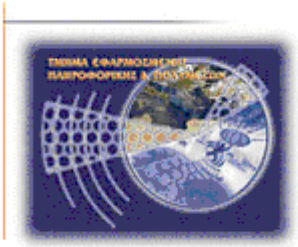
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Ασφαλής διαχείριση Microsoft Windows XP Professional σύμφωνα με την μεθοδολογία NIST SP 800-68 (Μέρος 1ο)

Παύλος Καραγιαννάκης(ΑΜ: 1898)
E-mail: epp1898@epp.teiher.gr

Ηράκλειο – 14/12/2009

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

Ασφαλής διαχείριση Microsoft Windows XP Professional σύμφωνα με την μεθοδολογία NIST SP 800-68 (Μέρος 1ο)

Υπεύθυνη Δήλωση*: Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι. Κρήτης.*

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της πτυχιακής εργασίας μου, Δρ. Μανιφάβα Χαράλαμπο. Οι οδηγίες του, οι υποδείξεις του και η κατανόηση που έδειξε κατά τη συγγραφή της εργασίας αποτέλεσαν καθοριστικά στοιχεία για την εκπόνησή της. Ήταν μεγάλη τιμή για εμένα να συνεργαστώ μαζί του.

Θα ήθελα επίσης να εκφράσω την ευγνωμοσύνη μου στην οικογένεια μου και στους ανθρώπους που είχα δίπλα μου όλη αυτήν την περίοδο.

Περίληψη

Χρησιμοποιώντας συγκεκριμένες ρυθμίσεις σύμφωνα με τη μεθοδολογία NIST, παρέχεται ένα υψηλό επίπεδο ασφάλειας για τα συστήματα με Windows XP Professional, ανάλογα με το ρόλο που έχει το κάθε σύστημα και σε ποιό περιβάλλον αυτό ανήκει. Όταν μία IT λίστα ελέγχου διαμόρφωσης ασφάλειας (πχ διεργασία προστασίας ή ελέγχου συστήματος) εφαρμόζεται σε ένα σύστημα σε συνδυασμό με εκπαιδευμένους διαχειριστές και με ένα αποτελεσματικό πρόγραμμα ασφάλειας, μπορεί να επιτευχθεί μία ουσιαστική μείωση στην έκθεση των αδυναμιών ενός συστήματος. Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των Ηνωμένων Πολιτειών (NIST) παρέχει πρότυπα ασφάλειας και συστάσεις που δίνουν τις απαραίτητες πληροφορίες στους διαχειριστές συστημάτων για τη διαμόρφωση των ρυθμίσεων ώστε να συμμορφώνονται με τις τοπικές πολιτικές ή με ειδικές περιπτώσεις ασφάλειας. Στην πτυχιακή εργασία παρουσιάζονται γνωστοί τύποι απειλών και γίνεται ανάλυση και διαμόρφωση των συστημάτων σε συγκεκριμένα περιβάλλοντα. Επιπλέον η εργασία μελετά και δοκιμάζει στην πράξη τα πρότυπα ασφάλειας που παρέχονται από το ινστιτούτο NIST.

Abstract

Using specific settings, according to the Methodology NIST, provides a high level of security for systems running Windows XP Professional, taking into account the role that each system plays and in which environment it belongs to. When an IT security configuration checklist (e.g., hardening or lockdown guide) is applied to a system in combination with trained system administrators and a sound and effective security program, a substantial reduction in vulnerability exposure can be achieved. The National Institute of Standards and Technology (NIST) provides security templates and recommendations that give the information necessary to the system administrators for the settings configuration so as to be complied with local policies or special security incidents. This thesis presents known types of threats and it analyzes and configures systems in certain environments. In addition this thesis examines and tests the security templates provided by the NIST institution.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Πίνακας Πινάκων

Κεφάλαιο 1

1. Εισαγωγή

1.1 Φορέας

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology [NIST]) ανέπτυξε αυτό το έγγραφο ως προαγωγή των θεσπισμένων ευθυνών του κάτω από την Ομοσπονδιακή Πράξη Διαχείρισης Ασφάλειας της Πληροφορίας (Federal Information Security Management Act [FISMA]) του 2002, Δημόσιος Νόμος (Ηνωμένων Πολιτειών της Αμερικής) 107-347.

Το NIST είναι υπεύθυνο για την ανάπτυξη προτύπων και οδηγιών, συμπεριλαμβανομένου των ελαχίστων απαιτήσεων για την παροχή επαρκών πληροφοριών ασφάλειας για όλες τις συντελεστικές λειτουργίες και στοιχεία, αλλά τέτοια πρότυπα και οδηγίες δεν απευθύνονται σε συστήματα εθνικής ασφάλειας. Αυτές οι οδηγίες είναι σύμφωνες με τις απαιτήσεις της εγκυκλίου A-130 του Υπουργείου Οικονομίας και Διοίκησης (Office of Management and Budget [OMB]) των Ηνωμένων Πολιτειών της Αμερικής, ενότητα 8b(3), "*Securing Agency Information Systems*", όπως αναλύεται στην ενότητα A-130, Παράρτημα IV: *Analysis of Key Sections*.

Αυτές οι οδηγίες είναι προετοιμασμένες για χρήση από Ομοσπονδιακούς παράγοντες. Μπορούν να χρησιμοποιηθούν από μη-κυβερνητικούς οργανισμούς σε εθελούσια βάση και δεν αποτελούν αντικείμενο κατοχύρωσης πνευματικών δικαιωμάτων (copyright), αν και η συμβολή στο συνολικό έργο είναι επιθυμητή.

Σε καμία περίπτωση αυτό το έγγραφο δεν αναιρεί τα πρότυπα και τις οδηγίες που έχουν δημιουργηθεί αποκλειστικά και υποχρεωτικά πάνω σε Ομοσπονδιακούς παράγοντες από τη Γραμματεία Εμπορίου υπό θεσπισμένης αρχής, ούτε και θα πρέπει αυτές οι οδηγίες να ερμηνευτούν ως εναλλακτική ή αντικατάσταση των υπαρχόντων αρχών της Γραμματείας Εμπορίου, του Συμβουλίου του OMB, ή οποιασδήποτε άλλης ομοσπονδιακής αρχής.

1.2 Αντικείμενο και Σκοπός

Αυτή η δημοσίευση αποσκοπεί στο να βοηθήσει τους επαγγελματίες IT στην ασφάλεια των σταθμών εργασίας Windows XP, των κινητών XP υπολογιστών και των XP υπολογιστών που χρησιμοποιούνται από τηλε-εργαζόμενους μέσα σε διάφορα περιβάλλοντα. Αυτός ο οδηγός θα πρέπει να εφαρμόζεται σε ολόκληρη την επιχείρηση μόνο από εκπαιδευμένους και ικανούς διαχειριστές συστήματος. Αν και ορισμένα μέρη του οδηγού που παρουσιάζονται σε αυτό το εγχειρίδιο μπορούν να εφαρμοστούν σε πολλές εκδόσεις των Windows XP, αυτός ο οδηγός είναι ειδικά σχεδιασμένος για Windows XP Professional συστήματα που τρέχουν Service Pack 2 (SP2) ή Service Pack 3 (SP3).[1]

[1] Το SP2, που κυκλοφόρησε τον Αύγουστο του 2004, περιέχει πολλές αλλαγές που μπορούν να επηρεάσουν την ασφάλεια και τη λειτουργικότητα του συστήματος και των εφαρμογών. Για περισσότερες πληροφορίες δείτε στο Windows XP SP2 Solution Center της Microsoft ((http://support.microsoft.com/ph/6794). Το SP3 κυκλοφόρησε τον Μάιο του 2008.

Ασφαλής διαχείριση Microsoft Windows XP Professional σύμφωνα με την μεθοδολογία NIST SP 800-68 (Μέρος 1ο)

Αυτός ο οδηγός παρέχει λεπτομερείς πληροφορίες για τα χαρακτηριστικά ασφάλειας των Windows XP, οδηγίες για τη διαμόρφωση της ασφάλειας γνωστών εφαρμογών, οδηγίες για την εγκατάσταση και διαμόρφωση συστημάτων σε περιβάλλον τομέα και οδηγίες για διαμόρφωση της ασφάλειας για το λειτουργικό σύστημα των Windows XP. Ο οδηγός καταγράφει τις μεθόδους που οι επαγγελματίες IT μπορούν να χρησιμοποιήσουν για να εφαρμόσουν κάθε ρύθμιση ασφάλειας που προτείνεται. Ο πρωταρχικός στόχος αυτού του εγχειριδίου είναι να προτείνει και να εξηγήσει δοκιμασμένες, ασφαλείς ρυθμίσεις για σταθμούς εργασίας Windows XP με αντικείμενο την απλοποίηση του διαχειριστικού βάρους της βελτίωσης της ασφάλειας των Windows XP συστημάτων σε πέντε τύπους περιβαλλόντων: μικρό γραφείο (small office) / γραφείο σπιτιού (home office) [SOHO], enterprise, ειδικής ασφάλειας-περιορισμένης λειτουργικότητας (specialized security-limited functionality [SSLF]), legacy και Federal Desktop Core Configuration [FDCC]. Οι προτεινόμενοι έλεγχοι είναι σύμφωνοι με τους ελάχιστους ελέγχους ασφάλειας για ένα IT σύστημα όπως παρουσιάζονται στη δημοσίευση NIST SP 800-53. Αυτός ο οδηγός και τα σχετικά πρότυπά του έχουν δημιουργηθεί σε υποστήριξη του Προγράμματος Εθνικής Λίστας Ελέγχου του NIST (NIST National Checklist Program).[2]

1.3 Υπευθύνων Κοινό

Αυτό το εγχειρίδιο έχει δημιουργηθεί για επαγγελματίες IT και ιδιαιτέρως για διαχειριστές συστημάτων Windows XP και προσωπικό ασφάλειας πληροφοριών. Το εγχειρίδιο υποθέτει πως ο αναγνώστης έχει εμπειρία στην εγκατάσταση και διαχείριση σε συστήματα βασισμένα στα Windows σε διαμορφώσεις τομέα και standalone. Το εγχειρίδιο συζητά σε τεχνικές λεπτομέρειες, διάφορες Windows XP ρυθμίσεις ασφάλειας μητρώου και εφαρμογών.

1.4 Σχεδιάγραμμα Αναφοράς

Αριθμός κεφαλαίου	Τίτλος	Σύντομη περιγραφή
1	Εισαγωγή	Εισαγωγή
2	Installation, Backup and Patching	Αυτό το τμήμα του οδηγού περιέχει συμβουλές για την εκτέλεση της εγκατάστασης Windows XP Professional, καθώς υποστήριξη και επιδιόρθωση των συστημάτων Windows XP Professional
3	Additional Windows XP Configuration Recommendations	Το τμήμα αυτό ασχολείται με τη πρόσθετη ασφάλεια που σχετίζεται με τις συστάσεις για τα Windows

[2] Για περισσότερες πληροφορίες πάνω στο πρόγραμμα, δείτε το NIST SP 800-70, *Security Configuration Checklists Program for IT Products*, και το NIST SP 800-70 Επανέκδοση 1 (Πρόχειρο), *National Checklist Program for IT Products*, που διατίθενται και τα δύο στη διεύθυνση: http://csrc.nist.gov/publications/PubsSPs.html.

		XP που όμως δεν περιλαμβάνονται στον κατάλογο προτύπων και των GPOs
4	Application Security Configuration Recommendations	Αυτό το τμήμα εξετάζει την διαμόρφωσης ασφαλείας για έξι τύπους εφαρμογών, που χρησιμοποιούνται συνήθως στα συστήματα Windows XP: ακολουθίες εφαρμογή της παραγωγικότητας, email(πελάτες ηλεκτρονικού ταχυδρομείου), Web browsers (προγράμματα περιήγησης στο Web), antivirus software(λογισμικό αντιμετώπισης ιών), προσωπικά firewalls και λογισμικά αντιμετώπισης ιών
5	Βιβλιογραφία	Βιβλιογραφία

Οι επαγγελματίες IT θα πρέπει να αναγνώσουν ολόκληρη τη δημοσίευση, συμπεριλαμβανομένου και των παραρτημάτων, προτού να χρησιμοποιήσουν τα πρότυπα ασφάλειας ή τα GPOs, ή να εφαρμόσουν οποιαδήποτε από τις άλλες υποδείξεις ή προτάσεις αυτού του οδηγού. Οι αναγνώστες με περιορισμένη εμπειρία στη διαχείριση και την ασφάλεια των Windows XP προτρέπονται να μην εφαρμόσουν αυτόνομα σε συστήματα τα πρότυπα, τα GPOs, ή άλλες υποδείξεις. Η τελέσφορη χρήση αυτής της δημοσίευσης προϋποθέτει εκτενή σχεδιασμό και δοκιμές.

Κεφάλαιο 2

2. Installation, Backup, and Patching

Αυτό το τμήμα του οδηγού περιέχει συμβουλές για την εκτέλεση της εγκατάστασης των Windows XP Professional, καθώς και την υποστήριξη και την επιδιόρθωση των συστημάτων των Windows XP Professional. Αναφέρει τους κινδύνους για ένα νέο σύστημα σε ένα δίκτυο και εξετάζει τους παράγοντες κατά το χωρισμό των σκληρών δίσκων σε Windows XP . Περιγράφει επίσης διάφορες τεχνικές εγκατάστασης και παρέχει πληροφορίες για την εκτέλεση τους. Ένα άλλο σημαντικό θέμα είναι η δυνατότητα των Windows XP να υποστηρίζουν και να αποκαθιστούν τις πληροφορίες σχετικά με τη διαμόρφωση των στοιχείων και των συστημάτων. Αυτό το τμήμα επίσης αναφέρει πώς γίνεται η ενημέρωση των υπαρχόντων συστημάτων μέσω της αναπροσαρμογής και των άλλων μέσων της Microsoft για να εξασφαλίσουν ότι <<τρέχουν>> τα πιο πρόσφατα service packs και hotfixes. Συμβουλές παρουσιάζονται επίσης στον προσδιορισμό των ελλειπόντων patches και των misconfigurations ασφάλειας στα συστήματα.
Οι οργανώσεις θα έπρεπε να έχουν υγιείς διοικητικές πολιτικές διαμόρφωσης ,διότι αυτοί κυβερνούν στις αλλαγές που γίνονται στα λειτουργικά συστήματα και στις εφαρμογές, όπως η εφαρμογή των patches σε ένα λειτουργικό σύστημα ή στις τοποθετήσεις εφαρμογών για να παρέχουν τη μεγαλύτερη ασφάλεια. Οι πολιτικές διαμόρφωσης πρέπει επίσης να εξετάσουν την αρχική εγκατάσταση του λειτουργικού συστήματος, την εγκατάσταση κάθε εφαρμογής και τους ρόλους, τις ευθύνες, και τις διαδικασίες για τις αλλαγές των συστημάτων που προκαλούνται με τις βελτιώσεις, τα patches και τις άλλες μεθόδους τροποποίησης.

2.1 Performing a New Installation

Αυτός ο οδηγός μας δείχνει μια νέα εγκατάσταση Windows XP Professional σχετικά με το πώς εκτελείται από την αρχή. Εάν ένας διαχειριστής ή ένας χρήστης αναβαθμίζει μια υπάρχουσα έκδοση των Windows XP , μερικές από τις συμβουλές υπάρχουν σε αυτόν τον οδηγό που όμως μπορούν να είναι ακατάλληλες και να προκαλέσουν προβλήματα. Επειδή ένα μηχάνημα δε είναι πάντα καλυμμένο και επίσης είναι τρωτό στην εκμετάλλευση μέσω του δικτύου καλό θα ήταν κατά τη διάρκεια της εγκατάστασης να είναι κλειστό στο δίκτυο . Εάν ένας υπολογιστής πρέπει να συνδεθεί με ένα δίκτυο, συνιστάται το δίκτυο να είναι απομονωμένο και ασφαλές (π.χ., προστατευμένος με firewall σε ένα έμπιστο δίκτυο) για να ελαχιστοποιήσει την έκθεση από επιθέσεις οποιοδήποτε δικτυού κατά τη διάρκεια της εγκατάστασης. [3]Εάν είναι δυνατόν, το πιο πρόσφατο service pack και τα κρίσιμα hotfixes πρέπει να μεταφορτωθούν από το site της Microsoft, έτσι ώστε να

[3] Οι διαχειριστές πρέπει να ακολουθήσουν τη πολιτική της οργάνωσης για τη σύνδεση των συστημάτων πληροφοριών ή να λάβουν την άμεση έγκριση από τη διαχείριση πριν συνδέουν οτιδήποτε νέα συστήματα σε Windows XP με τη οργάνωση των δικτύων.

αρχειοθετηθούν στα μέσα ανάγνωσης, όπως τα CD –ROMs και να κρατηθούν ασφαλή.

Εικόνα 1: Windows Install

2.1.1 Partitioning Advice

Μια από τις σημαντικότερες αποφάσεις κατά τη διάρκεια της εγκατάστασης είναι πώς να χωρίσει τους σκληρούς δίσκους. Η αρχική εκτίμηση είναι πόσο μεγάλη η μονάδα δίσκου είναι , παραδείγματος χάριν ο χωρισμός δεν συστήνεται για κάτω από 6 gigabytes. Για μεγαλύτερο , πρέπει να εξεταστούν οι ακόλουθοι παράγοντες:

- Πόσο μεγάλη είναι η μονάδα δίσκου;
- Πόσες φυσικές μονάδες δίσκου έχει ο υπολογιστής;
- Εάν το σύστημα έχει ένα μόνο δίσκο, υπάρχει λογικά η επιθυμία να διαχωριστούν το λειτουργικό σύστημα και εφαρμογές με τα δεδομένα; Ένα παράδειγμα για το όφελος από αυτό είναι ότι, αν το λειτουργικό σύστημα πρέπει να αναβαθμιστεί ή να εγκατασταθεί εκ νέου, τα δεδομένα μπορούν εύκολα να διατηρηθούν.
- Ποιος είναι ο σκοπός αυτού του υπολογιστή; Για παράδειγμα, εάν ένας υπολογιστής θα χρησιμοποιηθεί για κοινή χρήση αρχείων μέσα σε μια ομάδα εργασίας, μπορεί να είναι χρήσιμο να έχουμε χωρισμό του δίσκου για το μοίρασμα των αρχείων.
- Υπάρχει ανάγκη για απόλυση (π.χ. κατοπτρισμός των δεδομένων του τμήματος σε ένα δεύτερο δίσκο);

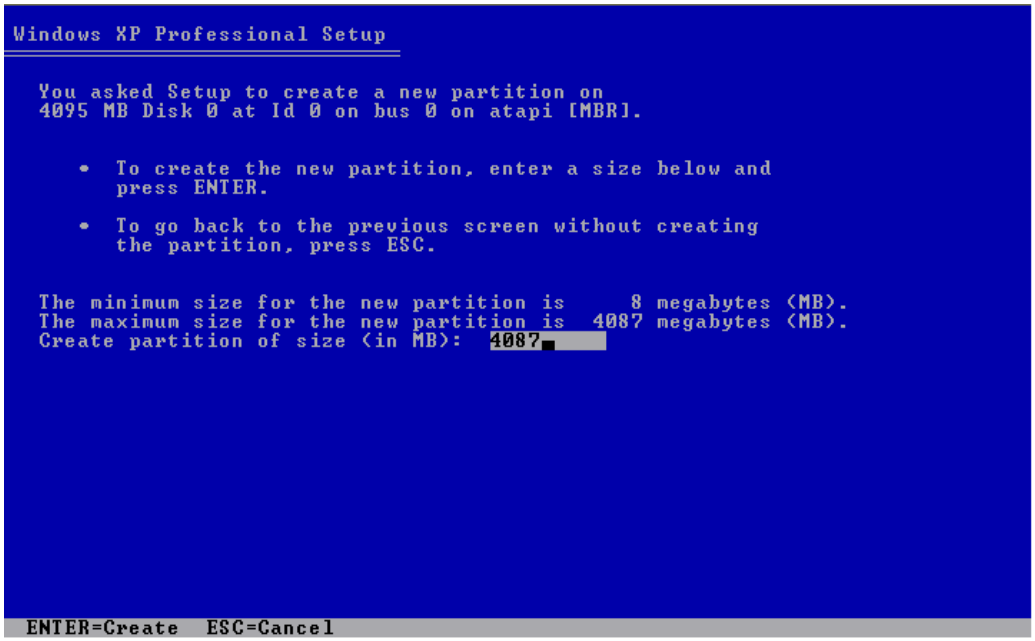
Τα Windows XP Professional παρέχουν ένα χαρακτηριστικό γνώρισμα γνωστό ως δυναμικοί δίσκοι.[4] Σε ένα δυναμικό δίσκο, τα μεγέθη των χωρισμάτων

[4] Για περισσότερες πληροφορίες, δείτε το MSKB article 314343, *Basic Storage Versus Dynamic Storage in Windows XP*, διαθέσιμο στο http://support.microsoft.com/?id=314343.

μπορούν να αλλάξουν όπως απαιτούνται. Παραδείγματος χάριν, ένας διαχειριστής θα μπορούσε να δημιουργήσει ένα μέρος του δίσκου για το λειτουργικό σύστημα και εφαρμογών και ένα άλλο μέρος για στοιχεία με μεγάλη κίνηση, αφήνοντας ένα μεγάλο μέρος του δίσκου διαθέσιμο για τη μελλοντική κατανομή. Όπως απαιτείται, ο διαχειριστής μπορεί να χρησιμοποιήσει τον ελεύθερου χώρο για να δημιουργήσει νέα χωρίσματα και για να επεκτείνει τα υπάρχοντα χωρίσματα. Αυτό παρέχει ιδιαίτερη ευελιξία για μελλοντική ανάπτυξη.

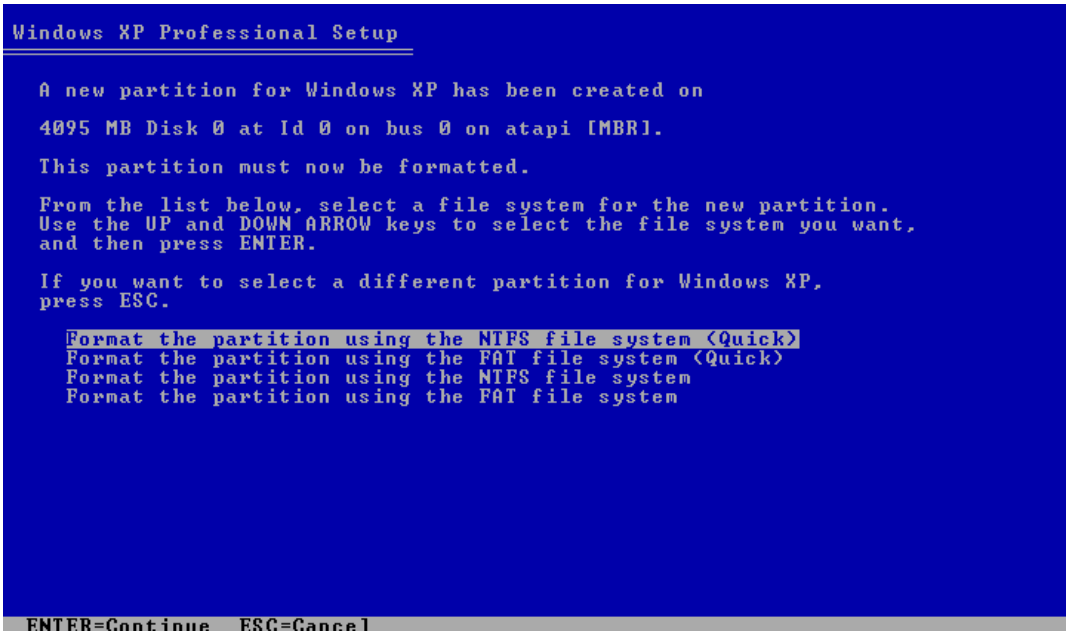
Οι χρήστες προειδοποιούνται, με οποιοδήποτε νέο χαρακτηριστικό γνώρισμα, οι δυναμικοί δίσκοι πρέπει να εξεταστούν πριν επεκτείνουν τα συστήματα παραγωγής του. Οι δυναμικοί δίσκοι μπορούν να είναι ασυμβίβαστοι με μερικές εφαρμογές, με συγκεκριμένα συστήματα συντήρησης και διαχείρισης.

Εικόνα 2: Λίστα με τα υπάρχοντα & μη υπάρχοντα partitions



Εικόνα 3: Δημιουργία μεγέθους του partition

Μια άλλη σημαντική εκτίμηση κατά τη διάρκεια της εγκατάστασης είναι ποιο τύπο του filesystem θα χρησιμοποιήσεις στο χώρισμα του δίσκου. Το NIST συστήνει να χρησιμοποιείται NTFS για κάθε χώρισμα, εκτός αν υπάρχει μια συγκεκριμένη ανάγκη να χρησιμοποιηθεί ένας άλλος τύπος filesystem. Η παράγραφος 3.1 περιέχει περισσότερες πληροφορίες για NTFS και άλλες επιλογές του filesystem.



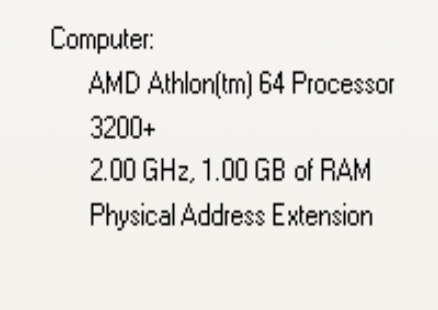
Εικόνα 4: Είδος διαμόρφωσης του δίσκου

2.1.2 Installation Methods

Υπάρχουν διάφοροι τρόποι για να εκτελεσθεί εγκατάσταση των Windows XP. Αυτό το τμήμα καλύπτει τρεις πρωτεύον μεθόδους: τη τοπική εγκατάσταση, τη κλωνοποιήση μέσω Sysprep και η απομακρυσμένη υπηρεσία εγκατάστασης (RIS).

2.1.2.1 Local Installation

Χαρακτηριστικά υπολογιστή



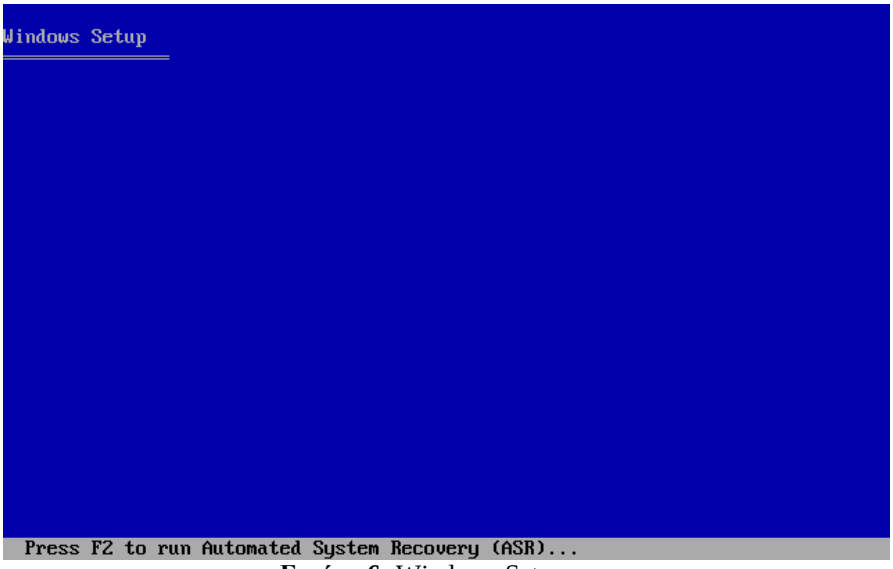
Εικόνα 5: Χαρακτηριστικά του υπολογιστή

Το CD που χρησιμοποίησα είναι : ***WINDOWS XP PROFESSIONAL SERVICE PACK 3 EDITION ENGLISH***

Πως κάνεις boot ένα cd?

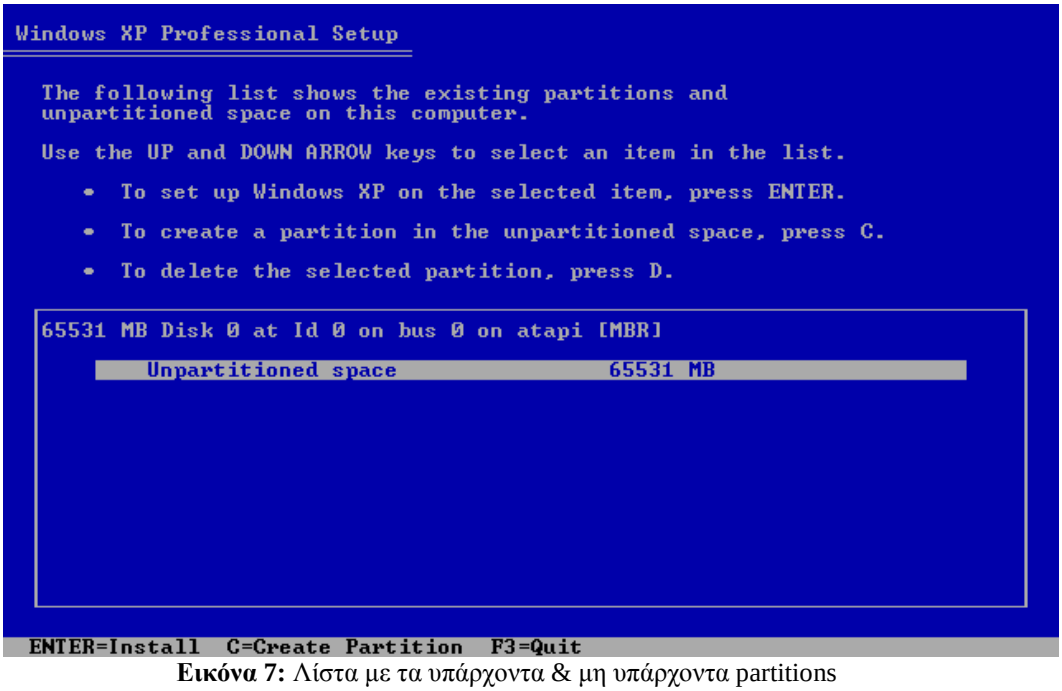
Αρχικά, κανείς επανεκκίνηση στον υπολογιστή ,καθώς ξεκίνα και εμφανίζεται η μαύρη οθόνη πατάς το κουμπί DEL και μπαίνεις στα BIOS του υπολογιστή σας. Καθώς βρίσκεστε στο μενού του BIOS ,πηγαίνετε με τα βελάκια στην επιλογή boot sequence και βάλτε να διαβάζει πρώτα το CD-ROM και δεύτερο το σκληρό σας δίσκο. Τέλος πηγαίνετε στη έξοδο και πατήστε save&settings για να βγείτε και να αποθηκεύσετε τις επιλογές σας.

Μετά τοποθετήστε το cd των windows που θέλετε να εγκαταστήσετε στο CD-ROM και κάνετε ξανά επανεκκίνηση στο υπολογιστή σας, έτσι όταν θα αρχίσει να ξεκινάει θα διαβάσει το CD και θα σας εμφανίσει το παρακάτω στη οθόνη.



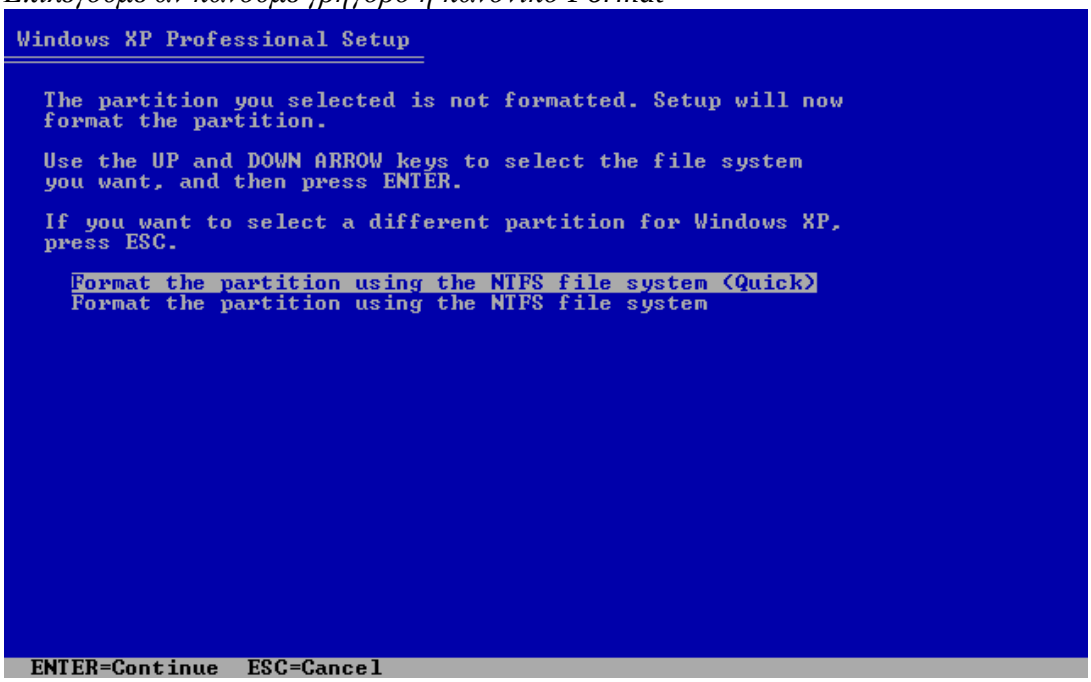
Εικόνα 6: Windows Setup

Μας δίνει τη δυνατότητα να διαλέξουμε αν θα εγκαταστήσουμε τα Windows XP σε ένα μέρος που υπάρχει ελεύθερος χώρος από το δίσκο μας(πατώντας ENTER) ή να δημιουργήσουμε ένα νέο μέρος στο δίσκου(πατώντας C) ή να διαλύσουμε το επιλεγμένο μέρος του δίσκου(αν είχαμε εγκατεστημένα π.χ. Windows XP HOME)και να τα εγκαταστήσουμε εκεί που ευρισκόντουσαν τα παλιά.



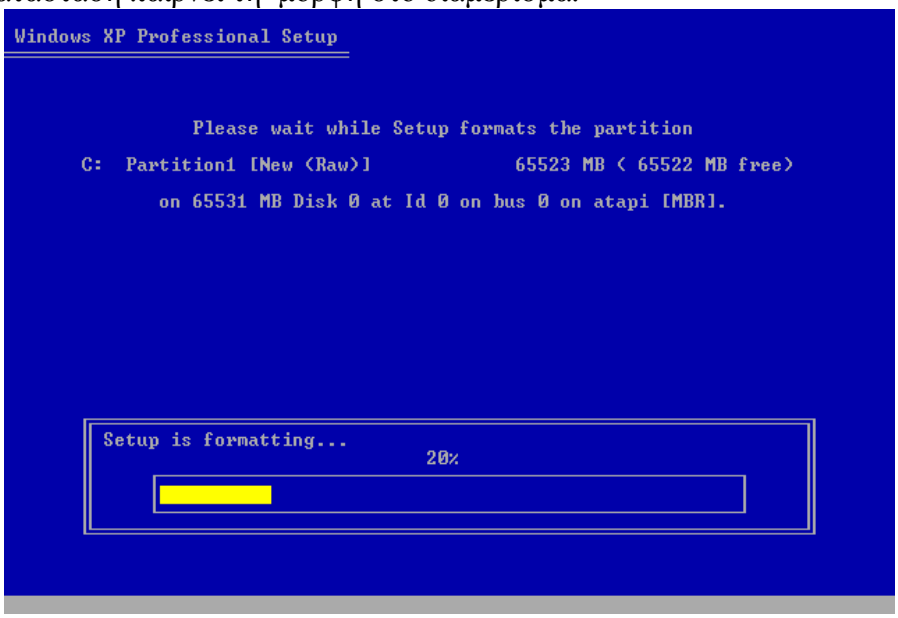
Εικόνα 7: Λίστα με τα υπάρχοντα & μη υπάρχοντα partitions

Επιλεγούμε αν κάνουμε γρήγορο ή κανονικό Format



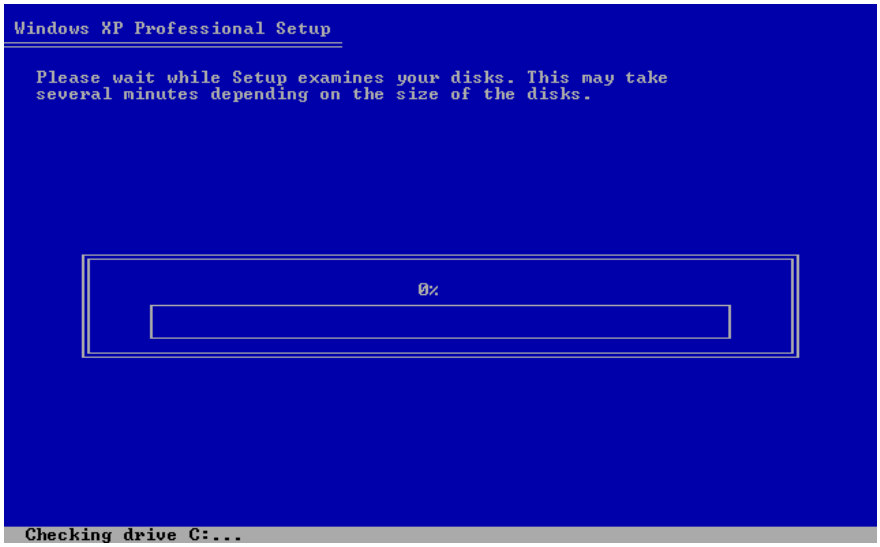
Εικόνα 8: Διαμόρφωση του partition

Η εγκατάσταση παίρνει τη μορφή στο διαμέρισμα.



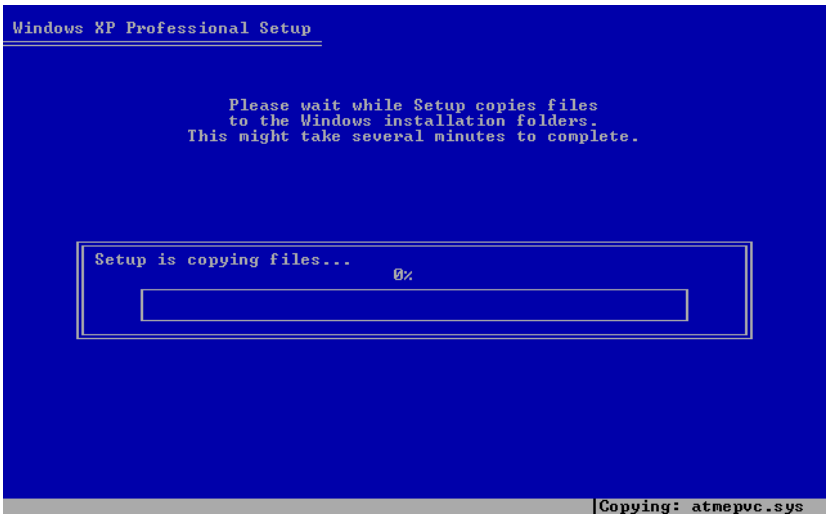
Εικόνα 8: Setup is formatting

Εδώ εξετάζει τους δίσκους σου. Μπορεί να πάρει η διαδικασία μερικά λεπτά ανάλογα με το μέγεθος του δίσκου.

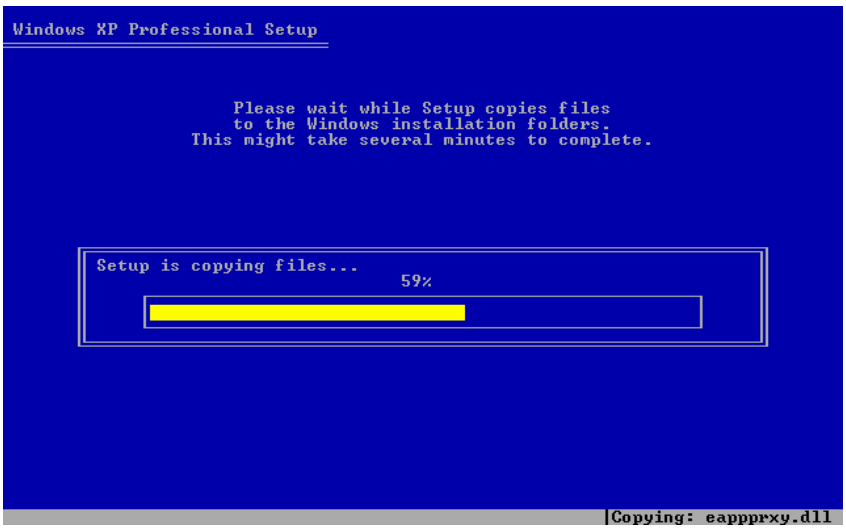


Εικόνα 9: Εξέταση δίσκων

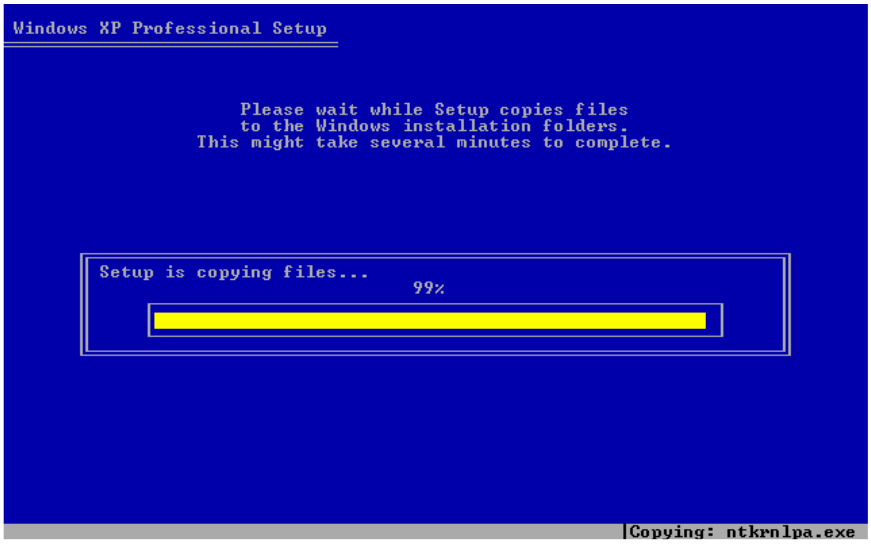
Το πρόγραμμα Εγκατάστασης αντιγράφει τα αρχεία για την εγκατάσταση των Windows



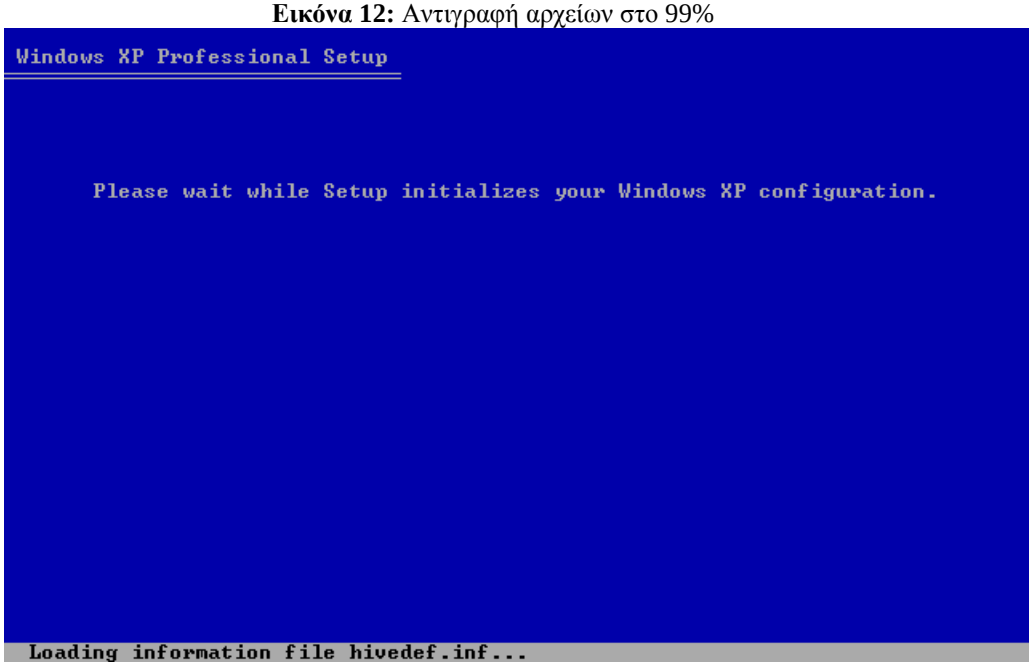
Εικόνα 10: Αντιγραφή αρχείων στο 0%



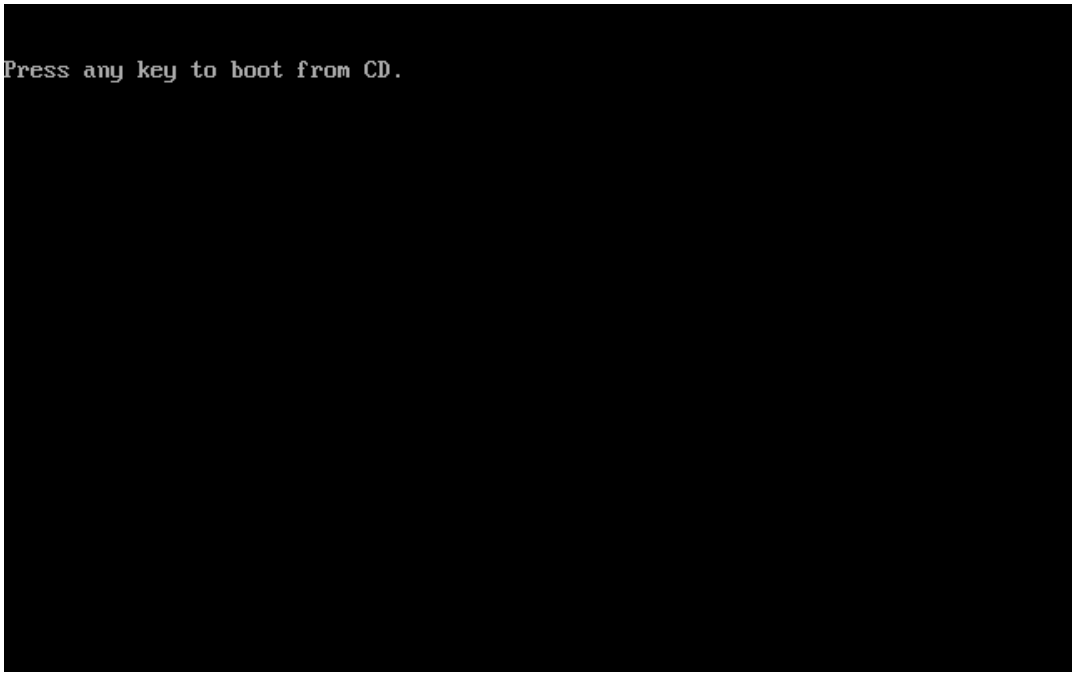
Εικόνα 11: Αντιγραφή αρχείων στο 59%



Εικόνα 12: Αντιγραφή αρχείων στο 99%



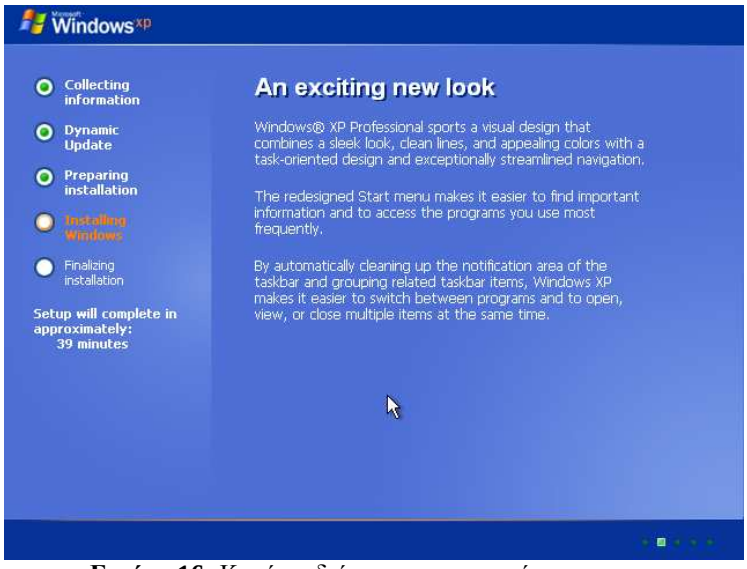
Εικόνα 13: Προετοιμασία εγκατάστασης των Windows στις ρυθμίσεις μας



Εικόνα 14: Εκκίνηση cd

Εικόνα 15: Εκκίνηση της εγκατάστασης

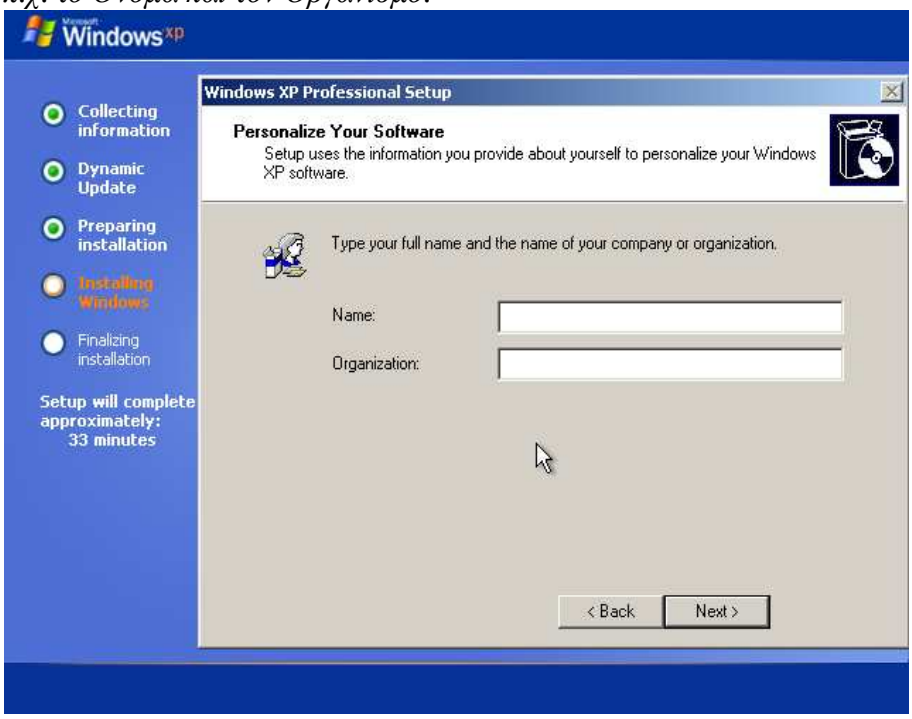
Αρχίζει η διαδικασίας εγκατάστασης που περίπου θα διαρκέσει 39 λεπτά. Εμφανίζει επίσης διάφορα κείμενα κατά τη διάρκεια της εγκατάστασης με τις δυνατότητες των Windows.



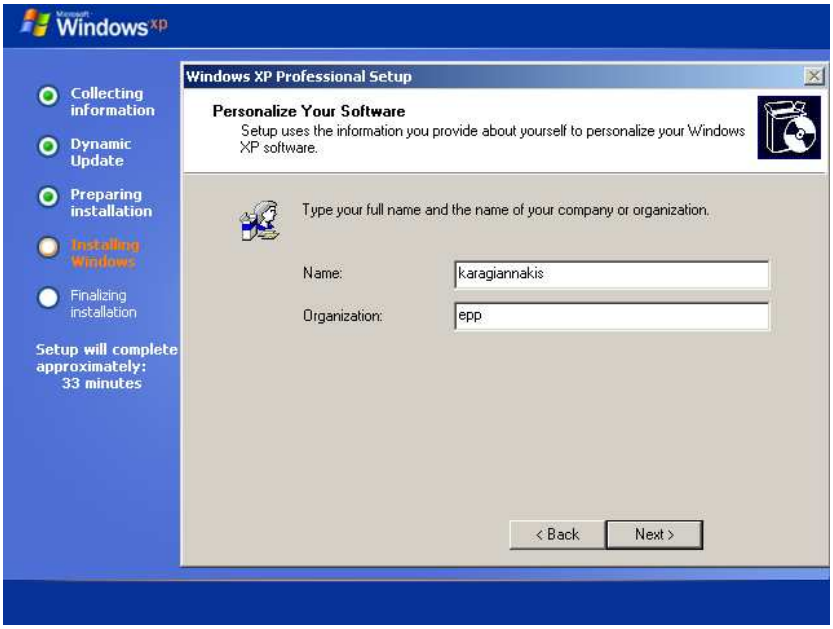
Εικόνα 16: Κατά τη διάρκεια της εγκατάστασης

Εικόνα 17: Συνέχεια της διάρκειας της εγκατάστασης

Κατά τη διάρκεια της εγκατάστασης σου ζήτα μερικά στοιχεία να συμπληρώνεις όπως π.χ. το Όνομα και τον Οργανισμό.



Εικόνα 18: Εισαγωγή ονόματος και οργανισμού

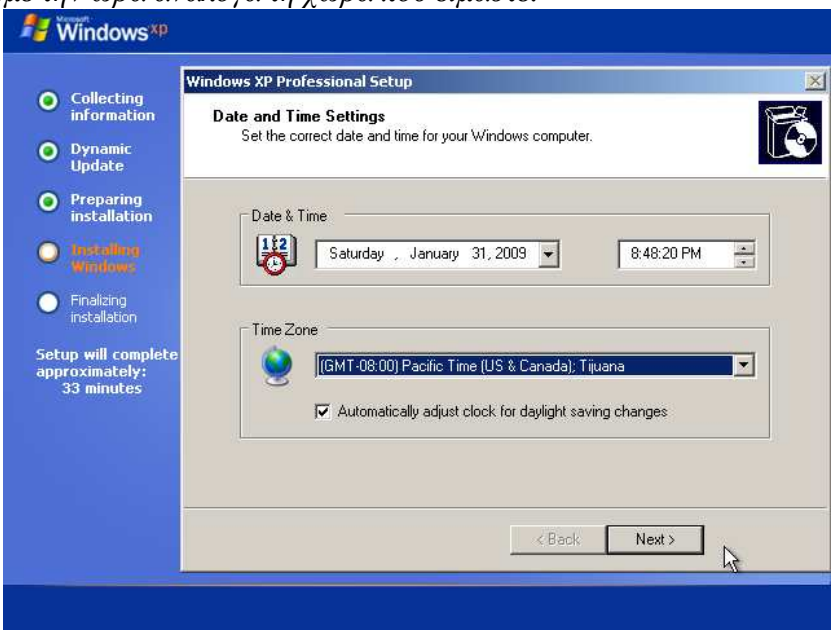


Εικόνα 19: Πληκτρολόγηση ονόματος και κωδικού

Επίσης μας ζητάει να δώσουμε όνομα για το υπολογιστή & κωδικό για το διαχειριστή με επιβεβαίωση.

Εικόνα 20: Εισαγωγή ονόματος υπολογιστή και κωδικό διαχειριστή

Ρυθμίζουμε την ώρα ανάλογα τη χώρα που είμαστε.



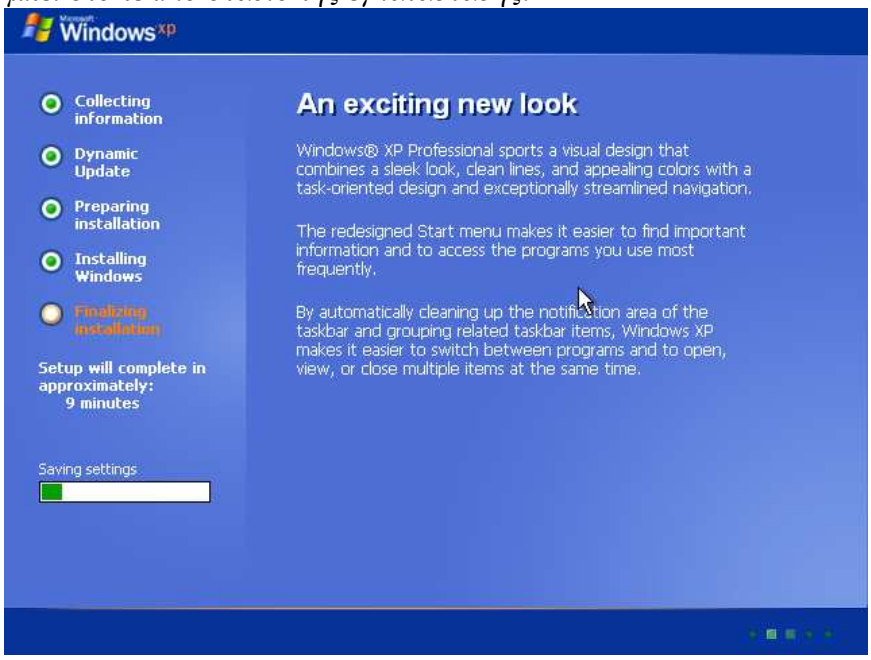
Εικόνα 21: Ρύθμιση ημερομηνίας και ώρα

Και συνεχίζεται η εγκατάσταση

Εικόνα 22: Συνέχεια εγκατάστασης

Εικόνα 23: Συνέχεια εγκατάστασης

Έχουμε μπει στο τελικό στάδιο της εγκατάστασης.



Εικόνα 24: Τελικό στάδιο εγκατάστασης

Εικόνα 25:Τέλος διαδικασίας εγκατάστασης

Μόλις τέλειωσε η διαδικασία εγκατάστασης.

Εικόνα 26: Εκκίνηση από το cd

Τα Windows αρχίζουν και φορτώνονται στον υπολογιστή.

Εικόνα 27: Εκκίνηση των Windows

Μας καλωσορίζουν και μας ευχαριστούν για την αγορά των Microsoft Windows Και τέλος κάποιες ρυθμίσεις που θα διαρκέσουν μερικά λεπτά για τα Windows.

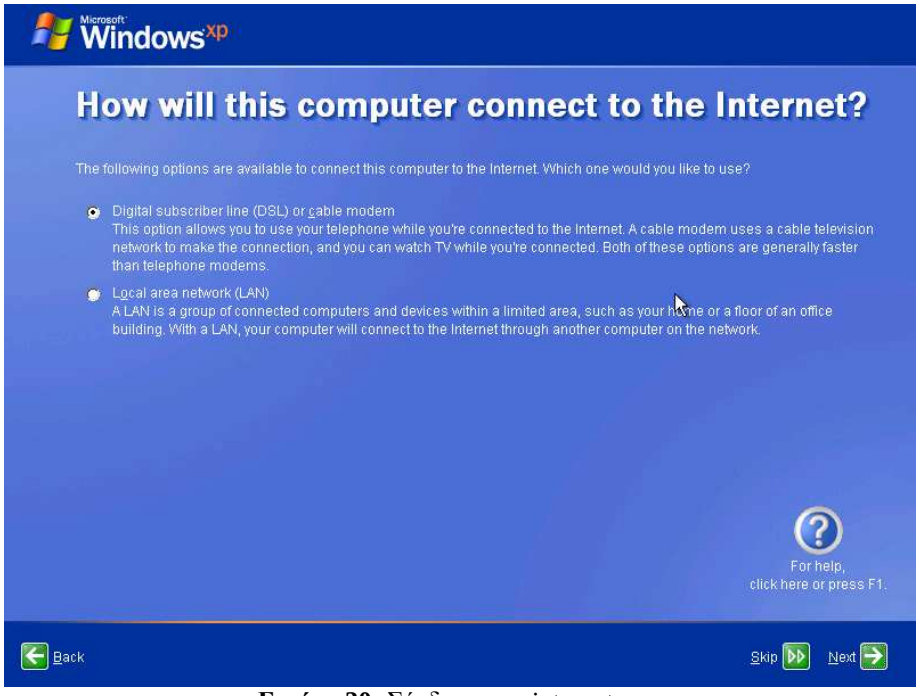
Εικόνα 28: Καλωσόρισμα των Windows

Σου δίνει τη δυνατότητα να διαλέξεις αν θες να σου εγκαθιστούν αυτόματα τις ενημερώσεις μόλις ενεργοποιήσεις σε λειτουργία του υπολογιστή(η οποία προτείνεται από τη Microsoft) ή να μη εγκαθιστούνε αυτόματα .

Εικόνα 29: Help protect your pc

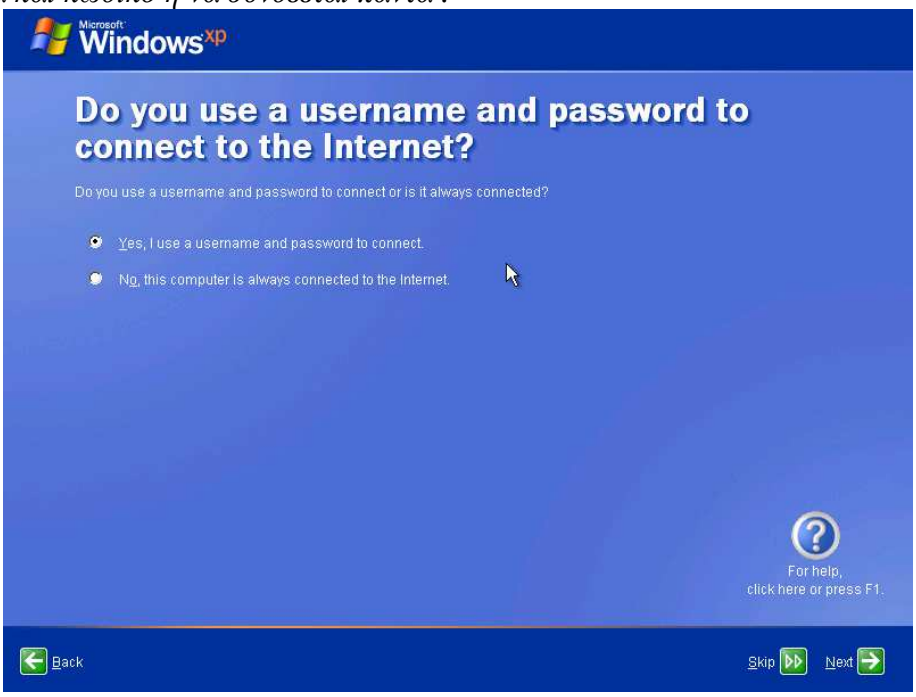
Στη συγκεκριμένη περίπτωση πατήσαμε τη δεύτερη επιλογή.

Σου έχει δυο επιλογές σχετικά με ποιο τρόπο να διαλέξεις να συνδεθείς στο Internet.



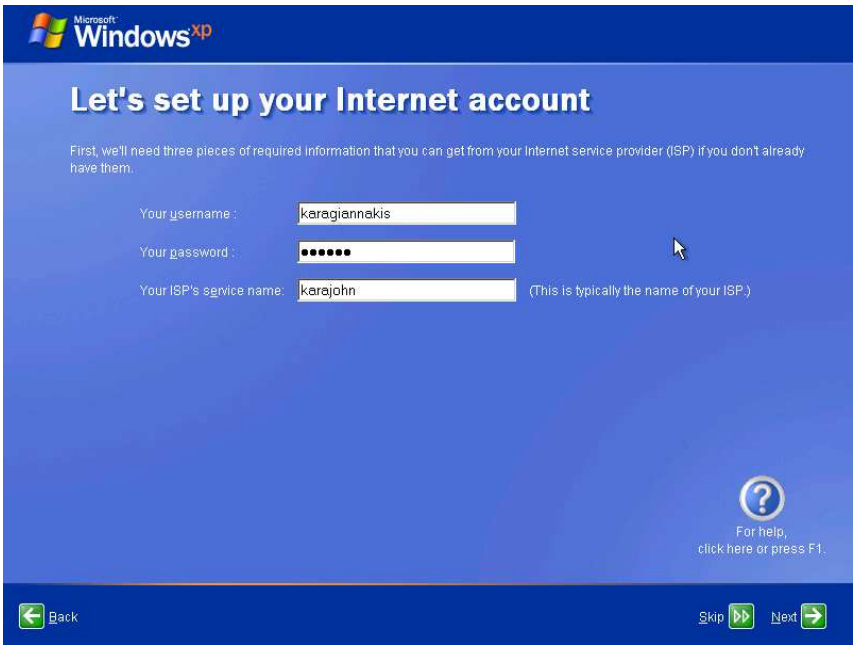
Εικόνα 30: Σύνδεση στο internet

Επίσης σου δίνουν τη δυνατότητα αν θες να συνδέεται στο Internet πατώντας όνομα και κωδικό ή να συνδέεται πάντα .



Εικόνα 31: σύνδεση στο internet με κωδικό και με username

Εδώ φτιάχνεις το λογαριασμό σου, δηλαδή όνομα ,κωδικό και το όνομα του παροχέα που θα συνδέεσαι στο Internet.



Εικόνα 32: Λογαριασμός internet

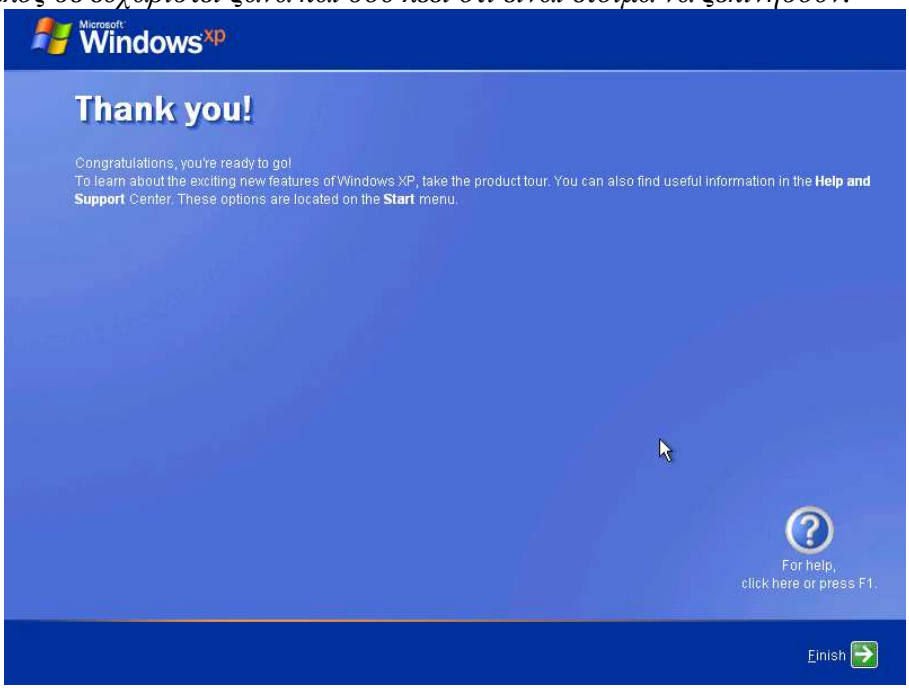
Ακόμα σου δίνουν τη δυνατότητα να γραφτείς μέλος της Microsoft ή κάποια άλλη φορά.

Εικόνα 33: Εγγραφή στη Microsoft

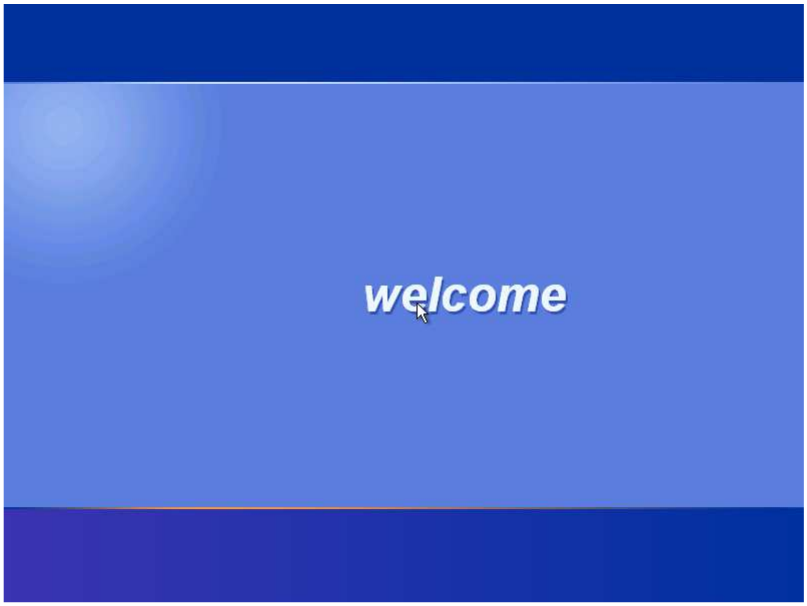
Μπορείς να δημιουργήσεις χρήστες με το ποιοι θα χειρίζονται το υπολογιστή.

Εικόνα 34: Δημιουργία χρηστών

Και τέλος σε ευχαριστεί ξανά και σου λέει ότι είναι έτοιμα να ξεκινήσουν.

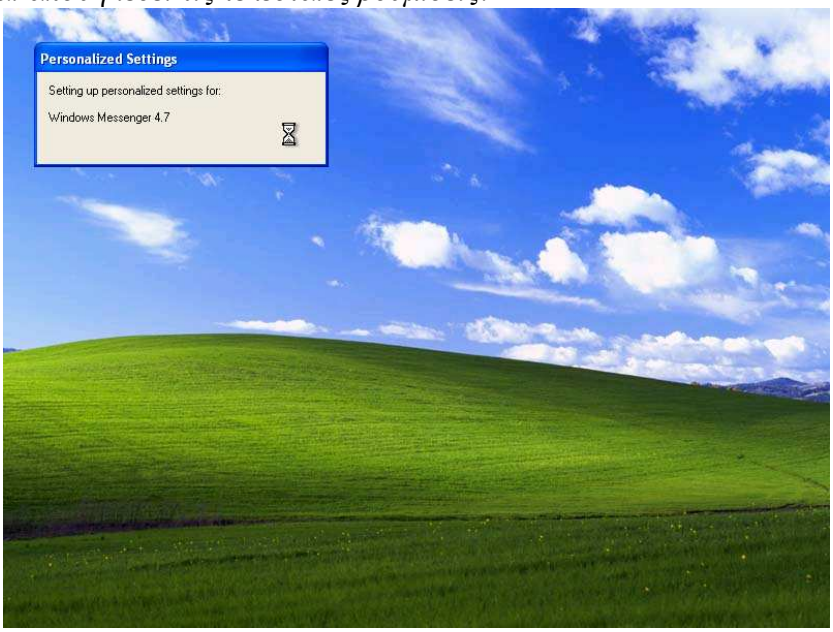


Εικόνα 35: Thank you



Εικόνα 36: Καλωσόρισμα

Εγκαθιστά και αποθηκεύει τις τελευταίες ρυθμίσεις.



Εικόνα 37: Τελευταίες ρυθμίσεις

Και τέλος είναι έτοιμα για χρήση .

Εικόνα 38: Επιφάνεια εργασίας

Η τοπική εγκατάσταση αναφέρεται στις παραδοσιακές μεθόδους εγκατάστασης των Windows, όπως η χρησιμοποίηση του CD της Microsoft. Αυτό είναι αποτελεσματικό μόνο για έναν μικρό αριθμό υπολογιστών επειδή απαιτεί την προσοχή των χρηστών σε όλη την εγκατάσταση. Κατά την εγκατάσταση των Windows XP από το CD, ακολουθήστε τα βήματα προεπιλογής, εκτός από τα εξής:

- Για το Network Setting configuration, επιλέξτε Custom[5] και να απενεργοποιείστε όλους τους Clients του δικτύου, τις υπηρεσίες και τα πρωτόκολλα που δεν απαιτούνται. Αν και αυτό θα βοηθούσε να περιοριστεί η έκθεση του υπολογιστή δικτύου σε επιθέσεις, εξετάζει τις συνέπιες που θα έχει η απενεργοποίηση της κάθε υπηρεσίας, επειδή αυτό μπορεί να προκαλέσει τη ακούσια διακοπή της απαιτούμενης λειτουργικότητας (π.χ. σύνδεση με απομακρυσμένους διακομιστές και εκτυπωτές). Βλέπετε τμήμα 3.5 για περισσότερες πληροφορίες σχετικά με πελάτες του δικτύου, τις υπηρεσίες και τα πρωτόκολλα. Σκεφτείτε την απενεργοποίηση των ακόλουθων υπηρεσιών:

  -Client για Microsoft Networks (οι περισσότεροι χρήστες θα απαιτήσουν αυτήν την υπηρεσία)
  - Client Service για NetWare.
  -Αρχεία και εκτυπωτής που μοιράζονται για τα δίκτυα της Microsoft
  - QoS Packet Scheduler [6]
  -Συμβατό πρωτόκολλο μεταφορών NWLink IPX/SPX/NetBIOS.

[5] Σε όλο αυτό τον οδηγό, ονόματα αρχείων, μενού, επιλογές και επισημαίνονται με έντονους χαρακτήρες κειμένου (π.χ., θυμάστε τον κωδικό μου)
[6] QoS stands για την ποιότητα της υπηρεσίας

- Εάν είναι δυνατόν, ορίστε μια διεύθυνση πρωτοκόλλου Διαδικτύου (IP), προκαθορίστε τη πύλη και το κεντρικό υπολογιστή συστημάτων ονόματος περιοχών (DNS).

- Ακόμα κι αν ο υπολογιστής θα πρέπει να ενταχθεί σε ένα τομέα, επιλέξτε να είστε μόνο σε μια ομάδα εργασίας και να αλλάξετε το όνομα της ομάδας εργασίας για κάτι άλλο από την προεπιλογή WORKGROUP.

- Ρύθμιση όλων των ειδικών ρυθμίσεων του περιβάλλοντος, όπως η ζώνη ώρας.

Όταν η εγκατάσταση υπαγορεύει για λογαριασμούς που θέλουν να προστεθούν , μόνο ένας λογαριασμός πρέπει να προστεθεί αρχικά. Οι άλλοι λογαριασμοί μπορούν πάντα να προστεθούν αργότερα μόλις το σύστημα είναι πλήρως επιδιορθωμένο και διαμορφωμένο. Εξ ορισμού, ο λογαριασμός που δημιουργείται κατά τη διάρκεια της εγκατάστασης και ο ενσωματωμένος λογαριασμός Administrator και οι δύο ανήκουν στην ομάδα Administrators. Μετά την αρχική εκκίνηση και μετά την εγκατάσταση, πρέπει να έχετε ορίσει δύο λογαριασμούς ισχυρών κωδικών πρόσβασης. Η επόμενη εργασία είναι να εγκαταστήσετε το τελευταίο Service Pack και τα Hotfixes(επείγουσες επιδιορθώσεις). Για παρουσιαστεί το μηχάνημα με τα τρέχοντα επίπεδα patches θα πρέπει να συνδεθεί με ένα κανονικό δίκτυο. Στη συνέχεια, η διαμόρφωση δικτύωσης (networking configuration) μπορεί να αλλάξει, όπως η ένταξή της εργασίας σε έναν τομέα ή να την αναθέσουν σε ομάδα εργασίας για να καταστεί η δυνατή κατανομή των πόρων της ομάδας εργασίας (π.χ. κοινή κατάλογοι, εκτυπωτές). Άλλες υπηρεσίες που τέθηκαν εκτός λειτουργίας κατά τη διάρκεια της εγκατάστασης μπορούν να ενεργοποιηθούν εάν είναι απαραίτητο. Είναι επίσης χρήσιμο να ανιχνεύσει μέσω του καταλόγου εγκατεστημένων τμημάτων των Windows, το οποίο καθορίζει τις αιτήσεις και τις χρησιμότητες (π.χ. παιχνίδια στο Internet) που δεν χρειάζονται και να αφαιρούνται.

2.1.2.2 Sysprep

Το Sysprep[7] είναι ένα εργαλείο που επιτρέπει μια εικόνα από μια ενιαία εγκατάσταση υπολογιστών Windows XP, γνωστή ως χρυσό σύστημα, για να κλωνοποιηθεί σε πολλαπλά συστήματα σε συνδυασμό με ένα πρόγραμμα λογισμικού κλωνοποίησης όπως το Ghost ή Disk Image. Αυτή η τεχνική μειώνει τη συμμετοχή των χρηστών στη διαδικασία εγκατάστασης περίπου 5 έως 10 λεπτά στην έναρξη της εγκατάστασης. Η προσέγγιση Sysprep έχει διάφορα οφέλη. Επειδή η τυποποιημένη εικόνα μπορεί να δημιουργηθεί με μια διαμόρφωση ισχυρής ασφαλείας, το Sysprep μειώνει τη δυνατότητα του ανθρώπινου λάθους κατά τη διάρκεια της διαδικασίας εγκατάστασης .Επιπλέον, η εγκατάσταση των Windows XP εμφανίζεται γρηγορότερα με το Sysprep. Αυτό είναι ευεργετικό όχι μόνο για την οικοδόμηση νέων συστημάτων αλλά και για να επανατοποθετηθεί και να μετατρέψει το λειτουργικό σύστημα και τις εφαρμογές γρηγορότερα όταν το χρειάζομαι, για παράδειγμα, ως αποτέλεσμα της αποτυχίας υλικού ή μιας μόλυνσης από ιούς. Στην προετοιμασία της «χρυσής» εικόνας για το Sysprep, είναι οι ίδιες οδηγίες που χρησιμοποιούνται για μια τοπική

[7] Αναφορά *στο πώς να χρησιμοποιήσετε το Sysprep: Μια εισαγωγή* σε http://technet.microsoft.com/en-us/library/bb457073.aspx για πιο λεπτομερείς οδηγίες.

εγκατάσταση, με την προσθήκη της διευκόλυνσης σε οποιαδήποτε αναγκαία υπηρεσία και της επιδιόρθωσης του συστήματος. Είναι επίσης σημαντικό να εξασφαλίσει τη φυσική εικόνα των μέσων ενημέρωσης, ώστε να μην είναι λάθος ή σκοπίμως αλλαχτεί.

2.1.2.3 Remote Installation Services

Οι μακρινές υπηρεσίες εγκατάστασης (RIS) [8] επιτρέπουν σε έναν υπολογιστή να τεθεί σε έναρξη από το δίκτυο και έπειτα να εγκαταστήσει αυτόματα μια εμφάνιση των Windows XP. Οι μακρινές υπηρεσίες εγκατάστασης (RIS) μπορούν να διαμορφωθούνγια να εκτελέσουν είτε μια εντελώς αυτοματοποιημένη και αφύλακτη εγκατάσταση με RISetup, είτε μια που απαιτεί την ελάχιστη συμμετοχή χρηστών (παρόμοια με το εργαλείο Sysprep) με RIPrep. Διάφορες εξαρτήσεις υλικού και λογισμικού υπάρχουν . Επομένως η τεκμηρίωση της Microsoft σχετικά με το εργαλείο θα πρέπει να ζητείται η γνώμη για τις λεπτομερείς οδηγίες σχετικά με τη ρύθμιση αυτής της μεθόδου εγκατάστασης.

Οι μακρινές υπηρεσίες εγκατάστασης (RIS) έχουν τα ίδια πλεονεκτήματα με το εργαλείο Sysprep. RIS έχουν το πρόσθετο πλεονέκτημα ότι δεν χρειάζεται το μηχάνημα που θα εγκατασταθεί να έχει άμεση πρόσβαση στα μέσα ενημέρωσης της φυσική εγκατάστασης (π.χ. ένα CD-ROM). Αυτό μπορεί να είναι ιδανικό σε SSLF περιβάλλον στο οποίο οι μηχανές μπορεί να μην έχουν CD-ROM. Το κύριο μειονέκτημα των RIS είναι ότι ο υπολογιστής πρέπει να είναι συνδεδεμένος σε ένα δίκτυο, ενώ αυτό είναι εγκατεστημένο. Αυτό θα μπορούσε να ανοίξει μια ευκαιρία για να εκμεταλλευτεί μια αδυναμία ασφάλειας προτού να ολοκληρωθεί η εγκατάσταση.

2.2 Backing Up Systems

Για να αυξηθεί η διαθεσιμότητα των στοιχείων σε περίπτωση βλάβης του συστήματος ή ένα σύστημα δεδομένων που προκαλείται από μια δύναμη failure[9] ή άλλη περίπτωση, τα Windows XP έχουν ενσωματωμένη τη δυνατότητα δημιουργίας αντιγράφων ασφαλείας και επαναφορά δεδομένων και συστημάτων. Από προεπιλογή, οι χρήστες εκτελούν το Backup ή Restore Wizard, που αυτοματοποιεί τις περισσότερες από τις διαδικασίες δημιουργίας αντιγράφων ασφαλείας και επαναφοράς. Για παράδειγμα, κατά τη διάρκεια ενός backup στο χρήστη παρουσιάζονται διάφορες επιλογές, μεταξύ των οποίων η υποστήριξη της τρέχουσας χρήσης των αρχείων και ρυθμίσεων, την υποστήριξη όλων των χρηστών σε αρχεία και ρυθμίσεις, καθώς και τη ενίσχυση όλου του συστήματος. Αυτό επιτρέπει στο χρήστη να υποστηρίζει τα στοιχεία και τα συστήματα χωρίς να πρέπει να προσδιοριστούν με το χέρι ποια αρχεία και ποιοι κατάλογοι πρέπει να υποστηριχτούν, εάν τα αρχεία του χρήστη είναι τα αρχεία όπου το πρόγραμμα αναμένει να είναι. Τρέξτε το Backup ή Restore Wizard να εκτελέσει τα ακόλουθα βήματα:

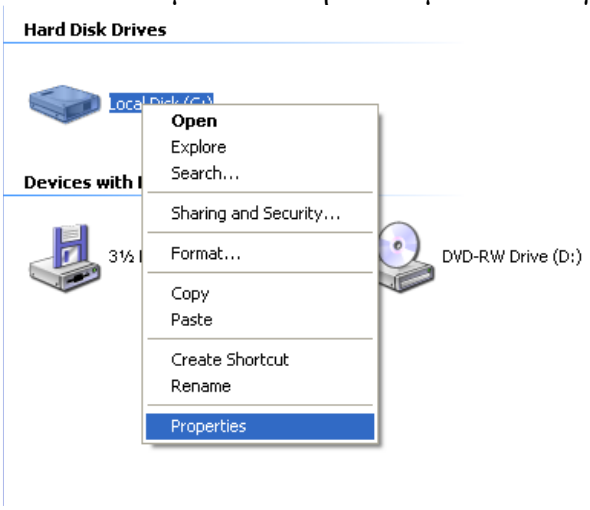
---

[8]. Για περισσότερες πληροφορίες για τη απομακρυσμένη υπηρεσία εγκατάστασης είναι διαθέσιμες από το *Remote Installation Services* στη σελίδα http://technet.microsoft.com/en-us/library/cc786442.aspx

[9] Μια συσκευή προστασία παροχής (UPS) και κύματος ηλεκτρικού ρεύματος μπορεί να παρέχει προσωρινή ενέργεια όταν η παρεχόμενη ενέργεια δεν είναι διαθέσιμη .

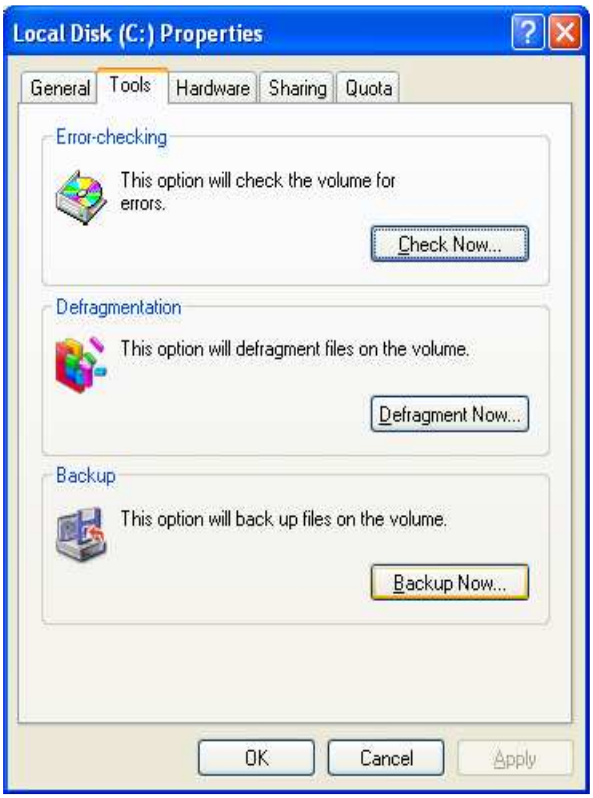
Ασφαλής διαχείριση Microsoft Windows XP Professional σύμφωνα με την μεθοδολογία NIST SP 800-68 (Μέρος 1ο)

1. Άνοιγμα **My Computer**. Πατάμε δεξί κλικ πάνω στο σκληρό μας δίσκο που περιέχει τα δεδομένα που θέλουμε να αποθηκεύσουμε και επιλέγουμε **Properties**..



Εικόνα 39: Local disk properties

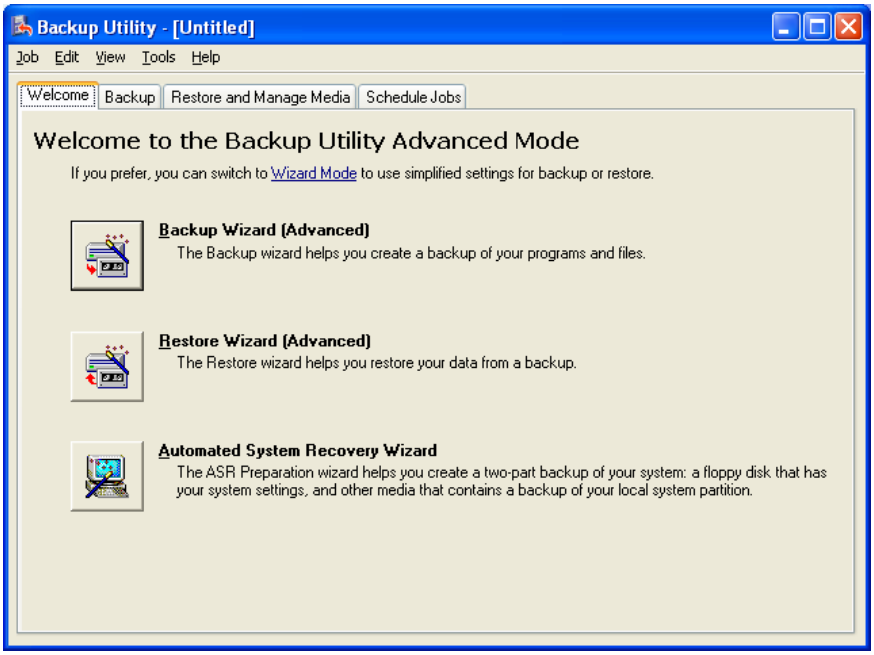
2.Πατάμε στη ετικέτα **Tools** . Πατάμε τώρα στο **Backup Now…**κουμπί. Αυτό ξεκινά το Backup ή Restore Wizard.



Εικόνα 40: Back Now

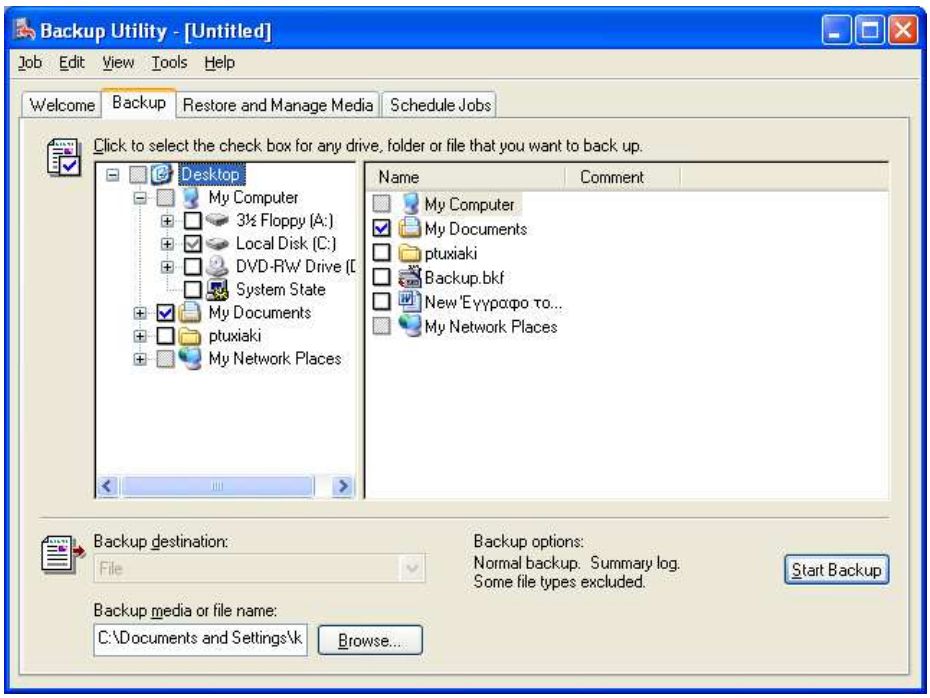
Εικόνα 41:Backup or Restore Wizard

*Πατώντας στο **Advanced Mode** μας εμφανίζει το παρακάτω παράθυρο με τις διάφορες επιλογές. Πατήστε στην ετικέτα **Backup.***



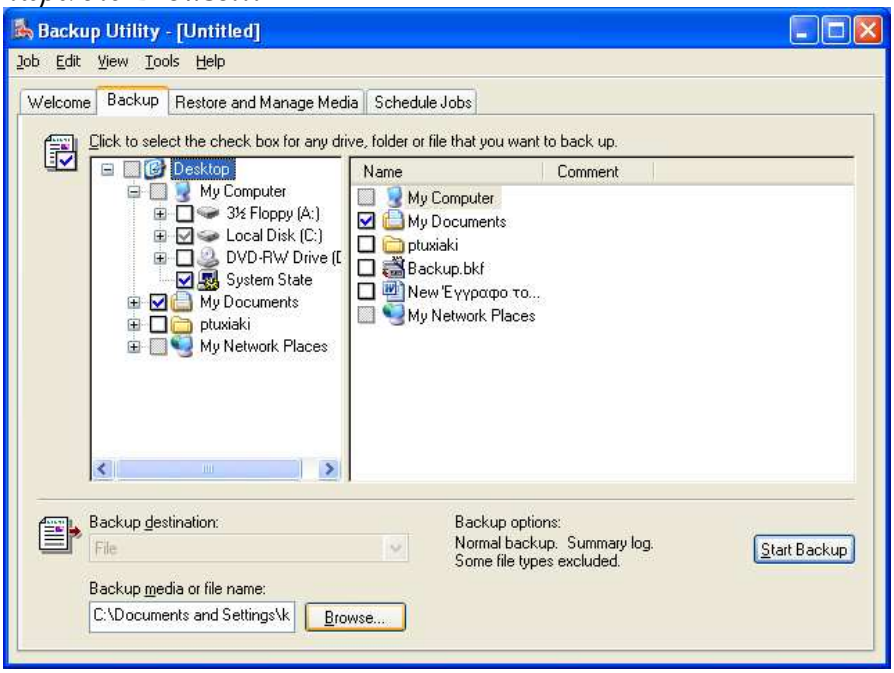
Εικόνα 42:Backup Utility

*Πατήστε το **System State** που βρίσκεται στο Desktop.*



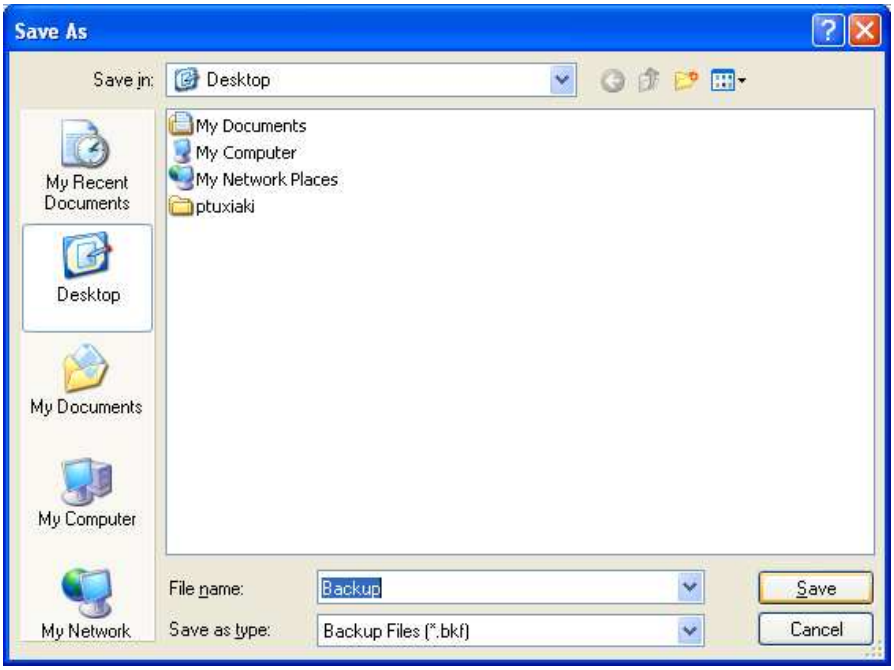
Εικόνα 43: Back up αρχείου

*Πατήστε τώρα στο **Browse…***



Εικόνα 44: Τοποθεσία αποθήκευσης αρχείου

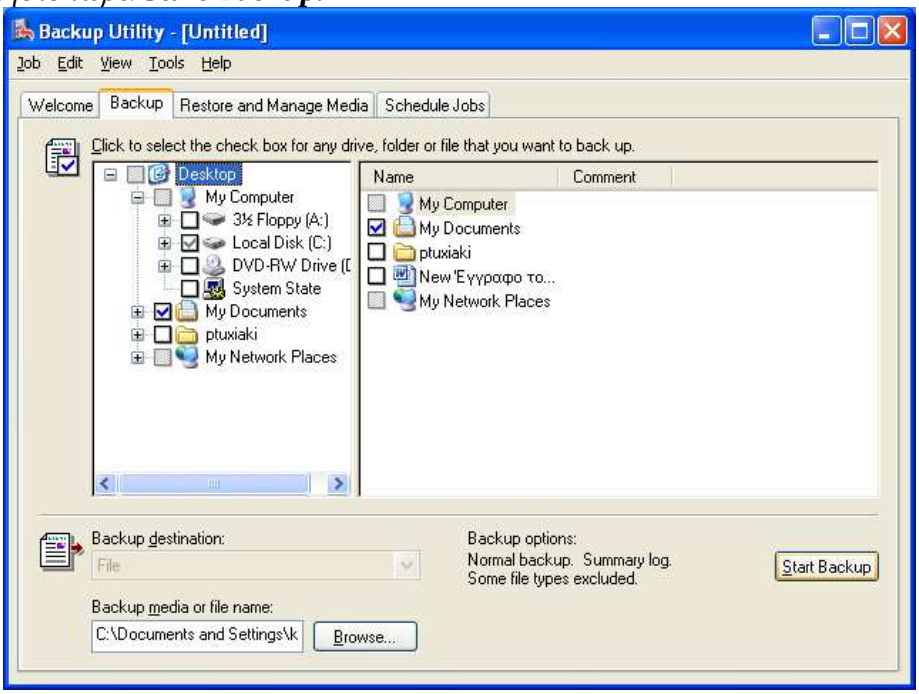
*Και διαλέξετε που θέλετε να αποθηκευτούν αυτά που θέλετε να κάνετε Backup και με τι όνομα και πατήστε **Save.***



Εικόνα 45: File name

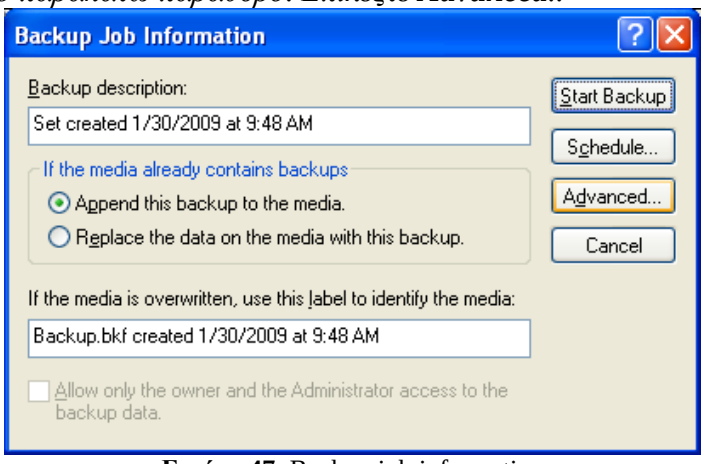
*Τώρα αφαιρέστε την επιλογή από **System State** που βρίσκεται στο Desktop.*

*Και πατήστε τώρα **Start Backup.***



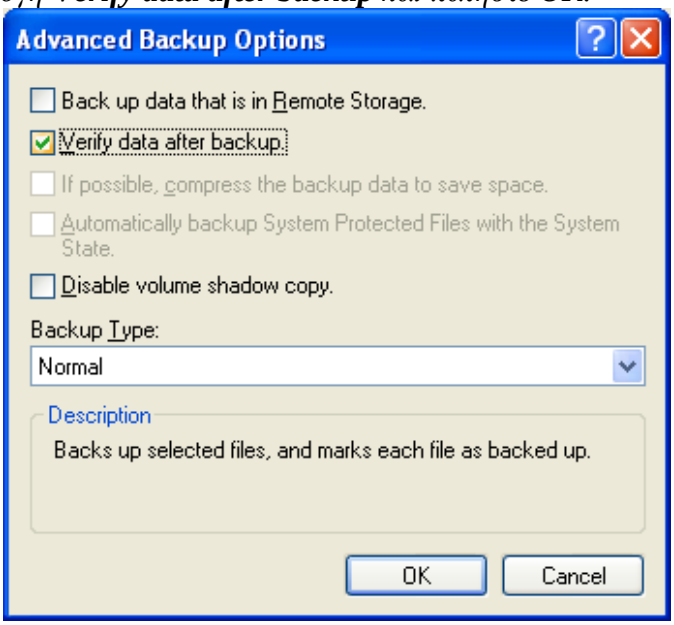
Εικόνα 46: Start Backup

Σας εμφανίζει το παρακάτω παράθυρο. Επιλέξτε ***Advanced****..*



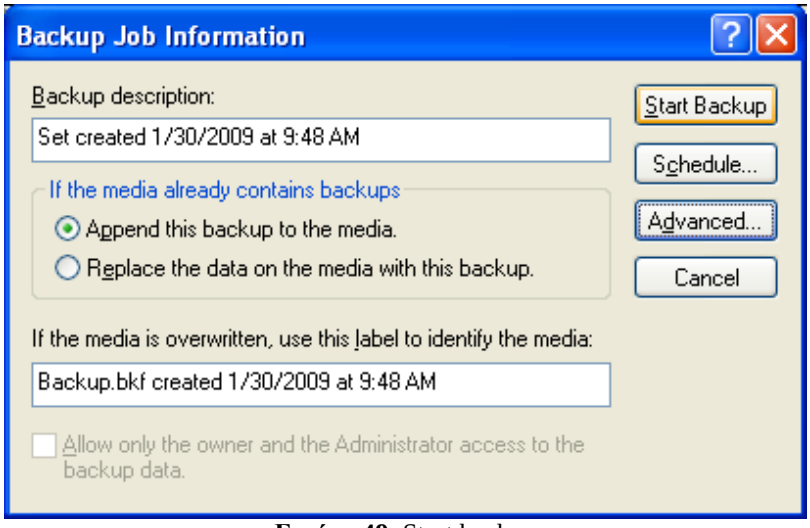
Εικόνα 47: Backup job information

Επιλέξτε την επιλογή ***Verify data after backup*** *και πατήστε OK.*



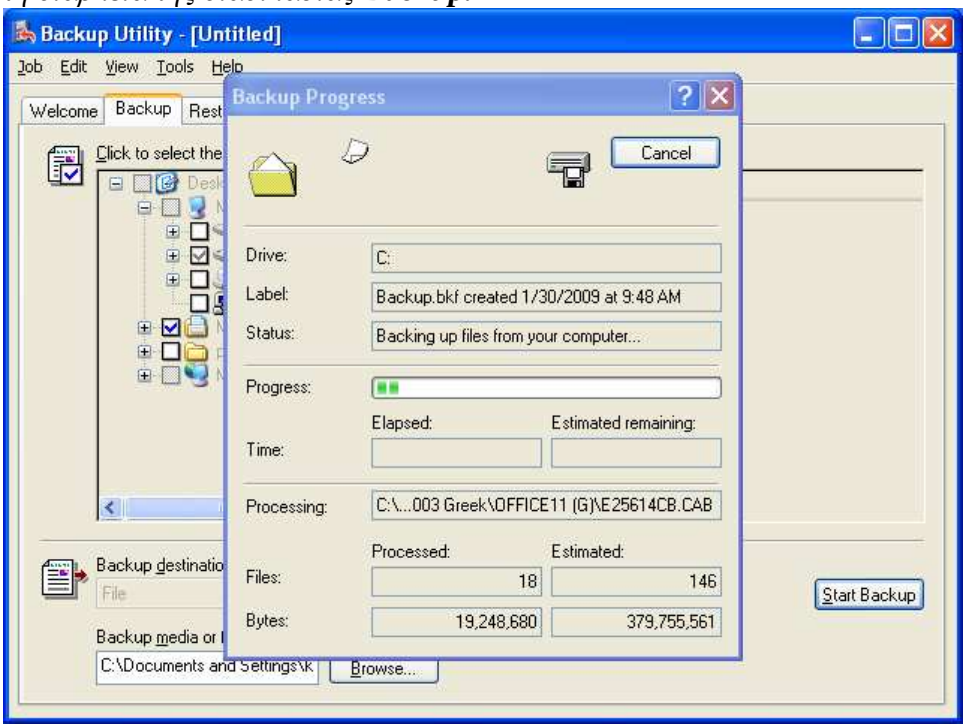
Εικόνα 48: Advanced backup Options

Τέλος πατήστε ***Start Backup*** *για να αρχίσει η διαδικασία* **.**



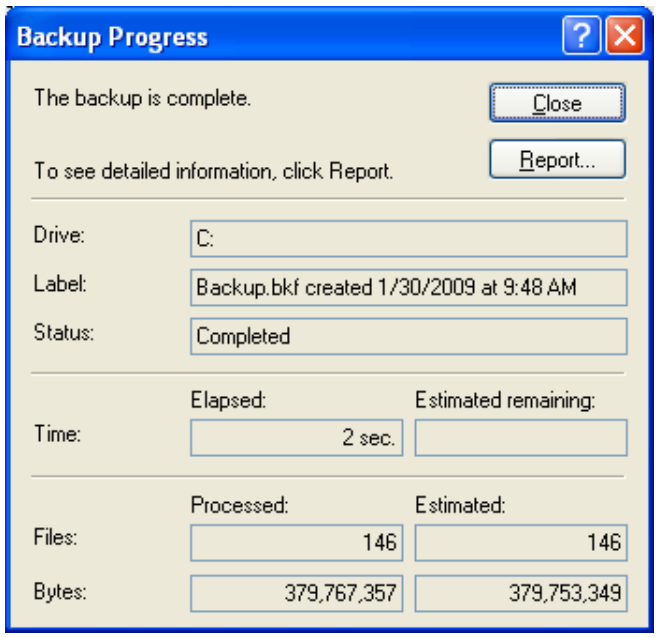
Εικόνα 49: Start backup

Κατά τη διάρκεια της διαδικασίας ***Backup.***



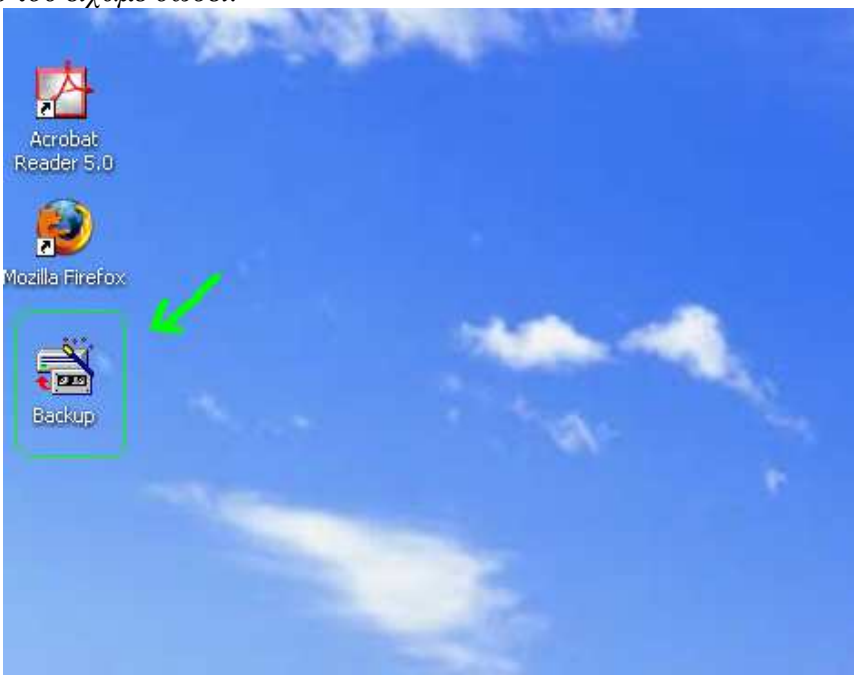
Εικόνα 50: Backup progress

Μόλις τελειώσει η διαδικασία σας εμφανίζει το παρακάτω παράθυρο με διάφορα σημαντικά στοιχεία. Πατήστε ***Close.***



Εικόνα 51: Τέλος backup progress

Βλέπουμε πως μας εμφάνισε το αρχείο του ***Backup*** *στην επιφάνεια εργασίας κ με το όνομα που του είχαμε δώσει.*



Εικόνα 52: Εμφάνιση backup αρχείου

Όταν ένα αντίγραφο ασφαλείας εκτελείται, το αποτέλεσμα είναι ένα αρχείο σε κατάληξη .Bkf (από προεπιλογή Backup.bkf). Εάν ένα πλήρες στήριγμα αντιγράφων

εκτελείται, το αυτοματοποιημένο σύστημα ανάκτησης Wizard θα προτρέψει το χρήστη να παρεμβάλει μια δισκέτα, η οποία θα μετατραπεί σε δίσκο αποκατάστασης που μπορεί να χρησιμοποιηθεί με το αρχείο .bkf για να αποκαταστήσει το σύστημα σε περίπτωση failure[10] όπως υποδηλώνει το όνομα , το Backup ή Restore Wizard μπορεί επίσης να χρησιμοποιηθεί για να επαναφέρετε ένα αντίγραφο ασφαλείας από ένα. bkf αρχείο Είναι πολύ σημαντικό να επαληθεύει περιοδικά τα αντίγραφα ασφαλείας και ότι αποκαθιστά μπορεί να πραγματοποιηθεί με επιτυχία; Η υποστήριξη ενός συστήματος μπορεί να μην είναι καλή εάν τα αντίγραφα ασφαλείας είναι αλλοιωμένα ή είναι λανθασμένα τα αρχεία που υποστηρίζονται, για παράδειγμα. Οι οργανισμοί πρέπει να έχουν τις πολιτικές και τις διαδικασίες που εξετάζουν την ολόκληρη διαδικασία δημιουργίας αντιγράφων ασφαλείας και ανάκτησης, καθώς επίσης και την προστασία και την αποθήκευση των εφεδρικών μέσων και των δίσκων αποκατάστασης. Επειδή τα backups του χρήστη μπορεί να περιέχουν ευαίσθητα δεδομένα, όπως τη διαμόρφωση του συστήματος και πληροφορίες σχετικά με τη ασφάλεια (π.χ., κωδικούς πρόσβασης), τα εφεδρικά μέσα αντιγράφων ασφαλείας θα πρέπει να προστατεύονται όσον αφορά την απαγόρευση της πρόσβασης. [11].

