1. 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 μίας 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 διαχειρίζεται τη διακίνηση της πληροφορίας ανάμεσα σε δίκτυα που έχουν ενδεχομένως διαφορετικό τύπο πρωτοκόλλου.
- Ο δρομολογητής διαβιβάζει πακέτα δεδομένων στον προορισμό τους.

2. Θέματα ασφαλείας

«Κακόβουλα λογισμικά»

Ο μεγαλύτερος κίνδυνος για τους Η.Υ. προέρχεται από τα λεγόμενα «κακόβουλα» λογισμικά, όπως οι ιοί, οι Δούρειοι Ίπποι(Trojan Horses) και 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, όμως το μήνυμα να 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.

Προγράμματα για τη διαγραφή ή προστασία του Η/Υ ενάντια σε Spyware 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.

Ο όρος **adware** χρησιμοποιείται περισσότερο για κάθε Adware 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.

Οι **dialers** είναι λογισμικά που δημιουργούν μια νέα dial-up (τηλεφωνική) σύνδεση στον Η/Υ και κάνουν κλήσεις από αυτήν 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 mail (http://www.go-online.gr/ebusiness/specials/article.html?article_id=641) 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 να γνωστοποιείται το email, όπως σε 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).

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. Ένα firewall πρόγραμμα μπορεί να διατίθεται ως μέρος μιας ολοκληρωμένης σουίτας προγραμμάτων ασφαλείας (Norton & McAfee Internet Security), ως δωρεάν firewall (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 και 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 αποτελεί επίσης 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.