Ασφάλεια Συστημάτων

Τζέριες Μπεσαράτ, PhD

25 Φεβρουαρίου 2022, Άρτα

Το μάθημα:

Τμήμα Πληροφορικής και Τηλεπικοινωνιών

Προπτυχιακό μάθημα

Ασφάλεια Συστημάτων

Εβδομαδιαίες ώρες διδασκαλίας 5

3 ώρες Θεωρία / 1 ώρα Φροντιστηριακές Ασκήσεις / 1 ώρα Εργαστηρίου

Ημέρα μαθήματος: Παρασκευή 11:00

Ερώτημα

Τι σημαίνει Ασφάλεια Συστημάτων;

Ασφάλεια Συστημάτων

Η ασφάλεια πληροφοριακών συστημάτων, ασφάλεια υπολογιστικών συστημάτων ή ασφάλεια υπολογιστών, είναι ένα **γνωστικό πεδίο** της επιστήμης της πληροφορικής, και ειδικότερα του κλάδου των υπολογιστικών συστημάτων, που ασχολείται με:

την προστασία των υπολογιστών, των δικτύων που τους διασυνδέουν και των δεδομένων σε αυτά τα συστήματα, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους.

Βασικές Αρχές

Η ασφάλεια πληροφοριακών συστημάτων στηρίζεται σε τρεις βασικές ιδέες:

- Ακεραιότητα
- Διαθεσιμότητα
- Εμπιστευτικότητα

Ιστορικές Εξελίξεις

Αρχές δεκαετίας του 1970

Για πρώτη φορά μελετήθηκε η «Ασφάλεια Συστημάτων»

Αρχές δεκαετίας του 1970

Ο πρώτος ιός, ο Creeper, εμφανίστηκε επίσης στις αρχές της δεκαετίας του 1970 στο ARPANET

1988

Κυκλοφόρησε το πρώτο δικτυακό "σκουλήκι" (worm), το σκουλήκι Morris. Εκτιμάται ότι 6.000 συστήματα προσβλήθηκαν από το "σκουλήκι"

2007

Ανακαλύφθηκαν περισσότεροι από 711.000 καινούργιοι ιοί.

Σήμερα

Η χρήση αδύναμων κωδικών πρόσβασης παραμένει μία από τις κυριότερες δυσκολίες που αντιμετωπίζει ο επαγγελματίας στον τομέα.

Πληροφορίες για το μάθημα

Το μάθημα έχει χωριστεί σε 10 Διαλέξεις.

Σύμφωνα με τον οδηγό σπουδών ας αναφερθούμε στα Μαθησιακά Αποτελέσματα και στις Γενικές Ικανότητες που θα αναπτυχθούν.

Μαθησιακά Αποτελέσματα

Με την επιτυχή ολοκλήρωση του μαθήματος, οι φοιτήτριες/ές θα έχουν:

- Κατανοήσει προηγμένα θέματα ασφαλείας με έμφαση τόσο στο επίπεδο της κρυπτογραφίας (θεωρητικό επίπεδο) όσο και στο επίπεδο των εφαρμογών.
- Κατανοήσει κρυπτογραφικά σχήματα που χρησιμοποιούνται σε διαφορετικές εφαρμογές ασφαλείας.
- Κατανοήσει και θα μπορούν να υλοποιούν σύγχρονους, προηγμένους, αλγορίθμους συμμετρικής και ασύμμετρης κρυπτογραφίας.
- Κατανοήσει θέματα ασφαλείας τόσο σε επίπεδο υλικού (επιθέσεις πλάγιου μονοπατιού, επιθέσεις σφάλματος, Δούρειου Ίπποι Υλικού) όσο και σε επίπεδο λογισμικού (κακόβουλο λογισμικό, μη εξουσιοδοτημένες αλλαγές κώδικα) καθώς και σε επίπεδο δικτύου (ασφάλεια δικτύων, πρωτόκολλα ασφαλείας ενσύρματων ή ασύρματων δικτύων καθώς και δικτύων αισθητήρων).
- Κατανοήσει θέματα που σχετίζονται με την προστασία προσωπικών δεδομένων και με την χρήση των ανωνύμων πιστοποιητικών.
- Κατανοήσει πρότυπα εφαρμογής εμπιστοσύνης σε επίπεδο συστήματος.
- Αποκτήσει γνώσεις και δεξιότητες ώστε να μπορούν να υλοποιούν εφαρμογές εμπιστοσύνης τόσο σε υλικό όσο και σε λογισμικό.

