Ασφάλεια Πληροφοριακών Συστημάτων

«Εισαγωγή»

Τμήμα Πληροφορικής, Πανεπιστήμιο Πειραιώς

Αν. Καθ. Π.Κοτζανικολάου **pkotzani@unipi.gr**

Διδάσκοντες μαθήματος: Αν. Καθ. Δ. Πολέμη, Αν. Καθ. Π. Κοτζανικολάου

Μαθήματα σχετικά με την ασφάλεια πληροφοριακών συστημάτων

1. Κρυπτογραφία

($5_ο$ εξ. Επιλ.)

2. Ασφάλεια δικτύων

($8_ο$ εξ. Υπ.Κατεύθ. ΔΥΣ)

3. Διοίκηση Ασφάλειας Συστημάτων

($8_ο$ εξ. Υπ.Κατεύθ. ΠΣΥ)

4. Ηλεκτρονικό επιχειρείν

($8_ο$ εξ. Υπ.Κατεύθ. ΠΣΥ)

Η παρακολούθηση των σχετικών μαθημάτων επιλογής λαμβάνεται υπόψη για την εκπόνηση πτυχιακής εργασίας

Μέθοδος αξιολόγησης

- Ενδιάμεσες εργαστηριακές ασκήσεις μικρής έκτασης (~5 ασκήσεις): 30%
- Απαλλακτική προγραμματιστική (περιλαμβάνει τμήμα των ασκήσεων): 50%
- Γραπτή πρόοδος: 20%

Σχετικά με την απαλλακτική εργασία

Καλείστε να αναπτύξετε μια διαδικτυακή εφαρμογή (ή να χρησιμοποιήσετε μία εφαρμογή την οποία έχετε ήδη αναπτύξει σε προηγούμενο μάθημα) και **να υλοποιήσετε/εφαρμόσετε βασικές υπηρεσίες/ τεχνολογίες ασφάλειας:**

- Μελέτη Ασφάλειας
- Αυθεντικοποίηση server / Αυθεντικοποίηση client
- Κρυπτογράφηση / ασφάλεια δικτυακής σύνδεσης
- Έλεγχος πρόσβασης χρηστών
- Ισχυροποίηση ασφάλειας κώδικα
- Έλεγχος αδυναμιών ασφάλειας

Διδακτικές μέθοδοι

- Διαλέξεις
- Εργαστηριακά μαθήματα
  - *Χρήση laptop*
- Συμμετοχή φοιτητών μέσω ενδιάμεσων εργασιών
  - Εργασίες μικρής κλίμακας
- Συχνή ενημέρωση σελίδας μαθήματος

  https://gunet2.cs.unipi.gr/courses/TMD108/

Δομή του μαθήματος

1. Εισαγωγικές έννοιες
2. Βασικές αρχές κρυπτογραφίας
3. Μοντέλα Εμπιστοσύνης – Υποδομές Δημόσιου Κλειδιού
4. Έλεγχος προσπέλασης και ιδιωτικότητα
5. Ασφάλεια λειτουργικών συστημάτων
6. Ασφάλεια σε τεχνολογίες (τεχνολογίες ελέγχου πρόσβασης, ασφάλεια στο Web, ασφάλεια λογισμικού, ...)
7. Μοντελοποίηση Απειλών
8. Ασφάλεια δικτύων
9. Παραδείγματα ασφάλειας σε εφαρμογές
10. Συμμετοχικές παρουσιάσεις εργασιών

1η θεματική ενότητα

1. Εισαγωγικές έννοιες

- Βασικές έννοιες ασφάλειας Π.Σ.
- Ο κύκλος ζωής της ασφάλειας
- Συστήματα διαχείρισης ασφάλειας
- Βασικά πρότυπα ασφάλειας
- Εποπτικό/ρυθμιστικό πλαίσιο

2η θεματική ενότητα

2. Κρυπτογραφικά συστήματα

- Εισαγωγή
- Κλασσική κρυπτογραφία
- Κρυπτοσυστήματα μοναδιαίας κλείδας (συμμετρική κρυπτογράφηση)
- Κρυπτοσυστήματα δημόσιας κλείδας (ασύμμετρη κρυπτογράφηση)
- Υβριδικά συστήματα

3η θεματική ενότητα

3. Μοντέλα Εμπιστοσύνης (Trust Models) - Υποδομή Δημόσιου Κλειδικού (ΥΔΚ) – Public Key Infrastructure (PKI)

- Μοντέλα Εμπιστοσύνης (Trust Models)
- Οργανωτικές δομές
- Υπηρεσίες ΥΔΚ / Συναρτήσεις ΥΔΚ
- Πρότυπα / Νομικό πλαίσιο
- Πολιτική ασφάλειας και δήλωση πρακτικών πιστοποίησης ΥΔΚ

4η θεματική ενότητα

4. Έλεγχος προσπέλασης - ιδιωτικότητα

- Συστήματα αναγνώρισης ταυτότητας και αυθεντικοποίησης
- Μοντέλα ελέγχου πρόσβασης
- Τεχνικές προστασίας και διαχείρισης ιδιωτικότητας

5η θεματική ενότητα

5. Ασφάλεια λειτουργικών συστημάτων

- Χρήστες, ομάδες και δικαιώματα
- Καταγραφή και έλεγχος
- Επιθέσεις σε επίπεδο Λ.Σ. (trapdoors, backdoors, logic bombs)
- Ιοί υπολογιστών και σφάλματα κώδικα

6η θεματική ενότητα

6. Ασφάλεια στις τεχνολογίες

- Βιομετρικές τεχνολογίες ελέγχου πρόσβασης
- Ασφάλεια σε τεχνολογίες IoT
- Ασφάλεια σε υπηρεσίες ιστού
- Εντοπισμός αδυναμιών ασφάλειας κατά τον προγραμματισμό
- …

7η θεματική ενότητα

7. Μοντελοποίηση Απειλών Ασφάλειας

- Μοντέλα Απειλών (Threat Models)
- Μοντελοποίηση επιτιθέμενων (Adversarial Models)
- Εφαρμογή μοντέλων σε πραγματικά συστήματα

8η θεματική ενότητα

8. Ασφάλεια δικτύων

- Εκτίμηση αδυναμιών / εργαλεία
- Έλεγχος ασφάλειας δικτυακής περιμέτρου

9η θεματική ενότητα

9. Παραδείγματα εφαρμογών και συστημάτων ασφάλειας

- Παρουσιάσεις (demo) πραγματικών συστημάτων
- Συγκριτική μελέτη
- Ερευνητικά ζητήματα

10η θεματική ενότητα

10. Συμμετοχικές παρουσιάσεις εργασιών

- Παρουσιάσεις εργασιών
- Ερωτήσεις/Απαντήσεις σχετικά με όλες τις θεματικές ενότητες του μαθήματος

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

1η Ενότητα
Εισαγωγικές Έννοιες –

1. Εισαγωγικές έννοιες

1. **Βασικές έννοιες ασφάλειας Π.Σ.**
2. Ο κύκλος ζωής της ασφάλειας
3. Συστήματα διαχείρισης ασφάλειας
4. Πρότυπα ασφάλειας
5. Εποπτικό/ρυθμιστικό πλαίσιο

Τι είναι ασφάλεια;

Security
Safety
Insurance
Assurance
Police
Fuse

} = Ασφάλεια ?

