Ενότητες 5.1 & 5.2

Σχολικό εργαστήριο πληροφορικής και εισαγωγή στα θέματα ασφάλειας

1. Εισαγωγή

Το μάθημα περιλαμβάνει την άκρως συνοπτική παρουσίαση θεμάτων που σχετίζονται με το Σχολικό εργαστήριο Πληροφορικής και ιδιαιτέρως με τα θέματα ασφαλείας.

Διδακτικοί Στόχοι

- Στοιχειώδεις γνώσεις για ον τρόπο λειτουργίας των σχολικών εργαστηρίων
- Βασικές γνώσεις για την ασφάλεια των σχολικών δικτύων και Η.Υ.

2. Βασικές έννοιες Δικτύων

Το Διαδίκτυο διασυνδέει μια μεγάλη ποικιλία συστημάτων και αποτελεί το μέσο επικοινωνίας για μια ακόμη μεγαλύτερη ποικιλία εφαρμογών. Το πρότυπο αναφοράς TCP/IP έπαιξε ένα σημαντικό ρόλο στην επικράτηση του. Το πρότυπο αναφοράς του Διαδικτύου μπορεί να οργανωθεί σε τέσσερα επίπεδα:

- Επίπεδο φυσικού μέσου-διασύνδεσης
- Επίπεδο δικτύου
- Επίπεδο μεταφοράς
- Επίπεδο εφαρμογών.

Το πρότυπο αναφοράς αυτό αποτελείται από δυο πρωτόκολλα επικοινωνίας το πρωτόκολλο ελέγχου μεταφοράς (TCP) και το πρωτόκολλο Διαδικτύου (IP). Σε κάθε κόμβο του Διαδικτύου έχει αντιστοιχισθεί μια διαφορετική διεύθυνση (διεύθυνση IP), η οποία έχει τη μορφή X.Y.Z.W, όπου κάθε γράμμα αντιστοιχεί σε έναν ακέραιο από

0 έως 255. Το Σύστημα Ονομασίας Περιοχών (DNS, Domain Name System), επιτρέπει την αντιστοίχιση μιας IP διεύθυνσης με ένα συμβολικό όνομα (για παράδειγμα τη διεύθυνση 194.177.193.129 με το συμβολικό όνομα www.pi-schools.gr, που αντιστοιχεί στο Παιδαγωγικό Ινστιτούτο).

Η ανταλλαγή πληροφοριών μεταξύ Η.Υ. πραγματοποιείται με τη βοήθεια πακέτων δεδομένων που αποστέλλονται προς το δίκτυο, δρομολογούνται και παραδίδονται στον παραλήπτη, ενώ ελέγχεται και η ακεραιότητα των δεδομένων.

Οι IP διευθύνσεις διακρίνονται σε διευθύνσεις τάξης-Α, τάξης-Β, τάξης-C, τάξης-D.

Εκτός των άλλων, το πρότυπο αναφοράς καθορίζει μια μοναδική διεύθυνση για κάθε εφαρμογή που καταχωρίζεται σε κάθε σταθμό εργασίας και έτσι εξασφαλίζεται ότι κάθε δρομολογούμενο πακέτο αντιστοιχείται με την ορθή εφαρμογή. Οι διευθύνσεις αυτές αποκαλούνται θύρες (ports).

Για τη βελτιστοποίηση της λειτουργίας των δικτύων χρησιμοποιούνται και μια σειρά από ενδιάμεσες συσκευές και διατάξεις:

Η γέφυρα διαχειρίζεται τη διακίνηση της πληροφορίας ανάμεσα σε τοπικά δίκτυα με τον ίδιο τύπο πρωτοκόλλου.

Η πύλη διακίνηση της πληροφορίας ανάμεσα σε δίκτυα που έχουν ενδεχομένως διαφορετικό τύπο πρωτοκόλλου.