Γενικές Ικανότητες

Με την επιτυχή ολοκλήρωση του μαθήματος, οι φοιτητές θα έχουν:

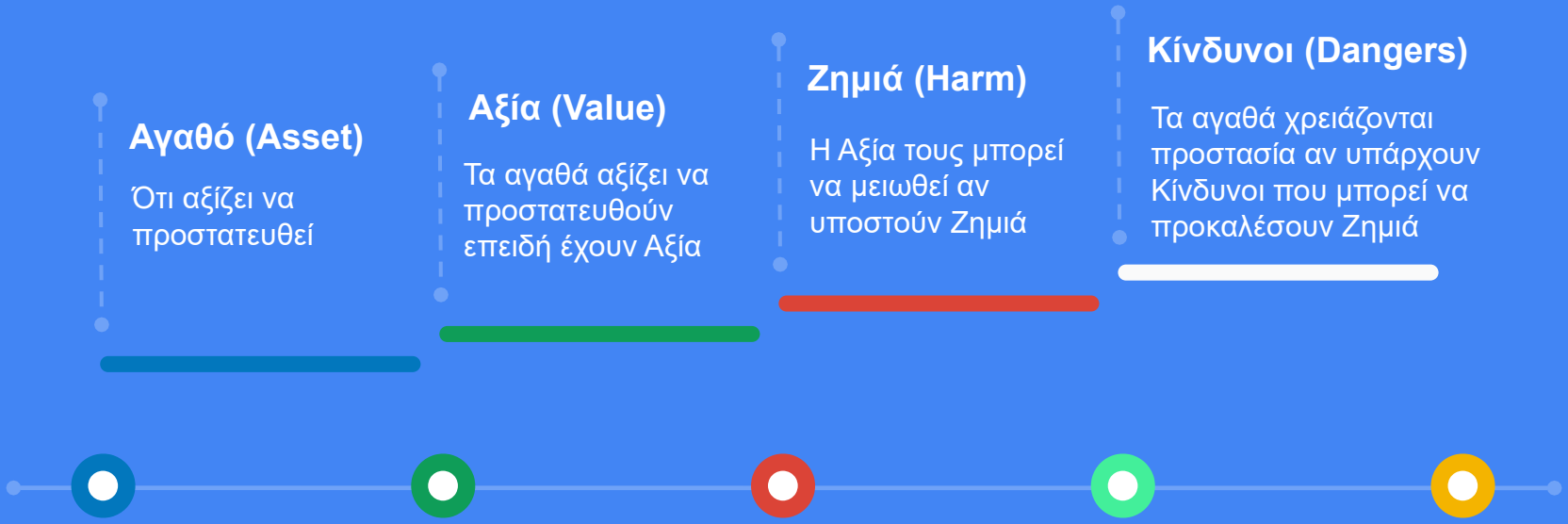
- Εφαρμογή της γνώσης στην πράξη.
- Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση των απαραίτητων τεχνολογιών.
- Προσαρμογή σε νέες καταστάσεις.
- Λήψη αποφάσεων.
- Αυτόνομη εργασία.
- Ομαδική εργασία.
- Σχεδιασμός και διαχείριση έργων.
- Άσκηση κριτικής και αυτοκριτικής.
- Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης.

Περιεχόμενα μαθήματος

Εισαγωγή

Η Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών αφορά **οντότητες** και **αντικείμενα** που αξίζει να προστατευθούν.

