

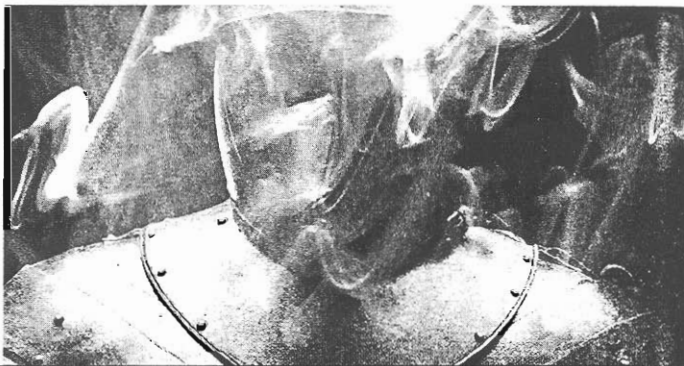
**Σ**ήμερα δεν υπάρχει PC που να μην είναι συνδεδεμένο στο Internet, όπως δεν υπάρχει χρήστης PC που να μην έχει ασχοληθεί, στον έναν ή στον άλλο βαθμό, με ζητήματα «δικτυακής ασφάλειας». Η συνήθης αφορμή είναι ένας νέος ιός, κάποιο worm ή ακόμη και ένας dialer, που από καθαρή απροσεξία αφήσαμε να φωλιάσει στο PC μας. Τους τελευταίους μήνες έχει προστεθεί άλλος ένας πανοκέφαλος στους διαχειριστές δικτύων, όπως επίσης και στους μεμονωμένους χρήστες. Αναφερόμαστε στο κατακλυσμικό φαινόμενο του spam, με άλλα λόγια στη μαζική και αδιάκριτη αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας. Μηνύματα που στη συντριπτική τους πλειονότητα χαρακτηρίζονται ως άχρηστα/παραπληρητικά/προσβλητικά/γελοία/ενοχλητικά – εδώ βάλτε το δικό σας χαρακτηρισμό. Το πρόβλημα του spam είναι πλέον τόσο έντονο, ώστε να γίνονται συζητήσεις ακόμη και για τη χρέωση της αποστολής e-mail, με στόχο την αποθάρρυνση των επαγγελματιών spammer.

**ΕΝΑ ΠΡΟΒΛΗΜΑ, ΔΙΑΦΟΡΕΤΙΚΕΣ ΣΤΑΣΕΙΣ.** Αν κρίνουμε από την καθημερινή εμπειρία καθώς και από τα δεκάδες σχετικά e-mail που λαμβάνουμε κάθε μήνα, η στάση που τηρούν οι χρήστες απέναντι στο υπαρκτό πρόβλημα της δικτυακής ασφάλειας καθορίζει σε σημαντικό βαθμό το πόσο ασφαλείς είναι. Σε γενικές γραμμές, λοιπόν, θα τολμούσαμε να κατατάξουμε τους χρήστες –χωρίς να εξαιρούμε εαυτούς– στις επόμενες τρεις κατηγορίες.

**ΑΔΙΑΦΟΡΟΣ, ΑΡΝΗΤΙΚΟΣ.** Πιστεύει ότι όλη αυτή η φιλοσοφία περί ιών, trojan, spam και τα συναφή υπάρχει και συντηρείται μόνο και μόνο για να πουλούν οι εταιρείες λογισμικού τα προϊόντα τους. Ο συγκεκριμένος χρήστης ίσως έχει εγκατεστημένο κά-

άχρισαν να κάνουν τα τρελά τους». Όταν πια ένας φίλος ή τεχνικός του ανοίξει τα μάτια, τότε ο άνθρωπός μας μάλλον θα μεταπηδήσει σε μία από τις ακόλουθες δύο κατηγορίες (πιθανότατα στην αμέσως επόμενη).

**ΠΑΡΑΝΟΪΚΟΣ, ΑΓΧΩΜΕΝΟΣ.** Του λείπουν βασικές τεχνικές γνώσεις και υποψιάζεται τους πάντες και τα πάντα – αυτός δεν πρόκειται να πιαστεί ποτέ κορόιδο! Στο PC του έχει εγκατεστημένες –τουλάχιστον– τις επόμενες εφαρμογές και εργαλεία: AntiVirus, AntiSpam, Firewall, AntiSpyware, Anonymizer. Όλα τα σχετικά προγράμματα τρέχουν διαρκώς στο υπόβαθρο και αναβαθμίζονται δύο φορές την ημέρα, αυτόματα, από τους αντίστοιχους σέρβερ. Ταυτόχρονα, αστυνομεύουν διαρκώς τον υπολογιστή εξοστρακίζοντας με επιτυχία τις επιθέσεις των cracker και απομακρύνοντας επικίνδυνους ιούς – ή τουλάχιστον αυτό πιστεύει ο φίλος μας. Την cache του browser την αδειάζει συχνά πυκνά, σβήνει όλα τα cookies –ακόμη και τα πραγματικά χρήσιμα– και οποιοδήποτε άλλο αρχείο θέλει να διαγράψει το περνά



**Εάν μέχρι σήμερα οι απερίσκεπτες ενέργειες έμεναν ατιμώρητες, σύντομα το παραμικρό λάθος θα το πληρώνουμε πολύ ακριβά.**

ποιο πρόγραμμα AntiVirus, αφού πρακτικά μόνο αυτό χρειάζεται. Δεν το ενημερώνει τακτικά – ειδικρινά, δεν βλέπει το λόγο να «τρελαίνεται». Περιττό βέβαια να πούμε ότι δεν χρησιμοποιεί προσωπικό Firewall. Τα Firewall είναι μόνο για τις μεγάλες εταιρείες και οργανισμούς, που, ομολογουμένως, διατρέχουν έναν κάποιον κίνδυνο. Εκείνος είναι ένας απλός χρήστης που κοιτάζει τη δουλειά του χωρίς να ενοχλεί κανέναν – ποιος έχει λόγο να ασχοληθεί μαζί του; Πάντως το πρόσφατο φαινόμενο του spam τον έχει ελαφρώς θορυβήσει. Απρόθυμα εγκατέστησε ένα εργαλείο AntiSpam αλλά προς όχι-και-τόσο-μεγάλη του έκπληξη διαπίστωσε ότι δεν βρίσκει από μόνο του όλα τα άχρηστα μηνύματα. Τι τα θέλεις, ντόρος να γίνεται για να πουλούν οι εταιρείες λογισμικού...

Τελικά θα έρθει η στιγμή που ο φίλος μας θα κολλήσει ιό/worm/trojan. Παρατηρώντας την κάπως παράξενη/απρόβλεπτη/χαστική συμπεριφορά του μηχανήματος, θα υποθέσει ότι πρόκειται περί μηχανικής βλάβης ή ότι τα Windows «πάλη

από ειδικό πρόγραμμα που καθιστά αδύνατη την επαναφορά του, ακόμη και με χρήση εκείνων των σούπερ εξειδικευμένων εργαλείων ανάκτησης που έχουν στο FBI. Εννοείται βέβαια ότι γι' αυτό –μα ποτέ– δεν στέλνει e-mail σε μη κρυπτογραφημένη μορφή, ακόμη και όταν πρόκειται να κανονίσει τις λεητομέρειες για την έξοδο του Σαββατοκύριακου. Προς το παρόν χρησιμοποιεί ένα απλό σύστημα συμμετρικής κρυπτογραφίας –ή όπως αλλιώς το λένε, τέλος πάντων– γιατί το PGP είναι κάπως περίπλοκο...

Κάποια στιγμή, ζώντας ένα σκληρό παρήληρημα ονσφόλλειας, εγκαθιστά στο PC του δεύτερο AntiVirus και δεύτερο Firewall – έτσι, για πρόσθετη ασφάλεια! Στην επόμενη επανεκκίνηση τα Windows δικαιολογημένα αυτοσπαραγγαλίζονται, ο φίλος μας στον πανικό του δεν σκέφτεται να μπει σε Safe Mode και να απεγκαταστήσει τις περιττές εφαρμογές, οπότε βυθίζεται στο σκοτάδι και στην απελπισία. Όλο το βράδυ ξενυχτά εγκαθιστώντας τα πάντα, λειτουργικό και εφαρμογές, από την αρχή.

Τα ημερώματα γεννάται στο νου του μια φριχτή υποψία. Κάτι κάνει εντελώς λάθος — τι ακριβώς δεν μπορεί να διακρίνει. Δύο ημέρες μετά ίσως αρχίσει τη μακρόσυρτη και επίπονη πορεία ένταξης προς την τρίτη και τελευταία κατηγορία.

**ΕΝΗΜΕΡΩΜΕΝΟΣ, ΜΕΤΡΗΜΕΝΟΣ.** Ο χρήστης της κατηγορίας διαθέτει ένα στέρεο θεωρητικό υπόβαθρο περί δικτύων και Internet, έχει μια καλή ιδέα για το πώς διαδίδονται ιοί, worm και άλλα κακόβουλα προγράμματα, ξέρει πώς να αποφεύγει τις κακοτοπιές στο Διαδίκτυο, ενώ γνωρίζει τις αρετές και τις αδυναμίες των εφαρμογών ασφαλείας που χρησιμοποιεί. Σπάνια αφήνει απείραχτες τις προκαθορισμένες ρυθμίσεις των προγραμμάτων, επιδιώκοντας να βελτιστοποιήσει τη συμπεριφορά τους για τις δικές του, ιδιαίτερες ανάγκες. Αν και έχει εγκατεστημένες εφαρμογές ασφαλείας διαφόρων ειδών, στο υπόβαθρο του λειτουργικού συστήματος έχει μονίμως φορτωμένες μόνο εκείνες που πραγματικά χρειάζεται: Firewall, AntiVirus και AntiSpam. Όλες τις υπόλοιπες τις εκτελεί περιστασιακά και κατ' απαίτηση.



Φροντίζει να ενημερώνει τακτικά λειτουργικό σύστημα και εφαρμογές, κατεβάζοντας και εγκαθιστώντας τα αντίστοιχα patches βελτιώσεων. Με λίγα λόγια ο φίλος μας ξέρει πολύ καλά τι κάνει. Πρακτικά, η ασφάλεια του μηχανήματός του θα υποβαθμιστεί αποκλειστικά και μόνο από δική του απροσεξία ή αμέλεια.

**Ο ΠΡΑΓΜΑΤΙΚΟΣ ΚΟΣΜΟΣ, ΔΙΚΤΥΩΜΕΝΟΣ.** Όπως και στον πραγματικό κόσμο, έτσι και στο Διαδίκτυο υπάρχουν οι νομοταγείς πολίτες, όπως υπάρχουν και οι όχι-και-τόσο νομοταγείς. Μία από τις προσφιλέστερες ασχολίες των τελευταίων είναι να δυσκολεύουν τη ζωή των πρώτων, έστω και από καθαρή αφέλεια ή ανωριμότητα. Οι «ατίθασοι» χωρίζονται στους cracker και στα λεγόμενα script kiddies. Ένας cracker συνήθως έχει υψηλότερο επίπεδο τεχνικής κατάρτισης. Όλη του την ενεργητικότητα τη διοχετεύει σε δικτυακές ενσασορήσεις που ξεκινούν από τις γκρίζες περιοχές της νομιμότητας και φτάνουν έως τις πιο σκοτεινές. Ενίοτε οι cracker κάνουν ό,τι κάνουν απλά και μόνο για την πρόκληση και την απόκτηση γνώσης, άλλότες πάλι οι σκοποί τους είναι περισσότερο συγκεκριμένοι και... δόλιοι.

Ο μέσος χρήστης είναι μάλλον απίθανο να τύχει της προσοχής ενός αληθινού cracker. Αντίθετα, τα script kiddies πραγματοποιούν

σύν ως επί το πλείστον τυφλά χτυπήματα. Ένα οποιοδήποτε σύστημα, σε οποιοδήποτε μέρος του κόσμου είναι υποψήφιος στόχος, αρκεί να έχει υποβαθμισμένη ασφάλεια. Με λίγα λόγια, τα script kiddies αποτελούν υπαρκτό κίνδυνο για κάθε φιλήσυχο δικτυακό πολίτη. Ίσως όμως ο μεγαλύτερος κίνδυνος να προέρχεται από εμάς τους ίδιους και τις συνήθειές μας, από την απροθυμία που επιδεικνύουμε στη λήψη απλών αλλά αποτελεσματικών μέτρων ασφαλείας. Παρά τις συχνότητες αναβοθμίσαις και τις επιδιορθώσεις ασφαλείας που εκδίδουν οι εταιρείες λογισμικού, παρά τους βροντερούς τίτλους και τα πρωτοσέλιδα, πολλά μεμονωμένα συστήματα και σέρβερ επιδεικνύουν αδικαιολόγητα κενά ασφαλείας. Άλλοτε, για όλες τις περιπτώσεις στις οποίες κατά καιρούς μηλέκουμ φταίει μια γενικότερη αντίληψη στον κόσμο των υπολογιστών, που αποθεώνει την ευκολία χρήσης βάζοντας σε δεύτερη μοίρα οποιαδήποτε άλλη προτεραιότητα. Ίσως κάποια μέρα το λογισμικό να γίνει πανεύκολο στη χρήση και ταυτόχρονα αληθινά ασφαλές. Μέχρι να έρθει αυτή η μέρα, να θυμάστε ότι κάποιοι εργάζονται πυρετωδώς προκειμένου να μετατρέπουν την ευκολία σε αδυναμία.