Ορισμοί της Ασφάλειας

- Security:
  - **Freedom from danger or anxiety**
  - Safety from criminal activity such as terrorism
  - A thing deposited or pledged as a guarantee of the fulfillment of an undertaking or the repayment of a loan, to be forfeited in case of default
  - A certificate attesting credit, the ownership of stocks or bonds, or the right to ownership connected with tradable derivatives

- Ασφάλεια:
  - **Η κατάσταση στην οποία δεν υπάρχουν κίνδυνοι, όπου αισθάνεται κανείς ότι δεν απειλείται.**
  - **Η αποτροπή κινδύνου ή απειλής, η εξασφάλιση σιγουριάς και βεβαιότητας**
  - Υπηρεσία της Αστυνομίας
  - Ηλεκτρική διάταξη που αποτρέπει πιθανά ατυχήματα
  - Μηχανισμός στην πόρτα αυτοκινήτου
  - Συμφωνία μεταξύ ασφαλιστικής εταιρείας και πελάτη
  - Ιατροφαρμακευτική περίθαλψη

Η έννοια της ασφάλειας πληροφοριακού συστήματος

- **Σύστημα:** ένα σύνολο από *κατάλληλα οργανωμένα* αλληλοεξαρτώμενα ή/και αλληλεπιδρώντα στοιχεία, τα οποία αποτελούν μία ενιαία οντότητα η οποία δρα για την εκπλήρωση συγκεκριμένων σκοπών

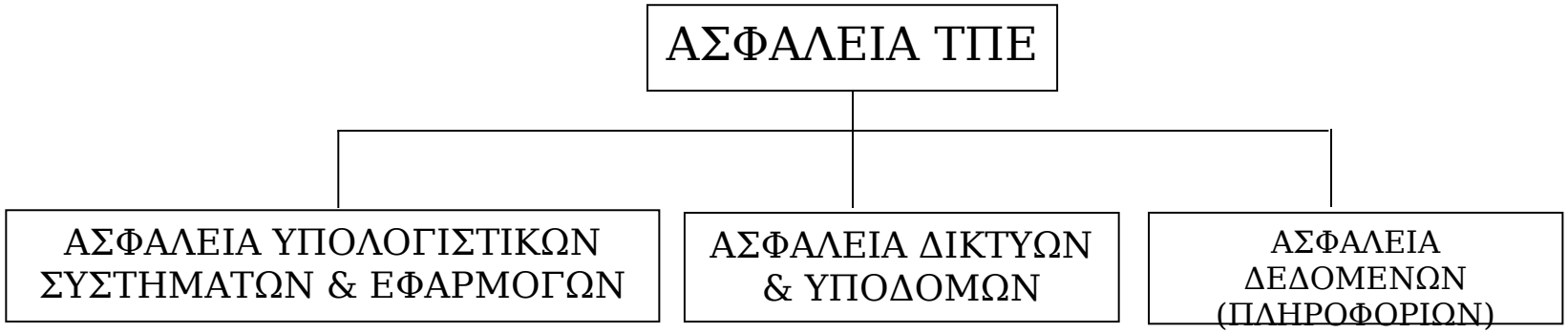
- **Πληροφοριακό σύστημα:** ένα οργανωμένο σύνολο το οποίο απαρτίζεται από:
  - **Ανθρώπους**
  - **Δεδομένα**
  - **Υλικό (h/w)**
  - **Λογισμικό (s/w)**
  - **Διαδικασίες**

  με σκοπό την υποστήριξη των επιχειρησιακών δραστηριοτήτων, μέσω της επεξεργασίας, ανταλλαγής και διαχείρισης πληροφορίας.

Τεχνική vs Ολιστική προσέγγιση

- **Ασφάλεια Τεχνολογιών Πληροφορίας & Επικοινωνιών (ΤΠΕ)** Information & Communication Technology (ICT) Security
  - Ασφάλεια υπολογιστικών συστημάτων & εφαρμογών
  - Ασφάλεια δικτύων & υποδομών
  - Ασφάλεια δεδομένων
- **Ολιστική προσέγγιση ασφάλειας Π.Σ.**
  - Ασφάλεια υπολογιστικών συστημάτων & εφαρμογών
  - Ασφάλεια δικτύων & υποδομών
  - Ασφάλεια δεδομένων **+ πληροφορίας**
  - **Ασφάλεια χρηστών (προσωπικού)**
  - **Λειτουργική ασφάλεια (διαδικασίες λειτουργίας)**

Τεχνική Προσέγγιση: Ασφάλεια ΤΠΕ



Ασφάλεια Υπολογιστικών Συστημάτων & Εφαρμογών

- Η διασφάλιση της ορθής λειτουργίας του υπολογιστικού συστήματος/εφαρμογής (hardware/software)
- Η προστασία από μη εξουσιοδοτημένη λογική πρόσβαση στο σύστημα/εφαρμογή
- Προστασία από μη εξουσιοδοτημένη τροποποίηση της διάρθρωσης του συστήματος
- Η προστασία από κακόβουλη χρήση (π.χ. εκτέλεση κακόβουλου λογισμικού)
- Η προστασία από λανθασμένες ενέργειες
- Η προστασία της διαθεσιμότητας των συστημάτων/ εφαρμογών
- Η φυσική προστασία των συστημάτων

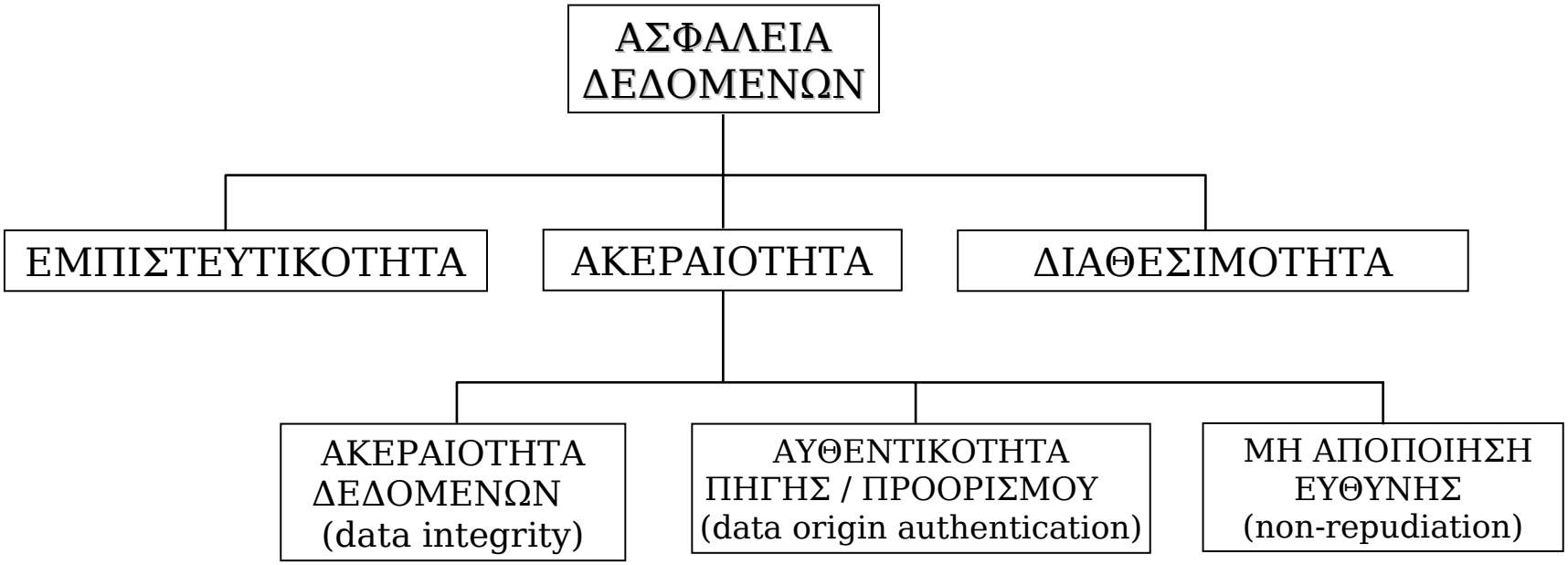
Ασφάλεια Δικτύων & Υποδομών

- Η προστασία από μη εξουσιοδοτημένη λογική πρόσβαση σε ένα δίκτυο
- Η προστασία από την παρακολούθηση του μέσου επικοινωνίας (υποκλοπή)
- Η προστασία από παράκαμψη ή τροποποίηση των κανόνων δρομολόγησης στο δίκτυο
- Η διασφάλιση της δικτυακής διασύνδεσης και η προστασία από τη διακοπή της επικοινωνίας
- Η φυσική προστασία των υποδομών επικοινωνίας (routers, gateways, κτλ)

