Λ.Σ. και Ασφάλεια Πληροφοριακών Συστημάτων

Κεφάλαιο 5

Ασφάλεια Πληροφοριακών Συστημάτων

Κωνσταντάτου Φωτεινή

fkonstanta@sch.gr

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.

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 αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή.**

Άτομο χωρίς εξουσιοδότηση είναι οποιοδήποτε δεν έχει άδεια πρόσβασης 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

Χάκερς (Hacker)

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.

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

Βασικές αρχές ασφάλειας Πληροφοριακών Συστημάτων - CIA triad

- **Εμπιστευτικότητα (confidentiality)**

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

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

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

Δραστηριότητα 5

- Ένα μικροβιολογικό εργαστήριο καταχωρίζει τα ιατρικά δεδομένα των πελατών – ασθενών σε ένα πληροφοριακό σύστημα που βρίσκεται εγκατεστημένο σε έναν υπολογιστή. Ο υπολογιστής αυτός βρίσκεται σε κοινόχρηστο χώρο, δεν προστατεύεται από κωδικό και είναι μόνιμα συνδεδεμένος με το Διαδίκτυο.
- Εξηγήστε με συντομία τους λόγους για τους οποίους το παραπάνω πληροφοριακό σύστημα δεν ικανοποιεί τουλάχιστον δύο από τις βασικές αρχές ασφάλειας πληροφοριακών συστημάτων (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα).

ΑΠΑΝΤΗΣΗ

- Παραβιάζεται η αρχή της Εμπιστευτικότητας δεδομένου ότι μη εξουσιοδοτημένα άτομα μπορούν να αποκτήσουν πρόσβαση στα ιατρικά δεδομένα: α) μέσω φυσικής πρόσβασης, αφού δεν υπάρχει κωδικός στον υπολογιστή και αυτός βρίσκεται σε κοινόχρηστο χώρο και β) μέσω του Διαδικτύου, σε περίπτωση κακόβουλης εισβολής χάκερ.
- Για τους ίδιους λόγους παραβιάζεται η αρχή της Ακεραιότητας διότι τα μη εξουσιοδοτημένα άτομα μπορούν να αλλοιώσουν τα δεδομένα

Βασικές Έννοιες

- **Απειλή** λέγεται καθετί που μπορεί να συμβεί από εσωτερικό ή εξωτερικό παράγοντα, από ανθρώπινο παράγοντα (πχ. λάθος χειρισμός), και να προκαλέσει πρόβλημα σ' έναν οργανισμό και να παρακάμψει κάποια από τις τρεις Βασικές Αρχές
- **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

Ορισμοί

- **Κίνδυνος:** είναι η πιθανότητα μια απειλή να γίνει πραγματικότητα.
- **Αντίμετρα (Countermeasures) ή Μέτρα Ασφαλείας (Security Measures) ή Μέτρα Προστασίας (Controls):** είναι το μέτρα που λαμβάνονται για την αντιμετώπιση μιας απειλής σε ένα Πληροφοριακό Σύστημα.
- **Ευπάθεια (Vulnerability):** είναι οι αδυναμίες που μπορεί να υπάρξουν σ’ ένα Πληροφοριακό Σύστημα και επιτρέπουν να γίνει κάποια Απειλή πραγματικότητα. Τέτοιες αδυναμίες μπορεί να υπάρξουν για παράδειγμα: στις ρυθμίσεις παραμέτρων του δικτύου, σε εγκατεστημένα προγράμματα, στον τρόπο που λειτουργεί ο οργανισμός κ.λπ.

Παραδείγματα απειλών

- φυσικές καταστροφές π.χ. πλημμύρα
- βλάβες υλικού
- ιός – κακόβουλο λογισμικό από χάκερς
- Λάθος ή εσκεμμένος χειρισμός χρηστών

Απειλή Vs Ευπάθεια

- Απειλή: να τεθεί ένας Εξυπηρετητής (Server) μη διαθέσιμος.
- Ευπάθεια: μικρό εύρος γραμμής (bandwidth) και λήψη πάρα πολλών αιτήσεων για την εμφάνιση της ιστοσελίδας του οργανισμού.

- Απειλή: να επιτραπεί σε όλους η λήψη ενός ηλεκτρονικού βιβλίου που πουλάει ο οργανισμός μέσω της ιστοσελίδας του.
- Ευπάθεια: λανθασμένες ρυθμίσεις στον Εξυπηρετητή Ιστοσελίδων επιτρέπουν τη λήψη του από όλους (Public Access)

Δραστηριότητα 6

Παραδείγματα απειλών

1. Η διαρροή πληροφοριών, τροποποίηση δεδομένων από κάποιον χάκερ που μπορεί να εισχωρήσει σε ένα πληροφοριακό σύστημα για να υποκλέψει στοιχεία. (Βιβλίο μαθητή σελ.66)

2. Η αναστολή λειτουργίας κάποιου υπολογιστικού συστήματος, όπως για παράδειγμα μπορεί να συμβεί σε έναν ιστότοπο μετά από σκόπιμη επίθεση με αποστολή υπερβολικά μεγάλου αριθμού ψεύτικων αιτήσεων για εξυπηρέτηση. (Βιβλίο μαθητή σελ.66) [1]

Παραδείγματα *ευπάθειας*:

1. Οι λανθασμένες ρυθμίσεις σε κάποιον Εξυπηρετητή Ιστοσελίδων μπορεί να επιτρέψουν την λήψη κάποιων αρχείων του από όλους όσους έχουν πρόσβαση στην διαδικτυακή του διεύθυνση χωρίς να είναι εξουσιοδοτημένοι για αυτό. (Βιβλίο μαθητή σελ.66) 2. Το μικρό εύρος ζώνης (bandwidth) σε μια γραμμή μπορεί να είναι ένα θέμα ευπάθειας που θα προκαλέσει πρόβλημα σε κάποιον εξυπερετητή εφόσον δεχθεί πάρα πολλές αιτήσεις για την εμφάνιση της ιστοσελίδας του.

Παραδείγματα μέτρων ασφαλείας που μας προσφέρει ένα λειτουργικό σύστημα;

- backup μπορούμε με κάποιο πρόγραμμα να ορίζουμε κάθε πότε να λαμβάνεται αντίγραφο ασφαλείας κάποιων αρχείων που θα ορίσουμε
- κωδικός σύνδεσης με όνομα χρήστη που μας ζητάει για να μπούμε στον υπολογιστή στο εργαστήριο ή στο μειλ μας ή στο web banking που θέλει και συχνή αλλαγή…
- ο έλεγχος πρόσβασης στο σύστημα αρχείων, οι μαθητές ΔΕΝ μπορείτε να διαγράψετε κάποια αρχεία στους υπολογιστές ζητάει κωδικό διαχειριστή, ο admin μπορεί να μας δώσειδικαιώματα και να μας αφαιρέσει.

