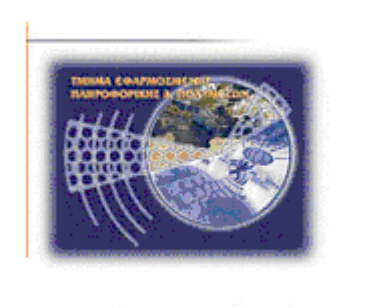
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Ασφαλής διαχείριση Microsoft Windows XP Professional σύμφωνα με την μεθοδολογία NIST SP 800-68 (Μέρος 2ο)

Κωνσταντίνος Τσέλιος (ΑΜ: 953)
E-mail: epp953@epp.teiher.gr

Ηράκλειο – 14/07/2009

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

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, παρέχεται ένα υψηλό επίπεδο ασφάλειας για Windows XP Professional συστήματα, 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 certain settings, provides a high security level for Windows XP Professional systems, taking into account the role that each system plays and in wich 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

Ευχαριστίες ... **ii**
Περίληψη ... **iii**
Abstract ... **iii**
Πίνακας Περιεχομένων ... **iv**
Πίνακας Εικόνων ... **vii**
Πίνακας Πινάκων ... **xii**
Κεφάλαιο 1 ... **1**
1. Εισαγωγή ... **1**
1.1 Φορέας ... 1
1.2 Αντικείμενο και Σκοπός ... 1
1.3 Απευθύνον Κοινό ... 2
1.4 Δομή Εγχειριδίου ... 2
Κεφάλαιο 2 ... **4**
2. Ανάπτυξη του Οδηγού Ασφάλειας για τα Windows XP ... **4**
2.1 Σύστημα με Windows XP – Ρόλοι και Απαιτήσεις ... 5
2.2 Κατηγοριοποίηση Ασφάλειας των Πληροφοριακών Συστημάτων και της Πληροφορίας ... 6
2.3 Βασικά Μέτρα Ασφάλειας και Ανάλυση Απειλών ... 8
2.3.1 Τοπικές Απειλές ... *9*
2.3.2 Απομακρυσμένες Απειλές ... *12*
2.4 Τεκμηρίωση Περιβαλλόντων και Ελέγχων Ασφάλειας ... 16
2.4.1 SOHO ... *16*
2.4.2 Enterprise ... *17*
2.4.3 Specialized Security-Limited Functionality (SSLF) ... *19*
2.4.4 Legacy ... *20*
2.4.5 FDCC ... *21*
2.4.6 Τεκμηρίωση Ασφάλειας ... *21*
2.5 Εφαρμογή και Δοκιμή Ελέγχων Ασφάλειας ... 22
2.6 Επίβλεψη και Συντήρηση ... 23
2.7 Σύνοψη και Υποδείξεις ... 24
Κεφάλαιο 3 ... **26**
3. Προεπισκόπιση Συστατικών Ασφάλειας (Components) των Windows XP ... **26**
3.1 Νέα χαρακτηριστικά στα Windows XP ... 26
3.1.1 Χαρακτηριστικά Δικτύου ... *26*
3.1.2 Πιστοποίηση και Εξουσιοδότηση ... *28*
3.1.3 Άλλα ... *30*
3.2 Χαρακτηριστικά Ασφάλειας Κληροδοτημένα από τα Windows 2000 ... 32
3.2.1 Kerberos ... *33*
3.2.2 Υποστήριξη Έξυπνων Καρτών ... *33*
3.2.3 Διαμοιρασμός Σύνδεσης Διαδικτύου ... *34*
3.2.4 Ασφάλεια Πρωτοκόλλου Διαδικτύου ... *34*
3.2.5 Κωδικοποίηση Συστήματος Διαχείρισης Αρχείων ... *34*
3.3 Σύνοψη και Υποδείξεις ... 35
Κεφάλαιο 4 ... **37**
4. Domain Controller - Active Directory ... **37**
4.1 Domain Controller (Ελεγκτής Τομέα) ... 37
4.2 Δομή του Active Directory ... 38

4.2.1 Αντικείμενα ... *39*
4.3 Εγκατάσταση και Εφαρμογή του Active Directory ... 41
4.3.1 Εγκατάσταση του Active Directory ... *42*
4.3.2 Προσθήκη Αντικειμένων ... *53*
4.3.3 Ομαδοποίηση Αντικειμένων ... *63*
4.3.4 Ιδιότητες αντικειμένων ... *68*
4.3.5 Καταχώρηση Client σε Τομέα ... *96*
4.4 Τοπολογία Δικτύου ... 104
Κεφάλαιο 5 ... 109
5. Επισκόπηση της Διαμόρφωσης και των Προτύπων Πολιτικής Ασφάλειας των Windows XP ... 109
5.1 Πρότυπα Ασφάλειας Windows XP ... 109
5.2 Ανάλυση και Διαμόρφωση ... 114
5.3 Διανομή Πολιτικής Ομάδων ... 121
5.4 Πρότυπα Διαχείρισης ... 138
5.5 Σύνοψη και Υποδείξεις ... 138
Κεφάλαιο 6 ... 139
6. Επισκόπηση Προτύπων Ασφάλειας του NIST για τα Windows XP ... 139
6.1 Πολιτικές Λογαριασμών ... 139
6.2 Τοπικές Πολιτικές ... 142
6.2.1 Πολιτική Ελέγχου ... *142*
6.2.2 Ανάθεση Δικαιωμάτων Χρηστών ... *146*
6.2.3 Επιλογές Ασφάλειας ... *146*
6.3 Πολιτικές Αναφορών Συμβάντων ... 148
6.4 Περιορισμένες Ομάδες ... 148
6.5 Υπηρεσίες Συστήματος ... 149
6.6 Δικαιώματα Αρχείων ... 155
6.7 Δικαιώματα Μητρώου ... 162
6.8 Τιμές Μητρώου ... 164
6.8.1 Αυτόματες Λειτουργίες ... *165*
6.8.2 Δικτύωση ... *166*
6.8.3 Άλλες Ρυθμίσεις Προτύπου ... *171*
6.8.4 Ρυθμίσεις Εκτός των Προτύπων του NIST ... *174*
6.9 Σύνοψη και Υποδείξεις ... 175
Βιβλιογραφία ... 177

Πίνακας Εικόνων

Εικόνα 2-1. Οι όψεις της ασφάλειας των Windows XP. 5
Εικόνα 2-2. Η Τυπική Αρχιτεκτονική Δικτύου SOHO..... 17
Εικόνα 2-3. Η Τυπική Αρχιτεκτονική Δικτύου Enterprise. 19
Εικόνα 2-4. Παραδείγματα Συστημάτων Specialized Security-Limited Functionality. 20
Εικόνα 4-1 Domain Controller Network. 38
Εικόνα 4-2 Εντολή dcpromo. 42
Εικόνα 4-3 Active Directory Installation Wizard βήμα 1ο. 42
Εικόνα 4-4. Active Directory Installation Wizard βήμα 2ο. 43
Εικόνα 4-5. Active Directory Installation Wizard βήμα 3ο. 43
Εικόνα 4-6. Active Directory Installation Wizard βήμα 4ο. 44
Εικόνα 4-7. Active Directory Installation Wizard βήμα 5ο. 44
Εικόνα 4-8. Active Directory Installation Wizard βήμα 6ο. 45
Εικόνα 4-9. Active Directory Installation Wizard βήμα 7ο. 46
Εικόνα 4-10. Active Directory Installation Wizard βήμα 8ο. 47
Εικόνα 4-11. Active Directory Installation Wizard βήμα 9ο. 47
Εικόνα 4-12. Active Directory Installation Wizard βήμα 10ο. 48
Εικόνα 4-13. Active Directory Installation Wizard βήμα 11ο. 49
Εικόνα 4-14. Active Directory Installation Wizard βήμα 12ο. 49
Εικόνα 4-15. Active Directory Installation Wizard βήμα 13ο Α. 50
Εικόνα 4-16. Active Directory Installation Wizard βήμα 13ο Β. 50
Εικόνα 4-17. Active Directory Installation Wizard βήμα 14ο: Network Configuration. 51
Εικόνα 4-18. Active Directory Installation Wizard βήμα 14ο: TCP/IP Properties. 51
Εικόνα 4-19. Active Directory Installation Wizard βήμα 14ο: IP Configuration. 52
Εικόνα 4-20. Active Directory Installation Wizard βήμα 14ο: DNS Installation. 52
Εικόνα 4-21. Active Directory Installation Wizard βήμα 15ο. 53
Εικόνα 4-22. Active Directory Installation Wizard βήμα 16ο. 53
Εικόνα 4-23. Active Directory Users and Computers. 54
Εικόνα 4-24. Add New OU. 55
Εικόνα 4-25. Ονοματοδότηση OU. 55
Εικόνα 4-26. Add New Embedded OU. 56
Εικόνα 4-27. Προεπισκόπιση OUs. 57
Εικόνα 4-28. Add New Computer. 58
Εικόνα 4-29. Ονοματοδότηση Computer. 58
Εικόνα 4-30. Add New Group. 59
Εικόνα 4-31. Ονοματοδότηση Group. 60
Εικόνα 4-32. Add New User. 61
Εικόνα 4-33. User Logon Name. 61
Εικόνα 4-34. Set User Password. 62
Εικόνα 4-35. Προεπισκόπιση ρυθμίσεων χρήστη. 62
Εικόνα 4-36. Προεπισκόπιση Users. 63
Εικόνα 4-37. Add Computer to Group βήμα 1ο. 64
Εικόνα 4-38. Add Computer to Group βήμα 2ο. 65
Εικόνα 4-39. Add Computer to Group βήμα 3ο Α. 65
Εικόνα 4-40. Add Computer to Group βήμα 3ο Β. 66
Εικόνα 4-41. Add Computer to Group βήμα 4ο. 66
Εικόνα 4-42. Add User to Group βήμα 1ο. 67
Εικόνα 4-43. Add User to Group βήμα 2ο Α. 67

Εικόνα 4-44. Add User to Group βήμα 2ο Β. 68
Εικόνα 4-45. Add User to Group βήμα 3ο. 68
Εικόνα 4-46. OU Properties. 69
Εικόνα 4-47. OU Properties: Η καρτέλα General. 70
Εικόνα 4-48. OU Properties: Η καρτέλα Managed By. 71
Εικόνα 4-49. OU Properties: Στην καρτέλα Managed By, η επιλογή Change Α. 71
Εικόνα 4-50. OU Properties: Στην καρτέλα Managed By, η επιλογή Change Β. 72
Εικόνα 4-51. OU Properties: Στην καρτέλα Managed By, η επιλογή Change Γ. 72
Εικόνα 4-52. OU Properties: Η καρτέλα COM+. 73
Εικόνα 4-53. OU Properties: Η καρτέλα Group Policy. 74
Εικόνα 4-54. OU Properties: Στην καρτέλα Managed By, η επιλογή Add: επιλέγουμε κάποιο από τα GPOs της λίστας που επιθυμούμε να προσθέσουμε στο OU. 74
Εικόνα 4-55. OU Properties: Στην καρτέλα Managed By, η επιλογή Edit: ανοίγει ο GPO Editor. 75
Εικόνα 4-56. OU Properties: Στην καρτέλα Managed By, η επιλογή Options: μπορούμε να επιλέξουμε No Override ή Disabled. 75
Εικόνα 4-57. Computer Properties. 76
Εικόνα 4-58. Computer Properties: Η καρτέλα General. 77
Εικόνα 4-59. Computer Properties: Η καρτέλα Member Of. 78
Εικόνα 4-60. Computer Properties: Η καρτέλα Location. 79
Εικόνα 4-61. Computer Properties: Η καρτέλα Managed By. 80
Εικόνα 4-62. Computer Properties: Η καρτέλα Dial-In. 81
Εικόνα 4-63. User Properties. 82
Εικόνα 4-64. User Properties: Η καρτέλα General. 83
Εικόνα 4-65. User Properties: Η καρτέλα Address. 84
Εικόνα 4-66. User Properties: Η καρτέλα Account. 85
Εικόνα 44-67. User Properties: Στην καρτέλα Account, η επιλογή Logon Hours. 85
Εικόνα 44-68. User Properties: Στην καρτέλα Account, η επιλογή Log On To. 86
Εικόνα 4-69. User Properties: Η καρτέλα Profile. 87
Εικόνα 4-70. User Properties: Η καρτέλα Telephones. 88
Εικόνα 4-71. User Properties: Η καρτέλα Organization. 89
Εικόνα 4-72. User Properties: Η καρτέλα Remote Control. 90
Εικόνα 4-73. User Properties: Η καρτέλα Terminal Services Profile. 91
Εικόνα 4-74. User Properties: Η καρτέλα COM+. 92
Εικόνα 4-75. User Properties: Η καρτέλα Member Of. 93
Εικόνα 4-76. User Properties: Η καρτέλα Dial-In. 94
Εικόνα 4-77. User Properties: Η καρτέλα Environment. 95
Εικόνα 4-78. User Properties: Η καρτέλα Sessions. 96
Εικόνα 4-79. My Computer Properties. 97
Εικόνα 4-80. System Properties. Στην καρτέλα Computer Name η επιλογή Change. 98
Εικόνα 4-81. Computer Name Changes. Η επιλογή Member Of Domain. 99
Εικόνα 4-82. Administrator authentication. 99
Εικόνα 4-83. Η οθόνη Welcome to domain. 100
Εικόνα 4-84. Ειδοποίηση για επανεκκίνηση. 100
Εικόνα 4-85. System Properties. Η καρτέλα Computer Name με τις αλλαγές. 101
Εικόνα 4-86. Επιβεβαίωση επανεκκίνησης. 101
Εικόνα 4-87. Εισαγωγή στον τομέα βήμα 1ο. 102
Εικόνα 4-88. Εισαγωγή στον τομέα βήμα 2ο. 102
Εικόνα 4-89. Εισαγωγή στον τομέα βήμα 3ο. 103
Εικόνα 4-90. Εισαγωγή στον τομέα βήμα 4ο. 103

Εικόνα 4-91. Εισαγωγή στον τομέα βήμα 5ο. 104
Εικόνα 4-92. Επιτυχής εισαγωγή στον τομέα. 104
Εικόνα 4-93. VM Host με ενεργά τα δύο Virtual Machines. 105
Εικόνα 4-94. Οι ρυθμίσεις δικτύου του VM Host. 106
Εικόνα 4-95. Οι ρυθμίσεις δικτύου του VM Domain Controller. 107
Εικόνα 4-96. Οι ρυθμίσεις δικτύου του VM Client. 108
Εικόνα 5-1 Εντολή Run. 110
Εικόνα 5-2. Ο φάκελος Templates. 110
Εικόνα 5-3. Εντολή MMC. 111
Εικόνα 5-4. Κονσόλα MMC. 111
Εικόνα 5-5. Add/Remove Snap-in. 111
Εικόνα 5-6. Security Templates Snap-in. 111
Εικόνα 5-7. Επιλέγουμε το πρότυπο enterprise. 112
Εικόνα 5-8. Αντικαθιστούμε τον ελάχιστο αριθμό χαρακτήρων του password με την τιμή 6. 112
Εικόνα 5-9. Έχουμε κάνει τις επιθυμητές αλλαγές και σώζουμε την κονσόλα. 113
Εικόνα 5-10. Ορίζουμε το όνομα της κονσόλας. 113
Εικόνα 5-11. Ο Administrative Tools φάκελος που αποθηκεύσαμε την κονσόλα μας. 114
Εικόνα 5-12 Security Configuration and Analysis Snap-in. 114
Εικόνα 5-13. Open Database. 115
Εικόνα 5-14. Import Teplate. 115
Εικόνα 5-15. Analyze Computer Now. 116
Εικόνα 5-16. Σώζουμε το αρχείο log. 116
Εικόνα 5-17. Μέρος του log file το οποίο είναι σε μορφή κειμένου και το χρησιμοποιεί η κονσόλα για να εξάγει την αναφορά σύγκρισης ρυθμίσεων. 117
Εικόνα 5-18. Αναφορά της ανάλυσης. 118
Εικόνα 5-19. Ιδιότητα “Change the system time”. 119
Εικόνα 5-20. Configure Computer Now. 120
Εικόνα 5-21. Configuring. 120
Εικόνα 5-22. Εξαγωγή προτύπου. 120
Εικόνα 5-23. Ο φάκελος που αποθηκεύτηκε το πρότυπο. 120
Εικόνα 5-24 Συνοπτικό διάγραμμα διεργασιών της ενότητας 5.3. 121
Εικόνα 5-25. Group Policy Object Editor Snap-in. 122
Εικόνα 5-26. Επιλογή GPO. 122
Εικόνα 5-27. Window Settings. 123
Εικόνα 5-28. Εισαγωγή Policy. 123
Εικόνα 5-29. Κομμάτι ενός custom template. 124
Εικόνα 5-30. Import του custom policy template 124
Εικόνα 5-31. Group Policy Management Snap-in. 125
Εικόνα 5-32. GPMC. 126
Εικόνα 5-33. Link existing GPO. 126
Εικόνα 5-34. Select GPO. 127
Εικόνα 5-35. Create and Link GPO. 127
Εικόνα 5-36. New GPO. 127
Εικόνα 5-37. Ονοματοδοσία GPO. 128
Εικόνα 5-38. Edit GPO. 128
Εικόνα 5-39. Custom GPO. 128
Εικόνα 5-40. Import Policy. 129
Εικόνα 5-41. Import Policy from. 129
Εικόνα 5-42. Security Settings. 130

Εικόνα 5-43. Σε 90 ημέρες θα ζητηθεί από το χρήστη να αλλάξει τον κωδικό εξουσιοδότησής του για την εισαγωγή του στον τομέα. 130
Εικόνα 5-44. Group Policy Modeling Wizard. 131
Εικόνα 5-45. Χρησιμοποιήσαμε τον Domain Controller στον τομέα domain.ktse.gr. 132
Εικόνα 5-46. Θέσαμε user τον Administrator (διαχειριστής server), και σαν υπολογιστή τον ίδιο τον Domain Controller. 132
Εικόνα 5-47. Σαν ιστότοπο θέσαμε την default του Domain Controller. 133
Εικόνα 5-48. Θέσαμε σαν ομάδα το KostasGroup. 133
Εικόνα 5-49. Θέσαμε ένα ανύπαρκτο αντικείμενο για να λάβουμε ένα σφάλμα. 134
Εικόνα 5-50. Στον συγκεκριμένο Domain Controller δεν θέσαμε WMI filters. 134
Εικόνα 5-51. Summary of Selection [τελική ανασκόπηση της προσομοίωσης]. 135
Εικόνα 5-52. Α' μέρος αναφοράς Group Policy Result. 136
Εικόνα 5-53. Β' μέρος αναφοράς Group Policy Result. 137
Εικόνα 6-1. Control Panel. 143
Εικόνα 6-2. Administrative Tools. 143
Εικόνα 6-3. Local Security Policy. 144
Εικόνα 6-4. Local Security Settings – Audit Policy. 144
Εικόνα 6-5. Audit Logon Events Properties. 145
Εικόνα 6-6. Local Security Settings – Audit Policy Customized. 145
Εικόνα 6-7. Local Security Setting – Security Options. 147
Εικόνα 6-8. Interactive Logon – Prompt User to Change Password Before. 148
Εικόνα 6-9. Administrative Tools – Services. 151
Εικόνα 6-10. Services. 151
Εικόνα 6-11. Clipbook ορισμένο στο Manual. 152
Εικόνα 6-12. Clipbook Properties. 152
Εικόνα 6-13. Clipbook ορισμένο στο Disabled. 153
Εικόνα 6-14. My Computer Properties. 153
Εικόνα 6-15. System Properties – General. 154
Εικόνα 6-16. System Properties – Remote. 154
Εικόνα 6-17. System Properties – Remote customized. 155
Εικόνα 6-18. Shared Folder Properties. 156
Εικόνα 6-19. Shared Folder Properties – Security. 156
Εικόνα 6-20. Απόδοση δικαιωμάτων βήμα 1^{ο}. 157
Εικόνα 6-21. Απόδοση δικαιωμάτων βήμα 2^{ο}. 157
Εικόνα 6-22. Απόδοση δικαιωμάτων βήμα 3^{ο}. 158
Εικόνα 6-23. Απόδοση δικαιωμάτων βήμα 4^{ο}. 158
Εικόνα 6-24. Απόδοση δικαιωμάτων βήμα 5^{ο}. 159
Εικόνα 6-25. Command Prompt. 160
Εικόνα 6-26. Cacls βήμα 1^{ο}. 160
Εικόνα 6-27. Cacls βήμα 2^{ο}. 161
Εικόνα 6-28. Cacls βήμα 3^{ο}. 161
Εικόνα 6-29. Cacls βήμα 4^{ο}. 162
Εικόνα 6-30. Cacls βήμα 5^{ο}. 162
Εικόνα 6-31. Registry Editor. 163
Εικόνα 6-32. Registry Editor – winreg. 163
Εικόνα 6-33. Winreg Permissions A. 164
Εικόνα 6-34. Winreg Permissions B. 164
Εικόνα 6-35. Winreg Permissions C. 164
Εικόνα 6-36. Winreg Permissions D. 164
Εικόνα 6-37. NoDriveTypeAutoRun. 165

Εικόνα 6-38. AutoAdminLogon cleartext. 165
Εικόνα 6-39. AutoAdminLogon. 166
Εικόνα 6-40. AutoReboot. 166
Εικόνα 6-41. NoDefaultExempt. 167
Εικόνα 6-42. AutoShareWks. 167
Εικόνα 6-43. Hidden. 167
Εικόνα 6-44. DisableIPSourceRouting. 168
Εικόνα 6-45. EnableDeadGWDetect. 168
Εικόνα 6-46. EnableCMPRedirect. 169
Εικόνα 6-47. KeepAliveTime. 169
Εικόνα 6-48. NoName ReleaseOnDemand. 170
Εικόνα 6-49. SynAttackProtect. 170
Εικόνα 6-50. TcpMaxConnectResponseRetransmissions. 171
Εικόνα 6-51. TcpMaxDataRetransmissions. 171
Εικόνα 6-52. ScreenSaverGracePeriod. 172
Εικόνα 6-53. NtfsDisable8dot3NameCreation. 172
Εικόνα 6-54. SafeDllSearchMode. 173
Εικόνα 6-55. WarningLevel. 173
Εικόνα 6-56. DisableSavePassword. 173

Πίνακας Πινάκων

Πίνακας 6-1 Περιγραφή Ευρέος Ελέγχου Πολιτικής Συστήματος..... 142
Πίνακας 6-2. Επιπρόσθετες Registry Values..... 174

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 Α-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 Α-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 Άυγουστο του 2004, περιέχει πολλές αλλαγές που μπορούν να επιρρεάσουν 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.

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 Απευθύνον 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 Δομή Εγχειριδίου

Το υπόλοιπο του εγχειριδίου είναι οργανομένο σε επτά κύριες ενότητες, και ακολουθούν επτά παραρτήματα.

- Η Ενότητα 2 παρέχει μία ματιά σε απειλές και ελέγχους ασφάλειας που είναι κατάλληλοι για διάφορα περιβάλλοντα, όπως μεγάλες επιχειρήσεις ή γραφεία σπιτιού, και περιγράφει την ανάγκη της τεκμηρίωσης, της εφαρμογής και της δοκιμής των ελέγχων, όπως επίσης και την επίβλεψη και συντήρηση συστημάτων σε συνεχόμενη βάση.

- Η Ενότητα 3 παρουσιάζει μία επισκόπιση των συστατικών ασφάλειας που παρέχονται από τα Windows XP.

- Η Ενότητα 4 παρουσίαζει την ανάγκη ύπαρξης του τομέα και των στοιχείων του και παρέχει οδηγίες για την εγκατάσταση ενός ελεγκτή τομέα καθώς και επιπρόσθετες πληροφορίες για τη διαμόρφωση των επί μέρους τμημάτων του.

- Η Ενότητα 5 συζητά τη διαμόρφωση της πολιτικής ασφάλειας και πώς είναι καλύτερο να χρησιμοποιηθούν τα πρότυπα ασφάλειας.

---

[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.

- Η Ενότητα 6 παρέχει μία επισκόπιση των ρυθμίσεων στα πρότυπα ασφάλειας του NIST και εξηγεί πώς οι ρυθμίσεις μπορούν να παρέχουν μεγαλύτερη ασφάλεια στα συστήματα.

- Το Παράρτημα A συζητά για τα πρότυπα ασφάλειας του NIST και τα GPO του Federal Desktop Core Configuration (FDCC).

- Το Παράρτημα B υπογραμμίζει μερικές από τις αλλαγές ασφάλειας στο Windows XP Service Pack 3 (SP3).

- Το Παράρτημα C χαρτογραφεί τους ελέγχους ασφάλειας και τις ρυθμίσεις των προτύπων αυτού του οδηγού, με τους ελέγχους της ειδικής δημοσίευσης του NIST 800-53 Επανέκδοση 2, *Recommended Security Controls for Federal Information Systems*.

- Το Παράρτημα D απαριθμεί τις TCP και UDP πόρτες που χρησιμοποιούνται συνήθως σε Windows XP συστήματα.

- Το Παράρτημα E απαριθμεί εργαλεία που μπορούν να είναι χρήσιμα στην ασφάλεια Windows XP συστημάτων και το Παράρτημα F απαριθμεί έντυπες και διαδικτυακές πηγές οι οποίες μπορούν να είναι χρήσιμες αναφορές ασφάλειας για τα Windows XP.

- Το Παράρτημα G απαριθμεί τα ακρωνύμια και τις συντομογραφίες που χρησιμοποιήθηκαν στον οδηγό.

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. Ανάπτυξη του Οδηγού Ασφάλειας για τα Windows XP

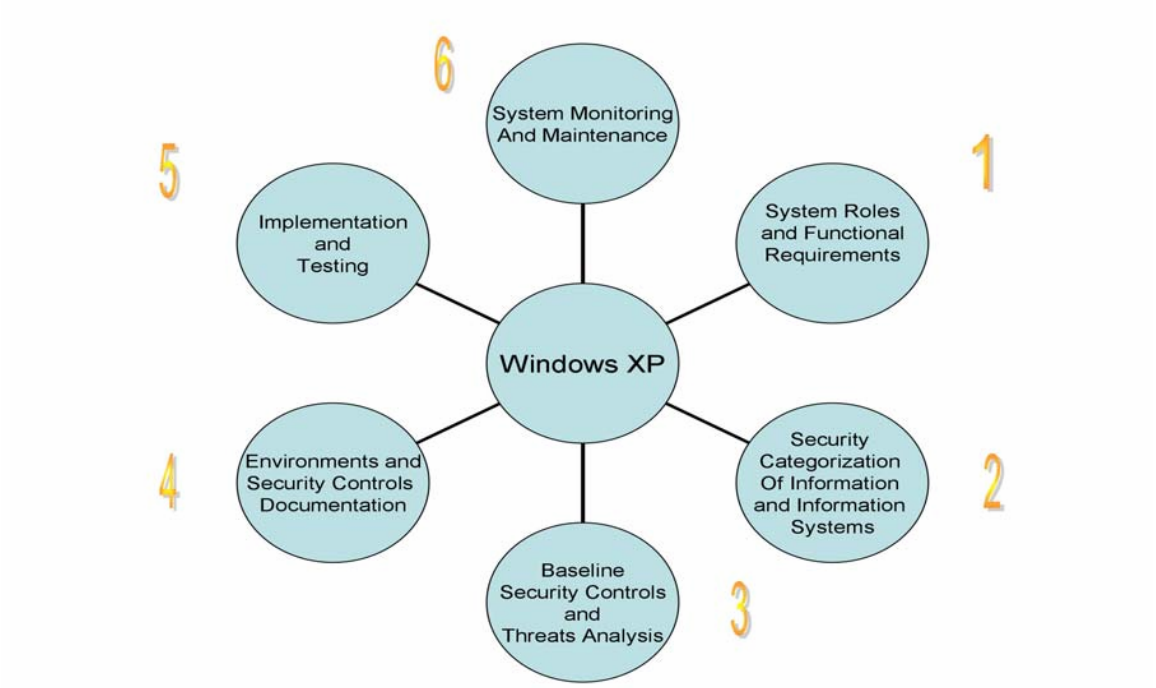
Σήμερα, στο περιβάλλον των υπολογιστών, η ασφάλεια όλων των υπολογιστικών πηγών, από συσκευές υποδομής δικτύου μέχρι επιτραπέζιους υπολογιστές χρηστών, είναι απαραίτητη. Υπάρχουν πολλές απειλές στους υπολογιστές των χρηστών, που κυμαίνονται από εκμετάλλευση απομακρυσμένα εκτελέσιμων υπηρεσιών δικτύου μέχρι κακόβουλο λογισμικό (malware) το οποίο διαδίδεται μέσω ηλεκτρονικού ταχυδρομείου, ιστοσελίδων και καταφόρτωση αρχείων. Αυξάνοντας την ασφάλεια σε κάθε υπολογιστή ξεχωριστά προστατεύεται από αυτές τις απειλές και ελαττώνεται η πιθανότητα έκθεσης κάποιου συστήματος ή η πιθανότητα κάποια δεδομένα να αποκαλυφθούν σε μη-εξουσιοδοτημένες ομάδες. Οι αποτελεσματικές και καλά δοκιμασμένες ρυθμίσεις ασφάλειας σημαίνουν λιγότερο χρόνο και χρήμα σπατάλης για εξάλειψη κακόβουλου λογισμικού, επαναφορά συστημάτων από backups και επανεγκατάσταση λειτουργικών συστημάτων και εφαρμογών. Επιπρόσθετα, διατηρώντας ισχυρή την ασφάλεια του host αυξάνεται η ασφάλεια του δικτύου (πχ, δίκτυα σπιτιού, επιχειρήσεων, κυβερνητικά δίκτυα, το διαδίκτυο)˙ για παράδειγμα, οι περισσότερες κατανεμημένες επιθέσεις άρνησης υπηρεσίας εναντίον δικτύων χρησιμοποιούν μεγάλο αριθμό εκτεθειμένων hosts.

Ο στόχος αυτού του οδηγού είναι η παροχή καθοδήγησης για ρυθμίσεις ασφάλειας σε χρήστες και διαχειριστές συστημάτων Microsoft Windows XP. Οι οδηγίες αυτές μπορούν να προσαρμοστούν σε οποιοδήποτε περιβάλλον, από ξεχωριστές SOHO εγκαταστάσεις μέχρι μεγάλους, γεωγραφικά διαχωρισμένους οργανισμούς. Παρόλο που αυτός ο οδηγός στοχεύει κυρίως σε επιχειρηματικά περιβάλλοντα και στα Windows XP Professional, ορισμένα μέρη του είναι επίσης κατάλληλα και για άλλες εκδόσεις των XP, όπως τα Windows XP Home, Windows XP Tablet PC Edition, και Windows XP Media Center Edition.[3] Αυτός ο οδηγός εκτείνεται σε μεγάλο εύρος γνώσεων προμηθευτών, κυβέρνησης και στην εμπειρία της κοινωνίας της ασφάλειας που αποκτήθηκε μέσω πολλών ετών παροχής ασφάλειας υπολογιστικών συστημάτων.

Αυτή η ενότητα του οδηγού έχει βασιστεί κυρίως στα βήματα που προτείνονται από το FISMA Implementation Project του NIST για την επίτευξη μεγαλύτερης ασφάλειας πληροφοριακών συστημάτων.[4] Οι ενότητες 2.1 και 2.2 απευθύνονται στην ανάγκη της κατηγοριοποίησης της πληροφορίας και των πληροφοριακών συστημάτων. Το κάθε Windows XP σύστημα μπορεί να ταξινομηθεί ως έχον έναν ή τρεις ρόλους˙ το κάθε σύστημα μπορεί επίσης να ταξινομηθεί σύμφωνα με το πιθανό αντίκτυπο που προκαλείται από παραβιάσεις ασφάλειας. Η ενότητα 2.3 περιγράφει απειλές και παρέχει παραδείγματα ελέγχων ασφάλειας που μπορούν να τις μετριάσουν. Η ενότητα 2.4 σκιαγραφεί τους βασικούς τύπους περιβαλλόντων πληροφοριακών συστημάτων – Small Office/Home Office (SOHO), Enterprise, Specialized Security-Limited Functionality, Legacy, and Federal Desktop Core Configuration (FDCC) – και συνδέει το κάθε περιβάλλον με τυπικές κατηγορίες απειλών και ελέγχων ασφάλειας. Η ενότητα 2.5 παρέχει μία περιεκτική σύνοψη

[3] Το NIST SP 800-69, *Guidance for Securing Microsoft Windows XP Home Edition*, παρέχει βήμα προς βήμα καθοδήγηση για τερματικούς Windows XP Home χρήστες για την ασφάλεια των συστημάτων τους. Είναι διαθέσιμο στη διεύθυνση http://csrc.nist.gov/publications/PubsSPs.html.
[4] Περισσότερες πληροφορίες σχετικά με αυτό το project είναι διαθέσιμες εδώ: http://csrc.nist.gov/groups/SMA/fisma/index.html.

της εφαρμογής των ελέγχων ασφάλειας και τη σπουδαιότητα της εκτέλεσης δοκιμών λειτουργικότητας και ασφάλειας. Τέλος, η ενότητα 2.6 συζητά την ανάγκη για επίβλεψη των ελέγχων ασφάλειας και τη συντήρηση του συστήματος. Η Εικόνα 2-1 δείχνει τις έξι όψεις της ασφάλειας των Windows XP οι οποίες καλύπτονται στις ενότητες 2.1 μέχρι 2.6.



Εικόνα 2-1. Οι όψεις της ασφάλειας των Windows XP.

2.1 Σύστημα με Windows XP – Ρόλοι και Απαιτήσεις

Για την ασφάλεια των Windows XP θα πρέπει να ληφθεί υπόψη ο ρόλος που έχει το σύστημα. Για το αντικείμενο του οδηγού αυτού τα συστήματα Windows XP μπορούν να καταταχτούν σε τρεις κατηγορίες:

- **Εσωστρεφή:** Ένα εσωστρεφές Windows XP σύστημα (Inward-Facing system) είναι ένας σταθμός εργασίας χρήστη (user workstation) ο οποίος είναι μέρος ενός δικτύου που δεν είναι άμεσα προσβάσιμο από το διαδίκτυο. Η φυσική πρόσβαση είναι περιορισμένη κατά κάποιο τρόπο (πχ, μόνο οι υπάλληλοι της εταιρίας έχουν πρόσβαση στο χώρο εργασίας). Σε πολλά περιβάλλοντα τα εσωστρεφή συστήματα μοιράζονται κοινές ρυθμίσεις hardware και software επειδή υπάρχει κεντρική διαχείριση (βλ. Microsoft domains, Novell networks). Επειδή ένα εσωστρεφές σύστημα είναι συνήθως, συνεχώς στο ίδιο περιβάλλον (πχ, ένας επιτραπέζιος υπολογιστής που βρίσκεται στο εταιρικό τοπικό δίκτυο [LAN]), οι απειλές που μπορεί να αντιμετωπίζει δεν αλλάζουν γρήγορα. Γενικά, τα εσωστρεφή συστήματα είναι σχετικά εύκολα όσον αφορά την ασφάλειά τους εν συγκρίσει με τα εξωστρεφή και τα κινητά συστήματα.

- **Εξωστρεφή:** Ένα εξωστρεφές Windows XP σύστημα (Outward-Facing system) είναι απευθείας συνδεδεμένο στο διαδίκτυο. Κλασικό παράδειγμα ενός τέτοιου συστήματος είναι ένας υπολογιστής σπιτιού (home PC), ο οποίος συνδέεται στο διαδίκτυο μέσω dial-up ή broadband σύνδεσης. Ένα τέτοιο σύστημα είναι ευπαθές σε κακόβουλες ανιχνεύσεις

(scans, probes), και εξαπολύονται εναντίον του απομακρυσμένες επιθέσεις. Συνήθως δεν έχει τα στρώματα προστασίας που έχει ένα τυπικό εσωστρεφές σύστημα, όπως ένα τείχος προστασίας δικτύου και συστήματα εντοπισμού εισβολής (intrusion detection systems). Τα εξωστρεφή συστήματα έχουν συχνά υψηλό ρίσκο έκθεσης, διότι έχουν συγκριτικά υψηλότερες ανάγκες ασφάλειας, παρόλα αυτά διαχειρίζονται από χρήστες με καθόλου ή ελάχιστη γνώση σε ζητήματα ασφάλειας. Επιπλέον, οι απειλές που δέχονται τα εξωστρεφή συστήματα μπορούν να αλλάξουν γρήγορα εφόσον οποιοσδήποτε μπορεί να αποπειραθεί να επιτεθεί σε αυτά οποιαδήποτε στιγμή.

- **Κινητά:** Ένα σύστημα με κινητό ρόλο (Mobile system) τυπικά κινείται σε πληθώρα από περιβάλλοντα και φυσικές τοποθεσίες. Για σύνδεση με κάποιο δίκτυο, αυτό το σύστημα μπορεί να χρησιμοποιήσει τόσο ενσύρματες μεθόδους (πχ, Ethernet, dial-up), όσο και ασύρματες μεθόδους (πχ, IEEE 802.11). Η κινητικότητα του συστήματος κάνει πιο δύσκολο το να υπάρχει κεντρική διαχείριση. Επιπλέον το σύστημα εκτίθεται σε ευρύτερο φάσμα απειλούμενων περιβαλλόντων· για παράδειγμα μέσα σε μία μόνο ημέρα το σύστημα μπορεί να είναι σε περιβάλλον σπιτιού, σε περιβάλλον γραφείου και σε ένα δωμάτιο κάποιου ξενοδοχείου. Μία επιπρόσθετη απειλή είναι η κλοπή ή ακόμη και η απώλεια του συστήματος. Αυτό μπορεί να οδηγήσει, το λιγότερο, σε απώλεια της παραγωγικότητας, αλλά μπορεί να οδηγήσει και σε γνωστοποίηση απόρρητων πληροφοριών ή και ένα πιθανό άνοιγμα μιας πίσω πόρτας (back door) στον οργανισμό εάν η απομακρυσμένη πρόσβαση δεν είναι σωστά ασφαλισμένη.

2.2 Κατηγοριοποίηση Ασφάλειας των Πληροφοριακών Συστημάτων και της Πληροφορίας

Το κλασικό μοντέλο για την ασφάλεια της πληροφορίας ορίζει την επίτευξη των εξής τριών στόχων: τη διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Η *εμπιστευτικότητα* αναφέρεται στην προστασία της πληροφορίας ώστε αυτή να μην είναι προσβάσιμη από μη-εξουσιοδοτημένα πρόσωπα. Η *ακεραιότητα* αναφέρεται στη διασφάλιση της γνησιότητας της πληροφορίας, δηλαδή ότι δεν έχει αλλοιωθεί το περιεχόμενό της και ότι η πηγή της είναι έγκυρη. Η *διαθεσιμότητα* σημαίνει πως η πληροφορία είναι προσβάσιμη από εξουσιοδοτημένους χρήστες. Κάθε στόχος εξετάζει μία διαφορετική πτυχή της παροχής προστασίας της πληροφορίας.

Η διαδικασία για να καθοριστεί το πόσο έντονα θα πρέπει να προστατευτεί ένα σύστημα βασίζεται κυρίως στο είδος των πληροφοριών που αυτό κατέχει και αποθηκεύει. Για παράδειγμα, ένα σύστημα που περιέχει ιατρικούς φακέλους, προφανώς χρειάζεται πολύ πιο ισχυρή προστασία από έναν υπολογιστή ο οποίος χρησιμοποιείται για θέαση δημοσίως δημοσιευμένων εγγράφων. Δεν θα πρέπει να θεωρηθεί ότι ένα τέτοιο σύστημα δεν χρειάζεται να προστατευθεί· κάθε σύστημα θα πρέπει να προστατεύεται, αλλά αλλάζει το επίπεδο προστασίας βάσει της αξίας του συστήματος και της πληροφορίας που αυτό κατέχει.

Υπάρχουν τρεις κατηγορίες βασισμένες στο πιθανό αντίκτυπο της παραβίασης ασφάλειας ενός συγκεκριμένου συστήματος. Αν το αντίκτυπο είναι: Χαμηλό (Low), Μέτριο (Moderate) ή Υψηλό (High).

- Το πιθανό αντίκτυπο είναι **Χαμηλό (LOW)** εάν η απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας, αναμένεται να έχει **περιορισμένες** αρνητικές συνέπειες στη λειτουργία του οργανισμού, στα στοιχεία του οργανισμού ή σε άτομα.

Περιορισμένη αρνητική συνέπεια σημαίνει πως, για παράδειγμα, η απώλεια της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας θα μπορούσε (i) να προκαλέσει υποβιβασμό της εφαρμογής και διατήρησης της αποστολής του οργανισμού σε έκταση και διάρκεια που ο οργανισμός είναι ικανός να εκτελεί τις θεμελιώδεις λειτουργίες του, αλλά η αποτελεσματικότητα των λειτουργιών είναι αισθητά μειωμένη· (ii) να έχει ως αποτέλεσμα μικρή ζημία στα στοιχεία του οργανισμού· (iii) να έχει ως αποτέλεσμα μικρή οικονομική απώλεια· (iv) να αποτελέσει σε μικρή ζημία ατόμων.

- Το πιθανό αντίκτυπο είναι **Μέτριο (MODERATE)** εάν η απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας, αναμένεται να έχει **σοβαρές** αρνητικές συνέπειες στη λειτουργία του οργανισμού, στα στοιχεία του οργανισμού ή σε άτομα. Σοβαρή αρνητική συνέπεια σημαίνει πως, για παράδειγμα, η απώλεια της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας θα μπορούσε (i) να προκαλέσει εμφανή υποβιβασμό της εφαρμογής και διατήρησης της αποστολής του οργανισμού σε έκταση και διάρκεια που ο οργανισμός είναι ικανός να εκτελεί τις θεμελιώδεις λειτουργίες του, αλλά η αποτελεσματικότητα των λειτουργιών είναι εμφανώς μειωμένη· (ii) να έχει ως αποτέλεσμα αξιοσημείωτη ζημία στα στοιχεία του οργανισμού· (iii) να έχει ως αποτέλεσμα αξιοσημείωτη οικονομική απώλεια· (iv) να αποτελέσει σε αξιοσημείωτη ζημία ατόμων χωρίς αυτό να προϋποθέτει απώλεια ζωής ή σοβαρό, απειλητικό για τη ζωή τραυματισμό.

- Το πιθανό αντίκτυπο είναι **Υψηλό (HIGHT)** εάν η απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας, αναμένεται να έχει **σφοδρές ή καταστροφικές** συνέπειες στη λειτουργία του οργανισμού, στα στοιχεία του οργανισμού ή σε άτομα. Σφοδρή ή καταστροφική συνέπεια σημαίνει πως, για παράδειγμα, η απώλεια της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας θα μπορούσε (i) να προκαλέσει δριμύ υποβιβασμό της εφαρμογής και διατήρησης της αποστολής του οργανισμού σε έκταση και διάρκεια που ο οργανισμός δεν είναι ικανός να εκτελεί μία ή περισσότερες θεμελιώδεις λειτουργίες του· (ii) να έχει ως αποτέλεσμα μείζονα ζημία στα στοιχεία του οργανισμού· (iii) να έχει ως αποτέλεσμα μείζονα οικονομική απώλεια· (iv) να αποτελέσει σε σφοδρή ή καταστροφική ζημία ατόμων που μπορεί να προϋποθέτει απώλεια ζωής ή σοβαρό, απειλητικό για τη ζωή τραυματισμό.

Κάθε σύστημα θα πρέπει να προστατεύεται βάσει του πιθανού αντίκτυπου που αυτό θα έχει, στην απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Τα μέτρα προστασίας (γνωστά και ως *security controls*) διαχωρίζονται σε δύο κατηγορίες. Πρώτα θα πρέπει να επιλυθούν οι αδυναμίες ασφάλειας στο σύστημα. Για παράδειγμα, εάν ένα σύστημα έχει μία γνωστή ευπάθεια που θα μπορούσαν να εκμεταλλευτούν κάποιοι επιτιθέμενοι χρήστες, το σύστημα θα πρέπει να επιδιορθωθεί έτσι ώστε αυτή η ευπάθεια να εξαλειφθεί ή να μετριαστεί. Κατόπιν, το σύστημα θα πρέπει να προσφέρει την απαιτούμενη λειτουργία στον κάθε εξουσιοδοτημένο χρήστη, έτσι ώστε κανείς να μη χρησιμοποιήσει λειτουργίες που δεν είναι απαραίτητες. Αυτή η αρχή είναι γνωστή ως *ελάχιστο προνόμιο* (least privilege). Η περιορισμένη λειτουργία και η επίλυση των αδυναμιών ασφάλειας έχουν ένα κοινό στόχο: να δίνουν στους επιτιθέμενους χρήστες όσο το δυνατόν λιγότερες ευκαιρίες να παραβιάσουν ένα σύστημα.

