HELLENIC REPUBLIC
UNIVERSITY OF MACEDONIA

Αποτροπή Διαρροής Δεδομένων

Θεοφάνης Β. Δημητρίου

Περιεχόμενα

- Εισαγωγή
- Σημαντικότητα του Προβλήματος.
- Πρόβλημα της Διαρροής Δεδομένων.
- Συνηθέστερες αιτίες Διαρροής Δεδομένων.
- Καταστάσεις Δεδομένων.
- Αρχιτεκτονική Τεχνικής.
- Επιλογή στρατηγικής DLP.
- Δομή DLP.
- Εφαρμογές OpenDLP και MyDLP.
- Συμπεράσματα – Προτάσεις.

Εισαγωγή

- Η διαρροή ή απώλεια δεδομένων (data leak/loss prevention - DLP) αποτελεί σήμερα ένα σημαντικό πρόβλημα για την ασφάλεια των πληροφοριακών συστημάτων (ΠΣ)
- Αποθήκευση τεράστιων όγκων δεδομένων σε διακομιστές (servers) και σε προσωπικούς υπολογιστές.
- Προστασία της εμπιστευτικότητας όλων των ειδών των δεδομένων είτε είναι προσωπικά, οικονομικά, πολιτικά κ.ά.
- Ενδεχομένως να υπάρξουν κυρώσεις από μια ενδεχόμενη διαρροή δεδομένων.

Σημαντικότητα του Προβλήματος

- Ανάπτυξη Πληροφοριακών Συστημάτων
- Η ατομική, η επιχειρηματική, η βιομηχανική ανάπτυξη εξαρτάται από τις πληροφορίες.
- Εξάρτηση της ανάπτυξης και τις οικονομίες από τις τεχνολογίες επικοινωνιών και πληροφοριών.
- Χρησιμοποίηση της πληροφορίας για μελλοντικές αποφάσεις.

Πρόβλημα της Διαρροής Δεδομένων

- Μεταβίβαση δεδομένων και πληροφοριών σε αναρμόδια πρόσωπα.
- Αποθήκευσή τους σε τόπο που δεν προοριζόταν αρχικά, χωρίς την παροχή της απαραίτητης ασφάλειας.
- Μη εξουσιοδοτημένοι χρήστες.
- Εξουσιοδοτημένοι χρήστες.
- Ανάγκη Τεχνολογικής Εφαρμογής:
  - Προστασία από τη Διαρροή Δεδομένων.
  - Αποδείξεις για την απόδοση ευθυνών.

Συνηθέστερες Αιτίες Διαρροής Δεδομένων

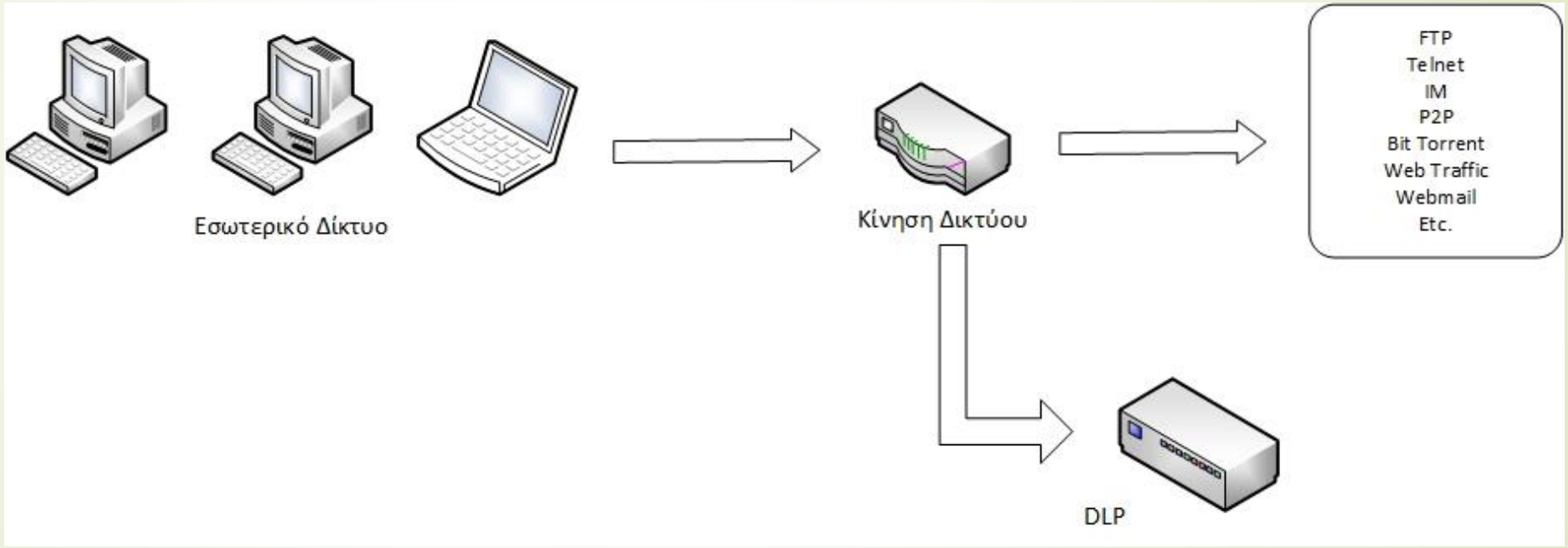
- Δημιουργία αναφοράς ή ενός εγγράφου από ένα χρήστη.
- Δυσαρεστημένοι υπάλληλοι.
- Αναβαθμισμένες εφαρμογές.
- Διαδικασία για την δημιουργία ασφαλών αντιγράφων ασφαλείας.
- Ξεπερασμένο υλικό το οποίο δωρίζεται.
- Δημιουργία εφαρμογής σε διαφορετικό μέρος.
- Ακατάλληλες ρυθμίσεις και ανεπαρκείς έλεγχοι ασφαλείας.