Δραστηριότητα 8

Το ηλεκτρονικό κατάστημα «The Almond Tree» πραγματοποίησε μεγάλη διαφημιστική καμπάνια για την προώθηση των προϊόντων του, ενώ ταυτόχρονα κάνει προσφορές έως 90% σε όσους αγοράσουν προϊόντα μέσα στο Σαββατοκύριακο. Όσοι όμως προσπάθησαν να επισκεφτούν τον δικτυακό τόπο του καταστήματος εκείνες τις μέρες, διαπίστωσαν ότι αυτός έχει τεθεί εκτός λειτουργίας και δεν κατάφεραν να κάνουν αγορές. Αιτία ήταν το μικρό εύρος γραμμής (bandwidth) του εξυπηρετητή και η λήψη πάρα πολλών αιτήσεων προβολής του ηλεκτρονικού καταστήματος.

1. Ποια ευπάθεια στο πληροφοριακό σύστημα επέτρεψε να συμβεί το παραπάνω περιστατικό;

2. Ποια μέτρα πρόληψης έπρεπε να τηρούνται για την αποφυγή του παραπάνω περιστατικού;

3. Ποια από τις βασικές αρχές ασφάλειας πληροφοριακών συστημάτων καταστρατηγείται στο παραπάνω περιστατικό;

ΑΠΑΝΤΗΣΕΙΣ 1

1. Η ευπάθεια αφορά το **μικρό εύρος γραμμής (bandwidth) του εξυπηρετητή** και την λήψη πάρα πολλών αιτήσεων προβολής (**αύξηση επισκεψιμότητας**) στο ηλεκτρονικό κατάστημα.
2. Έπρεπε να είχε **προβλεφθεί** η αύξηση των επισκέψεων στο ηλεκτρονικό κατάστημα (με δεδομένη την διαφημιστική καμπάνια) ώστε να γίνουν **ενέργειες για την αύξηση του εύρους γραμμής (bandwidth)**.
3. Καταστρατηγείται η **Αρχή της Διαθεσιμότητας**, αφού το ηλεκτρονικό κατάστημα (ως πληροφοριακό σύστημα) τέθηκε εκτός λειτουργίας και δεν εξυπηρετεί τα αιτήματα των χρηστών.

Δραστηριότητα 9

Ο κύριος Νομικός, δικηγόρος στο επάγγελμα, διατηρεί τα επαγγελματικά του έγγραφα στον σταθερό υπολογιστή του γραφείου του αλλά και στον φορητό υπολογιστή του. Σήμερα το πρωί διαπιστώνει πως έχει κλαπεί ο φορητός υπολογιστής του, τον οποίο είχε αφήσει μέσα στο αυτοκίνητό του. Ο κύριος Νομικός ανησυχεί ιδιαίτερα για τα προσωπικά δεδομένα των πελατών του που μπορεί να διαρρεύσουν, καθώς η είσοδος στον υπολογιστή γίνεται χωρίς κωδικό πρόσβασης.

1.Ποιες ευπάθειες στο πληροφοριακό σύστημα επέτρεψαν να συμβεί το παραπάνω περιστατικό;

2. Ποια μέτρα πρόληψης έπρεπε να τηρούνται για την αποφυγή του παραπάνω περιστατικού;

3. Ποια από τις βασικές αρχές ασφάλειας πληροφοριακών συστημάτων καταστρατηγείται στο παραπάνω περιστατικό;

ΑΠΑΝΤΗΣΕΙΣ 2

Οι ευπάθειες που παρουσιάζονται είναι:

α) η **πλημμελής φύλαξη** του φορητού υπολογιστή που αφέθηκε μέσα στο αυτοκίνητο και

β) η **έλλειψη στοιχείων ταυτοποίησης εισόδου (όνομα χρήστη και κωδικός)** για την είσοδο στον υπολογιστή.

Τα κυριότερα μέτρα πρόληψης για την αποφυγή του περιστατικού είναι:

α) ορισμός **κανόνων και διαδικασιών** για την μετακίνηση φορητών συσκευών που περιέχουν σημαντικά δεδομένα τα οποία δεν πρέπει να διαρρεύσουν,

β) ορισμός **στοιχείων ταυτοποίησης εισόδου** (όνομα χρήστη και κωδικός) για τον έλεγχο της πρόσβασης στον υπολογιστή.

Καταστρατηγείται η **Αρχή της Εμπιστευτι**κότητας, αφού τα δεδομένα μπορεί να γίνουν διαθέσιμα σε μη εξουσιοδοτημένα άτομα.

Δραστηριότητα 10

Η κυρία Νομικού, δικηγόρος στο επάγγελμα, διατηρεί όλα τα επαγγελματικά της έγγραφα σε πληροφοριακό σύστημα στον υπολογιστή του γραφείου της. Μία μέρα έλαβε ένα email από άγνωστο αποστολέα. Το μήνυμα έγραφε: «Δες το συνημμένο. Να τα πούμε! Φιλιά!!!». Προσπαθεί να ανοίξει το συνημμένο αρχείο αλλά δεν βλέπει κάτι. Αργότερα όμως διαπιστώνει πως επρόκειτο για κακόβουλο λογισμικό και πως όλα τα αρχεία της έχουν διαγραφεί!

1. Ποια ευπάθεια στο πληροφοριακό σύστημα επέτρεψε να συμβεί η διαγραφή των αρχείων;

2. Ποια μέτρα πρόληψης έπρεπε να είχαν ληφθεί για την αποφυγή του παραπάνω περιστατικού;

3. Με ποιο μέτρο πρόληψης αντιμετωπίζονται οι συνέπειες του παραπάνω περιστατικού;

4. Ποια από τις βασικές αρχές ασφάλειας πληροφοριακών συστημάτων καταστρατηγείται στο παραπάνω περιστατικό;

ΑΠΑΝΤΗΣΕΙΣ 3

1. Η κυριότερη ευπάθεια αφορά την **αποτυχία του συστήματος να ανιχνεύσει την ύπαρξη του κακόβουλου λογισμικού**. Αυτό μπορεί να οφείλεται στο ότι δεν υπάρχει εγκατεστημένο λογισμικό προστασίας από τους ιούς ή ότι αυτό δεν είναι σωστά ενημερωμένο.