Όταν το Backup ή Restore Wizard εκτελείται, παρουσιάζει μια επιλογή για να επιλέξετε το Advanced Mode. [12]. Έχει επιλογές για το Backup Utility interface, το οποίο δεν είναι και τόσο φιλική προς το χρήστη, αλλά παρέχει μεγαλύτερη customizability και περισσότερα χαρακτηριστικά. Για παράδειγμα, το βοηθητικό πρόγραμμα μπορεί να χρησιμοποιηθεί για να προγραμματίζετε backups. Σε γενικές γραμμές, οι διαχειριστές του συστήματος είναι πιο πιθανό να χρησιμοποιήσουν το βοηθητικό πρόγραμμα λειτουργίας, ενώ οι τελικοί χρήστες είναι πιο πιθανό να χρησιμοποιήσουν το Backup ή Restore Wizard mode.

Εκτός από τους εφεδρικούς οδηγούς και τις χρησιμότητες που παρέχονται από τα Windows XP, υπάρχουν επίσης διάφορες χρησιμότητες τρίτων για την υποστήριξη και την αποκατάσταση των αρχείων και των συστημάτων. Είναι σημαντικό να ελεγχθεί ότι το λογισμικό τρίτων μπορεί κατάλληλα να υποστηρίξει και να αποκαταστήσει συγκεκριμένους πόρους των Windows XP ,όπως το μητρώο των Windows και τα EFS-κρυπτογραφημένα αρχεία και φακέλους. Οι ενσωματωμένες χρησιμότητες των Windows XP χρησιμοποιούν επίσης μια εφεδρική τεχνική με ένα σκιώδες αντίγραφο backup εάν είναι δυνατό , πράγμα που σημαίνει ουσιαστικά θα πάρετε ένα στιγμιότυπο του συστήματος και στη συνέχεια εκτελεί ένα αντίγραφο ασφαλείας για το στιγμιότυπο. Με αυτό αποφεύγει τα προβλήματα με την προσπάθεια να ανοιχτούν τα backup αρχεία Το τρίτο μέρος που χρησιμοποιούνται βοηθητικά προγράμματα δημιουργίας αντιγράφων ασφαλείας των Windows XP, είναι

[10] Για περισσότερες πληροφορίες για την αυτόματη αποκατάσταση συστημάτων, δείτε το άρθρο της Microsoft με τίτλο *How to Set Up and Use Automated System Recovery in Windows XP*, διαθέσιμο στη σελίδα http://technet.microsoft.com/en-us/library/bb456980.aspx.

[11] Για πρόσθετη καθοδήγηση σχετικά backups and backup security, δείτε NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, διαθέσιμα στη σελιδα http://csrc.nist.gov/publications/PubsSPs.html.

[12] Για περισσότερες πληροφορίες για το προηγμένο τρόπο, δείτε το άρθρο της MSKB 308422, *How to use the Backup utility that is included in Windows XP to back up files and folders*, διαθέσιμο στη σελίδα http://support.microsoft.com/?id=308422, και άρθρο 309340, *How to use Backup to protect data and restore files and folders on your computer in Windows XP and Windows Vista*, διαθέσιμο στη σελίδα http://support.microsoft.com/?id=309340.

για συστήματα που θα πρέπει να έχουν καλούς μηχανισμούς για το χειρισμό των ανοιχτών αρχείων.

2.3 Updating Existing Systems

Η υποδοχή ασφάλειας που εξασφαλίζει ο υπολογιστής έχει γίνει όλο και περισσότερο σημαντικό. Υπό αυτήν τη μορφή, είναι σημαντικό να διατηρηθεί ένα πλήθος με τα τρέχοντα επίπεδα patches για να εξαλειφθούν τα γνωστά θέματα ευπάθειας και αδυναμίας [13] Σε συνδυασμό με το λογισμικό αντιμετώπισης ιών και ένα προσωπικό τείχος προστασίας, η επιδιόρθωση προχωρεί αρκετά στην εξασφάλιση ενός οικοδεσπότη ενάντια στις εξωτερικές επιθέσεις και την εκμετάλλευση. Η Microsoft παρέχει δύο μηχανισμούς για τη κατανομή των ενημερωμένων εκδόσεων ασφάλειας: Αυτόματες ενημερώσεις και το Microsoft Update. Στα μικρότερα περιβάλλοντα, καθεμία μέθοδος μπορεί να είναι ικανοποιητική για τη διατήρηση των σημερινών συστημάτων με patches(μπαλώματα). Άλλα περιβάλλοντα διαθέτουν λογισμικό διαχείρισης ελέγχου αλλαγής ή μια ενημερωμένη έκδοση κώδικα διαχείρισης προγράμματος που εξετάζει τα μπαλώματα πριν τη εγκατάσταση τους ; Η διανομή μπορεί έπειτα να προκύψει μέσω των τοπικών του Windows Update Services (WUS) ή Windows Server Update Services (WSUS), οι οποίοι παρέχουν τα εγκεκριμένα κώδικα ασφάλειας προς χρήση για τις αυτόματες αναπροσαρμογές feature[14]. Αυτό το τμήμα ασχολείται με τις αυτόματες αναπροσαρμογές και το Microsoft Update, καθώς επίσης και τις διοικητικές εκτιμήσεις των μπαλωμάτων για τα διοικούμενα περιβάλλοντα. Το τμήμα αυτό καθορίζει επίσης τους τύπους των ενημερωμένων εκδόσεων που συνήθως παρέχει η Microsoft.

2.3.1 Update Notification

Όπως περιγράφεται αργότερα σε αυτό το τμήμα, είναι δυνατό να ρυθμίσετε τα Windows XP για να κατεβάσετε τις κρίσιμες αναπροσαρμογές αυτόματα. Ωστόσο, εξακολουθεί να αφήνει άλλες ενημερώσεις που μπορούν να κατεβούν χειροκίνητα. Επομένως, είναι σημαντικό για τους διαχειριστές των συστημάτων Windows XP να ενημερώνονται για τις νέες αναπροσαρμογές της Microsoft. Η υπηρεσία ανακοίνωσης ασφάλειας της Microsoft είναι ένας κατάλογος διευθύνσεων που ειδοποιεί τους συνδρομητές για νέα θέματα σχετικά με τη ασφάλεια και τη διαθεσιμότητα όλων των τύπων αναπροσαρμογών της Microsoft [15]. Τα δελτία ασφάλειας της Microsoft είναι επίσης διαθέσιμα στο διαδίκτυο από τη TechNet Security TechCenter[16] . Τα μεμονωμένα δελτία εκδίδονται για κάθε νέα ευπάθεια και ενσωματώνονται στα μηνιαία δελτία που απαριθμούν τις ευπάθειες κατά σειρά την σημαντικότητας (π.χ.,

[13] Οι οργανώσεις θα πρέπει να έχουν μια διοικητική πολιτική διαμόρφωσης που περιλαμβάνει τις απαιτήσεις του συστήματος.

[14] WSUS κυκλοφόρησε ως αντικαταστάτης της WUS το Ιούνιο του 2005 . Για περισσότερες πληροφορίες σχετικά με τη WSUS, επισκεφτείτε το Windows Server Update Services Home στη σελίδα http://technet.microsoft.com/en-us/wsus/default.aspx. Πριν τα Windows XP Service Pack 2, WUS ήταν γνωστή ως Software Update Services (SUS).

[15] Οι χρήστες μπορούν να υπογράψουν για τη υπηρεσία ανακοίνωσης στη σελίδα http://www.microsoft.com/technet/security/bulletin/notify.mspx.

[16] The TechNet Security TechCenter βρίσκεται στη σελίδα http://technet.microsoft.com/en-us/security/default.aspx.

κρίσιμος, σημαντικός, μέτριος). Κάθε δελτίο παρέχει καθοδήγηση σχετικά υπό ποιες συνθήκες η προτεινόμενη στρατηγική μετριασμού (π.χ. patch) πρέπει να εφαρμοστεί.

Μερικές ενημερώσεις σχετικά με τη ασφάλεια του υπολογιστή μας βρίσκονται στη εξής σελίδα: http://www.microsoft.com/technet/Security/bulletin/notify.mspx

Microsoft Technical Security Notifications

For IT Professionals

Basic Alerts

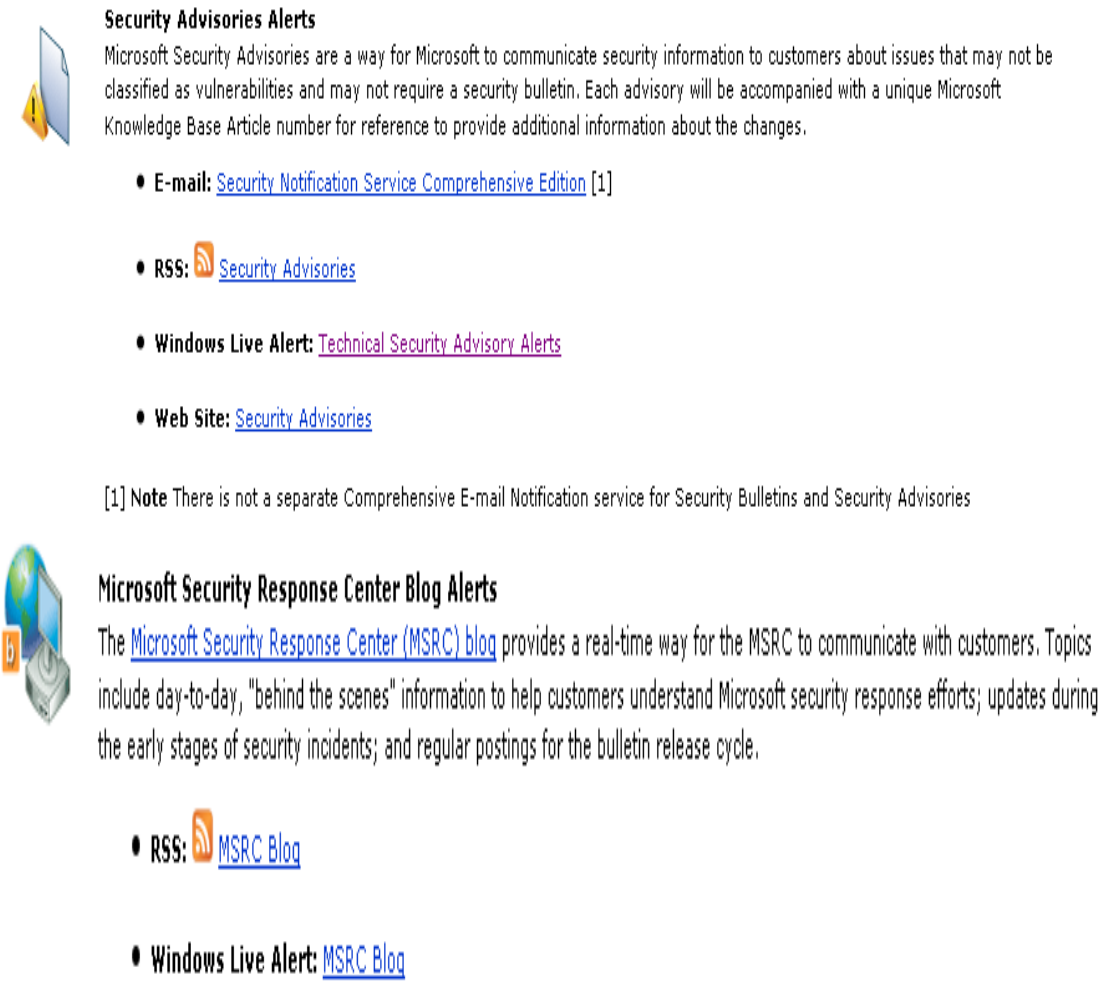
Microsoft's free monthly Security Notification Service provides links to security-related software updates and notification of re-released Microsoft Security Bulletins. The goal of this service is to provide accurate information you can use to protect your computers and systems from malicious attacks. These bulletins are written for IT professionals, contain in-depth technical information, and e-mails are digitally-signed with PGP.

- **E-mail:** Security Notification Service
- **RSS:** Security for IT Professionals
- **Windows Live Alert:** Technical Security Update Alerts
- **Web Site:** Bulletin Search

Comprehensive Alerts

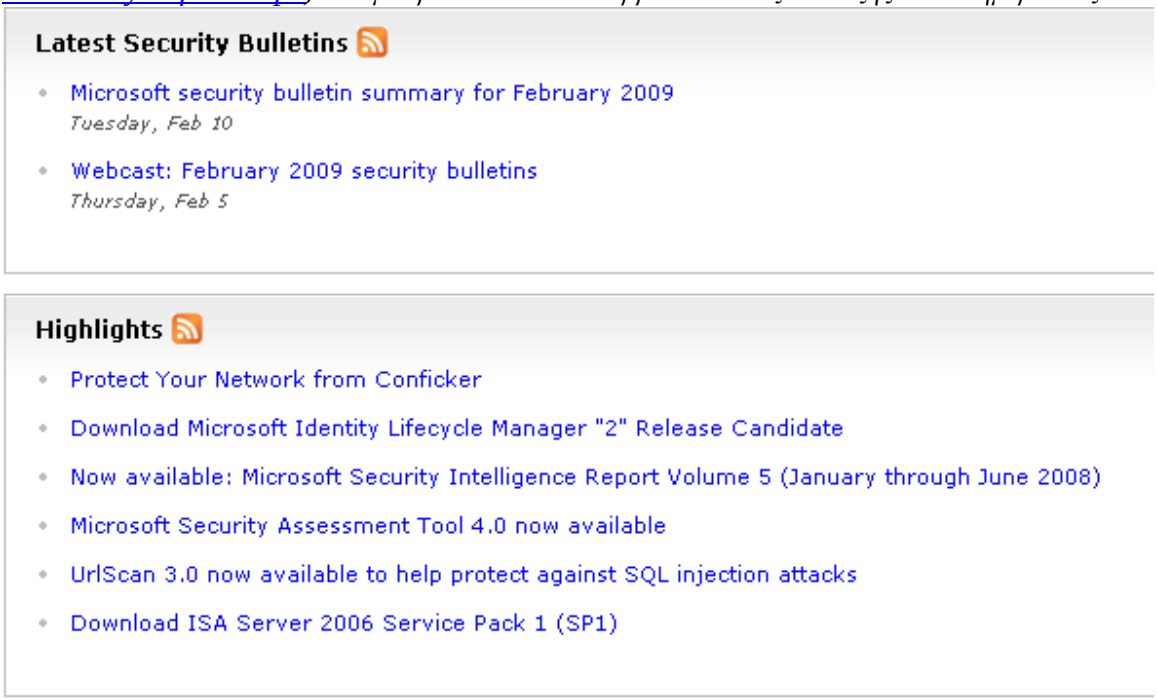
The free Comprehensive alerts serve as an incremental supplement to the Basic Alerts. It provides advance notification of upcoming security bulletins, Security advisories, and timely notification of any minor changes to previously released Microsoft Security Bulletins or Advisories. These notifications are written for IT professionals, contain in-depth technical information, and e-mails are digitally-signed with PGP.

- **E-mail:** Security Notification Service Comprehensive Edition
- **RSS:** Comprehensive Alerts
- **Web Site:** Bulletin Search



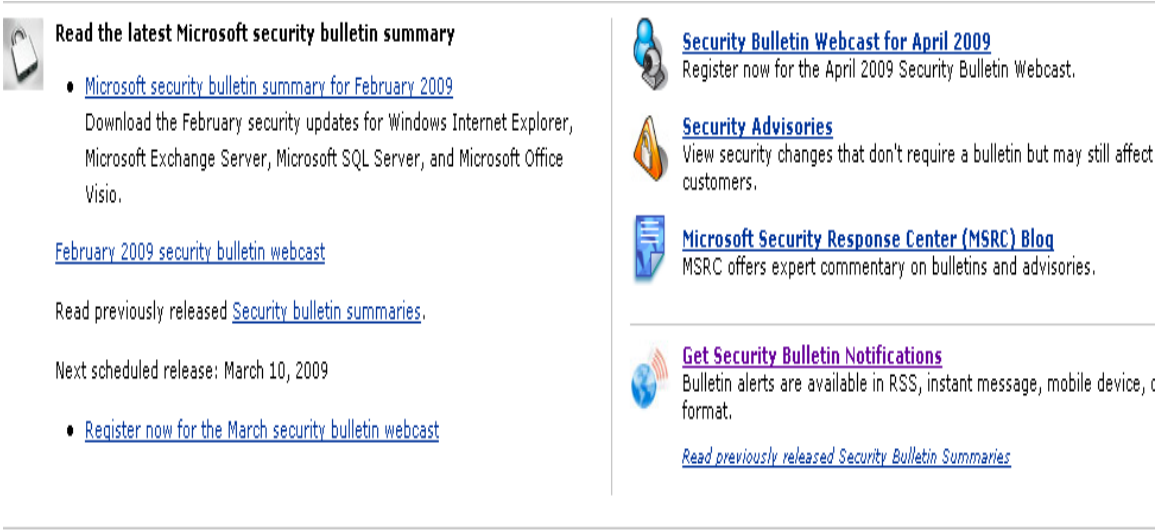
Εικόνα 53: Microsoft Technical Security Notifications

Στην υπηρεσίας Security TechCenter της Microsoft(http://technet.microsoft.com/en-us/security/default.aspx) μπορείτε να βρείτε τις εξής ενημερώσεις:



Εικόνα 54: Ενημερώσεις

Επίσης αν επισκεφτούμε την υπηρεσία της Microsoft Security Bulletin Search (http://www.microsoft.com/technet/security/current.aspx) μας εμφανίζει τα παρακάτω:



Εικόνα 55: The latest Microsoft security bulletin summary

2.3.2 Microsoft Update Types

Η Microsoft κυκλοφορεί ενημερωμένο κώδικα για τα Windows XP που σχετίζονται με τα θέματα ασφάλειας μέσω τριών μηχανισμών: hotfixes (επείγουσες επιδιορθώσεις), security rollups και Service Pack(πακέτο υπηρεσιών).

- Ένα hotfix είναι ένα μπάλωμα που διορθώνει ένα συγκεκριμένο πρόβλημα. Όταν μια νέα ευπάθεια ανακαλύπτεται στα Windows XP ή μια εφαρμογή της Microsoft (π.χ., Internet Explorer), η Microsoft αναπτύσσει ένα hotfix που θα επιλύσει το πρόβλημα. Τα Hotfixes απελευθερώνονται σε μεμονωμένη βάση όπως απαιτείται. Τα Hotfixes πρέπει να εφαρμοστούν πρακτικά για τις ευπάθειες που είναι πιθανό να χρησιμοποιηθούν (Όταν είναι δυνατόν, τα hotfixes θα πρέπει πρώτα να δοκιμαστούν σε ένα σύστημα μη παραγόμενο για να εξασφαλίσουν ότι δεν σπάζουν ακούσια τη λειτουργία ή δεν εισάγουν ένα νέο πρόβλημα ασφαλείας με το σπάσιμο ενός προηγούμενου hotfix.)

Εικόνα 56: Hotfix for windows xp

- Security rollup είναι μια συλλογή διάφορων hotfixes. Το Security rollup κάνει τις ίδιες αλλαγές στο σύστημα που θα εκτελούταν εάν κάθε hotfix εγκαθιστάτε χωριστά. Εντούτοις, είναι ευκολότερο να κατεβαστεί και να εγκατασταθεί ένα Security rollup από 10 hotfixes. Η Microsoft κυκλοφορεί το Security rollups περιστασιακά όταν αξίζει. Security rollups είναι πιο χρήσιμο για τα υπάρχοντα συστήματα που δεν έχουν διατηρηθεί και για την επιδιόρθωση των νέων συστημάτων.

- Ένα πακέτο υπηρεσιών (SP) είναι μια σημαντική βελτίωση στο λειτουργικό σύστημα που επιλύει δεκάδες προβλήματα λειτουργικού και ασφαλείας και εισάγει συχνά μερικά νέα χαρακτηριστικά γνωρίσματα ή κάνει σημαντικές αλλαγές στη ρύθμιση systems[17] . Τα πακέτα υπηρεσιών περιλαμβάνουν τα

[17] Πρόσθετες πληροφορίες σχετικά με τα πακέτα υπηρεσιών είναι διαθέσιμα από το άρθρο της MSKB 322389, *How to obtain the latest Windows XP service pack*, βρίσκεται στη σελίδα http://support.microsoft.com/?id=322389.

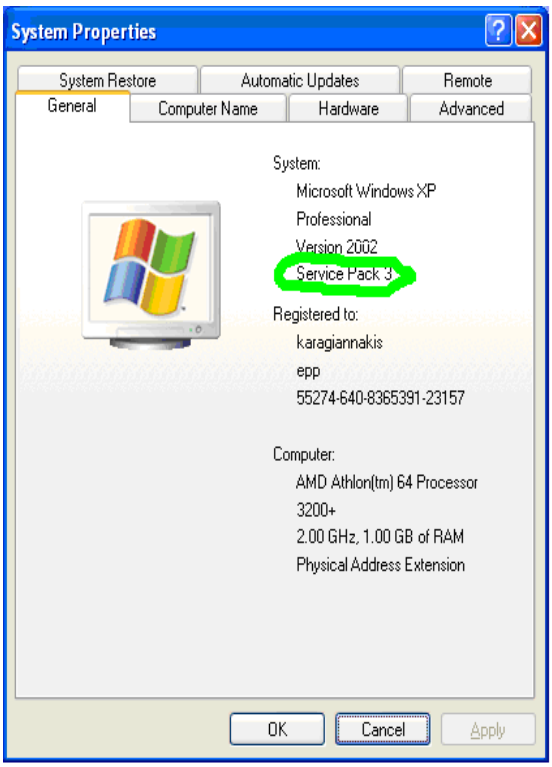
hotfixes που κυκλοφόρησαν, ώστε τη στιγμή που ένα SP έχει εφαρμοστεί σε ένα σύστημα, δεν είναι ανάγκη να εγκαταστήσετε τις επείγουσες επιδιορθώσεις διότι περιλαμβάνονται στο Service Pack. Τα πακέτα υπηρεσιών κυκλοφορούν κάθε λίγα χρόνια για παράδειγμα, τα Windows XP κυκλοφόρησαν το φθινόπωρο του 2001, το SP1το φθινόπωρο του 2002 ,το SP2 το καλοκαίρι του 2004 και SP3 την άνοιξη του 2008. Επειδή τα SPs κάνουν συχνά σημαντικές αλλαγές στο λειτουργικό σύστημα, οι οργανισμοί πρέπει να εξετάσουν το SP λεπτομερώς πριν από τη εγκατάσταση τους στην παραγωγή. Στα περιβάλλοντα SOHO, η καλύτερη επιλογή είναι να καθυστερηθεί η εγκατάσταση του SP για τουλάχιστον μερικές εβδομάδες έτσι ώστε τα πρωτοπόροι χρήστες να μπορούν να προσδιορίσουν τυχόν σφάλματα ή ζητήματα. Εντούτοις, εάν το SP παρέχει μια αποτύπωση για ένα σημαντικό θέμα ασφαλείας και η αποτύπωση δεν είναι διαθέσιμη μέσω των hotfixes, μπορεί να είναι λιγότερο επικίνδυνο να εγκατασταθεί το SP αμέσως από το να αφεθεί το σύστημα.

Εικόνα 57: service pack 3

ΤΑ SERVICE PACK ΠΟΥ ΥΠΑΡΧΟΥΝ ΓΙΑ XP

Service pack1	**17.5 MB**	**21/11/2001**
Service pack2	**266.0 MB**	**07/02/2003**
Service pack3	**316,4 MB**	**06/05/2008**
Service pack3 **2 έκδοση**	**97 KB**	**06/05/2008**
ΟΝΟΜΑ	**ΧΩΡΗΤΙΚΟΤΗΤΑ**	**ΗΜΕΡΑ ΕΚΔΟΣΗΣ**

Πίνακας 1: Services Pack



Εικόνα 58: System Properties

2.3.3 Automatic Updates

Μια εγκατάσταση που είναι διαθέσιμη στα συστήματα ως patch ,με μια μικρή επέμβαση του χρηστή είναι το χαρακτηριστικό γνώρισμα Automatic Updates. Όταν ενεργοποιηθεί, θα ελέγξει αυτόματα τους κεντρικούς υπολογιστές αναπροσαρμογών της Microsoft για τις αναπροσαρμογές του OS και για τις εφαρμογές της Microsoft, συμπεριλαμβανομένων των Service Pack (πακέτων υπηρεσιών), security roll-ups και hotfixes, καθώς επίσης και τις ενημερώσεις αναπροσαρμογών του υλικού των drivers[18]. Οι αυτόματες ενημερώσεις έχουν ένα χαρακτηριστικό γνώρισμα καθορισμού προτεραιοτήτων που εξασφαλίζει ότι οι πιο σημαντικές αναπροσαρμογές ασφάλειας θα εγκαθιστούν πριν από τις λιγότερο σημαντικές αναπροσαρμογές.

Αυτόματες ενημερώσεις παρέχουν τρεις επιλογές ρύθμισης για τους χρήστες:
- ειδοποιεί το χρήστη πριν από τη λήψη ή την εγκατάσταση τυχόν ενημερώσεων.
- Κατεβάζει τις αναπροσαρμογές αυτόματα αλλά ειδοποιεί το χρήστη πριν εγκαταστήσει τις αναπροσαρμογές.
- Κατεβάζει όλες τις αναπροσαρμογές και τις εγκαθιστά αυτόματα σύμφωνα με ένα καθορισμένο διάγραμμα.

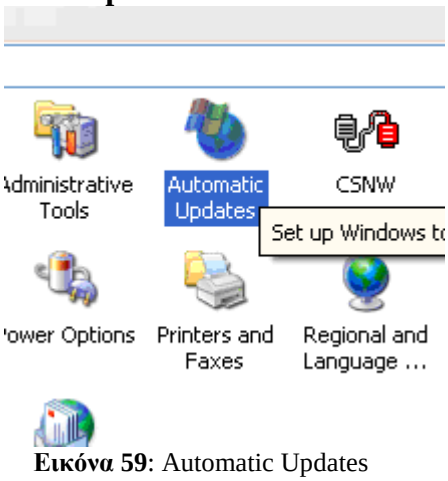
[18] Όπως περιγράφεται αργότερα σε αυτό το τμήμα , οι αυτόματες αναπροσαρμογές μπορούν να διαμορφωθούν για να χρησιμοποιηθούν για ένα τοπικό κεντρικό υπολογιστή αντί των κεντρικών υπολογιστών της Microsoft.

Γενικά, είναι καλύτερα να ρυθμίσετε το σύστημα για να λαβαίνετε τις ενημερώσεις αυτόματα, εκτός αν η χρήση εύρους ζώνης είναι μια ανησυχία. Για παράδειγμα, η λήψη ενημερωμένων εκδόσεων κώδικα θα μπορούσε να επηρεάσει αρνητικά την λειτουργία ενός υπολογιστή που είναι συνδεδεμένος στο Internet για μια αργή σύνδεση. Σε αυτήν την περίπτωση, θα ήταν προτιμητέο για τις αυτόματες αναπροσαρμογές να ρυθμισθούν για να ειδοποιούν το χρήστη ότι νέα patches είναι διαθέσιμα. Ο χρήστης πρέπει έπειτα να κάνει τις ρυθμίσεις για να κατεβάσει το patch την επόμενη φορά όταν δεν απαιτείται ο υπολογιστής για κανονική λειτουργία. Η επιλογή αν θα εγκαταστήσετε τις ενημερώσεις αυτόματα ή ο χρήστης να τις εγκαταστήσει εξαρτάται από την κατάσταση. Εάν ο χρήστης είναι πιθανό να αγνοήσει τις ανακοινώσεις, κατόπιν μπορεί να είναι αποτελεσματικότερο να εγκαταστήσει τις αναπροσαρμογές συμφώνα με το χρονοδιάγραμμα. Εάν το σύστημα είναι σε λειτουργία απρόβλεπτους ημέρες και χρόνους, κατόπιν μπορεί να είναι δύσκολο να τεθεί ένα χρονοδιάγραμμα που δεν θα παρεμποδίσει τη χρήση των συστημάτων. Ένα άλλο θέμα που πρέπει να ληφθεί υπόψη είναι ότι πολλές ενημερωμένες εκδόσεις απαιτούν την επανεκκίνηση του συστήματος που πρέπει να ενημερωθούν πριν από την έναρξη της ισχύος της.
Τα Windows XP προσφέρουν μια επιλογή << **Install updates and shutdown** >> στο πλαίσιο του διαλόγου shutdown, η οποία μπορεί να είναι χρήσιμη στο να υπενθυμίζει στους χρήστες να ξεκινήσει τη διαδικασία εγκατάστασης των ενημερωμένων εκδόσεων.

Συνιστάται ιδιαίτερα ότι η υπηρεσία Automatic Updates πρέπει να είναι σε θέση να διατηρεί το λειτουργικό σύστημα και τις βασικές εφαρμογές της Microsoft (π.χ. Internet Explorer, το Outlook Express) πλήρως ενημερωμένα. Για να είναι δυνατόν οι Αυτόματες ενημερώσεις, ακολουθήστε τα παρακάτω βήματα:

1. Πατήστε **Start** από το μενού και επιλέξτε **Control Panel** [19]

2. Διπλό κλικ στο **Automatic Updates**.

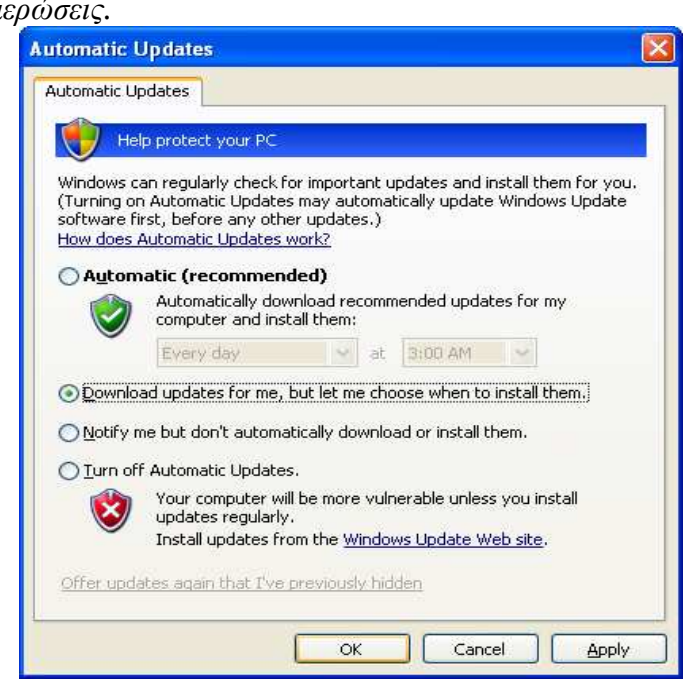


Εικόνα 59: Automatic Updates

[19] Ο πίνακας ελέγχου έχει δυο όψεις :Κλασσική και με Κατηγορία. Η Κλασσική όψη απαριθμεί κάθε αντικείμενο χωριστά και τα παρόμοια στοιχεία ομάδων κατηγοριοποιούνται από κοινού. Οι οδηγίες σε αυτόν τον οδηγό υποθέτουν ότι χρησιμοποιείται η κλασσική όψη. Για να αλλάξετε όψη στη κλασσική όψη, πατήστε την αλλαγή της κλασσικής όψης που βρίσκεται αριστερά στο παράθυρο του πίνακα ελέγχου.

1. Επιλέξτε το κατάλληλο κουμπί (όπως το **Download updates for me, but let me choose when to install them)**[20] και πατήστε **OK**.

Τι είναι το Help protect your pc?
Είναι μια υπηρεσία των Windows XP όπου ανάλογα πως θα το ρυθμίσουμε μπορεί να ελέγχει αν υπάρχουν σημαντικές ενημερώσεις. Αν πατήσουμε Automatic οι ενημερώσεις κατεβαίνουν και εγκαθιστούνται αυτόματα. Η δεύτερη επιλογή είναι να κατεβαίνουν αυτόματα οι ενημερώσεις αλλά θα εγκαθιστούνται χειροκίνητα. Η τρίτη επιλογή είναι να ενημερώνεις αν υπάρχουν αλλά να μην τις κατεβάζει και να μην τις εγκαθιστά .Και η τελευταία επιλογή είναι να απενεργοποιήσεις τις αυτόματες ενημερώσεις αλλά ο υπολογιστής σου δε θα είναι ασφαλείς και ούτε αξιόποιστος χωρίς τις ενημερώσεις.



Εικόνα 60: Help protect your pc

Ορισμένοι οργανισμοί δεν θέλουν τις τελευταίες ενημερωμένες εκδόσεις για την άμεση εφαρμογή τους στα συστήματα Windows. Για παράδειγμα, σε ένα διαχειριστικό περιβάλλον, μπορεί να είναι ανεπιθύμητη οι επείγουσες επιδιορθώσεις(hotfixes)που πρέπει να αναπτυχθούν στα συστήματα παραγωγής μέχρι να έχουν ελεγχθούν από τους διαχειριστές των Windows και τους διαχειριστές της ασφάλειας[21]. Επιπλέον, στα μεγάλα περιβάλλοντα, πολλά συστήματα μπορεί να χρειαστούν να κατεβάσουν το ίδιο hotfix ταυτόχρονα. Αυτό θα μπορούσε να έχει έναν σοβαρό αντίκτυπο στο εύρος ζώνης των δικτύων [22]. Οι οργανισμοί με τέτοιες ανησυχίες συχνά δημιουργούν ένα τοπικό WUS ή WSUS ενημερωμένο διακομιστή

[20] Αυτές οι οδηγίες είναι βασισμένες στην έκδοση των αυτόματων αναπροσαρμογών που κυκλοφόρησαν τον Αύγουστο του 2004. Η προηγούμενη έκδοση πρόσφερε την ίδια λειτουργία, αλλά χρησιμοποίησε διαφορετική διατύπωση.. Στα συστήματα με την παλαιότερη αυτόματη έκδοση αναπροσαρμογών, επιλέξτε το **Keep my computer up to date** στο παράθυρο ελέγχου, μετά διάλεξε το κατάλληλο κουμπί (such as **Notify me before downloading any updates and notify me again before installing them on my computer)** και πατήστε **OK**.

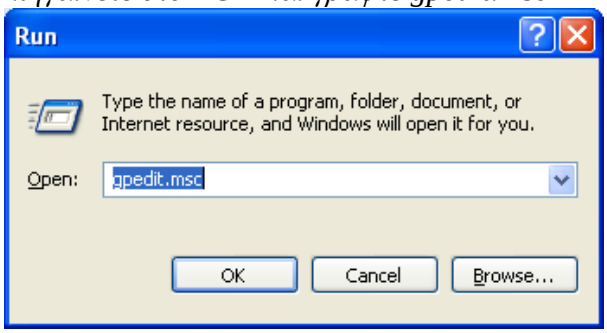
[21] Μερικά διοικούμενα περιβάλλοντα έχουν τις πολιτικές συντήρησης λογισμικού που απαγορεύουν τους χρήστες από την ενημέρωση των συστημάτων από τους ίδιους , πρώτιστα λόγω των πιθανών αρνητικών αποτελεσμάτων της ανάπτυξης των μη δοκιμασμένων αναπροσαρμογών

[22] Μερικές οργανώσεις επεκτείνουν τις αναπροσαρμογές χρησιμοποιώντας μόνο μέσα ανάγνωσης. Αυτό είναι ιδιαίτερα χρήσιμο για τα συστήματα με το χαμηλό εύρος ζώνης δικτύων(π.χ. modems) και τα συστήματα των untrusted δικτύων (έτσι ώστε μπορούν να επιδιορθωθούν πριν τοποθετηθούν στο δίκτυο).

που περιέχει τις εγκεκριμένες αναπροσαρμογές και περιορίζουν τις θέσεις από τις οποίες οι ενημερώσεις που μπορούν να ανακτηθούν μέσω της πολιτικής ομάδας. Η λειτουργία Automatic Updates των Windows XP για τα συστήματα θα πρέπει να ρυθμιστεί με το σημείο του τοπικού διακομιστή ενημέρωσης. Δυστυχώς, αν και WUS και WSUS παρέχουν μια μέθοδο για τις αναπροσαρμογές της Microsoft, δεν μπορεί να χρησιμοποιηθεί για να διανείμει τις ενημερώσεις λογισμικού τρίτων.

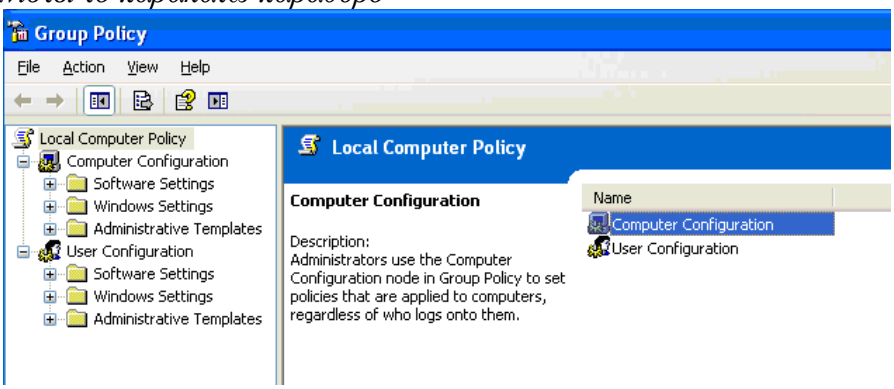
ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΤΟ LOCAL SERVER ΓΙΑ ΤΙΣ ΑΥΤΟΜΑΤΕΣ ΕΝΗΜΕΡΩΣΕΙΣ

Πατήστε START και πηγαίνετε στο RUN και γράψτε gpedit.msc



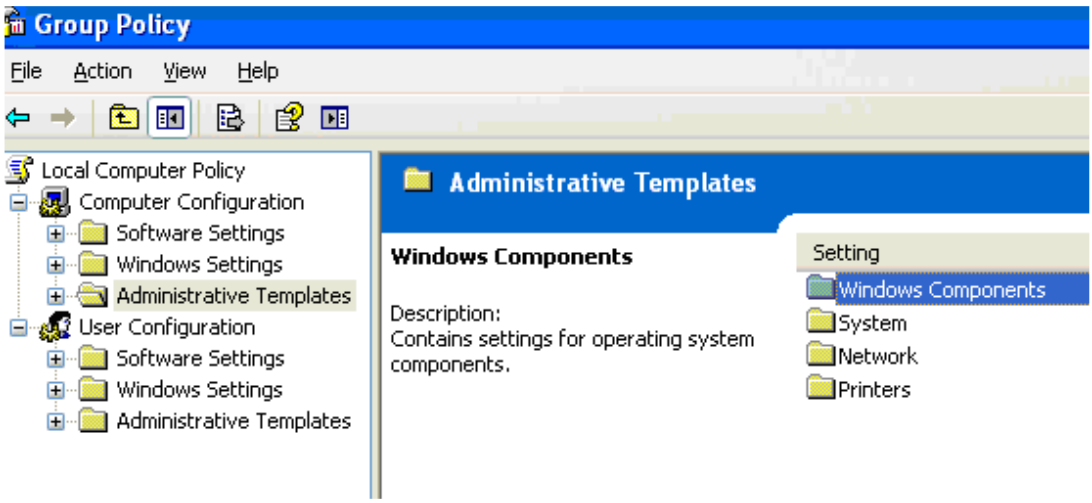
Εικόνα 61: Run

Θα εμφανιστεί το παρακάτω παράθυρο



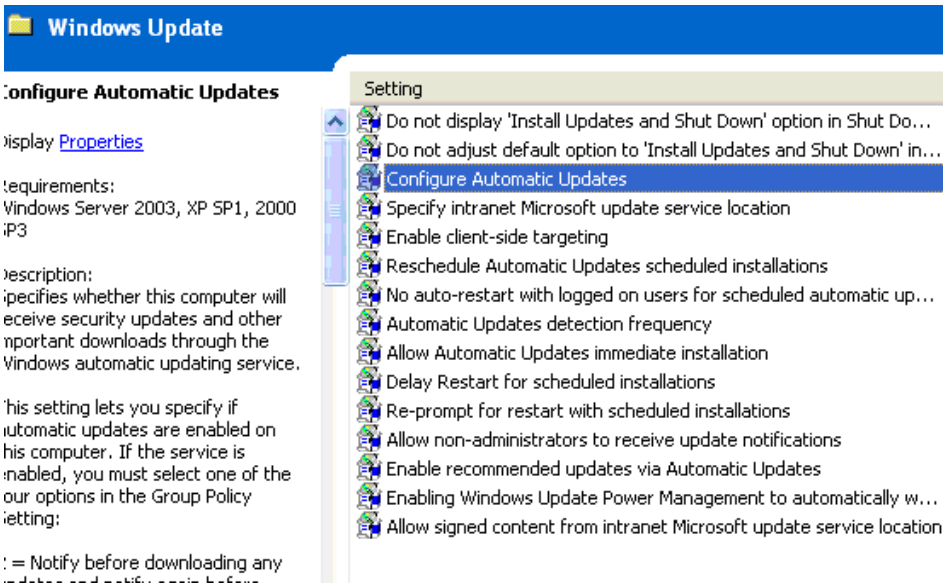
Εικόνα 62: Group Policy

Μπείτε στο Computer Configuration μετά στο Administrate Tools και στο Windows Components



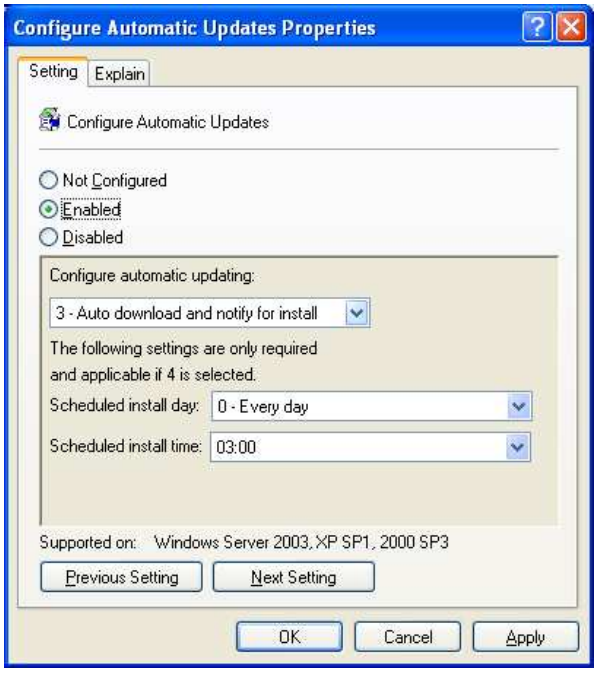
Εικόνα 63: Administrative tools

Μπείτε τώρα στο Windows Update και θα σας εμφανιστεί το παρακάτω παράθυρο. Πατήστε στο τρίτο κατά σειρά.



Εικόνα 64: Windows Update

Πατώντας τη τρίτη επιλογή εμφανίζεται το εξής παράθυρο. Πατήστε Enabled για να το ρυθμίσετε όπως θέλετε.



Εικόνα 65: Configure Automatic Updates Properties

Έχει 4 επιλογές:

- 2 - Notify for download and notify for install (ενημέρωση για τη λήψη και για τη εγκατάσταση)
- 3 - Auto download and notify for install(αυτόματη λήψη και ενημέρωση για τη εγκατάσταση)
- 4 - Auto download and schedule the install(αυτόματη λήψη και προγραμματισμένη η εγκατάσταση)
- 5 - Allow local admin to choose setting(επιτρέπει στο τοπικό διαχειριστή να διαλέξει τη ρύθμιση)

Αν διαλέξεις την επιλογή 4 θα μπορείς να χρησιμοποιείς τη προγραμματισμένη ημέρα εγκατάστασης και τη προγραμματισμένη ώρα εγκαταστάσεις των ενημερώσεων.

2.3.4 Microsoft Update

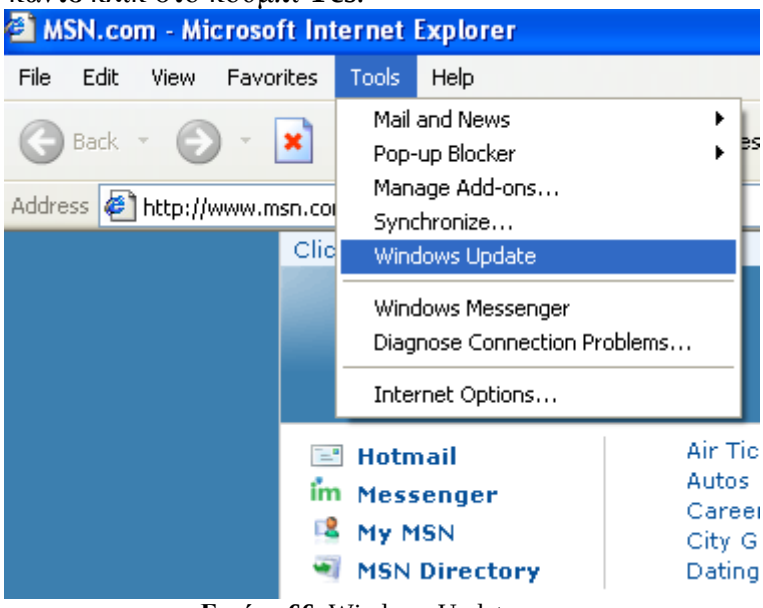
Οι χρήστες με δικαιώματα τοπικού διαχειριστή μπορούν επίσης να ενημερωθούν για τα συστήματά τους με την επίσκεψη τους στο Microsoft Update Web site. [23] Η τοποθεσία Microsoft Update ελέγχει τον υπολογιστή για να καθορίσει τις ενημερώσεις ασφαλείας και τη λειτουργικότητα και αν είναι διαθέσιμες να παράγουν μια λίστα των ενημερωμένων εκδόσεων. Ο χρήστης μπορεί στη συνέχεια να επιλέξει

[23] Η αναπροσαρμογή της Microsoft ήταν γνωστή ως Windows αναπροσαρμογή . Ο ιστοχώρος αναπροσαρμογών της Microsoft βρίσκεται στη σελίδα http://update.microsoft.com/. Αυτή η περιοχή μπορεί να χρησιμοποιηθεί μόνο με τον Internet Explorer Web browser. Οι υπολογιστές με Windows XP που δεν ενημερώνονται πλήρως μπορούν να επιδείξουν στο ιστοχώρο αναπροσαρμογών Windows αντί στο ιστοχώρο αναπροσαρμογών της Microsoft.

τις ενημερωμένες εκδόσεις οι οποίες θα πρέπει να εγκατασταθούν σε αυτό το διάστημα, και πατήστε στο Microsoft Update για την εκτέλεση των εγκαταστάσεων. Για να χρησιμοποιήσετε το Microsoft Update, ακολουθήστε τα παρακάτω βήματα:

1.<<Τρεξτε>> στον Internet Explorer.

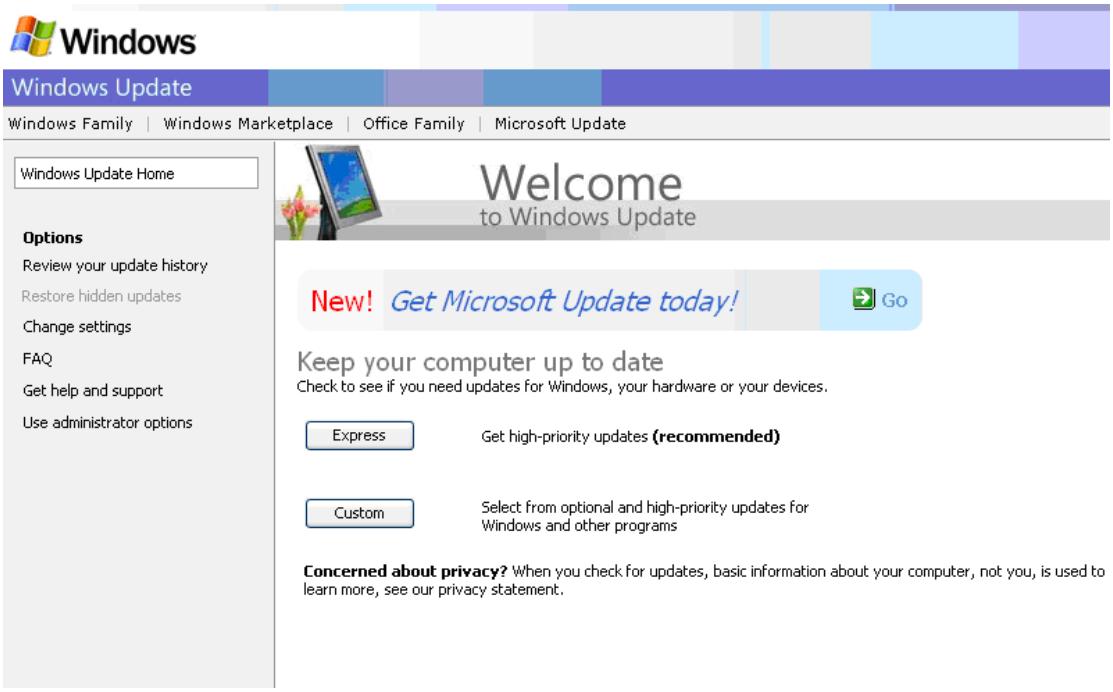
2. Από το μενού πηγαίνετε **Tools,** επιλέξτε **Windows Update** .Εάν εμφανιστεί ένα μήνυμα ζητώντας να εγκαταστήσετε και να εκτελέσετε το Windows Update, κάντε κλικ στο κουμπί **Yes**.



Εικόνα 66: Windows Update

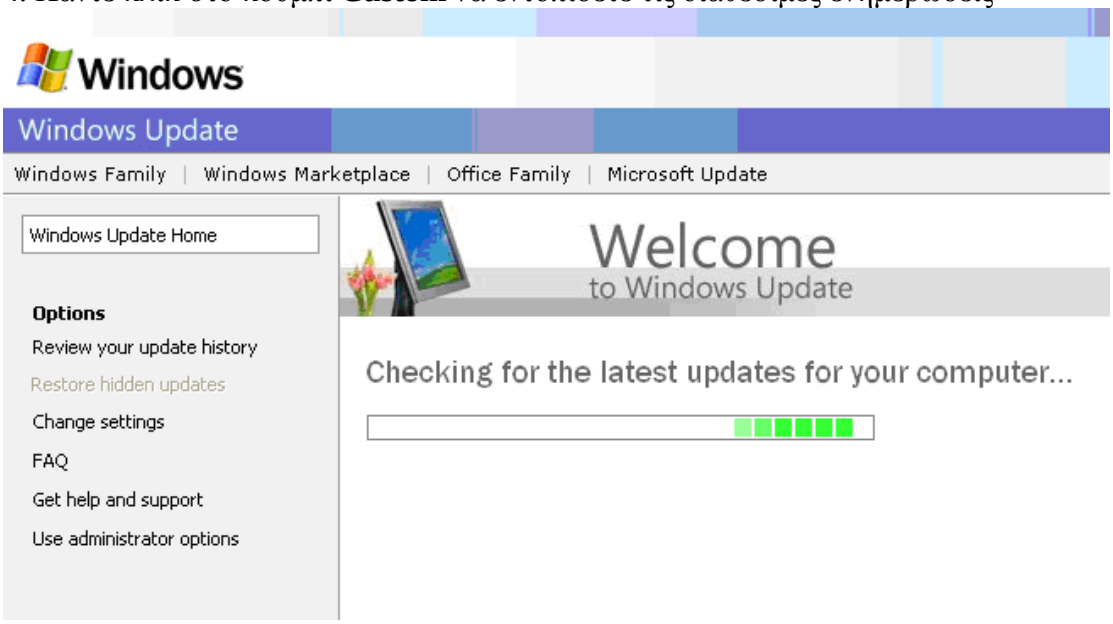
3. Εάν εμφανιστεί ένα μήνυμα λέγοντας ότι μια νέα έκδοση του Windows Update ή Microsoft Update στο λογισμικό είναι διαθέσιμη, κάντε κλικ στο **Install Now** or **Download and Install Now** να εγκατασταθεί η νέα έκδοση [24]Πολλαπλές ενημερώσεις μπορεί να χρειάζονται. Εάν ζητηθεί να το κάνετε, κλείστε το Internet Explorer ή επανεκκινήσετε τον υπολογιστή έτσι ώστε η νέα έκδοση του λογισμικού να είναι σε ισχύ. (Εάν απαιτείται επανεκκίνηση κόντε επανεκκίνηση με τις οδηγίες του πρώτου βήματος και επανεκκινήσετε τον υπολογιστή μόλις ολοκληρωθεί.

[24] Υπάρχουν πολλαπλές εκδόσεις της διεπαφής αυτής. Μια δηλώνει “Βάλε τη αναπροσαρμογή της Microsoft σήμερα!” και περιμένει το χρήστη να πατήσει **ΠΑΜΕ**, κατόπιν ρωτά το χρήστης να πατήσει στο κουμπί **ΞΕΚΙΝΑΜΕ ΤΩΡΑ** , αναθεωρεί μια συμφωνία αδειών, και πατάμε **ΣΥΝΕΧΕΙ**. Αφότου φορτωθεί ένας έλεγχος ActiveX, ο χρήστης πατάει **ΕΓΚΑΤΑΣΤΑΣΗ** για να εγκαταστήσει τη νέα έκδοση της αναπροσαρμογής της Microsoft.



Εικόνα 67: Microsoft Update

4. Κάντε κλικ στο κουμπί **Custom** να εντοπίσετε τις διαθέσιμες ενημερώσεις[25]

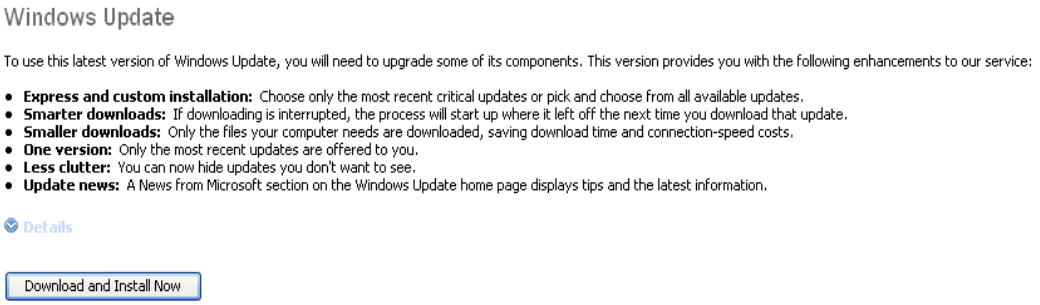


Εικόνα 68: Microsoft Update

5. Το Microsoft Update ελέγχει για ενημερώσεις και απαριθμεί τις διαθέσιμες ενημερώσεις. Ανάλογα με το επίπεδο του Service Pack του υπολογιστή, είτε

[25] Η επιλογή Custom μπορεί να εγκαταστήσει και την υψηλή προτεραιότητα και τις προαιρετικές αναπροσαρμογές και επιτρέπει στο χρήστη για να επιλέξει ποιές ενημερώσεις πρέπει να εγκατασταθούν. Η Express επιλογή ,μπορείς να εγκαταστήσεις μόνο τις αναπροσαρμογές με υψηλή προτεραιότητα και δεν επιτρέπει στο χρήστη για να επιλέξει ποιες αναπροσαρμογές πρέπει να εγκατασταθούν. Η χρησιμοποιώντας τη Express επιλογή μπορείς να αναγκάσεις το σύστημα να μεταφορτώσει και να εγκαταστήσει τα πακέτα υπηρεσιών αυτόματα.

το Service Pack 2 ή 3 ή χωρίς service pack με ενημερώσεις θα πρέπει να εμφανίζεται. Ακολουθήστε τα κατάλληλα βήματα για:

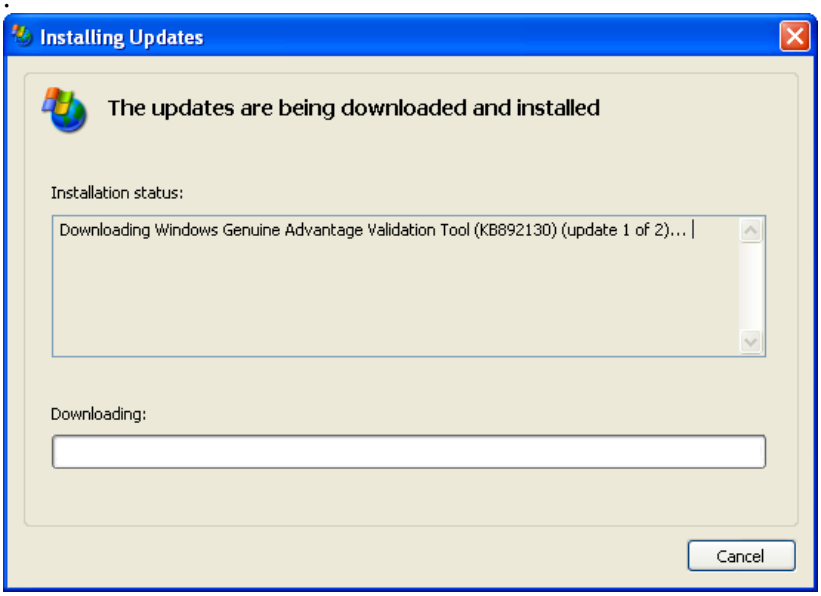


Εικόνα 69 Windows Update

a. Χωρίς service pack,οι ενημερώσεις ομαδοποιούνται με την υψηλότερη προτεραιότητα για ενημερώσεις του λογισμικού, υλικού και προαιρετικές ενημερώσεις .[26]

I. Μελετήστε τη λίστα των διαθέσιμων ενημερώσεων, επιλέξτε τη επιθυμητή (ή αποδεχθείτε την προεπιλεγμένη ρύθμιση), στη συνέχεια, κάντε κλικ **Review and install updates**. Σε ορισμένες περιπτώσεις ένα patch ενδέχεται να πρέπει να εγκατασταθεί από μόνο του? Ως εκ τούτου, ενδέχεται να μην είναι δυνατή η εγκατάσταση όλων των επιθυμητών patches με τη μία.

.

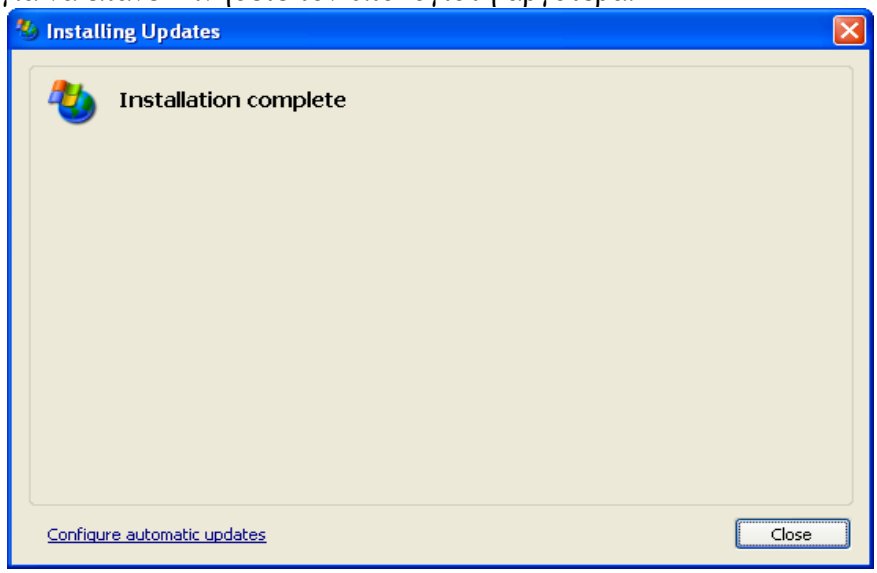


Εικόνα 70: Installing Updates

II. Επιβεβαιώστε ότι οι σωστές ενημερώσεις είναι εισηγμένες, και κάντε κλικ στο κουμπί .**Install Updates** για την εκτέλεση των εγκαταστάσεων. Μελετήστε τις συμφωνίες αδειών εκμετάλλευσης που εμφανίζονται και κάντε κλικ στο κατάλληλο κουμπί για κάθε μια.

[26] Οι αναπροσαρμογές υψηλής προτεραιότητας ορίζονται ως οι κρίσιμες αναπροσαρμογές, hotfixes, πακέτα υπηρεσιών, και ασφάλεια rollups . Οι προαιρετικές αναπροσαρμογές είναι αναπροσαρμογές υλικού και λογισμικού ανεξάρτητες από την ασφάλεια.

III. Η λήψη και η διαδικασία εγκατάσταση θα ξεκινήσει. Ανάλογα με τον αριθμό των ενημερώσεων και το διαθέσιμο εύρος ζώνης δικτύου, μπορεί να χρειαστούν από μερικά λεπτά έως μερικές ώρες για να κατεβάσετε και να εγκαταστήσετε τις ενημερωμένες εκδόσεις. Όταν οι εγκαταστάσεις εγκατασταθούν το Microsoft Update θα πρέπει να υποβάλει έκθεση η οποία θα δείχνει τις ενημερωμένες εκδόσεις που εγκαταστάθηκαν με επιτυχία. Επίσης ο χρήστης θα πρέπει να κάνει επανεκκίνηση, εάν οποιαδήποτε από τις ενημερώσεις απαιτούν επανεκκίνηση για την ολοκλήρωση της εγκατάσταση τους. Κάντε κλικ στο OK για επανεκκίνηση αμέσως ή CANCEL για να επανεκκίνησετε τον υπολογιστή αργότερα.



Εικόνα 71: Installation complete

Εικόνα 72: Installation Results

b. Τα Service Pack 2 ή 3 είναι δυνατόν να εγκατασταθούν μέσω του Microsoft Update, ακολουθώντας τα παρακάτω βήματα:[27]

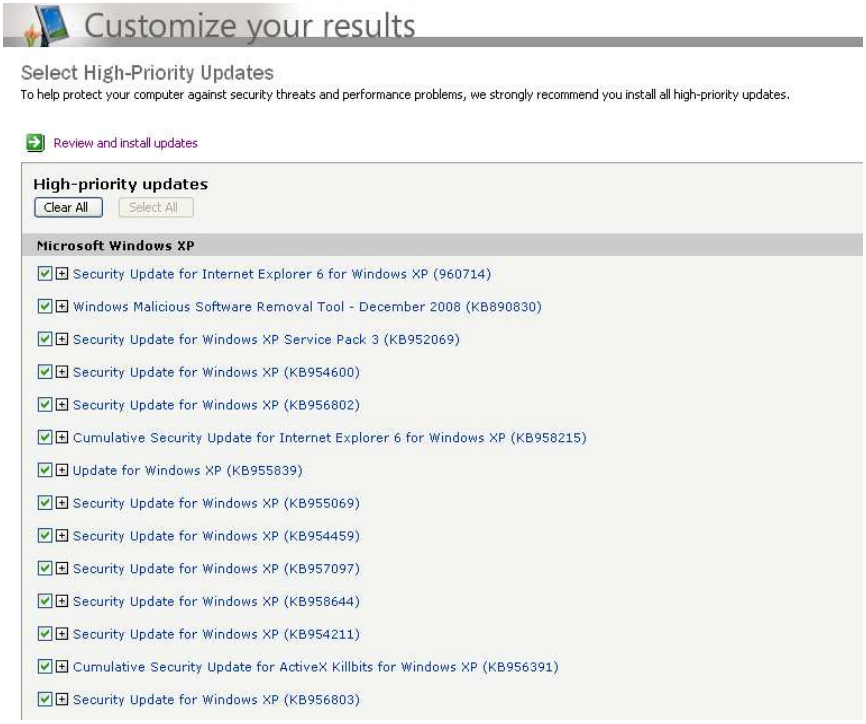
I. Κάντε κλικ στο **Download and Install Now**.

[27]Εάν ένα πακέτο υπηρεσιών εγκαθίσταται από το CD αντί μέσω της αναπροσαρμογής της Microsoft, τα βήματα που εκτελούνται θα διαφέρουν.

II. Επανεξέταση της άδειας χρήσης και κάντε κλικ στο κατάλληλο κουμπί.

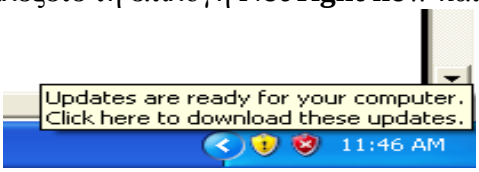
III. Το Service Pack θα έπρεπε να κατεβεί και εγκατασταθεί. Αυτό μπορεί να διαρκέσει μεγάλο χρονικό διάστημα, ανάλογα κυρίως με το μέγεθος του Service Pack καθώς και τον τύπο της σύνδεσης στο Internet και το εύρος ζώνης που είναι διαθέσιμο. Μια εγκατάσταση ή οδηγός εγκατάστασης μπορεί να ωθήσει τον χρήστη σε κάποιο σημείο? Κάντε κλικ στο **Next** για να συνεχίσετε.

IV. Μόλις ολοκληρωθεί η εγκατάσταση, μια περίληψη θα πρέπει να εμφανιστεί στις αναφορές με τις επιτυχείς εγκαταστάσεις. Κάντε κλικ στο κουμπί **Restart Now** για την επανεκκίνηση του υπολογιστή.



Εικόνα 73: Customize your results

V. Μετά τη επανεκκίνηση, εμφανίστηκε στη οθόνη το **Help protect your PC** .Οι αυτόματες ενημερώσεις ρυθμίζονται αργότερα με οδηγίες ,ώστε αυτή τη στιγμή, διαλέξετε τη επιλογή **Not right now** και πατήστε **Next**.



Εικόνα 74: Updates are ready

VI. Το **Security Center** ανοίγει και εμφανίζει την κατάσταση της ασφάλειας των προγραμμάτων. Δεδομένου ότι το λογισμικό αντιμετώπισης ιών και τα άλλα προγράμματα ασφαλείας δεν έχουν ακόμη εγκατασταθεί στον υπολογιστή. Η τρέχουσα κατάσταση είναι άνευ σημασίας. Κλείστε το **Security Center**.

6. Επαναλάβετε όλα αυτά τα βήματα έως ότου δεν είναι άλλες διαθέσιμες αναπροσαρμογές. Ανάλογα με ποιο πακέτο υπηρεσιών ήταν στον υπολογιστή, ο αριθμός πρόσθετων αναπροσαρμογών που πρέπει να εφαρμοστούν, μπορεί να πάρει διάφορους κύκλους ενημέρωσης στον υπολογιστή και της εκ νέου επανεκκίνηση του για να ενημερώσει μια νέα εγκατάσταση Windows XP απολύτως.

Επειδή τα Windows Update απαιτούν από τους τοπικούς διαχειριστές προνόμια και να εκτελούνται χειροκίνητα, η χρήση τους γενικά δεν συνιστάται εντός των επιχειρήσεων, των SSLF και FDCC περιβαλλόντων. Όπως περιγράφεται στο τμήμα 4.3.5, συνιστάται ότι όλες οι ενημερώσεις πρέπει να δοκιμάζονται και να επαληθεύονται πριν από τη συντονισμένη τοποθέτηση, με την οποία η χρήση του Microsoft Update θα μπορούσε να παρακαμφθεί. Το Microsoft Update έχει πρόσθετες δυσκολίες σε περιβάλλοντα επιχειρήσεων, διότι συνήθως δεν είναι ρεαλιστικό να τρέχει οποιαδήποτε εφαρμογή χειροκίνητα σε κάθε θέση εργασίας μέσα στην επιχείρηση καθώς και οι μεμονωμένοι χρήστες δεν μπορούν να έχουν τα απαραίτητα τοπικά διοικητικά δικαιώματα.

2.3.5 Patching in Managed Environments

Η επιχείρηση, SSLF και FDCC τα περιβάλλοντα, ειδικά εκείνα που θεωρούνται διοικητικά περιβάλλοντα, θα πρέπει να έχουν ένα διοικητικό πρόγραμμα patch που θα είναι αρμόδιο για την απόκτηση, το έλεγχο και την επαλήθευση του κάθε patch, τακτοποιώντας έπειτα για τη διανομή συστημάτων σε όλη την οργάνωση. Η έκδοση NIST SP 800-40 2.0, δημιουργεί ένα διοικητικό πρόγραμμα patch(μπαλώματος) και ευπάθειας, που παρέχει σε βάθος συμβουλές σχετικά με τη θέσπιση διαδικασιών ενημέρωσης κώδικα, καθώς και τον έλεγχο και την εφαρμογή των patches. [28]. Για κάθε patch που κυκλοφόρησε η ομάδα διαχείρισης patch θα πρέπει να έρευνα τις συνδεδεμένες ευπάθειες και την προτεραιότητα των patches κατάλληλα. Δεν είναι ασυνήθιστο για διάφορα patches που κυκλοφόρησαν σε σχετικά σύντομο χρονικό διάστημα και χαρακτηριστικά ένα ή δύο των patches είναι σημαντικότερο στην οργάνωση από τα άλλα. Κάθε patch πρέπει να εξεταστεί με τις διαμορφώσεις του συστήματος που είναι αντιπροσωπευτικές των συστημάτων οργάνωσης. Μόλις καθορίσει η ομάδα ότι το patch είναι κατάλληλο για ανάπτυξη, το patch πρέπει να διανεμηθεί μέσω των αυτοματοποιημένων ή χειροκίνητων μέσων για την εγκατάσταση σε όλα τα κατάλληλα συστήματα. (Υπάρχουν διάφορες εφαρμογές τρίτων που διατίθονται για τη διαχείριση και τη διανομή των patches, τα οποία υποστηρίζουν πολλούς τύπους πλατφορμών και προσφέρουν τη λειτουργία που υποστηρίζει τις επιχειρηματικές απαιτήσεις.) Τέλος, η ομάδα πρέπει να ελέγχει τα συστήματα περιοδικά για να επιβεβαιώνει ότι το patch έχει εγκατασταθεί στο κάθε σύστημα και να λαμβάνει μέτρα για να εξασφαλιστεί ότι τα ελλείποντα patches εφαρμόζονται.

[28] Η έκδοση της NIST SP 800-40 2.0 είναι διαθέσιμη στη σελίδα http://csrc.nist.gov/publications/PubsSPs.html

Η Microsoft προσφέρει τη ακόλουθη εντολή-γραμμών για εργαλεία που μπορούν να είναι χρήσιμα στην επέκταση hotfix, ως εξής:[29]

- Το εργαλείο qchain.exe επιτρέπει στα hotfixes που πρέπει εγκατασταθούν συγχρόνως, αντί για τη εγκατάστασης ενός hotfix, εκ νέου επανεκκίνηση, εγκαθιστώντας έπειτα ένα άλλο hotfix.[30]
- Το εργαλείο qfecheck.exe μπορεί να χρησιμοποιηθεί στη διαδρομή και για να ελέγξει τα εγκατεστημένα hotfixes.[31]

2.4 Identifying Security Issues

Η υποδοχή ασφάλειας εξαρτάται κατά ένα μεγάλο μέρος από την παραμονή ενημερωμένων patches ασφάλειας καθώς επίσης και τον εντοπισμό και άλλων αδυναμιών ασφάλειας. Η συσκευή ανάλυσης ασφάλειας βασικών γραμμών της Microsoft (MBSA) είναι ένα εργαλείο που μπορεί να σαρώσει τον τοπικό υπολογιστή και απομακρυσμένους υπολογιστές για να εντοπίσει θέματα ασφαλείας για το MBSA.[32] MBSA πρέπει να έχει δικαιώματα τοπικού διαχειριστή σε επίπεδο πρόσβασης σε κάθε υπολογιστή που ανιχνεύει. MBSA προσφέρει και τις γραφικές διεπαφές ενδιάμεσων χρηστών (GUI) και εντολή-γραμμών. MBSA μπορεί να προσδιορίσει ποιες αναπροσαρμογές λείπουν από το λειτουργικό σύστημα και τις κοινές εφαρμογές της Microsoft (π.χ., Internet Explorer, Media Player, Internet Information Services [IIS], Exchange Server, Δομημένη Γλώσσα Ερωτήσεων [SQL] Server) σε κάθε system[33]. Για το λειτουργικό σύστημα και για μερικές εφαρμογές(π.χ., Internet Explorer, IIS, SQL Server, Office), μπορεί επίσης να προσδιορίσει και άλλα θέματα ασφαλείας όπως είναι ανασφαλείς διαμορφώσεις και ρυθμίσεις. MBSA προσδιορίζει μόνο τα προβλήματα; Δεν έχει καμία δυνατότητα να αλλάξετε τις ρυθμίσεις ή να κάνετε λήψη και να εγκαταστήσετε τις αναπροσαρμογές στα συστήματα. Οι μέθοδοι που εξετάζονται στο σημείο 4.3 θα πρέπει να χρησιμοποιηθούν για να "κατεβάσετε" και να εφαρμόσετε τις ενημερωμένες εκδόσεις κώδικα.

Τα εργαλεία διαχείρισης επιχειρηματικής διαμόρφωσης επίσης είναι διαθέσιμα που μπορούν να χρησιμοποιηθούν για να αξιολογήσουν την ασφάλεια των συστημάτων Windows XP. Αυτά τα εργαλεία έχουν ποικίλες ικανότητες, όπως η σύγκριση των τοποθετήσεων ασφάλειας με τις τοποθετήσεις βασικών γραμμών και ο προσδιορισμός των ελλειπόντων patches. Μερικά εργαλεία μπορούν επίσης να διορθώσουν τα προβλήματα που βρίσκουν με την αλλαγή των τοποθετήσεων, την εγκατάσταση των

---

[29] Ο *οδηγός για την εγκατάσταση και την ανάπτυξη των αναπροσαρμογών για το δεύτερο πακέτο υπηρεσιών WINDOWS XP της Microsoft* είναι διαθέσιμος στη σελίδα http://technet.microsoft.com/en-us/library/bb457071.aspx.

[30] Για περισσότερες πληροφορίες, δείτε στο άρθρο της MSKB 296861, για το *πώς να εγκαταστήσει τις πολλαπλάσιες αναπροσαρμογές των WINDOWS ή hotfixes με μόνο επανεκκίνηση*, βρίσκεται στη σελίδα http://support.microsoft.com/?id=296861.

[31] Για περισσότερες πληροφορίες, δείτε στο άρθρο της MSKB 282784, *Qfecheck.exe ελέγχει τη εγκατάσταση των Windows 2000 and Windows XP hotfixes*, βρίσκεται στη σελίδα http://support.microsoft.com/?id=282784.

[32] MBSA είναι διαθέσιμο για κατέβασμα στη σελίδα http://technet.microsoft.com/en-us/security/cc184924.aspx.

[33] MBSA δεν μπορεί να προσδιορίσει όλους τους τύπους ζητημάτων ασφάλειας. Η Microsoft καταβάλει εξειδικευμένες χρησιμότητες που ονομάζονται Enterprise Scan Tools(εργαλεία επιχειρηματικής ανίχνευσης) για ζητήματα ασφάλειας που η MBSA δε μπορεί να ανιχνεύσει, όπως patches για προϊόντα της Microsoft που η MBSA δε υποστηρίζει . Για περισσότερες πληροφορίες σχετικά με τα Enterprise Scan Tools είναι διαθέσιμες από το άρθρο της MSKB 894193, *Πώς να βάλω και να χρησιμοποιώ the Enterprise Scan Tool*, το οποίο βρίσκεται στη σελίδα http://support.microsoft.com/?id=894193.

patches και την εκτέλεση άλλων ενεργειών. Τα εργαλεία μπορούν να παρέχουν μια ανεξάρτητη επαλήθευση του, ότι έλεγχοι ασφαλείας εφαρμόζονται σύμφωνα προορισμό τους και μπορεί να τεκμηριώσουν την επαλήθευση για τη χρήση τους στην επίδειξη συμμόρφωσης με τους νόμους, τους κανονισμούς και άλλες απαιτήσεις ασφάλειας. NIST έχει ηγηθεί στην ανάπτυξη του πρωτοκόλλου αυτοματοποίησης περιεχομένου ασφάλειας (SCAP), το οποίο είναι ένα σύνολο προδιαγραφών για την έκφραση των πληροφοριών ασφάλειας στα τυποποιημένα εργαλεία διαχείρισης επιχειρηματικών τρόπων [34] . Επιχειρήσεις διαχείρισης εργαλεία που υποστηρίζουν SCAP μπορούν να χρησιμοποιήσουν τις βασικές γραμμές ασφάλειας που γίνονται δημόσια - διαθέσιμες από τις οργανώσεις όπως NIST και μπορούν επίσης να παραγάγουν τυποποιημένα έντυπα που μπορούν να χρησιμοποιηθούν από άλλα εργαλεία.

Τα ατομικά συστήματα μπορούν επίσης να παρακολουθούν τη δική τους κατάσταση ασφάλειας και τους χρήστες των πιθανών προβλημάτων τους. Τα Windows XP προσφέρουν το κέντρο ασφάλειας Windows, το οποίο είναι μια υπηρεσία που μπορεί να ρυθμιστεί ώστε να παρακολουθεί την κατάσταση του τείχους του συστήματος (είτε το Windows Firewall ή ένα τείχος προστασίας) και το λογισμικό αντιμετώπισης ιών, καθώς και τις ρυθμίσεις για τις Αυτόματες ενημερώσεις[35].Το Windows Security Center μπορεί να δημιουργήσει ειδοποιήσεις, εάν το τείχος προστασίας, το λογισμικό αντιμετώπισης ιών, ή Αυτόματες ενημερώσεις δεν είναι ενεργοποιημένες , επίσης εάν ορισμένες σημαντικές ρυθμίσεις είναι μη ασφαλείς, όπως η μη ρύθμιση του λογισμικού ιών να εκτελεί τη ανίχνευση σε πραγματικό χρόνο και να μη τοποθετούνται οι αυτόματες ενημερώσεις και να εγκαταστήσει τις αναπροσαρμογές αυτόματα. Το Windows Security Center μπορεί να ελέγξει διάφορα είδη τοίχοι προστασίας και λογισμικό αντιμετώπισης ιών. Το Windows Security Center είναι πιο χρήσιμο σε περιβάλλοντα SOHO, ώστε οι χρήστες να μπορούν να παρακολουθούν την κατάσταση της ασφάλειας των συστημάτων τους. Σε ένα επιχειρηματικό περιβάλλον, τα συστήματα θα μπορούσαν να ενημερώνονται με άλλες μεθόδους αντί από τις Αυτόματες ενημερώσεις και το καθεστώς των συστημάτων firewalls και antivirus λογισμικών θα μπορούσαν να παρακολουθούνται από τα κεντρικά.

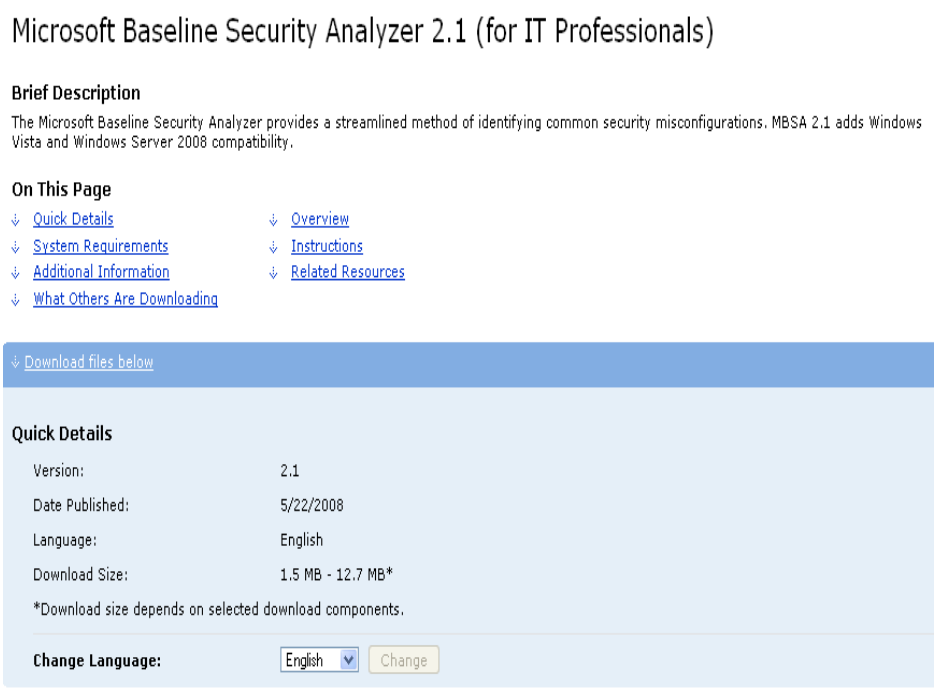
Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) είναι ένα εύχρηστο εργαλείο σχεδιασμένο για να βοηθάει τις μικρές και μεσαίες επιχειρήσεις που καθορίζουν την κατάσταση ασφάλειά τους, σύμφωνα με τις συστάσεις ασφάλειας της Microsoft προσφέρει συγκεκριμένες οδηγίες αποκατάστασης. Βελτιώνει τη διαδικασία διαχείρισης ασφάλειας, χρησιμοποιώντας το MBSA για τον εντοπισμό κοινών λανθασμένων ρυθμίσεων ασφάλειας και ενημερωμένων εκδόσεων ασφαλείας που λείπουν από τα συστήματα του υπολογιστή.

Πηγαίνετε στη σελίδα http://technet.microsoft.com/el-gr/security/cc184923(en-us).aspx και κατεβάστε το

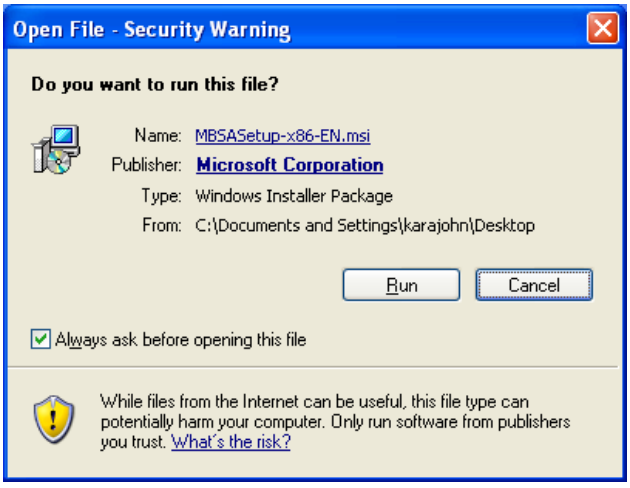
[34] Για περισσότερες πληροφορίες σχετικά με SCAP είναι διαθέσιμες στη σελίδα http://scap.nist.gov/.

[35] Για περισσότερες πληροφορίες σχετικά με το κέντρο ασφάλειας των Windows, δείτε το *Manage Your Computer's Security Settings in One Place*, που είναι διαθέσιμο στη σελίδα http://www.microsoft.com/windowsxp/using/security/internet/sp2_wscintro.mspx.



Εικόνα 75: Microsoft Baseline Security Analyzer

Μόλις τελειώσει η λήψη , εκτελέστε το πρόγραμμα

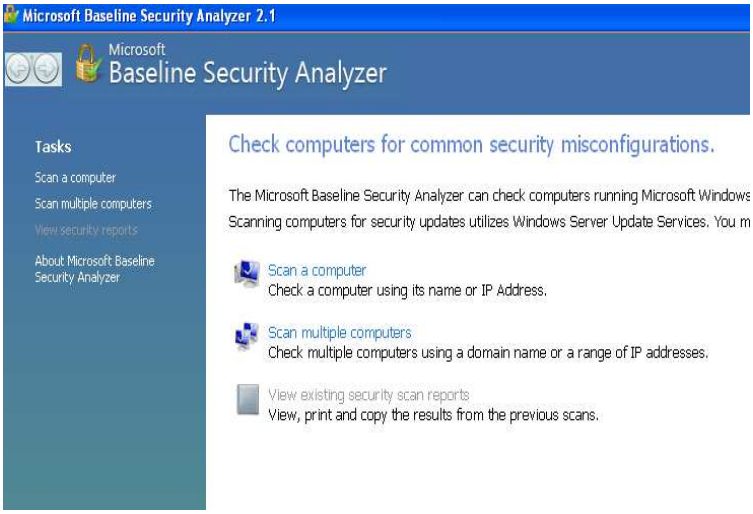


Εικόνα 76: Open File

Μόλις τελειώσει η εγκατάσταση του προγράμματος

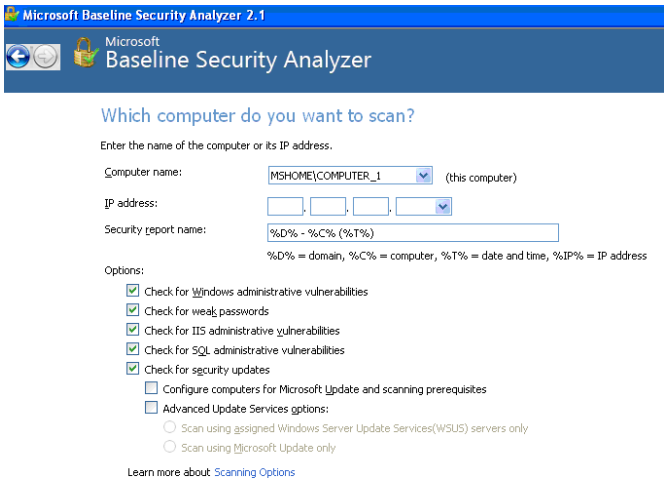
Εικόνα 77: MBSA Setup

Θα σας εμφανιστεί στη επιφάνεια εργασίας μια συντόμευση του προγράμματος. Πατήστε διπλό κλικ και θα σας εμφανιστεί το παρακάτω παράθυρο και πατήστε SCAN A COMPUTER



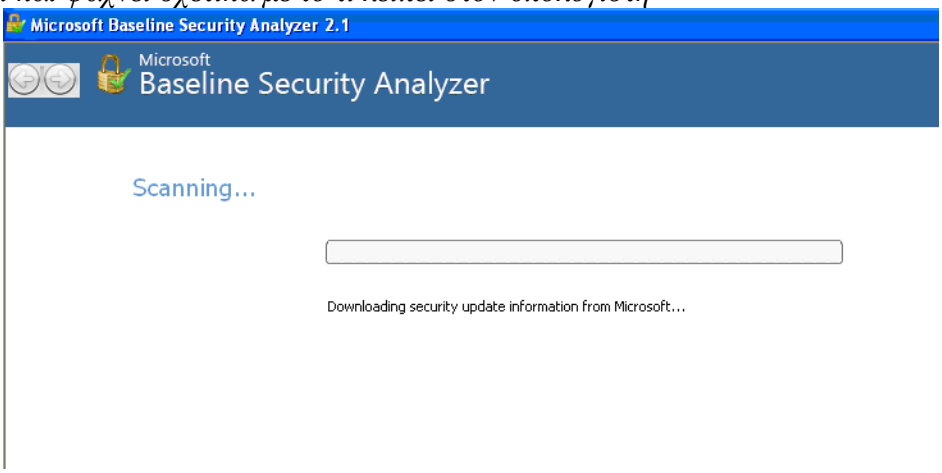
Εικόνα 78: Baseline Security Analyzer

Μετά εμφανίζεται το εξής παράθυρο. Πατήστε μόνο start τίποτα άλλο.



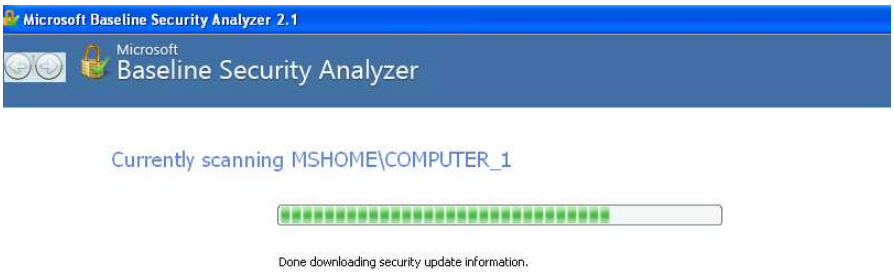
Εικόνα 79: Baseline Security Analyzer

Αρχίζει και ψάχνει σχετικά με το τι λείπει στον υπολογιστή



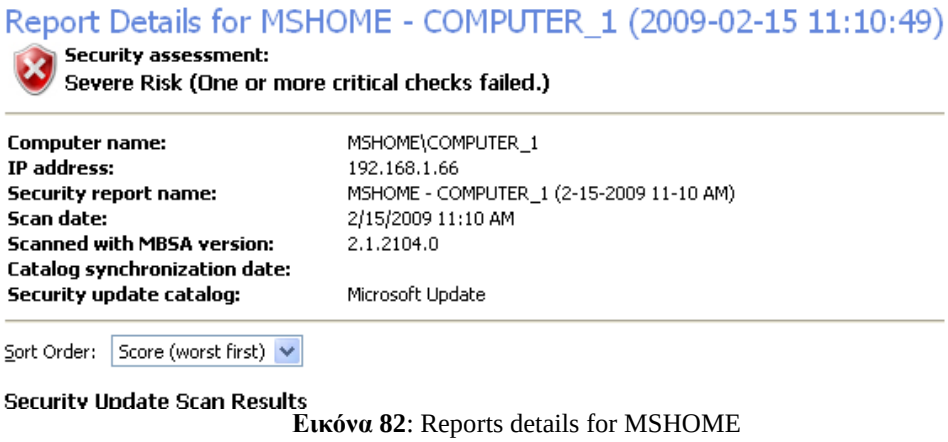
Εικόνα 80: Baseline Security Analyzer

Συνεχίζει



Εικόνα 81: Baseline Security Analyzer

Όταν τελειώσει η διαδικασίας ανίχνευσης εμφανίζεται το εξής παράθυρο με ακριβώς τι λείπει από τον υπολογιστή.



Εικόνα 82: Reports details for MSHOME

Score	Issue	Result
	Windows Security Updates	24 security updates are missing. 6 service packs or update rollups are missing. What was scanned Result details How to correct this
	Office Security Updates	1 service packs or update rollups are missing. What was scanned Result details How to correct this
	SQL Server Security Updates	No security updates are missing. What was scanned Result details

Windows Scan Results

Administrative Vulnerabilities

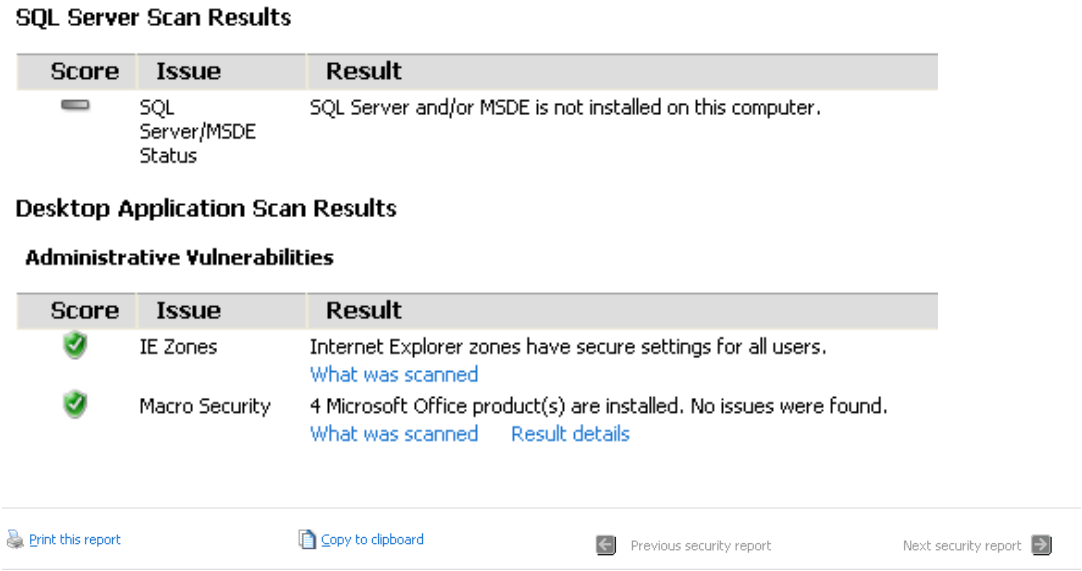
Score	Issue	Result
	Automatic Updates	The Automatic Updates feature is disabled on this computer. What was scanned How to correct this
	Incomplete Updates	No incomplete software update installations were found. What was scanned
	Windows Firewall	Windows Firewall is enabled and has exceptions configured. 2 of 3 network connections What was scanned Result details How to correct this
	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details
	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
	Guest Account	The Guest account is disabled on this computer. What was scanned
	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details
	Autologon	This check was skipped because the computer is not joined to a domain. What was scanned
	Password Expiration	This check was skipped because the computer is not joined to a domain. What was scanned

Additional System Information

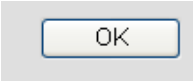
Score	Issue	Result
	Auditing	This check was skipped because the computer is not joined to a domain. What was scanned How to correct this
	Services	Some potentially unnecessary services are installed. What was scanned Result details How to correct this
	Shares	5 share(s) are present on your computer. What was scanned Result details How to correct this
	Windows Version	Computer is running Microsoft Windows XP. What was scanned

Internet Information Services (IIS) Scan Results

Score	Issue	Result
	IIS Status	IIS is not running on this computer.



Εικόνα 83: Αναφορά



2.5 Summary of Recommendations

(Τελικές Υποδείξεις)

- Χρησιμοποιήστε τις συστάσεις που παρουσιάζονται σε αυτό τον οδηγό μόνο για τα νέα Windows XP συστήματα, τα συστήματα δεν αναβαθμίζονται από προηγούμενες εκδόσεις των Windows. Για τις αναβαθμίσεις των συστημάτων, ορισμένες από τις συμβουλές σε αυτό τον οδηγό μπορεί να είναι ακατάλληλες και μπορεί να προκαλέσουν προβλήματα.

- Να έχετε καλή διαχείριση των πολιτικών που διέπουν τις τροποποιήσεις που έγιναν στα λειτουργικά συστήματα και τις εφαρμογές, όπως η εφαρμογή και η τροποποίηση των ρυθμίσεων των patches.

- Μέχρις ότου ένα νέο σύστημα έχει εγκατασταθεί πλήρως και patched, είτε να το κρατήσετε αποσυνδεδεμένο από όλα τα δίκτυα, ή να το συνδέσετε σε ένα απομονωμένο και ισχυρά προστατευμένο δίκτυο.

- Χρησιμοποιήστε NTFS για κάθε χώρισμα του σκληρού σας δίσκου εκτός αν υπάρχει μια ιδιαίτερη ανάγκη να χρησιμοποιηθεί ένας άλλος τύπος filesystem.

- Θέστε εκτός λειτουργίας όλων τους πελάτες, τις υπηρεσίες, και τα πρωτόκολλα δικτύων που δεν απαιτούνται.

- Αντιστοιχίστε ισχυρό κωδικό πρόσβασης για το ενσωματωμένο λογαριασμό διαχειριστή και για το λογαριασμό χρήστη που δημιουργήθηκε κατά την εγκατάσταση.

- Κρατήστε τα συστήματα μέχρι τα τρέχοντα επίπεδα patches για να αποβάλετε τις γνωστές ευπάθειες και αδυναμίες.

- Χρησιμοποιήστε το MBSA ή άλλες παρόμοιες χρησιμότητες κοινής ωφέλειας σε τακτική βάση για την αναγνώριση καθεστώτος σε θέματα patch.

\

Κεφάλαιο 3

3. Additional Windows XP Configuration Recommendations

Στο προηγούμενο τμήμα αυτού του οδηγού συζητήθηκαν ρυθμίσεις που εφαρμόζονται από πρότυπα του NIST και του GPOs. Το τμήμα αυτό ασχολείται με τη πρόσθετη ασφάλεια που σχετίζεται με τις συστάσεις για τα Windows XP που όμως δεν περιλαμβάνονται στον κατάλογο προτύπων και των GPOs. Οι συστάσεις αυτές θα πρέπει είτε να ρυθμιστεί χειροκίνητα ή εφαρμοστούν με τη βοήθεια των πρόσθετων .inf ή .adm αρχείων που δεν παρέχονται από το NIST. Οι συστάσεις σχετίζονται σε θέματα ασφάλειας του filesystem, σε λογαριασμούς χρηστών και ομάδων, σε έλεγχο, σε πολιτικές περιορισμού λογισμικού, σε δίκτυα, Windows Firewall, και IPsec.

Είναι σημαντικό να εξεταστεί η έννοια της ασφάλειας για ένα σταθμό εργασίας των Windows XP, όπως την πορεία των εργασιών. Οι συστάσεις που παρουσιάζονται στο παρόν τμήμα και τα προηγούμενα τμήματα δεν συνεπάγεται στην πλήρη σειρά ασφάλειας και στις ανησυχίες τους για όλη τη διάρκεια του κύκλου ζωής ενός σταθμού εργασίας των Windows XP. Οι διαχειριστές του συστήματος και οι τελικοί χρήστες θα πρέπει να εξετάσουν την έννοια ότι κάθε απόφαση τους σχετικά με ένα σταθμό εργασίας θα μπορούσε να είναι για την ασφάλειά του.