**ΜΕ ΨΥΧΡΑΙΜΙΑ ΚΑΙ ΣΥΝΕΣΗ.** Οι προσοίτες ευρυζωνικές συνδέσεις έχουν ήδη αρχίσει να κάνουν το πρώτο τους δειλό βήματα και στη χώρα μας. Σύντομα, ολόένα και περισσότεροι υπολογιστές θα είναι διαρκώς on-line, προσφέροντας στους ιδιοκτήτες τους πρωτόγνωρες ιντερνετικές εμπειρίες. Όμως μαζί με τα μεγάλα οφέλη έρχονται και τα μεγάλα ρίσκα. Εάν μέχρι σήμερα οι απερίσκεπτες ενέργειες έμεναν συχνά στιμώρητες —κυρίως λόγω της παροδικότητας των συνδέσεων—, αύριο είναι πολύ πιθανόν το παραμικρό λάθος να το πληρώνουμε πανάκριβα! Και όμως, αν αποκτήσουμε μερικές βασικές γνώσεις και φροντίζουμε για την τακτική μας ενημέρωση, δεν θα έχουμε κανένα λόγο να αισθανόμαστε ανασφαλείς. Εννοείται, βέβαια, ότι οφείλουμε να εξοικειωθούμε και με τις κατάλληλες εφαρμογές λογισμικού. Άλλες θα μοιάζουν περισσότερο φιλικές σε μια πρώτη επαφή, άλλες όχι. Αυτό που έχει σημασία είναι σε κάθε περίπτωση να καταλαβαίνουμε τι ακριβώς κάνουμε, ώστε να ξεχωρίζουμε εκείνο το πρόγραμμα που ταιριάζει καλύτερο στις ιδιαίτερες ανάγκες μας και να το εκμεταλλευόμαστε όσο το δυνατόν περισσότερο. Αγαπητοί φίλοι, στις επόμενες σελίδες δεν σκοπεύουμε να προβούμε σε μια απλή παράθεση προγραμμάτων για τη δικτυακή ασφάλεια, αν και όπως πιθανότατα έχετε ήδη διαπιστώσει κάθε άλλο παρά μας λείπουν (είναι οργανωμένα ανά κατηγορία χρήσης στο φάκελο «Security» του CD «Εφαρμογές Ασφαλείας»). Αντίθετα, επιχειρούμε να κάνουμε μια σφαιρική όσο και επικεντρωμένη επίθεση σε τέσσερις μεγάλες υποκατηγορίες του θέματος της διαδικτυακής ασφαλείας: Αντιμετώπιση κινδύνων που προέρχονται από το e-mail, Επιλογή κατάλληλης εφαρμογής Firewall, Ανωνυμία και προστασία ιδιωτικότητας, Κρυπτογράφηση περιεχομένου και έλεγχος αυθεντικότητας. Σε κάθε περίπτωση, πέρα από τις γενικές τοποθετήσεις και συμβουλές, παρουσιάζουμε δύο ή περισσότερες εφαρμογές, άλλες εντελώς δωρεάν και άλλες για δοκιμαστική χρήση, οι οποίες εκπληρώνουν στο ακέραιο την αποστολή τους.

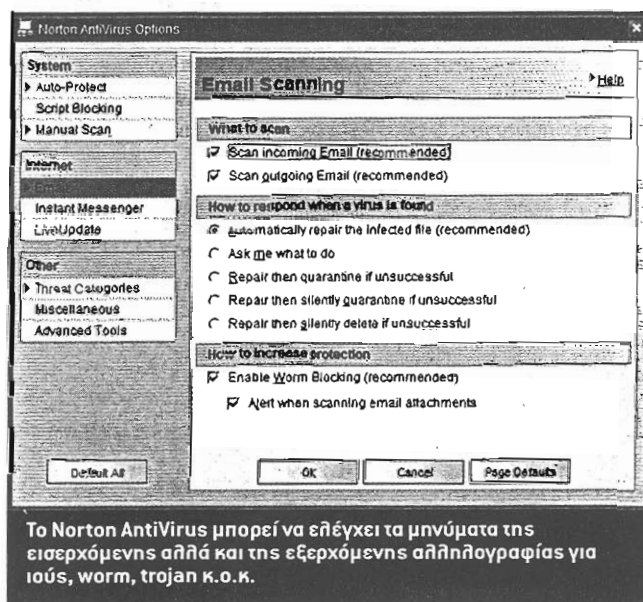
Καλή ανάγνωση και καλή διασκέδαση!

# ΕΝΟΧΛΗΤΙΚΟ, ΕΠΙΚΙΝΔΥΝΟ E-MAIL

Το ηλεκτρονικό ταχυδρομείο, η κατεξοχήν «δολοφονική εφαρμογή» του Internet, αποτελεί σήμερα το προσφιλέστερο μέσο για τη διάδοση ιών, πάσης φύσεως ζωυφίων, καθώς και για τη διακίνηση απίστευτων ποσοτήτων σαβούρας! Πώς θα πάρουμε πίσω το παλιό, καλό e-mail;

ΠΡΟΓΡΑΜΜΑΤΑ ΑΠΟ ΤΟ CD  
Φύκελοι Security/AntiVirus,  
Security/AntiSpam

**Μ**έχρι πριν από μία αιωνιότητα, δηλαδή πριν από οκτώ με εννέα περίπου χρόνια, οι ιοί των υπολογιστών διαδίδονταν κυρίως με την ανταλλαγή δισκετών. Τα σκουλήκια (worms) και οι δούρειοι ίπποι (trojan horses) ήταν γνωστά μόνο σε μια μικρή ελίτ από «γκουρού», οι οποίοι άλλοτε πειραματίζονταν και άλλοτε τρομοκρατούσαν ανυποψίαστους χρήστες, ελέγχοντας τους υπολογιστές τους από απόσταση. Σήμερα, όλα αυτά τα κακόβουλα προγράμματα και ζωύφια διαδίδονται κυρίως μέσω e-mail. Την ίδια στιγμή, στο στρότοπε των καλών, οι εταιρείες κατασκευής αντι-ιικών προγραμμάτων έχουν εξελίξει σε σημαντικό βαθμό τα προϊόντα τους, ώστε να ανιχνεύουν και να εξουδετερώνουν ιούς, worm—συχνά και trojan horse— από τη μνήμη του υπολογιστή, από τα αρχεία που είναι αποθηκευμένα στους σκληρούς δίσκους, καθώς και από τα συνημμένα της εισερχόμενης αλληλογραφίας. Στην πλειονότητα των περιπτώσεων, μεταξύ των συνημμένων ενός e-mail είναι πιθανόν να κρύβεται και κάποιο worm. Άπαξ και ενεργοποιηθεί, π.χ., στην προσπάθειά μας να δούμε τα περιεχόμενα του συνημμένου, το πρώτο πράγμα που θα κάνει είναι να στείλει ένα αντίγραφο του εαυτού του στους χρήστες που θα βρει στο βιβλίο διευθύνσεων του mail client. Το τι θα κάνει στη συνέχεια ποικίλλει ανά περίπτωση. Ίσως προκαλέσει μία καταστροφή, π.χ., διαγράφοντας αρχεία συγκεκριμένου φορμά. Από την άλλη, ίσως να απλώς καθίσει ήσυχο και να ενεργοποιηθεί σε συγκεκριμένη ημερομηνία. Τα τελευταία τέσσερα περίπου χρόνια είναι πολύ της μόδας οι λεγόμενες επιθέσεις DDoS (Distributed Denial of Service). Η ιδέα είναι απλή. Σε μια προκαθορισμένη ημερομηνία, προγράμματα τύπου worm που μέχρι εκείνη τη στιγμή περίμεναν σιωπηρά στα μηχανήματα ξενιστές, ενεργοποιούνται και όλα μαζί βομβαρδίζουν με αιτήσεις σύνδεσης ένα συγκεκριμένο διακομιστή. Εκείνος, επιχειρώντας να ανταποκριθεί σε όλες τις αιτήσεις, σύντομα καταλήγει ανήμπορος, αφού αδυνατεί να κάνει οποιαδήποτε χρήση εργασίας. Η προετοιμασία μιας επίθεσης DDos είναι αφενός σχετικά απλή υπόθεση, αφετέρου η αποτελεσματικότητά της είναι σχεδόν διασφαλισμένη. Ως πρόσθετο «όφελος», ο εντοπισμός του υπολογιστή που τα ξεκίνησε όλα είναι πρακτικά αδύνατος.



Μεταξύ μας, όταν σήμερα κάποιος «κοιλάει» ιό, worm ή οτιδήποτε άλλο από το e-mail του, αυτό οφείλεται καθαρά στη δική του απροσεξία ή/και αμέλεια. Βεβαίως, δεν πρέπει να ξεχνάμε και την περίπτωση που σε μια εταιρεία ο υπεύθυνος διαχειριστής συστήματος είναι κάπως... ανεύθυνος. Ίσως πάλη το PC των εργαζομένων να μην είναι εξοπλισμένα με πρόγραμμα AntiVirus, π.χ., λόγω κάποιας πολιτικής περιορισμού των εξόδων. Τελικά, σκοποθώπας κανείς μερικούς απλούς κανόνες, είναι σχεδόν 100% προστατευμένος από τους κινδύνους του e-mail. Μόνη περίπτωση να κολλήσει κάτι είναι να «χτυπηθεί» από έναν ολοκαίνουργιο ιό ή worm, ο οποίος είναι ακόμη άγνωστος στο αντι-ιικό ή ο χρήστης του δεν πρόλαβε να πάρει το αντίστοιχο update από την κατασκευάστρια εταιρεία. Συνοψίζοντας, όσον αφορά στο e-mail, καλό είναι να εφαρμόζουμε τους ακόλουθους κανόνες:

- Να εφοδιαστούμε με εφαρμογή AntiVirus, η οποία θα έχει, μεταξύ άλλων, ικανότητα ελέγχου της εισερχόμενης αλληλογραφίας. Το πρόγραμμα θα πρέπει να λειτουργεί διαρκώς στο υπόβαθρο του λειτουργικού συστήματος.
- Ανά τακτά χρονικά διαστήματα να ενημερώνουμε το AntiVirus, ώστε να γνωρίζει τους τελευταίους ιούς, worm, trojan horse κ.ο.κ. Σχεδόν όλα τα προγράμματα AntiVirus προσφέρουν

Επειτα από πλήρη έλεγχο του συστήματος, το Norton AntiVirus εντόπισε ένα δυνητικά επικίνδυνο εκτελέσιμο αρχείο. Στην πραγματικότητα πρόκειται για ένα εργαλείο ελέγχου της αποτελεσματικότητας των Firewall (βλ. παρακάτω), το οποίο πράγματι υλοποιεί «ύπουλες» τεχνικές! Κατά τα άλλα, είναι εντελώς ακίνδυνο.

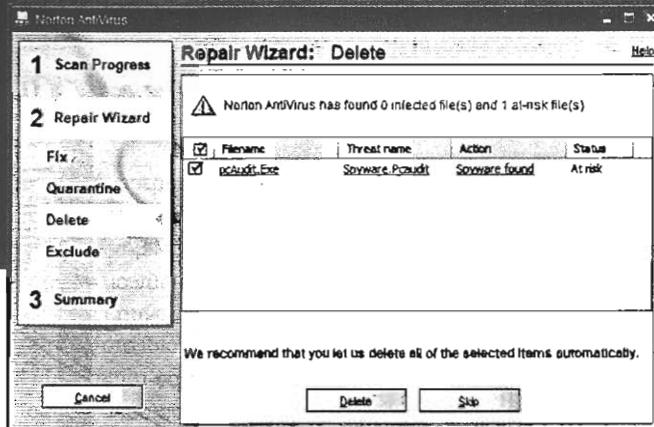
τη δυνατότητα αυτόματης ενημέρωσης από τους δικτυακούς τόπους των εταιρειών.

- Να μην ανοίγουμε ποτέ ένα συνημμένο, όταν προέρχεται από αποστολέα που δεν γνωρίζουμε ή/και δεν εμπιστευόμαστε. Επίσης, σε καμία περίπτωση να μην το ανοίγουμε αν για οποιονδήποτε λόγο μάς φαίνεται κάπως «παράξενο».

