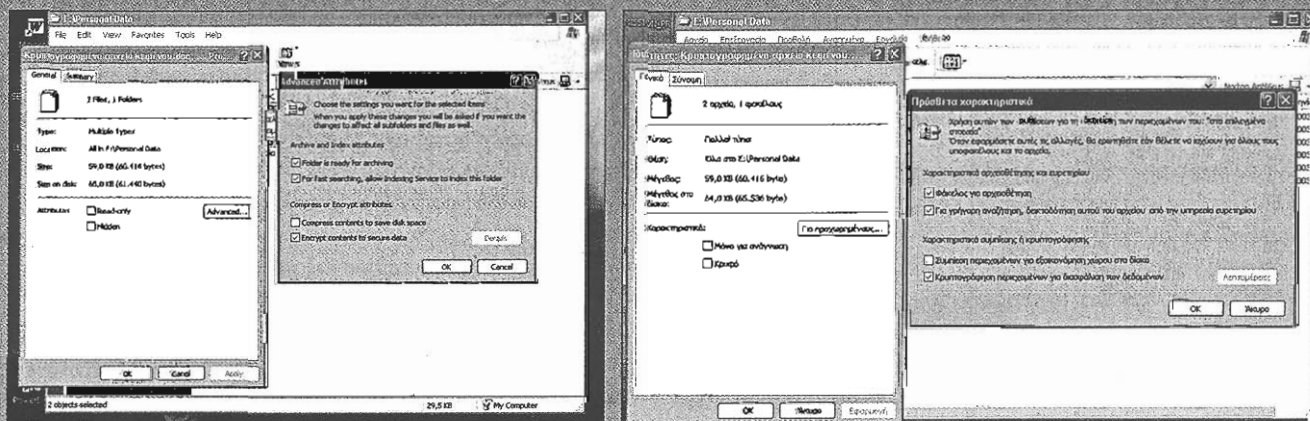


# Εξασφαλίστε το απόρρητο

Εάν το λειτουργικό σύστημα του υπολογιστή μας είναι τα Windows XP Professional, έχουμε τη δυνατότητα να προστατέψουμε το περιεχόμενο των αυστηρά προσωπικών μας δεδομένων από όσους χρήστες έχουν πρόσβαση στον υπολογιστή μας.

**Η** ασφάλεια των δεδομένων δεν είναι μία υπόθεση που αφορά μόνο στις επιχειρήσεις. Οι περισσότεροι άλλωστε από τους απλούς χρήστες υπολογιστών αποθηκεύουν στον εταιρικό ή τον οικιακό τους υπολογιστή δεδομένα προσωπικής φύσης, τα οποία θα προτιμούσαν να μην τα δουν άλλα, περίεργα μάτια. Τα δεδομένα αυτά μπορεί να είναι οικονομικά στοιχεία, αλληλογραφία, κείμενα, φωτογραφικό υλικό ή οποιοδήποτε αρχείο το οποίο καθένas από εμάς θεωρεί αυστηρά προσωπικό. Για να κρύψουμε τα δεδομένα αυτά από όσους έχουν δυνατότητα πρόσβασης στον υπολογιστή μας, υπάρχουν διάφορα προγράμματα. Αυτά συνήθως κρυπτογραφούν τα δεδομένα και για την αποκρυπτογράφηση ζητούν συγκεκριμένα κλειδιά ή κωδικούς. Στην περίπτωση, όμως, που το λειτουργικό σύστημα του υπολογιστή μας είναι τα Windows XP Professional, έχουμε τη δυνατότητα είτε να κρυπτογραφήσουμε τα δεδομένα είτε να επιτρέψουμε την πρόσβαση μόνο σε συγκεκριμένους χρήστες. Εννοείται ότι για το σκοπό αυτό δεν απαιτείται κάποιο πρόσθετο λογισμικό. Μοναδικός περιορισμός είναι ότι το σύστημα αρχείων του δίσκου που περιέχει τα αρχεία ή τους φακέλους που θέλουμε να προστατέψουμε πρέπει να είναι το NTFS (New Technology File System). Να σημειώσουμε ότι πρόσβαση συγκεκριμένων μόνο χρηστών σε αρχεία και φακέλους προσφέρουν και τα Windows 2000 Professional και NT 4.0, αλλά όχι τα Windows XP Home Edition. Ωστόσο, πριν αναφερθούμε αναλυτικότερα στους τρόπους με τους οποίους μπορούμε να προστατέψουμε το απόρρητο των δεδομένων μας, ας δούμε πώς μπορούμε να δημιουργήσουμε δίσκους με σύστημα αρχείων NTFS.

**ΔΙΑΜΟΡΦΩΣΗ ΣΕ NTFS.** Όπως και με το σύστημα αρχείων FAT32, έτσι και με το NTFS έχουμε τη δυνατότητα να διαμορφώσουμε είτε όλο το δίσκο είτε μεμονωμένες καταμήσεις (διαμερίσματα ή partitions). Ένας γρήγορος τρόπος για τη διαμόρφωση (φορμάρισμα) ενός δίσκου ή μιας υπάρχουσας κατάμησης μέσα από τον Windows Explorer (Εξερεύνηση των Windows) είναι να κάνουμε δεξί κλικ στο δίσκο ή στην κατάμηση και να επιλέξουμε «Format...» («Διαμόρφωση...»). Κατόπιν, θέτουμε στο πεδίο «File System» («Σύστημα αρχείων») την επιλογή «NTFS». Για ένα γρήγορο φορμάρισμα του δίσκου ή της κατάμησης θα ενεργοποιούμε την επιλογή «Quick Format» («Γρήγορη διαμόρφωση»), ενώ για ένα πλήρες ή συγκεκριμένη επιλογή πρέπει να είναι απενεργοποιημένη. Να σημειώσουμε ότι η δημιουργία καταμήσεων, η διαμόρφωση και, γενικότερα, η διαχείριση των δίσκων πραγματοποιούνται από το παράθυρο του «Computer Management» («Διαχείριση υπολογιστή»). Για να εμφανιστεί αυτό, κάνουμε δεξί κλικ στο εικονίδιο «My Computer» («Ο Υπολογιστής μου»), επιλέγουμε «Manage» («Διαχείριση») και, στη συνέχεια, «Disk Management» («Διαχείριση δίσκων»). Επειδή, όμως, τα Windows 3.x/95/98/98SE/Me και το MS-DOS δεν μπορούν να δουν δίσκους και καταμήσεις διαμορφωμένα σε NTFS, αν χρησιμοποιούμε κάποιο από αυτά τα λειτουργικά θα πρέπει να αφήσουμε τουλάχιστον ένα δίσκο ή μία κατάμηση στο σύστημα FAT32 (κατά προτίμηση τον C:). Τέλος, μπορούμε να μετατρέψουμε ένα δίσκο FAT16 ή FAT32 σε NTFS κάνοντας χρήση της εντολής «Convert [δίσκος]: /fs:ntfs /v» (π.χ., convert d: /fs:ntfs /v).



Για να κρυπτογραφήσουμε ένα αρχείο ή ένα φάκελο, το επιλέγουμε και, στη συνέχεια, από το παράθυρο των ιδιοτήτων του πατάμε το πλήκτρο «Advanced...» («Για προχωρημένους...»). Για να το συμπιέσουμε, ενεργοποιούμε την επιλογή «Encrypt contents to secure data» («Κρυπτογράφηση περιεχομένων για διασφάλιση των δεδομένων»).

## Πρέπει να θυμόμαστε:

Από τη στιγμή που θα κρυπτογραφήσουμε ένα φάκελο, οποιοδήποτε αρχείο ή φάκελο αντιγράψουμε ή δημιουργήσουμε μέσα σε αυτόν θα κρυπτογραφηθεί αυτόματα. Αν αντιγράψουμε ή μεταφέρουμε σε δίσκο με διαμόρφωση NTFS ένα κρυπτογραφημένο αρχείο ή φάκελο, θα παραμείνει κρυπτογραφημένο. Αντίθετα, αν η αντιγραφή ή η μεταφορά πραγματοποιηθεί σε δίσκο με διαμόρφωση FAT32 ή FAT16, τα δεδομένα δεν θα είναι πλέον κρυπτογραφημένα. Βέβαια, είναι προτιμότερο να κρυπτογραφούμε ολοκληρωμένους φακέλους και όχι μεμονωμένα αρχεία γιατί με αυτό τον τρόπο εξασφαλίζουμε περισσότερο το απόρρητο των δεδομένων μας. Αυτό συμβαίνει γιατί αρκετά προγράμματα (π.χ., το Word) όταν ανοίγουν ένα αρχείο —κρυπτογραφημένο ή μη—, δημιουργούν προσωρινά αρχεία. Επομένως, αν ο φάκελός μας δεν είναι κρυπτογραφημένος, ανοίγοντας ένα κρυπτογραφημένο κείμενο του Word, το πρόγραμμα θα δημιουργήσει ένα μη κρυπτογραφημένο προσωρινό αρχείο, το οποίο κάποιος τρίτος ενδεχομένως να μπορεί να διαβάσει, αν διαθέτει τις κατάλληλες γνώσεις για να το εντοπίσει. Δεδομένου ότι αρκετά προγράμματα δημιουργούν προσωρινά αρχεία στους προσωρινούς φακέλους Temp του υπολογιστή, αν ενδιαφερόμαστε για τη μέγιστη δυνατή προστασία των δεδομένων μας, καλό θα είναι να κρυπτογραφήσουμε και τους προσωρινούς φακέλους του λειτουργικού.

**ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΦΑΚΕΛΩΝ ΚΑΙ ΑΡΧΕΙΩΝ.** Τα Windows XP Professional έχουν τη δυνατότητα να κρυπτογραφήσουν αρχεία και φακέλους χρησιμοποιώντας την τεχνική EFS (Encrypted File System). Παρ' ότι η κρυπτογράφηση έχει ανάλογα αποτελέσματα με τον περιορισμό πρόσβασης σε φακέλους που θα περιγράψουμε παρακάτω, προσφέρει πρόσθετη ασφάλεια, καθώς διασφαλίζει το απόρρητο των δεδομένων ακόμα και στην περίπτωση που ο δίσκος με τα αρχεία μας πέσει στα χέρια κάποιου τρίτου. Αυτό συμβαίνει γιατί χρησιμοποιούνται δύο κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση, ένα δημόσιο (public key) και ένα ιδιωτικό (private key). Την πρώτη φορά που κρυπτογραφούμε κάποιο δεδομένο, τα Windows XP δημιουργούν ένα προσωπικό πιστοποιητικό κρυπτογράφησης (Personal Encryption Certificate) το οποίο περιέχει το δημόσιο/ιδιωτικό ζευγάρι κλειδιών που είναι απαραίτητο για την κρυπτογράφηση/αποκρυπτογράφηση των δεδομένων. Κάθε χρήστης που κρυπτογραφεί δεδομένα στον ίδιο υπολογιστή έχει το δικό του ξεχωριστό ζεύγος κλειδιών. Αυτό σημαίνει ότι τα δεδομένα μπορούν να διαβαστούν από άλλο χρήστη μόνο αν το έχουμε καθορίσει εμείς. Να σημειώσουμε, βέβαια, ότι έχουμε τη δυνατότητα να δημιουργήσουμε ειδικά πιστοποιητικά (Recovery Agent Certificates) για περιπτώσεις ανάκτησης δεδομένων.

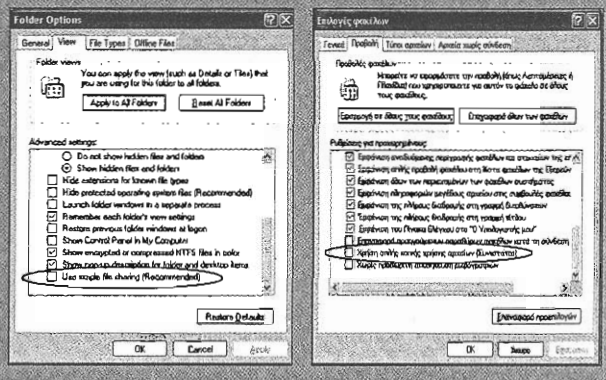
Θα πρέπει να τονίσουμε ότι η κρυπτογράφηση αρχείων καλό είναι να γίνεται μόνο σε ζωτικής σημασίας δεδομένα, καθώς, αν για οποιονδήποτε λόγο χάσουμε το προσωπικό πιστοποιητικό κρυπτογράφησης (π.χ., επανεγκατάσταση του λειτουργικού), δεν θα μπορούμε να δούμε τα κρυπτογραφημένα μας αρχεία. Για το σκοπό αυτό, συνιστάται να κρατάμε πάντα αντίγραφο του προσωπικού πιστοποιητικού κρυπτογράφησης.

