Φιλοθέη Κολίτση

«Ασφάλεια στα Δίκτυα Υπολογιστών»

Δραστηριότητα στην Ενότητα 6
ΠΑΚΕ Κεντρικής Μακεδονίας 2011-2012

Η ασφάλεια των πληροφοριών είναι ιδιαίτερα σημαντική στα σύγχρονα δίκτυα υπολογιστών. Η χρησιμοποίηση όλο και πιο προηγμένων τεχνολογιών οργάνωσης και διαχείρισης της πληροφορίας, όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων και τα σύγχρονα δίκτυα, προσφέρει αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες διαχείρισης και προσβασιμότητας των πληροφοριών, αυξάνει όμως ανάλογα και προβλήματα τα σχετικά με την προστασία και τη διαθεσιμότητα των πληροφοριών.

Η έννοια της ασφάλειας σε ένα Δίκτυο Υπολογιστών σχετίζεται με την ικανότητα μας α προστατεύουμε τις πληροφορίες μας από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση τους και γενικότερα, συνδέεται στενά με τρεις βασικές έννοιες: α) Διαθεσιμότητα-Availability, β) Εμπιστευτικότητα-Confidentiality, γ) Ακεραιότητα -Integrity

α) Διαθεσιμότητα : το να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός δικτύου υπολογιστών όταν τις χρειάζονται εξουσιοδοτημένοι χρήστες

β) Εμπιστευτικότητα : είναι η πρόληψη μη εξουσιοδοτημένης πρόσβασης στις διαθέσιμες πληροφορίες. Εδώ σαν υποκατηγορία μπορούμε να τοποθετήσουμε την ιδιωτικότητα-privacy που αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα

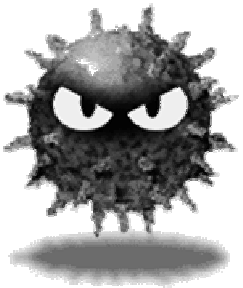
γ) Ακεραιότητα: πρόληψη από μη εξουσιοδοτημένη εγγραφή, διαγραφή ή μετατροπή των δεδομένων ενός πληροφοριακού συστήματος ή από βλάβη κάποιου συστήματος ή από άλλο τυχαίο γεγονός.

Κακόβουλες Επιθέσεις

Με την ανάπτυξη και τη διάδοση του διαδικτύου παράλληλα αναπτύχθηκε και τεχνολογία κακόβουλων επιθέσεων. Ξεκίνησε σαν παιχνίδι νεαρών κομπιουτεράδων που είχαν στόχο την επίδειξη των ικανοτήτων τους. Οι κακόβουλες επιθέσεις, όμως, γρήγορα εξελίχθηκαν σε εργαλεία που αναπτύσσονται με σκοπό την υποκλοπή πληροφοριών, την καταστροφή αρχείων, την παρεμπόδιση παροχής υπηρεσιών, εν τέλει υποβοηθώντας το οργανωμένο έγκλημα, κλέβοντας αριθμούς πιστωτικών καρτών, κωδικούς λογαριασμών (passwords), απόρρητα αρχεία και άλλα ψηφιακά μυστικά που αποκαλύπτουν οι χρήστες όταν κάνουν αγορές και

παραγγελίες στο Διαδίκτυο. Επιπλέον, υπάρχουν περιπτώσεις υποκλοπής και αξιοποίησης στοιχείων και πληροφοριών για εγκληματικούς ή στρατιωτικούς σκοπούς και ήδη έχουν κάνει την εμφάνισή τους κάποιοι ιοί που θεωρούνται οι πρόδρομοι της νέας γενιάς των ιών «κατασκόπων». Τα κυριότερα εργαλεία που έχουν αναπτυχθεί για αυτόν τον σκοπό είναι τα ακόλουθα: ιοί (viruses), σκουλήκια (Worms), δούρειοι ίπποι (trojan horses) κα. Ας τα δούμε όμως όλα αυτά λίγο πιο αναλυτικά.