- Να ρυθμίσουμε τα Windows ώστε να δείχνουν τις επεκτάσεις όλων των αρχείων. Ακολουθήστε, π.χ., τη διαδρομή <Control Panel→Appearance and Themes→Folder Options→View> και φροντίστε ώστε το κουτάκι «Hide extensions for know file types» να είναι ρεχικό. Μια κάπως παλιό αλλήλο αποτελεσματική τακτική των «ανήσυχων» χρηστών είναι να δίνουν στο κακόβουλο αρχείο ένα όνομα της μορφής picture.jpg.exe. Εάν τα Windows κρύβουν τις καταλήξεις γνωστών αρχείων, ο ανυποψίαστος χρήστης θα δει ένα όνομα της μορφής picture.jpg. Εάν το «χτυπήσει» για να δει την εικόνα, αυτό που θα πετύχει είναι να εκτελέσει κάποιο ιό, worm ή trojan horse. Σημειώστε, τέλος, ότι ορισμένα προγράμματα αλληλογραφίας έχουν τη δυνατότητα να βάζουν σε каранτίνα δυνητικά επικίνδυνα συνημμένα αρχεία (π.χ., με καταλήξεις EXE, VBS κ.ά.)

- Εάν κάποιος ISP δεν έχει εγκατεστημένα εργαλεία AntiVirus στους διακομιστές αλληλογραφίας του, να μην τον προτιμήσουμε. Σε περίπτωση που ο τωρινός ISP δεν έχει AntiVirus, καλό είναι να τον «πιέσουμε» ώστε να εγκαταστήσει κάποιο. Πάντως, άσχετα από το τι (δεν) κάνει ο εκάστοτε ISP, εμείς από την πλευρά μας πρέπει να έχουμε οπωσδήποτε αντι-ιικό στο PC μας.

**Η ΜΑΣΤΙΓΑ ΤΟΥ SPAM!** Ρίχνοντας κανείς μια ματιά στο περιεχόμενο των spam mail, επόμενο είναι να αναρωτηθεί γιατί οι spammer περιμένουν να βγάλουν χρήματα όταν, αν μη τι άλλο, παθαίνουν από τα μηνύματά τους είναι κατάφορα παραπληκτικά! Η λογική πάνω στην οποία βασίζουν τη δραστηριότητά τους είναι σχετικά απλή και ακούει στο όνομα «μαζική αποστολή». Υποθέστε ότι ανακαλύπτω μια ξεχασμένη συνταγή κέικ της γιαγιάς μου. Η φίλη μου το μαθαίνει και κάποια στιγμή την ακολουθεί, ψήνοντας ένα νοστιμότατο κέικ (εγώ με τίποτε δεν θα μπορούσα να κάνω κάτι τέτοιο). Ενθουσιασμένη μου λέει ότι άντα θα μπορούσα να την πουλήσω (τη συνταγή, όχι την ίδια), ας πούμε, για πέντε ευρώ. Με πείθει. Ανοίγουμε τότε το βιβλίο διευθύνσεων του mail client και βρίσκουμε όλα τα e-mail φίλων, γνωστών και συνεργατών. Μου δίνει και η φίλη μου αρκετές δικές τις διευθύνσεις και αμέσως αμέσως μαζεύουμε καμιά εκατοστή. Στη συνέχεια στέλνουμε σε όλους τους παραλήπτες το ίδιο, σύντομο e-mail, πληροφορώντας τους για τη θαυμάσια συνταγή και για την πρόθεσή μας να την αποκαλύψουμε, έναντι του συμβολικού ποσού των πέντε ευρώ. Μία εβδομάδα αργότερα ένας από τους εκατό απαντά στο e-mail, εκδηλώνοντας την πρόθεσή του να την αγοράσει. Τότε εγώ σκέφτομαι ότι έβγαλα πέντε ευρώ, πρακτικά χωρίς να κάνω τίποτε. Αν λοιπόν στείλω το ίδιο μήνυμα σε χίλιους, δέκα χιλιάδες ή ένα εκατομμύριο παραλήπτες, τηρουμένων των αναλογιών ενδέχεται να κερδί-



σω 50, 500 ή 5.000 ευρώ αντίστοιχα – πάντα χωρίς να κάνω τίποτε το ιδιαίτερο! Το πρόβλημα είναι ότι δυσκολεύομαι κάπως να βρω τόσο πολλές διευθύνσεις. Βλέπετε, δεν είμαι επαγγελματίας spammer (ούτε καν ερασιτέχνης είμαι).

Έτσι όπως έχει εξελιχθεί η κατάσταση με το spam, αν δεν θέλουμε να σκοτώνουμε το χρόνο μας ψαρεύοντας χρήσιμα e-mail μέσα από έναν ωκεανό άχρηστων, τότε οφείλουμε να τηρούμε ευλαβικά τους επόμενους κανόνες.

- Κάθε φορά που συμπληρώνουμε μια φόρμα on-line, δεν πρέπει ποτέ να δίνουμε το επίσημο e-mail μας. Αρκετές εταιρείες πουλούν λίστες με ηλεκτρονικές διευθύνσεις σε τρίτους, παρά τα αναγραφόμενα στα σχετικά license agreement. Ακόμη καλύτερα, καλό είναι να δίνουμε ένα ανύπαρκτο e-mail, π.χ., κάτι σαν diespammers@everywhere.net. Αν πάλλι απαιτείται μια έγκυρη διεύθυνση, π.χ., για την αποστολή ενός σειριακού αριθμού, τότε καλύτερα μπορούμε να δίνουμε τη διεύθυνση ενός λογαριασμού Web, που διατηρούμε για παρόμοιες περιπτώσεις.

- Όταν κάνουμε anonymous login σε κάποιο διακομιστή FTP, περριτό να πούμε ότι δεν πρέπει να δίνουμε κάποια υποκτική διεύθυνση e-mail (η ανώνυμη σύνδεση σε διακομιστές FTP γίνεται με username anonymous και password μια οποιαδήποτε διεύθυνση e-mail).

- Να αποφεύγουμε την «ανάρτηση» μιας διεύθυνσης e-mail σε δικτυακούς τόπους. Επίσης, όποτε γραφόμαστε σε κάποια υπηρεσία on-line, π.χ., σε ένα club ανθρώπων με παρόμοια ενδιαφέροντα, να ζητάμε την απόκρυψη της ηλεκτρονικής μας διεύθυνσης (συνήθως παρέχεται σχετική δυνατότητα). Οι spammer χρησιμοποιούν ειδικά προγράμματα-ρομπότ, τα λεγόμενα spambot, τα οποία διατρέχουν τον κυβερνοχώρο ψάχνοντας και αλιεύοντας διευθύνσεις e-mail από διάφορες ιστοσελίδες. Πάντως, οι spammer είναι τελικά πιθανού να βρουν την αληθινή μας διεύθυνση, αφού συχνά εξαπολύουν σε διάφορους διακομιστές αλληλογραφίας τα λεγόμενα dictionary attacks: Με κατάλληλα προγράμματα δοκιμάζουν τεράστιους αριθμούς διευθύνσεων της μορφής username@domain, πετώντας τις ανύπαρκτες και κρατώντας τις υπαρκτές.

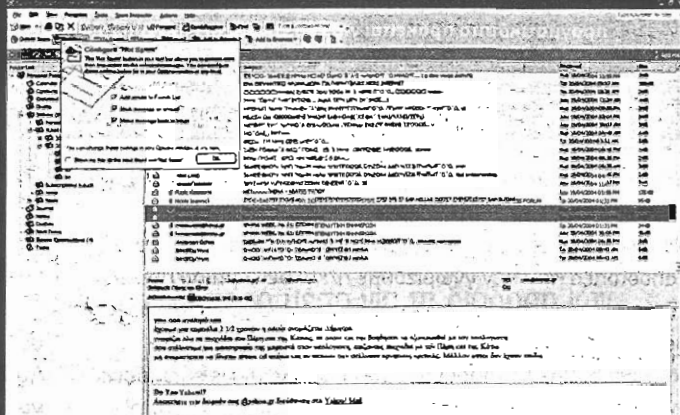
- Ποτέ να μην κάνουμε «unsubscribe» από λίστες διευθύνσεων για την αποστολή spam. Και μόνο που θα προσπαθήσουμε, ο spammer στην άλλη άκρη θα δει ότι η διεύθυνση αλληλογραφίας που ηλεκτροποήσαμε σε κάποια θυρίδα «unsubscribe» είναι ενεργή, οπότε: α. θα συνεχίσει να στέλνει spam, β. θα προωθήσει τη διεύθυνσή μας και σε άλλους spammer.

- Προτείνεται να ρυθμίσουμε το πρόγραμμα αλληλογραφίας μας ώστε να μην εμφανίζει από μόνο του τα περιεχόμενα μηνυμάτων σε HTML (εναλλακτικά, μπορούμε να

# ΑΦΙΕΡΩΜΑ | ANTIVIRUS ΚΑΙ ANTISPAM

απενεργοποιήσουμε την αυτόματη προεπισκόπηση των μηνυμάτων). Πολλά spam mail είναι σε μορφή HTML και περιλαμβάνουν τα λεγόμενα Web bug. Με λίγα λόγια, τα Web bug είναι τρικ που χρησιμοποιούν οι spammer προκειμένου να ελέγχουν αν μια διεύθυνση αποστολής είναι ενεργή.

- Εάν ο ISP μας δεν έχει ακόμη εγκαταστήσει πρόγραμμα AntiSpam στους διακομιστές αλληλογραφίας του, ίσως αξίζει να τον προτρέψουμε ώστε να το κάνει.
- Απαραίτητως να εγκαταστήσουμε στον υπολογιστή μας ένα καλό πρόγραμμα AntiSpam, με δυνατότητες αυτόματης εκμάθησης.



Το Spam Inspector μόλις έβαλε σε καραντίνα ένα μεγάλο αριθμό μηνυμάτων spam. Μεταξύ αυτών υπήρχαν και δύο e-mail που χαρακτηρίστηκαν ως spam χωρίς στην πραγματικότητα να είναι. Έτσι, τα προσθέτουμε στη λίστα «Fiends» κάνοντας ένα κλικ στο κουμπάκι «Not Spam!».



# ΑΜΕΙΛΙΚΤΟΣ ΣΥΝΟΡΙΟΦΥΛΑΚΑΣ

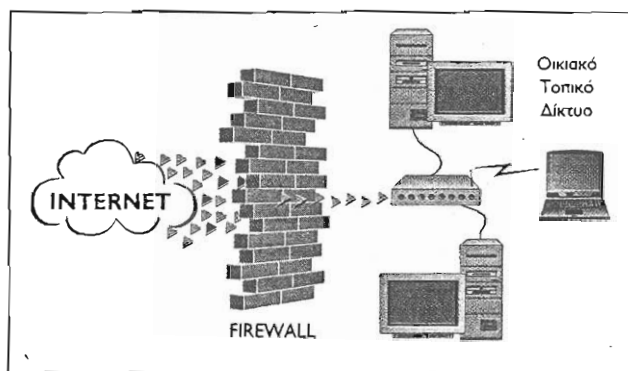
Ένα PC είναι απόλυτα ασφαλές όταν δεν συμμετέχει σε κανένα τοπικό δίκτυο ούτε βεβαίως και στο Internet. Στην πράξη, επιστρατεύοντας ένα ικανό πρόγραμμα Firewall παραμένουμε σε επαφή με τον υπόλοιπο κόσμο και ταυτόχρονα φτάνουμε σε ένα ιδανικό επίπεδο ασφαλείας. Υπό προϋποθέσεις.

ΠΡΟΓΡΑΜΜΑΤΑ ΑΠΟ ΤΟ CD

ΦΑΚΕΛΟΙ SECURITY/FIREWALLS, SECURITY/TESTING

**Α**ρκετοί στο άκουσμα και μόνο της λέξης Firewall σκέφτονται μεγάλα εταιρικά δίκτυα υψηλής ασφαλείας. Η παρουσία ενός Firewall «μπροστά» από έναν υπολογιστή ή ένα μικρό οικιακό δίκτυο τους φαίνεται τουλάχιστον περιττή. Πράγματι, ένα PC που συνδέεται στο Internet μέσω γραμμής PSTN ή ISDN και για λίγες μόνο ώρες την εβδομάδα ίσως μπορεί να παραμείνει ασφαλές χωρίς να προστατεύεται από Firewall. Βλέπετε, ακόμη και αν κάποιο παιδάκι με μπόλικο ελεύθερο χρόνο «σκανάρει» το PC και εντοπίσει προβλήματα ασφαλείας, όταν επιχειρήσει να εξαπολύσει την πραγματική επίθεση, η διεύθυνση IP του μηχανήματος-στόχου κατά πάσα πιθανότητα θα έχει αλλάξει. Υπάρχει όμως και ένα άλλο θέμα: Ο χρήστης που δεν χρησιμοποιεί Firewall οφείλει να είναι 100% βέβαιος ότι το PC του δεν φιλοξενεί κάποιο trojan horse. Βεβαίως, αυτό με τη σειρά του σημαίνει ότι οφείλει να γνωρίζει τι κρύβει στα εσώψυκά του καθένα από εκείνα τα εκκληνηκικά προγράμματα που βρίσκει στο Internet και πρόθυμα εγκαθιστά, προκειμένου να τα δοκιμάσει, να παίξει μαζί τους ή απλώς να κάνει τη δουλειά του. Εναλλακτικά, ο φίλος μας θα μπορούσε να εγκαταστήσει ένα προσωπικό Firewall και να ησυχάσει!