**ΠΩΣ ΠΙΝΕΤΑΙ Η ΚΡΥΠΤΟΓΡΑΦΗΣΗ.** Όπως είπαμε, μπορούμε να κρυπτογραφήσουμε αρχεία ή φακέλους σε δίσκους με διαμόρφωση NTFS. Για το σκοπό αυτό επιλέγουμε μέσα από τον Windows Explorer τους φακέλους ή τα αρχεία που θέλουμε να προστατέψουμε, κάνουμε δεξί κλικ πάνω τους και επιλέγουμε «Properties» («Ιδιότητες»). Στη συνέχεια, από την καρτέλα «General» («Γενικά») πατάμε το κουμπί «Advanced...» («Για προχωρημένους...») και ενεργοποιούμε την επιλογή «Encrypt contents to secure data» («Κρυπτογράφηση περιεχομένων για διασφάλιση των δεδομένων»). Επειδή τα κρυπτογραφημένα αρχεία ή/και φάκελοι δεν μπορούν να είναι συμπιεσμένα, δεν έχουμε τη δυνατότητα να ενεργοποιήσουμε ταυτόχρονα τις επιλογές κρυπτογράφησης και συμπίεσης «Compress contents to save disk space» («Συμπίεση περιεχομένων για εξοικονόμηση χώρου στο δίσκο»), που βρίσκονται στο ίδιο πλαίσιο. Για να ολοκληρωθεί η κρυπτογράφηση των δεδομένων, κλείνουμε τα παράθυρα διαλόγων πατώντας «OK». Αν έχουμε επιλέξει για κρυπτογράφηση έναν ή περισσότερους φακέλους, το λειτουργικό θα μας ρωτήσει αν θέλουμε να κρυπτογραφήσουμε τα δεδομένα μόνο στους φακέλους που επιλέξαμε («Apply changes to this folder only» ή «Εφαρμογή αλλαγών μόνο σε αυτό το φάκελο») ή και στους υποφακέλους τους («Apply changes to this folder, subfolders and files» ή «Εφαρμογή αλλαγών σε αυτό το φάκελο, υποφακέλους και αρχεία»). Αν έχουμε επιλέξει μεμονωμένα αρχεία ενός φακέλου, το λειτουργικό θα μας ρωτήσει αν θέλου-

με να κρυπτογραφήσει μόνο τα αρχεία («Encrypt the file only» ή «Κρυπτογράφηση μόνο του αρχείου») ή και τους φακέλους οι οποίοι τα περιέχουν («Encrypt the file and the parent directory» ή «Κρυπτογράφηση του αρχείου και του γονικού φακέλου»). Τέλος, αν έχουμε επιλέξει και αρχεία και φακέλους, το λειτουργικό θα μας ρωτήσει αν θέλουμε να κρυπτογραφήσει μόνο τα επιλεγμένα αρχεία και φακέλους («Apply changes to the selected items only» ή «Εφαρμογή αλλαγών μόνο στα επιλεγμένα στοιχεία») ή και τους υποφακέλους τους («Apply changes to the selected items, subfolders and files» ή «Εφαρμογή αλλαγών στα επιλεγμένα στοιχεία, υποφακέλους και αρχεία»). Αποφασίζουμε τι θέλουμε να κρυπτογραφήσουμε και πατάμε «OK» για να ολοκληρωθεί η κρυπτογράφηση. Κατά κανόνα, όταν κρυπτογραφούμε φακέλους, θέλουμε να κάνουμε το ίδιο και με τους υποφακέλους τους, ενώ, αντίθετα, σε ό,τι αφορά τα αρχεία, συνήθως θέλουμε να κρυπτογραφηθούν μόνο εκείνα που επιλέγουμε. Αφού ολοκληρωθεί η κρυπτογράφηση, τα κρυπτογραφημένα αρχεία ή/και φάκελοι εμφανίζονται στον Windows Explorer με πράσινο χρώμα. (Με μαύρο χρώμα εμφανίζονται τα απλά αρχεία, ενώ με μπλε τα συμπιεσμένα.) Από τη στιγμή που κρυπτογραφήσουμε κάποια δεδομένα, μπορούμε να εργαζόμαστε κανονικά με αυτά όπως με τα μη κρυπτογραφημένα, καθώς οι διαδικασίες της αποκρυπτογράφησης και της κρυπτογράφησης πραγματοποιούνται αυτόματα στο περιθώριο. Στην περίπτωση που θέλουμε να αποκρυπτογραφήσουμε μόνιμα κάποια δεδομένα από το παράθυρο της κρυπτογράφησης (δεξί κλικ στα δεδομένα/Properties/Advanced... ή δεξί κλικ στα δεδομένα/Ιδιότητες/Για προχωρημένους...) απλώς απενεργοποιούμε την επιλογή κρυπτογράφησης «Encrypt contents to secure data» («Κρυπτογράφηση περιεχομένων για διασφάλιση των δεδομένων»). Σε περίπτωση που θέλουμε να επιτρέψουμε και σε άλλους χρήστες την πρόσβαση σε ένα κρυπτογραφημένο αρχείο, το επι-

## Πώς εμφανίζουμε την καρτέλα «Security» («Ασφάλεια»)

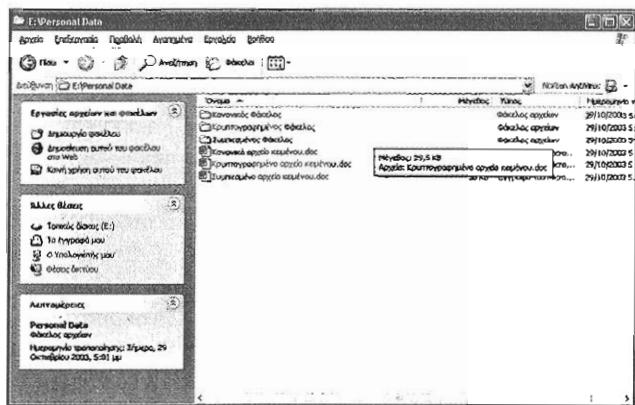
Αν η καρτέλα «Security» («Ασφάλεια») δεν εμφανίζεται στο παράθυρο ιδιοτήτων των αρχείων ή των φακέλων, θα πρέπει να ανοίξουμε τον Windows Explorer [Εξερεύνηση των Windows] και από το μενού «Tools» («Εργαλεία») να επιλέξουμε «Folder Options...» («Επιλογές φακέλων...»). Στη συνέχεια, μεταβαίνουμε στην καρτέλα «View» («Προβολή») και από το τμήμα «Advanced settings:» («Ρυθμίσεις για προχωρημένους:») απενεργοποιούμε την επιλογή «Use simple file sharing (Recommended)» («Χρήση απλής κοινής χρήσης αρχείων [Συνιστάται]»). Η συγκεκριμένη επιλογή είναι τελευταία στη λίστα στα αγγλικά Windows XP και προτελευταία στα ελληνικά.



λέγουμε, μεταφερόμαστε στο παράθυρο κρυπτογράφησης και πατάμε το κουμπί «Details» («Λεπτομέρειες»). Αν το κουμπί αυτό είναι ανενεργό, τότε ή δεν έχουμε κρυπτογραφήσει το αρχείο ή έχουμε επιλέξει κάποιο φάκελο ή περισσότερα του ενός κρυπτογραφημένα αρχεία. Για να επιτρέψουμε και σε άλλους χρήστες την πρόσβαση στο αρχείο, πατάμε το κουμπί «Add...» («Προσθήκη...») και στη συνέχεια «Find User...» («Εύρεση χρήστη...»). Στο παράθυρο που εμφανίζεται πατάμε το κουμπί «Advanced...» («Για προχωρημένους...»), κατόπιν «Find Now» («Εύρεση τώρα») και επιλέγουμε τους χρήστες που θέλουμε.

Για την εξαγωγή ενός αντιγράφου του προσωπικού πιστοποιητικού κρυπτογράφησης, ανοίγουμε τον Internet Explorer και από το μενού «Tools» («Εργαλεία») επιλέγουμε «Internet Options...» («Επιλογές Internet...»). Στη συνέχεια, μεταφερόμαστε στην καρτέλα «Content» («Περιεχόμενο») και πατάμε το κουμπί «Certificates...» («Πιστοποιητικά...»). Από την καρτέλα «Personal» («Προσωπικά στοιχεία») επιλέγουμε το χρήστη με τον οποίο έχουμε κάνει σύνδεση (login) στον υπολογιστή, πατάμε το κουμπί «Export...» («Εξαγωγή») και ακολουθούμε τις οδηγίες των επόμενων παραθύρων. Για την εισαγωγή ενός αντίγραφου του προσωπικού πιστοποιητικού κρυπτογράφησης, από το παράθυρο «Certificates...» («Πιστοποιητικά...») πατάμε το κουμπί «Import...» («Εισαγωγή...») και ακολουθούμε και πάλι τις οδηγίες των επόμενων παραθύρων.

**ΡΥΘΜΙΣΗ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ.** Εκτός από την κρυπτογράφηση των δεδομένων, η οποία, όπως είπαμε, θα πρέπει να γίνεται με μεγάλη προσοχή, μπορούμε να καθορίσουμε ποιοι χρήστες ή



Τα κρυπτογραφημένα αρχεία ή/και φάκελοι εμφανίζονται στο παράθυρο του Windows Explorer [Εξερεύνηση των Windows] με πράσινο χρώμα. Με μπλε χρώμα εμφανίζονται τα συμπίεσμα δεδομένα, ενώ με μαύρο τα απλά αρχεία και οι φάκελοι.

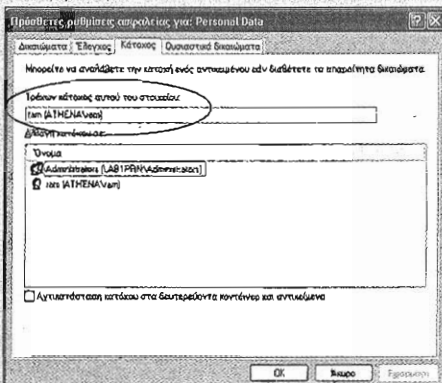
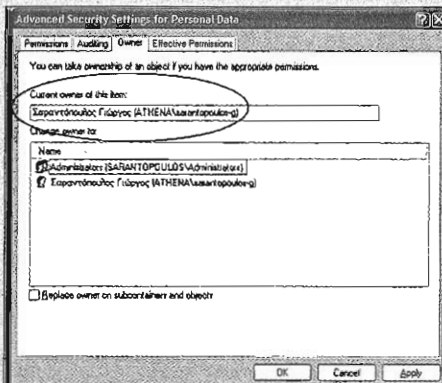
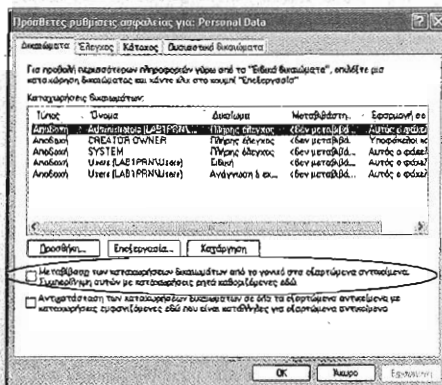
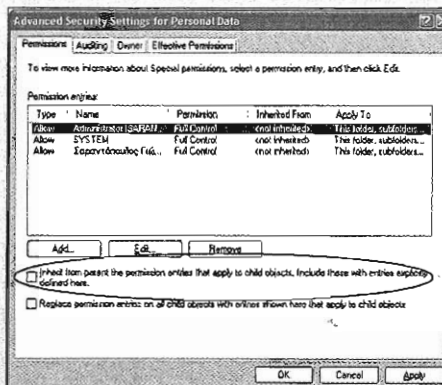
οιες ομάδες χρηστών θα έχουν πρόσβαση στα δεδομένα του υπολογιστή μας. Η δυνατότητα πρόσβασης ενός χρήστη στα δεδομένα ενός αρχείου ή ενός φακέλου, καθώς και οι επιτρεπτές ενέργειες που μπορούν να πραγματοποιηθούν με τα δεδομένα, καθορίζουν τα δικαιώματα του χρήστη στο συγκεκριμένο αρχείο ή φάκελο. Εάν, για παράδειγμα, κάποιος έχει μόνο δικαίωμα ανάγνωσης σε ένα αρχείο, τότε μπορεί να δει τα δεδομένα του, αλλά δεν μπορεί να τροποποιήσει, να διαγράψει ή να μετακινηθεί το αρχείο. Τις περισσότερες φορές είναι προτιμότερο να καθορίζουμε δικαιώματα πρόσβασης σε ομάδες χρηστών και όχι σε μεμονωμένους χρήστες. Ειδικά στην περίπτωση που ο υπολογιστής μας είναι συνδεδεμένος σε κάποιο Domain (Τομέα) με πολλούς χρήστες, ο διαχωρισμός των χρηστών σε ομάδες απλοποιεί σε μεγάλο βαθμό τον καθορισμό των δικαιωμάτων. Αυτό συμβαίνει γιατί από τη στιγμή που θα καθορίσουμε τα δικαιώματα των δεδομένων σε ομάδες χρηστών και όχι σε μεμονωμένους χρήστες, κάθε νέο χρήστη που προστίθεται στο Domain αρκεί να τον κατατάξουμε σε μία ή περισσότερες ομάδες χρηστών και να αποκτήσει αυτόματα τα απαραίτητα δικαιώματα στα δεδομένα. Στην περίπτωση, βέβαια, που ο υπολογιστής μας δεν είναι συνδεδεμένος σε δίκτυο με πολλούς υπολογιστές ή αν έχουμε πρόσβαση σε αυτόν μόνο δύο, τρεις χρήστες ή αν θέλουμε πρακτικά να απαγορεύσουμε την πρόσβαση σε όλους τους άλλους χρήστες, τότε είναι ευκολότερο να διανείμετε τα δικαιώματα πρόσβασης ανά χρήστη και όχι ανά ομάδα χρηστών.

Δικαιώματα μπορούμε να καθορίσουμε σε διάφορα αντικείμενα του λειτουργικού συστήματος ή του υπολογιστή, όπως τα αρχεία, οι φάκελοι, οι εκτυπωτές, τα κλειδιά μητρώου κ.λπ. Σε κάθε αντικείμενο μάλιστα αντιστοιχούν διαφορετικά δικαιώματα. Τα αρχεία, για παράδειγμα, έχουν δικαιώματα εκτέλεσης, ενώ οι φάκελοι όχι. Παρ' όλο αυτό, υπάρχουν κάποια δικαιώματα που είναι κοινά για τα περισσότερα αντικείμενα, όπως το δικαίωμα ανάγνωσης, το δικαίωμα τροποποίησης, η αλλαγή κατόχου και η διαγραφή. Όταν καθορίζουμε δικαιώματα, ορίζουμε το επίπεδο πρόσβασης που θα έχουν οι χρήστες. Έτσι, μπορούμε να επιτρέψουμε σε ένα χρήστη να διαβάζει τα περιεχόμενα ενός αρχείου, σε έναν άλλο να κάνει αλλαγές, και να απαγορεύσουμε την πρόσβαση όλων των υπόλοιπων χρηστών. Κάθε

αντικείμενο έχει έναν κάτοχο, ο οποίος από προεπιλογή του λειτουργικού συστήματος είναι ο δημιουργός του. Ανεξάρτητα από τα δικαιώματα που έχουν οριστεί, ο κάτοχος ενός αντικειμένου μπορεί οποιαδήποτε στιγμή να αλλάξει τα δικαιώματά του. Την κατοχή ενός αντικειμένου μπορεί να την πάρει όποιος χρήστης διαθέτει το δικαίωμα «Ανάληψη κατοχής» («Take ownership»). Οι διαχειριστές του συστήματος (ομάδα Administrators) διαθέτουν από προεπιλογή το δικαίωμα ανάληψης κατοχής, όμως δεν μπορούν να τη μεταβιβάσουν σε τρίτους. Για να αλλάξουμε τα δικαιώματα ενός αντικειμένου, θα πρέπει να είμαστε κάτοχοί του, να μας έχει εκχωρηθεί το δικαίωμα να κάνουμε αλλαγές (δικαίωμα «Change Permissions» ή «Αλλαγή δικαιωμάτων») ή να έχουμε τον πλήρη έλεγχο του αντικειμένου (δικαίωμα «Full Control» ή «Πλήρης έλεγχος»).

**ΑΛΛΑΓΗ ΔΙΚΑΙΩΜΑΤΩΝ ΣΤΑ ΔΕΔΟΜΕΝΑ.** Όπως είπαμε, τα δικαιώματα των δεδομένων καθορίζουν τι ακριβώς μπορεί να κάνει κάποιος με αυτά. Έτσι, αν θέλουμε να προστατέψουμε ορισμένα αρχεία και φακέλους του υπολογιστή μας, θα πρέπει να περιορίσουμε τα δικαιώματα των χρηστών σε αυτά. Επειδή τα αρχεία και οι φάκελοι έχουν διαφορετικά δικαιώματα, για την τροποποίηση των δικαιωμάτων θα πρέπει να επιλέξουμε αντικείμενα του ίδιου τύπου (π.χ., μόνο αρχεία ή μόνο φακέλους). Η διαδικασία πάντως που ακολουθούμε είναι ίδια, ανεξάρτητα από το είδος των δεδομένων. Τις περισσότερες φορές πραγματοποιούμε αλλαγές δικαιωμάτων σε φακέλους, γιατί με αυτό τον τρόπο αποτρέπουμε την πρόσβαση σε όλα τα αρχεία που περιέχει ο φάκελος.