Εισαγωγή


Αγαθό (Asset)
Ότι αξίζει να προστατευθεί
Αξία (Value)
Τα αγαθά αξίζει να προστατευθούν επειδή έχουν Αξία
Ζημιά (Harm)
Η Αξία τους μπορεί να μειωθεί αν υποστούν Ζημιά
Κίνδυνοι (Dangers)
Τα αγαθά χρειάζονται προστασία αν υπάρχουν Κίνδυνοι που μπορεί να προκαλέσουν Ζημιά

Εισαγωγή

1. Μέσα Προστασίας

Ο **Ιδιοκτήτης** (Owner) ενός προστατευόμενου Αγαθού χρησιμοποιεί **Μέσα Προστασίας** (Safeguards) είτε για να μειώσει τον **Κίνδυνο** να προξενηθεί **Ζημιά** στο **Αγαθό** είτε για να μειώσει τις συνέπειές της.

2. Κόστος

Η χρήση Μέσων Προστασίας επιφέρει **Κόστος**. Δεδομένου ότι τα Μέσα Προστασίας δεν μπορούν να εγγυηθούν πλήρη ασφάλεια, το Κόστος τους πρέπει να αναλογεί στην **Επισφάλεια** (Hazard) του Αγαθού αυτού, καθώς και στις συνέπειες που θα έχει μια Ζημιά στον Ιδιοκτήτη του.

3. Στόχος Ασφαλείας

Ο Ιδιοκτήτης είναι εκείνος που θα κρίνει, όταν θέτει το **Στόχο Ασφάλειας** (Infosec Goal), ποια είναι η πιο επωφελής ισορροπία ανάμεσα στο Κόστος, την Επισφάλεια και τις Συνέπειες.
Ο Ιδιοκτήτης μπορεί, επίσης, να αναζητήσει **Εξασφάλιση** (Assurance) ότι ο Στόχος του θα επιτευχθεί με τα Μέσα Προστασίας που θα χρησιμοποιήσει.

Εισαγωγή

Κάθε αγαθό έχει Ιδιότητες (Attributes) που πρέπει να προστατευθούν.

Οι Ζημιές μπορεί να προκληθούν από Κινδύνους και αφορούν Ζημιές όχι στα Αγαθά, αλλά στις Ιδιότητές τους. Οι ζημιές εκτιμούνται από τον Ιδιοκτήτη ή το Χρήστη. Ο Ιδιοκτήτης είναι αυτός που θα καθορίσει τους Στόχους, οι οποίοι προσδιορίζουν τη μέγιστη ανεκτή Ζημιά που οι Ιδιότητες μπορούν να υποστούν. Τα Μέσα Προστασίας αντιμετωπίζουν τους Κινδύνους αποτρέποντας τις Ζημιές και προστατεύουν τις Ιδιότητες και τα Αγαθά. Ο όρος Εξασφάλιση υπονοεί ότι τα Μέσα Προστασίας μπορούν να αντιμετωπίσουν τους Κινδύνους προστατεύοντας τα Αγαθά και τις Ιδιότητές τους από Ζημιές.

Βασικές Έννοιες των εννοιολογικών δένδρων

- Αγαθά
- Ιδιοκτήτες & Χρήστες
- Ιδιότητες
- Ζημιά
- Κίνδυνοι
- Στόχοι
- Εξασφάλιση
- Μέσα Προστασίας
- Ασφάλεια Υποδομών

Αγαθά (1/5)

- **Δεδομένα** (Data)
  Ένα σύνολο κατανοητών συμβόλων που έχουν καταγραφεί.

- **Πληροφορία** (Information)
  Τα δεδομένα μαζί με την έννοια που τους αποδίδεται

Αγαθά (2/5)

Ένα Υπολογιστικό Σύστημα ορίζεται μέσω του Υπολογιστικού Συγκροτήματος και ένα Πληροφοριακό Σύστημα ορίζεται μέσω του Υπολογιστικού Συστήματος

Πληροφοριακό Σύστημα

(Information System)
Υπολογιστικό Συγκρότημα μαζί με τις πληροφορίες που διαχειρίζεται.