Δεύτερη ευπάθεια αφορά τον ίδιο τον **χρήστη** που δεν αντιλαμβάνεται τον κίνδυνο από το άνοιγμα συνημμένων αρχείων από άγνωστο αποστολέα.

2. Τα κυριότερα μέτρα πρόληψης για την αποφυγή του περιστατικού είναι:

α) **εγκατάσταση λογισμικού προστασίας** από τους ιούς και ενημέρωσή του ανά τακτά χρονικά διαστήματα ή αυτόματα,

β) ορισμός **κανόνων και διαδικασιών για την λήψη μηνυμάτων ηλεκτρονικού** ταχυδρομείου (email) με συνημμένα, καθώς και για την εκτέλεση προγραμμάτων από τους χρήστες.

3. Το κυριότερο μέτρο που πρέπει να ληφθεί προληπτικά στο πλαίσιο του σχεδιασμού επαναφοράς είναι η **συστηματική λήψη αντιγράφων ασφαλείας (backup) όλων των αρχείων / δεδομένων**.

4. Καταστρατηγείται η **Αρχή της Διαθεσιμότητας**, αφού τα αρχεία έχουν διαγραφεί και το σύστημα δεν μπορεί να παρέχει τις πληροφορίες που του ζητούνται.

2ο μάθημα

Διαχείριση Ασφαλείας Πληροφοριακού Συστήματος

ΑΠΑΝΤΗΣΕΙΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑ 1

Α. ΚΑΤΑΣΤΑΣΗ	
Α1. Ύπαρξη μη ασφαλούς συνθηματικού (password)	ΕΥΠΑΘΕΙΑ
Α2. Καταστροφή από φυσικά φαινόμενα	*κενό*
Α3. Η πρόσβαση στο δίκτυο δεν περιορίζεται	ΕΥΠΑΘΕΙΑ
Α4. Τακτική λήψη αντιγράφων ασφαλείας	ΑΝΤΙΜΕΤΡΟ
Α5. Εγκατάσταση λογισμικού antivirus	ΑΝΤΙΜΕΤΡΟ
Α6. Μη εγκατάσταση ενημερώσεων λειτουργικού συστήματος	ΕΥΠΑΘΕΙΑ
Α7. Σωστή ρύθμιση συστήματος ανίχνευσης εισβολής	ΑΝΤΙΜΕΤΡΟ
Α8. Επιθέσεις κοινωνικής μηχανικής	*κενό*

Θέμα 18021

Ένα μικροβιολογικό εργαστήριο καταχωρίζει τα ιατρικά δεδομένα των πελατών – ασθενών σε ένα πληροφοριακό σύστημα εγκατεστημένο σε έναν υπολογιστή. Ο υπολογιστής αυτός δεν προστατεύεται από κωδικό πρόσβασης και βρίσκεται σε χώρο προσβάσιμο από όλους τους εργαζομένους του εργαστηρίου.

1. Να αναφέρετε δυο ευπάθειες που υπάρχουν στο παραπάνω πληροφοριακό σύστημα.
2. Ποιοι κίνδυνοι μπορεί να προκύψουν ως αποτέλεσμα των ευπαθειών που αναφέρατε; Μονάδες
3. Ποια μέτρα ασφάλειας προτείνετε για την αντιμετώπιση των ευπαθειών που αναφέρατε;

Απάντηση

- Οι ευπάθειες που αναφέρονται είναι: α) ο υπολογιστής δεν προστατεύεται από κωδικό πρόσβασης και β) ο υπολογιστής βρίσκεται σε χώρο προσβάσιμο από όλους τους εργαζομένους του εργαστηρίου.
- Οι κίνδυνοι που μπορεί να προκύψουν είναι: α) η πρόσβαση στα ιατρικά δεδομένα από μη εξουσιοδοτημένα άτομα και η διαρροή των δεδομένων αυτών και β) η αλλοίωση των ιατρικών δεδομένων από κακόβουλους μη εξουσιοδοτημένους χρήστες.
- Τα μέτρα ασφάλειας που πρέπει να ληφθούν αφορούν: α) την μετακίνηση του υπολογιστή σε χώρο με ελεγχόμενη πρόσβαση ώστε να μην επιτρέπεται η φυσική παρουσία μη εξουσιοδοτημένων ατόμων, β) την ταυτοποίηση των χρηστών του πληροφοριακού συστήματος, π.χ. με χρήση Ονόματος Χρήστη και Κωδικού γ) την απόδοση συγκεκριμένων ρόλων και αρμοδιοτήτων σε κάθε χρήστη.

Διαχείριση Ασφαλείας Πληροφοριακού Συστήματος

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)

Η Διαχείριση Κινδύνου ή Επικινδυνότητας είναι μια διαδικασία αναγνώρισης (ανεύρεσης):

a) **Ευπαθειών (vulnerabilities)** και **Απειλών (threats)** στις οποίες μπορούν εκτεθούν οι πληροφορίες που χρησιμοποιεί και παρέχει ένα Πληροφοριακό Σύστημα, καθώς και

b) των **Αντιμέτρων (Countermeasures)** ή **Μέτρων Ασφαλείας (Security Measures) ή Μέτρων Προστασίας (Controls)** που θα παρθούν για να μειωθεί ο κίνδυνος αλλοίωσης των πληροφοριών αυτών.

Γίνεται μέσω της Αξιολόγησης Κινδύνου (Risk Assesment)

Αξιολόγηση Κινδύνου

- 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.
- **Μέτρα ασφαλείας** που εφαρμόζονται προκειμένου να επιτύχουμε το επίπεδο ασφάλειας που επιθυμούμε.
  - **Διοικητικά μέτρα:** Ρόλοι και αρμοδιότητες, τρόπος διαχείρισης πληροφοριών, εσωτερικοί κανόνες λειτουργίας, πρόσληψη και αποχώρηση υπαλλήλου (πχ δέσμευση εμπιστευτικότητας), 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).

ΑΠΑΝΤΗΣΕΙΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑ 5

Α. ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ	
Α1. Απογραφή λογισμικού και υλικού	ΤΕΧΝΙΚΑ ΜΕΤΡΑ
Α2. Λήψη αντιγράφων ασφαλείας (backup)	ΤΕΧΝΙΚΑ ΜΕΤΡΑ
Α3. Εκπαίδευση χρηστών για τις λειτουργίες του Π.Σ.	ΔΙΟΙΚΗΤΙΚΑ ΜΕΤΡΑ
Α4. Περιγραφή της διαβάθμισης των πληροφοριών	ΔΙΟΙΚΗΤΙΚΑ ΜΕΤΡΑ
Α5. Αδιάλειπτη παροχή ρεύματος (UPS)	ΤΕΧΝΙΚΑ ΜΕΤΡΑ
Α6. Πρόσβαση στις κτιριακές εγκαταστάσεις	ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ
Α7. Αρχεία καταγραφής (log files)	ΤΕΧΝΙΚΑ ΜΕΤΡΑ
Α8. Περιγραφή ρόλων και αρμοδιοτήτων του προσωπικού ενός οργανισμού.	ΔΙΟΙΚΗΤΙΚΑ
Α9. Εγκατάσταση ισχυρών κλειδαριών στις εγκαταστάσεις των υπολογιστών	ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ
Α10. Ασφαλείς δοκιμές εφαρμογών λογισμικού	ΤΕΧΝΙΚΑ ΜΕΤΡΑ

Έλεγχος Πρόσβασης (Access Control)

Για να μπορέσει ένας οργανισμός να προστατεύσει τις πληροφορίες του από τυχαίες ή εσκεμμένες αλλοιώσεις εξουσιοδοτημένων και από εσκεμμένες αλλοιώσεις από μη εξουσιοδοτημένα άτομα θα πρέπει να εφαρμόσει ελέγχους πρόσβασης στα συστήματα και τους δικτυακούς του πόρους.

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 (πχ ποιος-τι), να προστατευτούν και να παρακολουθούνται.

2. Πρόσβαση σε συστήματα: οι χρήστες χρησιμοποιούν διάφορα συστήματα του δικτύου όπως διακομιστές (servers), εκτυπωτές (printers) αλλά και κάθε άλλο είδος διαμοιραζόμενης συσκευής (shared device) 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 (files) και Βάσεις Δεδομένων (Databases). Τα δεδομένα θα πρέπει να υπόκεινται σε περιορισμούς, προστασία και παρακολούθηση.

Ο Έλεγχος Πρόσβασης είναι σημαντικότατος για επιχειρήσεις, κυβερνητικούς οργανισμούς και χρησιμοποιείται για να αποτρέπονται απάτες και λάθη.

Έλεγχος Πρόσβασης

- **Πιστοποίηση Ταυτότητας (Authentication) και Εξουσιοδότηση (Authorization). Πιστοποίηση Ταυτότητας**

  Username & password, βιομετρικά στοιχεία (δακτυλικό αποτύπωμά, ίριδα ματιού κ.α.)
- **Εφαρμογή Ελέγχου Πρόσβασης**

ΑΠΑΝΤΗΣΕΙΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑ 6

Α. ΠΕΡΙΠΤΩΣΕΙΣ ΕΛΕΓΧΟΥ ΤΗΣ ΠΡΟΣΒΑΣΗΣ	**Β. ΕΝΕΡΓΕΙΕΣ ΤΩΝ ΧΡΗΣΤΩΝ**
Α1. Πρόσβαση σε συστήματα	Β1. Χρησιμοποιούν δικτυακούς εκτυπωτές
Α2. Δικτυακή πρόσβαση	Β2. Έχουν πρόσβαση να διαβάζουν και να τροποποιούν αρχεία
Α3. Πρόσβαση στα δεδομένα	Β3. Χρησιμοποιούν ένα διαμοιραζόμενο σκληρό δίσκο σε ένα δίκτυο
	Β4. Ενημερώνουν μια κοινή για όλους Βάση Δεδομένων
	Β5. Μπορούν να χρησιμοποιούν τα στοιχεία σύνδεσης τους για να συνδεθούν από διαφορετικούς και πολλούς υπολογιστές
	Β6. Έχουν την δυνατότητα να βλέπουν τα μηνύματα άλλων στο δίκτυο

Μελέτη περίπτωσης για έλεγχο πρόσβασης (θέμα 17987)

Σε ένα κατάστημα που εμπορεύεται ηλεκτρονικά είδη υπάρχει ένας υπολογιστής σε κοινόχρηστο χώρο όπου καταχωρούνται οι παραγγελίες των πελατών που το επισκέπτονται.

Ο υπάλληλος που αναλαμβάνει την καταχώριση και την εκτέλεση των παραγγελιών δεν χρησιμοποιεί κωδικούς για την σύνδεσή του στον υπολογιστή αλλά ούτε και στο σχετικό πρόγραμμα, ενώ τον χρόνο που δεν εξυπηρετεί πελάτες παίζει παιχνίδια, στον υπολογιστή αυτόν, που "κατεβάζει" από το διαδίκτυο.

Ποια περίπτωση ελέγχου της πρόσβασης θα έπρεπε να έχει εξασφαλιστεί για να ελαχιστοποιηθούν οι κίνδυνοι και γιατί;

Απάντηση

- Αρχικά, εφόσον ο χρήστης δεν χρησιμοποιεί κωδικούς για την σύνδεσή του στον υπολογιστή αλλά ούτε και στο πρόγραμμα διαχείρισης των πελατών, θα πρέπει να εφαρμοστεί **έλεγχος πρόσβασης στα δεδομένα** και ο χρήστης να αποκτήσει ατομικό λογαριασμό σύνδεσης με όνομα χρήστη και κωδικό τα οποία να μην κοινοποιήσει σε τρίτους. Έτσι προστατεύεται η Ακεραιότητα Δεδομένων.
- Ακόμα, επειδή ο υπάλληλος συνδέεται στο διαδίκτυο από τον συγκεκριμένο υπολογιστή για να παίξει παιχνίδια, θέτοντας έτσι σε κίνδυνο τα δεδομένα των πελατών από ιούς ή άλλες κακόβουλες ενέργειες, ακόμα και αν ο υπολογιστής διαθέτει κάποιου είδους προστασία (πχ antivirus) θα πρέπει να εφαρμοστεί **έλεγχος δικτυακής πρόσβασης.** Δηλαδή να μπουν κάποιοι περιορισμοί στη σύνδεση στο διαδίκτυο αν όχι να καταργηθεί εντελώς.
- Επίσης, καλό θα ήταν να υπάρχουν Αρχεία Καταγραφής συμβάντων (Log files) για κάθε ενέργεια που μπορεί να προκαλέσει απώλεια ή βλάβη ώστε να μπορεί να αναζητηθεί η πηγή (π.χ. Η/Υ ή χρήστης) που την προκάλεσε.