Για να αλλάξουμε τα δικαιώματα επιλέγουμε ένα ή περισσότερα αντικείμενα του ίδιου τύπου (π.χ., μόνο φακέλους), κάνουμε δεξί κλικ πάνω τους και διαλέγουμε «Properties» («Ιδιότητες»). Για την αλλαγή των δικαιωμάτων θα πρέπει να μεταβούμε στην καρτέλα «Security» («Ασφάλεια»). Από εκεί, στο πλαίσιο «Group or user names:» («Ονόματα ομάδων ή χρηστών:») βλέπουμε τους χρήστες ή τις ομάδες χρηστών για τους οποίους έχουν καθοριστεί δικαιώματα. Επιλέγοντας κάποιον από τη λίστα, στο πλαίσιο «Permissions for:» («Δικαιώματα για:») εμφανίζονται τα κυριότερα δικαιώματά του για τα επιλεγμένα αντικείμενα (στην περίπτωση μας για τους φακέλους). Δίπλα από κάθε δικαίωμα υπάρχουν δύο κουτάκια, ένα κάτω από τη στήλη «Allow» («Αποδοχή») και ένα κάτω από τη στήλη «Deny» («Άρνηση»). Όταν είναι τσεκαρισμένο το κουτάκι κάτω από τη στήλη αποδοχής, τότε ο χρήστης διαθέτει το αντίστοιχο δικαίωμα. Αντίθετα, όταν είναι τσεκαρισμένο το κουτάκι κάτω από τη στήλη άρνησης, τότε το αντίστοιχο δικαίωμα αφαιρείται από το χρήστη. Τέλος, αν δίπλα από ένα δικαίωμα δεν είναι τσεκαρισμένο κανένα κουτάκι, τότε το αντίστοιχο δικαίωμα δεν προσφέρεται μεν στο χρήστη, αλλά ταυτόχρονα δεν του αφαιρείται στην περίπτωση που ανήκει σε μία ομάδα χρηστών στην οποία προσφέρεται το εν λόγω δικαίωμα (π.χ., στην ομάδα των Administrators). Δεδομένου ότι η άρνηση ενός δικαιώματος υπερισχύει της προσφοράς, αν θέλουμε οπωσδήποτε να αποκλείσουμε ένα χρήστη από κάποιο δικαίωμα θα πρέπει να τσεκάρουμε το κουτάκι της άρνησης. Αν θέλουμε να μάθουμε ποια ακριβώς δικαιώματα διαθέτει ένας χρήστης ή μία ομάδα χρηστών, δεν έχουμε παρά να πατήσουμε το κουμπί «Advanced» («Για προχωρημένους») και να



Για να μεταβάλουμε τα δικαιώματα ενός φακέλου, τις περισσότερες φορές θα πρέπει πρώτα να μεταβούμε στην καρτέλα «Permissions» («Δικαιώματα») και να απενεργοποιήσουμε το πλαίσιο ελέγχου «Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.» («Μεταβίβαση των καταχωρίσεων δικαιωμάτων από το γονικό στα εξαρτώμενα αντικείμενα»). Στο παράθυρο διαλόγου που θα εμφανιστεί, συνήθως επιλέγουμε «Copy» («Αντιγραφή») για να τροποποιήσουμε τα δικαιώματα στους υπάρχοντες χρήστες και όχι «Remove» («Κατάργηση»), καθώς με αυτή την επιλογή θα πρέπει να καθορίσουμε εκ νέου χρήστες και δικαιώματα.

Ο κάτοχος ενός φακέλου ή ενός αρχείου εμφανίζεται στην καρτέλα «Owner» («Κάτοχος») των προχωρημένων (Advanced) επιλογών της καρτέλας ασφαλείας.

μεταβούμε στην καρτέλα «Effective Permissions» («Ουσιαστικά δικαιώματα»). Από εκεί επιλέγουμε το χρήστη που μας ενδιαφέρει πατώντας το κουμπί «Select...» («Επιλογή...») και ακολουθούμε την τυποποιημένη διαδικασία των Windows XP για την επιλογή χρήστη: Διαλέγουμε το Domain ή τον τοπικό υπολογιστή από το κουμπί «Locations...» («Τοποθεσίες»), καθορίζουμε το χρήστη πατώντας το κουμπί «Advanced...» («Για προχωρημένους...») και κατόπιν πατάμε το κουμπί «Find Now» («Εύρεση τώρα»). Όταν επιστρέψουμε στην καρτέλα των ουσιαστικών δικαιωμάτων, τα δικαιώματα που διαθέτει ο χρήστης έχουν τεκμαρισμένο το αντίστοιχο κουτάκι.

Τις περισσότερες φορές από την καρτέλα «Security» («Ασφάλεια») των ιδιοτήτων μπορούμε να προσθέσουμε ή να αφαιρέσουμε χρήστες, καθώς και να ρυθμίσουμε τα περισσότερα δικαιώματά τους χωρίς να χρειάζεται να μεταβούμε στις προχωρημένες (Advanced) επιλογές. Για να προσθέσουμε ένα χρήστη, πατάμε το κουμπί «Add...» («Προσθήκη...») και τον επιλέγουμε, ενώ για να τον αφαιρέσουμε από τη λίστα δικαιωμάτων τον διαλέγουμε και πατάμε το κουμπί «Remove» («Κατάργηση»). Στην περίπτωση που δεν επιτρέπεται να αφαιρέσουμε ένα χρήστη από τη λίστα ή θέλουμε να μεταβάλουμε ένα δικαίωμα αλλιώς τα κουτάκια αλλαγής δικαιωμάτων είναι ανενεργά και δεν επιδέχονται τροποποίηση, θα πρέπει να πατήσουμε το πλήκτρο «Advanced» («Για προχωρημένους») και από την καρτέλα «Permissions» («Δικαιώματα») να απενεργοποιήσουμε το πλαίσιο ελέγχου «Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.» («Μεταβίβαση των καταχωρίσεων δικαιωμάτων από το γονικό στα εξαρτώμενα αντικείμενα»). Στο παράθυρο

διαλόγου που θα εμφανιστεί είτε επιλέγουμε «Copy» («Αντιγραφή») για να τροποποιήσουμε τα δικαιώματα στους υπάρχοντες χρήστες είτε «Remove» («Κατάργηση») για να καθορίσουμε εκ νέου χρήστες και δικαιώματα. Να σημειώσουμε ότι τα δικαιώματα ενός φακέλου (γονικός φάκελος) μεταβιβάζονται σε όλους τους υποφακέλους του. Στην καρτέλα «Permissions» («Δικαιώματα») εμφανίζονται επιπρόσθετα μία λίστα με τους χρήστες στους οποίους έχουν καθοριστεί δικαιώματα, καθώς και μία μικρή περιγραφή των δικαιωμάτων. Επιλέγοντας ένα χρήστη και πατώντας το πλήκτρο «Edit...» («Επεξεργασία...»), βλέπουμε αναλυτικά όλα τα δικαιώματα –και όχι μόνο τα σπουδαιότερα–, όπως εμφανίζονται στη βασική καρτέλα ασφαλείας. Αν μόλις έχουμε αφαιρέσει την εξάρτηση των δικαιωμάτων από το γονικό φάκελο, μπορούμε από το πεδίο «Apply onto:» («Εφαρμογή σε:») να καθορίσουμε αν οι αλλαγές των δικαιωμάτων θα αφορούν στο φάκελο, στους υποφακέλους και στα αρχεία, μόνο στα αρχεία κ.λπ.

Τέλος, στην περίπτωση που θέλουμε να δούμε ποιος είναι ο κάτοχος ενός φακέλου, ενός αρχείου και γενικότερα ενός αντικειμένου, από την καρτέλα ασφαλείας των ιδιοτήτων του πατάμε το κουμπί «Advanced» («Για προχωρημένους») και επιλέγουμε την καρτέλα «Owner» («Κάτοχος»). Από εδώ μπορούμε να πληροφορηθούμε και να αλλάξουμε τον κάτοχο επιλέγοντας κάποιοι άλλο από τη διαθέσιμη λίστα.

**ΤΑ ΔΙΚΑΙΩΜΑΤΑ ΣΤΗΝ ΠΡΑΞΗ.** Αν θέλουμε να αποκλείσουμε την πρόσβαση από οποιονδήποτε άλλο χρήστη στα περιεχόμενα ενός φακέλου, θα πρέπει να μεταφερθούμε στην καρτέλα ασφαλείας και να αφαιρέσουμε όλους τους άλλους χρήστες από τη



λίστα. Από τη λίστα αυτή καλό θα ήταν να μην αφαιρέσουμε την ομάδα χρηστών SYSTEM, καθώς τη χρησιμοποιεί το λειτουργικό σύστημα για διάφορες εργασίες (π.χ., συμπίεση ή κρυπτογράφηση αρχείων και φακέλων). Αν θέλουμε να έχουμε μόνο εμείς δικαίωμα πρόσβασης στα δεδομένα, ας αφαιρέσουμε από τη λίστα χρηστών και τους διαχειριστές του τομέα με τον οποίο είναι συνδεδεμένος ο υπολογιστής μας (ομάδα Administrators του Domain). Τους διαχειριστές του τοπικού υπολογιστή μπορούμε να τους αφήσουμε ως δικλίδας ασφαλείας. Θα ήταν συνεπώς όμως να αφαιρέσουμε από την ομάδα των τοπικών διαχειριστών τους περιττούς χρήστες ή να δηλώσουμε ρητά άρνηση πρόσβασης σε όλους χρήστες ανήκουν στην ομάδα των τοπικών διαχειριστών αλλά δεν γνωρίζουμε τον κωδικό πρόσβασής τους. Ανάλογους περιορισμούς μπορούμε να θέσουμε και σε ένα δίσκο ή σε μια κατάρτηση δίσκου με σύστημα αρχείων NTFS από την καρτέλα ασφαλείας των ιδιοτήτων του δίσκου.

**ΕΠΑΝΑΚΤΗΣΗ ΕΛΕΓΧΟΥ.** Σε περίπτωση που εγκαταστήσουμε εκ νέου τα Windows XP ή μεταφέρουμε το σκληρό δίσκο σε άλλον υπολογιστή, θα πρέπει να επανακτήσουμε τον έλεγχο στα δεδομένα που είχαμε θέσει περιορισμούς πρόσβασης. Για το σκοπό αυτό, από την καρτέλα ασφαλείας των δεδομένων πατάμε «Advanced» («Για προχωρημένους»), μεταφερόμαστε στην καρτέλα «Owner» («Κάτοχος») και ορίζουμε τον εαυτό μας ως νέο κάτοχο. Από αυτή τη στιγμή μπορούμε να επανακαθορίσουμε τα δικαιώματα πρόσβασης και να δούμε τα δεδομένα μας. Να σημειώσουμε ότι αυτή τη διαδικασία μπορεί να την πραγματοποιήσει ανά πάσα στιγμή ένας administrator και να έχει πρόσβαση στα δεδομένα μας. Δεδομένου όμως ότι οι διαχειριστές του συστήματος μπορούν να αναλάβουν την κατοχή ενός αντικειμένου αλλά όχι και να τη μεταβιβάσουν, εμείς θα είμαστε σε θέση να εντοπίσουμε την παραβίαση, καθώς θα έχουμε χάσει την κυριότητα των δεδομένων μας. Για να μπορέσει όμως ένας διαχειριστής να αναλάβει την κατοχή, θα πρέπει να έχει πρόσβαση στον υπολογιστή μας. Αν θεωρούμε ότι μπορούμε και χωρίς τη συμβαλή του και ταυτόχρονα δεν παραβαίνουμε τους κανονισμούς της εταιρείας μας, τότε καλό θα ήταν να αποκλείσουμε τους διαχειριστές του τομέα ακόμα και από τη διαδικασία logon του υπολογιστή μας. Για να το πραγματοποιήσουμε αυτό, θα πρέπει να κάνουμε δεξί κλικ στο εικονίδιο του υπολογιστή μας, να διαλέξουμε «Manage» («Διαχείριση») και να μεταβούμε στην κατηγορία «Local Users and Groups» («Τοπικοί λογαριασμοί Users και Groups»). Κατόπιν, ανοίγουμε την κατηγορία Groups και από την ομάδα Administrators αφαιρούμε τους διαχειριστές του Τομέα και όποιον άλλο χρήστη δεν θέλουμε να έχει προνόμια διαχειριστή στον υπολογιστή μας. Εννοείται φυσικά ότι πρέπει να αφήσουμε τουλάχιστον τον εαυτό μας στην ομάδα των Administrators. Αν επιθυμούμε, βέβαια, μπορούμε να αναδιοργανώσουμε και τις υπόλοιπες ομάδες χρηστών τοποθετώντας όλους τους χρήστες που θέλουμε να μπαίνουν στον υπολογιστή μας στην ομάδα των απλών χρηστών (ομάδα Users). Στο κάτω κάτω, αν θέλουμε να κάνουμε μόνο εμείς κουμάντο στον υπολογιστή μας, όλοι οι άλλοι χρήστες θα πρέπει να έχουν περιορισμένες δυνατότητες.

# Ενεργοποιήστε τον κατάσκοπο του υπολογιστή σας

Θέλετε να γνωρίζετε ποια μηνύματα αποθηκεύει το λειτουργικό σύστημα για τους οδηγούς, την ασφάλεια του συστήματος και τις συσκευές; Θέλετε να ξέρετε ποιοι και πότε έχουν πρόσβαση σε συγκεκριμένα αρχεία του υπολογιστή σας; Αν η απάντηση στα παραπάνω ερωτήματα είναι καταφατική, τη λύση δίνουν τα Windows XP Professional.

**Τ**α Windows XP Professional, όπως και τα Windows 2000, καταγράφουν ορισμένα από τα συμβάντα του υπολογιστή σε ειδικά αρχεία. Με αυτό τον τρόπο οι διαχειριστές ή οι προγραμματιστές μπορούν να συγκεντρώνουν πληροφορίες για τα προβλήματα του υλικού, των εφαρμογών και της ασφάλειας του υπολογιστή ή να προβλέπουν προβλήματα που είναι δυνατόν να προκύψουν μελλοντικά και να επηρεάσουν την ομαλή λειτουργία του υπολογιστή. Αν, για παράδειγμα, ο οδηγός μιας συσκευής αποτύχει να φορτωθεί, αν μια κάρτα δικτύου αποσυνδέεται περιστασιακά από το δίκτυο ή αν μια εφαρμογή αναφέρει σφάλμα σε κάποιο από τα αρχεία της, το λειτουργικό θα καταγράψει αυτές τις αναφορές στα κατάλληλα αρχεία έτσι ώστε να είμαστε σε θέση να διαπιστώσουμε ή και να προβλέψουμε τη βλάβη ή το ελαττωματικό περιφερειακό. Επιπρόσθετα, αν πραγματοποιήσουμε τις κατάλληλες ρυθμίσεις στο λειτουργικό, μπορούμε να ελέγχουμε ποιοι χρήστες έχουν πρόσβαση στα αρχεία μας.