Ασφάλεια Δεδομένων (Πληροφοριών)

- Προστασία των δεδομένων κατά την επεξεργασία, αποθήκευση ή μετάδοσή τους, ως προς την:
  - **Εμπιστευτικότητα (Confidentiality)**
    - Η αποφυγή μη εξουσιοδοτημένης αποκάλυψης της πληροφορίας
  - **Ακεραιότητα (Integrity)**
    - Η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας
  - **Διαθεσιμότητα (Availability)**
    - Η αποφυγή μη εξουσιοδοτημένης προσωρινής ή μόνιμης παρακράτησης μιας πληροφορίας

Άλλες ιδιότητες ασφάλειας



Ολιστική προσέγγιση ασφάλειας Π.Σ.

- Η τεχνική πλευρά της ασφάλειας ΤΠΕ

  (δεδομένα, H/W, S/W) **+**

  Ανθρώπινος παράγοντας +

  Διαδικασίες Λειτουργίας +

  Περιβάλλον λειτουργίας

- Κατά συνέπεια πρέπει να λαμβάνονται υπόψη και:
  - Κανόνες χρήσης /λειτουργίας και διαδικασίες ασφάλειας (operational view)
  - Νομοθετικό / ρυθμιστικό πλαίσιο λειτουργίας (legal/regulatory view)

Πρακτική προσέγγιση ασφάλειας

- Κάθε Π.Σ. υποστηρίζει ορισμένες επιχειρησιακές δραστηριότητες (business processes). Άρα πρακτικός στόχος της ασφάλειας Π.Σ.
  - Η προστασία των επιχειρησιακών δραστηριοτήτων που υποστηρίζονται από του Π.Σ.
  - Η ορθή λειτουργία του Π.Σ.
- Η απόλυτη ασφάλεια είναι ΑΔΥΝΑΤΗ. Συνεπώς ακολουθείται η προσέγγιση μείωσης των κινδύνων (risk-based approach)
  - Εντοπισμός κινδύνων
  - Λήψη κατάλληλων **μέτρων (countermeasures)** ή **ελέγχων ασφάλειας (security controls)** για την αντιμετώπισή τους
    - Πρόληψης (prevention)
    - Ανίχνευσης (detection)
    - Αποκατάστασης (recovery)

Βασικοί όροι ασφάλειας

- **Αγαθό** (Asset)
  - Κάθε αντικείμενο ή πόρος το οποίο αξίζει να προστατευθεί.
    - Φυσικά Αγαθά (Physical Assets):
      - **Χρήστες**
      - Υπολογιστικά συστήματα
      - Δικτυακή υποδομή
      - Λοιπός εξοπλισμός
    - Αγαθά Δεδομένων (Data Assets):
      - Αρχεία (ηλεκτρονικά, έντυπα)
      - Λοιπά έγγραφα *(διαδικασίες)*
    - Αγαθά Λογισμικού (Software Assets):
      - Εφαρμογές
      - Λειτουργικά Συστήματα

Βασικοί όροι ασφάλειας

- **Ιδιοκτήτης αγαθού** (asset owner)
  - ονομάζεται το φυσικό ή νομικό πρόσωπο που έχει την ευθύνη και αρμοδιότητα για τη σωστή χρήση του αγαθού.
    - Π.χ. ο Διευθυντής Προσωπικού είναι ο ιδιοκτήτης των δεδομένων που αφορούν το προσωπικό ενός οργανισμού
      - … άρα έχει την ευθύνη για την προστασία των προσωπικών δεδομένων.
- **Χρήστης Αγαθού** (asset user)
  - Το φυσικό πρόσωπο που επεξεργάζεται ένα αγαθό, με την καθοδήγηση και εξουσιοδότηση του Ιδιοκτήτη του αγαθού

Βασικοί όροι ασφάλειας

- **Συνέπεια** (Impact)
  - Η απώλεια που θα προκληθεί από την προσβολή ενός αγαθού
    - Άμεσες Συνέπειες – π.χ.
      - κόστος επαναγοράς
      - κόστος διαμόρφωσης, εισαγωγής δεδομένων
    - Έμμεσες Συνέπειες – π.χ.
      - Κοινωνικές συνέπειες
      - Δυσφήμηση
      - Νομικές συνέπειες
      - Απώλειες από διακοπή ή παρεμπόδιση λειτουργιών

Βασικοί όροι ασφάλειας

- **Απειλή** (Threat)
  - Οποιοδήποτε γεγονός η εκδήλωση του οποίου προκαλεί αρνητικές συνέπειες (impact) σε κάποιο αγαθό
    - Φυσικές Απειλές:
      - Φωτιά, Σεισμός, Πλημμύρα,…
    - Ανθρώπινες Εσκεμμένες:
      - Κλοπή, Βανδαλισμός, Αλλοίωση, Αποκάλυψη πληροφορίας, hacking, cracking, Denial of Service, miss-routing, …)
    - Ανθρώπινες Τυχαίες:
      - Κακή χρήση πόρου, πρόκληση ζημιάς, τυχαία αποκάλυψη πληροφορίας κτλ

Βασικοί όροι ασφάλειας

- **Αδυναμία** (Vulnerability)
  - Οποιοδήποτε χαρακτηριστικό κάνει ευάλωτο ένα αγαθό σε μία ή περισσότερες απειλές, δηλαδή αυξάνει την πιθανότητα εκδήλωσης της απειλής
    - Π.χ: εάν η πρόσβαση σε ένα απόρρητο αρχείο δεν προστατεύεται, το αρχείο έχει μεγάλη αδυναμία στην απειλή της κλοπής
  - Οτιδήποτε μεγιστοποιεί τις συνέπειες από την εκδήλωση μίας απειλής
    - Π.χ: εάν δεν υπάρχει σύστημα αυτόματης πυρόσβεσης σε ένα χώρο, η συνέπειες από μία πιθανή πυρκαγιά θα είναι πολύ μεγάλες

Βασικοί όροι ασφάλειας

- **Κίνδυνος ή επικινδυνότητα ασφάλειας** (security risk)

  Επικινδυνότητα = Συνέπεια ⊗ Απειλή ⊗ Αδυναμία

  Security Risk = Impact ⊗ Threat ⊗ Vulnerability

- Οι κίνδυνοι ασφάλειας υπολογίζονται για όλα τα αγαθά ενός Π.Σ.
- Η διαδικασία υπολογισμού κινδύνων υποστηρίζεται από μεθοδολογίες και εργαλεία ανάλυσης επικινδυνότητας (risk analysis)