3.1 Filesystem Security

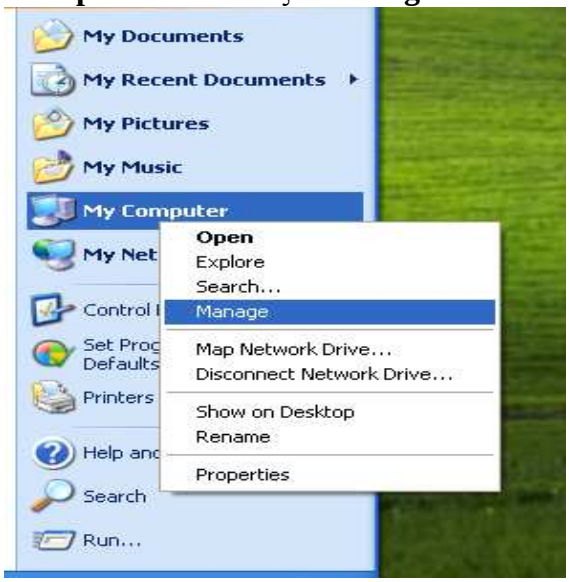
Filesystem ασφάλεια είναι ένα πολύ σημαντικό συστατικό της υποδοχής της ασφάλειας. Το τμήμα αυτό περιγράφει τα διαθέσιμα αρχεία στα Windows XP, το NTFS, File Allocation Table 16 (FAT16), και FAT32 και εξηγεί γιατί το NTFS θα πρέπει να χρησιμοποιείται. Το τμήμα Folder Options του Control Panel περιέχει αρκετές ρυθμίσεις που σχετίζονται με την ασφάλεια αρχείων, όπως τον προσδιορισμό των οποίων η εφαρμογή θα πρέπει να τρέξει ένα αρχείο με βάση την επέκταση αρχείου; Τμήμα αυτό ασχολείται με αυτές τις ρυθμίσεις και συνιστά τον τρόπο με τον οποίο θα πρέπει να καθοριστούν. Οι πληροφορίες αυτές μπορεί να είναι ιδιαίτερα χρήσιμες στην πρόληψη των malware που προκαλούνται από το κακόβουλο λογισμικό λειτουργίας αρχείων με επεκτάσεις αρχείων ασυνήθιστες. Επιπλέον, από προεπιλογή, τα Windows XP συστήματα έχουν ρυθμίσεις μητρώου που καταστέλλουν την απεικόνιση ορισμένων επεκτάσεων αρχείων. Η ενότητα αυτή εξηγεί πώς να βρείτε και να διαγράψετε τις ρυθμίσεις μητρώου, έτσι ώστε όλα τα ονόματα αρχείων θα εμφανίζονται με τον ίδιο τρόπο, ανεξάρτητα από την επέκταση αρχείου. Ένα άλλο θέμα που απευθύνεται στο τμήμα αυτό έχει την υποστήριξη της εμπιστευτικότητας και της ακεραιότητας των δεδομένων μέσα από το Σύστημα κρυπτογράφησης αρχείων (EFS).

3.1.1 NTFS

Από την άποψη ασφάλειας, το NTFS filesystem[36] είναι πολύ καλύτερο από τις άλλες επιλογές των XP αρχείων όπως το FAT16 και FAT32[37]. Ούτε το FAT16 ούτε το FAT32 δεν παρέχουν δυνατότητες για την καθιέρωση ελέγχου πρόσβασης για την κρυπτογράφηση αρχείων ή φακέλων. Τα Windows XP χρησιμοποιούν το NTFS με έκδοση 3.1. Είναι πολύ παρόμοια με την έκδοση 3.0, το οποίο χρησιμοποιείται από τα Windows 2000. Το πιο αξιοσημείωτο νέο χαρακτηριστικό στην έκδοση 3.1 είναι οι ποσοστώσεις στο δίσκο και το file encryption. Το NTFS [38] μπορεί επίσης να παρέχει υψηλής κοκκώδους ελέγχου πρόσβασης για τα αρχεία, φακέλους, καθώς και μετοχών, καθώς και άλλους πόρους για το σύστημα.

Για να βεβαιωθείτε ότι όλα τα τμήματα δίσκου είναι διαμορφωμένα με σύστημα αρχείων NTFS, είτε χρησιμοποιήστε το MBSA (που περιγράφεται στο τμήμα 2.4) ή εκτελέστε τα ακόλουθα βήματα:

1. Δεξί κλικ **My Computer** και επιλέξτε **Manage**.



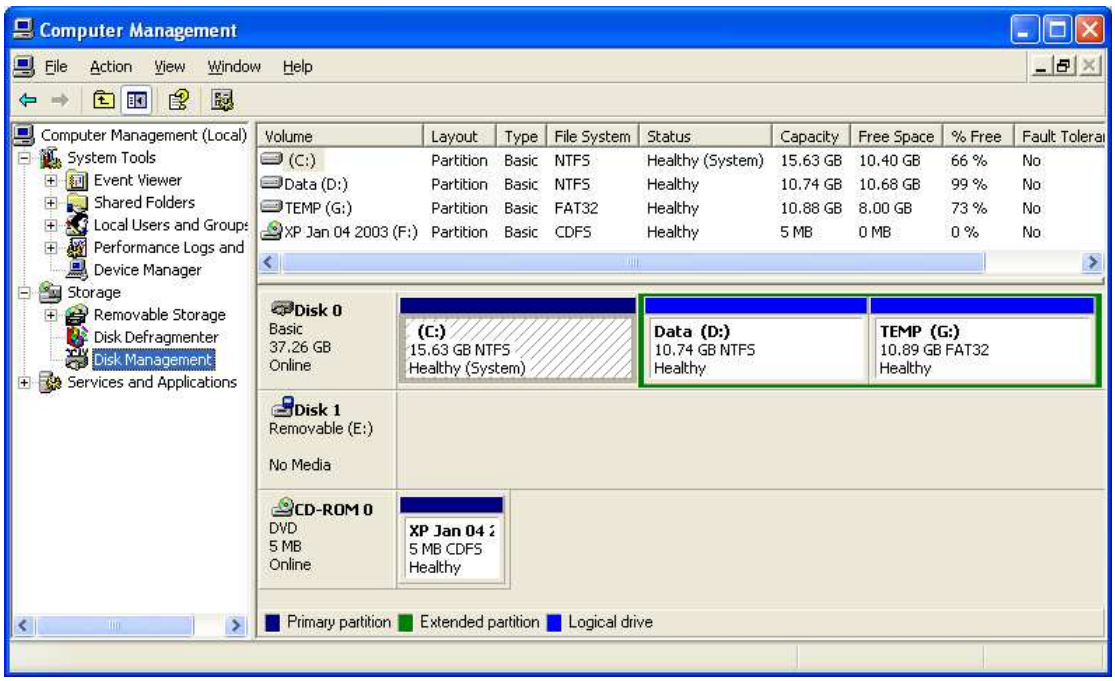
Εικόνα 84: Manage

2. Επιλέξτε το εργαλείο **Disk Management** που βρίσκεται κάτω από το **Storage** να επαληθεύσει ότι το nonremovable που χρησιμοποιείται στις κατατμήσεις NTFS. Για παράδειγμα, στη εικόνα 85 , οι C: και D: χρησιμοποιούν NTFS, και ο G: χρησιμοποιεί FAT32

[36] Για περισσότερες πληροφορίες σχετικά με τα NTFS αρχεία είναι διαθέσιμα από τη Microsoft στο άρθρο *How NTFS Works*, όπου βρίσκετε http://technet.microsoft.com/en-us/library/cc781134.aspx

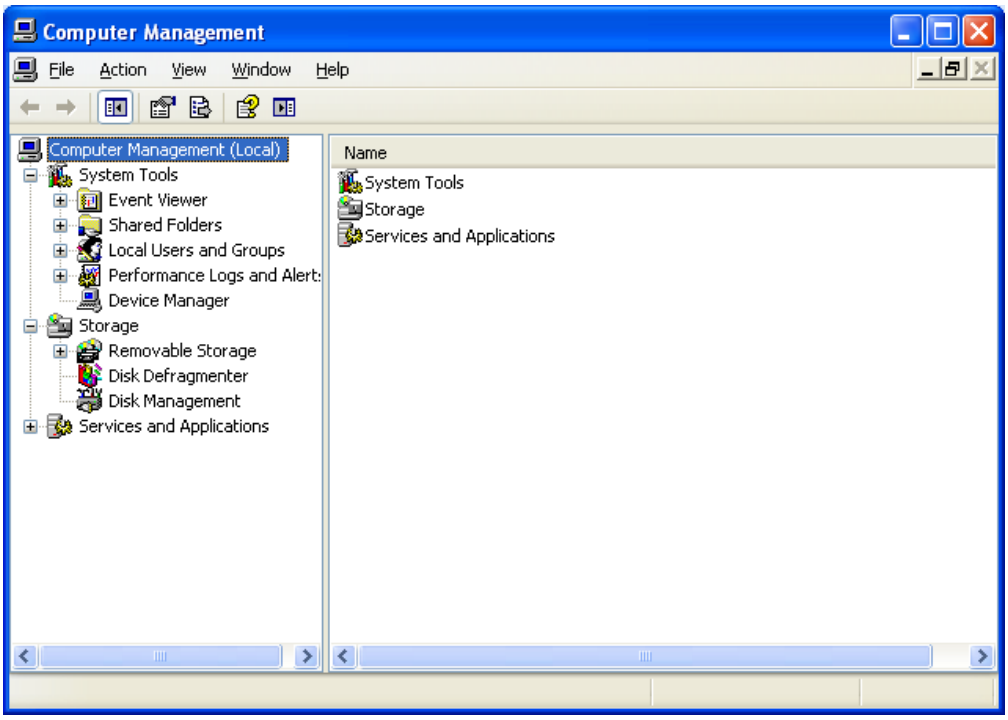
[37] Για σύγκριση των filesystems, δείτε το άρθρο του Charlie Russel's που ονομάζεται *NTFS vs. FAT: Which Is Right for You?*, διαθέσιμο στο http://www.microsoft.com/windowsxp/using/setup/expert/russel_october01.mspx.

[38] Για περισσότερες πληροφορίες σχετικά με τη έκδοση 3.1 του NTFS, δείτε MSKB άρθρο 310749, *New Capabilities and Features of the NTFS 3.1 File System*, διαθέσιμο στο http://support.microsoft.com/?id=310749.



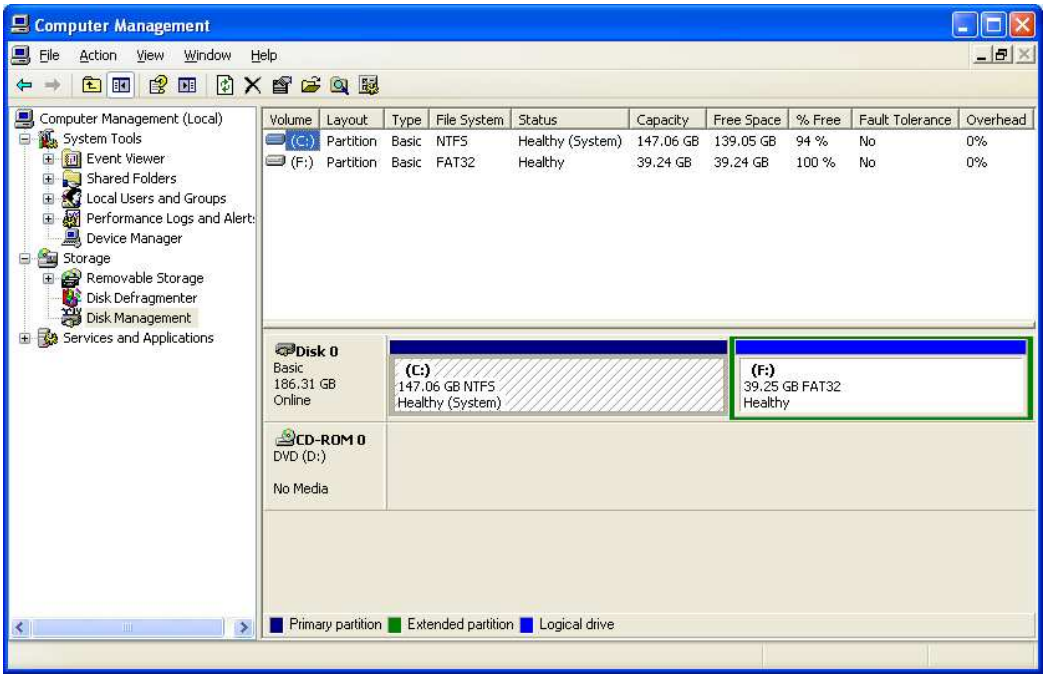
Εικόνα 85: Computer Management

Καθώς βρίσκεστε στο Computer Management πηγαίνετε στη καρτέλα Storage και επιλέξτε Disk Management



Εικόνα 86: Storage

Θα σας εμφανιστεί το παρακάτω παράθυρο όπου θα σας δείχνει τους σκληρούς σας δίσκους με τα χαρακτηριστικά τους(μέγεθος, ελεύθερος χώρος, το είδος του File system κτλ). Στη περίπτωση μας έχουμε 2 σκληρούς δίσκους, ο ένας(ο C δίσκος) μας έχει NTFS File system και ο άλλος(ο D δίσκος) FAT32

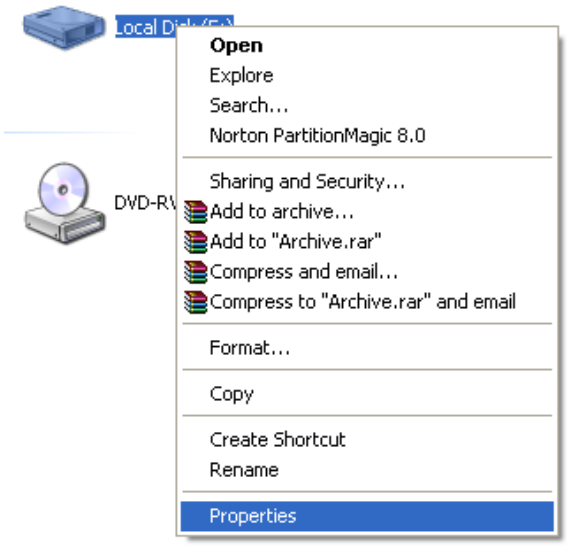


Εικόνα 87: Disk management

Στα περιβάλλοντα SSLF και FDCC, το NIST συνιστά ένθερμα για τα υφιστάμενα συστήματα που βασίζονται σε διαμερίσματα FAT ότι θα πρέπει να ανακατασκευαστούν με NTFS, δεν μετατρέπονται από FAT σε NTFS, επειδή FAT σε μετατροπή NTFS δεν καθορίζονται τα δικαιώματα NTFS στις ίδιες προκαθορισμένες τιμές όπως ανοικοδόμηση ενός συστήματος με το NTFS. Σε άλλα περιβάλλοντα, είναι προτιμητέο να ξαναφτιάξουν τα συστήματα με NTFS, αλλά επίσης θεωρείται αποδεκτό η εκτέλεση ενός FAT σε μετατροπή NTFS. Εκτελέστε τα ακόλουθα βήματα για τη μετατροπή διαμερίσματος FAT σε NTFS:

1. Κάνουμε backup στο σύστημα μας.

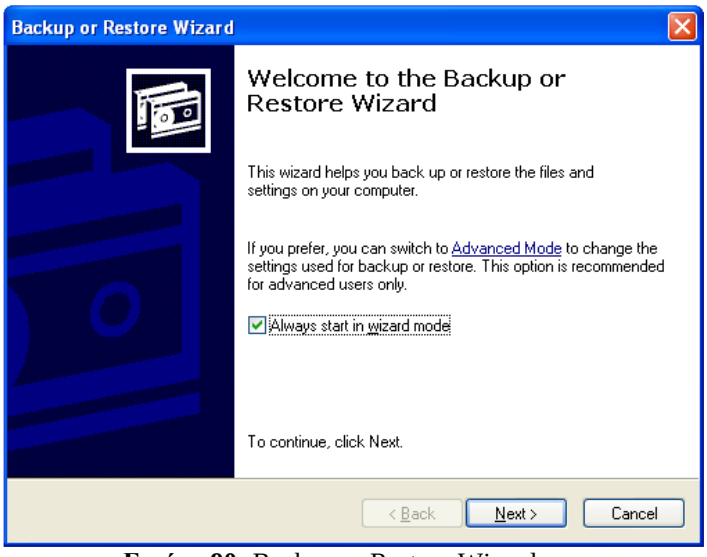
*Ανοίγουμε το **My Computer**. Πατάμε δεξί κλικ πάνω στο σκληρό μας δίσκο που περιέχει τα δεδομένα που θέλουμε να αποθηκεύσουμε και επιλέγουμε **Properties***



Εικόνα 88: Disk properties

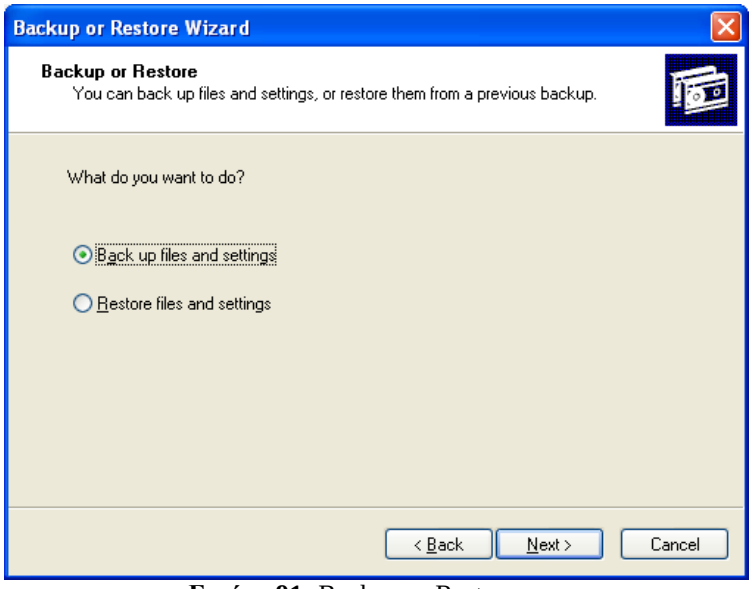
Πατάμε στη ετικέτα ***Tools*** *. Πατάμε τώρα στο κουμπί* ***Backup Now.*** *Αυτό ξεκινά το Backup ή Restore Wizard.*

Εικόνα 89: Back now



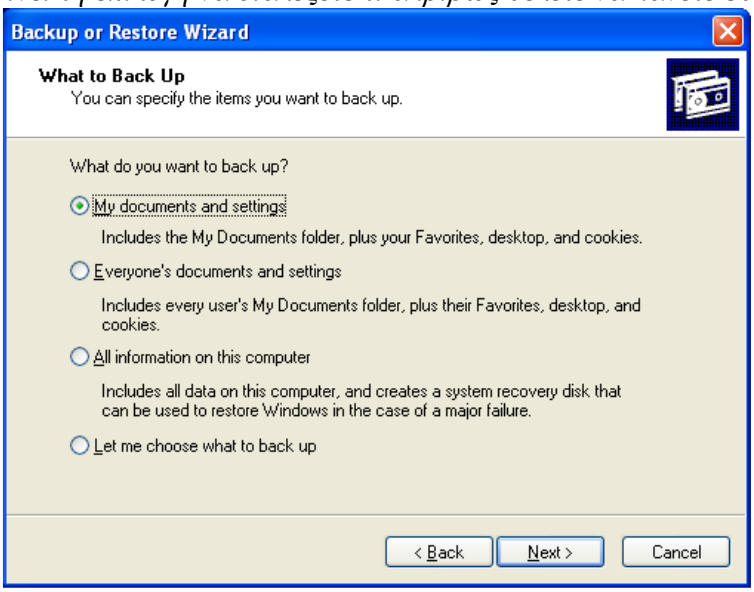
Εικόνα 90: Backup or Restore Wizard

Επιλέξτε την πρώτη επιλογή για το backup των αρχείων και των ρυθμίσεων.



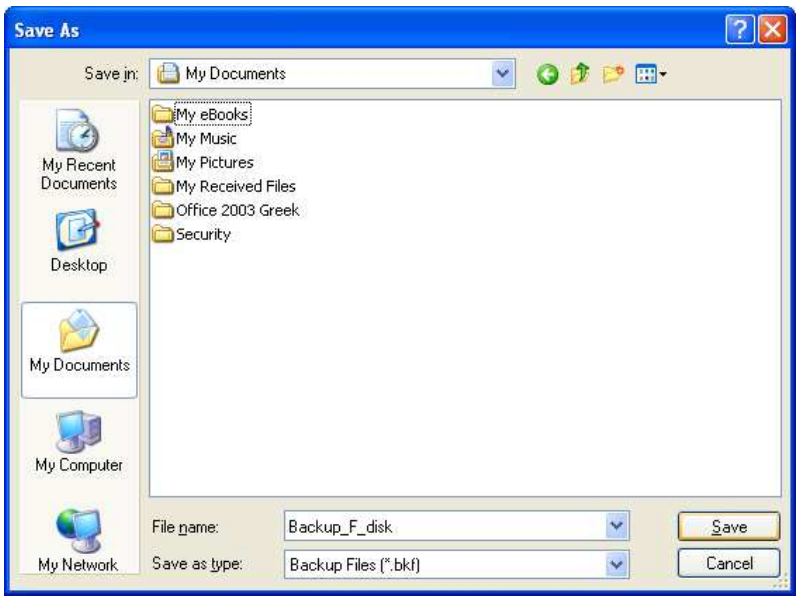
Εικόνα 91: Backup or Restore

Σας δίνει τη επιλογή να διαλέξετε τι ακριβώς θέλετε να κάνετε backup

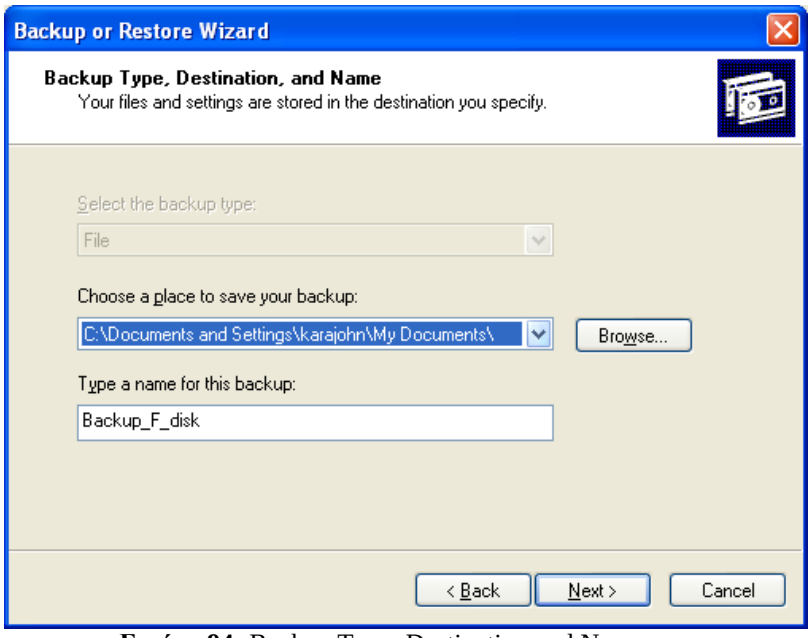


Εικόνα 92: What to Backup

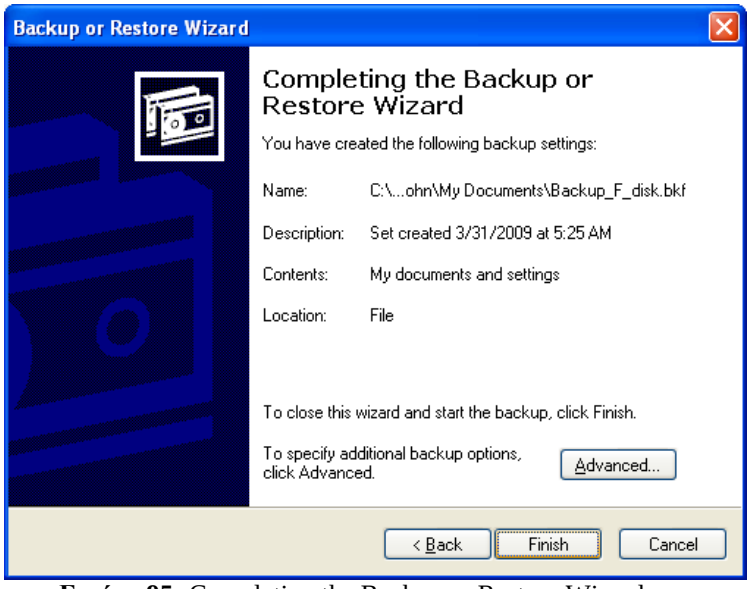
Και διαλέξετε που θέλετε να αποθηκευτούν αυτά που θέλετε να κάνετε Backup και με τι όνομα και πατήστε ***Save.***



Εικόνα 93: Save as

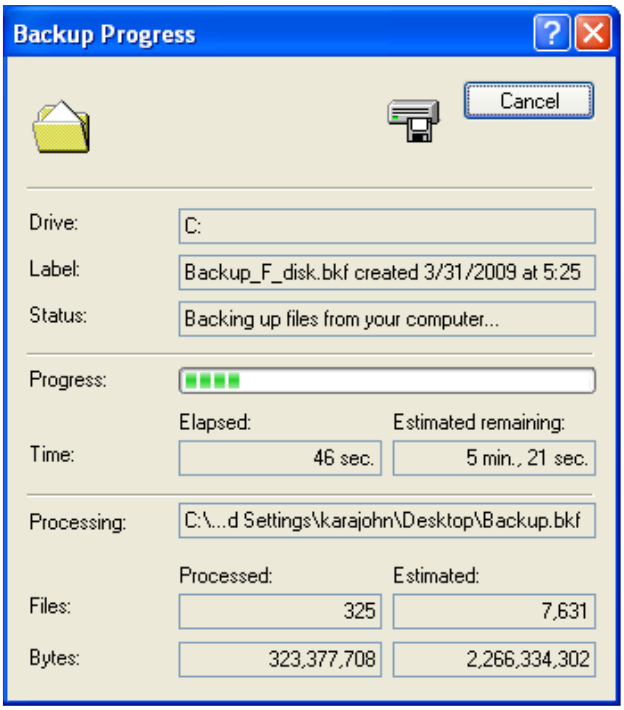


Εικόνα 94: Backup Type ,Destination and Name



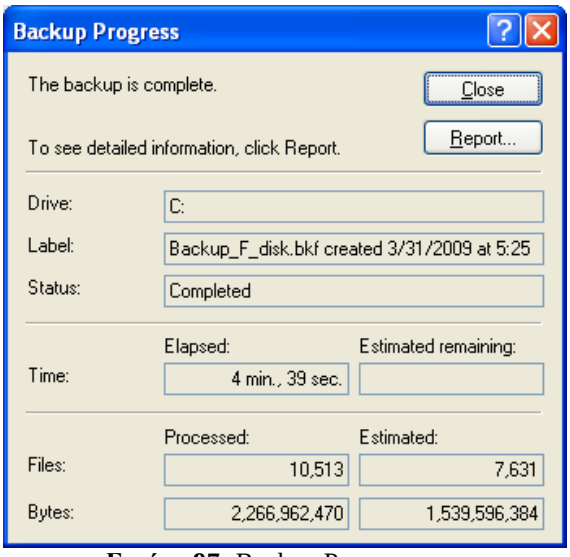
Εικόνα 95: Completing the Backup or Restore Wizard

Κατά τη διάρκεια της διαδικασίας ***Backup.***



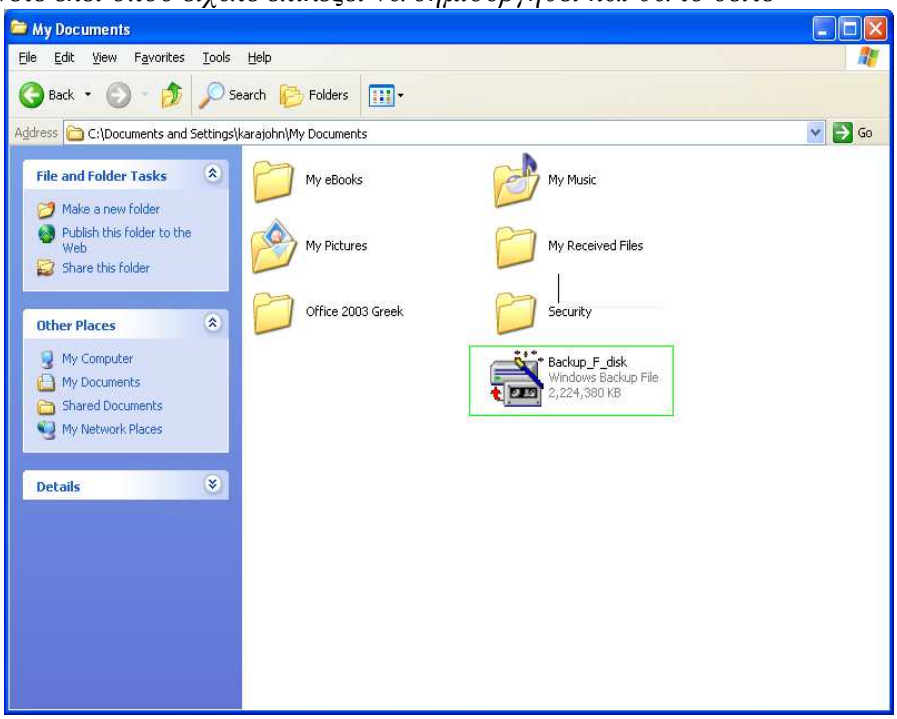
Εικόνα 96: Backup Progress

*Μόλις τελειώσει η διαδικασίας πατήστε **close***



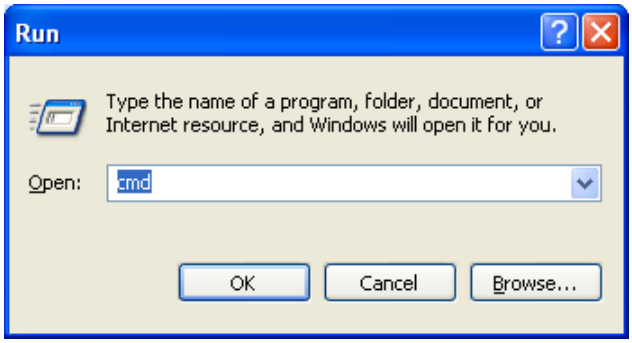
Εικόνα 97: Backup Progress

Πηγαίνετε εκεί όπου είχατε επιλέξει να δημιουργηθεί και θα το δείτε

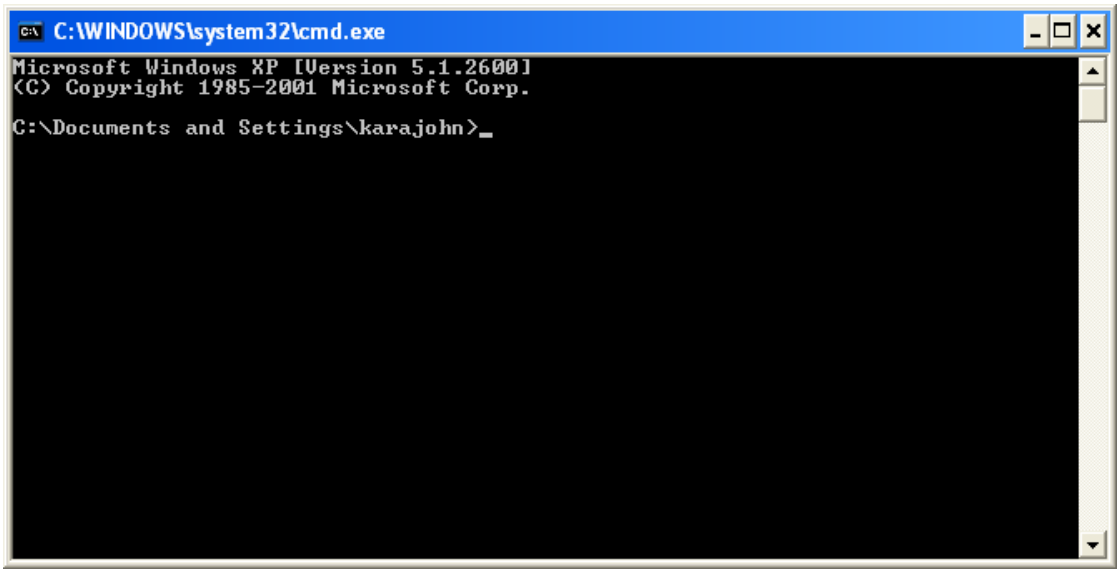


Εικόνα 98: Αρχείο Backup

2. Από το μενού Έναρξη, διαλέξτε **Run** και πληκτρολογήστε **cmd.exe** για να ανοίξει το παράθυρο των γραμμών εντολών.

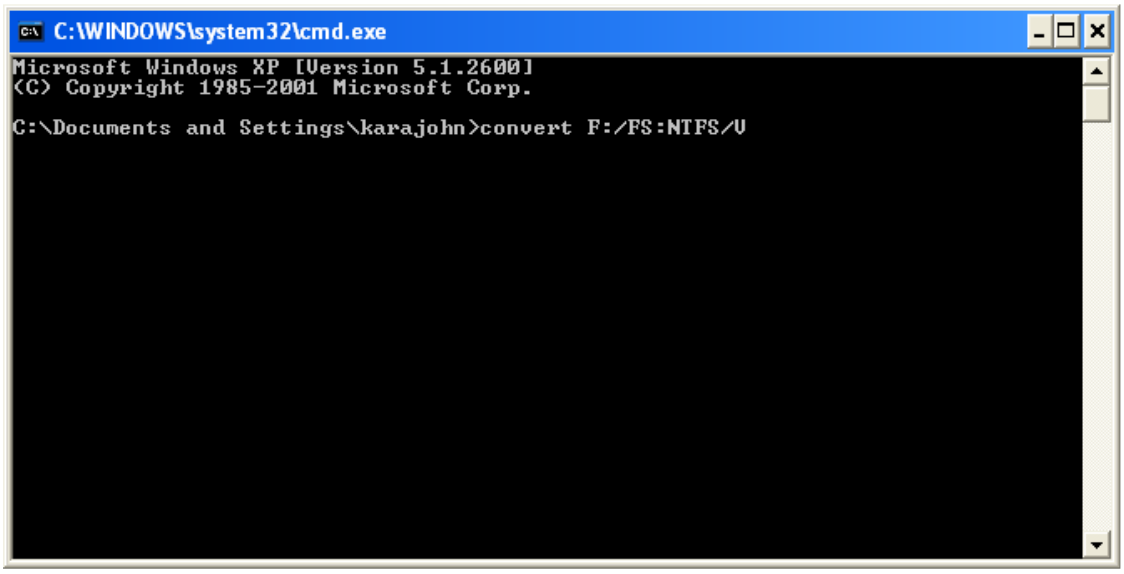


Εικόνα 99: Run

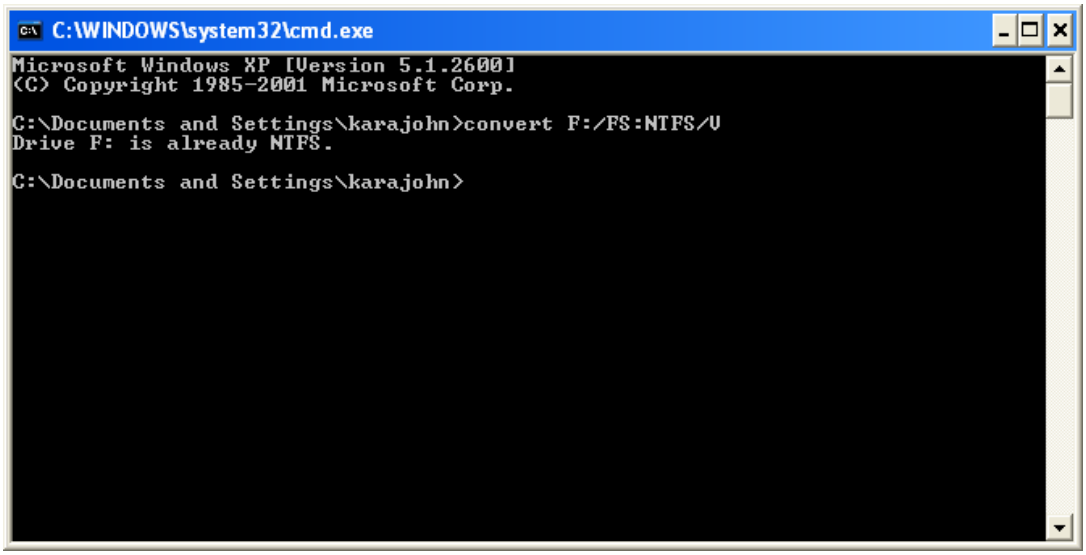


Εικόνα 100: Cmd

3. Εκτελέστε τη μετατροπή με τι σωστές παραμέτρους. Για παράδειγμα, η ακόλουθη εντολή θα μετατρέψει το δίσκο D σε NTFS σε ένα λεπτομερή mode: **convert F: /FS:NTFS /V**.

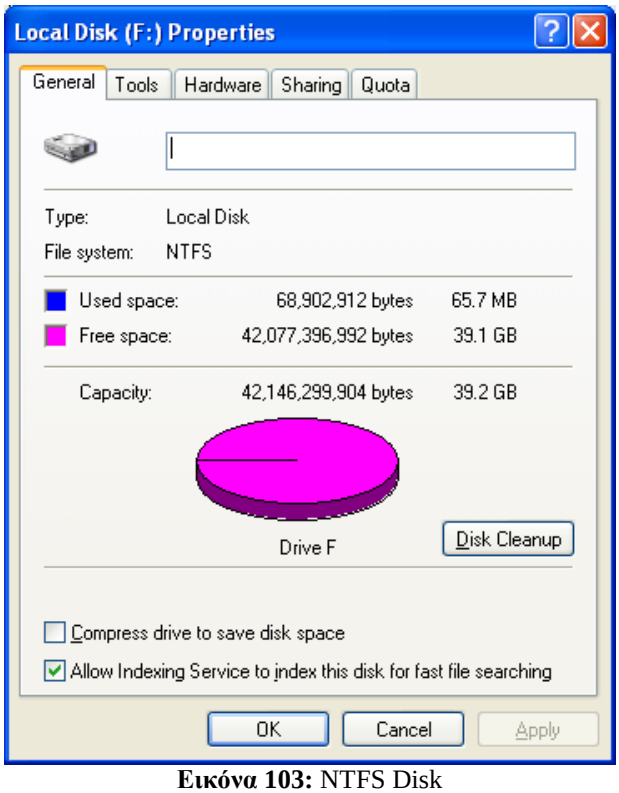


Εικόνα 101: Μετατροπή από FAT32 σε NTFS



Εικόνα 102: Επιτυχής μετατροπής

Μόλις τελειώσει η διαδικασία πηγαίνετε στο δίσκο όπου ήταν FAT32 και διαλέξτε properties και θα δείτε στο file system του δίσκου ότι τώρα είναι NTFS



Εικόνα 103: NTFS Disk

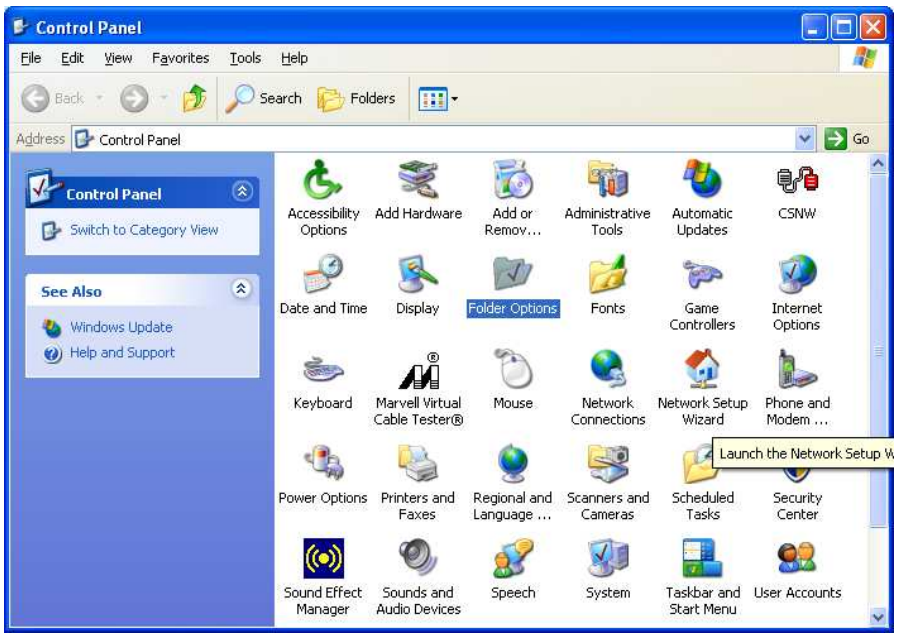
3.1.2 Folder Options

Η τροποποίηση των Folder Options μπορεί να βελτιώσει σημαντικά την άμυνα κατά του κακόβουλου λογισμικού. Το σύστημα μπορεί να ρυθμιστεί έτσι ώστε να βλέπετε

όλα τα ονόματα αρχείων πλήρη, συμπεριλαμβανομένων των επεκτάσεων. Επιπλέον, οι Folder Options περιέχουν ενώσεις μεταξύ τύπων αρχείων και προεπιλεγμένες εφαρμογές που τρέχουν κάθε τύπο αρχείου. Με την τροποποίηση των ενώσεων για τις επεκτάσεις αρχείων που χρησιμοποιούνται συχνά για κακόβουλους σκοπούς, τα εν λόγω αρχεία θα εκτελεστούν από τη εφαρμογή Notepad, το οποίο εξουδετερώνει τη αποτελεσματικά τους. Οι αλλαγές των Folder Options που περιγράφονται παρακάτω συνιστάται για κάθε περιβάλλον. Ο μόνος περιορισμός είναι ότι κάθε αρχείο με τη επέκταση του που μπορεί να έχει νόμιμη λειτουργία οργανισμού δεν θα πρέπει να remapped στο Notepad, διότι η λειτουργικότητα του μπορεί να σπαστεί. Εκτελέστε τα ακόλουθα βήματα, για να τροποποιήσετε τις Folder Options:

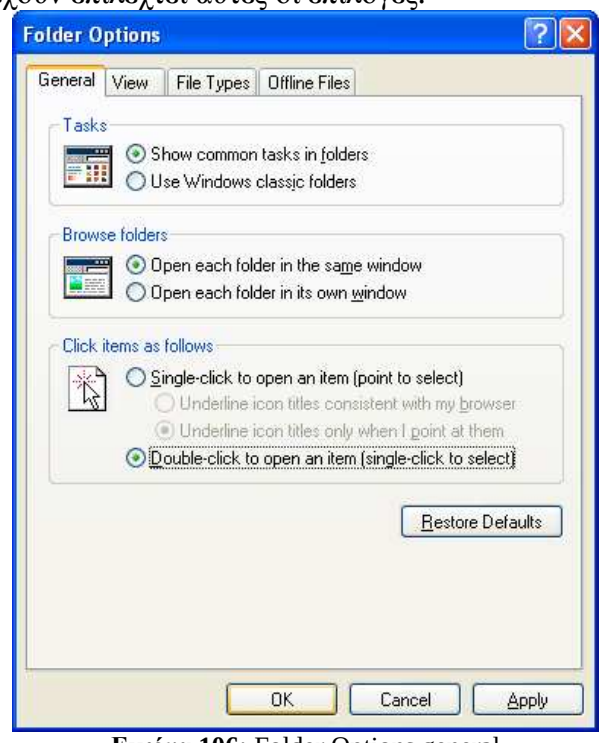
1. Πατήστε **Start** από το μενού και διαλέξτε **Control Panel**. Επιλέξτε **Folder Options**.

Εικόνα 104: Control Panel



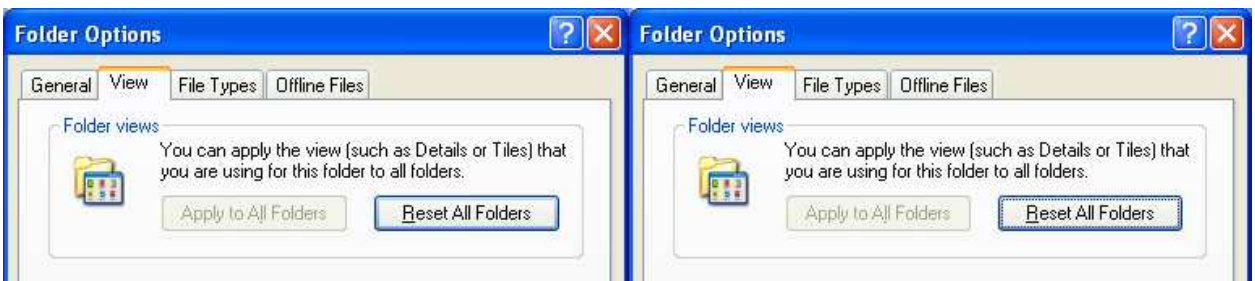
Εικόνα 105: Folder Options

2. Βεβαιωθείτε ότι, **Show common tasks in folders**, **Open each folder in the same window** και **Double-click to open an item (single-click to select)** έχουν επιλεχτεί αυτές οι επιλογές.

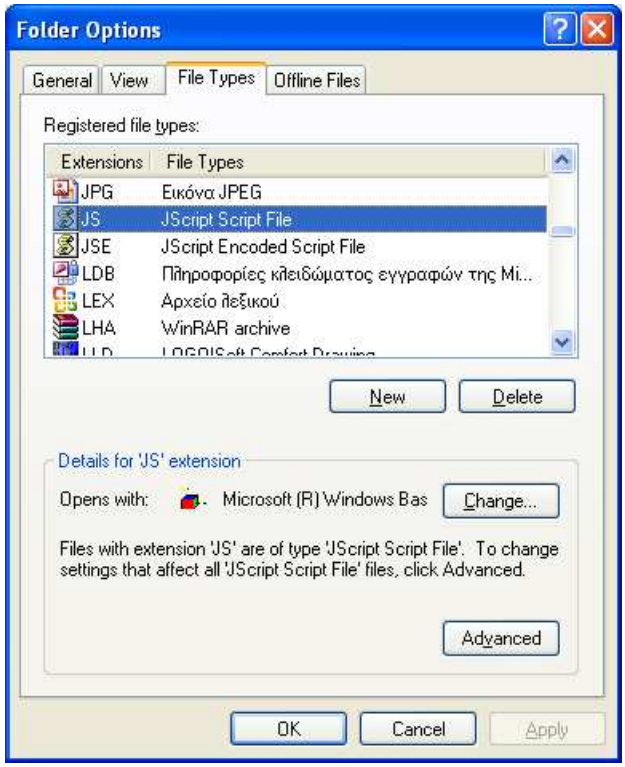


Εικόνα 106: Folder Options general

3. Επιλέξτε τη καρτέλα **View** . Βεβαιωθείτε ότι οι ρυθμίσεις αυτές ταιριάζουν με τις επιλογές των check boxes και των radio buttons όπως της παρακάτω εικόνας .



Επιλέξτε τη καρτέλα **File Types**. Κατεβάστε τη μπάρα στο παράθυρο με τα εγγεγραμμένα είδη αρχείων και επιλέξτε τη **JS** επέκταση και πατήστε στο κουμπί **Change**.



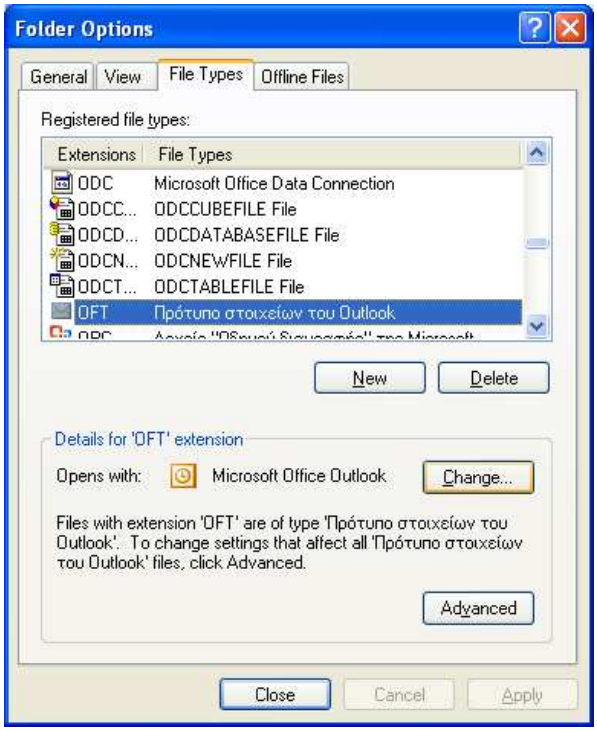
Εικόνα 107: File types

4. Επιλέξτε το πρόγραμμα του **Notepad** και πατήστε **OK**.

Εικόνα 108: Notepad

5. Επαναλάβετε τα δυο προηγούμενα βήματα για να αλλάξετε τις ακόλουθες επεκτάσεις: **JSE**, **OTF**, **REG**, **SCT**, **SHB**, **SHS, VBE, VBS**, **WSC**, **WSF**, και **WSH**.

Η διαδικασία συνεχίστηκε για όλες τις παραπάνω επεκτάσεις

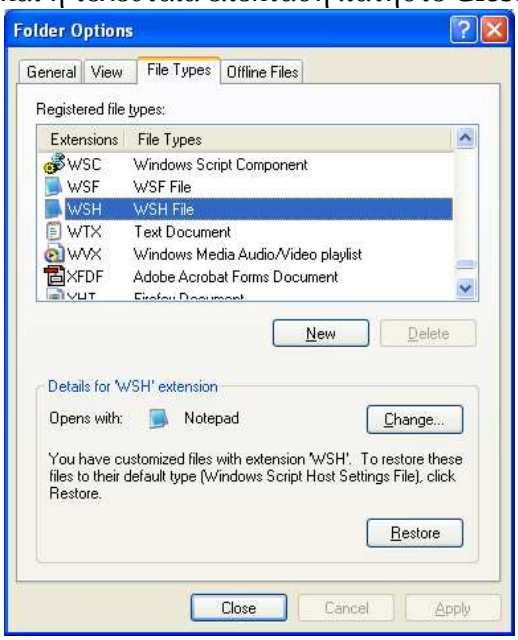


Εικόνα 109: Συνέχεια διαδικασίας βήμα 1

Εικόνα 110: Συνέχεια διαδικασίας βήμα 2

6. Πατήστε στο κουμπί **Close** και πατήστε **OK**.

Μόλις τελειώσει και η τελευταία επέκταση πατήστε **Close** και μετά **OK**



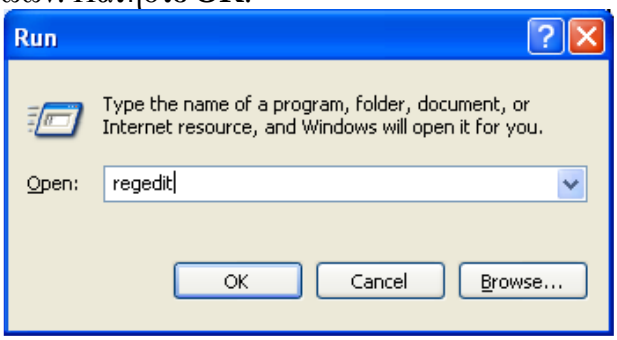
Εικόνα 111: Τέλος διαδικασίας

3.1.3 Show Hidden File Types

Ορισμένες επεκτάσεις αρχείων θα εξακολουθήσουν να παραμένουν κρυμμένες από το χρήστη, ακόμα και όταν το αρχείο **Hide file extension for known file types** η ρύθμιση του είναι απενεργοποιημένη. Εάν η τιμή μητρώου του **NeverShowExt** έχει οριστεί, τα Windows θα κρύψουν τις επεκτάσεις αρχείων των Windows για βασικούς τύπους αρχείων, ανεξάρτητα από άλλες επιλογές διαμόρφωσης του χρήστη. Για παράδειγμα, η επέκταση **.Lnk** σχετίζεται με τις συντομεύσεις των Windows για να παραμένουν κρυφές ακόμα και μετά από ένα χρήστη που έχει απενεργοποιήσει την επιλογή για να κρύψει τις επεκτάσεις. Οι Επιτιθέμενοι έχουν επωφεληθεί από αυτήν τη δυνατότητα για πολλά χρόνια με την αποστολή κακόβουλων αρχείων στους χρήστες που χρησιμοποιούν μια από τις κρυφές επεκτάσεις αρχείων[39]. Οι χρήστες δεν βλέπουν την επέκταση του αρχείου και είναι αφελείς λέγοντάς ότι το αρχείο είναι ασφαλές. Παρόλο που συνιστάται από πλευράς ασφαλείας να εμφανίζονται όλες οι επεκτάσεις αρχείων και ότι δεν θα έχει καμία επίπτωση στην λειτουργικότητα του συστήματος, οι χρήστες μπορούν να συγχέονται με την αλλαγή. Για παράδειγμα, τα περισσότερα εικονίδια για το μενού Έναρξη θα παρουσιάζουν με τη επέκταση **.Lnk** . Σε μια επιχείρηση, οι διαχειριστές μπορούν να αποφασίσουν για συμβιβασμό να δείχνουν όλες τις επεκτάσεις αρχείων εκτός από τη .Lnk.

Για την αποφυγή όλων των επεκτάσεων αρχείων από το να είναι κρυμμένες, εκτελέστε τα παρακάτω βήματα:

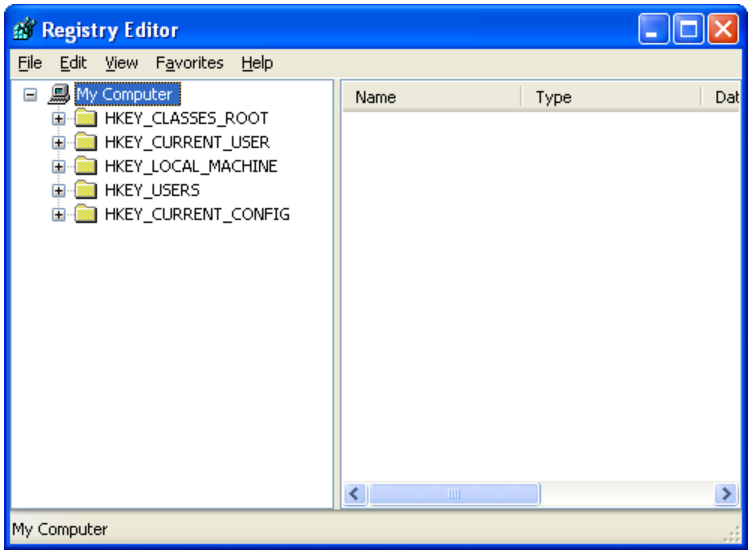
1. Πατήστε **Start** από το menu, επιλέξτε **Run**, και εισάγετε **regedit** να ανοίξει ο εκδότης μητρώων. Πατήστε **OK**.



Εικόνα 112: Run

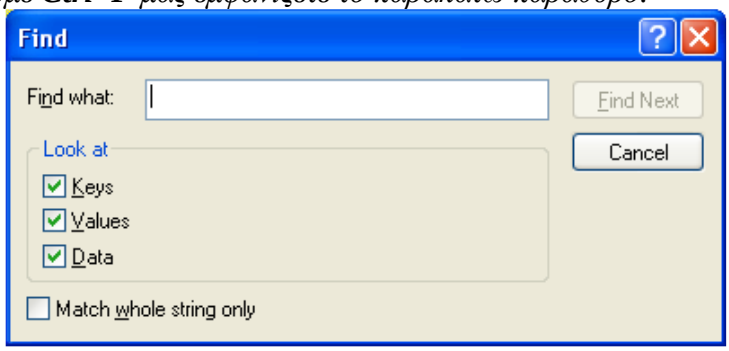
2. Πατήστε στη εικόνα My Computer και πατήστε **Ctrl+F**. Καθάρισε όλα **Keys** και **Data** από τα check boxes. Πληκτρολόγησε στη τιμή **NeverShowExt**. Πατήστε το κουμπί **Find Next**. Όταν βρεθεί η τιμή , πατήστε δεξί κλικ και **Delete**. Πατήστε **Yes** να επιβεβαιώσετε τη διαγραφή..

[39] Ένα παράδειγμα για αυτό που περιγράφεται είναι στο CERT®/CC Incident Note IN-2000-07, διαθέσιμο στη σελίδα http://www.cert.org/incident_notes/IN-2000-07.html.



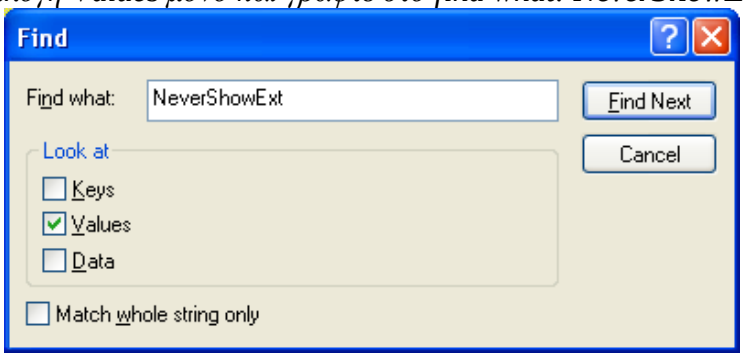
Εικόνα 113: Registry Editor

*Μόλις πατήσουμε **Ctrl+F** μας εμφανίζετε το παρακάτω παράθυρο.*



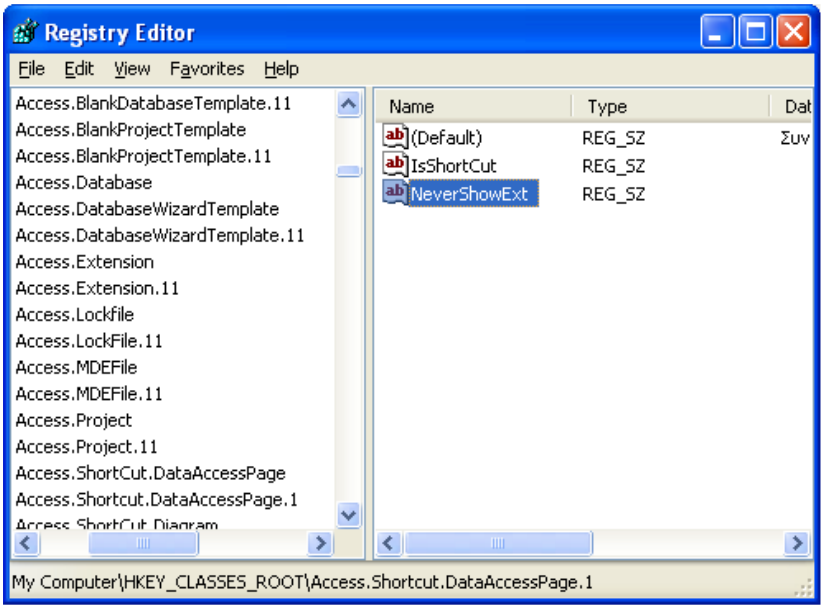
Εικόνα 114: Find

*Αφήστε την επιλογή Values μόνο και γράψτε στο find what: **NeverShowExt***



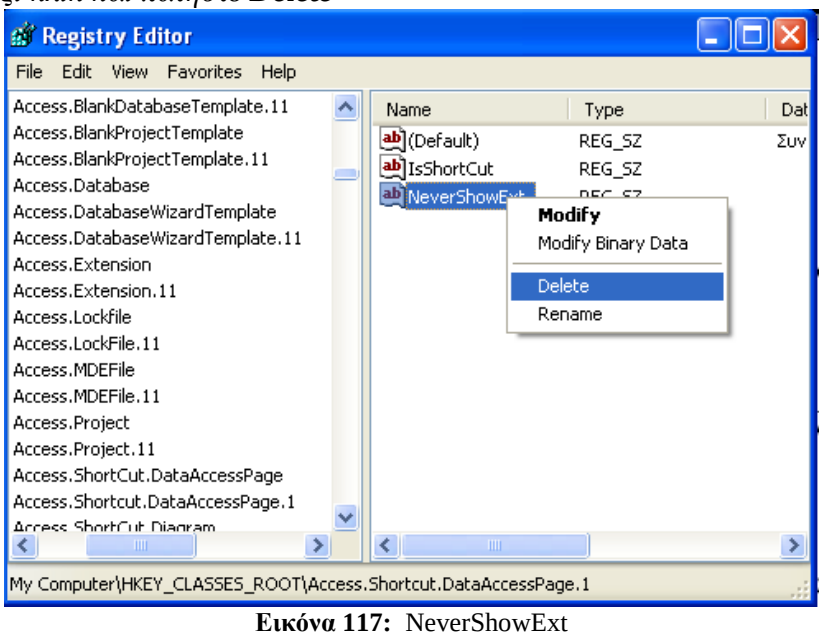
Εικόνα 115: Find what

Θα εμφανιστεί το παρακάτω παράθυρο με την επιλεγμένη λέξη που είχατε γράψει στο *find what. Πατήστε δεξί κλικ και πατήστε **Delete***



Εικόνα 116: Registry Editor

Πατήστε δεξί κλικ και πατήστε ***Delete***

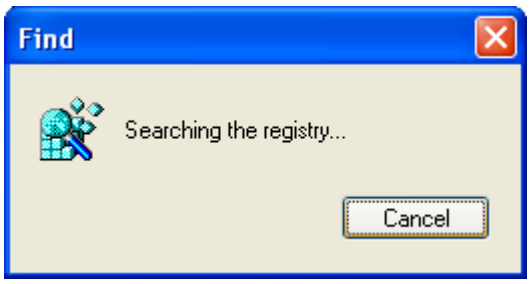


Εικόνα 117: NeverShowExt

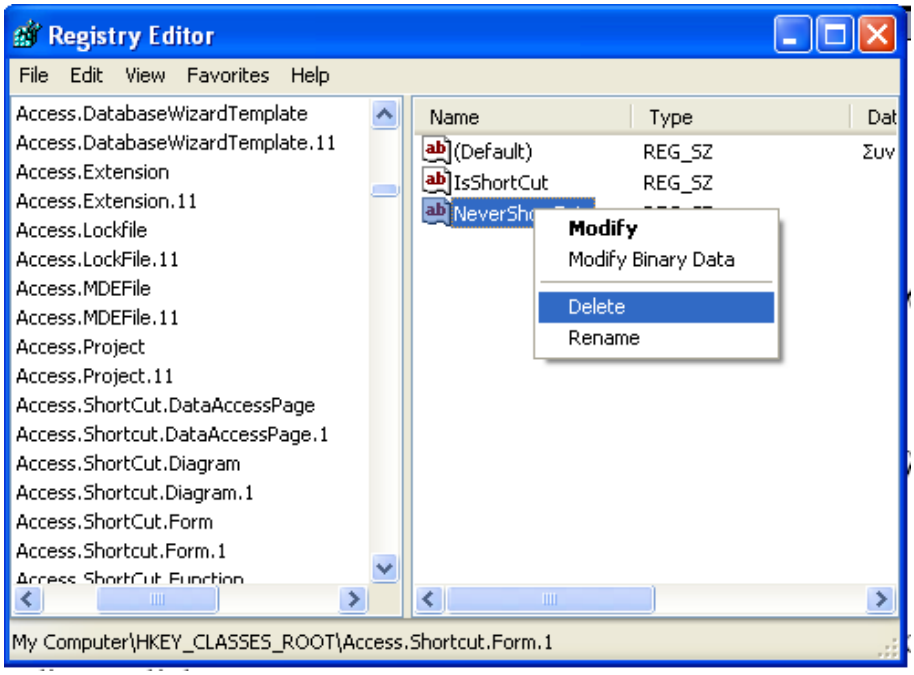
Πατήστε στη επιβεβαίωση ***Yes***

Εικόνα 118: Confirm Value Delete

3. Πατήστε το **F3** να βρείτε τη επόμενη εμφάνιση της αξίας και διαγράψτε την. Επαναλάβετε τη διαδικασία αυτή μέχρι να μη υπάρχει.



Εικόνα 119: Searching the registry



Εικόνα 120: Registry Editor

Όταν διαπιστώσει ότι δεν υπάρχει καμιά λέξη με το επιλεγμένο όνομα σου εμφανίζει το παρακάτω παράθυρο

Εικόνα 121: Registry Editor

4. Βγείτε από το **regedit** και κάντε επανεκκίνηση στον υπολογιστή σας.

3.1.4 EFS

Το Σύστημα κρυπτογράφησης αρχείων (EFS) έχει σχεδιαστεί για να αντιμετωπίσει πολλές ανησυχίες σχετικά με την ακεραιότητα των δεδομένων που αποθηκεύονται σε συστήματα των Windows XP. Τα EFS είναι σχεδιασμένα για να διατηρούν τα δεδομένα ιδιωτικά και δυσανάγνωστα για τους χρήστες χωρίς άδεια. Οι κακόβουλοι χρήστες με φυσική πρόσβαση σε υπολογιστή με Windows XP μπορούν να εκκινήσουν ένα σύστημα αρχείων, εκτός από το NTFS, παρακάμπτοντας αποτελεσματικά όλες τις εγγυήσεις που παρέχονται από το NTFS. Αυτό δίνει στο κακόβουλο χρήστη τη πρόσβαση σε όλα τα αρχεία που διαμένουν χωρίς κρυπτογράφηση στον σκληρό δίσκο του υπολογιστή. Το EFS χρησιμοποιεί κρυπτογράφηση αρχείων για τη μείωση των κινδύνων που συνδέονται με την κινητή πληροφορική και τη φυσική πρόσβαση χωρίς άδεια. Επειδή EFS μόνο παρέχει κρυπτογράφηση σε αρχεία και φακέλους σε διαμερίσματα NTFS, τα δεδομένα δεν προστατεύονται πλέον όταν είναι σε κάποιο άλλο σημείο (π.χ. σε συνημμένο e-mail, CD-ROM) ή μεταδίδονται μέσω του δικτύου. Άλλα μέτρα προστασίας πρέπει να χρησιμοποιείται, όπως μια σύνδεση εικονικού ιδιωτικού δικτύου (VPN) ή αρχείο τρίτο λογισμικό κρυπτογράφησης.

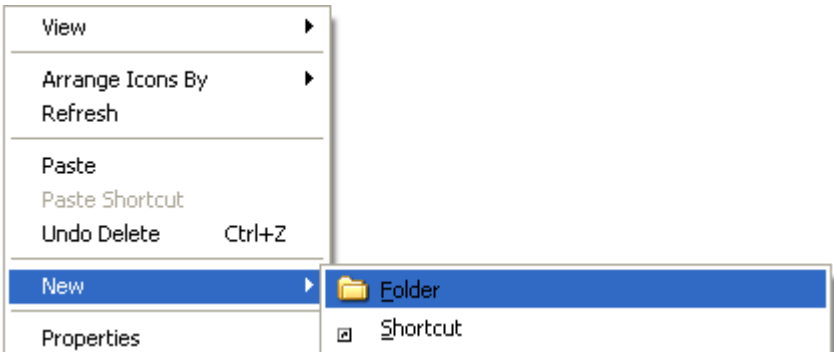
Το σύστημα EFS, το οποίο βασίζεται σε δημόσιο κλειδί κρυπτογράφησης, ενσωματώνετε καλά με την υποδομή του δημόσιου κλειδιού (PKI) στοιχεία που έχουν ενσωματωθεί στα Windows XP. Η πραγματική λογική η οποία εκτελεί την κρυπτογράφηση είναι ένα σύστημα παροχής υπηρεσιών που δεν μπορούν να κλείσουν. Το πρόγραμμα αυτό είναι χαρακτηριστικό για την πρόληψη παράνομης πρόσβασης, αλλά έχει ένα πρόσθετο πλεονέκτημα του να καταστεί η διαδικασία κρυπτογράφησης πλήρη διαφάνεια για τον χρήστη. Κάθε αρχείο που κάποιος χρήστης μπορεί να κρυπτογραφήσετε κρυπτογραφούνται χρησιμοποιώντας ένα τυχαία δημιουργημένο αρχείο κλειδί κρυπτογράφησης (ΦΕΚ).
Το EFS μπορεί να χρησιμοποιηθεί για να κρυπτογραφήσετε μεμονωμένα αρχεία και φακέλους σε NTFS volumes[40]. Η αρχική ρύθμιση του EFS επιτρέπει σε ένα χρήστη την κρυπτογράφηση και την αποκρυπτογράφηση αρχείων αμέσως, χωρίς οποιαδήποτε αλληλεπίδραση του διαχειριστή. Όταν ένας φάκελος είναι κρυπτογραφημένος, όλα τα νέα αρχεία που δημιουργούνται θα είναι κρυπτογραφημένα, όπως όλα τα έγγραφα που θα μετακομίζετε εκεί, έτσι ώστε οι χρήστες να μη χρειάζεται να κρυπτογραφούν με το χέρι κάθε νέο αρχείο. Με το EFS μπορείτε επίσης να κρυπτογραφήσετε αρχεία σε ένα κοινόχρηστο πόρο δικτύου και τη δυνατότητα να αποκρυπτογραφήσετε τα αρχεία, ακόμη και όταν δεν είναι συνδεδεμένα με αυτόν τον πόρο.

[40] Ένας περιορισμός της EFS για να εξετάσουμε, είναι όταν επιλέγουμε να κρυπτογραφήσουμε έναν ολόκληρο τόμο διότι ο όγκος στα οποία είναι εγκατεστημένα τα Windows XP δεν μπορεί να κρυπτογραφηθεί στο σύνολό του, διότι η αποκρυπτογράφηση του EFS δεν είναι διαθέσιμη μέχρι αργά της διαδικασίας εκκίνησης. Αυτό θα οδηγούσε στο OS να προσπαθήσει κατά την εκκίνηση, αλλά να αποτυγχάνει λόγω των απαραίτητων μερών του OS όπου αποκρυπτογραφούνται και δεν θα μπορούσαν να διαβαστούν για να ολοκληρωθεί η διαδικασία εκκίνησης.

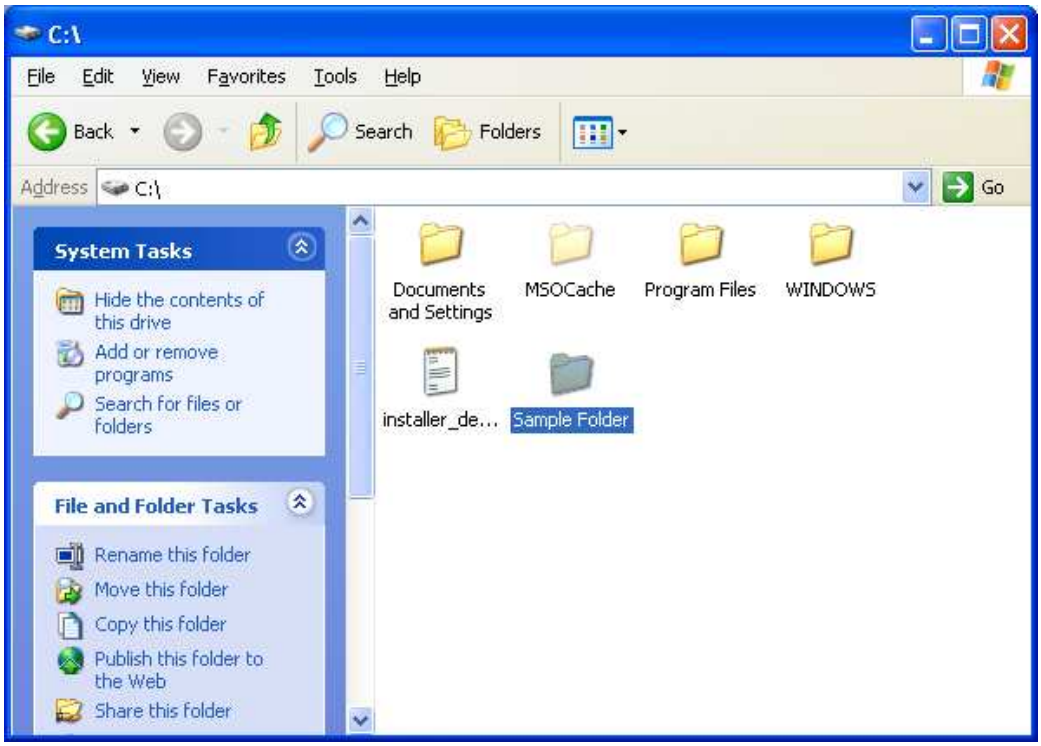
3.1.4.1 EFS Implementation Example

Το EFS μπορεί να υλοποιηθεί με τρεις τρόπους: από τις Properties του παράθυρο ενός φακέλου, από το παράθυρο "Ο υπολογιστής μου" και από το Windows Explorer. Κατά την εφαρμογή του EFS, συνιστάται ότι ο φάκελος κρυπτογράφησης θα δημιουργηθεί για ευαίσθητα αρχεία. Αυτό το παράδειγμα διαδικασίας περιγράφει τον τρόπο εφαρμογής του EFS για δείγμα φάκελου μέσα από το παράθυρο "Ο υπολογιστής μου".

1. Από το παράθυρο **My Computer**, δημιουργήστε ένα νέο και ονομάστε το **Sample Folder**.

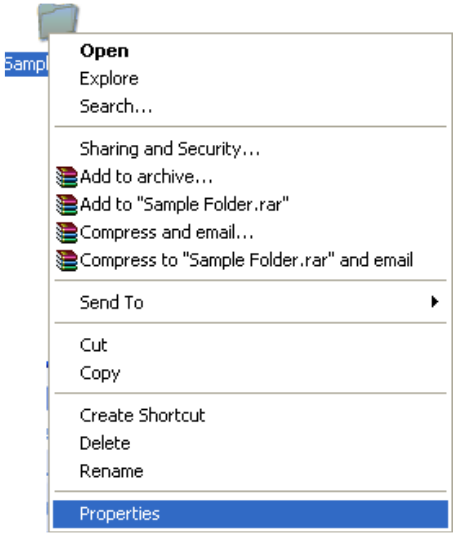


Εικόνα 122: New Folder

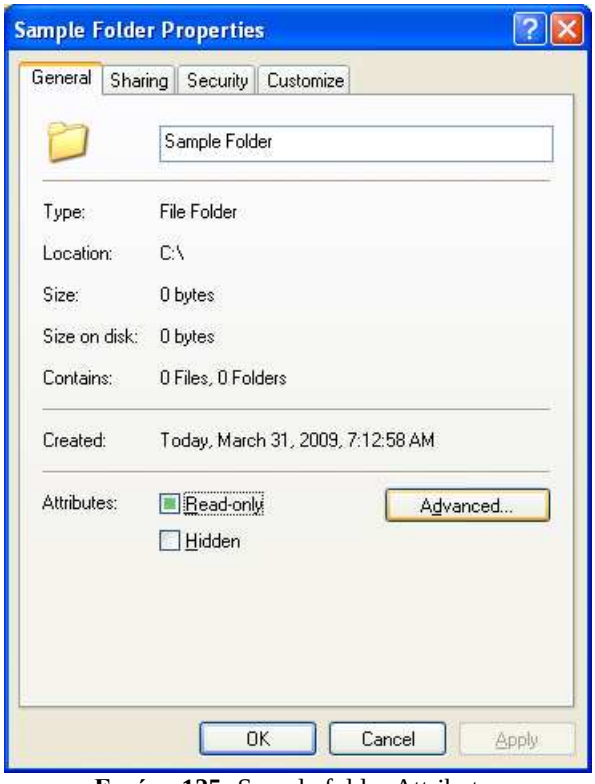


Εικόνα 123: Sample Folder

2. Δεξί κλικ πάνω στο **Sample Folder** και πατήστε **Properties**, πατήστε κλικ στο κουμπί **Advanced**. Με αυτό το κουμπί πρέπει να σας ανοίξει το **Advanced Attributes** παράθυρο.

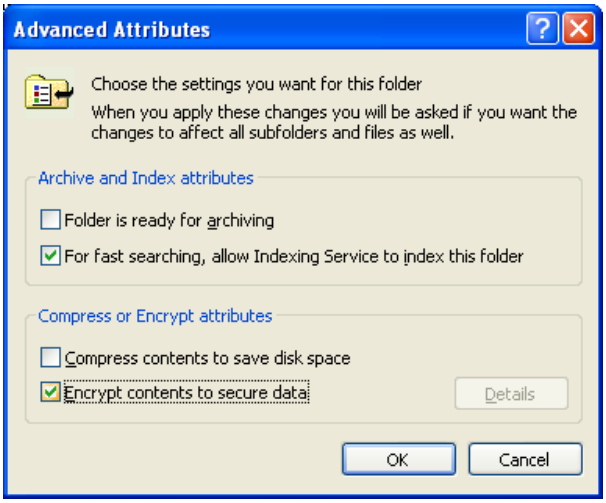


Εικόνα 124: Sample folder properties

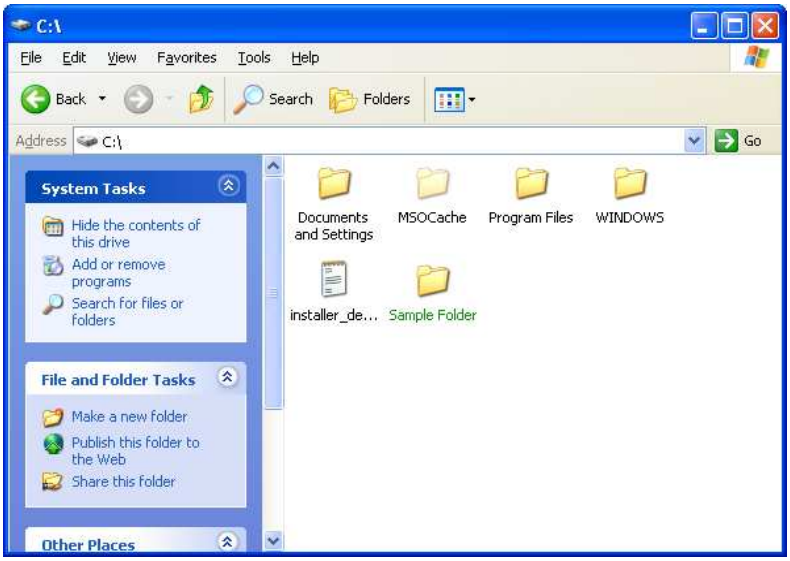


Εικόνα 125: Sample folder Attributes

3. Επιλέξτε το κουτί **Encrypt contents to secure data** και πατήστε **OK**. Πατήστε **OK** ξανά. Το χρώμα του **Sample Folder** θα πρέπει να έχει αλλαχθεί, αναφέροντας ότι όλα τα αρχεία που θα προστίθενται σε αυτόν το φάκελο θα πρέπει αυτομάτως να κρυπτογραφούνται..

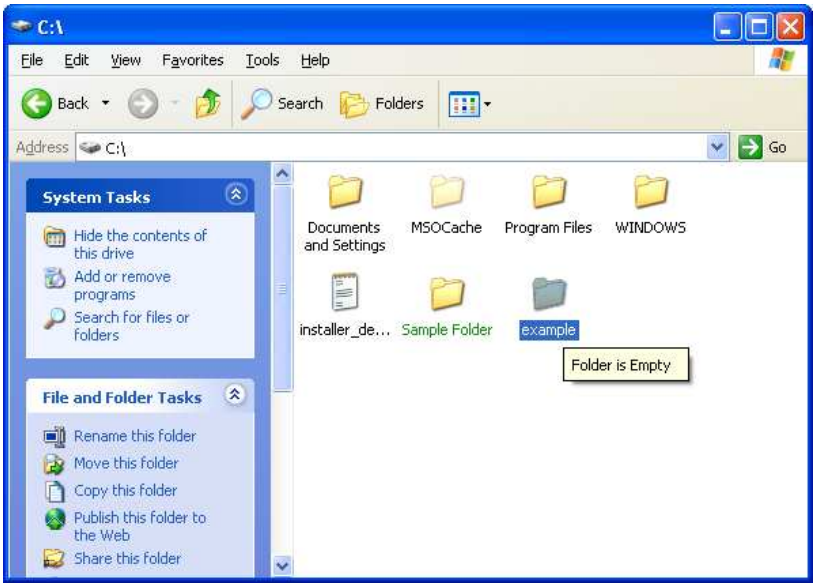


Εικόνα 126: Advanced Attributes



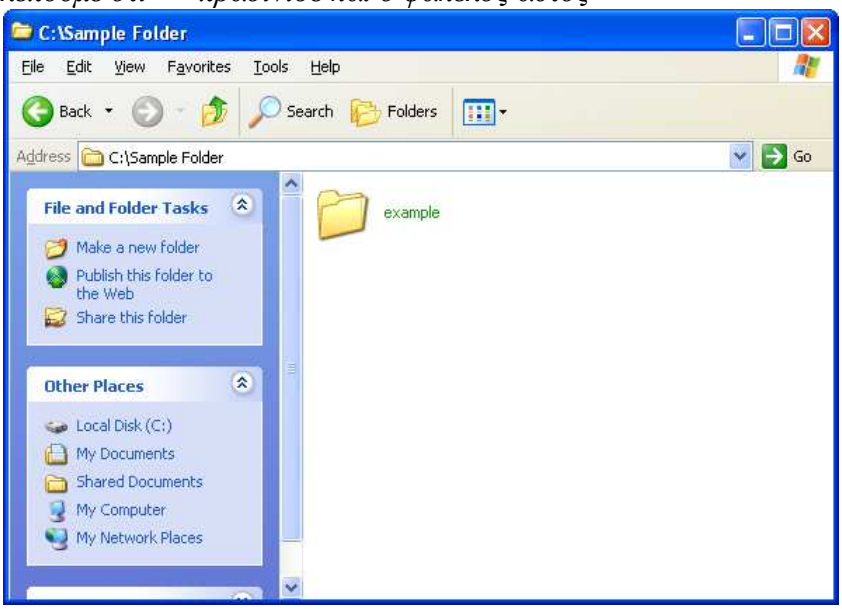
Εικόνα 127: Sample folder (2)

Δημιουργούμε ένα νέο φάκελο με το όνομα Example



Εικόνα 128: Example

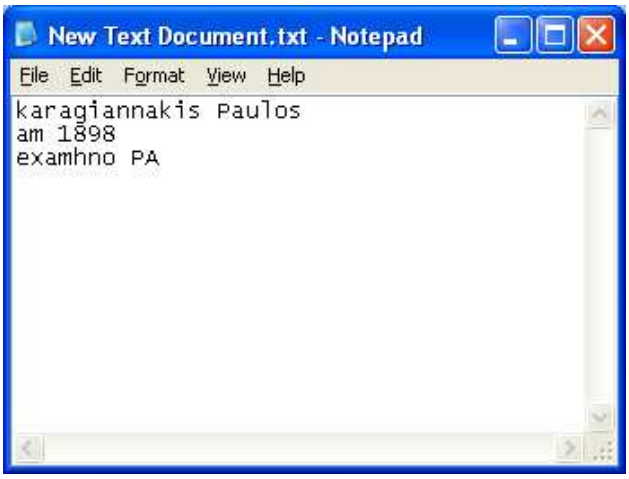
Κάνουμε αποκοπή το φάκελο Example και το κάνουμε επικόλληση στο Sample Folder. Βλέπουμε ότι <<πρασίνισε και ο φάκελος αυτός>>



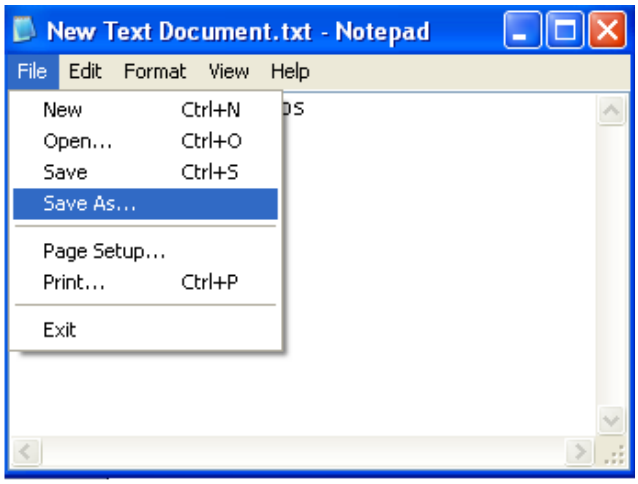
Εικόνα 129: Sample folder example

4. Ανοίξτε το σημειωματάριο και γράψτε κάτι μέσα. Αποθηκεύστε το αρχείο ως **Sample.txt** μέσα στο **Sample Folder**.

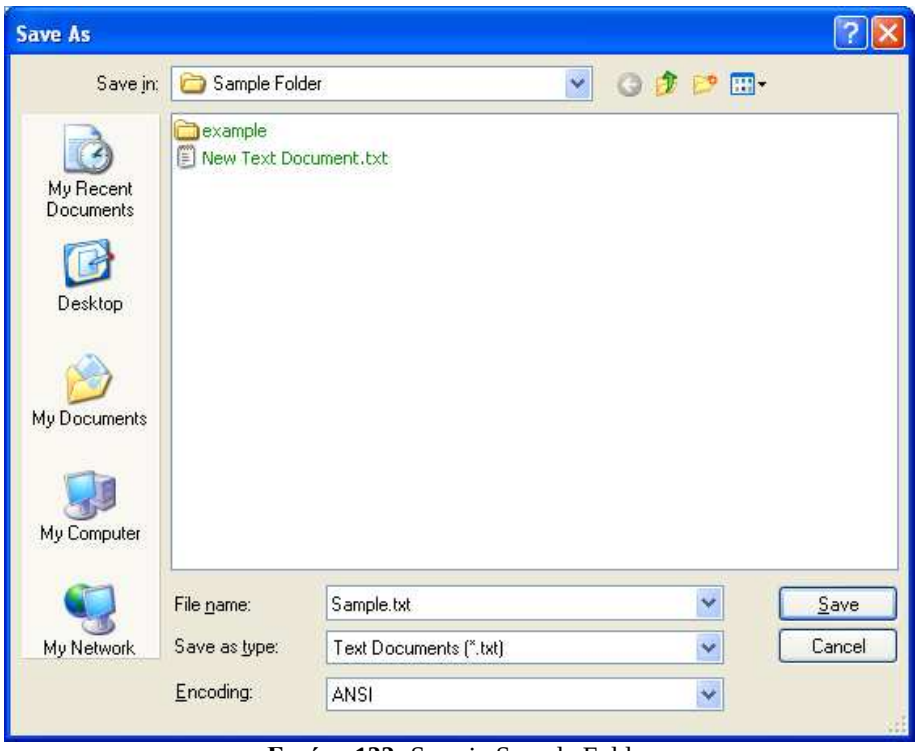
Εικόνα 130: Σημειωματάριο



Εικόνα 131: New Text Document

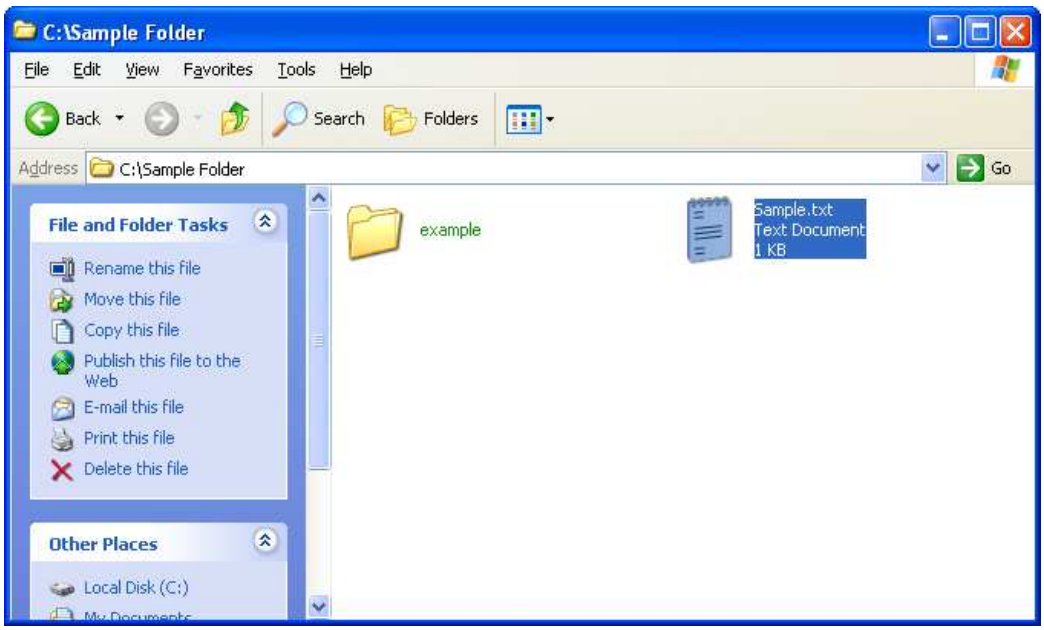


Εικόνα 132: Save As New Text Document



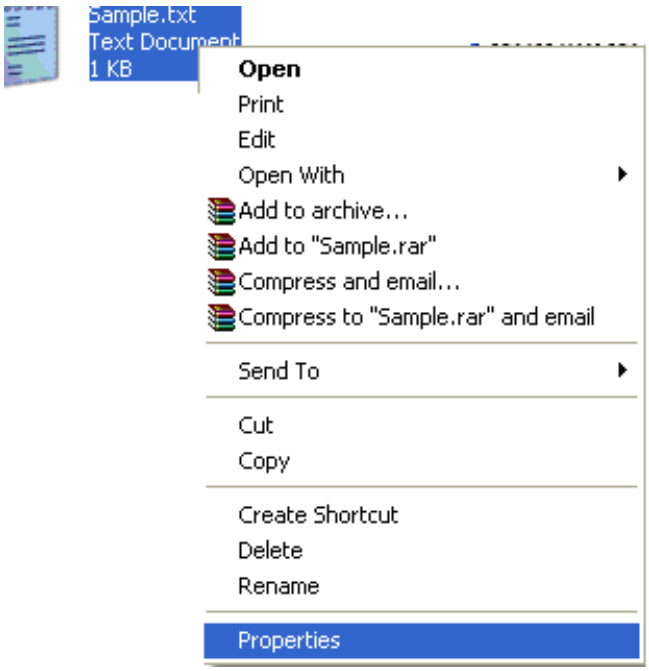
Εικόνα 133: Save in Sample Folder

5. Διπλό κλικ στο **Sample Folder** να δείτε τα περιεχόμενα του. Το χρώμα του **Sample.txt** του ονόματος αρχείου θα πρέπει να αναφερθεί ότι είναι κρυπτογραφημένο.

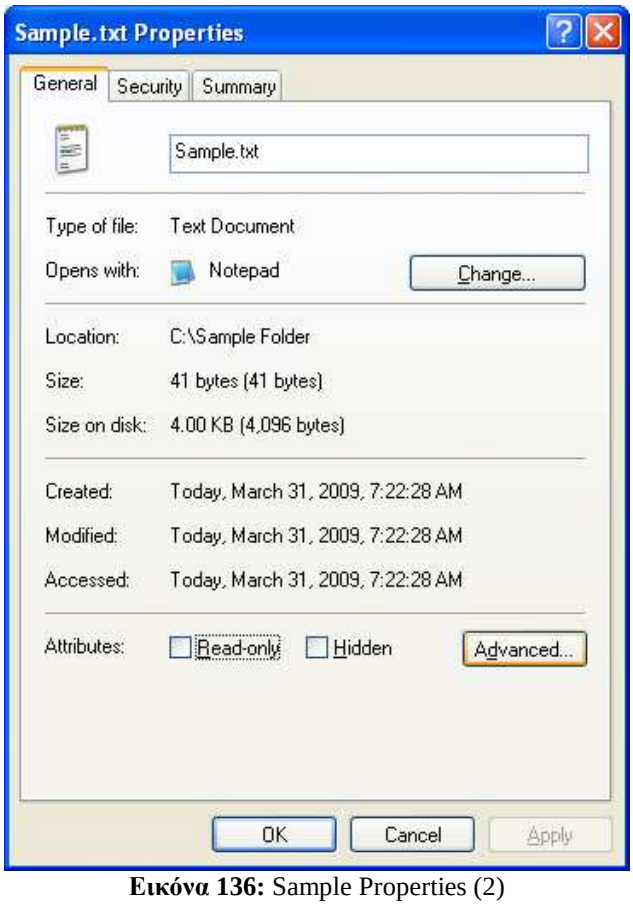


Εικόνα 134: Sample.txt

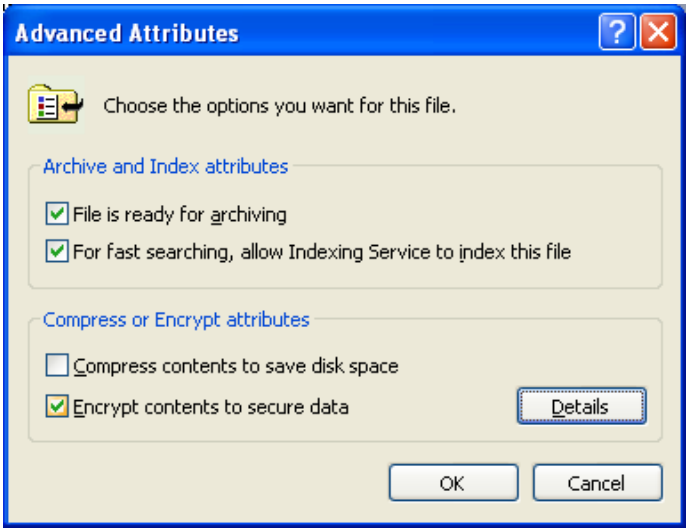
6. Δεξί κλικ στο **Sample.txt** και πατήστε **Properties**, μετά πατήστε το κουμπί **Advanced**. Αυτό επιβεβαιώνει ότι το αρχείο είναι κρυπτογραφημένο.



Εικόνα 135: Sample Properties



Εικόνα 136: Sample Properties (2)



Εικόνα 137: Advanced Attributes

3.1.4.2 EFS Data Recovery

Η διαδικασία EFS είναι διαφανής για τον τελικό χρήστη, επειδή το EFS είναι ενσωματωμένο με το NTFS. Άλλοι χρήστες με παρόμοια ή μικρότερα προνόμια δεν θα μπορούσαν να ανοίξουν ενός άλλου χρήστη το EFS διότι στο κρυπτογραφημένο αρχείο δεν έχουν το FEK. Σε ορισμένες περιπτώσεις, οι περιορισμοί πρόσβασης, όπως αυτές απαιτούν από τους χρήστες να επιτρέπουν να εφαρμόζουν τις διαδικασίες ανάκτησης δεδομένων. Για παράδειγμα, αν το ζεύγος-κλειδί που χρησιμοποιείται για την κρυπτογράφηση ενός αρχείου ήταν κατεστραμμένο, το αρχείο θα πρέπει να καθίστανται απρόσιτα χωρίς ένα Data Recovery Agent (DRA).

Στα Windows XP το EFS παρέχει ολοκληρωμένη υποστήριξη στη ανάκτηση δεδομένων. Η υποδομή ασφαλείας των Windows XP εφαρμόζει στη διαμόρφωση των δεδομένων ανάκτησης κλειδιών τόσο καλά ώστε το EFS αν δεν είναι απρόσιτο ένα ή περισσότερα κλειδιά ανάκτησης να δημιουργούνται. Αυτό γίνεται συνήθως κατά τη διάρκεια της διαδικασίας εγκατάστασης. Από προεπιλογή, η ανάκαμψη είναι ευθύνη του Διαχειριστή. Το EFS επιτρέπει την ανάκτηση παραγόντων να ρυθμίζουν τα δημόσια κλειδιά που χρησιμοποιούνται για να επιτρέψουν την ανάκτηση αρχείων. Μόνο το αρχείου που δημιουργείται με τυχαίο κλειδί κρυπτογράφησης είναι διαθέσιμο χρησιμοποιώντας την ανάκτηση κλειδιού, όχι όμως ενός χρήστη το ιδιωτικό κλειδί. Η δράση αυτή εξασφαλίζει ότι δεν είναι άλλες ιδιωτικές πληροφορίες φανερές κατά λάθος με την ανάκαμψη του πράκτορα. Σε ένα περιβάλλον τομέα, ο διαχειριστής του τομέα μπορεί εύκολα να προσθέσει έναν παράγοντα αποκατάστασης του EFS μέσω της Πολιτικής ομάδας. Αυτό το χαρακτηριστικό μπορεί να αντιμετωπίσει τον κίνδυνο της απώλειας δεδομένων, ως αποτέλεσμα του αρχικού χρήστη να χάσει την εντολή αποκρυπτογράφησης. Σε ένα αυτόνομο περιβάλλον, ένας πράκτορας ανάκτησης πρέπει να ορίζεται με το χέρι ή κανείς δεν θα είναι σε θέση να

αποκρυπτογραφήσει τις πληροφορίες, αν η εντολή κρυπτογράφησης χάνεται. Το EFS δεν θα πρέπει να χρησιμοποιηθεί σε περίπτωση που ένας παράγοντας αποκατάστασης δεν έχει ορισθεί.

Κατά την εξέταση της εφαρμογής του EFS σε οποιοδήποτε περιβάλλον, ιδιαίτερη προσοχή πρέπει να δοθεί στο πώς τα κλειδιά και ο DRA θα διαχειρίζεται. Εάν τα στοιχεία πρέπει να διατηρηθούν για μεγάλο χρονικό διάστημα, ενώ είναι κρυπτογραφημένα, η μακροπρόθεσμη διατήρηση των κατάλληλων κλειδιών για την αποκρυπτογράφηση των δεδομένων πρέπει να διευθετηθούν. Ανάλογα με τη φύση των πληροφοριών και την ανάγκη να τα κρατήσει, χάνοντας την ικανότητά της να αποκρυπτογραφήσει τα αρχεία θα μπορούσε να επηρεάσουν σοβαρά την αποστολή της οργάνωσης. Κατά την εξέταση της χρήσης των DRA, είναι σημαντικό ότι οργανωτικά ευαίσθητες πληροφορίες δεν θα πρέπει αποκαλυφθούν σε λάθος ανθρώπους που δεν θα πρέπει να έχουν πρόσβαση στις πληροφορίες.

Η διαδικασία ανάκτησης κλειδιών που περιέχονται στο ***Encrypted Data Recovery Agents*** *φάκελο περιγράφετε παρακάτω με 5 βήματα , δυστυχώς παρά τη συνεχή προσπάθεια μου δεν ήταν δυνατό να μπορέσω να ακολουθήσω τις οδηγίες του συστήματος και να ανακτήσω τα κλειδιά από το φάκελο διότι δεν υπήρχε αυτός ο φάκελο ούτε στο λογαριασμό του διαχειριστή αλλά ούτε κ του Guest.*

Η ανάκτηση κλειδιών που περιέχονται στο **Encrypted Data Recovery Agents** φάκελο μπορούν να υποστηριχθούν σε αφαιρούμενα μέσα από την καταγραφή στο σύστημα με το ενσωματωμένο λογαριασμό Administrator και να εκτελέσουν τις ακόλουθες ενέργειες:

1. Ανοίξτε το φάκελο **Encrypted Data Recovery Agents** που βρίσκεται εντός στο **Group Policy**.

2. Δεξί κλικ στο Πιστοποιητικό ότι θα πρέπει να εξάγεται .

3. Διάλεξε **All Tasks**, μετά **Export**.

4. Αποθηκεύστε το αρχείο σε αφαιρούμενα μέσα.

5. Για μεγίστη ασφάλεια, η ανάκαμψη του πιστοποιητικού του EFS μπορεί να μετακινηθεί από τον υπολογιστή μετά το επιτυχές backup από την επιλογή **Delete Private Key if the Export is Successful**. Αυτό συνιστάτε ιδιαιτέρως για κινητά συστήματα.

NIST συνιστά για το EFS να χρησιμοποιείται μόνο όταν το απόρρητο των εν λόγω πληροφοριών είναι ζωτικής σημασίας ζωής όταν το σύστημα αντιμετωπίζει σημαντικές φυσικές απειλές. Για παράδειγμα, το σύστημα EFS μπορεί να είναι μια λύση για την εξασφάλιση των δεδομένων σχετικά με τους κινητούς φορητούς υπολογιστές που βρίσκονται σε υψηλό κίνδυνο να χαθούν ή να κλαπούν και για υπολογιστές που περιέχουν ευαίσθητες πληροφορίες. Στις αποφάσεις σχετικά με το EFS ανάπτυξης θα πρέπει να λαμβάνετε υπόψη τα βασικά θέματα διαχείρισης όπου αναφέρονται σε αυτό το τμήμα. Αν διαχειριστής κλειδιών δεν αντιμετωπίζονται αποτελεσματικά, η χρήση του EFS θα μπορούσε να συμβάλει στην απώλεια

πολύτιμων πληροφοριών. Το EFS θα πρέπει οπωσδήποτε να ληφθεί υπόψη για SOHO και SSLF περιβάλλοντα; Μπορεί επίσης να είναι επωφελή για ορισμένα συστήματα στην επιχείρηση και για FDCC περιβάλλοντα εάν καταφέρουν τα κλειδιά να τα διαχειριστούν καλύτερα.

Στα συστήματα που χρησιμοποιούν το σύστημα EFS, το Syskey θα έπρεπε επίσης να χρησιμοποιηθεί για να αποδειχθεί το κλειδί εκκίνησης για να προστατεύει τα ιδιωτικά κλειδιά που χρησιμοποιούνται για τα EFS[41]. Από προεπιλογή για όλα τα συστήματα των Windows XP, είναι ενεργοποιημένη το Syskey και αποθηκεύει στη μηχανή το κλειδί που δημιουργείται τυχαία σε τεμάχια σε όλο το μητρώο για το τοπικό σύστημα. Ένας διαχειριστής μπορεί να reconfigure το Syskey έτσι ώστε να φυλάσσεται το τυχαίο κλειδί σε μια δισκέτα, αντί στο τοπικό σύστημα ή να καθορίσετε έναν κωδικό πρόσβασης διαχειριστή, που έχει επιλεχθεί ως κλειδί[42]. Το σύστημα τότε δεν θα μπορεί να ξεκινήσει χωρίς την εισαγωγή του αφαιρούμενου μέσου ή χωρίς πληκτρολογώντας τον καθορισμένο κωδικό πρόσβασης, αντίστοιχα.