**ΚΑΤΗΓΟΡΙΕΣ ΣΥΜΒΑΝΤΩΝ.** Τα Windows XP χρησιμοποιούν τρία αρχεία καταγραφής συμβάντων τα οποία βρίσκονται στο φάκελο «system32\config» των Windows XP (συνήθως είναι ο φάκελος «WINDOWS\system32\config» ή ο «WINNT\system32\config»). Τα συμβάντα που

σχετίζονται όμοια με την ασφάλεια του υπολογιστή καταγράφονται στο αρχείο «secevent.evnt», που ονομάζεται αρχείο καταγραφής ασφαλείας (Security log). Τα συμβάντα που δημιουργούνται από τις εφαρμογές που είτε είναι προεγκατεστημένες στα Windows XP είτε τις έχουμε εγκαταστήσει μόνοι μας καταγράφονται στο αρχείο «aprevent.evnt» το οποίο καλείται αρχείο καταγραφής εφαρμογών (Application log). Τέλος, οι καταγραφές που αφορούν στα ίδια τα Windows XP και στις συσκευές του υπολογιστή καταγράφονται στο αρχείο «sysevent.evnt», που ονομάζεται αρχείο καταγραφής συστήματος (System log). Να σημειώσουμε ότι, αν ο υπολογιστής έχει ρυθμιστεί ως ελεγκτής τομέα (domain controller), τότε χρησιμοποιούνται άλλα τρία αρχεία καταγραφής: ένα για την υπηρεσία καταλόγου (Directory service), ένα για την υπηρεσία αναπαραγωγής αρχείων (File Replication service) και ένα για την υπηρεσία Domain Name Service (DNS service). Οι τρεις προηγούμενες καταγραφές βέβαια δεν γίνονται από τους υπολογιστές των απλών χρηστών οι οποίοι διαθέτουν είτε Windows XP Professional είτε Windows XP Home Edition.

Αν θέλουμε να μάθουμε ποια συμβάντα (προγράμματα, περιφερειακά ή καταστάσεις) είναι δυνατόν να δημιουργήσουν

Type	Date	Time	Source	Category	Event	User	Computer
Warning	27/5/2004	6:53:07 μμ	Print	None	8	SYSTEM	SARANTOPOULOS
Warning	27/5/2004	6:53:34 μμ	Print	None	3	SYSTEM	SARANTOPOULOS
Warning	27/5/2004	6:53:34 μμ	Print	None	4	SYSTEM	SARANTOPOULOS
Warning	27/5/2004	6:53:34 μμ	Print	None	9	SYSTEM	SARANTOPOULOS
Error	27/5/2004	6:42:51 μμ	TermService	None	1111	N/A	SARANTOPOULOS
Error	27/5/2004	6:42:50 μμ	TermService	None	1111	N/A	SARANTOPOULOS
Warning	27/5/2004	6:42:41 μμ	Print	None	3	SYSTEM	SARANTOPOULOS
Warning	27/5/2004	6:42:40 μμ	Print	None	4	SYSTEM	SARANTOPOULOS
Warning	27/5/2004	6:42:40 μμ	Print	None	8	SYSTEM	SARANTOPOULOS
Warning	27/5/2004	3:10:30 μμ	Hardib	None	3019	N/A	SARANTOPOULOS
Error	27/5/2004	12:42:25 μμ	Print	None	33	SYSTEM	SARANTOPOULOS
Information	27/5/2004	12:41:56 μμ	Service Control Manager	None	7025	N/A	SARANTOPOULOS
Information	27/5/2004	12:41:56 μμ	Service Control Manager	None	7025	N/A	SARANTOPOULOS
Information	27/5/2004	12:41:56 μμ	Service Control Manager	None	7025	N/A	SARANTOPOULOS
Information	27/5/2004	12:41:55 μμ	Service Control Manager	None	7025	N/A	SARANTOPOULOS
Information	27/5/2004	12:41:54 μμ	Service Control Manager	None	7025	N/A	SARANTOPOULOS
Information	27/5/2004	12:41:53 μμ	Service Control Manager	None	7025	SYSTEM	SARANTOPOULOS
Error	27/5/2004	12:41:48 μμ	TermService	None	1111	N/A	SARANTOPOULOS
Error	27/5/2004	12:41:47 μμ	TermService	None	1111	N/A	SARANTOPOULOS
Information	27/5/2004	12:41:40 μμ	Service Control Manager	None	7025	N/A	SARANTOPOULOS
Information	27/5/2004	12:41:40 μμ	Service Control Manager	None	7025	LOCAL SERV...	SARANTOPOULOS
Information	27/5/2004	12:41:40 μμ	Service Control Manager	None	7025	N/A	SARANTOPOULOS

Η κονσόλα Event Viewer (Προβολής συμβάντων) στην αγγλική και ελληνική έκδοση των Windows XP εμφανίζεται πληκτρολογώντας «eventvwr.msc» από το παράθυρο εντολών («Start Run...» ή «Εναρξη... Εκτέλεση...»). Το αριστερό τμήμα του παραθύρου ονομάζεται «δέντρο της κονσόλας» (console tree) και κάτω από την ονομασία «Event Viewer (Local)» («Προβολή Συμβάντων (τοπικών)») υπάρχουν τρία στοιχεία, τα Application, Security και System (Εφαρμογή, Ασφάλεια και Σύστημα), τα οποία αντιστοιχούν στα αρχεία καταγραφής εφαρμογών, ασφαλείας και συστήματος. Επιλέγοντας κάποιο από αυτά, στο δεξιό τμήμα της κονσόλας παρουσιάζονται τα καταγεγραμμένα συμβάντα του αρχείου.

 Error	 Σφάλμα
 Warning	 Προειδοποίηση
 Information	 Επιτυχημένος έλεγχος
 Success Audit	 Αποτυχημένος έλεγχος
 Failure Audit	

Τα συμβάντα στα αρχεία καταγραφής χωρίζονται σε πέντε διαφορετικούς τύπους. Στα αγγλικά Windows XP είναι οι «Error», «Warning» και «Information» που εμφανίζονται στα συμβάντα των κατηγοριών Application και System, και οι «Success Audit» και «Failure Audit» που εμφανίζονται στα συμβάντα της κατηγορίας Security. Στα ελληνικά Windows XP οι τύποι των συμβάντων ονομάζονται αντίστοιχα «Σφάλμα», «Προειδοποίηση», «Πληροφορίες», «Επιτυχημένος έλεγχος» και «Αποτυχημένος έλεγχος».

εγγραφές στα αρχεία καταγραφής όταν συντρέχει κάποιος λόγος, θα πρέπει να ανοίξουμε το μητρώο (registry) πληκτρολογώντας από το παράθυρο εκτέλεσης εντολών («Start / Run...» ή «Εναρξη / Εκτέλεση...») την εντολή «regedit». Στη θέση «HKEY\_CURRENT\_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ Eventlog» υπάρχουν τρεις φάκελοι (κλειδιά), οι Application, Security και System, τους οποίους, αν ανοίξουμε, θα δούμε και άλλους υποφάκελους (υποκλειδιά). Αυτοί αντιστοιχούν στα συμβάντα που μπορούν να δημιουργήσουν εγγραφές στα αρχεία καταγραφής εφαρμογών, ασφάλειας και συστήματος. Εναλλακτικά, αντί να ανοίξουμε τους τρεις υποφάκελους, έχουμε τη δυνατότητα να τους επιλέξουμε και να ανοίξουμε το αρχείο [τιμή] «Source» που υπάρχει σε καθέναν από αυτούς.

## Η ΚΟΝΣΟΛΑ EVENT VIEWER («ΠΡΟΓΡΑΜΜΑ ΠΡΟΒΟΛΗΣ ΣΥΜΒΑΝΤΩΝ»)

. Για να δούμε τις «κατασκοπευτικές» καταγραφές του λειτουργικού συστήματος θα πρέπει να χρησιμοποιήσουμε το εργαλείο «Event Viewer» («Προβολή Συμβάντων») της κονσόλας διαχείρισης της Microsoft (Microsoft Management Console ή MMC). Να υπενθυμίσουμε ότι η κονσόλα διαχείρισης προσφέρει αρκετά εργαλεία για τον εύκολο καθορισμό των παραμέτρων και γενικά για τη διαχείριση του λειτουργικού συστήματος. Ο πιο απλός τρόπος για να εμφανίσουμε το παράθυρο της προβολής συμβάντων είναι να πληκτρολογήσουμε στο παράθυρο εκτέλεσης εντολών («Start / Run...» ή «Εναρξη / Εκτέλεση...») την εντολή «eventvwr.msc». Εναλλακτικά, μπορούμε να ανατρέξουμε μέσα στο «Control Panel» («Πίνακα ελέγχου») επιλέγοντας «Start / Control Panel» («Εναρξη / Πίνακας Ελέγχου»). Αν χρησιμοποιούμε την κλασική προβολή (Classic View), θα επιλέξουμε «Administrative Tools» («Εργαλεία διαχείρισης») και κατόπιν «Event Viewer» («Προβολή Συμβάντων»). Εάν χρησιμοποιούμε την προβολή κατηγοριών (Category View), τότε θα επιλέξουμε «Performance and Maintenance» («Επιδόσεις και Συντήρηση»), στη συνέχεια «Administrative Tools» («Εργαλεία διαχείρισης») και μετά «Event Viewer» («Προβολή Συμβάντων»).

Το παράθυρο που εμφανίζεται είναι η κονσόλα Event Viewer («Πρόγραμμα προβολής συμβάντων»). Το αριστερό τμήμα του παραθύρου ονομάζεται «δέντρο της κονσόλας» (console tree) και κάτω από την ονομασία «Event Viewer [Local]» («Προβολή Συμβάντων [τοπικών]») υπάρχουν τρία στοιχεία, τα Application, Security και System (Εφαρμογή, Ασφάλεια και Σύστημα), τα οποία αντιστοιχούν στα αρχεία καταγραφής εφαρμογών, ασφάλειας και συστήματος. Επιλέγοντας κάποιο από αυτά, το δεξί τμήμα της κονσόλας εμφανίζει τις εγγραφές του αντίστοιχου αρχείου καταγραφής. Στα αρχεία Application και System οι εγγραφές χωρίζονται σε τρεις διαφορετικούς τύπους μηνυμάτων, τους Error (Σφάλμα), Warning (Προειδοποίηση)

και Information (Πληροφορίες). Στο αρχείο Security οι εγγραφές χωρίζονται σε δύο τύπους: «Success Audit» («Επιτυχημένος έλεγχος») και «Failure Audit» («Αποτυχημένος έλεγχος»). As τους δούμε λίγο πιο αναλυτικά:

**Error (Σφάλμα).** Συμβολίζονται με έναν κόκκινο κύκλο μέσα στον οποίο υπάρχει με λευκό χρώμα το κεφαλαίο γράμμα «X». Οι εγγραφές αυτού του τύπου είναι οι πιο σημαντικές καθώς περιλαμβάνουν σφάλματα, απώλειες δεδομένων και προβλήματα λειτουργικότητας. Ως σφάλμα, για παράδειγμα, χαρακτηρίζεται η αποσύνδεση μιας κάρτας δικτύου ή η αποτυχία να φορτωθεί κατά την εκκίνηση μια συσκευή ή μια υπηρεσία (service).

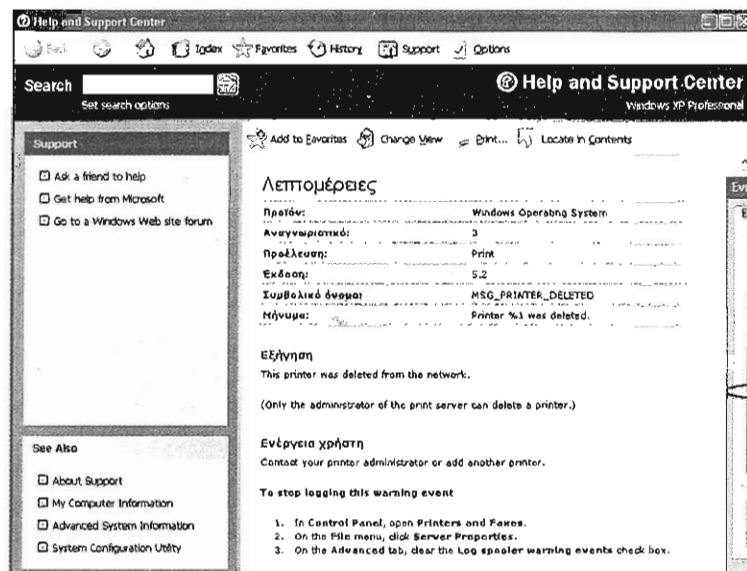
**Warning (Προειδοποίηση).** Συμβολίζονται με ένα κίτρινο τρίγωνο μέσα στο οποίο υπάρχει ένα θυμαστικό. Οι καταγραφές αυτού του τύπου αντιπροσωπεύουν λιγότερο σημαντικά προβλήματα από τον προηγούμενο τύπο, αλλά ενδέχεται να υποδεικνύουν μελλοντικά προβλήματα. Ως προειδοποίηση θεωρείται, π.χ., η αποτυχία να κλείσει ο υπολογιστής ύστερα από εντολή μας.

**Information (Πληροφορίες).** Συμβολίζονται από ένα λευκό συννεφάκι μέσα στο οποίο είναι γραμμένο με μπλε χρώμα το πεζό γράμμα «i». Οι καταγραφές αυτές μας πληροφορούν για διάφορα συμβάντα, όπως η χρήση ενός εκτυπωτή που είναι συνδεδεμένος στον υπολογιστή μας, η επιτυχής έναρξη ορισμένων εφαρμογών και υπηρεσιών (services), η σύνδεση ή η αποσύνδεση του μόντεμ με τον παροχέα υπηρεσιών Internet κ.λπ.

