην αντίδραση πριν από την εμφάνιση προβλημάτων.
- **Πρόσβαση στο δίκτυο από μη εξουσιοδοτημένους χρήστες:** Εφαρμογή συστήματος ελέγχου πρόσβασης (NAC - Network Access Control) για να διασφαλιστεί ότι μόνο εξουσιοδοτημένοι χρήστες

έχουν πρόσβαση στο δίκτυο. Επιπλέον, χρήση δυνατοτήτων συσκευασίας για κρυπτογράφηση της επικοινωνίας στο δίκτυο.

- **Πρόσβαση σε προσωπικά και εταιρικά δεδομένα:** Εφαρμογή πολιτικών πρόσβασης με βάση τον ρόλο του χρήστη και την ανάγκη του. Χρήση τεχνολογιών κρυπτογράφησης για την προστασία των δεδομένων σε κίνηση και αναπαραγωγή.
- **Παρωχημένο λογισμικό:** Εφαρμογή αυτοματοποιημένου συστήματος ενημέρωσης λογισμικού και επιθεώρησης τακτικά των εφαρμογών για την εντοπισμό και τη διόρθωση ευπαθειών.
- **Πρόσβαση σε δεδομένα του συστήματος:** Εφαρμογή περιορισμένων δικαιωμάτων πρόσβασης και αυστηρών πολιτικών πρόσβασης για την προστασία των δεδομένων του συστήματος.
- **Αποστολή ή λήψη εμπιστευτικών δεδομένων από μη εξουσιοδοτημένους χρήστες:** Εφαρμογή μέσων αυθεντικοποίησης και εξουσιοδότησης για την αποτροπή της αποστολής ή λήψης δεδομένων από μη εξουσιοδοτημένους χρήστες. Χρήση τεχνολογιών κρυπτογράφησης για την ασφαλή μετάδοση εμπιστευτικών δεδομένων.

4.4. Διαχείριση εμπιστευτικών δεδομένων

- **Αδύναμος κωδικός πρόσβασης**: Επιβολή πολιτικών για ισχυρούς κωδικούς πρόσβασης και εκπαίδευση των χρηστών για την επιλογή και τη διαχείριση ασφαλών κωδικών.
- **Κακόβουλο λογισμικό:** Εφαρμογή Αντι-Κακόβουλου Λογισμικού (Anti-Malware Software) και ενημέρωση Λογισμικού και Λειτουργικού Συστήματος με τις τελευταίες εκδόσεις και πατσιμένα με τις πιο πρόσφατες ασφαλειακές ενημερώσεις για μείωση τον κίνδυνο εκμετάλλευσης ευπαθειών.
- **Πρόσβαση σε προσωπικά και εταιρικά δεδομένα:** Εφαρμογή πολιτικών πρόσβασης με βάση τον ρόλο του χρήστη και την ανάγκη του. Χρήση τεχνολογιών κρυπτογράφησης για την προστασία των δεδομένων σε κίνηση και αναπαραγωγή.
- **Μη πλήρης αυθεντικοποίηση αποστολέα πακέτου:** Εφαρμογή μηχανισμών αυθεντικοποίησης στο επίπεδο των πακέτων δεδομένων στο δίκτυο. Αυτό μπορεί να περιλαμβάνει τη χρήση μηχανισμών όπως Digital Signatures ή HMAC (Hash-based Message Authentication Code) για να εξασφαλίσετε ότι τα πακέτα

δεδομένων προέρχονται από εξουσιοδοτημένους αποστολείς και δεν έχουν τροποποιηθεί κατά τη μετάδοση τους.

- **Πρόσβαση στο δίκτυο από μη εξουσιοδοτημένους χρήστες:** Εφαρμογή τεχνολογιών ελέγχου πρόσβασης, όπως IEEE 802.1X, που απαιτούν αυθεντικοποίηση χρήστη πριν από την παροχή πρόσβασης στο δίκτυο. Αυτό επιτρέπει την επαλήθευση ταυτότητας και την αντιστοίχιση των δικαιωμάτων πρόσβασης με τους χρήστες που πραγματοποιούν πρόσβαση στο δίκτυο.
- **Κακή αντιμετώπιση εσωτερικής απειλής:** Η υιοθέτηση μιας προληπτικής προσέγγισης, με τη χρήση λογισμικού ανίχνευσης απειλών και παραβάσεων, μπορεί να βοηθήσει στην ανίχνευση ανωμαλιών και στην αντίδραση πριν από την εμφάνιση προβλημάτων.
- **Μη κρυπτογραφημένη βάση δεδομένων:** Εφαρμογή της κρυπτογράφησης δεδομένων σε επίπεδο βάσης δεδομένων για προστασία των ευαίσθητων πληροφοριών.
- **Κρυφάκουσμα συνομιλιών και παρέμβαση τηλεφωνημάτων:** Επιλογή εφαρμογών επικοινωνίας που προσφέρουν ενσωματωμένη κρυπτογράφηση για τις κλήσεις και τα μηνύματα. Ορισμένες εφαρμογές ακόμα προσφέρουν ειδικά χαρακτηριστικά για ανωνυμία και ασφάλεια στις επικοινωνίες.

