ΤΕΧΝΟΛΟΓΙΕΣ & ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

ΙΩΑΝΝΗ Δ. ΙΓΓΛΕΖΑΚΗ

Εισαγωγή

- Το πρόβλημα της διαχείρισης της ασφάλειας πληροφοριών αποτελεί ένα ιδιαίτερα σημαντικό ζήτημα για τα σύγχρονα πληροφοριακά συστήματα, καθώς επηρεάζει σε παγκόσμια κλίμακα το ηλεκτρονικό επιχειρείν και την ανάπτυξη εθνικών και διεθνών κρίσιμων υποδομών.
- Η αξιοποίηση όλο και πιο προηγμένων τεχνολογιών, όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων, τα δίκτυα και το Διαδίκτυο, προσφέρει σημαντικές δυνατότητες, αλλά αυξάνει ανάλογα και τα προβλήματα που αφορούν την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

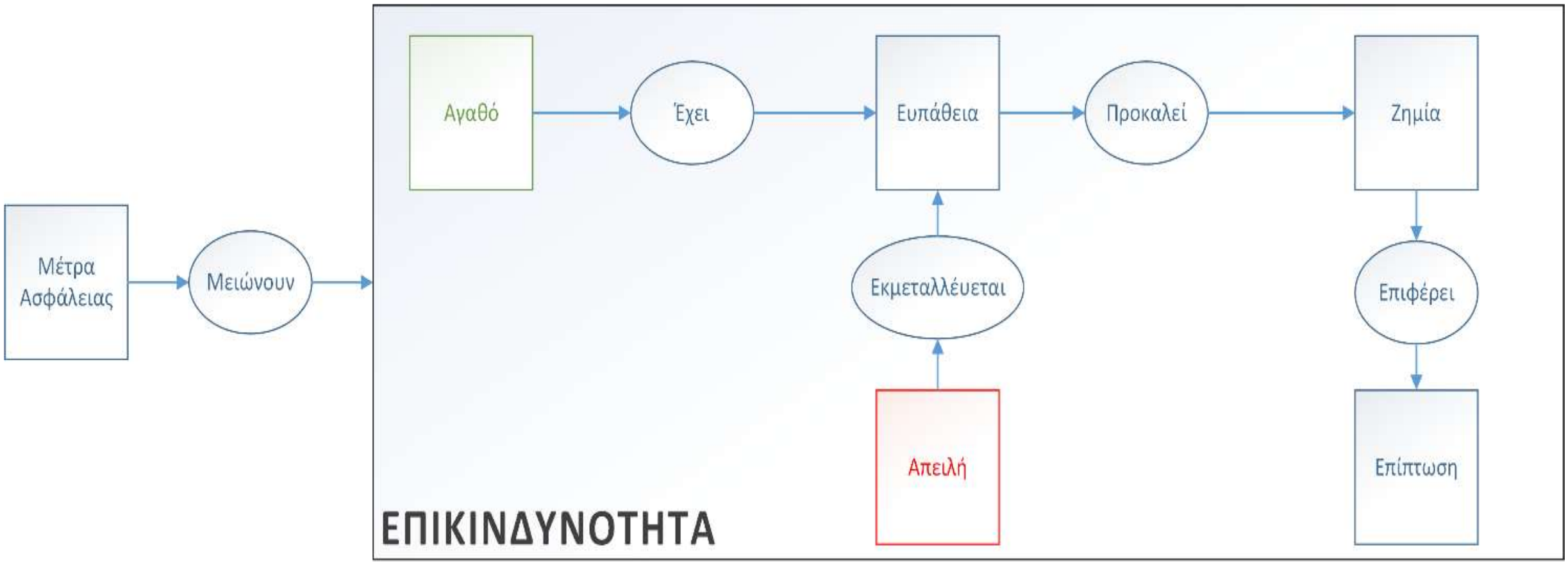
Πληροφοριακό σύστημα: Έννοια

- Το οργανωμένο σύνολο από ανθρώπους, λογισμικό, υλικό, διαδικασίες, εγκαταστάσεις και δεδομένα.
- Τα στοιχεία αυτά βρίσκονται σε μια συνεχή αλληλεπίδραση μεταξύ τους, αλλά και με το περιβάλλον, με σκοπό την παραγωγή και διαχείριση της πληροφορίας