Ο δρομολογητής διαβιβάζει πακέτα δεδομένων στον προορισμό τους.

3. Θέματα ασφαλείας

«Κακόβουλα» λογισμικά

Ο μεγαλύτερος κίνδυνος για τους Η.Υ. προέρχεται από τα λεγόμενα «κακόβουλα» λογισμικά όπως οι ιοί και οι Δούρειοι Ίπποι (Trojan Horses), τα worms. Τα κακόβουλα λογισμικά περιλαμβάνουν επίσης τις κατηγορίες spyware, adware, tracking cookies, dialers. Με τον όρο “spyware” χαρακτηρίζουμε συνήθως το λογισμικό που εγκαθίσταται λαθραία, χωρίς τη γνώση ή την άδεια του χρήστη, με στόχο να υποκλέψει πληροφορίες ή να ελέγξει τη λειτουργία του Η/Υ.

Αντίθετα προς τους ιούς (virus, worms), τα spyware δεν διαδίδονται με

πολλαπλασιασμό, δηλαδή δεν αντιγράφουν τον εαυτό τους. Ένας Η/Υ που έχει προσβληθεί από spyware, δεν μεταδίδει-εξαπλώνει τη «μόλυνσή του» μέσω του δικτύου. Συνήθως η εγκατάσταση του spyware πραγματοποιείται με εξαπάτηση του χρήστη κατά την επίσκεψή του σε ιστοσελίδες. Ο χρήστης μπορεί να δώσει τη συγκατάθεσή του για την εκτέλεση μιας λειτουργίας, κατά την επίσκεψη σε ιστοσελίδα, που όμως το μήνυμα είναι παραπλανητικό, ενώ η λειτουργία αντιστοιχεί στην εγκατάσταση του spyware. Σε άλλη περίπτωση μπορεί το λογισμικό που προσφέρεται στο χρήστη να μεταφέρει μαζί και spyware ή κατά την εγγραφή σε υπηρεσίες P2P ο χρήστης να οδηγείται και στη λήψη spyware.

Ένα spyware πρόγραμμα σπανίως συναντάται μόνο του. Συνήθως σε ένα «μολυσμένο» Η/Υ συνυπάρχουν πολλά spyware-adware, το οποία επηρεάζουν αισθητά την απόδοση του Η/Υ, επιβαρύνουν το φόρτο εργασίας του σκληρού δίσκου και αυξάνουν την κίνηση του δικτύου. Επίσης μπορούν να υπάρξουν και προβλήματα ευστάθειας του συστήματος, ενώ τα «συμπτώματα» να είναι παραπλανητικά και να οδηγούν ακόμη και σε ενδείξεις προβλήματος hardware.

Spyware

Προγράμματα για τη διαγραφή ή προστασία του Η/Υ ενάντια σε spyware έχουν αναπτυχθεί, αντίστοιχα προς τη λειτουργία των προγραμμάτων anti-virus

Θα πρέπει να αναφερθεί ότι τα spyware και adware προγράμματα δεν είναι πάντοτε επικίνδυνα για τη λειτουργία του Η/Υ. Σε κάθε περίπτωση όμως δεν παύουν να επιβαρύνουν τη λειτουργία του Η/Υ και του δικτύου, κυρίως στέλνοντας πληροφορίες στο δημιουργό τους. Κάποιες από τις κακόβουλες ενέργειες είναι :

- Υποκλέπτουν πληροφορίες που διακινεί ο χρήστης μέσω του Διαδικτύου.
- Συντομεύσεις και εικονίδια δικτυακών τόπων τοποθετούνται στην επιφάνεια εργασίας, χωρίς τη συγκατάθεση του χρήστη.
- Διαδικτυακοί τόποι καταχωρούνται στη λίστα των επιθυμητών διευθύνσεων, χωρίς τη συγκατάθεση του χρήστη.
- Η δραστηριότητα του φυλλομετρητή (browser) παρακολουθείται

και καταγράφεται.