3.1.5 Storage Device Sanitization and Disposal

Οι οργανισμοί θα πρέπει να ελέγχουν σωστά όλες τις συσκευές αποθήκευσης, συμπεριλαμβανομένων των σταθερών συσκευών (π.χ. σκληροί δίσκοι) καθώς και τα κινητά συστήματα και τα μέσα ενημέρωσης (π.χ. οπτικοί δίσκοι, μαγνητικοί δίσκοι, flash memory), πριν από την επαναχρησιμοποίηση τους ή τη διάθεση τους. Εάν στις συσκευές αποθήκευσης δεν είναι σωστά επεξεργασμένα τα δεδομένα, στις πληροφορίες θα μπορούσαν να έχουν πρόσβαση χωρίς άδεια. Τα Windows XP περιλαμβάνουν ένα βοηθητικό πρόγραμμα γραμμής εντολών που ονομάζεται cipher που προορίζεται για τη χρήση με το EFS σύστημα, αλλά μπορεί επίσης να χρησιμοποιηθεί ανεξάρτητα από το EFS σύστημα σε θαμνώδη δεδομένα από αχρησιμοποίητα τμήματα των δίσκων[43]. Με τη χρήση του / w διακόπτη, ένας διαχειριστής μπορεί να χρησιμοποιήσει το cipher να περάσει τρεις . Αν και αυτό μπορεί να είναι βολικό σε ορισμένες περιπτώσεις, γενικά συνιστάται να αποκτήσει έναν τρίτο εργαλείο που μπορεί να κάνει τουλάχιστον επτά όταν περνά η αντικατάσταση δεδομένων. Εναλλακτικές λύσεις για την αντικατάσταση δεδομένων περιλαμβάνετε το καλώδιο και η φυσική καταστροφή των συσκευών αποθήκευσης. [44] Ανεξάρτητα από τη μέθοδο που έχει επιλεγεί, οι οργανισμοί θα πρέπει να διατηρούν ένα αρχείο καταγραφής που θα παραθέτει κάθε συσκευή να καθαρίζεται και πώς τα στοιχεία των εγγράφων έχουν αφαιρεθεί.

---

[41] Η Microsoft προτείνει να χρησιμοποιείτε Syskey με EFS in *Encrypting File System in Windows XP and Windows Server 2003*, βρίσκεται στη σελίδα http://technet.microsoft.com/en-us/library/bb457065.aspx.

[42] Για περισσότερες πληροφορίες για την αλλαγή των modes του Syskey είναι διαθέσιμα στο άρθρο MSKB 143475 στη σελίδα http://support.microsoft.com/?id=143475.

[43] Για περισσότερες πληροφορίες σχετικά με τη κρυπτογράφηση των δεδομένων για να καταργήσετε το βοηθητικό πρόγραμμα , ανατρέξτε στο άρθρο με τίτλο *Encrypting File System in Windows XP and Windows Server 2003*, το οποίο είναι διαθέσιμο στη σελίδα http://technet.microsoft.com/en-us/library/bb457065.aspx.

[44] Για περισσότερες πληροφορίες για το sanitizing , καλώδιο και τη καταστροφή συσκευών αποθήκευσης είναι διαθέσιμα από το the Department of Defense's *National Industrial Security Program Operating Manual*, DoD 5220.22-M, όπου βρίσκεται στη σελίδα http://www.dtic.mil/whs/directives/corres/html/522022m.htm, και από το NIST SP 800-88, *Guidelines for Media Sanitization*, located at http://csrc.nist.gov/publications/PubsSPs.html.

3.2 User Accounts and Groups

Το τμήμα αυτό ασχολείται με τη σημασία της διασφάλισης των λογαριασμών των χρηστών και των ομάδων. Στα Windows XP εγκαθιστάς πολλούς λογαριασμούς χρηστών από προεπιλογή. Για να αποφεύγεται τη κακή χρήση των λογαριασμών αυτών, θα πρέπει να απενεργοποιηθεί ή να αντικατασταθεί με ισοδύναμο λογαριασμό. Επιπλέον, σε επίπεδο διοικητικών λογαριασμών θα πρέπει να χρησιμοποιούνται μόνο για το σύστημα διαχείρισης εργασιών, πράγμα που σημαίνει ότι τουλάχιστον ένα χρήστης στο επίπεδο αυτό πρέπει να δημιουργηθεί για την καθημερινή λειτουργία του συστήματος. Ένα άλλο σημαντικό έργο είναι να δημιουργήσετε μια δισκέτα επαναφοράς του κωδικού πρόσβασης, το οποίο μπορεί να χρησιμοποιηθεί για να τον ανακτήσει ο διαχειριστής επιπέδου για τη πρόσβαση στο σύστημα, εάν ο κωδικός πρόσβασης του διαχειριστή είναι ξεχασμένος. Η δισκέτα επαναφοράς του κωδικού πρόσβασης θα πρέπει να αποθηκεύεται σε μια ασφαλή θέση. (Η χρήση των δίσκων επαναφοράς κωδικού πρόσβασης δεν συνιστάται για τη διαχείριση σε περιβάλλοντα.) Στο τμήμα αυτό θα συζητήσουμε κάθε ένα από αυτά τα θέματα.

3.2.1 Built-in Accounts

Οι προκαθορισμένοι λογαριασμοί χρηστών χρησιμοποιούνται συχνά σε εκμετάλλευση κατά διαφόρων συστημάτων των ηλεκτρονικών υπολογιστών, συμπεριλαμβανομένων των Windows XP. Απενεργοποιώντας την προεπιλογή των λογαριασμών των χρηστών, θα είναι πιο δύσκολο για τους επιτιθέμενους να αποκτήσουν πρόσβαση σε έναν υπολογιστή. Αυτό δεν είναι μια αλάνθαστη λύση, αλλά αυτό θα αποθαρρύνει ορισμένους επιτιθέμενους οι οποίοι θα προτιμούσουν να αναζητούν εύκολους στόχους. Ο Guest λογαριασμός ιστορικά έχει ένα κοινό μέσο με το οποίο μπορούν να αποκτήσουν απομακρυσμένη πρόσβαση σε έναν υπολογιστή, αλλά είναι απενεργοποιημένη από προεπιλογή στα Windows XP. Μόλις ένας εισβολέας έχει εισβάλει στο Guest σε επίπεδο πρόσβασης, ο εισβολέας μπορεί να επιχειρήσει να ανυψώσει τα προνόμιά του για την περαιτέρω αξιοποίηση της μηχανής. Οι εισβολείς επίσης προσπαθούν να χρησιμοποιούν τον προεπιλεγμένο λογαριασμό του Administrator, έτσι ώστε ορισμένοι οργανισμοί μπορούν να επιλέξουν να δημιουργήσουν ένα νέο λογαριασμό διοικητικού επιπέδου με προνόμια και στη συνέχεια να απενεργοποιήσουν το αρχικό λογαριασμό Administrator. Κανονικά, ο λογαριασμός του χρήστη έχει δημιουργηθεί κατά την εγκατάσταση του διοικητικού επιπέδου με προνόμια, αλλά αυτό θα πρέπει να εξακολουθήσει να επαληθεύεται[45]. NIST συνιστά οι ενσωματωμένοι λογαριασμοί Administrator και

[45]Στη διαχείριση περιβάλλοντος , είναι κοινό για τη ασφάλεια και μόνο οι διαχειριστές συστήματος να έχουν πρόσβαση σε επίπεδο διαχειριστή του συστήματος και για να μην έχει κανείς guest επίπεδο πρόσβασης. Οι

Guest να απενεργοποιηθούν και να μετονομαστούν σε όλα τα συστήματα των Windows XP[46]. Αυτό μπορεί να γίνει με την τροποποίηση των προτύπων ασφαλείας του NIST ή τα GPO και να απορρίψουν τις ρυθμίσεις που ορίζονται ως πολιτική. Για να πραγματοποιήσετε τις αλλαγές αυτές χειροκίνητα, ακολουθήστε τα παρακάτω βήματα:

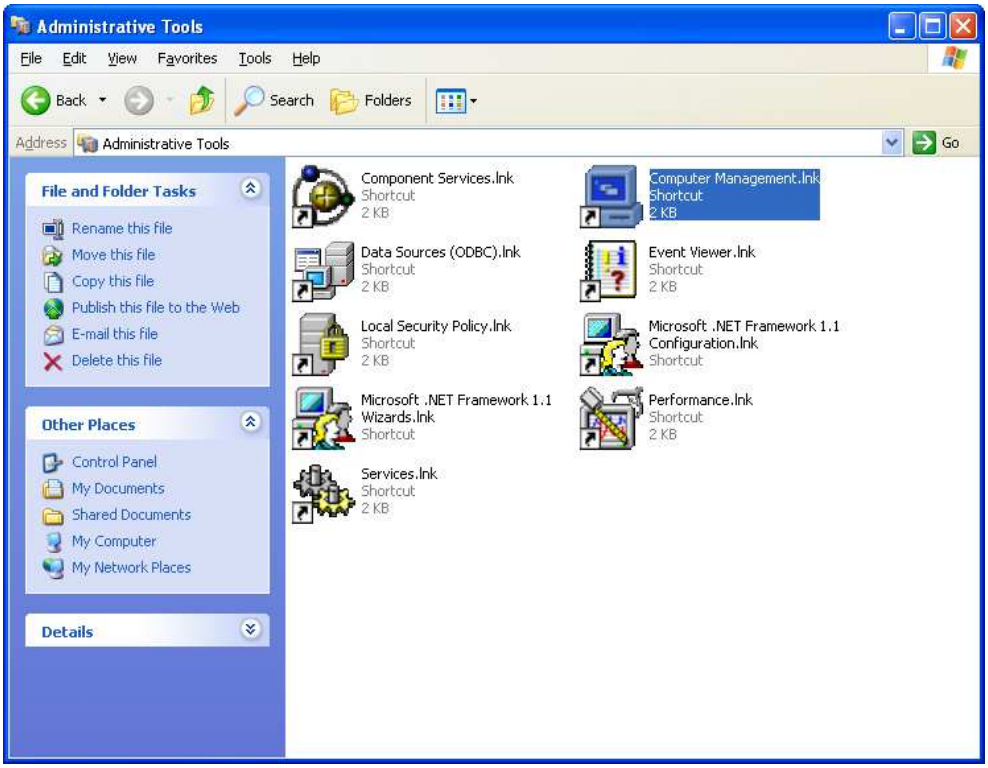
1. Πατήστε **Start** στο μενού και επιλέξτε **Control Panel**. Διπλό κλικ στο φάκελο **Administrative Tools**.

Εικόνα 138: Administrative tools

2. Διπλό κλικ στη συντόμευση **Computer Management**.

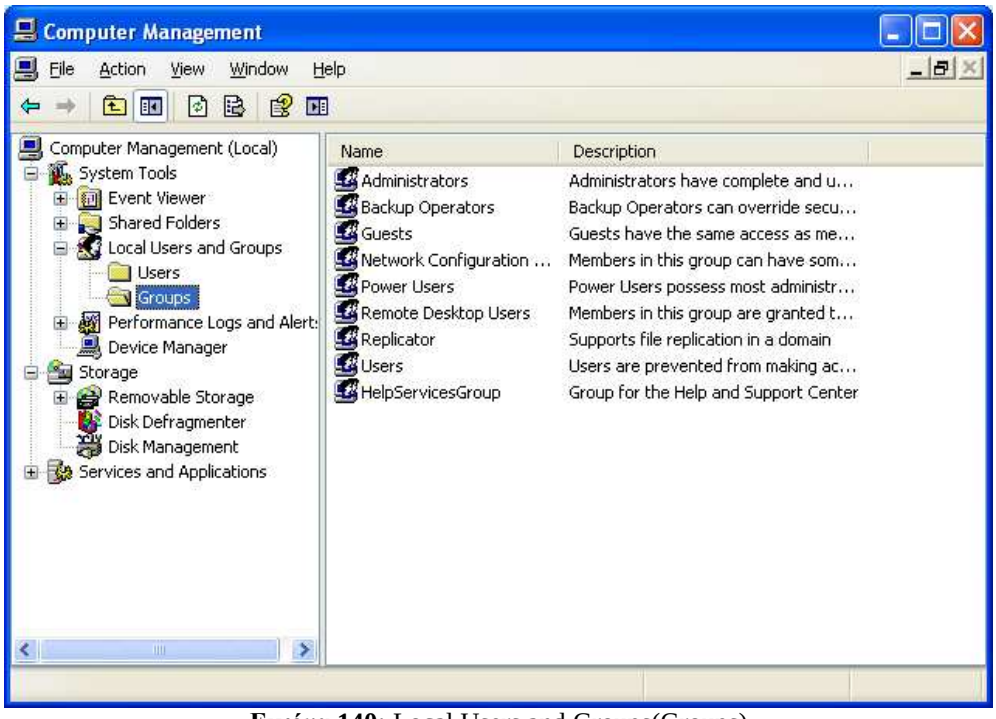
χρήστες πρέπει να ενημερώνονται με ότι μπορούν και με ότι δε μπορούν να κάνουν στα δικά τους συστήματαα (π.χ. εγκατάσταση λογισμικού) και οδηγίες για το πώς να ζητήσουν αλλαγές που απαιτούν σε επίπεδο πρόσβασης διαχειριστή.

[46] Ακόμα και αν ο built-in Administrator λογαριασμός είναι απενεργοποιημένος, μπορεί ακόμα να χρησιμοποιηθεί για συνδεθείτε με το σύστημα αν αυτό κάνει εκκίνηση με Safe Mode.



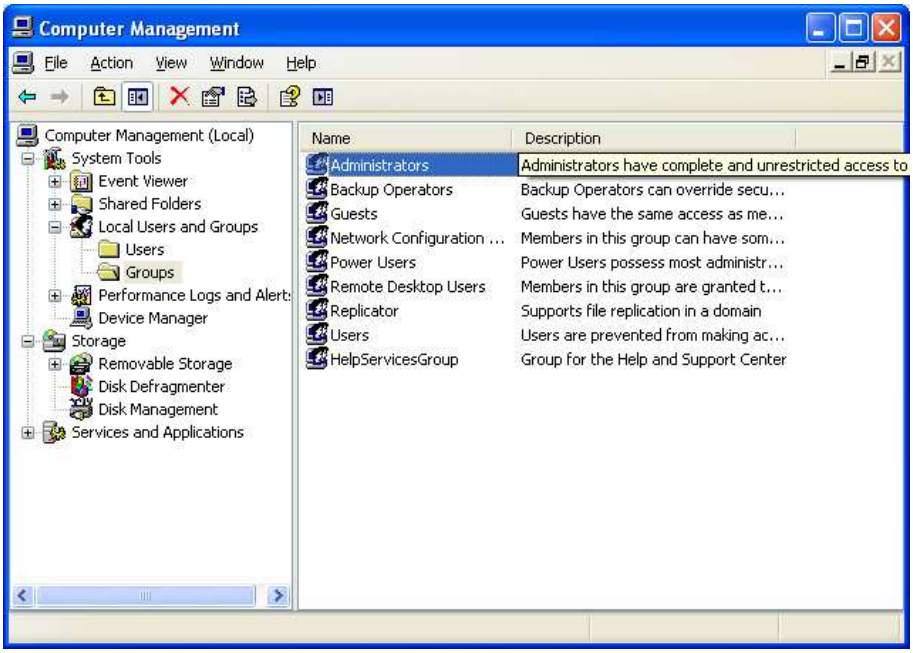
Εικόνα 139: Computer Management

3. Επεκτείνετε το **Local Users and Groups** και επιλέξτε το φάκελο **Groups** .



Εικόνα 140: Local Users and Groups(Groups)

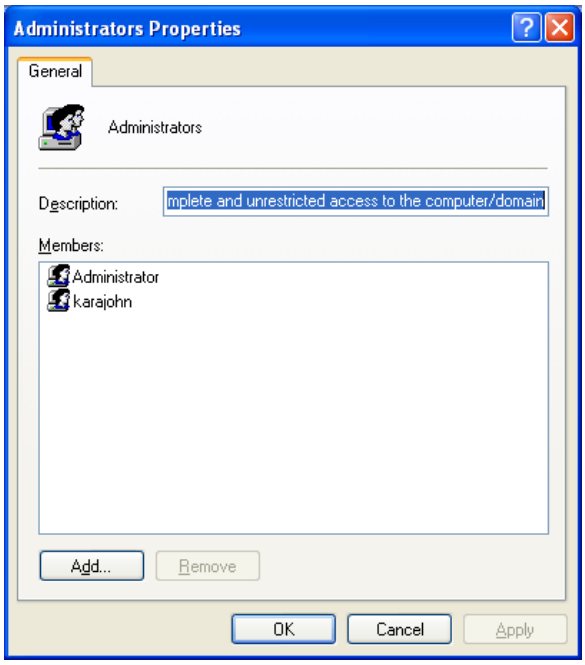
4. Ο κατάλογος των ομάδων θα πρέπει να εμφανίζεται στο δεξιό τμήμα του. Διπλό κλικ στη ομάδα **Administrators**.



Εικόνα 141: Administrators

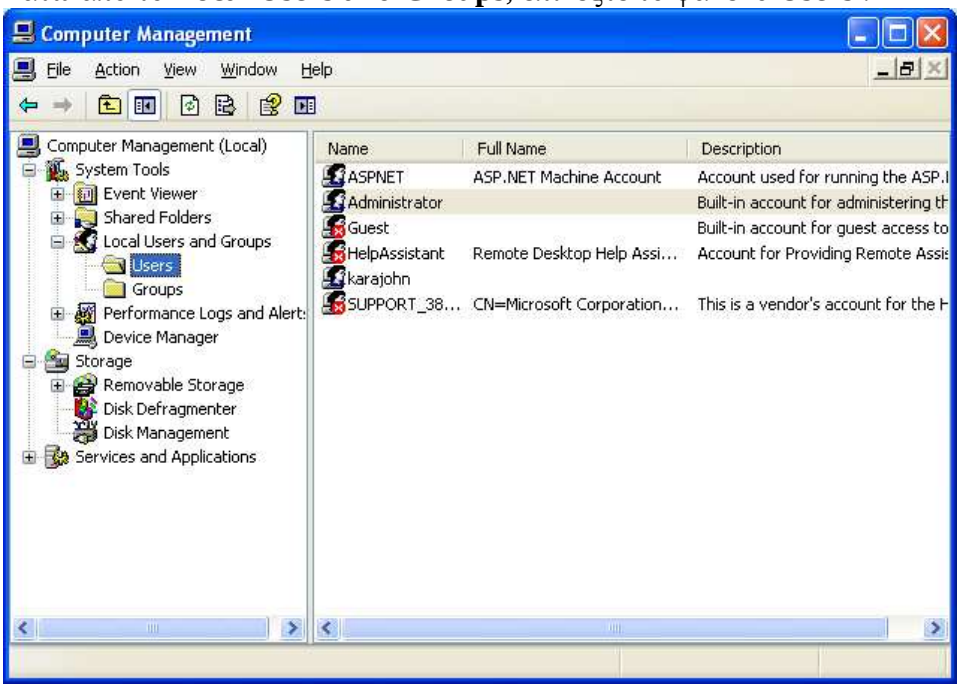
Επιβεβαιώστε ότι η ομάδα αποτελείται από μόνο δύο λογαριασμούς: το ενσωματωμένο λογαριασμό Administrator και το λογαριασμό που χρησιμοποιείται για να σκληρύνει το σύστημα. Αν ο λογαριασμός του χρήστη δεν είναι παρών, δημιουργήσετε ένα λογαριασμό χρήστη και προσθέσετε τον στην ομάδα Administrators.

5. Μη απενεργοποιήσετε το λογαριασμό Administrator μέχρι ο λογαριασμός του χρήστη προστεθεί στην ομάδα Administrators. Μετά την ολοκλήρωσή του, η ομάδα Administrators θα πρέπει να περιλαμβάνει μόνο από δύο λογαριασμούς. Κάντε κλικ στο κουμπί OK για να συνεχίσετε..



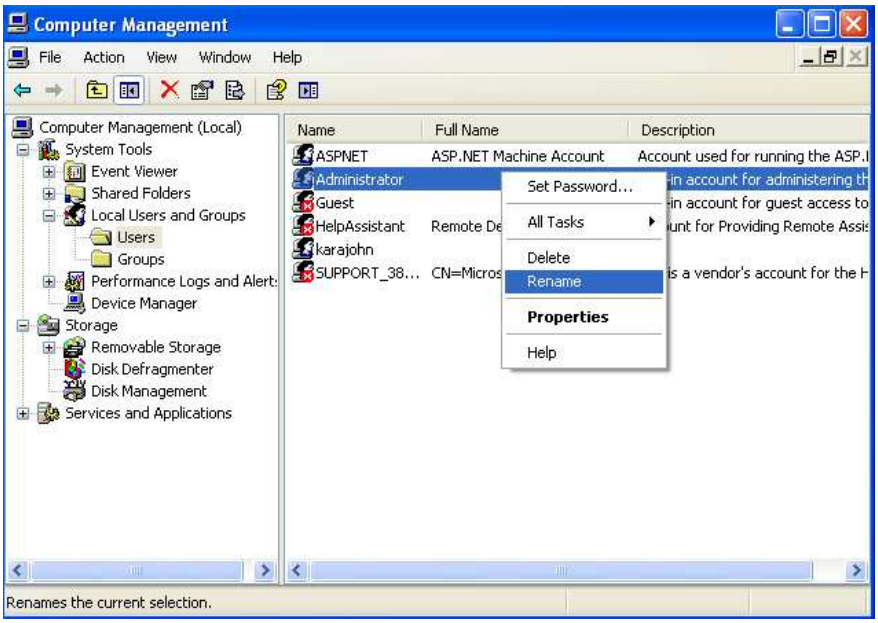
Εικόνα 142: Administrators Properties

6. Κάτω από το **Local Users and Groups**, επιλέξτε το φάκελο **Users** .



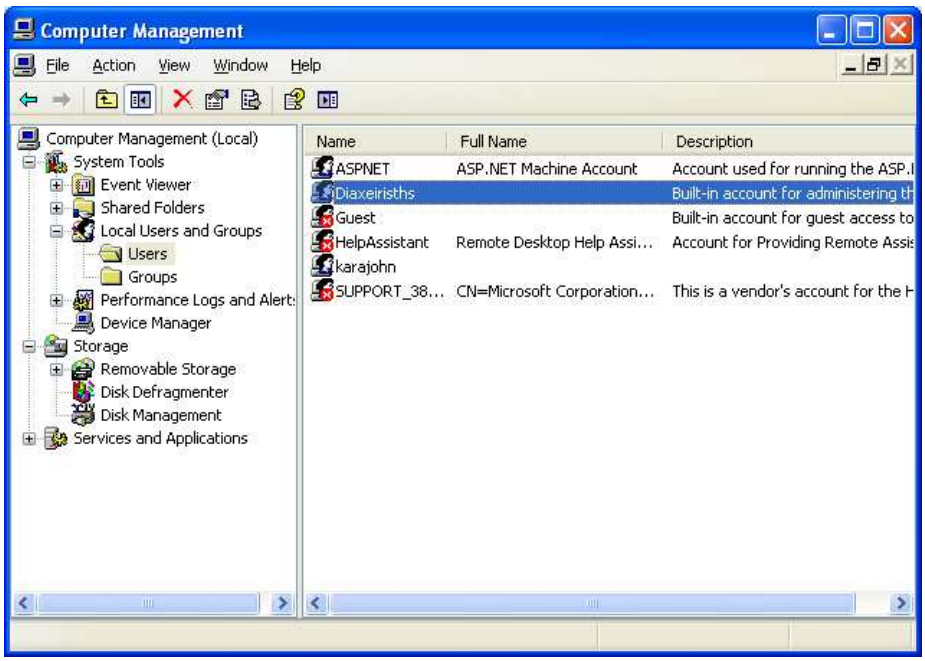
Εικόνα 143: Local Users and Groups(Users)

7. Κάντε δεξί κλικ στο λογαριασμό Administrator, πατήστε μετονομασία και πληκτρολογήστε το νέο όνομα. Δημιουργώντας σχετικά ένα ασαφή όνομα για το λογαριασμό έτσι ώστε να το καθιστά λιγότερο πιθανό να είναι στοχοθετημένο από έναν εισβολέα.



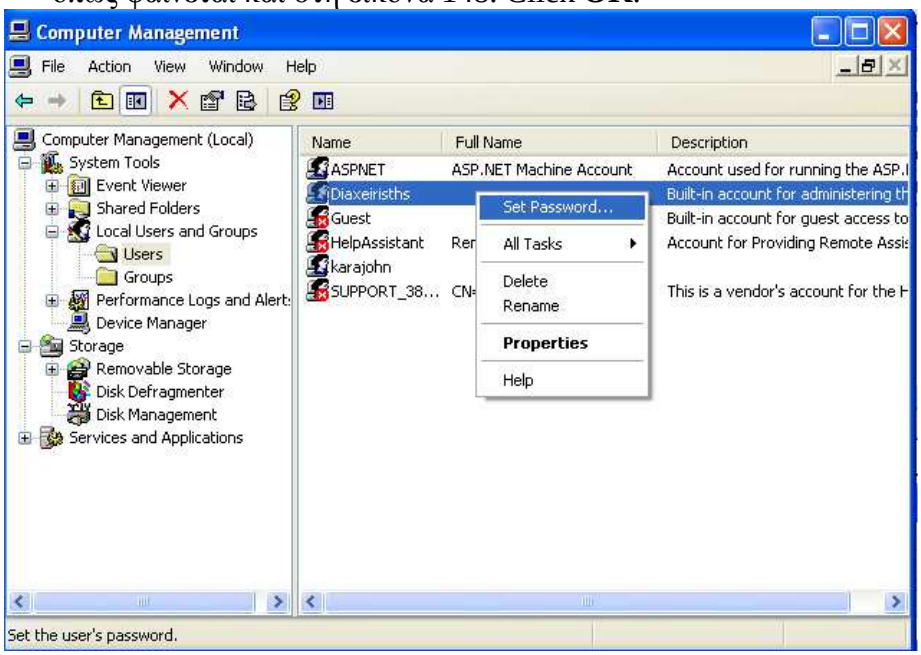
Εικόνα 144: Administrator Rename

Αλλάξαμε το όνομα από Administrator σε Diaxeiristh.



Εικόνα 145: Diaxeirisths

8. Κάντε δεξί κλικ και μετονομάστε το λογαριασμό του διαχειριστή επιλέξτε **Set Password** και χορηγήστε ένα ισχυρό κωδικό πρόσβασης που να αποτελείται από ένα μείγμα από χαραχτήρες ειδικά από κεφαλαίους και πεζούς χαραχτήρες όπως φαίνεται και στη εικόνα 148. Click **OK**.



Εικόνα 146: Diaxeirisths Set Password

Εικόνα 147: Set Password for Diaxeirisths

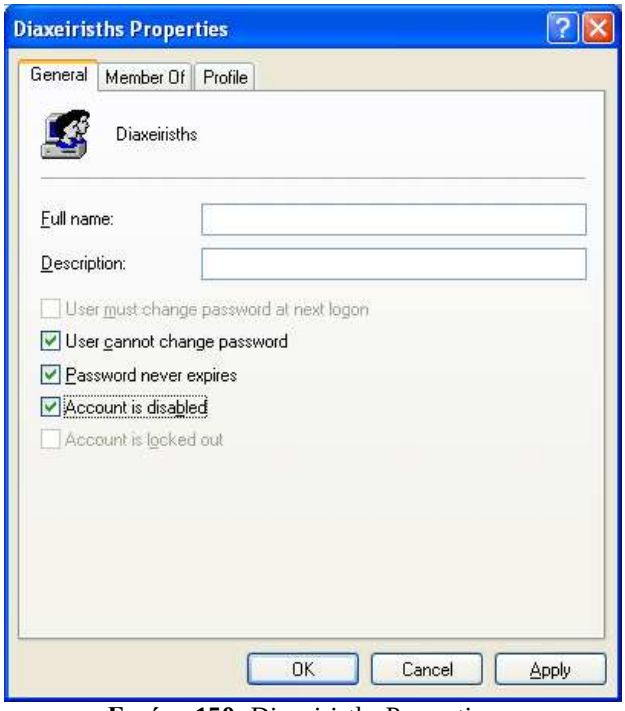
Εικόνα 148: New Password For Diaxeirisths

Εικόνα 149: The password has been set

9. Κάντε διπλό κλικ στο μετονομασμένο λογαριασμό του διαχειριστή και διαγράψτε τη περιγραφή του πεδίου ή βάλτε μια νέα περιγραφή. Βεβαιωθείτε ότι ο **User cannot change password**(Ο χρήστης δε μπορεί να αλλάξει το κωδικό), **Password never expires**(ο κωδικός ποτέ να μην λήγει) και **Account is disabled**(απενεργοποιημένος ο λογαριασμός)είναι επιλεγμένα τα κουτιά. Πατήστε **OK**.

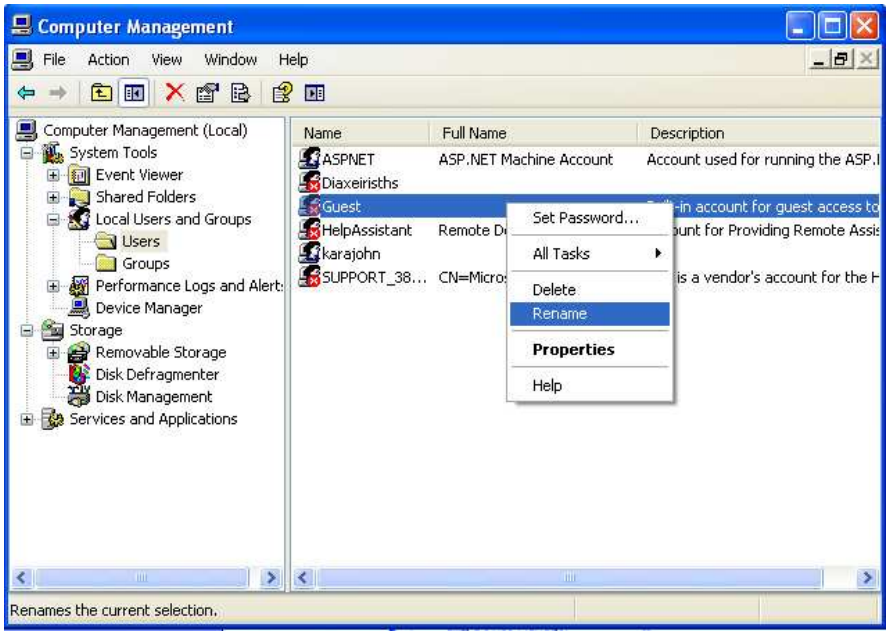
Σχετικά με αυτό το βήμα θα ήθελα να σας αναφέρω τη εμπειρία που πέρασα.

Όταν μετά από όλες αυτές τις ρυθμίσεις που είχα εγκαταστήσει στο υπολογιστή μου ,του έκανα επανεκκίνηση και όταν έφτασε η ώρα να βάλω το κωδικό έτσι ώστε να μπω στα Windows διαπίστωσα ότι δε μπορούσα να μπω με τίποτα και με κανένα άλλο κωδικό ή χρήστη(διότι τις ίδιες ρυθμίσεις έκανα και στο guest), διότι ο λογαριασμός μου ήταν απενεργοποιημένος και επίσης ο λογαριασμός αυτός ήταν του administrator. Έτσι σκέφτηκα ότι αυτό που μπορώ να κάνω ήταν να μπω στα Windows με τη μέθοδος safe mode(Επανεκκίνηση του υπολογιστή και πατημένο το πλήκτρο F8) και να ενεργοποιήσω το λογαριασμό μου ξανά έτσι ώστε να συνεχίσω να εγκαθιστώ τις ρυθμίσεις της μεθολογίας.



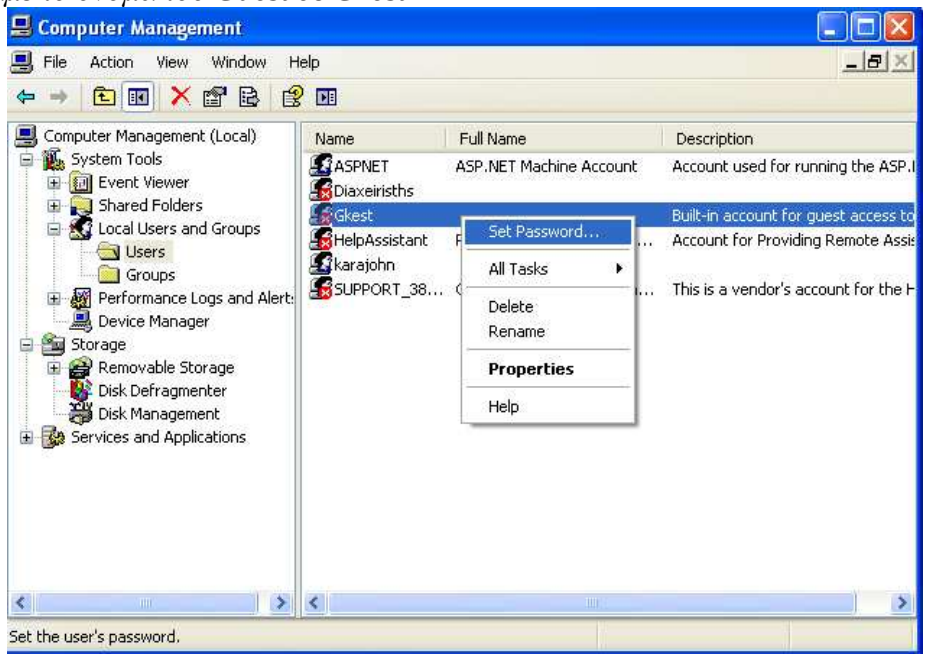
Εικόνα 150: Diaxeirisths Properties

10. Μετονομάστε το λογαριασμό του Guest και θέστε ένα ισχυρό κωδικό πρόσβασης για το προεπιλεγμένο λογαριασμό του guest, που να αποτελείται από ψηφία, ειδικούς, κεφαλαίους και πεζούς χαρακτήρες.

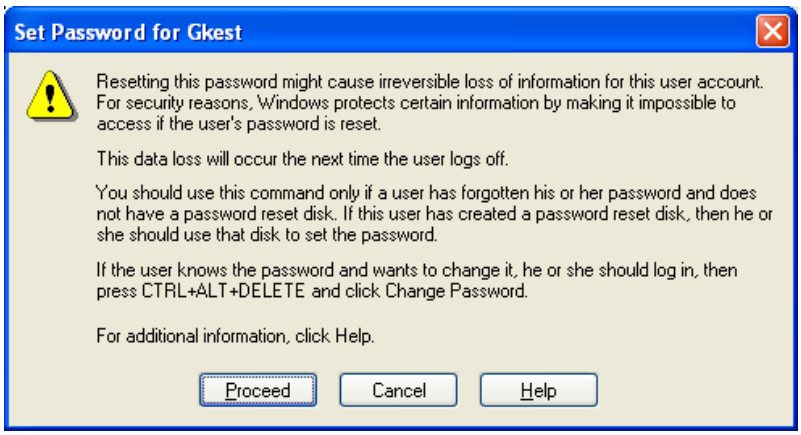


Εικόνα 151: Guest Rename

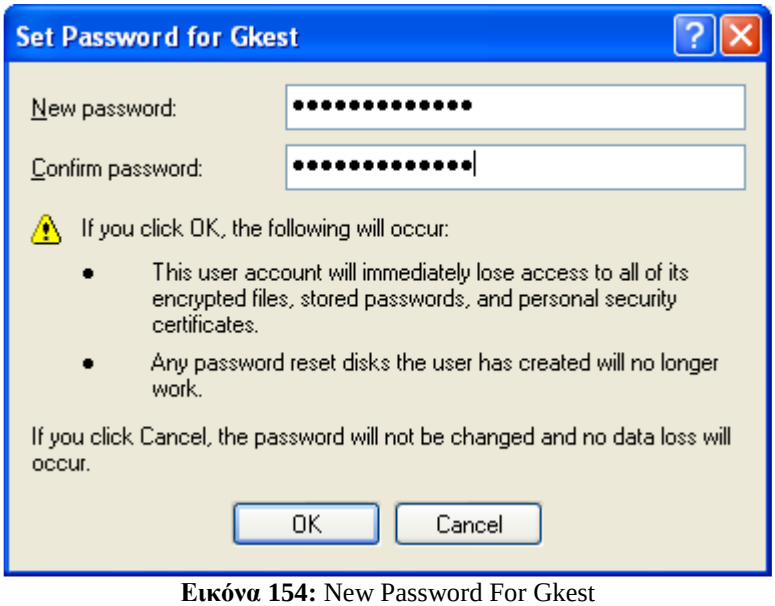
Αλλάξαμε το όνομα του Guest σε Gkest



Εικόνα 152: Gkest Set Password



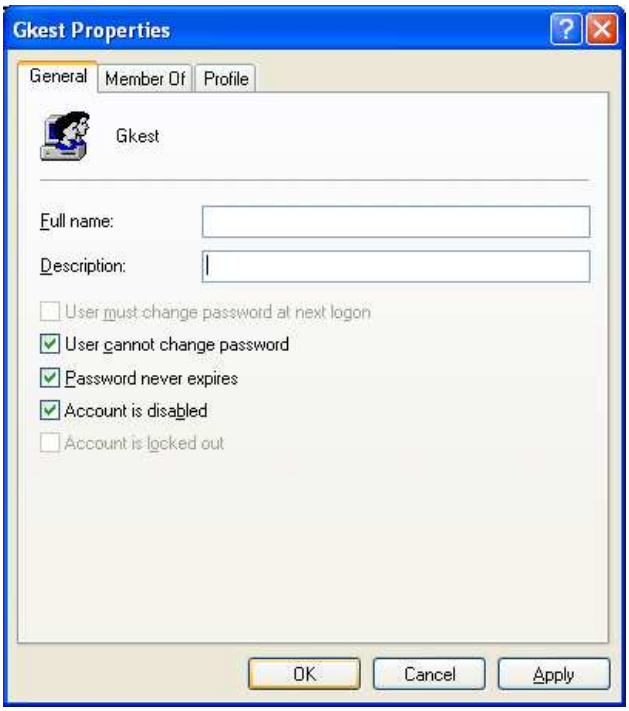
Εικόνα 153: Set Password for Gkest



Εικόνα 154: New Password For Gkest

Εικόνα 155: Gkest Password Has Been set

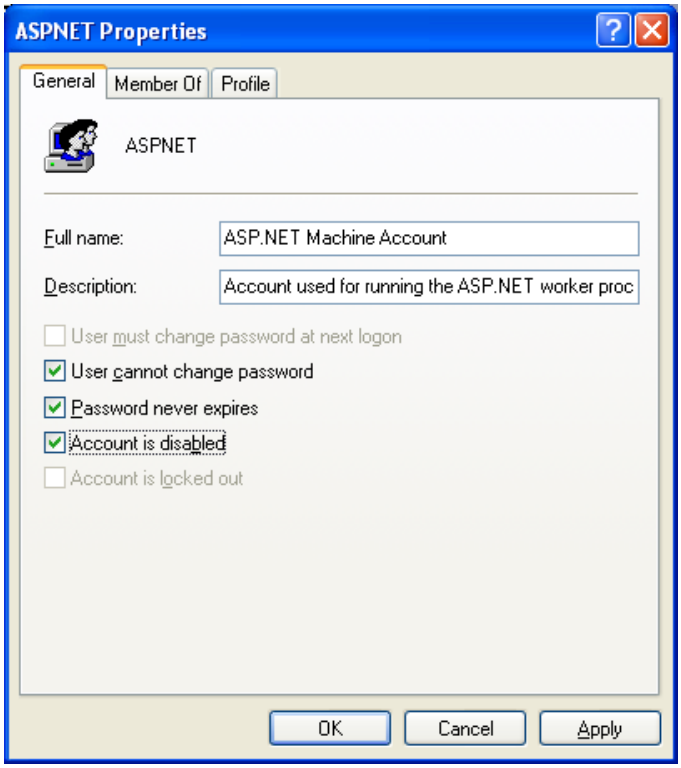
11. Κάντε διπλό κλικ στο λογαριασμό Guest που μετονομάστηκε επαληθεύσετε ότι ο χρήστης δεν μπορεί να αλλάξει τον κωδικό πρόσβασης(**User cannot change password**), τον κωδικό ποτέ να μην λήγει(**Password never expires**) και λογαριασμός να έχει απενεργοποιηθεί(**Account is disabled**) τα κουτιά είναι επιλεγμένα. Διαγράψτε τη περιγραφή του πεδίου ή πληκτρολογήστε μια νέα περιγραφή. Κάντε κλικ στο **OK**.



Εικόνα 156: Gkest Properties

12. Απενεργοποιήστε όλα τους άλλους ενσωματωμένους λογαριασμούς που δεν είναι απαραίτητοι. Ο πίνακας 2 παραθέτει όλους τους προεπιλεγμένους λογαριασμούς των Windows XP[47]. Για κάθε λογαριασμό, κάντε δεξί κλικ πάνω του, επιλέξτε **Properties**, επιλέξτε το λογαριασμό που είναι απενεργοποιημένο το πλαίσιο του **(Account is disabled)** και κάντε κλικ στο **OK**.

[47] Σε συστήματα των Windows, κάθε λογαριασμός του χρήστη συνδέεται με ένα μοναδικό αναγνωριστικό ασφαλείας (SID). Κάθε SID είναι μια ακολουθία γραμμάτων και ψηφιών που μπορούν για να χρησιμοποιηθούν για το εντοπισμού λογαριασμών που συνδέονται , ακόμη και αν το όνομα του χρήστη έχει αλλάξει. Για παράδειγμα, SID S-1-5-*domain*-500 χρησιμοποιείται από το λογαριασμό του διαχειριστή; Ακόμα και αν ο διαχειριστής μετονομαστεί, το SID παραμένει το ίδιο. Για περισσότερες πληροφορίες για τους λογαριασμούς των χρηστών Windows XP, συμπεριλαμβανόμενων των αναγνωριστικών ασφαλείας , διαθέσιμο από το άρθρο MSKB 243330 στη σελίδα http://support.microsoft.com/?id=243330.



Εικόνα 157: ASPNET Properties

User Account Name	Description	Default SID
Administrator	Ενσωματώνει λογαριασμό του υπολογιστή / του κύριου διαχειριστή	S-1-5-domain-500
Guest	Ενσωματώνει λογαριασμό για το guest για την πρόσβαση στον υπολογιστή / τομέα	S-1-5-domain-501
HelpAssistant	Λογαριασμός που απαιτείται για την παροχή βοήθειας για τον απομακρυσμένο υπολογιστή	N/A (variable)
SUPPORT_388945a0	Λογαριασμός για βοήθεια και υπηρεσία υποστήριξης	N/A (variable)
User-Created install account	Λογαριασμός αρχικός που δημιουργήθηκε κατά τη διάρκεια της εγκατάστασης	N/A (variable)

Πίνακας 2: Λογαριασμοί των Windows XP

NIST συνιστά οι διαχειριστές να επανεξετάζουν περιοδικά τους λογαριασμούς των χρηστών και να απενεργοποιούν αυτούς που είναι ανενεργές για 90 ημέρες, όπως επίσης και την προσωρινή απενεργοποίηση λογαριασμών μετά από 30 ημέρες. Οι οργανισμοί θα πρέπει επίσης να ακολουθούν διαδικασίες για την απενεργοποίηση

των λογαριασμών από τη στιγμή που δεν χρειάζονται πλέον (π.χ. όταν ο χρήστης αφήνει την οργάνωση, οι αρμοδιότητες του χρήστη αλλάζουν).Οι απενεργοποιημένοι λογαριασμοί θα πρέπει να διαγράφονται μετά από μια συγκεκριμένη χρονική περίοδο για την αποδέσμευση πόρων και την αποτροπή περιττών λογαριασμών έτσι ώστε να μην ενεργοποιηθούν ξανά τυχαία.

3.2.2 Built-in Groups

Τα Windows XP έχουν πολλές ομάδες που είναι γνωστές ως ειδικές ομάδες. των Windows XP όπου διαχειρίζονται από τα μέλη αυτόματα από τις ομάδες αυτές. Δύο ειδικές ομάδες που παρουσιάζουν ιδιαίτερο ενδιαφέρον από πλευράς ασφαλείας είναι: **Authenticated Users** και **Everyone**. **Authenticated Users** περιλαμβάνουν όλους τους λογαριασμούς (με εξαίρεση το Guest και τους Anonymous λογαριασμούς) που έχουν πιστοποιηθεί. Όλοι περιλαμβάνουν όλους τους τοπικούς και κύριους βασικούς λογαριασμούς που έχουν πρόσβαση στο σύστημα. Σε προηγούμενες εκδόσεις των Windows, οι χρήστες Anonymous συμπεριλαμβανόντουσαν στην ομάδα Everyone, η οποία δίνει συχνά παράνομη πρόσβαση στα συστήματα των χρηστών. Στα Windows XP, οι Anonymous συνδέσεις δεν είναι πλέον μέρος της ομάδας Everyone.

Από προεπιλογή, τα Windows XP περιλαμβάνουν επίσης πολλές τοπικές ομάδες. Οι τοπικές ομάδες διαφέρουν από τις ειδικές ομάδες, επειδή οι διαχειριστές μπορούν να διαχειρίζονται τα μέλη της κάθε τοπικής ομάδα, αλλά δεν μπορούν να αλλάζουν τη σύνθεση των ειδικών ομάδων. Ο πίνακας 3 περιγράφει κάθε τοπική ομάδα, εξηγεί τα δικαιώματα που έχουν σε σχέση με την ομάδα και τους καταλόγους των λογαριασμών που ανήκουν στην προεπιλεγμένη ομάδα .

Group Name	Description
Administrators	Οι διαχειριστές έχουν τη πλήρη και τη ανεμπόδιστη πρόσβαση στον υπολογιστή. Η προεπιλογή των μελών της ομάδας αυτής είναι ενσωματωμένο στο λογαριασμό του Administrator και το λογαριασμό που είχε αρχικά δημιουργηθεί για την εγκατάσταση. Μόνο οι λογαριασμοί που απαιτούνται πρόσβαση σε επίπεδο διαχειριστή θα πρέπει να είναι μέλη αυτής της ομάδας.
Back Operators	Η ομάδα αυτή μπορεί να υπερισχύει των περιορισμών ασφάλειας με μοναδικό σκοπό την υποστήριξη και την αποκατάσταση των αρχείων, συμπεριλαμβανομένων των αρχείων που προστατεύονται από το σύστημα EFS. Δεν υπάρχουν προεπιλεγμένα μέλη αυτής της ομάδας. Οι χρήστες που έχουν κάνει backup τα δεδομένα τους δεν θα πρέπει να συμμετέχουν σε αυτήν την ομάδα; Η ομάδα πρόκειται να χρησιμοποιηθεί από ένα αντίγραφο ασφαλείας του διαχειριστή ή από μια αυτοματοποιημένη διαδικασία δημιουργίας αντιγράφων ασφαλείας για τη διατήρηση και όλων των τυχόν στοιχείων σχετικά με το σύστημα, ανεξάρτητα από τις άλλες προστασίες ασφάλειας. Μόνο έμπιστοι χρήστες παρέχουν τέτοιες διαδικασίες ασφαλείας και

	αυτοί πρέπει να τοποθετούνται σε αυτή την ομάδα.
Guests	Αυτή η ομάδα έχει την ίδια πρόσβαση με την ομάδα Users, Εκτός από το ότι οι Guests δεν μπορούν να δουν τα αρχεία καταγραφής του OS. Ο λογαριασμός Guest είναι το μόνο προεπιλεγμένο μέλος αυτής της ομάδας.
HelpServicesGroup	Οι χρήστες αυτής της ομάδας μπορεί να αντιμετωπίσουν προβλήματα με τη χρήση ορισμένων υπηρεσιών κοινής ωφελείας. Οι χρήστες μπορούν να συνδέονται τοπικά εξ αποστάσεως με το σύστημα. Η Υποστήριξη υπόψη είναι το μόνο μέλος του ομίλου από προεπιλογή. Μόνο οι λογαριασμοί που χρησιμοποιούνται για την παροχή υποστήριξης θα πρέπει να ανήκουν σε αυτή την ομάδα.

Πίνακας 3: Περιγραφή Ομάδων

Group Name	Description
Network Configuration Operators	Τα μέλη της ομάδας αυτής έχουν δικαιώματα διαχειριστή για τη διαχείριση των ρυθμίσεων και για τη δικτύωση των χαρακτηριστικών. Δεν υπάρχουν προεπιλεγμένα μέλη αυτής της ομάδας.
Power Users	Στην ομάδα αυτή έχουν χορηγηθεί κάποια διοικητικά προνόμια. Ο σκοπός αυτής της ομάδας είναι να δώσει στους Power Users δικαιώματα όπου χρήστες δεν έχουν, έτσι ώστε Power Users να μπορούν να τρέχουν εφαρμογές. Ωστόσο, οι Power Users μπορούν συχνά αλλάζουν το περιορισμό των δικαιωμάτων τους ώστε να αποκτήσουν πλήρη δικαιώματα διαχειριστή. Δεν υπάρχουν προεπιλεγμένα τα μέλη αυτής της ομάδας. Το NIST συνιστά ιδιαίτερα ότι η ομάδα Power Users δεν μπορεί να χρησιμοποιηθεί και ότι τα προνόμια που παρέχονται με τους καθιερωμένους χρήστες να προσαρμοσθούν ελαφρώς εάν είναι αναγκαίο για να αντισταθμιστεί η κάθε αίτηση κληρονομιάς.
Remote Desktop Users	Αυτή η ομάδα έχει τα δικαιώματα για να συνδεθείτε με τον υπολογιστή από απόσταση, μέσω Remote Desktop Services. Δεν υπάρχουν προεπιλεγμένα μέλη αυτής της ομάδας. Μόνο οι χρήστες που χρειάζονται να έχουν πρόσβαση στο σύστημα μέσω της Remote Desktop θα πρέπει να ανήκουν σε αυτή την ομάδα.
Replicator	Η ομάδα αυτή είχε χρησιμοποιηθεί στον Windows NT 4.0 για να υποστηρίξει την αντιγραφή αρχείων στο τομέα διαμόρφωσης. Δεν χρησιμοποιείται στα Windows XP; Δεν υπάρχουν προεπιλεγμένα μέλη αυτής της ομάδας, και θα πρέπει να παραμείνει άδεια.
Users	Η ομάδα αυτή έχει περιορισμένα δικαιώματα που θα πρέπει να αποτρέπονται από τα μέλη από την οποία γίνεται η αλλαγή της στάση ασφάλειας του συστήματος. Οι χρήστες έχουν επαρκή δικαιώματα για να εκτελέσουν τα καθήκοντα που τους επιτρέπονται, αλλά δεν

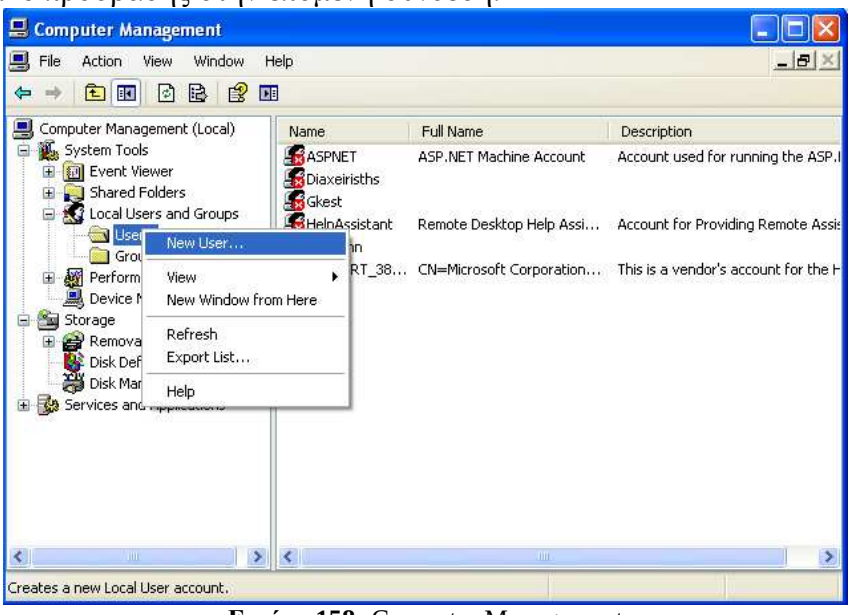
	αρκούν, για να αποκτήσουν πρόσβαση σε άλλα δεδομένα των χρηστών ή να καταστρέψουν εφαρμογές άλλων χρηστών. Τα προεπιλεγμένα μέλη αυτής της ομάδας είναι όλοι Authenticated Users και INTERACTIVE χρήστες. Επιπλέον, όταν ένας νέος λογαριασμός χρήστη δημιουργήθηκε με τον προκαθορισμένο τύπο του λογαριασμού Limited, τοποθετείται στην ομάδα Users. Όλοι οι χρήστες που έχουν κύρια ανάγκη τη πρόσβαση στο δίκτυο θα πρέπει να τοποθετηθούν στην ομάδα Users.

Πίνακας 4: Περιγραφή Ομάδων(2)

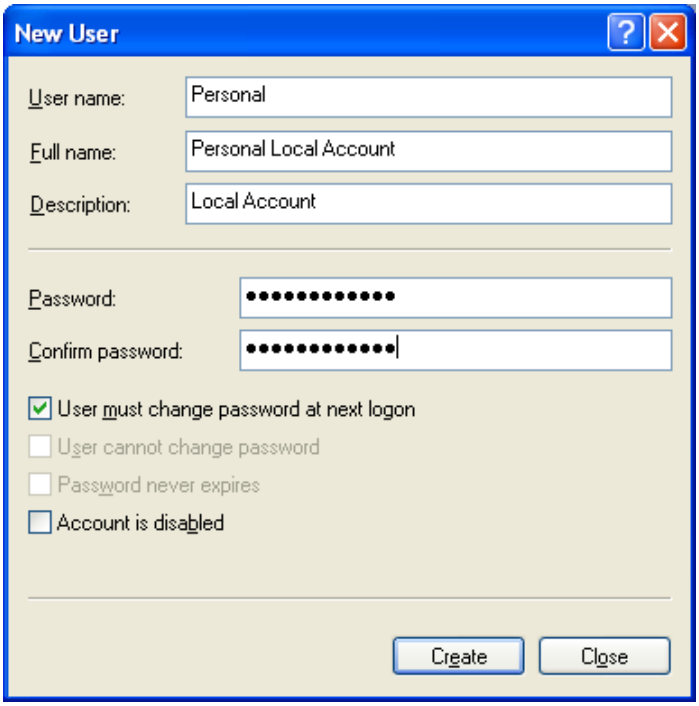
3.2.3 Daily Use Accounts

Συνιστάται ιδιαίτερα ότι ένας πρόσθετος λογαριασμός που ανήκει μόνο στην ομάδα Users μπορεί να δημιουργηθεί για κάθε χρήστη και χρησιμοποιείται για να λειτουργεί σε καθημερινή βάση (π.χ. έλεγχος του ηλεκτρονικού ταχυδρομείου, περιήγηση στο Web, για λειτουργικές εφαρμογές αυτοματισμού γραφείου). Ο εν λόγω λογαριασμός είναι γνωστός για καθημερινή ή για περιορισμένη χρήση. Λογαριασμοί που ανήκουν στην ομάδα Administrators θα πρέπει να χρησιμοποιούνται μόνο για την εκτέλεση των καθηκόντων της διαχείρισης του συστήματος, όπως την εγκατάσταση και τη εφαρμογή των ενημερώσεων του λογισμικού στο σύστημα, τη διαχείριση των λογαριασμών των χρηστών και για την τροποποίηση του συστήματος και την εφαρμογή των ρυθμίσεων. Επιπλέον, οι χρήστες δεν πρέπει να μοιράζονται τους λογαριασμούς; Έχοντας ένα ξεχωριστό λογαριασμό για κάθε χρήστη παρέχετε προστασία των δεδομένων και υποστηρίζει την υπευθυνότητα από τους περιορισμούς που επιβάλλονται σε συγκεκριμένες δράσεις στο λογαριασμό του χρήστη, που συνδέεται με ένα συγκεκριμένο πρόσωπο. Για να δημιουργήσετε ένα νέο πρότυπο λογαριασμού χρήστη για καθημερινή χρήση, ακολουθήστε τα παρακάτω βήματα:

1. Κάντε δεξί κλικ στο δεξιό παράθυρο και επιλέξτε **New User**. Πληκτρολογήστε το όνομα του χρήστη, το ονοματεπώνυμο, καθώς και τη περιγραφή της ομάδας και κάντε κλικ στο κουμπί **Create**. Θα σας ζητηθεί να πληκτρολογήσετε ένα κωδικό πρόσβασης στην επόμενη σύνδεση.

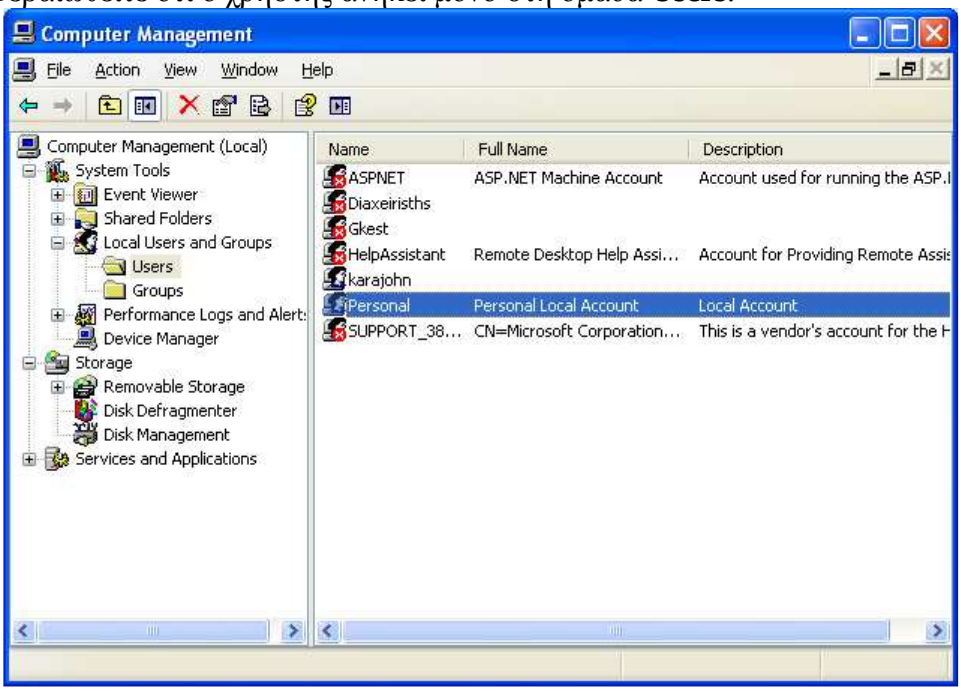


Εικόνα 158: Computer Management



Εικόνα 159: New User

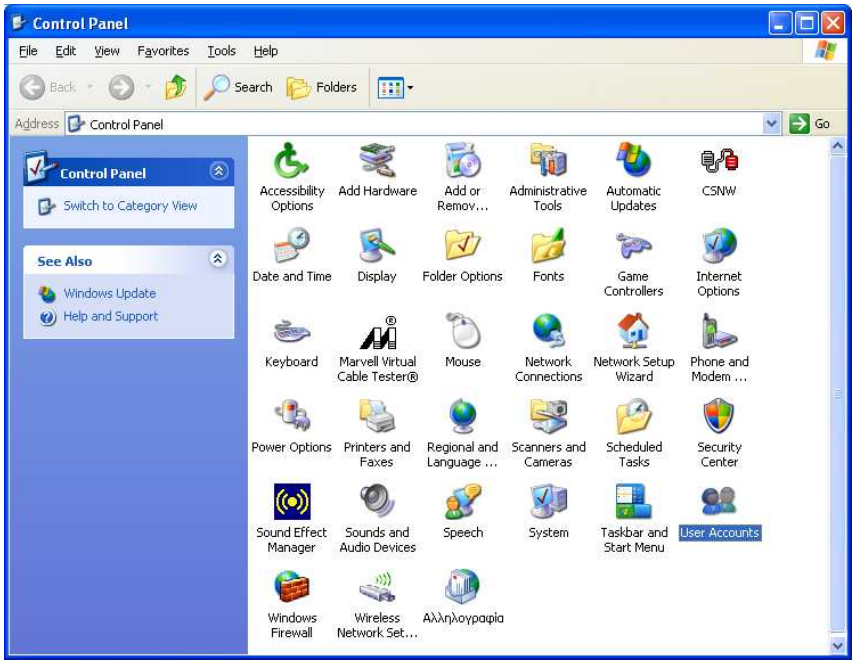
2. Βεβαιωθείτε ότι ο χρήστης ανήκει μόνο στη ομάδα **Users**.



Εικόνα 160: Computer Management

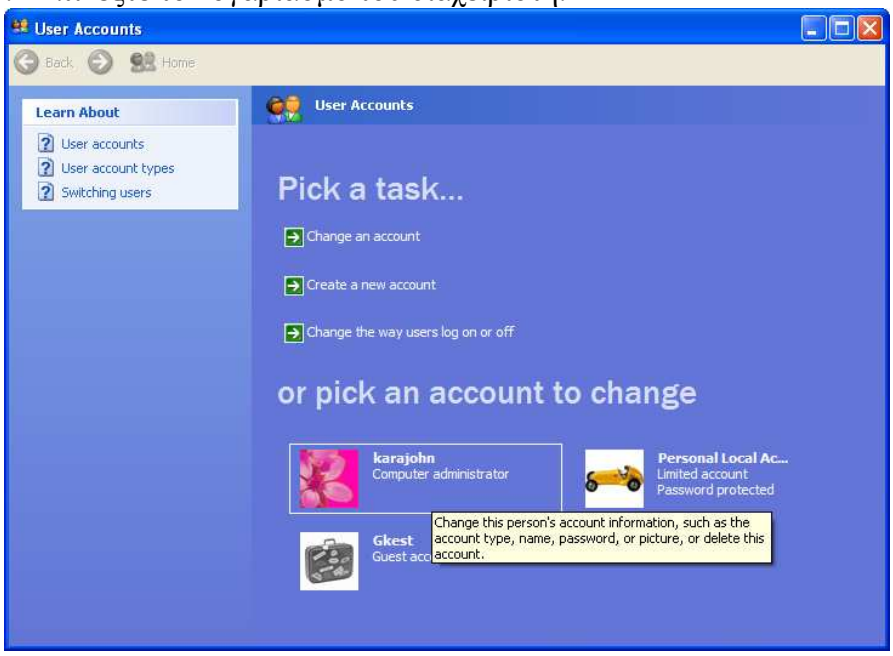
3. Αντιστοιχίστε ένα ισχυρό κωδικό πρόσβασης για το λογαριασμό του διαχειριστή, αν αυτό δε έχει γίνει ήδη.

    a. Πατήστε από το μενού **Start**, διαλέξτε **Control Panel** και πατήστε στο **User Accounts**.



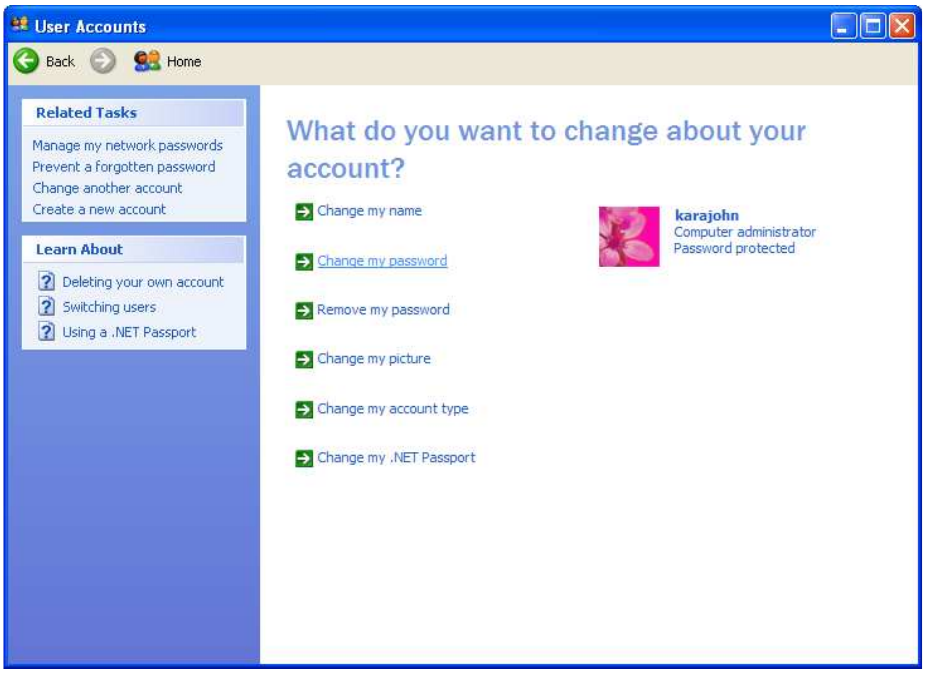
Εικόνα 161: Control Panel

b. Επιλέξτε το λογαριασμό του διαχειριστή.



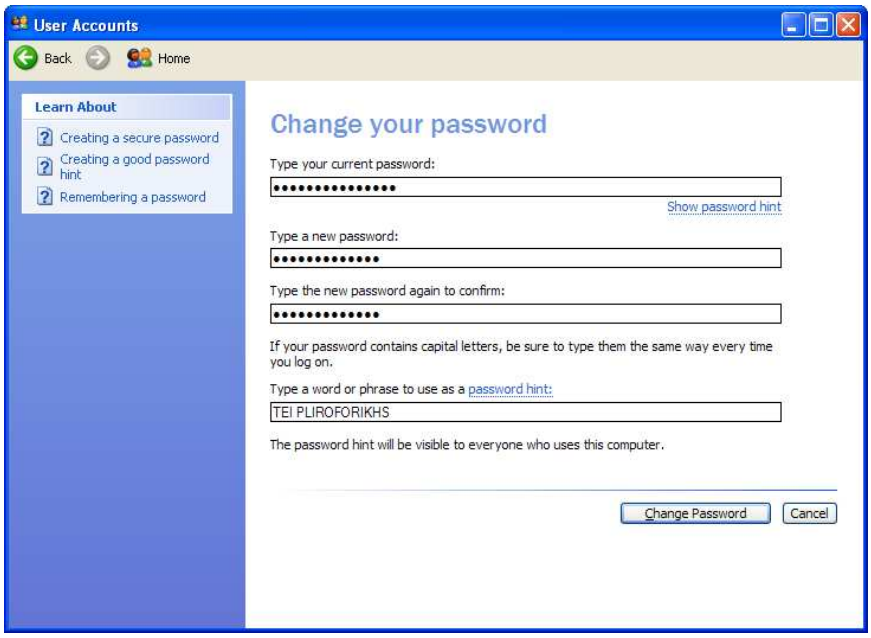
Εικόνα 162: User Accounts

c. Πατήστε στο **Change my password**.



Εικόνα 163: Computer Administrator

d. Πληκτρολογήστε το πρόσφατο κωδικό, βάλτε το νέο κωδικό και πληκτρολογήστε τον μια φορά ακόμα για να επιβεβαιωθεί. Κάντε κλικ στο κουμπί **Change Password**.

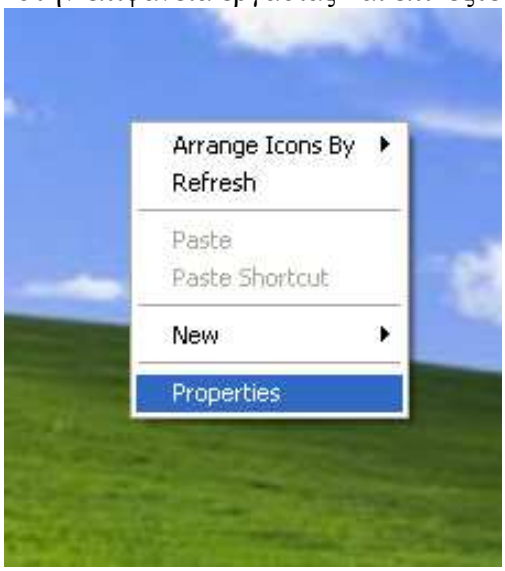


Εικόνα 164: Change Your Password

3.2.3 Local Session Protection

Είναι σημαντικό να παράσχετε προστασία έναντι της άνευ αδείας για πρόσβαση στα τοπικά συστήματα των Windows XP. Ένας τέτοιος έλεγχος είναι για το κλείδωμα της τρέχουσας χρήσης της συνόδου με αυτόματο ή χειροκίνητο τρόπο. Η προστασία της οθόνης μπορεί να κλειδωθεί αυτόματα μετά από μια περίοδο λειτουργίας του συστήματος έχοντας μείνει αδρανή για ένα συγκεκριμένο αριθμό λεπτών, απαιτώντας να βάλει τον κωδικό πρόσβασης το χρήστης πριν από το ξεκλείδωμα του συστήματος. NIST συνιστά ιδιαίτερα να χρησιμοποιείτε έναν κωδικό πρόσβασης για τη ενεργοποίηση της οθόνης των Windows XP σε όλα τα συστήματα που πρέπει προστατεύονται από την παράνομη πρόσβαση. Ρυθμίσεις για τη διευκόλυνση και τη οθόνη περιλαμβάνονται στο FDCC του GPO, αλλά δεν είναι του NIST στα πρότυπα ασφαλείας. Για να ρυθμίσετε έναν κωδικό πρόσβασης με δυνατότητες ενεργοποίησης της οθόνης, ακολουθήστε τα παρακάτω βήματα:

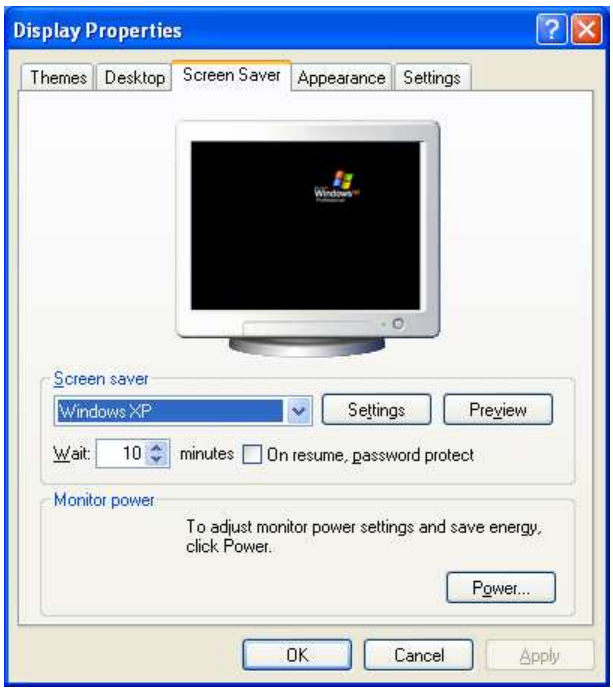
1. Πατήστε δεξί κλικ στην επιφάνεια εργασίας και επιλέξτε **Properties**.



Εικόνα 165: Properties Desktop

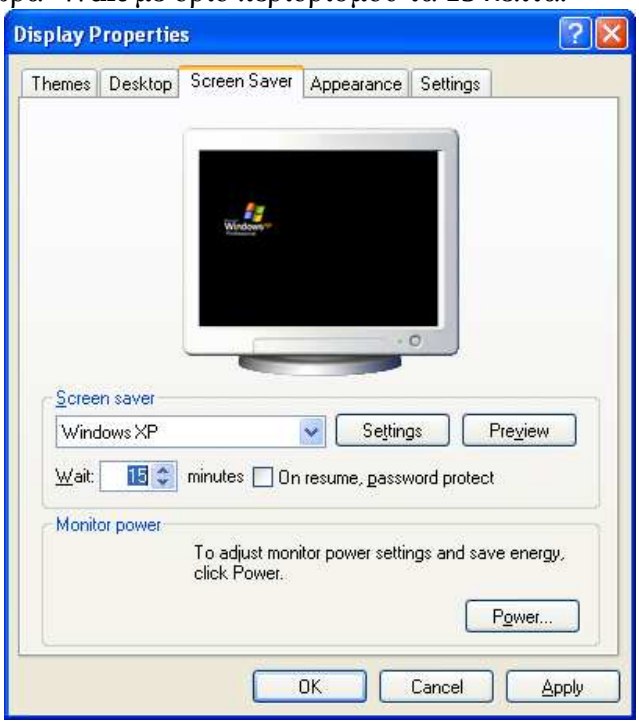
2. Πατήστε στη καρτέλα **Screen Saver** .

3. Ορίστε στο **Screen saver** σε κάτι άλλο **(None)**.



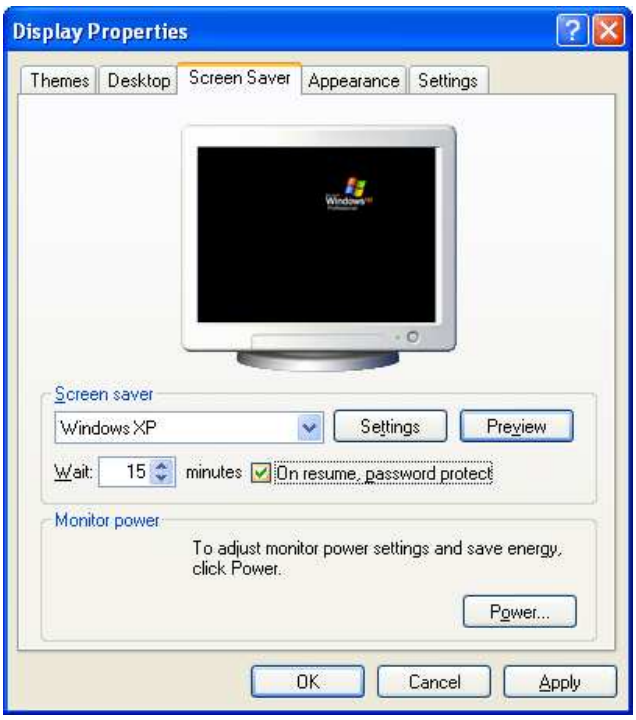
Εικόνα 166: Display Properties

4. Ορίστε την ώρα **Wait** με όριο περιορισμού τα 15 λεπτά.



Εικόνα 167: Screen Saver

5. Επιλέξτε το μαρκαρισμένο πλαίσιο **On resume, password protect** για να απαιτεί το κωδικό του χρήστη για να ξεκλειδωθεί το σύστημα.



Εικόνα 168: Screen Saver(2)

6. Πατήστε **OK**.

Υπάρχουν πολλοί τρόποι με τους οποίους οι χρήστες μπορούν να κλειδώσετε χειροκίνητα τις συνεδρίες. Η απλούστερη μέθοδος είναι να κρατήσετε πατημένο το πλήκτρο του λογοτύπου των Windows στο πληκτρολόγιο και στη συνέχεια να πατήσετε το πλήκτρο L. Αυτό κλειδώνει το σύστημα και εμφανίζει το παράθυρο διαλόγου **Unlock Computer**, που ειδοποιεί το χρήστη για να πληκτρολογήσει το όνομα χρήστη και το κωδικό πρόσβασης για να ξεκλειδωθεί το σύστημα. Άλλοι μέθοδοι κλειδώματος εξαρτώνται από τις ρυθμίσεις για την οθόνη υποδοχής και τα χαρακτηριστικά της Γρήγορη Εναλλαγής των Χρηστών, τα οποία συνδέονται με την υλοτομία σε συστήματα με Windows XP. Όταν η οθόνη υποδοχής είναι ενεργοποιημένη, τα ονόματα των χρηστών εμφανίζονται στην οθόνη και κάνοντας κλικ σε ένα πρόσωπο με το κατάλληλο όνομα χρήστη και πληκτρολογείτε το κωδικό πρόσβασης για να συνδεθείτε. Όταν η οθόνη υποδοχής είναι απενεργοποιημένο, οι χρήστες πρέπει να πληκτρολογήσουν το όνομα χρήστη και όχι να κάνουν κλικ πάνω τους . Όπως περιγράφεται σε τμήμα της μεθοδολογίας, το χαρακτηριστικό του Fast User Switching (FUS) είναι διαθέσιμο μόνο αν η οθόνη υποδοχής είναι ενεργοποιημένη και το σύστημα δεν αποτελεί τμήμα ενός τομέα. Υπό τις συνθήκες αυτές, FUS μπορεί να ενεργοποιηθεί ή να απενεργοποιηθεί. FUS επιτρέπει σε δύο χρήστες να είναι συνδεδεμένοι ταυτόχρονα, χρησιμοποιώντας το χαρακτηριστικό Switch User. Ωστόσο, ο τρέχων χρήστης δεν έχει πρόσβαση στο άλλο χρήστη της συνόδου.

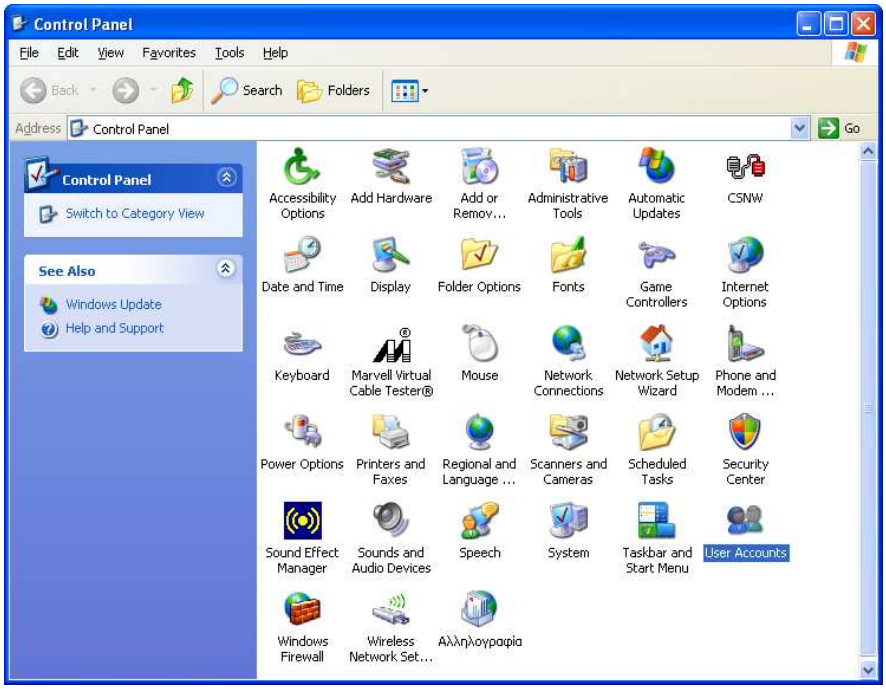
Ασφαλής διαχείριση Microsoft Windows XP Professional σύμφωνα με την μεθοδολογία NIST SP 800-68 (Μέρος 1ο)

Για να ενεργοποιήσετε ή να απενεργοποιήσετε την οθόνη υποδοχής και τα χαρακτηριστικά FUS, ακολουθήστε τα παρακάτω βήματα:

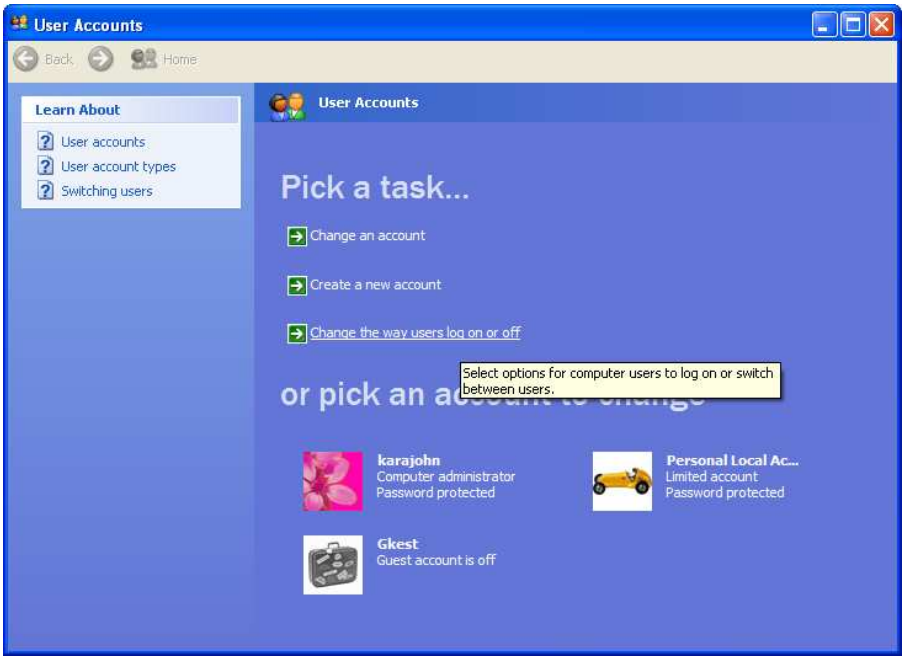
1. Από το μενού **Start**, επιλέξτε **Control Panel**.

Εικόνα 169: Control Panel

2. Κάντε κλικ στο **User Accounts**, μετά κάντε κλικ στο **Change the way users log on or off**.

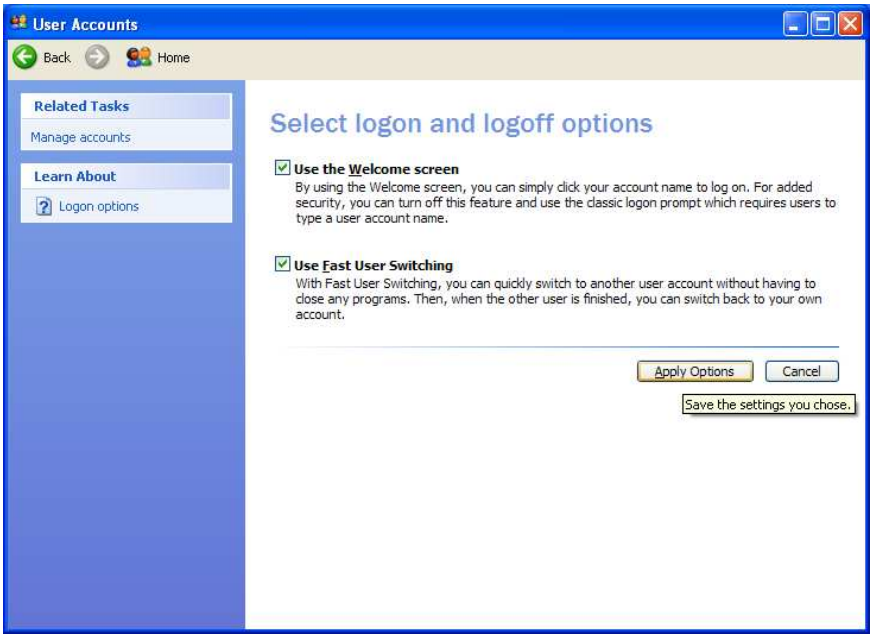


Εικόνα 170: User Accounts



Εικόνα 171: Change The Way Users Log On or Off

3. Επιλέξτε ή μη επιλέξετε τις επιλογές που ονομάζονται **Use the Welcome screen** και **Use Fast User Switching** ανάλογα με τη περίπτωση και πατήστε **Apply Options**.



Εικόνα 172: Select logon and logoff options

Εάν η οθόνη υποδοχής είναι απενεργοποιημένη, ο χρήστης μπορεί να κλειδώσει το σύστημα πατώντας CTRL + ALT + DEL, να ανοίξει το παράθυρο διαλόγου Ασφάλειας των Windows και στη συνέχεια να κάνει κλικ στο κουτί **Lock Computer**. Οι κλειδαριές της συνόδου και η εμφάνιση εμφανίζονται στο παράθυρο διαλόγου του **Unlock Computer.**

3.2.5 Password Reset Disk

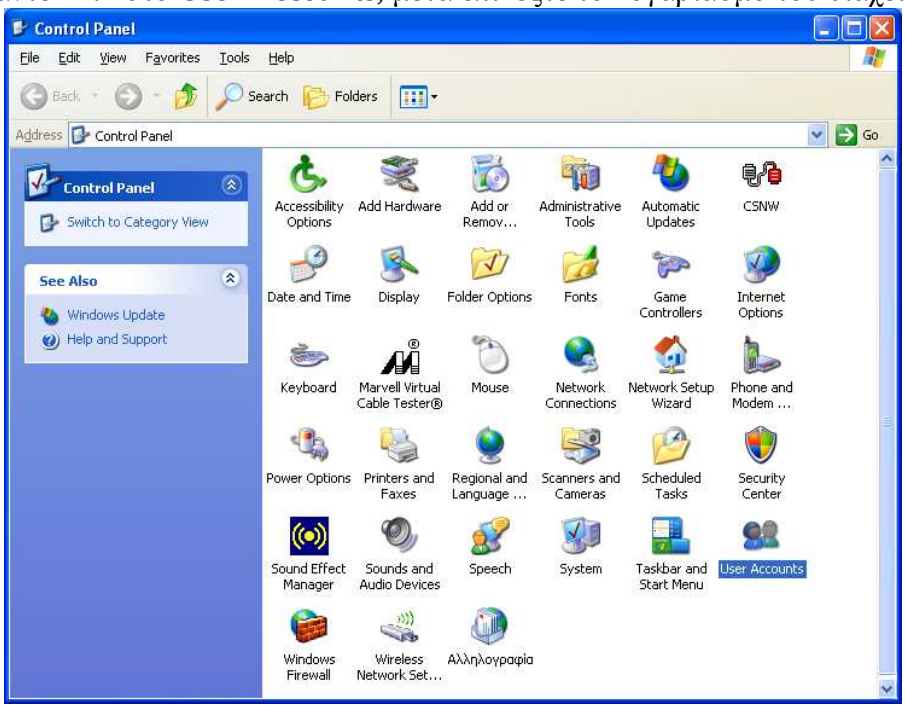
Για ένα σύστημα μέσα σε ένα μη διαχειρισμένο περιβάλλον, μια δισκέτα επαναφοράς κωδικού πρόσβασης θα μπορούσε να δημιουργήσει τον λογαριασμό του διαχειριστή και να αποθηκεύονται σε ασφαλή χώρο. Ο δίσκος μπορεί να χρησιμοποιηθεί εάν ο κωδικός πρόσβασης για το λογαριασμό του διαχειριστή ξεχαστεί ή χαθεί. Αν μια πρόσφατη δισκέτα επαναφοράς κωδικού πρόσβασης δεν είναι διαθέσιμη και κανείς δεν μπορεί να αποκτήσει πρόσβαση στο διοικητικό σύστημα, το σύστημα θα πρέπει πιθανόν να ξαναχτιστεί κάποια στιγμή (στην περίπτωση που ένα τρίτο εργαλείο χρησιμοποιηθεί για την επαναφορά του κωδικού πρόσβασης του λογαριασμού) [48].Για παράδειγμα, δεν μπορεί πλέον να είναι δυνατή η διατήρηση του συστήματος και ενημέρωση του. Επίσης, αν ένας λογαριασμός χρήστη είναι κλειδωμένος λόγω των πάρα πολλών των αποπειρών σύνδεσης που απέτυχαν, μπορεί να μην είναι δυνατό να ξεκλειδώσετε αυτόν. Έχοντας μια δισκέτα επαναφοράς κωδικού πρόσβασης είναι πιο σημαντικό για τα συστήματα που έχουν μόνο ένα ενεργοποιημένο λογαριασμό διαχειριστή ή περιέχουν σημαντικά στοιχεία, όπως είναι τυπικό SOHO σύστημα, καθώς και τα συστήματα που χρησιμοποιούν το σύστημα EFS. Στα διαχειρισμένα περιβάλλοντα, ιδίως αυτά στα οποία τα δεδομένα δεν πρέπει να είναι αποθηκευμένα σε desktop συστήματα, οι δίσκοι επαναφοράς του κωδικού πρόσβασης δεν χρησιμοποιούνται συχνά. Τα διαχειριστικά έξοδα για τη δημιουργία και την αποθήκευση δεκάδων χιλιάδων δίσκων επαναφοράς κωδικών πρόσβασης είναι παράλογη και συχνά ένας λογαριασμό διαχειριστή του τομέα, επίσης έχει πρόσβαση στο σύστημα. Για περιβάλλοντα στα οποία μια δισκέτα επαναφοράς κωδικού πρόσβασης χρειάζεται, πρέπει να εκτελέσετε τα ακόλουθα βήματα, για να τη δημιουργήσετε:

1. Από το μενού **Start**, διαλέξτε **Control Panel**.

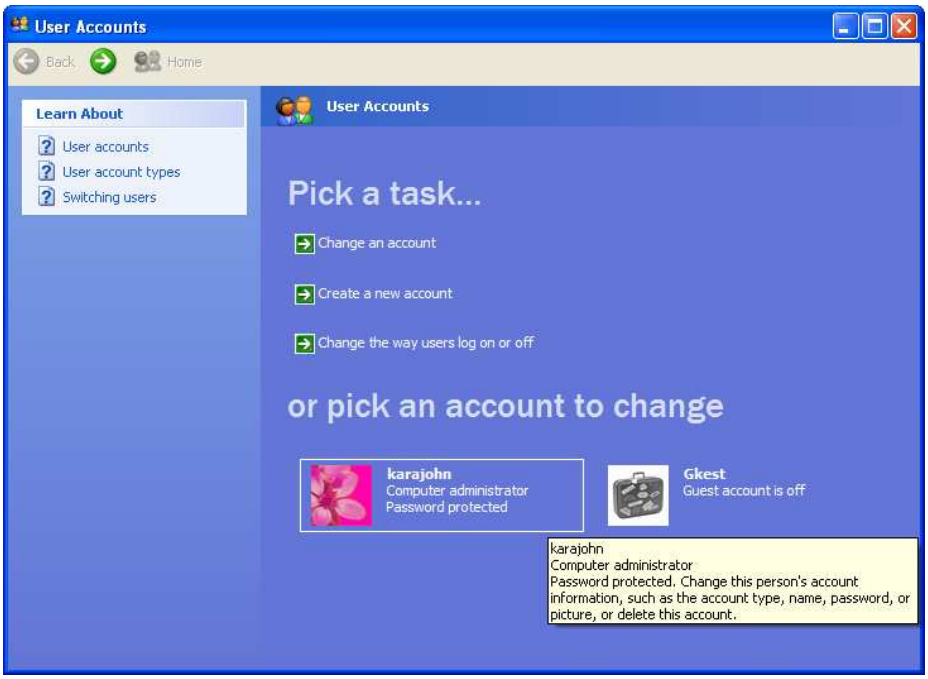
Εικόνα 173: Control Panel

[48] Χρησιμοποιώντας ένα εργαλείου τρίτου κατασκευαστή για να επαναφέρετε το λογαριασμό πρόσβασης για έναν λογαριασμό που θα καταστήσουν τα EFS στοιχεία για το λογαριασμό απροσπέλαστα.

2. Κάντε κλικ στο **User Accounts**, μετά επιλέξτε το λογαριασμό του διαχειριστή.

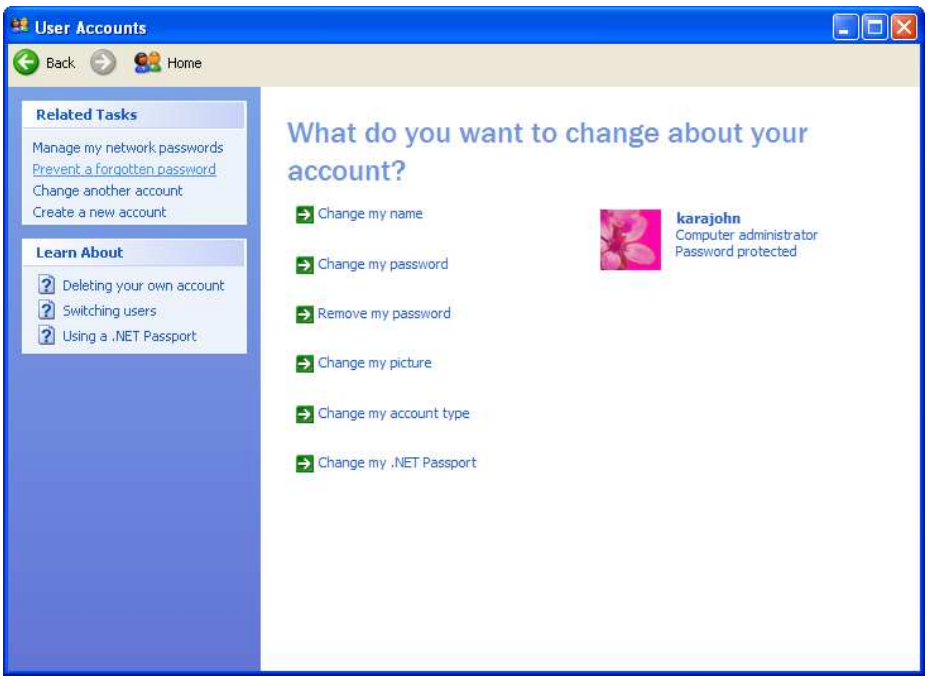


Εικόνα 174: User Accounts



Εικόνα 175: Computer Administrator

3. Στο Related Tasks, κάντε κλικ στο σύνδεσμο **Prevent a forgotten password**.

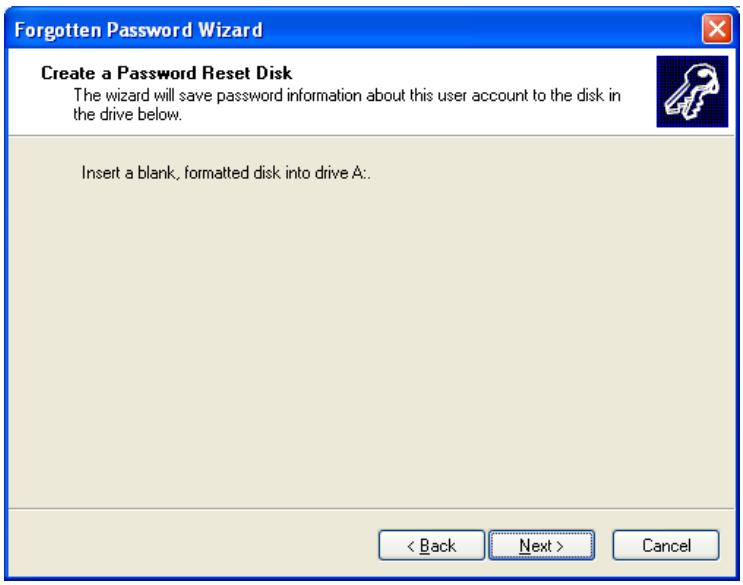


Εικόνα 176: Related Tasks

4. Το Forgotten Password Wizard θα πρέπει να αρχίσει. Πατήστε **Next**.

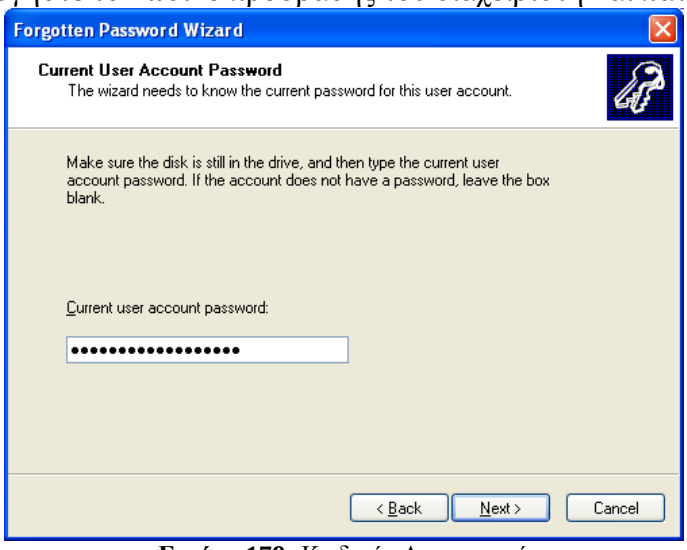
Εικόνα 177: Forgotten Password Wizard

5. Επιλέξτε μία **3 ½ Δισκέτα (A:)** στο προορισμό όπου ο κωδικός πρόσβασης θα αποθηκευτεί και κάντε κλικ στο **Next**.



Εικόνα 178: Create a Password Reset Disk

6. Πληκτρολογήστε το κωδικό πρόσβασης του διαχειριστή και πατήστε **Next**.



Εικόνα 179: Κωδικός Διαχειριστή

7. Ο wizard δημιουργεί το δίσκο. Όταν η δημιουργία τελειώσει , πατήστε **Next**.

8. Όταν ο wizard τελειώσει, πατήστε **Finish**.
9. Αποθηκεύστε το δίσκο με το κωδικό πρόσβασης σε ασφαλές μέρος.

Σχετικά με τη διαδικασία αποθήκευση επαναφοράς του κωδικού υπήρξε ένα πρόβλημα, ενώ όλα πήγαιναν σωστά μέχρι το 7^{ο} βήμα, έπειτα η διαδικασία του wizard έπαυε να συνεχίζετε και έτσι δεν ολοκληρωνόταν η διαδικασία αποθήκευσης του κωδικού στη δισκέτα. Προσπάθησα και με άλλους χρήστες και κωδικούς αλλά γινόταν το ίδιο.

Τη διαδικασία επαναφοράς του κωδικού δε μπόρεσα να την ακολουθήσω εξαιτίας του προβλήματος που είχα με τη διαδικασία αποθήκευσης του κωδικού επαναφοράς. Τα βήματα αναφέρονται παρακάτω.

Σε περίπτωση που λογαριασμό του διαχειριστή να ξεχαστεί, ακολουθήστε τα παρακάτω βήματα για να χρησιμοποιήσετε τη δισκέτα επαναφοράς του κωδικού πρόσβασης:

1. Κατά τη οθόνη σύνδεσης, επιλέξτε το λογαριασμό του διαχειριστή και πιέστε το Enter key ή κάντε κλικ στο κουμπί **right arrow** που βρίσκεται στα δεξιά του πεδίου κωδικού πρόσβασης.

2. Πατήστε στο σύνδεσμο **Use your password reset disk** .

3. Πατήστε **Next**.

4. Επιλέξτε τη **3 1/2 Δισκέτα (A:)** οδηγό και πατήστε **Next**.
5. Βάλτε το νέο κωδικό, ξανά πληκτρολογήστε το κωδικό για να το επιβεβαιώσει, και πατήστε **Next**.

6. Πατήστε **Finish**.

7. Στην οθόνη σύνδεσης, επιλέξτε του διαχειριστή το λογαριασμό και εισάγετε τον κωδικό πρόσβασης που δημιουργήθηκε πρόσφατα για την εξακρίβωση της γνησιότητας

8. Η πρόσφατη δισκέτα επαναφοράς του κωδικού πρόσβασης δεν είναι πλέον έγκυρη. Ξαναδημιουργήστε τη δισκέτα επαναφοράς του κωδικού πρόσβασης, ώστε να περιέχει το νέο κωδικό πρόσβασης.

Bes san guest gia na allaxeis password karajohn.

3.3 Auditing

Το τμήμα 6.2.1 περιγράφει ορισμένες ελεγκτικές δυνατότητες από τα συστήματα των Windows XP. Τα Windows XP μπορούν επίσης ελέγχουν άλλα πράγματα, όπως ενέργειες που πραγματοποιούνται σε μεμονωμένα αρχεία σε ένα σύστημα αρχείων NTFS. Για παράδειγμα, ο λογιστικός έλεγχος θα μπορούσε να ρυθμιστεί έτσι ώστε να συνδέονται όλες οι επιτυχημένες και να αποτυγχάνονται οι αλλαγές στο λειτουργικό σύστημα και στην εφαρμογή αρχείων προγράμματος ή να συνδεθείτε να έχετε πρόσβαση σε όλα τα κρίσιμα αρχεία δεδομένων. Το τμήμα αυτό ασχολείται με το αρχείο ελέγχου και εξηγεί επίσης τον τρόπο πρόσβασης στο Event Viewer, ένα εργαλείο για την αναθεώρηση των ελεγκτικών κορμών. Ένα άλλο θέμα που απευθύνεται σε αυτή την ενότητα είναι η σημασία του χρόνου συγχρονισμού με τον υποχρεωτικό έλεγχο.

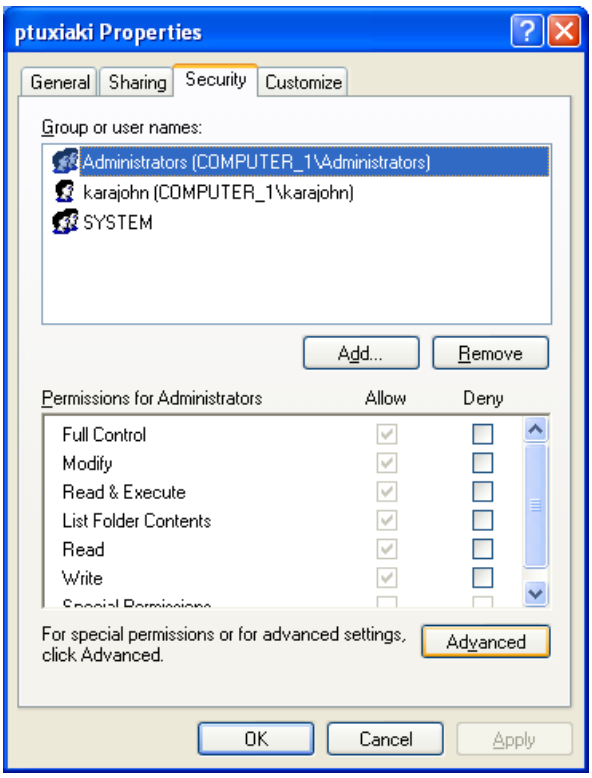
3.3.1 Individual File Auditing

Τα Windows XP παρέχουν μια μέθοδο για να ελέγχουν την πρόσβαση σε οποιοδήποτε αρχείο είναι αποθηκευμένο σε διαμέρισμα μορφοποιημένο NTFS. Αυτή η μέθοδος ελέγχου συνήθως χρησιμοποιείται για να ελέγχει την πρόσβαση σε ευαίσθητα αρχεία. Για να ρυθμίσετε τους επιμέρους φακέλους ελέγχου, ακολουθήστε τα παρακάτω βήματα:

1. Δεξί κλικ στο αρχείο και επιλέξτε **Properties**.