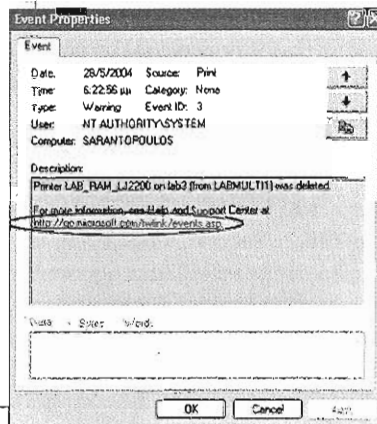
**Success Audit (Επιτυχημένος έλεγχος).** Συμβολίζονται με ένα κλειδί και αφορούν στις επιτυχημένες προσπάθειες του χρήστη ή του συστήματος να ολοκληρώσει μια διεργασία που έχει σχέση με την ασφάλεια — οι καταγραφές της επιτυχημένης εισόδου ή εξόδου, για παράδειγμα, ενός χρήστη στο λογαριασμό του (log on/log off) ή η προσπάθεια ενός αρχείου. Να σημειώσουμε όμως ότι για να πραγματοποιηθούν ανάλογες καταγραφές θα πρέπει να έχουμε δηλώσει προηγουμένως από την Κονσόλα καθορισμού ασφαλείας («Local Security Settings» ή «Τοπικές ρυθμίσεις ασφαλείας») ή από την Κονσόλα καθορισμού πολιτικής ομάδας («Group Policy» ή «Πολιτική ομάδας») ότι θέλουμε το λειτουργικό να παρακολουθεί αυτούς τους τομείς ασφαλείας. Για τις ρυθμίσεις αυτές θα αναφερθούμε αναλυτικότερα στη συνέχεια του άρθρου.

**Failure Audit (Αποτυχημένος έλεγχος).** Συμβολίζονται με ένα κλειδωμένο λουκέτο και αφορούν στις αποτυχημένες προσπάθειες του χρήστη ή του συστήματος να ολοκληρώσει μια διεργασία που έχει σχέση με την ασφάλεια. Καταγραφές αυτού του τύπου εμφανίζονται, π.χ., όταν ένας χρήστης δώσει λάθος κωδικό (password) και αποτύχει να μπει στο σύστημα (log on) ή προσπαθήσει να δει τα περιεχόμενα ενός φακέλου ή αρχείου όπου δεν έχει δικαιώματα πρόσβασης. Όπως και





Κάνοντας διπλό κλικ πάνω σε ένα καταγραφμένο συμβάν, μαθαίνουμε περισσότερες λεπτομέρειες γι' αυτό. Αν θέλουμε περισσότερες πληροφορίες για το τι μπορούμε να κάνουμε ώστε να αντιμετωπίσουμε το πρόβλημα, θα χρειαστεί να κάνουμε κλικ στα δεσμά που υπάρχει στο τέλος της περιγραφής. Για το σκοπό αυτό όμως θα πρέπει να είμαστε συνδεδεμένοι με το Internet.

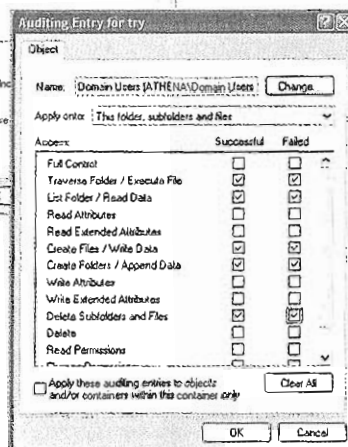
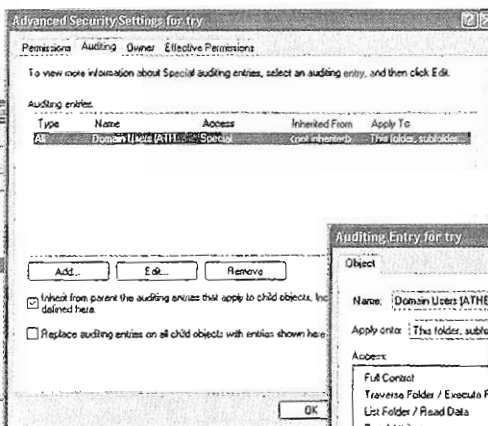
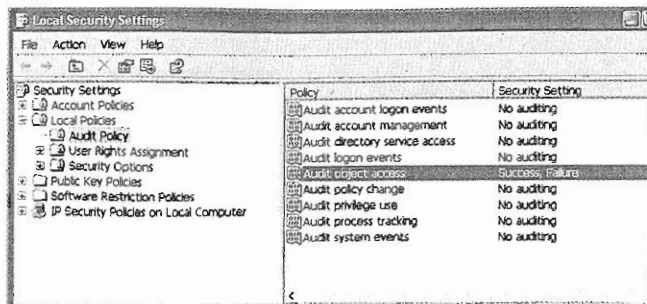


στις εγγραφές Success Audit, για να εμφανίζονται ανάλογες καταχωρίσεις στο αρχείο καταγραφής ασφάλειας θα πρέπει να έχουμε κάνει πρώτα ορισμένες ρυθμίσεις.

**ΠΕΡΙΓΡΑΦΗ ΤΩΝ ΣΥΜΒΑΝΤΩΝ.** Επιλέγοντας κάποιο από τα τρία αρχεία καταγραφής, στο δεξί τμήμα της κονσόλας εμφανίζονται οι εγγραφές του αρχείου ταξινομημένες με βάση τη χρονική στιγμή που έγιναν. Ταυτόχρονα, για κάθε εγγραφή υπάρχουν διάφορες στήλες οι οποίες αναγράφουν πληροφορίες για το είδος του συμβάντος. Στη στήλη Type (Τύπος) παρουσιάζεται ο τύπος του μηνύματος (Σφάλμα, Προειδοποίηση κ.λπ.), ενώ στις στήλες Date (Ημερομηνία) και Time (Ώρα) η χρονική στιγμή που πραγματοποιήθηκε το συμβάν που καταγράφεται. Να σημειώσουμε ότι το σύστημα αποθηκεύει τις εγγραφές με βάση την ώρα του Γκρίνουιτς και μας τις εμφανίζει στην τοπική μας ώρα λαμβάνοντας υπόψη τη χρονική διαφορά του τόπου μας από το Γκρίνουιτς. Επειδή παράλληλα λαμβάνει υπόψη και την αλλαγή της θερινής ώρας, οι εγγραφές που είχαν γίνει πριν στο αρχείο καταγραφής φαίνεται ότι πραγματοποιήθηκαν μία ώρα μετά. (Για παράδειγμα, αντί στις 5 μ.μ. που εμφανίζονταν, στις 6 μ.μ.) Στη στήλη Source (Προέλευση) αναφέρεται η εφαρμογή, η συσκευή ή η υπηρεσία με την οποία έχει σχέση το συμβάν (π.χ., W32Time, ccSetMgr, Service Control Manager κ.λπ.), ενώ στην Category (Κατηγορία) ο τύπος του συμβάντος (π.χ., log on/log off). Θα πρέπει όμως να επισημάνουμε ότι δεν ταξινομούνται όλες οι εγγραφές σε κάποια κατηγορία και γι' αυτό σε αρκετές εγγραφές στη στήλη της κατηγορίας αναφέρεται η λέξη None (Κομία). Στη στήλη Event (Συμβάν) αναφέρεται ο αριθμός που αντιστοιχεί στο είδος του συμβάντος. Να διευκρινίσουμε ότι κάθε συμβάν χαρακτηρίζεται από έναν ξεχωριστό αριθμό, ο οποίος σχετίζεται με μια περιγραφή κειμένου που παρουσιάζεται όταν ζητάμε αναλυτικές πληροφορίες για την εγγραφή. Στη στήλη User αναγράφεται ο λογαριασμός του χρήστη που έχει σχέση με το συμβάν που καταγράφηκε. Επειδή πολλές εγγραφές δεν

αφορούν σε κάποιον χρήστη αλλά προέρχονται από το λειτουργικό ή από ορισμένες ανεξάρτητες υπηρεσίες, αρκετές φορές στη στήλη User εμφανίζονται οι λέξεις SYSTEM ή N/A (Δ/Υ). Τέλος, στη στήλη Computer (Υπολογιστής) αναφέρεται το όνομα του υπολογιστή με τον οποίο σχετίζεται η καταγραφή.

**ΟΙ ΛΕΠΤΟΜΕΡΕΙΕΣ ΕΝΟΣ ΣΥΜΒΑΝΤΟΣ.** Αν θέλουμε να δούμε αναλυτικές πληροφορίες για την εγγραφή ενός συμβάντος, από το «δέντρο της κονσόλας» επιλέγουμε ένα αρχείο καταγραφής (Application, Security, System ή Εφαρμογή, Ασφάλεια, Σύστημα). Όπως είπαμε, στο δεξί τμήμα της κονσόλας θα εμφανιστούν οι καταγραφές του αρχείου, δηλαδή τα συμβάντα, με ορισμένες πληροφορίες για το είδος του καθενός (τύπος, χρόνος, πηγή, κατηγορία κ.λπ.). Για να δούμε τις λεπτομέρειες μιας εγγραφής θα πρέπει είτε να κάνουμε διπλό κλικ με το ποντίκι πάνω της είτε να την επιλέξουμε και να πατήσουμε Enter είτε να κάνουμε δεξί κλικ πάνω της και να διαλέξουμε «Properties» («Ιδιότητες»). Στο παράθυρο ιδιοτήτων που εμφανίζεται, στο πάνω τμήμα αναγράφονται οι πληροφορίες που φαίνονται και στο δεξί τμήμα της κονσόλας (τύπος, χρόνος, πηγή, κατηγορία κ.λπ.). Στο μεσαίο τμήμα του ίδιου παραθύρου αναφέρεται μια περιγραφή του συμβάντος. Στο τέλος της περιγραφής υπάρχει ένας δεσμός (παραπομπή), που, αν τον επιλέξουμε, το λειτουργικό μας πληροφορεί ότι θα στείλει τις πληροφορίες του συμβάντος στη Microsoft μέσω του Internet. Αν επιθυμούμε να μάθουμε περισσότερες λεπτομέρειες για το συμβάν, χρειάζεται να είμαστε συνδεδεμένοι στο Internet και να πατήσουμε το πλήκτρο «OK» («Ναι»). Με αυτό τον τρόπο θα εμφανιστεί το παράθυρο «Help and Support Center» («Κέντρο Βοήθειας και υποστήριξης») με περισσότερες πληροφορίες και προτάσεις για το τι μπορούμε να κάνουμε ώστε να αντιμετωπίσουμε το πρόβλημα. Στο κάτω τμήμα του παραθύρου παρουσιάζονται πληροφορίες σε δυοδική γλώσσα οι οποίες είναι χρήσιμες στους



Για να πληροφορηθούμε ποιοι χρήστες έχουν προσπαθήσει να δουν συγκεκριμένα αρχεία ή φακέλους του υπολογιστή μας, θα πρέπει πρώτα από την κονσόλα ρυθμίσεων ασφαλείας να ενεργοποιήσουμε τον έλεγχο πρόσβασης αντικειμένων (επιλογή «Audit object access» ή «Έλεγχος πρόσβασης αντικειμένων») της κατηγορίας. Κατόπιν θα πρέπει να καθορίσουμε ποιους φακέλους ή αρχεία θέλουμε να κατασκοπεύει ο υπολογιστής. Για το σκοπό αυτό μέσα από τον Windows Explorer (Εξερεύνηση των Windows) είναι απαραίτητο να εμφανίσουμε τις ιδιότητες των φακέλων ή των αρχείων και να μεταβούμε στην καρτέλα «Security» («Ασφάλεια»). Κατόπιν κάνουμε κλικ στο «Advanced» («Για προχωρημένους»), μεταφερόμαστε στην καρτέλα «Auditing» («Έλεγχος») και επιλέγουμε τους χρήστες και τις ενέργειες που θέλουμε να παρακολουθούμε.

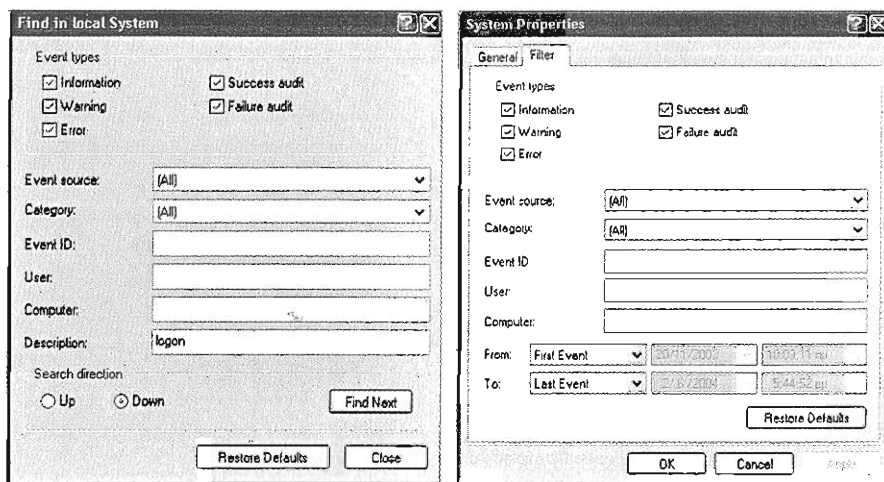
προγραμματιστές και στους τεχνικούς που γνωρίζουν περισσότερες λειτουργίες για το συγκεκριμένο συμβάν (π.χ., την εφαρμογή). Να διευκρινίσουμε όμως ότι δεν εμφανίζονται σε όλα τα συμβάντα πληροφορίες σε δυαδική γλώσσα και γι' αυτό σε ορισμένες εγγραφές το τελευταίο τμήμα του παραθύρου είναι ανενεργό.

Επίσης, στο πάνω τμήμα του παράθυρου ιδιοτήτων και δεξιά από τις πληροφορίες του συμβάντος υπάρχουν τρία εικονίδια με κατακόρυφη στοίχιση. Το πρώτο απεικονίζει ένα βέλος προς τα πάνω και μας μεταφέρει στην προηγούμενη καταγραφή, το δεύτερο απεικονίζει ένα βέλος προς τα κάτω και μας μεταφέρει στην επόμενη καταγραφή, ενώ το τρίτο είναι το γνωστό εικονίδιο αντιγραφής που συναντάμε στις γραμμές εργασίας αρκετών προγραμμάτων (συμβολίζει δύο σελίδες) το οποίο αντιγράφει στη μνήμη του υπολογιστή όλες τις πληροφορίες του παραθύρου. Εννοείται ότι με τη βοήθεια του πληκτρολογίου αντιγραφής μπορούμε να εισαγάγουμε τις λειτουργίες του συμβάντος σε οποιοδήποτε πρόγραμμα υποστηρίζει εισαγωγή κειμένου με τη διαδικασία της επικόλλησης (Paste).