**ΤΙ ΕΙΝΑΙ ΤΟ FIREWALL;** Μιλώντας γενικά, το Firewall είναι μια εφαρμογή λογισμικού ή συσκευή υλικού που παρεμβάλλεται

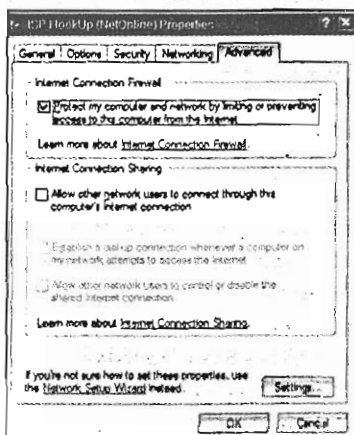


Τα Firewall προστατεύουν ένα δίκτυο από κάποιο άλλο, υποβάλλοντας τα διερχόμενα πακέτα πληροφορίας σε μια σειρά από ελέγχους. Στο σχήμα φαίνεται μια συσκευή Firewall, η οποία προστατεύει ένα μικρό οικιακό δίκτυο από το Internet.

μεταξύ δύο διαφορετικών δικτύων και φιλτράρει τα διακινούμενα πακέτα πληροφορίας. Το φιλτράρισμα γίνεται με βάση ένα σύνολο κριτηρίων που ορίζει ο διαχειριστής του Firewall. Κάθε φορά που ένα δικτυακό πακέτο αφήνει ανικανοποίητο τουλάχιστον ένα από τα κριτήρια, το Firewall εμποδίζει τη διέλευσή του. Αντίθετα, όταν το πακέτο ικανοποιεί όλα ανεξαιρέτως τα κριτήρια, τότε το Firewall το αφήνει να διέλθει. Εξετάζοντας τα προηγούμενα από μια ελαφρώς διαφορετική οπτική, διαπιστώνουμε ότι ένα Firewall προστατεύει το «εσωτερικό» δίκτυο από τον υπόλοιπο κόσμο.

Συσκευές Firewall υπάρχουν για μεγάλα εταιρικά δίκτυα, αλλά και για πολύ μικρότερα. Για παράδειγμα, αν στο σπίτι μας έχουμε τουλάχιστον δύο PC που «βγαίνουν» στο Internet, ίσως αποφασίσουμε να αγοράσουμε μια φτηνή συσκευή Firewall. Στην περίπτωση αυτή τα δίκτυα μεταξύ των οποίων παρεμβάλλεται το Firewall είναι από τη μία πλευρά το μικρό οικιακό LAN και από την άλλη ένα τεράστιο δίκτυο – το ίδιο το Internet! Ανάλογες παρατηρήσεις μπορούμε να κάνουμε και για τα Firewall που υλοποιούνται σε λογισμικό. Υπάρχουν εφαρμογές Firewall που τρέχουν σε μηχανήματα Unix και προστατεύουν μεγάλα εταιρικά δίκτυα. Στον αντίποδα βρίσκουμε

**Ενεργοποίηση του Firewall των Windows XP για μια σύνδεση dial-up. Σημειώστε ότι το εν λόγω Firewall ελέγχει μόνο την εισερχόμενη κίνηση (inbound traffic), αγνοώντας παντελώς την εξερχόμενη (outbound traffic).**



τα προσωπικά Firewall, μέριμνα των οποίων είναι η προστασία ενός και μόνο PC.

**ΔΙΑΜΟΡΦΩΝΟΝΤΑΣ ΤΑ ΚΡΙΤΗΡΙΑ.** Όπως είπαμε και προηγουμένως, ο διαχειριστής ενός Firewall έχει την ευχέρεια να καθορίζει κατά βούληση τα φίλτρα ελέγχου. Εκείνα με τη σειρά τους διαμορφώνονται συνδυάζοντας ένα πλήθος κριτηρίων, μερικά από τα οποία παραθέτουμε ευθύς αμέσως.

- **Ιντερνετική διεύθυνση IP.** Η πρόσβαση στο δίκτυο ή στον υπολογιστή «πίσω» από το Firewall επιτρέπεται ή απαγορεύεται με βάση την αριθμητική διεύθυνση IP. Ομοίως, μηχανήματα του εσωτερικού δικτύου με διαφορετικά IP ενδέχεται να έχουν διαφορετικά δικαιώματα πρόσβασης στον έξω κόσμο.

- **Όνομα περιοχής.** Μηχανήματα που ανήκουν σε μια ολόκληρη περιοχή (domain) ενδέχεται να έχουν διαφορετικά δικαιώματα πρόσβασης σε σύγκριση με μηχανήματα άλλων περιοχών.

- **Πρωτόκολλο επικοινωνίας.** Τα δικαιώματα πρόσβασης προς το εσωτερικό δίκτυο διαμορφώνονται με βάση το πρωτόκολλο επικοινωνίας. Για παράδειγμα, η πρόσβαση ενδέχεται να επιτρέπεται μόνο όταν το πρωτόκολλο επικοινωνίας είναι ένα εκ των FTP, HTTP.

- **Αριθμός θύρας.** Κάθε υπηρεσία που τρέχει σε ένα μηχανήμα επικοινωνεί με το εξωτερικό δίκτυο μέσω μιας ή περισσότερων αριθμημένων θυρών (ports). Για παράδειγμα, ένας διακομιστής ιστοσελίδων χρησιμοποιεί εξ ορισμού το port 80. Το Firewall μπορεί να ρυθμιστεί έτσι ώστε να επιτρέπει σε απομακρυσμένα μηχανήματα την πρόσβαση σε συγκεκριμένες θύρες και μόνο σε αυτές.

- **Λέξεις ή φράσεις-κλειδιά.** Εάν τα διερχόμενα πακέτα περιλαμβάνουν λέξεις ή φράσεις από μια απαγορευμένη λίστα, απορρίπτονται. Κατ' αυτό τον τρόπο καθίσταται αδύνατη ή δύσκολη η πρόσβαση σε δικτυακούς τόπους, π.χ., πορνογραφικού περιεχομένου.

Επιπρόσθετα, τα προσωπικά Firewall που τρέχουν στα PC έχουν τη δυνατότητα να επιτρέπουν ή να απαγορεύουν την πρόσβαση σε επίπεδο εφαρμογής. Μπορούμε, με άλλα λόγια, να ρυθμίζουμε το Firewall ώστε να επιτρέπει μόνο σε προκαθορισμένες εφαρμογές να βγαίνουν στον έξω κόσμο. Στη συνέχεια θα ασχοληθούμε αποκλειστικά με τα προσωπικά Firewall.

**Η ΓΑΤΑ ΚΑΙ ΤΟ ΠΟΝΤΙΚΙ.** Μεταξύ των εταιρειών κατασκευής

Firewall και των cracker διεξάγεται ένας διαρκής αγώνας.

Οι πρώτες επιχειρούν να κάνουν τα προγράμματά τους ολοένα και πιο αποτελεσματικά, ενώ οι δεύτεροι εφευρίσκουν διαρκώς νέες τεχνικές προκειμένου να τα ξεγελούν! Ας επιχειρήσουμε μια σκιαγράφιση αυτού του αγώνα. Κάθε σύγχρονο trojan ή worm χρησιμοποιεί τυπικές θύρες για να επικοινωνεί με τον έξω κόσμο. Έτσι, είναι σε θέση να διαπερνά ένα hardware Firewall ή ένα «χαζό» προσωπικό Firewall, αφού κανένα από αυτά δεν θα απαγόρευε εξ ορισμού την πρόσβαση, π.χ., στο port 80. Τα προσωπικά Firewall επιχειρούν να αντισταθμίσουν αυτό το μειονέκτημα κατοστρώνοντας κανόνες που βασίζονται στο όνομα. Λένε, για παράδειγμα, «επιτρέψε την πρόσβαση μόνο στα προγράμματα με όνομα iexplore.exe ή mozilla.exe ή... ή outlook.exe». «Σιγά τα ωά» σχολιά-

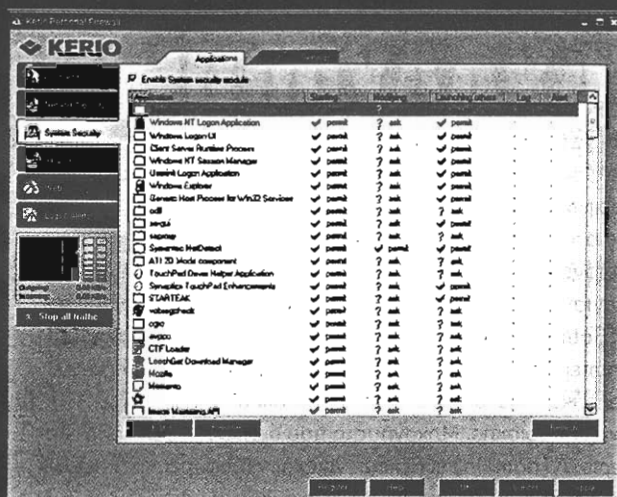
Είναι αρκετό το Firewall των Windows XP:

Προκειμένου να ενεργοποιήσουμε το ενσωματωμένο Firewall των Windows XP για μια ή περισσότερες συνδέσεις με τον έξω κόσμο, ακολουθούμε τη διαδρομή <Control Panel> >Network and Internet Connections > >Network Connections>. Εκεί κάνουμε δεξί κλικ πάνω σε μια σύνδεση που μας ενδιαφέρει και δίνουμε <Properties> >Advanced>. Η ενεργοποίηση του Firewall για τη συγκεκριμένη σύνδεση (network interface) πραγματοποιείται τσεκάροντας το κουτάκι «Protect my computer and network by limiting or preventing access to this computer from the Internet». Όμοια εργαζόμαστε και για άλλα network interfaces που ενδεχομένως υπάρχουν. Για παράδειγμα, ένας φορητός υπολογιστής επικοινωνεί με τον έξω κόσμο με δύο τουλάχιστον τρόπους: μέσω modem ή μέσω κάρτας δικτύου. Το κακό με το Firewall των Windows XP είναι ότι κάνει μισές δουλειές! Για την ακρίβεια, ενώ προσφέρει πλήρη προστασία και έλεγχο για την κίνηση «από έξω προς τα μέσα» (inbound traffic), αγνοεί παντελώς την κίνηση «από μέσα προς τα έξω» (outbound traffic). Έτσι, αν από δικό μας λάθος ή από παρέμβαση κάποιου άλλου χρήστη εγκατασταθεί στο PC μας ένα trojan horse, τότε θα είναι σε θέση να επικοινωνεί άνετα με τον υπολογιστή του επιτιθέμενου — ακόμη και αν το Firewall των Windows XP είναι ενεργοποιημένο. Γίνεται φανερό, λοιπόν, ότι η απάντηση στο ερώτημα της επικεφαλίδας είναι σαφώς αρνητική.

ζουν ειρωνικά οι cracker και μετονομάζουν τα προγράμματά τους σε iexplore.exe ή κάτι παρεμφερές. Θορυβημένοι οι κατασκευαστές Firewall αναρωτιούνται πώς μπόρεσαν να μην προβλέψουν μια τέτοια κίνηση! Απαντούν εξελίσσοντας τους κανόνες, ώστε για κάθε πρόγραμμα να δημιουργούν και ένα είδος «ψηφιακής υπογραφής» (βλ. και παρακάτω στο αφιέρωμα). Επειδή η ψηφιακή υπογραφή είναι μοναδική για κάθε αρχείο και ανεξάρτητη από το όνομά του, ένα καλό Firewall εύκολα μπορεί τώρα να ελέγχει εάν το iexplore.exe είναι πράγματι ο Internet Explorer ή κάτι άλλο, και συνεπώς πράττει αναλόγως. Η απάντηση των cracker είναι τρομακτικά ύπουλη: Τα σύγχρονα trojan έρχονται μεταμφιεσμένα ως plug-in «νυμίων» προγραμμάτων. Κάποια άλλοι χρησιμοποιούν τις ενεργές διεργασίες άλλων εφαρμογών, προκειμένου να επικοινωνούν όμορφα και καλώς με τον έξω κόσμο. Ορισμένα Firewall «γνωρίζουν» τις τεχνικές αυτές, οπότε, κάθε φορά που ένα πρόγραμμα καλεί κάποιο άλλο ή φορτώνει ένα plug-in, πληροφορούν σχετικά το χρήστη και περιμένουν από τον ίδιο να αποδεχτεί ή να απορρίψει την ενέργεια. Βεβαίως, καθ' όλη τη διάρκεια μιας τυπικής συνεδρίας του χρήστη με το PC του, πολλοί θα είναι οι εφαρμογές που, για τον άληθο ή το βήτα λόγο, θα καλέσουν ένα άλλο πρόγραμμα ή θα φορτώσουν ένα plug-in. Έτσι, κάθε φορά που το Firewall ζητά επιβεβαίωση για μια τέτοια ενέργεια, πριν δώσει ο χρήστης την οποιαδήποτε απάντηση οφείλει να γνωρίζει πολύ καλά τι συμβαίνει στο PC του! Για το λόγο αυτό αρκετά Firewall που μπορούν να ανιχνεύουν πότε μια εφαρμογή καλεί κάποια άλλη ή πότε διαβάζει plug-in έχουν την εν λόγω δυνατότητα εξ ορισμού απενεργοποιημένη. Το νηικό δίδαγμα συνο-



Καθορισμός δικαιωμάτων πρόσβασης διαφόρων εφαρμογών ενός συστήματος με τη βοήθεια του Kerio Personal Firewall. Παρατηρήστε ότι τα δικαιώματα πρόσβασης στο Internet δεν είναι κατ' ανάγκη ίδια με τα αντίστοιχα για την πρόσβαση σε ένα έμπιστο εσωτερικό δίκτυο (trusted network).



