

ΕΝΟΤΗΤΑ 5.1-2

Σχολικό εργαστήριο πληροφορικής και εισαγωγή στα θέματα ασφάλειας

```
graph TD; A[Σχολικό εργαστήριο πληροφορικής και εισαγωγή στα θέματα ασφάλειας] --> B[Στοιχειώδεις γνώσεις για τον τρόπο λειτουργίας των σχολικών εργαστηρίων]; A --> C[Βασικές γνώσεις για την ασφάλεια των σχολικών δικτύων και Η.Υ.]
```

Στοιχειώδεις γνώσεις για τον τρόπο λειτουργίας των σχολικών εργαστηρίων

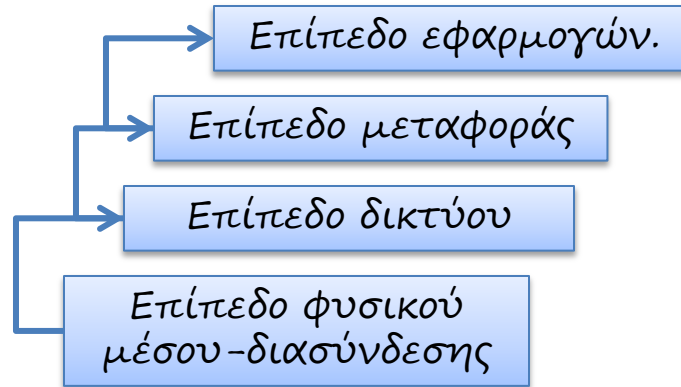
Βασικές γνώσεις για την ασφάλεια των σχολικών δικτύων και Η.Υ.

Βασικές έννοιες Δικτύων

Το Διαδίκτυο διασυνδέει μια μεγάλη ποικιλία συστημάτων

αποτελεί το μέσο επικοινωνίας για μια ακόμη μεγαλύτερη ποικιλία εφαρμογών

τέσσερα επίπεδα:



Το πρότυπο TCP/IP συνέβαλε στην επικράτηση του.

πρωτόκολλο ελέγχου μεταφοράς (TCP)

πρωτόκολλο Διαδικτύου (IP)

Σε κάθε κόμβο Διαδικτύου αντιστοιχίζεται 1 διαφορετική διεύθυνση (IP) για κάθε απλό PC, ή Server ή Διεύθυνση ιστοχώρου

έχει τη μορφή 255.255.255.255

Το Σύστημα Ονομασίας Περιοχών (DNS, Domain Name System), επιτρέπει την αντιστοίχιση μιας IP διεύθυνσης με ένα συμβολικό όνομα (π.χ. τη διεύθυνση 194.177.193.129 με το συμβολικό όνομα www.pi-schools.gr)

Βασικές έννοιες Δικτύων

Η ανταλλαγή πληροφοριών μεταξύ Η.Υ.:

πακέτα δεδομένων: αποστέλλονται, δρομολογούνται και παραδίδονται ενώ ελέγχεται και η ακεραιότητα των δεδομένων

Θύρα (port):
μια μοναδική διεύθυνση για κάθε εφαρμογή
καταχωρίζεται σε κάθε σταθμό εργασίας
καθορίζεται από το TCP/IP
εξασφαλίζεται ότι κάθε δρομολογούμενο πακέτο αντιστοιχείται με την ορθή εφαρμογή

Γέφυρα: διαχειρίζεται τη διακίνηση της πληροφορίας ανάμεσα σε τοπικά δίκτυα με τον ίδιο τύπο πρωτοκόλλου

Πύλη: διαχειρίζεται τη διακίνηση της πληροφορίας ανάμεσα σε δίκτυα που έχουν διαφορετικό τύπο πρωτοκόλλου.

Δρομολογητής: διαβιβάζει πακέτα δεδομένων στον προορισμό τους.

Θέματα ασφαλείας

Ο μεγαλύτερος κίνδυνος για τους Η.Υ.

«κακόβουλα» λογισμικά

ιοί

Δούρειοι Ίπποι
(Trojan Horses)

τα worms

διαδίδονται με
πολλαπλασιασμό,
αναπαράγουν τον
εαυτό τους

spyware

adware

cookies

tracking

dialers

spyware

Εγκαθίσταται λαθραία

Στόχος: να υποκλέψει - ελέγξει τον Η/Υ.