**ΤΑΞΙΝΟΜΗΣΗ ΚΑΙ ΕΥΡΕΣΗ ΣΥΜΒΑΝΤΩΝ.** Επειδή οι καταγραφές στα αρχεία συμβάντων είναι πάρα πολλές, η κονσόλα προβολής συμβάντων διαθέτει διάφορες λειτουργίες για την ανεύρεση συγκεκριμένων εγγραφών. Κατ' αρχάς, στο δεξί τμήμα της, όπου εμφανίζεται η λίστα με τις εγγραφές των συμβάντων, έχουμε τη δυνατότητα να τα ταξινομήσουμε με βάση όχι την ημερομηνία αλλά κάποιο άλλο κριτήριο (π.χ., τον αριθμό του συμβάντος). Για το σκοπό αυτό αρκεί να κάνουμε κλικ πάνω στην επικεφαλίδα της στήλης με την οποία θέλουμε να γίνει η ταξινόμηση. Για να επαναφέρουμε την ταξινόμηση με βάση τη χρονική στιγμή του συμβάντος αρκεί να διαλέξουμε από το μενού «View» («Προβολή») την επιλογή «Newest First» («Πρώτα η νεότερη»). Επιπρόσθετα, έχουμε την ευχέρεια να βρούμε εγγραφές με βάση συγκεκριμένα κρι-

τήρια επιλέγοντας «View / Find...» («Προβολή / Εύρεση...»). Στην περιοχή «Event types» («Τύποι συμβάντων») καθορίζουμε τον τύπο του συμβάντος που μας ενδιαφέρει, ενώ στα πιο κάτω πεδία εισαγάγουμε τα υπόλοιπα κριτήρια που μας αφορούν. Να σημειώσουμε ότι με την επιλογή εύρεσης δεν τροποποιείται η λίστα με τις εγγραφές και για το λόγο αυτό δεν είναι πάντα ιδιαίτερα εύχρηστη.

**ΦΙΛΤΡΑΡΙΣΜΑ ΣΥΜΒΑΝΤΩΝ.** Για την καλύτερη διαχείριση των συμβάντων μπορούμε να δημιουργήσουμε διαφορετικές λίστες προβολής με βάση συγκεκριμένα κριτήρια. Με αυτό τον τρόπο, έχουμε τη δυνατότητα να μεταφερόμαστε εύκολα από την αφιπτράριστη λίστα σε οποιαδήποτε φιλτραρισμένη. Για να δημιουργήσουμε μέσα στην κονσόλα προβολής συμβάντων αντίγραφο ενός αρχείου καταγραφής, επιλέγουμε από το «δέντρο της κονσόλας» το αρχείο καταγραφής που μας ενδιαφέρει και στη συνέχεια από το μενού «Action» («Ενέργεια») διαλέγουμε «New Log View» («Προβολή νέου αρχείου καταγραφής»). Για να φιλτράρουμε τα συμβάντα του αντιγράφου του αρχείου, το επιλέγουμε και από το μενού «View» («Προβολή») διαλέγουμε «Filter...» («Φίλτρο...»). Εναλλακτικά, μπορούμε να κάνουμε δεξί κλικ πάνω στο αρχείο που μας ενδιαφέρει, να επιλέξουμε «Properties» («Ιδιότητες») και να μεταφερθούμε στην καρτέλα «Filter...» («Φίλτρο...»). Το παράθυρο που εμφανίζεται έχει αρκετές ομοιότητες με το παράθυρο εύρεσης, διότι και εδώ συναντάμε την περιοχή καθορισμού του τύπου του συμβάντος και πεδία εισαγωγής κριτηρίων. Συνήθως φιλτράρουμε τα συμβάντα για να παρουσιαστούν οι εγγραφές συγκεκριμένου τύπου (π.χ., τα σφάλματα ή τις προειδοποιήσεις). Για να εμφανίσουμε τα συμβάντα συγκεκριμένου τύπου, στο τμήμα «Event types» («Τύποι συμβάντων») του παραθύρου αφήνουμε τσεκαρισμένα μόνο τα κουτάκια που αντιστοιχούν στους τύπους των συμβάντων που μας αφορούν. Με αυτό τον τρόπο στο δεξί τμήμα της κονσόλας εμφανίζονται μόνο οι εγγραφές που πληρούν τα κριτήρια που θέσαμε.



Τα παράθυρα εύρεσης και φιλτραρίσματος των συμβάντων.

**ΔΟΥΛΕΥΟΝΤΑΣ ΜΕ ΤΑ ΑΡΧΕΙΑ ΚΑΤΑΓΡΑΦΗΣ.** Μολονότι κατά κανόνα δεν χρειάζεται να ασχοληθούμε με το μέγεθος των αρχείων καταγραφής, έχουμε τη δυνατότητα να καθορίσουμε τόσο το μέγεθός τους όσο και τον ελάχιστο χρόνο που θα διατηρούνται οι εγγραφές των συμβάντων. Το προκαθορισμένο μέγεθος των αρχείων είναι 512KB, ενώ η ελάχιστη διάρκεια διατήρησης των εγγραφών είναι επτά ημέρες. Αν θέλουμε να τροποποιήσουμε τα στοιχεία αυτά, θα πρέπει να επιλέξουμε το αρχείο καταγραφής που μας ενδιαφέρει και από το μενού «Action» («Ενέργεια») να διαλέξουμε «Properties» («Ιδιότητες»). Από το ίδιο παράθυρο έχουμε την ευχέρεια να αλλάξουμε και το όνομα με το οποίο εμφανίζεται το κάθε αρχείο καταγραφής στο «δέντρο της κονσόλας». Αυτό είναι αρκετά χρήσιμο κυρίως για τα αντίγραφα των αρχείων που περιέχουν φιλτραρισμένα τα δεδομένα. Για να αποθηκεύσουμε ένα αρχείο καταγραφής το επιλέγουμε και κατόπιν από το μενού «Action» («Ενέργεια») διαλέγουμε «Save Log File As...» («Αποθήκευση του αρχείου καταγραφής ως...»). Να σημειώσουμε ότι η αποθήκευση μπορεί να γίνει είτε σε αρχείο τύπου .evt είτε σε αρχεία κειμένου τύπου .txt ή .csv. Αν αποθηκεύσουμε το αρχείο καταγραφής ως .evt, μπορούμε να το ανοίξουμε από την κονσόλα προβολής συμβάντων επιλέγοντας «Action / Open Log File...» («Ενέργεια / Άνοιγμα αρχείου καταγραφής...») και καθορίζοντας τον τύπο του αρχείου καταγραφής από το πεδίο «Log Type» («Τύπος αρχείου καταγραφής»). Τέλος, να επισημάνουμε ότι, αν θέλουμε να αποθηκεύσουμε μόνο τα αποτελέσματα ενός φιλτραρισμένου αρχείου, τότε από το μενού «Action» («Ενέργεια») θα πρέπει να επιλέξουμε «Export List...» («Εξαγωγή λίστας...»).

**ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΦΑΚΕΛΩΝ.** Όπως αναφέραμε, με τη βοήθεια της κονσόλας προβολής συμβάντων μπορούμε να πληροφορηθούμε ποιοι χρήστες είχαν πρόσβαση σε συγκεκριμένους φακέλους και αρχεία του υπολογιστή μας. Για το σκοπό αυτό όμως θα πρέπει πρώτα να ενεργοποιήσουμε την πολιτική ελέγχου παρακολούθησης αρχείων και φακέλων και κατόπιν να καθορίσουμε ποιοι φάκελοι ή αρχεία επιθυμούμε να

παρακολουθούνται από το λειτουργικό σύστημα. Μοναδική προϋπόθεση είναι ο δίσκος στον οποίο είναι αποθηκευμένα τα δεδομένα μας να βρίσκεται στο σύστημα NTFS. Ας δούμε όμως τα βήματα πιο αναλυτικά.

Ενεργοποίηση πολιτικής ελέγχου φακέλων. Από το παράθυρο εκτέλεσης εντολών («Start / Run...» ή «Εναρξη / Εκτέλεση...») πληκτρολογούμε την εντολή «secpol.msc» και πατάμε «OK» ώστε να εμφανιστεί η κονσόλα ρυθμίσεων ασφαλείας του τοπικού υπολογιστή. Κατόπιν, από το «δέντρο της κονσόλας» μεταβαίνουμε στην κατηγορία «Local Policies / Audit Policy» («Τοπικές πολιτικές / Πολιτική ελέγχου») και από το δεξί τμήμα της κάνουμε διπλό κλικ πά-

νω στην επιλογή «Audit object access» («Έλεγχος πρόσβασης αντικειμένων»). Από το παράθυρο που εμφανίζεται ενεργοποιούμε τις επιλογές «Success» («Επιτυχία») και «Failure» («Αποτυχία»), αν θέλουμε να καταγράφονται αντίστοιχα τόσο η επιτυχής όσο και η ανεπιτυχής πρόσβαση των χρηστών στους φακέλους και στα αρχεία μας.

Καθορισμός των προς παρακολουθήση φακέλων. Από τον Windows Explorer (Εξερεύνηση των Windows) ή το παράθυρο «My Computer» («Ο Υπολογιστής μου») κάνουμε δεξί κλικ στο φάκελο ή το αρχείο που θέλουμε να ξέρουμε αν θα το προσπελάσουν άλλοι χρήστες και επιλέγουμε «Properties» («Ιδιότητες»). Στη συνέχεια, μεταφερόμαστε στην καρτέλα «Security» («Ασφάλεια»). Αν αυτή δεν εμφανίζεται στο παράθυρο ιδιοτήτων του φακέλου ή των αρχείων, θα χρειαστεί να ανοίξουμε τον Windows Explorer (Εξερεύνηση των Windows) και από το μενού «Tools» («Εργαλεία») να επιλέξουμε «Folder Options...» («Επιλογές φακέλων...»). Στη συνέχεια, θα πρέπει να μεταβούμε στην καρτέλα «View» («Προβολή») και από το τμήμα «Advanced settings:» («Ρυθμίσεις για προχωρημένους:») να απενεργοποιήσουμε την επιλογή «Use simple file sharing (Recommended)» («Χρήση απλής κοινής χρήσης αρχείων [Συνιστάται]»). Η συγκεκριμένη επιλογή είναι τελευταία στη λίστα στην αγγλική έκδοση των Windows XP και προτελευταία στην ελληνική έκδοση. Από την καρτέλα ασφαλείας πατάμε το κουμπί «Advanced» («Για προχωρημένους») και μεταφερόμαστε στην καρτέλα «Auditing» («Έλεγχος»). Μετά, επιλέγουμε τους χρήστες ή τις ομάδες χρηστών για τις οποίες θέλουμε να καταγράφεται η πρόσβαση. Για το σκοπό αυτό κάνουμε κλικ στα πλήκτρα «Add... / Advanced... / Find Now...» («Προσθήκη... / Για προχωρημένους / Εύρεση τώρα»). Να σημειώσουμε ότι για να επιλέξουμε όλους τους χρήστες διαλέγουμε από τη λίστα την ομάδα χρηστών «Everyone». Αφού επιλέξουμε τους χρήστες εμφανίζεται η καρτέλα «Auditing Entry» («Καταχώριση δικαιώματος»), στην οποία καθορίζουμε με ακρίβεια ποιες ενέργειες των χρηστών επιθυμούμε να καταγράφονται. Ως ενέργεια θεωρείται η ανάγνωση ή η αποθήκευση ενός αρχείου, η εμφάνιση των

περιεχομένων ενός φακέλου, η μετακίνηση σε υποφάκελο, το σβήσιμο αρχείων ή φακέλων κ.λπ. Το σύστημα μπορεί να καταγράψει και τις επιτυχημένες και τις αποτυχημένες προσπάθειες προσπέλασης. Ας υποθέσουμε, για παράδειγμα, ότι έχουμε μοιράσει ένα φάκελο σε συγκεκριμένους μόνο χρήστες και έχουμε επιλέξει να καταγράφονται και οι επιτυχημένες και οι αποτυχημένες προσπάθειες πρόσβασης του φακέλου από όλους τους χρήστες. Ταυτόχρονα, κατά τον καθορισμό της πολιτικής ελέγχου έχουμε δηλώσει ότι θέλουμε να καταγράφονται και οι επιτυχημένες και οι αποτυχημένες προσπάθειες αντικειμένων. Όσοι χρήστες έχουν δικαιώματα πρόσβασης στο φάκελο κάθε φορά που θα μπαίνουν σε αυτόν, θα δημιουργείται στο αρχείο καταγραφής ασφαλείας μία εγγραφή επιτυχημένης πρόσβασης με τύπο «Success Audit» («Επιτυχημένος έλεγχος»). Στους χρήστες χωρίς δικαιώματα πρόσβασης, κάθε φορά που θα προσπαθούν να δουν τα περιεχόμενα του φακέλου θα τους απαγορεύεται η πρόσβαση και ταυτόχρονα θα δημιουργείται στο αρχείο καταγραφής ασφαλείας μία εγγραφή αποτυχίας πρόσβασης με τύπο «Failure Audit» («Αποτυχημένος έλεγχος»). Επομένως, για τις ενέργειες που θέλουμε να δημιουργούνται εγγραφές στο αρχείο καταγραφής τσεκάρουμε τα αντίστοιχα κουτάκια «Successful» («Αποδοχή») ή «Failed» («Άρνηση») για την επιτυχημένη ή αποτυχημένη προσπάθεια πρόσβασης των χρηστών.

Να επισημάνουμε ότι επειδή για κάθε διαφορετική ενέργεια δημιουργείται διαφορετική καταγραφή, καλό θα είναι να μην

επιλέγουμε την παρακολούθηση πολλών ενεργειών. Τις περισσότερες φορές άλλωστε μας αρκεί να παρακολουθούμε την αποδοχή ή την άρνηση ανάγνωσης και τροποποίησης των δεδομένων μας και ενδεχομένως τη δημιουργία ή τη διαγραφή φακέλων και αρχείων. Να διευκρινίσουμε επίσης ότι καλό θα είναι να μην παρακολουθούμε φακέλους στους οποίους έχει συχνή πρόσβαση το λειτουργικό σύστημα ή εμείς (π.χ., το φάκελο των Windows), διότι με αυτόν τον τρόπο δημιουργούμε πολλές εγγραφές και καθυστερούμε το σύστημα. Η παρακολούθηση άλλωστε πρέπει να γίνεται μόνο όπου είναι απαραίτητο. Αν επιθυμούμε, μπορούμε να παρακολουθούμε μόνο συγκεκριμένα αρχεία και όχι και τους φακέλους που τα περιέχουν.

Τέλος, για να πάρουμε την αναφορά από τον κατάσκοπο του λειτουργικού για το ποιος χρησιμοποίησε τα αρχεία μας, δεν έχουμε παρά να δούμε τις εγγραφές του αρχείου ασφαλείας από την κονσόλα προβολής συμβάντων. Οι εγγραφές που έχουν σχέση με την πρόσβαση αρχείων και φακέλων αναφέρουν ως κατηγορία την ένδειξη «Object Access» («Επιτυχημένος έλεγχος»). Αν κάνουμε διπλό κλικ πάνω σε αυτές, θα μάθουμε περισσότερες λεπτομέρειες για το είδος της καταγραφής, αν δηλαδή αφορά στην πρόσβαση στο φάκελο παρακολούθησης, στο άνοιγμα ή στην τροποποίηση ενός αρχείου κ.λπ. Να επισημάνουμε όμως ότι για κάθε ενέργεια που πραγματοποιήσει ο χρήστης θα υπάρχει ξεχωριστή εγγραφή.