Σημασία της ασφάλειας πληροφοριών

- Οι σύγχρονοι οργανισμοί εξαρτώνται από πληροφοριακά αγαθά σε ότι αφορά την αποτελεσματικότητα και τη κερδοφορία των λειτουργιών τους και για αυτό χρειάζεται να προστατεύουν αυτά τα αγαθά.
- Η διασφάλιση (assurance) της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών είναι σημαντική, ανεξάρτητα του κατά πόσον οι πληροφορίες αποτελούν αντικείμενο επεξεργασίας και διαχείρισης ή ανταλλάσσονται μεταξύ των συνεργαζόμενων οργανισμών.

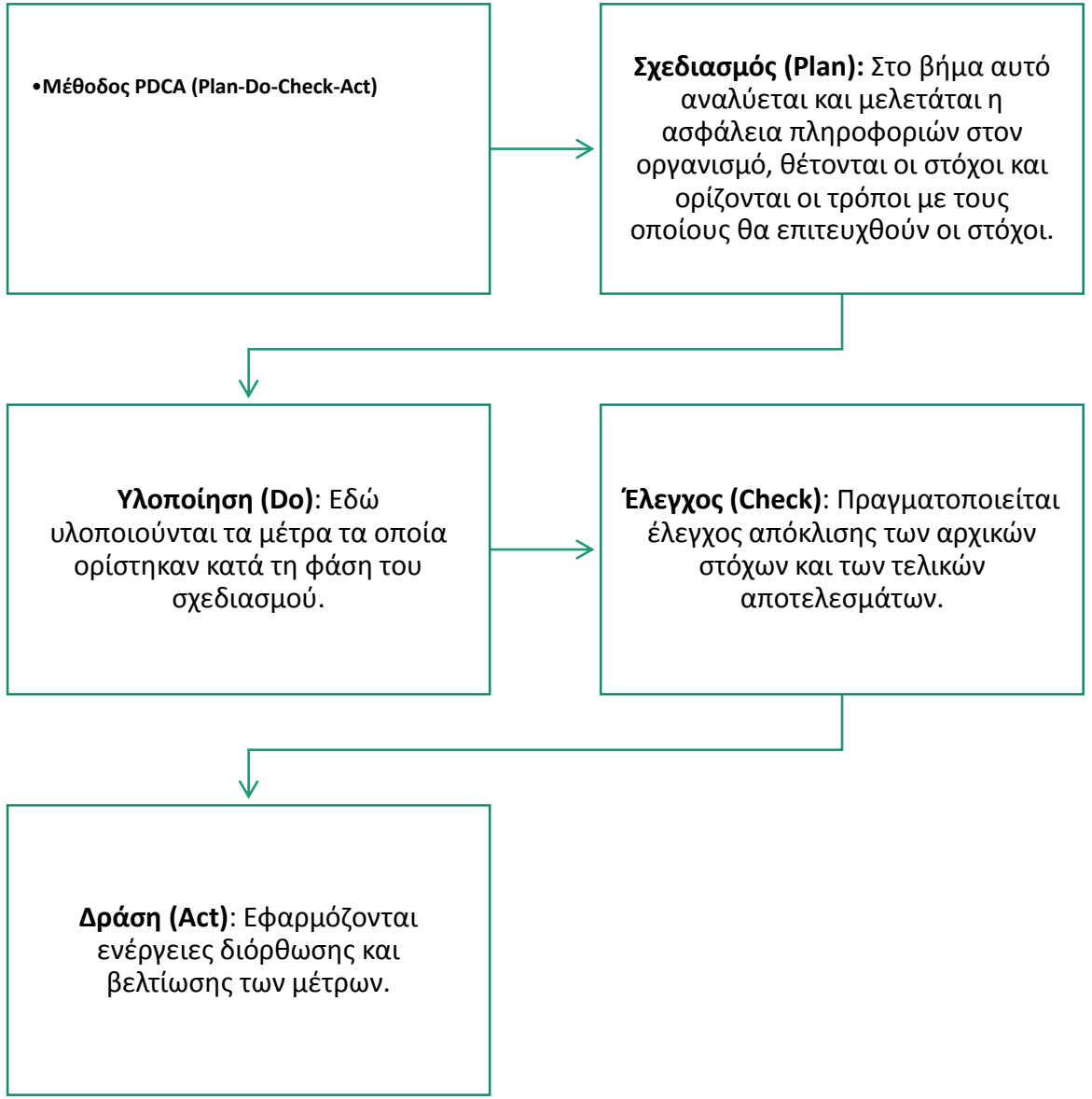
Ασφάλεια Πληροφοριών



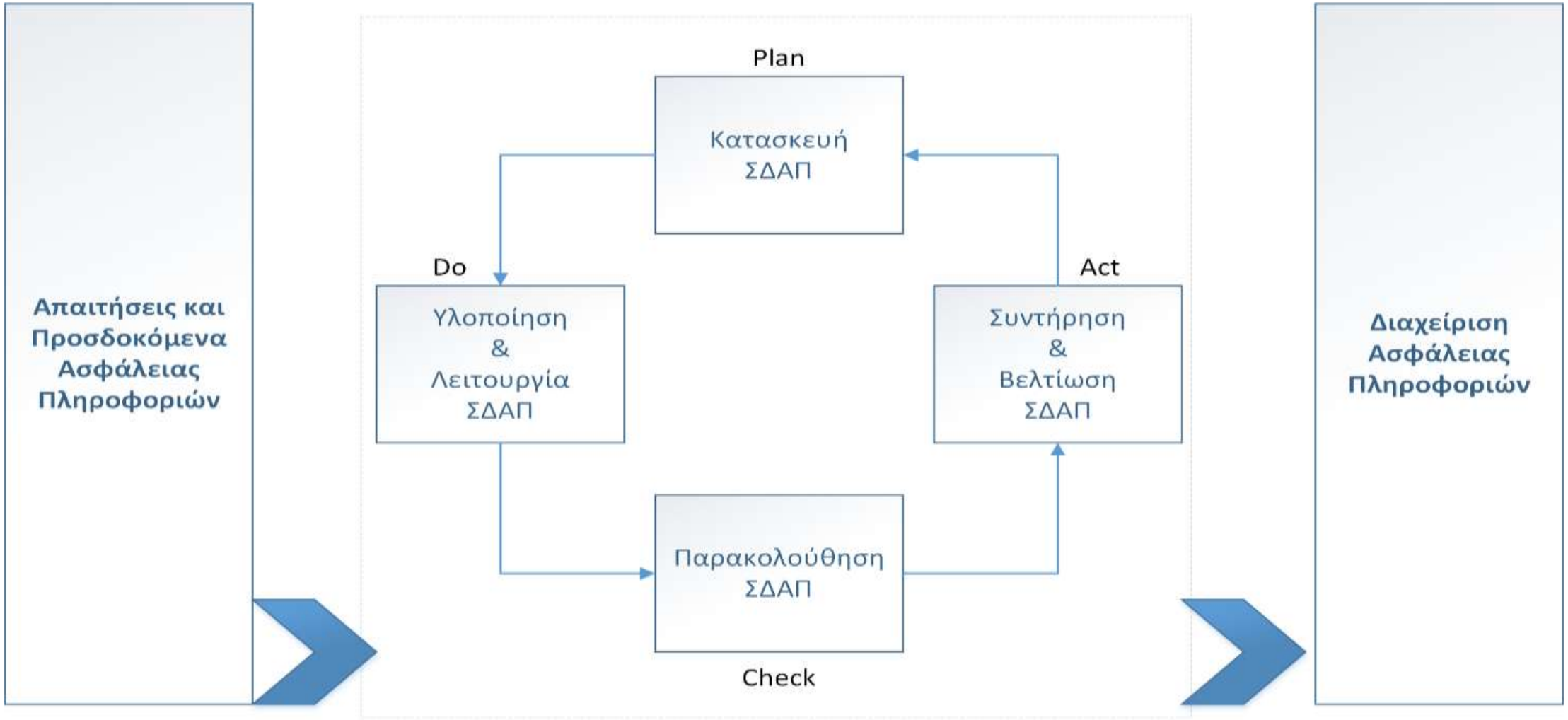
Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών

- Ο σχεδιασμός της ασφάλειας πληροφοριών ενός οργανισμού είναι μια επιχειρησιακή διεργασία, η οποία αποσκοπεί στο να παρέχονται τα κατάλληλα εργαλεία λήψης αποφάσεων, προκειμένου να μπορεί η διοίκηση να ασκήσει αποτελεσματικά το ρόλο της. Η ασφάλεια πληροφοριών δεν είναι ένα αμιγώς τεχνικό θέμα, αλλά συμπεριλαμβάνει ζητήματα και παραμέτρους από διάφορους χώρους (οικονομία, διοίκηση, κοινωνία κ.λπ.).
- Παράγοντες:
  - Αποδεκτό επίπεδο ασφάλειας.
  - Λειτουργικότητα του Πληροφοριακού Συστήματος που διαθέτει.
  - Κόστος που επιθυμεί να επωμισθεί ο οργανισμος.

Μεθοδολογία ανάπτυξης ΣΔΑΠ



Πρότυπο ISO/IEC 27001 – πλαίσιο διαχείρισης ασφάλειας πληροφοριών



Πρότυπα ISO 27K: οδηγός βέλτιστων πρακτικών για τη διαχείριση της ασφάλειας πληροφοριών και τη διαχείριση της σχετικής επικινδυνότητας

- **Όνομα** **Αντικείμενο**
- **ISO/IEC 27000** Εισαγωγή και λεξιλόγιο όρων
- **ISO/IEC 27001** Απαιτήσεις υλοποίησης και συντήρησης Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
- **ISO/IEC 27002** Πρακτικές διαχείρισης της ασφάλειας και επιλογής μέτρων ασφάλειας
- **ISO/IEC 27003** Οδηγίες σχεδιασμού ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
- **ISO/IEC 27004** Μετρικές εκτίμησης της αποτελεσματικότητας υλοποιημένου Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
- **ISO/IEC 27005** Οδηγίες διαχείρισης Επικινδυνότητας
- **ISO/IEC 27006** Οδηγίες ελέγχου και πιστοποίησης Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
- **ISO/IEC 27007** Οδηγίες ικανοτήτων ελεγκτών Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών
- **ISO/IEC 27008** Οδηγίες ελέγχου της υλοποίησης Συστήματος Διαχείρισης Ασφάλειας και Πληροφοριών
- **ISO/IEC 27010** Οδηγίες για κοινότητες ανταλλαγής πληροφοριών

Μέτρα προστασίας ΣΔΑΠ

- Το έγγραφο της πολιτικής ασφάλειας πληροφοριών.
- Ο επιμερισμός καθηκόντων σχετικών με την ασφάλεια πληροφοριών.
- Η ευαισθητοποίηση, η εκπαίδευση και η κατάρτιση σε θέματα ασφάλειας πληροφοριών.
- Η σωστή λειτουργία των εφαρμογών.
- Η διαχείριση των ευπαθειών.
- Η διαχείριση της επιχειρησιακής συνέχειας.
- Η διαχείριση των συμβάντων ασφάλειας και των συναφών βελτιώσεων που αφορούν την ασφάλεια πληροφοριών του οργανισμού.