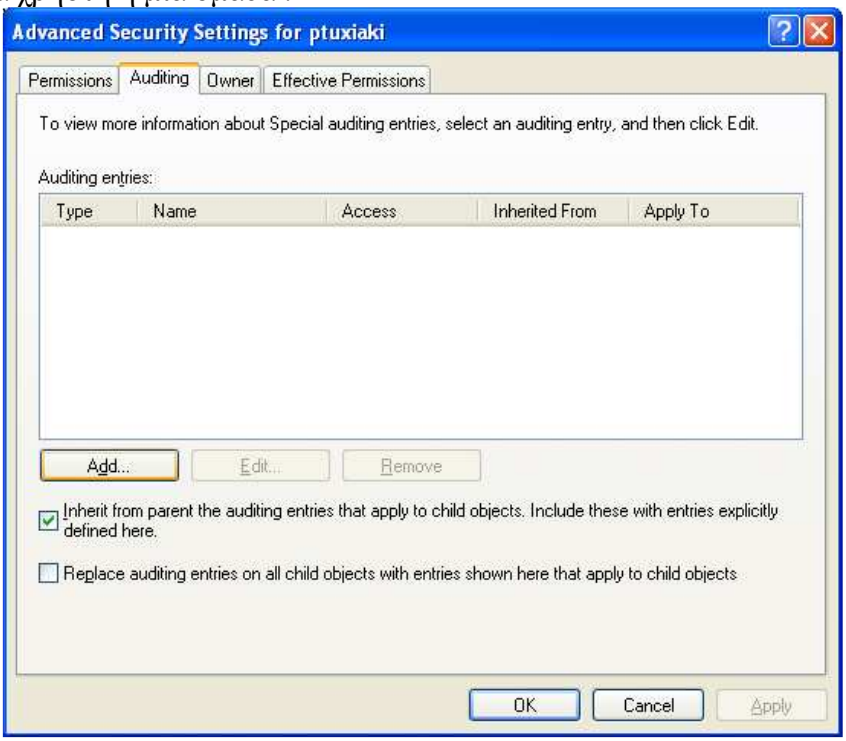
Εικόνα 180: Ptyxiaki Properties

2. Επιλέξτε τη καρτέλα **Security** και κάντε κλικ στο **Advanced**.

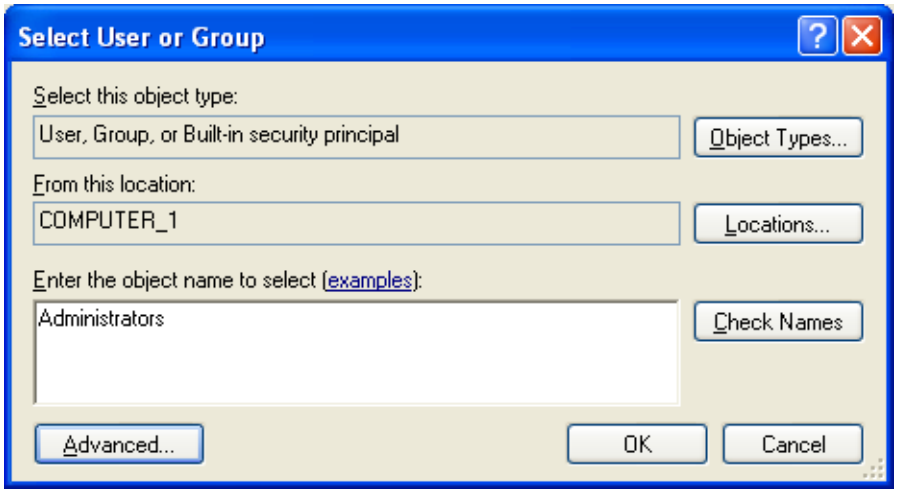


Εικόνα 181: Security

3. Επιλέξτε τη καρτέλα **Auditing** και κάντε κλικ στο **Add** για να προσδιορίσετε ένα χρήστη ή μια ομάδα .

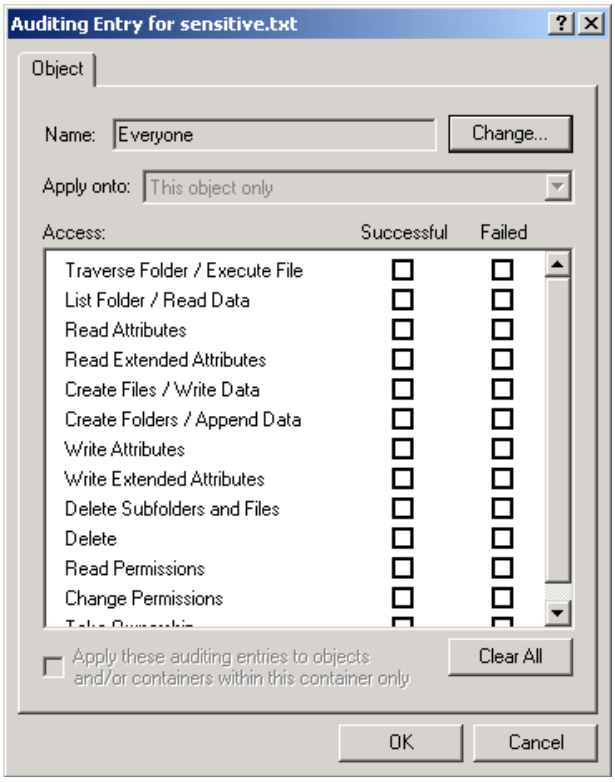


Εικόνα 182: Advanced Security Settings



Εικόνα 183: Select User or Group

4. Όπως φαίνεται στη εικόνα 184, επιλέξτε το αρχείο άδειας πρόσβασης των χαρακτηριστικών που θα πρέπει να ελέγχονται από τα κατάλληλα **Successful** και **Failed** πλαίσια έλεγχου.



Εικόνα 184: Auditing Entry For Sensitive

5. Η απόδοση του συστήματος ελέγχου μπορεί να προβληθεί χρησιμοποιώντας το **Event Viewer** (πρόγραμμα προβολής), όπως περιγράφεται στο τμήμα 3.3.2.

3.3.2 Reviewing Audit Logs

Ασφαλής διαχείριση Microsoft Windows XP Professional σύμφωνα με την μεθοδολογία NIST SP 800-68 (Μέρος 1ο)

Τα Windows XP περιλαμβάνουν ένα ενσωματωμένο συμπληρωματικό πρόγραμμα το MMC εργαλείο που ονομάζεται **Event Viewer** για την εξέταση της αίτησης, την ασφάλεια καθώς και τα μητρώα του συστήματος. Αυτά τα αρχεία περιέχουν τα αρχεία ελέγχου, ανάμεσα σε άλλα είδη πληροφοριών. Το μητρώο για κάθε σύστημα θα πρέπει να επανεξετάζεται σε τακτά διαστήματα για τον εντοπισμό αντικανονικών δραστηριοτήτων[49]. Στην επιχείρηση και στα FDCC περιβάλλοντα, η διαδικασία αυτή θα πρέπει να είναι αυτοματοποιημένη με τη χρήση ειδικού λογισμικού για κάθε σύστημα, όπως μια βάση υποδοχής εισχώρηση στο ανιχνεύσιμο σύστημα το οποίο παρακολουθεί τα αρχεία καταγραφής ή μέσω της χρήσης των κεντρικών μητρών των διακομιστών που λαμβάνουν αντίγραφα του αρχείου καταγραφής από κάθε σύστημα και να αναλύουν αυτά για ύποπτη δραστηριότητα.

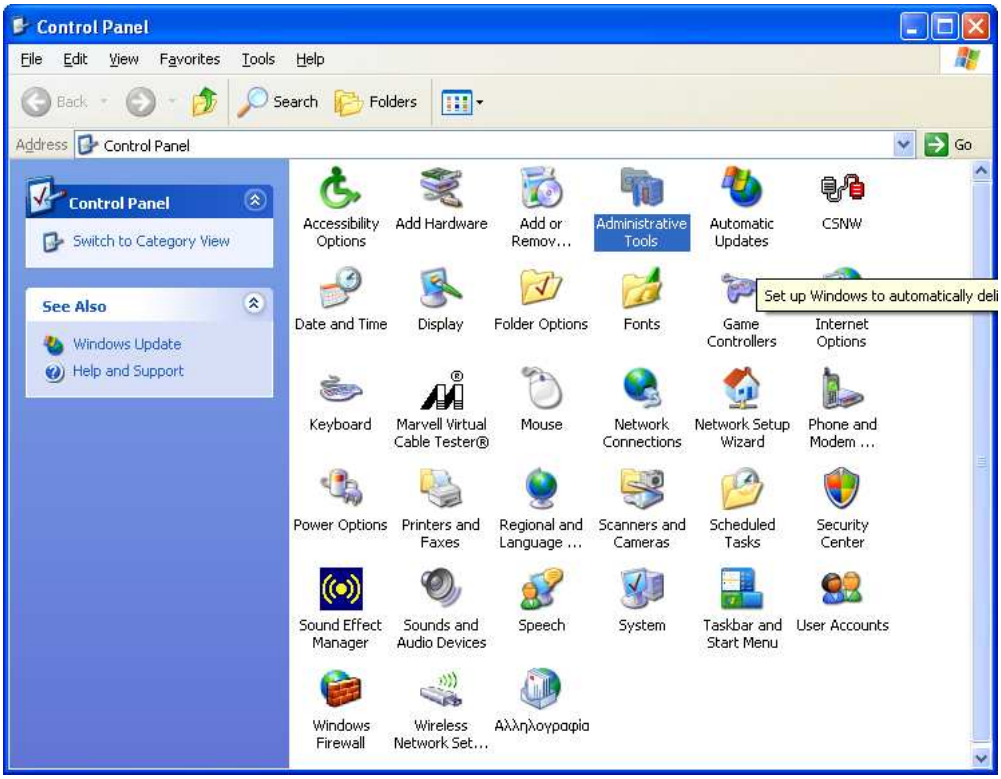
Για να αναθεωρήσει ελέγχου χρησιμοποιώντας το **Event Viewer** (πρόγραμμα προβολής) , ακολουθήστε τα παρακάτω βήματα:

1. Από το μενού **Start** , διαλέξτε **Control Panel**.

Εικόνα 185: Control Panel

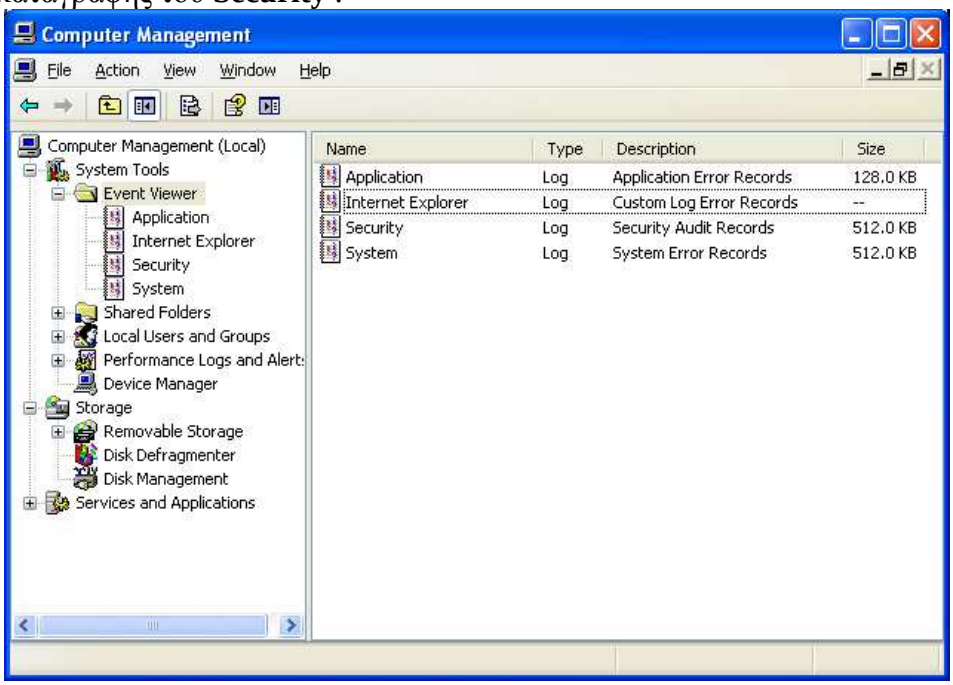
2. Επιλέξτε **Administrative Tools**, και διαλέξτε **Computer Management**.

[49]Σε SSLF περιβάλλοντα, τα audit logs θα πρέπει να επανεξετάζονται τουλάχιστον μια φορά τη εβδομάδα, κατά τη προτίμηση ημερησίως.

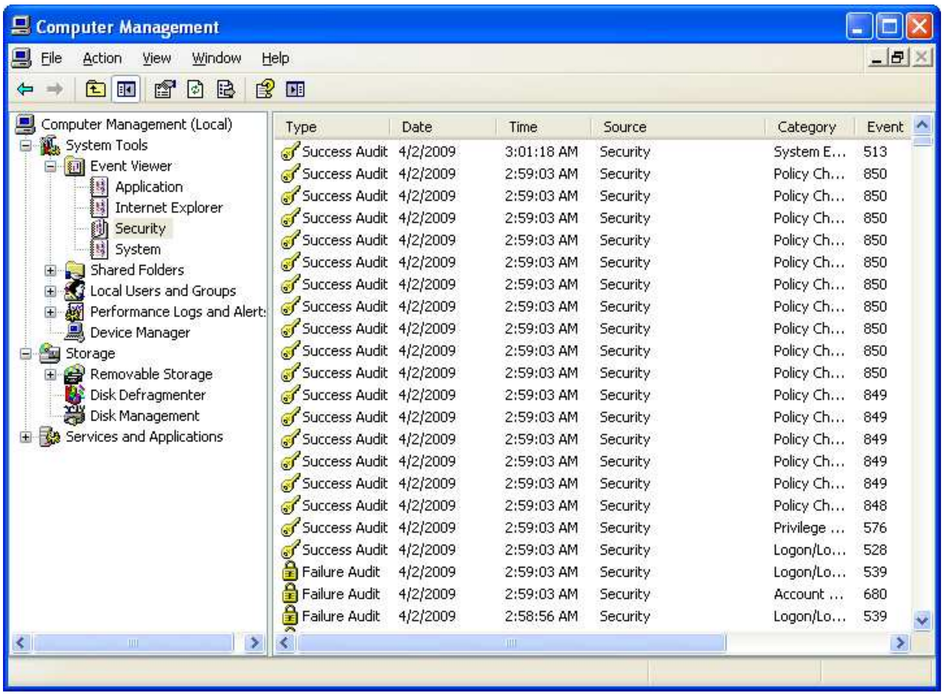


Εικόνα 186: Administrative Tools

3. Επεκτείνετε τη λίστα **System Tools** και στη συνεχεία επεκτείνετε το **Event Viewer**. Αυτό εμφανίζει τα 3 είδη των κορμών: **Application**, **Security**, και **System**. Η επανεξέταση του έλεγχου αρχείων , είναι αποθηκευμένα στο αρχείο καταγραφής του **Security** .



Εικόνα 187: System Tools



Εικόνα 188: Security

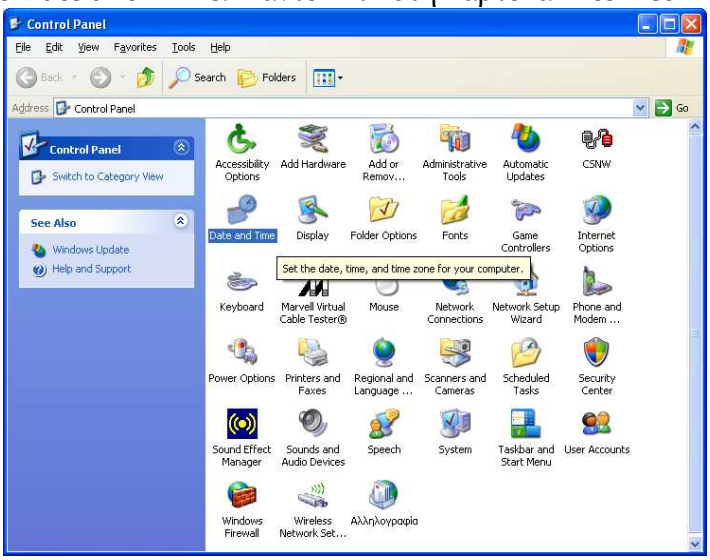
3.3.3 Time Synchronization

Είναι σημαντικό να ρυθμίσετε τα συστήματα των Windows XP να είναι συγχρονισμένα τα ρολόγια τους σε τακτική βάση με ακριβή χρόνο πηγών. Αν έλεγχος των logs περιέχουν στοιχεία για την επίθεση και το σύστημα του ρολογιού είναι ανακριβή, θα κάνει την ανάλυση της επίθεσης πιο δύσκολη και μπορεί επίσης να αποδυναμώσει την αποδεικτική αξία των logs (κορμών). Ο συγχρονισμός της ώρας είναι επίσης βολικό επειδή οι χρήστες δεν χρειάζονται να ρυθμίσουν χειροκίνητα το ρολόι για να αντισταθμίσει τις ανακρίβειες στο σύστημα της ώρας. Τα Windows XP χρησιμοποιούν το Network Time Protocol (NTP), για την ώρα του συγχρονισμού. Από προεπιλογή, τα συστήματα που συμμετέχουν σε ένα Active Directory (AD) συγχρονίζονται αυτόματα με τον ελεγκτή του τομέα (DC). Για να διαμορφώσετε ένα σύστημα των Windows XP το οποίο δεν αποτελεί μέλος του AD χρόνο για να εκτελέσετε συγχρονισμένο, ακολουθήστε τα παρακάτω βήματα:

1. Από το μενού **Start**, διαλέξτε **Control Panel**.

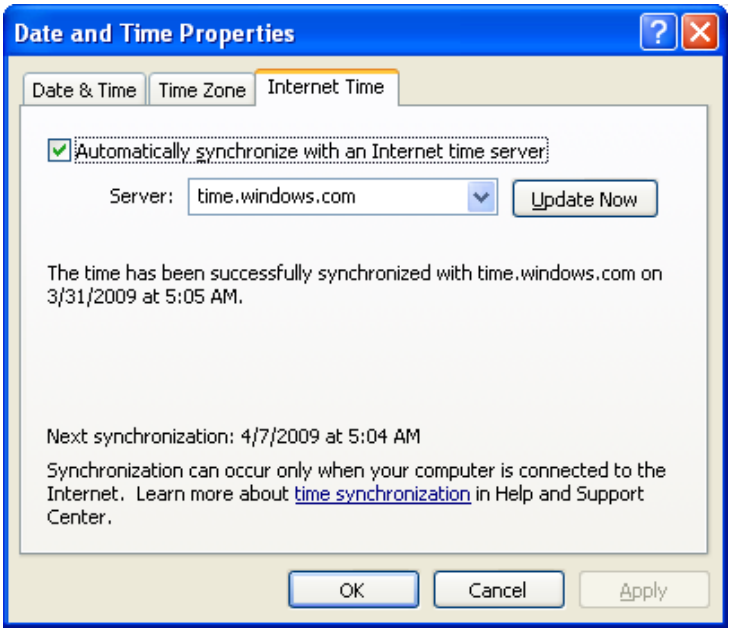
Εικόνα 189: Control Panel

2. Επιλέξτε **Date and Time**. Κάντε κλικ στη καρτέλα **Internet Time**.



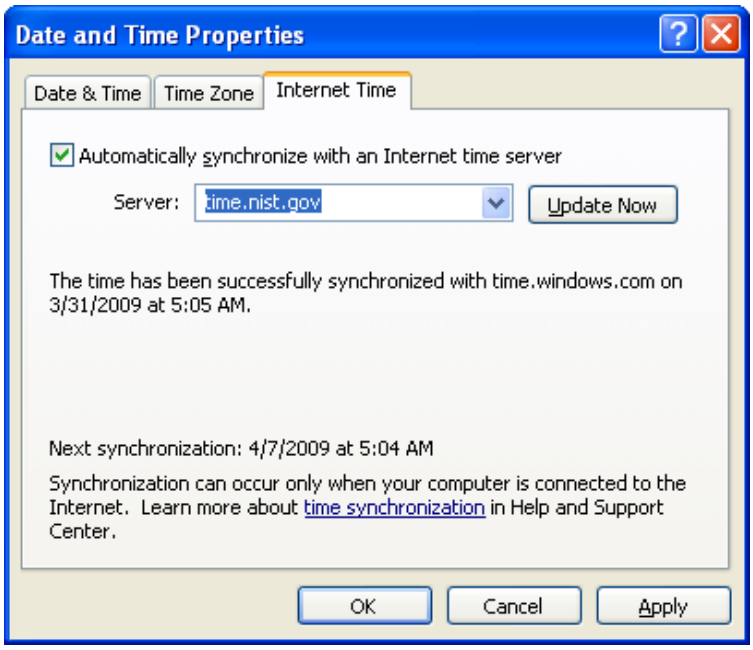
Εικόνα 190: Date and Time

3. Επιλέξτε το κουτί **Automatically synchronize with an Internet time server**.



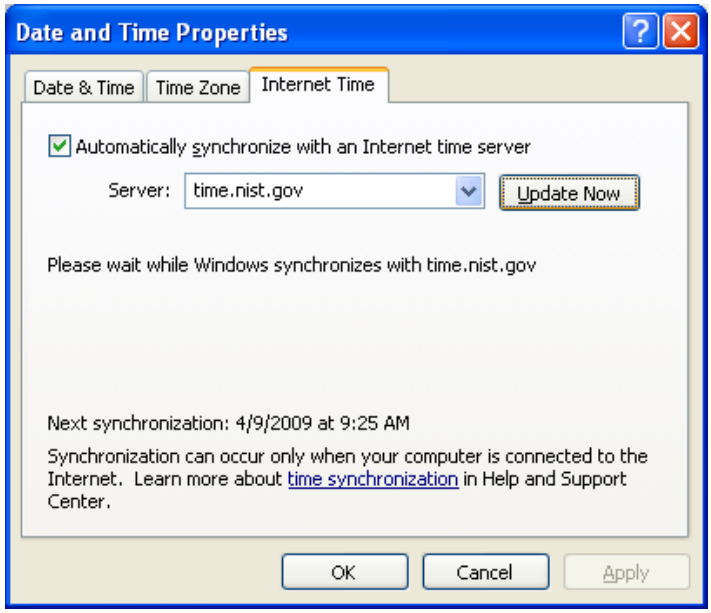
Εικόνα 191: Date and Time Properties

4. Εισάγετε το όνομα ή τη διεύθυνση IP ενός διακομιστή ώρας (π.χ. time-a.nist.gov). Οι περισσότερες επιχειρήσεις έχουν ένα ή περισσοτέρους εναλλακτικούς διακομιστές ώρας. Εάν ένας τέτοιος διακομιστής είναι διαθέσιμος, θα πρέπει να διευκρινισθεί, αντί ενός εξωτερικού διακομιστή ώρας.

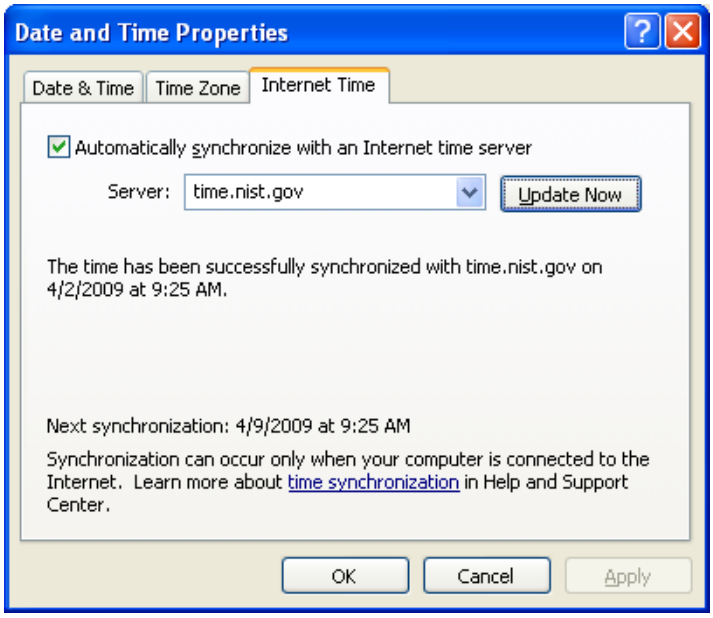


Εικόνα 192: Internet Time

5. Κάντε κλικ στο **Update Now** να επιβεβαιώσετε ότι η ώρα συγχρονισμού δουλεύει σωστά.



Εικόνα 193: Update Now



Εικόνα 194: Συγχρονίστηκε η ώρα

6. Πατήστε **OK**.

3.4 Software Restriction Policy

Οι πολιτικές περιορισμού λογισμικού παρέχουν στους διαχειριστές, με γνώμονα τις πολιτικές μηχανισμό που προσδιορίζει το λογισμικό για τη λειτουργία των συστημάτων τους και ελέγχει την ικανότητα του να εκτελέσει το λογισμικό. Χρησιμοποιώντας μια πολιτική περιορισμού λογισμικού, ο διαχειριστής μπορεί να αποτρέψει την εκτέλεση ανεπιθύμητων εφαρμογών, συμπεριλαμβανομένων των ιών και Trojan horses, καθώς και λογισμικό που είναι γνωστό ότι προκαλεί επιπτώσεις ,όταν έχει εγκατασταθεί. Μια πολιτική περιορισμού λογισμικού είτε είναι να

επιτραπεί ή να αρθεί. Η απεριόριστη ρύθμιση επιτρέπει να τρέχουν όλα τα προγράμματα, εκτός εκείνων που καθορίζονται ως απαγορευμένα. Αυτό είναι πιο κατάλληλο για οργανώσεις κατά την οποία οι χρήστες απαιτούν μεγάλη ευελιξία ως προς τα προγράμματα που μπορούν να εκτελέσουν. Με τον καθορισμό γνωστού προβληματικού λογισμικού, εφαρμογές χωρίς άδεια, Trojan horses και είναι γνωστό, αυτή η ρύθμιση μπορεί να προστατεύσει ένα πλήθος από γνωστών απειλών. Η ρύθμιση Disallowed δεν σημαίνει ότι τα προγράμματα μπορούν να εκτελούνται, εκτός εκείνων που περιλαμβάνονται στον κατάλογο των προγραμμάτων που έχουν τη δυνατότητα να τρέχουν. Αυτό είναι πιο πολύ για εντατική εργασία, διότι όλες οι αιτήσεις που χρειάζονται, πρέπει να προσδιοριστούν, αλλά θα προσφέρουν άριστη προστασία έναντι χωρίς άδειας προγραμμάτων εκτέλεσης. Η Disallowed ρύθμιση είναι γενικά κατάλληλη μόνο για την υψηλότερη ανάγκη ασφάλειας καταστάσεων, ενώ η ρύθμιση Unrestricted, είναι καταλληλότερη για την παρεμπόδιση ορισμένων ανεπιθύμητων εφαρμογών. Οι πολιτικές περιορισμού λογισμικού είναι πολύ πιθανόν να χρησιμοποιηθούν σε περιβάλλοντα SSLF.

Η πολιτική περιορισμού λογισμικού έχει πέντε στοιχεία:

- **Επίπεδα ασφάλειας.** Αυτό χρησιμοποιείται για να ρυθμίσετε το προεπιλεγμένο κανόνα ως **Disallowed** ή **Unrestricted**.

- **Πρόσθετους κανόνες**. Αυτό καταλόγους περιέχει όλες τις εξαιρέσεις από τον προεπιλεγμένο κανόνα. Οι κανόνες αυτοί μπορούν μόνο με αρχεία αναφοράς που αναγράφονται ως καθορισμένοι τύποι αρχείων. Επιπλέον, όταν περισσότερο από έναν κανόνα , έχει ορισθεί ότι ταιριάζει με ένα συγκεκριμένο πρόγραμμα, η πρώτη αντιστοίχιση κανόνα θα επιλεγεί.

- **Επιβολή.** Το αντικείμενο παρέχει επιλογές όσον αφορά τις πολιτικές. Μια επιλογή θα εφαρμόσει την πολιτική που δεν μόνο για τα εκτελέσιμα, αλλά και για τη βιβλιοθήκη δυναμικής σύνδεσης (DLL) των αρχείων. Αυτή η επιλογή έχει οριστεί από την **επιλογή Apply software restriction to the following**, **τότε όλα τα αρχεία λογισμικού**. Μια άλλη επιλογή επιτρέπει στις τοπικές αρχές να τρέχουν το λογισμικό όταν άλλοι χρήστες δεν μπορούν. Αυτή η επιλογή έχει οριστεί από την **επιλογή Apply software restriction to the following users,** τότε **όλοι οι χρήστες εκτός από τους τοπικούς διαχειριστές.**

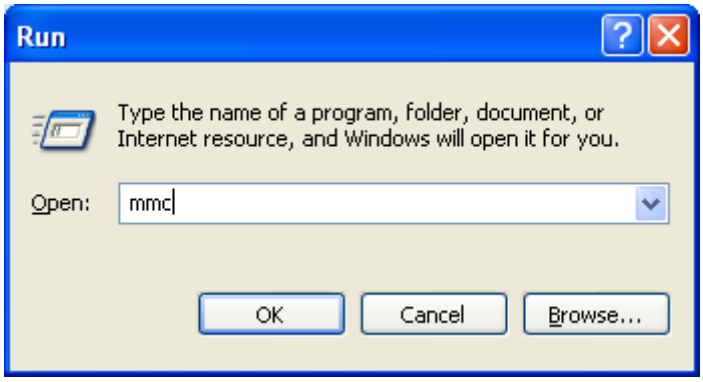
- **Καθορισμένοι τύποι αρχείων.** Αυτό παρέχει έναν τρόπο για να πούμε στις πολιτικές περιορισμού λογισμικού, των οποίων οι επεκτάσεις των αρχείων είναι εκτελέσιμα. Από προεπιλογή, αρκετά κοινά εκτελέσιμα αρχεία οι επεκτάσεις τους έχουν ήδη τεθεί. Οι επεκτάσεις των φακέλων μπορούν να προστεθούν και να διαγραφούν από τον κατάλογο, όπως απαιτείται.

- **Έμπιστοι εκδότες**. Περιέχει τον κατάλογο των εκδοτών των λογισμικών που είναι αξιόπιστοι, όπως οι τοπικές αρχές. Το σύστημα μπορεί να επαληθεύσει την αυθεντικότητα του εκδότη του ψηφιακού πιστοποιητικού πριν από την προσθήκη του εκδότη για τη λίστα των Trusted Publishers.

Για να δημιουργήσετε και να ρυθμίσετε μια πολιτική περιορισμού λογισμικού, ακολουθήστε τα παρακάτω βήματα:

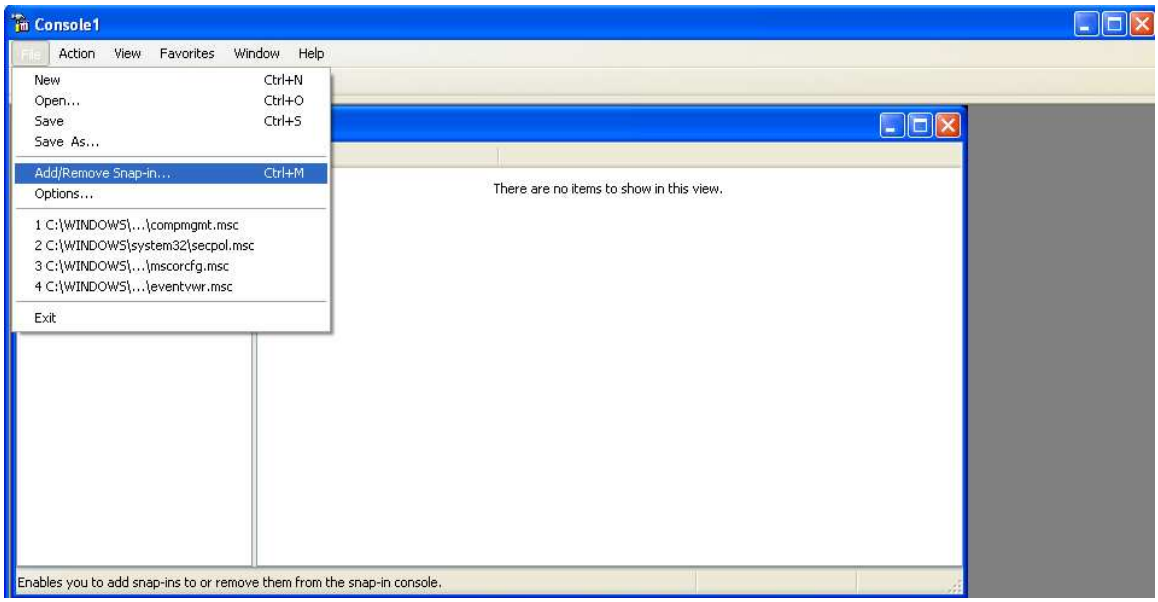
1. Κάντε εγγραφή ως τοπικός διαχειριστής ή ο κύριος διαχειριστής ή ως ένα χρήστη του οποίου έχει ανατεθεί η εξουσία να δημιουργεί πολιτικές περιορισμού λογισμικού.

2. Πατήστε **Start,** επιλέξτε **Run.** Στο πεδίο **Open** , πληκτρολογήστε **mmc** και πατήστε **OK.**

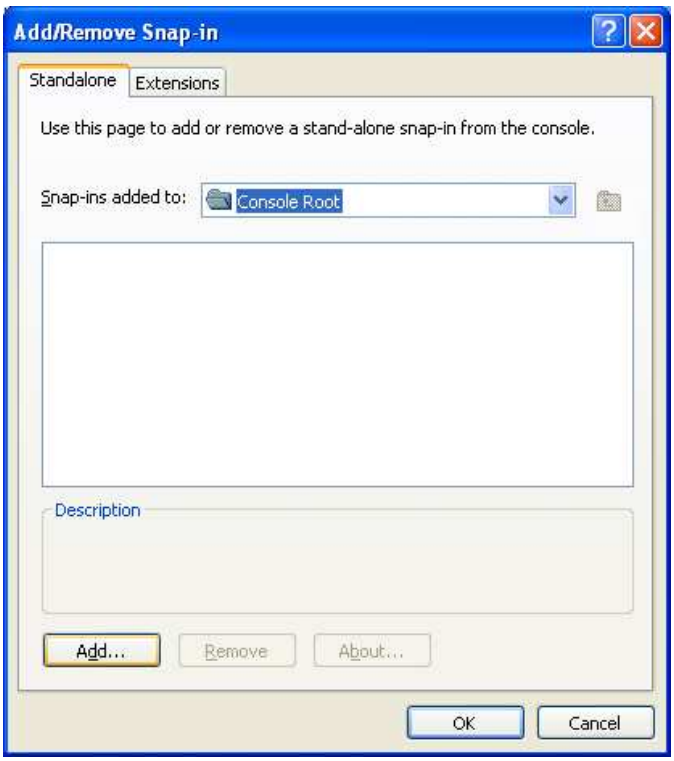


Εικόνα 195: Run

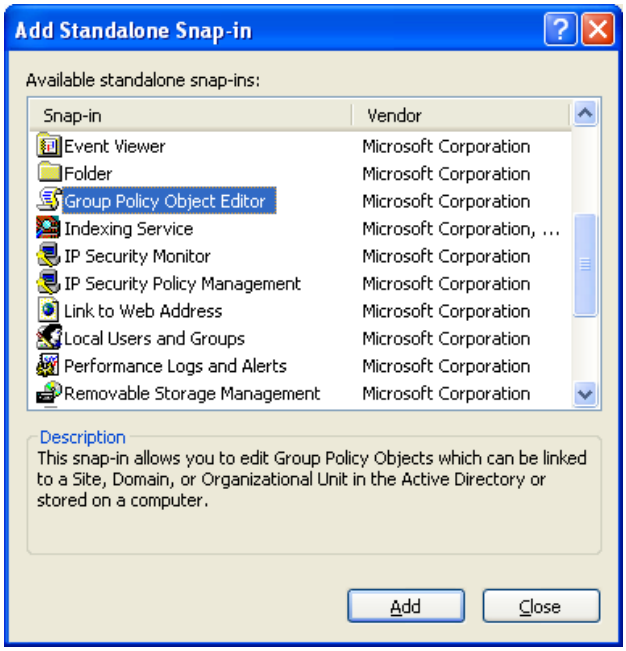
3. Το παράθυρο του **Console** θα εμφανιστεί. Κάντε κλικ πάνω στο **File**, μετά στο **Add/Remove Snap-in**, πάλι μετά **Add.** Επιλέξτε **Group Policy** και κάντε κλικ στο **Add**.



Εικόνα 196: Console1

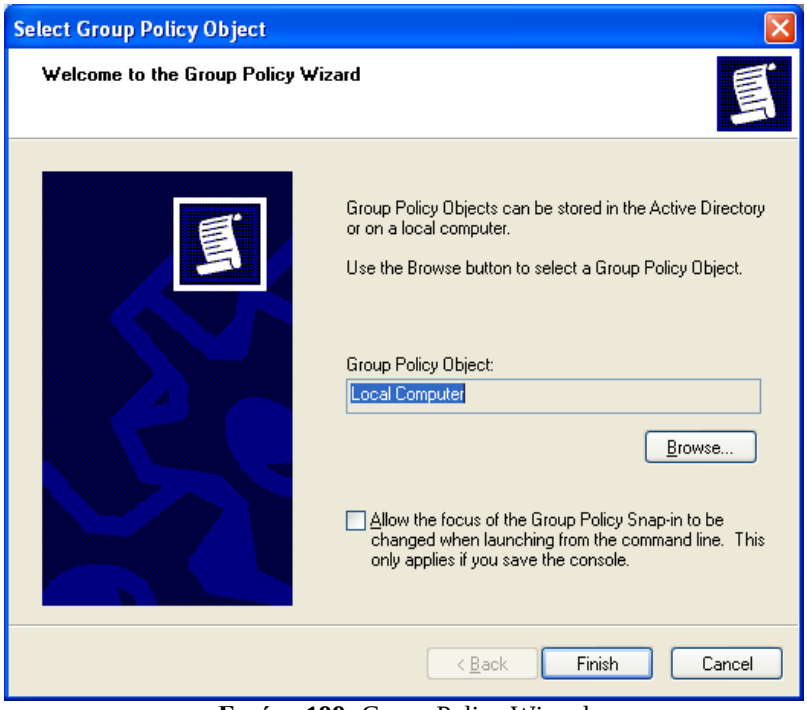


Εικόνα 197: Add/Remove Snap-in



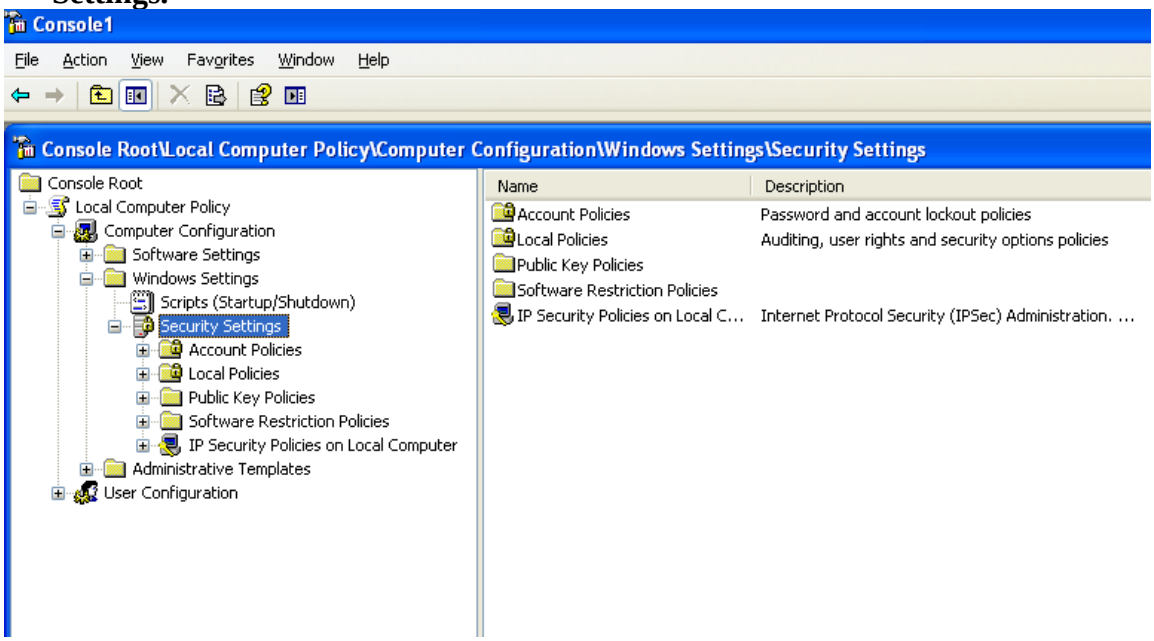
Εικόνα 198: Add Standalone Snap-in

4. Κάντε κλικ στο **Finish.**



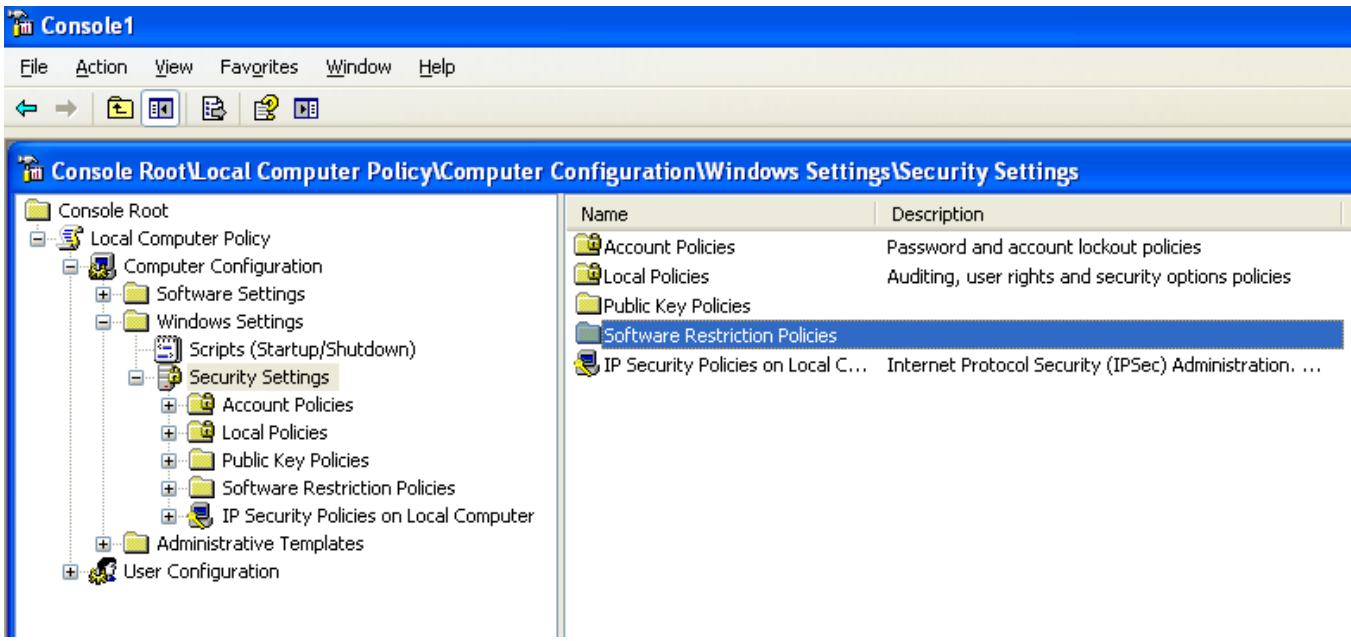
Εικόνα 199: Group Policy Wizard

5. Στο παράθυρο του Console, επεκτείνετε το **Local Computer Policy**, μετά το **Computer Configuration**, μετά το **Windows Settings**, μετά το **Security Settings.**

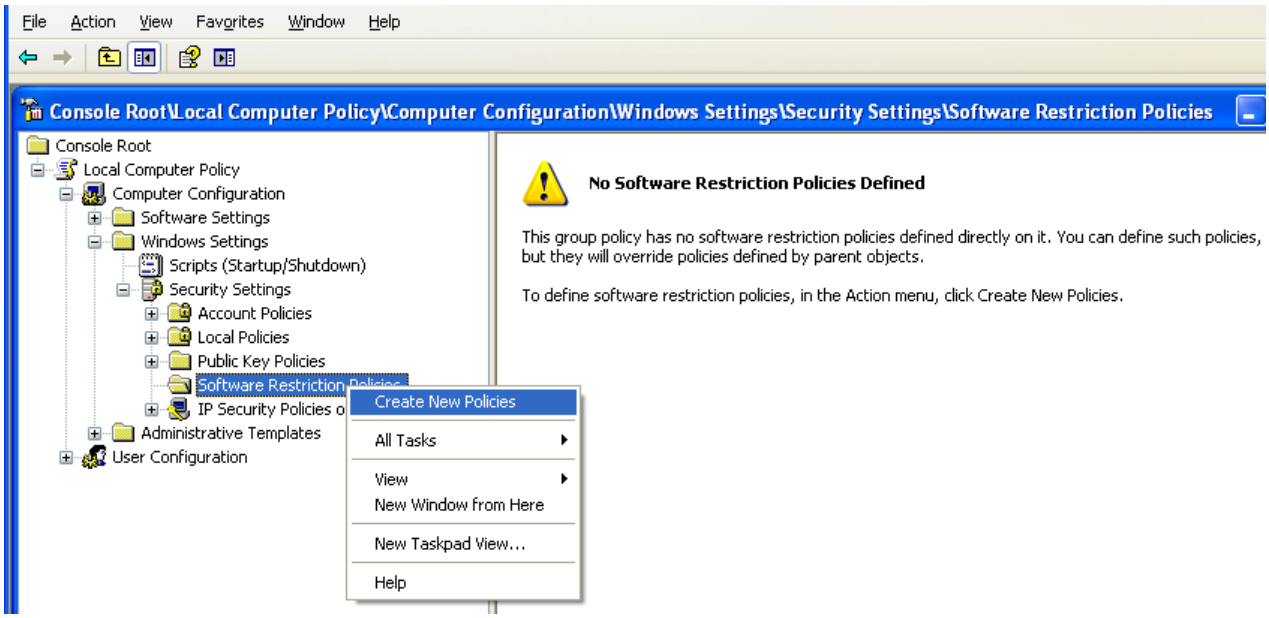


Εικόνα 200: Security Settings

6. Εάν στο φάκελο του **Security Settings(ρυθμίσεις ασφαλείας)** δε περιέχουν **Software Restriction Policies(πολιτικές περιορισμού λογισμικού)**, μια νέα πολιτική πρέπει να δημιουργήσετε. Για να το κάνετε αυτό , κάντε κλικ στο **Action,** μετά επιλέξτε **Create New Policies**. Επιστρέψτε στο φάκελο του **Security Settings** .

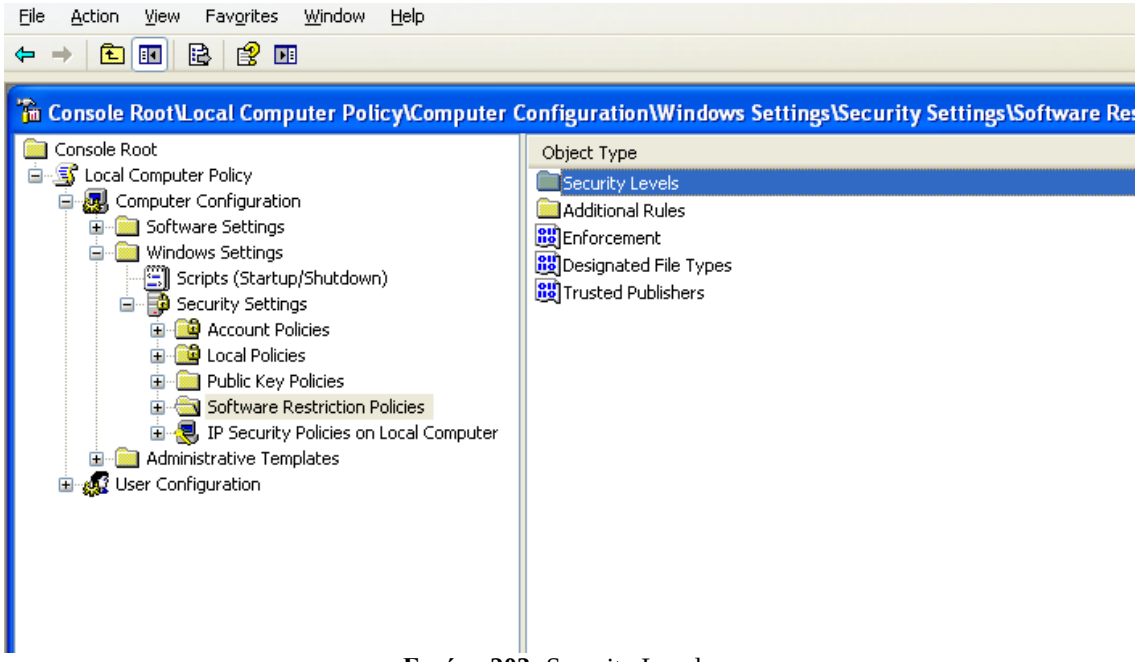


Εικόνα 201: Software Restriction Policies



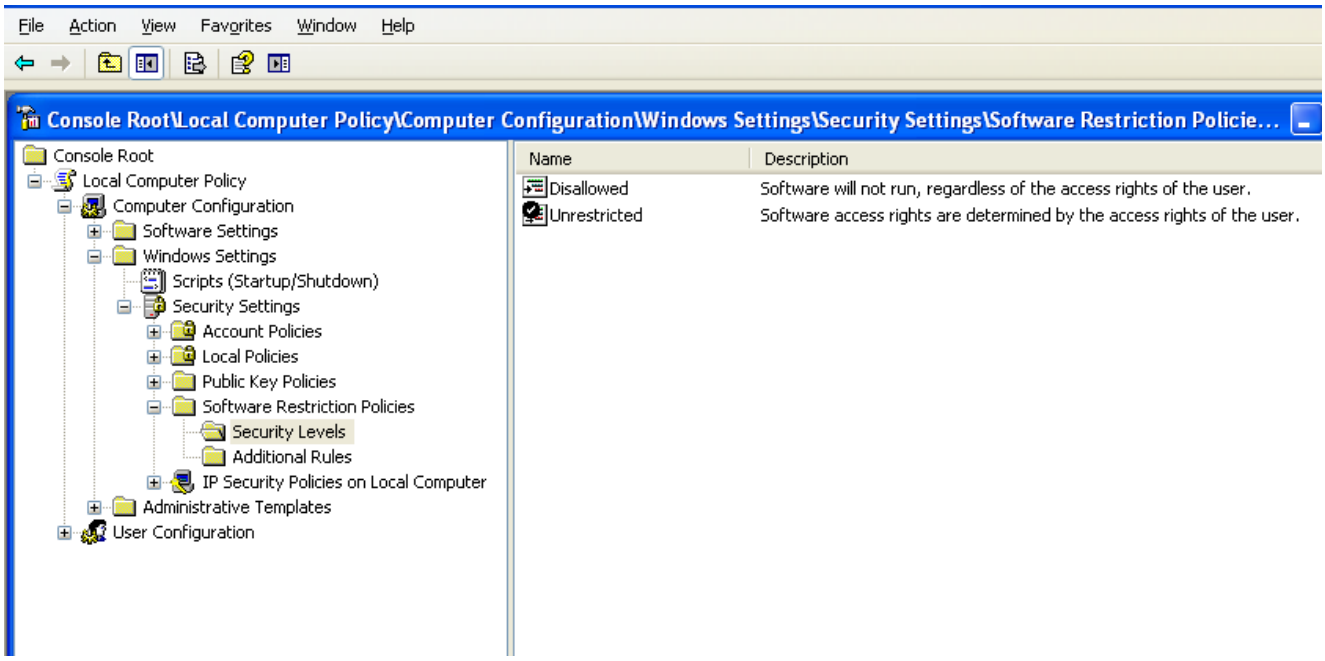
Εικόνα 202: Create New Policies

7. Από το φάκελο **Security Settings** , κάντε κλικ στο **Software Restriction Policies** και μετά στο φάκελο **Security Levels** . Αν στο φάκελο **Security Levels** δεν υπάρχει, μια νέα πολιτική πρέπει να δημιουργήσετε. Για να το κάνετε αυτό, κάντε κλικ στο **Action,** μετά επιλέξτε **Create New Policies**, και εισάγετε το στο φάκελο **Security Levels** .



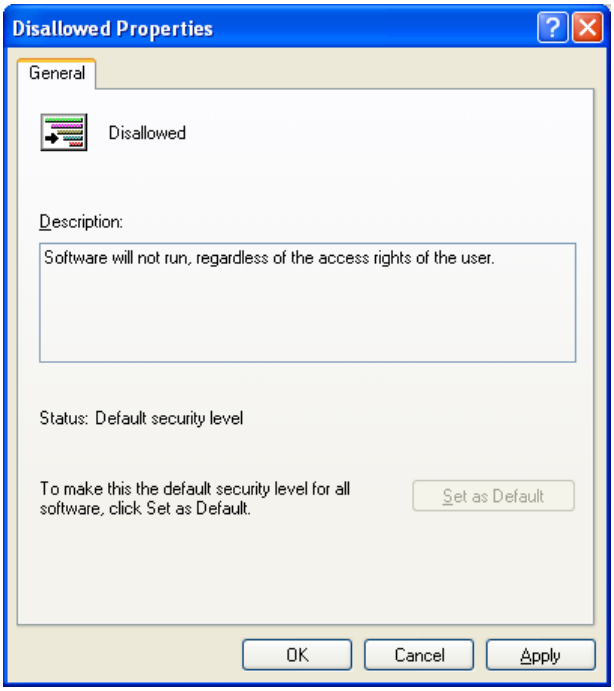
Εικόνα 203: Security Levels

8. Υπάρχουν δυο επιλογές: Disallowed (το λογισμικό δε θα τρέχει, ανεξάρτητα από τα δικαιώματα του χρήστη), και Unrestricted (τα δικαιώματα πρόσβασης στο λογισμικό καθορίζονται από τα δικαιώματα πρόσβασης του χρήστη.) Διπλό κλικ στο **Disallowed**. Κάντε κλικ στο **Set as Default**, και μετά επιλέξτε **OK** για να συνεχίσετε.



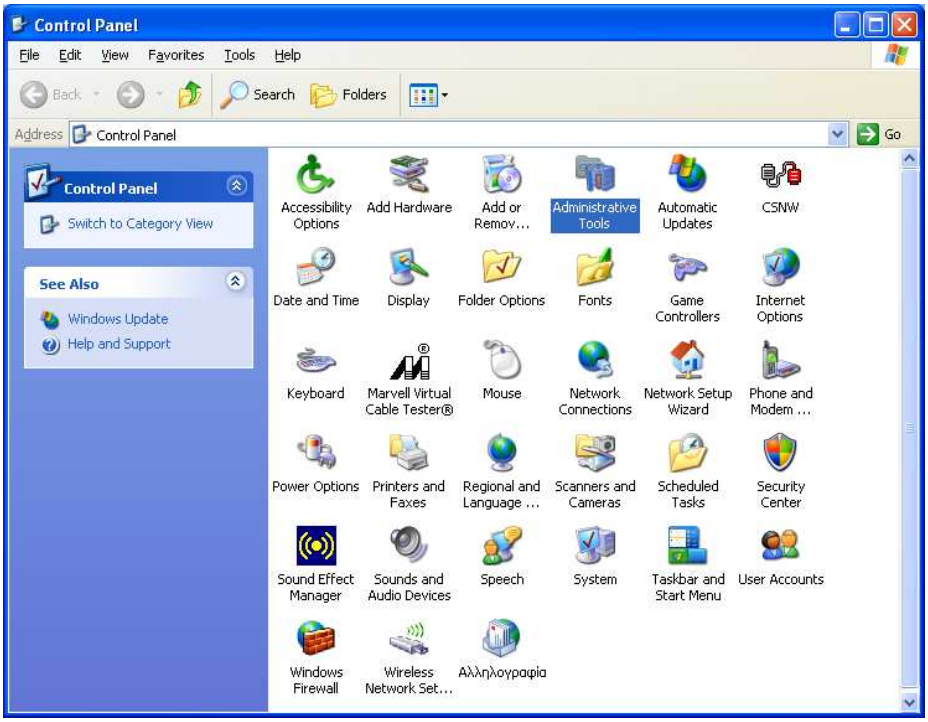
Εικόνα 204: Security levels Description

Εικόνα 205: Disallowed Properties

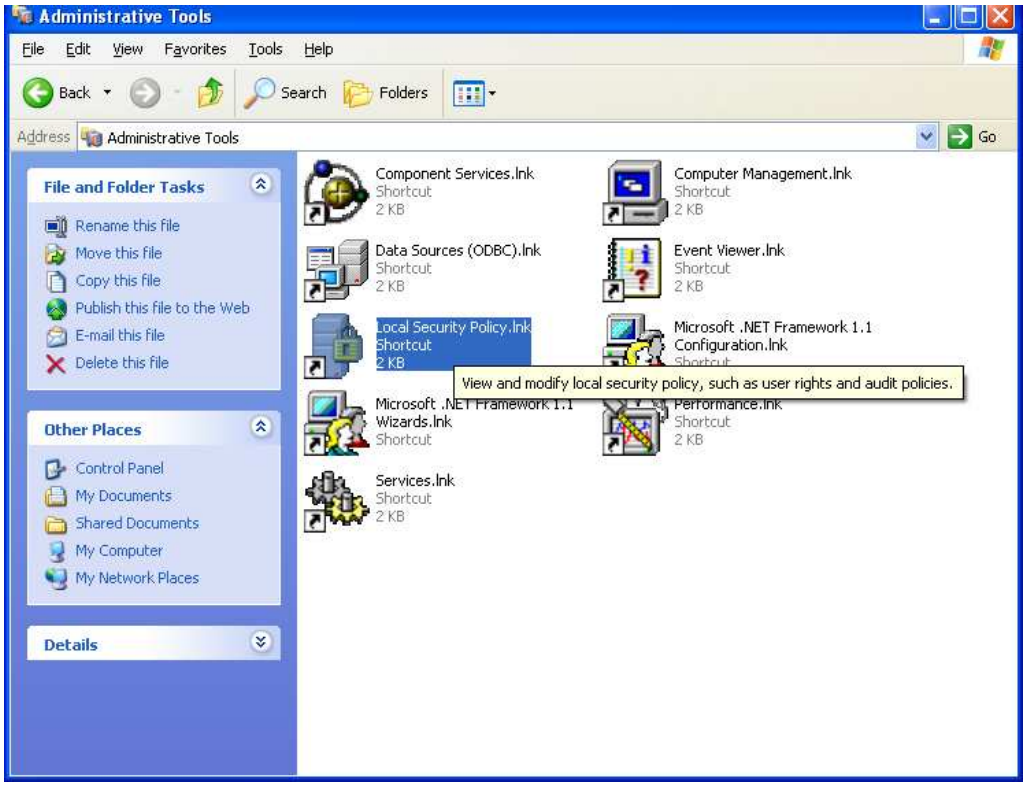


Εικόνα 206: Disallowed Set As Default

9. Για να ανοίξετε τη **Local Security Policy(τοπική πολιτική ασφαλείας),** κάντε κλικ στο **Start,** μετά επιλέξτε **Control Panel.** Κάντε κλικ στο **Administrative Tools**, και μετά κάντε κλικ στο **Local Security Policy**. Θα πρέπει να ανοιχτεί το παράθυρο του Local Security Settings.

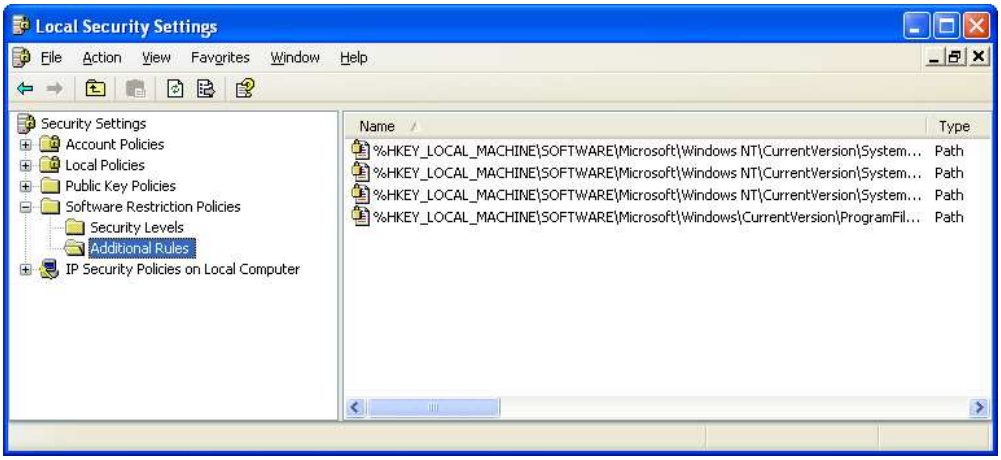


Εικόνα 207: Administrative Tools



Εικόνα 208: Local Security Policy

10. Επεκτείνετε το **Software Restrictions Policies** και κάντε κλικ στο φάκελο **Additional Rules** .Στο δεξιό τμήμα θα πρέπει να δείχνει τις προεπιλεγμένους κανόνες .

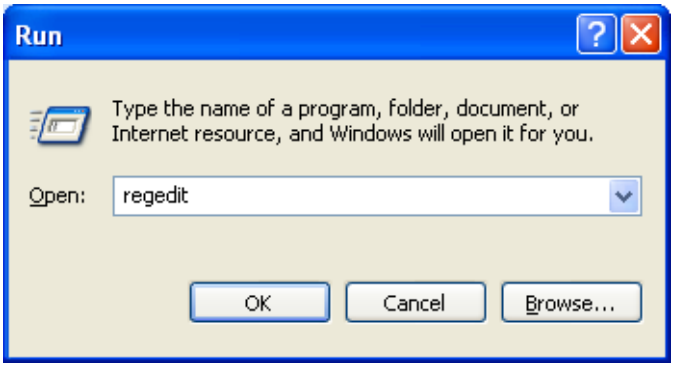


Εικόνα 209: Additional Rules

11. Κάντε δεξί κλικ στο πλαίσιο του δεξιού τμήματος και προσθέστε τους κανόνες για την εγκατάσταση από τις ακόλουθες επιλογές:

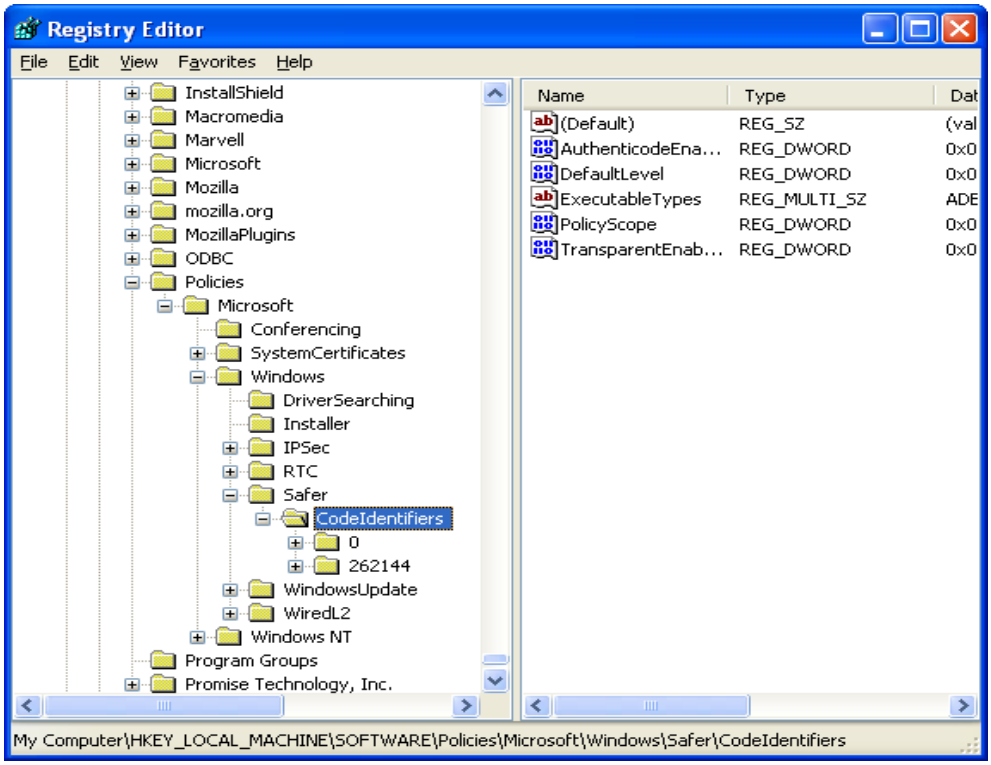
- **Certificate Rule(πιστοποιητικό άρθρο).** Το πιστοποιητικό άρθρο χρησιμοποιεί ένα πιστοποιητικό για την επαλήθευση γνησιότητας του προγράμματος που πρόκειται να εκτελεστεί. Από προεπιλογή, το πιστοποιητικό με βάση το **Software Policy** οι κανόνες είναι απενεργοποιημένοι. Για να ενεργοποιήσω τους **Certificate Rules,** επεξεργαστείτε το μητρώο όπως παρακάτω :

  - Κάντε κλικ στο **Start**, πατήστε **Run**, πληκτρολογήστε **regedit**, και μετά κάντε κλικ στο **OK**.



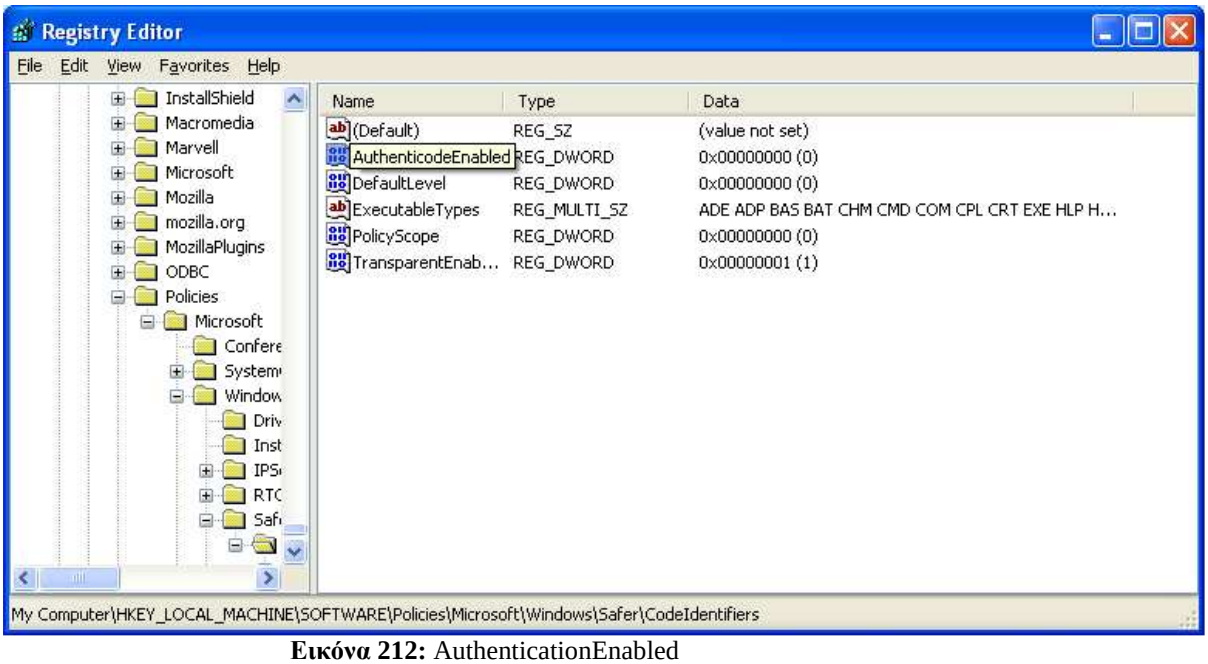
Εικόνα 210: Run

  - Επεξεργαστείτε το κλειδί **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows \Safer\CodeIdentifiers**.

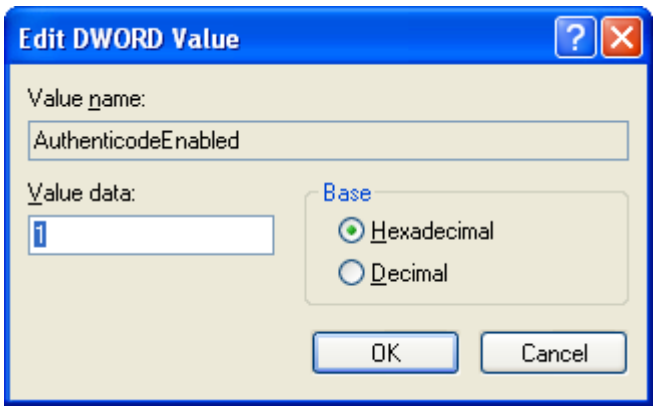


Εικόνα 211: Registry Editor

- Επιλέξτε τη τιμή **AuthenticodeEnabled** και αλλάξτε τη τιμή του δεδομένου από **0** σε **1**.



Εικόνα 212: AuthenticationEnabled



Εικόνα 213: Edit DWORD Value

- Πατήστε **OK,** κάντε κλικ στο **File** και **Exit** να κλείσετε το **regedit**.

- **Hash Rule**. Το hash rule επιτρέπει μόνο σε ένα πρόγραμμα για να εκτελεστεί αν το hash για το αρχείο αυτό ταιριάζει με το γνωστό καλό hash όπου το λειτουργικό σύστημα αναμένει. Αυτό προστατεύει από ένα πρόγραμμα που αντικαθίσταται από μια τροποποιημένη έκδοση που περιέχει κακόβουλα προγράμματα. Τα Hashes δεν εξαρτώνται από το όνομα του αρχείου ή τη θέση; Ως εκ τούτου, εάν ένα αρχείο έχει μετονομαστεί ή έχει μετακινηθεί, η εκτέλεση θα εξακολουθεί να επιτρέπεται ή θα απορρίπτεται με βάση το hash. Εάν το μέγεθος του αρχείου αλλάζει, το hash θα καθίσταται άκυρο και η εκτέλεση θα αμφισβητηθεί. Μπορεί να είναι resource-intensive για να εντοπίσει όλα τα προγράμματα που ενδέχεται να απαιτούνται σε κάθε σύστημα και να διατηρεί και να διανέμει τα τρέχουσα hashes για όλα τα προγράμματα.

- **Internet Zone Rule.** Ο κανόνας αυτός εφαρμόζεται για τον Windows Installer μόνο. Παρέχει ένα τρόπο για να περιορίσει το λογισμικό που μπορεί να εκτελείται από απομακρυσμένες τοποθεσίες.

- **Path Rule**. Το Path Rule επιτρέπει στο χρήστη να ορίσει τα αρχεία στα οποία επιτρέπεται να λειτουργούν με βάση τους περιορισμούς διαδρομής. Η διαδρομή μπορεί να είναι ένα ολόκληρος κατάλογος ή ένα συγκεκριμένο αρχείο. Κατά τον ορισμό ενός Path Rule, ιδιαίτερη προσοχή θα πρέπει να λαμβάνεται όταν το επίπεδο ασφαλείας έχει οριστεί σε Disallowed και καθορίζει τη διαδρομή του φακέλου των Windows, επειδή αυτό θα μπορούσε να εμποδίσει την εκτέλεση των προγραμμάτων ουσιαστικής σημασίας για τα Windows XP. Ένας κρίσιμος περιορισμός του Path Rule είναι ότι αν ένας ολόκληρος κατάλογο έχει καθοριστεί, όλα τα προγράμματα που βρίσκονται σε αυτόν τον κατάλογο θα πρέπει να επιτρέπονται να εκτελούνται. Αυτό σημαίνει ότι, χωρίς άδεια ή κακόβουλα προγράμματα που διατίθενται στην πορεία θα επιτρέπονται να εκτελούνται.

3.5 Securing Network Interfaces

Από προεπιλογή, τα Windows XP περιλαμβάνουν μια σειρά από πρωτόκολλα και συστατικά μέρη του δικτύου που συνήθως δεν απαιτούνται σε όλα τα περιβάλλοντα. Για παράδειγμα, the File and Printer Sharing for Microsoft Networks service και the

Client for Microsoft Networks περιλαμβάνονται στις περισσότερες εγκαταστάσεις των Windows XP. Τα χαρακτηριστικά αυτά επιτρέπουν στο χρήστη να μοιράζεται πόρους με το δίκτυο των Windows με άλλα συστήματα, αλλά το σύστημα μπορεί να αυξήσει το επίπεδο έκθεσης. Ο χρήστης θα πρέπει να λειτουργεί το σύστημα με μόνο τα απαραίτητα πρωτόκολλα δικτύου και να απενεργοποιεί τη Microsoft δικτύωση του client / server, εφόσον δεν τα χρησιμοποιεί.

3.5.1 Unneeded Networking Components

Όπως αναφέρθηκε στο τμήμα 2.1.2.1, το δίκτυο πελατών, των υπηρεσιών, καθώς και τα πρωτόκολλα που δεν είναι απαραίτητα θα πρέπει να απενεργοποιούνται. Αυτό μειώνει την πιθανότητα ότι το σύστημα θα είναι σε κίνδυνο ή κατάχρησης. Με προσοχή κατά την απενεργοποίηση των συνιστωσών του δικτύου, διότι αυτό μπορεί να προκαλέσει διακοπή λειτουργικότητας, μερικές φορές απροσδόκητα. Τα παρακάτω στοιχεία είναι υποψήφια για την απενεργοποίησή του:

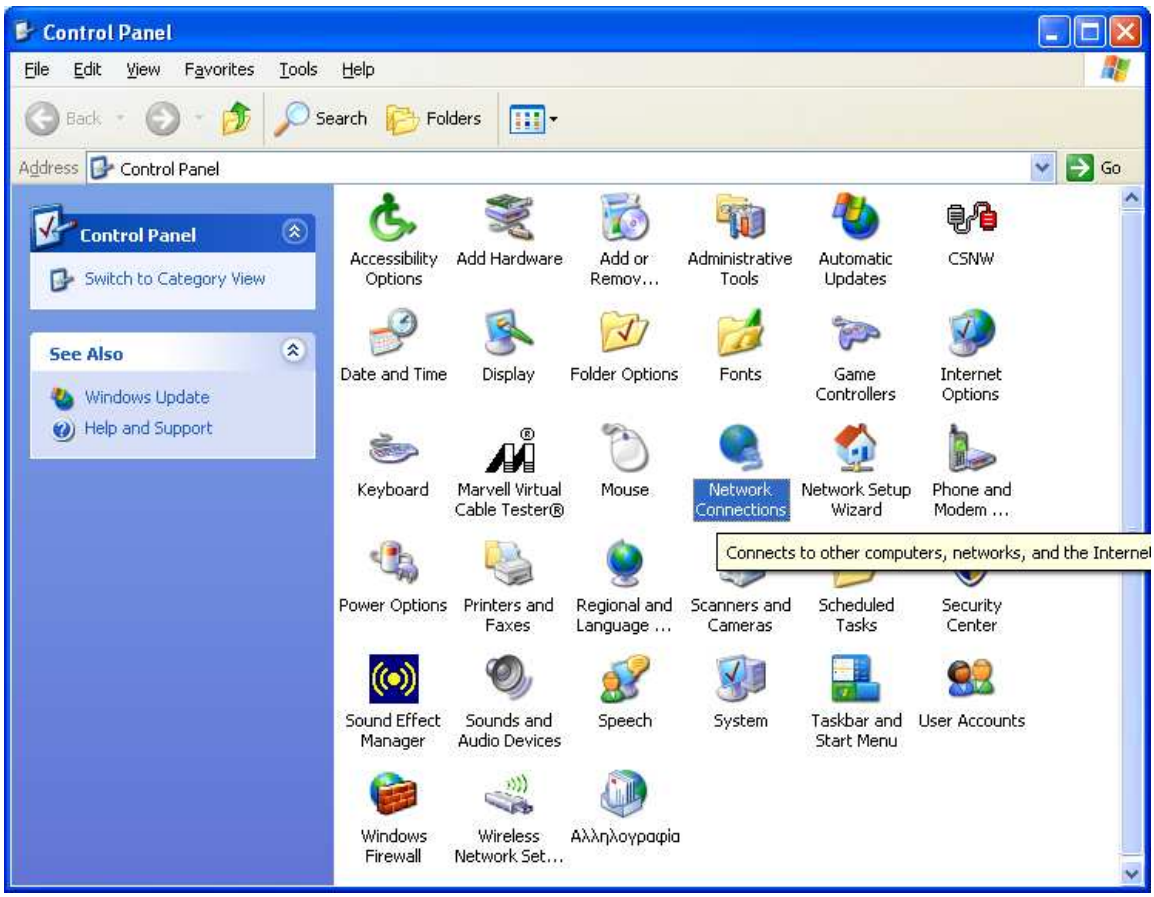
- **Το QoS Packet Scheduler** έχει σχεδιαστεί για να δώσει προτεραιότητα στη κίνηση στο δίκτυο με την εφαρμογή ή την υπηρεσία σε αργές συνδέσεις δικτύου. Οι περισσότερες εφαρμογές δεν είναι γνώστες του QoS και μερικές είναι ασυμβίβαστες με QoS, τόσο το QoS Packet Scheduler δεν είναι επωφελής στις περισσότερες περιπτώσεις. Σε γενικές γραμμές, το QoS Packet Scheduler θα πρέπει να είναι απενεργοποιημένο χωρίς να είναι ελεγμένο σε ένα συγκεκριμένο περιβάλλον που αποδεικνύει ότι είναι επωφελής για τον μετριασμό του εύρους ζώνης σε θέματα δικτύου .

- Η απεγκατάσταση της **χρήση αρχείων και εκτυπωτών για δίκτυα του Microsoft service** θα εμποδίσουν άλλα συστήματα από τη σύνδεση με το τοπικό αρχείο και τον εκτυπωτή ; Δεν θα αποτρέψει τους χρήστες του τοπικού δικτύου από τη σύνδεση στο απομακρυσμένο αρχείο και από τον εκτυπωτή . Επομένως, αφήστε αυτή την υπηρεσία να εγκατασταθεί μόνο εάν το τοπικό σύστημα μετέχει στους πόρους (π.χ. αρχεία, εκτυπωτές) και οι χρήστες χρειάζονται σχετικά με άλλα συστήματα και πρέπει να συνδεθούν με αυτούς τους πόρους μέσω του δικτύου ή με αναγκαίες εφαρμογές (π.χ., το MBSA, τη remote administration) που απαιτούν την υπηρεσία .

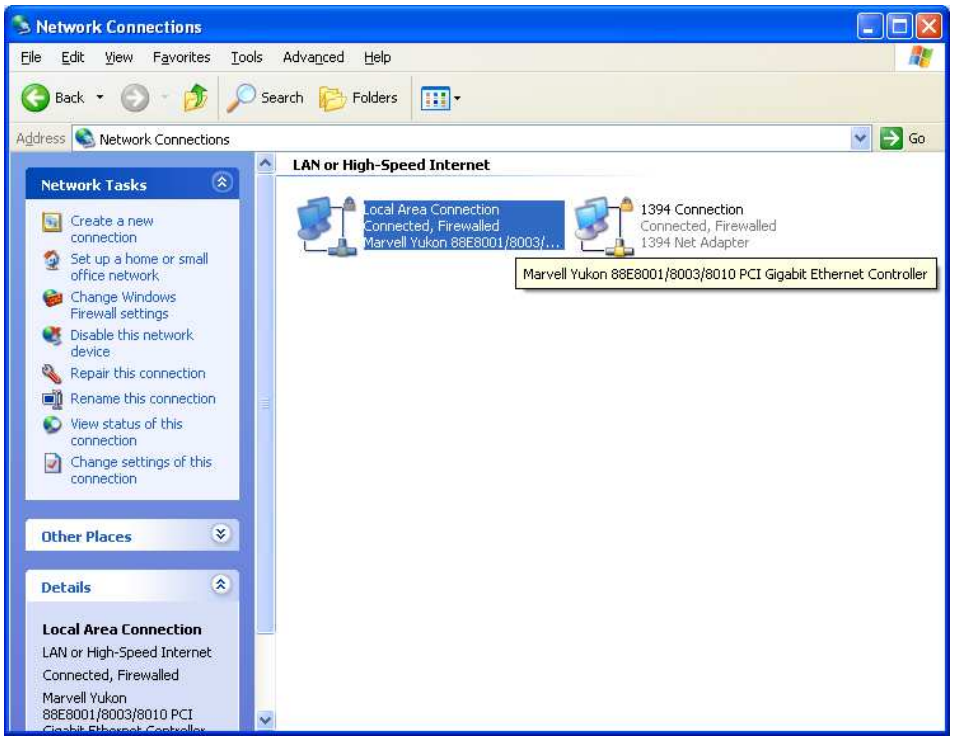
- Η απεγκατάσταση του προγράμματος **Client for Microsoft Networks** θα εμποδίσει το τοπικό σύστημα από τη εγκαθίδρυση συνδέσεων δικτύου με άλλα συστήματα αρχείων της Microsoft και από τον εκτυπωτή . Τα περισσότερα συστήματα θα απαιτήσουν από τον πελάτη να ενεργοποιηθούν, γι 'αυτό θα πρέπει γενικά να απενεργοποιηθεί μόνο όταν το σύστημα έχει ιδιαίτερα υψηλές ανάγκες ασφαλείας.

Για να απενεργοποιήσετε οποιαδήποτε από αυτά τα συστατικά, ακολουθήστε τα παρακάτω βήματα:

1. Κάντε κλικ στο μενού **Start**, διάλεξε **Control Panel**, επίλεξε **Network Connections**, και κάντε διπλό κλικ στο**Local Area Connection**.

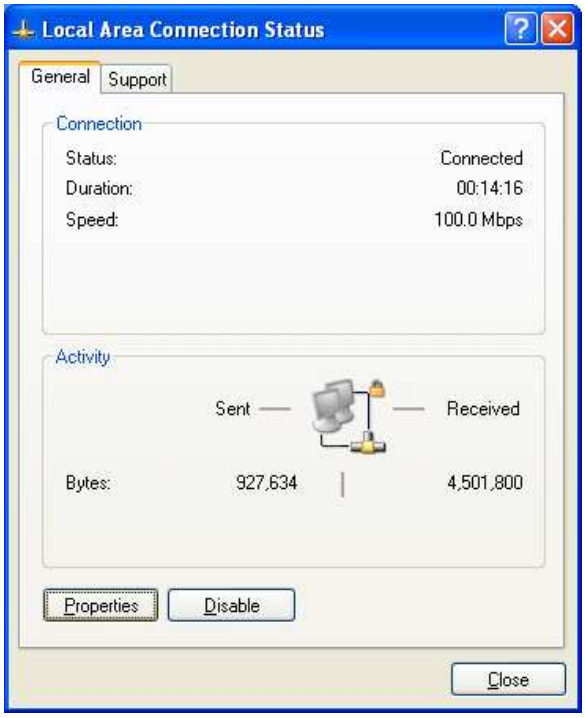


Εικόνα 214: Network Connections



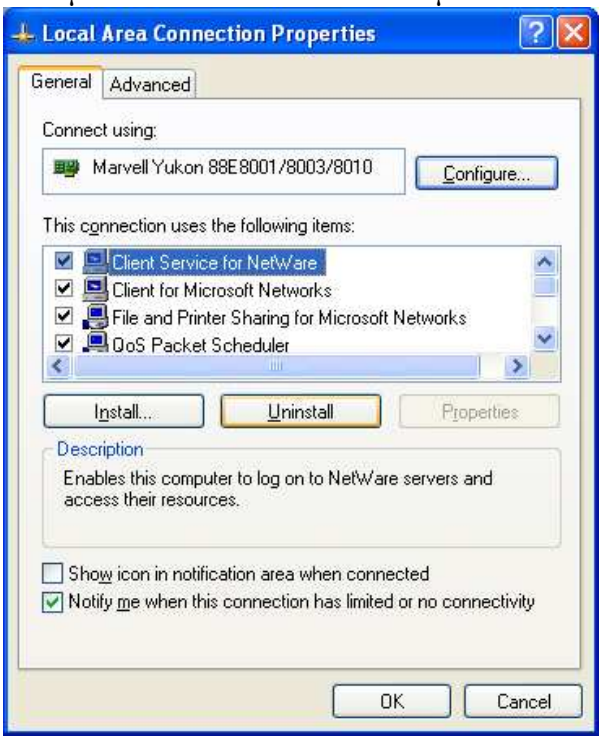
Εικόνα 215: Local Area Connection

2. Κάντε κλικ στο κουμπί **Properties**.



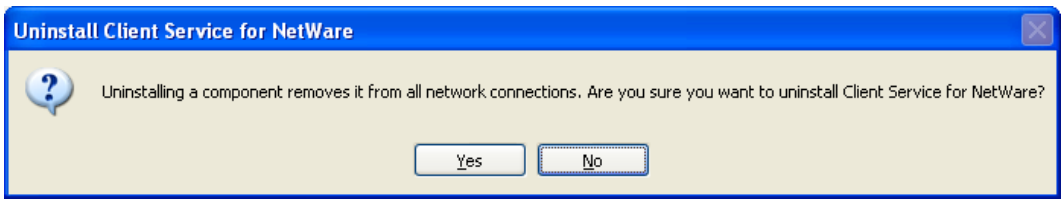
Εικόνα 216: Local Area Connection Properties

3. Επιλέξτε το αντικείμενο και κάντε κλικ στο κουμπί **Uninstall**.



Εικόνα 217: Client Service for NetWare

4. Πατήστε **Yes** να προχωρήσετε.

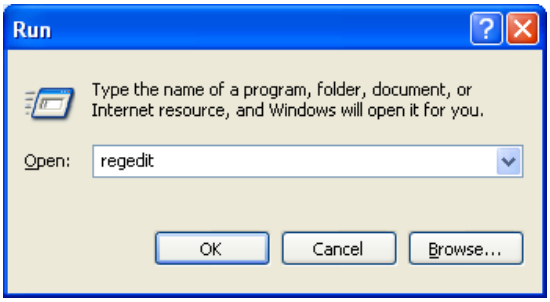


Εικόνα 218: Unistall Cilent Service For NetWare

3.5.2 Use of Port 445

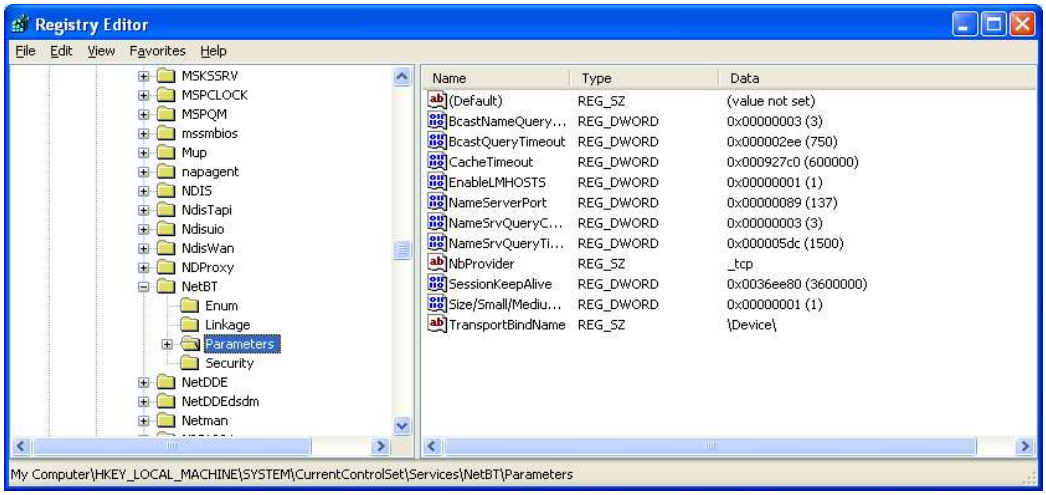
Εάν το σύστημα αυτό πρέπει να συνδεθεί με άλλα συστήματα Windows όπως μοίρασμα αρχείων, μπορείτε να χρησιμοποιείτε είτε την παραδοσιακή θύρα 139 ή νέα θύρα 445. Από προεπιλογή, αυτό θα προσπαθεί να συνδεθεί στη θύρα 139 πριν από τη προσπάθεια της θύρας 445, μέχρι την απενεργοποίηση της θύρας 445 θα πρέπει να οδηγείτε να εκθέτονται μόνο στη συμβατική θύρα 139. Πριν από την εφαρμογή αυτού του συστήματος τροποποίησης, αναφερθείτε σε τοπικές πολιτικές για να επιβεβαιωθεί ότι είναι αποδεκτό και κατάλληλο για το περιβάλλον. Επίσης, από προεπιλογή, το Windows Firewall αποκλείει όλη τη εισερχόμενη κίνηση δικτύου που προορίζονται για τη θύρα 445. Για να απενεργοποιήσετε τη χρήση της θύρας 445, ακολουθήστε τα παρακάτω βήματα:

1. Κάντε κλικ στο μενού **Start** και επιλέξτε **Run**. Ανοίξτε το **regedit** και πατήστε **OK**.



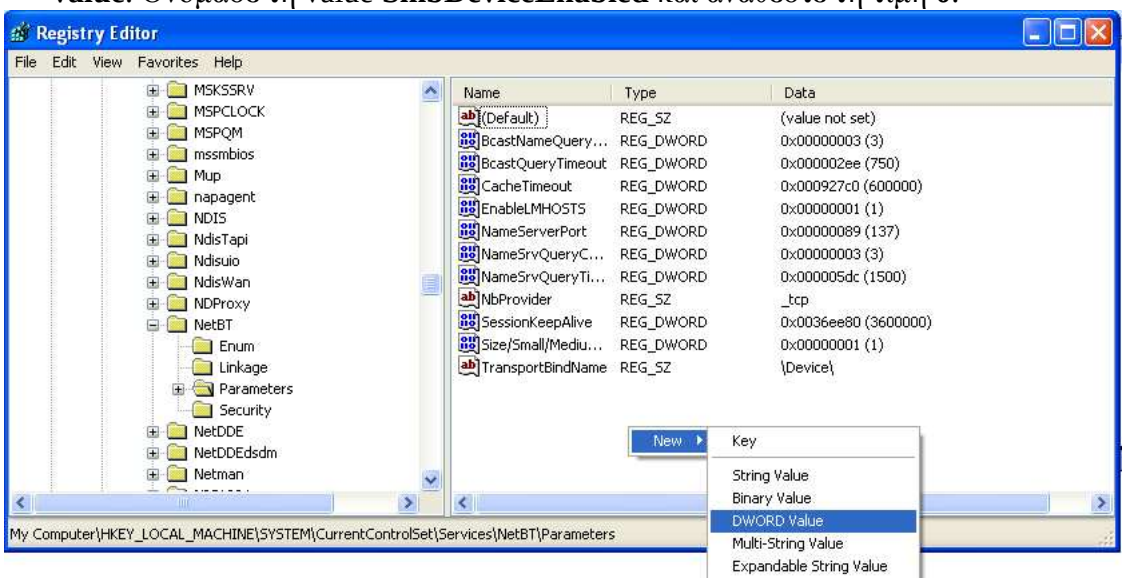
Εικόνα 219: Regedit

2. Εντοπίστε την ακόλουθη καταχώρηση: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters.**

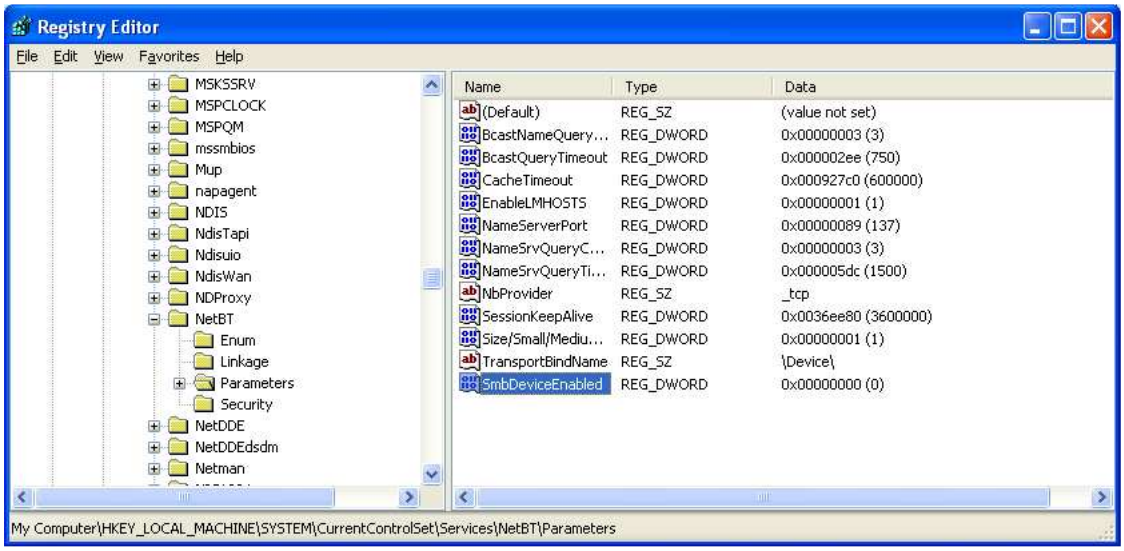


Εικόνα 220: NetBT Parameters

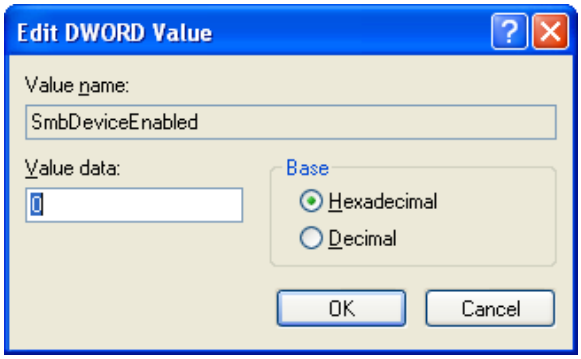
3. Κάντε δεξί κλικ στο δεξιό τμήμα , επιλέξτε **New**, και κάντε κλικ στο **DWORD value**. Ονόμασε τη value **SmbDeviceEnabled** και αναθέστε τη τιμή **0**.



Εικόνα 221: New DWORD Value



Εικόνα 222: SmbDeviceEnabled



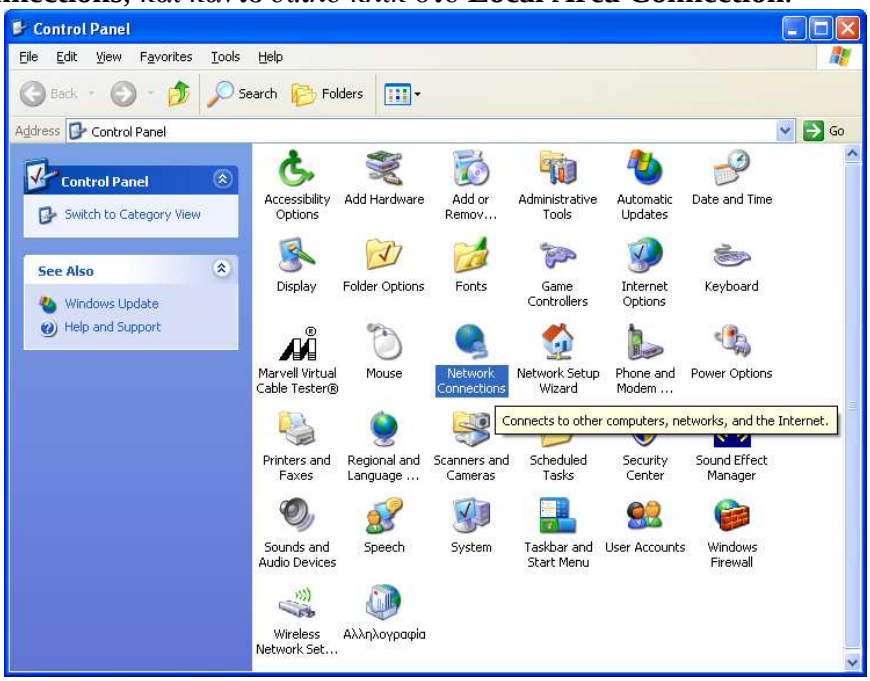
Εικόνα 223: Edit DWORD Value

4. Έξοδο από **regedit**.

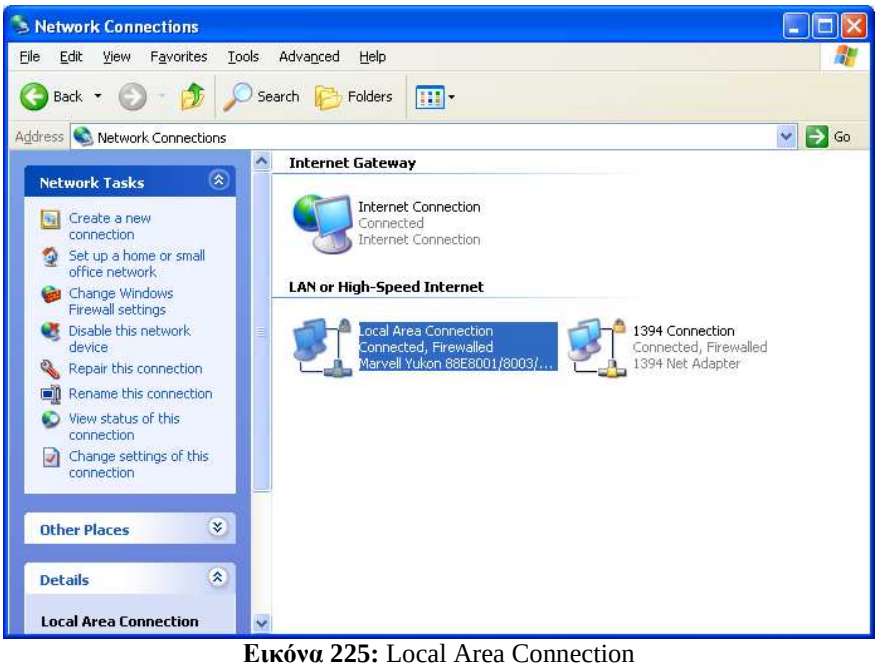
3.5.3 TCP/IP Configuration

Το προεπιλεγμένο πρωτόκολλο TCP / IP περιέχει κάποιες ρυθμίσεις που θα πρέπει να τροποποιηθούν για τη βελτίωση της ασφάλειας. Ωστόσο, κάθε ρύθμιση, θα μπορεί να έχει αρνητική επίπτωση στην λειτουργικότητα που παρέχει το σύστημα, γι 'αυτό είναι πολύ σημαντικό να κατανοήσουμε τις επιπτώσεις της αλλαγής κάθε ρύθμισης. Τα παρακάτω βήματα για την τροποποίηση των ρυθμίσεων περιλαμβάνουν επεξήγηση της σημασίας που έχει κάθε ρύθμιση:

1. Κάντε κλικ στο μενού **Start**, διαλέξτε **Control Panel**, επιλέξτε **Network Connections**, και κάντε διπλό κλικ στο **Local Area Connection**.

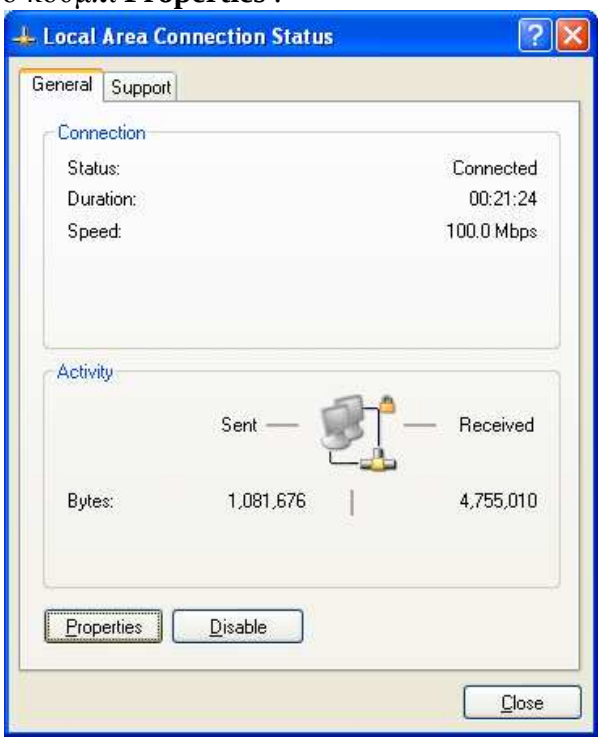


Εικόνα 224: Network Connections



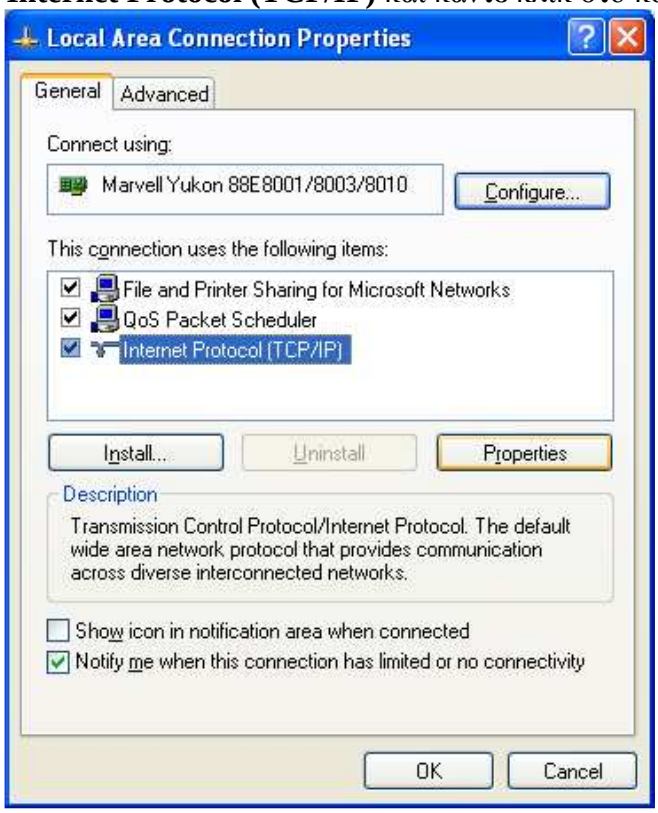
Εικόνα 225: Local Area Connection

2. Κάντε κλικ στο κουμπί **Properties** .