4.5. Προστασία από τη χρήση υπηρεσιών από τρίτους

- **Μη πλήρης αυθεντικοποίηση αποστολέα πακέτου:** Εφαρμογή μηχανισμών αυθεντικοποίησης στο επίπεδο των πακέτων δεδομένων στο δίκτυο. Αυτό μπορεί να περιλαμβάνει τη χρήση μηχανισμών όπως Digital Signatures ή HMAC (Hash-based Message Authentication Code) για να εξασφαλίσετε ότι τα πακέτα δεδομένων προέρχονται από εξουσιοδοτημένους αποστολείς και δεν έχουν τροποποιηθεί κατά τη μετάδοση τους.
- **Πρόσβαση στο δίκτυο από μη εξουσιοδοτημένους χρήστες:** Εφαρμογή τεχνολογιών ελέγχου πρόσβασης, όπως IEEE 802.1X, που απαιτούν αυθεντικοποίηση χρήστη πριν από την παροχή πρόσβασης στο δίκτυο. Αυτό επιτρέπει την επαλήθευση ταυτότητας και την αντιστοίχιση των δικαιωμάτων πρόσβασης με τους χρήστες που πραγματοποιούν πρόσβαση στο δίκτυο.

- **Κακή αντιμετώπιση εσωτερικής απειλής:** Η υιοθέτηση μιας προληπτικής προσέγγισης, με τη χρήση λογισμικού ανίχνευσης απειλών και παραβάσεων, μπορεί να βοηθήσει στην ανίχνευση ανωμαλιών και στην αντίδραση πριν από την εμφάνιση προβλημάτων.
- **Πρόσβαση σε δεδομένα του συστήματος:** Εφαρμογή περιορισμένων δικαιωμάτων πρόσβασης και αυστηρών πολιτικών πρόσβασης για την προστασία των δεδομένων του συστήματος.
- **Κρυφάκουσμα συνομιλιών και παρέμβαση τηλεφωνημάτων:** Επιλογή εφαρμογών επικοινωνίας που προσφέρουν ενσωματωμένη κρυπτογράφηση για τις κλήσεις και τα μηνύματα. Ορισμένες εφαρμογές ακόμα προσφέρουν ειδικά χαρακτηριστικά για ανωνυμία και ασφάλεια στις επικοινωνίες.
- **Λαναθασμένη διαμόρφωση (Misconfiguration):** Εφαρμογή εργαλείων αυτοματοποιημένου ελέγχου διαμόρφωσης για τον εντοπισμό και τη διόρθωση λανθασμένων ρυθμίσεων στο σύστημα. Αυτά τα εργαλεία μπορούν να βοηθήσουν στην εξάλειψη πιθανών ευπαθειών λόγω μη σωστών ρυθμίσεων.
- **Κακόβουλο λογισμικό:** Εφαρμογή Αντι-Κακόβουλου Λογισμικού (Anti-Malware Software) και ενημέρωση Λογισμικού και Λειτουργικού Συστήματος με τις τελευταίες εκδόσεις και πατσιμένα με τις πιο πρόσφατες ασφαλειακές ενημερώσεις για μείωση τον κίνδυνο εκμετάλλευσης ευπαθειών.
- **Μη εξουσιοδοτημένη πρόσβαση:** Εφαρμογή αυστηρών πολιτικών πρόσβασης, περιορισμός της πρόσβασης σε ανάγκες με βάση τον ρόλο του χρήστη και την χρήση πολιτικών πρόσβασης βάσει της αρχής του ελάχιστου δικαιώματος.

4.6. Προστασία λογισμικού

- **Κακόβουλο λογισμικό:** Εφαρμογή Αντι-Κακόβουλου Λογισμικού (Anti-Malware Software) και ενημέρωση Λογισμικού και Λειτουργικού Συστήματος με τις τελευταίες εκδόσεις και πατσιμένα με τις πιο πρόσφατες ασφαλειακές ενημερώσεις για μείωση τον κίνδυνο εκμετάλλευσης ευπαθειών.
- **Παρωχημένο λογισμικό:** Εφαρμογή αυτοματοποιημένου συστήματος ενημέρωσης λογισμικού και επιθεώρησης τακτικά των εφαρμογών για την εντοπισμό και τη διόρθωση ευπαθειών.