- Μεταβάλλουν τη διεύθυνση και δρομολογούν το φυλλομετρητή σε δικές τους τοποθεσίες.
- Εμφανίζουν αναδυόμενα διαφημιστικά παράθυρα (pop-ups ads)
- Γραμμές εργαλείων και εργαλεία αναζήτησης προστίθενται στο φυλλομετρητή, χωρίς τη συγκατάθεση του χρήστη.
- Προτιμήσεις και προσωπικές πληροφορίες, αποκτώνται και διοχετεύονται προς τρίτους, χωρίς τη συγκατάθεση του χρήστη.
- Η σελίδα έναρξης, καθώς και άλλες ρυθμίσεις τροποποιούνται, μη επιτρέποντας τη διόρθωσή τους από το χρήστη.
- Εμποδίζουν - καθυστερούν τη λειτουργία του Η/Υ.
- Δεσμεύουν χώρο του σκληρού δίσκου
- Αυξάνουν τη δικτυακή κίνηση
- Εγκαθιστούν επιπλέον λογισμικά.

Adware

Ο όρος adware χρησιμοποιείται περισσότερο για κάθε πρόγραμμα που εμφανίζει διαφημιστικά μηνύματα. Ακόμα και ένα πρόγραμμα διαχείρισης ηλεκτρονικής αλληλογραφίας, που διανέμεται χωρίς χρέωση και ως αντάλλαγμα εμφανίζει διαφημιστικά μηνύματα, συγκαταλέγεται στην κατηγορία adware. Εντούτοις και τα adware μπορούν να θεωρηθούν ως spyware, όταν η λειτουργία τους βασίζεται σε πληροφορίες που συλλέγουν κατασκοπεύοντας τον Η/Υ στον οποίο έχουν εγκατασταθεί.

Τα cookies (web cookies ή HTTP cookies ή tracking cookies) μπορούν να θεωρηθούν ως τα λιγότερο κακόβουλα, αφού τις περισσότερες φορές είναι απαραίτητα για την ευκολότερη περιήγησή μας. Για παράδειγμα η αυτόματη αναγνώριση του χρήστη κατά την είσοδό του σε ένα τόπο. Παρόλα αυτά κάποια προγράμματα προστασίας τα χαρακτηρίζουν ως αντικείμενα με στόχο την προώθηση ή διαφήμιση και γι' αυτό τα περιλαμβάνουν στη λίστα προς απομάκρυνση

Dialers

Οι dialers είναι λογισμικά που δημιουργούν μια νέα dial-up (τηλεφωνική) σύνδεση στον Η/Υ και κάνουν κλήσεις, από αυτή, σε αριθμούς υψηλής χρέωσης (π.χ. 090…), που δεν ανήκουν σε εταιρίες παροχής πρόσβασης στο Διαδίκτυο. Είναι η χειρότερη περίπτωση

κακόβουλου λογισμικού, τουλάχιστον από οικονομικής πλευράς, αφού το ύψος του τηλεφωνικού λογαριασμού μπορεί να φτάσει σε εκατοντάδες ή χιλιάδες ευρώ.

Οι dialers, ακόμη και αν υπάρχουν στον Η/Υ, δεν μπορούν να λειτουργήσουν αν ο Η/Υ δεν συνδέεται στο τηλεφωνικό δίκτυο μέσω PSTN (απλή τηλεφωνική γραμμή) ή ISDN γραμμής. Οι dialers ανιχνεύονται και αφαιρούνται με anti-virus και anti-spyware προγράμματα ή και με ειδικά anti-dialers προγράμματα (dialerSpy). Μπορούν να ανιχνευτούν όμως εύκολα και από το χρήστη, με έλεγχο των dial-up συνδέσεων δικτύου του Η/Υ. Επίσης μπορεί να ζητηθεί η συνδρομή της τηλεφωνικής εταιρίας, με στόχο τον έλεγχο των κλήσεων και του ύψους του λογαριασμού.

