Λ.Σ. και Ασφάλεια Πληροφοριακών Συστημάτων

Κεφάλαιο 5

Ασφάλεια Πληροφοριακών Συστημάτων

Διδάσκων: Σπάχος Κυριάκος

Εισαγωγή

Στο κεφάλαιο αυτό θα μάθετε για:

- το **αντικείμενο της Ασφάλειας Πληροφοριακών Συστημάτων** (Information Security System) και σημαντικά ιστορικά στοιχεία της.
- τα είδη των **Χάκερς** (hackers) και το **Ηλεκτρονικό έγκλημα**.
- τις βασικές έννοιες της Ασφάλειας Πληροφοριακών Συστημάτων, όπως την τριάδα **Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα** και την ανάγκη ύπαρξης χρηστών με διαφορετικά δικαιώματα.
- τη Διαχείριση και Αξιολόγησης Κινδύνου καθώς και για το **Σχέδιο Ασφαλείας** με **τις Πολιτικές Ασφαλείας** και τα **Αντίμετρα ασφαλείας.**
- το Σχεδιασμό Επιχειρησιακής Συνέχειας και Επαναφοράς από Καταστροφή, με τη βοήθεια των **Αντιγράφων Ασφαλείας**.
- τα προβλήματα ασφαλείας του λογισμικού και τα διάφορα είδη **κακόβουλου** λογισμικού.
- την **κρυπτογραφία** και τη χρησιμότητά της.
- τα βασικότερα εργαλεία **δικτυακής ασφάλειας**.
- τους σπουδαιότερους τρόπους **φυσικής ασφάλειας**.

Ασφάλεια Μηνυμάτων

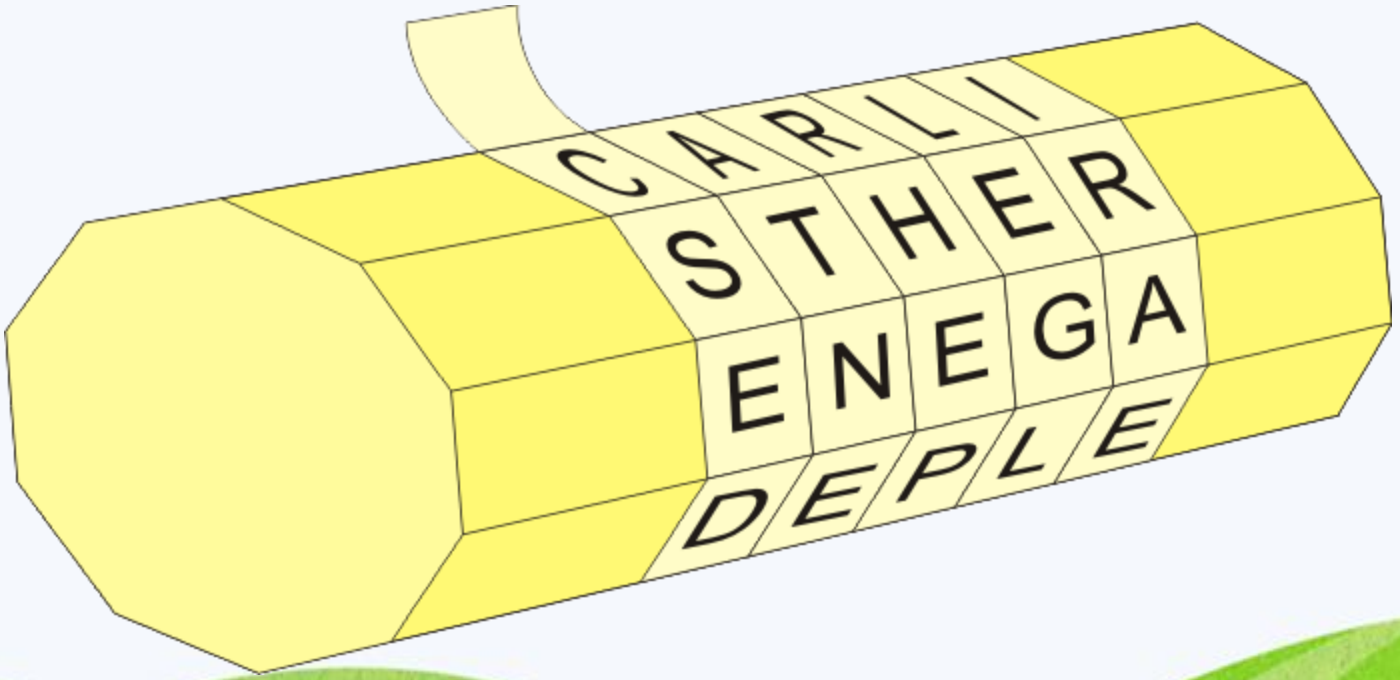
Με την ανάπτυξη του ανθρώπινου πολιτισμού έγινε κατανοητό το πόσο σημαντική είναι η **αποστολή μηνυμάτων με ασφάλεια**, χωρίς να κινδυνεύει δηλαδή να **μαθευτεί** αλλά και να μην **τροποποιηθεί** το περιεχόμενο των μηνυμάτων.