Ιός Υπολογιστή (virus)



Ένας ιός υπολογιστών (virus) είναι ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς τη γνώση ή την άδεια του χρήστη και να προσκολλάται πάνω σε κάποιο άλλο αρχείο δηλαδή να "μολύνει" τον υπολογιστή. Αυτό γίνεται συνήθως σε εκτελέσιμα αρχεία (.exe, .com, .bat), που, όταν τα εκτελέσουμε εμείς, τρέχει ταυτόχρονα και ο καταστροφικός τους κώδικας, ενώ παράλληλα ο ιός αντιγράφεται, δηλαδή προσκολλάται και σε άλλα αρχεία πολλαπλασιάζοντας τον εαυτό του. Ένας ιός μπορεί να προξενήσει μεγάλα προβλήματα τόσο στο software όσο και στο hardware. Μερικοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή, στον οποίο εγκαθίστανται. Αυτό μπορεί να συμβεί είτε με την καταστροφή των προγραμμάτων του είτε με τη διαγραφή αρχείων ή ακόμη και με τη μορφοποίηση (format) ολόκληρου του σκληρού δίσκου του υπολογιστή. Άλλοι δεν έχουν ως σκοπό να προκαλέσουν οποιαδήποτε ζημία, απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη κειμένου, βίντεο, ή ηχητικών μηνυμάτων, μερικές φορές αρκετά χιουμοριστικών. Όμως, ακόμη και αυτοί οι "καλοκάγαθοι" ιοί μπορούν να δημιουργήσουν προβλήματα στο χρήστη υπολογιστών: απασχολώντας τους πόρους του συστήματός μας (μνήμη, επεξεργαστή κλπ) προκαλούν καθυστέρηση στον υπολογιστή μας, και κάποιες φορές ασταθή συμπεριφορά του συστήματος που μπορεί να το οδηγήσει ακόμη και σε κατάρρευσή του (system crash). Τέλος, ένα μεγάλο ποσοστό των ιών δεν έχει σκοπό την καταστροφή των δεδομένων του χρήστη ή την παρενόχλησή του, αλλά την κλοπή προσωπικών του δεδομένων ή την εισαγωγή του υπολογιστή-στόχου σε κάποιο παράνομο δίκτυο χωρίς τη συγκατάθεση του χρήστη.

Αν όμως δε τρέξει κάποιος το μολυσμένο αρχείο τότε ο ιός δε μπορεί ούτε να μολύνει αλλά ούτε και να εξαπλωθεί. Με λίγα λόγια, χωρίς την ανθρώπινη παρέμβαση το μεγαλύτερο ποσοστό των ιών δε θα μπορούσαν να κάνουν απολύτως τίποτα.

Οι ιοί διαδίδονται από τον ένα υπολογιστή στον άλλο με δύο τρόπους: Είτε μέσω φορητού μέσου αποθήκευσης (δισκέτα, οπτικό δίσκο ή μνήμη

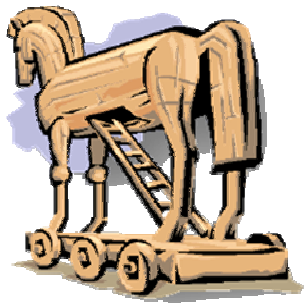
flash USB) είτε μέσω δικτύου. Ο δεύτερος τρόπος είναι σήμερα ο πλέον διαδεδομένος, λόγω της ευρείας διάδοσης του Διαδικτύου διεθνώς. Συνήθης τακτική είναι η αποστολή του ιού μέσω του ηλεκτρονικού ταχυδρομείου (e-mail), είτε ως συνημμένα είτε ως τμήμα αυτού καθαυτού του μηνύματος.
Οι ιοί ορισμένες φορές εσφαλμένα συγχέονται με τα "σκουλήκια" υπολογιστών (worms) και τους δούρειους ίππους (trojan horses).