Το Kerio Personal Firewall προσφέρει στο χρήστη τη δυνατότητα να καθορίζει ο ίδιος ποιες εφαρμογές μπορούν να καλούν άλλες, όπως επίσης και για ποιες εφαρμογές επιτρέπεται η αλληλαγγή των συστατικών τους (π.χ., βιβλιοθήκες, εκτελέσιμα αρχεία διαφόρων υποπρογραμμάτων κ.ο.κ.).

ψίζεται ως εξής: Μετά την εγκατάσταση ενός οποιουδήποτε Firewall ο χρήστης οφείλει να μελετά όλες τις διαθέσιμες επιλογές του προγράμματος και να τις τροποποιεί ανάλογα με τις ανάγκες και το επίπεδο τεχνογνωσίας που διαθέτει.

**ΕΛΕΓΧΟΣ ΔΥΝΑΤΟΤΗΤΩΝ.** Υπάρχουν διάφορα προγραμματάκια που χρησιμοποιούν στον έλεγχο της αποτελεσματικότητας ενός οποιουδήποτε Firewall (μερικά από αυτά θα βρείτε στο φάκελο Security/Testing του CD μας). Τα περισσότερα επικεντρώνονται στις εξερχόμενες συνδέσεις (outbound connections), αφού η συντριπτική πλειονότητα των σημερινών Firewall παρέχει άριστο έλεγχο των εισερχόμενων συνδέσεων (inbound connections).

Ένα διάσημο και άκρως αποκαλυπτικό πρόγραμμα της κατηγορίας είναι το pcAudit [[www.pccinternetpatrol.com](http://www.pccinternetpatrol.com)]. Αφού το τρέξουμε και συμφωνήσουμε στο license agreement που παρουσιάζει, μας προτρέπει να ανοίξουμε τον Internet Explorer και να επισκεφθούμε ένα δικτυακό τόπο όπου απαιτείται σύνδεση (log in) με όνομα χρήστη και συνθηματικό. Εκεί θα πρέπει να πληκτρολογήσουμε ένα τυχαίο όνομα χρήστη και ένα κάλπικο συνθηματικό. Λογικά, για κάθε πλήκτρο που πατάμε, στην οθόνη θα εμφανίζεται ένας αστερίσκος ή μια τελεία. Το pcAudit, όμως, θα παρακολουθεί κάθε χτύπημα πλήκτρου και θα το καταγράφει! Στη συνέχεια το πρόγραμμα θα πάρει ένα screenshot από την επιφάνεια εργασίας των Windows και θα επιχειρήσει να το στείλει στον τόπο [www.pccinternetpatrol.com](http://www.pccinternetpatrol.com). Εάν τα καταφέρει, θα τον ανοίξει στον Internet Explorer και εμείς θα δούμε τη φωτογραφία του desktop, τα στοιχεία που πληκτρολογήσαμε στο δικτυακό τόπο που επισκεφθήκαμε πριν από λίγο, καθώς και μια λίστα με αρχεία και φακέλους στα οποία θα είχε άμεση πρόσβαση ένας cracker, αν παραβίαζε την ασφάλεια του υπολογιστή μας! Σημειώστε ότι, ακόμη και αν το pcAudit πετύχει το σκοπό του, «αυστηρότερες» ρυθμίσεις στο Firewall ενδέχεται

να εμποδίσουν τη δράσή του σε επόμενη δοκιμή.

Τέλος, προκειμένου να ελέγξουμε την αποτελεσματικότητα του Firewall αναφορικά με τις εισερχόμενες συνδέσεις, μια δυνατότητα είναι να εκτελέσουμε τα on-line test του τόπου <http://erc.com/x/ne.dll?bh0bkyd2> (κάντε χρήση των ShieldsUP!!! Services).



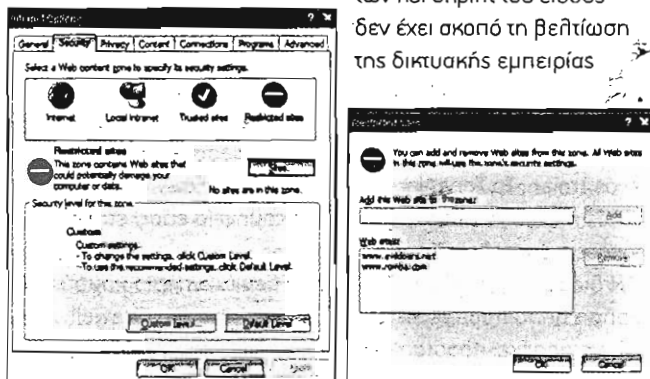
# ΑΠΑΤΗΛΗ ΑΝΩΝΥΜΙΑ, ΠΑΡΑΒΙΑΣΜΕΝΗ ΙΔΙΩΤΙΚΟΤΗΤΑ

Εάν νομίζετε ότι στο Internet μπορείτε να είστε αόρατοι, κάνετε λάθος. Εάν πιστεύετε ότι κανείς δεν ενδιαφέρεται για τις κινήσεις σας, ξανά κάνετε λάθος. Εάν κάποιοι νομίζουν ότι θα σας παρακολουθούν για πολύ καιρό ακόμα, ε, και αυτοί κάνουν λάθος!

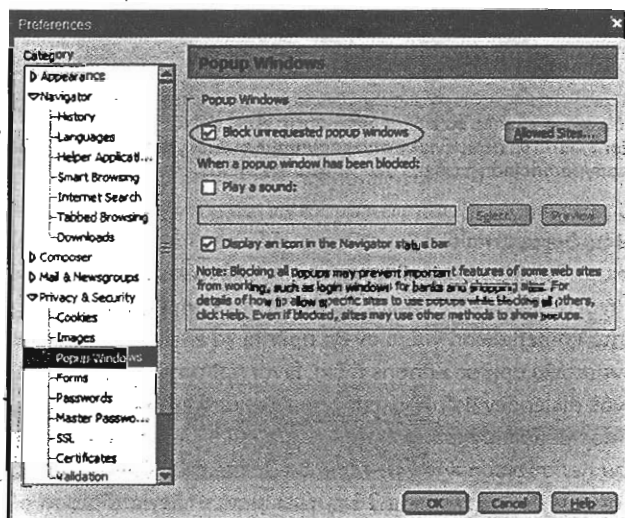
## ΠΡΟΓΡΑΜΜΑΤΑ ΑΠΟ ΤΟ CD ΦΑΚΕΛΟΙ SECURITY/ANONYMITY, SECURITY/ANTI-SPY, SECURITY/PRIVACY

Όταν οι άνθρωποι μιλούν για προστασία της ιδιωτικότητας στο Internet, συνήθως εννοούν διαφορετικά πράγματα, ενώ άλλες φορές χρησιμοποιούν τις έννοιες «ιδιωτικότητα» και «ανωνυμία» εναλλάξιμα. Σε γενικές γραμμές, ένας χρήστης του Διαδικτύου έχει ιδιωτικότητα όταν κάνει αυτό που θέλει χωρίς «εξωτερικούς» περισπασμούς και οχλήσεις. Επίσης, στοιχεία που τον αφορούν, όπως, π.χ., αριθμοί πιστωτικών καρτών, κωδικοί πρόσβασης, φυσικές και ηλεκτρονικές διευθύνσεις κ.ο.κ., δεν «διαρρέουν» σε τρίτους. Υπάρχουν προγράμματα και εργαλεία που προστατεύουν την ιδιωτικότητα στο δίκτυο, όπως το Spy Sweeper που θα δούμε στη συνέχεια. Πέρα από αυτά, εφαρμόζοντας μερικούς απλούς κανόνες, αποφεύγουμε σε μεγάλο βαθμό τις «κακοτοπίες», χωρίς να καταφεύγουμε σε εξειδικευμένο λογισμικό.

Όταν σερφάρουμε σε «περίεργους» δικτυακούς τόπους, είναι φρόνιμο να απενεργοποιούμε την υποστήριξη των Java, JavaScript και ActiveX. Αρκετές φορές η εκτέλεση προγραμμάτων και σκριπτ του είδους δεν έχει σκοπό τη βελτίωση της δικτυακής εμπειρίας



Προσθήκη επίφοβων δικτυακών τόπων στη λίστα με τους περιορισμένους δικτυακούς τόπους του Internet Explorer. Εξ ορισμού, Java, JavaScript και ActiveX απενεργοποιούνται αυτομάτως για τους τόπους της συγκεκριμένης λίστας.



Το πρόγραμμα πλοήγησης Mozilla επιτρέπει στο χρήστη να απενεργοποιήσει την εμφάνιση παραθύρων pop-up.

αλλά την ύπουλη «εμφύτευση» κακόβουλων προγραμμάτων στον υπολογιστή μας, όπως, π.χ., dialer και key-logger. Οι τελευταίοι παρακολουθούν κρυφίως τα πλήκτρα που πατάμε προσπαθώντας να αλιεύσουν κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών και άλλα προσωπικά δεδομένα. Τις πληροφορίες που συλλέγουν τις αποστέλλουν σε σύντομο χρόνο σε προκαθορισμένους δικτυακούς τόπους, προς εκμετάλλευση από cracker και script kiddies. Μια άλλη κατηγορία κακόβουλων προγραμμάτων είναι τα hijack, που αλλοιάζουν την αρχική σελίδα του προγράμματος πλοήγησης, φυσικά χωρίς την έγκρισή μας. Τους δικτυακούς τόπους που δεν εμπιστευόμαστε μπορούμε να τους εντάξουμε σε κάποια «περιορισμένη ζώνη» του προγράμματος πλοήγησης. Στον Internet Explorer, για παράδειγμα, ακολουθούμε τη διαδρομή <Tools>→Internet Options...→Security→Restricted sites→Sites...> και στο παράθυρο που εμφανίζεται δίνουμε μία προς μία τις διευθύνσεις των επίφοβων τόπων.

Ορισμένες δοκιμαστικές ή δωρεάν εκδόσεις προγραμμάτων κρύβουν μέσα τους τα λεγόμενα spyware. Πρόκειται για εφαρμογές που παρακολουθούν τις δικτυακές μας συνήθειες και

αποστέλλουν αναφορές σε εταιρείες, κυρίως για εμπορική εκμετάλλευση. Εκτός από την παραβίαση της ιδιωτικότητας, τα spyware υποκλέβουν και πολύτιμο bandwidth. Κατά περιπτώσεις, το license agreement στο οποίο πρέπει να συμφωνήσουμε πριν κατεβάσουμε ένα πρόγραμμα αναφέρει την παρουσία των spyware. Αυτή η πληροφορία όμως είναι συνήθως επιμελώς «θαμμένη» μέσα σε παραγράφους που μόνο νομικοί κατανοούν – χωρίς που στην πράξη κανείς δεν διαβάζει τέτοια agreement.

- Μια άλλη κατηγορία ανεπιθύμητων προγραμμάτων που συνοδεύουν δοκιμαστικές ή δωρεάν εκδόσεις εφαρμογών είναι τα λεγόμενα **adware**. Σκοπός τους είναι να κατεβάζουν διαφημιστικά μηνύματα και βιντεάκια flash από το Διαδίκτυο όσο είμαστε on-line και να τα εμφανίζουν είτε σε κάποιο πλαίσιο της «μητρικής» εφαρμογής είτε σε ξεχωριστό παράθυρο. Στις περιπτώσεις στις οποίες το adware είναι ξέχωρο από την εφαρμογή, αν το απεγκαταστήσουμε από την προσθαφαίρεση εφαρμογών, τότε η κύρια εφαρμογή κατά πάσα πιθανότητα θα πάψει να λειτουργεί. Μια πιθανή λύση είναι να απογορεύσουμε την πρόσβαση του adware στο δίκτυο δημιουργώντας έναν κατάλληλο κανόνα στο προσωπικό μας Firewall.

