ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Πληροφορικής

Εικόνα που περιέχει ορθογώνιο παραλληλόγραμμο, σχεδίαση

Το περιεχόμενο που δημιουργείται από τεχνολογία AI ενδέχεται να είναι εσφαλμένο.

Εργασία Μαθήματος ***Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων***

|  |  |
| --- | --- |
| Αρ. Άσκησης - Τίτλος Άσκησης | ***Ανάλυση και Διαχείριση Επικινδυνότητας*** |
| Όνομα φοιτητή - Αρ. Μητρώου  (όλων σε περίπτωση ομαδικής εργασίας) | Γιαννίκος Παναγιώτης – ΜΠΚΕΔ24007 |
| Μπαλτζής Δημήτρης – ΜΠΚΕΔ24026 |
| Ραυτόπουλος Μάριος – ΜΠΚΕΔ24034 |
| Ημερομηνία παράδοσης | 25/02/25 |

**Εργασία B: Ανάλυσης και Διαχείρισης Επικινδυνότητας**

Περιγραφή:

Επιλέξτε ένα οργανισμό/εταιρεία/φορέα που φιλοξενεί πληροφοριακό σύστημα ή περιγράψτε τα πληροφοριακά αγαθά που εμπλέκονται στην παροχή μιας Υπηρεσίας Εφοδιαστικής Αλυσίδας  και πραγματοποιήστε:

1. Μελέτη Ανάλυσης και Διαχείρισης Επικινδυνότητας η οποία θα πρέπει να περιλαμβάνει:
   * Περιγραφή της Μεθοδολογίας
   * Περιγραφή του Οργανισμού/ Εταιρίας/ Φορέα / Εφοδιαστικής Υπηρεσίας
   * Απαιτήσεις Ασφάλειας - Νομικές Απαιτήσεις
   * Χαρτογράφηση ΠΣ / αγαθών (Cartography)
   * Αποτίμηση Επιπτώσεων (Impact Assessment)
   * Αποτίμηση Απειλών (Threat Assessment)
   * Αποτίμηση Αδυναμιών (Vulnerability Assessment)
   * Αποτίμηση Κινδύνων (Risk Analysis)
   * Προτεινόμενα Μέτρα Προστασίας (Proposed Security Countermeasures)
   * Σχέδιο Υλοποίησης Μέτρων Προστασίας (Risk Treatment Plan)
2. Κατανομή οργανωτικών δομών και αρμοδιοτήτων ασφάλειας (Security Roles and Responsibilities)
3. Βασικές Πολιτικές Ασφάλειας (Access Control Policy, Password Policy, Logging Policy, Backup Policy)
4. Βασικές Διαδικασίες (Διαδικασία αντιμετώπισης περιστατικών ασφάλειας, Διαδικασία Backup, Διαδικασία Δημιουργίας / Διαγραφής Χρήστη)

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

[1. Μελέτη Ανάλυσης και Διαχείρισης Επικινδυνότητας 3](#_Toc189773537)

[1.1 Περιγραφή της Μεθοδολογίας 3](#_Toc189773538)

[1.2 Περιγραφή του Οργανισμού/ Εταιρίας/ Φορέα / Εφοδιαστικής Υπηρεσίας 4](#_Toc189773539)

[1.3 Απαιτήσεις Ασφαλείας – Νομικές Απαιτήσεις 4](#_Toc189773540)

[1.4 Χαρτογράφηση Αγαθών 5](#_Toc189773541)

[1.5 Αποτίμηση Επιπτώσεων (Impact Assessment) 7](#_Toc189773542)

[1.6 Αποτίμηση Απειλών (Threat Assessment) 8](#_Toc189773543)

[1.7 Αποτίμηση Αδυναμιών 8](#_Toc189773544)

[1.8 Αποτίμηση Κινδύνων (Risk Assessment) 9](#_Toc189773545)

[1.9 Προτεινόμενα Μέτρα Προστασίας ( Proposed Security Countermeasures) 9](#_Toc189773546)

[1.10 Σχέδιο Υλοποίησης Μέτρων Προστασίας 10](#_Toc189773547)

[2. Κατανομή οργανωτικών δομών και αρμοδιοτήτων ασφάλειας (Security Roles and Responsibilities) 10](#_Toc189773548)