Σκουλήκι (Worm)



Τα worms με τους ιούς μπορούν να θεωρηθούν κοντινά ξαδέρφια, αλλά η πιο κατάλληλη ερμηνεία τους θα ήταν υποκατηγορία ιού. Το worm με τον ιό κάνει πάνω κάτω το ίδιο πράγμα. Δηλαδή αντιγράφει και αυτό τον εαυτό του και μεταφέρεται από τον έναν υπολογιστή στον άλλον, με την διαφορά ότι το worm δε χρειάζεται βοήθεια από ανθρώπινο χέρι. Τα κάνει όλα μόνο του.
Ένας από τους μεγαλύτερους κινδύνους των worms είναι ότι λόγω της ικανότητας τους να αντιγράφονται μόνοι τους και να μεταφέρονται επίσης μόνοι τους μέσω δικτύου, μπορούν να εξαπλωθούν σε όλο τον κόσμο μέσα σε ένα σύντομο χρονικό διάστημα. Επίσης, μία ικανότητα των worms είναι ότι για να εξαπλωθούν χρησιμοποιούν συνήθως τις επαφές (contact list) του υπολογιστή που έχουν μολύνει.
Ένα άλλο μεγάλο πρόβλημα που δημιουργούν τα worms είναι ότι λόγω του όγκου των πληροφοριών που στέλνουν μέσω δικτύου, πολλές φορές είναι ικανά να ρίξουν ολόκληρα δίκτυα.

Δούρειος Ίππος (Trojan horse)



Το όνομα τους το πήρανε από την Ιλιάδα του Ομήρου. Έτσι και το Trojan αρχικά φαίνεται σαν ένα άκακο πρόγραμμα που τις περισσότερες φορές αναφέρει ότι θα σας φανεί χρήσιμο. Στην πραγματικότητα όμως οι προθέσεις του δεν είναι καθόλου καλές. Μόλις το κάνετε εγκατάσταση αρχίζουν τα προβλήματα. Μερικά Trojan έχουν σχεδιαστεί να είναι απλά ενοχλητικά, ενώ υπάρχουν όμως και κάποια που είναι πιο επιθετικά και μπορεί να διαγράφουν αρχεία από το σύστημα μας να υποκλέπτουν πληροφορίες κλπ.
Επίσης τα Trojans πολλές φορές δημιουργούν μια «κερκόπορτα» (backdoor) στον υπολογιστή που μολύνουν, δηλαδή δίνουν σε κακόβουλα άτομα (π.χ τον δημιουργό του Trojan) απομακρυσμένη

πρόσβαση στο σύστημα σας. Τις περισσότερες φορές αυτό γίνεται για την απόκτηση προσωπικών πληροφοριών (κωδικούς πρόσβασης, πιστωτικές κάρτες κτλπ).
Η διαφορά του Trojan horse από ιούς και worms, είναι ότι το Trojan αντιγράφεται από τον χρήστη του υπολογιστή σκόπιμα, νομίζοντας ότι είναι κάτι καλό και δεν αναπαράγεται μόνο του.

Spyware
Τα spyware είναι προγράμματα τα οποία συλλέγουν πληροφορίες, χωρίς να το γνωρίζει ο χρήστης του υπολογιστή. Τι περισσότερες φορές τα στοιχεία που συλλέγουν αφορούν τις κινήσεις του χρήστη στο διαδίκτυο π.χ. σε ποια sites μπαίνει.
Το spyware είναι ένα σύνολο προγραμμάτων τα οποία μεταδίδουν προσωπικά στοιχεία από τον υπολογιστή σας στο διαδίκτυο, χωρίς εσείς να γνωρίζετε ότι συμβαίνει αυτό.