Βασικοί όροι ασφάλειας

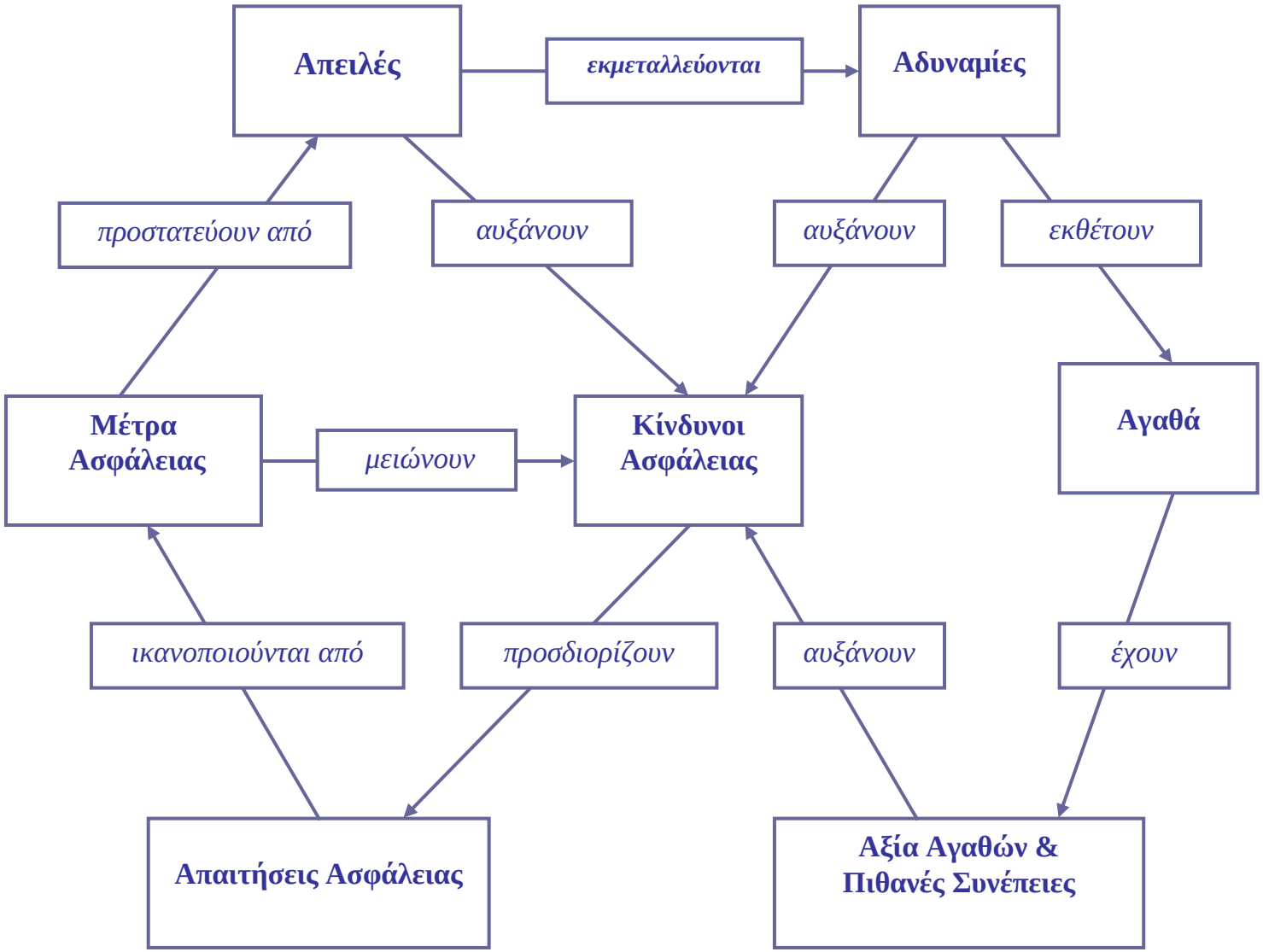
- **Μέτρο ασφάλειας (ή έλεγχος ασφάλειας)** (safeguard, security control, countermeasure):
  - Οτιδήποτε περιορίζει τον κίνδυνο για ένα ή περισσότερα αγαθά
    - **Προληπτικά μέτρα (preventive):**
      - στοχεύουν στο να αποτρέψουν κινδύνους
      - π.χ, η χρήση ενός συστήματος Firewall σε ένα δίκτυο αποτρέπει τη μη εξουσιοδοτημένη είσοδο πακέτων σε ένα δίκτυο.
    - **Μέτρα Ανίχνευσης (detective):**
      - αποσκοπούν στο να εντοπίσουν την πηγή της προσβολής σε ένα αγαθό, εφόσον το αγαθό αυτό έχει προσβληθεί από κάποιο κίνδυνο.
      - π.χ., η χρήση ενός Συστήματος Ανίχνευσης Εισβολών (Intrusion Detection System – IDS) σε ένα δίκτυο
    - **Μέτρα Αποκατάστασης (recovery):**
      - στοχεύουν στο να μειώσουν τον απαιτούμενο χρόνο για την ανάκαμψη μετά από την εκδήλωση μίας προσβολής σε ένα αγαθό.
      - π.χ., η λήψη εφεδρικών αρχείων σε ένα υπολογιστικό σύστημα ελαχιστοποιεί τον χρόνο ανάκαμψης ενός συστήματος από μία πιθανή διακοπή λειτουργίας.

Βασικοί όροι ασφάλειας

- **Κόστος** (cost)
  - Οποιαδήποτε επιβάρυνση προκύπτει από:
    - Την αγορά/εγκατάσταση ενός μέτρου ασφάλειας
    - Την χρήση/συντήρηση ενός μέτρου ασφάλειας

- **Διαχείριση επικινδυνότητας** (risk management)
  - Η διαδικασία προσδιορισμού, αξιολόγησης και επιλογής των κατάλληλων μέτρων ασφάλειας υποστηρίζεται από μεθοδολογίες και εργαλεία