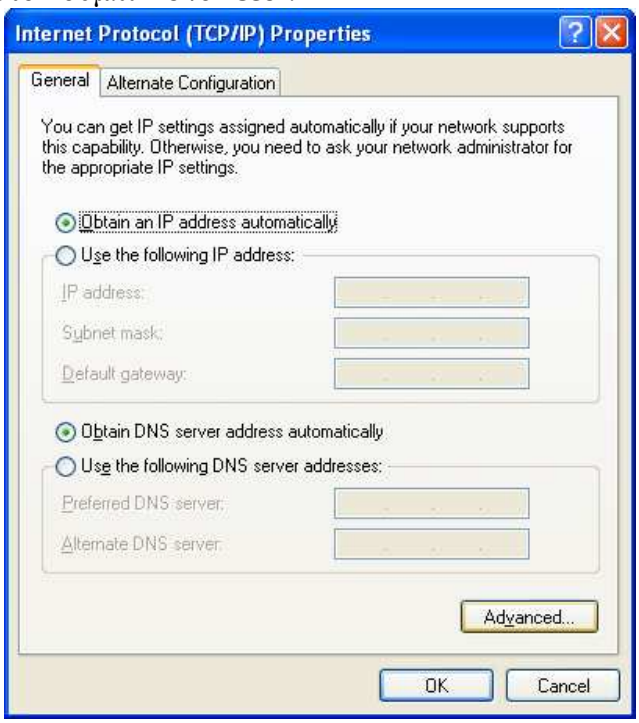
Εικόνα 226: Local Area Connection Properties

3. Επιλέξτε το **Internet Protocol (TCP/IP)** και κάντε κλικ στο κουμπί **Properties**.



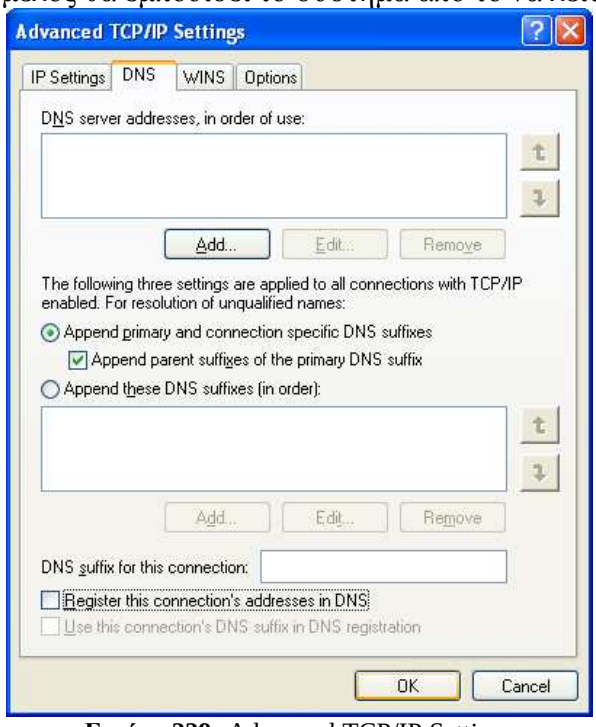
Εικόνα 227: Internet Protocol(TCP/IP)

4. Κάντε κλικ στο κουμπί **Advanced** .



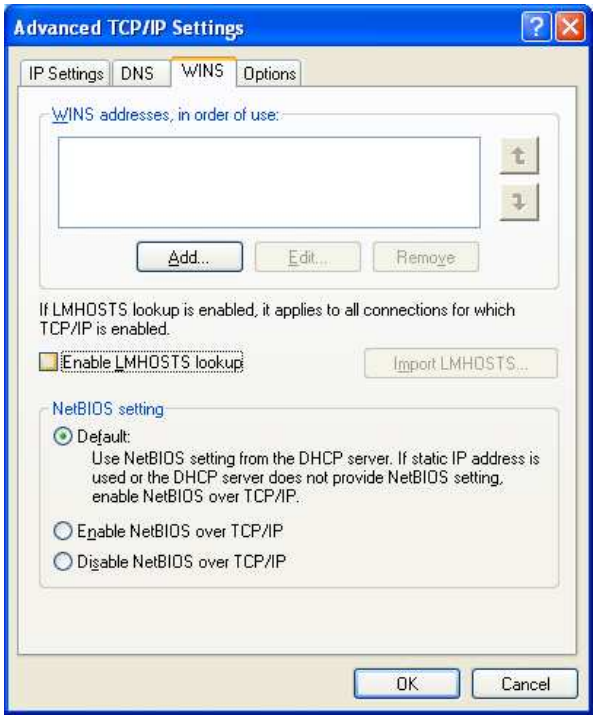
Εικόνα 228: Internet Protocol(TCP/IP) Properties

5. Επιλέξτε τη καρτέλα **DNS** και ξεμαρκάρετε το κουτί **Register this connection's addresses in DNS** . Αν το σύστημα έχει καταχωρηθεί στο DNS, θα μπορούσε να παρέχει πληροφορίες σχετικά με το σύστημα σε ένα παράνομο μέρος που με πληροφορίες σχετικά με το DNS . Όμως, απενεργοποιώντας αυτή τη ρύθμιση σε ένα πρόσθετο μέλος θα εμποδίσει το σύστημα από το να λειτουργήσει σωστά.



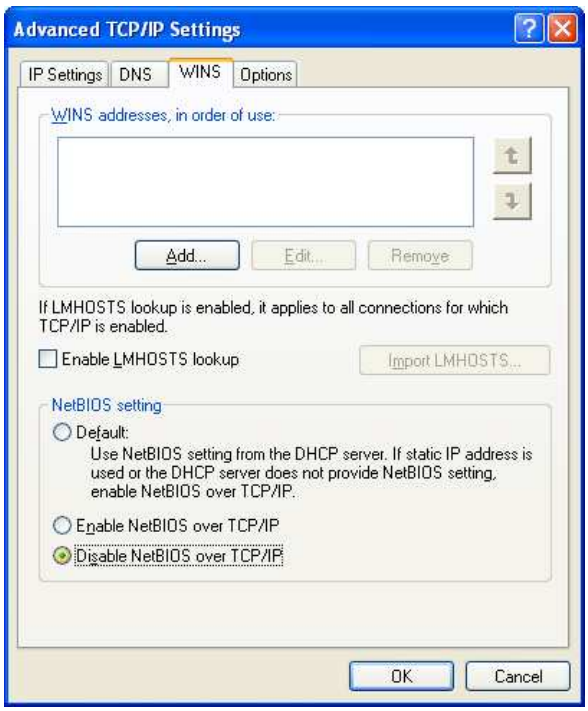
Εικόνα 229: Advanced TCP/IP Settings

6. Επιλέξτε τη καρτέλα **WINS** . Ξεμαρκάρετε το κουτί **Enable LMHOSTS lookup** εάν δεν είναι αναγκαίο για τη συμβατότητα με τα κληροδοτούμενα συστήματα..



Εικόνα 230: WINS

7. Επιλέξτε το κουμπί **Disable NetBIOS over TCP/IP** χωρίς αυτή η λειτουργία απαιτείται από το σύστημα. Γενικά, NetBIOS over TCP/IP χρειάζονται μόνο αν το σύστημα χρειάζεται να επικοινωνήσει με τα κληροδοτούμενα συστήματα που λειτουργούν με Windows NT, Windows 95, ή Windows 98. Αν το NetBIOS over TCP/IP είναι ενεργοποιημένος, οι πόροι του συστήματος μπορεί να εκτίθενται σε δίκτυο που βασίζεται στις επιθέσεις.



Εικόνα 231: Disable NetBIOS over TCP/IP

8. Πατήστε **OK**, πάλι **OK**, και μετά **Close**.

3.6 Windows Firewall

Το τείχος προστασίας των Windows είναι ενσωματωμένο στα Windows XP[50]. Μπορεί να ρυθμιστεί για να περιορίσεις όλες τις εισερχόμενες συνδέσεις, αλλά δεν μπορεί να μπλοκάρει κάθε φίλτρο ή τις εξερχόμενες συνδέσεις. Το Windows Firewall ανιχνεύει κάθε κυκλοφορία που προέρχεται από τον τοπικό κεντρικό υπολογιστή με τη διατήρηση ενός πίνακα όλων των επικοινωνιών. Τα εισερχόμενα πακέτα είναι επιτρεπτά, αν μια αντίστοιχη θέση στον πίνακα που δείχνει ότι η σύνδεση δικτύου έχει ξεκινήσει από το local host. Το κύριο όφελος του Windows Firewall είναι σε περιορισμό των συνδέσεων δικτύου σε έναν υπολογιστή, με αποτέλεσμα τη μείωση της έκθεσης του υπολογιστή σε δίκτυο που βασίζεται επιθέσεις, όπως τα worms.

Το τείχος προστασίας των Windows είναι ενεργοποιημένο από προεπιλογή για κάθε διασύνδεση δικτύου. Αυτό προσφέρει άμεση προστασία από επιθέσεις με βάση το δίκτυο για όλες τις συνδέσεις του δικτύου, συμπεριλαμβανομένων των LAN (ενσύρματων και ασύρματων), dial-up και VPN. Δυστυχώς, εξ ορισμού, μπορεί επίσης να απαιτείται και ακούσια διακοπή λειτουργικότητας. Για παράδειγμα, το Windows Firewall αποκλείει όλες τη εισερχόμενη κυκλοφορία που απευθύνεται στη θύρα TCP 445, η οποία μπορεί να εμποδίσει τους διαχειριστές να χρησιμοποιούν

[50]Το Windows Firewall προστέθηκε στο Windows XP στο Service Pack 2. Πριν από το SP2, το ενσωματωμένο ονομάστηκε Internet Connection Firewall (ICF). Για περισσότερες πληροφορίες για το ICF, διαβάστε το άρθρο MSKB 320855, *Description of the Windows XP Internet Connection Firewall*, διαθέσιμο στη σελίδα http://support.microsoft.com/?id=320855.

διάφορα όπως το MMC snap-ins για τη διαχείριση του συστήματος από απόσταση[51]. Επίσης, αν δεν έχει ρυθμιστεί σωστά, το Windows Firewall μπορεί επίσης να εμποδίσει τη χρήση των αρχείο της Microsoft και τις υπηρεσίες εκτύπωσης, καθώς και άλλες υπηρεσίες και εφαρμογές. Εάν το Windows Firewall και ένα τρίτο μέρος του host, βασισμένο σε προστασία είναι και τα δυο ενεργοποιημένα, το Windows Firewall μπορεί να εμποδίσει την κυκλοφορία των υπολοίπων τειχών προστασίας που έχει ρυθμιστεί έτσι ώστε να τα επιτρέπει, όπου επηρεάζουν τη λειτουργικότητα και ευχρηστία του συστήματος. Το Windows Firewall μπορεί επίσης να αυξήσει τη δυσκολία των troubleshootingproblems κατά τη σύνδεση με τις υπηρεσίες δικτύου. Ένα άλλο πιθανό πρόβλημα είναι ότι ορισμένοι άνθρωποι θα μπορούσαν να λάβουν μια ψευδή αίσθηση ασφάλειας από την παρουσία του Windows Firewall και να μην διατηρούν την ασφάλεια του συστήματος σωστά (π.χ., τη μη εφαρμογή του κώδικα ασφαλείας).

Όταν ενεργοποιηθεί και ρυθμιστεί σωστά, το Windows Firewall προσφέρει πολλά οφέλη, συμπεριλαμβανομένων των εξής:

- Θα επιτραπεί σε ορισμένα είδη κυκλοφορίας από το τοπικό υποδίκτυο μόνο. Από προεπιλογή, όταν η Microsoft networking services είναι διαθέσιμη, το Windows Firewall, ρυθμίζεται με τις κατάλληλες θύρες (UDP 137, UDP 138 TCP 139, και το πρωτόκολλο TCP 445) και θα δέχονται μόνο τα πακέτα που έχουν για πηγή μια διεύθυνση του τοπικού δευτερεύοντος δικτύου. Αν είναι ενεργοποιημένο το UPnP, τα Windows Firewall θεσπίζουν περιορισμούς για τις παρόμοιες θύρες UPnP (UDP 1900 και TCP 2869). Επειδή η Microsoft networking services και τα UPnP θα πρέπει κανονικά να χρησιμοποιούνται μόνο μεταξύ υπολογιστών σε τοπικό δίκτυο, αυτό το τείχος της πολιτικής δεν θα πρέπει να ασχολείται με το τυπικό της λειτουργίας. Επίσης περιορίζει την ικανότητα των απομακρυσμένων επιθέσεων και των κακόβουλων προγραμμάτων από την παραβίαση αυτών των υπηρεσιών.

- Η έγκριση αδείας μόνο από το τυπικό χρόνο εκκίνησης κυκλοφορίας (π.χ. το DHCP) κατά τη διάρκεια της εκκίνησης. Αυτό είναι δυνατό, επειδή το Windows Firewall έχει φορτωθεί πριν από τη στοίβα του TCP / IP. Ο περιορισμός των δραστηριοτήτων κατά τη διάρκεια της εκκίνησης του συστήματος προστατεύει το δικτύου που βασίζεται σε επιθέσεις (κυρίως από worms που αποστέλλονται συνεχώς από κακόβουλο πακέτα) που συμβαίνουν σε δευτερόλεπτα ή λεπτά κατά τη διάρκεια του συστήματος που χρειάζεται για την εκκίνηση.

- Η ρύθμιση εν μέρει κατά μη παρακολούθησης κατά τη διάρκεια εγκατάστασης και πλήρως μέσω της Πολιτικής ομάδας. Αυτό είναι πιο ευεργετικό για την εξασφάλιση εργασίας σε περιβάλλοντα επιχειρήσεων, ιδίως για τη διαχείριση σε περιβάλλοντα. Το Windows Firewall μπορεί επίσης να ρυθμιστεί μέσω της γραμμής διασύνδεσης.

- Η παροχή μιας ενιαίας διεπαφής για το firewalling IPv4 και IPv6 κυκλοφορίας.

[51] Οι διαχειριστές μπορούν να δημιουργούν εξαιρέσεις στους κανόνες για το Windows Firewall στο Group Policy, έτσι το τείχος προστασίας θα επιτρέπει στους διαχειριστές να συνδέονται στο σύστημα τωνWindows XP για συγκεκριμένες θύρες από έναν ειδικό management hosts.

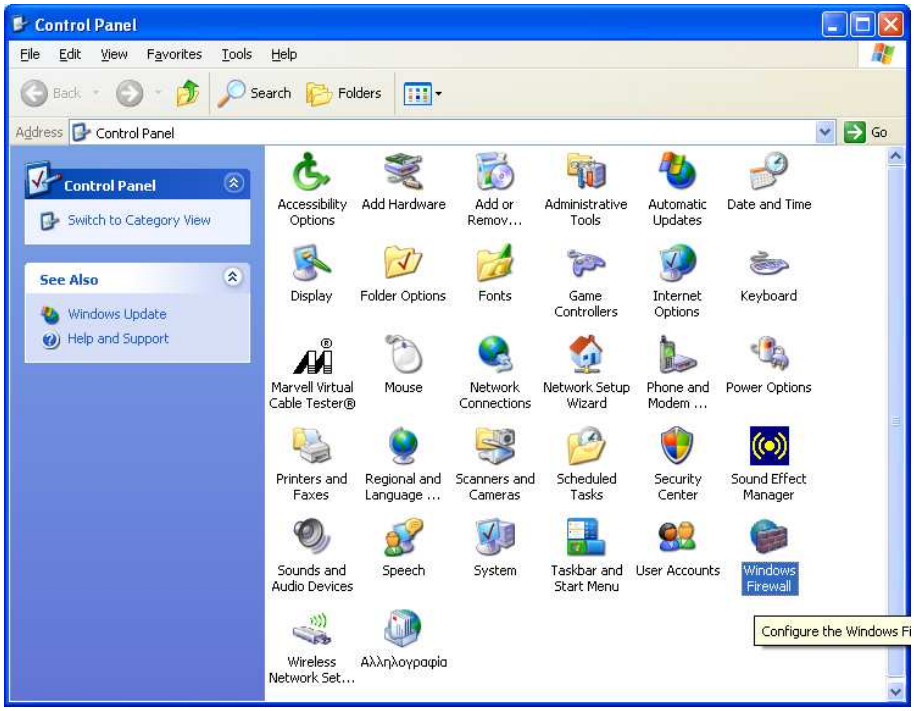
- Επιτρέποντας τη δημιουργία πολλαπλών τοίχων προστασίας προφίλ. Για παράδειγμα, ένας φορητός υπολογιστής θα μπορούσε να χρησιμοποιήσει ένα λιγότερο περιοριστικό για το προφίλ, όταν βρίσκεται σε LAN και ένα πιο περιοριστικό προφίλ όταν είναι άμεσα συνδεδεμένο με το Διαδίκτυο.

- Να διευκρινιστούν ποια προγράμματα μπορούν να χρησιμοποιούν συγκεκριμένες θύρες.

Όταν υπολογιστή με Windows XP Professional είναι μέλος ενός τομέα, ο διαχειριστής του τομέα μπορεί να επιτρέψει στο Group Policy να εμποδίζει τη χρήση του Windows Firewall, ενώ ο υπολογιστής είναι συνδεδεμένος με ένα εταιρικό δίκτυο. Αυτό επιτρέπει στον φορητό υπολογιστή να χρησιμοποιεί τους πόρους του επιχειρησιακού δικτύου χωρίς να προστίθεται πολυπλοκότητα για το χρήστη ή για το διαχειριστή του δικτύου. Όταν το laptop είναι να χρησιμοποιηθεί στο σπίτι ή σε δημόσια σύνδεση Internet hot spot, το τείχος προστασίας των Windows είναι διαθέσιμο λόγω του Group Policy που δεν εφαρμόζονται.

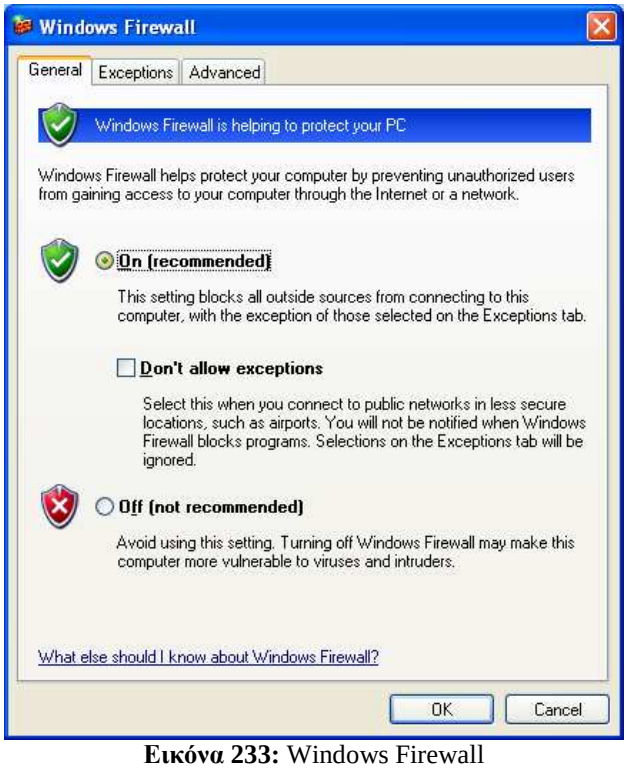
Παρά το γεγονός των μειονεκτημάτων των Windows Firewall, τα οφέλη ασφαλείας (π.χ. η μείωση της έκθεσης από νέα worms, δίνοντας στους διαχειριστές των συστημάτων περισσότερο χρόνο για να εφαρμόσουν ορισμένα patches) τα υπερκαλύπτουν, ώστε το NIST συνιστά την εφαρμογή του Windows Firewall. Ωστόσο, το Windows Firewall δεν πρέπει να εφαρμόζεται αν ένα τρίτο τείχος χρησιμοποιείται ήδη για την προστασία του συστήματος. Για να ενεργοποιήσετε και να ρυθμίσετε το Windows Firewall, ακολουθήστε τα παρακάτω βήματα:

1. Πατήστε στο μενού **Start** και διαλέξτε **Control Panel**. Διπλό κλικ **Windows Firewall**.



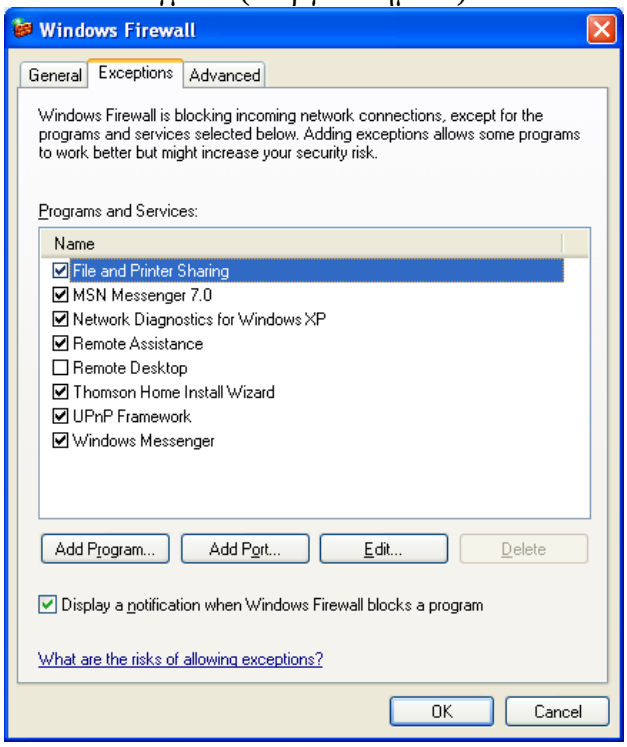
Εικόνα 232: Control Panel

2. Επιβεβαιώστε ότι το firewall είναι στο **On**.



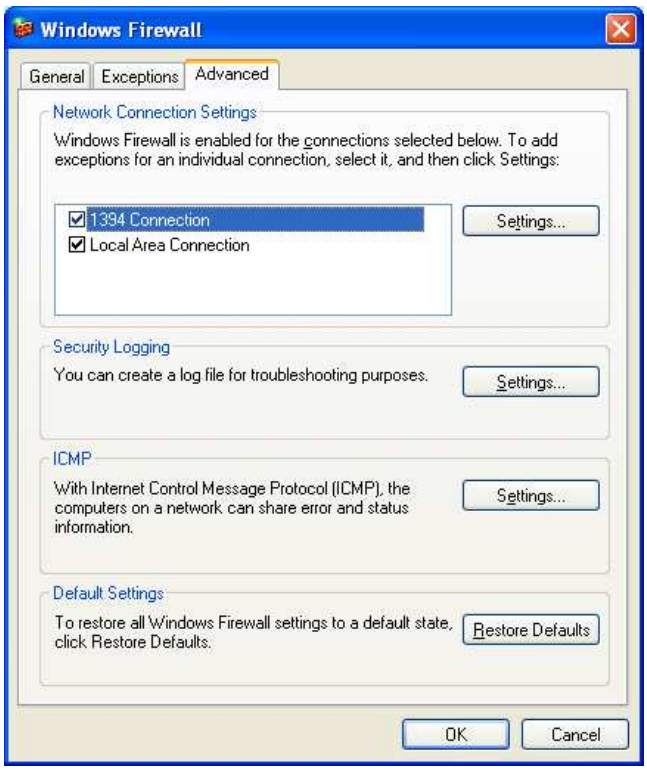
Εικόνα 233: Windows Firewall

3. Κάντε κλικ στη καρτέλα **Exceptions** . Επιβεβαιώστε ότι μόνο αυτά που χρειάζεστε να είναι επιλεγμένα (ενεργοποιημένα).



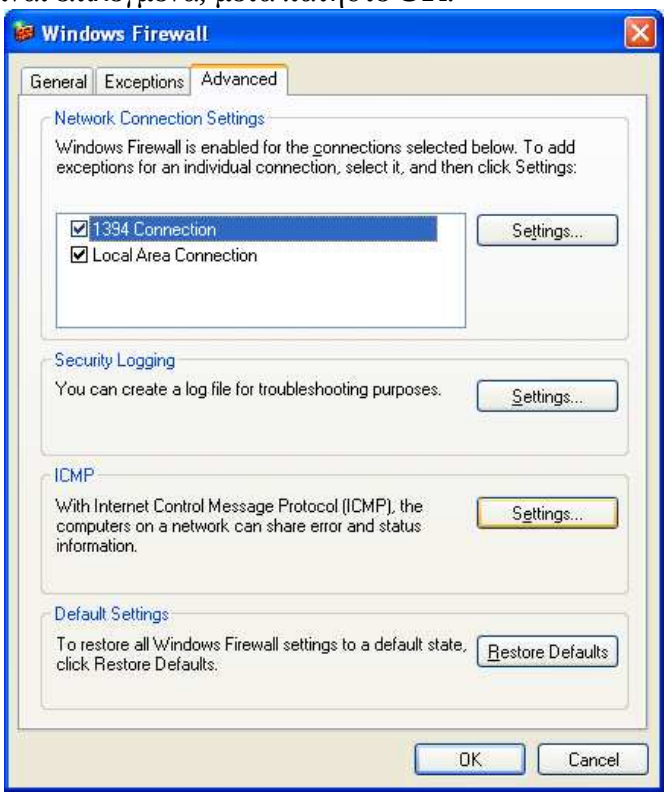
Εικόνα 234: Windows Firewall Exceptions

4. Κάντε κλικ στη καρτέλα **Advanced** . Επιβεβαιώστε ότι τα check boxes είναι επιλεγμένα για κάθε διεπαφή του δικτυού.

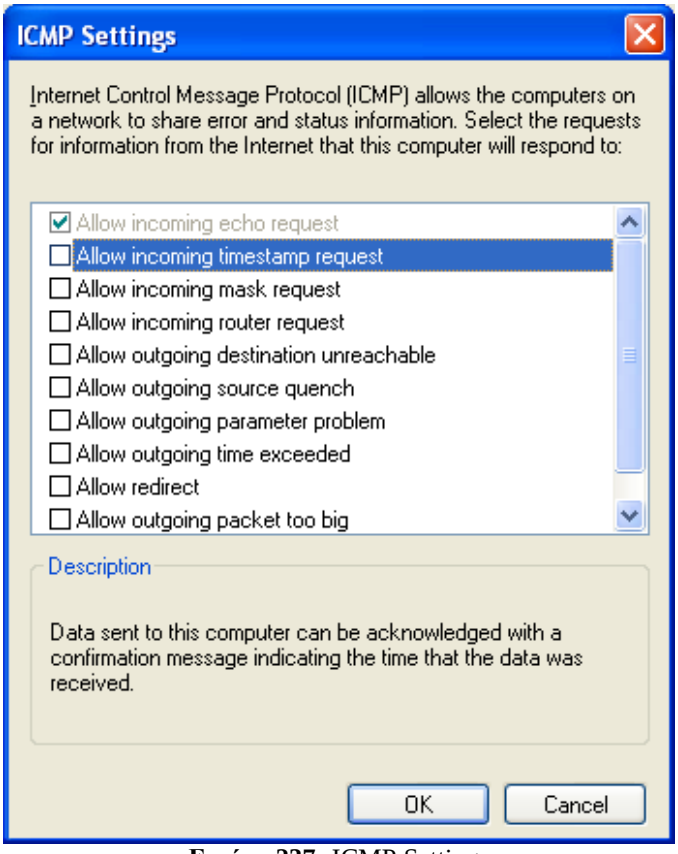


Εικόνα 235: Windows Firewall Advanced

5. Κάντε κλικ στο κουμπί **Settings** για το ICMP. Επιβεβαιώστε ότι κανένα check boxes δεν είναι επιλεγμένα, μετά πατήστε **OK**.

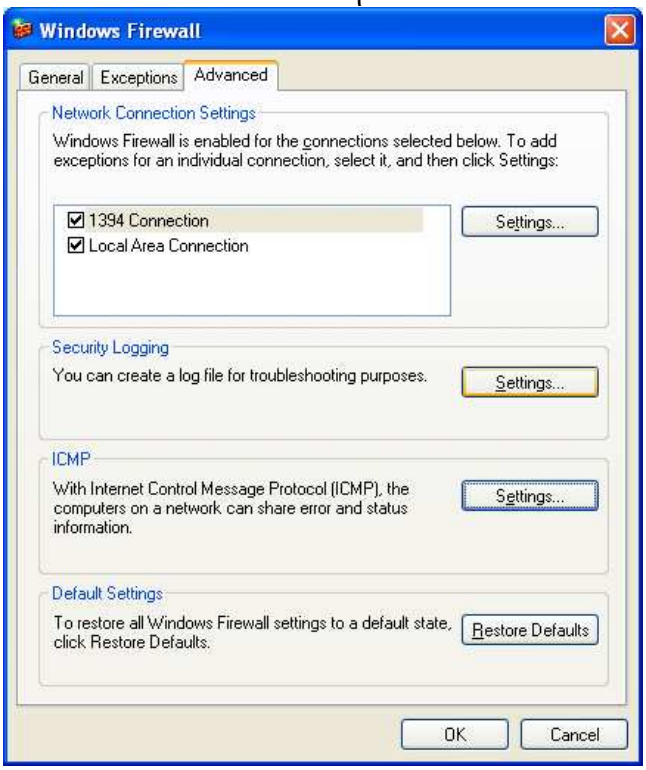


Εικόνα 236: ICMP

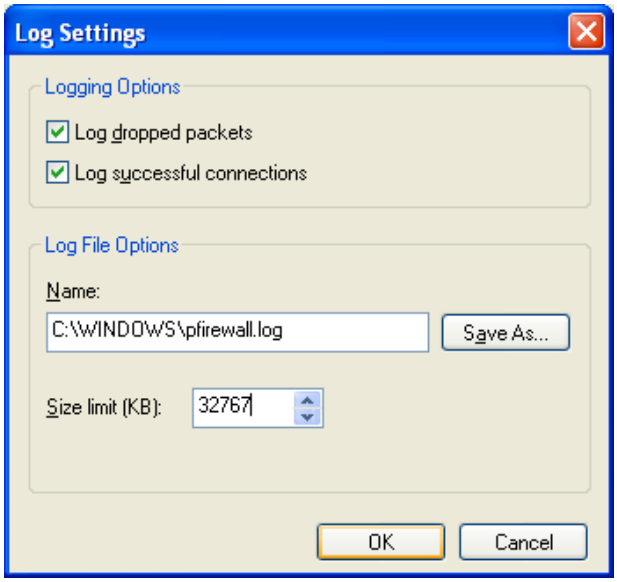


Εικόνα 237: ICMP Settings

6. Κάντε κλικ στο κουμπί **Settings** για το Security Logging. Επιλέξτε τα κουτιά **Log dropped packets** και **Log successful connections**. Βάλτε τη τιμή 32767 KB μέσα στο πεδίο του **Size limit** .Πατήστε **OK**.

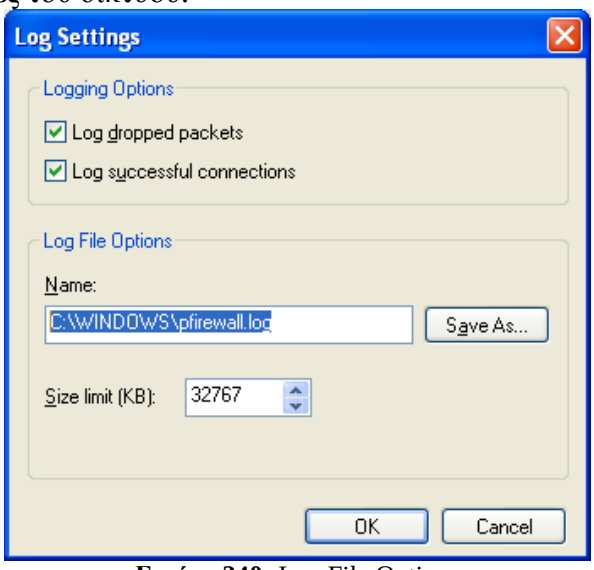


Εικόνα 238: Security Logging



Εικόνα 239: Log Settings

7. Από προεπιλογή, το log file **pfirewall.log** τοποθετείται στο κατάλογο **C:\Windows** .Το log file είναι βασισμένο σε κείμενο και περιέχει πολλά κομμάτια δεδομένων για κάθε αρχείο καταγραφής εισόδου, περιλαμβάνοντας την ημερομηνία και την ώρα που ελήφθη το πακέτο, τη κατάσταση(π.χ. η σύνδεση άνοιξε, έκλεισε, έπεσε),την IP, τη πηγή και το προορισμό των IP διευθύνσεων και θυρών, το μέγεθος του πακέτου, τις διάφορες τιμές του TCP header, και το είδος κ το κωδικό του ICMP .The log file θα πρέπει να επανεξετάζεται σε τακτά χρονικά διαστήματα για να ψάχνει τις ύποπτες δραστηριότητες του δικτυού.



Εικόνα 240: Log File Options

Τα FDCC τα GPO περιέχουν ρυθμίσεις ασφαλείας για το Windows Firewall. Πρόσθετες οδηγίες για τη ρύθμιση του Windows Firewall των Windows είναι διαθέσιμες από το site[52] της Microsoft.

[52] http://technet.microsoft.com/en-us/library/cc737845.aspx

Σε SSLF περιβάλλοντα ή σε άλλες καταστάσεις όπου δραστηριοποιούνται στη παρακολούθηση δικτύου είναι ιδιαίτερα σημαντική, η Microsoft παρέχει την υπηρεσία Port Reporter που ενδέχεται να χρήσιμη[53]. Πρέπει να συνδεθείτε με τις θύρες TCP και UDP, οι διαδικασίες που συνδέονται για κάθε θύρα, καθώς και για άλλες σχετικές πληροφορίες. Οι καταχωρήσεις μητρώου που δημιουργήθηκαν από τη θύρα του Reporter μπορεί να είναι πολύ χρήσιμες κατά τη διερεύνηση του συμβάντος ή στην αντιμετώπιση προβλημάτων δικτύου στην εφαρμογή των προβλημάτων ή σχετιζόμενων προβλημάτων.

3.7 IPsec

Το IPsec έχει σχεδιαστεί για την κρυπτογράφηση των δεδομένων, καθώς ταξιδεύει μεταξύ δύο υπολογιστών ή ενός υπολογιστή και μιας πύλης, προστατεύοντας τα δεδομένα από την τροποποίηση και τη ερμηνεία[54]. Το IPsec φιλτράρισμα μπορεί επίσης να χρησιμοποιηθεί για τον έλεγχο του δικτύου όπου ρέει περιορίζοντας και επιτρέποντας την κυκλοφορία χωρίς κρυπτογράφηση για συγκεκριμένες θύρες και πρωτόκολλα . Για παράδειγμα, το IPsec φιλτράρισμα (όπως επίσης και συσκευές φίλτρου δικτύου, όπως τείχος προστασίας με rulesets ή δρομολογητή ελέγχου με λίστες πρόσβασης) θα μπορούσε να επιτρέψει στα πρωτόκολλα δικτύου της Microsoft (π.χ., CIFS)να χρησιμοποιείτε ορισμένες αξιόπιστες τοποθεσίες ή για να αποτρέπετε τη χρήση εφαρμογών όπως αυτών των άμεσων μηνυμάτων και του peer-to-peer ανταλλαγής αρχείων που χρησιμοποιούν γνωστά νούμερα θυρών[55]. Χρησιμοποιούν φίλτρα IP, το IPsec εξετάζει όλα τα IP πακέτα για τις διευθύνσεις, τις θύρες, τις μεταφορές και τα πρωτόκολλα. Οι κανόνες που περιέχονται στην τοπική ομάδα ή στη ομάδα των πολιτικών IPsec να αγνοεί ή να εξασφαλίζει ειδικά πακέτα, ανάλογα με την αντιμετώπιση και το πρωτόκολλο δικτύου.

Από προεπιλογή, ορισμένες κινήσεις δεν είναι φιλτραρισμένες ή προστατεύονται από το Windows XP IPsec. Αυτά τα είδη της κίνησης είναι γνωστά ως *default exceptions*, εκπομπής και πολυεκπομπής, αυτά ισχύουν μόνον για τη μεταφορά φίλτρων IPsec:

- **Resource Reservation Protocol (RSVP)**. Χρησιμοποιείται για τη κίνηση της IP QoS. Απαιτείται στη QoS για να λειτουργεί τα Windows XP.

[53] Για περισσότερες πληροφορίες σχετικά με τη εγκατάσταση, τη ρύθμιση και τη χρήση της υπηρεσίας Port Reporter είναι διαθέσιμες από το άρθρο MSKB 837243, *Availability and description of the Port Reporter tool*, at http://support.microsoft.com/?id=837243. Το άρθρο αυτό παρέχει ένα σύνδεσμο για το που είναι διαθέσιμο το Port Reporter για να το κατεβάσουμε.

[54] Για περισσότερες πληροφορίες σχετικά με το IPsec, consult NIST SP 800-77, *Guide to IPsec VPNs*, διαθέσιμα στη σελίδα http://csrc.nist.gov/publications/PubsSPs.html.

[55] Ορισμένες εφαρμογές χρησιμοποιούν δυναμικούς αριθμούς θυρών, το οποίο IPsec filtering δε μπορεί να αντιμετωπιστεί αποτελεσματικά . Επίσης, μερικές εφαρμογές μπορεί να χρησιμοποιούν γνωστούς αριθμούς θυρών, όπως είναι το peer-to-peer εφαρμογή ανταλλαγής αρχείων που λειτουργεί στη θύρα 80, η οποία συνήθως σχετίζεται με Web κυκλοφορία. Παρεμπόδιση της χρήσης μιας τέτοιας θύρας μπορεί εκούσια να διακοπεί η λειτουργία. Ένα proxying firewall μπορεί να είναι αποτελεσματικό στο εντοπισμό και τη διακοπή της χρήσης των ανεπιθύμητων εφαρμογών, ανεξάρτητα από τις θύρες που χρησιμοποιούν.

- **Internet Key Exchange (IKE)**. IKE πηγή και προορισμός του User Datagram Protocol (UDP) θύρας 500 κυκλοφορίας χρησιμοποιείται σε πολλές συνθέσεις του VPN.

- **Kerberos**. Κύρια γνησιότητα του πρωτοκόλλου είναι που χρησιμοποιείται σε native περιβάλλοντα των Windows XP. Kerberos στη κυκλοφορία του χρησιμοποιεί τα πρωτόκολλα TCP και UDP πηγή και προορισμό τη θύρα 88.

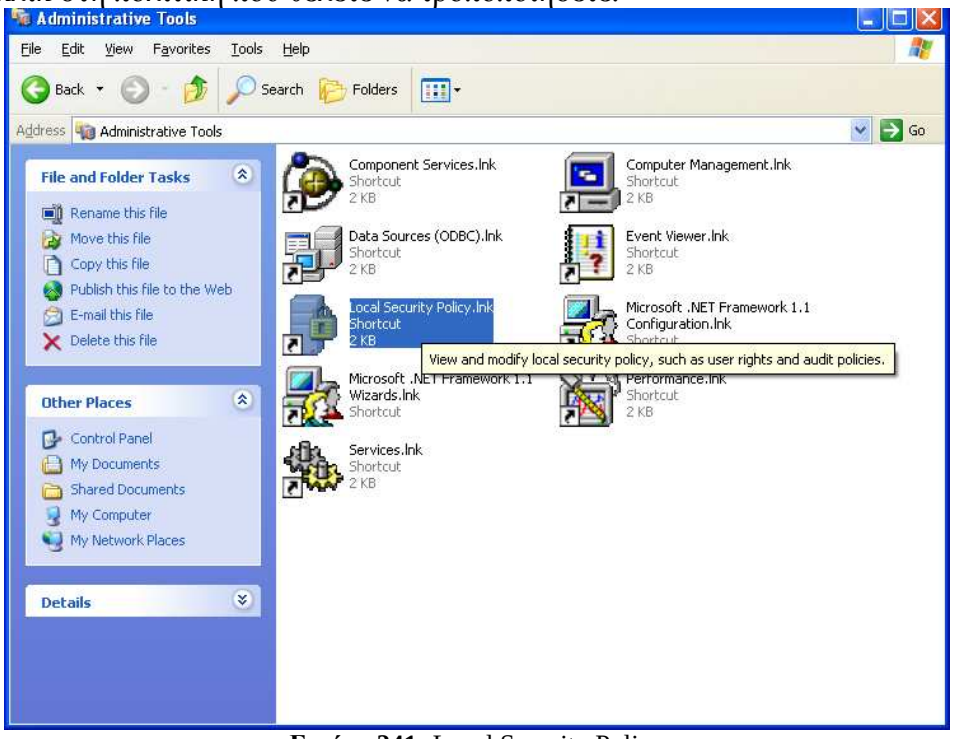
- **Broadcast**. Δίκτυο κίνησης από έναν αποστολέα σε πολλούς παραλήπτες. Χρησιμοποιείται για διάφορες λειτουργίες δικτύωσης.

- **Multicast**. Η κίνηση που στέλνεται από ένα αποστολέα σε πολλαπλούς δέκτες στη διεύθυνση με φάσμα 224.0.0.0 σε 239.255.255.255.

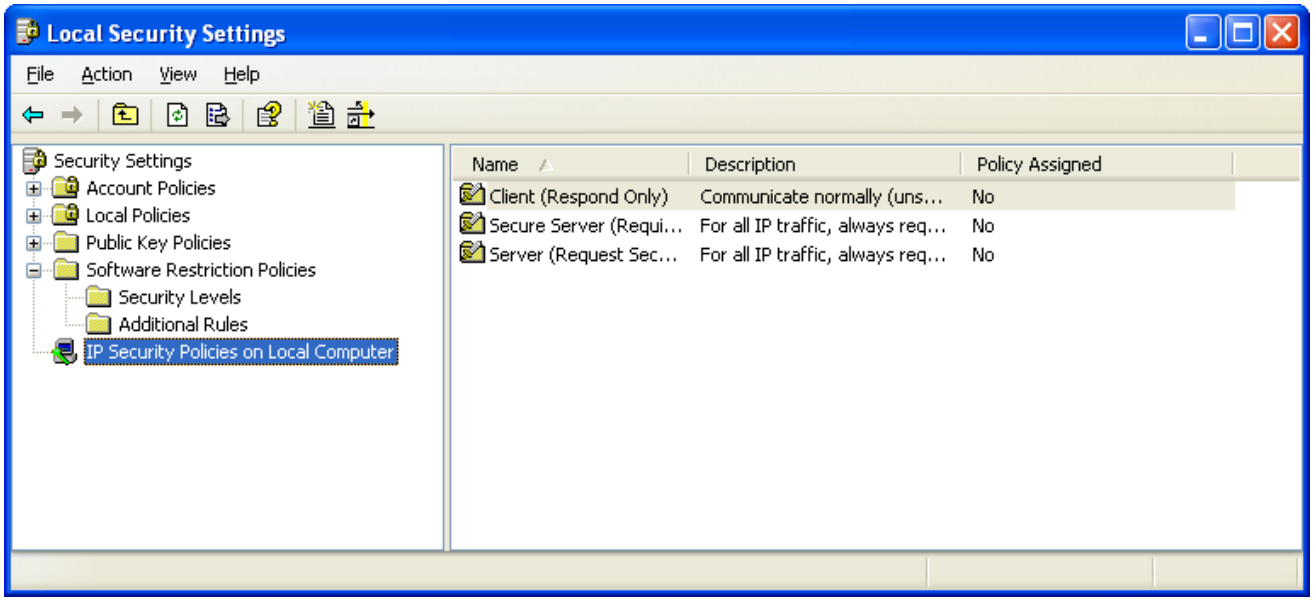
Η τιμή μητρώου DWORD μπορεί να μετακινηθεί στις περισσότερες από αυτές τις εξαιρέσεις και να επιτρέπει το φιλτράρισμα για τη παραπάνω κίνησηον. Στο **HKLM\SYSTEM\CurrentControlSet\Services\IPSec\NoDefaultExempt** κλειδί μπορεί να οριστεί σε 0 (προεπιλογή εξαιρέσεων είναι ακόμα ενεργή) ή 1 (απενεργοποιήσει της απαλλαγής για το RSVP και το Kerberos). Broadcast και multicast κυκλοφορία δε μπορεί να περιοριστεί.

Τα βήματα για να προσθέσετε ή να επεξεργαστείτε IPsec φίλτρα αναφέρονται παρακάτω.

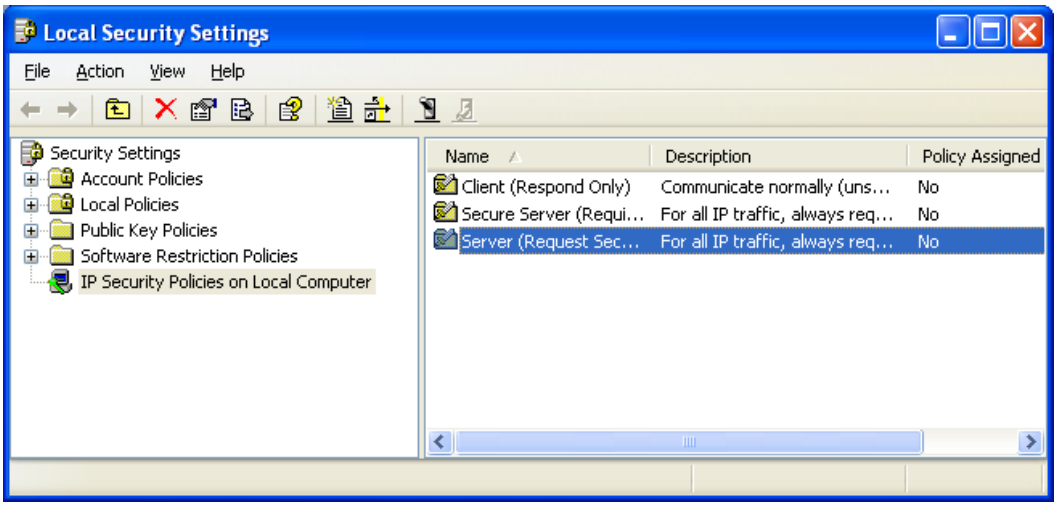
1. Στην **IP Security Policies** από το εργαλείο **Local Security Policy**, κάντε διπλό κλικ στη πολιτική που θέλετε να τροποποιήσετε.



Εικόνα 241: Local Security Policy

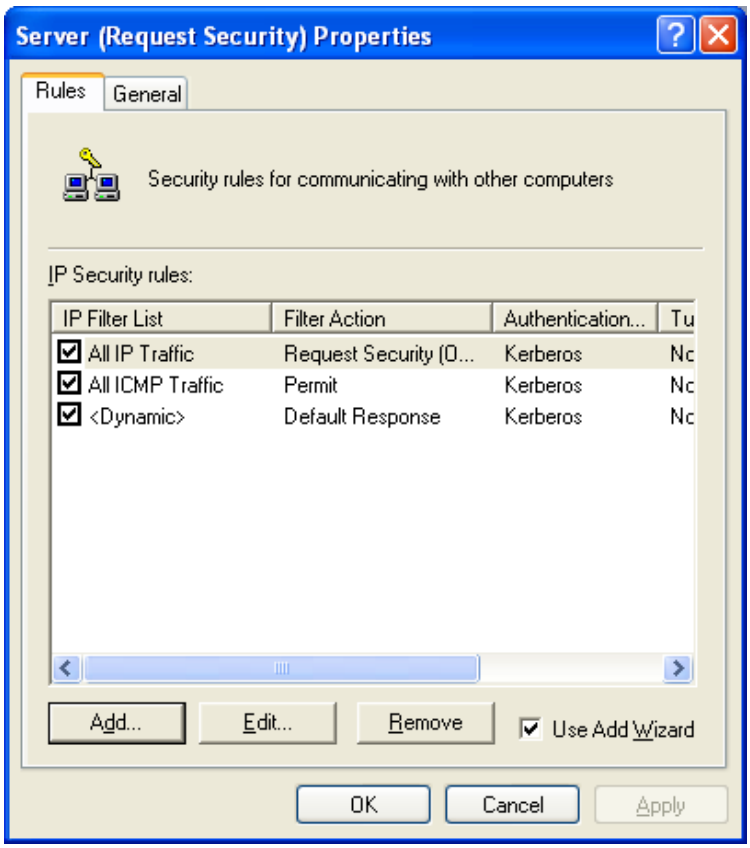


Εικόνα 242: IP Security Policies on Local Computer



Εικόνα 243: Server (Request Security)

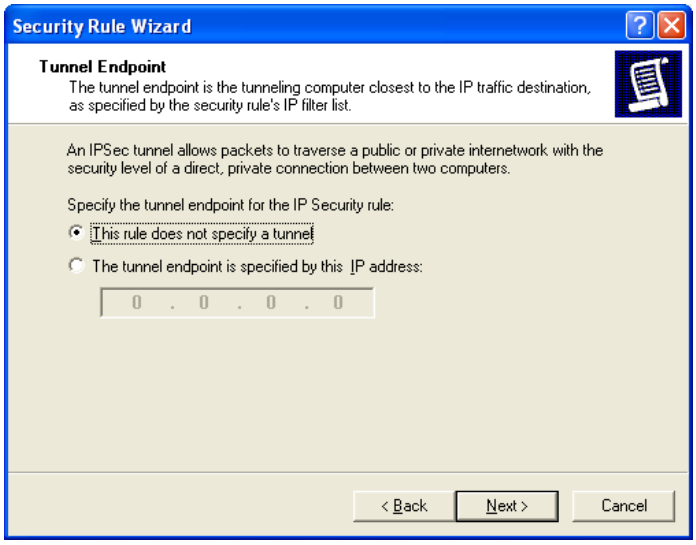
2. Για να προσθέσετε μια **IPsec filter list**, πατήστε Add πάνω στη καρτέλα **IP filter list** . Για να ρυθμίσετε ξανά μια υπάρχουσα **IP filter list**, διπλό κλικ στη **IP filter list**.



Εικόνα 244: Server (Request Security) Settings

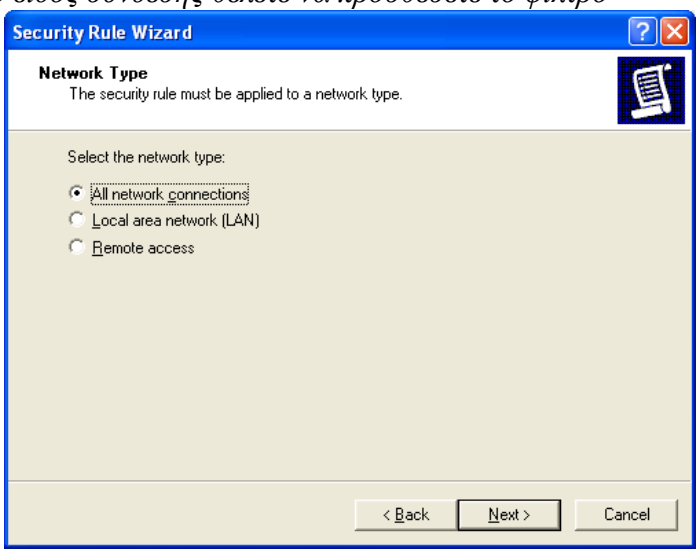
Πατήστε next για τη συνέχεια πρόσθεσης του φίλτρου

Εικόνα 245: Security Rule Wizard

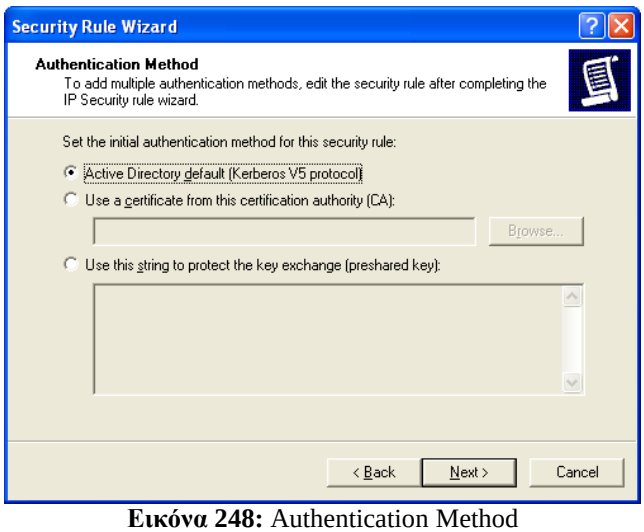


Εικόνα 246: Tunnel Endpoint

Διαλέξτε σε ποιο είδος σύνδεσης θέλετε να προσθέσετε το φίλτρο

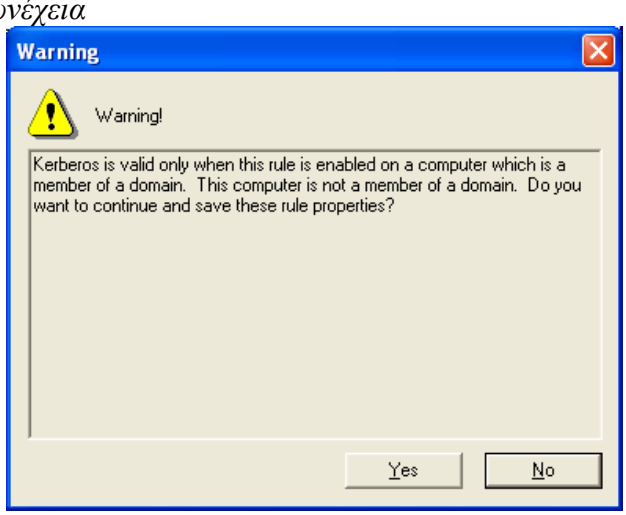


Εικόνα 247: Network Type



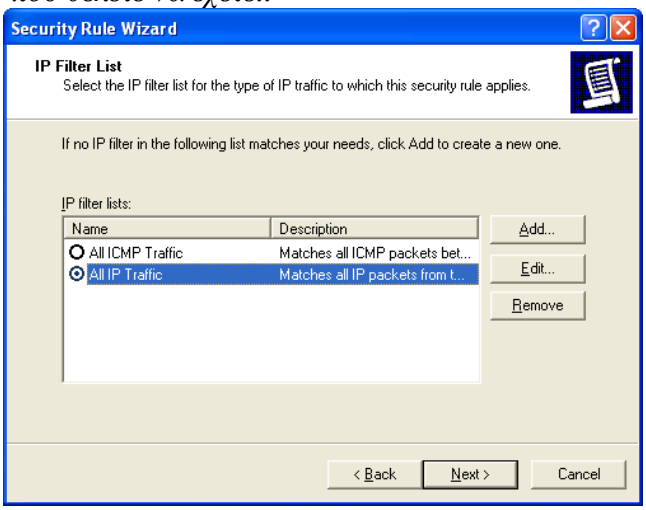
Εικόνα 248: Authentication Method

*Πατήστε **Yes** για συνέχεια*



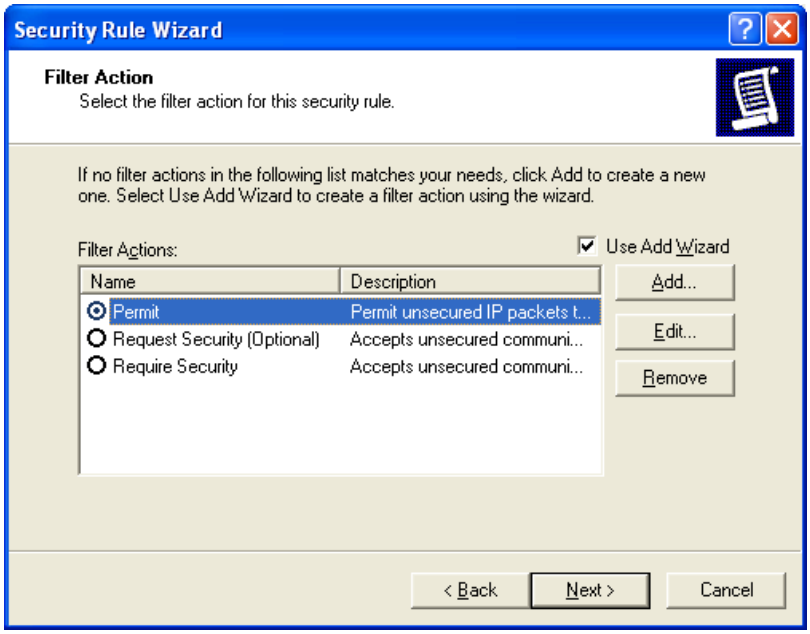
Εικόνα 249: Warning

Διαλέξτε το φίλτρο που θέλετε να έχετε..



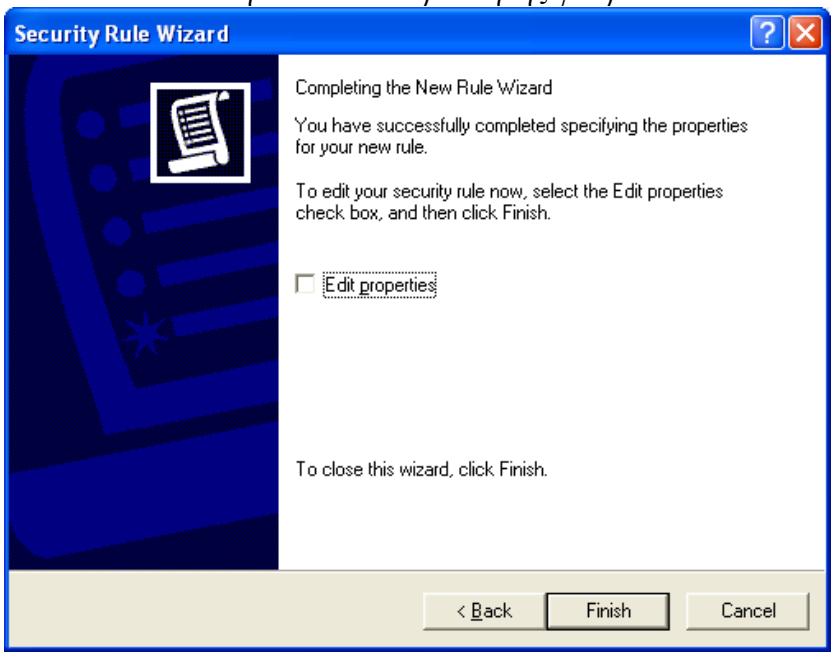
Εικόνα 250: IP Filter List

Τι είδους δράση να κάνει



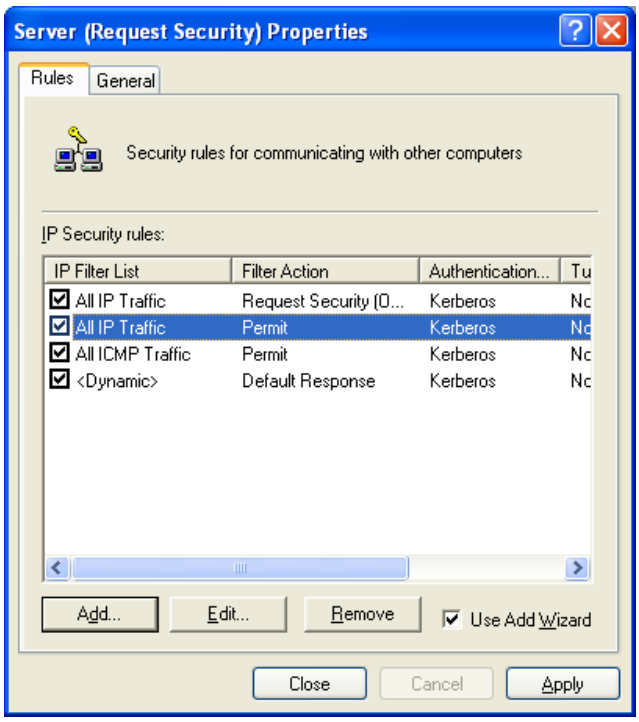
Εικόνα 251: Filter Action

*Πατήστε **Finish** να τελειώσει η διαδικασία προσθήκης φίλτρου.*



Εικόνα 252: Completing The New Rule Wizard

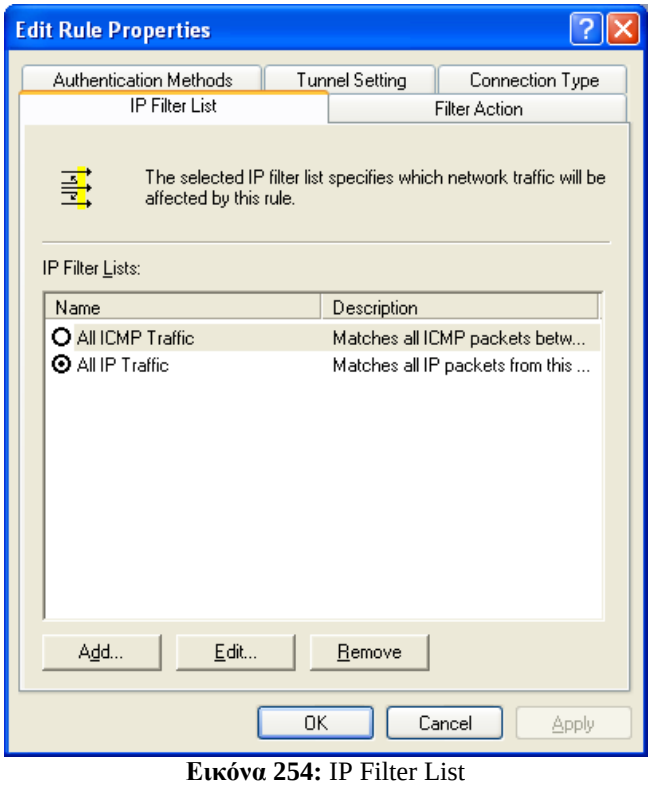
Βλέπουμε ότι μας έχει προσθέσει το φίλτρο το όποιο δημιουργήσαμε.



Εικόνα 253: Server (Request Security) Properties

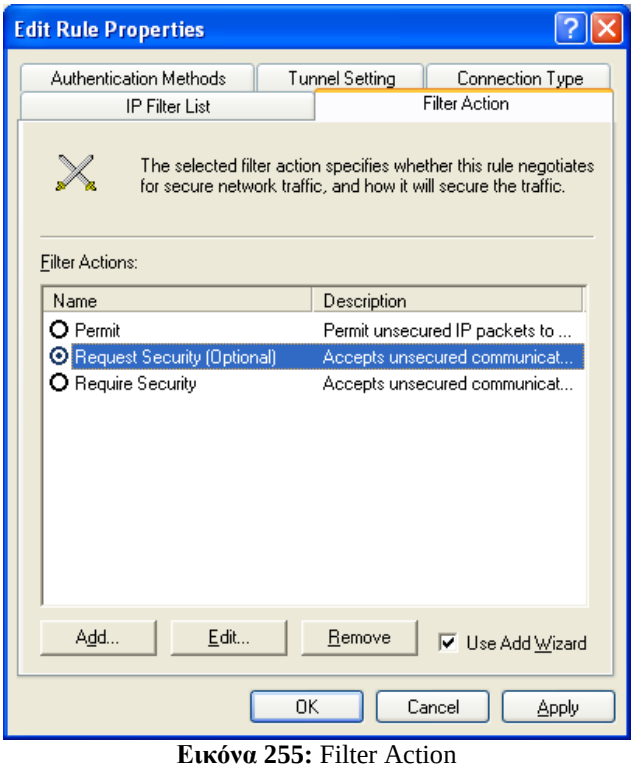
Για να ρυθμίσουμε τώρα ένα φίλτρο το όποιο ήδη υπάρχει πατήστε διπλό κλικ πάνω στο φίλτρο το οποίο θέλετε να ρυθμίσετε.

Μπορείτε να αλλάξετε το φίλτρο



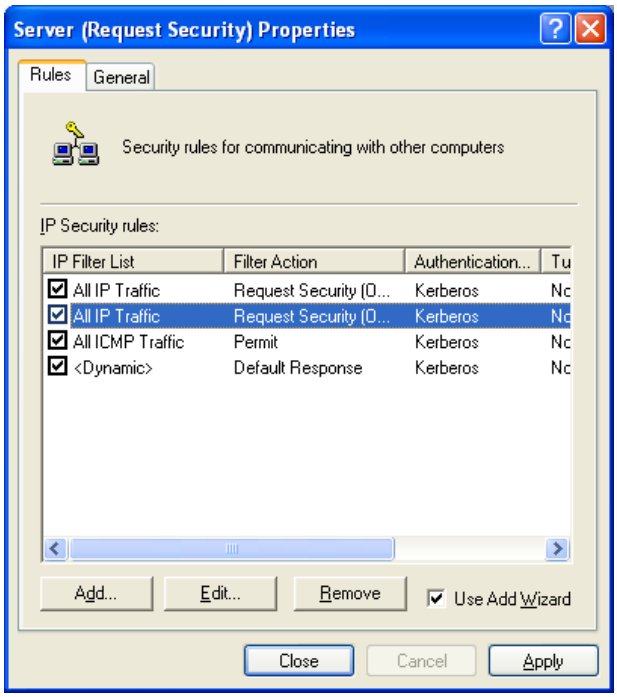
Εικόνα 254: IP Filter List

Τη λειτουργία του φίλτρου.



Εικόνα 255: Filter Action

Βλέπουμε εδώ ότι έχει αλλάξει μόνο τη δράση του φίλτρου από Permit σε Request Security..



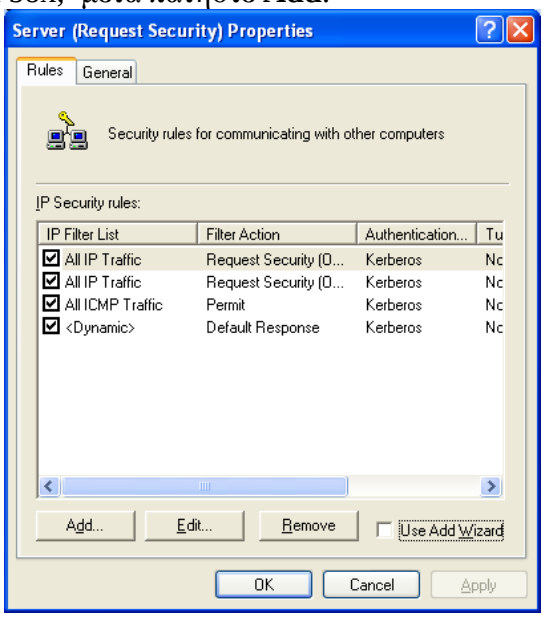
Εικόνα 256: Server (Request Security) Properties

3. Στη **IP Filter List**, κάντε ένα από τα ακόλουθα:

– Για να χρησιμοποιήσετε το IP Filter Wizard για να δημιουργήσετε ένα φίλτρο, επιβεβαιώστε ότι το **Use Add Wizard** check box είναι επιλεγμένο, και μετά πατήστε **Add**.

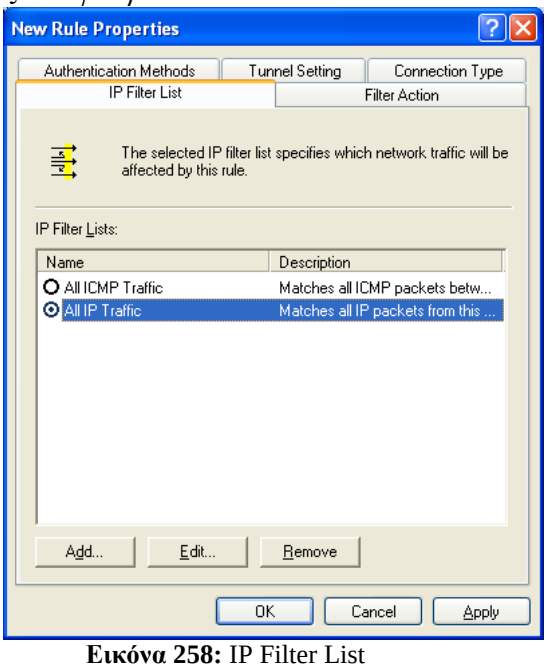
Η διαδικασία που αναφέραμε προηγουμένως είναι η πρόσθεση φίλτρου με τη βοήθεια του IP Filter Wizard

– Για να δημιουργήσεις ένα φίλτρο χειροκίνητα , ξεμάρκαρετε το **Use Add Wizard** check box, μετά πατήστε **Add**.



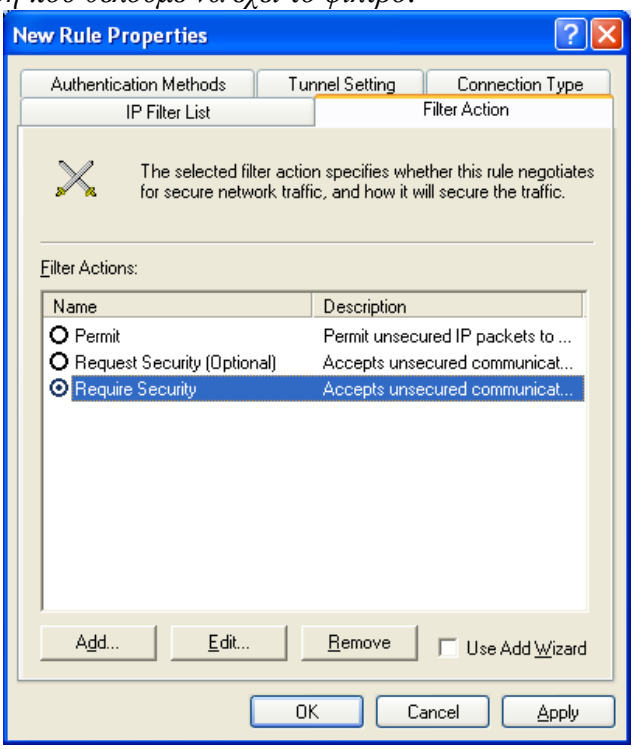
Εικόνα 257: Χωρίς τη χρήση του Add Wizard

Διαλέγουμε το είδος του φίλτρου



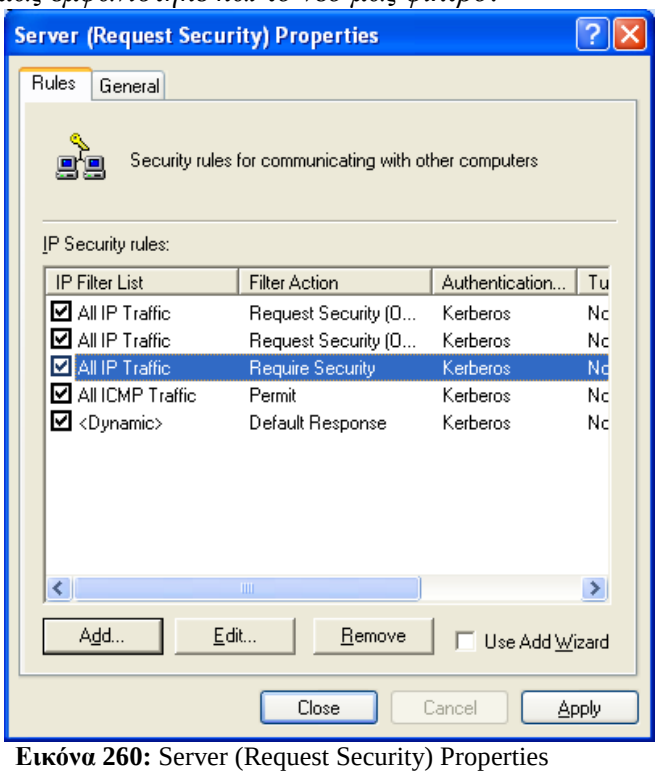
Εικόνα 258: IP Filter List

Επίσης τη δράση που θέλουμε να έχει το φίλτρο.



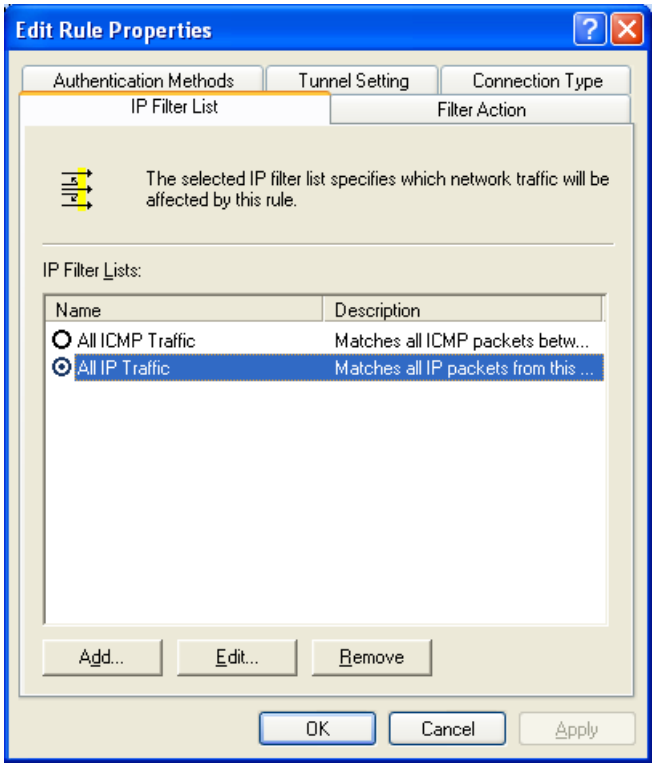
Εικόνα 259: Filter Action

Βλέπουμε ότι μας εμφανίστηκε και το νέο μας φίλτρο.



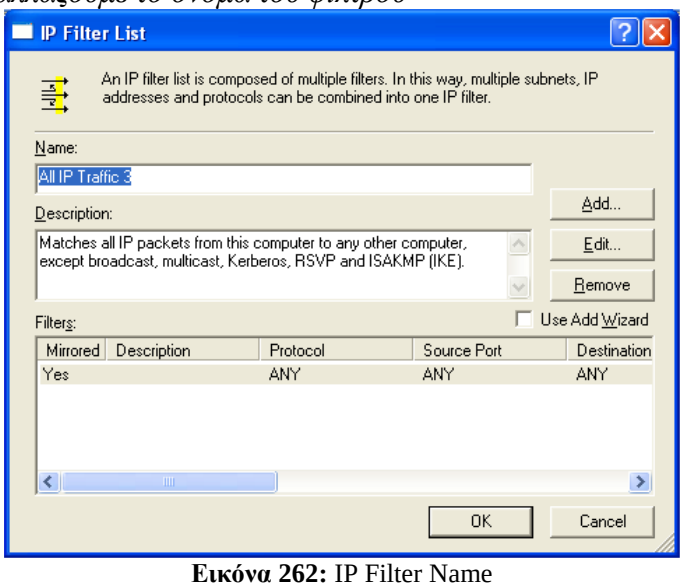
Εικόνα 260: Server (Request Security) Properties

– To reconfigure an existing filter, double-click the filter.



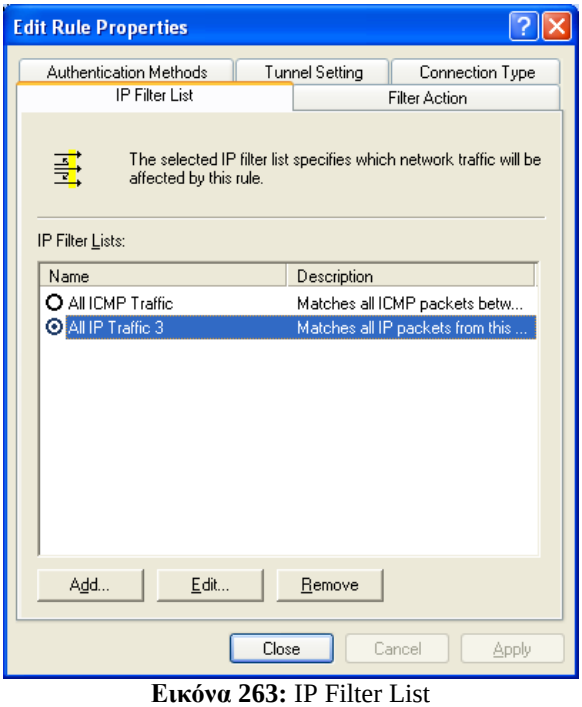
Εικόνα 261: IP Filter List

Για παράδειγμα αλλάζουμε το όνομα του φίλτρου



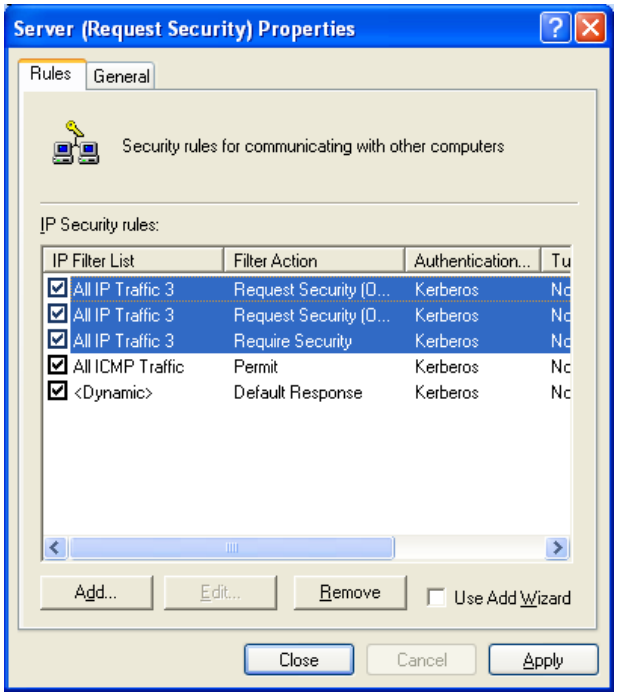
Εικόνα 262: IP Filter Name

Βλέπουμε ότι άλλαξε το όνομα για το είδος αυτό του φίλτρου



Εικόνα 263: IP Filter List

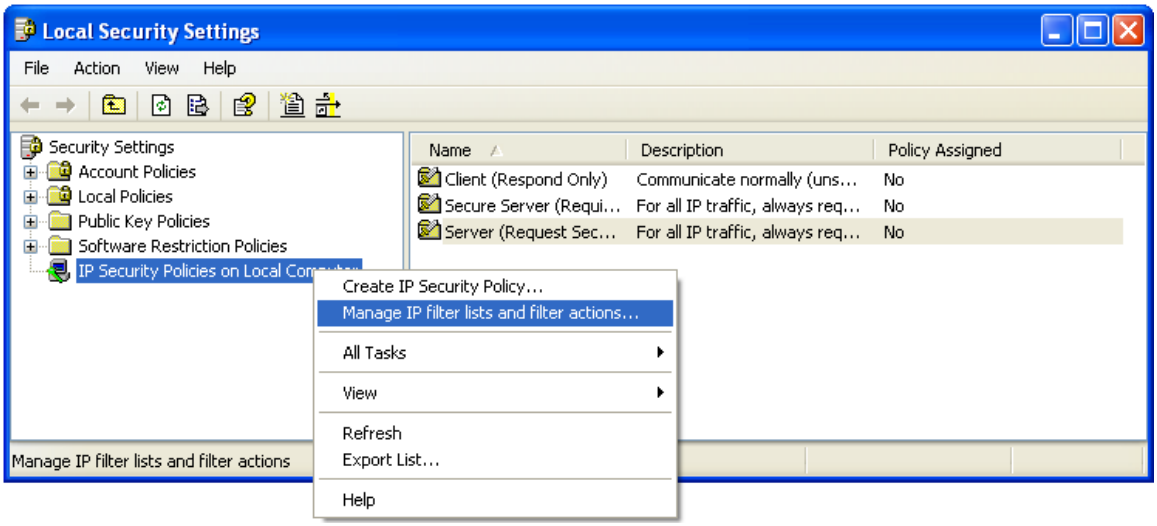
Και τέλος βλέπουμε ότι μας άλλαξε όλα τα φίλτρα του είδους με το όνομα που αλλάξαμε.



Εικόνα 264: Server (Request Security) Properties

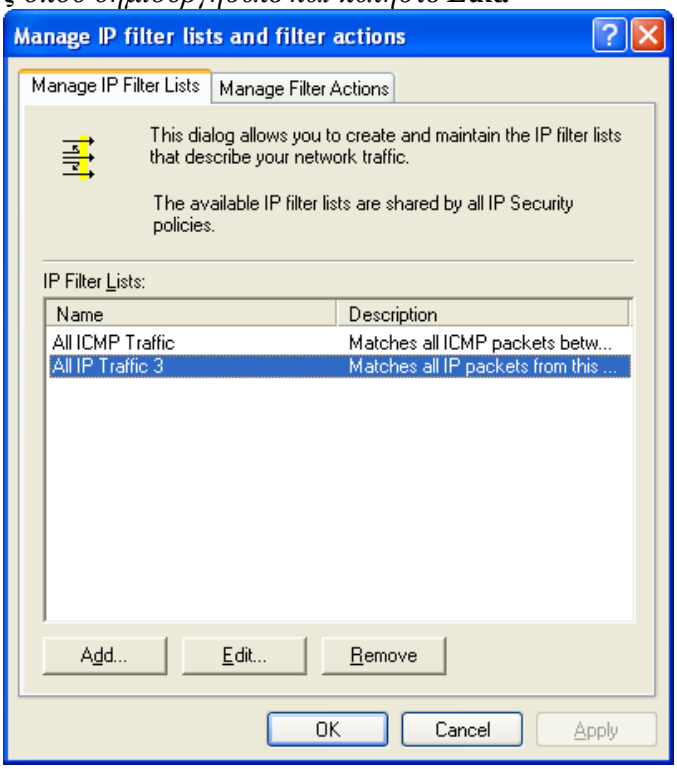
4. Στη καρτέλα **Addressing** , επιλέξτε τη **Source Address** όπως δείχνει ο πίνακας 5:

*Πηγαίνετε στο **Local Security Settings** επεκτείνετε τη καρτέλα **Security Settings** και πατήστε δεξί κλικ στο **IP Security Policies on Local Connection** και διαλέξτε **Manage IP filter …***



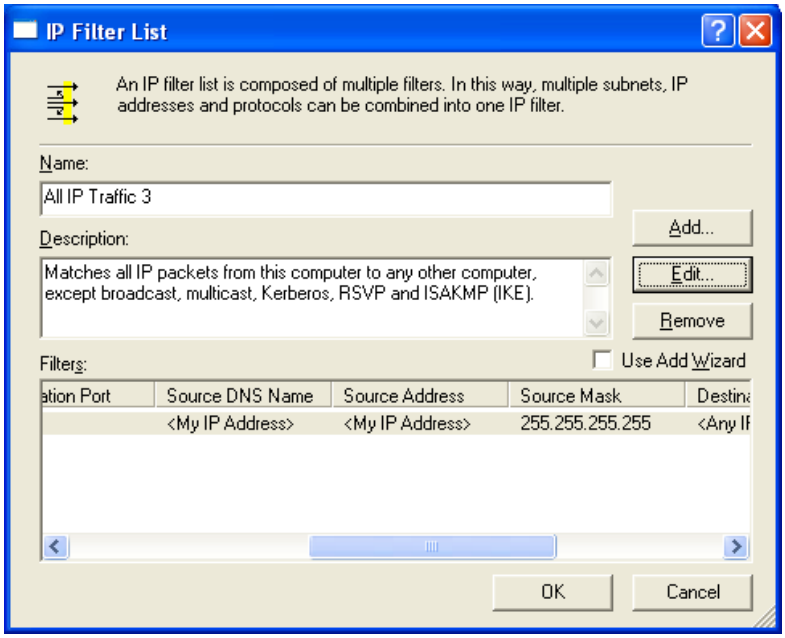
Εικόνα 265: Manage IP Filter Lists and Filter Actions

*Πατήστε στο είδος όπου δημιουργήσατε και πατήστε **Edit.***



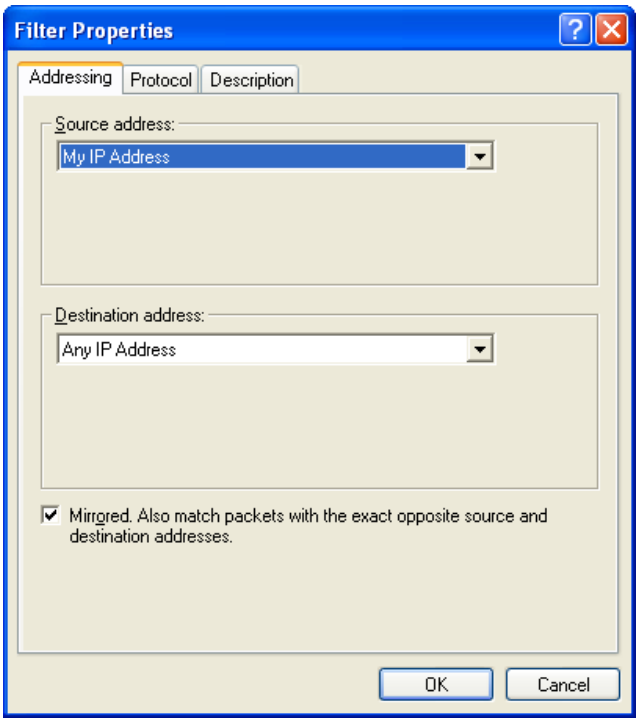
Εικόνα 266: Manage IP Filter Lists

Πατήστε πάλι ***Edit***



Εικόνα 267: IP Filter List

Διαλέξτε τώρα τη ***Source address.***

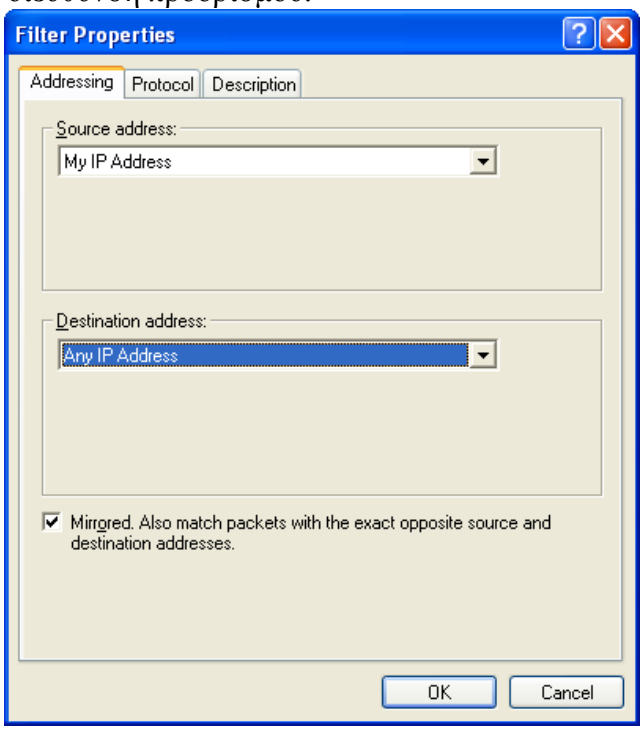


Εικόνα 268: Filter Properties

Select	To Secure Packets From
My IP Address	Όλες οι διευθύνσεις IP για τον υπολογιστή, για τα οποία το φίλτρο έχει ρυθμιστεί.
Any IP Address	Κάθε υπολογιστής.
A Specific DNS Name	Το Domain Name System (DNS), το όνομα που ορίζεται στο όνομα του κεντρικού υπολογιστή. Το όνομα DNS είναι ορισμένο για διευθύνσεις IP και στη συνέχεια, για φίλτρα που δημιουργούνται αυτόματα για να επιλυθούν οι διευθύνσεις IP. Αυτή η επιλογή είναι διαθέσιμη μόνο κατά τη δημιουργία νέων φίλτρων..
A Specific IP Address	Η διεύθυνση IP που καθορίζεται σε διεύθυνση IP.
A Specific DNS Subnet	Η διεύθυνση IP που καθορίζεται στην διεύθυνση IP και τη μάσκα υποδικτύου καθορίζεται στο Subnet Mask.

Πίνακας 5: IP Address & DNS Name

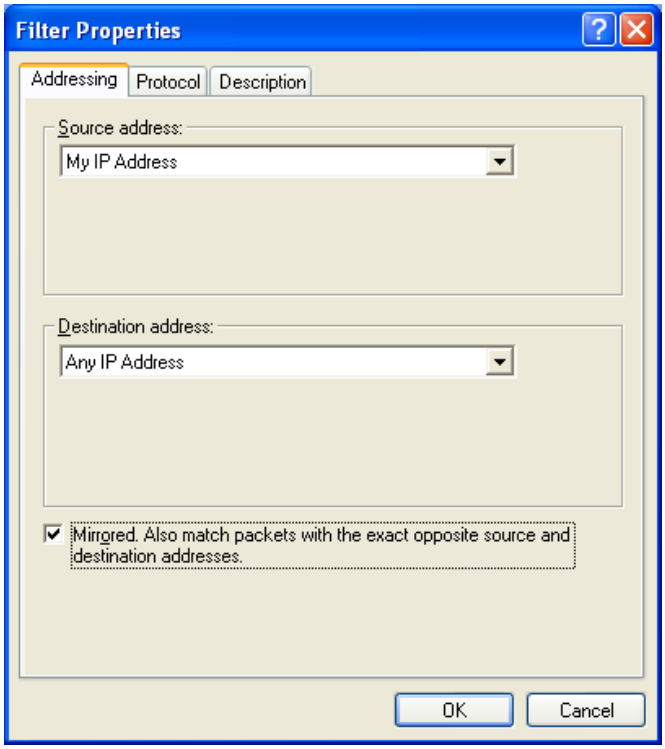
5. Κάντε κλικ στο κουμπί **Destination Address** και επαναλάβατε το προηγούμενο βήμα για τη διεύθυνση προορισμού.



Εικόνα 269: Destination Address

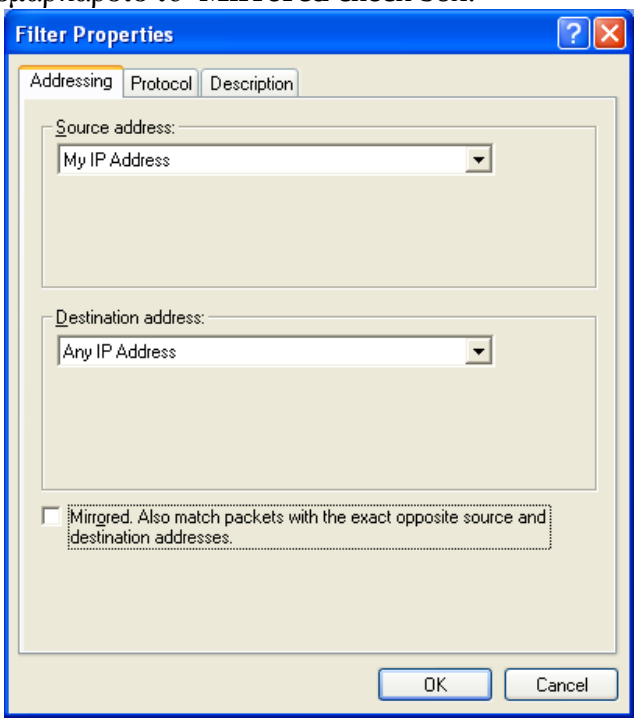
6. Σύμφωνα με το **Mirrored**, επιλέξτε τη κατάλληλη ρύθμιση από τη παρακάτω λίστα:

   – Για αυτόματη λειτουργία 2 φίλτρων με βάση τις ρυθμίσεις του φίλτρου (ένα για κίνηση προς το προορισμό και ένα για κυκλοφορία από το προορισμό), επιλέξτε το **Mirrored** check box.



Εικόνα 270: Επιλεγμένο το Mirrored

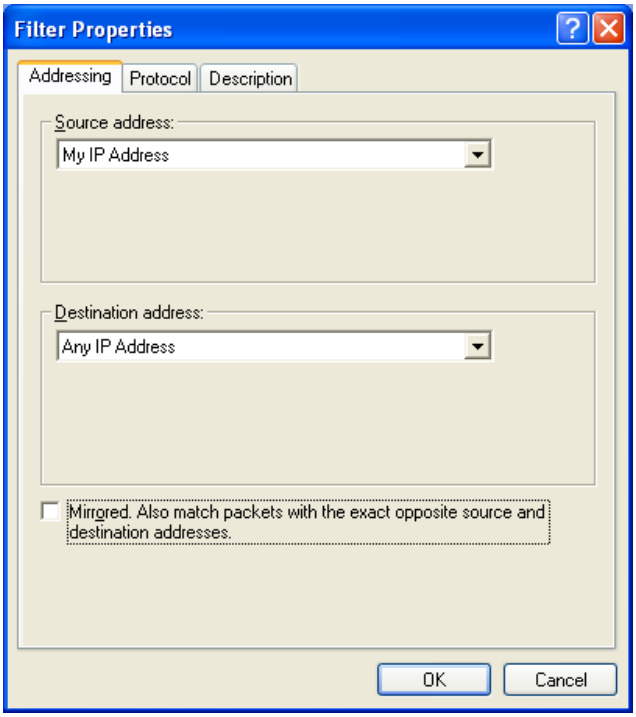
–Για να δημιουργήσετε ένα φίλτρο και μόνο με βάση τις ρυθμίσεις του φίλτρου, ξεμαρκάρετε το **Mirrored** check box.



Εικόνα 271: Μη Επιλεγμένο το Mirrored

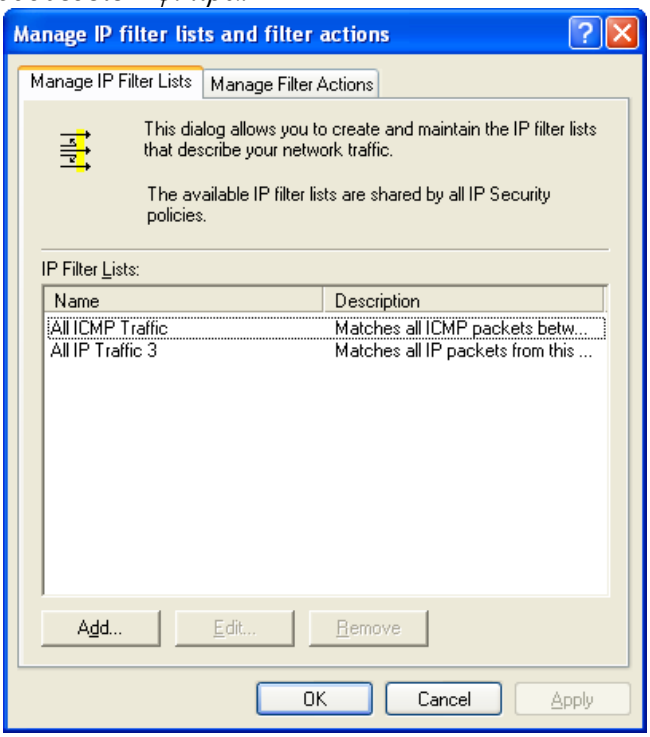
– Για να δημιουργήσετε ένα φίλτρο για IPsec tunnel, ξεμαρκάρετε το **Mirrored** check box. Δημιουργήστε 2 λίστες φίλτρων: το ένα που περιγράφει τη κίνηση που πρέπει να στέλνετε μέσο της σήραγγας (εξερχόμενη κίνηση) και το άλλο να περιγράφει τη κίνηση που πρέπει να

λαμβάνετε μέσο της σήραγγας (εισερχόμενη κίνηση). Στη συνέχεια δημιουργήστε δυο κανόνες που θα χρησιμοποιεί το εισερχόμενο και εξερχόμενο φίλτρο στις λίστες της πολιτικής.