Ανάλυση και αποτίμηση επικινδυνότητας

	Χαρακτηρισμός Συστήματος.	Αναγνώριση Απειλής.	Αναγνώριση Ευπάθειας.
Ανάλυση Μηχανισμών Ασφάλειας.	Προσδιορισμός Πιθανότητας.	Ανάλυση Επίπτωσης.	Προσδιορισμός Επικινδυνότητας.
	Προτάσεις μηχανισμών Ελέγχου.	Τεκμηρίωση Αποτελεσμάτων.	

Χαρακτηρισμός συστήματος

- Συλλογή πληροφοριών για το ΠΣ (υλικό, λογισμικό, δίκτυο, χρήστες, πολιτικές ασφαλείας, αρχιτεκτονική συστήματος ασφαλείας, διοικητικοί έλεγχοι, ροές πληροφοριών, φυσικό περιβάλλον.
- Εργαλεία:
  - Ερωτηματολόγιο στο προσωπικό
  - Συνέντευξη με το διοικητικό προσωπικό
  - Εταιρικά έγγραφα
  - Αυτοματοποιημένα εργαλεία συλλογής πληροφοριών

Αναγνώριση απειλών

- Καταγραφή λίστας από ευπάθειες του πληροφοριακού συστήματος, που θα μπορούσαν να γίνουν αντικείμενο εκμετάλλευσης από ενδεχόμενες απειλές.
  - Αν το πληροφοριακό σύστημα δεν έχει σχεδιαστεί ακόμη, η αναζήτηση ευπαθειών θα πρέπει να επικεντρωθεί στις πολιτικές ασφάλειας του οργανισμού, στις σχεδιασμένες διαδικασίες ασφαλείας, καθώς και τις απαιτήσεις του συστήματος.
  - Αν το σύστημα είναι ήδη σε λειτουργία, η αναγνώριση των ευπαθειών θα πρέπει να επεκταθεί ώστε να περιέχει περισσότερη εξειδικευμένη πληροφορία, όπως σχεδιασμένα χαρακτηριστικά ασφάλειας μέσα στα έγγραφα του σχεδίου ασφαλείας, καθώς και αποτελέσματα της αξιολόγησης της ασφάλειας του συστήματος.

Ανάλυση μηχανισμών ασφάλειας

- Ο σκοπός αυτού του σταδίου είναι να αναλύσει τους μηχανισμούς ασφάλειας που ήδη εφαρμόζονται, ή σχεδιάζονται για εφαρμογή στον οργανισμό για να ελαττώσουν ή να εξαλείψουν την πιθανότητα εκμετάλλευσης ευπαθειών του συστήματος από διάφορες απειλές.

Προσδιορισμός πιθανότητας

- Για τον υπολογισμό της πιθανότητας εμφάνισης ενός περιστατικού ασφάλειας, λαμβάνεται υπόψη το κίνητρο των απειλών και η ικανότητα των δυνητικά επιτιθέμενων, η φύση της ευπάθειας, η ύπαρξη και η αποτελεσματικότητα των υφιστάμενων μέτρων προστασίας
- Η πιθανότητα μπορεί να είναι:
  - Υψηλή, όταν η απειλή έχει υψηλά κίνητρα, μεγάλη αποτελεσματικότητα και τα υφιστάμενα μέτρα προστασίας δεν επαρκούν.
  - Μεσαία, όταν η απειλή έχει υψηλά κίνητρα και μεγάλη αποτελεσματικότητα, αλλά τα υφιστάμενα μέτρα προστασίας επαρκούν.
  - Χαμηλή, όταν η απειλή δεν έχει υψηλά κίνητρα, δεν έχει αποτελεσματικότητα και τα υφιστάμενα μέτρα προστασίας επαρκούν.