# Δικλίδες ασφαλείας

Τα προγράμματα πλοήγησης στο Internet προσφέρουν αρκετές ρυθμίσεις ασφαλείας που μπορούν να εξασφαλίσουν έως ένα βαθμό τις δικτυακές μας περιηγήσεις. Η ύπαρξη προγραμμάτων AntiVirus και AntiSpyware είναι η δεύτερη γραμμή άμυνας.

**Ο** ή τα καλά και τα κακά του μεγαλύτερου δικτύου του κόσμου (Internet) περνούν μέσα από κάποιο πρόγραμμα πλοήγησης στο Internet. Ιαί, σκούληκια και διάφορες άλλες κακόβουλες εφαρμογές εκμεταλλεύονται, μεταξύ άλλων, διάφορες αδυναμίες των συγκεκριμένων προγραμμάτων για να διαδοθούν ή να κάνουν ζημιά στον υπολογιστή μας.

Ο Internet Explorer της Microsoft έχει πολλή άκρη κατηγορηθεί για τις δεκάδες αδυναμίες/προβλήματα ασφαλείας, τα οποία αφήνουν ανοιχτές κερκόπορτες στον υπολογιστή για πάσης φύσεως επιθέσεις.

Τα βασικά μέτρα άμυνας που έχει στη διάθεσή του ο χρήστης είναι δύο: οι τακτικές εγκαταστάσεις των κρίσιμων ενημερώσεων από το Windows Update του λειτουργικού συστήματος, η εγκατάσταση στον υπολογιστή μας προγραμμάτων AntiVirus και AntiSpyware αλλά και η ενεργοποίηση του firewall των Windows XP. Πληροφορίες για όλα αυτά τα θέματα, καθώς και δοκιμαστικές εκδόσεις αρκετών εφαρμογών ασφαλείας θα βρείτε στο τεύχος 191 του RAM (Μάιος 2005).

Επιπρόσθετα, τα ίδια τα προγράμματα πλοήγησης προσφέρουν κάποια μέτρα για την ασφάλεια των δικτυακών μας περιηγήσεων.

Ειδικά ο Internet Explorer έχει το πιο περίπλοκο –και θεωρητικά το καλύτερο– σύστημα ασφαλείας σε σύγκριση με τους Firefox και Opera, προσφέροντας πολλές ρυθμίσεις και

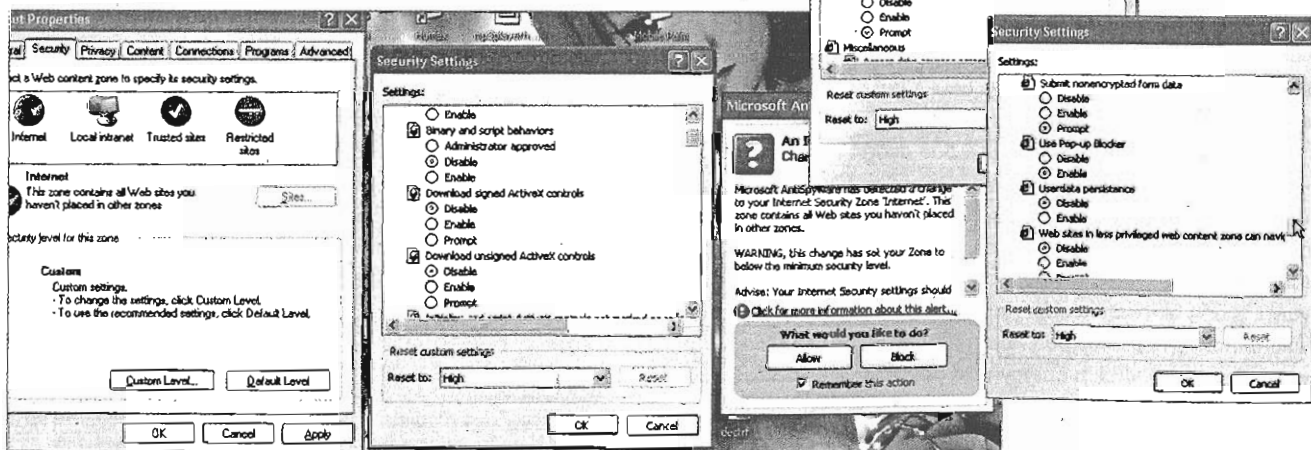
επιλογές στο χρήστη. Παράλληλα βέβαια αυξάνεται και η δυσκολία παραμετροποίησής του από τους πιο άπειρους χρήστες.

Παρακάτω θα παρουσιάσουμε τις βασικές ρυθμίσεις ασφαλείας και των τριών δημοφιλών προγραμμάτων πλοήγησης στο Internet, δίνοντας μεγαλύτερη έμφαση σε αυτές του IE.

**ΠΟΛΛΑΠΛΑ ΕΠΙΠΕΔΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ IE 6 SP2.** Ο Internet Explorer (IE) έχει φτάσει στην έκδοση 6, με τη Microsoft να ετοιμάζει κυρωτάως την έκδοση 7. Πρόκειται για το πρότυπο που χρησιμοποιείται σήμερα για την πρόσβαση στο Internet, αφού μέχρι πρότινος πολλοί δικτυακοί τόποι τον απαιτούσαν για να εμφανίσουν σωστά το περιεχόμενό τους, ενώ κατέχει και μεγάλο μερίδιο «αγοράς» όντας ενσωματωμένος στα Windows XP. Προσφέρει τις πιο ολοκληρωμένες ρυθμίσεις ασφαλείας, αλλά από την άλλη παρουσιάζει και αρκετές αδυναμίες που τις εκμεταλλεύονται οι διάφοροι κακόβουλοι τύποι για να μας εκνευρίζουν και να κάνουν τη ζωή μας πιο δύσκολη.

Η αξιόθελος πτέρνα του IE δεν είναι άλλη από τα ActiveX Controls. Πρόκειται για μικρά προγράμματα που μπορεί να εκτελέσει ο IE, προσφέροντάς μας διάφορες χρήσιμες λειτουργίες. Μέσω των ActiveX, για παράδειγμα, μπορούμε να ανοίξουμε ένα κείμενο Word μέσα από τον IE ή να εκτελέ-

Ο Internet Explorer προσφέρει πληθώρα ρυθμίσεων ασφαλείας, δικαιολογημένα θα λέγαμε, αφού έχει τις περισσότερες αδυναμίες. Η καρδιά του συστήματος ασφαλείας είναι οι τέσσερις ζώνες πρόσβασης, οι οποίες προσφέρουν αυστηρά ή πιο ελαστικά μέτρα εναντίον διαφόρων απειλών.





## Βασικές προϋποθέσεις ασφάλειας

σουμε έναν έλεγχο on-line για ιούς και δεκάδες άλλες εφαρμογές. Δυστυχώς όμως, εφόσον τα ActiveX εκτελούνται τοπικά στον υπολογιστή μας, αυτό σημαίνει ότι μπορούν να κάνουν και αρκετά περισσότερα πράγματα, όπως, για παράδειγμα, να αποτελέσουν κερκόπορτα για δούρειους ίππους και ιούς.

Γι' αυτόν το λόγο πολλοί είναι εκείνοι που προτείνουν την απενεργοποίησή τους. Εμείς αφήνουμε τη συγκεκριμένη επιλογή σε εσάς. «Παίξτε» με τις ρυθμίσεις που θα σας παρουσιάσουμε και αποφασίστε κατά πόσο η αυστηρότητα στην εφαρμογή τους, επηρεάζει τους δικτυακούς τόπους που συνήθιζετε να επισκέπτεστε.

Πρόσβαση στις ρυθμίσεις [Internet Options] του Internet Explorer μπορείτε να έχετε είτε από το μενού Εργαλεία [Tools] του προγράμματος είτε από τον Πίνακα Ελέγχου [Control Panel] είτε από το Κέντρο Ασφάλειας [Security Center], εφόσον έχει εγκατασταθεί στον υπολογιστή το Service Pack 2 των Windows XP, το οποίο επίσης θα βρείτε στον Πίνακα Ελέγχου. Σε αυτό το σημείο θα πρέπει να αναφέρουμε ότι οι παρακάτω ρυθμίσεις του IE ακολουθούν τις προδιαγραφές του Service Pack 2 των Windows XP.

### Καρτέλα Γενικά [General]

Από εδώ μπορείτε χειροκίνητα να σβήσετε τα προσωρινά αρχεία του IE και τα cookies. Έχετε υπόψη σας ότι σβήνοντας τα cookies θα χάσετε την αυτοματοποιημένη είσοδο σε κάποιους δικτυακούς τόπους (περισσότερα για το θέμα παρακάτω).

### Καρτέλα Ασφάλεια [Security]

Ο IE προσφέρει τέσσερα επίπεδα ασφάλειας αναφορικά με την πρόσβαση στο Internet:

Internet, το οποίο αφορά στη γενική πρόσβαση στο Διαδίκτυο και προσφέρει μια ισορροπημένη σχέση μεταξύ ασφάλειας και λειτουργικότητας δικτυακών τόπων.

Τοπικό Intranet για πρόσβαση σε τοπικό δίκτυο, με πιο χαλαρές ρυθμίσεις, αφού θεωρητικά πρόκειται για σφαλώς πιο ασφαλές περιβάλλον από το Internet.

Αξιόπιστες και Ελεγχόμενες τοποθεσίες με ελάχιστες ή μέγιστες ρυθμίσεις ασφάλειας.

Στη ζώνη Internet η αρχική ρύθμιση είναι «Μεσαίο». Σε αυτό το επίπεδο επιτρέπεται η εκτέλεση ActiveX Controls, τουλάχιστον όσων έχουν κάποια πιστοποίηση. Βέβαια, η ύπαρξη πιστοποίησης στα ActiveX αλλά και στις εφαρμογές που κατεβάζουμε από διάφορους δικτυακούς τόπους δεν σημαίνει ότι κατ' ανάγκη είναι και ασφαλή. Παράλληλα, αρχεία που δεν έχουν κάποια πιστοποίηση σπάνια θα δημιουργήσουν πρόβλημα.

Εάν επιλέξετε «Προσαρμοσμένο επίπεδο» στην ίδια καρτέλα, μπορείτε να επέμβετε σε δεκάδες επιλογές. Από εκεί έχετε τη δυνατότητα να απενεργοποιήσετε τα ActiveX.

Οι ρυθμίσεις της επιλογής «Υψηλό επίπεδο» καταργούν πολλές από τις δυνατότητες του Internet Explorer, συμπεριλαμβανομένων των ActiveX, της εκτέλεσης εφαρμογών Java, Javascript αλλά και του κατεβάσματος αρχείων. Μια καλή λύση είναι να ορίσετε το επίπεδο ασφάλειας ως «Υψηλό» και ακολουθώντας να επιλέξετε «Προσαρμοσμένο επίπεδο» και να

1. Να ενημερώνετε συχνά τα Windows με τις τελευταίες κρίσιμες ενημερώσεις από το Windows update ([windowsupdate.microsoft.com](http://windowsupdate.microsoft.com)).

2. Να έχετε εγκαταστήσει το Service Pack 2 των Windows XP.

3. Να υπάρχουν εγκατεστημένα, πάση θυσία, στον υπολογιστή σας ένα αντι-ιικό και ένα πρόγραμμα AntiSpyware.

4. Να έχετε ενεργοποιήσει το Windows Firewall (δείτε ιδιότητες παραθύρου σύνδεσης → ρυθμίσεις για προχωρημένους) ή να εγκαταστήσετε κάποιο άλλο με περισσότερες δυνατότητες

επιτρέψετε, για παράδειγμα, το κατέβασμα αρχείων και την εκτέλεση εφαρμογών Java.

Εάν δείτε ότι παρουσιάζονται προβλήματα με δικτυακούς τόπους που επισκέπτεστε με την επιλογή «Υψηλό επίπεδο», μπορείτε να επιτρέψετε την εκτέλεση πιστοποιημένων ActiveX Control, πάλι μέσω της επιλογής «Προσαρμοσμένο επίπεδο».

Στο Τοπικό Intranet η αρχική ρύθμιση είναι «Μεσαίο-χαμηλό», ενώ έχετε τη δυνατότητα να επιλέξετε συγκεκριμένους δικτυακούς τόπους που εμπιστεύεστε και να τους τοποθετήσετε στη ζώνη «Αξιόπιστες τοποθεσίες» με χαλαρά μέτρα ασφαλείας. Για παράδειγμα, δεν θα μπορούσατε να έχετε πρόσβαση στο [windowsupdate.microsoft.com](http://windowsupdate.microsoft.com) χωρίς ActiveX Controls. Μια λύση είναι να εισαγάγετε στις «Αξιόπιστες τοποθεσίες» τη διεύθυνση με την ακόλουθη μορφή:

«\*.windowsupdate.microsoft.com». Με αυτό τον τρόπο θα επιτρέψετε την πρόσβαση του υπολογιστή σας σε διάφορους διακομιστές του Windows Update με τις πιο χαλαρές ρυθμίσεις ασφάλειας. Έτσι, εισάγετε τις ακριβείς διευθύνσεις που εμπιστεύεστε ή διάφορες διευθύνσεις κάτω από ένα domain, για παράδειγμα, \*.dolnet.gr.

Στις Ελεγχόμενες τοποθεσίες ισχύει φυσικά η ρύθμιση «Υψηλό». Αυτές προσφέρουν το ανώτερο επίπεδο ασφάλειας αλλά χαμηλή λειτουργικότητα. Σε αυτή την κατηγορία ανήκουν ύποπτοι δικτυακοί τόποι, όπως, για παράδειγμα, με σπαρμένους κωδικούς για εφαρμογές, roz περιεχόμενο κ.ο.κ. Βέβαια, υπάρχει η περίπτωση να υπάρξει πρόβλημα κατά την είσοδό σας στους συγκεκριμένους δικτυακούς τόπους με τις αυστηρές ρυθμίσεις, αλλά από την άλλη υπάρχει κάποιος βαθμός προστασίας. Και φυσικά, εφόσον επισκέπτεστε συχνά τέτοιους τόπους, θα πρέπει πάση θυσία να υπάρχουν εγκατεστημένες στον υπολογιστή σας εφαρμογές AntiVirus και AntiSpyware.