Σχεδιασμός Επαναφοράς από καταστροφή

Οι καταστροφές μπορεί να είναι τόσο σημαντικές ώστε να πρέπει να διακοπεί η λειτουργία για απροσδιόριστο χρονικό διάστημα.

Καταστροφές από ανθρώπινο παράγοντα	Καταστροφές από φυσικά φαινόμενα
Κακόβουλες ενέργειες	πλημμύρες
λάθη	σεισμοί
εμπρησμοί	κεραυνοί
Τρομοκρατικές ενέργειες	

Σχέδιο ανάκαμψης από καταστροφή καταρτίζεται με στόχο την **άμεση και ορθή λειτουργία** του οργανισμού. Το σχέδιο αυτό θα πρέπει να περιγράφει ποιες ενέργειες και το πότε και από ποιον για να γίνει όσο γίνεται γρηγορότερα η αντιμετώπιση των συνεπειών μιας καταστροφής για να μπορέσει να λειτουργήσει η επιχείρηση. Πιθανόν μετά από καταστροφή ενός σκληρού δίσκου, καταστροφή του server της εταιρείας, υποκλοπή ευαίσθητων δεδομένων, Αλλοίωση δεδομένων, Διακοπή της επικοινωνίας

Δραστηριότητα 7

3ο μάθημα

Μέτρα ασφαλείας και αντίγραφα ασφαλείας

Μέτρα Ασφαλείας

- Έλεγχος Πρόσβασης
- Αντίγραφα ασφαλείας (backup)
- Λογισμικό προστασίας από κακόβουλο λογισμικό (antivirus)
- Ενημερώσεις (updates) Λειτουργικών Συστημάτων και Εφαρμογών
- Ασφάλεια Δικτύου

Μέτρα Ασφάλειας
Ερώτηση θέμα 20034

Για κάθε μία από τις απειλές που αναφέρονται στις παρακάτω προτάσεις προτείνετε ένα αντίμετρο που θα μπορούσε να χρησιμοποιηθεί για να την προλάβει ή να την αντιμετωπίσει.

1. Απώλεια των δεδομένων ενός σκληρού δίσκου λόγω μηχανικής βλάβης

Λήψη εφεδρικών αντιγράφων ασφαλείας

2. Υποκλοπή ευαίσθητων προσωπικών δεδομένων από υπολογιστικό σύστημα, από επιτιθέμενο που εκμεταλλεύτηκε γνωστό κενό ασφαλείας του Λειτουργικού Συστήματος.

Εγκατάσταση των ενημερώσεων ασφαλείας του Λειτουργικού Συστήματος

3. Συχνές διακοπές ρεύματος στην περιοχή που βρίσκεται το κέντρο μηχανογράφησης μιας επιχείρησης.

Εγκατάσταση συστήματος αδιάλειπτης παροχής ρεύματος

4. Εισαγωγή κακόβουλου λογισμικού σε υπολογιστικό σύστημα.

Εγκατάσταση προγράμματος προστασίας από κακόβουλο λογισμικό (antivirus).

5. Διοίκηση και προσωπικό ενός οργανισμού που δεν γνωρίζει πως να αντιμετωπίσει μια περίπτωση παραβίασης ασφάλειας.

Κατάρτιση του Σχεδίου Ασφαλείας (Security Plan) του οργανισμού

Αντίγραφα ασφαλείας

Η λήψη αντιγράφων ασφαλείας με σωστό τρόπο είναι απαραίτητη, γιατί αυτό θα βοηθήσει στο να επιτευχθεί γρηγορότερα διαθεσιμότητα του συστήματος αλλά και της ακεραιότητας των δεδομένων του. Η διαδικασία κατά την οποία χρησιμοποιούνται τα αντίγραφα ασφαλείας για να διορθωθούν προβλήματα λέγεται επαναφορά (restore).

Ανάλογα με την **κρισιμότητα των δεδομένων** μια εταιρεία αναπτύσσει την στρατηγική λήψης αντιγράφων ασφαλείας. Π.χ. μπορεί να καταφύγει σε πολύ ακριβές λύσεις για την αποθήκευση των αντιγράφων ασφαλείας και την γρηγορότερη λειτουργία και υψηλή διαθεσιμότητα (π.χ. Τράπεζα: server mirroring, συστοιχίες δίσκων, storage area network -SAN κτλ). Επιπλέον προσωπικό και χώροι

Οι Επιλογές στοχεύουν σε ταχύτατη επαναφορά των συστημάτων και την επιχειρησιακή συνέχεια.

- Στις απλούστερες περιπτώσεις κάθε οργανισμός θα πρέπει να κρατά ένα είδος αντιγράφων ασφαλείας ακόμα και σε μέσα μικρής ταχύτητας.

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)

Δραστηριότητα 2 (18014)

2.2. Στον υπολογιστή του λογιστηρίου μιας εταιρείας είναι αποθηκευμένα τα αρχεία Α, Β, Γ και Δ. Ο παρακάτω πίνακας δείχνει πότε τροποποιούνται τα αρχεία αυτά κατά την διάρκεια 4 εβδομάδων. Τα αρχεία τροποποιούνται κατά τις εργάσιμες ημέρες ενώ στο τέλος κάθε εβδομάδας, το Σάββατο, δημιουργούνται τα αντίγραφα ασφαλείας.

	1η Εβδομάδα	2η Εβδομάδα	3η Εβδομάδα	4η Εβδομάδα
Α	✓		✓	
Β			✓	
Γ		✓		
Δ				✓

Α) Πότε είναι προτιμότερο ο διαχειριστής του υπολογιστή να πάρει αυξητικό αντίγραφο ασφαλείας (incremental backup) που θα περιέχει τα αρχεία Α και Γ;

Β) Πότε πρέπει να πάρουμε αντίγραφο ασφαλείας που θα περιέχει όλα τα τροποποιημένα αρχεία, και τι είδους αντίγραφο ασφαλείας μπορεί να είναι αυτό;

Δραστηριότητα 2- απάντηση

Α) Εφόσον τα αρχεία τροποποιούνται κατά τις εργάσιμες ημέρες και ώρες ενώ τα αντίγραφα ασφαλείας δημιουργούνται το Σάββατο, μπορούμε να πάρουμε αυξητικά αντίγραφα ως εξής: για το αρχείο Α το Σάββατο της 1ης Εβδομάδας και για το αρχείο Γ το Σάββατο της 2ης εβδομάδας.