Η ασφαλής αποστολή μηνυμάτων ήταν μια σημαντική παράμετρος που απασχόλησε και συνεχίζει να απασχολεί κάθε κοινωνία

Κρυπτεία σκυτάλη (Σπάρτη)

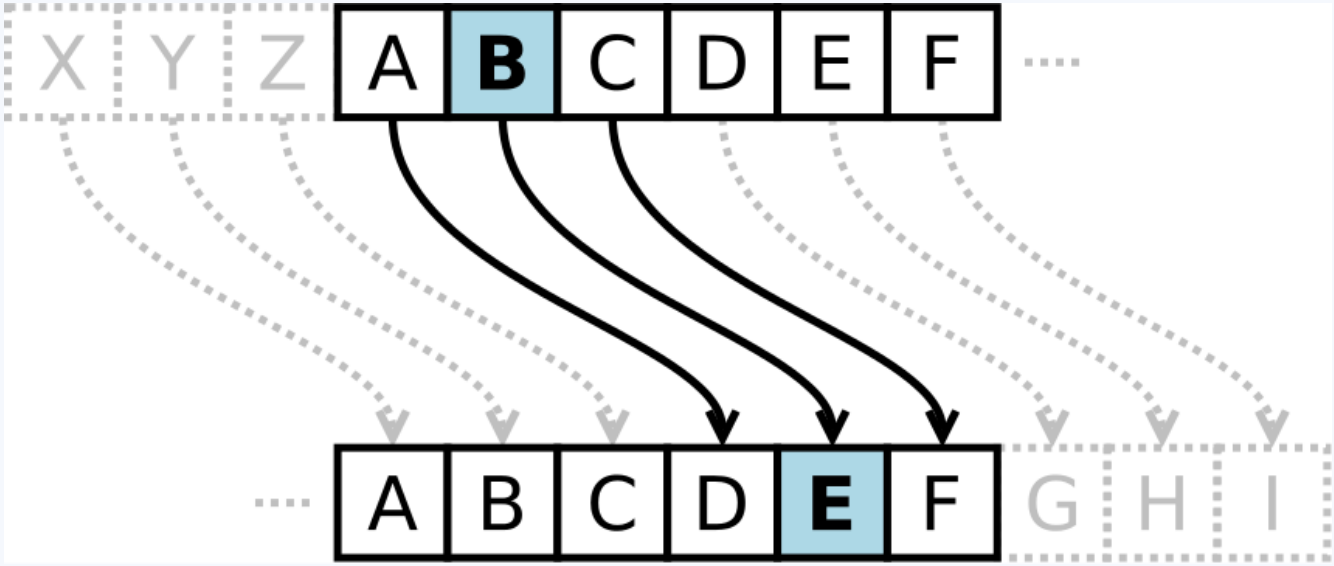
- Μία σκυτάλη **τυχαίων διαστάσεων** κόβονταν **στη μέση**.
- Το ένα τμήμα το φύλαγαν οι έφοροι της Σπάρτης και το άλλο το έπαιρνε μαζί του ο εκάστοτε επικεφαλής του στρατεύματος.
- Όταν ένα από τα δύο μέρη ήθελε να επικοινωνήσει με το άλλο, τύλιγε μια μακρόστενη λουρίδα, από ύφασμα ή περγαμηνή, γύρω από το κομμάτι της σκυτάλης που είχε. **Ο τρόπος που θα το τύλιγε είχε προσυμφωνηθεί.**
- Εκεί επάνω έγραφε το μήνυμα που ήθελε πάλι με κάποιον **προσυμφωνημένο τρόπο.**
- Κατόπιν ξετύλιγε την λουρίδα υφάσματος στην οποία πλέον δεν ήταν δυνατή η άμεση ανάγνωση του μηνύματος.
- Ο παραλήπτης τύλιγε πάλι τη λουρίδα με τον προσυμφωνημένο τρόπο και **αφού η σκυτάλη είχε την ίδια διάμετρο τα γράμματα συνέπιπταν**.
- Μετά χρησιμοποιούσαν τον συμφωνημένο τρόπο ανάγνωσης και αποκρυπτογράφησης του κειμένου.