Adware
Τα προγράμματα αυτά είναι μια υποκατηγορία του spyware, που δεν στέλνουν προσωπικά δεδομένα αλλά επιτρέπουν σε άλλους χρήστες (τους κατασκευαστές τους), να παρακολουθούν τις κινήσεις σας στον υπολογιστή σας με στόχο να εκθέσουν το χρήστη σε διαφημιστικά μηνύματα. Επιπλέον ευθύνονται για πολλά pop-ups (διαφημιστικά παράθυρα που ανοίγουν μόνα τους όταν επισκεφτούμε κάποια άλλη ιστοσελίδα αυτά αυτόματα ανοίγουν νέο παράθυρο του φυλλομετρητή μας σε μια διεύθυνση που θέλουν να μας «προτείνουν» να επισκεφτούμε «αναγκαστικά»)

Coockies
Τα cookies είναι ένα είδος αρχείων, τα οποία δημιουργούνται και αποθηκεύονται στον σκληρό δίσκο του υπολογιστή μας από τα Web sites που επισκεπτόμαστε στο Διαδίκτυο, με απώτερο σκοπό την αναγνώρισή μας από τα ίδια Web sites την επόμενη φορά που θα βρεθούμε στις ιστοσελίδες τους.
Υποτίθεται ότι εξυπηρετούν χρήσιμους σκοπούς για τους χρήστες του Διαδικτύου, καθώς συγκεντρώνουν πληροφορίες σχετικά με τις καταναλωτικές τους συνήθειες, τις οποίες μπορούν να αξιοποιήσουν sites μεγάλων εταιρειών για να εξειδικεύσουν έτσι ή και να βελτιώσουν τα προϊόντα ή τις υπηρεσίες τους. Μια πολύ κοινή χρήση των cookies είναι να αποθηκεύσουν το όνομα χρήστη (user name) και τον μυστικό κωδικό ή συνθηματικό (password) που χρησιμοποιούμε, ώστε να μην χρειάζεται να τα ξαναπληκτρολογήσουμε την επόμενη φορά που θα συνδεθούμε με κάποια ιστοσελίδα.

Όμως, η σημαντικότερη χρήση των cookies είναι να παρακολουθούν και να καταγράφουν (κατασκοπεύουν) τις κινήσεις μας στο Διαδίκτυο, συνήθως τις καταναλωτικές, όπως σε ποια sites περιηγούμαστε και πόσο χρόνο μένουμε σ' αυτά, πόσο συχνά τα επισκεπτόμαστε κ.ά. Ακόμη και μέσα στο ίδιο το site μπορούν να καταγράψουν σε ποιες ιστοσελίδες έχουμε προτίμηση. Για παράδειγμα όταν επισκεπτόμαστε ηλεκτρονικά καταστήματα φαίνεται ότι η ιστοσελίδα «θυμάται» πότε την επισκεφτήκαμε τελευταία φορά, τι προϊόντα αναζητήσαμε ή αγοράσαμε και μας «προτείνει» κάποια αντίστοιχα που «πιστεύει» ότι θα μας ενδιέφεραν, μετά από στατιστική ανάλυση των προτιμήσεων άλλων χρηστών που έχουν κοινά ενδιαφέροντα με μας.
Μπορούμε από τις κατάλληλες επιλογές του φυλλομετρητή μας να εμποδίσουμε την αποθήκευση των cookies στον σκληρό μας δίσκο αλλά τότε αρκετές ιστοσελίδες δεν θα λειτουργήσουν σωστά πλήρως «αναγκάζοντάς μας έτσι» να τους δώσουμε τη δυνατότητα να διαχειριστούν τα cookies όπως αυτά έχουν προγραμματιστεί.