Αν και κάθε σύστημα θα πρέπει να είναι φτιαγμένο ιδανικά για να είναι όσο το δυνατόν ασφαλέστερο, αυτό γενικά δεν είναι εφικτό επειδή το σύστημα πρέπει να καλύπτει τις λειτουργικές απαιτήσεις των χρηστών του. Ένα άλλο κοινό πρόβλημα με τα μέτρα ασφάλειας είναι ότι συχνά καθιστούν τα συστήματα λιγότερο κατάλληλα ή δυσκολότερα στο

να χρησιμοποιηθούν. Όταν η χρηστικότητα είναι ζήτημα, πολλοί χρήστες θα προσπαθήσουν να παρακάμψουν τα μέτρα ασφάλειας· για παράδειγμα, εάν οι κωδικοί πρόσβασης θα πρέπει να είναι μεγάλοι και σύνθετοι, οι χρήστες μπορεί να τους καταγράψουν. Η εξισορρόπηση της ασφάλειας, της λειτουργικότητας, και της χρηστικότητας είναι συχνά μια πρόκληση.

Μια άλλη θεμελιώδης αρχή είναι η χρησιμοποίηση πολλαπλών στρωμάτων ασφάλειας. Για παράδειγμα, ένα host σύστημα μπορεί να προστατευθεί από την εξωτερική επίθεση με διάφορα μέτρα, συμπεριλαμβανομένου κάποιου τείχους προστασίας δικτύου, κάποιου host-based τείχους προστασίας και κάποιου patch λειτουργικού συστήματος. Το κίνητρο για την χρησιμοποίηση πολλαπλών στρωμάτων είναι ότι εάν ένα στρώμα αποτύχει ή δεν μπορέσει να αντιδράσει σε μια ορισμένη απειλή, τα άλλα στρώματα μπορούν να αποτρέψουν μία επιτυχή παραβίαση του συστήματος. Ένας συνδυασμός network-based και host-based μέτρων είναι περισσότερο αποτελεσματικός στην παροχή συνεπούς προστασίας των συστημάτων.

Το NIST SP 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems*, προτείνει την ελάχιστη βασική διαχείριση και τους ελάχιστους λειτουργικούς και τεχνικούς ελέγχους ασφάλειας για τα πληροφοριακά συστήματα.[5] Αυτοί οι έλεγχοι είναι για να εφαρμοστούν βάσει των κατηγοριών ασφάλειας που προτείνονται από το FIPS 199, όπως προαναφέρθηκε σε αυτή την ενότητα. Αυτός ο οδηγός θα πρέπει να βοηθήσει τις αρχές να συναντήσουν τις βασικές προϋποθέσεις για τα Windows XP Professional συστήματα που θα αναπτυχθούν στα περιβάλλοντά τους.

2.3 Βασικά Μέτρα Ασφάλειας και Ανάλυση Απειλών

Για την ασφάλεια ενός συστήματος, είναι βασικό να καθοριστούν πρώτα οι απειλές που πρέπει να μετριαστούν. Η γνώση των απειλών είναι επίσης το κλειδί στην κατανόηση των λόγων που πρέπει να πραγματοποιηθούν διάφορες ρυθμίσεις. Οι περισσότερες απειλές ενάντια στα δεδομένα και τους πόρους του συστήματος υφίστανται, είτε λόγω λάθους, είτε λόγω ύπαρξης πιθανών bugs στο λειτουργικό σύστημα και εφαρμογών λογισμικού που δημιουργούν εκμεταλλεύσιμα τρωτά σημεία, ή λάθη που γίνονται από χρήστες και διαχειριστές. Οι απειλές μπορεί να εμπλέκουν σκόπιμους δράστες (intentional actors) (πχ, ένας επιτιθέμενος που θέλει να προσπελάσει πιστωτικές κάρτες σε ένα σύστημα) ή τους ακούσιους δράστες (unintentional actors) (πχ, ένας διαχειριστής που ξεχνά να θέσει εκτός λειτουργίας τους λογαριασμούς χρήστη ενός υπαλλήλου που δεν υφίσταται πλέον στον οργανισμό). Οι απειλές μπορούν να είναι τόσο τοπικές, πχ, ένας δυσαρεστημένος υπάλληλος, όσο και απομακρυσμένες, όπως πχ, ένας επιτιθέμενος από μια άλλη χώρα. Οι ακόλουθες ενότητες περιγράφουν κάθε σημαντική κατηγορία απειλών, απαριθμούν τα πιθανά μέτρα ασφάλειας, παρέχουν παραδείγματα απειλών και συνοψίζουν τον πιθανό αντίκτυπο των απειλών. Ο κατάλογος των απειλών δεν είναι διεξοδικός· αντιπροσωπεύει απλά τις σημαντικότερες κατηγορίες απειλών που λήφθηκαν υπόψη κατά τη διάρκεια της επιλογής των μέτρων ασφάλειας όπως περιγράφονται σε αυτό τον οδηγό. Οι οργανισμοί θα πρέπει να διεξάγουν αποτιμήσεις κινδύνου για να αναγνωρίσουν τις συγκεκριμένες απειλές εναντίον των συστημάτων τους και να καθορίσουν την αποτελεσματικότητα των υπαρχόντων ελέγχων ασφάλειας που αντιδρούν στις απειλές και μετέπειτα να εκτελούν την

[5] Το NIST SP 800-53 Revision 2, που δημιουργήθηκε ως απάντηση στο FISMA, είναι διαθέσιμο εδώ: http://csrc.nist.gov/publications/PubsSPs.html.

εξομάλυνση κινδύνου ώστε να αποφασίσουν ποια επιπρόσθετα μέτρα (εφόσον αυτά υπάρχουν) θα πρέπει να εφαρμοστούν.[6]

2.3.1 *Τοπικές Απειλές*

Οι τοπικές απειλές είτε απαιτούν τη φυσική πρόσβαση στο σύστημα είτε τη λογική πρόσβαση στο σύστημα (πχ, ένας λογαριασμός ενός εξουσιοδοτημένου χρήστη). Οι τοπικές απειλές ομαδοποιούνται σε τρεις κατηγορίες: διεργασία εκκίνησης (boot process), μη-εξουσιοδοτημένη τοπική πρόσβαση, και αναπροσαρμογή προνομίων.

Διεργασία εκκίνησης

- **Απειλή:** Ένας μη εξουσιοδοτημένος χρήστης εκκινεί έναν υπολογιστή από κάποιο τρίτο μέσο (πχ, από εξωτερικό δίσκο ή από κάποια Universal Serial Bus (USB) token συσκευή αποθήκευσης). Αυτό θα μπορούσε να επιτρέψει στον επιτιθέμενο για να παρακάμψει τα μέτρα ασφάλειας του λειτουργικού συστήματος (OS) και να έχει πρόσβαση σε πληροφορίες.

- **Παραδείγματα:**
  - Κάποιος υπάλληλος, ενώ ταξιδεύει, τοποθετεί σε λάθος μέρος ένα φορητό υπολογιστή και κάποιος που το αποκτά προσπαθεί να δει τί ευαίσθητα δεδομένα περιέχει.

  - Ένας δυσαρεστημένος υπάλληλος εκκινεί έναν υπολογιστή από τρίτο μέσο για να παρακάμψει κάποια μέτρα ασφάλειας, έτσι ώστε να πετύχει πρόσβαση σε ευαίσθητα αρχεία (πχ, απόρρητα, τοπικά αποθηκευμένα δεδομένα, τοπικό αρχείο κωδικού πρόσβασης).

- **Αντίκτυπος:** Μη-εξουσιοδοτημένα μέλη μπορούν να προκαλέσουν απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας.

- **Πιθανά Μέτρα:**
  - Εφαρμογή φυσικών μέτρων ασφάλειας (πχ, κλειδωμένες πόρτες, πρόσβαση μόνο με αναγνωριστικό μέσο) για τον περιορισμό της πρόσβασης στον εξοπλισμό.[7]

  - Ενεργοποίηση ενός δυνατού και δύσκολου να εικαστεί κωδικού εξουσιοδότησης για το Basic Input Output System (BIOS) και διαμόρφωση του BIOS ώστε να κάνει εκκίνηση μόνο από τον τοπικό δίσκο, αν υποθέσουμε πως το κουτί που περιέχει το λειτουργικό σύστημα και τα δεδομένα, είναι φυσικά ασφαλισμένα. Αυτό θα βοηθήσει στην προστασία των δεδομένων, εκτός και αν αφαιρεθεί ο δίσκος από τον υπολογιστή.

---

[6] Το NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, περιέχει καθοδήγηση για την εκτέλεση αποτίμησης και εξομάλυνσης κινδύνου. Είναι διαθέσιμο για καταφόρτωση εδώ: http://csrc.nist.gov/publications/PubsSPs.html.

[7] Οι οργανισμοί θα πρέπει να έχουν μία φυσική και περιβαλλοντική πολιτική προστασίας η οποία να περιέχει προδιαγραφές για παροχή επαρκούς φυσικής προστασίας για συστήματα και δίκτυα. Οι περισσότεροι τεχνικοί έλεγχοι μπορούν εύκολα να καταρριφθούν εάν δεν υφίσταται φυσική ασφάλεια.

- Ασφάλεια των τοπικών αρχείων μέσω κρυπτογράφησης για να αποτραπεί η πρόσβαση σε δεδομένα στην περίπτωση όπου το φυσικό μέσο τοποθετηθεί σε άλλο υπολογιστή.

Μη-εξουσιοδοτημένη Τοπική Πρόσβαση

- **Απειλή:** Κάποιο άτομο που δεν του επιτρέπεται η πρόσβαση σε ένα σύστημα επιτυγχάνει τοπική πρόσβαση σε αυτό.

- **Παραδείγματα:**
  - Ένας επισκέπτης σε μια επιχείρηση κάθεται σε έναν αφύλακτο υπολογιστή και συνδέεται μαντεύοντας ένα εύκολο και αδύναμο κωδικό πρόσβασης ενός λογαριασμού χρήστη.

  - Ένας πρώην υπάλληλος επιτυγχάνει τη φυσική πρόσβαση στις εγκαταστάσεις του οργανισμού και χρησιμοποιεί τα παλαιά στοιχεία του λογαριασμού του για να συνδεθεί και να αποκτήσει πρόσβαση στους πόρους της επιχείρησης.

- **Αντίκτυπος:** Επειδή ένα μη-εξουσιοδοτημένο πρόσωπο μπορεί να παριστάνει τον εξουσιοδοτημένο χρήστη, αυτό θα μπορούσε αποτελέσει την απώλεια εμπιστευτικότητας και ακεραιότητας· εάν ο χρήστης έχει δικαιώματα διαχείρισης, αυτό θα μπορούσε να προκαλέσει και την απώλεια διαθεσιμότητας.

- **Πιθανά Μέτρα:**
  - Απαίτηση έγκυρης επικύρωσης ονόματος χρήστη και κωδικού πρόσβασης προτού επιτραπεί οποιαδήποτε πρόσβαση στους πόρους του συστήματος και ενεργοποίηση της προστασίας οθόνης με απαιτούμενο κωδικό πρόσβασης. Αυτές οι ενέργειες βοηθούν στο να αποτρέψουν έναν επιτιθέμενο από να πλησιάσει έναν υπολογιστή και να αποκτήσει άμεση πρόσβαση.

  - Ενεργοποίηση ενός banner κατά την είσοδο στο σύστημα που να περιέχει προειδοποίηση των πιθανών νομικών συνεπειών κακόβουλης χρήσης.[8]

  - Εφαρμογή μίας πολιτικής που να ενθαρρύνει τη χρησιμοποίηση ισχυρότερων κωδικών πρόσβασης, έτσι ώστε είναι δυσκολότερο για έναν επιτιθέμενο να τους εικάσει.

  - Θα πρέπει να μην χρησιμοποιείται ή επαναχρησιμοποιείται ένας κοινός κωδικός πρόσβασης σε περισσότερους από ένα λογαριασμούς· για παράδειγμα ο κωδικός πρόσβασης για ένα προσωπικό λογαριασμό ηλεκτρονικού ταχυδρομείου δεν πρέπει να είναι ο ίδιος με αυτόν που χρησιμοποιείται για την πρόσβαση στο Windows XP host.

[8] Το Υπουργείο Δικαιοσύνης των Ηνωμένων Πολιτιών της Αμερικής, παρέχει δείγματα banner (shamples) στο Παράρτημα Α (Appendix A) του *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, που είναι διαθέσιμο στη διεύθυνση: http://www.cybercrime.gov/s&smanual2002.htm.

- Εδραίωση και ενθάρρυνση μίας πολιτικής που να ελέγχει τη διαγραφή των υπαλλήλων που αποχώρισαν και να προβαίνει στη άμεση απενεργοποίηση των λογαριασμών τους.

- Φυσική ασφάλεια των εξωτερικών συσκευών αποθήκευσης ή των μέσων όπως τα CD-ROMs, τα οποία περιέχουν τις πολύτιμες πληροφορίες. Ένα πρόσωπο που αποκτά πρόσβαση σε έναν χώρο εργασίας μπορεί να βρει ευκολότερο το να αποσπάσει εξωτερικά μέσα αποθήκευσης από να προσπαθήσει να αποκτήσει πρόσβαση σε ένα σύστημα σε επίπεδο χρήστη.

Αναπροσαρμογή Προνομίων

- **Απειλή:** Ένα εξουσιοδοτημένο πρόσωπο με κανονικά δικαιώματα επιπέδου χρήστη, αναπροσαρμόζει τα προνόμια του λογαριασμού του, για να επιτύχει πρόσβαση σε επίπεδο διαχειριστή.

- **Παραδείγματα:**
  - Ένας χρήστης εκμεταλλεύεται μια ευπάθεια σε μια υπηρεσία για να αποκτήσει δικαιώματα διαχειριστή και να έχει πρόσβαση σε αρχεία κάποιου άλλου χρήστη.

  - Ένας χρήστης μαντεύει τον κωδικό πρόσβασης για ένα λογαριασμό επιπέδου διαχειριστή, επιτυγχάνει πλήρη πρόσβαση στο σύστημα, και θέτει εκτός λειτουργίας διάφορα μέτρα ασφάλειας.

- **Αντίκτυπος:** Επειδή ο χρήστης αποκτά πλήρη δικαιώματα στο σύστημα, μπορεί να προκληθεί απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας.

- **Πιθανά Μέτρα:**
  - Περιορισμένη πρόσβαση σε όλους τους λογαριασμούς επιπέδου διαχειριστή και των εργαλείων διαχείρισης, στα αρχεία διαμόρφωσης και στις ρυθμίσεις. Χρησιμοποίηση ισχυρών, δύσκολων να εικαστούν κωδικών πρόσβασης σε όλους τους λογαριασμούς επιπέδου διαχειριστή.[9] Μη χρησιμοποίηση των λογαριασμών διαχειριστή τομέα από client τερματικά που δεν έχουν δικαιώματα διαχείρισης. Αυτές οι ενέργειες θα καταστήσουν δυσκολότερο για τους χρήστες το να προβούν σε αναπροσαρμογή των προνομίων τους.

  - Απενεργοποίηση των αχρησιμοποίητων τοπικών υπηρεσιών. Ευπάθειες σε αυτές τις υπηρεσίες μπορούν να επιτρέψουν στους χρήστες να αναπροσαρμόσουν τα προνόμιά τους.

  - Εγκατάσταση ενημερώσεων στις εφαρμογές και στο OS (πχ, hotfixes, service packs, patches). Αυτές οι ενημερώσεις επιλύουν ευπάθειες συστημάτων μειώνοντας τον αριθμό των μέσων επίθεσης που μπορούν να χρησιμοποιηθούν.

[9] NIST SP 800-63, Electronic Authentication Guideline, contains additional information on password strength. Είναι διαθέσιμο για καταφόρτωση εδώ: http://csrc.nist.gov/publications/PubsSPs.html.

- Κρυπτογράφηση των ευαίσθητων δεδομένων. Ακόμα και με πρόσβαση επιπέδου διαχειριστή να μην είναι δυνατή η πρόσβαση σε κρυπτογραφημένα αρχεία από το χρήστη.

2.3.2 *Απομακρυσμένες Απειλές*

Αντίθετα από τις τοπικές απειλές, οι απομακρυσμένες απειλές δεν απαιτούν φυσική ή λογική πρόσβαση στο σύστημα. Οι κατηγορίες απομακρυσμένων απειλών που περιγράφονται σε αυτό το κεφάλαιο είναι οι υπηρεσίες δικτύου, η γνωστοποίηση δεδομένων, και τα κακόβουλα ωφέλιμα φορτία (malicious payloads).

Υπηρεσίες Δικτύου

- **Απειλή:** Απομακρυσμένα επιτιθέμενοι χρήστες εκμεταλλεύονται μία ευπαθή υπηρεσία δικτύου στο σύστημα. Αυτό συνεπάγεται τη μη-εξουσιοδοτημένη πρόσβαση σε υπηρεσίες και δεδομένα και το αποτέλεσμα της κατάστασης άρνησης υπηρεσίας (Denial of Service [DoS] condition).

- **Παραδείγματα:**
  - Ένα worm ψάχνει για συστήματα που έχουν κάποια ανασφάλιστη υπηρεσία που ακούει σε μία συγκεκριμένη πόρτα και έπειτα χρησιμοποιεί την υπηρεσία αυτή για να κερδίσει τον πλήρη έλεγχο του συστήματος.

  - Κάποιος επιτιθέμενος χρήστης επιτυγχάνει να έχει τον πλήρη έλεγχο του συστήματος μέσω μίας υπηρεσίας η οποία δεν απαιτούσε έλεγχο ταυτότητας.

  - Κάποιος επιτιθέμενος χρήστης προσποιείται έναν εξουσιοδοτημένο χρήστη εκμεταλλευόμενος ένα ανίσχυρο πρωτόκολλο απομακρυσμένης πρόσβασης.

- **Αντίκτυπος:** Εξαρτημένου του τύπου της υπηρεσίας δικτύου που εκμεταλλεύεται, μπορεί να προκληθεί απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας.

- **Πιθανά Μέτρα:**
  - Απενεργοποίηση υπηρεσιών που δεν χρησιμοποιούνται. Αυτό δίνει στους κακόβουλους χρήστες λιγότερες πιθανότητες να παραβιάσουν το σύστημα.

  - Δοκιμή και εγκατάσταση ενημερώσεων λογισμικού και λειτουργικού (πχ hotfixes, service packs, patches). Αυτές οι ενημερώσεις μπορούν να επιλύσουν ευπάθειες λογισμικού του συστήματος μειώνοντας τον αριθμό των μέσων επίθεσης που θα μπορούσαν να χρησιμοποιηθούν.

  - Απαίτηση επικύρωσης στοιχείων προτού επιτραπεί η πρόσβαση σε κάποια υπηρεσία. Εφαρμογή μίας πολιτικής που να ενθαρρύνει τη χρησιμοποίηση ισχυρότερων κωδικών πρόσβασης, έτσι ώστε είναι δυσκολότερο για έναν επιτιθέμενο να τους εικάσει. Εδραίωση και ενθάρρυνση μίας πολιτικής που να ελέγχει τη διαγραφή των υπαλλήλων που αποχώρισαν και να προβαίνει στη άμεση απενεργοποίηση των λογαριασμών τους. Αυτές οι ενέργειες βοηθούν να εξασφαλιστεί ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση σε κάθε υπηρεσία.

- Δεν θα πρέπει να χρησιμοποιούνται αδύναμες εφαρμογές και πρωτόκολλα απομακρυσμένης πρόσβασης· αντί αυτών θα πρέπει να χρησιμοποιούνται μόνο πρότυπα, κοινώς αποδεκτά ισχυρά πρωτόκολλα (πχ, Internet Protocol Security [Ipsec], Secure Shell [SSH], Transport Layer Security [TLS]) για την απομακρυσμένη πρόσβαση και συντήρηση των συστημάτων.

- Χρησιμοποίηση των τειχών προστασίας (firewalls) ή των φίλτρων μεταφερόμενων πακέτων για να υπάρχει πρόσβαση σε κάθε υπηρεσία αυστηρά και μόνο από εξουσιοδοτημένα τερματικά. Αυτό αποτρέπει τα μη-εξουσιοδοτημένα τερματικά από το να πετυχαίνουν πρόσβαση σε υπηρεσίες και επιπλέον αποτρέπει τα worms από το να εξαπλωθούν από το ένα τερματικό στο άλλο.

- Ενεργοποίηση κάποιου banner κατά την είσοδο στο σύστημα που να περιέχει προειδοποίηση των πιθανών νομικών συνεπειών κακόβουλης χρήσης.

Γνωστοποίηση Δεδομένων

- **Απειλή:** Κάποιο τρίτο πρόσωπο αποσπά απόρρητα δεδομένα που στάλθηκαν πάνω σε ένα δίκτυο.

- **Παραδείγματα:**
  - Σε ένα δίκτυο που δεν χρησιμοποιεί switch, ένα τρίτο πρόσωπο χρησιμοποιεί ένα εργαλείο παρακολούθησης δικτύου. Όταν ένας νόμιμος χρήστης μεταδίδει κάποιο αρχείο με ανασφαλή τρόπο, το τρίτο πρόσωπο υποκλέπτει το αρχείο και εισβάλει στα δεδομένα του.

  - Ένας επιτιθέμενος χρήστης αποσπά ονόματα χρηστών και κωδικούς ασφάλειας που στάλθηκαν από ένα αρχικό κείμενο (plaintext) πάνω σε κάποιο τμήμα ενός δικτύου.

- **Αντίκτυπος:** Η υποκλοπή δεδομένων μπορεί να οδηγήσει σε απώλεια εμπιστευτικότητας. Εάν υποκλαπούν δεδομένα πιστοποίησης (πχ, passwords) μπορεί να προκληθεί η απώλεια εμπιστευτικότητας και ακεραιότητας και πιθανά η απώλεια διαθεσιμότητας, σε περίπτωση που τα δεδομένα πιστοποίησης που έχουν υποκλαπεί έχουν προνόμια σε επίπεδο διαχείρισης.

- **Πιθανά Μέτρα:**
  - Χρησιμοποίηση δικτύων με switches που καθιστά δυσκολότερη την παρακολούθηση πακέτων (packet sniffing).

  - Χρησιμοποίηση ασφαλούς συστήματος ταυτοποίησης και πιστοποίησης χρηστών, όπως το NT LanManager version 2 (NTLMv2) ή το Kerberos.

  - Κρυπτογράφηση των επικοινωνιών δικτύου ή των δεδομένων των εφαρμογών μέσω της χρησιμοποίησης διαφόρων πρωτοκόλλων (πχ TLS, Ipsec SSH). Έτσι προστατεύονται τα δεδομένα και δεν καθίσταται δυνατή η προσπέλασή τους από τρίτους.

Κακόβουλα Ωφέλιμα Φορτία (Malicious Payloads)

- **Απειλή:** Τα κακόβουλα ωφέλιμα φορτία όπως ιοί, worms, Trojan horses και ενεργό περιεχόμενο (active content) επιτίθενται με πολλά μέσα επίθεσης. Τερματικοί χρήστες του συστήματος πυροδοτούν κακόβουλα ωφέλιμα φορτία.

- **Παραδείγματα:**
  - Κάποιος χρήστης επισκέπτεται μία ιστοσελίδα στο διαδίκτυο και κατεβάζει ένα παιχνίδι που εμπεριέχει ένα Trojan horse. Όταν ο χρήστης εγκαθιστά το παιχνίδι στον υπολογιστή, μαζί του εγκαθίσταται και το Trojan horse το οποίο εκθέτει το σύστημα.

  - Κάποιος χρήστης με δικαιώματα επιπέδου διαχείρισης περιηγείται στο διαδίκτυο και κατά λάθος επισκέπτεται μία κακόβουλη ιστοσελίδα η οποία καταφέρνει να μολύνει το σύστημα.

  - Κάποιος χρήστης εγκαθιστά και χειρίζεται ένα peer-to-peer (P2P) λογισμικό διαμοιρασμού αρχείων για να κατεβάσει μουσική και το λογισμικό αυτό εγκαθιστά μία εφαρμογή spyware στο σύστημα.

  - Κάποιος χρήστης ανοίγει και εκτελεί ένα ωφέλιμο φορτίο που ήταν συνηγμένο σε κάποιο spam μήνυμα, ή μήνυμα εξαπάτησης.

- **Αντίκτυπος:** Το κακόβουλο λογισμικό συχνά κερδίζει πλήρη δικαιώματα σε επίπεδο διαχείρισης στο σύστημα, ή αθέλητα καταρρίπτει το σύστημα. Το κακόβουλο λογισμικό μπορεί να επιφέρει απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας.

- **Πιθανά Μέτρα:**
  - Λειτουργία του συστήματος σε καθημερινή βάση χρησιμοποιώντας περιορισμένο λογαριασμό χρήστη. Χρησιμοποίηση λογαριασμών επιπέδου διαχειριστή μόνο όταν είναι αναγκαίο για συγκεκριμένες εργασίες συντήρησης. Πολλά στιγμιότυπα malware δεν μπορούν να μολύνουν κάποιο σύστημα εκτός εάν ο τρέχον χρήστης έχει προνόμια διαχειριστή.

  - Εκπαίδευση των χρηστών για αποφυγή μολύνσεων από κακόβουλο λογισμικό, και γνωστοποίηση προς αυτούς μιας τοπικής πολιτικής που αφορά τη χρήση δυνητικών μεθόδων μετάδοσης όπως λογισμικό άμεσης ανταλλαγής μηνυμάτων (instant messaging [IM]) και P2P υπηρεσιών διαμοιρασμού αρχείων. Χρήστες που είναι εξοικειωμένοι με τις τεχνικές εξάπλωσης κακόβουλου λογισμικού θα είναι λιγότερο πιθανό να μολύνουν τα συστήματά τους.

  - Χρησιμοποίηση αντιβιοτικών προγραμμάτων και εφαρμογών εντοπισμού spyware καθώς και removal utilities, ως αυτοματοποιημένο τρόπο προστασίας από μολύνσεις και ανίχνευσης των μολύνσεων που δεν εμποδίστηκαν.

  - Χρησιμοποίηση clients ηλεκτρονικού ταχυδρομείου οι οποίοι υποστηρίζουν φίλτρα για spam μηνύματα – να παρέχει αυτοματοποιημένη διαδικασία ανίχνευσης και να θέτει σε καραντίνα τα μηνύματα που αναγνωρίζονται ως spam ή έχουν τα ίδια χαρακτηριστικά όπως αυτά ενός τυπικού spam.

- Δεν θα πρέπει να εγκαθίστανται ή να χρησιμοποιούνται μη εγκεκριμένες εφαρμογές (πχ, P2P, IM) και να συνδέονται σε άγνωστους εξυπηρετητές. Επιμόρφωση των χρηστών όσον αφορά το πιθανό αντίκτυπο που προκαλείται με τη χρήση των P2P, IM και άλλων μη έμπιστων εφαρμογών λογισμικού.

- Ρύθμιση του λογισμικού των server και client, όπως servers και clients ηλεκτρονικού ταχυδρομείου, Web proxy servers και clients και τις εφαρμογές παραγωγικότητας, έτσι ώστε να περιοριστεί η έκθεση σε malware. Για παράδειγμα, servers και clients ηλεκτρονικού ταχυδρομείου θα πρέπει να ρυθμίζονται έτσι ώστε να εμποδίζουν στην ηλεκτρονική αλληλογραφία τα επισυναπτόμενα αρχεία με συγκεκριμένη κατάληξη. Αυτό μπορεί να βοηθήσει στον περιορισμό της πιθανότητας μολύνσεων των συστημάτων.

- Ρύθμιση των συστημάτων, ιδιαιτέρως των SSLF περιβαλλόντων, έτσι ώστε οι εκ προεπιλογής συνάφειες αρχείων (file association) να εμποδίζουν την αυτόματη εκτέλεση αρχείων ενεργού περιεχομένου (πχ, Java, JavaScript, ActiveX).

Αυτή η ενότητα περιέγραψε διάφορους τύπους τοπικών και απομακρυσμένων απειλών οι οποίες μπορούν να επιδράσουν αρνητικά στα συστήματα. Τα πιθανά μέτρα που απαριθμήθηκαν για τις απειλές είναι κυρίως τεχνικά, όπως και τα μέτρα που συζητήθηκαν σε όλο το έγγραφο. Ωστόσο, είναι σημαντικό για τον επιπλέον περιορισμό των κινδύνων λειτουργίας κάποιου Windows XP συστήματος χρησιμοποιώντας επίσης διοικητικούς και λειτουργικούς ελέγχους. Παραδείγματα σημαντικών λειτουργικών ελέγχων είναι ο περιορισμός της φυσικής πρόσβασης σε κάποιο σύστημα· η εκτέλεση σχεδιασμού ενδεχόμενων περιστατικών· [10] η δημιουργία backup των συστημάτων, η αποθήκευση των backups σε αξιόπιστη και ασφαλής τοποθεσία και η τακτική δοκιμή των backups· και η επίβλεψη των Microsoft mailing lists για σχετικές ανακοινώσεις ασφάλειας. Οι διοικητικοί έλεγχοι μπορούν να περιέχουν την ανάπτυξη πολιτικών όσον αφορά την ασφάλεια των Windows XP συστημάτων και τη δημιουργία πλάνου για τη συντήρηση των Windows XP συστημάτων. Επιλέγοντας και εφαρμόζοντας διοικητικούς, λειτουργικούς και τεχνικούς ελέγχους για τα Windows XP, οι οργανισμοί μπορούν να εξομαλύνουν καλύτερα τις απειλές που μπορούν να αντιμετωπίσουν τα Windows XP συστήματα.

Ένας άλλος λόγος για τη χρησιμοποίηση πολλαπλών τύπων ελέγχων είναι για να παρέχουμε καλύτερη ασφάλεια σε καταστάσεις όπου ένας ή περισσότεροι έλεγχοι μπορούν να καταστρατηγηθούν ή αλλιώς να παραβιαστούν. Αυτό μπορεί να γίνει όχι μόνο από επιτιθέμενους, αλλά επίσης από εξουσιοδοτημένους χρήστες χωρίς κακόβουλη πρόθεση. Για παράδειγμα, καταγράφοντας μία λίστα κωδικών σε μία οθόνη για ευκολία μπορεί να οδηγήσει στην κατάργηση των ελέγχων που σχεδιάστηκαν να εμποδίζουν μη-εξουσιοδοτημένη τοπική πρόσβαση σε αυτό το σύστημα. Η εγκαθίδρυση μίας πολιτικής ενάντια στην καταγραφή κωδικών (διοικητικός έλεγχος), η επιμόρφωση των χρηστών σχετικά με τους κινδύνους της έκθεσης κωδικών (λειτουργικός έλεγχος) και η εκτέλεση περιοδικών φυσικών ελέγχων για αναγνώριση κοινοποιημένων κωδικών (λειτουργικός έλεγχος), μπορούν να είναι όλα χρήσιμα στον περιορισμό των κινδύνων που εγκυμονεί η καταγραφή των κωδικών. Οι τεχνικοί έλεγχοι μπορούν επίσης να είναι χρήσιμοι, όπως η

[10] Για περισσότερες πληροφορίες αναφορικά με το σχεδιασμό ενδεχόμενων περιστατικών (contingency planning), αναφερθείτε στο NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, που είναι διαθέσιμο εδώ: http://csrc.nist.gov/publications/PubsSPs.html.

χρησιμοποίηση έξυπνων καρτών (smart cards) ή κάποια άλλη μέθοδο άλλη από την χρησιμοποίηση κωδικών για την πιστοποίηση συστημάτων.

2.4 Τεκμηρίωση Περιβαλλόντων και Ελέγχων Ασφάλειας

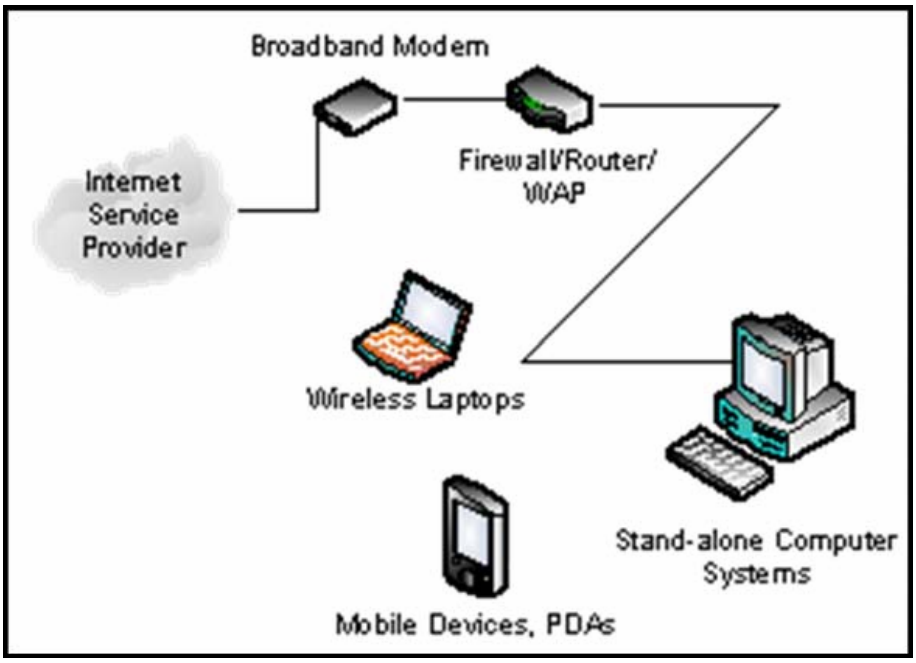
Αυτή η ενότητα περιγράφει τους τύπους των περιβαλλόντων στα οποία κάποιο Windows XP host μπορεί να αναπτυχθεί – SOHO, enterprise και προσαρμοσμένο – όπως περιγράφεται στο National Checklist Program του NIST.[11] Τα τρία τυπικά προσαρμοσμένα περιβάλλοντα για τα Windows XP είναι το ειδικής ασφάλειας-περιορισμένης λειτουργικότητας (specialized security-limited functionality), το οποίο είναι για συστήματα με υψηλό κίνδυνο επιθέσεων ή έκθεσης δεδομένων, με την ασφάλειας να έχει προτεραιότητα έναντι της λειτουργικότητας· το κληροδοτημένο (legacy) το οποίο είναι προορισμένο για καταστάσεις στις οποίες το Windows XP σύστημα έχει ιδιαίτερες ανάγκες οι οποίες δεν ταιριάζουν στα άλλα προφίλ, όπως η απαίτηση για συμβατότητα προς τα πίσω (backward compatibility) με συμβατές (legacy) εφαρμογές ή εξυπηρετητές· και το Federal Desktop Core Configuration (FDCC), το οποίο είναι για συστήματα που χρειάζονται να είναι ασφαλισμένα χρησιμοποιώντας μία διαμόρφωση ασφάλειας σύμφωνα με εντολή του OMB, γνωστό ως FDCC.[12] Η κάθε περιγραφή του περιβάλλοντος συνοψίζει επίσης τις θεμελιώδης απειλές και ελέγχους όπου είναι τυπικά μέρη του περιβάλλοντος. Επιπρόσθετα στην τεκμηρίωση των ελέγχων, το κάθε περιβάλλον θα πρέπει να έχει και διάφορες άλλες τεκμηριώσεις σχετικές με την ασφάλεια, όπως την αποδεκτή χρησιμοποίηση πολιτικών και τις κατάλληλες ενημερώσεις ασφάλειας, που επηρεάζουν τη διαμόρφωση και τη χρήση των συστημάτων και των εφαρμογών. Το τελευταίο μέρος αυτής της ενότητας απαριθμεί μερικούς κοινούς τύπους τεκμηρίωσης σχετικούς με την ασφάλεια.

2.4.1 *SOHO*

Το SOHO, που ορισμένες φορές ονομάζεται standalone, περιγράφει μικρές, ανεπίσημες εγκαταστάσεις που χρησιμοποιούνται για σκοπούς σπιτιού ή επιχείρησης. Το SOHO περικλείει μία ποικιλία από μικρής κλίμακας περιβάλλοντα και συσκευές, που εκτείνονται από φορητούς υπολογιστές, φορητές συσκευές και υπολογιστές σπιτιού, μέχρι τηλεπικοινωνιακά συστήματα που βρίσκονται σε broadband δίκτυα, σε μικρές επιχειρήσεις και μικρά υποκαταστήματα μιας επιχείρησης. Η Εικόνα 2-2 δείχνει μία τυπική αρχιτεκτονική δικτύου για το SOHO. Ιστορικά τα SOHO περιβάλλοντα είναι τα λιγότερο ασφαλισμένα και τα περισσότερο έμπιστα. Γενικά, τα άτομα που εκτελούν SOHO διαχείριση συστήματος είναι τα λιγότερο ενημερωμένα και με τις λιγότερες γνώσεις σχετικά με την ασφάλεια. Αυτό συχνά αποτελεί στο να είναι τα περιβάλλοντα λιγότερο ασφαλή απ' ότι χρειάζονται επειδή η εστίαση είναι γενικά στη λειτουργικότητα και στην ευκολία της χρήσης τους. Ένα σύστημα SOHO μπορεί να μη χρησιμοποιεί κανένα λογισμικό ασφάλειας (πχ, λογισμικό antivirus, προσωπικό τείχος προστασίας). Σε ορισμένες περιπτώσεις, δεν υπάρχουν έλεγχοι βάσει δικτύου όπως τείχη προστασίας, έτσι τα SOHO συστήματα μπορεί να είναι άμεσα εκτιθέμενα σε εξωτερικές επιθέσεις. Συνεπώς, τα SOHO περιβάλλοντα είναι συχνά στο στόχαστρο εκμετάλλευσης – όχι απαραίτητα για την απόκτηση πληροφοριών, αλλά περισσότερο συχνά για να χρησιμοποιηθούν για την επίθεση σε άλλους υπολογιστές, ή τυχαία ως παράπλευρη ζημιά για την διάδοση κάποιου worm.

---

[11] Περισσότερες πληροφορίες για αυτό το project είναι διαθέσιμες στη διεύθυνση http://checklists.nist.gov/.
[12] Περισσότερα θα βρείτε στη διεύθυνση http://fcw.com/articles/2008/01/25/omb-stresses-fdcc-compliance-means-100-percent.aspx.



Εικόνα 2-2. Η Τυπική Αρχιτεκτονική Δικτύου SOHO.

Επειδή οι βασικές απειλές στα περιβάλλοντα SOHO είναι εξωτερικές και οι SOHO υπολογιστές έχουν γενικά λιγότερο περιοριστικές πολιτικές απ' ότι οι enterprise ή οι specialized security-limited functionality υπολογιστές, τείνουν να είναι περισσότερο τρωτοί σε επιθέσεις από τις κατηγορίες των απομακρυσμένων απειλών. (Αν και οι απομακρυσμένες απειλές είναι η κύρια ανησυχία για τα SOHO περιβάλλοντα, είναι εξίσου σημαντική η προστασία ενάντια σε άλλες απειλές.) Τα SOHO συστήματα απειλούνται κυρίως από επιθέσεις ενάντια σε υπηρεσίες δικτύου και από τα κακόβουλα ωφέλιμα φορτία (πχ, ιοί, worms). Αυτές οι επιθέσεις είναι οι πιο πιθανές για να επηρεάσουν τη διαθεσιμότητα (πχ, κατάρριψη του συστήματος, κατανάλωση ολόκληρου του εύρους ζώνης του δικτύου, διακοπή της λειτουργικότητας) αλλά μπορούν επίσης να επηρεάσουν την ακεραιότητα (πχ, μόλυνση αρχείων δεδομένων) και της εμπιστευτικότητας (πχ, παροχή απομακρυσμένης πρόσβασης σε ευαίσθητα δεδομένα, αποστολή αρχείων δεδομένων σε τρίτους σε μορφή ηλεκτρονικής αλληλογραφίας).

Η ασφάλεια SOHO βελτιώνεται με την εξάπλωση μικρών, φθηνών, hardware-based τείχη προστασίας δρομολογητές (firewall routers) τα οποία προστατεύουν σε κάποιο βαθμό τα SOHO μηχανήματα που έχουν πίσω τους. Η υιοθεσία προσωπικών τειχών προστασίας επίσης βοηθάει στην καλύτερη ασφάλεια των SOHO περιβαλλόντων. Ακόμα ένα κλειδί στην ασφάλεια του SOHO είναι η ισχυροποίηση των hosts πάνω στο SOHO δίκτυο καλύπτοντας τις ευπάθειες και αλλάζοντας τις ρυθμίσεις για να περιοριστεί η άσκοπη λειτουργικότητα.

2.4.2 *Enterprise*

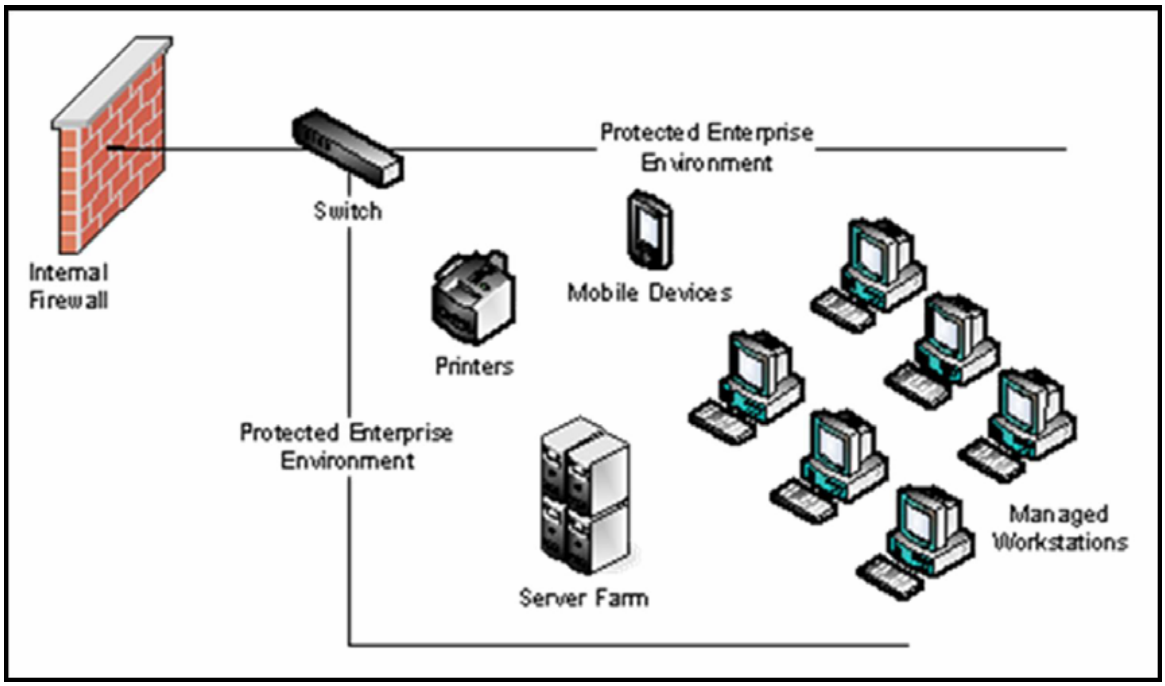
Το περιβάλλον enterprise, επίσης γνωστό και ως managed (διοικούμενο), αποτελείται κυρίως από μεγάλα οργανωτικά συστήματα με καθορισμένες, οργανωμένες σουίτες διαμορφώσεων hardware και software, που αποτελούνται συνήθως από κεντρικά διοικούμενους σταθμούς εργασίας και εξυπηρετητές, που προστατεύονται από απειλές στο διαδίκτυο με τείχη

προστασίας και άλλες συσκευές ασφάλειας δικτύου. Η Εικόνα 2-3 δείχνει μία τυπική αρχιτεκτονική δικτύου του enterprise. Τα enterprise περιβάλλοντα έχουν γενικά μία ομάδα αφιερωμένη στην υποστήριξη χρηστών και στην παροχή ασφάλειας. Ο συνδυασμός δομής και έμπειρου προσωπικού επιτρέπει την εφαρμογή καλύτερων πρακτικών ασφάλειας κατά τη διάρκεια της αρχικής εφαρμογής του συστήματος και στην μετέπειτα υποστήριξη και συντήρηση. Οι enterprise εγκαταστάσεις συνήθως χρησιμοποιούν ένα μοντέλο τομέα για την αποτελεσματική διοίκηση μίας πληθώρας ρυθμίσεων και επιτρέπουν τον διαμοιρασμό των πηγών (πχ, εξυπηρετητές αρχείων, εκτυπωτές). Το enterprise μπορεί να ενεργοποιήσει μόνο τις υπηρεσίες που χρειάζονται για τις συνήθεις λειτουργίες της επιχείρησης, με τις άλλες πιθανές οδούς εκμετάλλευσης εξαλειμμένες ή απενεργοποιημένες. Η διοίκηση πιστοποίησης, λογαριασμού και πολιτικής μπορεί να διαχειριστεί κεντρικά για τη διατήρηση συνεχούς στάσης ασφάλειας δια μήκους ενός οργανισμού.