[3. Βασικές Πολιτικές Ασφάλειας (Access Control Policy, Password Policy, Logging Policy, Backup Policy) 11](#_Toc189773549)

[4. Βασικές Διαδικασίες (Διαδικασία αντιμετώπισης περιστατικών ασφάλειας, Διαδικασία Backup, Διαδικασία Δημιουργίας / Διαγραφής Χρήστη) 12](#_Toc189773550)

# **1. Μελέτη Ανάλυσης και Διαχείρισης Επικινδυνότητας**

## 1.1 Περιγραφή της Μεθοδολογίας

Η μεθοδολογία που ακολουθείται βασίζεται στις πρακτικές ISO 27005 για τη διαχείριση και αποτίμηση κινδύνων. Η ανάλυση επικεντρώνεται στα πληροφοριακά αγαθά που σχετίζονται με την υπηρεσία Managed SIEM που παρέχει το Security Operations Center (SOC).

Μια υπηρεσία Managed SIEM είναι ιδανική γιατί:

Συλλέγει, αποθηκεύει, επεξεργάζεται και αναλύει πληροφοριακά δεδομένα.

Διαχειρίζεται logs, ειδοποιήσεις ασφαλείας, network traffic, threat intelligence data.

Εμπλέκει πολλές κατηγορίες πληροφοριακών αγαθών, όπως πελατειακά δεδομένα, λειτουργικά δεδομένα και δεδομένα ασφαλείας.

Είναι κρίσιμη για τη λειτουργία επιχειρήσεων που θέλουν να εντοπίζουν και να αποκρίνονται σε απειλές.

Αρχικά, πραγματοποιείται ταυτοποίηση και αποτίμηση της αξίας των πληροφοριακών αγαθών, συμπεριλαμβανομένων των δεδομένων, των λογισμικών, του υλικού εξοπλισμού και των φυσικών υποδομών που εμπλέκονται στην υπηρεσία. Η αξία των πληροφοριακών αγαθών καθορίζει και την αξία των αγαθών στα οποία συμπεριλαμβάνεται.

Στη συνέχεια, εκτελείται Impact Assessment, όπου αξιολογούνται οι πιθανές επιπτώσεις από απώλεια εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας των αγαθών. Σε αυτή τη διαδικασία, υιοθετείται η προσέγγιση worst-case scenario, καταγράφοντας τη μέγιστη δυνατή επίδραση που θα μπορούσε να προκύψει.

Ακολουθεί Threat & Vulnerability Assessment, όπου εντοπίζονται οι πιθανές απειλές και αδυναμίες που θα μπορούσαν να επηρεάσουν την υπηρεσία SOC, βασισμένες σε διεθνή πρότυπα, στατιστικά στοιχεία κυβερνοεπιθέσεων (π.χ., ENISA Threat Landscape, MITRE ATT&CK) και security controls που εφαρμόζονται σε SOCs.

Τέλος, πραγματοποιείται Risk Analysis, όπου εκτιμάται το συνολικό ρίσκο, και διαμορφώνεται ένα Risk Treatment Plan. Το σχέδιο αυτό περιλαμβάνει προτεινόμενα μέτρα προστασίας και στρατηγικές μετριασμού των κινδύνων, διασφαλίζοντας τη συνέχεια και την ασφαλή λειτουργία του SOC.

## 1.2 Περιγραφή του Οργανισμού/ Εταιρίας/ Φορέα / Εφοδιαστικής Υπηρεσίας

Η ανάλυση επικεντρώνεται στην υπηρεσία managed SIEM, η οποία διασφαλίζει την συνεχιζόμενη παρακολούθηση και ασφάλεια των πληροφοριακών συστημάτων ενός οργανισμού ή υπηρεσίας. Οι βασικές λειτουργίες περιλαμβάνουν:

Παρακολούθηση Δικτύου (Network Monitoring):

Ανίχνευση Νέων Συσκευών: Παρακολούθηση του δικτύου για την αναγνώριση νέων συσκευών που συνδέονται με το δίκτυο.

Διαχείριση Καταγραφών Δικτύου (Network Logs): Ανάλυση των καταγραφών του δικτύου για την ανίχνευση ανωμαλιών και παραβιάσεων.