Β) Το διαφορικό αντίγραφο ασφαλείας(differential backup) της 4ης εβδομάδας θα περιέχει τα αρχεία Α, Β, Γ και Δ με τις τροποποιήσεις τους.

Επίσης και το πλήρες αντίγραφο (full backup) αν θα δημιουργηθεί την 4η εβδομάδα θα περιέχει τα τροποποιημένα Α,Β,Γ και Δ.

Δραστηριότητα 2Γ (18045)

Έστω πως το Σαββατοκύριακο σε κάποιο υπολογιστικό σύστημα γίνεται το πλήρες αντίγραφο ασφαλείας (full Backup). Την Δευτέρα τροποποιήθηκε το αρχείο Α , την Τετάρτη το αρχείο Β και το αρχείο Γ, ενώ την Πέμπτη, πάλι το αρχείο Β.

α) Τι θα πάρει το αυξητικό αντίγραφο ασφαλείας (incremental backup) την Τετάρτη και

β) Τι θα πάρει το διαφορικό αντίγραφο ασφαλείας (differential backup) την Πέμπτη;

ΑΠΑΝΤΗΣΗ

Το αυξητικό αντίγραφο ασφαλείας (incremental backup) της Τετάρτης θα πάρει το αρχείο Β και το αρχείο Γ.

Το διαφορικό αντίγραφο ασφαλείας (differential backup) της Πέμπτης θα πάρει όλα τα αρχεία δηλ. Το αρχείο Α που τροποποιήθηκε την Δευτέρα, το αρχείο Γ που τροποποιήθηκε την Τετάρτη και το αρχείο Β που τροποποιήθηκε τελευταία φορά την Πέμπτη.

Αντίγραφα ασφαλείας - Διατήρηση

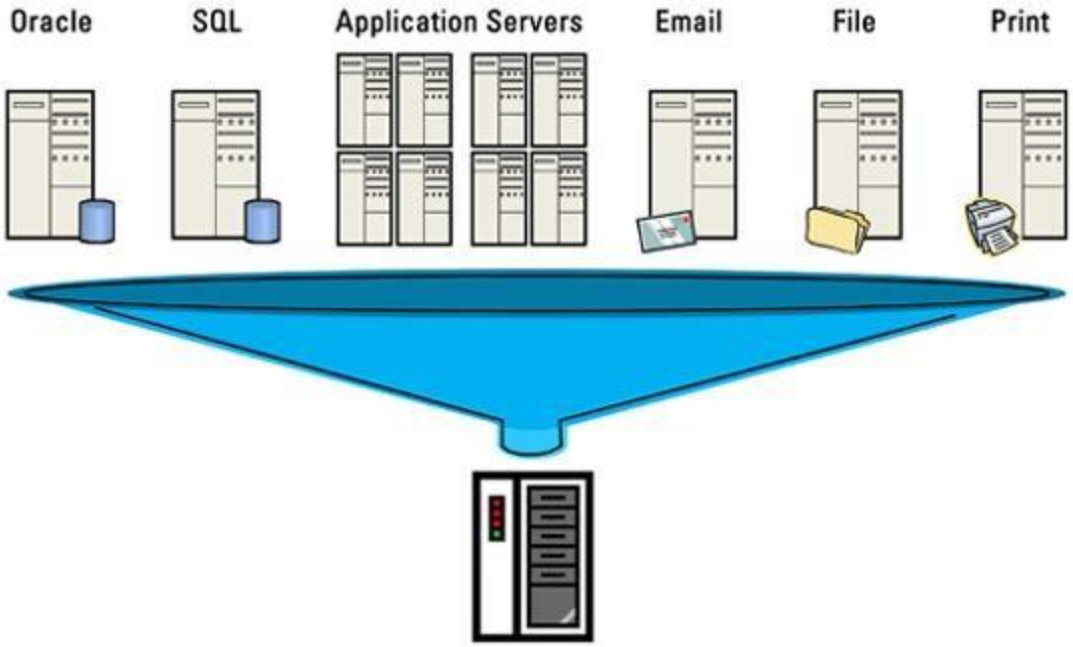
Τα αντίγραφα ασφαλείας θα πρέπει:

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

Σύγχρονες τάσεις

- Λήψη εικόνων των δίσκων (disk image) με κατάλληλο λογισμικό που να υποστηρίζει και διαφορικό και αυξητικό αντίγραφο ασφαλείας
- Εικονοποιημένοι Διακομιστές
- Αποθήκευση στο Νέφος

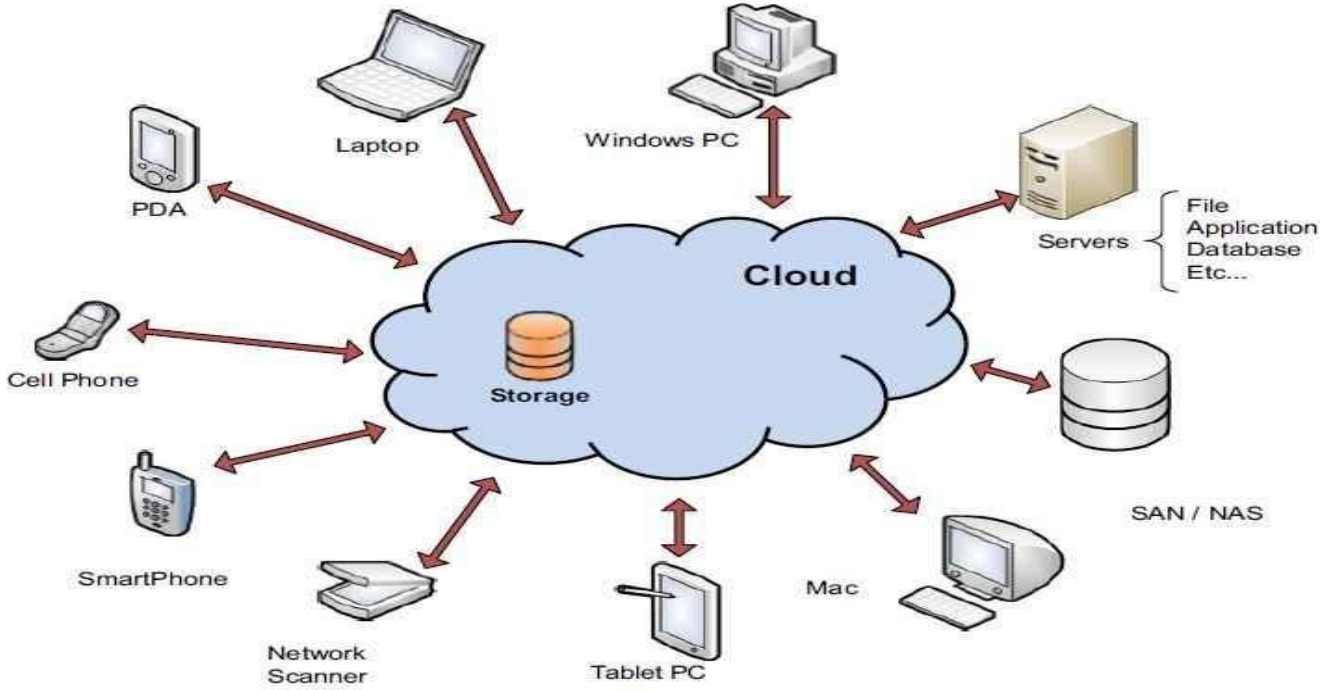
Εικονικοποιημένοι Διακομιστές (Server Virtualization)