Το περιβάλλον enterprise είναι περισσότερο περιοριστικό και παρέχει λιγότερη λειτουργικότητα απ’ ότι το περιβάλλον SOHO. Τα διοικούμενα περιβάλλοντα συνήθως έχουν καλύτερο έλεγχο στη ροή διάφορων τύπων κίνησης, όπως η φίλτρανση του δικτύου βάσει πρωτοκόλλων και πορτών των συνδέσεων του enterprise με εξωτερικά δίκτυα. Εξαιτίας της υποστηρικτικής και σε μεγάλο βαθμό ομοιογενούς φύσης του περιβάλλοντος enterprise, είναι συνήθως ευκολότερη η χρησιμοποίηση περισσότερων περιοριστικών ρυθμίσεων λειτουργικότητας από όσες έχουν τα SOHO περιβάλλοντα. Τα περιβάλλοντα enterprise επίσης τείνουν να εφαρμόζουν διάφορα στρώματα άμυνας (πχ, firewalls, antivirus severs, συστήματα εντοπισμού εισβολών, συστήματα patch management, φίλτρανση ηλεκτρονικής αλληλογραφίας), τα οποία παρέχουν μεγαλύτερη προστασία για τα συστήματα. Σε πολλά enterprise περιβάλλοντα, η διαλειτουργικότητα με τα συστήματα legacy μπορεί να μην είναι σημαντική απαίτηση, διευκολύνοντας περαιτέρω τη χρήση περισσότερο περιοριστικών ρυθμίσεων. Σε κάποιο enterprise περιβάλλον, αυτός ο οδηγός θα πρέπει να χρησιμοποιηθεί από προχωρημένους χρήστες και διαχειριστές συστημάτων. Οι ρυθμίσεις του περιβάλλοντος enterprise ανταποκρίνονται σε μία επιχειρησιακή θέση ασφάλειας η οποία θα προστατέψει τις πληροφορίες σε ένα περιβάλλον μέτριας επικινδυνότητας.

Στο περιβάλλον enterprise τα συστήματα είναι συνήθως ευπαθή σε τοπικές και απομακρυσμένες απειλές. Για την ακρίβεια, οι απειλές συχνά περικλείουν όλες τις κατηγορίες που έχουν περιγραφεί στην ενότητα 2.3**.** Οι τοπικές απειλές, όπως είναι η μη-εξουσιοδοτημένη χρήση από ένα σταθμό εργασίας κάποιου άλλου χρήστη, συχνά οδηγεί σε απώλεια εμπιστευτικότητας (πχ, μη-εξουσιοδοτημένη πρόσβαση σε δεδομένα), αλλά μπορεί επίσης να οδηγήσει σε απώλεια ακεραιότητας (πχ, τροποποίηση δεδομένων) ή διαθεσιμότητας (πχ, κλοπή ενός συστήματος). Οι απομακρυσμένες απειλές μπορούν να προταθούν όχι μόνο από επιτιθέμενους εκτός του οργανισμού, αλλά και από εσωτερικούς χρήστες οι οποίοι επιτίθενται σε άλλα εσωτερικά συστήματα κατά μήκους του δικτύου του οργανισμού. Οι περισσότερες τρύπες στην ασφάλεια δημιουργούνται από απομακρυσμένες απειλές οι οποίες εμπλέκουν κακόβουλα ωφέλιμα φορτία που αποστέλλονται από εξωτερικούς παράγοντες, όπως ιοί και worms που αποκτώνται μέσω ηλεκτρονικής αλληλογραφίας ή μολυσμένων ιστοσελίδων. Οι απειλές ενάντια στις υπηρεσίες δικτύου τείνουν να επηρεάζουν ένα μικρότερο αριθμό συστημάτων και μπορούν να προξενηθούν από εσωτερικούς ή εξωτερικούς παράγοντες. Τόσο τα κακόβουλα ωφέλιμα φορτία όσο και οι επιθέσεις υπηρεσιών δικτύου είναι πολύ πιθανό να επηρεάσουν τη διαθεσιμότητα (πχ, κατάρριψη του συστήματος, κατανάλωση ολόκληρου του εύρους ζώνης του δικτύου, διακοπή της λειτουργικότητας) αλλά μπορούν επίσης να επηρεάσουν την ακεραιότητα (πχ, μόλυνση αρχείων δεδομένων) και την εμπιστευτικότητα (πχ, παροχή απομακρυσμένης

πρόσβασης σε ευαίσθητα δεδομένα). Οι απειλές αποκάλυψης δεδομένων τείνουν να έρχονται από εσωτερικούς παράγοντες οι οποίοι επιβλέπουν την κίνηση στα τοπικά δίκτυα και επηρεάζουν κυρίως την εμπιστευτικότητα.



Εικόνα 2-3. Η Τυπική Αρχιτεκτονική Δικτύου Enterprise.

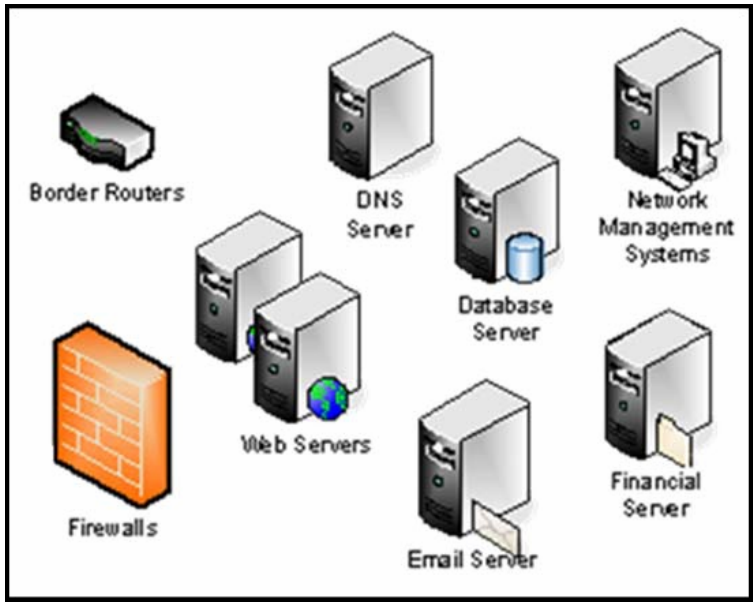
2.4.3 *Specialized Security-Limited Functionality (SSLF)*

Ένα περιβάλλον specialized security-limited functionality (SSLF) είναι οποιοδήποτε περιβάλλον, δικτυωμένο ή standalone, όπου βρίσκεται σε υψηλό κίνδυνο έκθεσης δεδομένων. Η Εικόνα 2-4 δείχνει παραδείγματα συστημάτων τα οποία βρίσκονται συχνά σε SSLF περιβάλλοντα, συμπεριλαμβανομένου εξωστρεφών, e-mail, και DNS servers και firewalls. Τυπικά, η παροχή επαρκούς ισχυρής προστασίας για αυτά τα συστήματα συνεπάγεται μία σημαντική μείωση στη λειτουργικότητά τους. Υποθέτει πως τα συστήματα έχουν περιορισμένη ή εξειδικευμένη λειτουργικότητα σε ένα υψηλά απειλητικό περιβάλλον, όπως είναι ένα εξωστρεφές firewall ή ένας δημόσιος Web server, ή των οποίων το περιεχόμενο των δεδομένων ή ο σκοπός της αποστολής τους είναι τέτοιας αξίας, που οι επιθετικές ανταλλαγές χάριν της ασφάλειας ξεπερνούν τις ενδεχόμενες αρνητικές συνέπειες σε βάρος χρήσιμων ιδιοτήτων συστημάτων, όπως συμβατές (legacy) εφαρμογές ή τη διαλειτουργικότητα με άλλα συστήματα. Το περιβάλλον SSLF περιλαμβάνει υπολογιστές οι οποίοι περιέχουν άκρως απόρρητες πληροφορίες (πχ, αρχείο προσωπικού, ιατρικά αρχεία, οικονομικές πληροφορίες) και εκτελούν οργανωτικές λειτουργίες ζωτικής σημασίας (πχ, λογιστικά, επεξεργασία μισθοδοσίας, έλεγχος εναέριας κυκλοφορίας). Αυτοί οι υπολογιστές μπορούν να βρίσκονται στο στόχαστρο από τρίτους για εκμετάλλευση, όμως μπορούν επίσης να βρίσκονται στο στόχαστρο έμπιστων παραγόντων εντός του οργανισμού.

Ένα SSLF περιβάλλον μπορεί να είναι υποσύνολο ενός SOHO ή ενός enterprise περιβάλλοντος. Για παράδειγμα, τρεις επιτραπέζιοι υπολογιστές σε κάποιο enterprise περιβάλλον οι οποίοι κρατούν εμπιστευτικά δεδομένα υπαλλήλων, μπορούν να θεωρηθούν ως ένα SSLF περιβάλλον μέσα σε ένα enterprise περιβάλλον. Επιπρόσθετα, ένας φορητός

υπολογιστής ο οποίος χρησιμοποιείται από έναν κινητό εργάτη μπορεί να είναι ένα SSLF περιβάλλον μέσα σε ένα SOHO περιβάλλον. Ένα SSLF περιβάλλον εκτός οποιουδήποτε περιβάλλοντος μπορεί να είναι ένα ανεξάρτητο περιβάλλον – για παράδειγμα, μια κυβερνητική εγκατάσταση ασφάλειας που έχει να κάνει με ευαίσθητα δεδομένα.

Τα συστήματα σε SSLF περιβάλλοντα αντιμετωπίζουν τις ίδιες απειλές με τα συστήματα σε enterprise περιβάλλοντα. Οι απειλές τόσο από εσωτερικούς όσο και από εξωτερικούς παράγοντες αποτελούν ανησυχία. Εξαιτίας των κινδύνων και των πιθανών συνεπειών μίας έκθεσης σε ένα SSLF περιβάλλον, αυτό έχει συνήθως την περισσότερο λειτουργική, περιοριστική και ασφαλή διαμόρφωση. Η προτεινόμενη διαμόρφωση είναι σύνθετη και παρέχει τη μέγιστη προστασία εις βάρους της ευκολίας χρήσης, της λειτουργικότητας και της απομακρυσμένης διαχείρισης συστήματος. Σε ένα SSLF περιβάλλον, αυτός ο οδηγός στοχεύει σε πεπειραμένους ειδικούς σε θέματα ασφάλειας και σε διαχειριστές συστημάτων οι οποίοι κατανοούν τον αντίκτυπο της εφαρμογής των αυστηρών αυτών απαιτήσεων.



Εικόνα 2-4. Παραδείγματα Συστημάτων Specialized Security-Limited Functionality.

2.4.4 *Legacy*

Ένα περιβάλλον legacy περιέχει παλαιότερα συστήματα ή εφαρμογές που χρησιμοποιούν απαρχαιωμένους μηχανισμούς επικοινωνίας. Αυτό συχνά συμβαίνει όταν οι μηχανές που λειτουργούν σε ένα περιβάλλον legacy χρειάζονται περισσότερο ελαστικές ρυθμίσεις έτσι ώστε να μπορούν να επικοινωνούν με τους απαραίτητους πόρους. Για παράδειγμα, ένα σύστημα μπορεί να χρειάζεται να χρησιμοποιήσει υπηρεσίες και εφαρμογές οι οποίες απαιτούν ανασφαλείς μηχανισμούς πιστοποίησης όπως συνεδριάσεις μηδενικού χρήστη (null user sessions) και ανοιχτοί αγωγοί (open pipes). Εξαιτίας αυτών των ειδικών αναγκών, το σύστημα δεν ταιριάζει σε κανένα από τα τυπικά περιβάλλοντα· συνεπώς, θα πρέπει να ταξινομηθεί ως ένα σύστημα περιβάλλοντος legacy. Τα περιβάλλοντα legacy μπορούν να υπάρχουν μέσα σε SOHO και enterprise περιβάλλοντα και σε σπάνιες περιπτώσεις εξίσου μέσα σε SSLF περιβάλλοντα. Εξαρτώμενης της κατάστασης, ένα legacy περιβάλλον μπορεί να αντιμετωπίσει οποιοδήποτε συνδυασμό από εσωτερικές και εξωτερικές απειλές. Ο

πιθανός αντίκτυπος των απειλών θα πρέπει να προσδιοριστεί λαμβάνοντας υπ' όψιν τις απειλές που αντιμετωπίζει το σύστημα (όπως έχουν περιγραφεί στις προηγούμενες τρεις ενότητες) και έπειτα να ληφθεί υπ' όψιν ο επιπλέον κίνδυνος που έχει το σύστημα εξαιτίας των legacy προσαρμογών.

2.4.5 *FDCC*

Το περιβάλλον Federal Desktop Core Configuration (FDCC) περιέχει συστήματα τα οποία χρειάζονται να είναι ασφαλισμένα χρησιμοποιώντας μία διαμόρφωση ασφάλειας σύμφωνα με εντολή του OMB, γνωστό ως FDCC.[13] Από το φθινόπωρο του 2008, υφίστανται οι διαμορφώσεις ασφάλειας του FDCC μόνο για συστήματα Windows XP Professional Service Pack 2 και Microsoft Windows Vista Enterprise Service Pack 1. Το Windows XP FDCC είναι βασισμένο στην προσαρμογή που πραγματοποιήθηκε από την Αεροπορία, των υποδείξεων αυτού του εγγράφου για το SSLF και στην προσαρμογή που πραγματοποιήθηκε από το Υπουργείο Άμυνας, των υποδείξεων του Οδηγού Ασφάλειας της Microsoft για το Internet Explorer 7.0. Η διαμόρφωση του FDCC είναι ευρύτερη από τις προηγούμενες διαμορφώσεις για τα Windows XP, ενσωματώνοντας ρυθμίσεις από το Internet Explorer, το Windows Firewall και άλλα χαρακτηριστικά λειτουργικού συστήματος που δεν εμπεριέχονταν σε προηγούμενες προσπάθειες διαμόρφωσης.[14]

Επειδή η FDCC διαμόρφωση των Windows XP προτίθεται να αναπτυχθεί κυρίως σε διαχειριζόμενα συστήματα, τα βασικά χαρακτηριστικά των enterprise περιβαλλόντων, όπως οι κύριες απειλές εναντίον των συστημάτων και η βασική τεχνική γραμμή των πρακτικών ασφάλειας για τα συστήματα, είναι επίσης βασικά χαρακτηριστικά των FDCC περιβαλλόντων.[15]

2.4.6 *Τεκμηρίωση Ασφάλειας*

Ένας οργανισμός τυπικά έχει πολλά έγγραφα σχετικά με την ασφάλεια των συστημάτων Windows XP. Πρωτίστως, ανάμεσα στα έγγραφα, είναι ο οδηγός διαμόρφωσης ασφάλειας των Windows XP ο οποίος καθορίζει πώς τα συστήματα Windows XP θα πρέπει να διαμορφώνονται και να ασφαλίζονται.[16] Όπως αναφέρθηκε στην Ενότητα 2.2, το NIST SP 800-53 αποσκοπεί στους διοικητικούς, λειτουργικούς και τεχνικούς ελέγχους ασφάλειας για τα συστήματα, κάθε ένας από τους οποίους θα πρέπει να συνδέεται με την τεκμηρίωση. Επιπρόσθετα των διαδικασιών τεκμηρίωσης για την εφαρμογή και τη συντήρηση διαφόρων

---

[13] Η αρχική σελίδα του FDCC βρίσκεται στη διεύθυνση http://fdcc.nist.gov/.

[14] Αν και η διαμόρφωση FDCC περιέχει ρυθμίσεις για το Internet Explorer και το Windows Firewall, δεν εξουσιοδοτεί τη χρήση τους. Οι οργανισμοί είναι ελεύθεροι να χρησιμοποιήσουν άλλους φυλλομερτητές δικτύου αντί ή επιπλέον του Internet Explorer και είναι επίσης ελεύθεροι να χρησιμοποιήσουν άλλο επιτραπέζιο τείχος προστασίας αντί του Windows Firewall.

[15] Το OMB έχει ορίσει πέντε ρόλους περιβαλλόντων / συστημάτων σχετικά του FDCC. Αυτά τα περιβάλλοντα δεν είναι άμεσα σχετιζόμενα με τα περιβάλλοντα που αναφέρονται σε αυτή τη δημοσίευση και μία συζήτηση για τους ρόλους των περιβαλλόντων / συστημάτων ορισμένων από το OMB είναι εκτός της βλέψης αυτής της δημοσίευσης. Περισσότερες πληροφορίες είναι διαθέσιμες από το OMB Υπόμνημα 08-22, "Guidance on the Federal Desktop Core Configuration (FDCC)" στη διεύθυνση http://www.whitehouse.gov/omb/memoranda/fy2008/m08-22.pdf.

[16] Οι οργανισμοί θα πρέπει να επιβεβαιώσουν πως οι οδηγοί διαμόρφωσης των ρυθμίσεων ασφάλειάς τους για τα Windows XP είναι σύμφωνοι με αυτή τη δημοσίευση. Οι οργανισμοί χωρίς οδηγούς διαμόρφωσης των ρυθμίσεων ασφάλειας για τα Windows XP θα πρέπει να τροποποιήσουν αυτό το έγγραφο για να δημιουργήσουν έναν οδηγό διαμόρφωσης, προσαρμοσμένος στις ανάγκες των περιβαλλόντων τους.

ελέγχων, κάθε περιβάλλον θα πρέπει να έχει επίσης και άλλες σχετικές με την ασφάλεια πολιτικές και τεκμηριώσεις που επηρεάζουν τη διαμόρφωση, τη συντήρηση και τη χρήση συστημάτων και εφαρμογών. Παραδείγματα τέτοιων εγγράφων είναι τα ακόλουθα:

- Κανόνες συμπεριφοράς και πολιτική αποδεκτής χρήσης
- Πολιτική, σχεδιασμός και διαδικασίες διαμόρφωσης διοίκησης
- Εξουσιοδότηση σύνδεσης στο δίκτυο
- IT σχεδιασμός ενδεχόμενων περιστατικών
- Επίγνωση ασφάλειας και εκπαίδευση για τερματικούς χρήστες και διαχειριστές.

2.5 Εφαρμογή και Δοκιμή Ελέγχων Ασφάλειας

Η εφαρμογή των ελέγχων ασφάλειας μπορεί να είναι αποθαρρυντικό έργο. Όπως περιγράφτηκε στην ενότητα 2.2, πολλοί έλεγχοι ασφάλειας έχουν ένα αρνητικό αντίκτυπο στη λειτουργικότητα και στη χρηστικότητα του συστήματος. Σε ορισμένες περιπτώσεις, ένας έλεγχος ασφάλειας μπορεί να έχει αρνητικές συνέπειες ακόμα και σε άλλους έλεγχους ασφάλειας. Για παράδειγμα, η εγκατάσταση ενός patch θα μπορούσε ακουσίως να παραβιάσει ένα άλλο patch, ή η ενεργοποίηση ενός τείχους προστασίας θα μπορούσε ακουσίως να εμποδίσει ένα λογισμικό ενάντια σε ιούς (antivirus) από το να ενημερώσει τη βάση του ή να διαρρήξει ένα λογισμικό διαχείρισης patch, ένα λογισμικό απομακρυσμένης διαχείρισης και άλλα σχετικά με τη συντήρηση utilities. Συνεπώς είναι σημαντική η εκτέλεση δοκιμών για όλους τους ελέγχους ασφάλειας για να προσδιοριστεί ποιος ο αντίκτυπος που έχουν στην ασφάλεια, στη λειτουργικότητα και στη χρηστικότητα του συστήματος και να εκτελεστούν τα κατάλληλα βήματα για την αγόρευση σημαντικών ζητημάτων.

Όπως περιγράφεται στην ενότητα 5, το NIST έχει συνθέσει ένα σύνολο από πρότυπα ασφάλειας, όπως επίσης και επιπρόσθετες υποδείξεις για αλλαγές διαμόρφωσης σχετικές με την ασφάλεια. Οι έλεγχοι που προτείνονται σε αυτό τον οδηγό και τα Windows XP πρότυπα ασφάλειας του NIST είναι σύμφωνα με τους ελέγχους του FISMA, όπως έχουν συζητηθεί στην ενότητα 2.2. Το πρότυπο του NIST για τα SSLF περιβάλλοντα αντιπροσωπεύει την ομοφωνία των ρυθμίσεων από διάφορους οργανισμούς, συμπεριλαμβανομένου των DISA, Microsoft, NIST, NSA, και USAF. Τα πρότυπα του NIST για τα περιβάλλοντα Enterprise, SOHO, και Legacy είναι βασισμένα στα πρότυπα και τις υποδείξεις της Microsoft. Το NIST επίσης έχει κάνει διαθέσιμα Αντικείμενα Πολιτικής Ομάδας (Group Policy Objects [GPO]) για το FDCC περιβάλλον.

Αν και η καθοδήγηση που παρουσιάζεται σε αυτό το έγγραφο έχει υποστεί αξιοσημείωτους ελέγχους, κάθε σύστημα είναι μοναδικό, έτσι είναι βεβαίως πιθανό για ορισμένες ρυθμίσεις να προκαλέσουν απροσδόκητα προβλήματα. Οι διαχειριστές συστήματος θα πρέπει να εκτελέσουν δικούς τους ελέγχους, ιδίως για τις εφαρμογές που χρησιμοποιούνται από τους οργανισμούς τους, για την αναγνώριση προβλημάτων λειτουργικότητας και χρηστικότητας προτού η καθοδήγηση αυτή εφαρμοστεί κατά μήκος των οργανισμών.[17] Είναι επίσης σημαντικό να επικυρωθεί πως έχουν εφαρμοστεί σωστά οι επιθυμητές ρυθμίσεις ασφάλειας και πως λειτουργούν ως αναμένεται.

[17] Οποιεσδήποτε αλλαγές πραγματοποιηθούν στις ρυθμίσεις του προτύπου θα πρέπει να τεκμηριωθούν, ως μέρος της όλης τεκμηρίωσης της διαμόρφωσης ασφάλειας του Windows XP συστήματος.

2.6 Επίβλεψη και Συντήρηση

Το κάθε σύστημα χρειάζεται να επιβλέπεται και να συντηρείται τακτικά έτσι ώστε να μπορούν να αναγνωριστούν και να κατευνάζονται άμεσα ζητήματα ασφάλειας, ελαχιστοποιώντας την πιθανότητα μίας παραβίασης στην ασφάλεια. Ωστόσο, ανεξάρτητα από το πόσο προσεκτικά επιβλέπονται και συντηρούνται τα συστήματα, μπορούν ακόμα να λάβουν χώρα κάποια περιστατικά, οπότε οι οργανισμοί θα πρέπει να είναι προετοιμασμένοι για να αποκριθούν σε αυτά.[18] Εξαρτημένου του περιβάλλοντος, ορισμένες προληπτικές ενέργειες μπορούν να είναι μερικώς ή πλήρως αυτοματοποιημένες. Καθοδήγηση για την εκτέλεση διάφορων δραστηριοτήτων επίβλεψης και συντήρησης παρέχεται σε διαδοχικές ενότητες αυτού του εγγράφου ή σε άλλες δημοσιεύσεις του NIST. Συνιστώμενες ενέργειες περιέχουν τα κάτωθι:

- Επίβλεψη και συνδρομή σε διάφορες ταχυδρομικές λίστες ειδοποίησης ευπαθειών (πχ, Microsoft Security Notification Service[19])
- Απόκτηση και εγκατάσταση ενημερώσεων λογισμικού (πχ, patches εφαρμογών και λειτουργικού συστήματος, υπογραφές αντιβιοτικών προγραμμάτων)
- Επίβλεψη των αναφορών συμβάντων (event logs) για αναγνώριση προβλημάτων και ύποπτης δραστηριότητας
- Παροχή απομακρυσμένης διαχείρισης και βοήθειας
- Επίβλεψη αλλαγών στις ρυθμίσεις λειτουργικού συστήματος και λογισμικού
- Προστασία και καθαρισμός μέσων
- Άμεση απόκριση σε ύποπτα περιστατικά
- Αποτίμηση της θέσης ασφάλειας του συστήματος μέσα από αποτιμήσεις ευπαθειών[20]
- Απενεργοποίηση άχρηστων λογαριασμών χρηστών και διαγραφή λογαριασμών που έχουν απενεργοποιηθεί για καιρό
- Συντήρηση του συστήματος, των περιφερειακών και των εξαρτημάτων hardware (περιοδικά και όποτε χρειάζεται) και διατήρηση αναφορών για όλες τις δραστηριότητες συντήρησης hardware.

---

[18] Οι οργανισμοί θα πρέπει να έχουν μία πολιτική απόκρισης σε περιστατικά και μία τυπική ικανότητα απόκρισης σε αυτά τα περιστατικά. Για καθοδήγηση στο χειρισμό, στην προετοιμασία και στην εκτέλεση περιστατικών, δείτε το NIST SP 800-61 Επανέκδοση 1, *Computer Security Incident Handling Guide*, που διατίθεται εδώ: http://csrc.nist.gov/publications/PubsSPs.html.

[19] Η Microsoft παρέχει προειδοποιήσεις ηλεκτρονικού ταχυδρομείου όπου ειδοποιούν τους συνδρομητές όποτε η Microsoft εκδίδει ένα σημαντικό δελτίο ασφάλειας ή κάποια προειδοποίηση για έναν ιό. Επιπρόσθετες πληροφορίες είναι διαθέσιμες στη διεύθυνση http://signup.alerts.live.com/brochure/index.jsp.

[20] Δείτε το NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, για περισσότερες πληροφορίες σχετικά με την εκτέλεση αποτιμήσεων ευπαθειών. Η δημοσίευση είναι διαθέσιμη στη διεύθυνση http://csrc.nist.gov/publications/PubsSPs.html.

Οι οργανισμοί θα πρέπει να είναι ενήμεροι πως η Microsoft έχει ανακοινώσει σχέδια σταδιακής απόσυρσης των Windows XP και έχει ήδη σταματήσει την πώλησή τους. Οι οργανισμοί θα πρέπει να σκεφτούν προσεκτικά τη δημιουργία πλάνων μετάβασης για μία ενδεχόμενη μεταφορά από τα Windows XP σε ένα πλήρως υποστηριζόμενο επιτραπέζιο λειτουργικό σύστημα.[21]

2.7 Σύνοψη και Υποδείξεις

- ✓ Προστασία του κάθε συστήματος βάσει του πιθανού αντίκτυπου στο σύστημα στην απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας.

- ✓ Ελαχιστοποίηση των ευκαιριών που έχουν οι επιτιθέμενοι για να παραβιάσουν το σύστημα, επιλύοντας αδυναμίες ασφάλειας και περιορίζοντας τη λειτουργικότητα σύμφωνα με την αρχή του ελάχιστου προνομίου.

- ✓ Επιλογή ελέγχων ασφάλειας που να παρέχουν μία λογική ασφαλή λύση ενώ υποστηρίζεται η λειτουργικότητα και η χρηστικότητα που απαιτείται από τους χρήστες.

- ✓ Χρησιμοποίηση πολλαπλών στρωμάτων ασφάλειας έτσι ώστε εάν ένα στρώμα αποτύχει ή διαφορετικά δεν μπορέσει να αντιδράσει σε μία συγκεκριμένη απειλή, τα άλλα στρώματα μπορούν να αποτρέψουν την απειλή από το να παραβιάσει επιτυχώς το σύστημα.

- ✓ Διεξαγωγή αποτιμήσεων επικινδυνότητας για την αναγνώριση απειλών εναντίον συστημάτων και προσδιορισμός της αποτελεσματικότητας των υπαρχόντων ελέγχων ασφάλειας που αντιδρούν στις απειλές. Εκτέλεση εξομάλυνσης κινδύνου ώστε να αποφασιστεί ποια επιπρόσθετα μέτρα (εφόσον αυτά υπάρχουν) θα πρέπει να εφαρμοστούν.

- ✓ Τεκμηρίωση των διαδικασιών εφαρμογής και συντήρησης ελέγχων ασφάλειας. Συντήρηση άλλων πολιτικών και τεκμηριώσεων σχετικών με την ασφάλεια που επηρεάζουν τη διαμόρφωση, τη συντήρηση και τη χρήση των συστημάτων και των εφαρμογών, όπως πολιτική αποδεκτής χρήσης, πολιτική διαχείρισης διαμόρφωσης και IT προγραμματισμός πιθανοτήτων.

- ✓ Δοκιμή όλων των ελέγχων ασφάλειας, συμπεριλαμβανομένων των ρυθμίσεων στα πρότυπα ασφάλειας του NIST, για τον προσδιορισμό του αντίκτυπου που έχουν στην ασφάλεια, στη λειτουργικότητα και στη χρηστικότητα του συστήματος. Εκτέλεση των κατάλληλων βημάτων για την αγόρευση σημαντικών ζητημάτων προτού εφαρμοστούν οι έλεγχοι στα συστήματα παραγωγής.
- ✓ Επίβλεψη και συντήρηση σε τακτικά διαστήματα έτσι ώστε να μπορούν να αναγνωριστούν και να κατευνάζονται άμεσα ζητήματα ασφάλειας. Συνιστώμενες ενέργειες περιλαμβάνουν την απόκτηση και εγκατάσταση ενημερώσεων λογισμικού, την επίβλεψη αναφορών συμβάντων (event logs), την παροχή απομακρυσμένης διαχείρισης και βοήθειας, την επίβλεψη αλλαγών στις ρυθμίσεις του λειτουργικού συστήματος και του λογισμικού, την προστασία και τον καθαρισμό των μέσων, την άμεση απόκριση σε

[21] http://www.microsoft.com/windows/windows-xp/future.aspx.

ύποπτα περιστατικά, την εκτέλεση αποτιμήσεων ευπαθειών, την απενεργοποίηση και διαγραφή άχρηστων λογαριασμών χρηστών και τη συντήρηση του hardware.

Κεφάλαιο 3

3. Προεπισκόπιση Συστατικών Ασφάλειας (Components) των Windows XP

Σε αυτή την ενότητα θα γίνει μία γενική παρουσίαση διαφόρων χαρακτηριστικών ασφάλειας που προσφέρονται από το λειτουργικό σύστημα Windows XP Professional. Πολλά από τα components έχουν κληρονομηθεί από τα Windows 2000 και τα περισσότερα έχουν υποστεί βελτιώσεις και έχουν εμπλουτιστεί. Τα Windows XP περιέχουν επίσης διάφορα καινούργια χαρακτηριστικά ασφάλειας. Αυτός ο οδηγός παρέχει γενικές περιγραφές για τα περισσότερα από αυτά τα χαρακτηριστικά, με δείκτες ή συνδέσμους για περισσότερο λεπτομερείς πληροφορίες όπου αυτό είναι δυνατό.

3.1 Νέα χαρακτηριστικά στα Windows XP

Τα Windows XP διατίθενται με διάφορα νέα χαρακτηριστικά. Κάθε ένα από αυτά τα χαρακτηριστικά περιγράφεται εν συντομία παρακάτω και τα περισσότερα περιλαμβάνουν επίσης παραπομπές σε κάποια ιστοσελίδα της Microsoft, η οποία παρέχει περισσότερο λεπτομερείς πληροφορίες. Αυτή η ενότητα περιλαμβάνει επίσης μία ανάλυση της επίδρασης σε επίπεδο ασφάλειας του κάθε χαρακτηριστικού και γενικές υποδείξεις για το πότε θα πρέπει αυτό να χρησιμοποιηθεί ή όχι. Τα νέα χαρακτηριστικά ασφάλειας στα Windows XP είναι τα ακόλουθα:

3.1.1 *Χαρακτηριστικά Δικτύου*

- **Windows Firewall.**[22] Το Windows Firewall είναι ένα stateful προσωπικό τείχος προστασίας.[23] Όταν οριστεί κατάλληλα, περιορίζει την πρόσβαση που έχουν άλλοι υπολογιστές στο Windows XP μηχάνημα μέσω δικτύου. Αυτό μειώνει σημαντικά την έκθεση του μηχανήματος σε επιθέσεις μέσω δικτύου, όπως είναι το Blaster Worm.[24] Το Windows Firewall μπορεί επίσης να χρησιμοποιηθεί για την προστασία των διαμοιραζόμενων καταλόγων και αρχείων, όταν ένας φορητός υπολογιστής χρησιμοποιείται εκτός του φυσιολογικού ασφαλούς και έμπιστου περιβάλλοντός του, ή για να προστατεύει την πρόσβαση σε διαμοιραζόμενους καταλόγους και αρχεία σε κάποιο αναξιόπιστο δίκτυο. Οι διαχειριστές τομέα μπορούν να απενεργοποιήσουν τη χρήση του Windows Firewall από την Πολιτική Ομάδας [Group Policy],[25] αλλά δεν

---

[22] Το Windows Firewall προστέθηκε στα Windows XP με το Service Pack 2. Πριν το SP2, το ενσωματωμένο τείχος προστασίας ονομαζόταν Internet Connection Firewall (ICF). Για περισσότερες πληροφορίες για το ICF, ανατρέξτε στο Microsoft Knowledge Base (MSKB) άρθρο 320855, *Description of the Windows XP Internet Connection Firewall*, το οποίο είναι διαθέσιμο εδώ: http://support.microsoft.com/?id=320855.

[23] Για περισσότερες πληροφορίες αναφορικά με το Windows Firewall επισκεφτείτε τη διεύθυνση: http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx.

[24] Το Blaster Worm εξαπλώνεται εγκαθιδρύοντας συνεδρίες με συγκεκριμένες Microsoft TCP πόρτες υπηρεσίας [service ports] (κυρίως την 135, αλλά και τις 139 και 445). Ένα προσωπικό τείχος προστασίας μπορεί να εμποδίσει ανεπιθύμητες προσπάθειες σύνδεσης σε αυτές τις πόρτες, αποτρέποντας κάποιο worm, όπως το Blaster, από το να μολύνει επιτυχώς το σύστημα. Για περισσότερες πληροφορίες δείτε το *CERT® Advisory CA-2003-20, W32/Blaster Worm*, το οποίο είναι διαθέσιμο εδώ: http://www.cert.org/advisories/CA-2003-20.html.

[25] Για το Group Policy υπάρχει εκτενέστερη αναφορά σε επόμενο κεφάλαιο.

ενδείκνυται, εκτός εάν αυτό συγκρούεται με κάποια απαιτούμενη λειτουργία, ή είναι ήδη σε λειτουργία κάποιο έμμεσα εμπλεκόμενο τείχος προστασίας.[26] Οι διαχειριστές μπορούν επίσης να χρησιμοποιήσουν την Πολιτική Ομάδας για να ορίσουν οποιαδήποτε επιλογή ρύθμισης του Windows Firewall. Το Windows Firewall μπορεί να προσθέσει άλλο ένα στρώμα στο μοντέλο ασφάλειας δικτύου σε enterprise, SSLF και FDCC περιβάλλοντα, και κάποιες φορές είναι το μόνο στρώμα στην άμυνα δικτύου στα SOHO περιβάλλοντα.

- **Γεφύρωση Δικτύου.** Μία γέφυρα δικτύου [network bridge] επιτρέπει σε δύο ανόμοια δίκτυα (πχ Ethernet και dialup, wireless ή token ring) να ενώνονται χωρίς να χρησιμοποιηθεί dedicated και ακριβό hardware. Η σύνδεση μεταξύ των δύο δικτύων είναι διάφανη, που σημαίνει ότι δεν γίνεται μεταγλώττιση των διευθύνσεων δικτύου μεταξύ των δικτύων και οι ακριβείς προσδιορισμένες διευθύνσεις στο κάθε δίκτυο είναι ορατές στο άλλο. Ενώ η δικτύωση επιτρέπει την ένωση των δύο δικτύων με την ελάχιστη δυνατή ποσότητα εργασίας, έχει σοβαρές επιπλοκές ασφάλειας. Εάν δεν είναι ενεργοποιημένο και ρυθμισμένο σωστά κάποιο προσωπικό τείχος προστασίας, όπως το Windows Firewall, η γέφυρα δεν θα παρέχει καμία προστασία ασφάλειας δικτύου σε κανένα από τα δίκτυα τα οποία διασυνδέει, εκθέτοντάς τα σε επιθέσεις του ενός στο άλλο. Μία γέφυρα δικτύου μπορεί να εκθέσει συστήματα που βρίσκονται σε πολλαπλά δίκτυα, σε επιπρόσθετες απειλές, έτσι το NIST δεν συνιστά την εφαρμογή γέφυρας χρησιμοποιώντας ένα Windows XP σύστημα, εκτός εάν χρειάζεται συγκεκριμένα για κάποιο καθήκον και έχει εκτελεστεί κάποια αποτίμηση ή εξομάλυνση κινδύνου.

- **Απομακρυσμένη Βοήθεια [Remote Assistance - RA].** Η RA παρέχει ένα τρόπο απομακρυσμένης τεχνικής υποστήριξης όταν συναντάται πρόβλημα με κάποιο υπολογιστή.[27] Συνεδρίες RA μπορούν να εκκινηθούν μέσω του Windows Messenger, μέσω αιτήματος e-mail και μέσω κάποιας Web e-mail υπηρεσίας (συμπληρώνοντας κάποια φόρμα αίτησης βοήθειας). Δυστυχώς, εάν δεν είναι σωστά ρυθμισμένη η RA, μη εξουσιοδοτημένα πρόσωπα μπορούν να τη χρησιμοποιήσουν για να πετύχουν απομακρυσμένη πρόσβαση στο σύστημα. Συνεπώς, η RA θα πρέπει να χρησιμοποιείται μόνο εάν είναι διαθέσιμοι έμπειροι διαχειριστές ασφάλειας, οι οποίοι θα τη ρυθμίσουν έτσι ώστε να περιορίσουν αυστηρά τη χρήση της και εάν η περίμετρος του δικτύου (πχ, τείχος προστασίας) είναι ορισμένη ώστε να αποτρέπει εξωτερικούς παράγοντες από τη χρησιμοποίηση της RA για να αποκτήσουν πρόσβαση σε εσωτερικά μηχανήματα. Σε διαφορετικές περιπτώσεις η RA θα πρέπει να απενεργοποιείται.

- **Απομακρυσμένη Επιφάνεια Εργασίας.** Το χαρακτηριστικό Απομακρυσμένη Επιφάνεια Εργασίας [Remote Desktop] επιτρέπει σε κάποιο χρήστη να έχει απομακρυσμένη πρόσβαση σε κάποιο Windows XP Professional σύστημα, από έναν άλλο υπολογιστή.[28] Αυτό παρέχει μία άλλη μέθοδο για τους απομακρυσμένους επιτιθέμενους να προσπαθήσουν να επιτύχουν την πρόσβαση σε κάποιο υπολογιστή, εικάζοντας τους

---

[26] Εάν προκύψει κάποια σύγκρουση, το NIST προτείνει την τροποποίηση των ρυθμίσεων του Windows Firewall από τον οργανισμό, έτσι ώστε να επιτρέπει την απαιτούμενη λειτουργικότητα, όπως οι έρευνες εσωτερικού δικτύου για αδυναμίες, παρά την καθολική απενεργοποίηση του Windows Firewall.

[27] Περισσότερες πληροφορίες για την RA, συμπεριλαμβανομένου και οδηγιών απενεργοποίησής της βρίσκονται εδώ: http://www.microsoft.com/windowsxp/using/helpandsupport/rafaq-general.mspx.

[28] Για πληροφορίες σχετικά με την οργάνωση του Remote Desktop διαβάστε το άρθρο της Microsoft, *Get Started using Remote Desktop with Windows XP Professional*, το οποίο είναι διαθέσιμο εδώ: http://www.microsoft.com/windowsxp/using/mobility/getstarted/remoteintro.mspx.

κωδικούς πρόσβασης των προεπιλεγμένων λογαριασμών χρηστών. Γενικά το Remote Desktop θα πρέπει να χρησιμοποιείται μόνο εάν υφίστανται διάφορα άλλα στρώματα ελέγχων ασφάλειας, τα οποία αποτρέπουν την άμεση έκθεση του συστήματος στους επιτιθέμενους. Ακόμη και τότε, οι διαχειριστές θα πρέπει να λάβουν σοβαρά υπόψιν τους την επιχειρησιακή ανάγκη να υπάρχει απομακρυσμένη πρόσβαση στο σύστημα και θα πρέπει να σκεφτούν πιθανές εναλλακτικές λύσεις, οι οποίες δεν θα εκθέτουν το σύστημα σε επιθέσεις.

- **Αυτόματη Ρύθμιση Wireless.** Όταν είναι παρούσα μία κάρτα διεπαφής ασύρματου δικτύου (network interface card [NIC]), ο υπολογιστής θα προσπαθήσει αυτόματα να προσχωρήσει σε οποιοδήποτε ασύρματο δίκτυο εντοπίσει, σε μία επαληθευμένη λίστα από προτιμώμενα δίκτυα.[29] Αυτό επιτρέπει σε έναν υπολογιστή να περιάγεται εύκολα από σημείο πρόσβασης σε σημείο πρόσβασης (access point [AP][30]), χωρίς να χρειάζεται αναδιαμόρφωση των ρυθμίσεων, το οποίο αποτελεί προνόμιο. Ωστόσο, το σύστημα μπορεί να αποκαλύψει πληροφορίες σχετικά με τα Service Set Identifiers [SSID][31] για προτιμώμενα access points και access points όπου είχε προηγούμενα συνδεθεί, τα οποία μπορούν να συλληφθούν από κάποιο επιτιθέμενο και να χρησιμοποιηθούν για να καθοριστεί ένα access point-απατεώνας (rogue access point). Επειδή η Αυτόματη Ρύθμιση Wireless μπορεί να οριστεί έτσι ώστε να συνδέεται σε οποιοδήποτε δίκτυο, ένα access point-απατεώνας μπορεί να κοροϊδέψει τον υπολογιστή και να συνδεθεί σε κάποιο εχθρικό δίκτυο, το οποίο θα μπορεί να επιτεθεί στον υπολογιστή ή να συλλάβει δεδομένα από αυτόν. Το NIST συνιστά τα συστήματα να είναι ρυθμισμένα έτσι ώστε να μην προσπαθούν αυτόματα να συνδέονται σε οποιοδήποτε δίκτυο.

- **Ασφάλεια Wireless.** Για να παρέχονται καλύτερες λύσεις για την ασφάλεια wireless, δημιουργήθηκε μία ομάδα επιμέλειας που ονομάζεται Wi-Fi Alliance, η οποία δημιούργησε ένα προϊόν πιστοποίησης με το όνομα Wi-Fi Protected Access (WPA). Στα Windows XP SP2 και SP3, οι hosts με NICs που υποστηρίζουν WPA μπορούν να χρησιμοποιούν χαρακτηριστικά που παρέχονται από το WPA, όπως η χρήση του Advanced Encryption Security [AES] για την κωδικοποίηση επικοινωνιών δικτύου.[32]

- **Περιορισμοί TCP/IP Raw Sockets.** Μία αλλαγή που παρουσιάστηκε στα Windows XP SP2, η οποία μπορεί να επηρεάσει κάποιους χρήστες, είναι ο περιορισμός στα raw sockets της TCP/IP στοίβας. Ορισμένα εργαλεία ασφάλειας, όπως οι σαρωτές αδυναμιών δικτύου, χρησιμοποιούν raw sockets για τη δημιουργία πακέτων. Τα Windows XP SP2 και SP3 περιορίζουν τον αριθμό των ημιτελών εξωθούμενων πακέτων ανά δευτερόλεπτο, τα οποία μπορούν να διακόψουν τέτοια εργαλεία.

3.1.2 *Πιστοποίηση και Εξουσιοδότηση*

- **Εξατομικευμένο Login.** Αυτό το χαρακτηριστικό επιτρέπει στο κάθε άτομο που χρησιμοποιεί ένα Windows XP υπολογιστή να έχει ένα ατομικό λογαριασμό χρήστη, το

---

[29] Περισσότερες πληροφορίες για το Wireless Auto Configuration, δείτε το άρθρο *The Wireless XP Wireless Zero Configuration Service*, το οποίο είναι διαθέσιμο από το Microsoft TechNet στη διεύθυνση: http://technet.microsoft.com/en-us/library/bb878124.aspx.
[30] Περισσότερα για τα Wireless Access Points: http://en.wikipedia.org/wiki/Wireless_access_point.
[31] Περισσότερα για τα Service Sets: http://en.wikipedia.org/wiki/SSID.
[32] Περισσότερα για το WPA θα βρείτε εδώ: http://www.microsoft.com/windowsxp/using/networking/security/wireless.mspx.

οποίο και συνίσταται. Έτσι επιτρέπεται στα προσωπικά δεδομένα (πχ, κάθε λογαριασμός έχει το δικό του My Documents φάκελο) και στις ρυθμίσεις (πχ, τα Αγαπημένα του Internet Explorer και τις ρυθμίσεις ασφάλειας) να διατηρούνται μυστικά από τους άλλους χρήστες. Αυτό επίσης, αυξάνει την υπευθυνότητα· για παράδειγμα όταν ενεργοποιηθεί κάποιος έλεγχος, ο διαχειριστής μπορεί να προσδιορίσει από ποιόν χρήστη εκτελέστηκε η συγκεκριμένη ενέργεια.