Υπολογιστικό Σύστημα

(IT System)
Υπολογιστικό Συγκρότημα εγκατεστημένο σε συγκεκριμένη τοποθεσία, με συγκεκριμένο λειτουργικό περιβάλλον, που ανταποκρίνεται σε συγκεκριμένο σκοπό

Υπολογιστικό Συγκρότημα

(IT Assembly)
Συλλογή υπολογιστικού υλικού, λογισμικού, τηλεπικοινωνιακού εξοπλισμού ή άλλων υπολογιστικών εξαρτημάτων που χρησιμοποιείται για τη διαχείριση πληροφοριών.

Αγαθά (3/5)

- Η ουσία της έννοιας Υπολογιστικό Συγκρότημα είναι ότι αποτελεί μόνο μία συλλογή από υπολογιστικά και άλλα στοιχεία (πχ. υλικό, λογισμικό, τηλεπικοινωνιακός εξοπλισμός κλπ.) τα οποία, ως σύνολο, είναι από μόνα τους ικανά να επεξεργασθούν Πληροφορίες (ή Δεδομένα) και να παράσχουν ένα επίπεδο λειτουργικότητας

- Η έννοια του Υπολογιστικού Συστήματος περιλαμβάνει, εκτός από τα τεχνικά συστατικά του, το λειτουργικό περιβάλλον και το σκοπό για τον οποίο το Υπολογιστικό Σύστημα υπάρχει. Το λειτουργικό περιβάλλον περιλαμβάνει και τους ανθρώπους που είναι απαραίτητοι για τη λειτουργία των τεχνικών μερών του συστήματος και που θεωρούνται ως Υπολογιστικοί Πόροι. Ο σκοπός του Υπολογιστικού Συστήματος εκφράζεται μέσω του λογισμικού εφαρμογών.

Αγαθά (4/5)

- Η έννοια του Πληροφοριακού Συστήματος περιλαμβάνει όλα τα τεχνικά συστατικά του Υπολογιστικού Συγκροτήματος, το περιβάλλον στο οποίο λειτουργεί το σύστημα, το σκοπό (όλα μαζί συγκροτούν το Υπολογιστικό Σύστημα) και επιπλέον τις Πληροφορίες. Στο βαθμό που οι άνθρωποι είναι υπεύθυνοι για την μεταφορά της Πληροφορίας στο Υπολογιστικό Σύστημα, και συνεπώς εκτελούν λειτουργίες απαραίτητες για την πληρότητα και την ακρίβεια των Πληροφοριών, μπορεί να θεωρηθεί ότι αποτελούν μέρος του ίδιου του Πληροφοριακού Συστήματος.

- Η έννοια των Υπολογιστικών Πόρων περιλαμβάνει κάθε στοιχείο του Υπολογιστικού Συστήματος, εκτός από τις Πληροφορίες ή τα Δεδομένα που διαχειρίζεται. Αντίθετα με το Υπολογιστικό Συγκρότημα, οι Υπολογιστικοί Πόροι δεν είναι απαραίτητο να διαχειρίζονται τις Πληροφορίες από μόνοι τους, με την προϋπόθεση ότι θα μπορούν να το κάνουν με τη συνεργασία άλλων Υπολογιστικών Πόρων. Ενα Υπολογιστικό Συγκρότημα και ένα Υπολογιστικό Σύστημα είναι και τα δύο παραδείγματα Υπολογιστικών Πόρων. Ενα Πληροφοριακό Σύστημα δεν είναι Υπολογιστικός Πόρος.

Αγαθά (5/5)

- **Υπολογιστικός Πόρος** (IT Resource)
  Οτιδήποτε αξιοποιείται από ένα υπολογιστικό σύστημα για να διαχειριστεί πληροφορίες.
- **Εφαρμογή** (Application)
  Πληροφορίες, λογισμικό και διαδικασίες που έχουν σχεδιαστεί για την επίτευξη συγκεκριμένων στόχων.
- **Υπολογιστικό Αντικείμενο** (IT Object)
  Υπολογιστικό συγκρότημα ή υπολογιστικό σύστημα ή πληροφοριακό σύστημα ή υπολογιστικό εξάρτημα ή προϊόν.
- **Αξία** (Value)
  Σπουδαιότητα εκφραζόμενη σε χρηματικούς ή άλλους όρους .
- **Αγαθό** (Asset)
  Πληροφορίες, δεδομένα ή υπολογιστικοί πόροι που έχουν αξία.