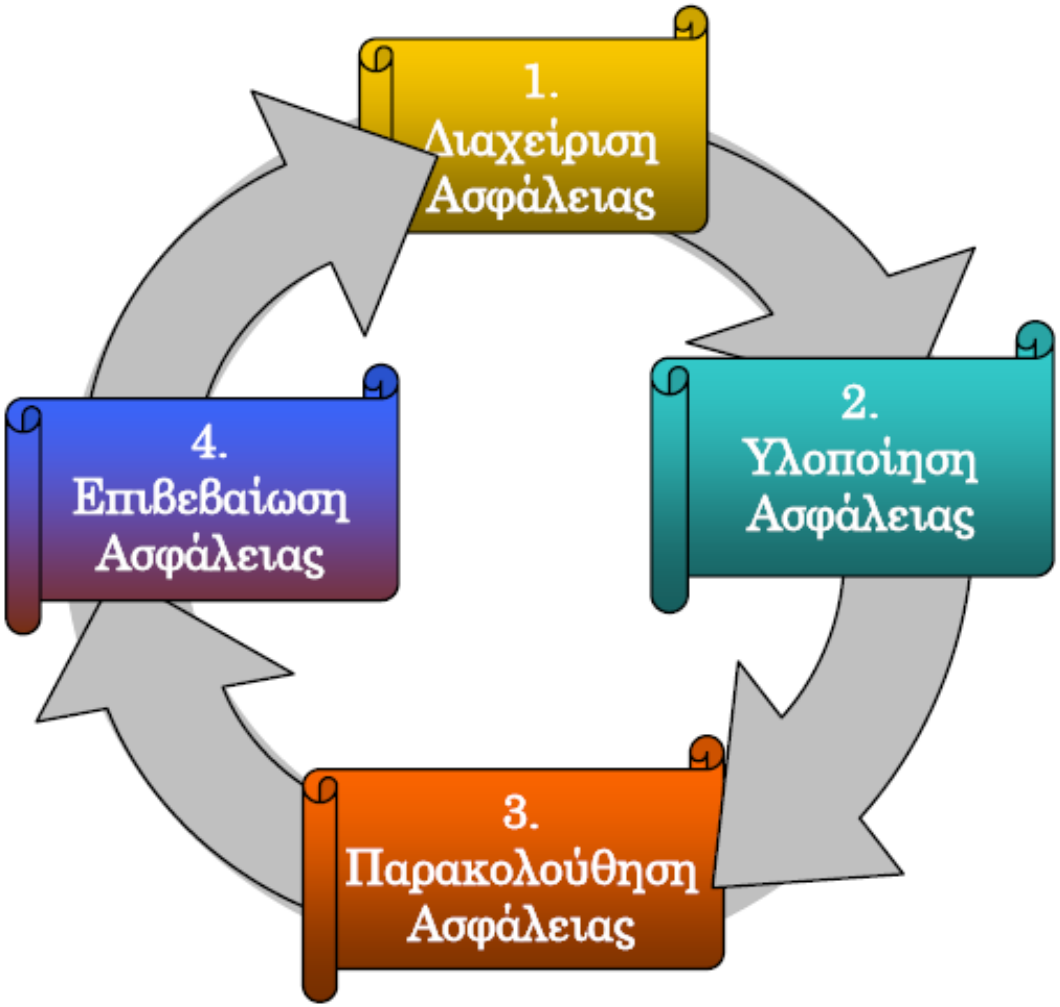
Διασύνδεση βασικών όρων ασφάλειας



1. Εισαγωγικές έννοιες

1. Βασικές έννοιες ασφάλειας Π.Σ.
2. **Ο κύκλος ζωής της ασφάλειας**
3. Συστήματα διαχείρισης ασφάλειας
4. Πρότυπα ασφάλειας
5. Εποπτικό/ρυθμιστικό πλαίσιο

Ο «κύκλος ζωής» της ασφάλειας



Διαχείριση Ασφάλειας (Security Management) – 1/2

- Η φάση αυτή αποτελεί το **στρατηγικό σχεδιασμό της ασφάλειας**
- Καθορισμός των γενικών κατευθύνσεων και της πολιτικής για την επαρκή προστασία του Π.Σ.
- Ανάλυση απαιτήσεων ασφάλειας
  - συστημάτων
  - εφαρμογών
  - υποδομών
  - πληροφοριών ενός οργανισμού
- Εντοπισμός των ευαίσθητων από πλευράς ασφάλειας σημείων
  - ανάλογα με βαθμό κρισιμότητας των επιχειρηματικών λειτουργιών που υποστηρίζουν

Διαχείριση Ασφάλειας (Security Management) – 2/2

- Η φάση της Διαχείρισης Ασφάλειας περιλαμβάνει δραστηριότητες όπως:
  1. Διενέργεια Ανάλυσης και Διαχείρισης Κινδύνου (Risk Analysis and Risk Management)
  2. Σύνταξη Πολιτικής Ασφάλειας (Security Policy)
  3. Σύνταξη Σχεδίου Συνέχειας Λειτουργιών (Business Continuity Plan)
  4. Σύνταξη Σχεδίου Ανάκαμψης Συστημάτων (Disaster Recovery Plan)

Υλοποίηση Ασφάλειας (Security Implementation) – 1/4

- Πραγματοποιείται ο **σχεδιασμός** και η **εγκατάσταση/ διαμόρφωση/ λειτουργία** των τεχνικών λύσεων που απαιτούνται για την υλοποίηση των απαιτήσεων ασφάλειας.
- (Α) Σχεδιασμός της αρχιτεκτονικής ασφάλειας του δικτύου
  - τοπολογία του δικτύου
  - καθορισμός των σημείων ελέγχου εισόδου και εξόδου
  - σχεδιασμός του ελέγχου πρόσβασης
  - διαχωρισμός του δικτύου σε εικονικά ιδιωτικά δίκτυα (VPN) ή ανεξάρτητες ζώνες

Υλοποίηση Ασφάλειας (Security Implementation) – 2/4

- (Β) Σχεδιασμός της ασφάλειας των συστημάτων και των εφαρμογών
  - Καθορισμός ομάδων χρηστών και δικαιωμάτων για συστήματα και εφαρμογές
  - Καθορισμός μέτρων ελέγχου πρόσβασης
  - Σχεδιασμός μέτρων ασφάλειας συστημάτων (προστασία από ιούς, παραμετροποίηση ΛΣ και εφαρμογών, αντίγραφα ασφαλείας, διαδικασίες ασφάλειας κτλ.

Υλοποίηση Ασφάλειας (Security Implementation) – 3/4

- (Γ) Καθορισμός προδιαγραφών για συστήματα ασφάλειας, όπως:
  - Firewall, IDS, Δρομολογητές,
  - Συστήματα ελέγχου πρόσβασης, Anti-virus , Υποδομές διαχείρισης κλειδιών, συστήματα λήψης εφεδρικών αρχείων κτλ.
  - Διαμόρφωση ρυθμίσεων ασφάλειας σε λειτουργικά συστήματα, εφαρμογές, εξυπηρετητές υπηρεσιών κτλ.

Υλοποίηση Ασφάλειας (Security Implementation) – 4/4

- (Δ) Πραγματοποιείται η υλοποίηση, εγκατάσταση, διαμόρφωση, δοκιμή και πραγματική λειτουργία:
  - του απαιτούμενου εξοπλισμού ασφάλειας (υλικού και λογισμικού)
    - π.χ η εγκατάσταση και παραμετροποίηση firewall, IDS, anti-virus, PKI, κτλ.
  - η παραμετροποίηση των συστημάτων και των εφαρμογών
    - π.χ. η διαμόρφωση των χρηστών Λ.Σ. και εφαρμογών, των δικαιωμάτων πρόσβασης κτλ.

Παρακολούθηση Ασφάλειας (Security Monitoring)

- Περιλαμβάνει εργασίες όπως:
  - την καθημερινή παρακολούθηση ορθής λειτουργίας των συστημάτων
    - αρχεία καταγραφής (log files) Λ.Σ./εφαρμογών
    - Έλεγχος χρηστών και δικαιωμάτων
  - την τακτική ενημέρωση/ επικαιροποίηση των εφαρμογών και συστημάτων ασφάλειας
    - π.χ. κανόνων πρόσβασης του firewall, IDS
    - ενημέρωση (update) του anti-virus, IDS, κτλ.
  - την παρακολούθηση των εξειδικευμένων μηχανισμών εντοπισμού πιθανών προβλημάτων ασφάλειας όπως
    - firewall/IDS/ani-virus alerts, κτλ

Επιβεβαίωση Ασφάλειας (Security Assurance) – 1/2

- Στο στάδιο αυτό πραγματοποιούνται έλεγχοι για:
  - την διασφάλιση της πλήρους και ορθής εφαρμογής των επιλεγμένων μέτρων
  - της αποτελεσματικότητας των μέτρων να αντιμετωπίσουν τα πραγματικά και πιθανώς μεταβαλλόμενα προβλήματα ασφάλειας

- Οι έλεγχοι αυτοί μπορεί να είναι
  - εσωτερικοί (internal audits) ή
  - εξωτερικοί έλεγχοι από ανεξάρτητους φορείς (external/independent audits)

Επιβεβαίωση Ασφάλειας (Security Assurance) – 2/2

- Η διεξαγωγή των ελέγχων μπορεί να στηρίζεται σε
  - ερωτηματολόγια ελέγχου διαδικασιών (checklists)
  - τεχνικούς ελέγχους, penetration tests κτλ.