Δε διαδίδονται με πολλαπλασιασμό

Εξαπατούν το χρήστη σε ιστοσελίδες

Καταφάσκει σε μήνυμα παραπλανητικό

Επιβαρύνουν το φόρτο εργασίας του σκληρού

Αυξάνουν την κίνηση του δικτύου

Προβλήματα ευστάθειας του συστήματος

Η σελίδα έναρξης τροποποιείται

Εικονίδια στην επιφάνεια εργασίας, χωρίς
συγκατάθεση του χρήστη.

Sites καταχωρούνται στη λίστα «αγαπημένα»

Η δραστηριότητα του browser

παρακολουθείται και καταγράφεται

Δρομολογούν το φυλλομετρητή σε δικές τους
τοποθεσίες.

Αναδυόμενα διαφημιστικά παράθυρα

Προτιμήσεις και προσωπικές πληροφορίες,

αποκτώνται και διοχετεύονται προς τρίτους

Γραμμές εργαλείων και εργαλεία αναζήτησης

προστίθενται στο φυλλομετρητή

Εγκαθιστούν επιπλέον λογισμικά.

«κακόβουλα» λογισμικά

ιοί

Δούρειοι
Ίπποι (Trojan
Horses)

τα worms

spyware

tracking

adware

cookies

dialers

Ο όρος: κάθε πρόγραμμα που εμφανίζει διαφημιστικά μηνύματα (υπάρχουν και καλόβουλα)

όταν συλλέγουν πληροφορίες που κατασκοπεύοντας τον Η/Υ → κακόβουλα

τα λιγότερο κακόβουλα

Βοηθούν στην εύκολη περιήγησή μας

η αυτόματη αναγνώριση του χρήστη κατά την είσοδό του σε ένα τόπο

ύποπτα για προώθηση ή διαφήμιση

Λογισμικά που δημιουργούν μια νέα dial-up σύνδεση

Υψηλής χρέωσης (π.χ. 090...) → τα πιο κακόβουλα

Μόνο σε απλές συνδέσεις PSTN ή ISDN όχι ADSL

ανιχνεύονται και αφαιρούνται με anti-virus και anti-spyware και με ειδικά anti-dialers (dialerSpy).

«κακόβουλα» λογισμικά

SPAM

τα email με ενοχλητικό περιεχόμενο

συγκρατάλονται

ανεπιθύμητες διαφημίσεις για προϊόντα

ανεπιθύμητα newsletters, chain mails κτλ

δεν πρέπει να υπάρχει απάντηση σε άγνωστα μηνύματα

Ακόμα και η αίτηση για διαγραφή (Remove) ενημερώνει τον spammer ότι πρόκειται για ενεργή διεύθυνση → λήψη περισσότερων μηνυμάτων

να αποφεύγεται η εγγραφή σε λίστες αλληλογραφίας (mailing lists).

δυνατότητα αποκλεισμού αποστολέων (block address).

Μη ριζική λύση: spammers → πλαστή ηλεκτρ. διεύθυνση αποστολέα ή διαφορετική διεύθυνση για κάθε αποστολή (spoofing).

Phishing

προσπάθεια απόσπασης- υποκλοπής προσωπικών στοιχείων.

Σκοπός:

Να χρησιμοποιηθούν σε μη εξουσιοδοτημένες οικονομικές συναλλαγές

μέσω πλαστών ιστοσελίδων

που απαιτούν εγγραφή

μιμούνται επίσημες σελίδες (π.χ. τραπεζών, υπουργείων κλπ)

Προστασία

Προγράμματα firewall

Λειτουργίες

ως μέρος ολοκληρωμένης σουίτας
(Norton & McAfee Internet Security, Kaspersky)

δωρεάν firewalls (ZoneAlarm)

ως πυρηνικό χαρακτηριστικό του λειτουργικού
συστήματος (Linux).

Προστασίας κατά εισβολών
στο σύστημα από hackers

Ελέγχου της εξερχόμενης κυκλοφορίας (traffic)

δίνοντας επιλογές αποδοχής, απόρριψης της
αποστολής των packets που επιχειρείται

Ο ίδιος ο χρήστης πρέπει να:

είναι προσεκτικός στις επιλογές του

να ελέγχει προσεκτικά τα e-mails που λαμβάνει

να γνωρίζει τους κινδύνους του Διαδικτύου