- Ποτέ και υπό καμία περίπτωση δεν πρέπει να αποστέλλουμε «ευαίσθητο» στοιχεία σε δικτυακούς τόπους οι οποίοι δεν υποστηρίζουν το πρωτόκολλο ασφαλούς επικοινωνίας SSL (Secure Sockets Layer). Διαφορετικά, τα δεδομένα μας θα ταξιδεύουν σε απλή, μη κρυπτογραφημένη μορφή και οποιοσδήποτε θα είναι σε θέση να τα δει, μάλιστα χωρίς να καταβάλει ιδιαίτερη προσπάθεια. Όταν μια συνεδρία είναι ασφαλής, το καταλαβαίνουμε με δύο τρόπους: α. Κάτω δεξιά στην μπάρα του browser εμφανίζεται ένα ενδεικτικό εικονίδιο (π.χ., ένα κλειστό λουκέτο) και β. Το πρωτόκολλο επικοινωνίας στην μπάρα διευθύνσεων του browser θα είναι «https» και όχι «http». Εκτός από τον απομακρυσμένο διακομιστή, τις ασφαλείς συνεδρίες πρέπει να υποστηρίζει και το πρόγραμμα-πληκτρονίου, με άλλα λόγια ο browser. Πάντως, όλα τα σύγχρονα προγράμματα πλοήγησης, Internet Explorer, Mozilla, Opera κ.ά., υποστηρίζουν το SSL, ανεξάρτητα από το λειτουργικό σύστημα που τρέχουν.

- Τα προγράμματα πλοήγησης Mozilla, Firefox και Opera έχουν τη δυνατότητα να αποτρέπουν την εμφάνιση παραθύρων με διαφημίσεις. Στον Mozilla, για παράδειγμα, ακολουθούμε τη διαδρομή <Edit>→<Preferences>→<Privacy & Security>→<Pop-up Windows> και τσεκάρουμε την επιλογή «Block unrequested pop-up windows». Παρόμοιες ικανότητες θα αποκτήσει και ο Internet Explorer, μετά την κυκλοφορία του Service Pack 2 για τα Windows XP.

**ΔΙΕΚΔΙΚΩΝΤΑΣ ΤΗΝ ΑΝΩΝΥΜΙΑ.** Αρκετός κόσμος πιστεύει ότι στο Internet είναι άδρατος, ότι μπορεί να λέει και να κάνει ό,τι θέλει χωρίς ποτέ να υπάρξουν αρνητικές επιπτώσεις στον αληθινό του βίο. Και όμως, η ανωνυμία στο Διαδίκτυο δεν επιτυγχάνεται τόσο εύκολα όσο πιστεύουν μερικοί χρήστες. Κάθε φορά, για παράδειγμα, που επισκεπτόμαστε ένα δικτυακό τόπο, στα αρχεία καταγραφής του διακομιστή ιστοσελίδων μένουν πληροφορίες που αφορούν στην ημερομηνία και στην ώρα της επίσκεψης, στις σελίδες που προβάλαμε και στα αρχεία που κατεβάσαμε. Καταγράφονται, επίσης, η αριθμητική διεύθυνση του

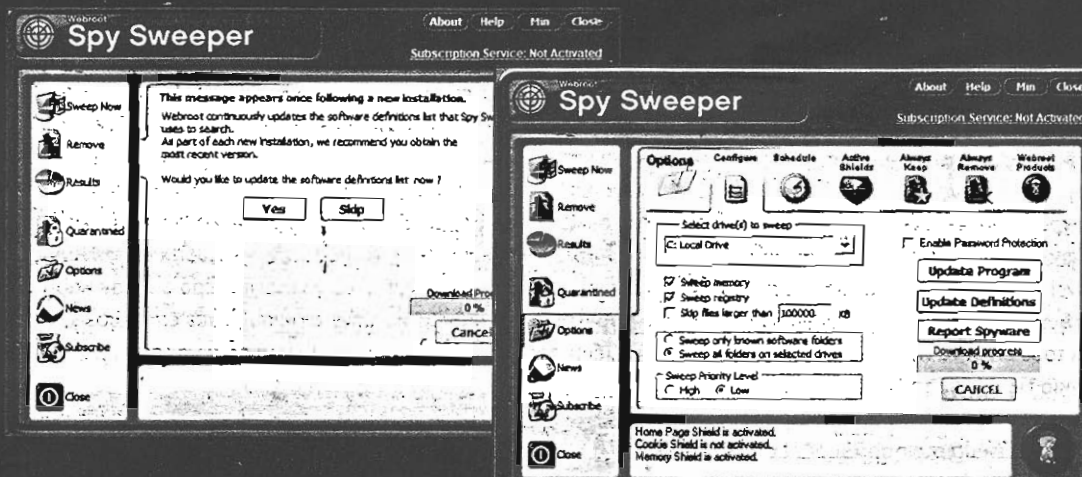
μηχανήματος, η περιοχή (domain) στην οποία ανήκει, το όνομα του ISP κ.ο.κ. Προκειμένου να πάρετε μια καλή ιδέα για την ποσότητα των πληροφοριών που συλλέγονται σε έναν τόπο, σας παροτρύνουμε να πάτε τώρα αμέσως στη διεύθυνση [privacy.net](http://privacy.net). Το πρώτο πράγμα που θα δείτε εκεί είναι η διεύθυνση IP του υπολογιστή σας. Αυτό όμως δεν είναι τίποτε μπροστά σε αυτά που θα σας αποκαλυφθούν αν ζητήσετε την πλήρη ανάλυση (κλικ στο δεσμό της γραμμής «Full analysis», πάνω αριστερά). Από τα προηγούμενα γίνεται φανερό ότι, εάν κάποιος προβεί σε μια παράνομη ενέργεια με σοβαρές επιπτώσεις, η θιγμένη πλευρά έχει την τεχνική δυνατότητα να τον εντοπίσει.

## Σκληρός AntiDialer!

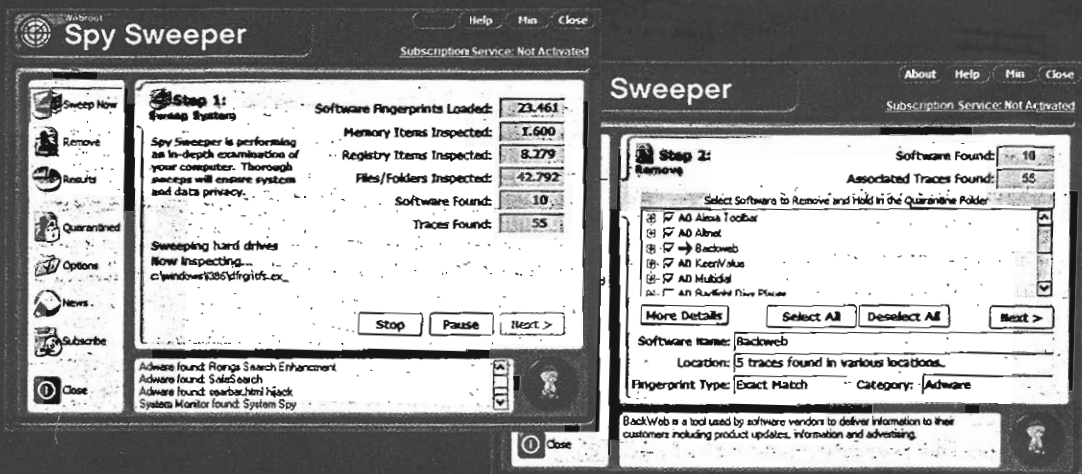
Αρκετά εργαλεία αυτόματης αφαίρεσης spyware, keyboard logger, hijacker και άλλων κακόβουλων προγραμμάτων έχουν τη δυνατότητα να εντοπίζουν και τους διαβόητους dialer. Αναφερόμαστε σε εκείνα τα ύπουλα προγράμματα που διακόπτουν αιφνίδια τη σύνδεση στο Internet και σιωπηρά πραγματοποιούν κλήσεις στο εξωτερικό. Τη δράση των dialer εμποδίζουν και ορισμένα προγράμματα Firewall, όπως το Kerio Personal Firewall, τα οποία επιτρέπουν τηλεφωνικές κλήσεις μόνο σε προκαθορισμένους αριθμούς. Μολταυτά, τα κρούσματα με τους dialer εξακολουθούν να είναι συχνά, αφού πολλοί χρήστες αγνοούν την ύπαρξή τους ή/και δεν γνωρίζουν πώς να τους αφαιρέσουν με χρήση εργαλείων λογισμικού. Επιπρόσθετα, πάντα υπάρχει η πιθανότητα κάποιοι dialer να ξεγελούν τα προγράμματα-διώκτες τους. Αν κρίνουμε μόνο από τα σχετικά e-mail παραπόνων που λαμβάνουμε κάθε μήνα στο περιοδικό, οι περισσότεροι χρήστες που έπεσαν «θύματα» κάποιου dialer ανακάλυψαν τι συνέβη αφού έλαβαν τον παραφουσκωμένο λογαριασμό του ΟΤΕ.

Μια «σκληρή» λύση για την αντιμετώπιση των dialer προτείνει η ελληνική εταιρεία Galaxy electric & electronics. Πρόκειται για το φίλτρο TL001 GALAXY, μια μικρή συσκευή που παρεμβάλλεται μεταξύ μόντεμ και τηλεφωνικής πρίζας και επιτρέπει τηλεφωνικές κλήσεις μόνο προς αριθμούς ΕΠΑΚ (δεν απαιτεί τροφοδοσία ή μπαταρίες). Έτσι, ακόμη και αν το PC μας είναι γεμάτο dialer –δίδωλο ευχάριστη κατάσταση, ομοιολογούμενως–, κανείς τους δεν θα μπορέσει να πραγματοποιήσει κλήσεις. Το TL001 GALAXY κοστίζει 75 ευρώ, του ΦΠΑ συμπεριλαμβανομένου. Για περισσότερες πληροφορίες μπορείτε να επικοινωνήσετε με την εταιρεία Galaxy, στο τηλέφωνο 210 6830.030.





Αμέσως μετά την εγκατάσταση του Spy Sweeper ο χρήστης παροτρύνεται να κατεβάσει από το Διαδίκτυο τις πλέον πρόσφατες ενημερώσεις γύρω από spyware, key-logger και άλλα κακόβουλα προγράμματα (αριστερά). Πριν ξεκινήσει ο έλεγχος του συστήματος, καλό είναι να γίνουν ορισμένες μικρορυθμίσεις που αφορούν στην ίδια τη διαδικασία (δεξιά).



Το Spy Sweeper «σκανάρει» το σύστημα για προγραμματιστικά «ζώδια». Ήδη, στο μηχανήμα μας έχει βρει δέκα (αριστερά). Μετά την ολοκλήρωση του ελέγχου παρουσιάζει τα ευρήματά του και περιμένει επιβεβαίωση ώστε να προχωρήσει στην εκκαθάριση. Για κάθε προτεινόμενο αρχείο παρέχονται αναλυτικές πληροφορίες σχετικά με τη «φύση» και το σκοπό που επιτελεί (δεξιά).

Το μόνο που χρειάζεται είναι να «κερδίσει» τη συνεργασία των αρχών, μερικών τηλεπικοινωνιακών φορέων και κάποιων εταιρειών παροχής υπηρεσιών Internet.

Υπάρχουν όμως και οι χρήστες που πιστεύουν στη δικτυακή ανωνυμία ως δικαίωμα και όχι ως άλληθοι για τη διεξαγωγή παράνομων, συκοφαντικών ή άλλων κατακριτέων πράξεων. Ένας τρόπος για να την έχουν είναι να σερφάρουν στο Internet μέσω ενός ανώνυμου διακομιστή μεσοδιάβασης (anonymous proxy server), με αντίτιμο τη χαμηλότερη ταχύτητα σύνδεσης. Ένας proxy του είδους μεταμφιέζει μέρος των πληροφοριών που προέρχονται από το μηχανήμα του πελάτη, με αποτέλεσμα ο σέρβερ να μην καταγράφει τα πραγματικά του στοιχεία. Στη διεύθυνση [www.atominersoft.com/products/alive-proxy/proxy-list](http://www.atominersoft.com/products/alive-proxy/proxy-list) υπάρχει μία λίστα με διευθύνσεις IP από δωρεάν anonymous proxy, με τα αντίστοιχα port από τα οποία «ακούνε» τις αιτήσεις των πελατών. Παρόμοιες δωρεάν υπηρεσίες παρέχονται και από τον τόπο [www.stayinvisible.com](http://www.stayinvisible.com). Έχετε υπόψη ότι, όταν η Java είναι ενεργοποιημένη, τότε ο εντοπισμός του αληθινού IP που έχει το μηχανήμα-πελάτης είναι εφικτός, αφού τα Java Applet μπορούν να διαβάσουν το IP από τις αντίστοιχες μεταβλητές συστήματος και να το μεταδώσουν στον πελάτη. Κλείνοντας το θέμα, θα θέλαμε να τονίσουμε emphaticά ότι ακόμη και στην περίπτωση που μεταξύ πελάτη και εξυπηρέτη υπάρχει μια ολοκληρη ακολουθία από ανώνυμους proxy, όταν συντρέξουν

οι λόγοι, τότε ο εντοπισμός της αληθινής ταυτότητας του πελάτη είναι θεωρητικά εφικτός: Αρκεί να συνεργαστούν οι κατάλληλες αρχές και να είναι διαθέσιμα τα αρχεία καταγραφής των εμπλεκόμενων μηχανημάτων (ξεκινώντας αντίστροφα, από τον εξυπηρέτη προς τον πελάτη).