Πλεονεκτήματα:

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

Αποθήκευση στο νέφος (Cloud Storage)



Πλεονεκτήματα:

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

Δραστηριότητα 3. Σύγχρονες στρατηγικές λήψης αντιγράφων ασφαλείας Οι σύγχρονες στρατηγικές λήψης αντιγράφων ασφαλείας είναι αυτές της λήψης εικόνων των δίσκων (disk image) από ένα υπολογιστικό σύστημα. Αντιστοιχίστε τις στρατηγικές αυτές από την στήλη Α, με τα πλεονεκτήματα που παρέχουν στο σύστημα από την στήλη Β.

Α. Σύγχρονες Στρατηγικές λήψης αντιγράφων ασφαλείας	**Β. Πλεονεκτήματα που παρέχουν**
Α1. Χρήση Εικονικοποιημένων Διακομιστών (Server Virtualization)	Β1. μεγάλος αποθηκευτικός χώρος με χαμηλό κόστος
	Β2. εύκολη μεταφορά
	Β3. μπορεί να συνεχίσει την λειτουργία του σχεδόν άμεσα, εάν προκύψει hardware πρόβλημα.
Α2. Αποθήκευση στο Νέφος (Cloud Storage)	Β4.αυτοματοποιείται η διαδικασία Αντιγράφων Ασφαλείας
	Β5. μειώνει την ανάγκη ύπαρξης διαφορετικών χώρων για την αποθήκευση των Αντιγράφων Ασφαλείας.
	Β6. βοηθά στο να επιτευχθεί γρηγορότερα διαθεσιμότητα του συστήματος
	Β7. μειώνεται η ανάγκη Υλικού (Hardware) και χώρου τοποθέτησής τους

Λογισμικό Κακόβουλης Χρήσης (Malware)

είναι το λογισμικό που μπορεί να προκαλέσει κάποιου είδους ζημιά στα συστήματα. Υπάρχουν άτομα αλλά και ομάδες ατόμων που χρησιμοποιούν προγράμματα ή εκμεταλλεύονται (*exploit*) κενά ασφαλείας εγκατεστημένων προγραμμάτων για διάφορους λόγους. Υπάρχουν πολλά είδη κακόβουλου λογισμικού με γνωστότερες κατηγορίες τις εξής:

1. **Spyware:** σκοπό έχουν την συλλογή πληροφοριών και την αποστολή τους στον δημιουργό τους. Καταγράφουν τις δραστηριότητες σε σελίδες αλλά και ό,τι πληκτρολογεί (keylogger) ο χρήστης ακόμα και κωδικούς.

2. **Adware:** αυτά προβάλλουν ανεπιθύμητες διαφημίσεις και ενδεχομένως να καταγράφουν τις συνήθειες του χρήστη και να τις αποστέλλουν στον δημιουργό τους. Συνήθως είναι μέρος δωρεάν προγραμμάτων αλλά και πρόσθετων σε φυλλομετρητές.

3. **Trojan** (horse): αυτό που επιδιώκουν είναι να δώσουν άμεση πρόσβαση στον διαχειριστή τους στο σύστημα και τα αρχεία του. Η εγκατάστασή του γίνεται υπό την κάλυψη κάποιουχρήσιμου προγράμματος ή παιχνιδιού. Με την εκτέλεση του μολυσμένου αρχείου (του Δούρειου ίππου - trojan) το οποίο έχει μέσα του δυο προγράμματα, το χρήσιμο και το Trojan, εγκαθίστανται και τα δυο και το χρήσιμο εκτελείται κανονικά.

4. **Viruses:** ο προορισμός τους καθορίζεται από τον δημιουργό τους. Μπορεί να είναι ακίνδυνοι αλλά και επιβλαβής για συστήματα και χρήστες. Μεταδίδονται μέσω της εκτέλεσης των αρχείων στα οποία έχουν προσκολληθεί σε άλλα υγιή αρχεία.

5. **Worms:** μπορούν να στέλνουν προσωπικά δεδομένα στους δημιουργούς τους. Μεταδίδονται μέσω δικτύων και ηλεκτρονικών μηνυμάτων (emails) και επιβαρύνουν την κίνηση του δικτύου

6. **Backdoor:** με τις Κερκόπορτες ο δημιουργός τους αποκτά κανάλι επικοινωνίας με τον Η/Υ

όπου εγκαταστάθηκε και μπορεί να εκτελέσει εντολές σε αυτόν όποτε θελήσει. Συνήθως εισχωρούν με την βοήθεια Trojan.

7. **Botnet:** είναι το δίκτυο από Bots, δηλαδή τους Η/Υ θύματα με το κακόβουλο λογισμικό. Η εγκατάσταση του λογισμικού γίνεται συνήθως από φυλλομετρητές, από Trojan και από συνημμένα ηλεκτρονικών μηνυμάτων (email attachments). Το δίκτυο των Η/Υ θυμάτων μπορεί και ελέγχεται κεντρικά μέσω πρωτοκόλλων όπως το IRC, HTTP και συχνά χρησιμοποιείται για επιθέσεις Άρνησης Υπηρεσιών (Denial of Services).