Spam

Είναι τα email με ενοχλητικό περιεχόμενο. Στο **spam** (http://www.go-online.gr/ebusiness/specials/article.html?article_id=641) mail συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και sites καθώς επίσης και διάφοροι άλλοι τύποι email (ανεπιθύμητα newsletters, chain mails κτλ).

Για τη μείωση των λαμβανόμενων spam emails, δεν πρέπει να γίνεται απάντηση σε άγνωστα μηνύματα, καθώς μπορεί να εκληφθεί ως απόκριση για την αποστολή περισσότερων μηνυμάτων. Ακόμα και η αίτηση για διαγραφή (Remove) ενημερώνει τον spammer ότι πρόκειται για ενεργή ηλεκτρονική διεύθυνση, γεγονός που μπορεί να γίνει αφορμή για τη λήψη ακόμη περισσότερων μηνυμάτων. Επιπλέον, θα πρέπει να αποφεύγεται η εγγραφή σε λίστες αλληλογραφίας (mailing lists). Συχνά οι spammers διαθέτουν μεθόδους συλλογής ηλεκτρονικών διευθύνσεων, τις οποίες βρίσκουν κυρίως σε επίσημους δικτυακούς τόπους. Επίσης δεν θα πρέπει γνωστοποιείται το email, όπως οι φόρμες εγγραφής σε διάφορες διαδικτυακές υπηρεσίες. Ορισμένα προγράμματα διαχείρισης ηλεκτρονικής αλληλογραφίας (όπως το Outlook της Microsoft) παρέχουν τη δυνατότητα αποκλεισμού ορισμένων αποστολέων (block address). Με αυτό τον τρόπο ο χρήστης μπορεί να περιορίσει τον αριθμό των εισερχομένων spam mails και να τα διαχειριστεί καλύτερα, εφόσον γνωρίζει την ηλεκτρονική διεύθυνση του αποστολέα τους. Ωστόσο, η λύση αυτή δεν

είναι ριζική, καθώς είναι σχεδόν πάγια τακτική των spammers η χρήση πλαστής ηλεκτρονικής διεύθυνσης αποστολέα ή και διαφορετικής για κάθε αποστολή (spoofing).

Phishing

Ο όρος Phishing χρησιμοποιείται για να δηλώσει μια προσπάθεια απόσπασης- υποκλοπής προσωπικών στοιχείων τα οποία θα χρησιμοποιηθούν σε μη εξουσιοδοτημένες οικονομικές συναλλαγές. Συνήθως πραγματοποιείται μέσω πλαστών ιστοσελίδων, που απαιτούν εγγραφή ή μιμούνται επίσημες σελίδες αξιόπιστων οργανισμών (π.χ. τράπεζες, υπουργεία), σε συνδυασμό με την αποστολή ενημερωτικών spam emails.

4. Προστασία

Πρώτη φροντίδα για την προστασία των ψηφιακών δεδομένων απέναντι στους κινδύνους που εγκυμονεί το Διαδίκτυο δεν είναι άλλη από την επιλογή και την χρήση ενός firewall προγράμματος. Ενός firewall που μπορεί να διατίθεται ως μέρος μιας ολοκληρωμένης σουίτας προγραμμάτων ασφαλείας (Norton & McAfee Internet Security), δωρεάν firewalls (ZoneAlarm) ή ακόμη και ως γηγενές χαρακτηριστικό του πυρήνα ενός λειτουργικού συστήματος (Linux). Ένα από τα πιο σημαντικά κριτήρια επιλογής Internet firewall θα πρέπει να είναι οι λεγόμενες λειτουργίες ελέγχου της εξερχόμενης κυκλοφορίας (traffic), δίνοντάς σας επιλογές αποδοχής, απόρριψης (πρόσκαιρης ή μόνιμης) της αποστολής των packets που επιχειρεί να στείλει μια εφαρμογή.