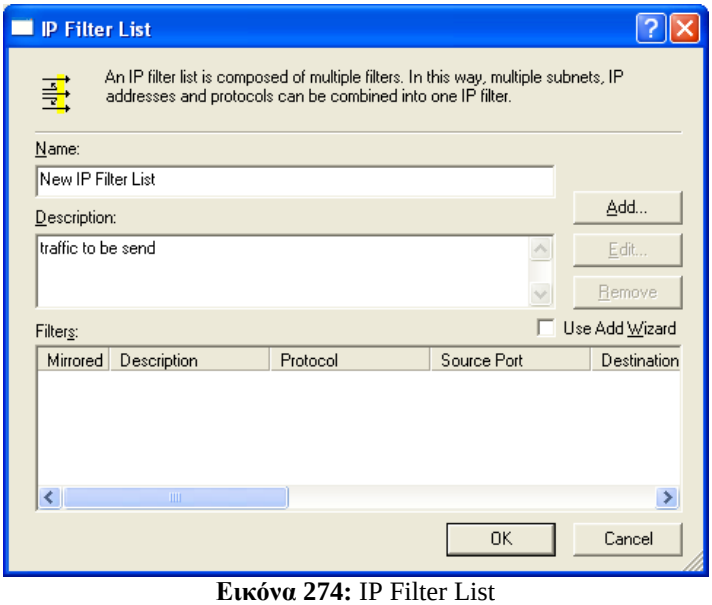
Εικόνα 272: Μη Επιλεγμένο το Mirrored

*Πατήστε **add** να προσθέσετε 2 φίλτρα.*



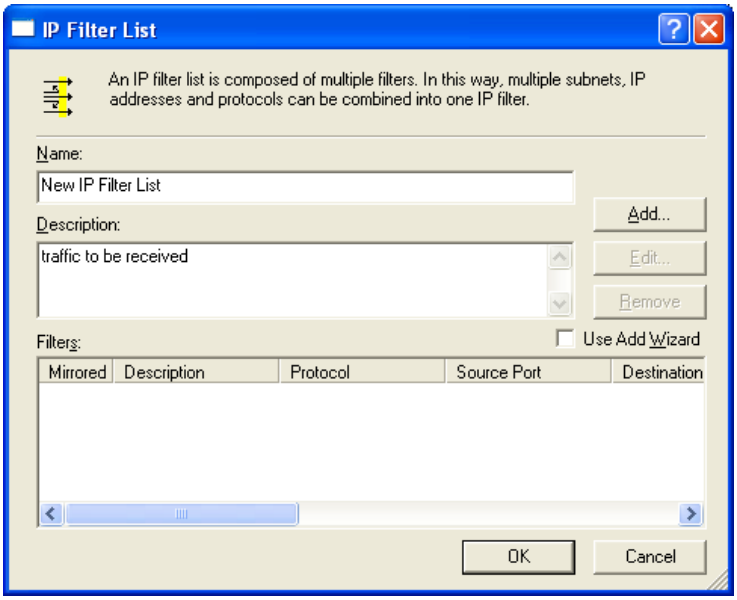
Εικόνα 273: Manage IP Filter Lists

Πατήστε μια περιγραφή για το πρώτο φίλτρο για παράδειγμα «Traffic to be send». Και πατήστε OK



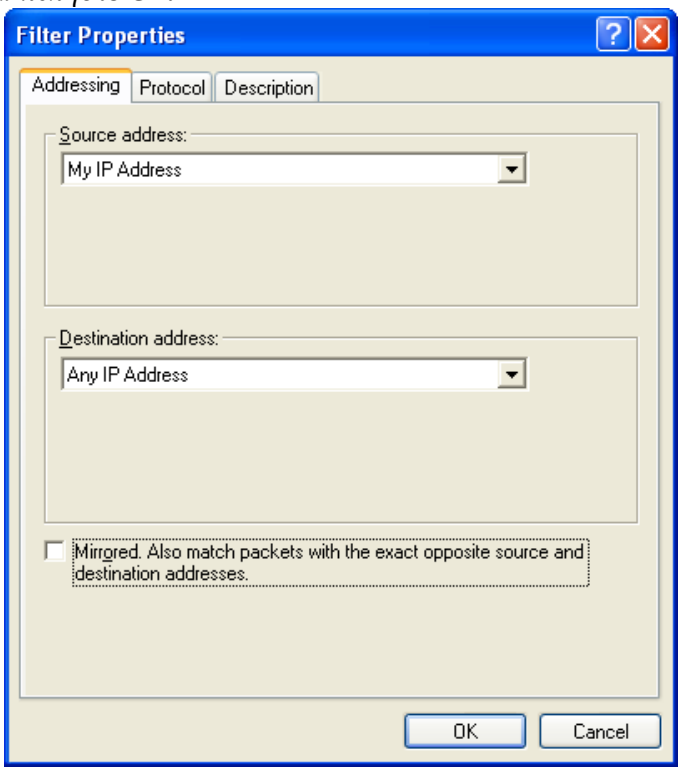
Εικόνα 274: IP Filter List

Πατήστε μια περιγραφή για το δεύτερο φίλτρο για παράδειγμα «Traffic to be received». Και πατήστε OK



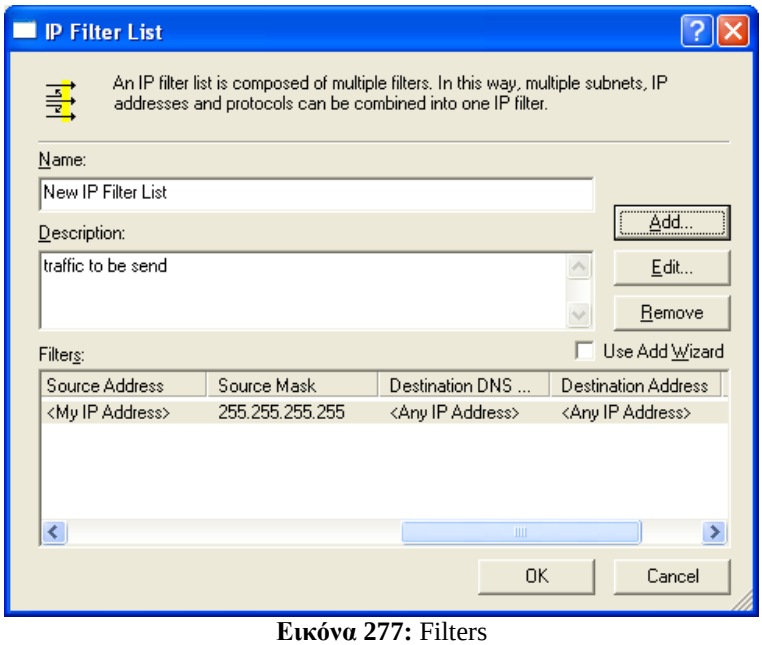
Εικόνα 275: IP Filter List Description

*Για το πρώτο φίλτρο πατήστε Source address :**My IP Address** ,Destination address :**Any Address** και πατήστε **Ok.***



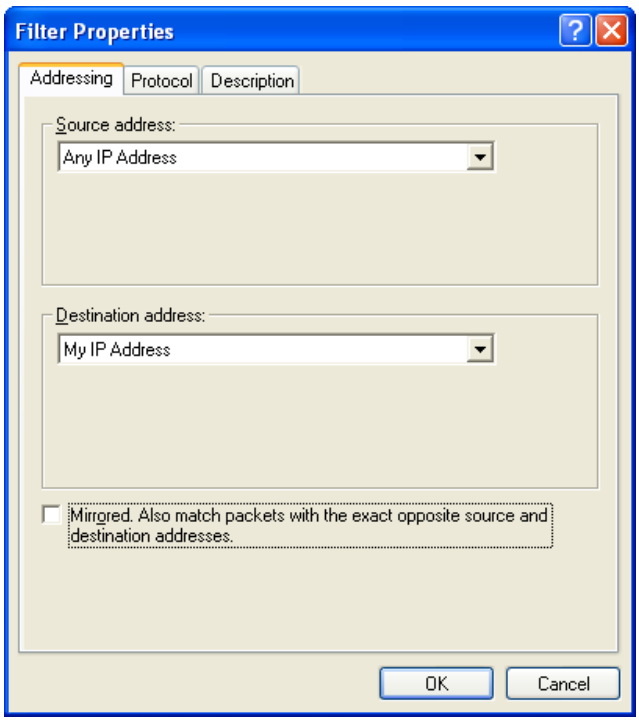
Εικόνα 276: Filter Properties

Μας εμφανίζει στο φίλτρο μας τη *Source address και τη Destination address που βάλαμε.*



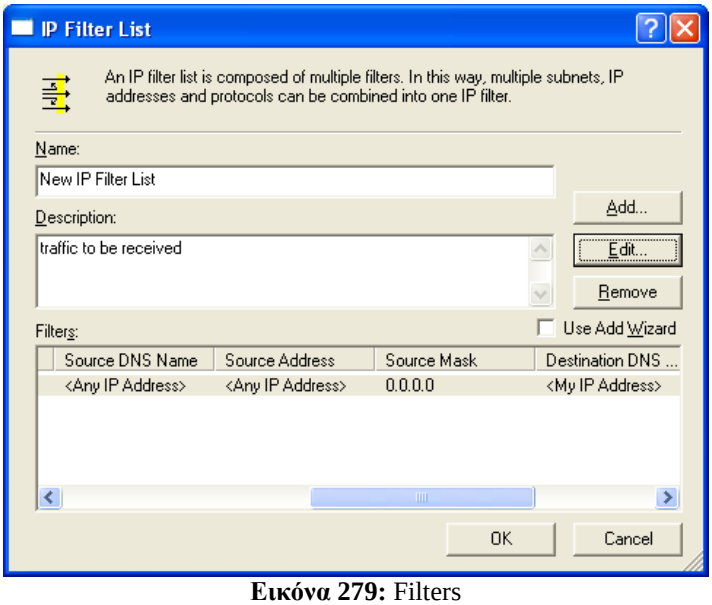
Εικόνα 277: Filters

Για το δεύτερο φίλτρο πατήστε Source address : ***Any Address****, Destination address :* ***My IP Address*** *και πατήστε* ***Ok.***



Εικόνα 278: Addressing

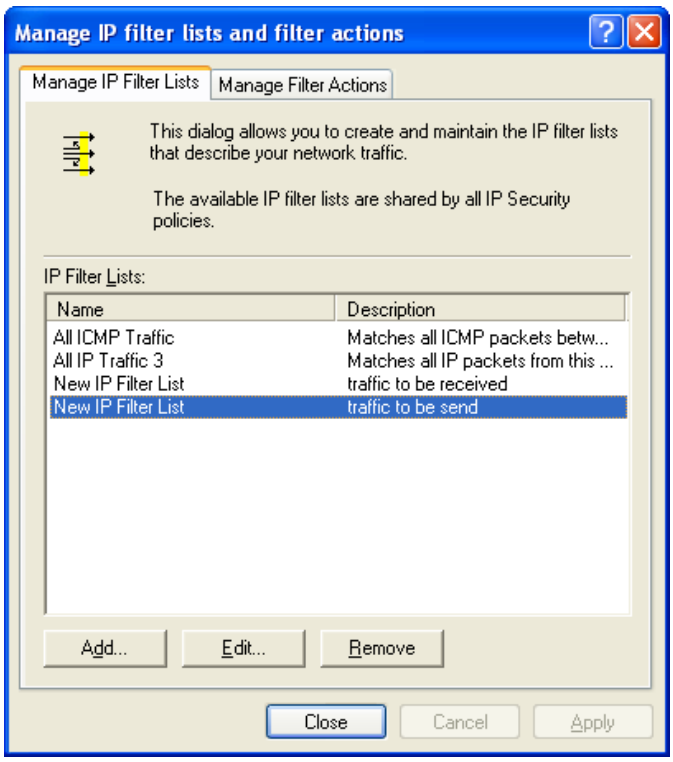
Μας εμφανίζει στο φίλτρο μας τη *Source address και τη Destination address που βάλαμε.*



Εικόνα 279: Filters

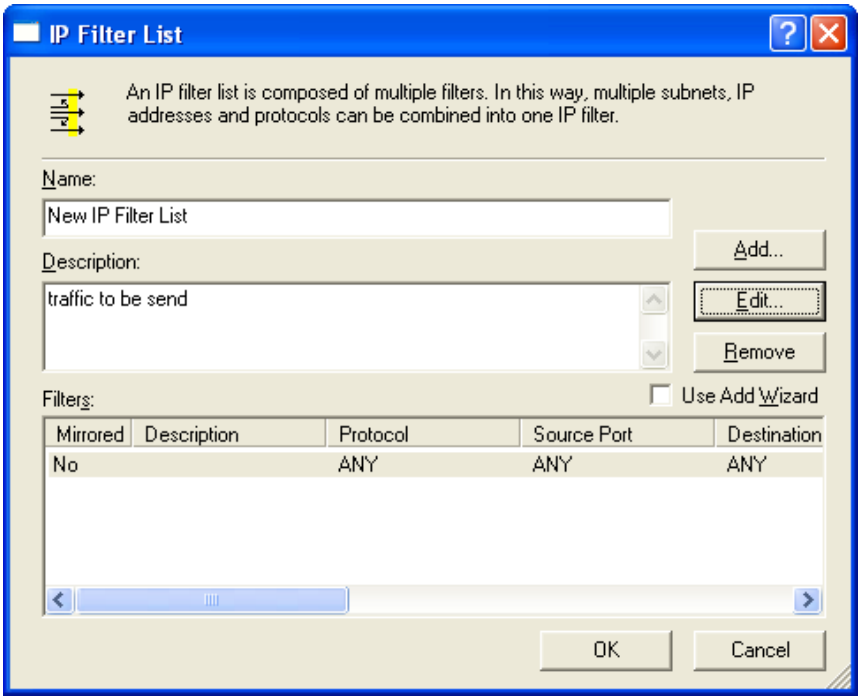
7. Στη καρτέλα **Description**, πληκτρολογήστε μια περιγραφή για αυτό το φίλτρο. Για παράδειγμα, ***«specify to which computers and traffic types it applies »***

Πατήστε ***Edit.***



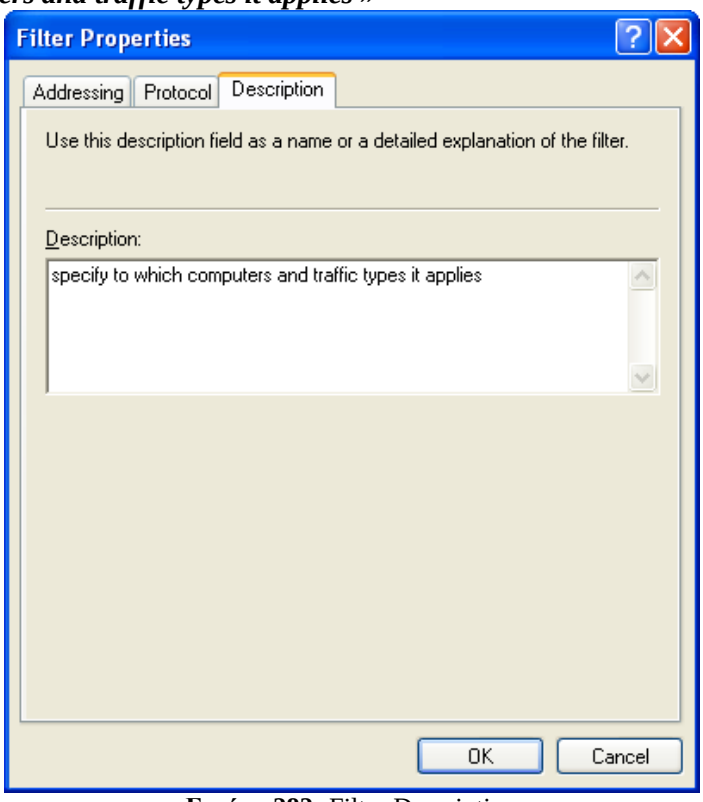
Εικόνα 280: Edit Manage IP Filters Lists

Ξανά ***Edit.***



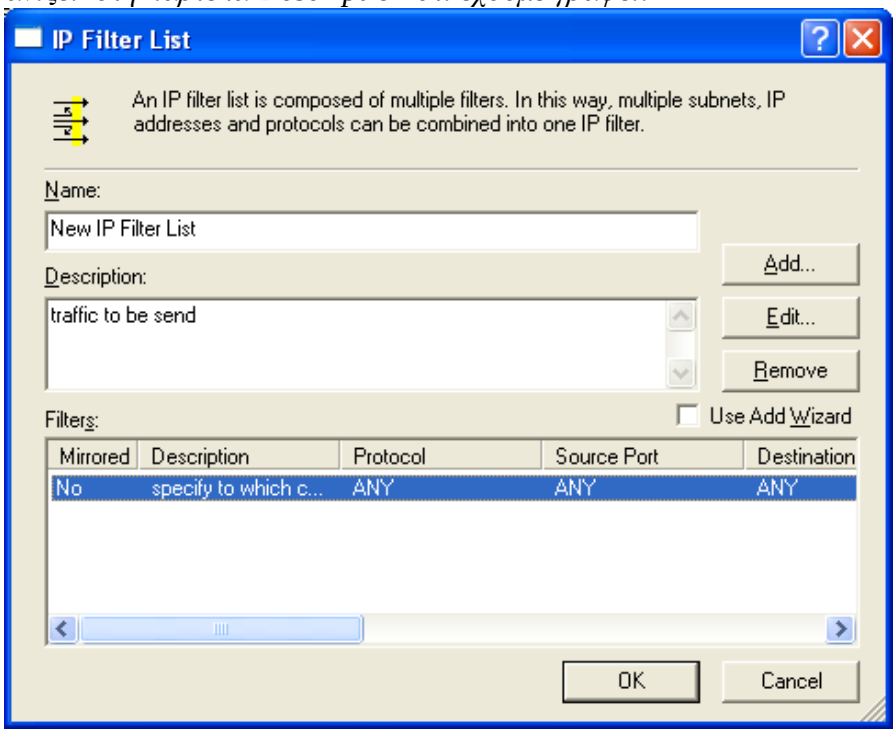
Εικόνα 281: Edit IP Filter List

Πηγαίνετε στη καρτέλα «Description»και δώστε μια περιγραφή για παράδειγμα ***«specify to which computers and traffic types it applies »***



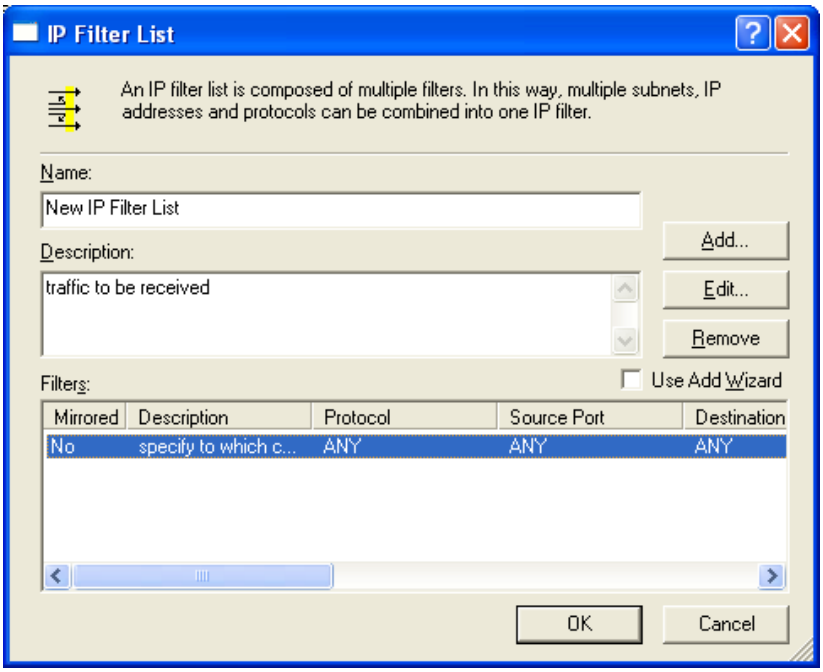
Εικόνα 282: Filter Description

Μας εμφανίζει στη καρτέλα Description ότι έχουμε γράψει.



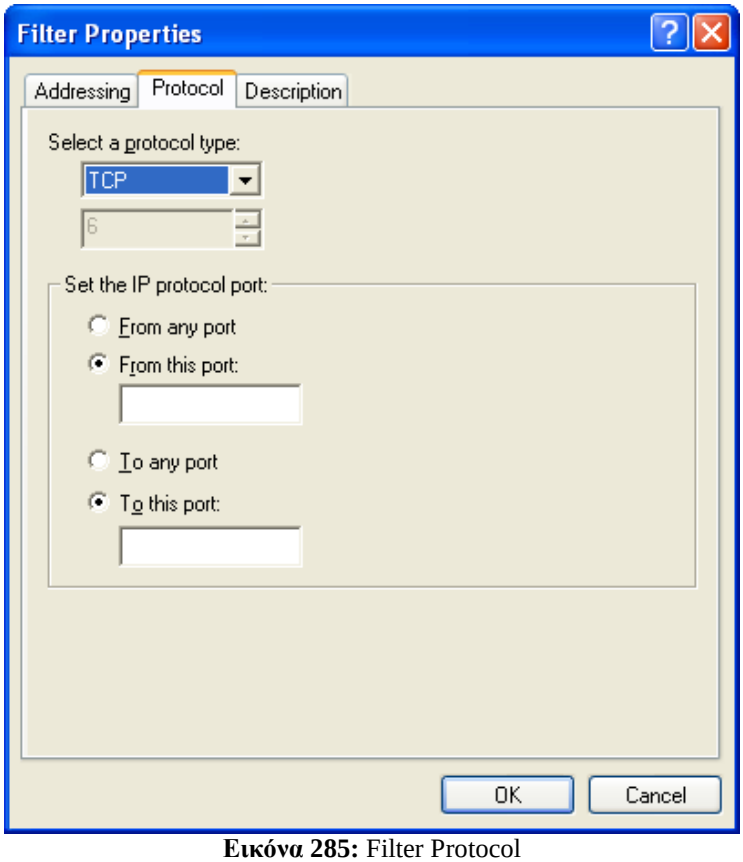
Εικόνα 283: Description

Την ίδια κάνουμε και για το δεύτερο φίλτρο



Εικόνα 284: Description (2)

8. Αν εκτός από το IP filtering σε ειδικό πρωτόκολλο ή ο αριθμός θύρας είναι απαραίτητος, ρυθμίστε τις προηγούμενες ρυθμίσεις του φίλτρου στη καρτέλα **Protocol** .



Εικόνα 285: Filter Protocol

3.8 Wi-Fi Network Configuration

Τα Windows XP παρέχουν ενσωματωμένη υποστήριξη για ασύρματη δικτύωση (γνωστό και ως ασύρματα πίστεως, ή Wi-Fi) [56]. Από προεπιλογή, τα Windows XP συστήματα χρησιμοποιούν Wi-Fi σε λειτουργία υποδομής, που σημαίνει ότι είναι clients της σύνδεση με ένα ασύρματο σημείο πρόσβασης (AP). (Η εναλλακτική λύση είναι ad hoc mode, το οποίο σημαίνει ότι οι ασύρματοι clients συνδέονται ο κάθε ένας χωρίς ένα AP. Το Ad hoc mode χρησιμοποιείται σπανίως.) Το πιο συχνά χρησιμοποιούμενο πρωτόκολλο Wi-Fi, είναι το IEEE 802.11b, το οποίο επικαλείται το WEP (Wired Equivalent Privacy) πρωτόκολλο, το οποίο έχει διάφορα γνωστά θέματα ασφαλείας. Για να υπάρξει μια πιο ασφαλής λύση στο Wi-Fi, μια βιομηχανική ομάδα που ονομάζεται Wi-Fi Alliance έχει δημιουργήσει ένα προϊόν πιστοποίησης που ονομάζεται Wi-Fi Protected Access (WPA)[57]. Το WPA απαιτεί αυστηρότερα μέτρα ασφαλείας από ότι προβλέπει το WEP, συμπεριλαμβανομένων των πιο εύρωστων αυθεντικότητας και διαχείρισης κλειδιών , η υποχρεωτική κρυπτογράφηση (συμπεριλαμβανομένων προαιρετικής υποστήριξης τη AES), για τον έλεγχο και την ακεραιότητα των δεδομένων. Το NIST συνιστά ότι οι χρήστες των Windows XP με Wi-Fi πρέπει να χρησιμοποιούν μια ισχυρότερη λύση από την ασφάλεια του WEP όποτε είναι πιθανόν[58]. Για το πρότυπο WPA, αυτό προϋποθέτει την εγκατάσταση ενός νέου οδηγού προσαρμογέα δικτύου για κάθε σύστημα των Windows XP, ενημέρωση προγραμμάτων δράσης για την υποστήριξη του WPA, τη ρύθμιση του Wi-Fi και clients για να επωφεληθούν από τα WPA features[59].

[56] Για περισσότερες πληροφορίες σχετικά με τη ασφάλεια του Wi-Fi, δείτε NIST SP 800-48 Revision 1, *Guide to Securing Legacy IEEE Wireless Networks* and NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i* (http://csrc.nist.gov/publications/PubsSPs.html). Windows-specific Wi-Fi references include *Securing Wireless LANs with Certificate Services* (http://www.microsoft.com/technet/security/prodtech/windowsserver2003/pkiwire/swlan.mspx?mfr=true) and *Securing Wireless LANs with PEAP and Passwords* (http://www.microsoft.com/downloads/details.aspx?FamilyID=60c5d0a1-9820-480e-aa38-63485eca8b9b&displaylang=en).

[57] More information on WPA is available from http://www.microsoft.com/windowsxp/using/networking/security/wireless.mspx.

[58] FIPS 140-2, *Security Requirements for Cryptographic Modules*, είναι υποχρεωτική και δεσμευτική για τις ομοσπονδιακές υπηρεσίες που έχουν προσδιορίσει ότι ορισμένες πληροφορίες πρέπει να προστατεύονται από μέσα κρυπτογραφίας. Για περισσότερες πληροφορίες σχετικά με τα FIPS-validated προϊόντα, visit http://csrc.nist.gov/groups/STM/index.html. WPA δεν απαιτεί FIPS-approved αλγορίθμους κρυπτογράφησης, αλλά από το διάδοχο, WPA2, WPA2 βασίζεται στο IEEE 802.11i. Οι οργανισμοί θα πρέπει να εξετάζουν προσεκτικά τη χρήση των προϊόντων με πιστοποίηση WPA2 και τα προϊόντα να υποστηρίζουν IEEE 802.11i αντί του non-FIPS-εφόσον εγκριθούν οι αλγόριθμοι που παρέχονται από το SP2. Για περισσότερες πληροφορίες σχετικά με το SP3's στη υποστήριξη του WPA and WPA2, δείτε το Appendix B.

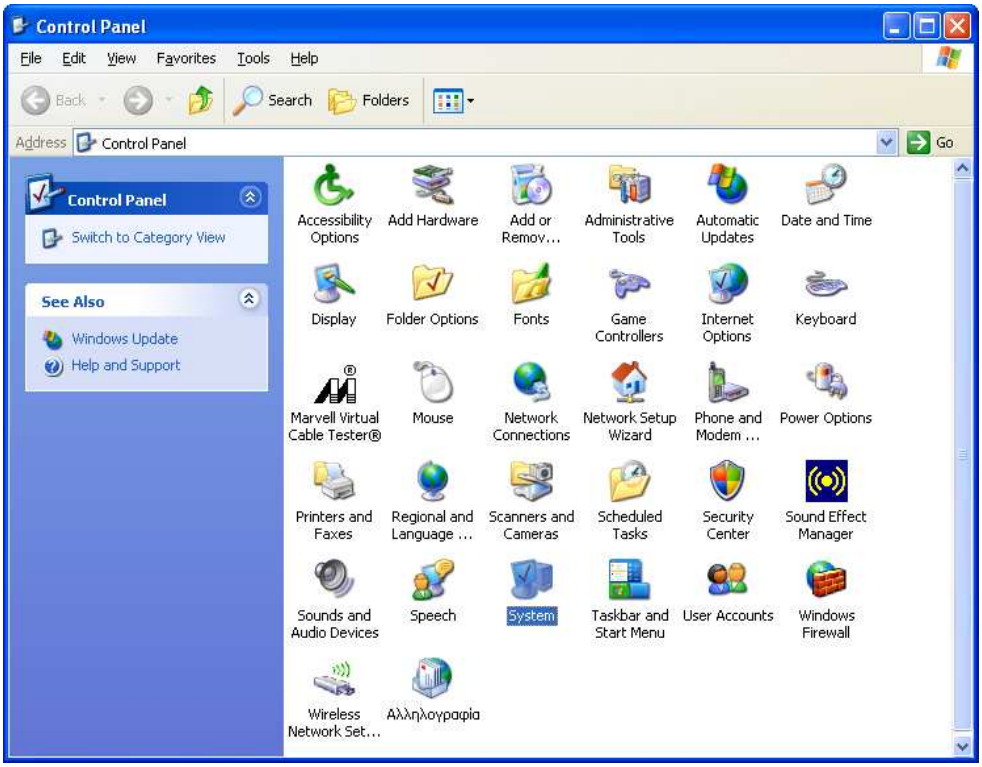
[59] The Microsoft TechNet article titled *Wireless Deployment Technology and Component Overview* (http://technet.microsoft.com/en-us/library/bb457015.aspx) περιέχει λεπτομερείς οδηγίες σχετικά με τη δημιουργία και τη διασφάλιση της ασύρματης σύνδεσης. Το άρθρο The Microsoft TechNet ονομάζεται *Configuring Windows XP IEEE 802.11 Wireless Networks for the Home and Small Business* παρέχει μια καλή επισκόπηση του θέματος; Αυτό είναι διαθέσιμο στη σελίδα http://www.microsoft.com/technet/network/wifi/wifisoho.mspx.

3.9 Memory Files

Στα συστήματα των Windows XP, το περιεχόμενο της μνήμης μπορεί να είναι αποθηκευμένα σε διάφορους τύπους αρχείων, συμπεριλαμβανομένων των αρχείων ένδειξης σφαλμάτων μνήμης, αρχείων τηλεειδοποίησης και αρχείων αδρανοποίησης. Κάθε ένα από αυτά τα αρχεία μπορεί ακούσια να εγγράφει ευαίσθητες πληροφορίες (π.χ., κωδικούς πρόσβασης, αποκρυπτογραφούνται στοιχεία) που θα μπορούσαν στη συνέχεια να ανακτηθούν από έναν εισβολέα. Όπως περιγράφεται παρακάτω, στον περιορισμό της χρήσης ή στη διατήρηση αυτών των αρχείων μπορεί να συμβάλουν στην πρόληψη της παράνομης πρόσβασης σε συστήματα και δεδομένα:

- **Memory Dump File.** Ένα memory dump file δημιουργείται κατά τη διάρκεια ενός σφάλματος προϋπόθεση για την αποθήκευση των περιεχομένων της μνήμης. Εφόσον δεν απαιτούνται ειδικά για λόγους αντιμετώπισης προβλημάτων, τα dump αρχεία δεν θα πρέπει να δημιουργούνται[60]. Η δράση αυτή μπορεί να πραγματοποιείται με σκοπό τα εξής:

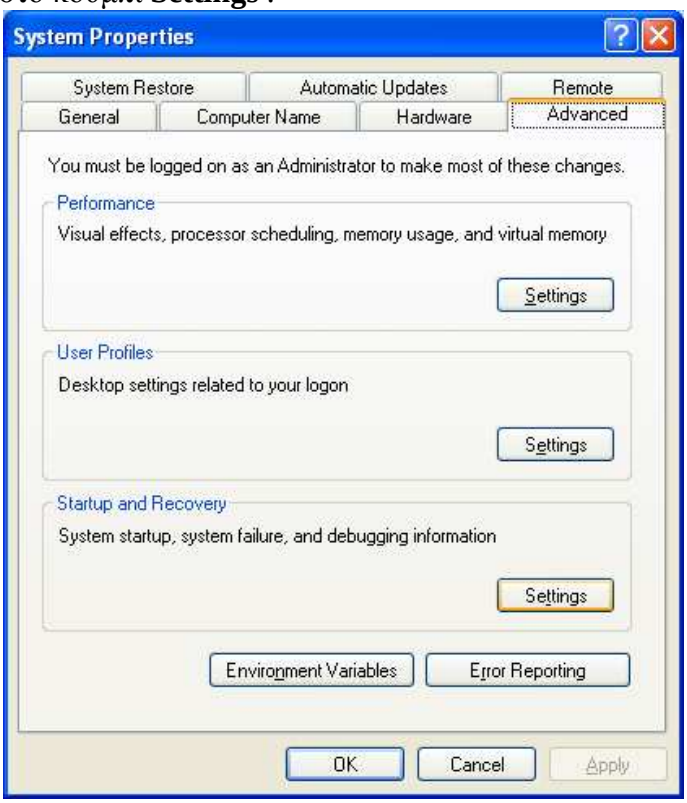
1. Ανοίξτε το **Control Panel** και επιλέξτε **System**. Επιλέξτε τη καρτέλα **Advanced** .



Εικόνα 286: System

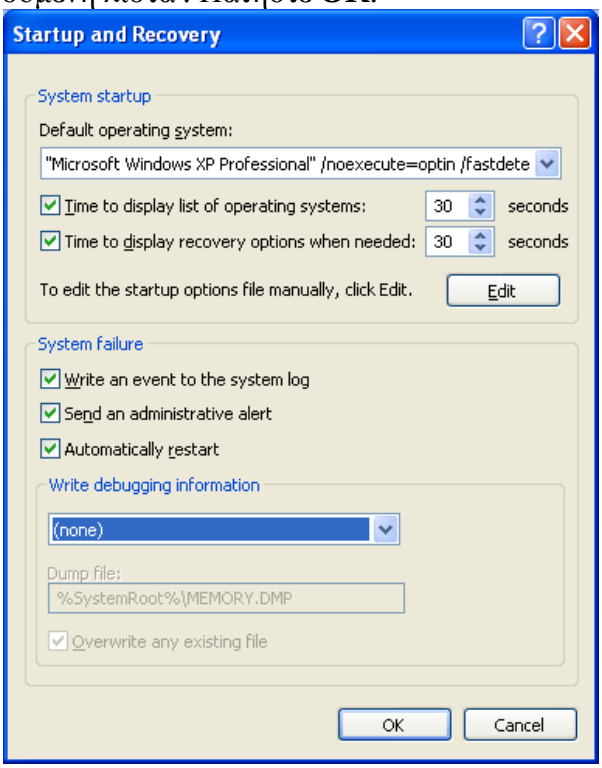
[60] Για περισσότερες πληροφορίες, δείτε το άρθρο MSKB 307973, *How to configure system failure and recovery options in Windows*, διαθέσιμο στη σελίδα http://support.microsoft.com/?id=307973, και το άρθρο 254649, *Overview of memory dump file options for Windows Server 2003, Windows XP, and Windows 2000*, διαθέσιμο στη σελίδα http://support.microsoft.com/?id=254649.

2. Στο **Startup and Recovery** στο τμήμα της καρτέλας **Advanced** , κάντε κλικ στο κουμπί **Settings** .



Εικόνα 287: System Properties

3. Στο **Write Debugging Information**, επιλέξτε **(none)** από τη αναπτυσσόμενη λίστα . Πατήστε **OK**.



Εικόνα 288: Startup and Recovery

- **Paging File.** Ένα paging file είναι ένα αρχείο που έχει κάποια από τα περιεχόμενα της μνήμης των Windows XP. Αυτό θα μπορούσε να περιλαμβάνει ευαίσθητες πληροφορίες. Όταν το σύστημα είναι απενεργοποιημένο και γίνεται επανεκκίνηση, τα Windows XP δεν επαναχρησιμοποίηση τα πυλαία περιεχόμενο του paging file. Ένας εισβολέας που αποκτά φυσική πρόσβαση στο μηχάνημα θα μπορούσε ενδεχομένως να έχει πρόσβαση σε ευαίσθητες πληροφορίες του paging file, έτσι οργανώσεις θα πρέπει να ρυθμίζουν τα Windows XP, για να καταργούν κάθε φορά που το σύστημα έχει απενεργοποιηθεί[61]. Πάντως, αυτό το σύστημα επιβραδύνει το reboots, ιδιαίτερα σε συστήματα με μεγάλες ποσότητες RAM. Το τμήμα 6.2.3 έχει οδηγίες για τη ρύθμιση αυτή της επιλογή ασφάλειας χειροκίνητα.

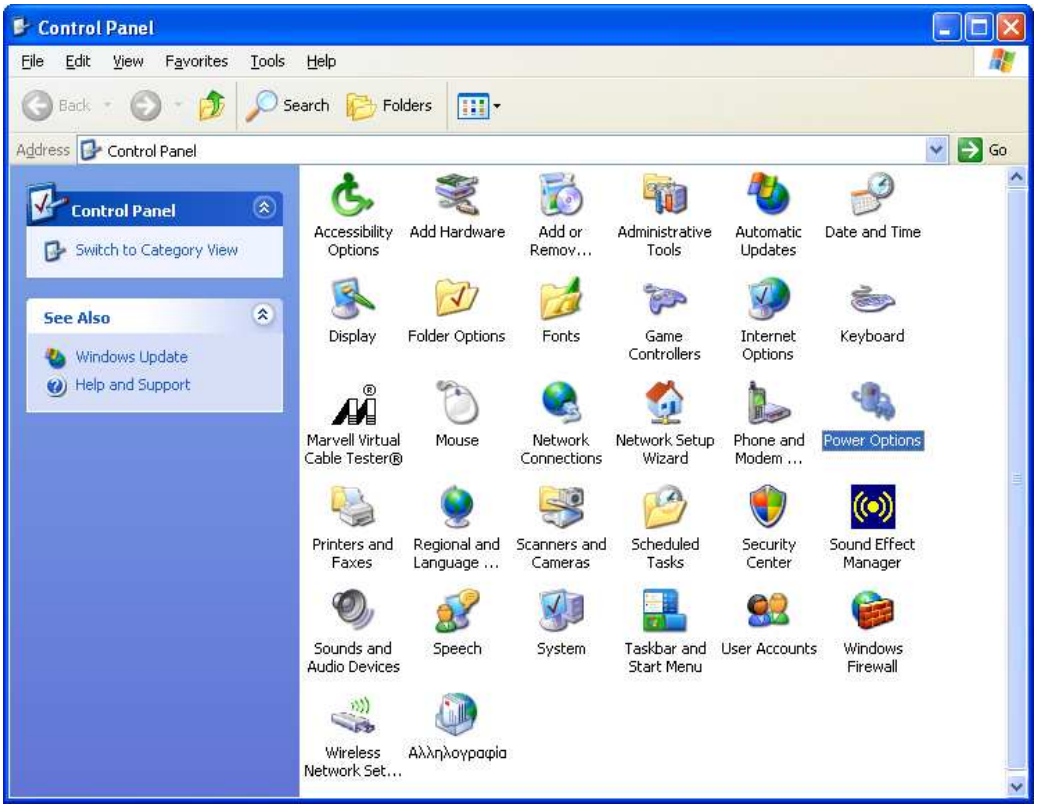
- **Hibernation File.** Ένα Hibernation File έχει δημιουργηθεί για τη διατήρηση της τρέχουσας κατάστασης του συστήματος (συνήθως ένα laptop) με την καταγραφή της μνήμης και το άνοιγμα των αρχείων πριν από τον τερματισμό του συστήματος. Στο σύστημα στη επόμενη ενεργοποίηση, η κατάσταση του συστήματος θα έχει αποκατασταθεί. Οι οργανισμοί ενδέχεται να επιθυμούν να εξετάσουν την απενεργοποίηση με τη χρήση των αρχείων αδρανοποίησης για τα SSLF συστήματα. Για να το κάνετε αυτό, ακολουθήστε τα παρακάτω βήματα:

  1. Ανοίξτε το **Control Panel**.

Εικόνα 289: Control Panel

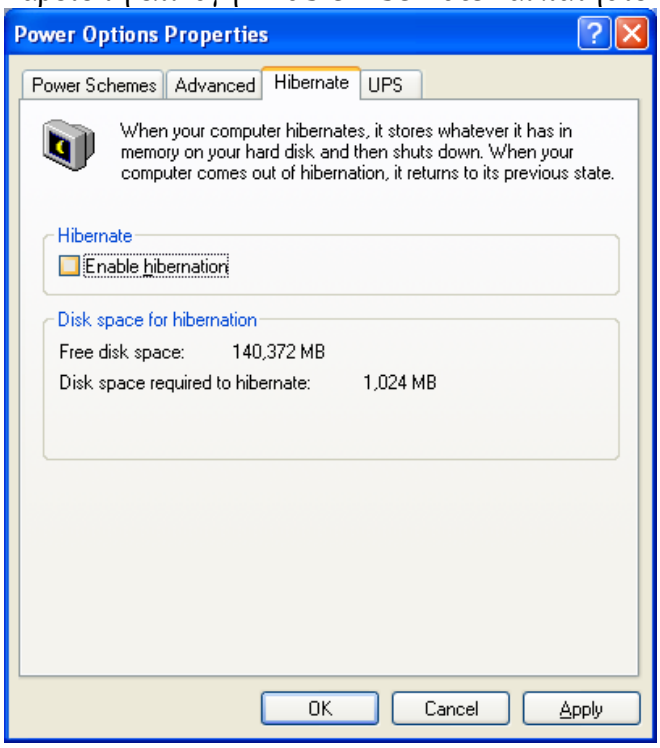
  2. Κάντε κλικ πάνω στο **Power Options** και στη συνέχεια κάντε κλικ στη καρτέλα **Hibernate** .

[61] For more information, see MSKB article 314834, *How to Clear the Windows Paging File at Shutdown*, available at http://support.microsoft.com/?id=314834.



Εικόνα 290: Power Options

3. Ξεμαρκάρετε τη επιλογή **Enable hibernate** και πατήστε **Apply**.



Εικόνα 291: Power Hibernate Properties

3.10 Summary of Recommendations

(Τελικές Υποδείξεις)

- Στην επιχείρηση, τα SSLF και FDCC περιβάλλοντα, ανακατασκευάζουν τα υπάρχοντα συστήματα που βασίζονται στη FAT κατατμήσεις με NTFS, αντί της μετατροπής FAT σε NTFS.

- Τροποποιήστε το Folder Options έτσι ώστε να βελτιωθούν άμυνες κατά των κακόβουλων προγραμμάτων δείχνοντας πλήρως όλα τα ονόματα αρχείων για τη τροποποίηση των επεκτάσεων των αρχείων που χρησιμοποιείται συχνά για κακόβουλους σκοπούς.

- Deploy EFS όταν το απόρρητο των εν λόγω πληροφοριών είναι ζωτικής σημασίας ή όταν το σύστημα αντιμετωπίζει σημαντικές φυσικές απειλές. Κάθε EFS ανάπτυξης θα πρέπει να λάβει υπόψη βασικά θέματα διαχείρισης. Αν η διαχείριση κλειδιών δεν αντιμετωπίζονται αποτελεσματικά, η χρήση του EFS θα μπορούσε να συμβάλει στην απώλεια πολύτιμων πληροφοριών. Σε συστήματα που χρησιμοποιούν το EFS σύστημα, η χρήση του Syskey να θεσπίσει ένα κλειδί εκκίνησης που θα προστατεύει τα ιδιωτικά κλειδιά που χρησιμοποιούνται για το EFS σύστημα.

- Έλεγχο όλων των συσκευών αποθήκευσης, συμπεριλαμβανομένων των σταθερών συσκευών καθώς και των κινητών συστημάτων και των μέσων ενημέρωσης, πριν από την επαναχρησιμοποίηση τους ή τη διάθεσης τους.

- Δημιουργήστε ένα ξεχωριστό λογαριασμό επιπέδου χρήστη για κάθε πρόσωπο που εκτελεί καθημερινά λειτουργία ενός συστήματος. Χρησιμοποιήστε το επιπέδου λογαριασμών του διαχειριστή για το σύστημα διαχείρισης καθηκόντων μόνο.

- Σε μη διαχειριζόμενα περιβάλλοντα, να δημιουργήσετε μια δισκέτα επαναφοράς κωδικού πρόσβασης για το σύστημα και να το αποθηκεύει σε μια φυσικά ασφαλή θέση.

- Απενεργοποιήστε και μετονομάστε τους built-in Administrator και Guess accounts λογαριασμούς.

- Χρησιμοποιήστε έναν κωδικό πρόσβασης στο screen-saver για την προστασία του συστήματος από την χωρίς άδεια τοπικής πρόσβασης.

- Επανεξέταση των audit logs σε τακτική βάση.

- Χρησιμοποιήστε το Windows Firewall για να περιορίσετε τις εισερχόμενες συνδέσεις δικτύου αν το σύστημα δεν προστατεύεται από ένα τρίτο μέρος τείχος προστασίας.

- Χρησιμοποιήστε μια πιο ισχυρή λύση από την ασφάλεια του WEP, όπου είναι δυνατόν, για ασύρματη δικτύωση.

- Ρύθμιση του συστήματος ώστε να μην δημιουργούν dump αρχεία, αν δεν είναι πράγματι αναγκαία για λόγους αντιμετώπισης προβλημάτων.

Κεφάλαιο 4

4 Application Security Configuration Recommendations

Αυτό το τμήμα εξετάζει την διαμόρφωσης ασφαλείας για έξι τύπους εφαρμογών, που χρησιμοποιούνται συνήθως στα συστήματα Windows XP: ακολουθίες εφαρμογή της παραγωγικότητας , e-mail(πελάτες ηλεκτρονικού ταχυδρομείου), Web browsers (προγράμματα περιήγησης στο Web), antivirus software (λογισμικό αντιμετώπισης ιών), προσωπικά firewalls και λογισμικά αντιμετώπισης ιών[62]. Τα παραδείγματα διαμόρφωσης στόχων ασφάλειας περιλαμβάνουν την αφήγηση μιας εφαρμογής για να γίνει η λήψη των ενημερωμένων εκδόσεων αυτόματα σε εβδομαδιαία βάση, απενεργοποίηση περιττών λειτουργιών και επιλογών που επιτρέπουν στους χρήστες να εγκρίνουν ορισμένες ενέργειες, όπως η αποδοχή ενός cookie σε ένα πρόγραμμα περιήγησης στο Web. Ο σκοπός αυτού του κεφαλαίου είναι να επισημάνει τα σημαντικά στοιχεία για τη ρύθμιση των παραμέτρων ασφαλείας για κάθε τύπο εφαρμογής. Οι δυνατότητες διαμόρφωσης ασφαλείας διαφέρουν μεταξύ των προϊόντων, για αυτό οι συστάσεις που παρέχονται στο τμήμα αυτό δεν είναι πλήρης και δεν ισχύουν για κάθε προϊόν.

Οι περισσότερες από τις συστάσεις ρύθμισης ασφαλείας σε αυτό το τμήμα προορίζονται ειδικά για την παροχή προστασίας από ιούς, worms, Trojan horses, spyware, και άλλων ειδών malware[63]. Όταν ρυθμίζετε τις αιτήσεις, οι διαχειριστές και οι χρήστες θα πρέπει επίσης να συμμορφώνονται με τη τοπικούς πολιτική σχετικά με τη χρήση των μακροεντολών , του κινητού κώδικα (π.χ., Java, JavaScript, ActiveX), browser plug-ins, και άλλους τύπους κώδικα που μπορούν να εγκυμονούν αυξημένο κίνδυνο ασφαλείας.

Οι οργανισμοί θα πρέπει προσεκτικά να εξετάσουν τις ρυθμίσεις των εφαρμογών ασφαλείας πριν από την εγκατάσταση τους σε μια οργάνωση για να εξασφαλίζουν ότι είναι επαρκώς ισχυρή για την οργάνωση των αναγκών του και ότι δεν προκαλεί παρεμβολές σε άλλες ακούσιες λειτουργίες[64]. Επίσης, συστήνεται να εκτελεστεί ένα σύστημα αντιγράφων ασφαλείας, προτού εγκαταστήσετε ή ανασχεδιάσετε το λογισμικό, γιατί οι ενέργειες αυτές θα μπορούσαν να τροποποιήσουν το σύστημα αρχείων, το μητρώο των Windows ή άλλα κρίσιμα στοιχεία του συστήματος. Είναι σημαντικό να διατηρηθεί ένα λειτουργικό αντίγραφο ασφαλείας του συστήματος σε περίπτωση σφάλματος. Η παράγραφος 2.2 περιλαμβάνει πληροφορίες για τη εκτέλεση των συστημάτων ασφαλείας.

[62] Οι εφαρμογές στο τμήμα αυτό δεν είναι καθόλου πλήρη ,η λίστα των αιτήσεων για την εγκατάσταση σε υπολογιστές με Windows XP , αυτός ο οδηγός δεν υποδηλώνει την υποστήριξη ορισμένων προϊόντων.

[63] Για περισσότερες πληροφορίες σχετικά με το κακόβουλο λογισμικό, ανατρέξτε στο NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*, και NIST SP 800-28 Έκδοση 2, *Guidelines on Active Content and Mobile Code* , τα οποία είναι διαθέσιμα στη σελίδα http://csrc.nist.gov/publications/PubsSPs.html.

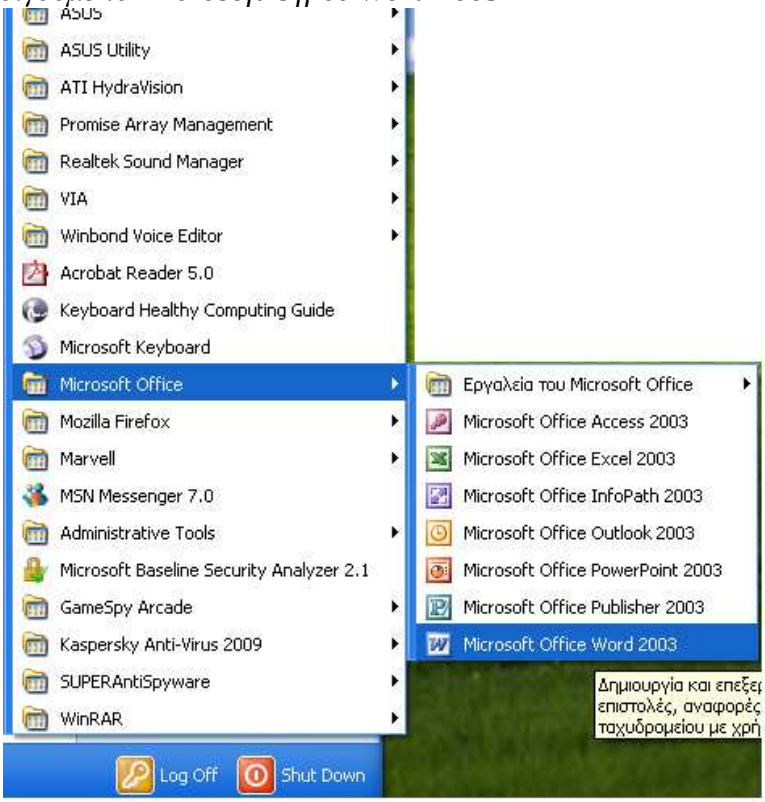
[64] Πρόσθετες πληροφορίες σχετικά με τις πιθανές ασυμβατότητες μεταξύ των εφαρμογών Windows XP SP2 ή SP3 είναι διαθέσιμα από τη Microsoft Application Compatibility και User Account Control http://technet.microsoft.com/en-us/windows/aa905066.aspx.

4.1 Productivity Application Suites

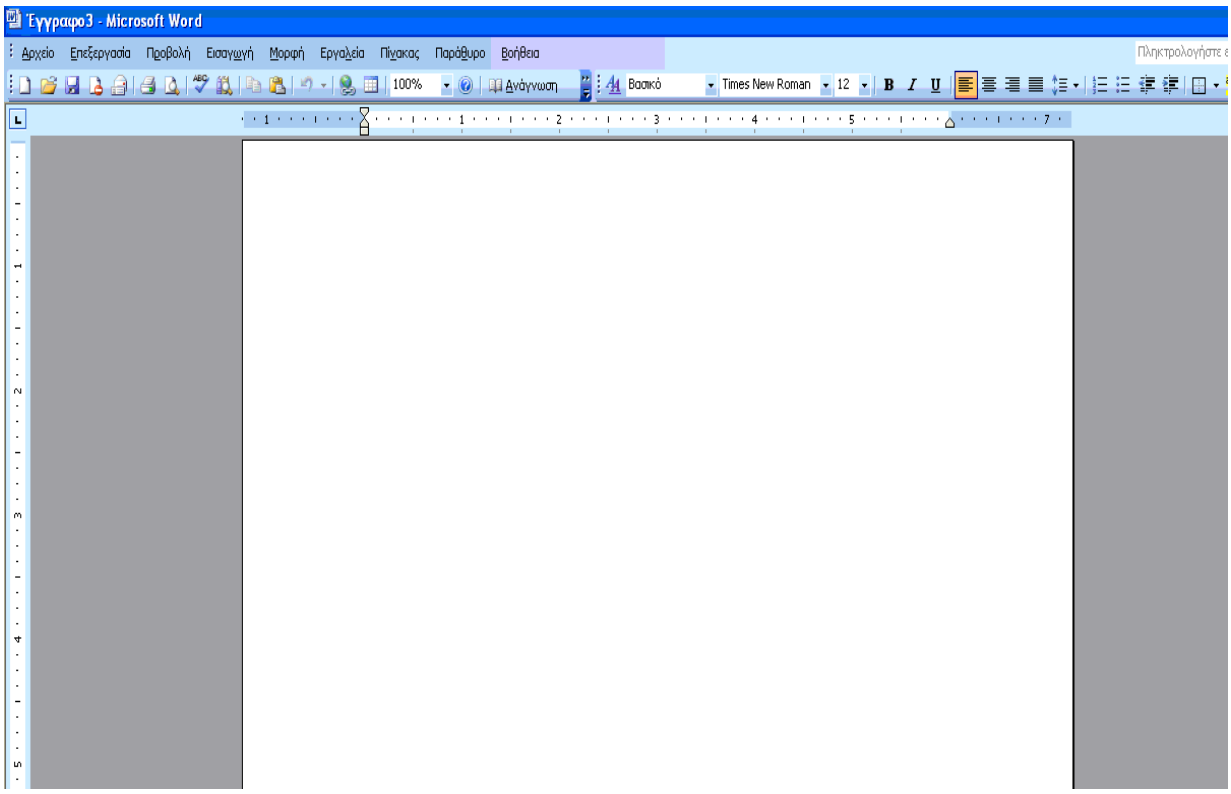
Η παραγωγικότητα της εφαρμογή suit αναφέρεται σε μια σειρά από ολοκληρωμένες εφαρμογές που παρέχει αρκετά διαφορετικά είδη λειτουργιών, όπως η επεξεργασία κειμένου και τα λογιστικά φύλλα. Συνήθως, κάθε αίτηση εντός της suit έχει παρόμοια διεπαφή και πολλά χαρακτηριστικά γνωρίσματα που παρέχονται από δύο ή περισσότερες εφαρμογές στη suit. Συστάσεις για την εξασφάλιση της εφαρμογής στη παραγωγικότητα της suit περιλαμβάνουν:

Σα παράδειγμα για τη εξασφάλιση στην εφαρμογή μιας productivity application suit εφαρμόσαμε για το Microsoft Office Word 2003.

Ανοίγουμε το Microsoft Office Word 2003



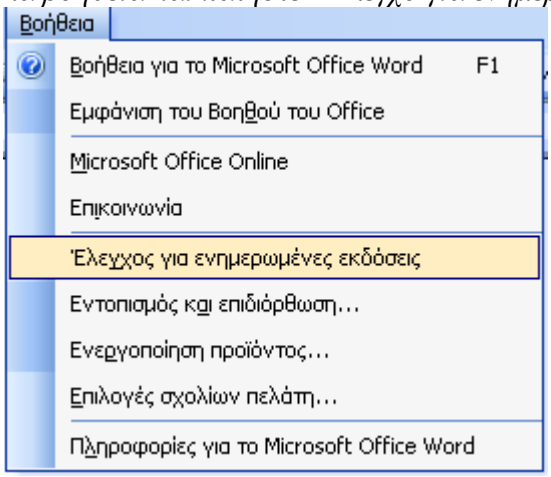
Εικόνα 292: Microsoft Office Word 2003



Εικόνα 293: Έγγραφο Microsoft Word

- Βεβαιωθείτε ότι όλες οι παραγωγικότητες των εφαρμογών suites διατηρούν τα τρέχουσα patches και ενημερώσεις.

Πηγαίνετε στη καρτέλα βοήθεια και πατήστε "Έλεγχο για ενημερωμένες εκδόσεις"



Εικόνα 294: Έλεγχος για Ενημερωμένες εκδόσεις

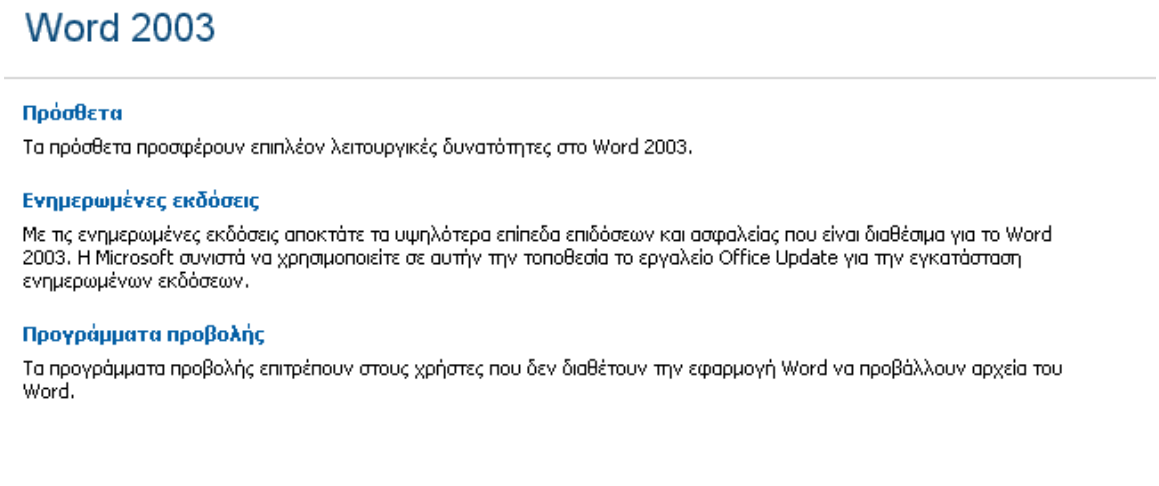
Θα σας πάει στη σελίδα της Microsoft όπου βρίσκονται τα office(word,excel,access κτλ) Πατήστε office 2003(την έκδοση που χρησιμοποιείται) στη στήλη με τα στοιχεία λήψης.

Εικόνα 295: Στοιχεία Λήψεις

Μόλις το πατήσετε θα σας εμφανίσει το εξής;

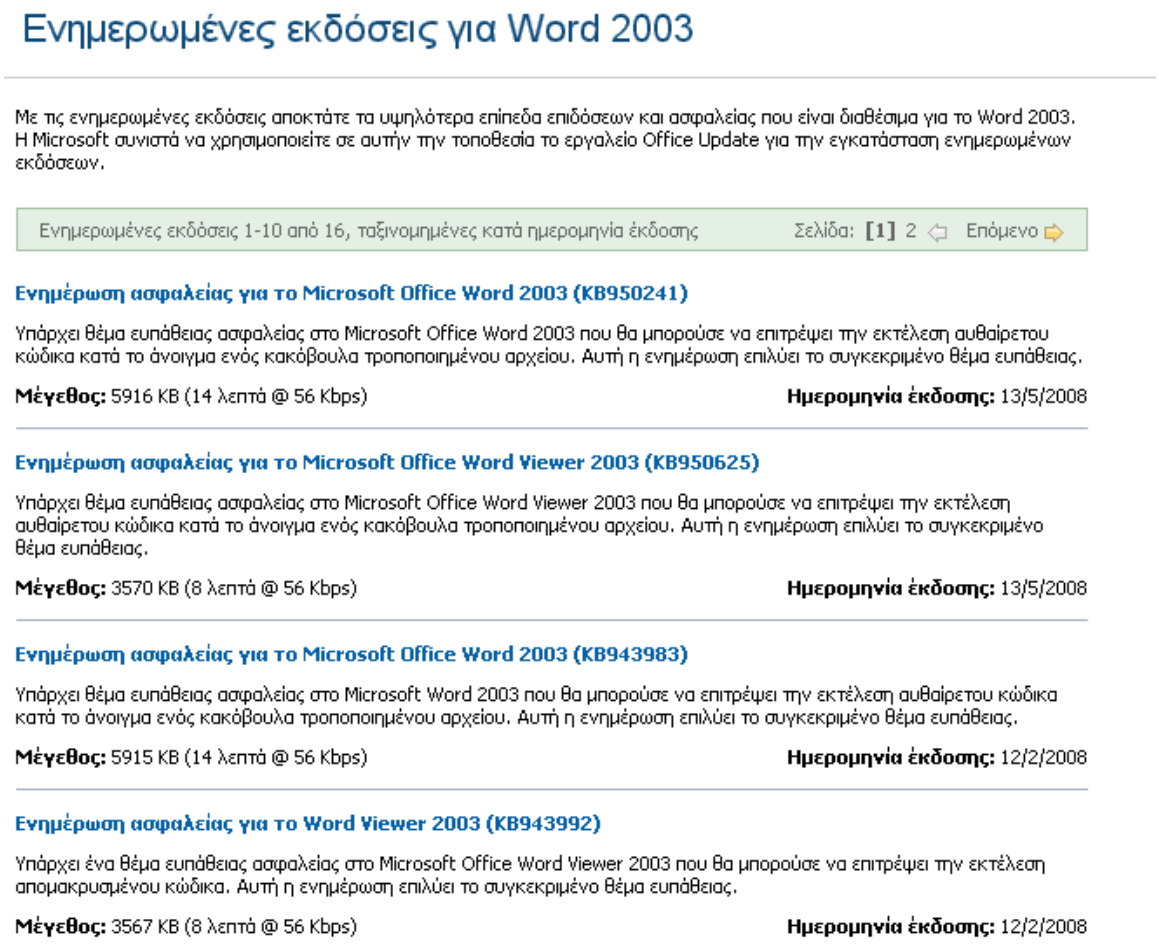
Εικόνα 296: Λήψεις για το Office 2003

Πατήστε Word 2003 και θα εμφανιστεί το παρακάτω



Εικόνα 297: Λήψεις για το Word 2003

Πατήστε "Ενημερωμένες εκδόσεις" και θα σας εμφανιστούν οι ενημερώσεις που είναι διαθέσιμες.



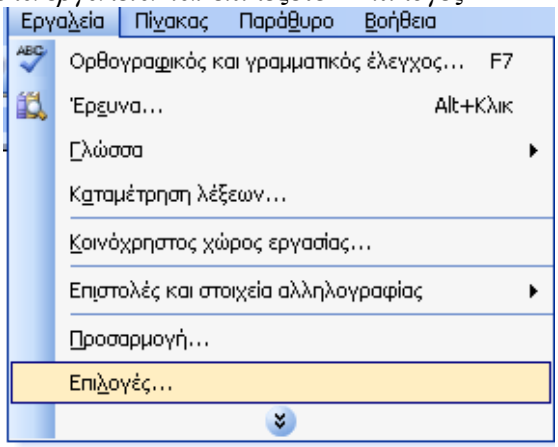
Εικόνα 298: Ενημερωμένες εκδόσεις για το Word 2003

Επιλέξτε όποια θέλετε και θα εγκατασταθεί αυτόματα.

- Ρύθμιση των χαρακτηριστικών της μακροεντολής, έτσι ώστε να μειωθεί η πιθανότητα ότι αυτά θα πρέπει να αξιοποιηθούν για τη διάδοση του

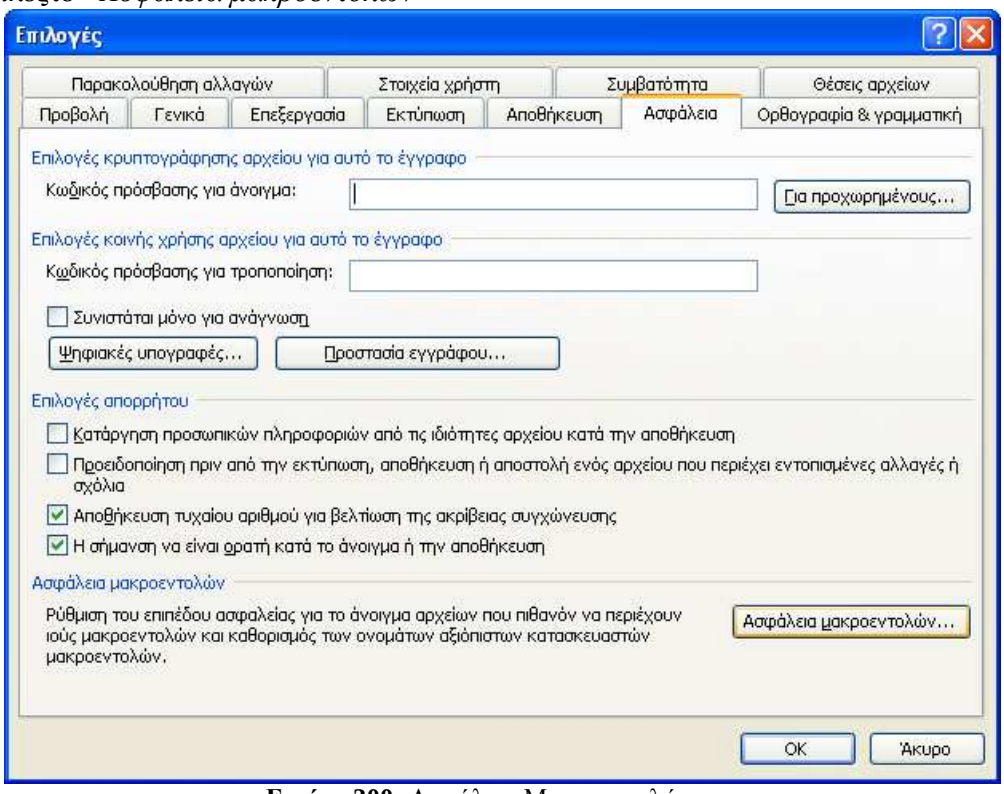
κακόβουλου λογισμικού. Για παράδειγμα, ορισμένοι διαχειριστές των suites επιτρέπουν να προσδιορίζετε αν οι μακροεντολές είναι δυνατό να εκτελεστούν αυτόματα ή αν ο χρήστης να έχει τη συγκατάθεσή του για τη λειτουργία της κάθε μακροεντολής. Άλλο ένα χαρακτηριστικό που προσφέρεται από κάποιες suites είναι να διευκρινιστεί από ποιους καταλόγους οι μακροεντολές είναι δυνατό να εκτελεστούν.

Πηγαίνετε στη καρτέλα εργαλεία και επιλέξετε "Επιλογές"



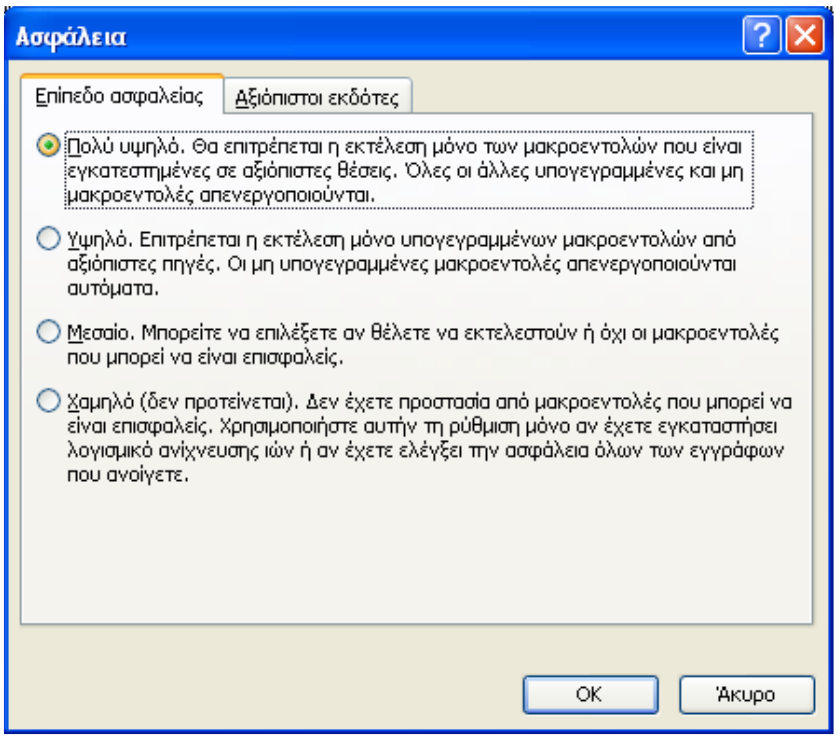
Εικόνα 299: Ρύθμιση των Χαρακτηριστικών της Μακροεντολής

Εμφανίζεται το παρακάτω παράθυρο. Πατήστε στη καρτέλα "Ασφάλεια" και μετά επιλέξτε "Ασφάλεια μακροεντολών"



Εικόνα 300: Ασφάλεια Μακροεντολών

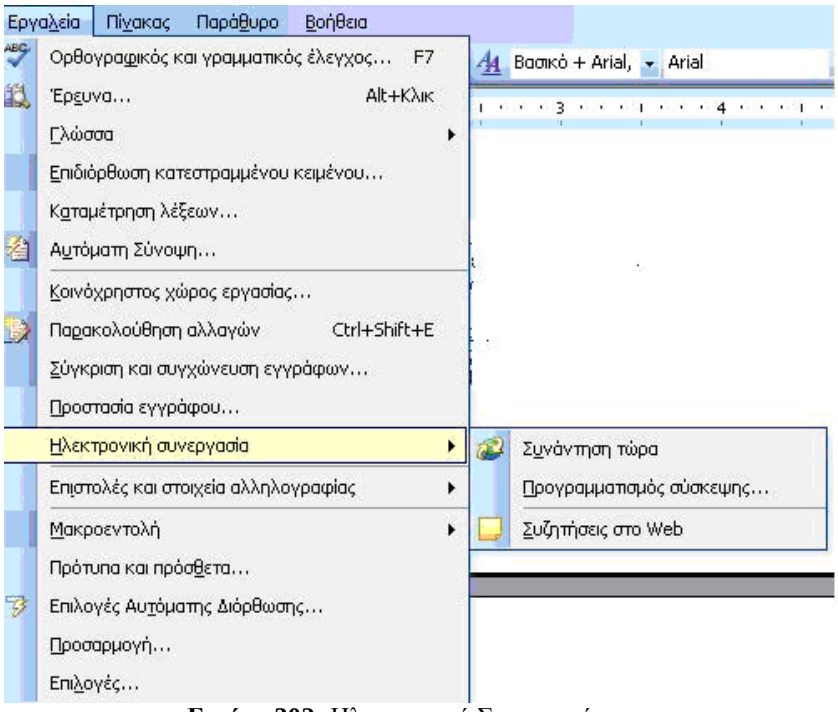
Επιλέξτε το πρώτο radio button όπου είναι επίπεδο ασφαλείας υψηλό και πατήστε OK



Εικόνα 301: Επίπεδο ασφαλείας

- Απενεργοποίηση των δυνατοτήτων συνεργασίας εάν δεν είναι χρήσιμες.

Πηγαίνετε στη καρτέλα εργαλεία και επιλέξετε "Ηλεκτρονική συνεργασία "και επιλέξτε μια από 3 επιλογές αν τυχόν θέλετε να ενεργοποιήσετε την ηλεκτρονική συνεργασία .



Εικόνα 302: Ηλεκτρονική Συνεργασία

4.2 Web Browsers

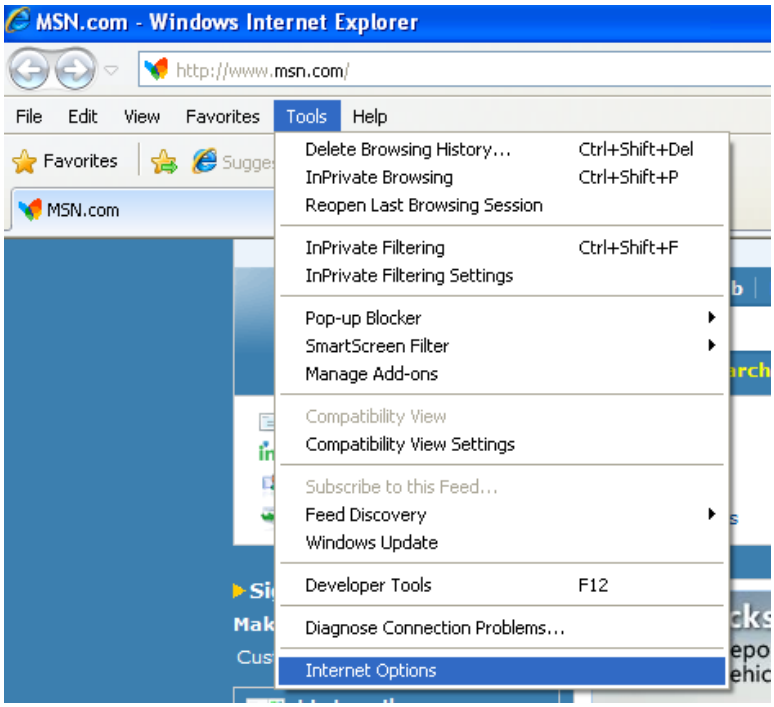
Οι Web browsers είναι ικανοί για συντακτική ανάλυση με πολλές μορφές ενεργού κώδικα, συμπεριλαμβανομένης της JavaScript, ActiveX, και Java, κακόβουλα άτομα συχνά να επωφεληθούν από το να επιτεθούν στα συστήματα, με το να διανέμουν κακόβουλο λογισμικό ή με κάποιο άλλο τρόπο να επηρεάζουν αρνητικά τα συστήματα. Για παράδειγμα, ορισμένοι τύποι cookies κατατίθενται στο σύστημα ενός χρήστη όπου μπορούν να χρησιμοποιηθούν για την παρακολούθηση του χρήστη στις συνήθειες περιήγησης του και να τις αναφέρουν σε έναν εξωτερικό διακομιστή. Ως εκ τούτου, οι οργανισμοί θα πρέπει να εξετάζουν προσεκτικά τις πιθανές επιπτώσεις της με το να επιτρέπουν αυτές τις λειτουργίες. Συστάσεις για την ασφάλεια στους web browsers ακολουθούν:

Οι πιο γνωστοί web browsers είναι:
1. INTERNET EXPLORER 8
2. FIREFOX 3.0.7
3. GOOGLE CHROME
4. SAFARI 4

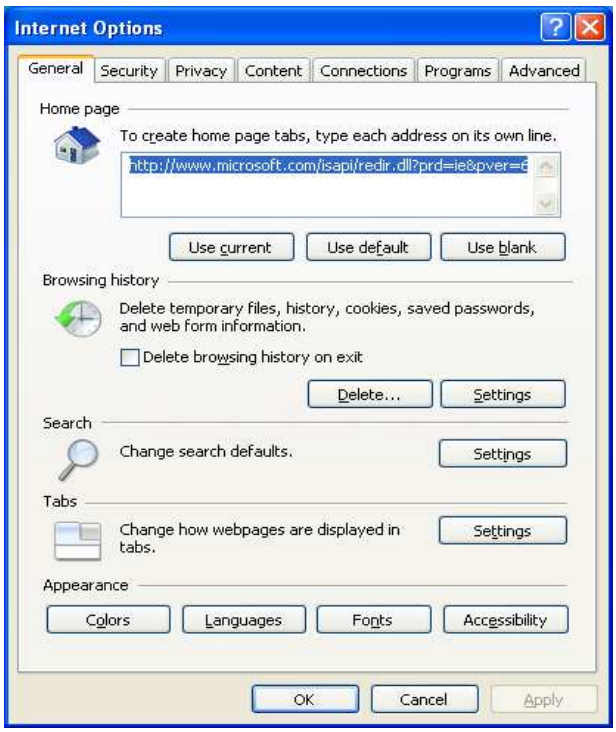
Θα εξετάσουμε τον INTERNET EXPLORER 8 σχετικά με τη ασφάλεια του.

- Βεβαιωθείτε ότι όλοι οι web browsers διατηρούν τα τρέχουσα patches και ενημερώσεις.

Ανοίξτε τον internet explorer και επιλέξετε από την καρτέλα tools "internet options"

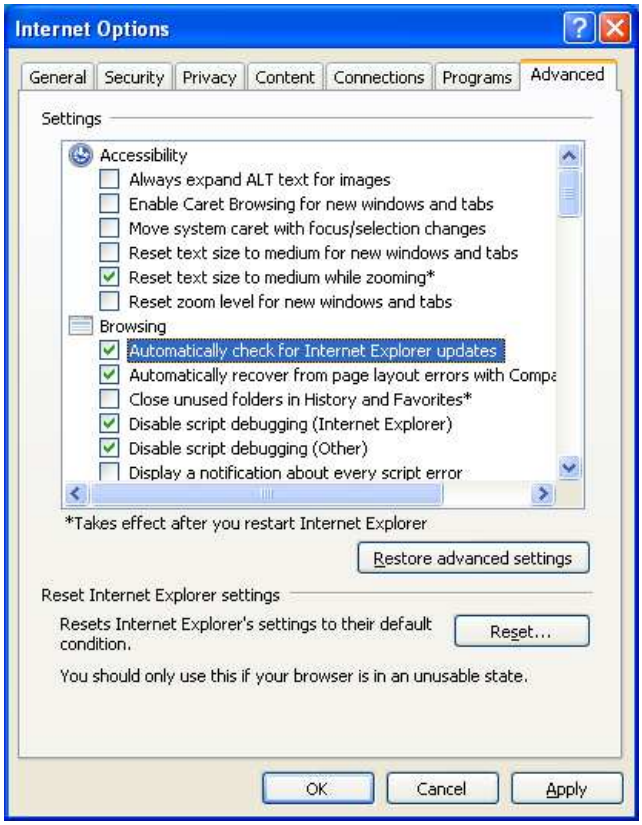


Εικόνα 303: Tools



Εικόνα 304: Internet Options

Επιλέξετε από τη καρτέλα advanced στο Browsing την πρώτη και δεύτερη επιλογή όπου να ενημερώνεται αυτόματα ο browser για τυχόν ενημερώσεις και πατήστε Apply και μετά Ok.

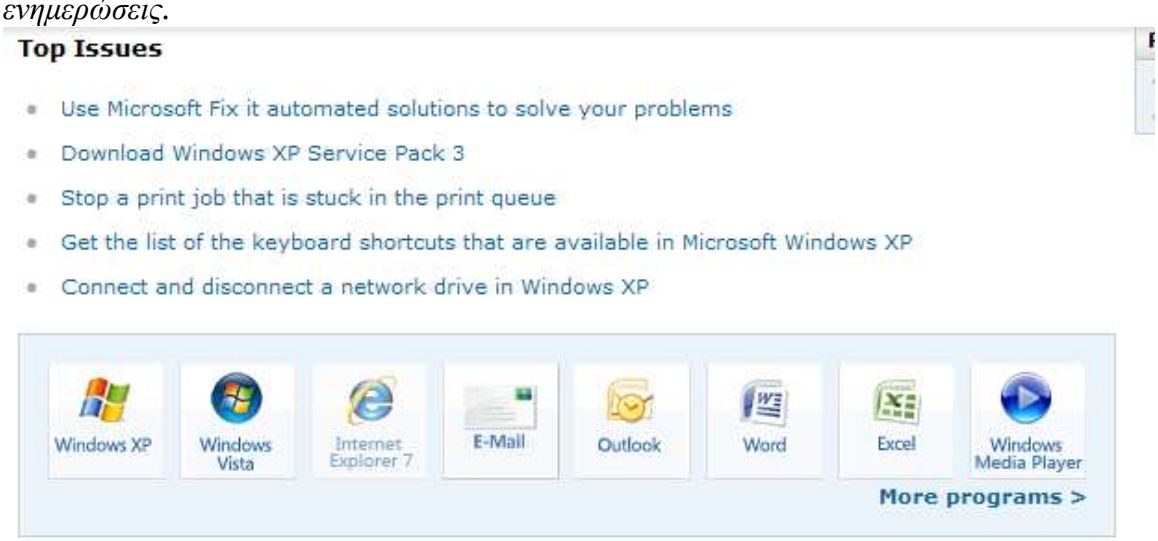


Εικόνα 305: Browsing

Επιπρόσθετα επιλέξτε από τη καρτέλα Help ”Online Support”

Εικόνα 306: Online Support

Θα σας εμφανίσει μερικά από τα προϊόντα της Microsoft όπου υπάρχουν ενημερώσεις.



Εικόνα 307: Προϊόντα της Microsoft με Διαθέσιμες Ενημερώσεις

Επειδή χρησιμοποιώ το internet explorer 8 που πρόσφατα εμφανίστηκε δε υπάρχουν ενημερώσεις. Για παράδειγμα θα σας δείξω πως θα γινόταν αν είχα το internet explorer 7. Πατώντας πάνω στο εικονίδιο του internet explorer 7 θα μας εμφάνιζε το εξής .

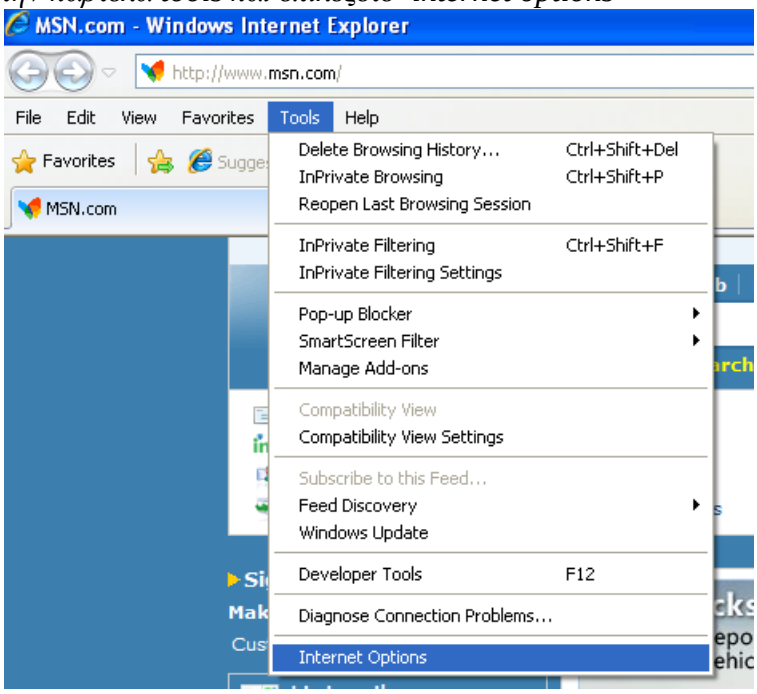
Εικόνα 308: Internet Explorer 7

Πατώντας στο "Downloads and updates" θα μας εμφανίσει τις πιο δημοφιλείς λήψεις και ενημερώσεις.

Εικόνα 309: Popular Downloads and Updates

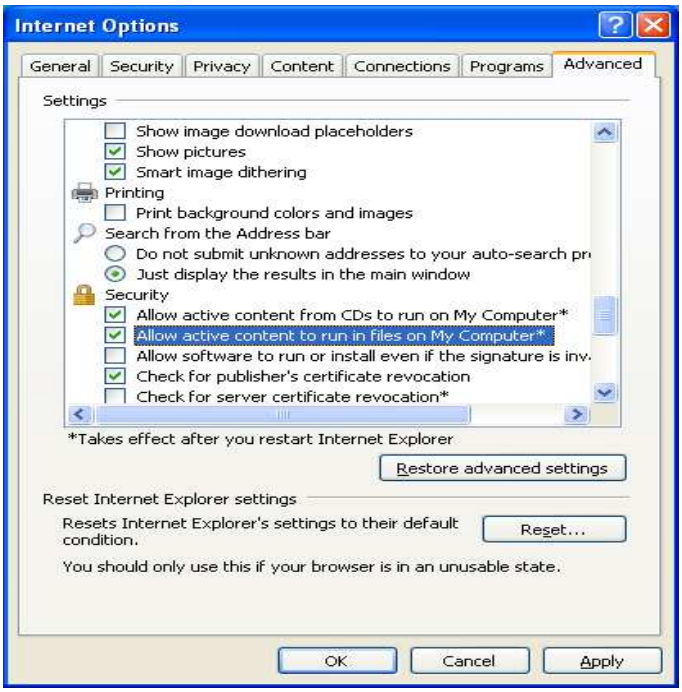
- Περιορίστε το ενεργό περιεχόμενο και τις δέσμες ενεργειών, όπως διευκρινίζεται το είδος του ενεργού περιεχομένου και σενάρια που μπορούν να διενεργούνται από τις όποιες τοποθεσίες ή τα είδη των θέσεων (π.χ., η οργάνωση των διακομιστών, των εξωτερικών servers).

Πηγαίνετε στην καρτέλα tools και επιλέξετε"internet options"



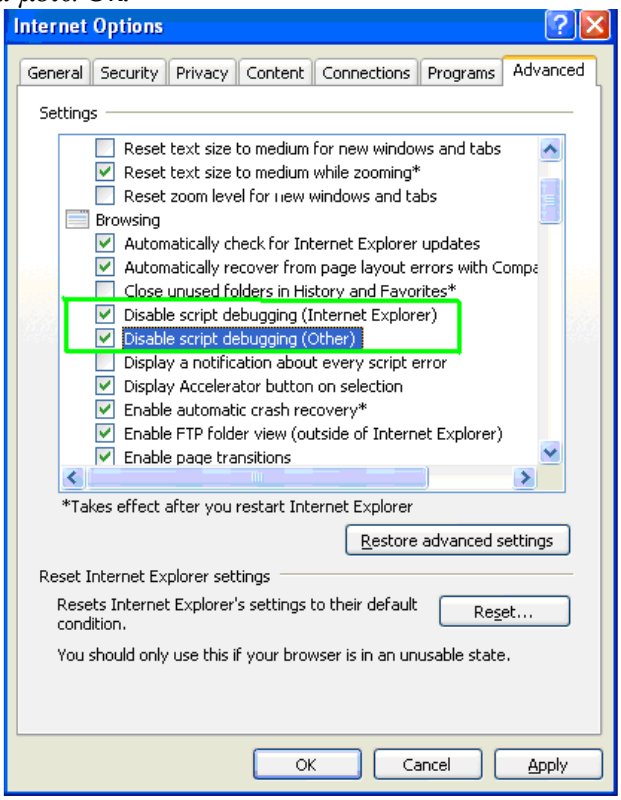
Εικόνα 310: Internet Options

Επιλέξετε από τη καρτέλα advanced στο Security τη δεύτερη επιλογή και πατήστε Apply και μετά Ok.



Εικόνα 311: Security

Επιλέξετε από τη καρτέλα advanced στο Browsing την τέταρτη και πέμπτη επιλογή πατήστε Apply και μετά Ok.

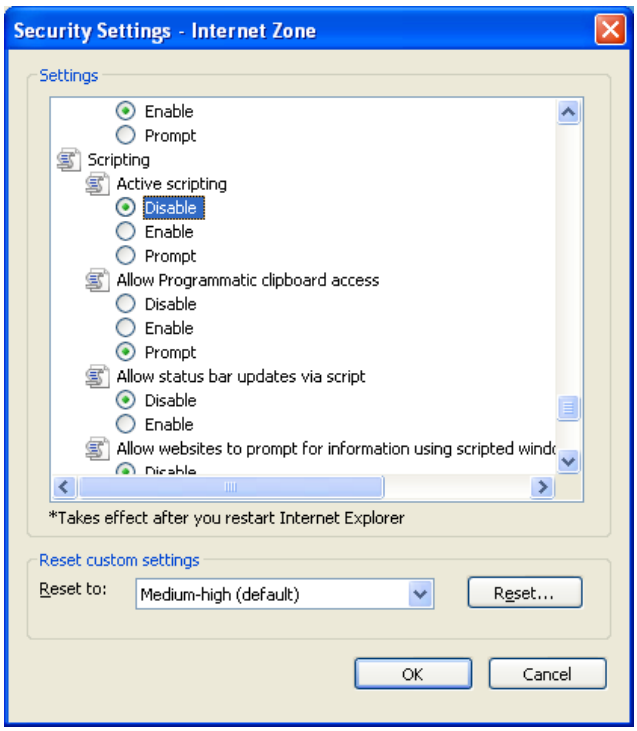


Εικόνα 312: Advanced Browsing

Επίσης πηγαίνετε στη καρτέλα security των windows options και επιλέξτε "Custom level"

Εικόνα 313: Custom Level

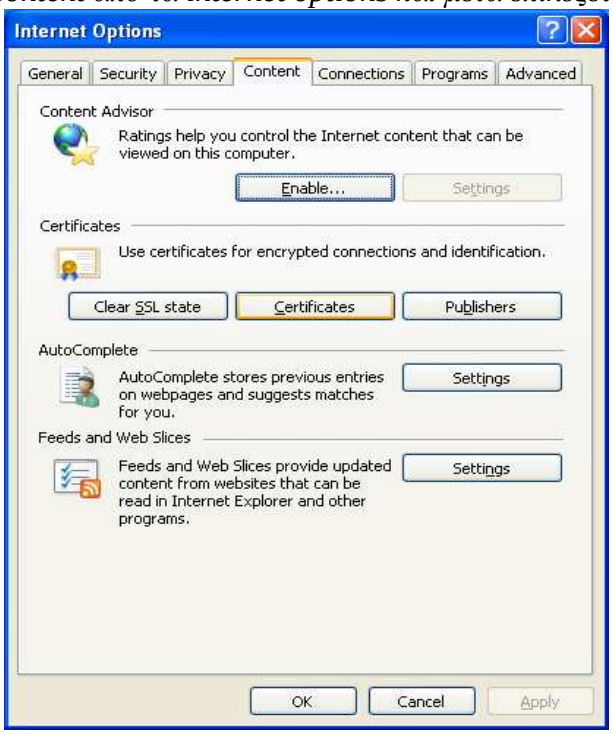
Και τέλος επιλέξτε "Disabled" στο radio button του Active scripting



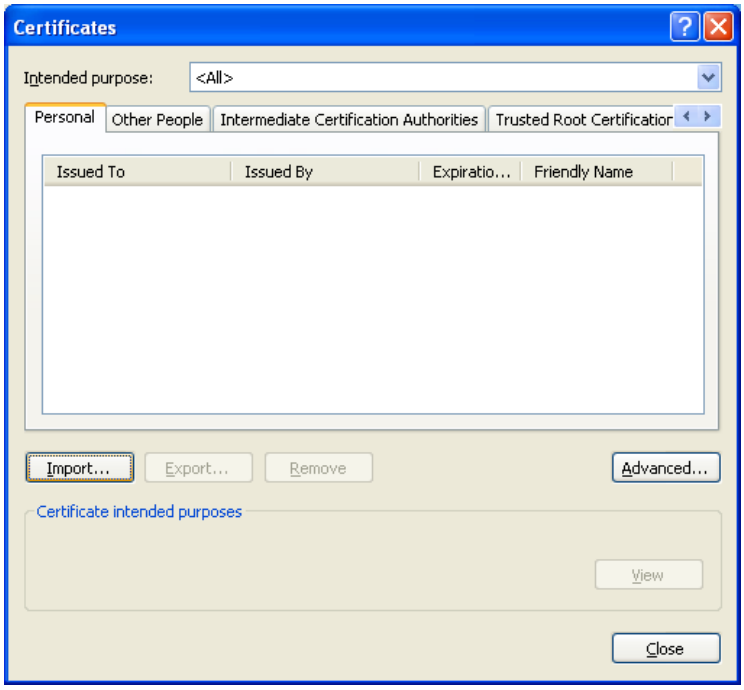
Εικόνα 314: Security Settings-Internet Zone

- Να επαληθεύσετε ότι στο πρόγραμμα περιήγησης στο Web το ψηφιακό πιστοποιητικό δεν έχει ανακληθεί πριν από την αποδοχή, ότι είναι νόμιμο και τρέχον.

Επιλέξτε τη καρτέλα content από τα internet options και μετά επιλέξετε certificates



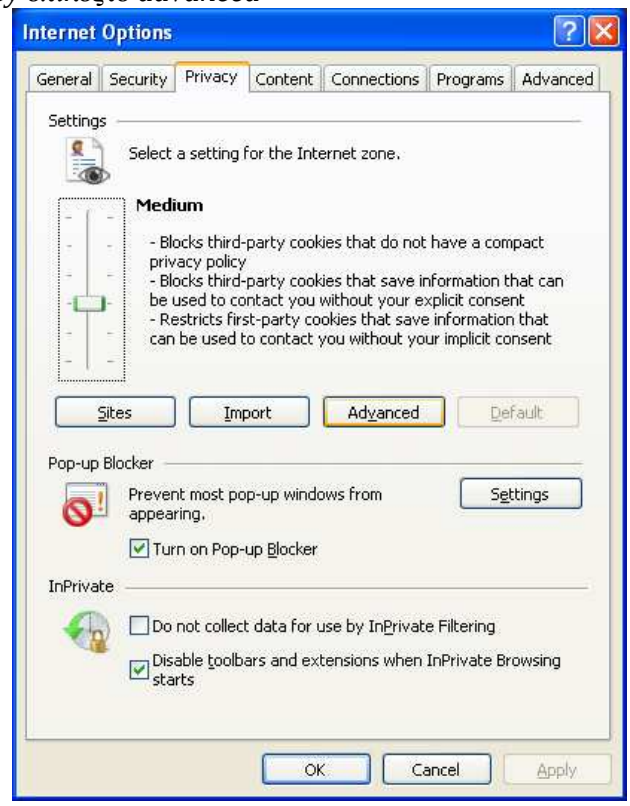
Εικόνα 315: Content



Εικόνα 316: Certificates

- Περιορίστε τον χειρισμό των cookies .Για παράδειγμα, να προτρέψετε τους χρήστες να αποδέχονται κάθε τρίτου cookie που παρουσιάζεται στο σύστημα και να επιτρέπουν τα cookies μόνο για τον δικτυακό τόπο καταγωγής.

Στην καρτέλα Privacy επιλέξτε advanced



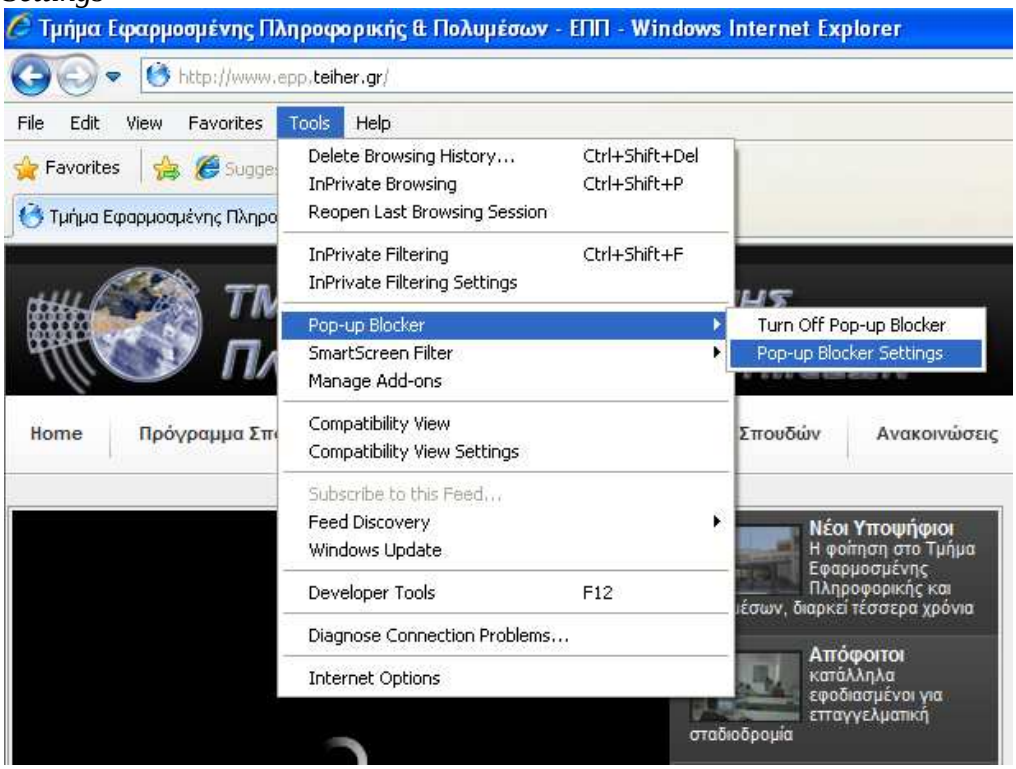
Εικόνα 317: Privacy Advanced

Επιλέξτε το κουτάκι που λέει "Override automatic cookie handing" και πατήστε στο Third-party Cookies"Block".

Εικόνα 318: Advanced Privacy Settings

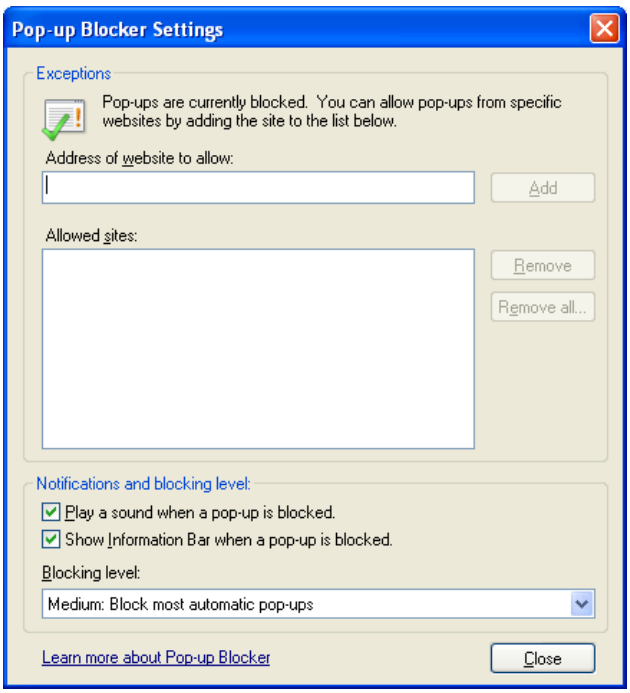
- Ενεργοποιήστε στα προγράμματα περιήγησης των αναδυόμενων παράθυρων τον blocker, και οι τυχόν επιτρεπόμενες τοποθεσίες σε μια λίστα εξαιρέσεων.

Από τη καρτέλα Tools του internet explorer επιλέξτε "Pop-up Blocker→ Pop-up Settings



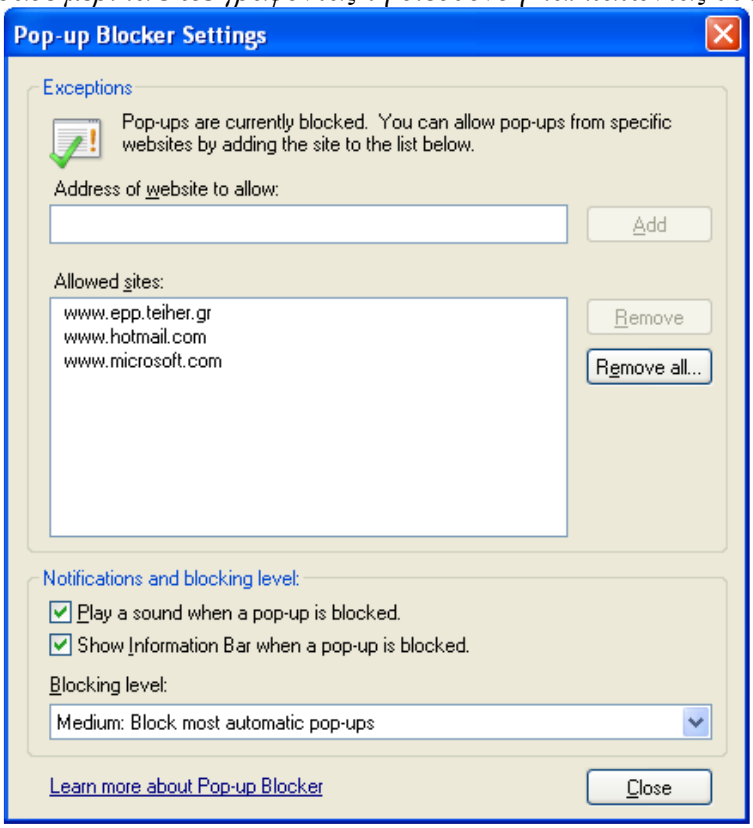
Εικόνα 319: Pop-up Blocker

Εμφανίζετε το παρακάτω παράθυρο όπου σε ενημερώνει να προσθέσεις τα επιτρεπόμενα sites



Εικόνα 320: Pop-up Blocker Settings

Ενδεικτικά πέρασε μερικά sites γράφοντας τη διεύθυνση και πατώντας add



Εικόνα 321: Allowed Sites

4.3 E-mail Clients

Το e-mail έχει γίνει κύριο μέσο για τις επιχειρήσεις και τις προσωπικές επικοινωνίες, καθώς και η διάδοση του κακόβουλου λογισμικού. Η προσεκτική ρύθμιση του ηλεκτρονικού ταχυδρομείου των πελατών δεν είναι σημαντικό μόνο για την προστασία ενός συγκεκριμένου υπολογιστή, αλλά και για την πρόληψη της εξάπλωσης των ιών και worms από τον υπολογιστή σε άλλους. Η εξασφάλιση e-mail χρησιμοποιώντας εφαρμογές περιλαμβανομένων του antivirus και το antispyware λογισμικό, στην ευαισθητοποίηση των χρηστών στη χρήση e-mail με πρακτικές ασφάλειας, που περιορίζουν τα προνόμια για τη κατάσχεση e-mail με καταλόγους,[65] και τη σωστή ρύθμιση των πελατών του ηλεκτρονικού ταχυδρομείου, συμπεριλαμβανομένων και των μηχανισμών του anti-spam[66]. Για να λειτουργήσει μια αίτηση e-mail με ασφαλή τρόπο, συνιστάται η εφαρμογή του λογισμικού να <<μπαλώνεται>> ταχτικά[67] και ότι η εκτέλεση των ενεργών περιεχόμενων να περιορίζεται ή να απενεργοποιείτε πλήρως. Διάφορες συστάσεις ασφαλείας για τους e-mail client ακολουθούν:

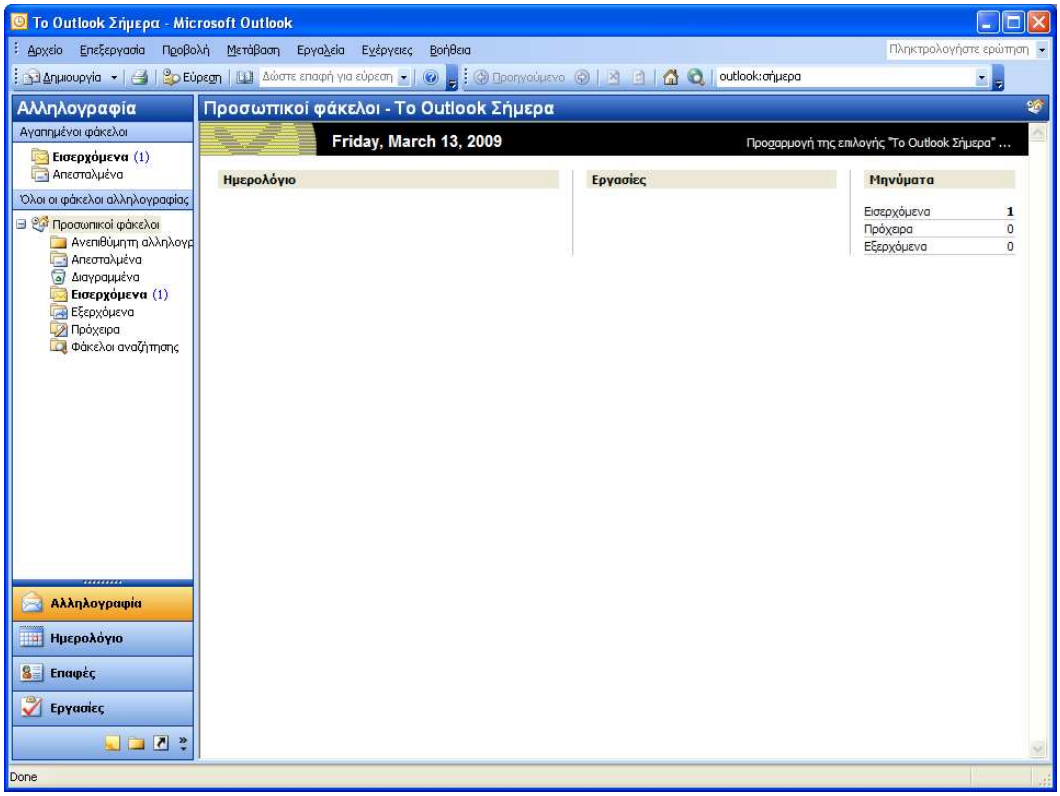
Θα ενσωματώσουμε τις συστάσεις ασφαλείας για παράδειγμα στο Microsoft Outlook Email. Ανοίξτε το Outlook πηγαίνοντας start→ all programs(αν δε σας στο εμφανίζει αμέσως)και κάντε διπλό κλικ στο εικονίδιο του Outlook και θα ανοίξει το πρόγραμμα.

Εικόνα 322: Άνοιγμα του Microsoft Office Outlook

[65] Η ρύθμιση κατάσχεσης e-mail του καταλόγου, έτσι ώστε τα αρχεία αυτά να μην μπορούν να εκτελεστούν (π.χ., την άρση των Execute από τους καταλόγους) Η ρύθμιση αυτή μπορεί να προλάβει ορισμένες μορφές κακόβουλων συνημμένων από το να τρέχει σε συστήματα. Ένας χρήστης θα χρειαστεί να προχωρήσει σε ένα τέτοιο αρχείο σε ένα απροστάτευτο κατάλογο και στη συνέχεια να εκτελέσει και να μολύνει το σύστημα. Όλοι οι χρήστες πρέπει να έχουν επίγνωση αυτού και να αναθέσουν στης αποδεκτές μεθόδους για τον χειρισμό των συνημμένων.

[66] Το spam μπορεί να επηρεάσει αρνητικά την ασφάλεια με διάφορους τρόπους. Για παράδειγμα, μερικά spam περιέχουν κακόβουλα περιεχόμενα που θα μπορούσαν να μολύνουν τα συστήματα των χρηστών? Τα Spam σε άλλες χρήσεις κοινωνικής μηχανικής τεχνικής μπορούν να κάνουν κόλπο στους χρήστες να επισκέπτονται phony σε ιστοσελίδες ή άλλων επικαλυπτόμενων και ευαίσθητων πληροφοριών, όπως αριθμούς κοινωνικής ασφάλισης, αριθμούς πιστωτικών καρτών, και κωδικούς πρόσβασης.

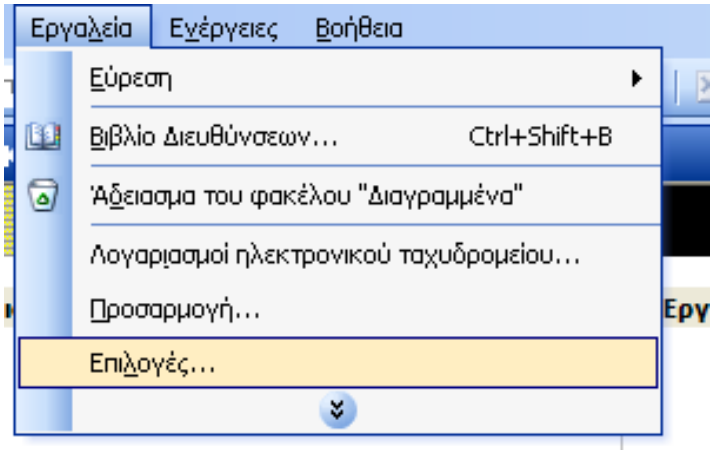
[67] Στα διαχειρισμένα περιβάλλοντα, οι ενημερώσεις θα πρέπει να εκτελούνται σύμφωνα με τις τοπικές πολιτικές.