Dialers

Τα dialers αποτελούν έναν από τους μεγαλύτερους κινδύνους που κυκλοφορούν στο Διαδίκτυο. Δεν στοχεύουν να βλάψουν τον υπολογιστή μας ή τα αρχεία μας αλλά την ίδια μας την τσέπη μ' έναν πολύ ύπουλο τρόπο. Το dialer είναι ένα πρόγραμμα το οποίο αναγκάζει τον υπολογιστή μας να κάνει κλήσεις μέσω του modem και να συνδεθεί μ' άλλους servers απ' ότι έχουμε εμείς οι ίδιοι ρυθμίσει (π.χ. OTEnet) και συνεπώς ο λογαριασμός του τηλεφώνου μας να αυξάνεται εκθετικά.

Οι Επιθέσεις DoS (Denial of Service)

Οι επιθέσεις του τύπου DoS (Denial of Service), που είναι γνωστές και ως επιθέσεις άρνησης υπηρεσίας, αποτελούν μια από τις σοβαρότερες επιθέσεις που μπορούν να εκδηλωθούν σ' ένα Web site ή σ' ένα δίκτυο υπολογιστών. Οι επιθέσεις αυτές είναι καταστροφικές για τις εταιρείες και έχουν μεγάλο οικονομικό κόστος.
Το κόστος αφορά τις χαμένες ώρες λειτουργίας μιας επιχείρησης αλλά και το κόστος που απαιτείται για τον εντοπισμό και την αντιμετώπιση αυτών των επιθέσεων. Ουσιαστικά μια τέτοια επίθεση έχει ως αποτέλεσμα την αδυναμία της εταιρείας να εξυπηρετήσει τους πελάτες της.
Η επίθεση συνίσταται στην εκδήλωση χιλιάδων αιτήσεων σύνδεσης σ' έναν server και σε διάστημα μερικών ημερών, με απώτερο στόχο τον κατάρρευση του server από την αδυναμία του να ανταποκριθεί σ' έναν τόσο μεγάλο αριθμό αιτήσεων.

Οι Επιθέσεις DDoS (Distributed Denial of Service)

Τελευταία έχουν αρχίσει να κάνουν την εμφάνισή τους και οι λεγόμενες κατανεμημένες επιθέσεις άρνησης υπηρεσίας, γνωστές με τον όρο DDoS (Distributed Denial of Service). Σύμφωνα με το σενάριο, κάποια συγκεκριμένη ημερομηνία, προγράμματα τύπου worm που μέχρι τότε περίμεναν σιωπηρά στα μηχανήματα όπου φιλοξενούνταν, ξαφνικά ενεργοποιούνται και αρχίζουν όλα μαζί να στέλνουν αιτήσεις σύνδεσης σ' έναν συγκεκριμένο server. Ο server δέχεται τόσες πολλές αιτήσεις που αδυνατεί να ανταποκριθεί σ' όλες και αναπόφευκτα καταρρέει.
Πρόκειται για μια εξελιγμένη μορφή των επιθέσεων του τύπου DoS, οι οποίες είναι πιο αποτελεσματικές όσον αφορά τα καταστροφικά αποτελέσματα που επιφέρουν καθώς η επίθεση πραγματοποιείται από πολλά σημεία ταυτόχρονα. Αυτός που σκοπεύει να κάνει μια τέτοια επίθεση, φροντίζει αρχικά να αποκτήσει δικαιώματα administrator σ' όσο το δυνατόν περισσότερα συστήματα υπολογιστών μπορεί. Η επίθεση πραγματοποιείται μέσω αυτοματοποιημένων scripts (σεναρίων) για την ανακάλυψη συστημάτων που διαθέτουν χαμηλά στάνταρτ ασφαλείας. Από τη στιγμή που ο επιτιθέμενος αποκτήσει πρόσβαση σ' έναν αριθμό συστημάτων που θεωρεί ικανοποιητικό, φορτώνει το script για να εξαπολύσει την επίθεσή του.