Μοτίβα Επικοινωνίας Συσκευών (Device Communication Patterns): Εξετάζονται τα πρότυπα επικοινωνίας των συσκευών για τον εντοπισμό ύποπτης δραστηριότητας.

Ανατροφοδότηση Απειλών (Threat Intelligence Feeds): Χρήση feeds από αξιόπιστες πηγές για τη λήψη ενημερώσεων σχετικά με νέες απειλές ή κακόβουλο λογισμικό.

Αναγνώριση Ευπαθειών (Vulnerabilities) και Ενημερώσεις Λογισμικού (Patches): Παρακολούθηση και εφαρμογή των τελευταίων ενημερώσεων και διορθώσεων ασφάλειας.

Ανίχνευση και Αντιμετώπιση Περιστατικών (Incident Detection and Response):

Αντιμετώπιση Σοβαρών Περιστατικών: Χρησιμοποιούνται manuals και πρωτόκολλα αντίδρασης σε περιστατικά (incident response protocols) για την άμεση και οργανωμένη διαχείριση σοβαρών περιστατικών ασφαλείας.

Ενημερώσεις για Ενημέρωση Λογισμικού (Updates for Software Patches): Διαχείριση και εφαρμογή ενημερώσεων για το λογισμικό, εξασφαλίζοντας ότι το σύστημα παραμένει προστατευμένο από νέες απειλές.

Ασφαλής Χρήση Πρωτοκόλλων και Κωδικών Πρόσβασης: Ενημέρωση για την αποφυγή χρήσης ανασφαλών πρωτοκόλλων και κωδικών πρόσβασης και την προώθηση ασφαλών πρακτικών, όπως η υιοθέτηση MFA (Multi-Factor Authentication).

Έρευνα Πιθανών Κινδύνων: Διαρκής ανάλυση της ασφάλειας για να εντοπιστούν και να αντιμετωπιστούν πιθανοί κίνδυνοι πριν επηρεάσουν τα συστήματα ή τα δεδομένα.

## 1.3 Απαιτήσεις Ασφαλείας – Νομικές Απαιτήσεις

Απαιτήσεις Ασφαλείας για την Υπηρεσία SOC:

Ελεγχόμενη Πρόσβαση:

Χρήση συστημάτων ελέγχου πρόσβασης για την ασφαλή πρόσβαση στους χώρους όπου πραγματοποιείται η παρακολούθηση και διαχείριση των δεδομένων (π.χ., SOC rooms).

Εφαρμογή καρτών ή άλλων μέσων ασφαλούς πρόσβασης για να διασφαλιστεί ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε κρίσιμα δεδομένα και εργαλεία παρακολούθησης.

Εκπαίδευση Προσωπικού:

Συνεχής εκπαίδευση του προσωπικού του SOC σε θέματα κυβερνοασφάλειας, αντιμετώπισης περιστατικών και κοινωνικής μηχανικής για να διασφαλιστεί ότι μπορούν να αναγνωρίζουν και να αντιδρούν σε νέες και εξελισσόμενες απειλές.

Αντιμετώπιση Περιστατικών Ασφαλείας:

Ορισμός σαφών διαδικασιών και πρωτοκόλλων αντίδρασης για την άμεση και αποτελεσματική διαχείριση περιστατικών ασφαλείας που εντοπίζονται μέσω του SOC.

Τεκμηρίωση και εφαρμογή των διαδικασιών για να διασφαλιστεί η ταχεία και σωστή ανταπόκριση σε περιστατικά και η ενημέρωση για αλλαγές, όπως ενημερώσεις λογισμικού ή αδυναμίες πρωτοκόλλων.

Ασφαλής Πρόσβαση:

Χρήση Multi-Factor Authentication (MFA) και Role-Based Access Control (RBAC) για να περιορίζεται η πρόσβαση στα δεδομένα και τα εργαλεία παρακολούθησης του SOC μόνο σε εξουσιοδοτημένο προσωπικό.

Κρυπτογράφηση:

Εφαρμογή κρυπτογράφησης τόσο σε δεδομένα που μεταφέρονται όσο και σε δεδομένα που αποθηκεύονται, για να διασφαλιστεί η προστασία της εμπιστευτικότητας των δεδομένων που διαχειρίζεται η υπηρεσία SOC.