Μια συνηθισμένη περίπτωση εφαρμογής που ενσωματώνει firewall, περιλαμβάνει τέσσερις λειτουργίες ασφαλείας, ένα firewall, διαχείριση προγραμμάτων, κλείδωμα της σύνδεσης, και ζώνες οι οποίες σας ενημερώνουν για κάθε πρόγραμμα που προσπαθεί να συνδεθεί με το διαδίκτυο.

Το firewall επίσης αποτελεί εργαλείο προστασίας κατά εισβολών στο σύστημα από hackers.

Ωστόσο, πέρα από τα τεχνικά μέσα, εκείνο που εξασφαλίζει την καλύτερη προστασία από όλα τα κακόβουλα λογισμικά είναι ο ίδιος ο χρήστης ο οποίος πρέπει να είναι προσεκτικός στις επιλογές του, να γνωρίζει τους κινδύνους του Διαδικτύου και να ελέγχει προσεκτικά τα e-mails που λαμβάνει.

5. Προτεινόμενες Δραστηριότητες

Δραστηριότητα 1η	Από τη διεύθυνση : http://free.grisoft.com/doc/5390/us/frt/0 κατεβάστε το AVG Anti-Virus Free Edition. Διαπιστώστε με ποιο τρόπο πραγματοποιείται η εγκατάσταση του.
Δραστηριότητα 2η	Παρακολουθείστε το video clip για τη λειτουργία των ιών http://computer.howstuffworks.com/virus.htm. Σχολιάστε τους τρόπους με τους οποίους μεταδίδονται οι ιοί
Δραστηριότητα 3η	Από τη διεύθυνση : http://www.safer-networking.org/gr/tutorial/index.html κατεβάστε το Spybot και διαπιστώστε με ποιο τρόπο πραγματοποιείται η εγκατάσταση του.

Δραστηριότητα 4η

Διαβάστε και σχολιάστε την παρακάτω πραγματική περίπτωση fishing email.

MR.AHMED SALEH
DIRECTOR PROJECT IMPLEMENTATION,
FEDERAL AIRPORT AUTHORITY OF NIGERIA (FAAN)
LAGOS-NIGERIA.
TELEPHONE:234-803-3035481
ATTN:MD/CEO
I AM A DIRECTOR IN THE FEDERAL AIRPORT AUTHORITY OF NIGERIA.I SEEK THE ASSISTANCE OF A RELIABLE FOREIGN COMPANY OR INDIVIDUAL INTO WHOSE BANK ACCOUNT I CAN TRANSFER THE SUM OF US$25.5M (TWENTY FIVE MILLION, FIVE HUNDRED THOUSAND UNITED STATES DOLLARS).
……
I HAVE PUT IN MOTION THE MACHINERY FOR THE TAKE OFF OF THIS TRANSACTION AND FURTHER ACTION WILL COMMENCE IMMEDIATELY I HEAR FROM YOU. I HAVE AGREED THAT AFTER THE TRANSFER OF THE MONEY INTO YOUR ACCOUNT, YOU SHALL BE ENTITLED TO 30% OF THE TOTAL SUM, I SHALL TAKE 65% WHILE 5% HAS BEEN MAPPED OUT TO REIMBURSE ALL LOCAL AND INTERNATIONAL EXPENSES THAT MAY BE INCURRED IN THE COURSE OF THE TRANSACTION.
…….
PLEASE IF THIS PROPOSAL IS ACCEPTABLE TO YOU, INDICATE BY RETURN MAIL. SHOULD INCASE YOU HAVE ANY QUESTION, FEEL FREE TO ASK. INCLUDE YOUR PRIVATE TELEPHONE AND FAX NUMBERS WHILE REPLYING.

I EXPECT YOUR RESPONSE.