4.7. Διαχείριση ασφάλειας δικτύου

- **Μη κρυπτογραφημένη βάση δεδομένων:** Εφαρμογή της κρυπτογράφησης δεδομένων σε επίπεδο βάσης δεδομένων για προστασία των ευαίσθητων πληροφοριών.
- **Κακή αντιμετώπιση εσωτερικής απειλής:** Η υιοθέτηση μιας προληπτικής προσέγγισης, με τη χρήση λογισμικού ανίχνευσης απειλών και παραβάσεων, μπορεί να βοηθήσει στην ανίχνευση ανωμαλιών και στην αντίδραση πριν από την εμφάνιση προβλημάτων.
- **Αδύναμος κωδικός πρόσβασης**: Επιβολή πολιτικών για ισχυρούς κωδικούς πρόσβασης και εκπαίδευση των χρηστών για την επιλογή και τη διαχείριση ασφαλών κωδικών.
- **Αποκλεισμός των υπηρεσιών (DoS) επιθέσεις:** Η χρήση λύσεων όπως οι firewalls, οι intrusion detection και οι ανιχνευτές κακόβουλου λογισμικού μπορεί να βοηθήσει στον εντοπισμό και τον αποκλεισμό αυτών των επιθέσεων.
- **Ανεπαρκής ασφάλεια δεδομένων:** Η διαμόρφωση της πρόσβασης στα δεδομένα με τη χρήση τεχνολογιών όπως η διαχείριση ταυτοποίησης και πρόσβασης (IAM), καθώς και η εφαρμογή της αρχής του χωρισμού των καθηκόντων, μπορεί να βοηθήσει στην προστασία των δεδομένων από εσωτερικές απειλές.
- **Απάτη διαπιστευτηρίων (Credential Phishing):** Εκπαίδευση των χρηστών για την αναγνώριση απάτης διαπιστευτηρίων, χρήση διπλού παράθυρου ελέγχου, εφαρμογή της πολυπαραμετρικής πιστοποίησης και χρήση πιστοποιητικών SSL.
- **Μη εξουσιοδοτημένη πρόσβαση:** Εφαρμογή αυστηρών πολιτικών πρόσβασης, περιορισμός της πρόσβασης σε ανάγκες με βάση τον ρόλο του χρήστη και την χρήση πολιτικών πρόσβασης βάσει της αρχής του ελάχιστου δικαιώματος.
- **Πρόσβαση στο δίκτυο από μη εξουσιοδοτημένους χρήστες:** Εφαρμογή τεχνολογιών ελέγχου πρόσβασης, όπως IEEE 802.1X, που απαιτούν αυθεντικοποίηση χρήστη πριν από την παροχή πρόσβασης στο δίκτυο. Αυτό επιτρέπει την επαλήθευση ταυτότητας και την αντιστοίχιση των δικαιωμάτων πρόσβασης με τους χρήστες που πραγματοποιούν πρόσβαση στο δίκτυο.
- **Παρωχημένο λογισμικό:** Εφαρμογή αυτοματοποιημένου συστήματος ενημέρωσης λογισμικού και επιθεώρησης τακτικά των εφαρμογών για την εντοπισμό και τη διόρθωση ευπαθειών.
- **Πρόσβαση σε προσωπικά και εταιρικά δεδομένα:** Εφαρμογή πολιτικών πρόσβασης με βάση τον ρόλο του χρήστη και την ανάγκη

του. Χρήση τεχνολογιών κρυπτογράφησης για την προστασία των δεδομένων σε κίνηση και αναπαραγωγή.

- **Αποστολή ή λήψη εμπιστευτικών δεδομένων από μη εξουσιοδοτημένους χρήστες:** Εφαρμογή μέσων αυθεντικοποίησης και εξουσιοδότησης για την αποτροπή της αποστολής ή λήψης δεδομένων από μη εξουσιοδοτημένους χρήστες. Χρήση τεχνολογιών κρυπτογράφησης για την ασφαλή μετάδοση εμπιστευτικών δεδομένων.

4.8. Προστασία από ιομορφικό λογισμικό

- **Κακόβουλο λογισμικό:** Εφαρμογή Αντι-Κακόβουλου Λογισμικού (Anti-Malware Software) και ενημέρωση Λογισμικού και Λειτουργικού Συστήματος με τις τελευταίες εκδόσεις και πατσιμένα με τις πιο πρόσφατες ασφαλειακές ενημερώσεις για μείωση τον κίνδυνο εκμετάλλευσης ευπαθειών.
- **Παρωχημένο λογισμικό:** Εφαρμογή αυτοματοποιημένου συστήματος ενημέρωσης λογισμικού και επιθεώρησης τακτικά των εφαρμογών για την εντοπισμό και τη διόρθωση ευπαθειών.