Προστασία Δικτύου:

Εφαρμογή firewall, Intrusion Detection Systems (IDS) και Intrusion Prevention Systems (IPS) για τη διαρκή παρακολούθηση και προστασία των δικτύων που χρησιμοποιούνται από την υπηρεσία SOC, αναγνωρίζοντας και εμποδίζοντας ενδεχόμενες επιθέσεις.

Προστασία Δεδομένων Προσωπικού Χαρακτήρα (GDPR):

Εξασφάλιση της συναίνεσης από τα υποκείμενα των δεδομένων πριν από την επεξεργασία τους για σκοπούς ασφάλειας.

Διασφάλιση των δικαιωμάτων των υποκειμένων δεδομένων, όπως το δικαίωμα στη διαγραφή και το δικαίωμα στη φορητότητα των δεδομένων, για όλα τα δεδομένα που επεξεργάζεται η υπηρεσία SOC.

Νομικές Απαιτήσεις για την Υπηρεσία SOC:

Συμμόρφωση με Διεθνή Πρότυπα Ασφαλείας:

Η υπηρεσία SOC πρέπει να συμμορφώνεται με διεθνή πρότυπα ασφάλειας, όπως το ISO 27001, για τη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριακών συστημάτων που παρακολουθούνται και προστατεύονται μέσω του SOC.

Εφαρμογή διαδικασιών και πρωτοκόλλων για την αποδοχή και εφαρμογή των προτύπων ασφαλείας που σχετίζονται με τη διαχείριση των δεδομένων στον τομέα της κυβερνοασφάλειας.

## 1.4 Χαρτογράφηση Αγαθών

**1. Δεδομένα Πελατών (Customer Data)**

**Περιγραφή:** Τα δεδομένα των πελατών περιλαμβάνουν προσωπικά και οργανωτικά δεδομένα που δίνονται στην υπηρεσία SOC κατά την έναρξη και τη συνεχή παροχή της υπηρεσίας.

**Παραδείγματα:**

* Προσωπικά δεδομένα (ονόματα, διευθύνσεις, στοιχεία επικοινωνίας).
* Δεδομένα υποδομής (τοπολογία δικτύου, συσκευές, endpoints, δικτυακές ρυθμίσεις).
* Πληροφορίες πρόσβασης χρηστών (authentication logs, δικαιώματα πρόσβασης).
* Πολιτικές ασφαλείας και compliance requirements (ISO 27001, GDPR, NIST).
* **Threat Intelligence Feeds** (δεδομένα από εξωτερικές πηγές όπως VirusTotal, AbuseIPDB, CVEs).
* **Asset Inventory** (λίστα με συσκευές και υπηρεσίες που προστατεύει το SOC).

**Ασφάλεια:** Τα δεδομένα πρέπει να προστατεύονται μέσω κρυπτογράφησης, ελέγχου πρόσβασης και συμμόρφωσης με νομικά και κανονιστικά πλαίσια (GDPR, ISO 27001).

**2. Εσωτερικά Δεδομένα (SOC Internal Data)**

**Περιγραφή:** Δεδομένα που αφορούν το εσωτερικό περιβάλλον του SOC, όπως στοιχεία εργαζομένων και αρχεία ελέγχου.

**Παραδείγματα:**

* Προσωπικά δεδομένα SOC analysts (user credentials, επίπεδα πρόσβασης).
* **Logins των SOC Analysts** (ποιος συνδέθηκε και πότε).
* **Audit Logs** (ενέργειες των SOC analysts στο SIEM, αλλαγές σε correlation rules, response actions).
* Πολιτικές πρόσβασης και διαχείρισης χρηστών.

**Ασφάλεια:** Η πρόσβαση πρέπει να περιορίζεται με Role-Based Access Control (RBAC) και να καταγράφεται κάθε ενέργεια για forensic ανάλυση και auditing.

**3. Operational Data (Monitoring, Analysis Data)**

**Περιγραφή:** Δεδομένα που συλλέγονται από το SIEM και άλλες πηγές παρακολούθησης για την ανίχνευση και αντιμετώπιση απειλών.