6. Ερωτήσεις

1. Αντίστοιχα με την προστασία από τους ιούς υπάρχουν τα λεγόμενα προγράμματα γονεϊκής προστασίας (parental control). Εντοπίστε πληροφορίες για αυτά στο Διαδίκτυο. Θεωρείτε ότι είναι ασφαλή και ότι πρέπει να τα χρησιμοποιούν οι γονείς;

7. Ασκήσεις

Επισκεφτείτε τη σελίδα http://www.hackerwatch.org/probe/
και επιλέξτε τον έλεγχο port scan. Παρατηρώντας τα αποτελέσματα σχολιάστε τις θύρες και τις υπηρεσίες που αντιστοιχούν σε αυτές.

8. Βιβλιογραφία - Δικτυογραφία

Δικτυογραφία

Ενδεικτικές ψηφιακές πηγές

http://free.grisoft.com/doc/5390/us/frt/0 AVG antivirus και AVG internet security

http://www.avast.com/eng/avast_4_home.html
AVAST antivirus

http://www.freeantivirusinfo.com
Norton Antivirus

http://www.pctools.com/free-antivirus/
PC TOOLS antivirus

http://www.free-av.de
AVIRA antivirus

http://el.wikipedia.org/wiki/Antivirus_software
http://computer.howstuffworks.com/virus.htm
Υλικό για ιούς

http://www.freeware-apps.com/index.php
Δωρεάν λογισμικά προστασίας

http://www.noadware.net/research/
Κατάλογος των Spyware και adware, με τον αντίστοιχο πίνακα ενεργειών, καθώς επίσης και με τα σχετιζόμενα αρχεία και καταχωρήσεις στη Registry.

http://www.go-online.gr/ebusiness/specials/article.html?article_id=409
Ασφαλής πλοήγηση στο Διαδίκτυο

http://www.go-online.gr/ebusiness/specials/article.html?article_id=1173
Αντιμετώπιση spyware

http://www.tech-faq.com/ylang/el/free-spyware-removal.shtml
Πρόγραμμα προστασία ανοικτού κώδικα

http://www.lavasoftusa.com/
Δωρεάν πρόγραμμα προστασίας

http://www.pctools.com/spyware-doctor/
Δοκιμαστική έκδοση λογισμικού προστασίας (με πλήρη λειτουργία προστασίας real time).
http://www.freeware-apps.com/index.php
Αντιμετώπιση dialers, spyware και άλλων κακόβουλων λογισμικών

http://www.pcworld.com/tc/spyware/
http://it.ccri.edu/helpdesk/spyware-faqs.shtml
http://www.hsbc.gr/gr/about/security/five-golden-rules/anti-spyware-software/
Δικτυακοί τόποι με ενημερωτικά στοιχεία

http://www.leechvideo.com/video/view1599665.html
ρυθμίσεις Win XP firewall (video clip)

http://www.go-online.gr/ebusiness/specials/index.html
ενημερωτικό υλικό για firewall, spam, phishing

http://www.personalfirewall.comodo.com
COMODO Firewall

http://www.download.com/3000-2092-10039884.html
ZONE ALARM Firewall

http://el.wikipedia.org/wiki/Antivirus_software
http://el.wikipedia.org/wiki/Firewall
Ηλεκτρονικές πηγές για Antivirus – Firewall

http://computer.howstuffworks.com/firewall.htm
(Πλήρες άρθρο με εικόνες και επεξήγηση για τη λειτουργία των Firewall)

http://www.spamunit.com/
Δικτυακός τόπος ενημέρωσης και παροχής προγραμμάτων εναντίον του spam

http://www.hackerwatch.org/probe/
On line εργαλείο ελέγχου του firewall (των θυρών του Η/Υ)

Ενδεικτική βιβλιογραφία

Βιβλιογραφία

- Πανέτσος Σπύρος (2007) ΕΠΙΚΟΙΝΩΝΙΕΣ & ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ. Εκδόσεις Τζιόλας.