- **Απλός Διαμοιρασμός Αρχείων.**[33] Αυτό το χαρακτηριστικό είναι ενεργοποιημένο εκ προεπιλογής στα Windows XP Professional συστήματα σε κάποια ομάδα εργασίας ή αλλιώς workgroup, αλλά είναι απενεργοποιημένο σε Windows XP Professional συστήματα σε κάποιο τομέα ή αλλιώς domain. Όταν είναι ενεργοποιημένος ο Απλός Διαμοιρασμός Αρχείων [Simple File Sharing], μόνον ο λογαριασμός Guest μπορεί να χρησιμοποιηθεί για να επιτευχθεί η πρόσβαση στο σύστημα μέσω δικτύου. Αυτό σημαίνει πως οι επιτιθέμενοι δεν μπορούν να καταφέρουν απομακρυσμένη πρόσβαση εικάζοντας τους κωδικούς από άλλους λογαριασμούς, όπως είναι ο λογαριασμός Administrator. Όταν δεν είναι ενεργοποιημένος ο Απλός Διαμοιρασμός Αρχείων, ο διαχειριστής μπορεί να θέσει δικαιώματα για διαφορετικούς λογαριασμούς χρήστη. Τα προνόμια θα πρέπει να είναι περιορισμένα, έτσι ώστε μόνο οι χρήστες με νόμιμη ανάγκη απομακρυσμένης πρόσβασης στο σύστημα να μπορούν να την έχουν και έτσι ώστε αυτοί να έχουν τα ελάχιστα δυνατά απαιτούμενα προνόμια.

- **Περιορισμοί Κενού Κωδικού Πρόσβασης.** Στα Windows XP Professional, οι λογαριασμοί χρηστών με μηδενικούς ή κενούς κωδικούς πρόσβασης μπορούν να χρησιμοποιηθούν μόνο για την πρόσβαση στην οθόνη logon του φυσικού συστήματος. Αυτό σημαίνει ότι οι λογαριασμοί με μηδενικούς ή κενούς κωδικούς δε μπορούν να χρησιμοποιηθούν πάνω σε δίκτυα ή με την υπηρεσία second logon (RunAs). Αυτό εμποδίζει τους επιτιθέμενους και το κακόβουλο λογισμικό από το αποκτήσουν απομακρυσμένη πρόσβαση μέσω κενών κωδικών.

- **Διαχείριση Διαπιστευτηρίων.** Η Διαχείριση Διαπιστευτηρίων [Credential Management] επιτρέπει στους χρήστες να αποθηκεύουν πληροφορίες πιστοποίησης για λειτουργικά συστήματα και εφαρμογές.[34] Για παράδειγμα, όταν το σύστημα προτρέπει ένα χρήστη να θέσει ένα username και ένα password για να εισχωρήσει σε μία συγκεκριμένη εφαρμογή, το παράθυρο προτροπής εμπεριέχει ένα dialog box με τίτλο **Remember my password**. Οποιοσδήποτε αποκτήσει πρόσβαση σε αυτό το σύστημα σαν να ήταν ο ίδιος ο χρήστης (πχ η αφύπνιση ενός παραμελημένου σταθμού εργασίας) τότε θα ήταν ικανός να χρησιμοποιήσει όλες τις πηγές στις οποίες με τα αποθηκευμένα διαπιστευτήρια είχε παραχωρηθεί η πρόσβαση. Συνεπώς, οι κωδικοί θα πρέπει να αποθηκεύονται μόνο σε περιβάλλοντα στα οποία υπάρχει η ελάχιστη φυσική απειλή, είτε ο κωδικός έχει τετριμμένη τιμή (πχ ένα δοκιμαστικό σε μία δημόσια ιστοσελίδα).

- **Γρήγορη Εναλλαγή Χρηστών [Fast User Switch - FUS].** Αυτό το χαρακτηριστικό επιτρέπει σε δύο ή περισσότερους χρήστες να είναι συνδεδεμένοι στο ίδιο Windows XP

---

[33] Για περισσότερες πληροφορίες για τον Απλό Διαμοιρασμό Αρχείων ή Simple File Sharing δείτε στο MSKB το άρθρο 304040, *How to configure file sharing in Windows XP*, που είναι διαθέσιμο εδώ: http://support.microsoft.com/?id=304040.

[34] Για μία επισκόπηση του Credential Management, δείτε το άρθρο της Microsoft, *Stored User Names and Passwords overview* στη διεύθυνση: http://technet.microsoft.com/en-us/library/cc786845.aspx.

σύστημα ταυτοχρόνως.[35] Μόνο μία συνεδρία χρήστη είναι ενεργή στο δεδομένο χρόνο. Η χρήση του FUS συνιστάται σε συστήματα όπου ο χρήστης μπορεί να χρειαστεί χρονικά άμεση πρόσβαση σε ένα σύστημα το οποίο χρησιμοποιεί κάποιος άλλος, διότι διατηρεί την ασφάλεια και το απαράβατο και για τους δύο χρήστες, ενώ ελαχιστοποιεί την επίδραση στη χρηστικότητα. Υποθέτοντας πως κάθε λογαριασμός έχει από ένα κωδικό, το άτομο που επί του παρόντος χρησιμοποιεί το σύστημα, δεν μπορεί να έχει πρόσβαση στις συνεδρίες των άλλων χρηστών. Το FUS είναι διαθέσιμο μόνο σε συστήματα τα οποία έχουν ιδιαίτερα χαρακτηριστικά, όπως είναι αυτά που δεν είναι μέλη κάποιου τομέα.[36]

- **Χρήση Μοντέλου Αντικειμένου Κατανεμημένης Συνιστώσας [Distributed Component Object Model - DCOM] και Κλήσης Απομακρυσμένης Διαδικασίας [Remote Procedure Call - RPC].** Ένα χαρακτηριστικό το οποίο προστέθηκε στα Windows XP SP2, είναι ότι η ανώνυμη χρήση των DCOM και RPC δεν είναι πλέον επιτρεπτή. Οι COM servers έχουν λίστες ελέγχου πρόσβασης, οι οποίες μπορούν να αποτρέψουν την μη-εξουσιοδοτημένη πρόσβαση σε COM διαδικασίες. Οι αλλαγές στα RPC και DCOM σκοπεύουν στο να εξαλείψουν διάφορες μεθόδους που χρησιμοποιούνται από το κακόβουλο λογισμικό για να επιτίθεται σε συστήματα. Ωστόσο αυτές οι αλλαγές μπορούν επίσης να διακόψουν πολλά υπάρχοντα προγράμματα. Όλες οι εφαρμογές που χρησιμοποιούν το DCOM ή το RPC θα πρέπει να δοκιμάζονται εκτενώς με τα Windows XP SP2 και SP3 προτού αναπτυχθούν επί της επιχείρησης.

- **Χρήση Κατανεμημένου Συντονιστή Δοσοληψίας [Distributed Transaction Coordinator - DTC].** Το DTC χρησιμοποιείται για το χειρισμό των δοσοληψιών για βάσεις δεδομένων και άλλες πηγές. Στα Windows XP SP2 και SP3, η πρόσβαση δικτύου μέσω DTC είναι απενεργοποιημένη εκ προεπιλογής. Τα Windows XP SP2 προσθέτουν επίσης διάφορες ρυθμίσεις διαμόρφωσης ασφάλειας για το DTC οι οποίες δεν ήταν διαθέσιμες προηγούμενα. Για παράδειγμα οι διαχειριστές μπορούν να καθορίσουν εάν θα είναι επιτρεπτή η εξερχόμενη ή εισερχόμενη DTC δραστηριότητα. Οι διαχειριστές μπορούν επίσης να απαιτήσουν αμοιβαία διαμόρφωση μεταξύ των DTC τερματικών σημείων [endpoints], το οποίο προκαλεί επίσης την κωδικοποίηση των DTC επικοινωνιών δικτύου. Οι οργανισμοί θα πρέπει να ρυθμίσουν το DTC ώστε να παρέχει μόνο πρόσβαση που χρειάζεται από τις εφαρμογές και να τις προστατεύουν με αμοιβαία πιστοποίηση και κωδικοποίηση όταν κάτι τέτοιο είναι εφικτό.

3.1.3 *Άλλα*

- **Κέντρο Ασφάλειας των Windows.** Το Κέντρο Ασφάλειας των Windows [Windows Security Center], που είναι προσβάσιμο από το Control Panel, παρέχει μία και μοναδική διεπαφή για διάφορα σχετικά με την ασφάλεια χαρακτηριστικά.[37] Εξετάζει το σύστημα για λογισμικό τείχους προστασίας και επικυρώνει το ότι είναι ενεργό, ότι είναι διαμορφωμένο να εκτελεί σάρωση σε πραγματικό χρόνο και ότι έχει τις τελευταίες

---

[35] Για μια περιγραφή στο πώς χρησιμοποιείται το FUS δείτε στο MSKB το άρθρο 279765, *How to Use the Fast User Switching Feature in Windows XP*, στη διεύθυνση http://support.microsoft.com/?id=279765.

[36] Περισσότερες πληροφορίες σχετικά με αυτό το ζήτημα διαβάστε στο MSKB το άρθρο 294739, *A discussion about the availability of the Fast User Switching feature*, στη διεύθυνση http://support.microsoft.com/?id=294739.

[37] Περισσότερες πληροφορίες σχετικά με το Windows Security Center: http://www.microsoft.com/windowsxp/using/security/internet/sp2_wscintro.mspx.

ενημερώσεις για ιούς. Το Κέντρο Ασφάλειας των Windows ελέγχει επίσης την κατάσταση του χαρακτηριστικού Automatic Updates και δίνει συστάσεις για αναδιαμόρφωσή του, ώστε να επιβεβαιωθεί ότι οι ενημερώσεις λαμβάνουν χώρα σωστά. Εάν το Κέντρο Ασφάλειας των Windows εντοπίσει ένα ζήτημα με κάποιο εργαλείο ασφάλειας, θα ειδοποιήσει το χρήστη κατά το login και θα εμφανίσει ένα κόκκινο εικονίδιο στην μπάρα εργασίας για να προειδοποιήσει το χρήστη για το ζήτημα αυτό. Αυτό μπορεί να οδηγήσει σε ταχύτερη αναγνώριση και ανάλυση της κακής διαμόρφωσης ή άλλων προβλημάτων του εργαλείου ασφάλειας.

- **Διαμοιραζόμενοι Φάκελοι.** Όταν είναι ενεργοποιημένο το χαρακτηριστικό αυτό [Shared Folders] παρέχει φακέλους που ονομάζονται Shared Documents και Shared Pictures, οι οποίοι είναι προσβάσιμοι από όλους τους χρήστες.[38] Αυτό επιτρέπει στους χρήστες να διαμοιράζονται αρχεία χωρίς να χρειάζεται να διαμοιράζονται λογαριασμούς χρηστών, ή να επιτρέπουν την πρόσβαση άλλων χρηστών σε προσωπικούς τους φακέλους.[39] Οι Διαμοιραζόμενοι Φάκελοι παρέχουν μία λύση για ένα SOHO περιβάλλον, για τον διαμοιρασμό αρχείων στα οποία κάθε χρήστης στο σύστημα θα μπορεί να έχει πρόσβαση και να τα τροποποιεί. Εάν είναι αναγκαία η περιορισμένη πρόσβαση (πχ, πρόσβαση ορισμένων χρηστών, ή read-only πρόσβαση), η χρήση των Διαμοιραζόμενων Φακέλων δε συνιστάται.

- **Πολιτική Περιορισμού Λογισμικού.** Το χαρακτηριστικό Πολιτική Περιορισμού Λογισμικού [Software Restriction Policy] επιτρέπει στον διαχειριστή να οριοθετήσει το τι λογισμικό θα εκτελείται σε ένα δεδομένο υπολογιστή. Η Πολιτική Περιορισμού Λογισμικού μπορεί να καθοριστεί είτε ως περιοριστική, είτε ως απορριπτική. Η απορριπτική πολιτική θα απαγορεύσει την εκτέλεση όλων των προγραμμάτων, εκτός αυτών που η εκτέλεσή τους έχει οριστεί να επιτρέπεται. Αυτό μπορεί να χρησιμοποιηθεί για να περιοριστεί το λογισμικό ώστε να εκτελείται μόνο σε εγκεκριμένες εφαρμογές του οργανισμού, ή εναλλακτικά για την προστασία από την εκτέλεση κακόβουλου λογισμικού. Παρότι η απορριπτική πολιτική παρέχει ισχυρή ασφάλεια, απαιτεί χρονικά εντατική οργάνωση και συντήρηση, έτσι είναι εφικτή για ορισμένα μόνο SSLF περιβάλλοντα. Η περιοριστική πολιτική μπορεί να είναι χρήσιμη στην αποτροπή εκτέλεσης προγραμμάτων με αρνητικές συνέπειες στην ασφάλεια, όπως είναι τα προγράμματα διαμοιρασμού αρχείων peer-to-peer και τα Trojan Horses.

- **Universal Plug and Play [UPnP].** Το UPnP παρέχει στα Windows XP ένα τρόπο για την αυτόματη διαμόρφωση συσκευών δικτύου, αναγνωρίσιμων μέσω UPnP (UPnP-aware device), όπως είναι τα τείχη προστασίας των SOHO.[40] Για παράδειγμα ένα Windows XP σύστημα μπορεί δυναμικά να αιτηθεί το άνοιγμα πορτών από το UPnP-aware τείχος προστασίας για να ενεργοποιηθεί μία μεταφορά αρχείου από έναν IM client. Τα Windows XP έχουν βελτιωθεί στο UPnP από την αρχική εφαρμογή των Windows ME, και πλέον παρέχουν καλύτερη χρηστικότητα και απόδοση. Ωστόσο το UPnP έχει αδυναμίες απομακρυσμένης εκμετάλλευσης, έτσι το NIST συνιστά την απενεργοποίησή

---

[38] Το χαρακτηριστικό αυτό δεν μπορεί να είναι ενεργό εάν το σύστημα διαχείρισης αρχείων δεν είναι διαμορφωμένο ως NTFS.

[39] Για περισσότερες πληροφορίες για τον Διαμοιρασμό Αρχείων στα Windows XP δείτε στο MSKB το άρθρο 304040, *How to configure file sharing in Windows XP*, που είναι διαθέσιμο εδώ: http://support.microsoft.com/?id=304040.

[40] Περισσότερες πληροφορίες για το UPnP, δείτε το άρθρο της Microsoft, *Universal Plug and Play in Windows XP*, που είναι διαθέσιμο εδώ: http://technet.microsoft.com/en-us/library/bb457049.aspx.

του, εκτός εάν είναι απαραίτητο το χαρακτηριστικό της δυναμικής αναβάθμισης [dynamic updating].

- **Παρεμπόδιση Εκτέλεσης Δεδομένων [Data Execution Prevention - DEP].** Διάφοροι τύποι επεξεργαστών περιέχουν υποστήριξη Παρεμπόδισης Εκτέλεσης (που είναι γνωστό και ως no execute, ή NX), όπου είναι ένα τρόπος προστασίας της μνήμης για την παρεμπόδιση της εκμετάλλευσης. Εάν τα Windows XP SP2 ή SP3 εκτελούνται σε ένα σύστημα που διαθέτει επεξεργαστή με υποστήριξη NX, το χαρακτηριστικό DEP των Windows XP μπορεί να χρησιμοποιήσει το NX γα να προστατεύσει το σύστημα από υπερχειλίσεις του προσωρινού καταχωρητή (buffer overflow). Πολλοί επιτιθέμενοι και κακόβουλο λογισμικό χρησιμοποιούν επιθέσεις υπερχείλισης του προσωρινού καταχωρητή, για να πετύχουν μη-εξουσιοδοτημένη πρόσβαση σε συστήματα ή ακόμη και να τα καταρρίψουν. Το NX εξουδετερώνει τις υπερχειλίσεις προσωρινού καταχωρητή, παρακολουθώντας συνεχώς ποιο τμήμα της μνήμης του συστήματος περιέχει εκτελέσιμο κώδικα και ποιο όχι. Εάν μία προσπάθεια υπερχείλισης του προσωρινού καταχωρητή προκαλέσει την τοποθέτηση νέου εκτελέσιμου κώδικα στη μνήμη, αυτός δεν θα εκτελεστεί εάν τοποθετηθεί σε μία περιοχή η οποία δεν έχει σημειωθεί να εμπεριέχει εκτελέσιμο κώδικα.[41] Εκ προεπιλογής το DEP είναι ενεργοποιημένο μόνο για θεμελιώδη προγράμματα των Windows και υπηρεσίες όπου χρησιμοποιείται η υποστήριξη NX για επεξεργαστές 32-bit. Σε συστήματα επεξεργαστών 64-bit, το DEP είναι ενεργοποιημένο εκ προεπιλογής για όλα τα προγράμματα. Το NIST συνιστά να είναι διαμορφωμένο το DEP για να προστατεύει τα προγράμματα και τις υπηρεσίες σε συστήματα 32-bit και 64-bit, έχοντας εκτελέσει εκτενείς ελέγχους για διαπίστευση πως κάθε πρόγραμμα και υπηρεσία δεν έχει ασυμβατότητες με το DEP.

3.2 Χαρακτηριστικά Ασφάλειας Κληροδοτημένα από τα Windows 2000

Σε αυτή την ενότητα θα συζητηθούν τα περισσότερο σημαντικά χαρακτηριστικά ασφάλειας που κληροδοτήθηκαν από τα Windows 2000: Kerberos, υποστήριξη Έξυπνων Καρτών [Smart Card], Διαμοιρασμός Σύνδεσης Διαδικτύου [Internet Connection Sharing], Ασφάλεια Πρωτοκόλλου Διαδικτύου [Internet Protocol Security] και Κωδικοποίηση Συστήματος Διαχείρισης Αρχείων [Encrypting File System]. Για το κάθε χαρακτηριστικό ασφάλειας, η ενότητα αυτή παρέχει μία περιληπτική περιγραφή καθώς επίσης και μία ανάλυση της επίδρασης σε επίπεδο ασφάλειας του κάθε χαρακτηριστικού και γενικές υποδείξεις για το πότε θα πρέπει αυτό να χρησιμοποιηθεί ή όχι. Είναι εκτός του σκοπού αυτού του οδηγού να καλύψει εις βάθος αυτά τα χαρακτηριστικά, οπότε υπάρχουν δείκτες ή σύνδεσμοι με επιπρόσθετες πληροφορίες όπου χρειάζονται.

---

[41] Περισσότερες πληροφορίες για την παρεμπόδιση εκτέλεσης δεδομένων στα Windows XP είναι διαθέσιμες από το 3ο μέρος (Memory Protection Technologies) του *Changes to Functionality in Microsoft Windows XP Service Pack 2*, το οποίο βρίσκεται εδώ: http://www.microsoft.com/downloads/details.aspx?FamilyID=7bd948d7-b791-40b6-8364-685b84158c78&DisplayLang=en, και από το MSKB στο άρθρο 875352, *A detailed description of the Data Execution Prevention (DEP) feature in Windows XP Service Pack 2, Windows XP Tablet PC Edition 2005, and Windows Server 2003*, το οποίο είναι διαθέσιμο εδώ: http://support.microsoft.com/?id=875352.

3.2.1 *Kerberos*

Σε κάποιο τομέα, τα Windows XP Professional παρέχουν υποστήριξη για την MIT Kerberos v.5 πιστοποίηση, όπως ορίζεται στο Internet Engineering Task Force (IETF) [42] Request for Comment (RFC) 1510.[43] Το πρωτόκολλο Kerberos συνετάχθει από τρία υπό-πρωτόκολλα: το Authentication Service (AS) Exchange, το Ticket-Granting Service (TGS) Exchange και το Client/Server (CS) Exchange. Το πρότυπο Kerberos v.5 μπορεί να χρησιμοποιηθεί μόνο σε αμιγώς περιβάλλοντα τομέα Windows.[44] Τα μέλη τομέα Windows χρησιμοποιούν το Kerberos ως το εκ προεπιλογής client/server πρωτόκολλο πιστοποίησης δικτύου, αντικαθιστώντας τις παλαιότερες και λιγότερο ασφαλής μεθόδους πιστοποίησης NTLM και LanManager (LM). Οι παλαιότερες μέθοδοι υποστηρίζονται ακόμη για να επιτρέπουν την πιστοποίηση των legacy Windows clients σε κάποιο περιβάλλον τομέα Windows. Οι standalone σταθμοί εργασίας Windows XP Professional και τα μέλη τομέων NT δεν χρησιμοποιούν το Kerberos για την τοπική πιστοποίηση, αλλά το παραδοσιακό NTLM. Επειδή το Kerberos παρέχει ισχυρότερη προστασία για τα διαπιστευτήρια του logon από ότι οι παλαιότερες μέθοδοι πιστοποίησης, θα πρέπει να χρησιμοποιείται όποτε είναι δυνατό. Το NIST συνιστά την απενεργοποίηση των LM και NTLM v1 σε SSLF και FDCC περιβάλλοντα, και την απενεργοποίηση του LM στα άλλα περιβάλλοντα.

3.2.2 *Υποστήριξη Έξυπνων Καρτών*

Στο παρελθόν, το αλληλεπιδρόν logon σήμαινε την ικανότητα πιστοποίησης του χρήστη σε κάποιο δίκτυο χρησιμοποιώντας μία φόρμα από διαμοιρασμένα διαπιστευτήρια, όπως ένα επαναδιατυπωμένο password. Τα Windows XP Professional υποστηρίζουν το αλληλεπιδρόν logon δημοσίου κλειδιού χρησιμοποιώντας ένα πιστοποιητικό X.509 v.3 που είναι αποθηκευμένο σε μία έξυπνη κάρτα [smart card]. (Αυτό μπορεί μόνο να χρησιμοποιηθεί για την καταχώρηση σε λογαριασμούς τομέα, όχι σε τοπικούς λογαριασμούς, εκτός εάν κάποιο έμμεσα εμπλεκόμενο λογισμικό αντικαταστήσει το ενσωματωμένο γραφικό ταυτοποίησης και πιστοποίησης [GINA].) Αντί κάποιου κωδικού, ο χρήστης δακτυλογραφεί ένα προσωπικό αριθμό ταυτοποίησης (Personal Identification Number [PIN]) στο GINA, και το PIN πιστοποιεί το χρήστη στην κάρτα. Αυτή η διεργασία είναι πλήρως ενοποιημένη με την εφαρμογή του Kerberos από τη Microsoft. Η πιστοποίηση βάσει έξυπνης κάρτας είναι κατάλληλη για τα SSLF περιβάλλοντα στα οποία είναι προαπαιτούμενη η ισχυρή πιστοποίηση και η πιστοποίηση του ενός παράγοντα (one-factor authentication) είναι ανεπαρκής. Οι έξυπνες κάρτες παρέχουν πιστοποίηση δύο παραγόντων (two-factor authentication), επειδή οι χρήστες πρέπει να κατέχουν τη φυσική έξυπνη κάρτα και να γνωρίζουν το PIN. Εάν χρησιμοποιούνται έξυπνες κάρτες ή άλλοι συμβολικοί τύποι πιστοποίησης (tokens), ο οργανισμός θα πρέπει να έχει μία πολιτική και διαδικασίες για να εκπαιδεύσει τους χρήστες για να χρησιμοποιούν σωστά τα tokens (πχ, να μην τα μοιράζονται με άλλους χρήστες) και να τα προστατεύουν (πχ, να αναφέρουν άμεσα την απώλεια ενός κλεμμένου token).

---

[42] Η κεντρική σελίδα του IETF βρίσκεται στη διεύθυνση http://www.ietf.org.
[43] Ολόκληρη η αναφορά RFC 1510 είναι διαθέσιμη εδώ: http://www.freesoft.org/CIE/RFC/1510/index.htm.
[44] Για περισσότερο λεπτομερή επεξήγηση για το πώς λειτουργεί το Kerberos σε περιβάλλοντα τομέα Windows, αναφερθείτε στο άρθρο 217098 του MSKB, *Basic Overview of Kerberos User Authentication Protocol in Windows 2000*, που είναι διαθέσιμο εδώ: http://support.microsoft.com/?id=217098.

3.2.3 *Διαμοιρασμός Σύνδεσης Διαδικτύου*

Ο Διαμοιρασμός Σύνδεσης Διαδικτύου (Internet Connection Sharing [ICS]) επιτρέπει σε ένα Windows XP σύστημα να διαμοιράζεται μία σύνδεση διαδικτύου με άλλους υπολογιστές.[45] Το ICS χρησιμοποιείται συχνά σε SOHO περιβάλλοντα (πχ, συνδεσιμότητα στο διαδίκτυο η οποία παρέχεται από ένα modem σε ένα σύστημα). Το ICS μπορεί να παρέχει υπηρεσία Μεταγλώττισης Διεύθυνσης Δικτύου (Network Address Translation [NAT]) σε άλλα συστήματα, το οποίο τα κρύβει στην ουσία από την κοινή θέα. Σε ένα κοινόχρηστο περιβάλλον, οι διαχειριστές τομέα μπορούν να αποτρέψουν τα συστήματα από το να χρησιμοποιήσουν το ICS μέσω του Group Policy. Τα φορητά Windows XP Professional συστήματα δεν χρειάζονται αναδιαμόρφωση ώστε να χρησιμοποιούν το ICS σε κάποιο SOHO δίκτυο και να μην το χρησιμοποιούν σε κάποιο κοινόχρηστο δίκτυο· το Group Policy το φροντίζει αυτόματα. Γενικά το ICS δεν θα πρέπει να χρησιμοποιείται σε επιχειρηματικά δίκτυα, αλλά αποτελεί λύση για SOHO περιβάλλοντα με περιορισμένη συνδεσιμότητα. Συνίσταται η χρήση τείχους προστασίας σε βάση host (host-based firewall), όπως το Windows Firewall στον host ο οποίος εκτελεί ICS. Όχι μόνο μπορεί το τείχος προστασίας να παρέχει προστασία στο ICS host, αλλά μπορεί επίσης να βοηθήσει στην προστασία των συστημάτων πίσω από το ICS, από επιθέσεις εξωτερικών παραγόντων.

3.2.4 *Ασφάλεια Πρωτοκόλλου Διαδικτύου*

Τα Windows XP περιέχουν μία εφαρμογή του προτύπου IETF Internet Protocol Security (IPSec), που ονομάζεται Windows IP Security.[46] Παρέχει υποστήριξη σε επίπεδο δικτύου για εμπιστευτικότητα και ακεραιότητα. Η εμπιστευτικότητα επιτυγχάνεται κωδικοποιώντας πακέτα, το οποίο εμποδίζει μη-εξουσιοδοτημένους παράγοντες από το να επιτύχουν πρόσβαση σε δεδομένα, όπως αυτά περνούν από τα δίκτυα. Η ακεραιότητα υποστηρίζεται υπολογίζοντας μία επαναδιατύπωση για κάθε πακέτο, που βασίζεται μερικώς σε κάποιο κρυφό κλειδί, διαμοιραζόμενο μεταξύ των αποστολέα και παραλήπτη, και στέλνοντας την επαναδιατύπωση μέσα στο πακέτο. Ο παραλήπτης θα υπολογίσει ξανά την επαναδιατύπωση και εάν ταιριάζει με την αρχική, τότε το πακέτο δεν αλλοιώθηκε κατά την μεταγωγή. Το Windows IP Security προσφέρει επίσης δυνατότητες φιλτραρίσματος πακέτων, τέτοιες όπως ο περιορισμός της κίνησης βάσει της IP διεύθυνσης της πηγής ή του προορισμού. Το Windows IP Security παρέχει μία λύση για την προστασία της διέλευσης των δεδομένων από δημόσια δίκτυα (πχ, το διαδίκτυο) και για την προστασία ευαίσθητων δεδομένων σε ιδιωτικά δίκτυα (πχ, ένα εταιρικό LAN). Επίσης χρησιμοποιείται ευρέως για την προστασία επικοινωνιών ασύρματου δικτύου σε enterprise και SOHO περιβάλλοντα. Χρησιμοποιώντας το Windows IP Security σε συνδυασμό με κάποιο προσωπικό τείχος προστασίας, όπως το Windows Firewall, μπορεί να παρέχει προστασία ενάντια σε επιθέσεις βάσει δικτύου, περιορίζοντας τόσο τα εισερχόμενα όσο και τα εξερχόμενα πακέτα.

3.2.5 *Κωδικοποίηση Συστήματος Διαχείρισης Αρχείων*

Η Κωδικοποίηση Συστήματος Διαχείρισης Αρχείων (Encrypting File System [EFS]) παρέχει στους χρήστες μία μέθοδο διαφανούς κωδικοποίησης ή αποκωδικοποίησης αρχείων και

---

[45] Περισσότερες πληροφορίες για το ICS, δείτε το άρθρο της Microsoft, *How to configure Internet Connection Sharing in Windows XP*, που είναι διαθέσιμο εδώ: http://support.microsoft.com/?id=306126.

[46] Περισσότερες πληροφορίες για την εφαρμογή του Windows IP Security, δείτε το *Step-by-Step Guide to Internet Protocol Security (IPSec)* στη διεύθυνση http://technet.microsoft.com/en-us/library/bb742429.aspx.

φακέλων που ανήκουν σε έναν NTFS διαμορφωμένο τόμο.[47] Στην πρότυπη έκδοση των Windows XP, το EFS μπορούσε να χρησιμοποιήσει είτε τον αλγόριθμο Triple Data Encryption Standard (3DES), ο οποίος είναι ισχυρότερη εκδοχή του Data Encryption Standard (DES), είτε τον Extended Data Encryption Standard (DESX).[48] Το Windows XP Service Pack 1 (SP1) προσέθεσε υποστήριξη για τον αλγόριθμο Advanced Encryption Standard (AES) και τα SP1, SP2 και SP3 συστήματα χρησιμοποιούν τον AES εκ προεπιλογής για την κωδικοποίηση του συστήματος διαχείρισης αρχείων. Αυτή είναι μία αλλαγή από τα Windows 2000, τα οποία χρησιμοποιούσαν τον DESX εκ προεπιλογής. Επιπλέον, το EFS τώρα διατηρεί την κωδικοποίηση, που σημαίνει πως οποιοδήποτε αρχείο ή φάκελος το οποίο έχει καθοριστεί ως κωδικοποιημένο, θα παραμείνει κωδικοποιημένο εάν μεταφερθεί σε κάποιο άλλο διαμορφωμένο NTFS σύστημα διαχείρισης αρχείων. Μία ακόμη μεγάλη διαφοροποίηση από τα Windows 2000 είναι ότι τα κωδικοποιημένα με το EFS αρχεία, μπορούν πλέον να διαμοιραστούν ανάμεσα σε πολλαπλούς χρήστες πάνω σε ένα δίκτυο.[49] Ωστόσο, τα αρχεία συνεχίζουν να μεταδίδονται δια μήκους του δικτύου, χωρίς να είναι κωδικοποιημένα (εκτός από όταν χρησιμοποιείται το Web Distributed Authoring and Versioning [WebDAV][50], το οποίο θα μεταδίδει κωδικοποιημένα τα αρχεία δια μήκους των δικτύων), έτσι οι χρήστες θα πρέπει να μεταφέρουν τα αρχεία μέσω διαφορετικού πρωτοκόλλου κωδικοποίησης, όπως το TLS ή το IPSec.[51] Το EFS είναι προτιμότερο να χρησιμοποιείται για την παροχή τοπικής κωδικοποίησης για αρχεία και είναι επίσης ιδιαίτερα χρήσιμο για φορητούς υπολογιστές και άλλα συστήματα με υψηλό κίνδυνο φυσικής επίθεσης.

3.3 Σύνοψη και Υποδείξεις

- ✓ Να μην εφαρμόζεται μία γέφυρα δικτύου χρησιμοποιώντας έναν Windows XP υπολογιστή, εκτός εάν είναι αυστηρά αναγκαίος για την διεκπεραίωση κάποιου καθήκοντος και έχει εκτελεστεί αποτίμηση και εξομάλυνση κινδύνου.

- ✓ Ενεργοποίηση του Remote Assistance μόνο εάν είναι διαμορφωμένο ώστε η χρήση του να είναι αυστηρά περιορισμένη και εάν η περίμετρος του δικτύου είναι διαμορφωμένη ώστε να αποτρέπει εξωτερικούς παράγοντες από τη χρησιμοποίησή του για να αποκτήσουν πρόσβαση σε εσωτερικά μηχανήματα.

- ✓ Χρησιμοποίηση του Remote Desktop μόνο εάν υφίστανται διάφορα άλλα στρώματα ελέγχων ασφάλειας, τα οποία αποτρέπουν την άμεση έκθεση του συστήματος στους επιτιθέμενους και οι διαχειριστές θα πρέπει να έχουν λάβει σοβαρά υπόψιν τους την επιχειρησιακή ανάγκη να υπάρχει απομακρυσμένη πρόσβαση στο σύστημα και θα πρέπει να έχουν σκεφτεί πιθανές εναλλακτικές λύσεις, οι οποίες δεν θα εκθέτουν το σύστημα σε επιθέσεις.

- ✓ Θα πρέπει τα συστήματα να είναι ρυθμισμένα έτσι ώστε να μην προσπαθούν αυτόματα να συνδέονται σε οποιοδήποτε ασύρματο δίκτυο.

---

[47] Για περισσότερες πληροφορίες δείτε το άρθρο της Microsoft, *Encrypting File System in Windows XP and Windows Server 2003*, στη διεύθυνση http://technet.microsoft.com/en-us/library/bb457065.aspx.
[48] Περισσότερα για τον αλγόριθμο DES δείτε εδώ: http://en.wikipedia.org/wiki/Data_Encryption_Standard.
[49] Ενώ οι χρήστες μπορούν να διαμοιραστούν κωδικοποιημένα EFS αρχεία, οι Ομάδες δεν μπορούν.
[50] Η κεντρική σελίδα του WebDAV βρίσκεται στη διεύθυνση http://www.webdav.org.
[51] Περισσότερα για το πρωτόκολλο TLS θα βρείτε εδώ: http://en.wikipedia.org/wiki/Secure_Sockets_Layer.

- ✓ Μόνο οι χρήστες με νόμιμη ανάγκη απομακρυσμένης πρόσβασης στο σύστημα να μπορούν να την έχουν.

- ✓ Ρύθμιση των συστημάτων να αποθηκεύουν κωδικούς λειτουργικού συστήματος και εφαρμογών μόνο σε περιβάλλοντα στα οποία υπάρχει η ελάχιστη φυσική απειλή, είτε να αποθηκεύουν κωδικούς που έχουν τετριμμένη τιμή.

- ✓ Απενεργοποίηση του UPnP εκτός εάν είναι απαραίτητο το χαρακτηριστικό της δυναμικής αναβάθμισης για τη συμβατότητα με άλλες συσκευές, όπως τα SOHO τείχη προστασίας.

- ✓ Απενεργοποίηση των LM και NTLM v1 σε SSLF και FDCC περιβάλλοντα.

- ✓ Χρήση host-based firewall σε συστήματα που εκτελείται το ICS.

- ✓ Χρησιμοποίηση του Windows IP Security για την προστασία της διέλευσης των δεδομένων από δημόσια δίκτυα και για την προστασία ευαίσθητων δεδομένων σε ιδιωτικά δίκτυα.

Κεφάλαιο 4

4. Domain Controller - Active Directory

Τα Windows NT χρησιμοποιούν την έννοια του τομέα, για τη διαχείριση της πρόσβασης σε ένα σύνολο δικτυακών πηγών (εφαρμογές, εκτυπωτές κοκ) για μια ομάδα χρηστών. Ο χρήστης χρειάζεται να εισέλθει στον τομέα για να αποκτήσει πρόσβαση στις πηγές, οι οποίες μπορεί να βρίσκονται σε έναν αριθμό διαφορετικών εξυπηρετητών στο δίκτυο. Ο τομέας συνδυάζει μερικά από τα πλεονεκτήματα της ομάδας εργασίας [workgroup] και του καταλόγου [directory]. Η ομάδα εργασίας είναι μία ομάδα χρηστών η οποία ανταλλάσσει μεταξύ της πρόσβαση σε πηγές διαφορετικών υπολογιστών και ο κατάλογος είναι μία ομάδα χρηστών η οποία διαχειρίζεται κεντρικά από έναν administrator. Η έννοια του τομέα δεν επιτρέπει μόνο την πρόσβαση σε πηγές που βρίσκονται σε διαφορετικούς εξυπηρετητές, αλλά επιτρέπει επιπλέον να δοθεί σε ένα τομέα πρόσβαση σε κάποιον άλλο τομέα μέσω *σχέσης εμπιστοσύνης*. Με αυτή τη διευθέτηση, ο χρήστης χρειάζεται να εισέλθει μόνο στον πρώτο τομέα για να έχει επιπλέον πρόσβαση και στις πηγές του δεύτερου.

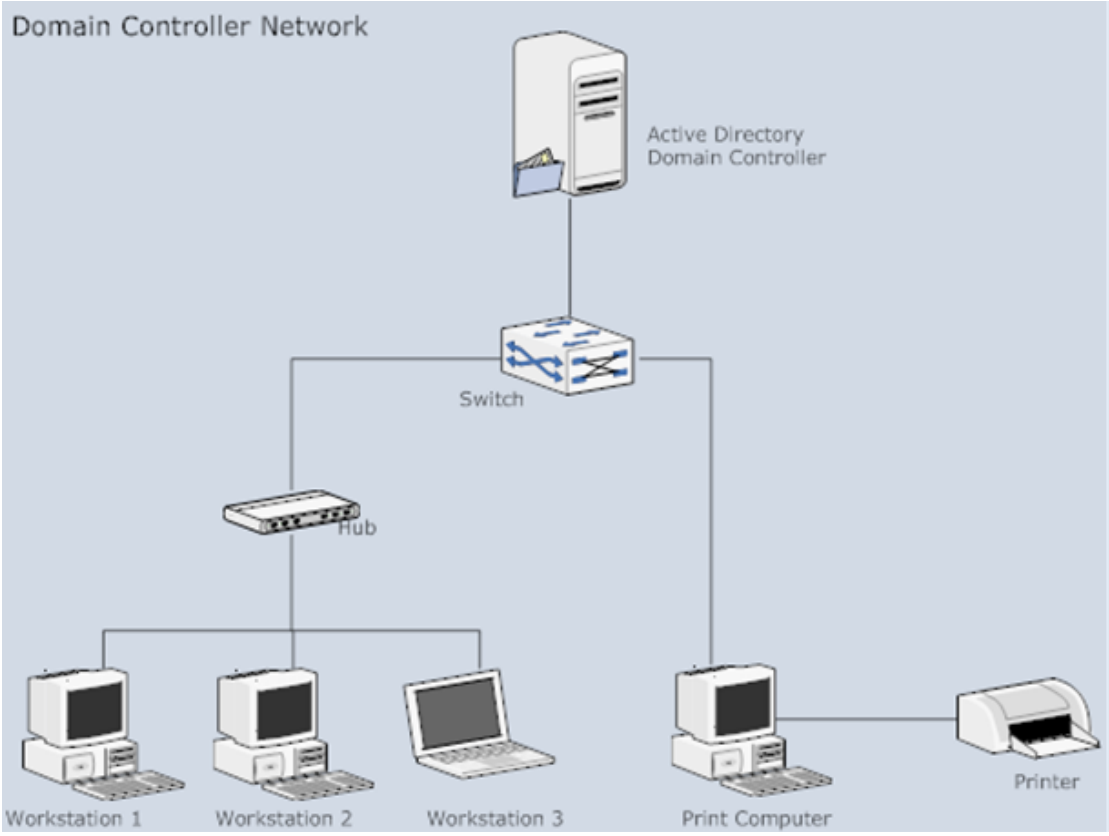
4.1 Domain Controller (Ελεγκτής Τομέα)

Στα συστήματα Windows Server, ο Ελεγκτής Τομέα ή αλλιώς **DC** (Domain Controller) είναι ένας εξυπηρετητής ο οποίος ανταποκρίνεται σε αιτήματα πιστοποίησης ασφάλειας (πχ login, έλεγχος δικαιωμάτων, κτλ) μέσα σε ένα τομέα του. Αν και οι DCs ποικίλουν ανάλογα με την έκδοση του Windows Server και τους λειτουργικούς τους ρόλους, σχεδόν όλοι οι μοντέρνοι DCs έχουν ορισμένα κοινά θεμελιώδη χαρακτηριστικά: ένα instance μίας βάσης δεδομένων LDAP,[52] ένα Κέντρο Διανομής Κλειδιού ή αλλιώς KDC (Key Distribution Center),[53] και ένα Κοινό Σύστημα Αρχείων Διαδικτύου ή αλλιώς CIFS (Common Internet File System),[54] μαζί με άλλες τοπικές και δικτυακές υπηρεσίες που χρειάζονται για την επικοινωνία εξυπηρετητή-πελάτη για κάθε μία από αυτές τις βασικές διεργασίες.

[52] Το Lightweight Directory Access Protocol, ή αλλιώς LDAP είναι ένα application protocol για διαμόρφωση και querying υπηρεσιών καταλόγου που εκτελούνται πάνω από το TCP/IP. Περισσότερες πληροφορίες είναι διαθέσιμες εδώ: http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol.

[53] Στην κρυπτογραφία ένα KDC είναι μέρος ενός κρυπτοσυστήματος το οποίο αποσκοπεί στην ελάττωση του κινδύνου που εγκυμονεί η ανταλλαγή κλειδιών. Περισσότερες πληροφορίες είναι διαθέσιμες εδώ: http://en.wikipedia.org/wiki/KDC.

[54] Το CIFS είναι μετονομασία του SMB (Server Message Block) πρωτοκόλλου που πραγματοποίησε η Microsoft.



Εικόνα 4-1 Domain Controller Network.

Στα Windows NT ο ένας DC ανά τομέα διαμορφώνεται ως ο Πρωταρχικός Ελεγκτής Τομέα ή αλλιώς **PDC** (Primary Domain Controller), ενώ όλοι οι άλλοι είναι Εφεδρικοί Ελεγκτές Τομέα ή αλλιώς **BDCs** (Backup Domain Controllers). Ένας BDC μπορεί να πιστοποιήσει χρήστες σε ένα τομέα, όμως όλες οι αναβαθμίσεις του τομέα μπορούν να υλοποιηθούν μόνο μέσω του PDC, ο οποίος μετέπειτα διαδίδει αυτές τις αλλαγές σε όλους τους BDCs του τομέα. Εάν ο PDC δεν είναι διαθέσιμος (ή δεν μπορεί να επικοινωνήσει με το χρήστη που αιτήθηκε της όποιας αλλαγής), η αναβάθμιση θα αποτύχει. Σε περίπτωση που ο PDC θα ήταν συνεχώς μη διαθέσιμος (πχ αποτυχία του μηχανήματος), ένας υπάρχον BDC θα μπορούσε να προαχθεί σε PDC. Εξαιτίας της σημαντικής φύσης του PDC, οι καλύτερες μέθοδοι προστάζουν πως ο PDC θα πρέπει να είναι αφιερωμένος αποκλειστικά και μόνο στις υπηρεσίες τομέα και να μη χρησιμοποιείται για υπηρεσίες αρχείων, εκτύπωσης και εφαρμογών, οι οποίες μπορούν να καθυστερήσουν ή ακόμα και να καταρρίψουν το σύστημα. Μερικοί διαχειριστές δικτύου πήγαν ένα βήμα πιο πέρα και έθεσαν online ένα dedicated BDC, με άμεσο σκοπό να είναι διαθέσιμος προς προαγωγή εάν αποτύχει ο PDC.

4.2 Δομή του Active Directory

Από τα Windows 2000 και μεταγενέστερα παρουσιάστηκε το **Active Directory** [AD], το οποίο ελαχιστοποίησε σημαντικά τη θεωρία των πρωτευόντων και των εφεδρικών ελεγκτών τομέα χάριν στο multi-master replication.[55] Ωστόσο, υπάρχει ακόμα ένας αριθμός από

[55] Το multi-master replication είναι μία μέθοδος κατασκευής πανομοιότυπου μιας βάσης δεδομένων, όπου επιτρέπεται να αποθηκεύει σε αυτήν δεδομένα, μία ομάδα υπολογιστών και να αναβαθμίζεται από κάθε μέλος

ρόλους που μπορεί να εκτελέσει ένας ελεγκτής τομέα, οι οποίοι ονομάζονται Flexible Single Master of Operation ή αλλιώς FSMO.[56] Τα FSMOs είναι ειδικά καθήκοντα ελεγκτή τομέα, που χρησιμοποιούνται εκεί όπου οι πρότυπες μέθοδοι μεταφοράς δεδομένων και αναβάθμισης είναι ανεπαρκείς. Ειδικότερα, τα FSMOs είναι καθήκοντα τα οποία δεν αρμόζουν στο multi-master replication και είναι πραγματοποιήσιμα μόνο με single-master βάση δεδομένων. Εάν χαθεί ο εξυπηρετητής ο οποίος εκτελεί έναν από αυτούς τους ρόλους, ο τομέας ενεργεί ακόμα και εάν ο εξυπηρετητής δεν θα είναι ξανά διαθέσιμος, κάποιος διαχειριστής μπορεί να καθορίσει έναν εναλλακτικό ελεγκτή τομέα ο οποίος θα αναλάβει να εκτελέσει αυτό το ρόλο. Η διαδικασία αυτή είναι γνωστή ως “κατάσχεση” ρόλου (“seizing” role).