Καταστάσεις Δεδομένων

- Δεδομένα σε Κίνηση. (Data in Motion)
- Δεδομένα σε Αποθήκευση.(Data at Rest)
- Δεδομένα σε Χρήση. (Data in Use)

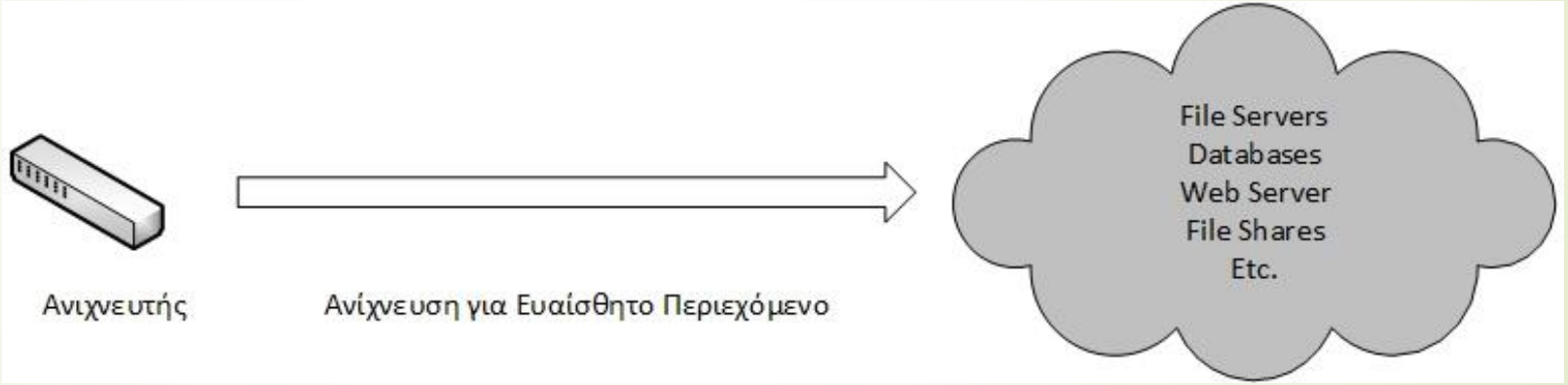
Καταστάσεις Δεδομένων

- Δεδομένα σε Κίνηση. (Data in Motion)
  - Μετακίνηση δεδομένων από ένα σημείο σε ένα άλλο.
  - Παρεμβολή λύσης ανάμεσα στα σημεία.