4.9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

- **Πρόσβαση στο δίκτυο από μη εξουσιοδοτημένους χρήστες:** Εφαρμογή τεχνολογιών ελέγχου πρόσβασης, όπως IEEE 802.1X, που απαιτούν αυθεντικοποίηση χρήστη πριν από την παροχή πρόσβασης στο δίκτυο. Αυτό επιτρέπει την επαλήθευση ταυτότητας και την αντιστοίχιση των δικαιωμάτων πρόσβασης με τους χρήστες που πραγματοποιούν πρόσβαση στο δίκτυο.

- **<u>Μη εξουσιοδοτημένη πρόσβαση</u>:** Εφαρμογή αυστηρών πολιτικών πρόσβασης, περιορισμός της πρόσβασης σε ανάγκες με βάση τον ρόλο του χρήστη και την χρήση πολιτικών πρόσβασης βάσει της αρχής του ελάχιστου δικαιώματος.
- **<u>Κακόβουλο λογισμικό</u>:** Εφαρμογή Αντι-Κακόβουλου Λογισμικού (Anti-Malware Software) και ενημέρωση Λογισμικού και Λειτουργικού Συστήματος με τις τελευταίες εκδόσεις και πατσιμένα με τις πιο πρόσφατες ασφαλειακές ενημερώσεις για μείωση τον κίνδυνο εκμετάλλευσης ευπαθειών.
- **<u>Αποκλεισμός των υπηρεσιών (DoS) επιθέσεις</u>:** Η χρήση λύσεων όπως οι firewalls, οι intrusion detection και οι ανιχνευτές κακόβουλου λογισμικού μπορεί να βοηθήσει στον εντοπισμό και τον αποκλεισμό αυτών των επιθέσεων.

4.10. Ασφάλεια εξοπλισμού

- **<u>Αντικατάσταση και Επισκευή Κατεστραμμένου Εξοπλισμού</u>:** Σε περίπτωση φυσικής επίθεσης στον εξοπλισμό, είναι σημαντικό να αντικατασταθεί ή να επισκευαστεί άμεσα ο κατεστραμμένος εξοπλισμός. Επιπλέον, πρέπει να διερευνηθεί η αιτία της επίθεσης και να ληφθούν τα αναγκαία μέτρα για να αποφευχθεί η επανάληψη του περιστατικού.

4.11. Φυσική ασφάλεια κτιριακής εγκατάστασης

- **<u>Αντικατάσταση και Επισκευή Κατεστραμμένου Εξοπλισμού</u>:** Σε περίπτωση φυσικής επίθεσης στον εξοπλισμό, είναι σημαντικό να αντικατασταθεί ή να επισκευαστεί άμεσα ο κατεστραμμένος εξοπλισμός. Επιπλέον, πρέπει να διερευνηθεί η αιτία της επίθεσης και να ληφθούν τα αναγκαία μέτρα για να αποφευχθεί η επανάληψη του περιστατικού.

5. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

ΥΛΙΚΟ	ΑΠΕΙΛΗ
FIREWALL	Malware, Perimeter Attacks, Resource Exhaustion Attacks, Unwanted Communication, Destructive Attacks
WEB APPLICATION SERVER	DoS Attacks, Injection Attacks, Authentication Bypass, Data Breaches, Malware
ACCESS POINT	Unauthorized access, Authentication Attack, DoS Attacks, Forced Entry, Malware
Domain Controller / File Server	Unauthorized access, Malware, Excessive Privilege Abuse, Insider threats, Network attacks

Οι 4 αυτές συσκευές πιστεύουμε ότι είναι οι πιο κρίσιμες καθώς από αυτές εξαρτάται άμεσα η σωστή λειτουργία της βιομηχανίας, και τη διαφύλαξη των ευαίσθητων δεδομένων των πελατών καθώς και του προσωπικού. Συχνά, οι κατασκευαστές δεν επενδύουν πάνω στην ασφάλεια τους, κυρίως λόγω του κόστους, διότι επένδυση σε μέτρα ασφαλείας μπορεί να είναι δαπανηρή. Δεν το κάνουν όλοι οι κατασκευαστές αυτό, όμως όταν η ασφάλεια παραμελείται, μπορεί να οδηγήσει σε σοβαρές συνέπειες για τους εργαζόμενους, τους πελάτες και την ευρύτερη κοινότητα. Ως εκ τούτου, είναι σημαντικό για τους κατασκευαστές να δίνουν προτεραιότητα στην ασφάλεια και να επενδύουν σε μέτρα που προστατεύουν τους εργαζομένους τους και το κοινό.