Κρυπτεία σκυτάλη



Κώδικας Καίσαρα

Ο Κώδικας του Καίσαρα είναι μία από τις απλούστερες και πιο γνωστές τεχνικές κωδικοποίησης στην κρυπτογραφία. Είναι **κώδικας αντικατάστασης** στον οποίο κάθε γράμμα του κειμένου αντικαθίσταται από κάποιο άλλο γράμμα με **σταθερή απόσταση** κάθε φορά στο αλφάβητο. Η μέθοδος πήρε το όνομά της από τον Ιούλιο Καίσαρα, ο οποίος την χρησιμοποιούσε στην προσωπική του αλληλογραφία.



Συσκευή Αίνιγμα (Enigma)

Η βασική αρχή λειτουργίας της Enigma ήταν απλή:

- Πιέζοντας ένα πλήκτρο από το πληκτρολόγιο της μηχανής το ηλεκτρικό σήμα που ξεκινούσε από αυτό το πλήκτρο, περνούσε μέσα από τους 3 ρότορες κατέληγε σε ένα λαμπτήρα, ο οποίος υποδείκνυε ένα **«τυχαίο» γράμμα στον πίνακα λυχνιών**, ακριβώς από πάνω από το πληκτρολόγιο, το οποίο θα αναμεταδίδοταν μέσω ασυρμάτου σε κώδικα Mors, ένα κρυπτογραφημένο μήνυμα
- Αυτό βέβαια προϋποθέτει και οι δύο χειριστές να έχουν τις μηχανές **τους ρυθμισμένες κατά τον ίδιο τρόπο** (ίδια θέση ρότορα).

Το δυνατό χαρακτηριστικό, και παράλληλα αδυναμία της Enigma ήταν ότι αν πατούσαμε π.χ. το «Α», **όσες φορές και να το πατούσαμε στον πίνακα με τους λαμπτήρες δεν θα έβγαινε ποτέ το Α, ανεξαρτήτως ρύθμισης.**

Χρησιμοποιήθηκε αρχικά για εμπορικούς σκοπούς και στη συνέχεια από τη ναζιστική Γερμανία. Αποκρυπτογραφήθηκε με τη βοήθεια του Alan Turing.

Συσκευή Αίνιγμα (Enigma)

«Σκουλήκι» Morris (Morris warm)

Στις 2 Νοεμβρίου του 1988, ο Robert Tappan Morris, μεταπτυχιακός φοιτητής της επιστήμης υπολογιστών του πανεπιστημίου Κορνέλ, εξαπέλυσε ένα σκουλήκι που έγινε γνωστό ως **"σκουλήκι Morris",** διαταράσσοντας ίσως και το 10% των υπολογιστών του Διαδικτύου τότε.

Το 1989 ο Morris ήταν ο πρώτος άνθρωπος που κατηγορήθηκε με βάση νόμο των ΗΠΑ περί Ηλεκτρονικής Απάτης και Κατάχρησης.

Κέβιν Μίτνικ (Kevin Mitnick)

Ο Κέβιν Μίτνικ (Kevin Mitnick) είναι ένας από τους γνωστότερους μέχρι σήμερα χάκερς. Την περίοδο του 1985 -1987 είχε εισβάλει στα συστήματα των μεγαλυτέρων εταιριών της εποχής εκείνης, καθώς επίσης είχε υποκλέψει και στοιχεία εκατοντάδων πιστωτικών καρτών. Καταδικάστηκε το 1987.