4.2.1 *Αντικείμενα*

Το Active Directory [AD] είναι μία υπηρεσία καταλόγου που χρησιμοποιείται για την αποθήκευση πληροφοριών που αφορούν τις πηγές δικτύου κατά μήκος ενός τομέα, καθώς και τον διοικητικό συγκεντρωτισμό του δικτύου. Η δομή του AD είναι ένα ιεραρχικό πλαίσιο αντικειμένων. Τα αντικείμενα εμπίπτουν σε τρεις ευρείες κατηγορίες: τις πηγές (πχ εκτυπωτές), τις υπηρεσίες (πχ email) και τους χρήστες (λογαριασμοί χρηστών και ομάδες). Το AD παρέχει πληροφορίες στα αντικείμενα, οργανώνει τα αντικείμενα, ελέγχει την πρόσβαση και θέτει ασφάλεια.

Κάθε αντικείμενο αντιπροσωπεύει μία διακεκριμένη οντότητα [αναλόγως έναν υπολογιστή, έναν εκτυπωτή ή μία ομάδα] και τις ιδιότητές της. Συγκεκριμένα αντικείμενα μπορούν επίσης να είναι containers άλλων αντικειμένων. Ένα αντικείμενο είναι μοναδικά προσδιορισμένο από το όνομά του και έχει ένα σύνολο ιδιοτήτων, δηλαδή τα χαρακτηριστικά και οι πληροφορίες που μπορεί αυτό να περιέχει, που είναι ορισμένο από ένα σχήμα, το οποίο επίσης καθορίζει το είδος του αντικειμένου που μπορεί να αποθηκευτεί στο AD.

Αντικείμενα Sites

Το αντικείμενο ιστότοπος ή **Site** μέσα στο AD αντιπροσωπεύει μία φυσική γεωγραφική τοποθεσία όπου φιλοξενούνται δίκτυα. Τα sites μπορούν να χρησιμοποιηθούν για την ανάθεση των Group Policy Objects, για να διευκολύνουν την ανακάλυψη πηγών, για τη διαχείριση του active directory replication και τη διαχείριση της κίνησης των δικτυακών συνδέσμων. Τα Sites μπορούν να αντιστοιχηθούν σε άλλα Sites και στα Site-linked αντικείμενα μπορεί να ανατεθεί μία τιμή κόστους η οποία αντιπροσωπεύει την ταχύτητα, την αξιοπιστία, τη διαθεσιμότητα ή την οποιαδήποτε πραγματική ιδιότητα ή φυσική πηγή. Στα αντικείμενα Sites μπορεί επίσης να ανατεθεί ένα schedule.

αυτής της ομάδας. Το ίδιο το multi-master replication σύστημα είναι υπεύθυνο για την διάδοση των τροποποιήσεων των δεδομένων που πραγματοποίησε το κάθε μέλος στην υπόλοιπη ομάδα, καθώς και για την επίλυση των όποιων αντιφάσεων που μπορεί να προκληθούν μεταξύ ταυτόχρονων αλλαγών που πραγματοποίησαν διαφορετικά μέλη. Περισσότερες πληροφορίες είναι διαθέσιμες εδώ: http://en.wikipedia.org/wiki/Multi-master_replication.

[56] Περισσότερες πληροφορίες για τα FISMOs είναι διαθέσιμες εδώ: http://en.wikipedia.org/wiki/Flexible_single_master_operation.

Αντικείμενα Forests – Trees – Domains

Το πλαίσιο του Active Directory που κρατάει τα αντικείμενα μπορεί να παρατηρηθεί από έναν αριθμό επιπέδων. Στην κορυφή της δομής βρίσκεται το δάσος ή αλλιώς **forest**. Το forest είναι μια συλλογή από το κάθε αντικείμενο, τις ιδιότητές του και των κανόνων, δηλαδή της σύνταξης των ιδιοτήτων, μέσα στο AD. Τα **forest**, **tree** (δέντρο) και **domain** (τομέας) είναι τα λογικά μέρη σε ένα AD δίκτυο.

Το AD forest περιέχει ένα ή περισσότερα μεταβατικά και έμπιστα αντιστοιχισμένα trees. Ένα tree είναι μία συλλογή από ένα ή περισσότερα domains και domain trees που είναι και πάλι σε μία μεταβατική έμπιστη ιεραρχία. Τα domains προσδιορίζονται από την DNS ονομαστική δομή τους, το namespace.[57] Τα αντικείμενα που κρατούνται μέσα σε ένα domain μπορούν να ομαδοποιηθούν σε containers που ονομάζονται Organizational Units [OUs]. Τα OUs δίνουν σε ένα domain ιεραρχία, διευκολύνουν τη διαχείρισή του και μπορούν να δώσουν την εικονικότητα της δομής του AD στον οργανισμό, με γεωγραφικούς και οργανωτικούς όρους. Τα OUs μπορούν να περιέχουν άλλα OUs, στην πραγματικότητα τα domains είναι containers υπό αυτή την έννοια, και μπορούν να κρατούν πολλαπλά εμφωλευμένα OUs. Η Microsoft προτείνει όσο το δυνατό λιγότερα domains μέσα στο AD και την αναδοχή της παραγωγής της δομής και της βελτίωσης της εφαρμογής των πολιτικών και της διαχείρισης στα OUs. Το OU είναι το κοινό επίπεδο στο οποίο εφαρμόζονται οι Πολιτικές Ομάδων, οι οποίες είναι οι ίδιες αντικείμενα του AD και ονομάζονται Group Policy Objects [GPOs], ωστόσο οι πολιτικές μπορούν επίσης να εφαρμοστούν σε domains ή sites. Το OU είναι το επίπεδο στο οποίο ανατίθενται κατά γενικό κανόνα οι διαχειριστικές δυνάμεις, αλλά το granular delegation μπορεί να εκτελεστεί και σε μεμονωμένα αντικείμενα ή ιδιότητες.

Το AD επίσης υποστηρίζει τη δημιουργία ομαδοποιήσεων Sites, τα οποία είναι περισσότερο φυσικά παρά λογικά, οι οποίες καθορίζονται από ένα ή περισσότερα IP υποδίκτυα. Τα Sites διακρίνονται σε χαμηλής ταχύτητας (πχ Wan, VPN) και υψηλής ταχύτητας (πχ LAN) συνδέσεις, είναι ανεξάρτητα από τη δομή του domain και των OUs και είναι κοινά κατά μήκος όλου του forest. Τα Sites χρησιμοποιούνται για τον έλεγχο της κίνησης του δικτύου που παράγεται από το replication, καθώς και να παραπέμπει τους πελάτες στους πλησιέστερους DCs.

Ο πραγματικός διαχωρισμός της πληροφοριακής υποδομής του οργανισμού στην ιεραρχία του ενός ή περισσότερων τομέων και των top-level OUs είναι μία απόφαση κλειδί. Κοινά μοντέλα είναι ανά επιχειρησιακή μονάδα, ανά γεωγραφική τοποθεσία, ανά υπηρεσία IT, ή ανά τύπο αντικειμένου, τα οποία μοντέλα χρησιμοποιούνται συχνά και συνδυαστικά. Τα OUs θα πρέπει να δομούνται πρωτίστως για τη διευκόλυνση του διαχειριστικού delegation και, δευτερευόντως, για τη διευκόλυνση της μεθόδου πολιτικής ομάδας. Μολονότι τα OUs σχηματίζουν ένα διαχειριστικό όριο, το μόνο πραγματικό όριο ασφάλειας είναι το ίδιο το forest και ο διαχειριστής κάποιου τομέα του forest θα πρέπει να θεωρείται και να είναι έμπιστος δια μήκους όλων των τομέων ενός forest.

---

[57] Γενικά το namespace είναι ένα κενό container το οποίο παρέχει ένα πλαίσιο για τα αντικείμενα (πχ ονόματα, τεχνικούς όρους ή λέξεις). Για περισσότερες πληροφορίες ανατρέξτε εδώ: http://en.wikipedia.org/wiki/Namespace_(computer_science).

Οι πληροφορίες του AD κρατούνται φυσικά σε έναν ή περισσότερους ισόβαθμους DCs, αντικαθιστώντας το PDC/BDC μοντέλο. Ο κάθε DC έχει ένα αντίγραφο του AD˙ οι αλλαγές σε έναν υπολογιστή συγχρονίζονται (συγκλίνουν) μεταξύ όλων των DC υπολογιστών μέσω του multi-master replication. Οι εξυπηρετητές που έχουν προσχωρήσει σε ένα AD, και οι οποίοι δεν είναι DCs, ονομάζονται Εξυπηρετητές Μέλη (Server Members). Η βάση δεδομένων του AD είναι χωρισμένη σε διαφορετικά αποθηκευτικά μέρη ή διαμερίσματα (partitions). Το διαμέρισμα "Schema" περιέχει τον προσδιορισμό των κλάσεων αντικειμένων και των ιδιοτήτων μέσα σε ένα Forest. Το διαμέρισμα "Configuration" περιέχει πληροφορίες για τη φυσική δομή και τη διάταξη του forest (όπως την τοπολογία ιστότοπου). Το διαμέρισμα "Domain" κρατάει όλα τα αντικείμενα που δημιουργήθηκαν μέσα σε αυτό τον τομέα. Τα δύο πρώτα διαμερίσματα δημιουργούν πανομοιότυπα σε όλους τους DCs μέσα στο forest. Το διαμέρισμα Domain δημιουργεί πανομοιότυπα μόνο στους DCs που βρίσκονται μέσα στον ίδιο του τον τομέα. Ένα υποσύνολο αντικειμένων στο διαμέρισμα Domain δημιουργεί επίσης πανομοιότυπα στους DCs που έχουν διαμορφωθεί ως γενικοί κατάλογοι (global catalogs).

Σε forests τα οποία έχουν πολλαπλούς τομείς (multi-domain forests), η βάση του AD διαμερίζεται. Καθ' αυτό τον τρόπο, κάθε τομέας διατηρεί μία λίστα που περιέχει μόνο τα αντικείμενα που ανήκουν σε αυτόν. Έτσι, για παράδειγμα, όταν ένας χρήστης δημιουργείται σε κάποιο τομέα, τότε θα καταχωρηθεί στη λίστα των DCs αυτού και μόνο του τομέα. Οι εξυπηρετητές γενικού καταλόγου (GC Servers) χρησιμοποιούνται για να παρέχουν γενική καταχώριση λιστών για όλα τα αντικείμενα ενός Forest. Ο γενικός κατάλογος κρατείται σε DCs που είναι διαμορφωμένοι ως GC Servers, οι οποίοι παράγουν πανομοιότυπα όλων των αντικειμένων από όλους τους τομείς, στους εαυτούς τους, και ως εκ τούτου παρέχουν τη γενική καταχώριση λιστών. Ωστόσο, για να μειωθεί η κίνηση του replication και να κρατηθεί μικρή σε μέγεθος η βάση δεδομένων του GC, παράγονται πανομοιότυπα επιλεγμένων μόνο ιδιοτήτων του κάθε αντικειμένου. Αυτό ονομάζεται partial attribute set (PAS) και μπορεί να τροποποιηθεί, τροποποιώντας το schema και επιλέγοντας τις ιδιότητες για τις οποίες θα δημιουργηθούν πανομοιότυπα στον GC.

Αντίθετα με προηγούμενες εκδόσεις των Windows, οι οποίες χρησιμοποιούσαν το NetBIOS για να επικοινωνούν, το AD είναι πλήρως ενοποιημένο με τα DNS[58] και TCP/IP. Για να είναι πλήρως λειτουργικός ο DNS εξυπηρετητής θα πρέπει να υποστηρίζει SRV resource records ή service records.[59] Ακόμα, το AD είναι απαραίτητο στοιχείο για πολλές υπηρεσίες των Windows μέσα σε έναν οργανισμό, όπως το Exchange.[60]

4.3 Εγκατάσταση και Εφαρμογή του Active Directory

Σε αυτή την ενότητα θα δούμε βήμα προς βήμα την εγκατάσταση και διαμόρφωση ενός Domain Controller με Active Directory και θα δοθούν παραδείγματα δημιουργίας αντικειμένων (πχ ομάδες, υπολογιστές, χρήστες). Η εγκατάσταση του Active Directory μπορεί να πραγματοποιηθεί σε συστήματα Windows 2000 Server, Windows Server 2003 και Windows Server 2008.

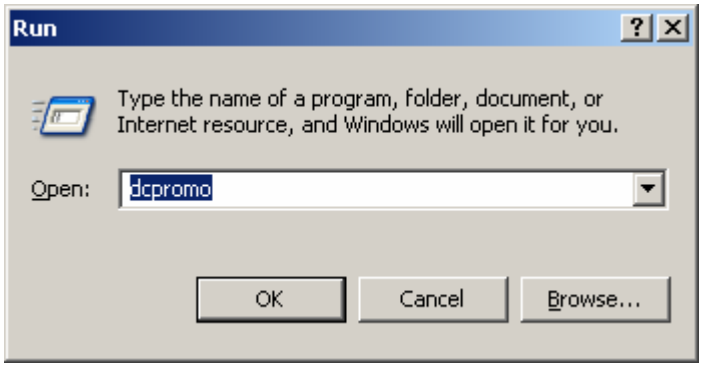
---

[58] Για την ακρίβεια το DNS είναι απαραίτητο για την ορθή λειτουργία του AD.
[59] Περισσότερες πληροφορίες είναι διαθέσιμες από το site υποστήριξης της Microsoft στη διεύθυνση: http://technet.microsoft.com/en-us/library/cc961719.aspx.
[60] Στη διεύθυνση http://en.wikipedia.org/wiki/Microsoft_Exchange_Server, μπορείτε να αντλήσετε πληροφορίες για τον Microsoft Exchange Server.

4.3.1 *Εγκατάσταση του Active Directory*

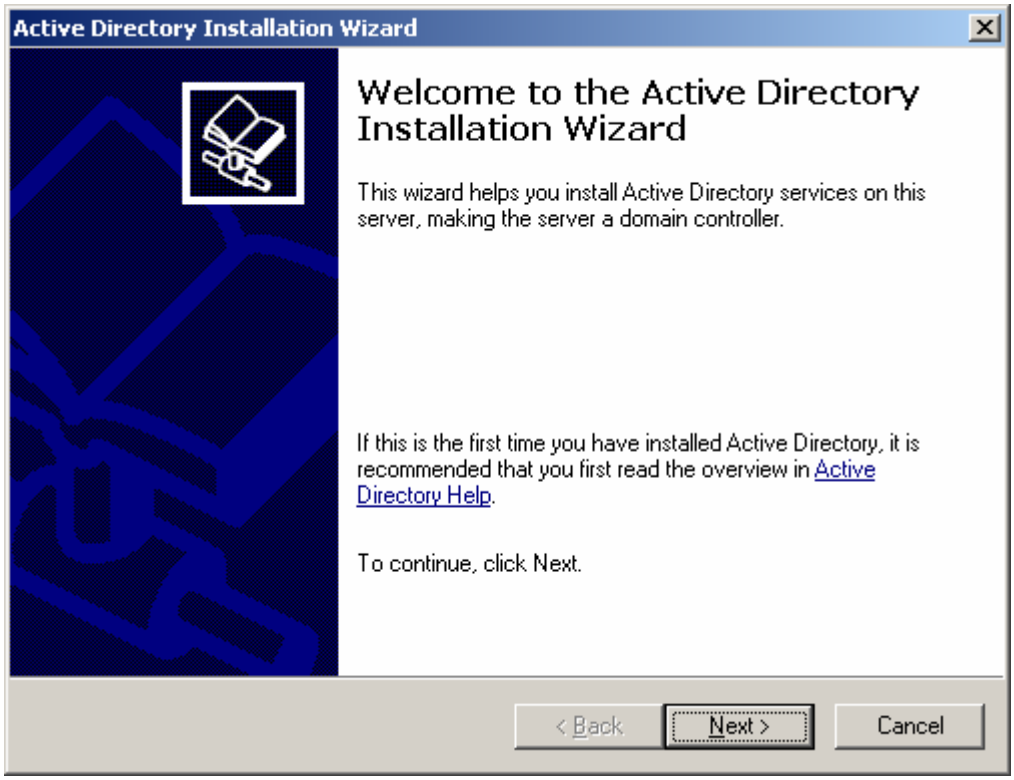
Για να εκκινήσουμε την εγκατάσταση σε κάποιο τέτοιο σύστημα ακολουθούμε τα παρακάτω βήματα:

1. Εκκίνηση του οδηγού εγκατάστασης χρησιμοποιώντας τη **Run** εντολή του **Start** menu γράφοντας **dcpromo**.



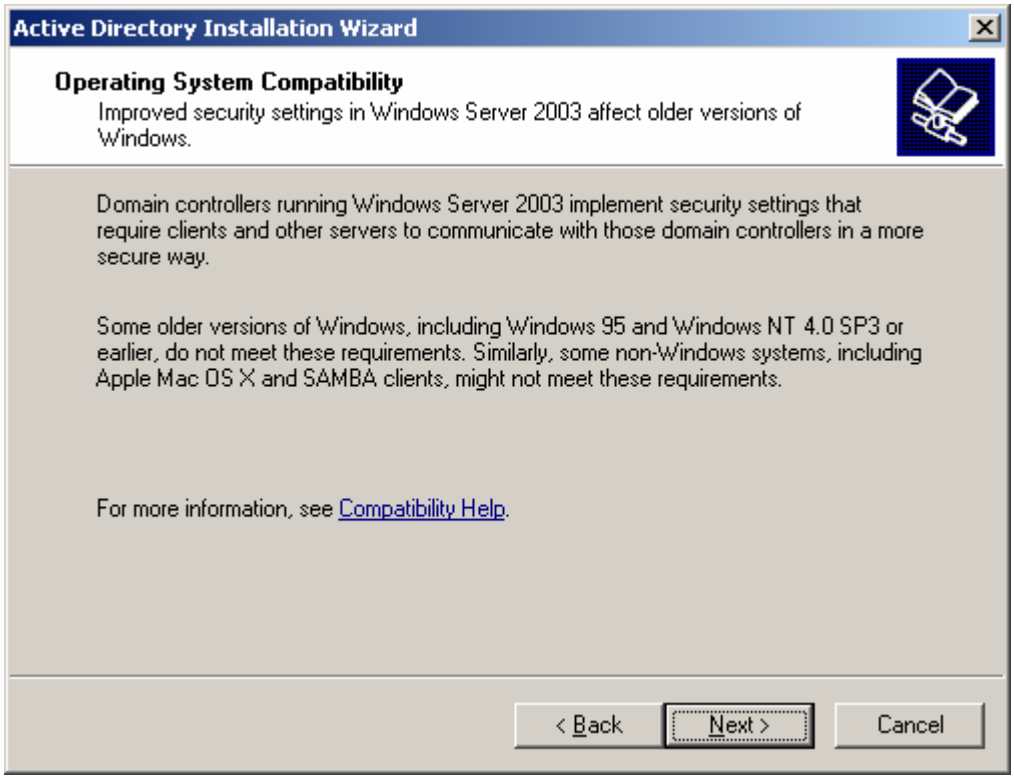
Εικόνα 4-2 Εντολή dcpromo.

2. Πατάμε **Next**.



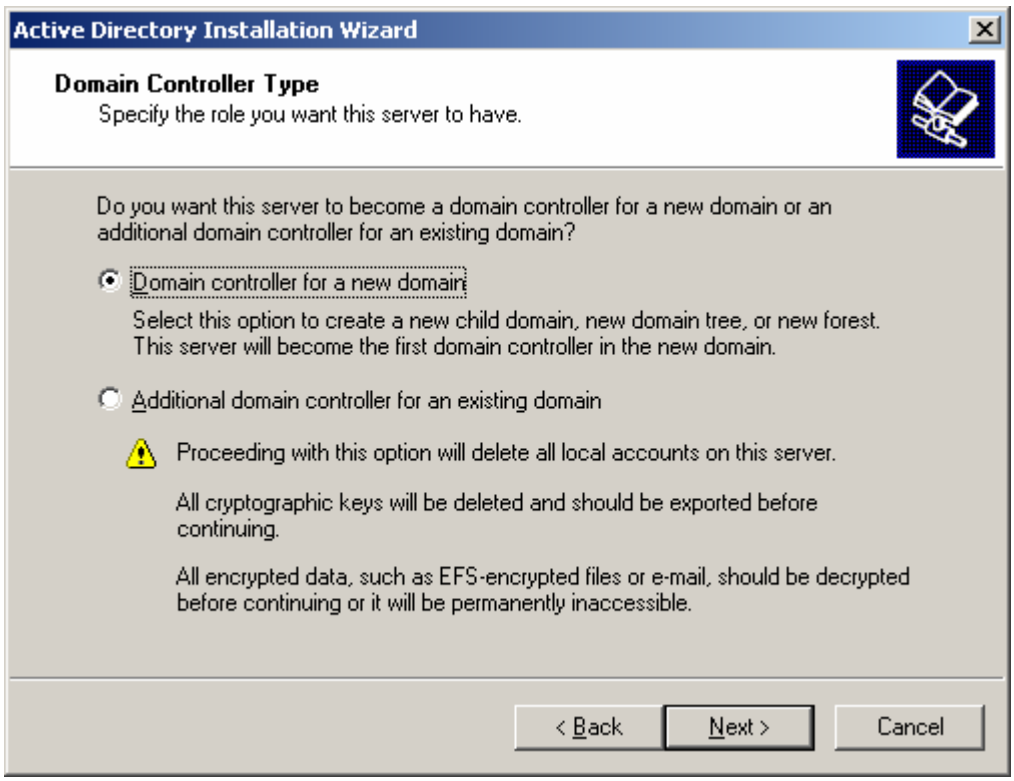
Εικόνα 4-3 Active Directory Installation Wizard βήμα 1ο.

3. Πατάμε και πάλι **Next**.



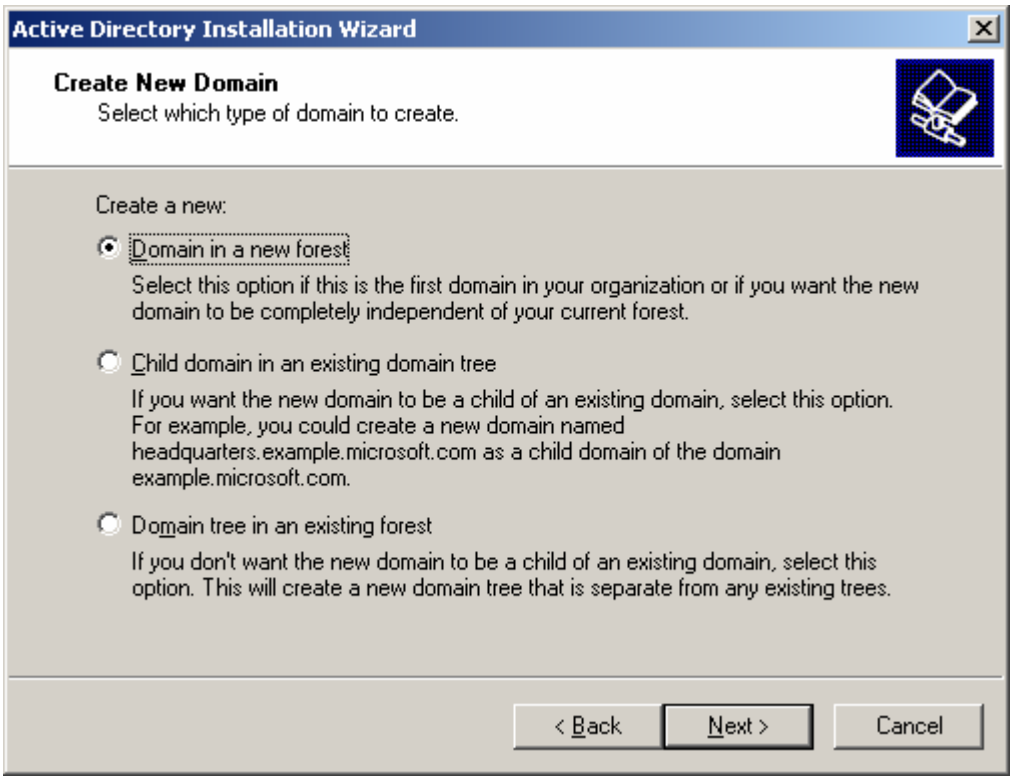
Εικόνα 4-4. Active Directory Installation Wizard βήμα 2ο.

4. Εφόσον είναι η πρώτη και μοναδική εγκατάσταση στο σύστημα επιλέγουμε **Domain controller for a new domain**, και πατάμε **Next.**



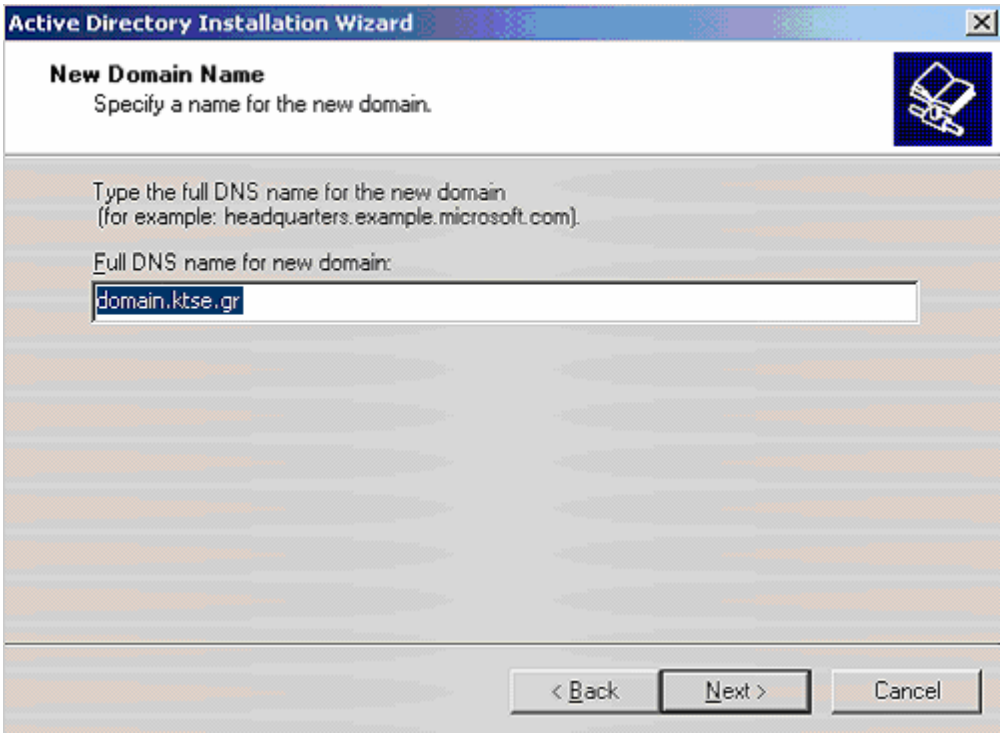
Εικόνα 4-5. Active Directory Installation Wizard βήμα 3ο.

5. Επιλέγουμε **Domain in a new forest** και πατάμε **Next**.



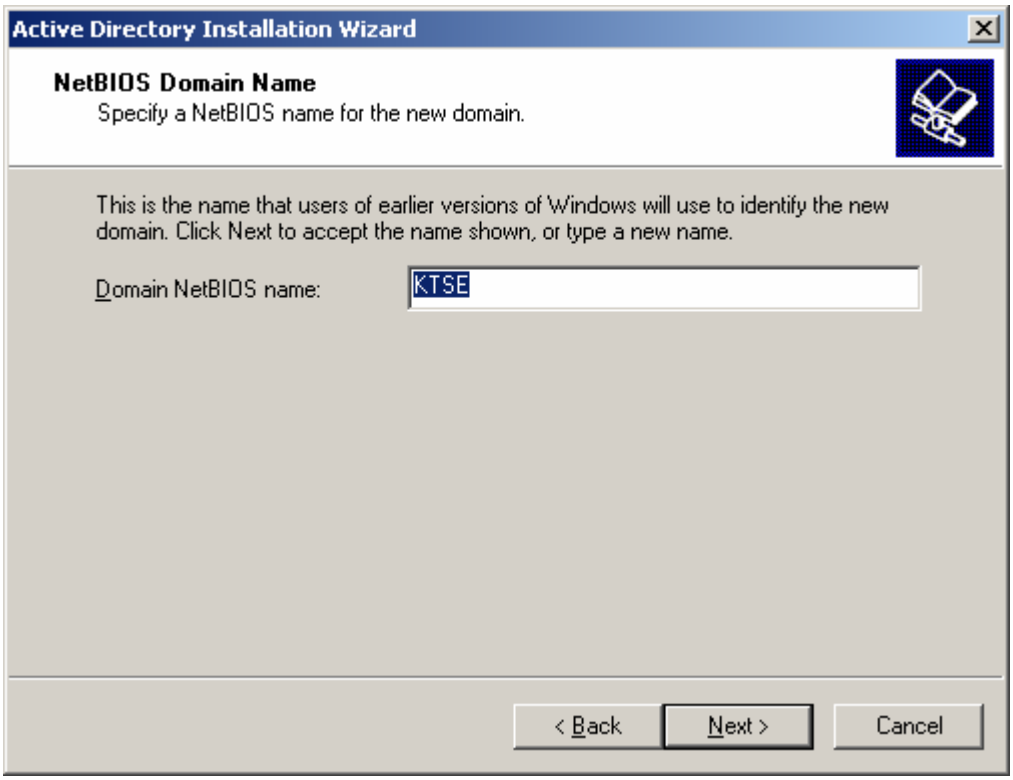
Εικόνα 4-6. Active Directory Installation Wizard βήμα 4ο.

6. Ονομάζουμε το καινούργιο domain και πατάμε **Next**.



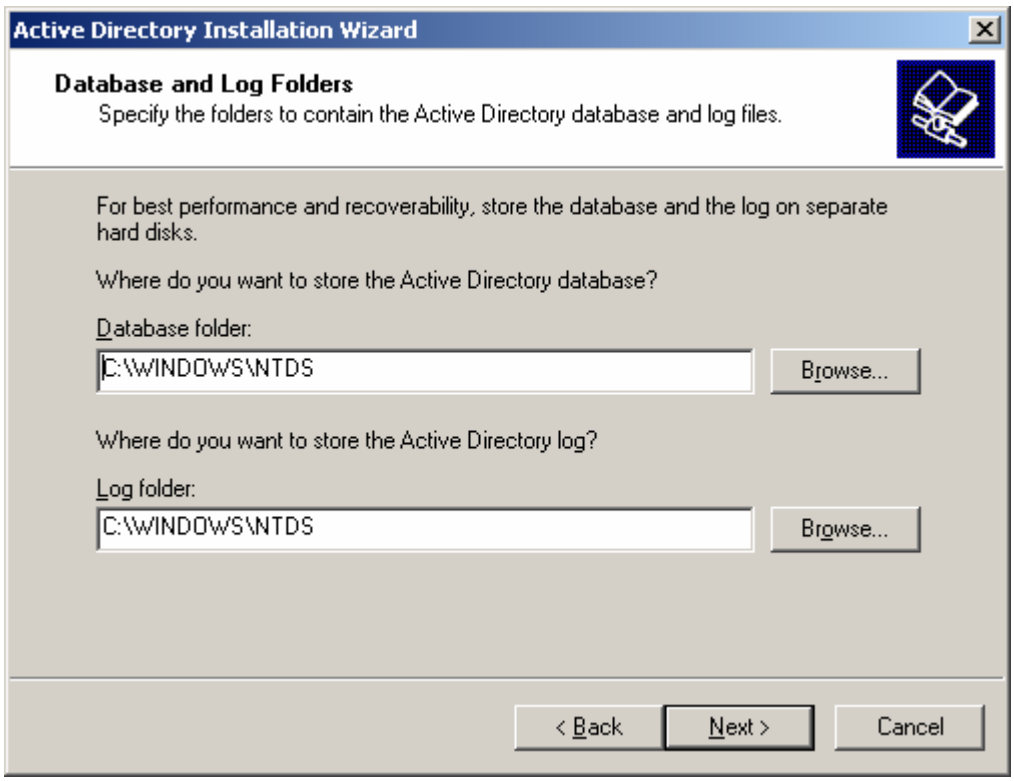
Εικόνα 4-7. Active Directory Installation Wizard βήμα 5ο.

7. Θέτουμε το NetBIOS όνομα του domain και πατάμε **Next**.



Εικόνα 4-8. Active Directory Installation Wizard βήμα 6ο.

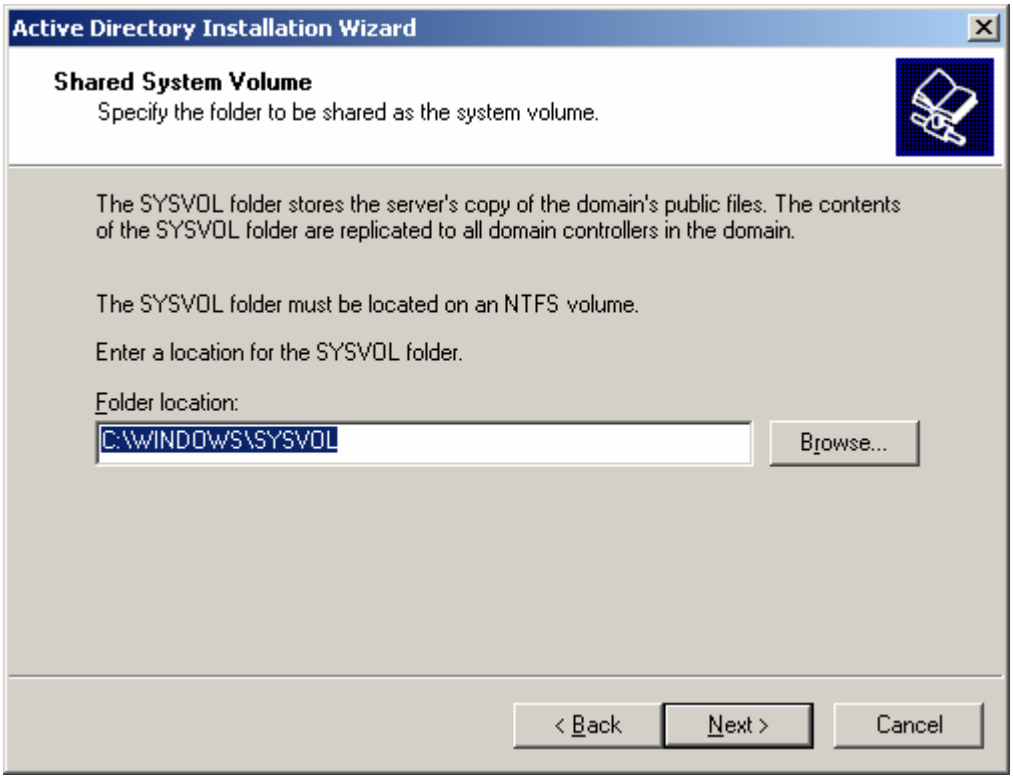
8. Αφήνουμε τους προεπιλεγμένους καταλόγους αποθήκευσης των logs και της βάσης δεδομένων και πατάμε **Next**.



Εικόνα 4-9. Active Directory Installation Wizard βήμα 7ο.

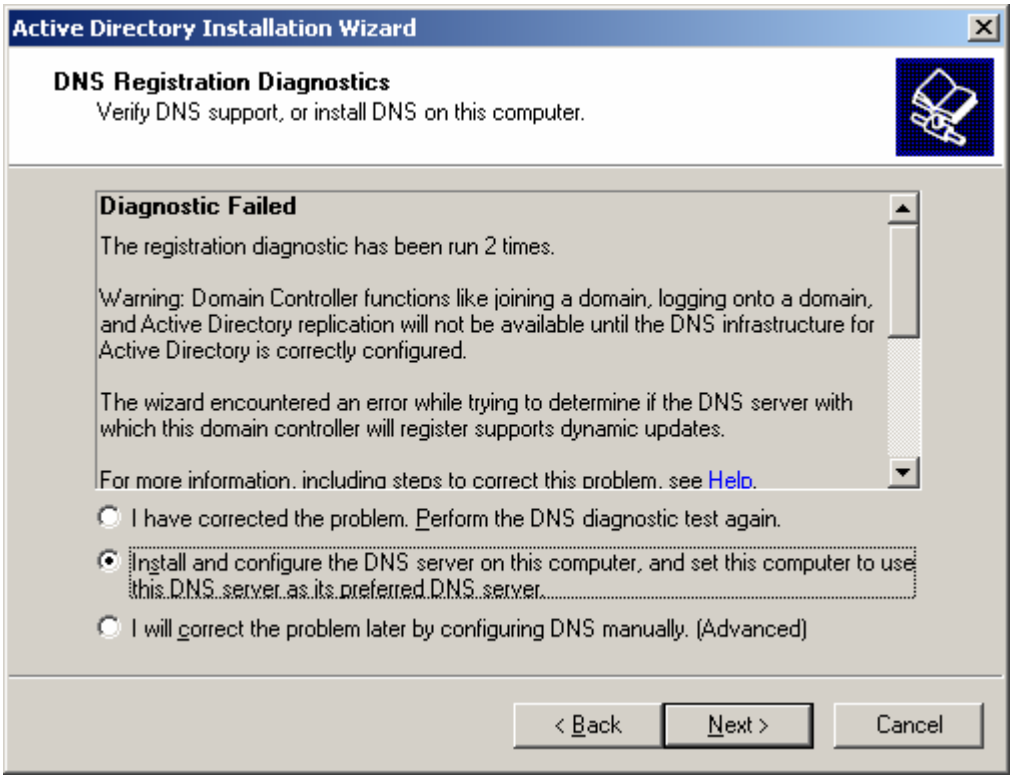
9. Αφήνουμε τον προεπιλεγμένο κατάλογο αποθήκευσης των αντιγράφων των δημόσιων αρχείων του domain και πατάμε **Next.**[61]

[61] Προσοχή, σε περίπτωση που θέταμε ένα άλλο κατάλογο, αυτός θα έπρεπε να είναι σε κάποιο NTFS διαμορφωμένο διαμέρισμα.



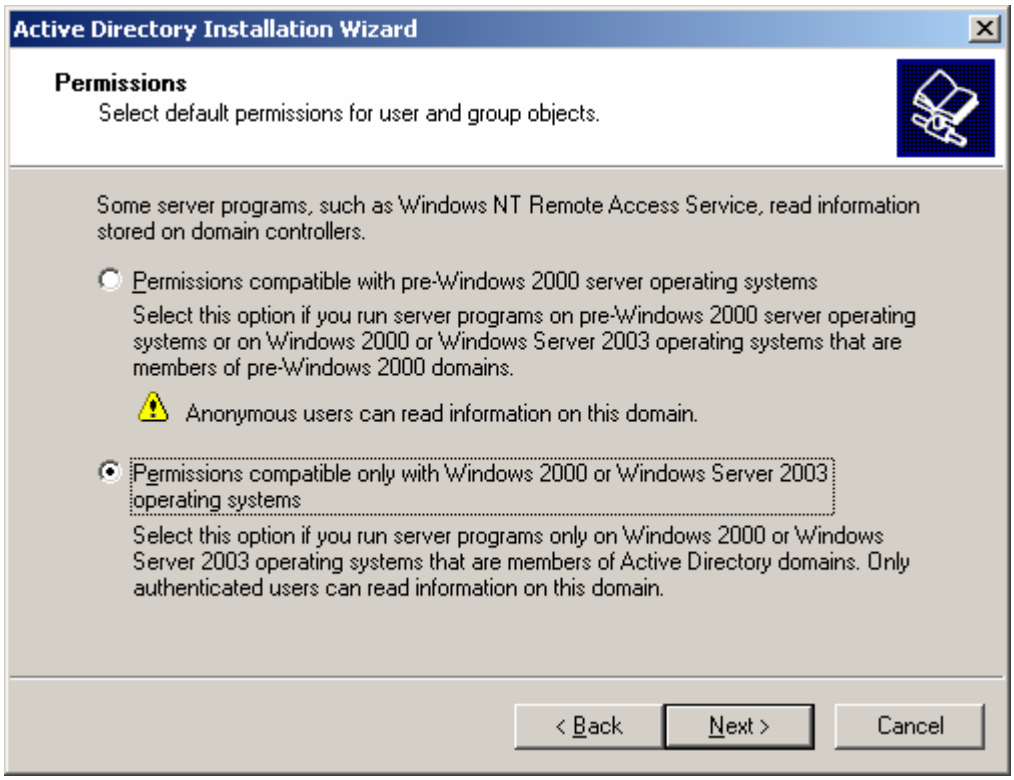
Εικόνα 4-10. Active Directory Installation Wizard βήμα 8ο.

10. Το μήνυμα που παίρνουμε σε αυτή τη οθόνη σημαίνει πως δεν έχουμε διαμορφώσει την DNS υπηρεσία στον εξυπηρετητή. Επιλέγουμε **Install and configure** και πατάμε **Next.**



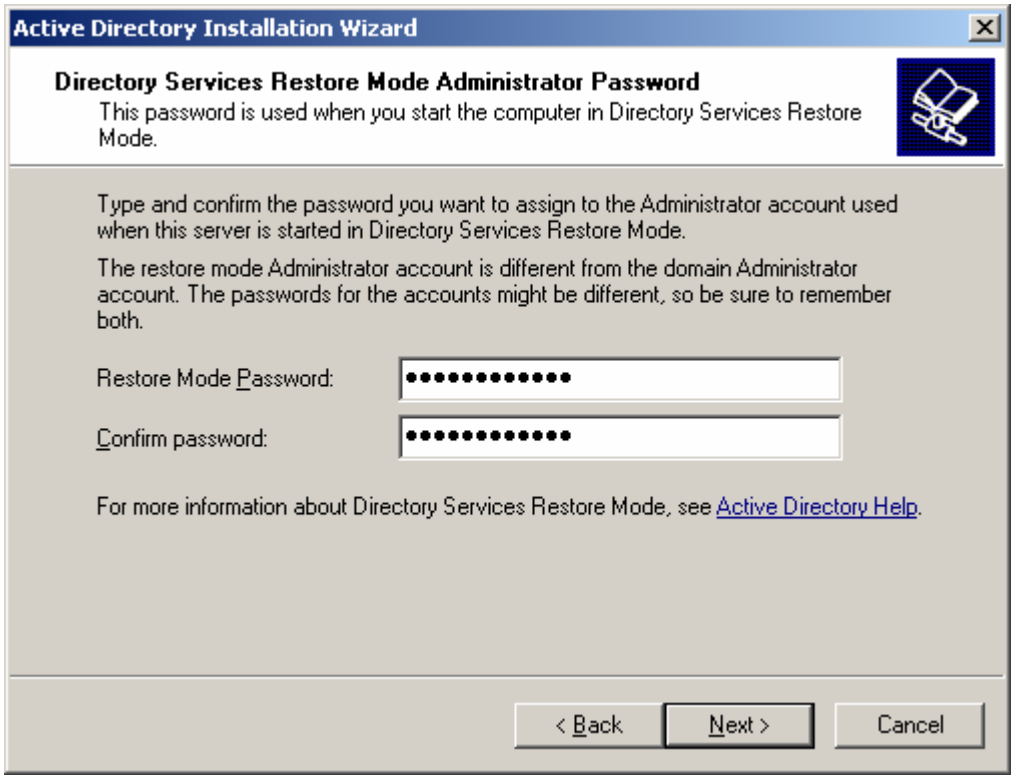
Εικόνα 4-11. Active Directory Installation Wizard βήμα 9ο.

11. Εφόσον δεν θα υπάρξει πρόσβαση από κάποιον εξυπηρετητή προγενέστερο της έκδοσης Windows 2000 Server, επιλέγουμε **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems** και πατάμε **Next**.