Καταστάσεις Δεδομένων

- Δεδομένα σε Αποθήκευση.(Data at Rest)
  - Δεδομένα καταχωρημένα σε κάποιο μέσο αποθήκευσης όπως είναι για παράδειγμα οι βάσεις δεδομένων.
  - Η ανακάλυψη ευαίσθητων δεδομένων σε βάσεις δεδομένων ή αποθετήρια δεδομένων.



Καταστάσεις Δεδομένων

- Δεδομένα σε Χρήση. (Data in Use)
  - Βασίζονται στη λύση αντιπροσώπου - πράκτορα (agent) ο οποίος εγκαθίστανται στους τερματικούς σταθμών των χειριστών.
  - Σε φορητούς υπολογιστές
  - Παρακολουθεί κάθε πληροφορία η οποία απομακρύνεται χρησιμοποιώντας αφαιρούμενες συσκευές, όπως είναι οι δισκέτες, CD's, USB's, κλπ.

Τι περιλαμβάνει ένα πρόγραμμα DLP

- Κεντρική Διαχείριση.
- Δημιουργία Πολιτικών.
- Εκτέλεση Ροής Εργασίας.

Τεχνικές Ανάλυσης Περιεχομένου

- Κανόνες και Ρυθμιστικές Εκφράσεις.
- Αποτυπώματα σε βάσεις δεδομένων.
- Λεπτομερείς αντιστοίχιση αρχείου.
- Μερική ταύτιση αρχείου.
- Στατιστική ανάλυση.
- Εννοιολογική

UNIVERSITY OF MACEDONIA
HELLENIC REPUBLIC

Αρχιτεκτονική Τεχνικής

- **Δεδομένα σε Κίνηση**
  - Παρακολούθηση Δικτύου
  - Ενσωμάτωση Ηλεκτρονικού Ταχυδρομείου
  - Ενσωμάτωση ή Μπλοκάρισμα στον Εξυπηρετητή.
    - Γέφυρα
    - Μεσολαβητής
    - TCP Poisoning
  - Εσωτερικά Δίκτυα.

Αρχιτεκτονική Τεχνικής

- **Δεδομένα σε Αποθήκευση**
  - Ανεύρεση στον τερματικό σταθμό.
  - Ανεύρεση αποθηκευμένων.
  - Ανεύρεση Server.

Αρχιτεκτονική Τεχνικής

- **Ενέργειες & Επιβολές**
  - Ειδοποίηση/Αναφορά
  - Προειδοποίηση.
  - Καραντίνα και Ειδοποίηση.
  - Καραντίνα και Κρυπτογράφηση.
  - Καραντίνα/Έλεγχος Πρόσβασης.
  - Μετακίνηση ή Διαγραφή.

Αρχιτεκτονική Τεχνικής

- **Δεδομένα σε Χρήση**
  - Χρησιμοποίηση πράκτορα.