# ΑΣΦΑΛΕΙΑ ΚΑΙ ΦΕΡΕΓΓΥΟΤΗΤΑ

...Και μετά την εγκατάσταση εργαλείων Firewall, AntiVirus, AntiSpam και AntiSpyware, ένας αδιάκριτος χρήστης διαβάζει με χαρακτηριστική ευκολία την αλληλογραφία μας. Λίγο αργότερα κάποιος άλλος επιτήδειος στήνει ένα δικτυακό τόπο «μαϊμού» και ψαρεύει τον αριθμό της πιστωτικής μας κάρτας. Τελικά, μήπως η προστασία στο Διαδίκτυο αποτελεί ουτοπία;

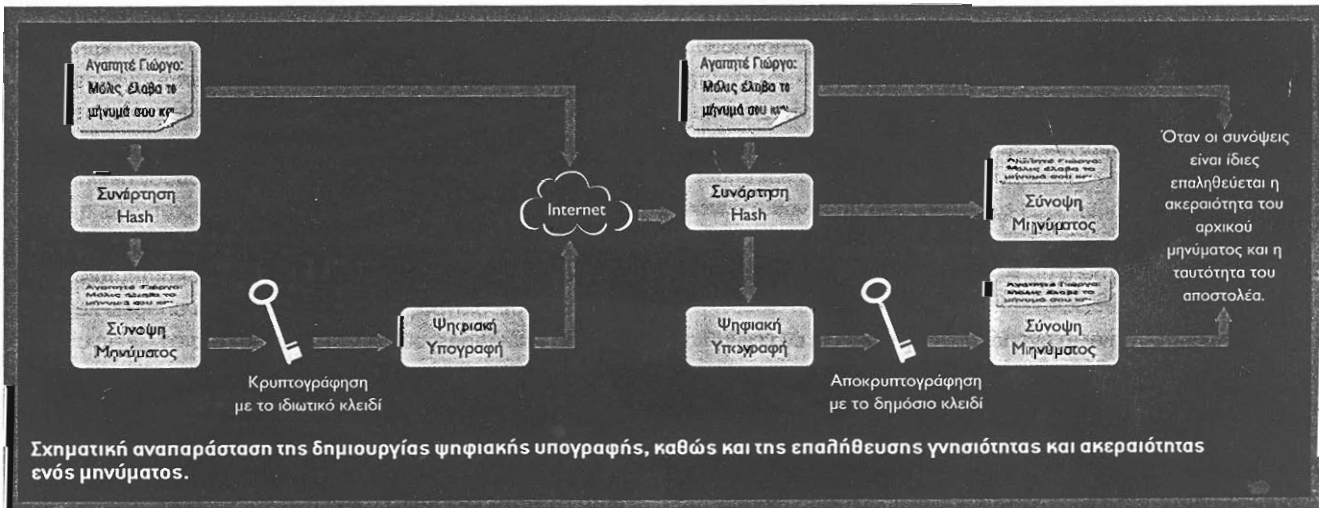
## ΠΡΟΓΡΑΜΜΑΤΑ ΑΠΟ ΤΟ ΕΘ Φάκελος Security/Cryptography

**Α**s υποθέσουμε ότι το PC μας, στο σπίτι ή στο γραφείο, είναι εξοπλισμένο με ένα καλό Firewall και πρόγραμμα AntiVirus. Το τελευταίο είναι έτσι ρυθμισμένο ώστε να εντοπίζει και να εξουδετερώνει αυτόματα ιούς, worm και άλλα κακόβουλα προγράμματα. Παρομοίως και το Firewall ελέγχει εξονυχιστικά εισερχόμενα και εξερχόμενα πακέτα, έχει ερμητικό κλειστές όλες τις χρησιμοποιούμενες θύρες και αφήνει μόνο τις διαπιστευμένες εφαρμογές να επικοινωνούν με τον έξω κόσμο. Αν στην όλη εικόνα προσθέσουμε ένα πρόγραμμα AntiSpyware, θα έχουμε μια πλήρη σουίτα εφαρμογών ασφαλείας. Εάν όλα τα σχετικά προγράμματα ενημερώνονται τακτικά και εμείς από την πλευρά μας κατέχουμε ορισμένες βασικές γνώσεις, ώστε να αποφεύγουμε κακοτοπιές και παγίδες, τότε μπορούμε να υποθέσουμε ότι πρακτικά είμαστε ασφαλείς.

Υπάρχουν όμως περιπτώσεις στις οποίες όλα τα προηγούμενα μέτρα αποδεικνύονται ανεπαρκή. Όποιο και αν είναι, για παράδειγμα, το αρχικό φορμά ενός e-mail, όταν φεύγει από το PC μας και μέχρι να φτάσει στον παραλήπτη θα ταξιδεύει υπό μορφή απλού κειμένου. Εάν κάποιος είναι αποφασισμένος να το

διαβάσει, έχει τρόπους να το πετύχει, π.χ., με τη χρήση ενός sniffer. Οστόσο, ακόμη και αν αποκλείσουμε την περίπτωση του sniffer, κατά περιπτώσεις το περιεχόμενο ενός e-mail είναι τόσο «ευαίσθητο», που δεν εμπιστευόμαστε ούτε τους διαχειριστές των εμπελεκόμενων διακομιστών αλληλογραφίας. Ιδανικά, θα θέλαμε ορισμένα —αν όχι όλα— από τα e-mail μας να κυκλοφορούν «εκεί έξω» σε κρυπτογραφημένη μορφή, και μόνο οι καθορισμένοι παραλήπτες να είναι σε θέση να τα διαβάζουν.

Άλλο ένα κεφαλαιώδες ζήτημα ασφαλείας έχει να κάνει με την ταυτοποίηση και τη γνησιότητα. Πώς είμαστε βέβαιοι ότι ο αποστολέας ενός e-mail είναι πράγματι εκείνος που ισχυρίζεται; Από τη στιγμή που υπάρχουν εργαλεία για το «μαγείρεμα» της κεφαλίδας ενός e-mail, η ηλεκτρονική διεύθυνση του αποστολέα δεν αποτελεί πάντα επαρκή απόδειξη για την πραγματική του ταυτότητα. Εξάλλου, κάποιος θα μπορούσε να υποκλέψει ένα μήνυμα καθ' οδόν, να τροποποιήσει το περιεχόμενό του και έπειτα να μας το στείλει, σαν να μη συνέβη τίποτε. Ομοίως και με ένα δικτυακό τόπο. Τι μας κάνει να πιστεύουμε ότι το ηλεκτρονικό κατάστημα που βλέπουμε σήμερα στον browser είναι ίδιο με εκεί-





νο που επισκεφθήκαμε χθες; Δεν θα μπορούσε κάποιος να έχει στήσει μια δικτυακή βιτρίνα του καταστήματος, π.χ., με σκοπό να αλιεύσει αριθμούς πιστωτικών καρτών από ανυποψίαστους αγοραστές; Εξετάζοντας την υπόθεση από καθαρά τεχνική σκοπιά, διαπιστώνουμε ότι δεν υπάρχει τίποτα που θα έκανε αδύνατη μια τέτοια απόπειρα. Και όμως, πολλοί από εμάς εμπιστευόμαστε τακτικά, σε διάφορους δικτυακούς τόπους, αριθμούς πιστωτικών καρτών και άλλα προσωπικά δεδομένα. Μήπως δεν κάνουμε καλά;

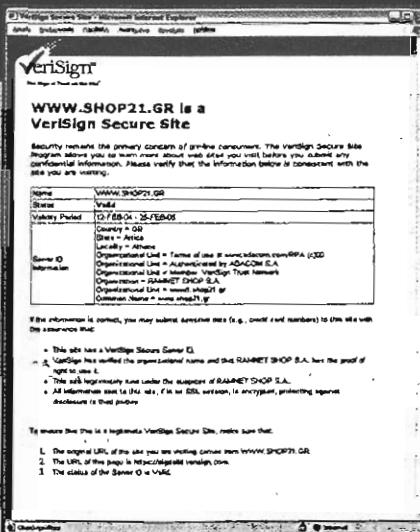
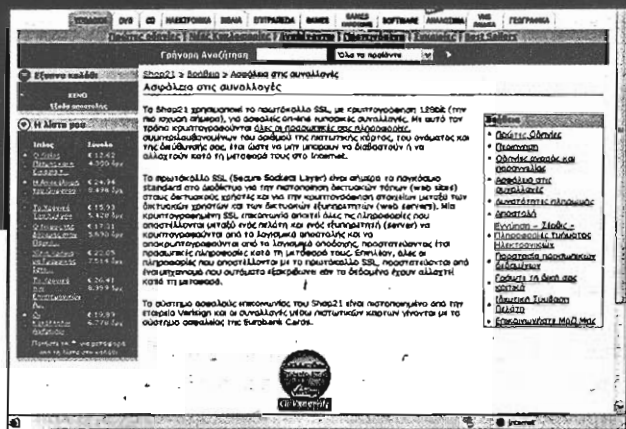
**ΜΕΤΑΣΧΗΜΑΤΙΖΟΝΤΑΣ ΤΟ ΝΟΗΜΑ.** Οι αποτελεσματικότερες μέθοδοι για την απόκρυψη ευαίσθητων δεδομένων από αδιάκριτα βλέμματα βασίζονται στις αρχές της κρυπτογραφίας. Γενικά, ως σύστημα κρυπτογράφησης ορίζεται ένας μηχανισμός ή αλγόριθμος μετατροπής ενός αρχικού συνόλου δεδομένων (plaintext) σε μια νέα μορφή (ciphertext), από την οποία είναι αδύνατον να εξαχθεί νόημα. Το ciphertext αποτελεί την κρυπτογραφημένη έκδοσή του αρχικού συνόλου δεδομένων. Η διαδικασία της κρυπτογράφησης απαιτεί την παρουσία μιας ακολουθίας χαρακτήρων, το λεγόμενο κλειδί (key). Η αποκρυπτογράφηση, με άλλα λόγια η λήψη του plaintext από το ciphertext, απαιτεί την παρουσία ενός άλλου κλειδιού. Έτσι, όταν αποστέλλουμε ένα e-mail σε κρυπτογραφημένη μορφή, ακόμη και αν κάποιος υποκλέψει όλο τα πακέτα που το αποτελούν και τα συναρμολογήσει, χωρίς το κατάλληλο κλειδί αποκρυπτογράφησης δεν θα καταφέρει να βγάλει νόημα. Η ηλιονότιη των σύγχρονων συστημάτων κρυπτογράφησης εμπίπτουν σε δύο μεγάλες κατηγορίες.

- **Κρυπτογραφία συμμετρικού κλειδιού (symmetric key cryptography).** Το κλειδί της κρυπτογράφησης ταυτίζεται πάντα με εκείνο της αποκρυπτογράφησης. Έτσι, όταν εγώ θέλω να στείλω ένα κρυπτογραφημένο e-mail ή αρχείο σε κάποιο συνάδελφο, αρχικά το κρυπτογραφώ, χρησιμοποιώντας το κατάλληλο κλειδί. Γνωρίζω ότι το διαθέτει και εκείνος, οπότε, όταν θα λάβει το κρυπτογραφημένο μήνυμα, θα μπορέσει να πάρει το plaintext, με άλλα λόγια θα αποκτήσει πρόσβαση στο μη κρυπτογραφημένο περιεχόμενο. Η κρυπτογραφία συμμετρικού κλειδιού υλοποιείται εύκολα και οι σχετικοί αλγόριθμοι είναι γρήγοροι. Το μειονέκτημά της έγκειται στη διανομή του ίδιου του κλειδιού: Αν το αποκτήσουν μη εξουσιοδοτημένα πρόσωπα, τότε θα έχουν και εκείνο πρόσβαση στο κρυπτογραφημένο περιεχόμενο. Έτσι, η χρήση της συμμετρικής κρυπτογραφίας προτείνεται όταν το περιεχόμενο παραμένει στον υπολογιστή όπου κρυπτογραφήθηκε.