Ιδιοκτήτης και Χρήστης

- **Ιδιοκτήτης** (Owner)
  Πρόσωπο που κατέχει ή είναι υπεύθυνο για ένα αγαθό και που έχει το δικαίωμα να καθορίσει πώς μπορεί να χρησιμοποιηθεί, να μεταβληθεί ή να διατεθεί το αγαθό αυτό.
- **Εξουσιοδότηση** (Authorisation)
  Άδεια που παρέχεται από έναν ιδιοκτήτη για κάποιο σκοπό.
- **Εξουσιοδοτημένος** (Unauthorised)
  Με την άδεια του ιδιοκτήτη για κάποιο σκοπό
- **Χρήστης** (User)
  Πρόσωπο ή διεργασία που χρησιμοποιεί ολόκληρο ή μέρος του πληροφοριακού συστήματος

Ιδιότητες (1/5)

- **Υπηρεσία** (Service)
  Σύνολο λειτουργιών που παρέχονται σε ένα χρήστη από ένα υπολογιστικό σύστημα.
- **Προσπέλαση** (Access)
  Η δυνατότητα μιας οντότητας να αξιοποιεί πληροφορίες ή υπολογιστικούς πόρους, στο πλαίσιο ενός πληροφοριακού συστήματος.
- **Προσπέλαση Πληροφορίας** (Information Access)
  Η δυνατότητα κάποιου να χρησιμοποιεί συγκεκριμένες πληροφορίες ενός πληροφοριακού συστήματος.
- **Προσπέλαση Συστήματος** (System Access)
  Η δυνατότητα κάποιου να χρησιμοποιεί υπολογιστικούς πόρους στο πλαίσιο ενός πληροφοριακού συστήματος

Ιδιότητες (2/5)

Συχνά πρέπει να εξουσιοδοτήσουμε ορισμένους χρήστες για κάποια μορφή Προσπέλασης, αλλά - ταυτόχρονα - να αρνηθούμε την εξουσιοδό

	Περιορίζουν	***Επιτρέπουν***	***Ουδέτεροι/Μικτοί***
Πληροφορία	Εμπιστευτικότητα Ακεραιότητα Αυθεντικότητα	Διαθεσιμότητα Πληροφοριών Εγκυρότητα	Προσπέλαση Πληροφοριών Ασφάλεια Ασφάλεια Πληροφοριών
Υπολογιστικοί Πόροι		Διαθεσιμότητα Συστήματος	Προσπέλαση Συστήματος Ασφάλεια Υπολογιστικού Συστήματος
Πληροφοριακό Σύστημα		Διαθεσιμότητα	Προσπέλαση Ασφάλεια Πληροφο- ριακών Συστημάτων

Ιδιότητες (3/5)

- **Ακεραιότητα** (Integrity)
  Αποφυγή μη εξουσιοδοτημένες τροποποίησης μιας πληροφορίας
- **Αυθεντικότητα** (Authenticity)
  Αποφυγή ατελειών και ανακριβειών κατά τη διάρκεια εξουσιοδοτημένων τροποποιήσεων μιας πληροφορίας
- **Εγκυρότητα** (Validity)
  Απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας
- **Εμπιστευτικότητα** (Confidentiality)
  Αποφυγή αποκάλυψης πληροφοριών χωρίς την άδεια του ιδιοκτήτη τους
- **Διαθεσιμότητα Πληροφοριών** (Information Availability)
  Αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας σε εξουσιοδοτημένους χρήστες

Ιδιότητες (4/5)

- **Ασφάλεια** (Security)
  Προστασία της διαθεσιμότητας πληροφοριών, της ακεραιότητας και της εμπιστευτικότητας.
- **Ασφάλεια Πληροφοριών** (Information Security)
  Διασφάλιση εμπιστευτικότητας, εγκυρότητας, αυθεντικότητας, ακεραιότητας και διαθεσιμότητας πληροφοριών