Μετά την αποφυλάκισή του συνέχισε να ασχολείται με το χάκινγκ ταξιδεύοντας σε διάφορες πολιτείες της Αμερικής για να αποφύγει πάλι τη σύλληψη.

Τελικά το 1995 συνελήφθη και καταδικάστηκε σε 5 χρόνια φυλάκιση. Όταν αποφυλακίστηκε το 2000 **του απαγόρευσαν της χρήση συσκευών με πληκτρολόγιο για χρόνια**.

Πληροφοριακό σύστημα & Ασφάλεια

Πληροφοριακό σύστημα:

Είναι ένα σύνολο **ανθρώπινου δυναμικού**, **υπολογιστών** και **διαδικασιών**, τα οποία συνεργάζονται αρμονικά για να βοηθήσουν έναν οργανισμό να πετύχει τους στόχους του. (πχ το TAXIsnet του Υπουργείου Οικονομικών)

Ασφάλεια Πληροφοριακών συστημάτων

Η Ασφάλεια Πληροφοριακών Συστημάτων είναι ένας τομέας της επιστήμης της Πληροφορικής, ο οποίος ασχολείται με την **προστασία των δεδομένων ενός Πληροφοριακού Συστήματος από άτομα χωρίς εξουσιοδότηση.**

Άτομο χωρίς εξουσιοδότηση είναι οποιοδήποτε δεν έχει άδεια πρόσβαση σε κάποιο τμήμα του πληροφοριακού συστήματος.

Ηλεκτρονικό έγκλημα

Ηλεκτρονικό Έγκλημα ***είναι οι αξιόποινες εγκληματικές*** **πράξεις** που τελούνται με **την βοήθεια ηλεκτρονικών υπολογιστών** και που τιμωρούνται από τη νομοθεσία.

Ανάλογα με τον τρόπο που πραγματοποιούνται διαχωρίζονται σε εγκλήματα που έγιναν με τη χρήση Ηλεκτρονικών Υπολογιστών **(computer crime)** και σε Κυβερνοεγκλήματα **(cyber crime)**, εάν έγιναν μέσω του Διαδικτύου.
Ηλεκτρονικά Εγκλήματα θεωρούνται τα παρακάτω:

- Τροποποίηση δεδομένων - Κλοπή δεδομένων
- Εισβολή σε δίκτυο - Σαμποτάζ σε δίκτυο
- Μη εξουσιοδοτημένη πρόσβαση
- Διασπορά ιών - Υπόθαλψη αδικημάτων
- Πλαστογραφία - Απάτη

Hacker

Χάκερς (hackers):

άτομα ή ομάδες ατόμων, που έχουν βαθιές γνώσεις Λ.Σ. και γλωσσών προγραμματισμού, και οι οποίοι **είναι εξαιρετικά μεγάλη απειλή για δικτυωμένα συστήματα** γιατί εισβάλουν μέσω του διαδικτύου.

Ανάλογα με τις ηθικές τους αρχές χωρίζονται στις εξής κατηγορίες:

- Οι **Black hats hackers** πολλές φορές λέγονται και **Crackers** και συνήθως εισβάλουν σε συστήματα με σκοπό να κλέψουν, να καταστρέψουν δεδομένα, δημιουργούν κακόβουλο λογισμικό, σπάνε προγράμματα, υποκλέπτουν κωδικούς κ.λπ.
- Οι **White hats hackers** ψάχνουν για «κενά»ασφαλείας σε ΛΣ και εφαρμογές και τους λόγους υπάρξεώς τους. Δεν έχουν σκοπό την καταστροφή δεδομένων και συνήθως ενημερώνουν τους υπεύθυνους για τα κενά ασφαλείας.
- Οι **Gray hats hackers**. Είναι άτομα που χρησιμοποιούν τους υπολογιστές για να τιμωρήσουν υποτιθέμενους εγκληματίες του Κυβερνοχώρου. Ονομάζονται και χακτιβιστές (hacktivists) όταν μεταφέρουν πολιτικά μηνύματα μέσω διαδικτύου.