- Ανάλογα με τα αποτελέσματα των ελέγχων ενδέχεται να προκύψει η ανάγκη για **αναθεώρηση της στρατηγικής ασφάλειας**.

- Ο έλεγχος της αναθεώρησης θα πρέπει να πραγματοποιείται ανεξάρτητα από το εάν θα γίνουν τελικά οι αλλαγές ή όχι.

1. Εισαγωγικές έννοιες

1. Βασικές έννοιες ασφάλειας Π.Σ.
2. Ο κύκλος ζωής της ασφάλειας
3. **Συστήματα διαχείρισης ασφάλειας**
4. Πρότυπα ασφάλειας
5. Εποπτικό/ρυθμιστικό πλαίσιο

Σύστημα Διαχείρισης Ασφάλειας Π.Σ. (ΣΔΑΠ)

- Ένα Σύστημα Διαχείρισης Ασφάλειας Π.Σ. (Information Security Management System – ISMS) ορίζεται ως:
  - Ένα (υπο-) σύστημα διοίκησης (management system) το οποίο βασίζεται σε μία προσέγγιση επικινδυνότητας (risk-based approach), με σκοπό τον ορισμό, την εφαρμογή, λειτουργία, παρακολούθηση, επικαιροποίηση και βελτίωση της ασφάλειας ενός Π.Σ.
- Το βασικό πρότυπο για τη δημιουργία ενός ΣΔΑΠ είναι το πρότυπο ISO 27001 (πρώην ISO 17799)

Σύστημα Διαχείρισης Ασφάλειας **ISO 27001**

- Είναι de facto standard για τον καθορισμό ενός ΣΔΑΠ
- Ακολουθεί τη δομή προτύπων συστημάτων διοίκησης
- Είναι συμβατό με άλλα ISO πρότυπα συστημάτων διοίκησης όπως ISO 9001, 14001, 18001, κτλ.
- Ακολουθεί ένα «κύκλο ζωής», το μοντέλο PDCA (Plan-Do-Check-Act)

Μοντέλο PDCA του προτύπου ISO 27001

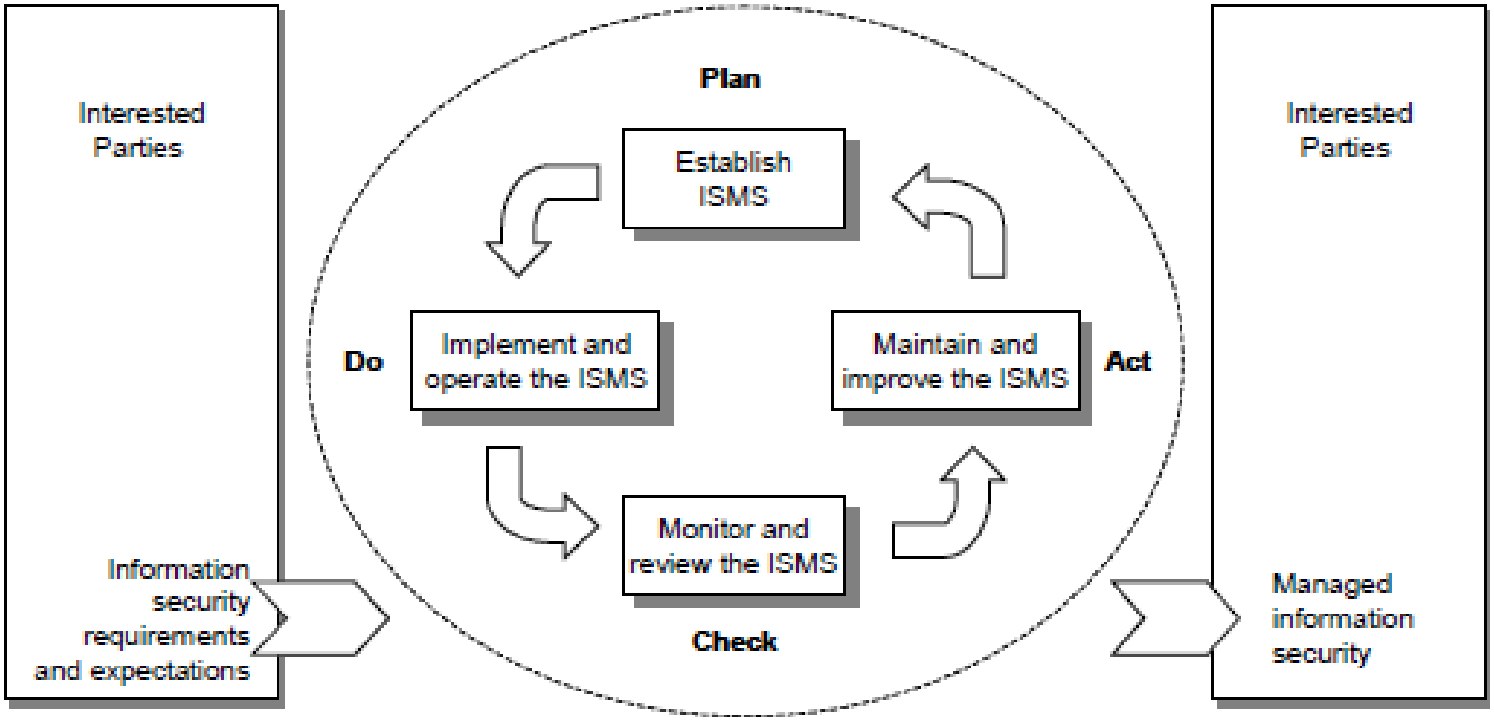


Figure 1 — PDCA model applied to ISMS processes

Πηγή: ISO 27001:2005

Ένα γενικό πλαίσιο αποτίμησης της ασφάλειας Π.Σ.

1. Προσδιορισμός των Αγαθών του Συστήματος

- Φυσικά αγαθά
  - Χρήστες, υλικό, λογισμικό κτλ.
- Αγαθά Δεδομένων
  - Έντυπα αρχεία, ηλεκτρονικά αρχεία, Βάσεις δεδομένων
- Άυλα αγαθά
  - Φήμη
  - Ηθικό συνεργατών
  - Επίπεδο προστασία απόρρητων / προσωπικών δεδομένων

Ένα γενικό πλαίσιο αποτίμησης της ασφάλειας Π.Σ.

2. Προσδιορισμός των Απειλών **(για κάθε αγαθό)**
   - Σκόπιμες, προερχόμενες από ανθρώπους
     - Πλαστοπροσωπία χρήστη
     - Κλοπή κωδικού χρήστη
     - Εκμετάλλευση κενών ασφάλειας (δικτύου, Λ.Σ., εφαρμογών κτλ)
     - Κακή χρήση των πόρων
     - Μη εξουσιοδοτημένη ανάγνωση
     - Είσοδος κακόβουλου λογισμικού
     - Κλοπή
     - Απάτη
     - Βανδαλισμός κτλ

Ένα γενικό πλαίσιο αποτίμησης της ασφάλειας Π.Σ.

(2)… Προσδιορισμός των Απειλών

- Μη Σκόπιμες (τυχαίες) απειλές
  - Λανθασμένη χρήση συστήματος
  - Προγραμματιστικό σφάλμα
  - Εσφαλμένη εφαρμογή διαδικασίας
  - Μη σκόπιμη αποκάλυψη δεδομένων
  - Μη σκόπιμη φθορά εξοπλισμού
  - Πρόβλημα τάσης ρεύματος
- Φυσικές / περιβαλλοντικές
  - Πλημμύρα, Σεισμός, Κεραυνός, ηλεκτρικά προβλήματα, κτλ

Ένα γενικό πλαίσιο αποτίμησης της ασφάλειας Π.Σ.