Ιδιότητες (5/5)

- **Διαθεσιμότητα Συστήματος** (System Availability)
  Αποτροπή της μη διάθεσης υπολογιστικών πόρων σε εξουσιοδοτημένους χρήστες.
- **Ασφάλεια Υπολογιστικού Συστήματος** (IT System Security)
  Διασφάλιση διαθεσιμότητας συστήματος και ασφάλειας πληροφοριών, καθώς και των παραμέτρων που αποτελούν τμήμα του υπολογιστικού συστήματος.
- **Ασφάλεια Πληροφοριακού Συστήματος** (Information System Security)
  Ασφάλεια πληροφοριών και υπολογιστικού συστήματος για δεδομένο πληροφοριακό σύστημα.
- **Διαθεσιμότητα** (Availability)
  Αποφυγή καθυστερήσεων στην εξουσιοδοτημένη προσπέλαση πληροφοριών ή υπολογιστικών πόρων.

Ζημιά

Συναφείς με Κίνδυνο	Συναφείς με Στόχο
Ρήγμα Ασφάλειας	Επίπτωση Συνολική Επικινδυνότητα
Παραβίαση	Απομένουσα Συνολική Επικινδυνότητα Απομένουσα Επισφάλεια

Κίνδυνοι (1/2)

- **Ρήγμα Ασφάλειας** (Breach of Security)
  Μη εξουσιοδοτημένη αποκάλυψη, τροποποίηση ή απόκρυψη πληροφοριών
- **Παραβίαση** (Violation)
  Γεγονός κατά το οποίο περιορίστηκαν κάποιες από τις αυθεντικότητα, διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, εγκυρότητα.
- **Απειλή** (Threat)
  Ό,τι μπορεί να περιορίσει την ασφάλεια ενός πληροφοριακού συστήματος
- **Αδυναμία** (Vulnerability)
  Χαρακτηριστικό ενός πληροφοριακού συστήματος που μπορεί να επιτρέψει να συμβεί μία παραβίαση

Κίνδυνοι (2/2)

- **Επισφάλεια** (Hazard)
  Πιθανότητα να συμβεί μία παραβίαση
- **Περιστατικό** (Incident)
  Γεγονός που συνέβη ενδεχομένως εξαιτίας μιας απειλής

Φυσική Απειλή	Ανθρώπινη Απειλή	Τεχνική Απειλή
Τυχαία Απειλή		Σκόπιμη Απειλή
	Ανθρώπινη Αδυναμία	Τεχνική Αδυναμία

Στόχοι

- **Κόστος** (Cost)
  Πόροι που απαιτούνται για την πραγματοποίηση μιας ενέργειας
- **Μέσο Προστασίας** (Safeguard)
  Μέτρο σχεδιασμένο για να εμποδίσει μια παραβίαση είτε να μειώσει τις επιπτώσεις της
- **Επίπτωση** (Impact)
  Απώλεια μίας αξίας ή αύξηση του κόστους ή άλλη ζημία που μπορεί να προκύψει ως συνέπεια μιας παραβίασης
- **Επικινδυνότητα** (Risk)
  Συνδυασμός επίπτωσης με επισφάλεια
- **Συνολική Επικινδυνότητα** (Overall Risk)
  Σύνολο όλων των επικινδυνοτήτων

Εξασφάλιση

- **Εξασφάλιση** (Assurance)
  Εμπιστοσύνη ότι ένα αντικειμενικός σκοπός ή μια απαίτηση επιτυγχάνονται

- **Η ανάλυση αυτή μπορεί να βασίζεται:**
  α) στην απόδειξη ότι οι λειτουργίες που υποστηρίζονται από ένα Υπολογιστικό Αντικείμενο γίνονται με βάση τις προδιαγραφές,
  β) σε δειγματοληπτικό έλεγχο ότι οι λειτουργίες του Υπολογιστικού Αντικειμένου είναι οι αναμενόμενες,
  γ) σε επιθεώρηση της ανάπτυξης και λειτουργίας του Υπολογιστικού Αντικειμένου.

