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

**Α. Περιγραφή της Μεθοδολογίας**

H μεθοδολογία ακολουθεί τις πρακτικές του ISO 27001 καθώς δημιουργούμε Information Security Management System (ISMS), αλλά και ISO27005 πραγματοποιώντας διαχείριση και αποτίμηση αγαθών, απειλών, αδυναμιών και κινδύνων.

**Β. Περιγραφή του Οργανισμού**

Πρόκειται για έναν ανερχόμενο οργανισμό στο χώρο της τεχνολογίας, που αποτελείται από 30 εργαζομένους και δραστηριοποιείται σε αρκετούς τομείς με κατά κύριο λόγο τις παροχές Κυβερνοασφάλειας.

Η εταιρεία βρίσκεται στην Ελλάδα, στο κέντρο της Αθήνας.

**Γ. Απαιτήσεις Ασφαλείας – Νομικές Απαιτήσεις**

Οι υπηρεσίες πληρούν τις νομικές απαιτήσεις που σχετίζονται με την προστασία των δεδομένων προσωπικού χαρακτήρα (GDPR, NIS Directive) και ακολουθούν τα διεθνή πρότυπα ασφαλείας, όπως το ISO 27001, για τη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριακών συστημάτων.

**Δ. Χαρτογράφηση Αγαθών**

Information Data:

Δεδομένα Πελατών ( π.χ. Προσωπικά Δεδομένα Πελατών, Τοπολογίες/ Δίκτυα, Logs)

Εσωτερικά Δεδομένα Εταιρείας ( π.χ. οικονομικά στοιχεία, στοιχεία εργαζομένων)

Δεδομένα Πνευματικής/Ψηφιακής Ιδιοκτησίας(π.χ. αλγόριθμοι, λογισμικό, μεθοδολογίες, ερευνητικά στοιχεία)

Operational Data (Network traffic, alerts, logs, …)

Backup Data (αντίγραφα εσωτερικών στοιχείων εταιρείας, ιστορικά συμβάντα πελατών, …)

Software:

Open-Source λογισμικά: λογισμικά που χρησιμοποιεί η εταιρία για έρευνα και να αναπτύξει μεθοδολογίες και στατιστικά. ( π.χ. GitHub, threat intelligence platforms, visual studio, ...)

Επιχειρησιακά λογισμικά: λογισμικά που χρησιμοποιούνται για την παροχή υπηρεσιών. (Π.χ. SIEM, EDR, …)

Microsoft Office Suite

Λειτουργικά συστήματα: Windows, Linux

Hardware:

Συσκευές χρηστών: Phones, Laptops, workstations

Συσκευές δικτύου: servers, load balancers, routers, firewalls, switches,

Συσκευές αποθηκευτικού χώρου: file server, NAS

Physical Assets:

Offices (Computer Rooms, Conference Room, …)

Data Center (network and storage equipment)

Security systems (cameras, physical cards, alarms)

Το αντιμετωπίζουμε ως ένα ενιαίο αγαθό που τα περιλαμβάνει όλα -> Headquarters

Η ανάλυση που θα γίνει έχει ως επίκεντρο τα πληροφοριακά αγαθά. Εφόσον λοιπόν προσδιορίσουμε την αξία των πληροφοριακών αγαθών θα αποδώσουμε την ίδια αξία και στα αγαθά των υπολοίπων αγαθών ( software, hardware, physical) στα οποία ανήκει το εκάστοτε πληροφοριακό αγαθό. Η αξιολόγηση γίνεται με βάση τη σημαντικότητα των πληροφοριακών αγαθών για τις υπηρεσίες που προσφέρει η εταιρεία. Αφού προσδιορίσουμε λοιπόν το business impact των πληροφοριακών αγαθών και κατά συνεπαγωγή και των υπολοίπων, θα προχωρήσουμε σε threat και vulnerability assessment με βάση στατιστικά στοιχεία και τα security controls της εταιρείας.

Σε κάθε assessment κρατάμε το χειρότερο σενάριο ( την μεγαλύτερη βαθμολογία δηλαδή)

Τέλος, θα αποδώσουμε το risk treatment plan στο οποίο θα φαίνεται συνολικό ρίσκο το οποίο εξάγεται από τα παραπάνω στατιστικά καθώς και οι επόμενες κινήσεις της εταιρείας για κάθε περίπτωση.

**E. Αποτίμηση Επιπτώσεων (Impact Assessment)**

Εδώ κοιτάμε το possible impact στο κάθε asset με βάση το CIA triad.

Έχουμε impact level low=0, very low=1, med=2, high=3, very high=4

**Ζ: Αποτίμηση Απειλών (Threat Assessment)**

Έχουμε threat level 0=low= once every 10 years, 1=med=once a month, 2=high=once a month.

**H. Αποτίμηση Αδυναμιών**

Έχουμε vulnerability level:

0=low= <33% πιθανότητα να συμβεί το threat

1=med= 33 % < πιθανότητα να συμβεί το threat < 66%

2=high= πιθανότητα να συμβεί το threat > 66%

**Θ. Αποτίμηση Κινδύνων (Risk Assessment)**

Η αποτίμηση του κινδύνου για κάθε asset γίνεται προσθέτοντας το impact value, threat value, vulnerability value

0-2=low

3-5=med

6-8=high

\*\*αυτό με βάση τα νούμερα που έχουμε αποδώσει ήδη\*\*

**Ι. Προτεινόμενα Μέτρα Προστασίας ( Proposed Security Countermeasures)**

Χρήση βιομετρικών ελέγχων πρόσβασης για τις αίθουσες υπολογιστών.

Τακτική ενημέρωση και επιδιόρθωση των συστημάτων λογισμικού.

προστασίας 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.

**K. 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.

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

IT administrator team: Υπεύθυνος για τις ενημερώσεις λογισμικού, τις διαδικασίες δημιουργίας αντιγράφων ασφαλείας και την αντιμετώπιση περιστατικών.

Cyber Security team: Διεξάγει τακτικές αξιολογήσεις απειλών και παρακολουθεί τη δραστηριότητα του συστήματος.

CISO: Αναπτύσσει και επιβλέπει την εφαρμογή της στρατηγικής ασφάλειας πληροφοριών του οργανισμού και διασφαλίζει τη συμμόρφωση με τα κανονιστικά πλαίσια (π.χ. GDPR, ISO 27001, NIST).

DPO: Επιβλέπει τις στρατηγικές προστασίας δεδομένων και διασφαλίζει τη συμμόρφωση με τους νόμους περί απορρήτου δεδομένων (π.χ. GDPR)

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

Access Control Policy: Role-based access στα συστήματα της εταιρίας.

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.

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

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

Αντιμετώπιση περιστατικών:

Καθορισμός κατηγοριών περιστατικών και προτεραιοτήτων αντιμετώπισης.

Τεκμηρίωση και αναφορά όλων των περιστατικών ασφαλείας.

Αποκατάσταση αντιγράφων ασφαλείας:

Μηνιαίος έλεγχος της ακεραιότητας των αντιγράφων ασφαλείας.

Διατήρηση σαφούς πρωτοκόλλου αποκατάστασης.

Διαχείριση χρηστών:

Εξασφάλιση ασφαλούς εισόδου/εξόδου των εργαζομένων.

Απενεργοποίηση λογαριασμών αμέσως μετά την αποχώρηση του υπαλλήλου.