8. **Rootkit:** είναι ένα πολύ δύσκολα εντοπιζόμενο κακόβουλο λογισμικό που συνήθως καλύπτει άλλα κακόβουλα λογισμικά όπως τα Backdoors.

Δραστηριότητα 4

2.2. Παρακάτω δίνονται κάποια παραδείγματα κακόβουλου λογισμικού. Ποιες από τις τρεις βασικές αρχές της ασφάλειας πληροφοριακών συστημάτων (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα) απειλούν;

1. Spyware
2. Adware
3. Botnet
4. Viruses

Να δικαιολογήσετε την απάντησή σας. Να ληφθεί υπόψιν ότι ένας τύπος κακόβουλου λογισμικού μπορεί να απειλήσει περισσότερες από μία αρχές.

Απάντηση

1. Το κακόβουλο λογισμικό τύπου spyware απειλεί την εμπιστευτικότητα αφού μπορεί να καταγράψει ακόμα και τους μυστικούς κωδικούς του χρήστη.

2. Το κακόβουλο λογισμικό τύπου adware απειλεί την διαθεσιμότητα, αφού αν το πλήθος των ανεπιθύμητων διαφημίσεων που προβάλλει είναι εκτεταμένο, μπορεί να κάνει τον υπολογιστή να αποκρίνεται αργά και άρα να μην μπορεί να χρησιμοποιηθεί. Επίσης αν καταγράφει τις συνήθειες του χρήστη απειλεί την εμπιστευτικότητα.

3. Το κακόβουλο λογισμικό τύπου botnet απειλούν τη διαθεσιμότητα αφού μπορεί να χρησιμοποιηθούν για την διεξαγωγή (κατανεμημένων) επιθέσεων άρνησης εξυπηρέτησης.

4. Το κακόβουλο λογισμικό τύπου virus μπορεί να απειλήσει τόσο την ακεραιότητα αφού τροποποιεί τα δεδομένα των αρχείων αλλά και του συστήματος ώστε να διαδοθεί. Επιπλέον μπορεί να απειλήσει και τη διαθεσιμότητα, αφού μπορεί να καταστήσει ένα σύστημα μη λειτουργικό (πχ. να μην εκκινεί ο υπολογιστής επειδή έχει καταστραφεί κάποιο αρχείο εκκίνησης).

Λογισμικό προστασίας από Κακόβουλο Λογισμικό (antivirus)

Η προσβολή συστημάτων εντός ενός οργανισμού μπορεί να προκαλέσει προβλήματα στις Βασικές Αρχές ασφαλείας : Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα.

Κριτήρια επιλογής προγραμμάτων:

- Δυνατότητες προστασίας που προσφέρει
- Δυνατότητες συστήματος που θα εγκατασταθεί
- Ανίχνευση όλων των ειδών κακόβουλων λογισμικών
- Ανίχνευση συμπιεσμένων αρχείων
- Αυτόματη ανίχνευση USB συσκευών
- Προστασία των ηλεκτρονικών μηνυμάτων και άμεσων μηνυμάτων

Κατάλληλες ρυθμίσεις

- Αυτόματη ενημέρωση της βάσης του και του προγράμματος
- Ενεργοποίηση των δυνατοτήτων του προγράμματος προστασίας
- Τακτικό πλήρη έλεγχο του συστήματος
- Προστασία των ρυθμίσεων με κωδικό

Ενημερώσεις (Updates) Λειτουργικών Συστημάτων και Εφαρμογών

- Εφαρμογές (συνηθέστερα προγράμματα που γίνεται στόχος επιθέσεων είναι οι φυλλομετρητές) ιστοσελίδων (web browsers) και διάφορα πρόσθετα που χρησιμοποιούν αυτοί

Οι εταιρείες παραγωγής λογισμικού εκδίδουν συχνά ενημερώσεις των προγραμμάτων τους, για να επιδιορθώσουν διάφορα προβλήματα, μεταξύ των οποίων και **κενά ασφαλείας**. Για διευκόλυνση έχουν ενσωματωμένο έλεγχο για ενημερώσεις και εγκατάστασή τους και μπορεί να ελεγχθεί εύκολα αυτό από τις ρυθμίσεις του κάθε προγράμματος.

- Λειτουργικά Συστήματα

αυτόματος έλεγχος για ενημερώσεις του και η εφαρμογή τους σχεδόν σε όλα στα

συστήματα. Στα κρίσιμα συστήματα πρώτα θα πρέπει να γίνεται έλεγχος για το πώς θα τα επηρεάσουν οι ενημερώσεις πριν εγκατασταθούν, προκειμένου να αποφευχθούν προβλήματα διαθεσιμότητάς τους.

Επιβάλλεται οι χρήστες να συνδέονται στα συστήματα με λογαριασμούς **περιορισμένων δικαιωμάτων** (τυπικού χρήστη – typical user). Σε περιπτώσεις συνδέσεως με πλήρη δικαιώματα (διαχειριστή – Administrator για Windows ή root για Linux) είναι ιδιαίτερα επικίνδυνη η προσβολή από κακόβουλο λογισμικό γιατί αυτό θα μπορεί να επηρεάσει πολύ σοβαρότερα ένα σύστημα από ότι εάν είχε γίνει σε απλού χρήστη σύνδεση.

Ασφάλεια Δικτύου

- Τείχος Προστασίας (Firewall)
- Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network – VPN)
- Σύστημα Ανίχνευσης Εισβολής (Intrusion Detection System – IDS)

Δραστηριότητα 6. ΘΕΜΑ 4 (21427)

4.1

Για την πρόταση 1 θα απαιτηθούν:

10GB + 1GB + 2GB + 1GB + 2GB + 1GB = 17GB

Για την πρόταση 2 θα απαιτηθούν:

10GB + 1GB + 3GB + 4GB + 6GB + 7GB = 31GB

4.2

Αν εφαρμοστεί η πρόταση 1 θα ανακτηθεί αρχικά το backup της Κυριακής και στη συνέχεια το backup κάθε ημέρας με τη σειρά.

Αν εφαρμοστεί η πρόταση 2 θα ανακτηθεί αρχικά το backup της Κυριακής και στη συνέχεια το backup της Παρασκευής.

4.3

Η πρόταση 1 έχει το πλεονέκτημα ότι τα αντίγραφα ασφαλείας καταλαμβάνουν λιγότερο χώρο.

Η πρόταση 2 έχει το πλεονέκτημα ότι η διαδικασία επαναφοράς είναι πολύ πιο απλή.