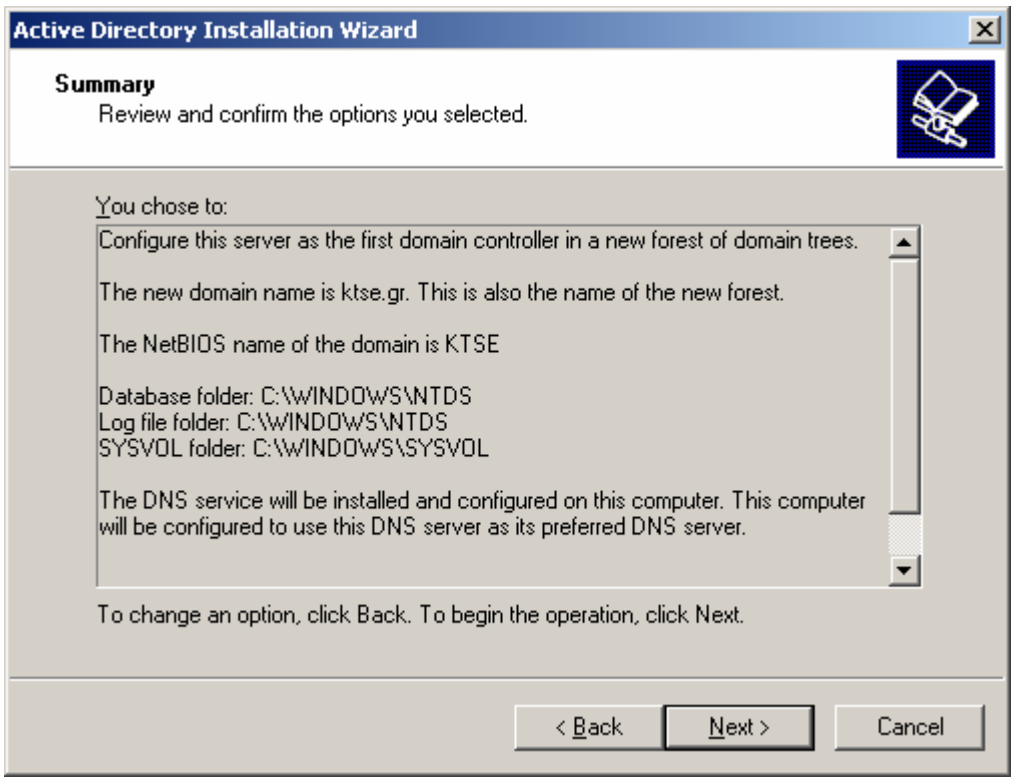
Εικόνα 4-12. Active Directory Installation Wizard βήμα 10ο.

12. Θέτουμε το **Restore mode password** το οποίο μπορεί να χρειαστεί στο διαχειριστή σε περίπτωση αποτυχίας του εξυπηρετητή, οπότε θα πρέπει να είναι εύκολο να το θυμάται αλλά δύσκολο να εικαστεί, και πατάμε **Next.**



Εικόνα 4-13. Active Directory Installation Wizard βήμα 11ο.

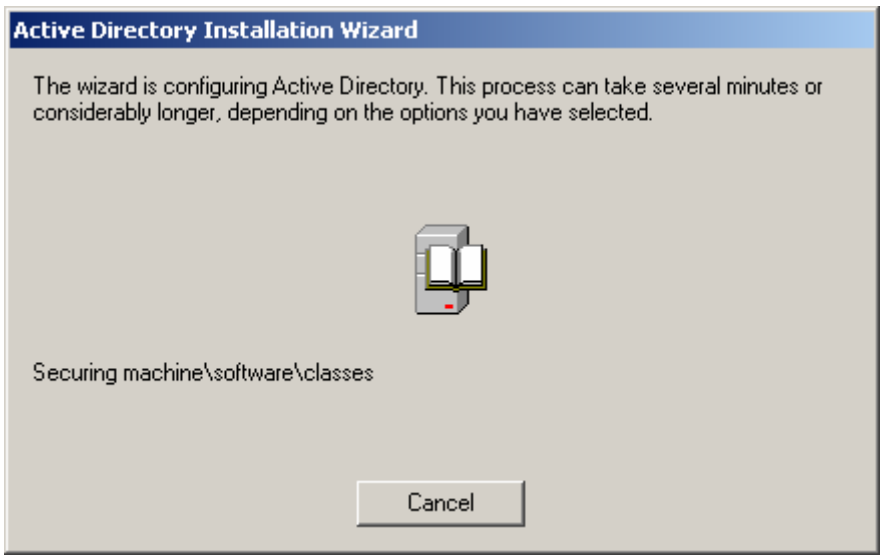
13. Παρατηρούμε την περίληψη όσων πρόκειται να εφαρμοστούν και εφόσον είμαστε σύμφωνοι πατάμε **Next.**



Εικόνα 4-14. Active Directory Installation Wizard βήμα 12ο.

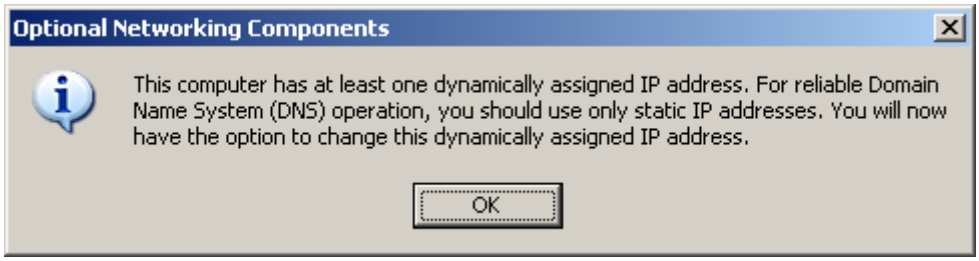
14. Η εφαρμογή της εγκατάστασης ξεκινάει σε αυτό το σημείο και μπορεί να διαρκέσει ορισμένα λεπτά. Δημιουργείται το forest και οι απαραίτητοι κατάλογοι καθώς και η εγκατάσταση της υπηρεσίας DNS.

Εικόνα 4-15. Active Directory Installation Wizard βήμα 13ο Α.



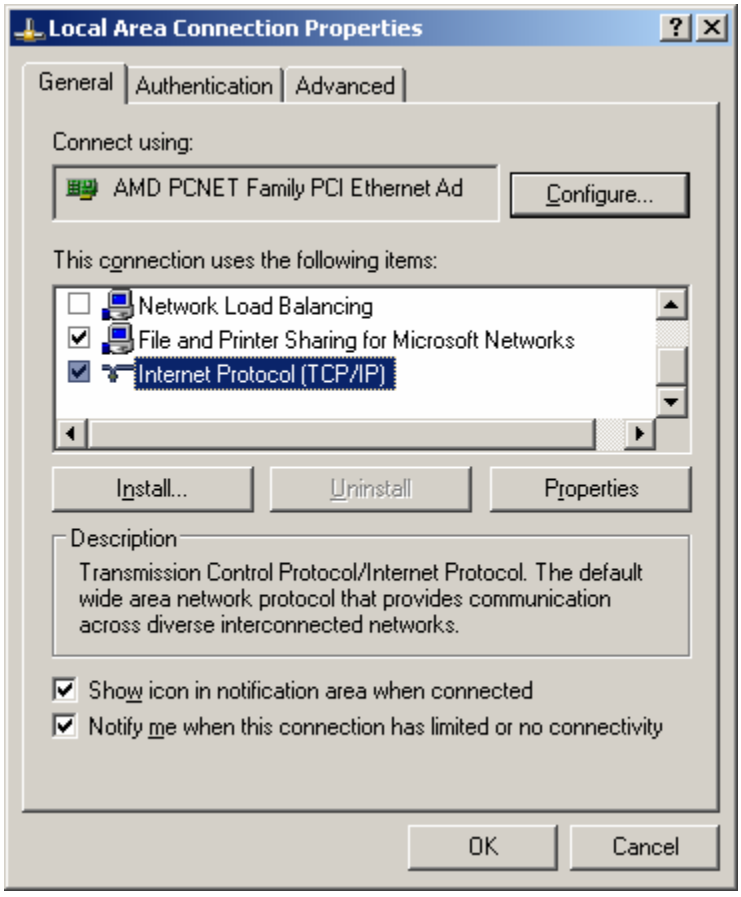
Εικόνα 4-16. Active Directory Installation Wizard βήμα 13ο Β.

15. Σε αυτό το σημείο ο DC έχει πάρει μία δυναμική διεύθυνση από το DHCP και καλούμαστε να δώσουμε μία στατική IP διεύθυνση στο μηχάνημα. Πατάμε **OK** για να εκκινήσουμε τη διαδικασία.



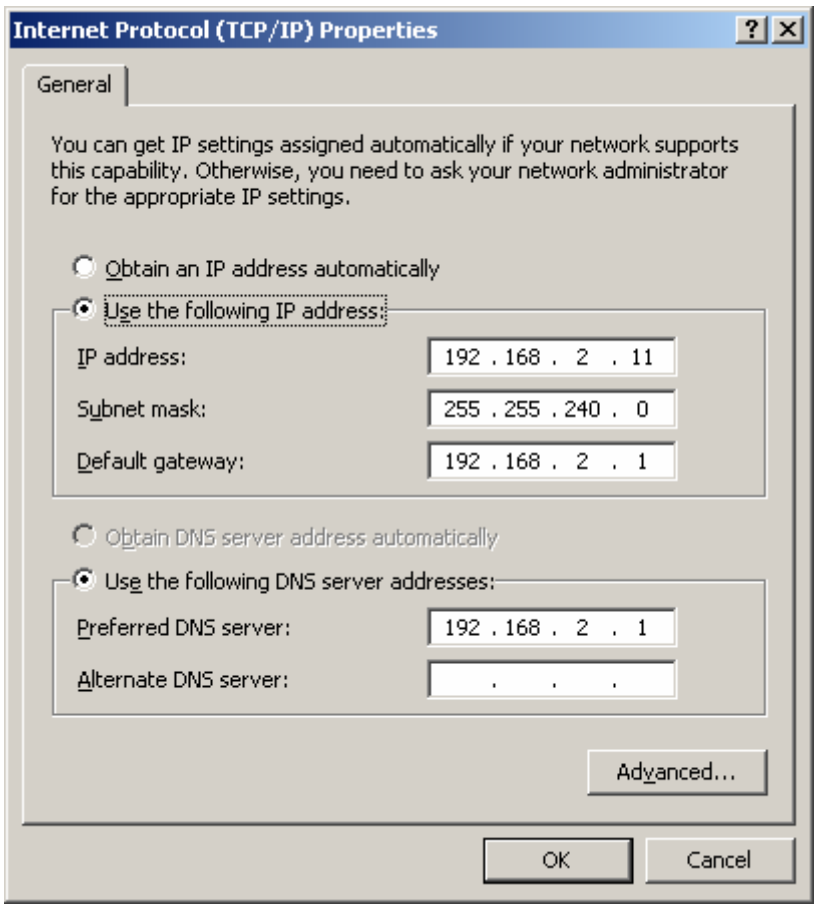
Εικόνα 4-17. Active Directory Installation Wizard βήμα 14ο: Network Configuration.

16. Επιλέγουμε **Internet Protocol (TCP/IP)** και πατάμε **Properties**.



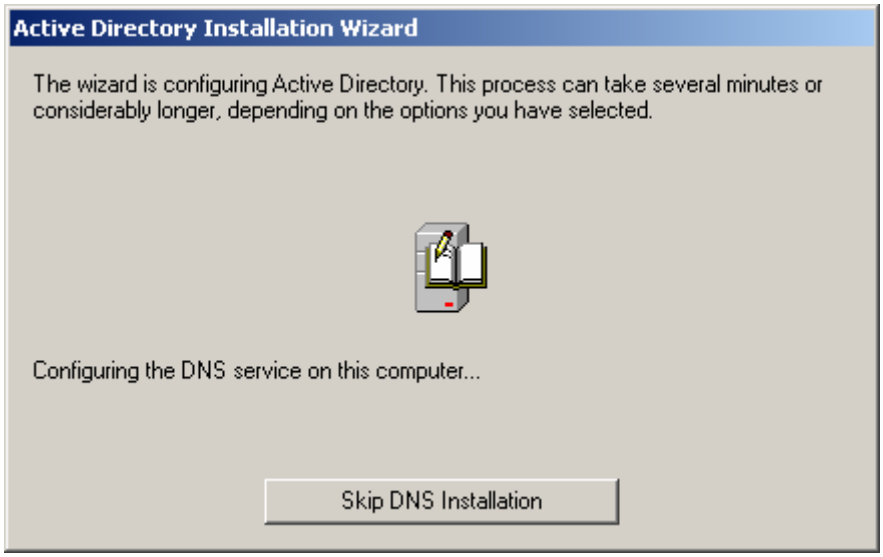
Εικόνα 4-18. Active Directory Installation Wizard βήμα 14ο: TCP/IP Properties.

17. Θέτουμε την επιθυμητή στατική **IP** διεύθυνση, το **Subnet mask**, ανάλογα με το πόσους υπολογιστές επιθυμούμε να έχουν πρόσβαση στον τομέα, και **Default gateway**, ανάλογα με την τοπολογία του δικτύου, **Preferred DNS Server** και πατάμε **OK**.



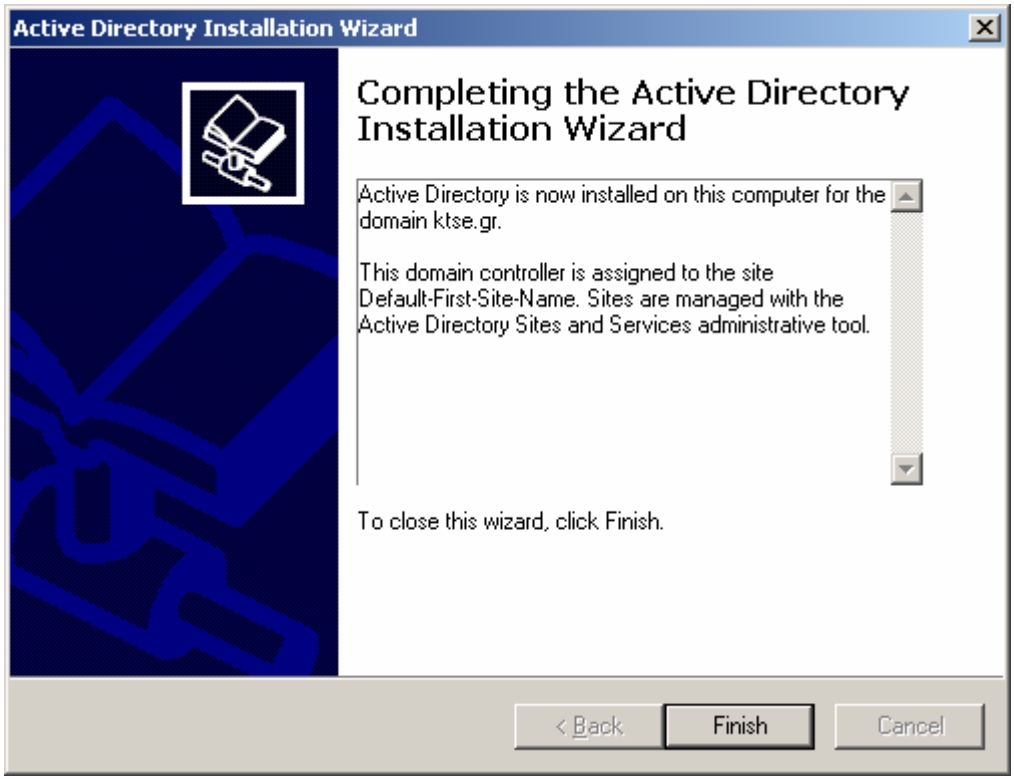
Εικόνα 4-19. Active Directory Installation Wizard βήμα 14ο: IP Configuration.

18. Συνεχίζεται η εγκατάσταση του DNS.



Εικόνα 4-20. Active Directory Installation Wizard βήμα 14ο: DNS Installation.

19. Πατάμε **Finish** για να ολοκληρωθεί η εγκατάσταση.



Εικόνα 4-21. Active Directory Installation Wizard βήμα 15ο.

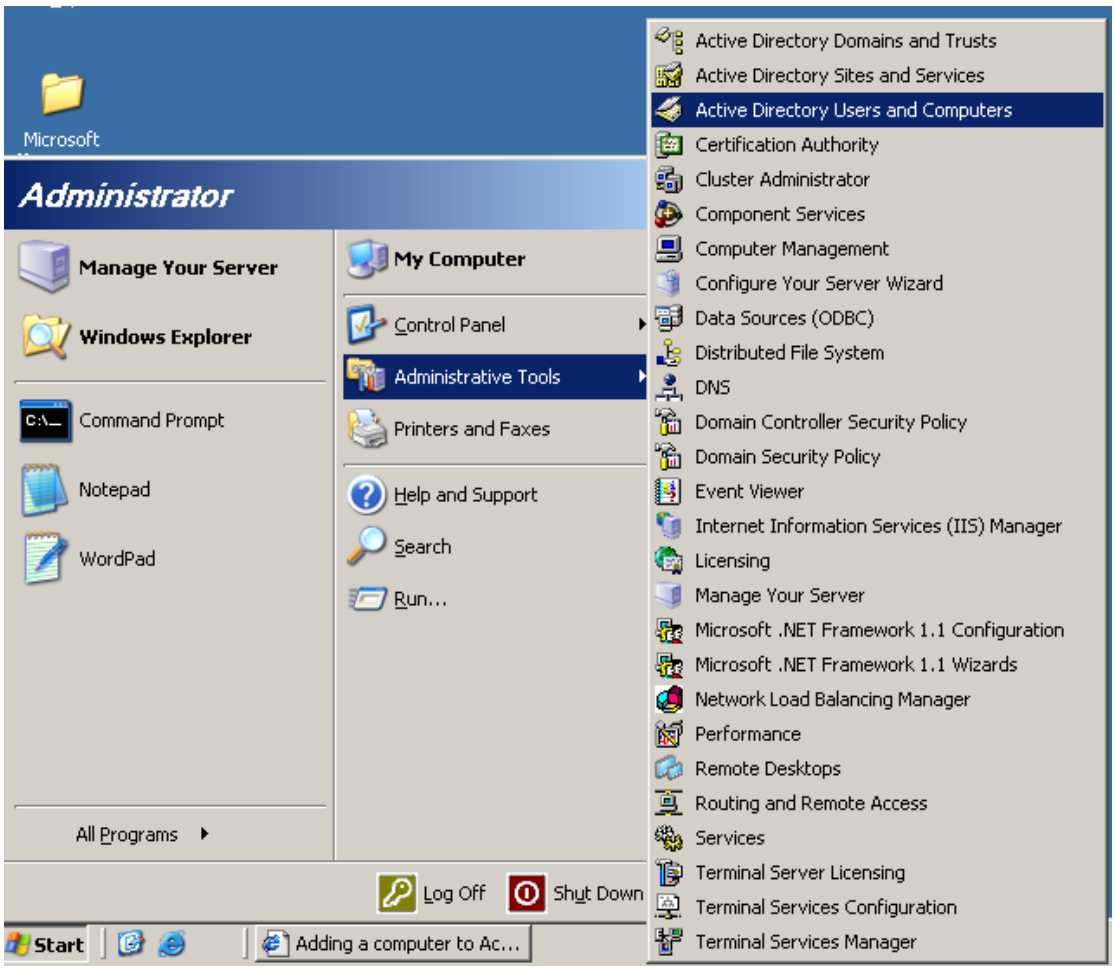
20. Πατάμε **Restart Now**, όπως απαιτείται, για να επανεκκινήσουμε το μηχάνημα.

Εικόνα 4-22. Active Directory Installation Wizard βήμα 16ο.

4.3.2 *Προσθήκη Αντικειμένων*

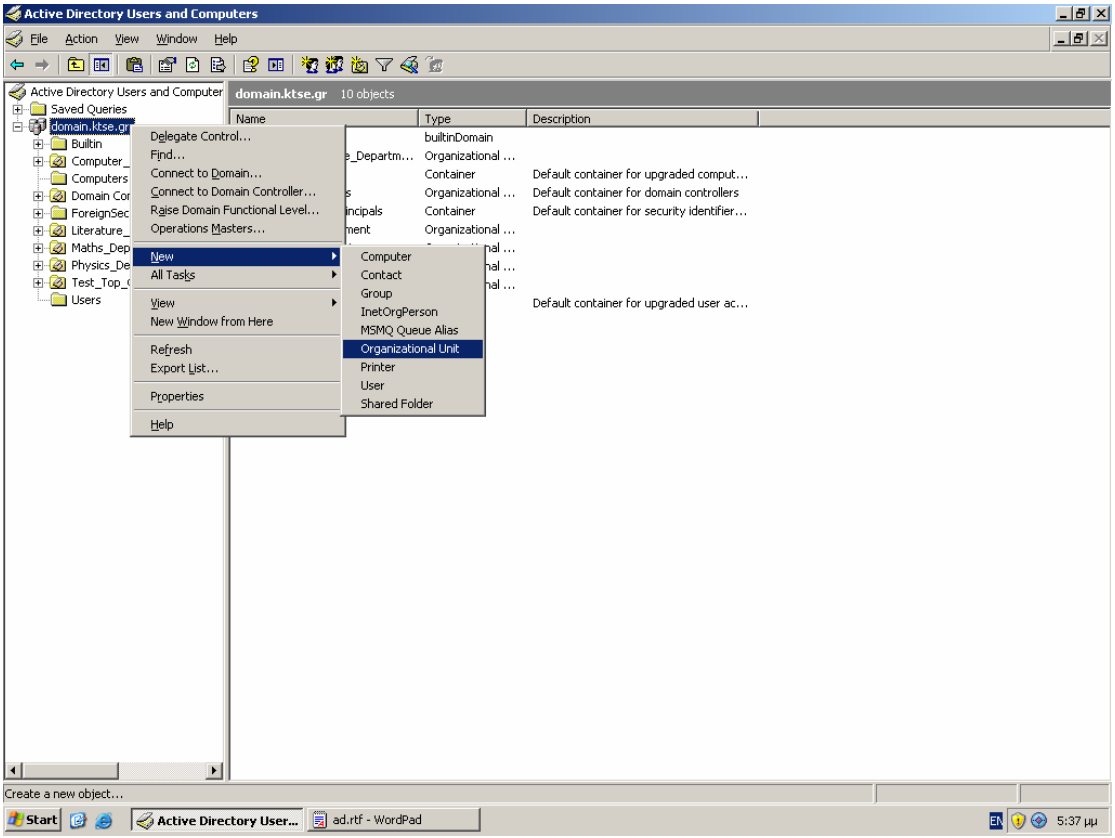
Μετά την ολοκλήρωση της εγκατάστασης του Active Directory μπορούμε να ξεκινήσουμε να προσθέτουμε αντικείμενα μέσα στο domain και να διαμορφώσουμε τις ιδιότητές τους. Τα αντικείμενα μπορεί να είναι από υπολογιστές μέχρι χρήστες.
Για να προσθέσουμε OUs σε κάποιο domain ακολουθούμε τα παρακάτω βήματα:

1. Πατάμε **Start** menu, και επιλέγουμε μέσα από το submenu **Administrative Tools** το **Active Directory Users and Computers**.



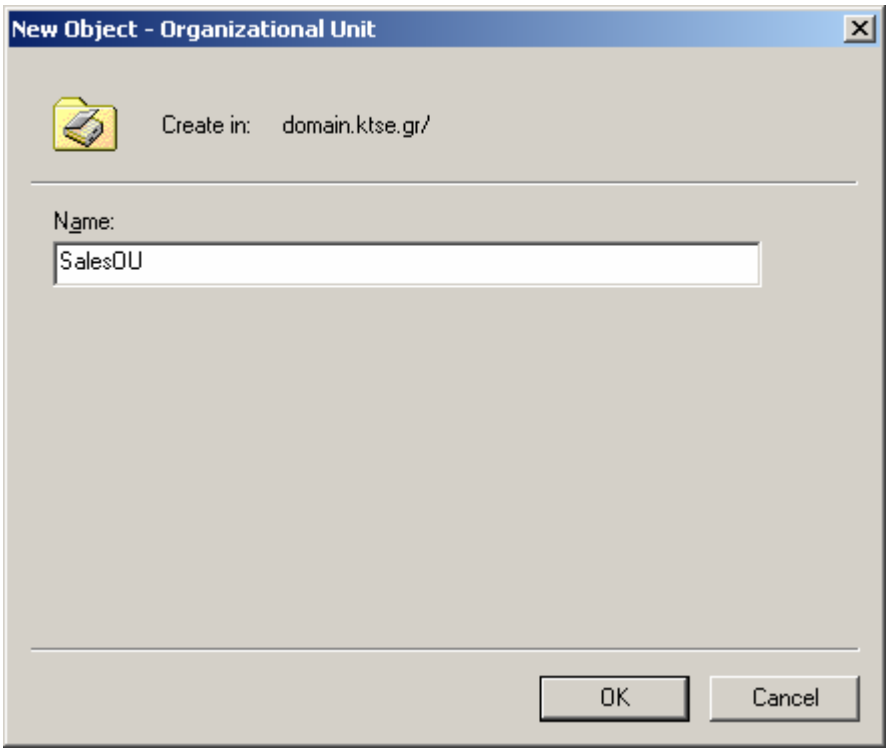
Εικόνα 4-23. Active Directory Users and Computers.

2. Κάνουμε δεξί κλικ στο επιθυμητό domain και πατάμε **New** και έπειτα **Organizational Unit**.



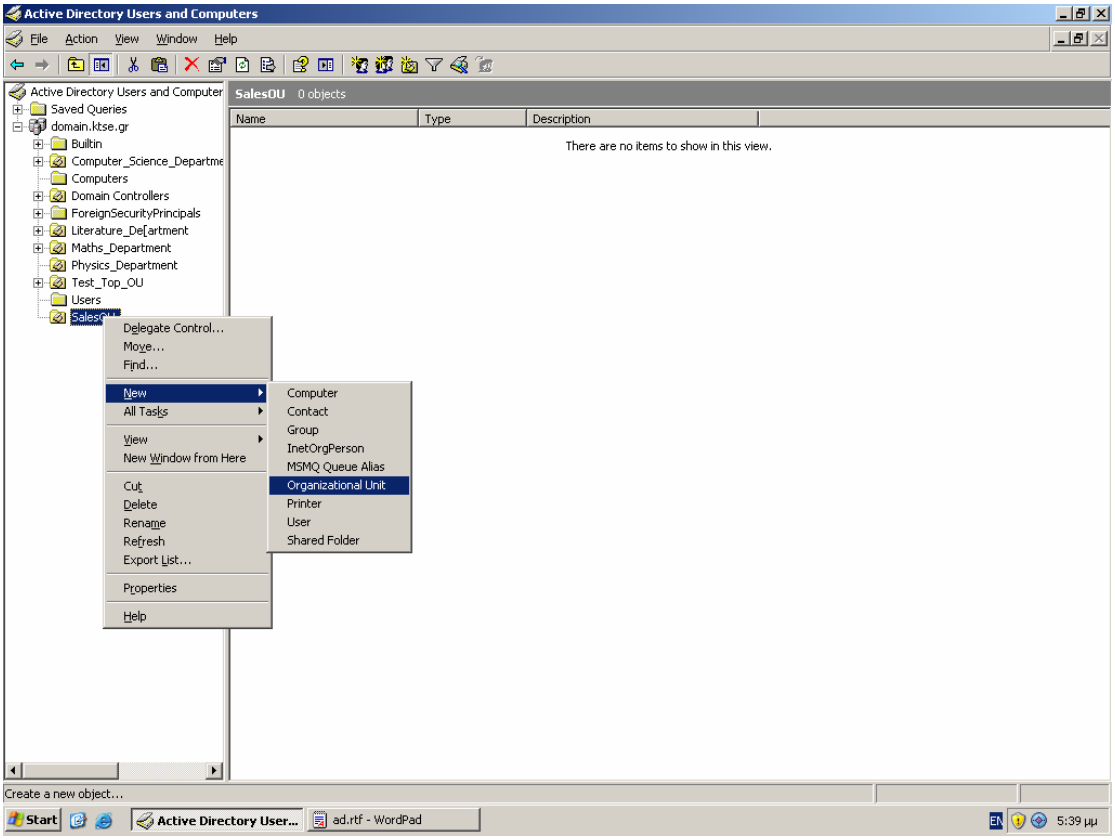
Εικόνα 4-24. Add New OU.

3. Στο πεδίο **Name** θέτουμε το όνομα του OU και πατάμε **OK**.



Εικόνα 4-25. Ονοματοδότηση OU.

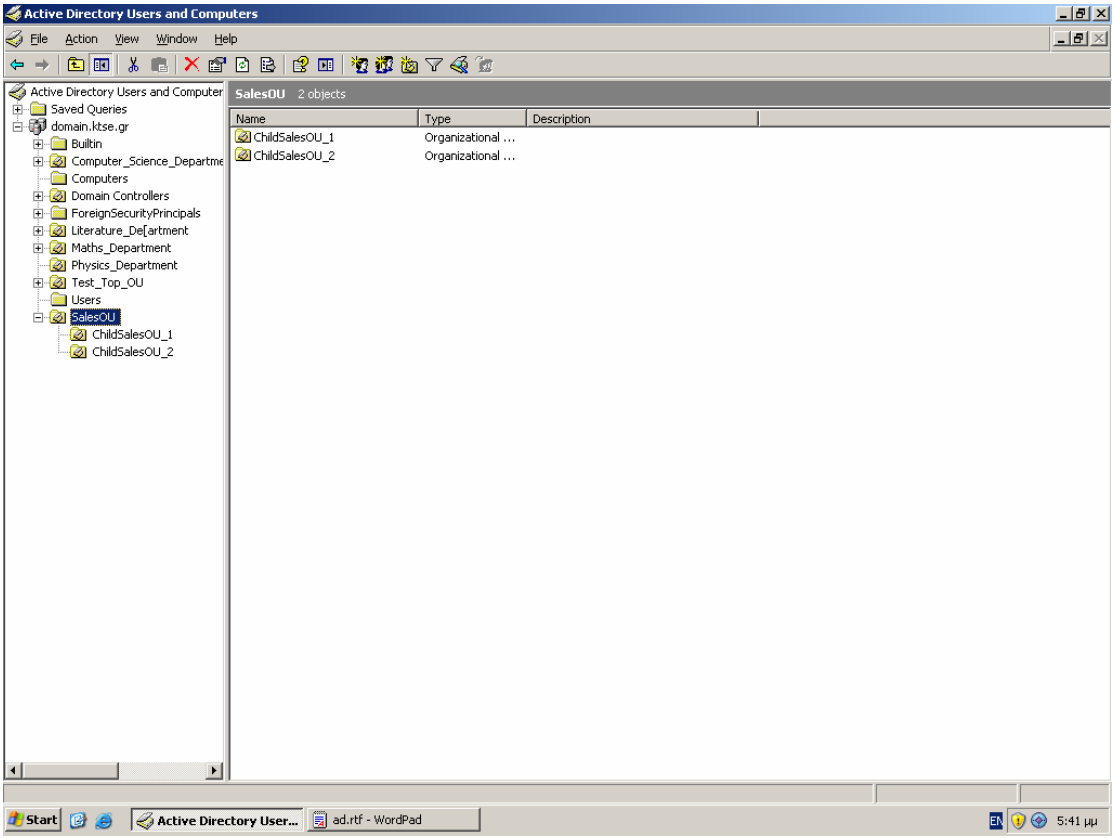
4. Για να προσθέσουμε ένα εμφωλευμένο OU κάνουμε δεξί κλικ στο επιθυμητό OU και πατάμε **New** και έπειτα **Organizational Unit**.



Εικόνα 4-26. Add New Embedded OU.

5. Στο πεδίο **Name** θέτουμε το όνομα του εμφωλευμένου OU και πατάμε **OK**.

6. Επαναλαμβάνουμε τη διαδικασία μέχρι να προσθέσουμε τον επιθυμητό αριθμό OUs.

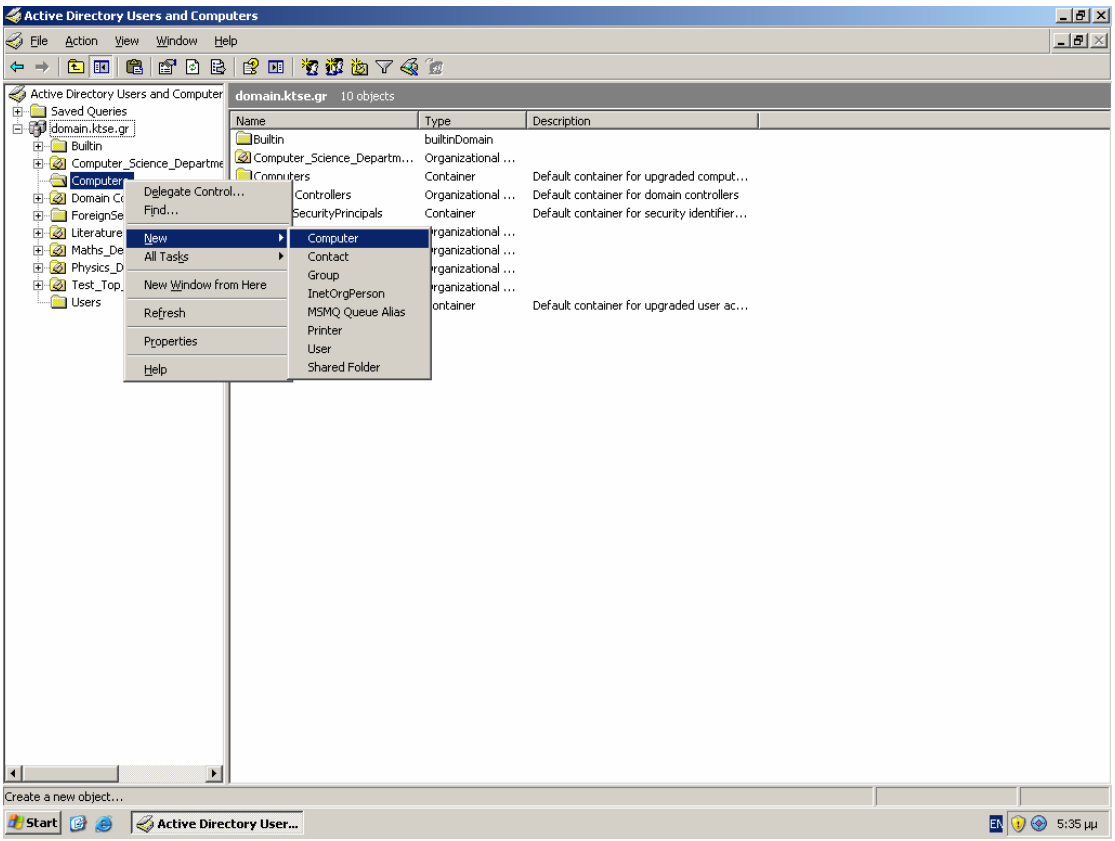


Εικόνα 4-27. Προεπισκόπιση OUs.

Για να προσθέσουμε υπολογιστές σε κάποιο domain ακολουθούμε τα παρακάτω βήματα:

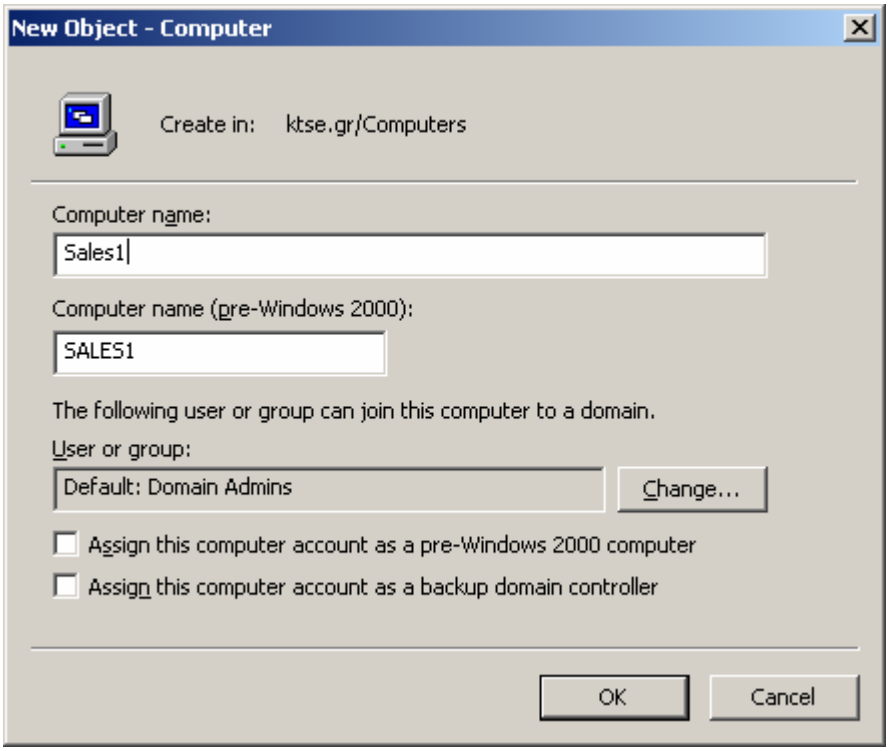
1. Πατάμε **Start** menu, και επιλέγουμε μέσα από το submenu **Administrative Tools** το **Active Directory Users and Computers**.

2. Κάνουμε δεξί κλικ στο **Computers** και πατάμε **New** και έπειτα **Computer**.



Εικόνα 4-28. Add New Computer.

3. Ονομάζουμε το αντικείμενο και πατάμε **OK**.

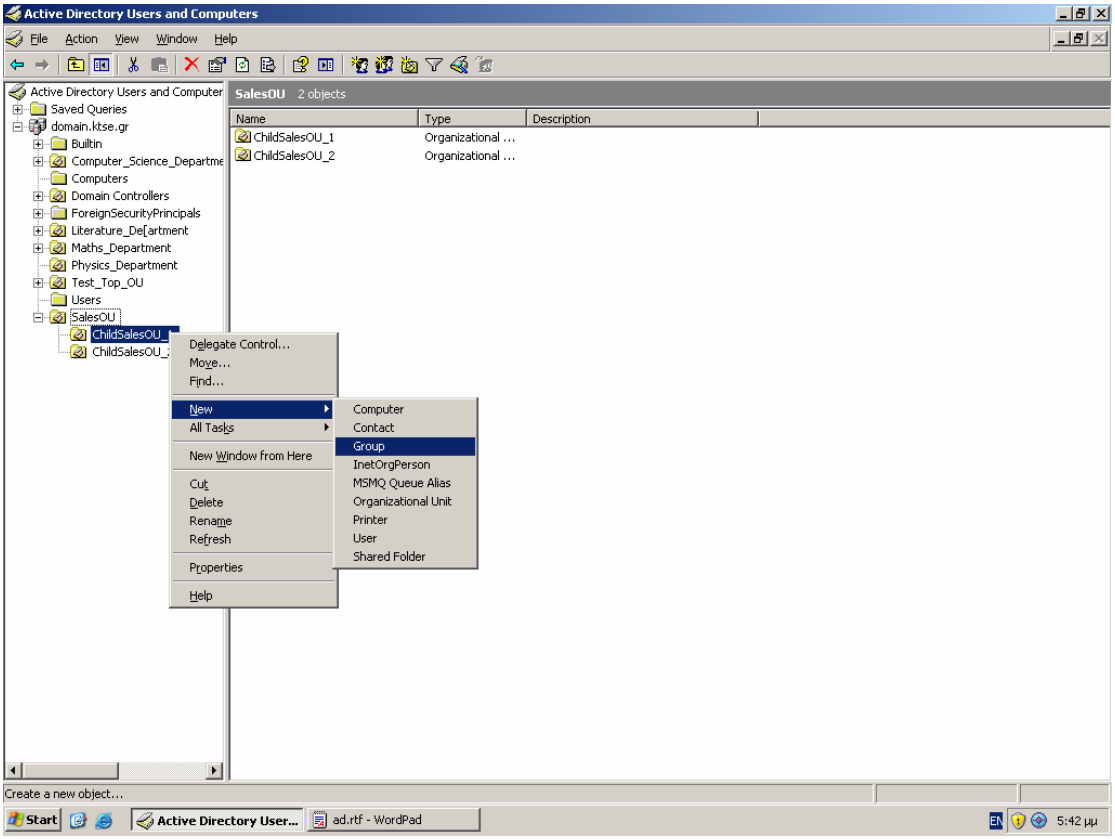


Εικόνα 4-29. Ονοματοδότηση Computer.

Για να προσθέσουμε ομάδες σε κάποιο domain ακολουθούμε τα παρακάτω βήματα:

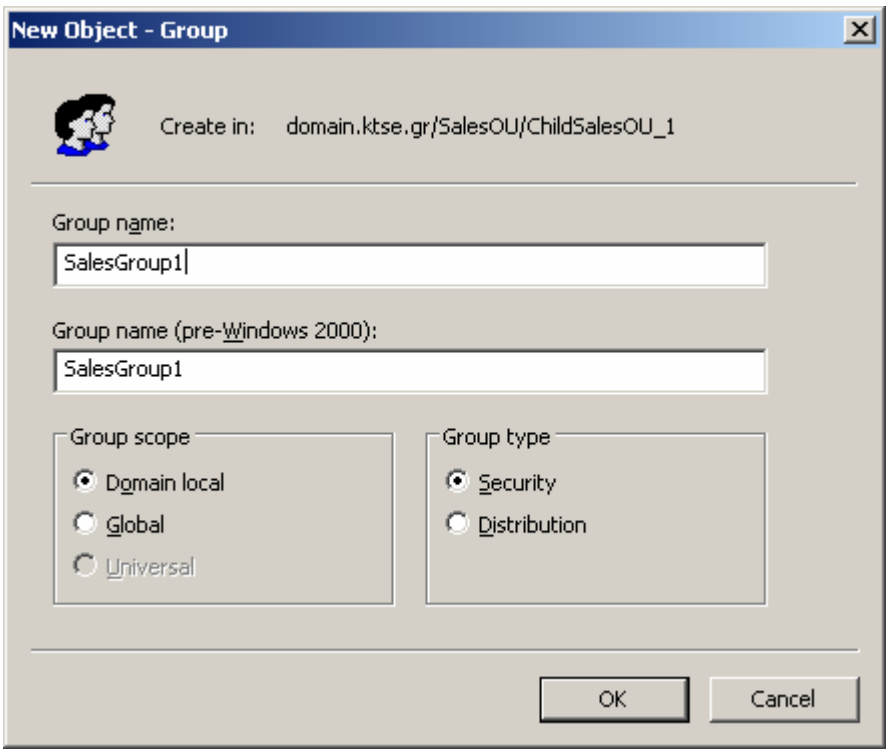
1. Πατάμε **Start** menu, και επιλέγουμε μέσα από το submenu **Administrative Tools** το **Active Directory Users and Computers**.

2. Κάνουμε δεξί κλικ στο επιθυμητό αντικείμενο (πχ OU) και πατάμε **New** και έπειτα **Group**.



Εικόνα 4-30. Add New Group.

3. Στο πεδίο **Group name** θέτουμε το όνομα της ομάδας, στο **Group scope** επιλέγουμε εάν η ομάδα θα είναι global ή θα είναι τοπική μόνο στο συγκεκριμένο domain, στο **Group type** επιλέγουμε **Security** εάν θέλουμε να είναι επιτρεπτή η διαχείριση και η απόδοση δικαιωμάτων, ενώ εάν θέλουμε να χρησιμοποιηθεί εξολοκλήρου ως λίστα διανομής ηλεκτρονικού ταχυδρομείου θα επιλέξουμε **Distribution** και πατάμε **OK**.

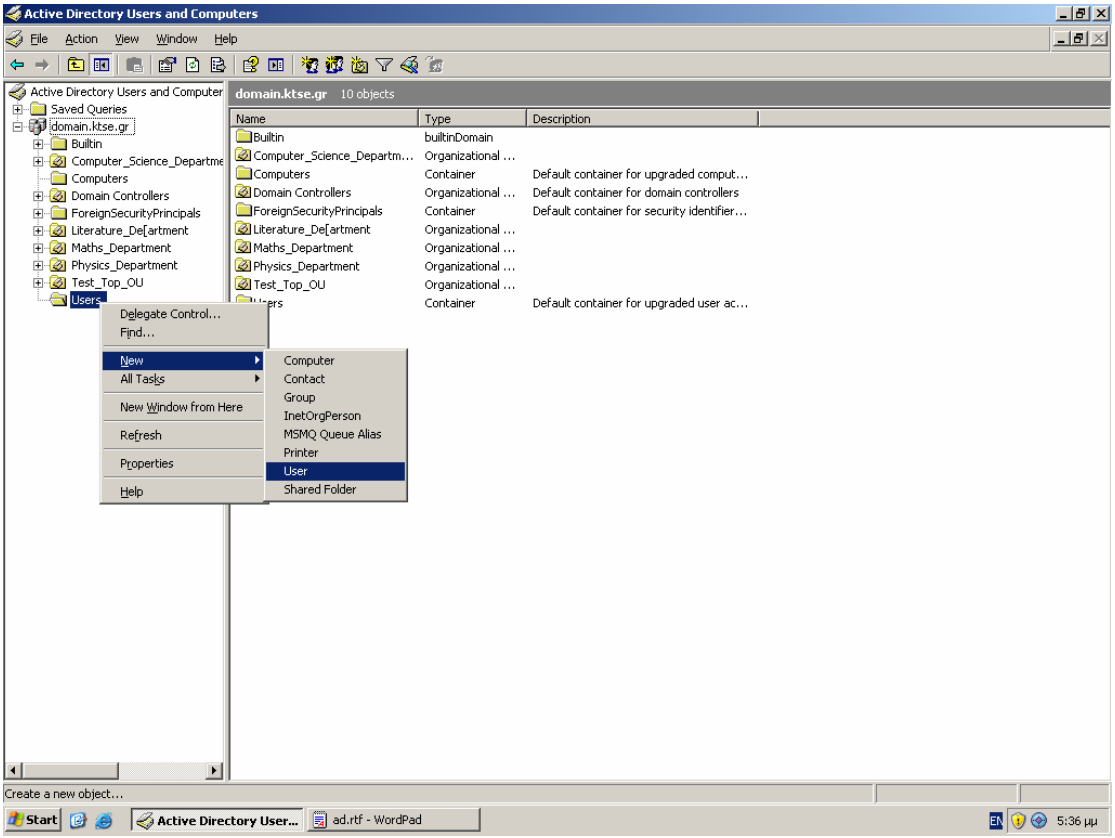


Εικόνα 4-31. Ονοματοδότηση Group.