Social Engineering

Κοινωνική Μηχανική (social engineering).

Προσπάθεια **εξαπάτησης διαφόρων ατόμων**, με σκοπό την απόσπαση **εμπιστευτικών πληροφοριών**. Οι πληροφορίες αυτές μπορεί να είναι προσωπικές, αλλά ενδέχεται να αφορούν και τον χώρο εργασίας. Ονόματα, ημερομηνίες γεννήσεως, κωδικοί, αριθμοί τηλεφώνων, ταχυδρομικές διευθύνσεις, ηλεκτρονικές διευθύνσεις (πολλές φορές οι χρήστες δίνουν τέτοια στοιχεία μέσω ιστοσελίδων Κοινωνικής Δικτύωσης) και τραπεζικά στοιχεία είναι κάποιες από τις πληροφορίες που ίσως είναι στόχος των ενδιαφερομένων.

Η γνωστότερη τεχνική που χρησιμοποιούν για την απόσπαση πληροφοριών είναι το **ηλεκτρονικό ψάρεμα (phishing),** *όπου συνήθως χρησιμοποιούνται* **πλαστά ηλεκτρονικά μηνύματα (πχ. από τράπεζες) και σύνδεσμοι προς πλαστές ιστοσελίδες** και ζητούν την καταχώρηση των πληροφοριών που τους ενδιαφέρουν.

Απειλές κατά των δεδομένων

Απειλή

λέγεται καθετί που μπορεί να συμβεί από εσωτερικό ή εξωτερικό παράγοντα και να προκαλέσει πρόβλημα σ' έναν οργανισμό.

Απειλές κατά των δεδομένων

- Διαρροή πληροφοριών,
- τροποποίηση δεδομένων
- αναστολή λειτουργίας κάποιου υπολογιστικού συστήματος, όπως ένας διακομιστής ιστοσελίδων.

Εάν συμβεί κάτι από αυτά τότε ανάλογα με το είδος των πληροφοριών (π.χ. ιατρικές εξετάσεις, σχέδια ενός μηχανήματος κ.λπ.), μπορεί να προκληθούν **προβλήματα οικονομικά και κοινωνικά** σε ιδιώτες και επιχειρήσεις.

Βασικές αρχές ασφάλειας

1. **Εμπιστευτικότητα (confidentiality)**
   Στόχος της είναι η εξασφάλιση πως τα δεδομένα **δε θα γίνουν διαθέσιμα**, δε θα μπορούν να τα διαβάσουν δηλαδή, μη **εξουσιοδοτημένα** άτομα.

2. **Ακεραιότητα (integrity)**
   Η αρχή της Ακεραιότητας εξασφαλίζει πως τα δεδομένα δε θα υποστούν **καμία αλλοίωση από μη εξουσιοδοτημένα άτομα** ή **με μη ανιχνεύσιμο τρόπο**.

3. **Διαθεσιμότητα (Availability)**
   Αυτή εξασφαλίζει πως το σύστημα **θα μπορεί να παρέχει τις πληροφορίες** του, όταν του ζητηθούν και **μέσα σε αποδεκτά χρονικά όρια**.

Έλεγχος πρόσβασης (access control)

Ο έλεγχος πρόσβασης εφαρμόζεται σε τρεις περιπτώσεις:

1. **Δικτυακή πρόσβαση:**
   οι χρήστες έχουν την δυνατότητα **πρόσβασης σ' όλους τους πόρους του δικτύου**. Για το λόγο αυτό θα πρέπει στους πόρους του δικτύου να μπουν περιορισμοί, να προστατευτούν και να παρακολουθούνται.
2. **Πρόσβαση σε συστήματα:**
   οι χρήστες **χρησιμοποιούν** διάφορα συστήματα του δικτύου όπως servers, printers αλλά και **κάθε άλλο είδος διαμοιραζόμενης συσκευής** στο δίκτυο. Η πρόσβαση σ' αυτές τις συσκευές θα πρέπει να περιορίζεται, να προστατεύεται και να παρακολουθείται.
3. **Πρόσβαση στα δεδομένα:**
   οι χρήστες έχουν πρόσβαση στα δεδομένα του δικτύου. Διαβάζουν και τροποποιούν αρχεία και Βάσεις Δεδομένων (Databases). Τα δεδομένα θα πρέπει να υπόκεινται σε περιορισμούς, προστασία και παρακολούθηση.