### Καρτέλα Εμπιστευτικότητα [Privacy]

Από εδώ ορίζονται οι βασικές επιλογές για τη λειτουργία των cookies. Αυτά τοποθετούνται από κάποιο δικτυακό τόπο σε ένα συγκεκριμένο σημείο στο σκληρό μας δίσκο και χρησιμοποιούνται από το εκδότο πρόγραμμα πλοήγησης για να προσφέρουν αυτόματα είσοδο σε διάφορες υπηρεσίες, να

## Mozilla Firefox - Opera

Ο αυξανόμενος αριθμός χρηστών που προτιμούν διαφορετικά από τον Explorer προγράμματα περιήγησης στο Internet, όπως, για παράδειγμα, ο Mozilla Firefox και ο Opera, αιτιολογείται εν μέρει από το γεγονός ότι τα προγράμματα αυτά δεν έχουν πολλές από τις αδυναμίες του Internet Explorer, ενώ διατηρούν αρκετά από τα χαρακτηριστικά του.

Επίσης, αρκετοί δικτυακοί τόποι είναι δυνατόν να μην εμφανίζονται σωστά ή και καθόλου με αυτά τα προγράμματα, με αιτίες είτε τη μη υλοποίηση των κλειστών επεκτάσεων της γλώσσας HTML του IE, την απουσία ActiveX αλλά και με άλλες εγγενείς αδυναμίες, όπως, για παράδειγμα, η μη ομαλή διαχείριση των μη λατινικών γραμματοσειρών.

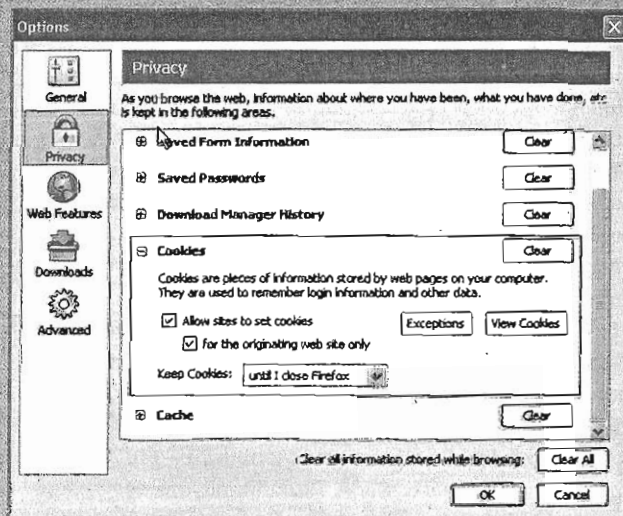
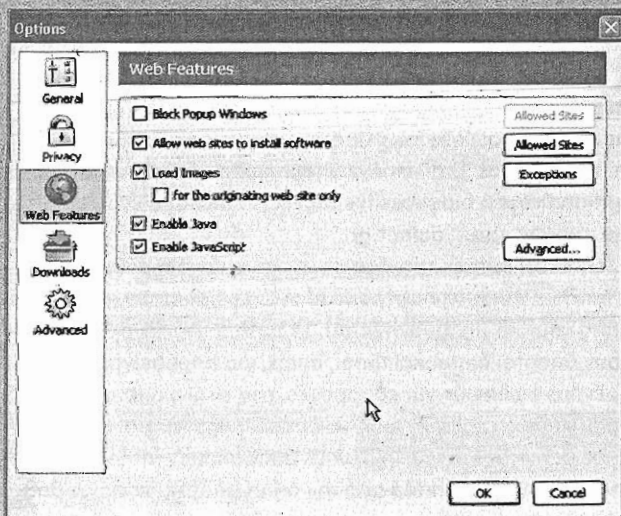
Βέβαια, για κανένα λόγο αυτό δεν σημαίνει ότι τα συγκεκριμένα προγράμματα δεν κάνουν καλά τη δουλειά τους. Ο Firefox, π.χ., προσφέρει ένα εύχρηστο και απλό περιβάλλον εργασίας με πολλαπλές καρτέλες (tab) δικτυακών τόπων στο ίδιο παράθυρο και ένα πανίσχυρο εργαλείο ανασήθησης δεδομένων σε μια ιστοσελίδα, ενώ με τις εκατοντάδες επεκτάσεις (Extensions) μπορεί να μεταμορφωθεί σε πανίσχυρο εργαλείο πρόσβασης σε πάσης φύσεως περιεχόμενο του Internet. Από την άλλη πλευρά, ο Opera διακρίνεται, μεταξύ άλλων, για τη μεγάλη ταχύτητα εμφάνισης των σελίδων. Επίσης, προσφέρει πολλαπλές καρτέλες στο ίδιο παράθυρο εργασίας, ενώ ενσωματώνει και εφαρμογή αποστολής και λήψης e-mail.

Το γεγονός ότι τόσο ο Firefox όσο και ο Opera δεν υποστηρί-

ζουν ActiveX εγγενώς δεν σημαίνει ότι δεν παρουσιάζουν κάποιες αδυναμίες. Για παράδειγμα, η τελευταία έκδοση 1.03 του Firefox διορθώνει αρκετά προβλήματα ασφάλειας. Ίσως το γεγονός ότι κατέχουν μικρά μερίδια μεταξύ των προγραμμάτων περιήγησης στο Internet αποθαρρύνουν τους διάφορους κακόβουλους από το να ασχοληθούν μαζί τους. Μερικοί μάλιστα κατακρίνουν την πολιτική της ομάδας ανάπτυξης του προγράμματος, η οποία διανέμει τον Firefox μέσω ενός κατακερματισμένου δικτύου διακομιστών, με συνέπεια να εγείρεται θέμα πιστοποίησης των αρχείων που διατίθενται προς κατέβασμα. Επίσης, τα Extension του Firefox διατηρούν κάποια χαρακτηριστικά του συστήματος ActiveX, με αποτέλεσμα να κρύβουν και αυτά κάποιους κινδύνους, αν και μέχρι στιγμής δεν έχει παρουσιαστεί κάποιο ύποπτο κρούσμα.

**ΠΥΘΜΙΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ MOZILLA FIREFOX 1.03.** Όπως προαναφέραμε, ο Firefox γενικά φημίζεται για την απλότητά του, κάτι που ισχύει και για τις ρυθμίσεις του. Από το μενού Tools → Options εισερχόμαστε στις ρυθμίσεις του πλοηγού. Στην επιλογή Privacy επιλέγουμε το σταυρά δίπλα από τα Cookies και αποφασίζουμε εάν θα τα χρησιμοποιήσουμε. Η καλύτερη επιλογή θα ήταν να μην το κάνουμε και στη συνέχεια να επιλέξουμε στα «Exceptions» τους δικτυακούς τόπους που επιτρέπουμε (Allow) να τοποθετούν cookies στον υπολογιστή μας. Εάν αυτό σας φαίνεται πολύπλοκο, επιλέξτε «Allow sites to

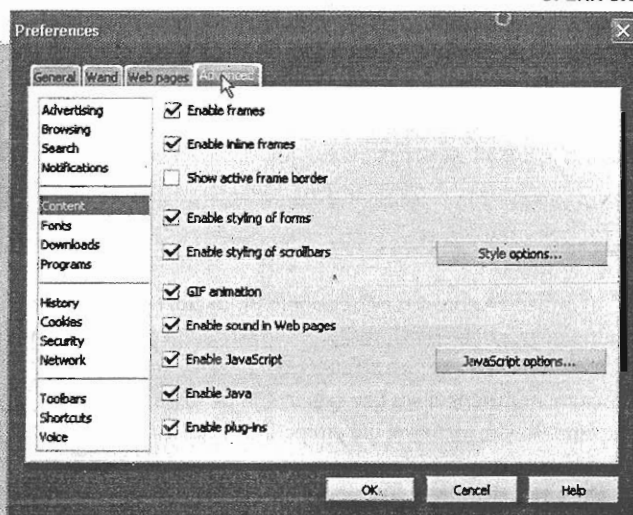
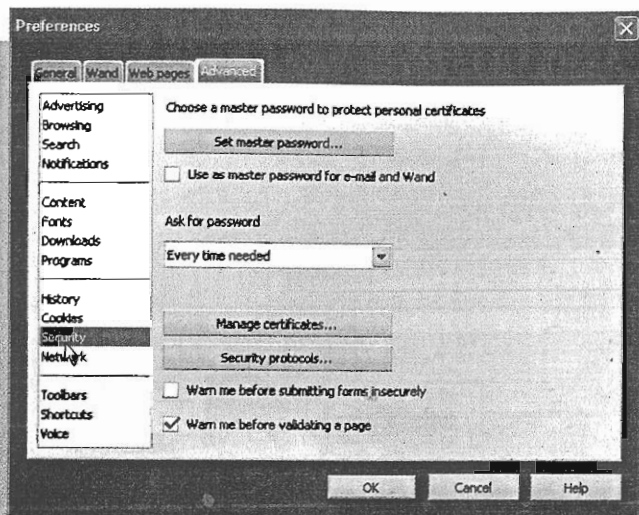
### FIREFOX 1.03



συμπληρώνουν αυτόματα φόρμες, να εμφανίζουν στοιχεία που έχετε ήδη αναζητήσει σε κάποια μηχανή, το καλδί αγορών σας κ.ά. Δυστυχώς τα cookies, μεταξύ άλλων, μπορούν να καταγράφουν τις δικτυακές κινήσεις μας και να στέλνουν το στοιχείο αυτά στους διαχειριστές δικτυακών τόπων χωρίς την άδειά μας. Η αρχική επιλογή εδώ είναι «Μεσαίο». Θα σας συστήναμε να το ορίσετε τουλάχιστον σε «Μέτριο-υψηλό» ή «Υψηλό».

Εάν επιθυμείτε να επέμβετε χειροκίνητα, επιλέξτε «Για προχωρημένους», «Παράκαμψη αυτόματου χειρισμού cookies» και εν συνεχεία την επιλογή «Επιτρέψτε τα cookies αρχικού κατασκευαστή», ενώ αποκλείστε αυτά από τρίτους.

Από τις εκάστοτε ρυθμίσεις μπορείτε να εξαιρέσετε συγκεκριμένους δικτυακούς τόπους, επιλέγοντας «Τοποθεσίες» πάντα στην καρτέλα «Εμπιστευτικότητα».



set cookies» και «For the originating web site only», «Until I Close Firefox». Βέβαια, με αυτό τον τρόπο θα χάνονται και οι κωδικοί εισόδου, για παράδειγμα, σε διάφορα fora συζητήσεων που επισκέπτεστε καθημερινά, κάθε φορά που κλείνετε τον Firefox. Οπότε σε αυτή την περίπτωση καλό θα ήταν να τοποθετήσετε στα «Exceptions» το δικτυακό τόπο που επιθυμείτε να διατηρεί τα cookies ακόμη και μετά το κλείσιμο του πλοηγού.

Πάντα στις επιλογές του Firefox, και συγκεκριμένα στα Web Features, μπορούμε να ορίσουμε εάν ο πλοηγός δεν θα επιτρέπει την αυτόματη εμφάνιση διαφημιστικών παραθύρων (pop-up) γενικά ή μόνο αυτών που προέρχονται από συγκεκριμένους τόπους, εάν θα επιτρέπει την αυτόματη εγκατάσταση λογισμικού (θα προτείνουμε εκεί να είναι τοποθετημένος ο επίσημος τόπος ενημέρωσης [update.mozilla.org](http://update.mozilla.org)). Τέλος, στις ίδιες επιλογές μπορείτε να επιτρέψετε ή όχι την εκτέλεση εφαρμογών Java και Javascript. Η πιο ασφαλής επιλογή είναι φυσικά η απενεργοποίησή τους, αλλά έτσι θα χάσετε κάποιο βαθμό λειτουργικότητας και ευχρηστίας σε δικτυακούς τόπους που χρησιμοποιούν αυτές τις τεχνολογίες.

Στην επιλογή «Advanced», και συγκεκριμένα στο «Security», θα πρέπει να είναι επιλεγμένα τα SSL 2.0, SSL 3.0, TLS 1.0.

**ΡΥΘΜΙΣΕΙΣ ΑΣΦΑΛΕΙΑΣ OPERA 8.0.** Από το μενού Tools→Delete Private Data→Advanced μπορείτε να σβήσετε άμεσα διάφορες πληροφορίες και στοιχεία σχετικά με την πρόσβασή σας σε

δικτυακούς τόπους, όπως, για παράδειγμα, cookies, ιστορικά διευθύνσεων που εισαγάγατε κ.ά.

Από το μενού Tools→Quick Preferences έχετε τη δυνατότητα άμεσα και εύκολα να απενεργοποιήσετε τα cookies, Java και Javascripts.

Οι καθαυτές ρυθμίσεις του Opera υπάρχουν στο μενού Tools→Preferences→Advanced.

**Επιλογή Advertising.** Ο Opera διατίθεται σε δύο εκδόσεις: τη δωρεάν και την επί πληρωμή. Η πρώτη διαθέτει ένα σύστημα διαφημίσεων το οποίο παρακολουθεί τους δικτυακούς τόπους που επισκέπτεστε και εμφανίζει σχετικές διαφημίσεις στο πάνω μέρος του προγράμματος.

**Επιλογή Content.** Από εδώ μπορείτε να απενεργοποιήσετε σε μόνιμη βάση τη Java και Javascript.

**Επιλογή Cookies.** Εάν δεν εμπιστεύεστε τα cookies, έχετε τη δυνατότητα να απενεργοποιήσετε τόσο τα κανονικά όσο και αυτά τρίτων. Θα προτείνουμε να επιτρέψετε τα κανονικά και να αποτρέψετε τα cookies τρίτων να εγκατασταθούν στον υπολογιστή σας.

Στην ίδια κατηγορία μπορείτε να επιλέξετε να σβήνονται τα νέα cookies κάθε φορά που βγαίνετε από τον Opera, ενώ καλό θα είναι να μην είναι επιλεγμένο το «Accept cookies with incorrect paths».

**Επιλογή Security.** Επιλέγετε «Security Protocols». Θα πρέπει να είναι τσεκαρισμένα τουλάχιστον τα τρία πρώτα πρωτόκολλα [SSL2, SSL3, TLS 1.0].

### Καρτέλα Για προχωρημένους (Advanced)

Αρχικά είναι απαραίτητο να επιλέξετε «Εναλλακτική προεπιλογή» και ακολούθως από τη σχετικά μεγάλη λίστα ρυθμίσεων δεν θα πρέπει να είναι επιλεγμένα τα «Ενεργοποίηση της εγκατάστασης κατ' απαίτηση (Internet Explorer)» (Enable Install On Demand [Internet Explorer]) και «Ενεργοποίηση της εγκατάστασης κατ' απαίτηση (άλλων)» (Enable Install On Demand [Other]) στην

κατηγορία Περιήγηση. Επίσης, θα πρέπει να είναι επιλεγμένα τα: «Άδεια του φακέλου Temporary Internet Files κατά το κλείσιμο» (Empty Temporary Internet Files when browser is closed) και «Να μην αποθηκεύονται οι κρυπτογραφημένες σελίδες στο δίσκο» (Do not encrypted pages on disk) στην κατηγορία Ασφάλεια.