3. Καθορισμός συχνότητας και σοβαρότητας των απειλών

- Στατιστικές τεχνικές
- Αποτελέσματα ελέγχων
- Αποτίμηση υλικών και άυλων αγαθών

- Το τελικό αποτέλεσμα είναι:
  - Για κάθε ζεύγος αγαθό – απειλή, ποια είναι η πιθανότητα εμφάνισης της απειλής;

Ένα γενικό πλαίσιο αποτίμησης της ασφάλειας Π.Σ.

4. Καταγραφή & αξιολόγηση υφιστάμενων μέτρων

- Τεχνικά μέτρα ασφάλειας
  - **Υπάρχουν συστήματα ελέγχου προσπέλασης**; (password, ID cards, certificates, Access Lists, κτλ)
  - **Υπάρχουν συστήματα ασφάλειας δικτύου**; (Firewall, IDS, κτλ)
  - Λοιπά συστήματα ασφάλειας.
- Διαδικασίες
  - **Υπάρχουν κατάλληλες διαδικασίες ασφάλειας** (π.χ. διαδικασία χειρισμού περιστατικών ασφάλειας);
- Αποτίμηση αδυναμιών ασφάλειας
  - Δοκιμές εντοπισμού τεχνικών ευπαθειών
  - Αδυναμίες διαδικασιών

Ένα γενικό πλαίσιο αποτίμησης της ασφάλειας Π.Σ.

5. Αποτίμηση κινδύνων ασφάλειας

- Εντοπισμός κινδύνων με βάση την εκτίμηση των πιθανών συνεπειών (impact), απειλών και αδυναμιών ασφάλειας
- **Επικινδυνότητα = Συνέπεια ⊗ Απειλή ⊗ Αδυναμία**
- Ταξινόμηση των κινδύνων

Ένα γενικό πλαίσιο αποτίμησης της ασφάλειας Π.Σ.

6. Καθορισμός σχεδίου ασφάλειας(security plan)

- Με βάση τους κινδύνους που προέκυψαν, ποια επιπλέον μέτρα χρειάζονται;
  - Μείωση πιθανότητας απειλής ή/και μείωση αδυναμίας.
- Καθορισμός προτεραιοτήτων
- Καθορισμός Πολιτικής Ασφάλειας και διαδικασιών ασφάλειας

Πολιτική και Διαδικασίες Ασφάλειας

- Η Πολιτική Ασφάλειας καθορίζει σε γενικές γραμμές, επιτρεπτές και μη επιτρεπτές ενέργειες για όλες τις κατηγορίες χρηστών και για όλα τα αγαθά του Π.Σ.
- Οι πολιτικές υπαγορεύουν μέτρα ασφάλειας
- Τα μέτρα ασφάλειας υλοποιούνται με μηχανισμούς ασφάλειας
- Σύνθεση πολιτικών
  - Σε περίπτωση αντικρουόμενων πολιτικών, χρειάζεται μηχανισμός επίλυσης διαφορών

1. Εισαγωγικές έννοιες

1. Βασικές έννοιες ασφάλειας Π.Σ.
2. Ο κύκλος ζωής της ασφάλειας
3. Συστήματα διαχείρισης ασφάλειας
4. **Πρότυπα ασφάλειας**
5. Εποπτικό/ρυθμιστικό πλαίσιο

Πρότυπα Ασφάλειας

- Υπάρχουν πρότυπα για πολλούς τομείς της ασφάλειας. Μερικά βασικά πρότυπα είναι:
  - ISO 27001: Πρότυπο για τον καθορισμό απαιτήσεων ασφάλειας Π.Σ.
  - ISO 27002: Πρότυπο για την εφαρμογή ΣΔΑΠ με βάση τις απαιτήσεις ασφάλειας του 27001
  - ISO 27005: Πρότυπο για τη διαχείριση πληροφοριακού κινδύνου
  - ISO/IEC 7498-2 και ITU-T X.800: Πρότυπα ασφάλειας δικτύων

Το πρότυπο ISO 27001

- Διακρίνει την ασφάλεια σε **δέκα βασικούς τομείς.**
  1. **Πολιτική Ασφάλειας**
  2. **Οργανωτική Ασφάλεια**
  3. **Ταξινόμηση και Έλεγχος Αγαθών**
  4. **Ασφάλεια σε Θέματα Προσωπικού**
  5. **Φυσική και Περιβαλλοντολογική Ασφάλεια**
  6. **Διαχείριση Τηλεπικοινωνιών και Λειτουργιών**
  7. **Έλεγχος Πρόσβασης**
  8. **Ανάπτυξη και Συντήρηση Συστημάτων**
  9. **Διαχείριση Συνέχειας Λειτουργιών**
  10. **Νομική Συμμόρφωση**
- Για κάθε έναν από αυτούς τους τομείς δίνονται συγκεκριμένες προδιαγραφές ασφάλειας.
- Όσο πιο κοντά στις προδιαγραφές αυτές είναι μια επιχείρηση, τόσο πιο ασφαλής είναι.

Το πρότυπο ISO 27002

- Το ISO 27001 θέτει τις απαιτήσεις ασφάλειας, όχι τον τρόπο εφαρμογής τους
- ISO 27002:2005 – **Κώδικας εφαρμογής (code of practice)**
- Διεξοδικός κατάλογος αποδεκτών μέτρων ασφάλειας
- Ανάλυση των μέτρων ασφάλειας του ISO 27001
- Αποτελεί βάση για την εφαρμογή του ISO 27001
- Μη πιστοποιήσιμο

Το πρότυπο ISO 27005

- Το ISO 27005:2008 (Information security risk management) περιλαμβάνει οδηγίες για την ανάλυση διαχείριση πληροφοριακού κινδύνου σε έναν οργανισμό
- Δεν παρέχει κάποια συγκεκριμένη μεθοδολογία
- Μπορούν να χρησιμοποιηθούν διάφορες μεθοδολογίες ανάλυσης και διαχείρισης πληροφοριακού κινδύνου, σύμφωνα με το πρότυπο 27005.

Τα πρότυπα ISO 7498-2, ITU-T X.800

- Καθορίζει στόχους ασφάλειας για κάθε επίπεδο δικτύου
- Οι στόχοι ασφάλειας επιτυγχάνονται μέσω **πολιτικών ασφάλειας (security policies)**:
  - το σύνολο κριτηρίων το οποίο ορίζει την παροχή υπηρεσιών ασφάλειας
- **υπηρεσίες ασφάλειας (security services):**
  - υπηρεσία η οποία παρέχεται από ένα επίπεδο δικτύου, προκειμένου να εξασφαλιστεί η επαρκής προστασία των συστημάτων ή των μεταδιδόμενων δεδομένων
- Μία υπηρεσία ασφάλειας υλοποιείται με τη βοήθεια κατάλληλων **μηχανισμών ασφάλειας (security mechanisms)**
  - μηχανισμοί που μπορούν να χρησιμοποιηθούν για να επιβάλουν τεχνικά την εφαρμογή μια υπηρεσίας ασφάλειας

1. Εισαγωγικές έννοιες

1. Βασικές έννοιες ασφάλειας Π.Σ.
2. Ο κύκλος ζωής της ασφάλειας
3. Συστήματα διαχείρισης ασφάλειας
4. Πρότυπα ασφάλειας
5. **Εποπτικό/ρυθμιστικό πλαίσιο**