Διαχείρισης Ασφαλείας Π.Σ.

Σκοπός:

Προστασία των Π.Σ. περιορίζοντας τον κίνδυνο παραβίασης μιας εκ των βασικών αρχών ασφαλείας. Οι διαδικασίες που περιλαμβάνει είναι:

1. **Διαχείριση κινδύνου:**
   Προσδιορισμός του αποδεκτού επιπέδου ασφαλείας και του κόστους που αυτό συνεπάγεται.

2. **Σχέδιο ασφαλείας:**
   Ανάπτυξη και εφαρμογή ενός σχεδίου με στόχο την επίτευξη του επιπέδου ασφαλείας.

3. **Επαναφορά μετά από καταστροφή:**
   Διαδικασίες επαναφοράς Π.Σ. μετά από Καταστροφή και η Επιχειρησιακή συνέχεια

Διαχείριση Κινδύνου (Risk Management)

- Προσδιορισμός των **πιθανών ζημιών** που μπορεί να προκαλέσει μια καταστροφή, σε σχέση με το **κόστος των προληπτικών μέτρων** για την αντιμετώπισή του.

- Συνυπολογισμός της **πιθανότητας πραγματοποίησης** μιας απειλής και τις **επιπτώσεις** που θα έχει στην ομαλή λειτουργία του οργανισμού καθώς και το **οικονομικό κόστο**ς από την πραγματοποίηση της απειλής.

Σχέδιο Ασφαλείας (Security Plan)

Πολιτική Ασφάλειας:

Έγγραφο στο οποίο περιγράφονται οι **στόχοι της ασφάλειας**, η **προστασία** του Π.Σ. και οι **διαδικασίες** που πρέπει να ακολουθούνται από όλους για να επιτευχθούν οι στόχοι.

Αντίμετρα ή Μέτρα ασφαλείας ή Έλεγχοι:

Πρόκειται για τα **μέτρα** που πρέπει να λάβουμε προκειμένου να επιτύχουμε το επίπεδο ασφάλειας που επιθυμούμε.

- **Διοικητικά μέτρα:** Ρόλοι κι αρμοδιότητες, εσωτερικοί κανόνες λειτουργίας, πρόσληψη και αποχώρηση υπαλλήλου, εκπαίδευση χρηστών κτλ.
- **Τεχνικά μέτρα:** έλεγχος πρόσβασης, log files, backup, συντήρηση λογισμικού, UPS, έλεγχος σωστής λειτουργίας του λογισμικού ασφαλείας, κτλ.
- **Μέτρα φυσικής ασφάλειας:** Ασφάλεια πρόσβασης στις κτιριακές εγκαταστάσεις ή σε συγκεκριμένους χώρους (π.χ server, αποθήκευση backup αρχείων κτλ).

Επαναφορά από καταστροφή

Σχέδιο αντιμετώπισης μιας καταστροφής (ανθρώπινη ενέργεια ή φυσικό φαινόμενο), με στόχο την **άμεση και ορθή λειτουργία** του οργανισμού. Το σχέδιο αυτό θα πρέπει να απαντά σε όλες τις πιθανές περιπτώσεις καταστροφής, να εξηγεί δηλαδή τι θα συμβεί σε περίπτωση:

- καταστροφής ενός σκληρού δίσκου.
- καταστροφής του server της εταιρείας
- υποκλοπής ευαίσθητων δεδομένων
- Αλλοίωσης δεδομένων
- Διακοπής της επικοινωνίας

Αντίγραφα ασφαλείας

Ανάλογα με την **κρισιμότητα των δεδομένων** μια εταιρεία μπορεί να καταφύγει σε πολύ ακριβές λύσεις για την αποθήκευση των αντιγράφων ασφαλείας (π.χ. Τράπεζα: server mirroring, συστοιχίες δίσκων κτλ).