**Παραδείγματα:**

* Δεδομένα κίνησης δικτύου (NetFlow, DNS queries, firewall logs).
* Συναγερμοί ασφαλείας (SIEM alerts, IDS/IPS detections).
* Logs από endpoints, servers, firewalls, cloud services.
* **Threat Intelligence Data** (κακόβουλες IP, hash κακόβουλων αρχείων, phishing URLs).
* **Correlation Rules** (κανόνες που εφαρμόζει το SIEM για την αναγνώριση επιθέσεων).

**Ασφάλεια:** Τα δεδομένα πρέπει να παρακολουθούνται συνεχώς, να αναλύονται σε πραγματικό χρόνο και να διασφαλίζεται η ακεραιότητά τους μέσω hashing και immutable storage.

**4. Documentation (Έγγραφα και Πολιτικές)**

**Περιγραφή:** Τεκμηρίωση που αφορά τη λειτουργία του SOC και τις διαδικασίες απόκρισης σε περιστατικά ασφαλείας.

**Παραδείγματα:**

* Security Policies & Compliance Documents (ISO 27001, NIST, GDPR).
* **SOC Playbooks** (καθορισμένες διαδικασίες για αντιμετώπιση περιστατικών, π.χ. phishing response, malware analysis).
* Οδηγίες χρήσης εργαλείων (SIEM, SOAR, EDR).
* Εκπαιδευτικά υλικά για τους SOC Analysts.

**Ασφάλεια:** Πρέπει να υπάρχει περιορισμός πρόσβασης μέσω RBAC, καταγραφή αλλαγών (version control) και αποθήκευση σε ασφαλή τοποθεσία.

**5. Backup/Historical Data (Backup και Ιστορικά Δεδομένα)**

**Περιγραφή:** Δεδομένα που σχετίζονται με τη διατήρηση ιστορικών καταγραφών και την αποκατάσταση μετά από περιστατικά ασφαλείας.

**Παραδείγματα:**

* Αποθηκευμένα logs από SIEM, firewall, IDS/IPS.
* **Log Retention Policies** (κανόνες για τη διατήρηση logs, π.χ. 6 μήνες, 1 έτος).
* **Forensic Data** (ψηφιακά ίχνη, ιστορικά alerts, memory dumps για ανάλυση περιστατικών).

**Ασφάλεια:** Απαιτείται κρυπτογράφηση των backup, χρήση immutable storage και τακτικός έλεγχος της δυνατότητας

**Λογισμικά**

Community-driven and Accessible platforms (Free-tier tools):

Περιγραφή: Τα εργαλεία αυτά, όπως το GitHub και τα threat intelligence platforms, χρησιμοποιούνται για τη συνεργασία, την ανάλυση απειλών, και την ανάπτυξη εργαλείων ασφαλείας και στρατηγικών.

Ασφάλεια: Η χρήση αυτών των εργαλείων πρέπει να συνοδεύεται από τη συνεχή παρακολούθηση των ενημερώσεων ασφαλείας και την εφαρμογή πρακτικών διαχείρισης ευπαθειών για να εξασφαλιστεί ότι δεν εισάγονται νέοι κίνδυνοι από ανασφαλή εργαλεία.

Operational Software (Επιχειρησιακά Λογισμικά):

Περιγραφή: Αυτά τα εργαλεία περιλαμβάνουν συστήματα παρακολούθησης δικτύου, SIEM, και άλλα συστήματα που χρησιμοποιούνται για την ανάλυση, ανίχνευση, και ανταπόκριση σε απειλές. Αυτά τα εργαλεία είναι κρίσιμα για την παροχή της υπηρεσίας SOC.

Ασφάλεια: Η προστασία αυτών των συστημάτων περιλαμβάνει τη χρήση πολιτικών ασφαλείας, τη διασφάλιση της διαθεσιμότητας και ακεραιότητας των δεδομένων και την κατάλληλη εκπαίδευση του προσωπικού για τη σωστή χρήση τους.

Microsoft Office Suite: Θα πρέπει να υπάρχουν και πολιτικές για την προστασία των δεδομένων που διαχειρίζονται μέσω αυτών των εργαλείων, όπως μέσω κρυπτογράφησης αρχείων ή ασφαλούς αποθήκευσης.