Νομικές/ρυθμιστικές απαιτήσεις ασφάλειας

- Η συλλογή και επεξεργασία δεδομένων, καθώς και η ανταλλαγή τους μέσω δικτύων, προϋποθέτει την τήρηση νομικών και ρυθμιστικών απαιτήσεων ασφάλειας
- Θα πρέπει να λαμβάνονται υπόψη, κατά το στρατηγικό σχεδιασμό της ασφάλειας Π.Σ.
- Ανάλογα με το είδος του οργανισμού, ενδέχεται να υπάρχουν διαφορετικές απαιτήσεις, π.χ.
  - Π.Σ. παρόχου υπηρεσιών υγείας (νοσοκομείο)
  - Π.Σ. παρόχου δικτύου επικοινωνίας (ISP)
  - Π.Σ. παρόχου υπηρεσιών πιστοποίησης (PKI), κτλ

Προστασία δεδομένων (1/3)

- Σύνταγμα της Ελλάδας (άρθρο 9Α)
  - “καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων…”
- Νόμος 2472/97 για την προστασία δεδομένων. Ορίζει κατηγορίες προσωπικών και ευαίσθητων δεδομένων
- **Δεδομένα προσωπικού χαρακτήρα:** Κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων (φυσικό πρόσωπο) και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί.
  - Δεν περιλαμβάνονται τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν να ταυτοποιηθούν τα φυσικά πρόσωπα.

Προστασία δεδομένων (2/3)

- **Ευαίσθητα δεδομένα:** Ειδικές κατηγορίες δεδομένων που αφορούν
  - Φυλετική ή εθνική προέλευση
  - Πολιτικά φρονήματα
  - Θρησκευτικές ή φιλοσοφικές πεποιθήσεις
  - Συμμετοχή σε συνδικαλιστική οργάνωση
  - Θέματα υγείας
  - Κοινωνική πρόνοια
  - Ερωτική/ιδιωτική ζωή
  - Ποινικές διώξεις ή καταδίκες

Προστασία δεδομένων (3/3)

- Μόνο με συγκατάθεση του υποκειμένου (χρήστη) επιτρέπεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα.
  - Υπάρχουν συγκεκριμένες εξαιρέσεις που επιτρέπεται και χωρίς τη συγκατάθεση του χρήστη.
- Για τα ευαίσθητα δεδομένα, απαγορεύεται η συλλογή και επεξεργασία.
  - Επιτρέπεται μόνο κατ' εξαίρεση, μετά από άδεια της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), η οποία είναι ανεξάρτητη Αρχή, υπεύθυνη για τη ρύθμιση των σχετικών θεμάτων
- Απαιτείται η δήλωση στην ΑΠΔΠΧ του υπεύθυνου επεξεργασίας

General Data Protection Regulation (GDPR)

- Νέα νομοθεσία της ΕΕ για την Προστασία Προσωπικών Δεδομένων
  - Παρουσιάστηκε: **14 Απριλίου 2016**
  - Τίθεται σε ισχύ: **25 Μαΐου 2018**
- Κύριες αλλαγές [9]:
  - **Increased Territorial Scope** (Ισχύει και εκτός ΕΕ, εφόσον τα δεδομένα που επεξεργάζεται κάποιος αφορούν κατοίκους της ΕΕ)
  - **Penalties** (μέχρι το 4% του παγκόσμιου ετήσιου τζίρου ή €20.000.000, όποιο είναι μεγαλύτερο!)
  - **Consent** (πρέπει να είναι σαφής η συμφωνία των κατόχων των δεδομένων)

GDPR: Δικαιώματα υποκειμένων (data subject rights) (1/2)

- **Breach Notification**
  - Υποχρεωτική ενημέρωση, εντός 72 ωρών
- **Right to Access**
  - Δικαιώμα ενημέρωσης των υποκειμένων, εάν γίνεται επεξεργασία των προσωπικών τους δεδομένων και για ποιο λόγο.
  - Δωρεάν λήψη ηλεκτρονικού αντιγράφουThis change is a dramatic shift to data transparency and empowerment of data subjects.
- **Right to be Forgotten**
  - Δικαίωμα ελέγχου για την οριστική διαγραφή των δεδομένων
  - Έλεγχος του δικαιώματος του υποκειμένου σε σχέση με το “κοινό συμφέρον”

GDPR: Δικαιώματα υποκειμένων (data subject rights) (2/2)

- **Data portability**
  - Δικαίωμα υποκειμένου να λάβει τα δεδομένα που τον αφορούν από έναν “ελεγκτή δεδομένων” (data controller) και να τα μεταφέρει σε κάποιον άλλο ελεγκτή δεδομένων.
- **Privacy by Design**
  - Εισαγωγή τεχνικών προστασίας δεδομένων από τη σχεδιασμού των συστημάτων και όχι σαν επιπλέον στοιχεία (add-on). Ελαχιστοποίηση των δεδομένων (data minimisation)
  - Περιορισμός της πρόσβασης στα δεδομένα με βάση την αρχή της ανάγκης χρήσης (needing to act out the processing)
- **Data Protection Officers**
  - Ορισμός DPO με συγκεκριμένα κριτήρια και υποχρεώσεις

Απόρρητο επικοινωνιών (1/2)

- Σύνταγμα της Ελλάδας (Άρθρο 19, παρ. 2)
  - «…με σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο».
- Νόμος 3115/2003
  - Σύσταση της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) με σκοπό τον έλεγχο και την εποπτεία
- Κανονισμοί Διασφάλισης Απορρήτου των Επικοινωνιών της ΑΔΑΕ
  - Απαιτείται η εφαρμογή Πολιτικής Ασφάλειας για τη διασφάλιση του απορρήτου των επικοινωνιών, από όλους τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών

Απόρρητο επικοινωνιών (2/2)

- Οι εφαρμογή των Κανονισμών Διασφάλισης Απορρήτου των Επικοινωνιών είναι υποχρεωτική για όλους τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών
- Απαιτείται η λήψη μέτρων ασφάλειας για την προστασία:
  - Των ***«εσωτερικών δεδομένων»*** *(Content data):* Το πραγματικό περιεχόμενο της επικοινωνίας.
  - Των ***«εξωτερικών δεδομένων»*** *(Context data):* Δεδομένα που χρησιμοποιούνται για τον έλεγχο και την παροχή της επικοινωνίας. Π.χ.:
    - Τηλεφωνικός Αριθμός, διεύθυνση IP, διεύθυνση e-mail, ημερ./ώρα σύνδεσης/ αποσύνδεσης κτλ

Βιβλιογραφία

1. Δ. Πολέμη, Χ. Δημητριάδης, Σ. Παπαστεργίου, Α. Καλιαντζόγλου, Εργαστηριακά θέματα ασφάλειας, 2006.
2. Σ. Κάτσικας Δ. Γκρίτζαλης, Σ. Γκρίτζαλης, «Ασφάλεια Πληροφοριακών Συστημάτων», Εκδόσεις Νέων Τεχνολογιών, 2003.
3. International Standardization Organization, ISO/IEC 27001, Information Technology – Security Techniques – Information security management systems – Requirements, 2005.
4. International Standardization Organization, ISO/IEC 27002:2005, Information technology – Security techniques – Code of Practice for Information Security Management, 2007.
5. International Standardization Organization, ISO/IEC 27005:2008, Information technology – Security techniques Information security risk management, 2008.)
6. “Information Security Policies, Procedures and Standrards – Guideline for Effective Information Security Management:, Tomas R. Peltier, Auerbach publications, ISBN: 0-8493-1137-3, CRC Press, 2002.
7. “Information Security Risk Analysis”, Publisher: Auerbach Publications; 1st edition (January 23, 2001), ISBN: 0849308801
8. www.iso27001security.com
9. http://www.eugdpr.org/key-changes.html