**Τίτλος:**

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)

**Μελέτη Ανάλυσης και Διαχείρισης Επικινδυνότητας**

**Α. Περιγραφή της Μεθοδολογίας**

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

**Β. Περιγραφή του Οργανισμού**

**Πρόκειται για έναν μικρό οργανισμό, που αποτελείται από 30 εργαζομένους που παρέχει υπηρεσίες Cyber Security, IT, αλλά δραστηριοποιείται και στο χώρο της ψηφιοποίησης αγροτικών περιοχών της Ελλάδος.**

**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**

**Hardware:**

**\*\*το hardware το αντιμετωπίζουμε ως hardware μόνο. Δεν κάνουμε include το software / data που σχετίζoνται. Οπότε κοιτάμε περισσότερο το availability τους .\*\***

**30 Laptops των εργαζομένων**

**2 workstations που τρέχουν συνεχώς επεξεργασία δεδομένων**

**printers/scanners**

**firewall**

**Synology NAS ο κύριος αποθηκευτικός χώρος της εταιρείας**

**file server**

**web server για το website της εταιρείας**

**UPS**

**Mobile Devices**

**Security cameras**

**Drone equipment**

**Software:**

**\*\*εδώ μας απασχολεί το integrity και το availability περισσότερο\*\***

**Windows OS**

**Microsoft Office Suite**

**Business-Specific Software (π.χ κάποιο cyber security software που χρησιμοποιείται για phishing campaigns, network monitoring, …, ή κάποιο drone software που κάνει επεξεργασία και αποθήκευση εικόνων/βίντεο.)**

**Virtual Machines**

**Physical Assets:**

**HeadQuarters**

**Computer Room (που έχει web server/ nas/ ups/ file server/ firewall/ .. γενικά το περισσότερο it equipment)**

**Storage Room (η αποθήκη που περιέχει όλα τα drones/controllers/… γενικά όλο το equipment.**

**Data:**

**Στοιχεία Πελατών ( π.χ. Προσωπικά Δεδομένα Υπαλλήλων, Προσωπικά Δεδομένα Πελατών, Τοπολογίες/ Δίκτυα)**

**Στοιχεία Υπαλλήλων Εταιρείας**

**Στοιχεία καταγραφής των drone**

**Οικονομικές Συμφωνίες / Συμβάσεις**

**Backup data**

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

**\*\*αυτός κάνει impact assessment και threat assessment στα information data. Δεν δείχνει κάτι για τα υπόλοιπα, τώρα δε ξέρω αν θέλει να μείνουμε εκεί ή να κάνουμε για όλα αναλυτικά. Αναφέρει όμως πιθανά threats για κάθε είδος asset -> Data, Hardware, Software, Physical Assets. \*\***

**\*\*Επίσης τα information data το συνδέουμε και με τα υπόλοιπα assets στο impact assessment. Τα υπόλοιπα τα κάνουμε μόνα τους.\*\***

**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**

**Πχ**

**Client Data: confidentiality high, integrity medium, availability medium**

**Laptops/Workstations: confidentiality low, integrity low, availability medium**

**Modem/Router: all high**

**Windows OS: confidentiality low, integrity high, availability high**

**Synology NAS: all high**

**File server: all med**

**Web server: conf low, integrity high, availability med**

**Business Software: confidentiality high, integrity high, availability high**

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

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

**Hardware Threats:**

**Malicious destruction**

**Theft/loss of equipment**

**Damage through physical causes (power outage, earthquakes, …) that causes system failure.**

**Software Threats:**

**OS Vulnerabilities**

**Unauthorized access to systems (hacking)**

**Malware**

**Information Data Threats:**

**Theft/loss of data**

**Intentional/accidental disclosure of confidential or regulated data**

**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 and vulnerability value**

**0-2=low**

**3-5=med**

**6-8=high**

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

**\*\*Πρέπει να συμπληρωθεί το excel για όλα τα παραπάνω\*\***

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

**Physical Security Measures**

Use biometric access controls for computer rooms.

**Technical Security Measures**

Regularly update and patch software systems.

Deploy endpoint protection on all laptops and workstations.

**Administrative Security Measures**

Conduct regular cybersecurity awareness training for employees.

Implement and enforce a robust password policy.

Establish an incident response team.

**K. Σχέδιο Υλοποίησης Μέτρων Προστασίας**

**Είναι το risk assessment και προσθέτεις strategy (accept, avoid, transfer, mitigate) risk, risk owner, control implementation, implementation date, residual risk**

**\*\*για τα οποία πρέπει να έχουμε κανόνες. Πχ**

**0-4 accept**

**5-8 mitigate**

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

IT Administrator: Responsible for software updates, backup processes, and incident response.

Security Analyst: Conducts regular threat assessments and monitors system activity.

CISO:

DPO:

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

**Access Control Policy:** Role-based access to systems and data. Regular review of access permissions.

**Password Policy:** Minimum 12-character passwords including upper, lower case, special characters, numbers.

Mandatory rotation every 90 days.

**Logging Policy**

Log all system access and administrative actions.

Retain logs for at least one year.

**Backup Policy**

Conduct daily backups of critical data.

Store backups in an encrypted format offsite.

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

Incident Response:

Define incident categories and response priorities.

Document and report all security incidents.

Backup Restoration:

Test backup integrity monthly.

Maintain a clear restoration protocol.

User Management:

Ensure secure onboarding/offboarding of employees.

Disable accounts immediately upon employee departure.