- **Κατά τη διαδικασία Εξασφάλισης υπάρχουν τρία ερωτήματα που πρέπει να απαντηθούν:**
  α) λειτουργούν τα Μέσα Προστασίας σύμφωνα με τις προδιαγραφές;
  β) είναι αποτελεσματικά;
  γ) είναι κατάλληλα;

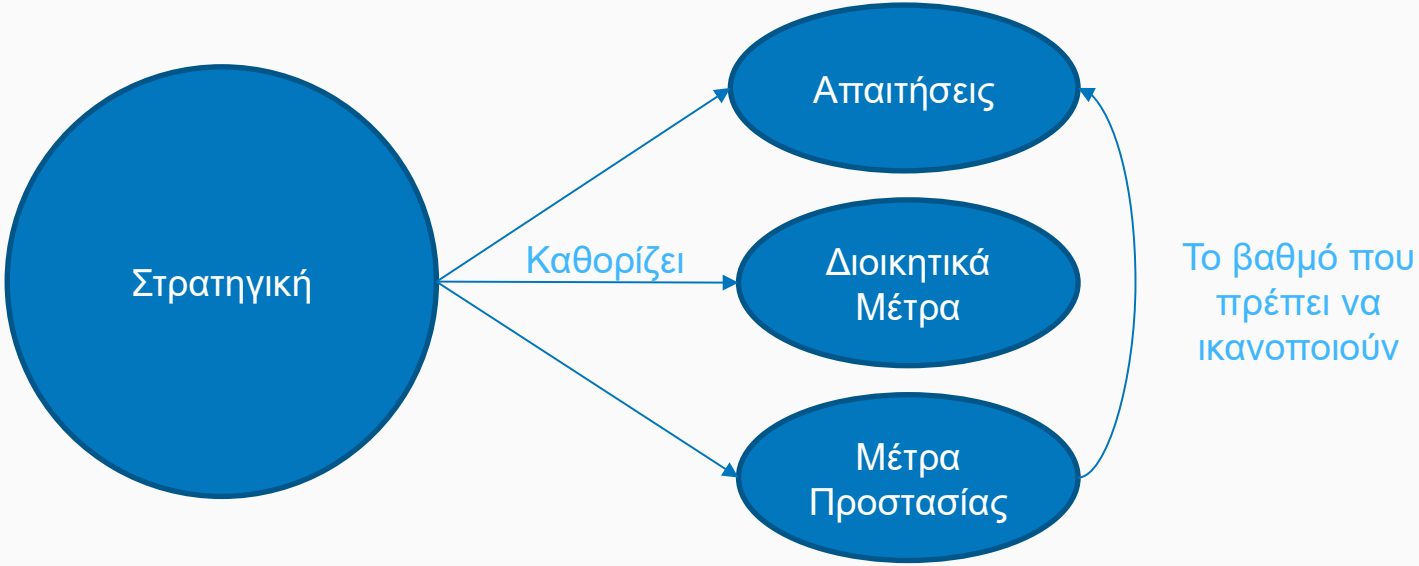
Μέσα Προστασίας

Ένας Ιδιοκτήτης πρέπει να εκπονήσει ένα γενικό σχέδιο ασφάλειας για να πετύχει τους Αντικειμενικούς Σκοπούς του. Από αυτό θα εξαχθούν αναλυτικότερα σχέδια που καθορίζουν τα συγκεκριμένα Μέσα Προστασίας που θα χρησιμοποιηθούν και τον τρόπο που θα υλοποιηθούν.

Το σύνολο των γενικών σχεδίων ονομάζεται Στρατηγική.