Στις απλούστερες περιπτώσεις κάθε οργανισμός θα πρέπει να κρατά ένα είδος αντιγράφων ασφαλείας ακόμα κα σε μέσα μικρής ταχύτητας. (π.χ. μαγνητικές ταινίες)

Αντίγραφα ασφαλείας

Ένα τυπικό αντίγραφο ασφαλείας μπορεί να περιλαμβάνει:

1. **Πλήρες (full backup)** εβδομαδιαίο αντίγραφο ασφαλείας σε μαγνητικές ταινίες. Κάθε ταινία επανεγγράφεται την αντίστοιχη εβδομάδα του επόμενου μήνα.

2. Μηνιαίο ή ετήσιο (αποθήκευση για πολλά χρόνια)

3. Και πρόσθετα **καθημερινό** διαφορικό ή αυξητικό αντίγραφο ασφαλείας (**όχι και τα δύο**)
   - **Αυξητικό** αντίγραφο ασφαλείας: Παίρνει αντίγραφο μόνο στα αρχεία που μεταβλήθηκαν εκείνη την ημέρα. (Ένα μέσο αποθήκευσης ανά ημέρα)
   - **Διαφορικό** αντίγραφο ασφαλείας: Παίρνει κάθε μέρα αντίγραφο όλων των αρχείων που μεταβλήθηκαν από το προηγούμενο πλήρες αντίγραφο (Ένα μέσο αποθήκευσης ανά εβδομάδα)

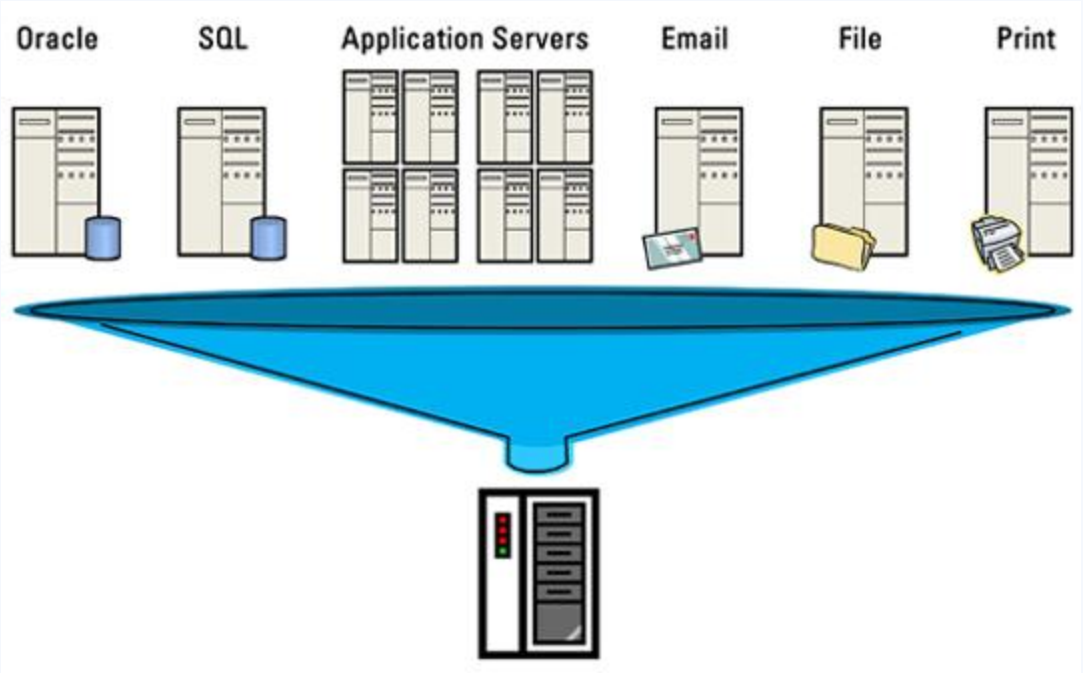
Αντίγραφα ασφαλείας – Διατήρηση

Τα αντίγραφα ασφαλείας θα πρέπει:

1. Να **κρυπτογραφούνται** αν χρειάζεται
2. Να **μην χαθεί ποτέ** κανένα
3. Να **προστατεύονται** από φωτιά, νερό κτλ.
4. Να **βρίσκονται σε διαφορετική τοποθεσία** από αυτή του οργανισμού. Η επιλογή της τοποθεσίας πρέπει να λαμβάνει υπόψη τα παρακάτω:
   - Η περιοχή να βρίσκεται σε ασφαλή απόσταση από αυτήν του οργανισμού.
   - Να υπάρχει εύκολη πρόσβαση στην περιοχή προκειμένου να ανακτηθούν γρήγορα.
   - Την ασφάλεια του χώρου
   - Το κόστος