Spam
Είναι η μαζική αποστολή email με ενοχλητικό περιεχόμενο. Στο spam mail συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες καθώς επίσης και διάφοροι άλλοι τύποι email (ανεπιθύμητα newsletters, chain mails κτλ).
Ορισμένα προγράμματα διαχείρισης ηλεκτρονικής αλληλογραφίας παρέχουν τη δυνατότητα αποκλεισμού ορισμένων αποστολέων (block address). Έτσι μπορούμε να περιορίσουμε τον αριθμό των εισερχομένων spam mails και να αποκλείσουμε τη λήψη τους από τη συγκεκριμένη ηλεκτρονική διεύθυνση του αποστολέα τους.

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, ενώ συχνά περιλαμβάνουν επίσημα logos εταιρειών καθώς και πληροφορίες από τα site τους για να πείσουν τα υποψήφια θύματα τους για την αληθοφάνειά τους
Για να αποφύγουμε το phising μπορούμε απλά να μην απαντάμε σε κάποιο μήνυμα που λάβαμε και νομίζουμε ότι είναι ένα phishing e-mail

αλλά και να μην κλικάρουμε ποτέ τις συνδέσεις μέσα στα e-mail αλλά να πληκτρολογούμε μόνοι μας τις διευθύνσεις απευθείας στον φυλλομετρητή μας ή να χρησιμοποιούμε τα προσωπικά μας bookmarks.

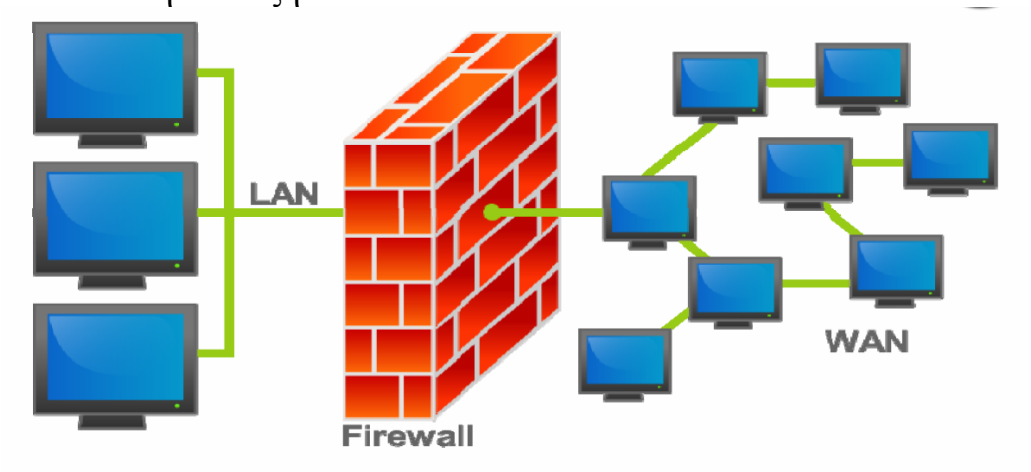
Τρόποι Προστασίας από κακόβουλες επιθέσεις – Προγράμματα Antivirus



Για την προστασία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, γνωστή ως αντιϊκό πρόγραμμα (antivirus). Προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος, τα αντιϊκά εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς εντολές από το χρήστη, και παραμένουν ως διαδικασίες στη μνήμη (memory resident), ώστε να είναι σε θέση να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό χρόνο. Τα προγράμματα αυτά πρέπει να αναβαθμίζονται σε τακτική βάση, ώστε να είναι σε θέση να αντιμετωπίζουν με επιτυχία τους νεοδημιουργούμενους ιούς. Σήμερα, αρκετοί οίκοι δημιουργίας λογισμικού ασχολούνται με τη δημιουργία τέτοιων προγραμμάτων. Τα αντιϊκά είναι σε θέση τόσο να εντοπίσουν μόλυνση τη στιγμή που αποπειράται, όσο και να "καθαρίσουν" τυχόν μολυσμένα αρχεία που εντοπίζουν.
Από τα πιο γνωστά αντικά προγράμματα είναι το Norton Antivirus της εταιρείας Symantec, το McAfee της εταιρείας Network Associates, το Kaspersky, το Panda, το Sophos, το F-Prot της εταιρείας Frisk, το F-Secure, το Avira καθώς και το AntiVir και το AVG της εταιρείας Grisoft που διατίθενται δωρεάν για προσωπική χρήση. Όλα έχουν τη δυνατότητα αυτόματης ενημέρωσης (update) μέσω του Διαδικτύου.
Υπάρχουν αρκετά και αξιόλογα προγράμματα τα οποία μπορούν να μας προσφέρουν κάποια προστασία (να διαγράψουν τα ήδη εγκατεστημένα spyware), η προστασία όμως που μας προσφέρουν δεν είναι απόλυτη. Δύο αρκετά καλά πρόγραμμα είναι το Spybot - Search and Destroy και το Ad-Aware SE Personal, τα οποία μάλιστα διανέμονται δωρεάν στο Διαδίκτυο.