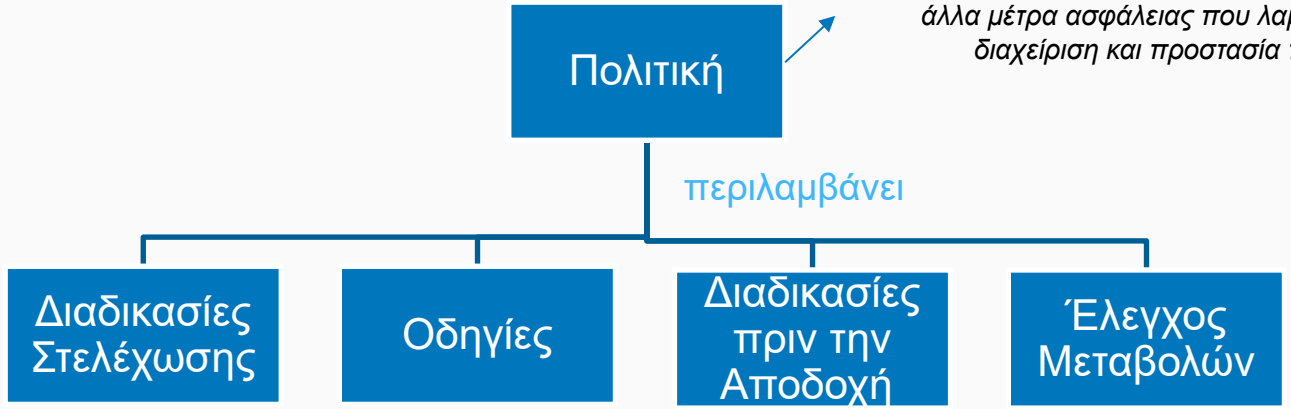
Στρατηγική (Strategy)
Σχέδιο πραγματοποίησης των αντικειμενικών σκοπών κάποιων πληροφοριακών συστημάτων

Μέσα Προστασίας



Διοικητικά Μέτρα

Περιγραφή του συνόλου των κανόνων, μέτρων και διαδικασιών που καθορίζουν τα φυσικά, διαδικαστικά και άλλα μέτρα ασφάλειας που λαμβάνονται κατά τη διαχείριση και προστασία των αγαθών.



Στρατηγική

Η Στρατηγική ορίζει το βαθμό στον οποίο τα Μέσα Προστασίας πρέπει να ικανοποιούν τις Απαιτήσεις, καθώς και το βαθμό στον οποίο η Επισφάλεια θα είναι αποδεκτή ή ποια μέσα μείωσης των Επιπτώσεων της Παραβίασης θα χρησιμοποιηθούν.

Σκοπός των Μέσων Προστασίας

Ο σκοπός των Μέσων Προστασίας είναι να εξασφαλίσουν ότι οι Αντικειμενικοί Σκοποί θα επιτευχθούν.

Υπάρχουν τρεις ταξινομήσεις των συναφών με τα Μέσα Προστασίας όρων, με βάση:

- πότε ένα Μέσο Προστασίας ενεργοποιείται
- τη φύση του Αγαθού και των Ιδιοτήτων που προστατεύει
- τα τεχνικά και άλλα μέσα με τα οποία υλοποιείται

Μέσα Προστασίας

Τα Μέσα Προστασίας μπορούν να δράσουν ως εξής:

- σταματώντας την Απειλή πριν πραγματοποιηθεί ή μειώνοντας την πιθανότητα να πραγματοποιηθεί
- παρέχοντας παθητική αντίσταση στην Απειλή
- προσφέροντας ενεργητική αντίσταση στην Απειλή
- μειώνοντας την ευπάθεια των Πληροφοριών ή των Υπολογιστικών Αντικειμένων
- μειώνοντας την Επίπτωση στον οργανισμό.

Ασφάλεια Υποδομών

Η Ασφάλεια Υποδομών αποτελεί αναπόσπαστο τμήμα της γενικότερης εννοιολογικής προσέγγισης του ζητήματος της Ασφάλειας. Για την παροχή ασφάλειας σε υποδομές τύπου κτιριακής εγκατάστασης χρησιμοποιούνται τρεις κυρίως τεχνολογίες: Συστήματα Περιμετρικής Ασφάλειας (Perimeter Intrusion Detection Systems), Κλειστά Κυκλώματα Τηλεόρασης (Closed Circuit TV) και Συστήματα Ελέγχου Φυσικής Προσπέλασης (Access Control Systems)