Για να προσθέσουμε χρήστες σε κάποιο domain ακολουθούμε τα παρακάτω βήματα:

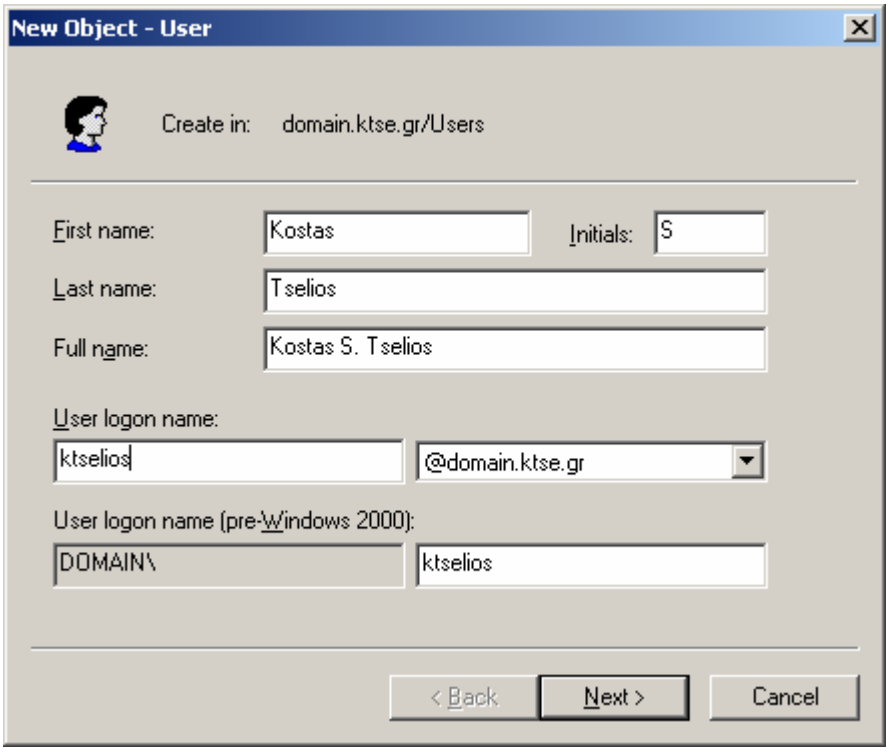
1. Πατάμε **Start** menu, και επιλέγουμε μέσα από το submenu **Administrative Tools** το **Active Directory Users and Computers**.

2. Κάνουμε δεξί κλικ στο **Users** και πατάμε **New** και έπειτα **User**.



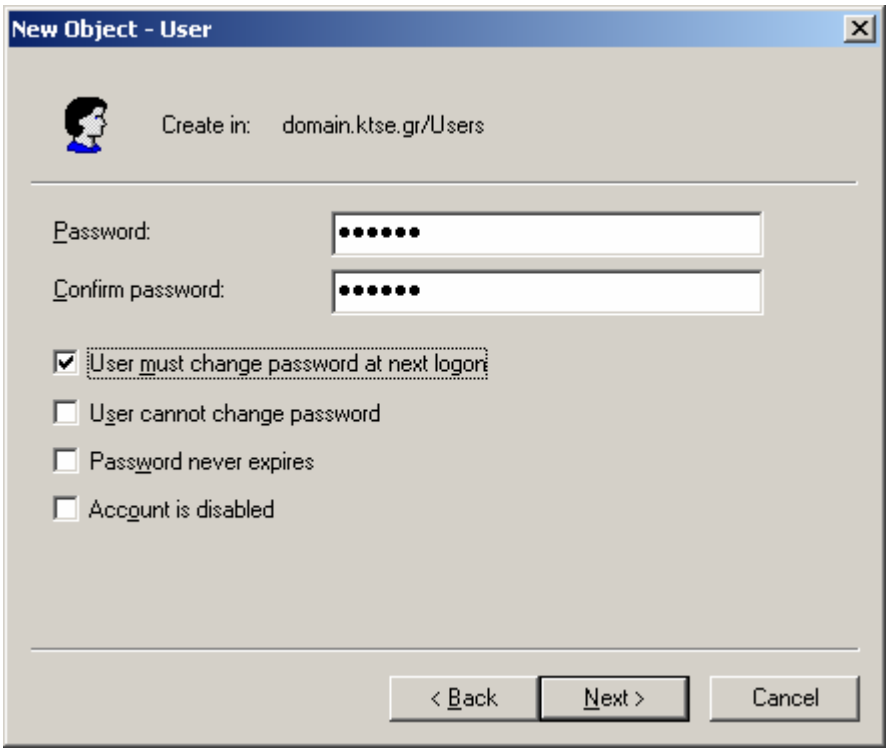
Εικόνα 4-32. Add New User.

3. Θέτουμε τα στοιχεία του χρήστη και το **User logon name** και πατάμε **Next**.



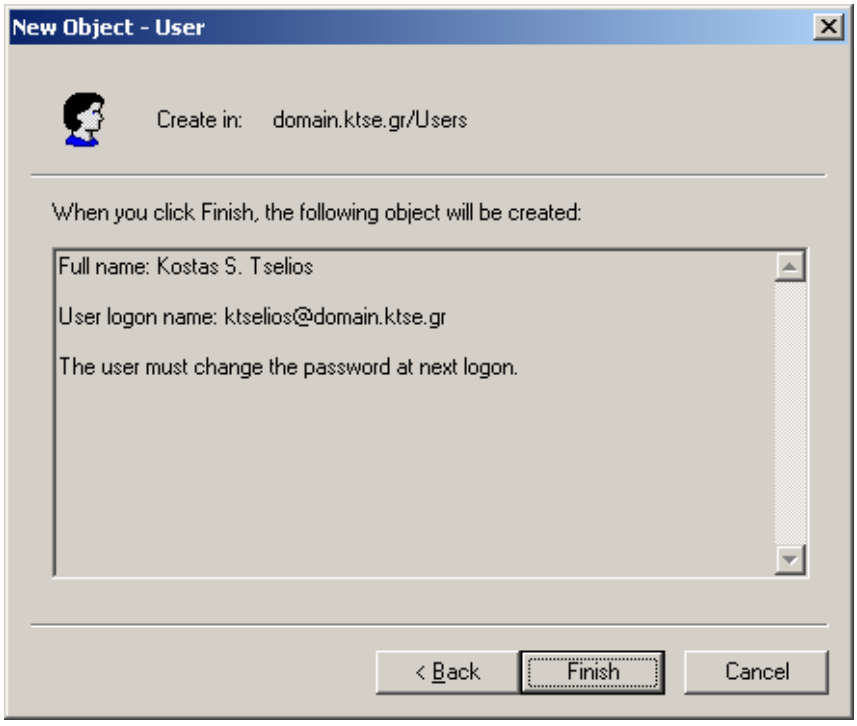
Εικόνα 4-33. User Logon Name.

4. Θέτουμε το **Password**, επιλέγουμε τα επιθυμητά **check boxes** και πατάμε **Next**.



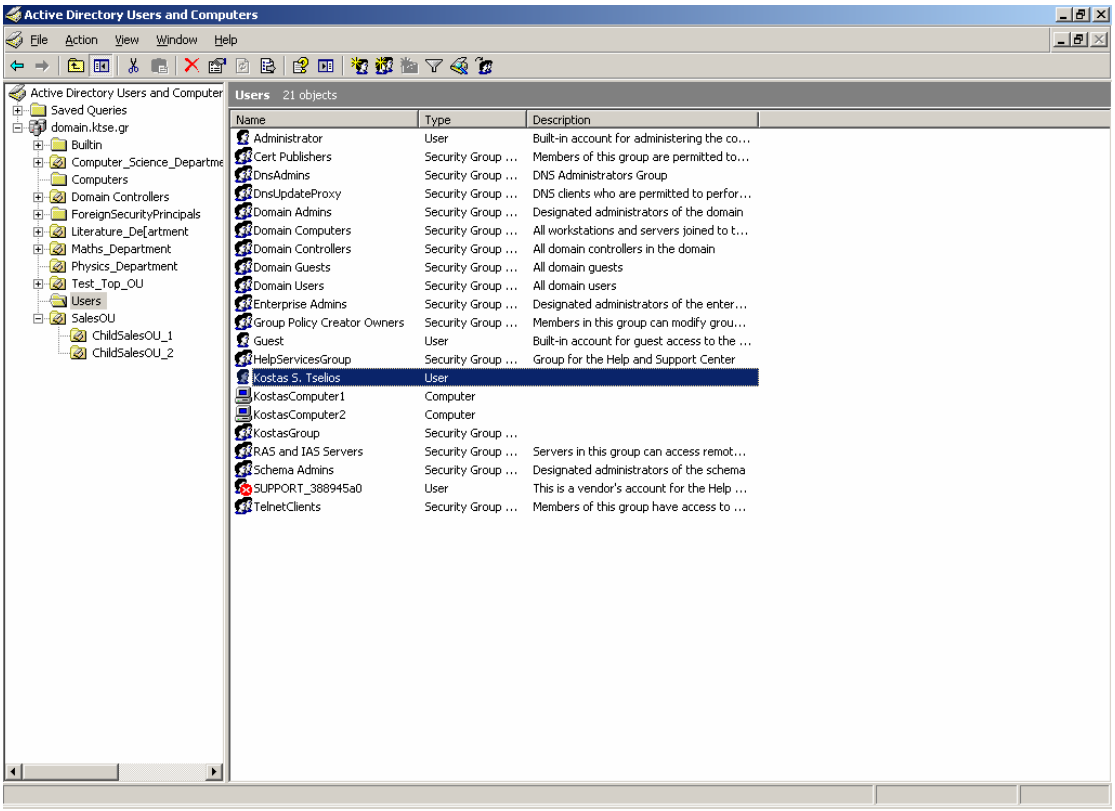
Εικόνα 4-34. Set User Password.

5. Παρατηρούμε το αντικείμενο που θα δημιουργηθεί και τις ιδιότητές του και εφόσον είμαστε σύμφωνοι πατάμε **Finish**.



Εικόνα 4-35. Προεπισκόπιση ρυθμίσεων χρήστη.

6. Επαναλαμβάνουμε τη διαδικασία μέχρι να προσθέσουμε τον επιθυμητό αριθμό χρηστών.

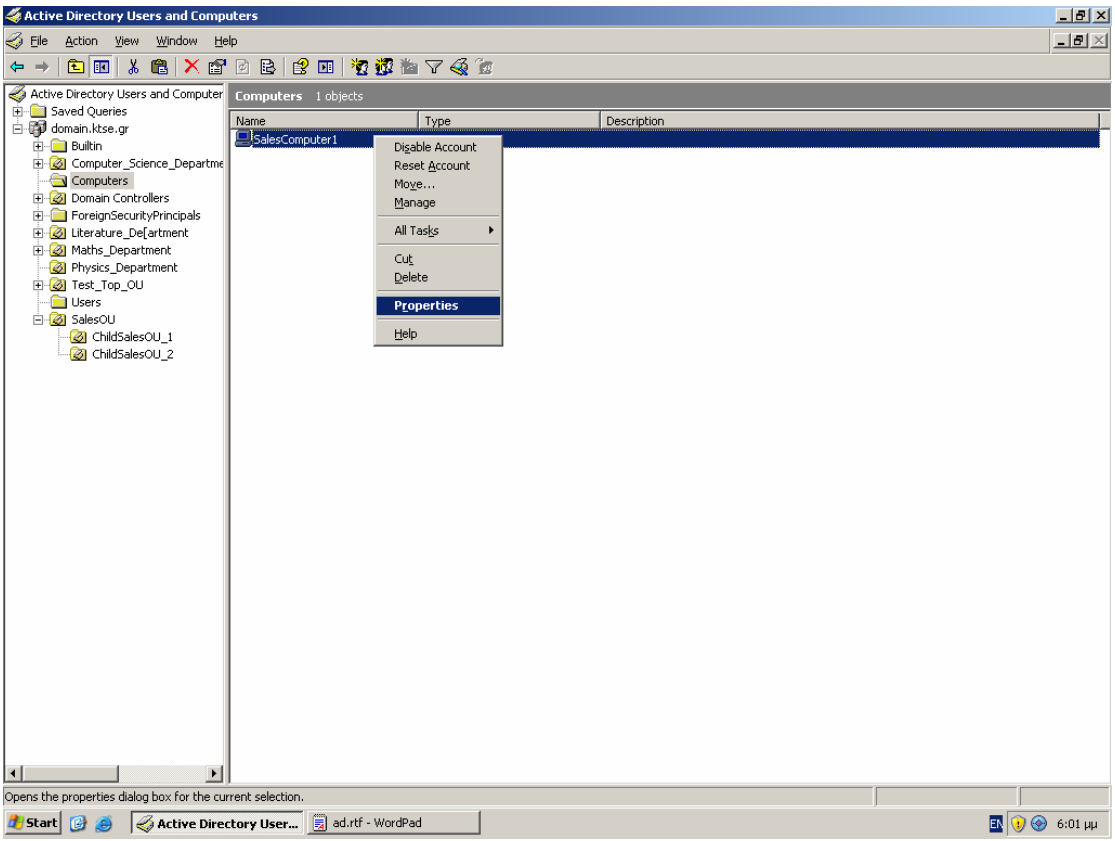


Εικόνα 4-36. Προεπισκόπιση Users.

4.3.3 *Ομαδοποίηση Αντικειμένων*

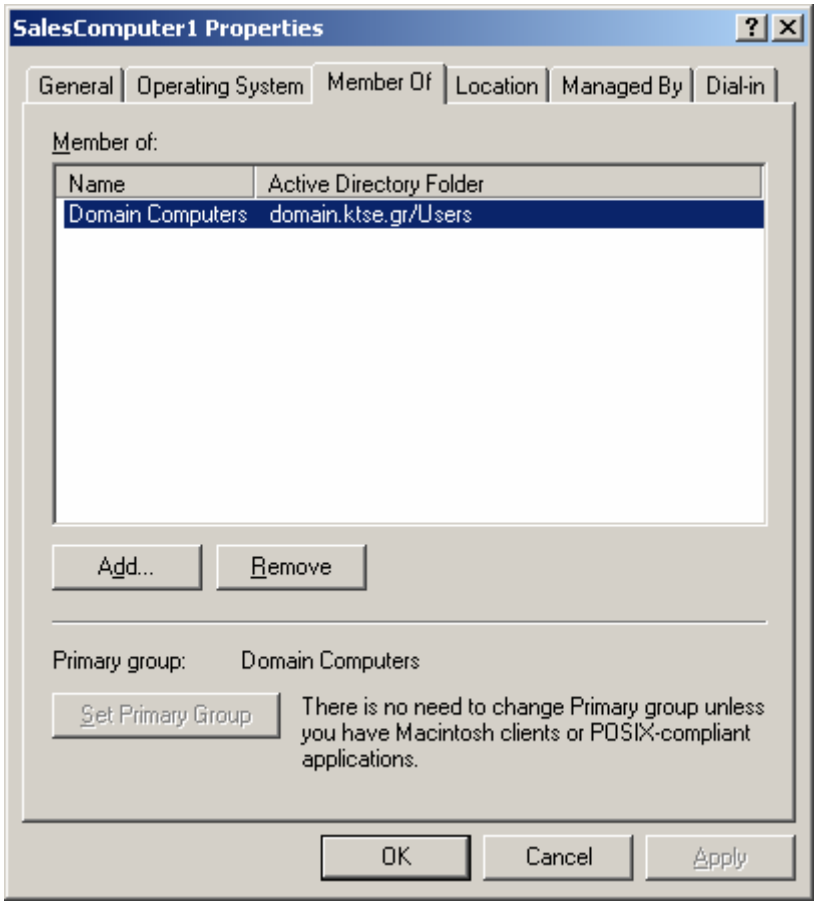
Κάποια αντικείμενα μπορούν να ανατεθούν σε άλλα και με αυτό τον τρόπο είναι δυνατό να πετύχουμε κοινή διαχείρηση και ομαδοποίηση αντικειμένων. Η πιο κοινή ανάθεση είναι η ομαδοποίηση, δηλαδή η ανάθεση ενός αντικειμένου σε μία Ομάδα. Σε αυτή την ενότητα θα παρατηρηθεί η διαδικασία ανάθεσης σε Ομάδα των αντικειμένων Computers και Users. Για να αναθέσουμε έναν υπολογιστή σε μία Ομάδα ακολουθούμε τα παρακάτω βήματα:

1. Κάνουμε δεξί κλικ στο επιθυμητό αντικείμενο και πατάμε **Properties**.



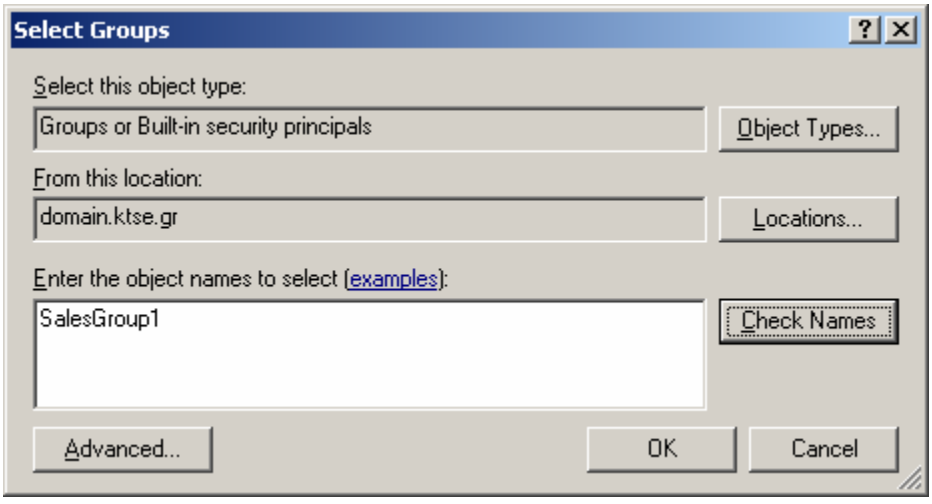
Εικόνα 4-37. Add Computer to Group βήμα 1ο.

2. Στην καρτέλα **Member Of** πατάμε **Add**.



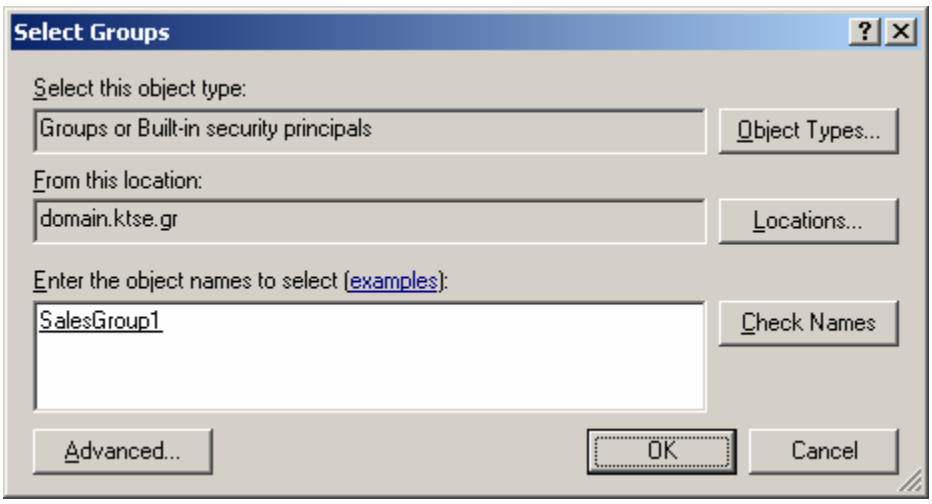
Εικόνα 4-38. Add Computer to Group βήμα 2ο.

3. Στο πεδίο **object names** θέτουμε το όνομα του Group που επιθυμούμε την ανάθεση και πατάμε **Ckeck Names** για να γίνει ο έλεγχος του ονόματος του αντικειμένου.



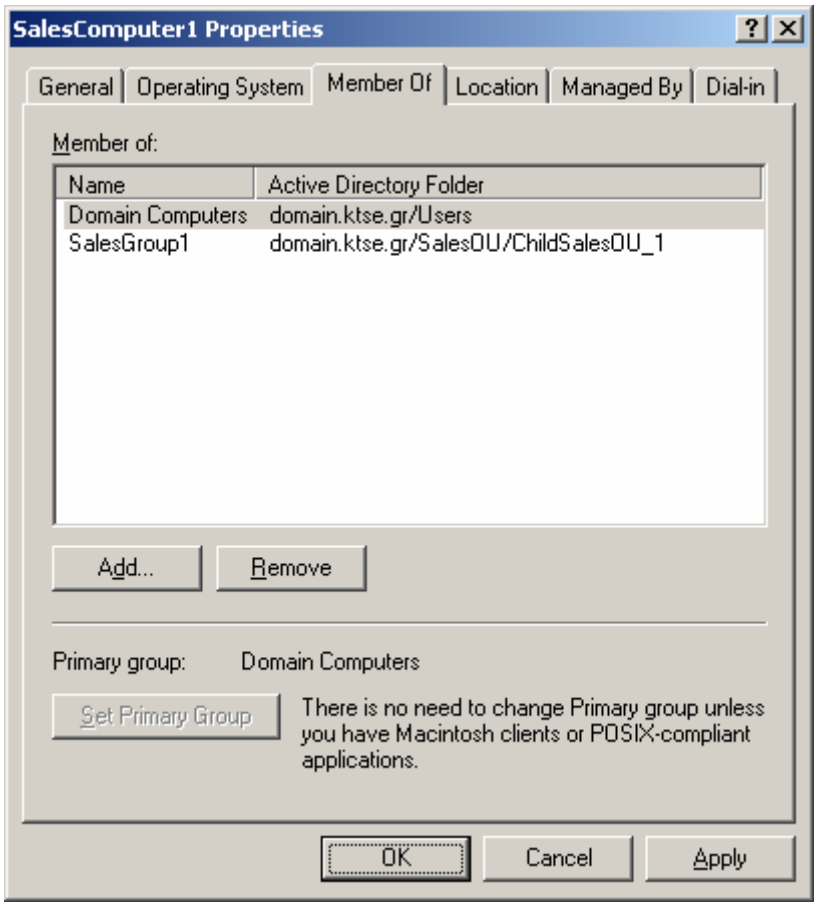
Εικόνα 4-39. Add Computer to Group βήμα 3ο Α.

4. Εφόσον έχει πραγματοποιηθεί ο έλεγχος και στο πεδίο **object names** είναι υπογραμμισμένο το αντικείμενο, πατάμε **OK**.



Εικόνα 4-40. Add Computer to Group βήμα 3ο Β.

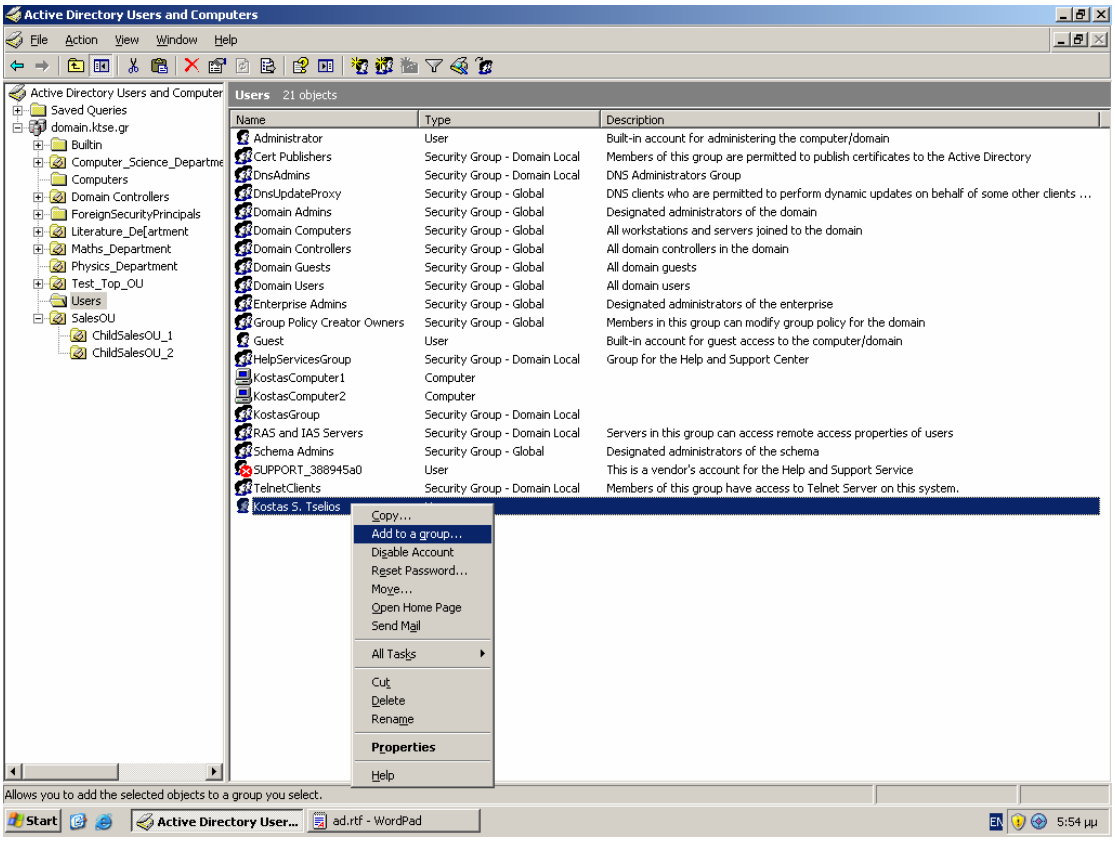
5. Παρατηρούμε τη νέα καταχώριση που θα πραγματοποιηθεί και εφόσον είμαστε σύμφωνοι πατάμε **OK.**



Εικόνα 4-41. Add Computer to Group βήμα 4ο.

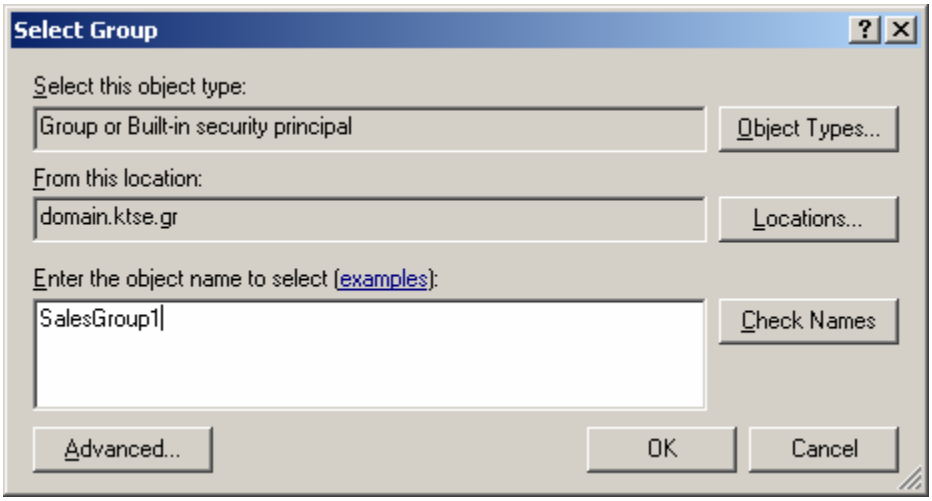
Για να αναθέσουμε ένα χρήστη σε μία Ομάδα ακολουθούμε τα παρακάτω βήματα:

1. Κάνουμε δεξί κλικ στο επιθυμητό αντικείμενο και πατάμε **Add to a group**.



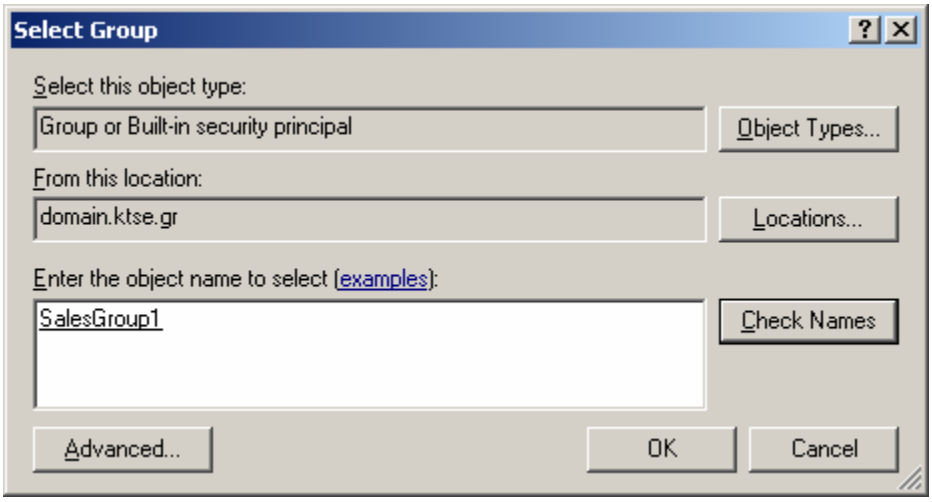
Εικόνα 4-42. Add User to Group βήμα 1ο.

2. Στο πεδίο **object names** θέτουμε το όνομα του Group που επιθυμούμε την ανάθεση και πατάμε **Ckeck Names** για να γίνει ο έλεγχος του ονόματος του αντικειμένου.



Εικόνα 4-43. Add User to Group βήμα 2ο Α.

3. Εφόσον έχει πραγματοποιηθεί ο έλεγχος και στο πεδίο **object names** είναι υπογραμμισμένο το αντικείμενο, πατάμε **OK**.



Εικόνα 4-44. Add User to Group βήμα 2ο Β.

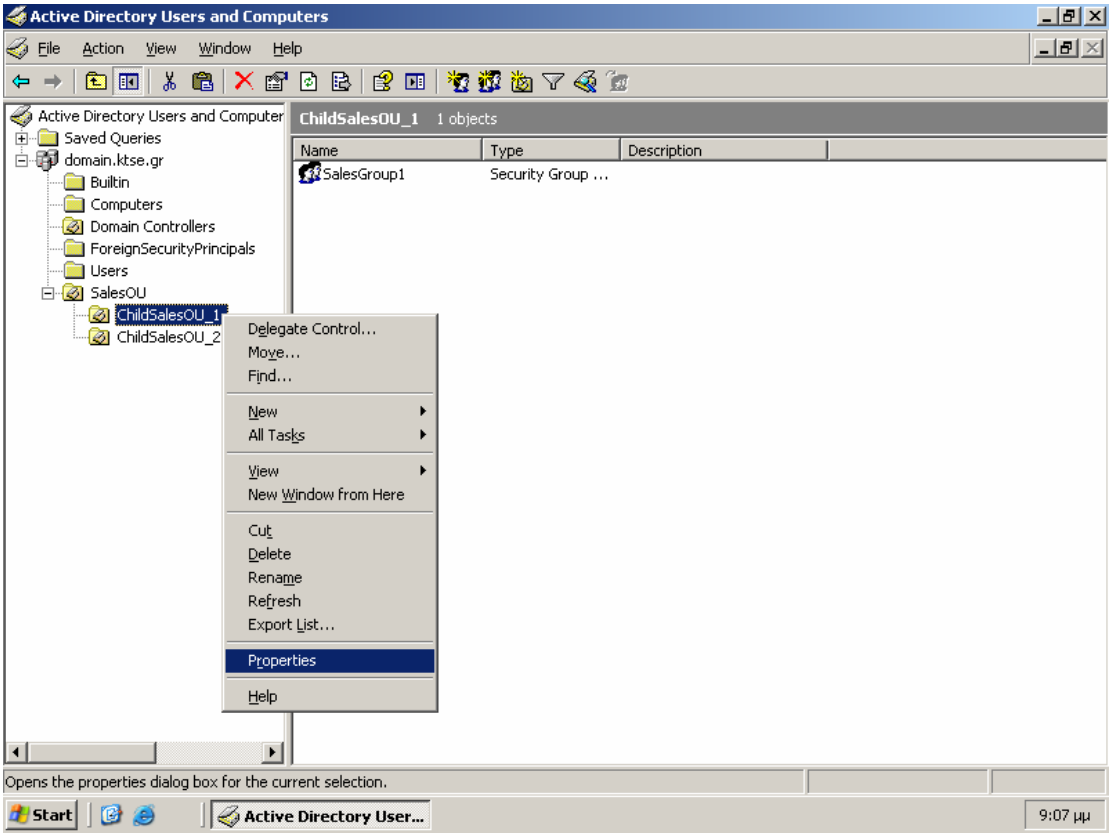
4. Πατάμε **OK**.

Εικόνα 4-45. Add User to Group βήμα 3ο.

4.3.4 *Ιδιότητες αντικειμένων*

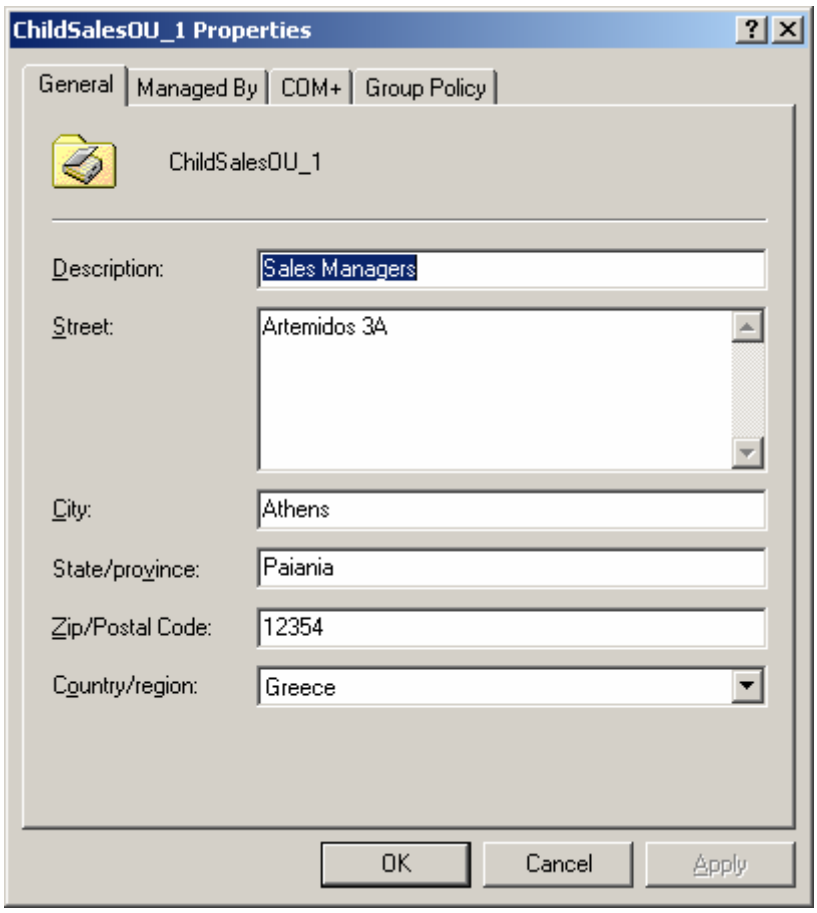
Κάθε αντικείμενο που δημιουργείται σε κάποιο domain έχει ιδιότητες με τις οποίες καθιστά δυνατή τη διαχείρισή του και καθορίζει την υπόστασή του και το ρόλο που αυτό έχει μέσα στο domain ή ακόμα και στο forest (αν για παράδειγμα το αντικείμενο είναι global). Σε αυτή την ενότητα θα παρατηρήσουμε τις ιδιότητες των σημαντικότερων αντικειμένων που βρίσκονται σε ένα domain ή forest.
Για να παρατηρήσουμε τις ιδιότητες των Organizational Units ακολουθούμε τα παρακάτω βήματα:

1. Κάνουμε δεξί κλικ στο επιθυμητό OU και πατάμε **Properties**.



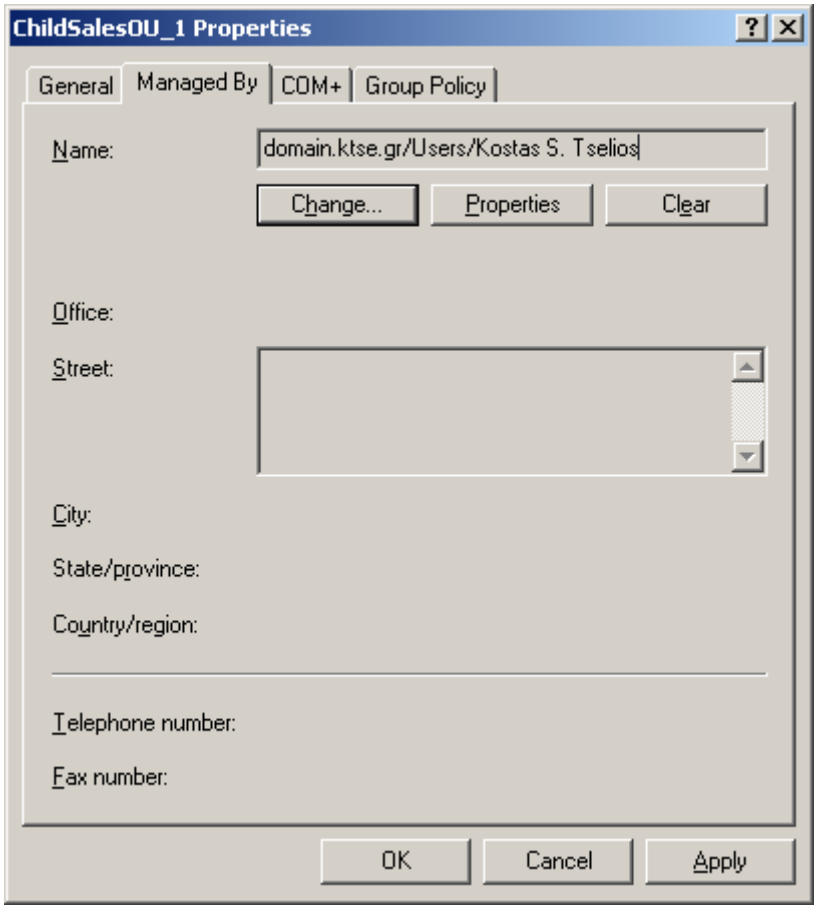
Εικόνα 4-46. OU Properties.

2. Στην καρτέλα **General** παρατηρούμε και τροποποιούμε τις πληροφορίες οργανισμού του αντικειμένου.

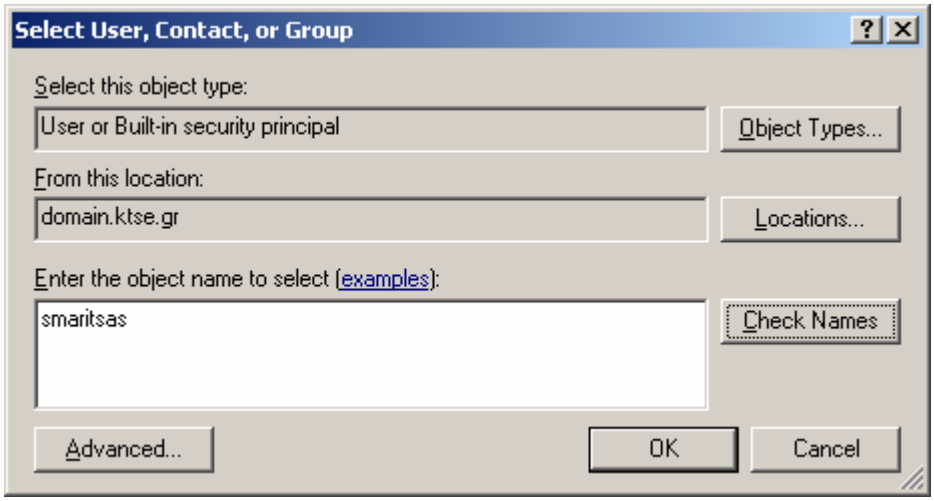


Εικόνα 4-47. OU Properties: Η καρτέλα General.

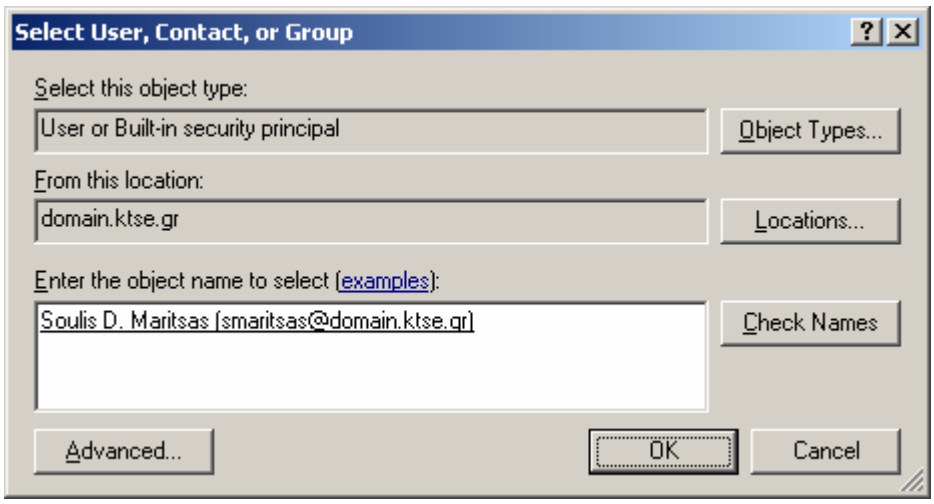
3. Στην καρτέλα **Manged By** μπορούμε να θέσουμε ή να αλλάξουμε τον υπεύθυνο διαχείρισης του αντικειμένου. Για να αλλάξουμε τον manager του OU πατάμε **Change**, στο object name θέτουμε το όνομα του χρήστη και πατάμε **Check Names**. Εφόσον το όνομα είναι σωστό και φαίνεται υπογραμισμένο πατάμε **OK**. Εάν δεν επιθυμούμε να θέσουμε κάποιον ως manager του αντικειμένου, πατάμε **Clear**.



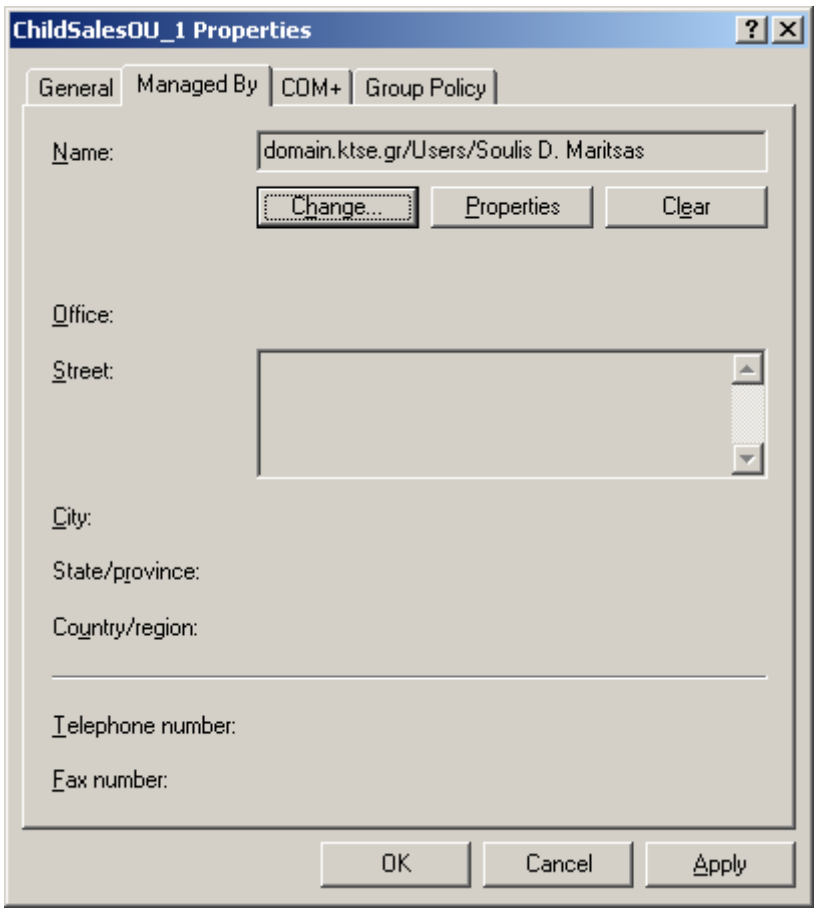
Εικόνα 4-48. OU Properties: Η καρτέλα Managed By.