Αντίγραφα ασφαλείας – Τάσεις

Εικονικοποιημένοι Διακομιστές (Server Virtualization)

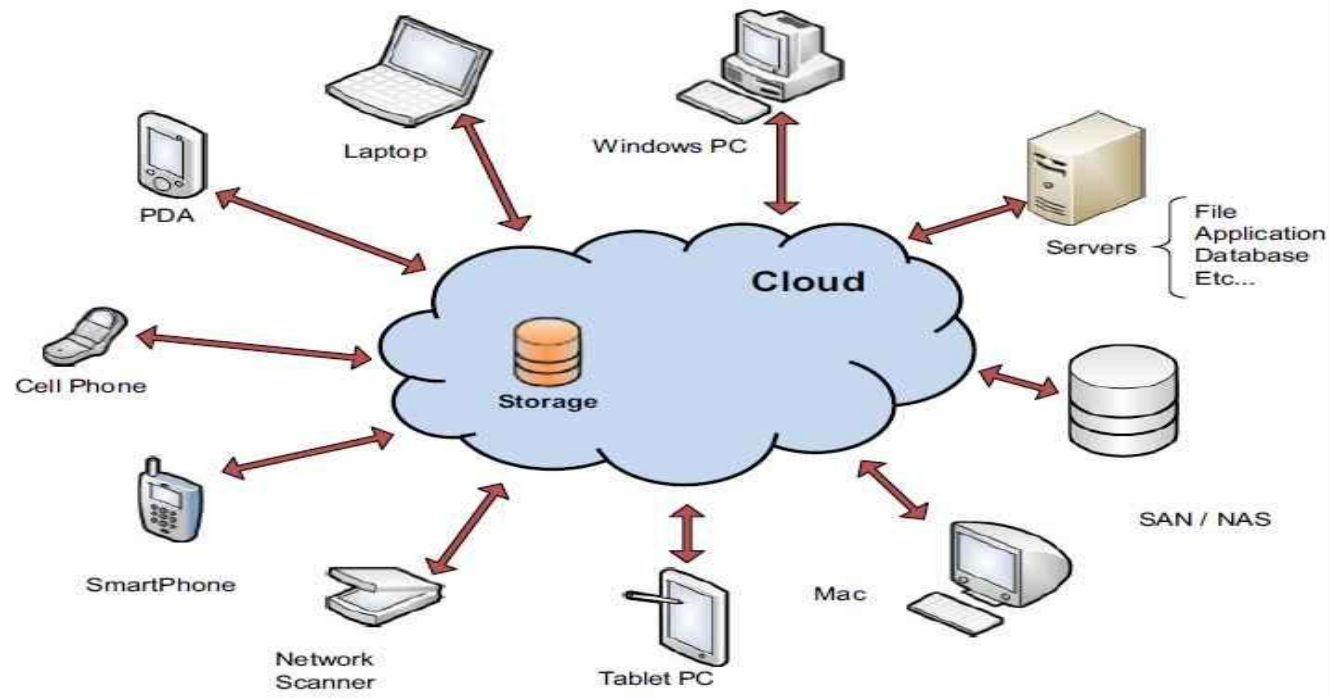


Πλεονεκτήματα:

- Εύκολη μεταφορά των δεδομένων
- Μειώνεται η ανάγκη σε υλικό και χώρο αποθήκευσης
- Συνέχιση της λειτουργίας σχεδόν άμεσα μετά από πρόβλημα στο hardware.

Αντίγραφα ασφαλείας – Τάσεις

Αποθήκευση στο νέφος (Cloud Storage)



Πλεονεκτήματα:

- Μεγάλος αποθηκευτικός χώρος με μικρό κόστος
- Αυτοματοποιημένη διαδικασία αντιγράφων ασφαλείας.
- Δεν απαιτείται ιδιαίτερος χώρος αποθήκευσης των αντιγράφων ασφαλείας.