Καθορισμός Αποτροπής Διαρροής Δεδομένων

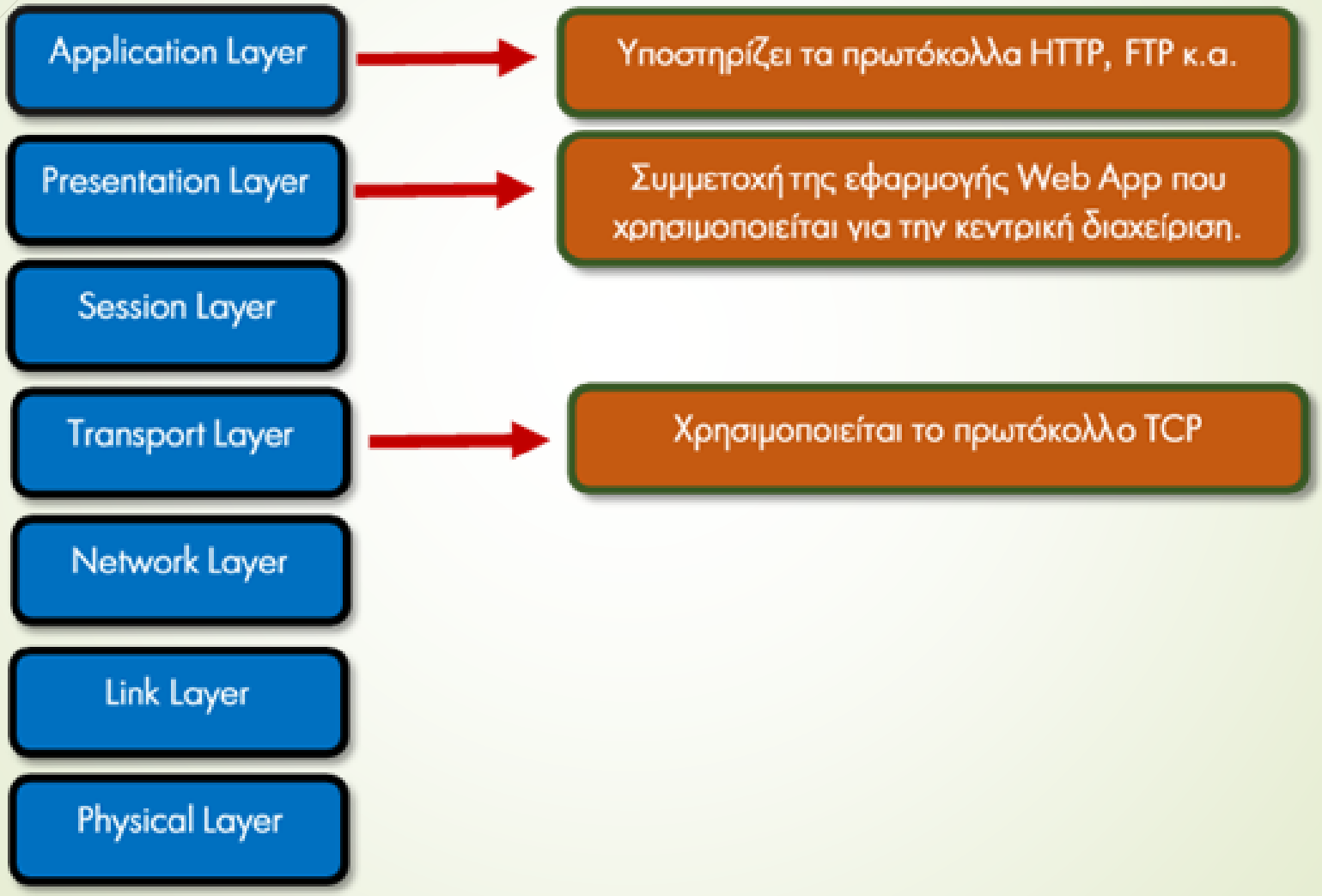
- Εντοπισμός και κατηγοριοποίηση ευαίσθητων δεδομένων
- Παρακολούθηση και έλεγχος της κίνησης των ευαίσθητων δεδομένων μεταξύ των δικτύων.
- Παρακολούθηση και έλεγχος της κίνησης ευαίσθητων πληροφοριών σε σχέση με το σύστημα του τελικού χρήστη.

Καθορισμός Αποτροπής Διαρροής Δεδομένων

Επιλογή Στρατηγικές DLP

- Καθορισμός των αναγκών και προετοιμασία του οργανισμού.
- Επίσημες Απαιτήσεις
- Αξιολόγηση Εφαρμογών.
- Εσωτερικοί Έλεγχοι

Μοντέλο Αναφοράς DLP



Στοιχεία που απαιτούνται για DLP

- Κονσόλα Διαχείρισης DLP
- Διάφορα πρωτόκολλα διαχείρισης DLP
- Πράκτορας Διαχείρισης της Εφαρμογής.
- Δικτυακές συσκευές.

Εφαρμογή OpenDLP

- Ανιχνεύει τα δεδομένα σε αποθήκευση.
- Λειτουργεί με πράκτορα ή χωρίς πράκτορα.
- Αυτόματη σάρωση.

Εφαρμογή MyDLP

- DLP Network
- DLP Endpoint.
- DLP Web UI.

Συμπεράσματα – Προτάσεις

- Ευαισθητοποίηση της διοίκησης του οργανισμού
- Ευαισθητοποίηση του προσωπικού.
- Εφαρμογή τεχνικής και στρατηγικής της πολιτικής ασφαλείας που θα αποφασιστεί.
- Πρέπει να:
  - Τεθούν σωστά οι απαιτήσεις
  - Ποια τμήματα θα εμπλακούν
  - Πώς θα πραγματοποιηθεί η σχεδίαση.

ΤΕΛΟΣ ΠΑΡΟΥΣΙΑΣΗΣ