**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) για να προσδιορίσουμε τα αγαθά του οργανισμού, αλλά και ISO27005 πραγματοποιώντας διαχείριση και αποτίμηση αγαθών, απειλών, αδυναμιών και κινδύνων, των πληροφοριακών αγαθών που εμπλέκονται στην υπηρεσία που θα αναλύσουμε. Συνεπώς η μελέτη γίνεται γύρω από την υπηρεσία του οργανισμού και αφορά τα πληροφοριακά αγαθά που εμπλέκονται.

**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.

Θα αναλύσουμε κυρίως την υπηρεσία SOC ( Security Operations Center) που περιλαμβάνει network monitoring, analyzing alerts, investigating incidents, … .

Οι διαδικασίες τέτοιων υπηρεσιών περιλαμβάνουν κυρίως:

Monitoring network traffic -> new devices on the network, network logs, device communication patterns, threat intel feeds, alerts, vulnerabilities, patches, ….

Incident Detection and Response -> με βάση manuals and incident response protocols αντιμετώπιση των σοβαρών περιστατικών, updates for software patches, ενημέρωση για μη χρησιμοποίηση insecure protocols and passwords και γενικότερα έρευνα κάθε πιθανού κινδύνου με βάση τα alerts.

**Γ. Απαιτήσεις Ασφαλείας – Νομικές Απαιτήσεις**

Απαιτήσεις Ασφαλείας:

Ελεγχόμενη Πρόσβαση: Έλεγχος Πρόσβασης στο χώρο υποδοχής του οργανισμού. Χρήση καρτών για την πρόσβαση σε χώρους της εταιρείας.

Εκπαίδευση Προσωπικού: Συνεχής εκπαίδευση σε θέματα κυβερνοασφάλειας και κοινωνικής μηχανικής.

Αντιμετώπιση περιστατικών ασφαλείας: Καθορισμός και τεκμηρίωση διαδικασιών για άμεση ανταπόκριση σε περιστατικά ασφάλειας.

Ασφαλής Πρόσβαση: Χρήση MFA, role-based access control

Κρυπτογράφηση: Σε δεδομένα εν κινήσει αλλά και σε κατάσταση ηρεμίας.

Προστασία Δικτύου: firewall, IDS, IPS

Προστασία των δεδομένων προσωπικού χαρακτήρα (GDPR): Εξασφάλιση συναίνεσης για την επεξεργασία δεδομένων. Υλοποίηση δικαιωμάτων υποκειμένων δεδομένων (π.χ., δικαίωμα στη διαγραφή).

Συμμόρφωση με 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, Infrastructure, Devices, Τοπολογίες/ Δίκτυα, Logs) -> Δεδομένα που δίνονται κυρίως στην αρχή ( πριν την εφαρμογή της υπηρεσίας δηλαδή, καθώς είναι απαραίτητα για την ύπαρξή της) και μπορεί να ανανεωθούν κατά τη διάρκεια των υπηρεσιών.

Εσωτερικά Δεδομένα ( π.χ. προσωπικά στοιχεία εργαζομένων, access rights, compliance data, …) -> αφορούν προσωπικά δεδομένα εργαζομένων, δικαιώματα και δεδομένα συμμόρφωσης της εταιρείας ως προς τις υπηρεσίες που προσφέρει.

Operational Data (Network traffic, alerts, logs, …) -> live δεδομένα που βοηθούν στον εντοπισμό ανωμαλιών στην κίνηση του δικτύου και ειδοποιήσεις που σημαίνουν πιθανούς κινδύνους.

Documentation (π.χ. manuals, best practices, training materials, playbooks, reports …) -> Δεδομένα της εταιρίας που προετοιμάζουν τους εργαζομένους της εταιρείας κατάλληλα για την διενέργεια των υπηρεσιών, χρήσιμες πρακτικές, καθώς και reports που μπορεί να δημιουργηθούν μελλοντικά.

Backup/Recovery Data (αντίγραφα εσωτερικών στοιχείων εταιρείας, ιστορικά συμβάντα πελατών, system recovery documentation…) -> οδηγίες σε περίπτωση ανάγκης, ιστορικά δεδομένα που μπορεί να χρειαστούμε

Software:

Open-Source λογισμικά: λογισμικά που χρησιμοποιούνται για να βοηθήσουν τον κύκλο εργασιών, την έρευνα και να βοηθήσουν την εταιρία να αναπτύξει μεθοδολογίες, στατιστικά και να είναι ενημερωμένη για όλα τα νέα στο χώρο της Κυβερνοασφάλειας. ( π.χ. GitHub, threat intelligence platforms, …)

Επιχειρησιακά λογισμικά: λογισμικά που χρησιμοποιούνται για την παροχή υπηρεσιών. (Π.χ. Network Monitoring, 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, που σχετίζονται με το service αυτό. 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. 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 levels:

low=0

very low=1

med=2

high=3

very high=4

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

Έχουμε threat levels με βάση το αν έχει συμβεί η απειλή στον οργανισμό που μελετάμε:

0=low= once every 10 years

1=medium=once a month

2=high=once a month.

**H. Αποτίμηση Αδυναμιών**

Έχουμε vulnerability levels με βάση τα security controls του οργανισμού υπό μελέτη:

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%

\*threat + value =likelihood of an incident

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

Η αποτίμηση του κινδύνου για κάθε asset γίνεται προσθέτοντας το impact value, threat value, vulnerability value (ή αλλιώς impact + likelihood). Οπότε η κλίμακα του συνολικού κινδύνου κυμαίνεται από 0 έως 8.

Πιο συγκεκριμένα:

0-2=low risk

3-5=med risk

6-8=high risk

**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: 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 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.

* 1. **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.

* 1. **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.