Λειτουργικά Συστήματα(Operational Systems): Η ασφάλεια των λειτουργικών συστημάτων Windows και Linux πρέπει να είναι σε υψηλά επίπεδα, καθώς είναι τα βασικά περιβάλλοντα για τα εργαλεία SOC.

**Υλικό**

Συσκευές Χρηστών:

Περιγραφή: Περιλαμβάνουν συσκευές όπως κινητά τηλέφωνα, laptops, workstations που χρησιμοποιούνται για την πρόσβαση και εκτέλεση των καθηκόντων της υπηρεσίας SOC.

Ασφάλεια: Πρέπει να εφαρμόζονται αυστηρές πολιτικές για την ασφαλή πρόσβαση στις συσκευές (π.χ. χρήση MFA, συστήματα απομακρυσμένης διαχείρισης για την προστασία των συσκευών).

Συσκευές Δικτύου:

Περιγραφή: Αυτές οι συσκευές περιλαμβάνουν servers, firewalls, routers, και άλλα δικτυακά εξαρτήματα που χρησιμοποιούνται για την παρακολούθηση και διαχείριση της δικτυακής υποδομής.

Ασφάλεια: Η προστασία των συσκευών αυτών περιλαμβάνει την εφαρμογή πολιτικών παρακολούθησης για την ανίχνευση επιθέσεων, τη διασφάλιση της διαθεσιμότητας του δικτύου και την ασφαλή διαχείριση των διαμορφώσεων.

Συσκευές Αποθηκευτικού Χώρου:

Περιγραφή: Αφορά διακομιστές αρχείων και συστήματα NAS που χρησιμοποιούνται για την αποθήκευση δεδομένων.

Ασφάλεια: Η κρυπτογράφηση των δεδομένων αποθήκευσης και η διαχείριση δικαιωμάτων πρόσβασης σε αυτά τα συστήματα είναι κρίσιμες για την αποφυγή της μη εξουσιοδοτημένης πρόσβασης.

**Φυσικά Αγαθά**

Αναφερόμαστε στο **Headquarters** το οποίο περιλαμβάνει τα παρακάτω:

Offices (Computer Rooms, Conference Room, …):

Περιγραφή: Περιλαμβάνει τα γραφεία, τα δωμάτια υπολογιστών και άλλους χώρους όπου διεξάγεται η εργασία της υπηρεσίας SOC.

Ασφάλεια: Η φυσική προστασία αυτών των χώρων περιλαμβάνει την πρόσβαση με κάρτες ασφαλείας, την καταγραφή της φυσικής πρόσβασης και την εγκατάσταση συστημάτων ασφαλείας (κάμερες, συναγερμοί).

Data Center (Network and Storage Equipment):

Περιγραφή: Τα κέντρα δεδομένων που φιλοξενούν τους servers, τα συστήματα δικτύου και την υποδομή αποθήκευσης.

Ασφάλεια: Χρειάζεται αυστηρός έλεγχος πρόσβασης και κανονιστικά πλαίσια για την προστασία της υποδομής και την ασφαλή αποθήκευση των δεδομένων.

Security Systems (Cameras, Physical Cards, Alarms):

Περιγραφή: Περιλαμβάνει τα συστήματα φυσικής ασφαλείας που χρησιμοποιούνται για την προστασία των χώρων και των υποδομών.

Ασφάλεια: Η φυσική ασφάλεια πρέπει να συνδυάζεται με ψηφιακά συστήματα παρακολούθησης για να εξασφαλίζεται η προστασία σε όλους τους τομείς της υπηρεσίας.

## 1.5 Αποτίμηση Επιπτώσεων (Impact Assessment)

Θα εκτιμήσουμε τι επιπτώσεις θα είχε μια παραβίαση ή διαρροή στα πληροφοριακά αγαθά που ορίσαμε. Μπορούμε να τις κατηγοριοποιήσουμε βάσει **εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας (CIA Triad)**.