Εικόνα 323: Microsoft Office Outlook

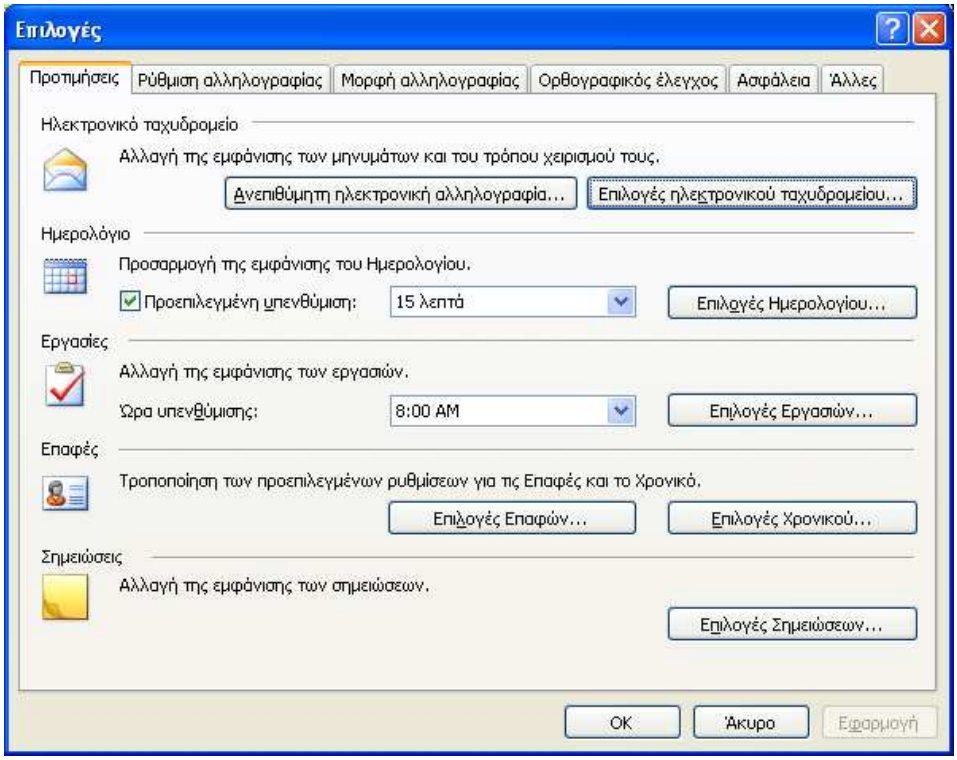
- Ενεργοποίηση του junk e-mail με δυνατότητες φιλτραρίσματος.

Πηγαίνετε στη καρτέλα εργαλεία και πατήστε "Επιλογές"



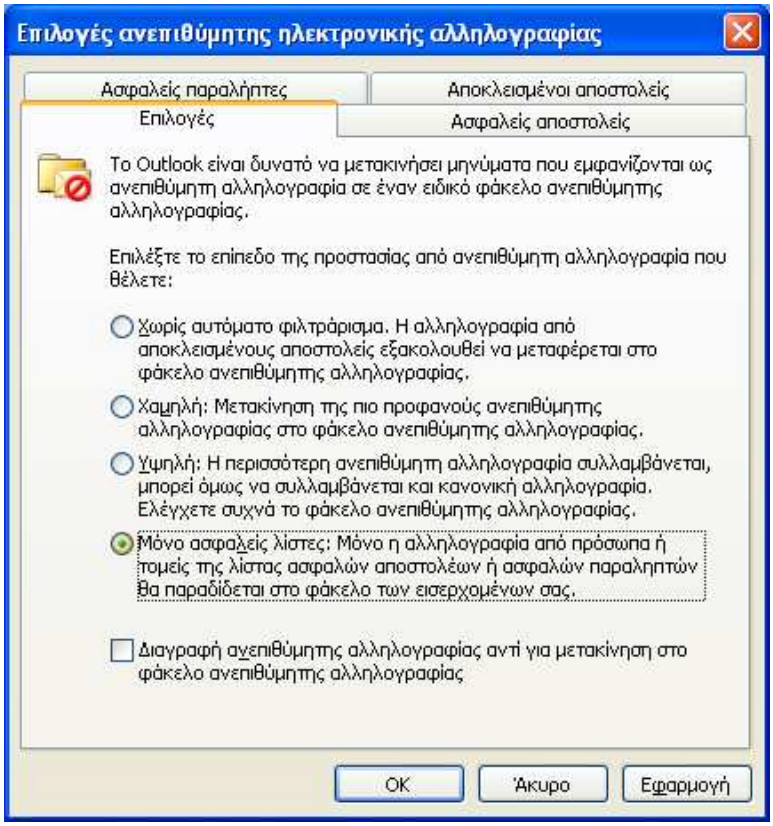
Εικόνα 324: Επιλογές Εργαλείων

Πατήστε τώρα στη καρτέλα Προτιμήσεις την επιλογή "Επιλογές ηλεκτρονικού ταχυδρομείου.."



Εικόνα 325: Επιλογές Ηλεκτρονικού Εμπορίου

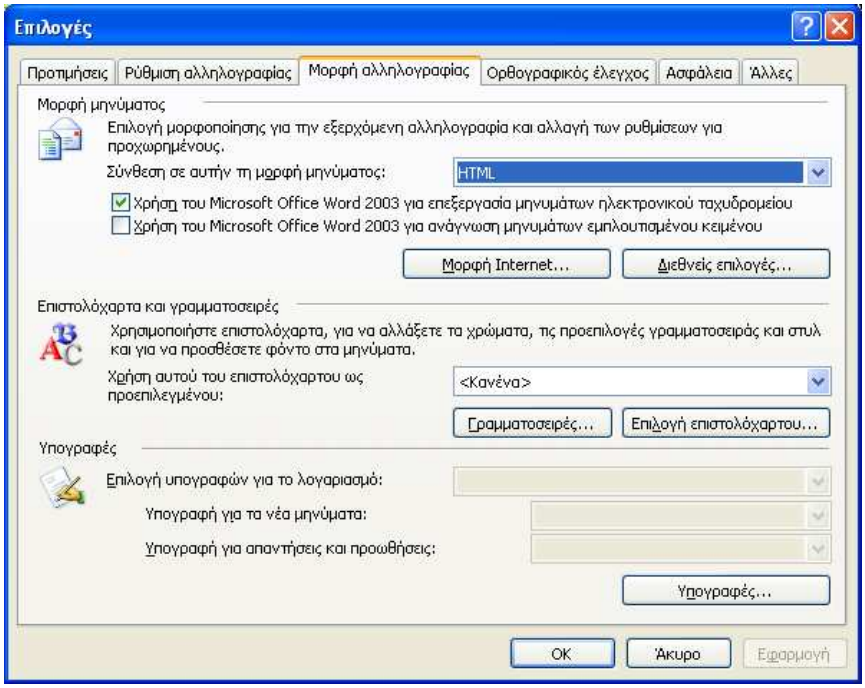
Και διαλέξτε από τις Επιλογές το τέταρτο radio button"Μόνο ασφαλείς λίστες".



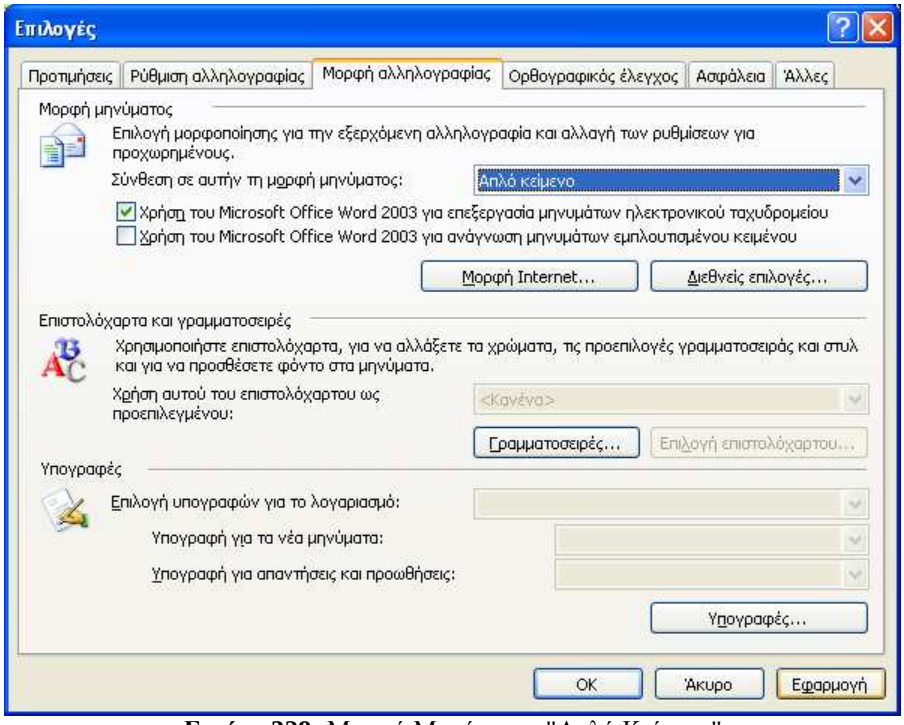
Εικόνα 326: Επιλογές ανεπιθύμητης ηλεκτρονικής αλληλογραφίας

- Ορίστε την προεπιλεγμένη μορφή για τη σύνθεση μηνύματος του ηλεκτρονικού ταχυδρομείου σε απλό κείμενο (όχι HTML, εμπλουτισμένο κείμενο, κλπ.)

Πηγαίνετε στη καρτέλα εργαλεία και πατήστε "Επιλογές". Μετά πηγαίνετε στη καρτέλα Μορφή της αλληλογραφίας και αλλάξτε την επιλογή "Σύνθεση σε αυτήν τη μορφή μηνύματος" από html σε απλό κείμενο. Πατήστε Εφαρμογή και μετά OK



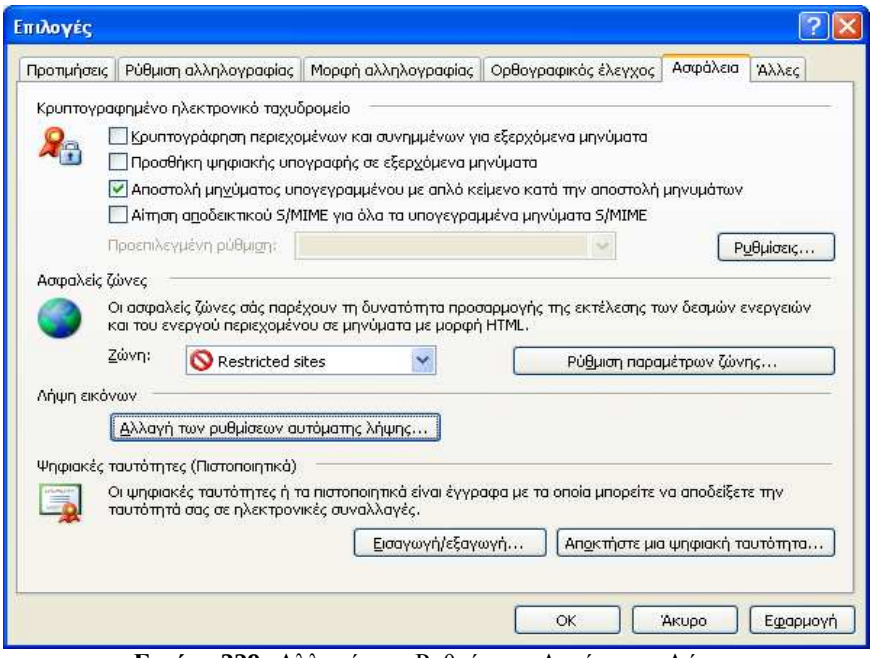
Εικόνα 327: Μορφή Αλληλογραφίας



Εικόνα 328: Μορφή Μηνύματος "Απλό Κείμενο"

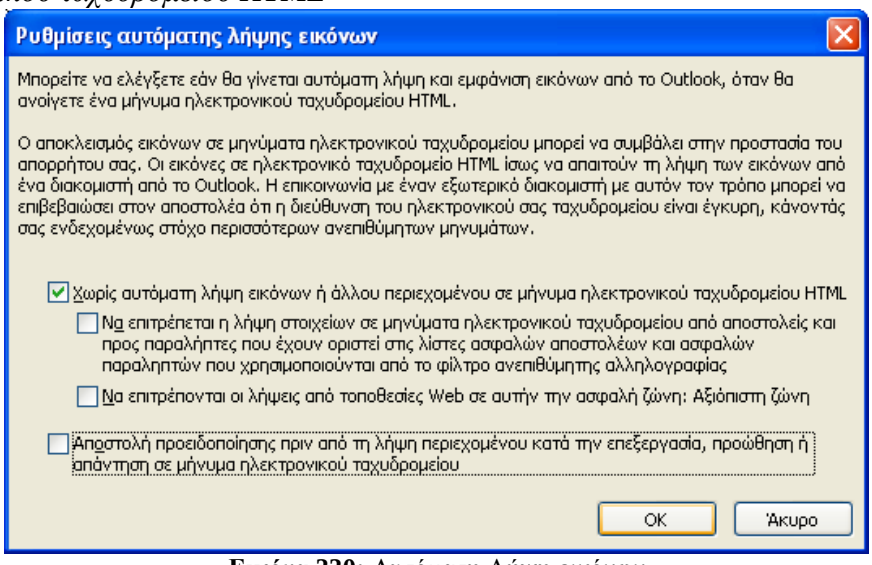
- Απενεργοποιήστε την φόρτωση των εικόνων μέσα σε απομακρυσμένα μηνύματα e-mail. Ένα από τα οφέλη από την ενεργοποίηση αυτής της ρύθμισης είναι ότι εμποδίζει τα spam από τα μηνύματα που χρησιμοποιούν μικρές εικόνες εντός e-mail για να παρακολουθούν τους χρήστες που τα έχουν ανοίξει.

Πηγαίνετε στη καρτέλα εργαλεία και πατήστε "Επιλογές". Μετά πηγαίνετε στη καρτέλα Ασφάλεια και στη Λήψη Εικόνων πατήστε την επιλογή "Αλλαγή των ρυθμίσεων αυτόματης λήψης"



Εικόνα 329: Αλλαγή των Ρυθμίσεων Αυτόματης Λήψης

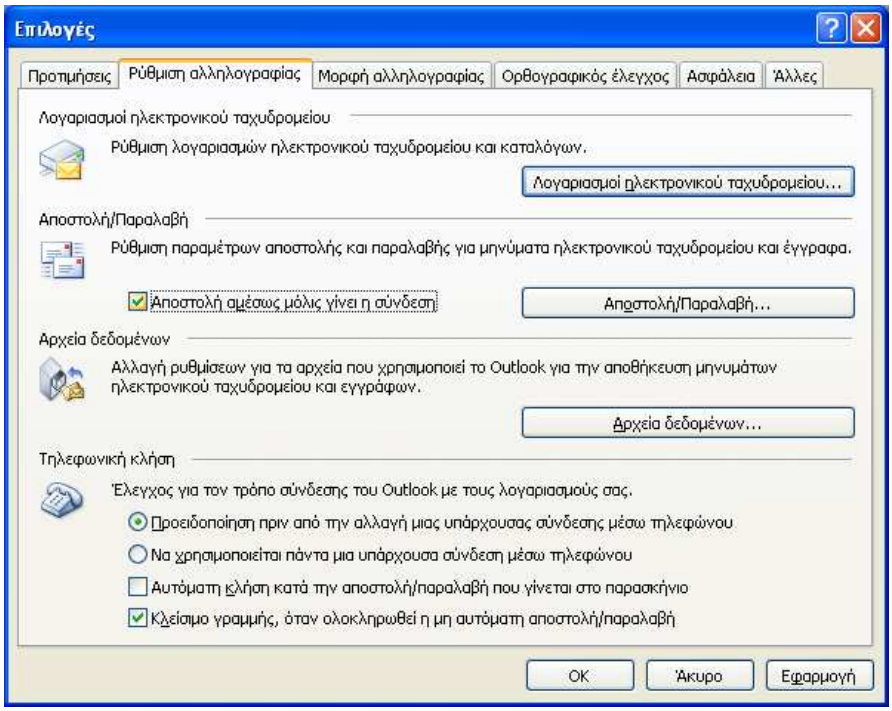
Επιλέξτε την πρώτη επιλογή "Χωρίς αυτόματη λήψη ή άλλου περιεχομένου σε μήνυμα ηλεκτρονικού ταχυδρομείου HTML"



Εικόνα 330: Αυτόματη Λήψη εικόνων

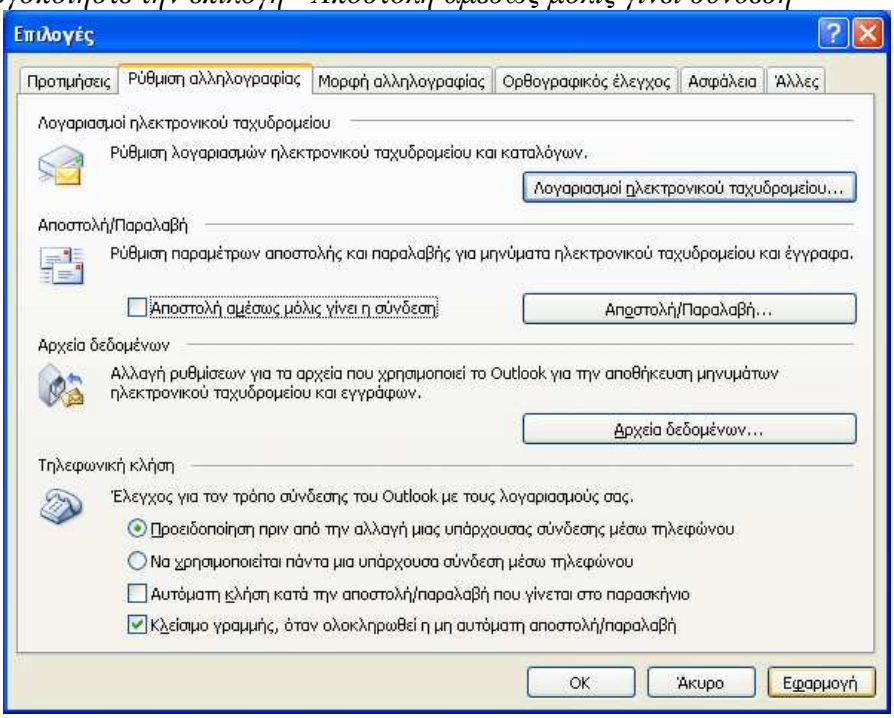
- Απενεργοποίηση του αυτόματου άνοιγμα των e-mail. Το Αυτόματο άνοιγμα μπορεί να προκαλέσει κακόβουλο περιεχόμενο που πρέπει να εκτελεστεί χωρίς τη συμμετοχή του χρήστη.
- Απενεργοποιήστε την αυτόματη αποστολή που επιστρέφουν έσοδα.

Στη καρτέλα εργαλεία και πατήστε "Επιλογές" και μετά Ρύθμιση αλληλογραφίας



Εικόνα 331: Ρύθμιση Αλληλογραφίας

Απενεργοποιήστε την επιλογή "Αποστολή αμέσως μόλις γίνει σύνδεση"



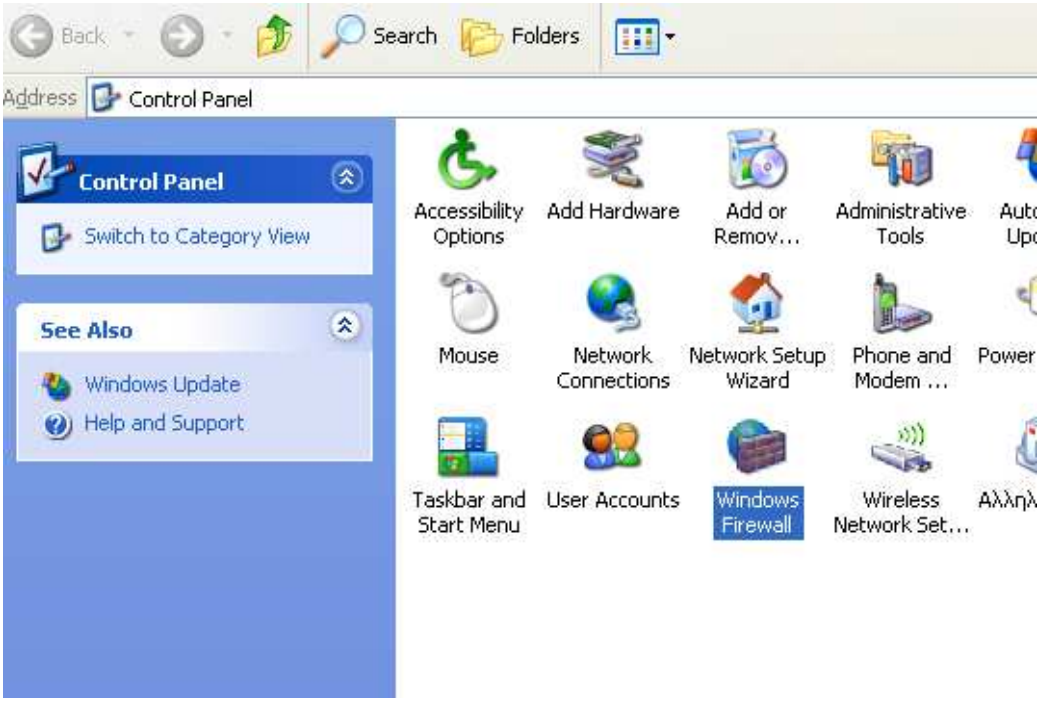
Εικόνα 332: Απενεργοποίηση Αυτόματης Αποστολής

4.4 Personal Firewalls

Τα προσωπικά τείχη προστασίας παρέχουν περιορισμούς στις εισερχόμενες δραστηριότητες του δικτύου (και εννοείται και εξερχόμενη δραστηριότητας) σε επίπεδο υποδοχής. Αρχικά, τα προσωπικά firewalls κυρίως χρησιμοποιούνταν για τους οικοδεσπότες που είχαν άμεση πρόσβαση από το Internet, αλλά όλο ένα και οι οργανισμοί χρησιμοποιούν προσωπικά firewalls σε σχεδόν όλους τους κεντρικούς υπολογιστές για να περιοριστεί η εξάπλωση των worms, μεταξύ και άλλων λόγων. Μερικά προσωπικά firewalls μπορούν επίσης να περιορίσουν ορισμένους τύπους εφαρμογών δραστηριότητας, όπως η παρακολούθηση εισερχόμενων και εξερχόμενων e-mails με σημάδια από κακόβουλο λογισμικό και να απενεργοποιούν προσωρινά τις υπηρεσίες ηλεκτρονικού ταχυδρομείου, εάν η δραστηριότητα αυτή ανιχνευτεί. Μερικά προσωπικά firewalls επίσης παρέχουν πρόσθετη ασφάλεια για προγράμματα περιήγησης ιστού, όπως η πάταξη αναδυόμενων παράθυρων και το χειρισμό ενεργού κώδικα.

Για να ανοίξετε το”Windows Firewall” πηγαίνετε Control Panel πατήστε διπλό κλικ και θα σας εμφανίστε ένα παράθυρο με διάφορα εικονίδια , εκεί βρίσκεται και το”Windows Firewall” . Ανοίξτε το πατώντας διπλό κλικ στο εικονιδίου του.

Εικόνα 333: Control Panel

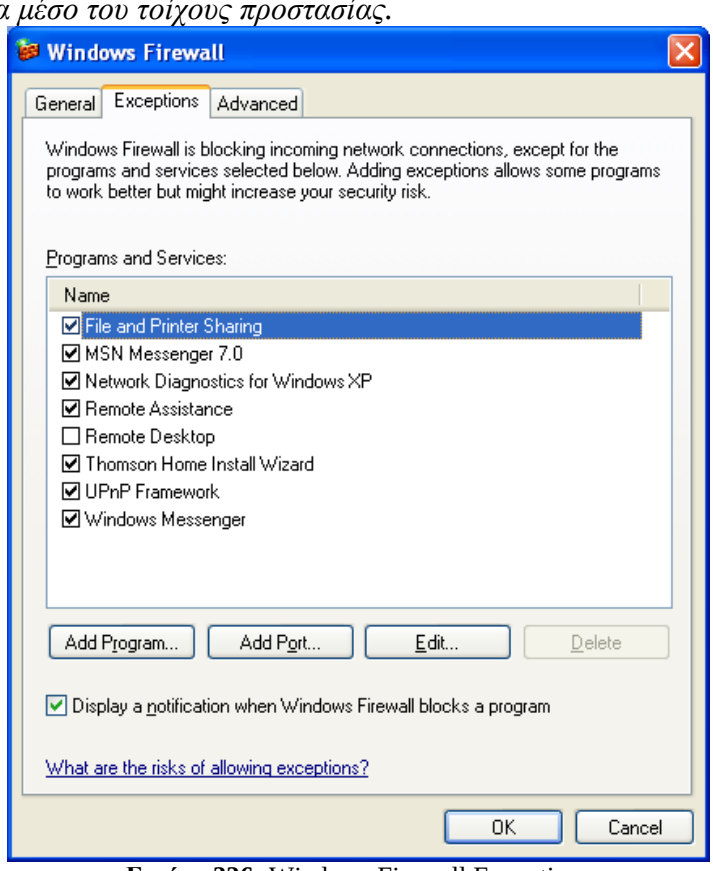


Εικόνα 334: Windows Firewall

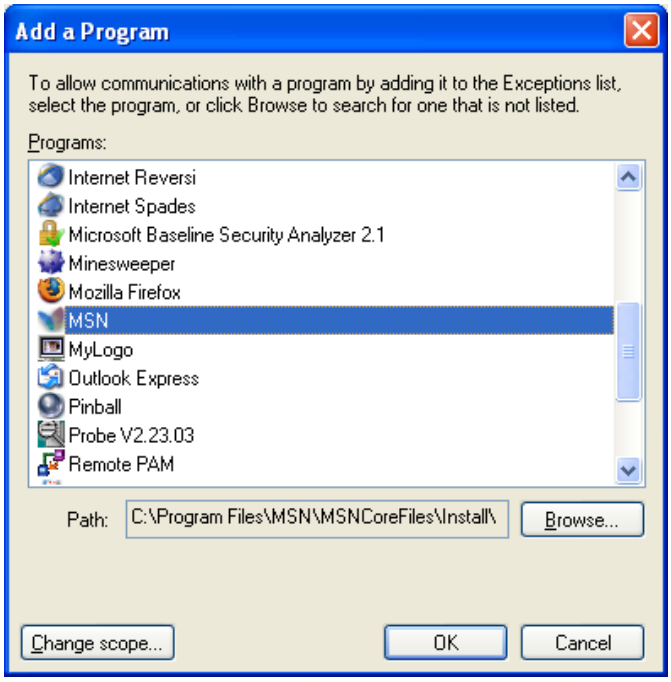
Μόλις ανοίξει θα εμφανιστεί το παρακάτω παράθυρο. Επιλέξτε το πρώτο radio button “On (recommended)”.

Εικόνα 335: Windows Firewall is Helping to Protect your PC

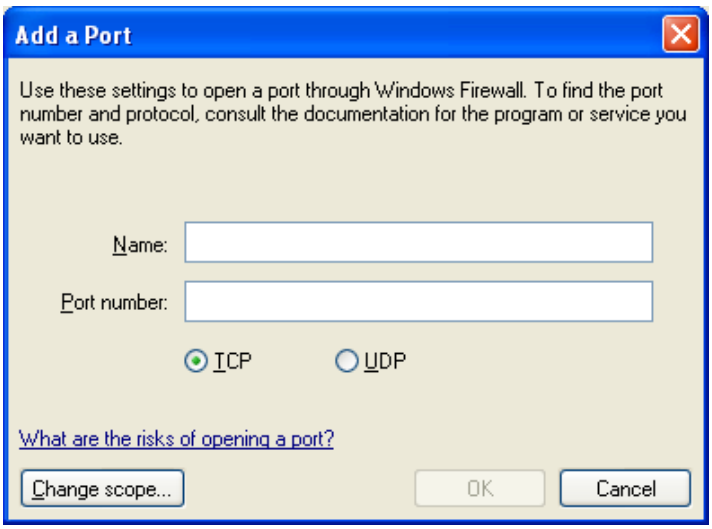
Πατώντας στη καρτέλα Exceptions (εξαιρέσεις), μπορείς να επιλέξεις ή να προσθέσεις ένα πρόγραμμα(add Program..) ή μια θύρα (add Port..) για να τη επικοινωνία μέσο του τοίχους προστασίας. Οι εξαιρέσεις ελέγχουν τον τρόπο με τον οποίο επικοινωνούν τα προγράμματα μέσο του τοίχους προστασίας.



Εικόνα 336: Windows Firewall Exceptions

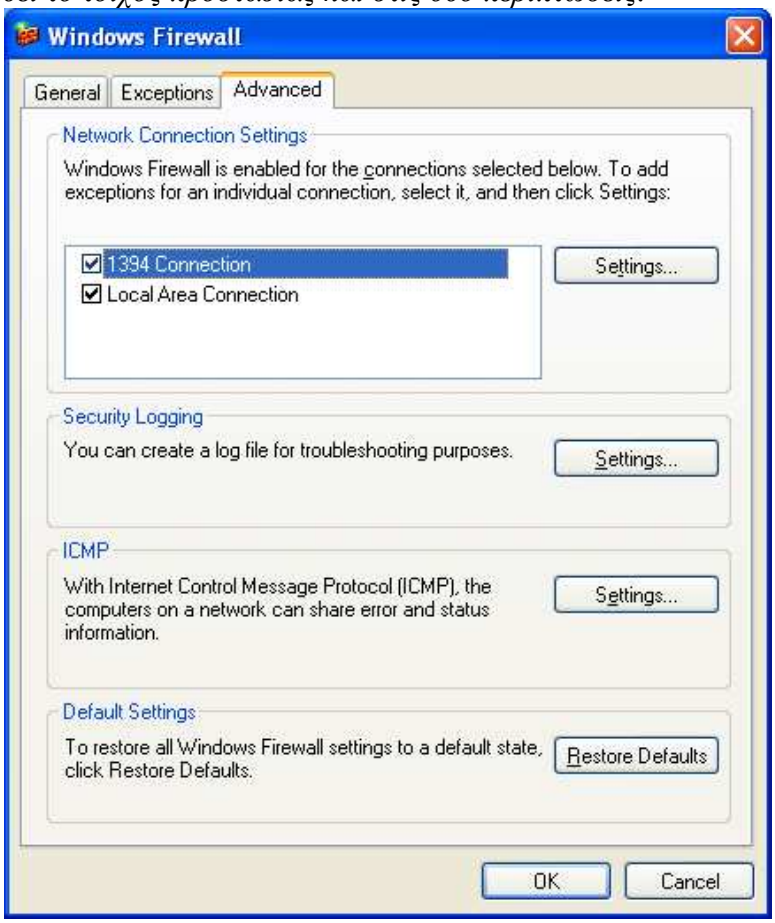


Εικόνα 337: Add a Program



Εικόνα 338: Add a Port

Πηγαίνοντας στη καρτέλα Advanced(για προχωρημένους) υπάρχουν ρυθμίσεις πιο εξεζητημένες. Μια σημαντική ρύθμιση που πρέπει να έχετε κάνει αν χρησιμοποιείται ασύρματη σύνδεση ή τοπική ρύθμιση είναι να έχετε επιλέξει και τις δύο επιλογές για να σας προστατεύει το τοίχος προστασίας και στις δύο περιπτώσεις.



Εικόνα 339: Windows Firewall Advanced

Λόγω των ικανοτήτων των προσωπικών firewalls είναι τόσο ποικίλα, έτσι ώστε οι οργανισμοί θα πρέπει να εξετάζουν προσεκτικά κάθε προϊόν, κατά τον καθορισμό των ικανοτήτων του, με τη ρύθμιση αυτή. Πρόσθετες πληροφορίες για τα προσωπικά τοίχοι προστασίας είναι διαθέσιμα από τη NIST SP 800-41 Αναθεώρηση 1 (Σχέδιο), Οδηγός για Firewalls και Firewall Policy.[68] Επίσης, το τμήμα 7.6 του παρούσας δημοσίευσης περιγράφει το Windows Firewall, ένα προσωπικό τείχος προστασίας που παρέχεται με τα Windows XP Professional.

4.5 Antivirus Software

Το λογισμικό αντιμετώπισης ιών είναι ένα ουσιαστικό στοιχείο στη διασφάλιση των συστημάτων Windows XP, αλλά δεν μπορεί να παράσχει πλήρη προστασία έναντι όλων των malware. Οι καλές πρακτικές υπολογιστών θα πρέπει να ακολουθηθούν, ακόμη και όταν είναι εγκατεστημένο το λογισμικό εντοπισμού ιών, στη δυνατότητα και την πλήρη ενημέρωση. Παραδείγματα ορθής πρακτικής δεν είναι το απροσδόκητο άνοιγμα συνημμένων αρχείων και η διαμόρφωση εφαρμογών να μην εκτελεστούν μακροεντολές ή ενσωματωμένα ετικέτες HTML από προεπιλογή. Το τμήμα 7.1.2 παρέχει κατευθύνσεις για τη χαρτογράφηση των ενεργών περιεχόμενων επεκτάσεις αρχείων, έτσι ώστε τα αρχεία να μην εκτελούνται αυτόματα από προεπιλογή. Οι καλές πρακτικές επίσης συμβάλουν στην προστασία από το παράθυρο στο μικρό χρονικό διάστημα μεταξύ της απελευθέρωσης ενός νέου ιού και στη διαθεσιμότητα της υπογραφής ενημερωμένων ιών.[69]

Μερικά από τα πιο γνωστά λογισμικά αντιμετώπισης ιών είναι:

1. *BitDefender Antivirus 2009*
2. *Norton AntiVirus 2009*
3. *Panda Antivirus Pro 2009*
4. *Kaspersky Antivirus 2009*
5. *F-Secure Internet Security 2009*

Παρόλο που υπάρχουν πολλές διαθέσιμες μάρκες αντιμετώπισης λογισμικού, προσφέρουν παρόμοια λειτουργικότητα.

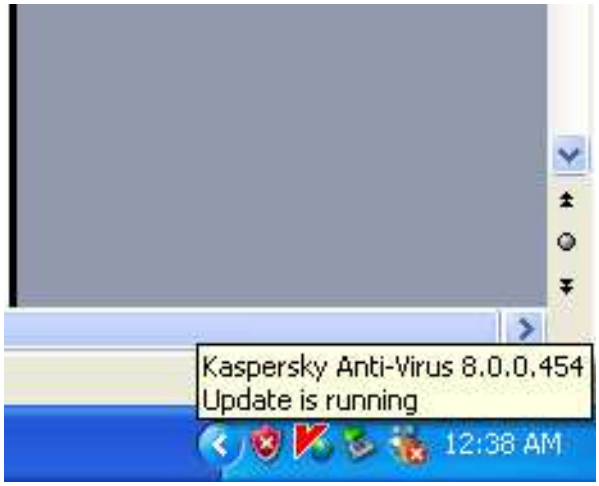
Εγκαταστήσαμε το Kaspersky Antivirus 2009 για να σας δείξουμε μερικές από τις λειτουργίες των λογισμικών αντιμετώπισης ιών. Περίπου όλα τα λογισμικά δουλεύουν με τον ίδιο τρόπο.

- Σάρωμα κρίσιμων μερών του συστήματος, όπως τα αρχεία εκκίνησης, το σύστημα BIOS, και τα αρχεία εκκίνησης

[68] http://csrc.nist.gov/publications/PubsDrafts.html

[69] Για περισσότερες πληροφορίες σχετικά με το λογισμικό εντοπισμού ιών και κακόβουλου λογισμικού, βλ. NIST SP 800-83, Guide to Malware Incident πρόληψη και τον χειρισμό, που διατίθεται στη http://csrc.nist.gov/publications/PubsSPs.html.

Μόλις εγκατασταθεί το πρόγραμμα εμφανίζεται κάτω δεξιά στη οθόνη μας. Πάνω στο εικονίδιο πατήστε δεξί κλικ και πατήστε στο όνομα του λογισμικού.



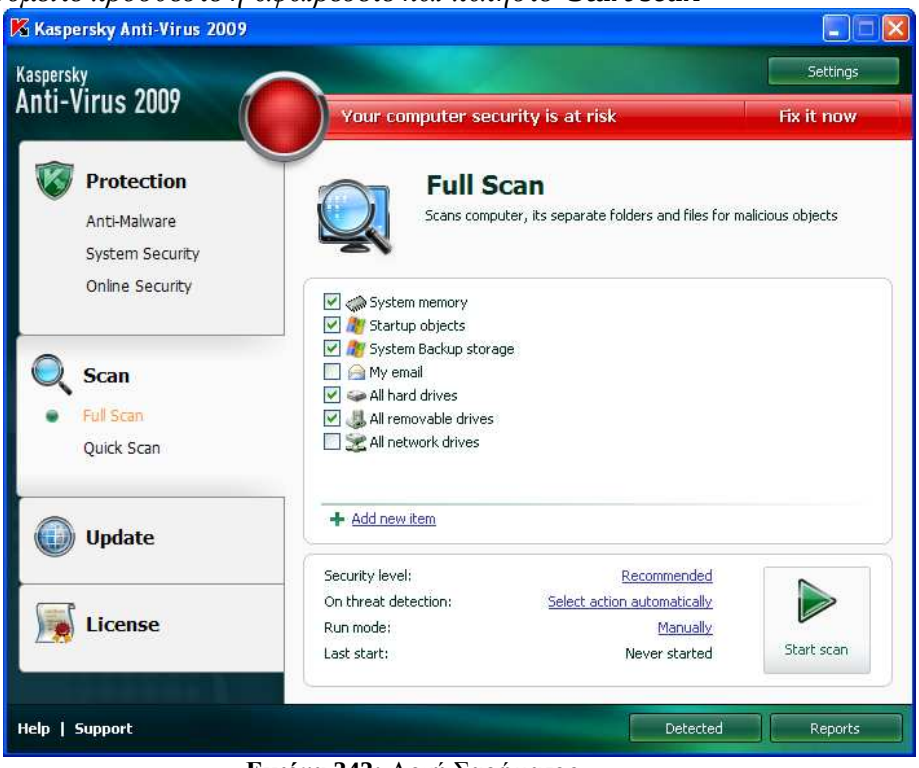
Εικόνα 340: Εμφάνιση του Anti-Virus

Εικόνα 341: Εμφάνιση του Προγράμματος

Θα σας εμφανιστεί το πρόγραμμα. Για σάρωση των κρίσιμων αρχείων πατήστε ***Scan*** *και μετά full scan*

Εικόνα 342: Λογισμικό Αντιμετώπισης Ιών

Έχει ήδη προεπιλεγμένα αρχεία και φακέλους που πρέπει να σαρωθούν, αν επιθυμείτε προσθέστε ή αφαιρέσετε και πατήστε ***Start scan***

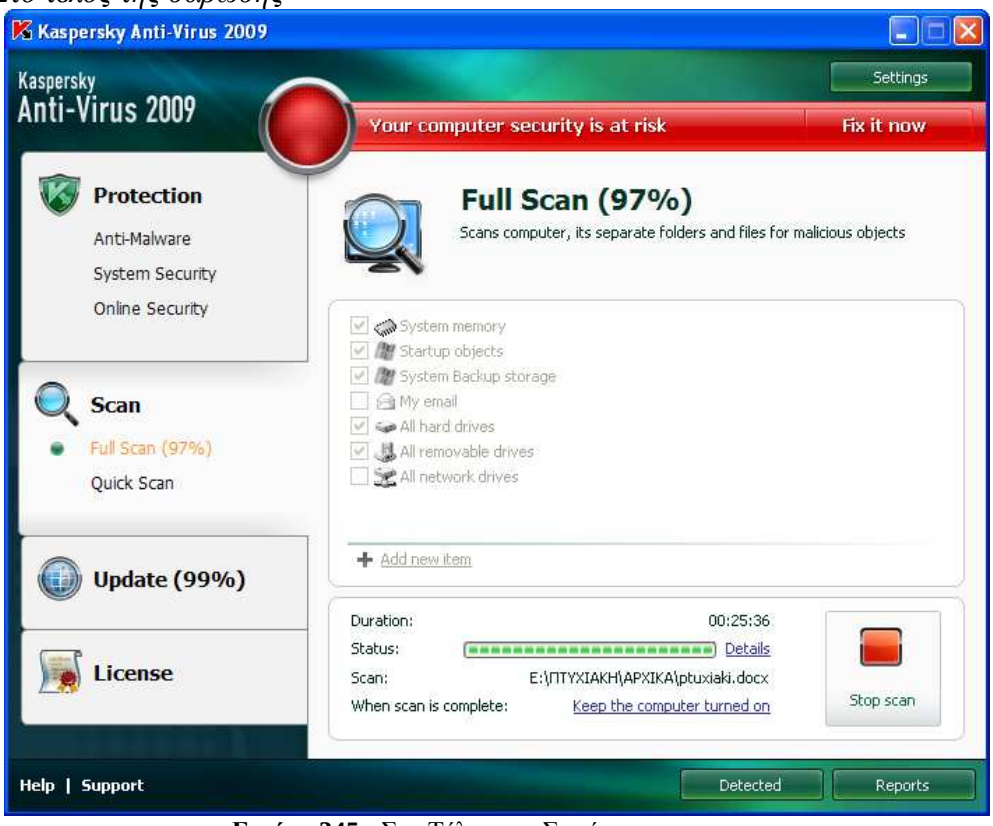


Εικόνα 343: Αρχή Σαρώματος

Κατά τη διάρκεια του σαρώματος

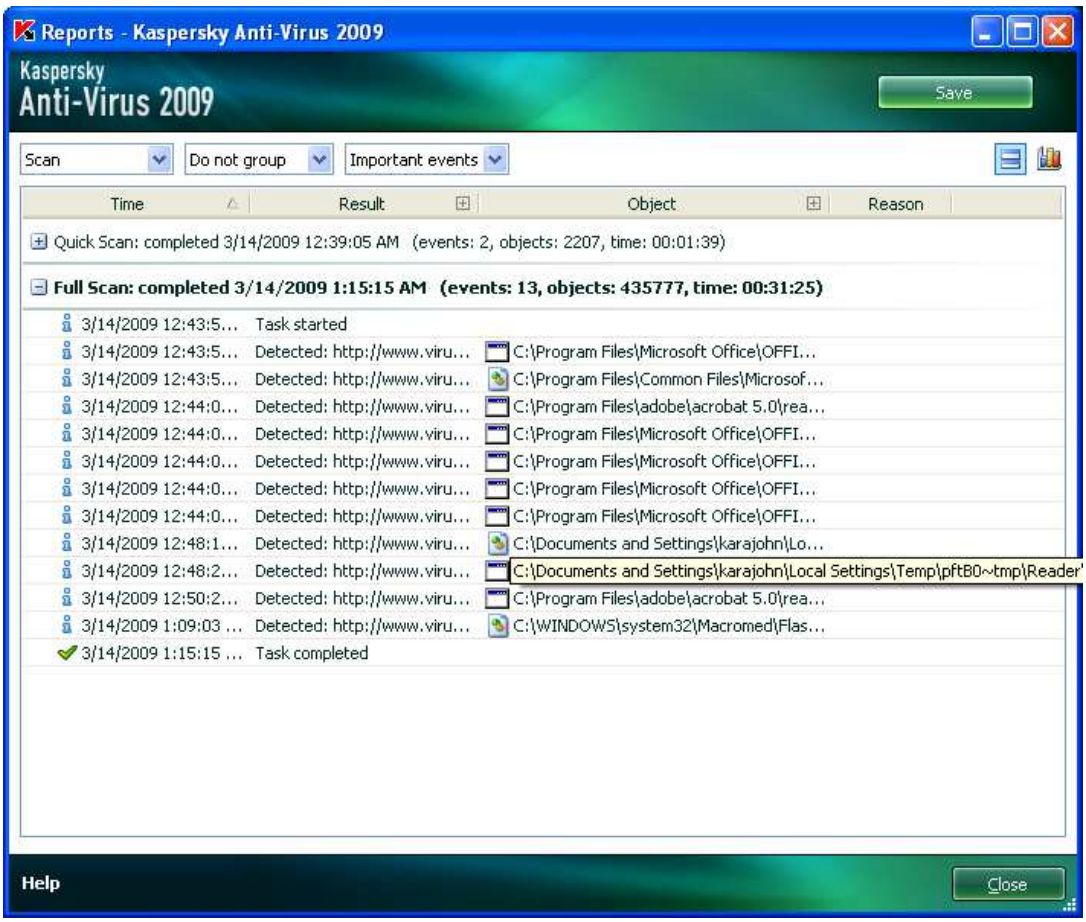
Εικόνα 344: Κατά τη Διάρκεια του Σαρώματος

Στο τέλος της σάρωσης



Εικόνα 345: Στο Τέλος του Σαρώματος

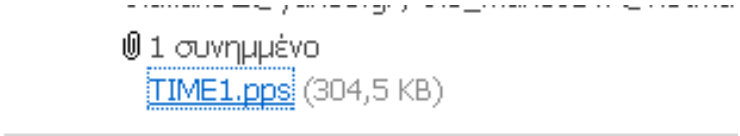
Μόλις τελειώσει η σάρωση πατήστε "Reports" για να μας εμφανίσει τι βρήκε.



Εικόνα 346: Αποτέλεσμα της Σάρωσης

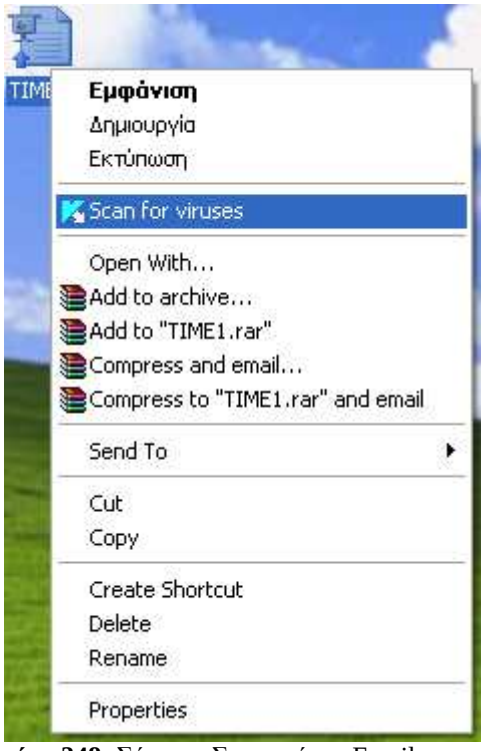
- Παρατηρώντας το σε πραγματικό χρόνο τις δραστηριότητες του υπολογιστή και του λειτουργικού συστήματος για να ελέγξετε για ύποπτη δραστηριότητα? Ένα καλό παράδειγμα είναι η σάρωση όλων συνημμένων του ηλεκτρονικού ταχυδρομείου, γνωστό για τους ιούς, όπως ηλεκτρονικά μηνύματα που αποστέλλονται και λαμβάνονται

Για παράδειγμα έρχεται στο email μας ένα email με συνημμένο μήνυμα από άγνωστο ή γνωστό μας,



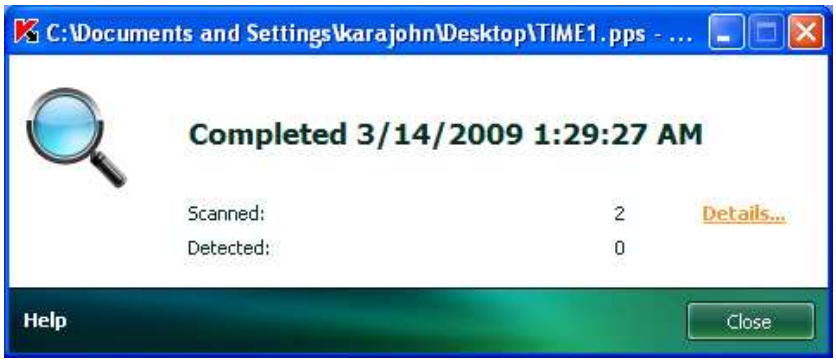
Εικόνα 347: Συνημμένο Email

Για ελέγξουμε αν έχει ιό ή όχι μόλις κατεβάσουμε το αρχείο και πριν το ανοίξουμε πατήστε δεξί κλικ και "Scan for viruses"



Εικόνα 348: Σάρωμα Συνημμένου Email

Το λογισμικό θα το ελέγξει και θα σου εμφανίσει αν έχει ιό η όχι.



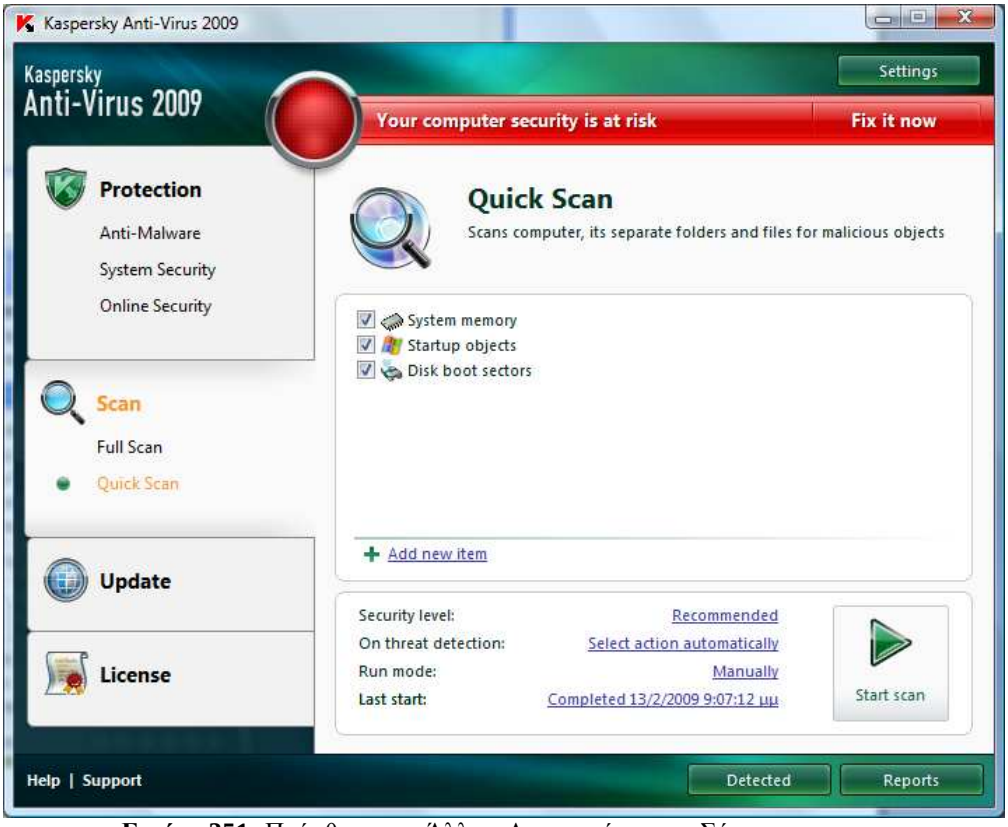
Εικόνα 349: Αποτέλεσμα Σαρώματος

- σάρωση όλων των αρχείων σε έναν σκληρό δίσκο για γνωστούς ιούς. Το NIST συνιστά το antivirus λογισμικού σε συστήματα των Windows XP να ρυθμιστεί για να ανίχνευση όλων των σκληρών δίσκων τακτικά για να εντοπίζει τυχόν μολυσμένα σύστημα αρχείων.

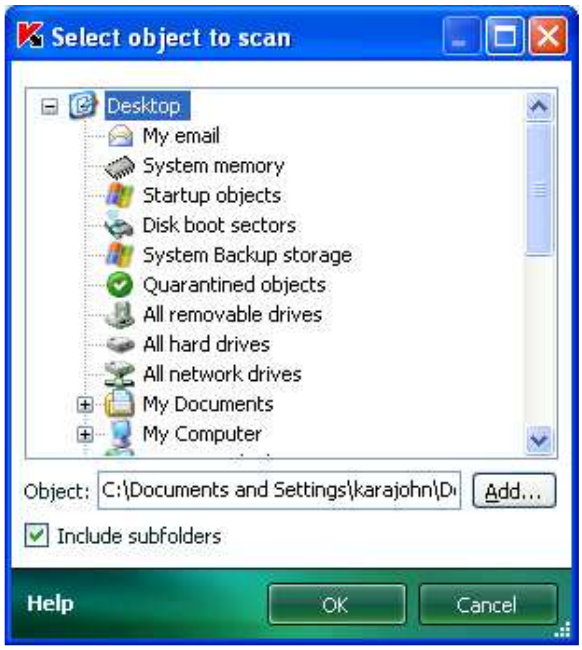
*Διαλέξτε από το **Scan " Quick Scan "** στο κεντρικό μενού του λογισμικού*

Εικόνα 350: Γρήγορο Σάρωμα

Για να προσθέσετε τους σκληρούς σας δίσκους πατήστε "+ Add new Item"

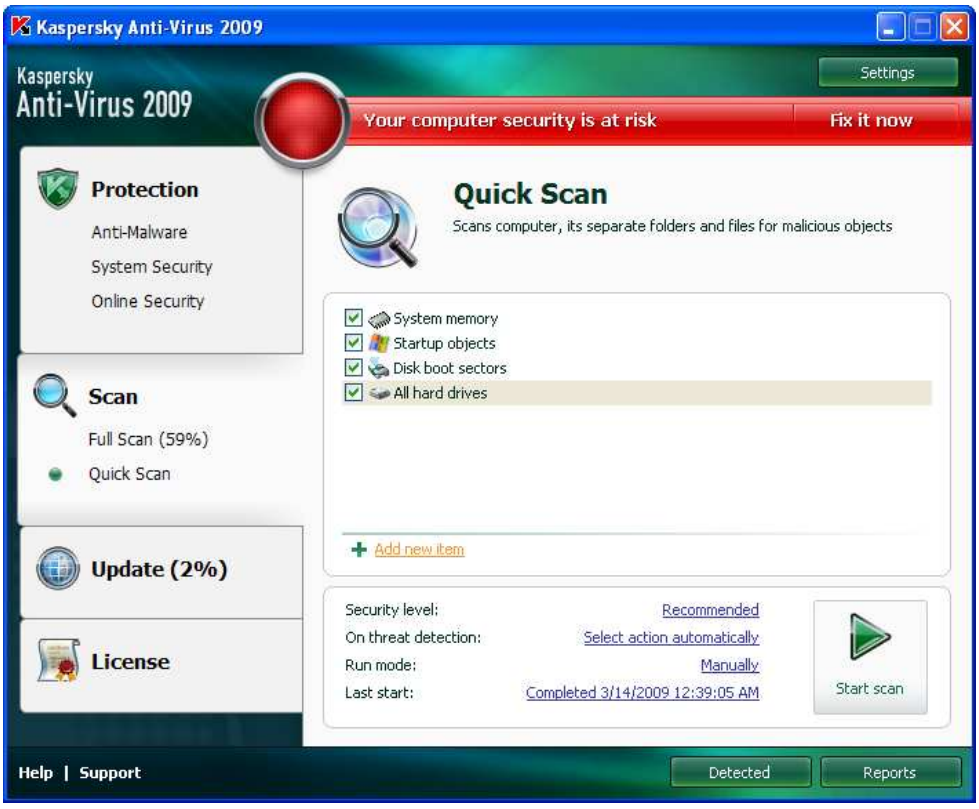


Εικόνα 351: Πρόσθεση και Άλλων Αντικειμένων για Σάρωση



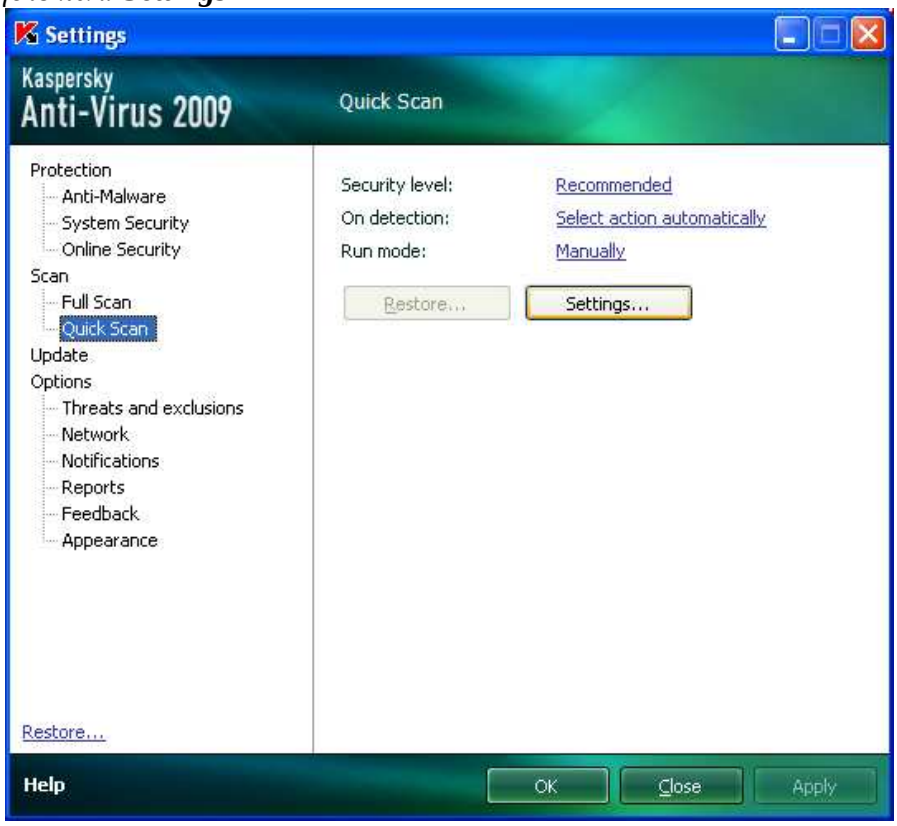
Εικόνα 352: Επιλογή Αντικειμένου για Σάρωση

Έτσι προσθέσατε τους σκληρούς σας δίσκους. Τώρα πατήστε ***Settings*** *όπου βρίσκετε πάνω δεξιά στο μενού του λογισμικού για να ρυθμίσετε το λογισμικό σας να κάνει σάρωση ανά τακτικά διαστήματα.*



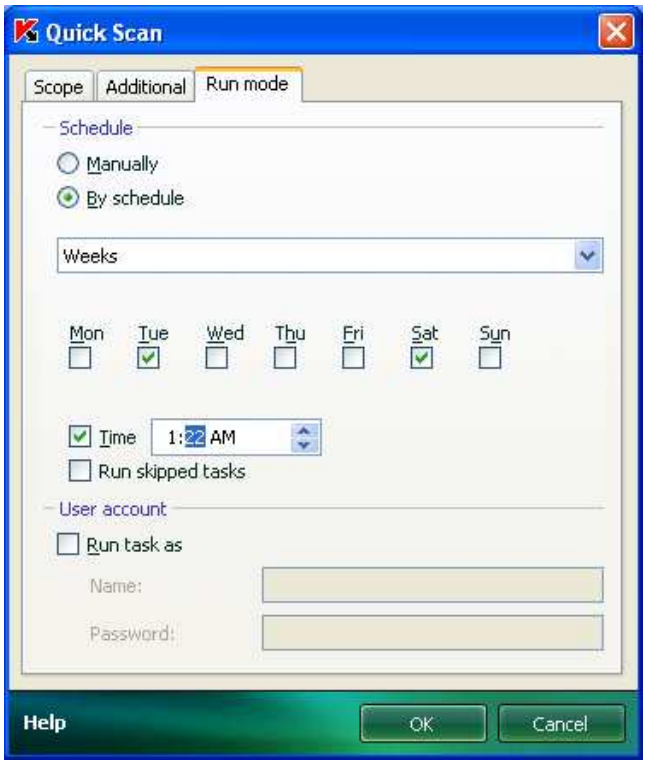
Εικόνα 353: Settings Anti-Virus

Πατήστε πάλι ***Settings***



Εικόνα 354: Settings Scan

Πατήστε τώρα By schedule για να ρυθμίσετε κάθε πότε θέλετε να κάνετε σάρωση



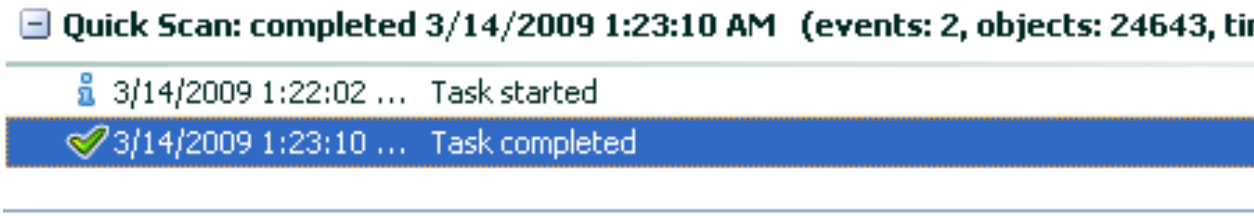
Εικόνα 355: Quick Scan "By Schedule"

Ρυθμίζετε ανά πότε θέλετε να κάνετε τη σάρωση. Για παράδειγμα παραπάνω ρυθμίσαμε να κάνει σάρωση 2 φορές τη βδομάδα(Τρίτη και Σάββατο) και ώρα 1 και 22 λεπτά μετά μεσημβρίας.

Όντως ακριβώς 1 και 22 λεπτά το Σάββατο άρχισε να σαρώνει αυτόματα.

Εικόνα 356: Γρήγορη Σάρωση Με ρύθμισης Ώρας και Ημερομηνίας

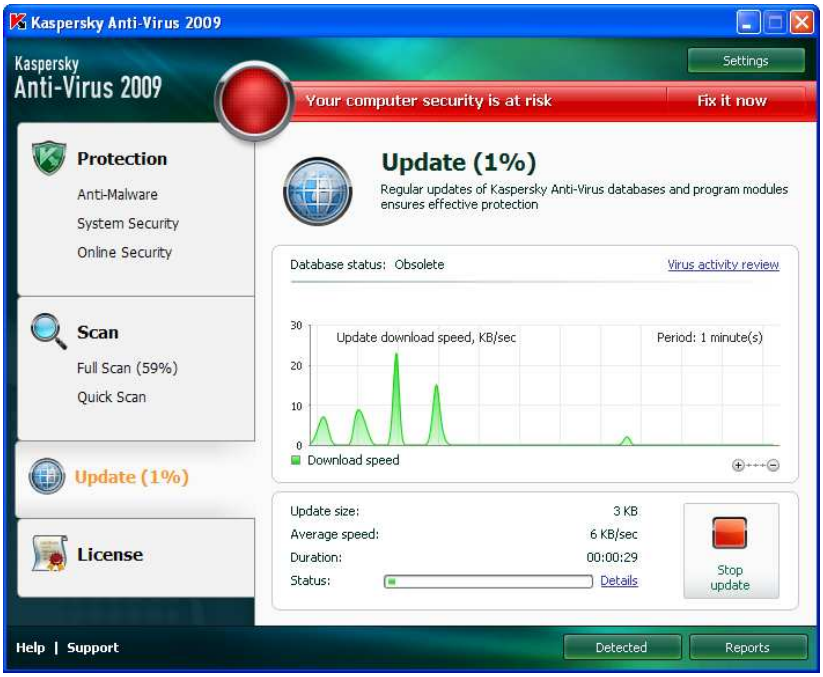
Μόλις τέλειωσε το σάρωμα πατώντας το Reports μας έβγαλε αν βρήκε κάτι..



Εικόνα 357: Αποτέλεσμα Γρήγορης Σάρωσης Με ρύθμισης Ώρας και Ημερομηνίας

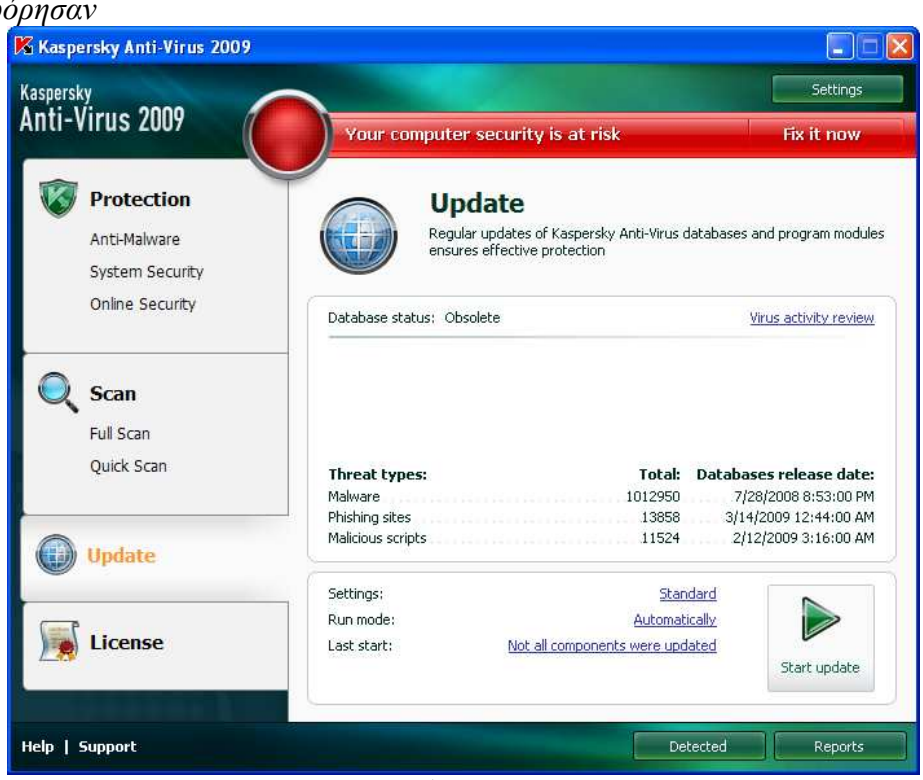
- Αυτόματη λήψη και εγκατάσταση ενημερωμένων εκδόσεων από την τοποθεσία Web του προμηθευτή (ή ένα τοπικό διακομιστή σε ένα περιβάλλον που να τα διαχειρίζεται) ημερησίως.

*Πατώντας από το κεντρικό μενού **Update** κατεβάζετε αυτόματα τις ενημερώσεις και πατήστε Start update. Παρακάτω βλέπετε ένα παράθυρο κατά τη διάρκεια της λήψης ενημερώσεων.*



Εικόνα 358: Screenshot

Μόλις τελειώσει η λήψη μας εμφανίζει τις βάσεις δεδομένων με τις ημερομηνίες που κυκλοφόρησαν



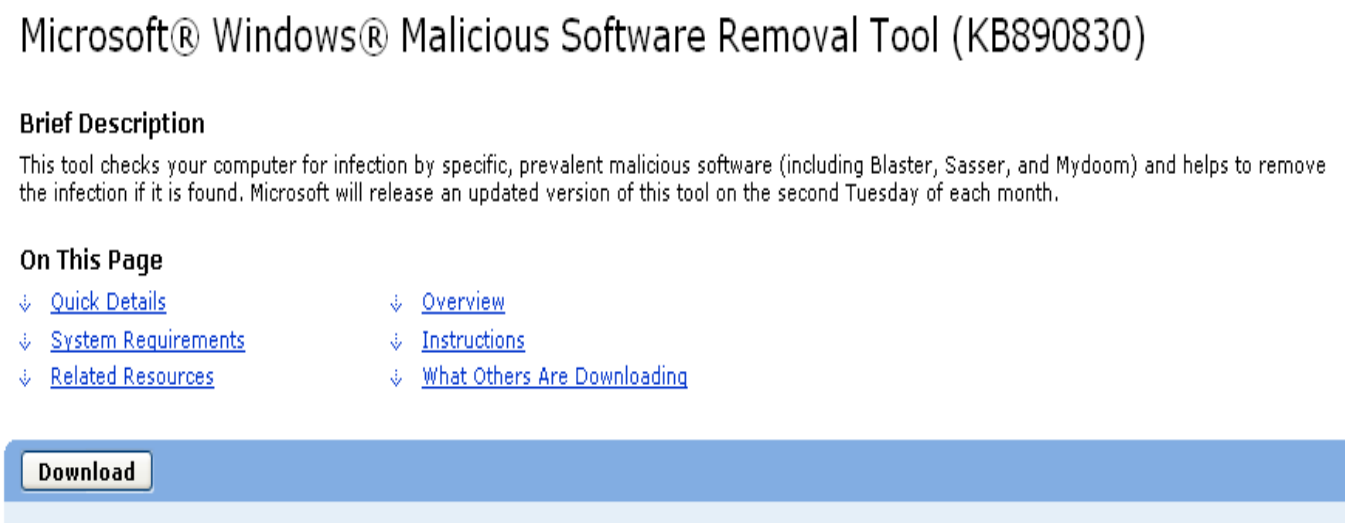
Εικόνα 359: Λήψη Ενημερώσεων

Κάθε μία από αυτές τις λειτουργίες, είναι σημαντικές και δεν πρέπει ούτε να αγνοηθεί αλλά ούτε να απενεργοποιηθεί αν δεν είναι απαραίτητο. Παρά το γεγονός ότι ο εγγενής κίνδυνος πίσω από την τεχνολογία ανίχνευσης ιών, που είναι γνωστό κυρίως ως intercepts ιών, αυτό δεν μειώνει τη σημασία του λογισμικού. Το NIST συνιστά με

έμφαση ότι κάθε σύστημα των Windows XP χρησιμοποιεί ρυθμισμένα σωστά και διατηρημένα το λογισμικό αντιμετώπισης ιών. Το λογισμικό αντιμετώπισης ιών θα πρέπει να εγκατασταθεί αμέσως μετά την αρχική εγκατάσταση των Windows XP και στη συνέχεια, θα πρέπει να ενημερώνεται με τις νεότερες υπογραφές και patches αντιμετώπισης λογισμικού . Το λογισμικό αντιμετώπισης ιών θα πρέπει στη συνέχεια, εκτελεί πλήρη σάρωση του συστήματος για τον εντοπισμό τυχόν μολύνσεων.

Η Microsoft προσφέρει επίσης ένα βοηθητικό πρόγραμμα που ονομάζεται Windows Malicious Software Removal Tool. Κατά τους ελέγχους της και προσπαθεί να άρει ορισμένες κοινές απειλές κακόβουλου λογισμικού, όπως τα worms και τα rootkits. Το εργαλείο μπορεί να εγκατασταθεί σε συστήματα αυτόματα μέσω των Αυτόματων ενημερώσεων ή από το Microsoft Update, ή μπορεί να γίνει λήψη ή να εκτελεστεί άμεσα από το Microsoft Web του site.[70] Επειδή το εργαλείο έχει σχεδιαστεί για να ανιχνεύει μόνο ένα μικρό αριθμό κοινών απειλών, είναι ένα συμπλήρωμα για το λογισμικό αντιμετώπισης ιών, δεν το αντικαθιστά.

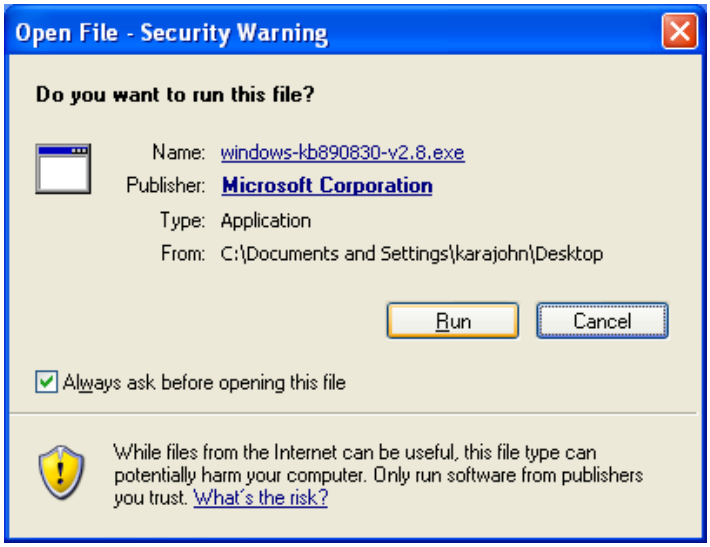
Στη σελίδα της Microsoft βρίσκετε το Windows Malicious Software Removal Tool όπου μπορείτε να κάνετε λήψη.



Εικόνα 360: Windows Malicious Software Removal Tool

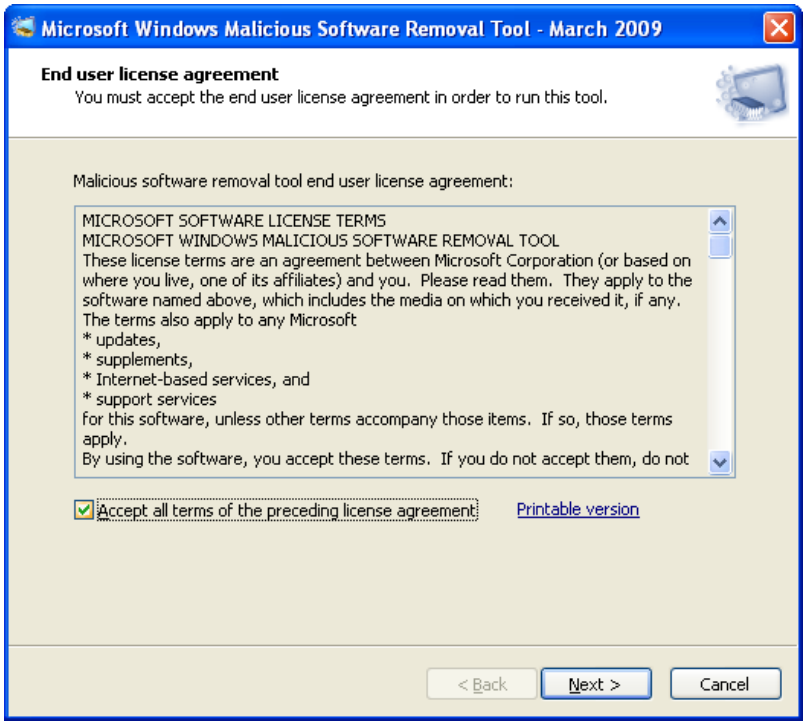
Εγκαταστήστε το πρόγραμμα

[70] Το εργαλείο είναι διαθέσιμο σε http://www.microsoft.com/security/malwareremove/default.mspx. Πρόσθετες πληροφορίες είναι διαθέσιμες από MSKB άρθρο 890830, που διατίθεται στη http://support.microsoft.com/?id=890830.



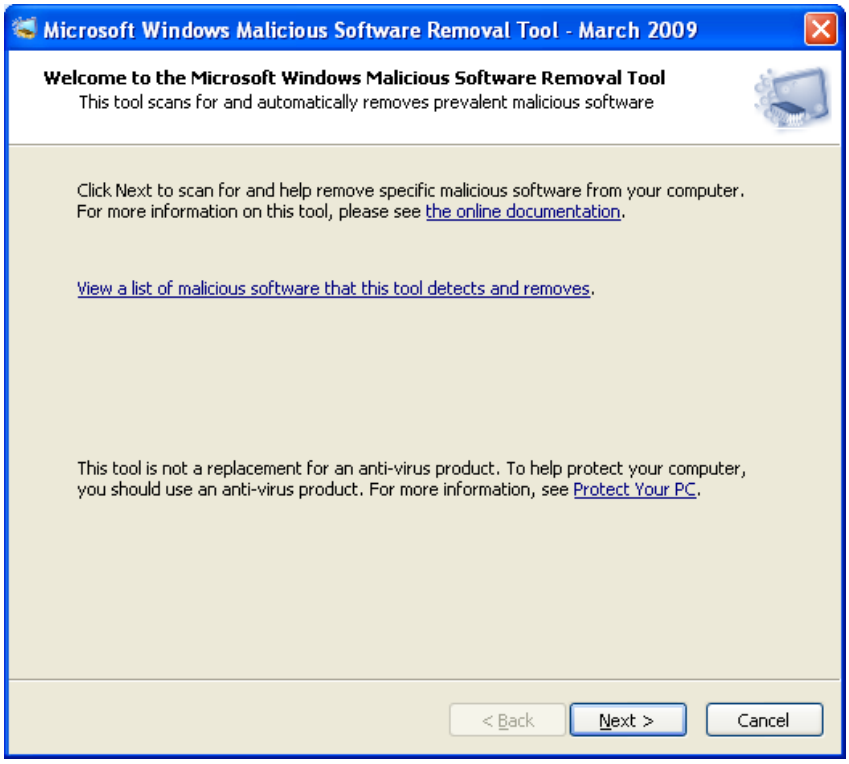
Εικόνα 361: Εγκατάσταση Προγράμματος

δεχτείτε του όρους για τη εγκατάσταση του



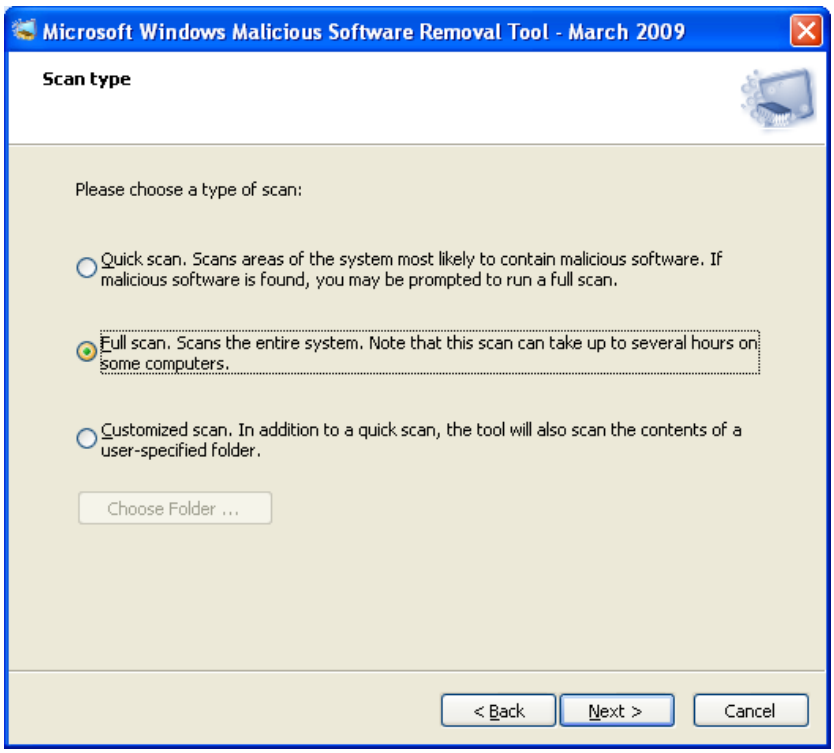
Εικόνα 362: Αποδοχή Όρων του Windows Malicious Software Removal Tool

Πατήστε Next



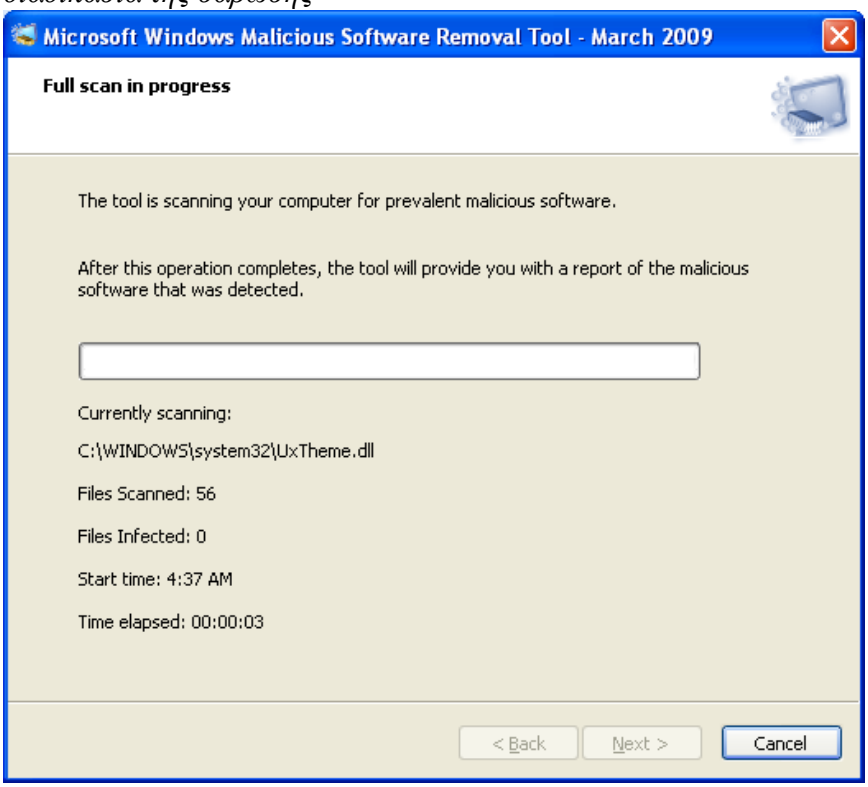
Εικόνα 363: Άνοιγμα Προγράμματος

Και διαλέξτε το σάρωμα που θέλετε να κάνετε. Η καλύτερη επιλογή είναι ***Full scan*** *και πατήστε Next*



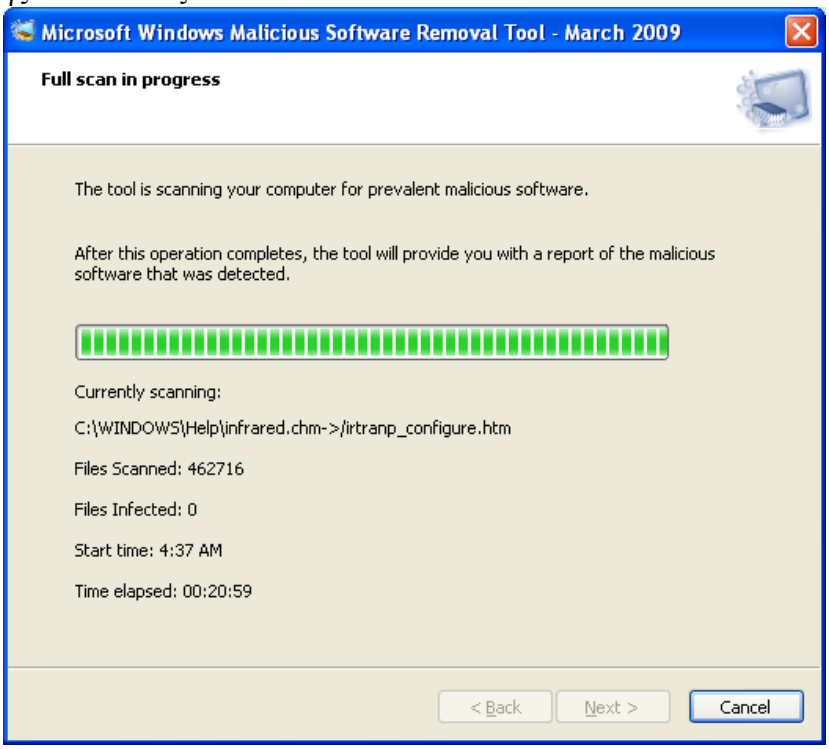
Εικόνα 364: Πλήρες Σάρωση

Αρχίζει η διαδικασία της σάρωσης



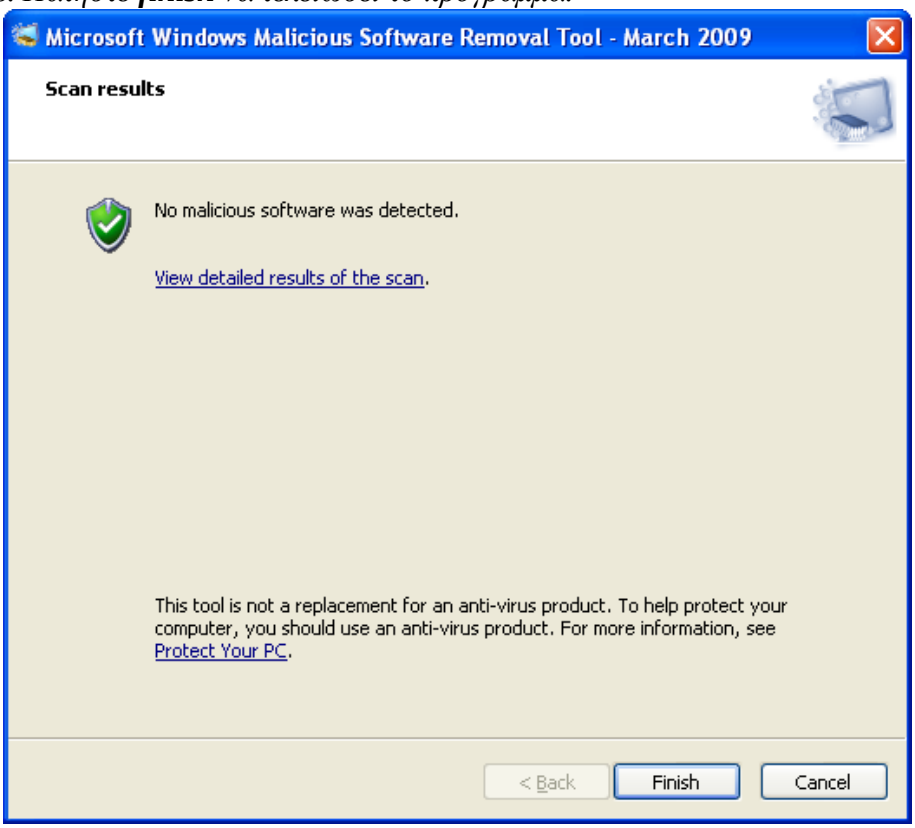
Εικόνα 365: Αρχή Διαδικασίας Σάρωσης

Στο τέλος της διαδικασίας



Εικόνα 366: Τέλος Διαδικασίας Σάρωσης

Μόλις τελειώσει διαδικασία σου εμφανίζει αν βρέθηκε τίποτα. Στη περίπτωση μας δε βρέθηκε. Πατήστε ***finish*** *να τελειώσει το πρόγραμμα.*



Εικόνα 367: Αποτελέσματα Σάρωσης

4.6 Antispyware Software

Το Spyware αναφέρεται σε λογισμικό που συνθέτει τη συλλογή πληροφοριών και τη χρήση συνδετικότητας χωρίς τη γνώση του χρήστη, συνήθως για την παρακολούθηση στη συμπεριφορά των χρηστών (π.χ., ιστοσελίδες που επισκέφθηκε) και τα αναφέρει σε μια κεντρική τοποθεσία. Παραδείγματα spyware περιλαμβάνουν αυτόνομο πρόγραμμα που εγκαθίσταται στο σύστημα ενός χρήστη και ενός cookie εντοπισμού που τοποθετείται στο πρόγραμμα περιήγησης στο Web. Το Spyware δεν παραβιάζει μόνο την ιδιωτική ζωή των χρηστών, αλλά μπορεί επίσης να προκαλέσει προβλήματα σε λειτουργικά συστήματα, όπως επιβράδυνση στις επιδόσεις ή σε εφαρμογές που προκαλούν αστάθεια. Το Antispyware λογισμικό έχει δημιουργηθεί για να εντοπίσει πολλά είδη spyware και για τα συστήματα απομόνωσης ή αφαίρεσης spyware αρχείων. Πολλά προγράμματα λογισμικού εντοπισμού ιών προσφέρουν ορισμένες δυνατότητες και antispyware.

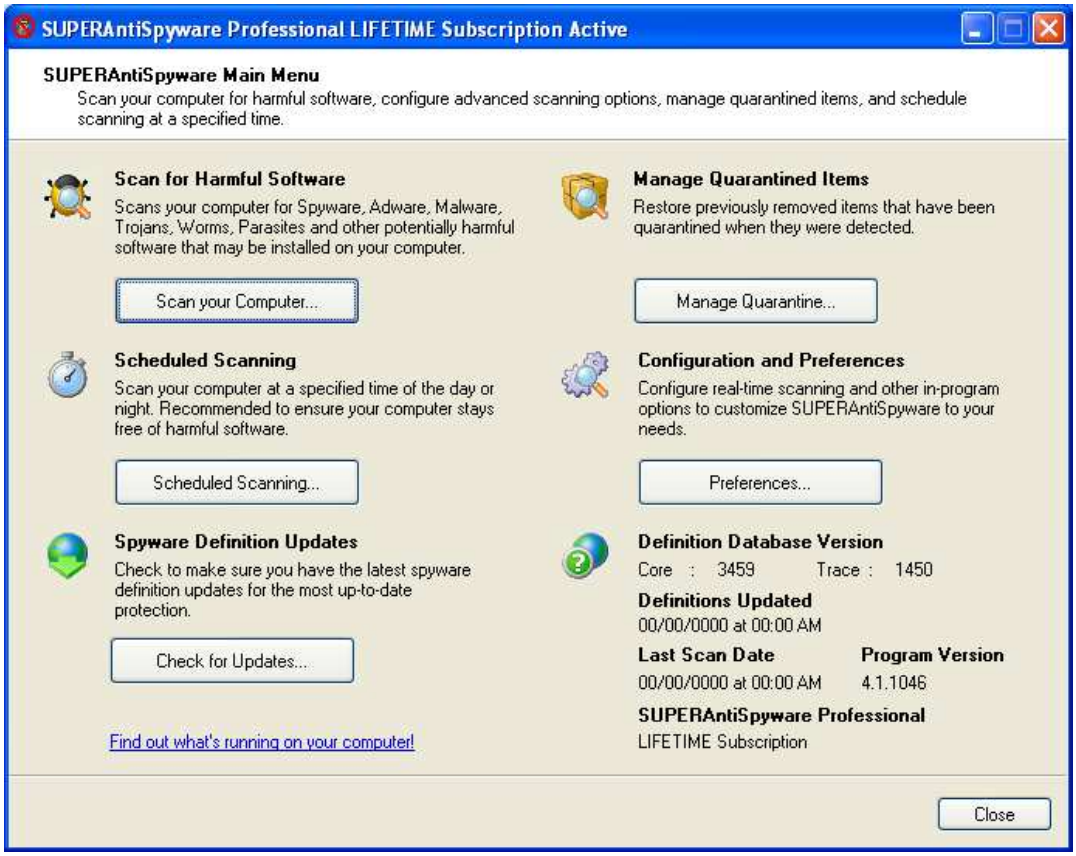
Το NIST συνιστά ότι κάθε σύστημα των Windows XP πρέπει να χρησιμοποιεί είτε antispyware λογισμικό είτε λογισμικό αντιμετώπισης ιών με ισχυρές δυνατότητες antispyware . Το λογισμικό θα πρέπει να εγκατασταθεί αμέσως μετά την εγκατάσταση των Windows XP και στη συνέχεια να ενημερωθεί με τις νεότερα υπογραφές και άλλες ενημερωμένες εκδόσεις. Το λογισμικό θα πρέπει στη συνέχεια, να εκτελέσει πλήρη σάρωση του συστήματος για τον εντοπισμό τυχόν μολύνσεων. Το

λογισμικό θα πρέπει επίσης να ρυθμιστεί για αυτόματη λήψη και εγκατάσταση ενημερωμένων εκδόσεων καθημερινά.

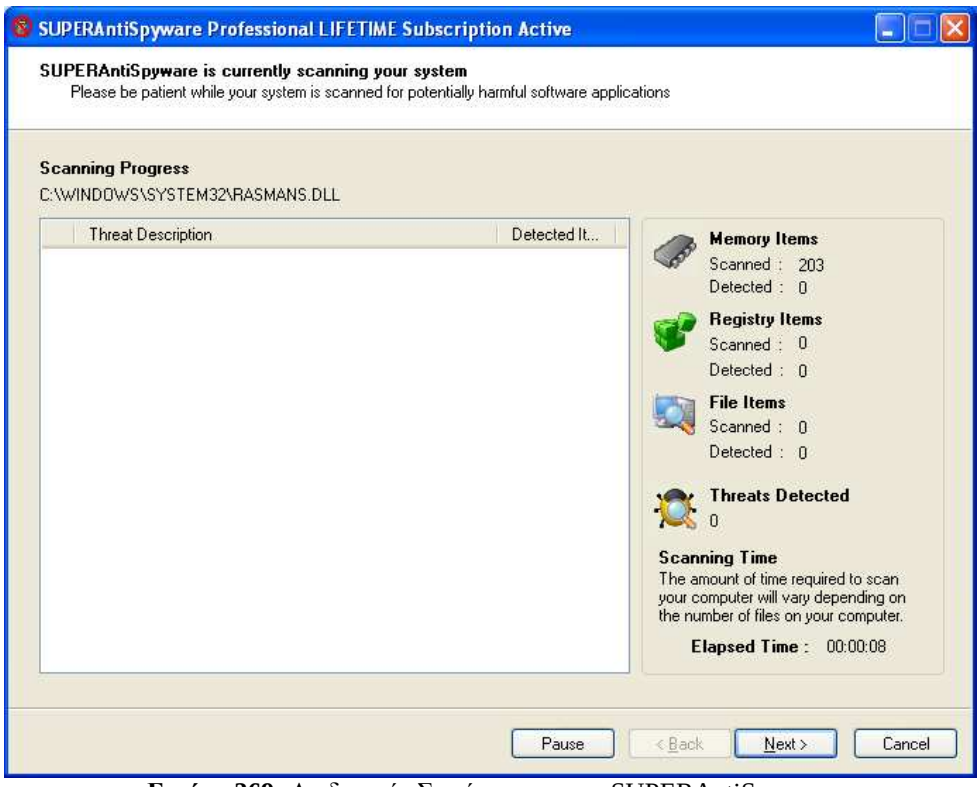
Παρότι το λογισμικό αντιμετώπισης ιών μας έχει δυνατότητες Antispyware , εγκαταστήσαμε και ένα λογισμικό Spyware για περισσότερη ασφάλεια.

Το λογισμικό που εγκαταστήσαμε είναι το SUPERAntiSpyware ένα από τα πολλά που κυκλοφορούν στη αγορά.

Από το μενού του λογισμικού, πατήστε "Scan your Computer" για να κάνουμε σάρωση να δούμε αν έχουμε κανένα επιβλαβές λογισμικό .

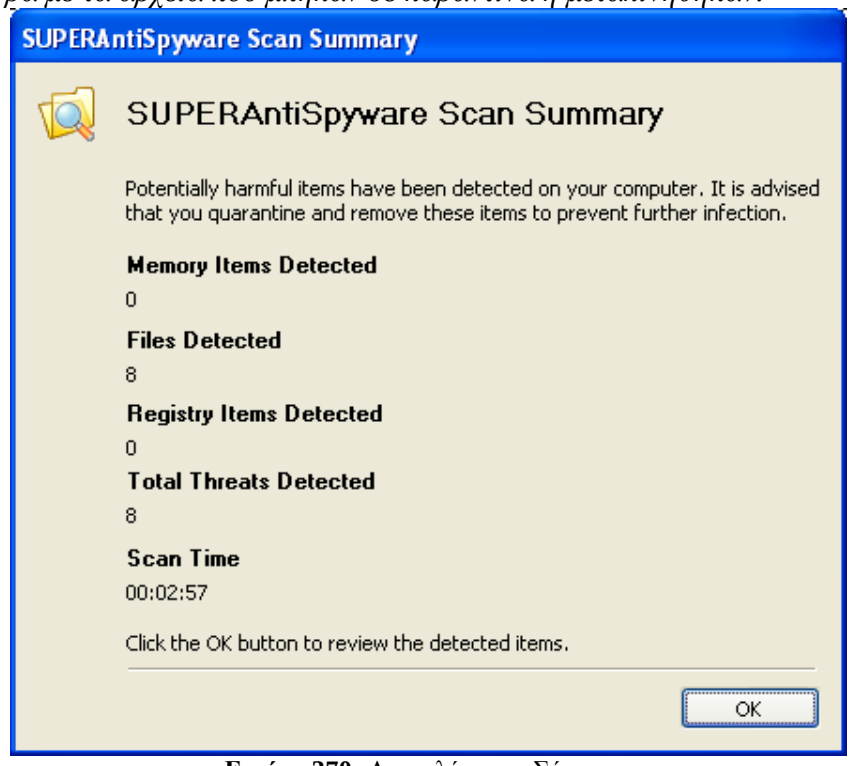


Εικόνα 368: Σάρωση του Υπολογιστή με το SUPERAntiSpyware



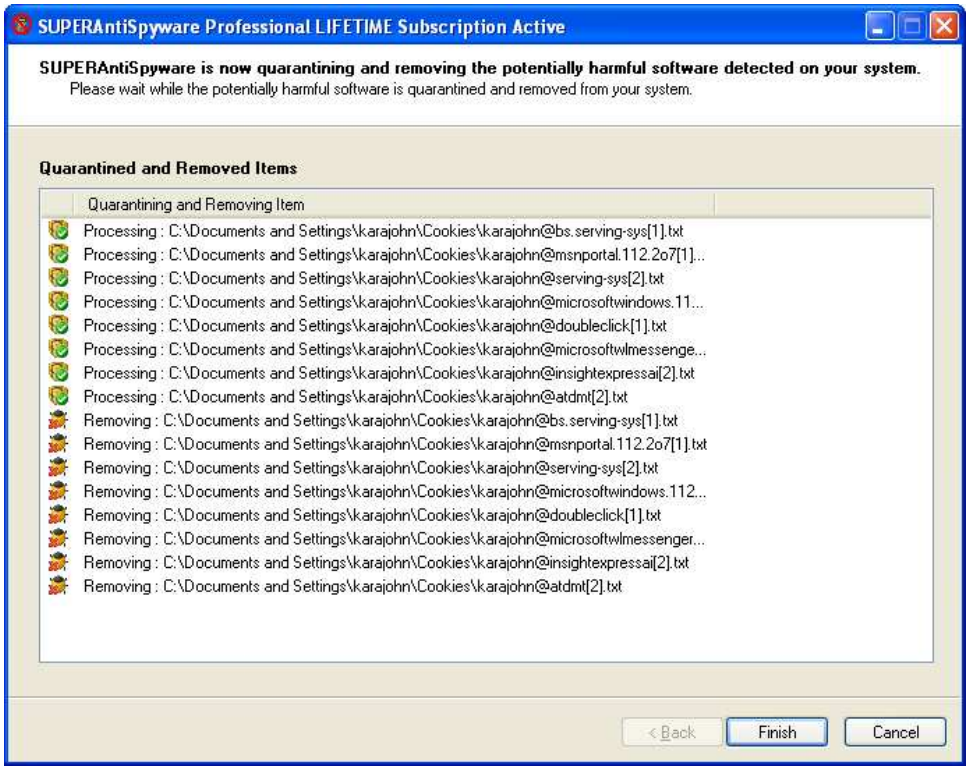
Εικόνα 369: Διαδικασία Σαρώματος με το SUPERAntiSpyware

Μόλις τελειώσει η διαδικασία σαρώματος μας εμφανίζει αν βρήκε τίποτα επιβλαβές. Στη περίπτωση μας ανιχνεύτηκαν 8 αρχεία επιβλαβές. Πατώντας OK μας εμφανίζει και μια αναφορά με τα αρχεία που μπήκαν σε καραντίνα ή μετακινήθηκαν.



Εικόνα 370: Αποτελέσματα Σάρωσης

*Πατώντας **Finish***

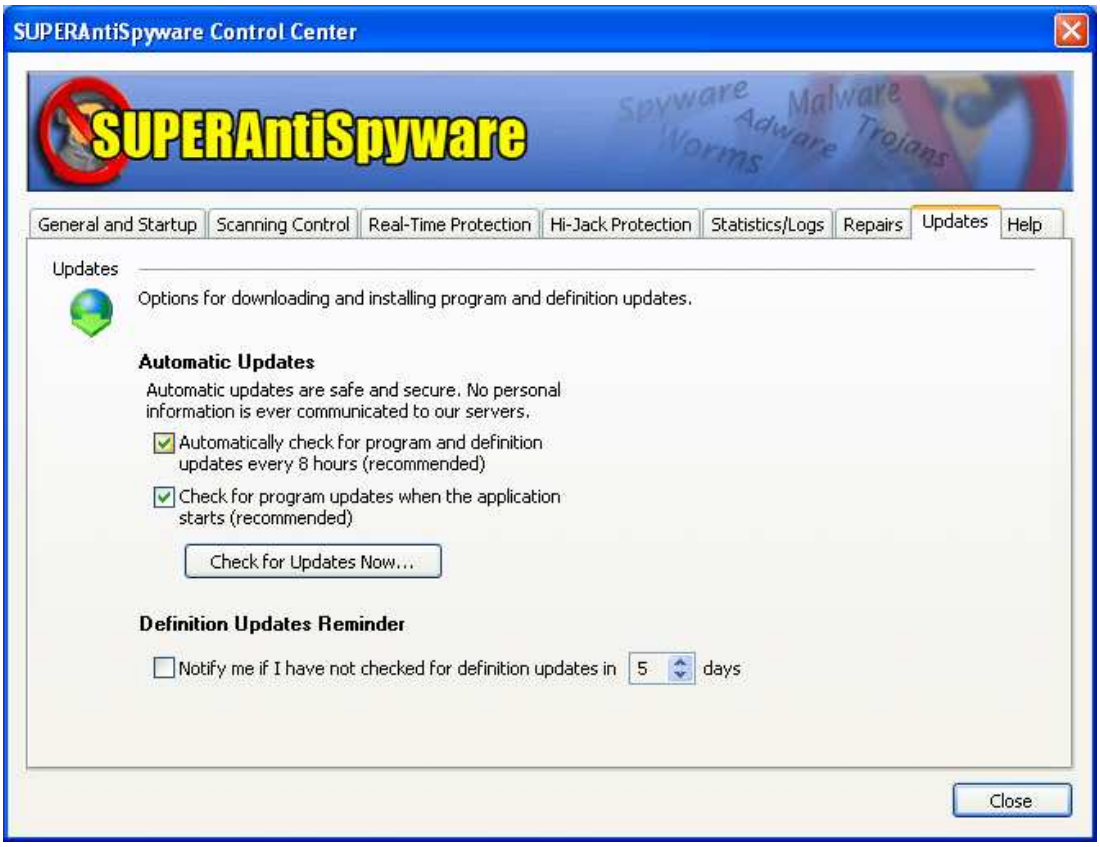


Εικόνα 371: Μετακίνηση και Τοποθέτηση σε Καραντίνα των Βλαβερών Αρχείων

Μας εμφανίζει το παρακάτω παράθυρο όπου μας λέει ότι μπήκαν σε καραντίνα και μετακινήθηκαν . Πατώντας ΟΚ επιστρέφουμε στο κύριο μενού

Εικόνα 372: Τα Βλαβερά Αρχεία Τοποθετήθηκαν σε Καραντίνα και Μετακινήθηκαν

Τέλος να ρυθμίσετε να γίνετε αυτόματα η λήψη και η εγκατάσταση των ενημερώσεων.



Εικόνα 373: Έλεγχος για Αυτόματη Λήψη

Βιβλιογραφία

Βιβλιογραφία

Οδηγός του National Institute of Standards and Technology (NIST) http://csrc.nist.gov/itsec/SP800-68r1.pdf

Λαζαρίδης Ν (2001). *Λεξικό Πληροφορικής*. Αθήνα: Εκδόσεις Πελεκάνος.