Ανάλυση επίπτωσης

- Η επίπτωση ενός γεγονότος ασφάλειας (π.χ. μιας επίθεσης) μπορεί να περιγραφεί με τους όρους απώλειας ή υποβάθμισης των τριών κύριων χαρακτηριστικών της ασφάλειας: ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα.

Προσδιορισμός επικινδυνότητας

Κλίμακα επικινδυνότητας

- Υψηλή επικινδυνότητα: Άμεση ανάγκη για διορθωτικά μέσα.
- Μεσαία επικινδυνότητα: Ανάγκη για διορθωτικά μέσα σε εύλογο χρονικό διάστημα.
- Χαμηλή επικινδυνότητα: Αποδοχή της ή διορθωτικά μέσα.

Επόμενα βήματα

- Προτεινόμενα μέτρα προστασίας
  - προτείνονται εκείνα τα μέτρα προστασίας, τα οποία μπορούν να περιορίσουν τις ευπάθειες ή να τις εκμηδενίσουν
- Τεκμηρίωση αποτελεσμάτων
  - καταγραφή των αποτελεσμάτων σε μία ολοκληρωμένη αναφορά.

Σχέδιο ασφάλειας

- Στόχοι και σχέδια του οργανισμού σε σχέση με την ασφάλεια πληροφοριών.
- Ρόλοι και καθήκοντα εμπλεκομένων.
- Ρητή δήλωση υποστήριξης της Διοίκησης ως προς τη συμμόρφωση με την πολιτική.
- Δέσμευση της διοίκησης για ενεργό συμμετοχή.
- Πλάνο ελέγχων των διαδικασιών.
- Πλάνο παροχής κατάλληλης κατάρτισης του προσωπικού.

- http://noc.eap.gr/index.php/kentriki-politiki-asfaleias-pol20
- **πρότυπο ISO/IEC 17799**

Πολιτική ασφάλειας

- Στόχος της πολιτικής ασφάλειας (security policy) πληροφοριών είναι η παροχή κατευθύνσεων και υποστήριξης για ζητήματα ασφάλειας πληροφοριών. Η διοίκηση του οργανισμού θα πρέπει να καθορίσει μια σαφή και ξεκάθαρη πολιτική, την οποία και θα υποστηρίζει έμπρακτα. Η πολιτική αυτή θα πρέπει να ρυθμίζει ζητήματα ασφάλειας σε όλα τα επίπεδα του οργανισμού. Προτεινόμενα μέτρα:
- Έγγραφο της πολιτικής ασφάλειας πληροφοριών.
- Αναθεώρηση της πολιτικής ασφάλειας πληροφοριών.

Διαχείριση αγαθών

- Απόδοση ευθυνών για αγαθά
- Διαβάθμιση πληροφοριών
- Ασφάλεια ανθρώπινων πόρων
- Φυσική και περιβαλλοντική ασφάλεια
  - Στόχος είναι η αποτροπή μη-εξουσιοδοτημένης φυσικής πρόσβασης, ζημιάς και παρέμβασης στις εγκαταστάσεις και το πληροφοριακό σύστημα του οργανισμού. Οι κρίσιμής σημασίας εγκαταστάσεις επεξεργασίας δεδομένων θα πρέπει να βρίσκονται σε ασφαλείς περιοχές, προστατευμένες από μια περίμετρο ασφάλειας και από τους κατάλληλους μηχανισμούς. Θα πρέπει να προστατεύονται φυσικά από μη-εξουσιοδοτημένη πρόσβαση, παρεμβολές και καταστροφή.