Για παράδειγμα:

* **Δεδομένα Πελατών** → Υψηλός αντίκτυπος αν διαρρεύσουν (GDPR, οικονομική ζημία, απώλεια φήμης).
* **Operational Data** → Αν αλλοιωθεί ή διαγραφεί, μπορεί να χαθούν κρίσιμα στοιχεία για επιθέσεις.
* **Backup/Recovery Data** → Αν δεν είναι διαθέσιμα, μπορεί να επηρεάσουν την αποκατάσταση μετά από επίθεση.

**Ιmpact levels:**

low=0

very low=1

med=2

high=3

very high=4

## 1.6 Αποτίμηση Απειλών (Threat Assessment)

Εδώ χαρτογραφούμε τις πιθανές απειλές (π.χ., malware, insider threats, phishing, APTs).

* **Για Operational Data:** Επιθέσεις τύπου Man-in-the-Middle (MitM), αλλοίωση δεδομένων, DoS.
* **Για Backup/Recovery Data:** Ransomware, καταστροφή αντιγράφων ασφαλείας.
* **Για Δεδομένα Πελατών:** Phishing, ανεπαρκής διαχείριση πρόσβασης.

**Τhreat levels:**

0=low= once every 10 years

1=medium=once every 3 years

2=high=once a year

## 1.7 Αποτίμηση Αδυναμιών

Εδώ εντοπίζουμε τα αδύναμα σημεία που μπορεί να εκμεταλλευτεί μια απειλή.

* **Μη κρυπτογραφημένη επικοινωνία** → Εύκολος στόχος για MitM.
* **Παλιές εκδόσεις λογισμικού** → Επιρρεπείς σε γνωστά exploits.
* **Κακή διαχείριση πρόσβασης** → Insider threats.

**Vulnerability levels:**

0=low= <33% πιθανότητα να συμβεί το χειρότερο σενάριο

1=med= 33 % < πιθανότητα να συμβεί το χειρότερο σενάριο < 66%

2=high= πιθανότητα να συμβεί το χειρότερο σενάριο > 66%

## 1.8 Αποτίμηση Κινδύνων (Risk Assessment)

Η αποτίμηση του κινδύνου για κάθε asset γίνεται προσθέτοντας το impact value, threat value, vulnerability value (ή αλλιώς impact + likelihood).

threat + value =likelihood of an incident

**Likelihood levels:**

0=low= very unlikely

1=low= unlikely

2=medium= possible

3=high= likely

4=very high= frequent

Οπότε η κλίμακα του συνολικού κινδύνου κυμαίνεται από 0 έως 8.

**Risk Levels:**

0-2=low risk

3-5=med risk

6-8=high risk

## 1.9 Προτεινόμενα Μέτρα Προστασίας (Proposed Security Countermeasures)

Χρήση βιομετρικών ελέγχων πρόσβασης για τις αίθουσες υπολογιστών.

Τακτική ενημέρωση και επιδιόρθωση των συστημάτων λογισμικού.

Προστασία συσκευών σε όλους τους φορητούς υπολογιστές και τους σταθερούς υπολογιστές.

Διεξαγωγή τακτικής εκπαίδευσης ευαισθητοποίησης των εργαζομένων σε θέματα κυβερνοασφάλειας.

Εφαρμογή και επιβολή ισχυρής πολιτικής κωδικών πρόσβασης.

Δημιουργία ομάδας αντιμετώπισης περιστατικών.

## 1.10 Σχέδιο Υλοποίησης Μέτρων Προστασίας

Ως προτεραιότητα θα αντιμετωπίσουμε τους κινδύνους που αποτιμάμε με βαθμολογία 5-8 , την τελευταία βαθμίδα της μεσαίας επικινδυνότητας και όλες τις υψηλές.

Θα προχωρήσουμε σε αποδοχή κινδύνου από την βαθμολογία 0-4.

# **Κατανομή οργανωτικών δομών και αρμοδιοτήτων ασφάλειας (Security Roles and Responsibilities)**

IT administrator team: Υπεύθυνοι για τις ενημερώσεις λογισμικού, τις διαδικασίες δημιουργίας αντιγράφων ασφαλείας και την συνεχή υποστήριξη της εταιρίας.

Cyber Security team: Υπεύθυνοι για την εφαρμογή μέτρων προστασίας και παρακολούθηση των συστημάτων του οργανισμού. Δημιουργία ελέγχων απειλών και ευπαθειών.