Ένα επιπλέον μέτρο προστασίας είναι η χρήση ενός **ψηφιακού τείχους προστασίας (firewall)** προγράμματος. Ένα firewall 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).
Τα προγράμματα firewall μας επιτρέπουν να ελέγχουμε την εισερχόμενη και την εξερχόμενη κυκλοφορία (traffic), δίνοντάς μας επιλογές

αποδοχής, απόρριψης (πρόσκαιρης ή μόνιμης) της αποστολής των δεδομένων που επιχειρεί να στείλει μια εφαρμογή. Το firewall επίσης αποτελεί εργαλείο προστασίας κατά εισβολών στο σύστημα από hackers αφού μας ενημερώνει για κάθε ύποπτη κίνηση που επιχειρείται για πρόσβαση σε δεδομένα του υπολογιστή μας και μας ρωτάει αν επιτρέπουμε την ολοκλήρωσή της ή όχι.
Μία τυπική διάταξη firewall.



Τέλος, μια πολύ καλή συμβουλή είναι να λαμβάνουμε πολύ τακτικά, ίσως και καθημερινά, **αντίγραφα ασφαλείας (back-up)** των αρχείων μας, σε εξωτερικό σκληρό δίσκο, έτσι ώστε ακόμα και στην ακραία περίπτωση που χάσουμε σημαντικά αρχεία από την επίθεση κάποιου ιού, να μπορέσουμε να τα ανακτήσουμε άμεσα.

Βιβλιογραφία

Επιμορφωτικό υλικό για την εκπαίδευση των επιμορφωτών στα Πανεπιστημιακά Κέντρα Επιμόρφωσης, 2011, *Τεύχος 1: Γενικό Μέρος*, Β΄ Έκδοση Αναθεωρημένη και Βελτιωμένη, Πάτρα, Μάιος 2011.

Δικτυογραφία

http://www.pctools.com/free-antivirus/
http://computer.howstuffworks.com/virus.htm
http://www.noadware.net/research/
http://www.go-online.gr/ebusiness/specials/article.html?article_id=409
http://www.go-online.gr/ebusiness/specials/article.html?article_id=1173
http://it.ccri.edu/helpdesk/spyware-faqs.shtml
http://www.personalfirewall.comodo.com
http://computer.howstuffworks.com/firewall.htm
http://www.securelist.com/en/threats/detect
http://www.cknow.com/cms/vtutor/types-of-viruses.html
http://searchsecurity.techtarget.com/definition/Elk-Cloner
http://el.wikipedia.org/wiki/Firewal
http://el.wikipedia.org/wiki/Δούρειος_Ίππος_(Λογισμικό)
http://el.wikipedia.org/wiki/Ιός_(πληροφορική)
http://en.wikipedia.org/wiki/Antivirus_software
http://away.gr/2009/12/05/virus-trojan-horse-worms-spyware/

Antivirus

http://www.avira.com/en/avira-free-antivirus
http://free.avg.com/ww-en/homepage
http://gr.norton.com/antivirus/