Διαχείριση αγαθών

- Ασφάλεια εξοπλισμού
  - Τοποθέτηση και προστασία εξοπλισμού.
  - Μέσα υποστήριξης.
  - Ασφάλεια καλωδίωσης.
  - Συντήρηση εξοπλισμού.
  - Ασφάλεια εξοπλισμού εκτός των χώρων του οργανισμού.
  - Ασφαλής καταστροφή ή επαναχρησιμοποίηση εξοπλισμού.
  - Μετακίνηση αγαθών εκτός των χώρων του οργανισμού
- Διαχείριση επικοινωνιών και λειτουργιών

(συνέχεια)

- Σχεδιασμός και αποδοχή συστήματος
- Προστασία από κακόβουλο λογισμικό
- Λήψη εφεδρικού αντιγράφου ασφαλείας
- Διαχείριση ασφάλειας δικτύου – μέτρα προστασίας δικτύου, ασφάλεια δικτυακών υπηρεσιών
- Χειρισμός αποθηκευτικών μέσων
- Ασφάλεια υπηρεσιών ηλεκτρονικού εμπορίου
- Επίβλεψη

Έλεγχος πρόσβασης

- Διαχείριση πρόσβασης χρηστών
  - Διαδικασία εγγραφής χρηστών.
  - Διαχείριση προνομίων χρηστών.
  - Διαχείριση διαπιστευτηρίων (credentials) των χρηστών.
  - Επιθεώρηση προνομίων των χρηστών
- Ευθύνες χρηστών
- Έλεγχος πρόσβασης δικτύου
- Έλεγχος πρόσβασης σε λειτουργικά συστήματα
- Έλεγχος πρόσβασης σε πληροφορίες και εφαρμογές

Προμήθεια, ανάπτυξη και συντήρηση πληροφοριακών συστημάτων

- Απαιτήσεις ασφάλειας πληροφοριακών συστημάτων
- Ορθή επεξεργασία από τις εφαρμογές
- Κρυπτογραφικά μέτρα προστασίας. Σκοπός είναι η προστασία της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των πληροφοριών με κρυπτογραφικά μέσα. Για το σκοπό αυτό θα πρέπει να αναπτυχθεί μια πολιτική χρήσης κρυπτογραφικών μέτρων προστασίας
- Ασφάλεια αρχείων συστήματος. Θα πρέπει να ελέγχεται η πρόσβαση στα αρχεία του συστήματος και στον πηγαίο κώδικα των προγραμμάτων
- Διαχείριση τεχνικών ευπαθειών

Συμβάντα ασφάλειας

- **Αναφορά συμβάντων και ευπαθειών ασφάλειας**
- Σκοπός είναι η διασφάλιση του ότι τα συμβάντα και οι ευπάθειες ασφάλειας πληροφοριών γνωστοποιούνται με τρόπο που επιτρέπει την έγκαιρη λήψη κατάλληλων ενεργειών.
- **Διαχείριση συμβάντων ασφάλειας**
- Σκοπός είναι η διασφάλιση της εφαρμογής μιας συνεπούς και αποτελεσματικής προσέγγισης για τη διαχείριση των συμβάντων ασφάλειας πληροφοριών
- **Σχεδιασμός επιχειρησιακής συνέχειας**

Συμμόρφωση

- Καθορισμός της εφαρμοζόμενης νομοθεσίας.
- Δικαιώματα πνευματικής ιδιοκτησίας.
- Προστασία των αρχείων δεδομένων του οργανισμού.
- Προστασία του απόρρητου των προσωπικών πληροφοριών.
- Πρόληψη κακής χρήσης των μέσων αποθήκευσης, διακίνησης και επεξεργασίας πληροφοριών.
- Νόμιμη χρήση των κρυπτογραφικών μέσων
- **Συμμόρφωση με πολιτικές ασφάλειας, πρότυπα και τεχνικές**
- **Επιθεώρηση πληροφοριακών συστημάτων**

Διακυβέρνηση – Επικινδυνότητα - Συμμόρφωση