Chief Information Security Officer (CISO): Αναπτύσσει και επιβλέπει την εφαρμογή της στρατηγικής ασφάλειας πληροφοριών του οργανισμού και τις πολιτικές ασφαλείας που θα ακολουθηθούν και διασφαλίζει τη συμμόρφωση με τα κανονιστικά πλαίσια (π.χ. GDPR, ISO 27001).

Data Protection Officer (DPO): Επιβλέπει τις στρατηγικές προστασίας δεδομένων και διασφαλίζει τη συμμόρφωση με τους νόμους περί απορρήτου δεδομένων (π.χ. GDPR). Υπεύθυνος για την αντιμετώπιση παραβιάσεων προσωπικών δεδομένων.

# **Βασικές Πολιτικές Ασφάλειας (Access Control Policy, Password Policy, Logging Policy, Backup Policy)**

Access Control Policy: Role-based access στα συστήματα της εταιρίας, ώστε κάθε εργαζόμενος να έχει πρόσβαση μόνο σε δεδομένα που είναι απαραίτητα για τη δουλεία τους. Ενσωμάτωση extra layer προστασίας σε κρίσιμες υποδομές (π.χ. MFA)

Password Policy: Κωδικοί πρόσβασης τουλάχιστον 12 χαρακτήρων που περιλαμβάνουν κεφαλαία, πεζά, ειδικούς χαρακτήρες, αριθμούς, και υποχρεωτική αλλαγή ανά μικρά χρονικά διαστήματα.

Logging Policy: Καταγραφή όλων των προσβάσεων στο σύστημα και των διοικητικών ενεργειών. Αποθήκευση των logs για μελλοντική παρακολούθηση.

Backup Policy: Πραγματοποίηση αντιγράφων ασφαλείας ανά τακτά χρονικά διαστήματα και αποθήκευση τους σε κρυπτογραφημένη μορφή.

# **4. Βασικές Διαδικασίες (Διαδικασία αντιμετώπισης περιστατικών ασφάλειας, Διαδικασία Backup, Διαδικασία Δημιουργίας / Διαγραφής Χρήστη)**

**Διαδικασία Αντιμετώπισης Περιστατικών Ασφάλειας:**

Δημιουργία διαδικασίας η οποί θα περιλαμβάνει:

Αναγνώριση περιστατικού: Αναφορά από χρήστες ή ανίχνευση από συστήματα SIEM.

Κατηγοριοποίηση: Καθορισμός της σοβαρότητας και της προτεραιότητας.

Αντίδραση: Άμεση απομόνωση του περιστατικού (π.χ., αποσύνδεση συσκευής από το δίκτυο).

Ανάλυση και τεκμηρίωση: Διερεύνηση των αιτιών και καταγραφή των ενεργειών.

Αποκατάσταση: Επαναφορά υπηρεσιών και εφαρμογή πρόσθετων μέτρων ασφαλείας.

Αναφορά: Αναφορά στον CISO και, εφόσον απαιτείται, στις αρμόδιες αρχές.

**Διαδικασία Backup:**

Συχνότητα: Δημιουργία εβδομαδιαίων πλήρων αντιγράφων.

Αποθήκευση: Τα αντίγραφα αποθηκεύονται κρυπτογραφημένα και σε διαφορετική τοποθεσία.

Έλεγχος: Τακτική δοκιμή αποκατάστασης για εξασφάλιση λειτουργικότητας.

**Διαδικασία Δημιουργίας/Διαγραφής Χρήστη:**

Δημιουργία:

Υποβολή αίτησης από τον προϊστάμενο του τμήματος.

Χορήγηση δικαιωμάτων με βάση το ρόλο του χρήστη.

Ενημέρωση του χρήστη για τις πολιτικές ασφάλειας.

Διαγραφή:

Άμεση απενεργοποίηση του λογαριασμού μετά την αποχώρηση του χρήστη.

Αποθήκευση των δεδομένων του χρήστη για καθορισμένο χρονικό διάστημα.

Αναθεώρηση των προσβάσεων για να διασφαλιστεί ότι δεν παραμένουν ενεργές συνδέσεις.