- **Κρυπτογραφία δημόσιου κλειδιού (public key cryptography).** Τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης διαφέρουν μεταξύ τους. Το ένα από τα δύο είναι γνωστό μόνο στον κάτοχό του και ονομάζεται μυστικό ή ιδιωτικό (private). Το άλλο κλειδί είναι διαθέσιμο σε οποιονδήποτε ενδιαφερόμενο και ονομάζεται δημόσιο (public)<sup>1</sup>. Σε ένα σύστημα κρυπτογραφίας δημόσιου κλειδιού, για κάθε ιδιωτικό κλειδί υπάρχει ακριβώς ένα δημόσιο. Δεδομένα που κρυπτογραφούνται

1. Στο διαδίκτυο υπάρχουν τόποι με λίστες δημόσιων κλειδιών – κάτι σαν τηλεφωνικοί κατάλογοι. Από εκεί βρίσκουμε δημόσια κλειδιά άλλων χρηστών ή προσθέτουμε τα δικά μας (βλ., π.χ., [www.keyserver.net](http://www.keyserver.net)).





Παράδειγμα δικτυακού τόπου που φέρει ψηφιακό πιστοποιητικό της VeriSign (αριστερά). Με ένα κλικ πάνω στο σχετικό εικονίδιο βλέπουμε πληροφορίες που αφορούν στην έκδοση του πιστοποιητικού (δεξιά).

τας. Έτσι, ο συνεργάτης αποφασίζει να υπογράψει το μήνυμα που πρόκειται να μου στείλει. Αρχικά, θα τροφοδοτήσει το μήνυμά του σε μια συνάρτηση hash, δημιουρ-

με χρήση του ενός κλειδιού αποκρυπτογραφούνται από το αντίστοιχο «ταίρι» και μόνο από αυτό. Ας δούμε πώς εφαρμόζονται οι αρχές της δημόσιας κρυπτογραφίας στην πράξη, και συγκεκριμένα στην αποστολή ηλεκτρονικής αλληλογραφίας. Επιθυμώ να στείλω ένα μήνυμα σε κάποιο φίλο. Σε ένα παλαιότερο, δικό του e-mail που έχω κρατήσει, υπάρχει συνημμένο το δημόσιο κλειδί του. Χρησιμοποιώντας το κρυπτογραφώ το δικό μου μήνυμα και του το στέλνω. Το μήνυμα αποκρυπτογραφείται μόνο με χρήση του αντίστοιχου ιδιωτικού κλειδιού, το οποίο κατέχει μόνο ο φίλος μου, επομένως μόνο εκείνος θα μπορέσει να το διαβάσει. Βέβαια, ο φίλος μου θα πρέπει να είναι προσεκτικός και να μη δίνει σε κανέναν το ιδιωτικό του κλειδί. Επιπρόσθετα, σφειδίζει να προστατεύει την πρόσβαση στο ίδιο το κλειδί, με χρήση κατάλληλης συνθηματικής φράσης (pass-phrase)<sup>2</sup>. Το προφανές πλεονέκτημα της δημόσιας κρυπτογραφίας έγκειται στη διανομή του δημόσιου κλειδιού. Δύο δημοφιλή συστήματα κρυπτογράφησης είναι το εμπορικό PGP (Pretty Good Privacy, [www.pgp.com](http://www.pgp.com)) και το GnuPG (GNU Privacy Guard, [www.gnupg.org](http://www.gnupg.org)), το οποίο αποτελεί Ελεύθερο Λογισμικό.

Κατά κανόνα, οι δημόσιοι αλγόριθμοι κρυπτογράφησης είναι πολύ πιο αργόι από τους συμμετρικούς. Έτσι, σε πολλές πρακτικές εφαρμογές ακολουθείται η μέση οδός της λεγόμενης «υβριδικής κρυπτογραφίας» (hybrid cryptography). Συγκεκριμένα, για την κρυπτογράφηση ενός μηνύματος επιστρατεύεται κάποιος συμμετρικός αλγόριθμος. Το κλειδί όμως της αποκρυπτογράφησης, που φυσικά ταυτίζεται με εκείνο της κρυπτογράφησης, πριν διανεμηθεί στους προβλεπόμενους παραλήπτες κρυπτογραφείται με χρήση ενός δημόσιου αλγόριθμου (ο χρόνος επεξεργασίας ενός οποιουδήποτε αλγόριθμου κρυπτογράφησης είναι ευθέως ανάλογος του μεγέθους των δεδομένων εισόδου).

**ΘΕΜΑ ΓΝΗΣΙΟΤΗΤΑΣ.** Το ζήτημα της ηλεκτρονικής ηλαιοπροσωπίας αντιμετωπίζεται με τη χρήση των ηλεκτρονικών υπογραφών (digital certificates): Με απλά λόγια, αποτελούν το ηλεκτρονικό ισοδύναμο των συνηθισμένων, χειρόγραφων υπογραφών. Ας υποθέσουμε ότι λαμβάνω ένα σημαντικό e-mail από ένα συνεργάτη. Θέλω να είμαι απόλυτα βέβαιος ότι το έστειλε ο ίδιος και όχι, π.χ., κάποιος ανταγωνιστής που θέλει να μου αποσπάσει επαγγελματικά μυστικά. Από τη στιγμή που κυκλοφορούν εργαλεία «fake mail», η ηλεκτρονική διεύθυνση του παραλήπτη δεν μου αρκεί ως αποδεικτικό στοιχείο της πραγματικής του ταυτότητας.

γώντας με τον τρόπο αυτό ένα είδος ηλεκτρονικού δακτυλικού αποτυπώματος, τη λεγόμενη σύνοψη του μηνύματος (message digest). Μια συνάρτηση hash μπορούμε να τη φανταζόμαστε ως ένα μηχανισμό, κλεισμένο μέσα σε ένα μαύρο κουτί. Οι λεπτομέρειες που αφορούν στον τρόπο λειτουργίας του μηχανισμού ποσώς μας ενδιαφέρουν. Ξέρουμε όμως ότι στη μία πλευρά του κουτιού υπάρχει μια είσοδος και στην απέναντι μια έξοδος. Μέσω της εισόδου τροφοδοτούμε το μαύρο κουτί με ένα οσοδήποτε μεγάλο ή μικρό μήνυμα. Σε κάθε περίπτωση, στην έξοδο του κουτιού παίρνουμε μια ακολουθία χαρακτήρων σταθερού μήκους: Αυτή είναι η σύνοψη του μηνύματος. Εάν τροφοδοτήσουμε ξανά το κουτί με ένα —έστω και ελάχιστο— τροποποιημένο μήνυμα, η σύνοψη που θα πάρουμε θα είναι παντελώς διαφορετική από την προηγούμενη. Η μεγάλη «ευσαισθησία» στα δεδομένα εισόδου αποτελεί μια από τις πολυτιμότερες ιδιότητες των συναρτήσεων hash. Αν και είναι δυνατόν να βρούμε δύο διαφορετικά μηνύματα που να δίνουν την ίδια σύνοψη, είναι αστρονομικά απίθανο να το καταφέρουμε. Απίστευτα δύσκολη είναι και η αντιστροφή μιας συνάρτησης hash: Είναι ιλιγγιωδώς απίθανο να πάρουμε το αρχικό μήνυμα, ξεκινώντας από τη σύνοψή του.

Ο συνεργάτης μου, λοιπόν, δημιουργεί τη σύνοψη του μηνύματος που πρόκειται να μου στείλει. Ακολουθώντας την κρυπτογραφία με χρήση του ιδιωτικού του κλειδιού. Το ciphertext που θα πάρει είναι η ψηφιακή υπογραφή του μηνύματος. Τελικά, θα επισυνάψει την υπογραφή στο μήνυμα και θα μου το στείλει. Όταν το λάβω, κρυπτογραφώ το μήνυμά μου με βεβαιωθώ για την ταυτότητα του αποστολέα, αρχικά θα αποκρυπτογραφήσω την υπογραφή, φυσικά με τη βοήθεια του δημόσιου κλειδιού του (υποτιθέμενου) συνεργάτη. Εάν αποτύχω, τότε ομέσως καταλαβαίνω ότι το μήνυμα το έστειλε κάποιος παραχαράκτης! Εάν πάλι τα καταφέρω, μένει να επαληθεύσω ότι το περιεχόμενο του μηνύματος δεν μεταβλήθηκε κατά την αποστολή. Προς τούτο, βάζω στη όλη τη σύνοψη του μηνύματος (την ήπια αποκρυπτογραφώντας την ψηφιακή υπογραφή) και υπολογίζω με τη δική μου συνάρτηση hash τη σύνοψη του μηνύματος που έχω τώρα μπροστά μου<sup>3</sup>.

2. Τα σύγχρονα συστήματα δημόσιας κρυπτογραφίας, πριν επιτρέψουν τη χρήση του ιδιωτικού κλειδιού απαιτούν την εισαγωγή συγκεκριμένης συνθηματικής φράσης. Αυτή την έχει ήδη καθορίσει ο ιδιοκτήτης του κλειδιού και, φυσικά, μόνο εκείνος τη γνωρίζει.
3. Από τη στιγμή που εγώ και ο συνεργάτης μου χρησιμοποιούμε το ίδιο σύστημα κρυπτογράφησης, η συνάρτηση hash δεν αλλάζει.

Εάν διαπιστώσω ότι είναι διαφορετική από αυτή που μόλις έβα-  
λα στην άκρη, τότε καταλαβαίνω ότι το περιεχόμενο του μηνύ-  
ματος άλλαξε, χωρίς να το γνωρίζει ο αποστολέας του! Διαφο-  
ρετικό βεβαιώνομαι ότι όλα έχουν καλώς και η πνευματική μου  
γρήνη επανέρχεται :-). Κάπου εδώ αξίζει να σημειώσουμε ότι  
οι όλες οι προηγούμενες ενέργειες (δημιουργία σύμφων, ψη-  
φιακής υπογραφής, σύγκριση συνόψεων κ.ο.κ.) γίνονται αυτό-  
ματα, από κατάλληλο λογισμικό.

**ΟΙ ΡΙΖΕΣ ΤΗΣ ΕΜΠΙΣΤΟΣΥΝΗΣ.** Πώς είμαστε βέβαιοι ότι το δη-  
μόσιο κλειδί ενός συνεργάτη είναι πράγματι δικό του; Τι μας  
διαβεβαιώνει ότι το κλειδί αυτό δεν προέρχεται από κάποιον  
cracker, ο οποίος γνωρίζει τα στοιχεία του εν λόγω συνεργάτη;  
Στην πραγματικότητα ποτέ δεν θα ήμαστε βέβαιοι, αν δεν υπήρ-  
χαν οι Αρχές Πιστοποίησης (Certification Authorities, CA), όπως  
η VeriSign ([www.verisign.com](http://www.verisign.com)). Μια τέτοια Αρχή είναι ένας  
έμπιστος οργανισμός ή εταιρεία που εκδίδει, κατόπιν σχετικής  
αίτησης, τα λεγόμενα πιστοποιητικά (certificates). Ένα πιστο-  
ποιητικό διαβεβαιώνει ότι ο κάτοχός του πράγματι διαθέτει το  
δημόσιο κλειδί που ισχυρίζεται. Βέβαια, πριν από την έκδοση  
ενός πιστοποιητικού η Αρχή Πιστοποίησης διεξάγει έρευνα σχε-  
τικά με την αξιοπιστία του πελάτη της. Η Αρχή Πιστοποίησης  
έχει δικαίωμα να μην εκδώσει ή και να ακυρώσει ένα πιστοποι-  
ητικό, όταν συντρέχουν κάποιοι λόγοι. Εκτός από τα πιστοποιητι-  
κά που αφορούν σε μεμονωμένους χρήστες, υπάρχουν και πι-  
στοποιητικά για ολόκληρους δικτυακούς τόπους. Έτσι, είμαστε  
βέβαιοι ότι η τράπεζα ή το δικτυακό κατάστημα με το οποίο  
ετοιμαζόμαστε να κάνουμε μια συναλλαγή είναι πράγματι αυτό

που φαίνεται. (Οι έγκυροι δικτυακοί τόποι φέρουν τα σήματα των  
αντίστοιχων αρχών πιστοποίησης. Με ένα κλικ επάνω στο σήμα  
εμφανίζεται το σχετικό πιστοποιητικό.) Τέλος, τη γνησιότητα  
μιας Αρχής Πιστοποίησης τη βεβαιώνει κάποια άλλη Αρχή και  
πάλι λέγοντας. Έχουμε, λοιπόν, μια ακολουθία Αρχών Πιστοποί-  
ησης, που συγκροτεί την ονομαζόμενη αλυσίδα εμπιστοσύνης  
(chain of trust). Στη μία άκρη της αλυσίδας είναι η Αρχή που  
«συναντήσαμε» σε κάποιο δικτυακό τόπο και στην άλλη άκρη,  
τη ρίζα (root), βρίσκεται μια καθολικά αποδεκτή Αρχή.