Εικόνα 4-49. OU Properties: Στην καρτέλα Managed By, η επιλογή Change A.

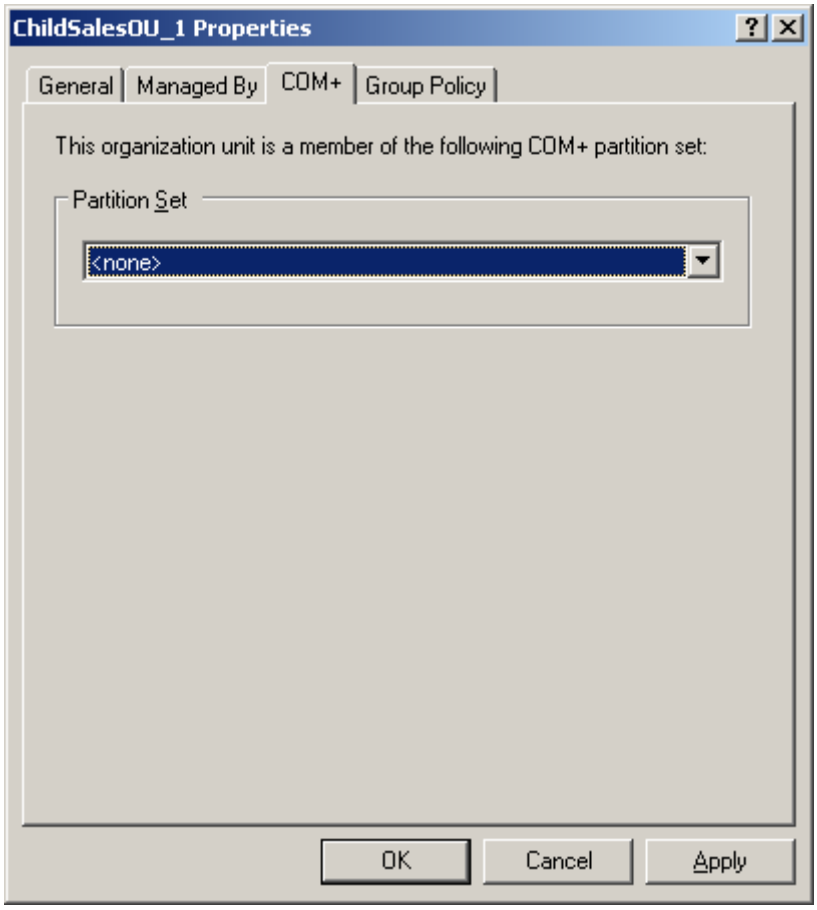


Εικόνα 4-50. OU Properties: Στην καρτέλα Managed By, η επιλογή Change Β.



Εικόνα 4-51. OU Properties: Στην καρτέλα Managed By, η επιλογή Change Γ.

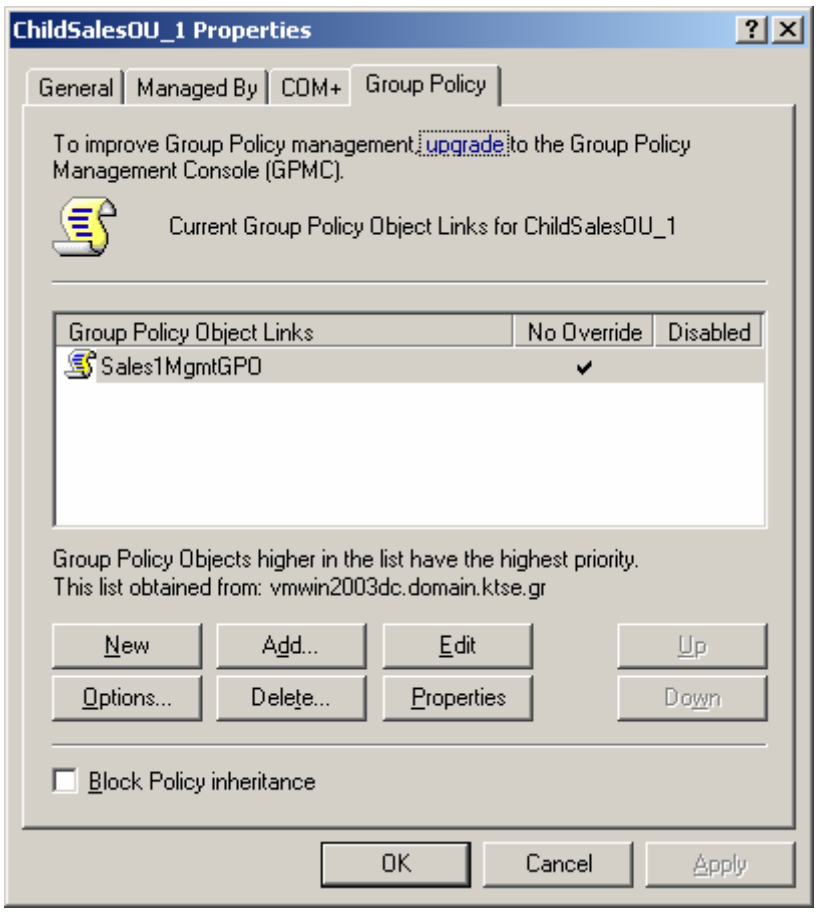
4. Στην καρτέλα COM+ μπορούμε να κάνουμε το αντικείμενο μέλος ενός COM+ διαμερίσματος.[62]



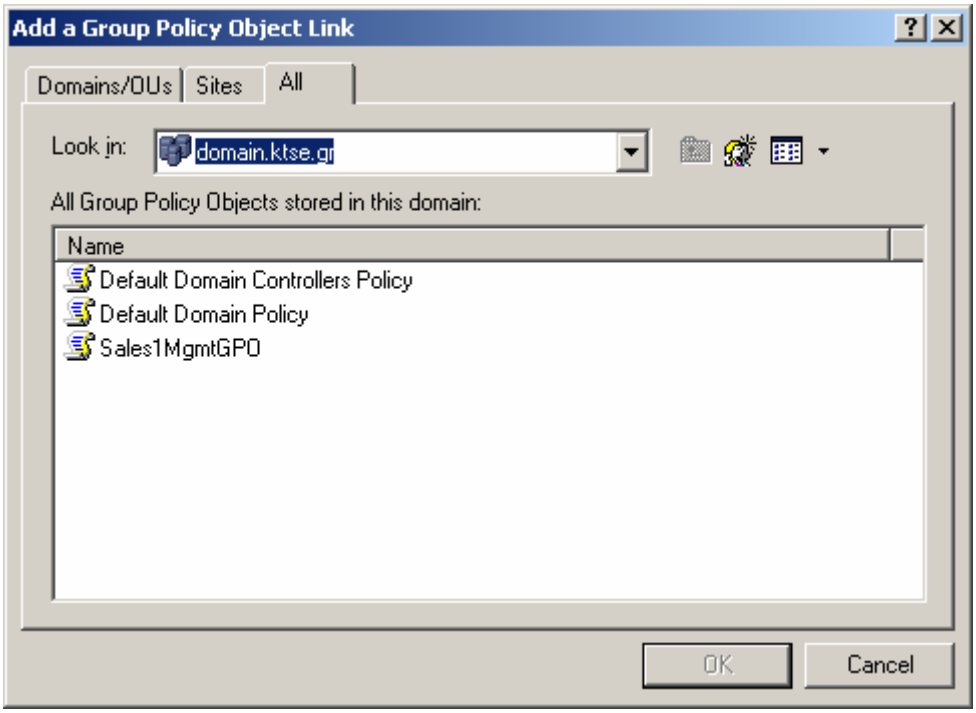
Εικόνα 4-52. OU Properties: Η καρτέλα COM+.

5. Στην καρτέλα Group Policy μπορούμε να αναθέσουμε ένα GPO στο αντικείμενο, καθώς και να το τροποποιήσουμε.

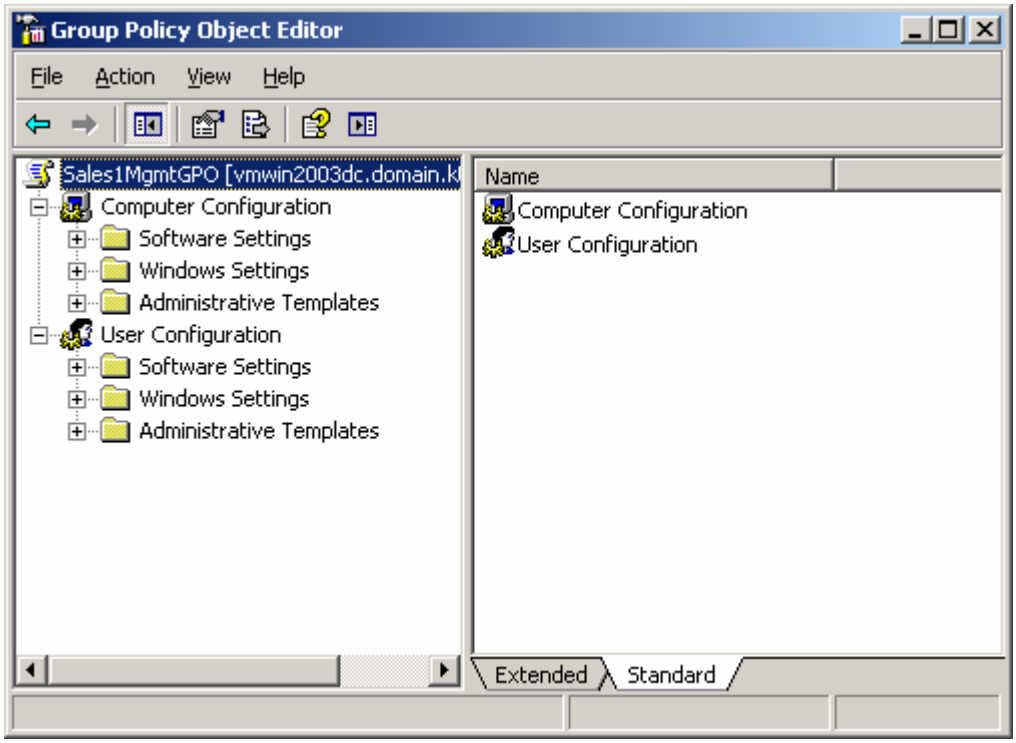
[62] Περισσότερες πληροφορίες για τα COM+ διαμερίσματα μπορείτε να βρείτε εδώ: http://msdn.microsoft.com/en-us/library/ms686110(VS.85).aspx.



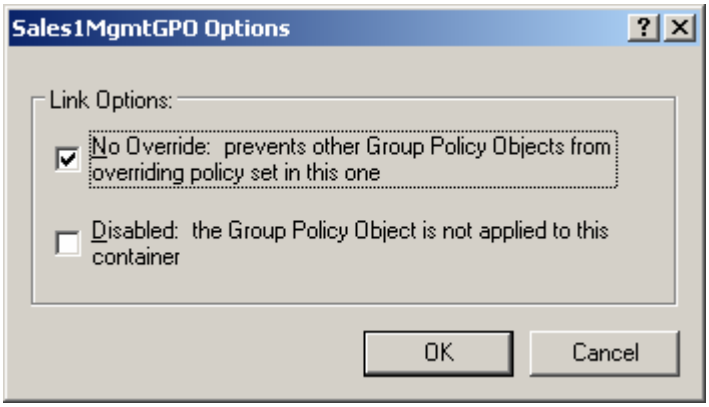
Εικόνα 4-53. OU Properties: Η καρτέλα Group Policy.



Εικόνα 4-54. OU Properties: Στην καρτέλα Managed By, η επιλογή Add: επιλέγουμε κάποιο από τα GPOs της λίστας που επιθυμούμε να προσθέσουμε στο OU.



Εικόνα 4-55. OU Properties: Στην καρτέλα Managed By, η επιλογή Edit: ανοίγει ο GPO Editor.

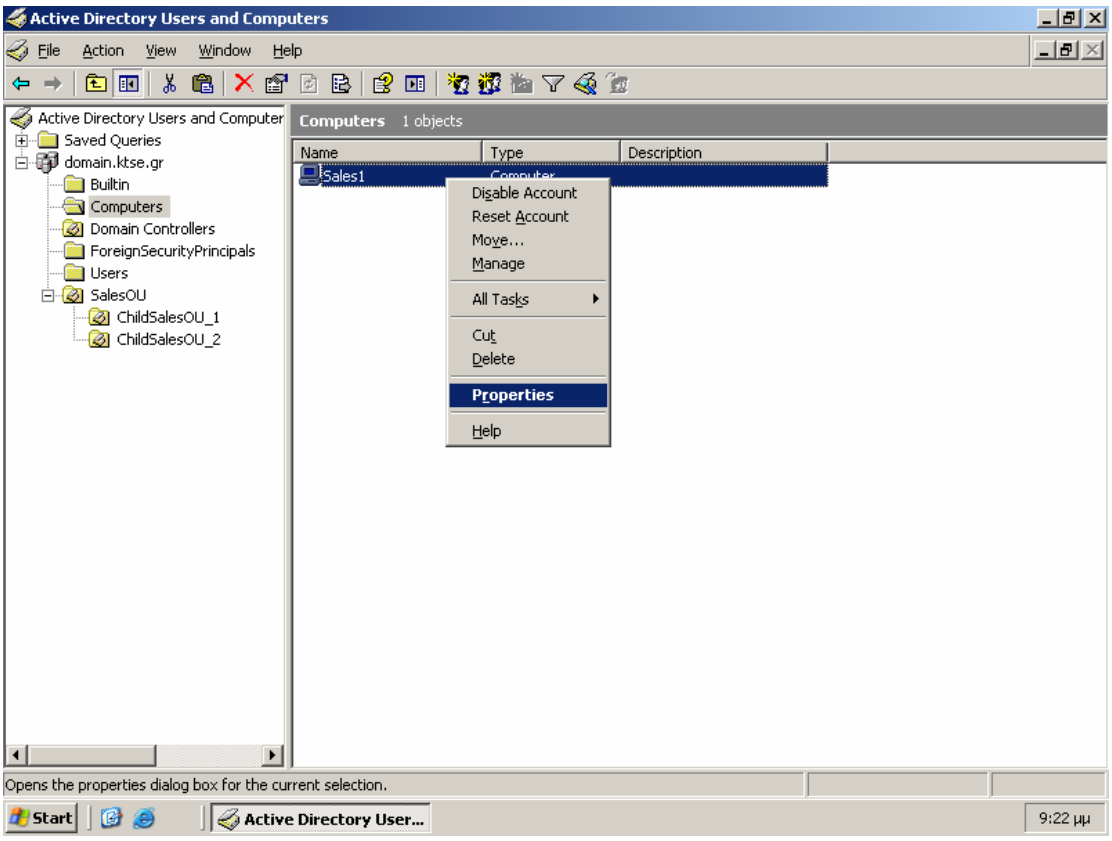


Εικόνα 4-56. OU Properties: Στην καρτέλα Managed By, η επιλογή Options: μπορούμε να επιλέξουμε No Override ή Disabled.[63]

Για να παρατηρήσουμε τις ιδιότητες των Computers ακολουθούμε τα παρακάτω βήματα:

1. Κάνουμε δεξί κλικ στο επιθυμητό αντικείμενο και πατάμε **Properties**.

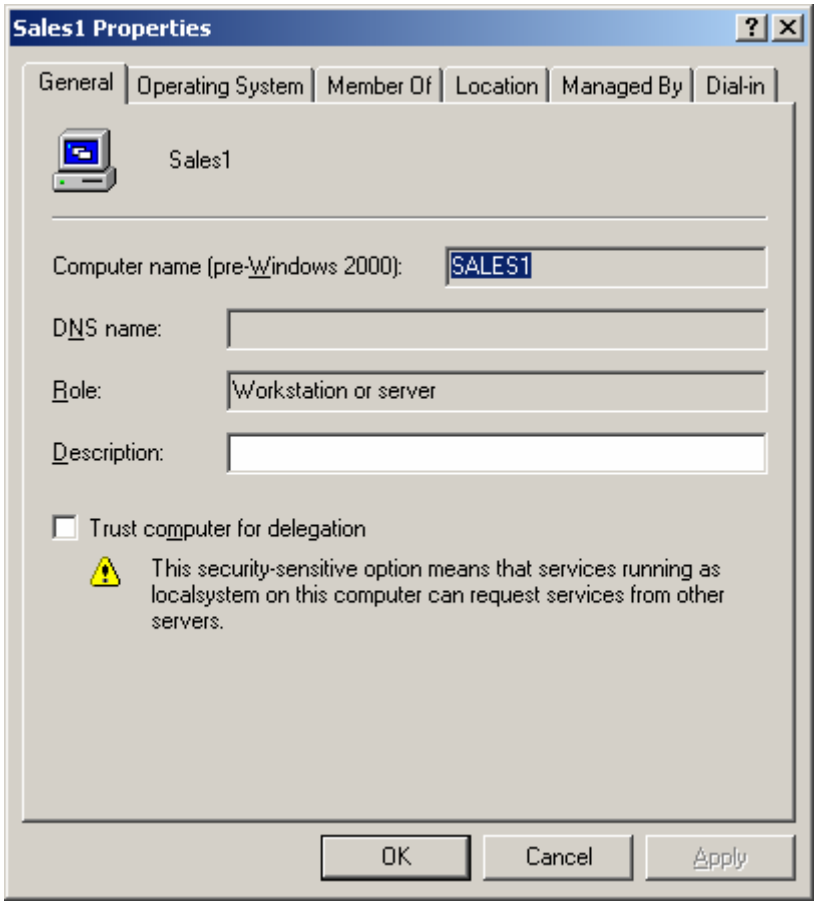
[63] Μπορούμε να επιλέξουμε No Override εάν επιθυμούμε την ανάθεση ενός μόνο GPO, ή Disabled εάν δεν επιθυμούμε καμία ανάθεση σε GPO.



Εικόνα 4-57. Computer Properties.

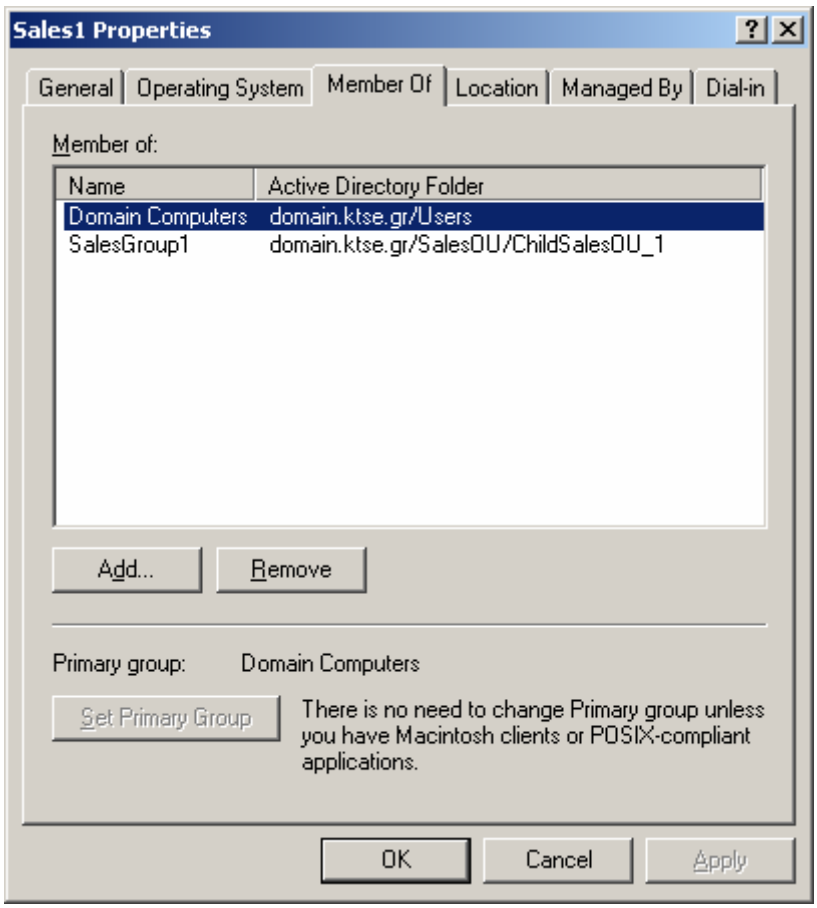
2. Στην καρτέλα General παρατηρούμε τις γενικές πληροφορίες του αντικειμένου και δίνεται η επιλογή Trust coputer for delegation, που σημαίνει πως ο υπολογιστής αυτός μπορεί να έχει πρόσβαση σε πηγές και υπηρεσίες άλλων υπολογιστών.[64]

[64] Το delegation είναι δυνατό χάριν της υποστήριξής του από το Kerberos authentication protocol. Περισσότερες πληροφορίες είναι διαθέσιμες στη διεύθυνση: http://technet.microsoft.com/en-us/library/cc961952.aspx.



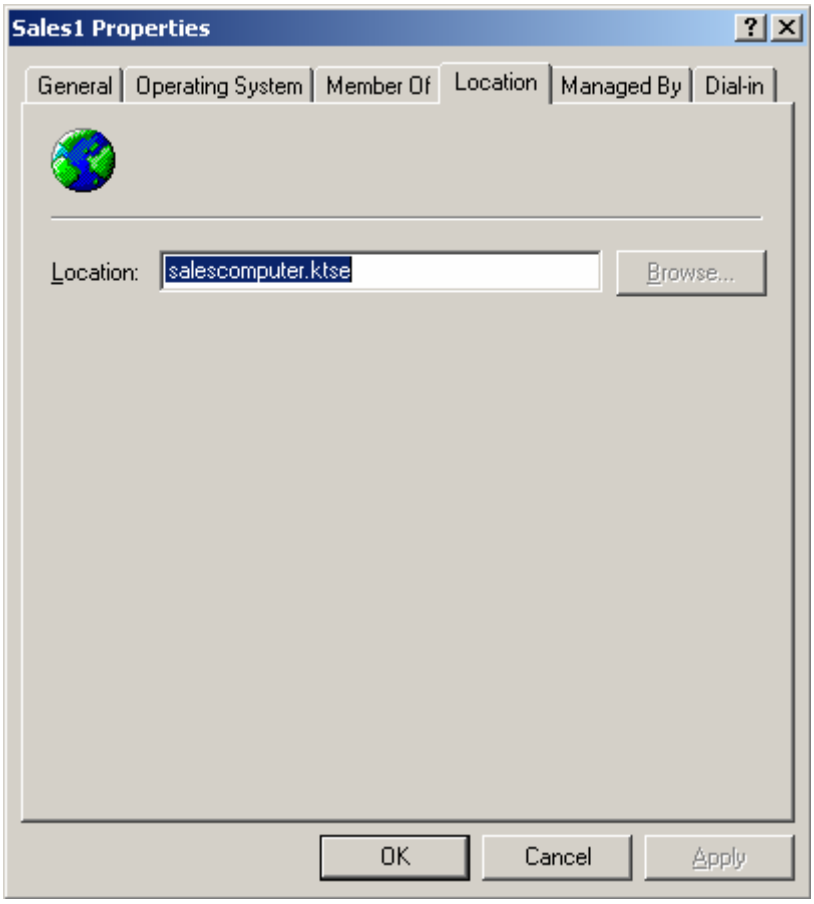
Εικόνα 4-58. Computer Properties: Η καρτέλα General.

3. Στην καρτέλα Member Of μπορούμε να αναθέσουμε το αντικείμενο σε κάποια ομάδα όπως περιγράφηκε πιο πάνω σε αυτή την ενότητα.



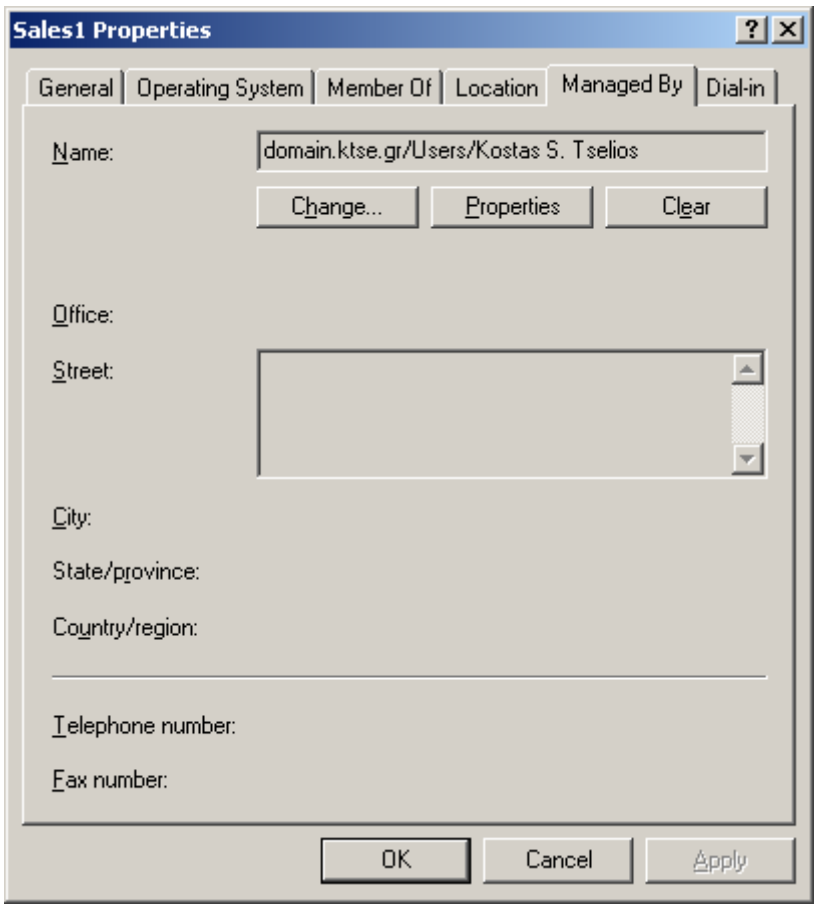
Εικόνα 4-59. Computer Properties: Η καρτέλα Member Of.

4. Στην καρτέλα **Location** μπορούμε να παρατηρήσουμε ή να αλλάξουμε τη διεύθυνση του υπολογιστή στο domain με τη μορφή computername.domain.



Εικόνα 4-60. Computer Properties: Η καρτέλα Location.

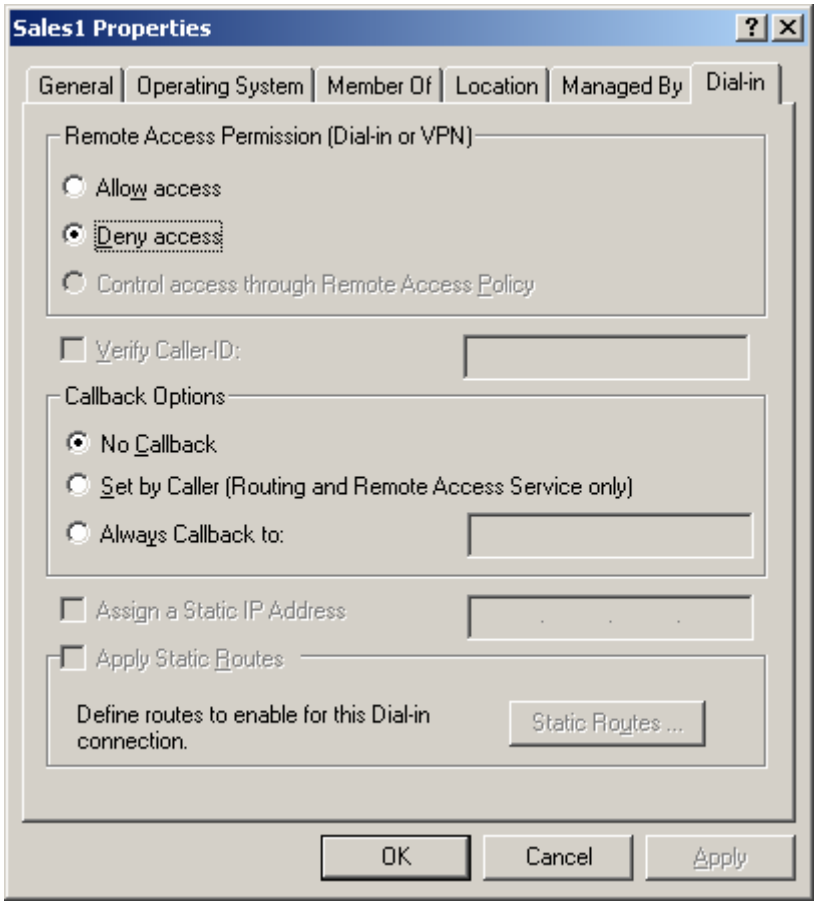
5. Στην καρτέλα Managed By μπορούμε να θέσουμε ή να αλλάξουμε τον υπεύθυνο διαχείρισης του αντικειμένου. Για να αλλάξουμε τον manager του OU πατάμε Change, στο object name θέτουμε το όνομα του χρήστη και πατάμε Check Names. Εφόσον το όνομα είναι σωστό και φαίνεται υπογραμισμένο πατάμε OK. Εάν δεν επιθυμούμε να θέσουμε κάποιον ως manager του αντικειμένου, πατάμε Clear.



Εικόνα 4-61. Computer Properties: Η καρτέλα Managed By.

6. Στην καρτέλα **Dial-In** μπορούμε να επιτρέψουμε ή να απαγορεύσουμε την πρόσβαση μέσω Dial-In ή VPN.[65] Το callback γίνεται, αφού έχει γίνει η ταυτοποίηση και έχει εδραιωθεί η σύνδεση, αποσυνδέοντας το χρήστη και επανιδρύοντας τη σύνδεση με αυτόν, λίγες στιγμές αργότερα, για εξακρίβωση της ταυτότητάς του.[66] Οι επιλογές που δίνονται για το callback είναι: **No Callback** (δεν είναι ενεργοποιημένο), **Set by Caller** (για χρήστες που αλλάζουν τοποθεσίες και αριθμούς) και **Always Callback to** (στο πεδίο αυτό θέτουμε τον αριθμό του εξοπλισμού που είναι συνδεδεμένος ο χρήστης και που θα καλεστεί κατά το callback). Στην επιλογή **Assign a Static IP Adress** αναθέτουμε μία στατική IP διεύθυνση στο αντικείμενο. Στην επιλογή **Apply Static Routes**, στον διάλογο **Static Routes** θέτουμε τις ρυθμίσεις που θέλουμε να έχει ο Dial-In υπολογιστής (Προορισμός [Destination], Μάσκα δικτύου [Network Mask] και Metric [αριθμός αλμάτων]).

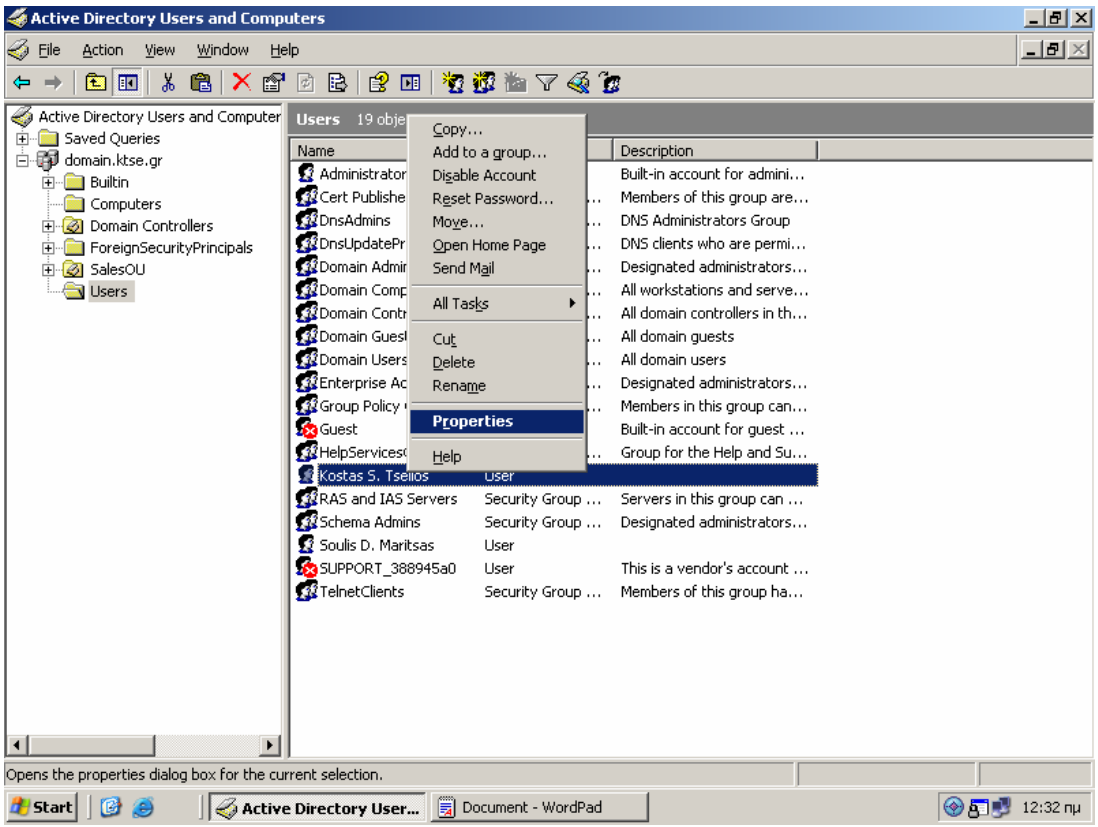
[65] Η διαφορά των Dial-In και VPN έγκειται στο ότι το Dial-In έχει να κάνει με σύνδεση σε modems, ενώ το VPN έχει να κάνει με σύνδεση σε τερματικά.
[66] http://technet.microsoft.com/en-us/library/cc778189.aspx.



Εικόνα 4-62. Computer Properties: Η καρτέλα Dial-In.

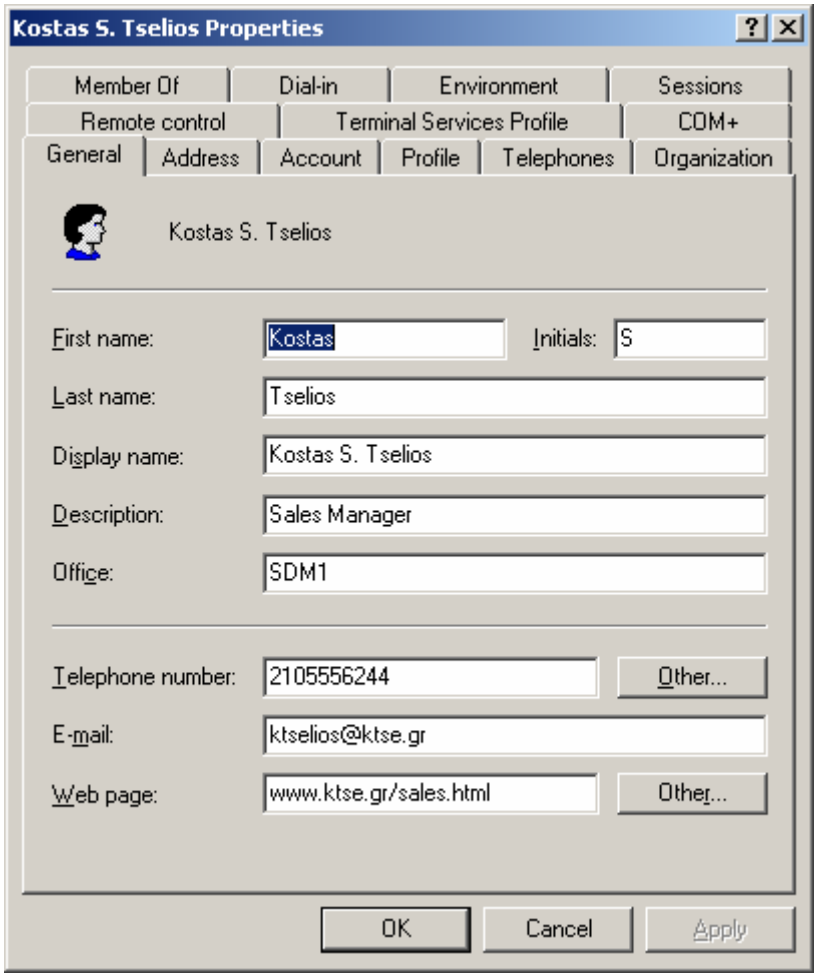
Για να παρατηρήσουμε τις ιδιότητες των Users ακολουθούμε τα παρακάτω βήματα:

1. Κάνουμε δεξί κλικ στον επιθυμητό User και πατάμε **Properties**.



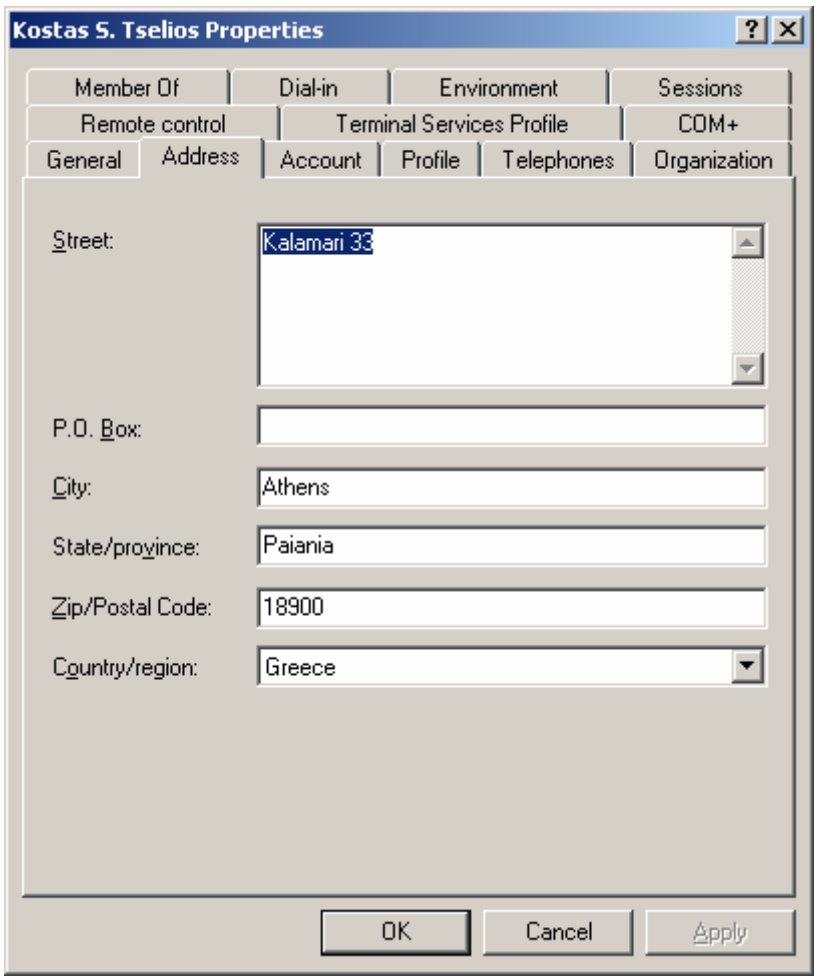
Εικόνα 4-63. User Properties.

2. Στην καρτέλα **General** παρατηρούμε και τροποποιούμε τις γενικές πληροφορίες του αντικειμένου.



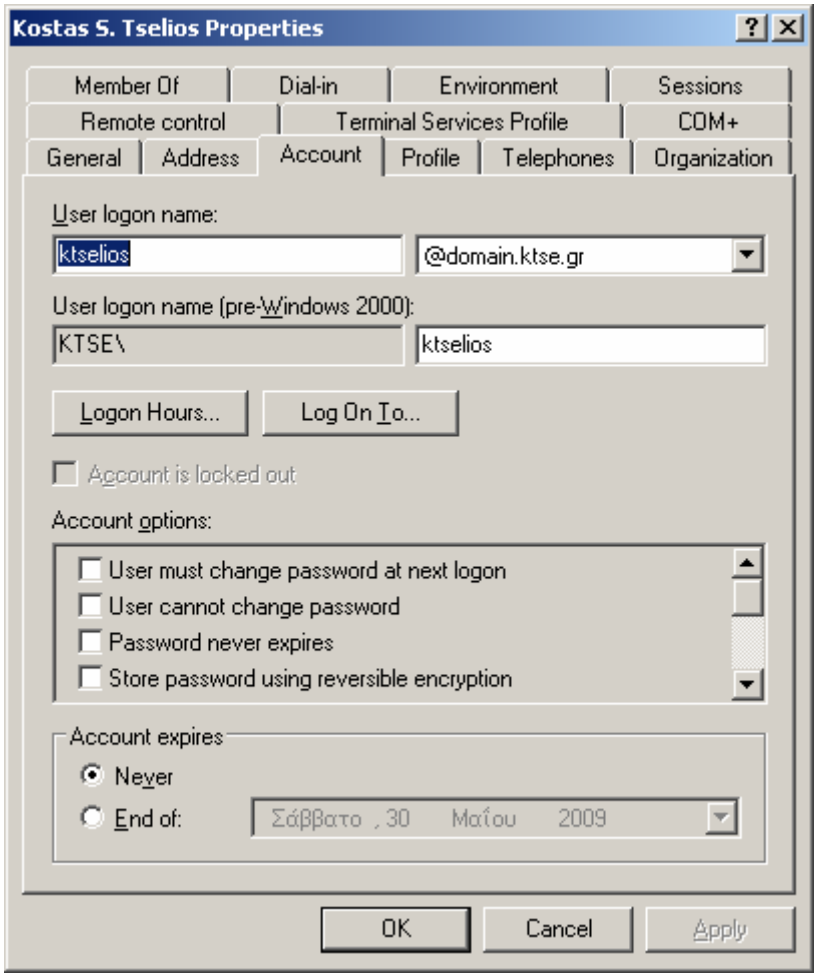
Εικόνα 4-64. User Properties: Η καρτέλα General.

3. Στην καρτέλα **Address** παρατηρούμε και τροποποιούμε πληροφορίες όσον αφορά τη φυσική διεύθυνση, την πόλη και τον ταχυδρομικό κωδικό του αντικειμένου.

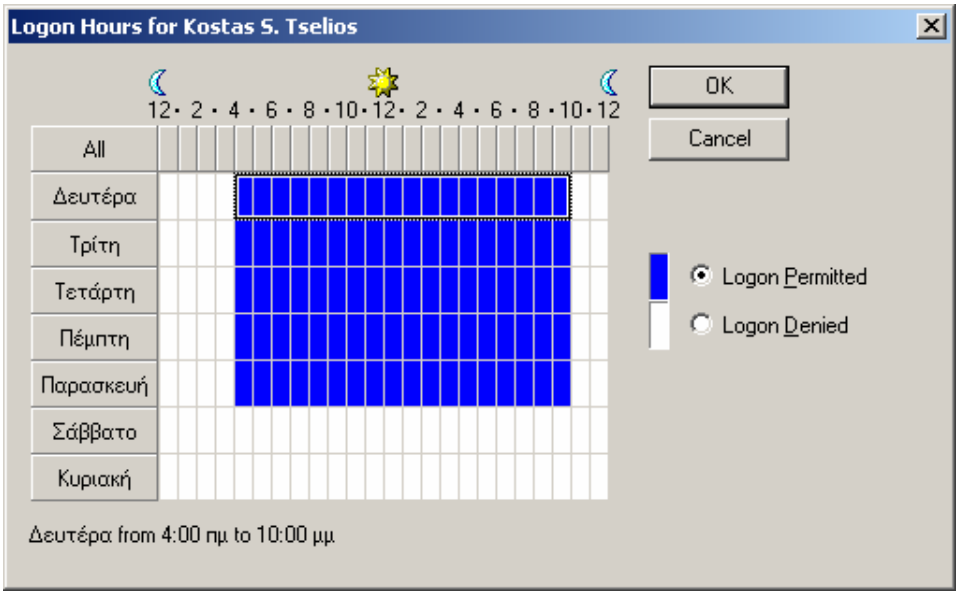


Εικόνα 4-65. User Properties: Η καρτέλα Address.

4. Στην καρτέλα **Account** μπορούμε να διαχειριστούμε το λογαριασμό του χρήστη. Πατώντας την επιλογή **Logon Hours** μπορούμε να περιορίσουμε την πρόσβαση του χρήστη, ανάλογα με τις επιθυμητές ώρες και μέρες, και στην επιλογή **Log On To** μπορούμε να περιορίσουμε την πρόσβαση του χρήστη ανάλογα με τους επιθυμητούς επιτρεπτούς υπολογιστές. Δίνονται επίσης επιλογές για το λογαριασμό του χρήστη, όπως να αλλάξει αναγκαστικά τον κωδικό κατά την πρώτη πρόσβαση στον τομέα ή να μην δίνεται καθόλου η δυνατότητα αλλαγής κωδικού. Στην επιλογή **Account Expires** μπορούμε να θέσουμε το αν και πότε θα λήξει ο λογαριασμός του εκάστοτε χρήστη.

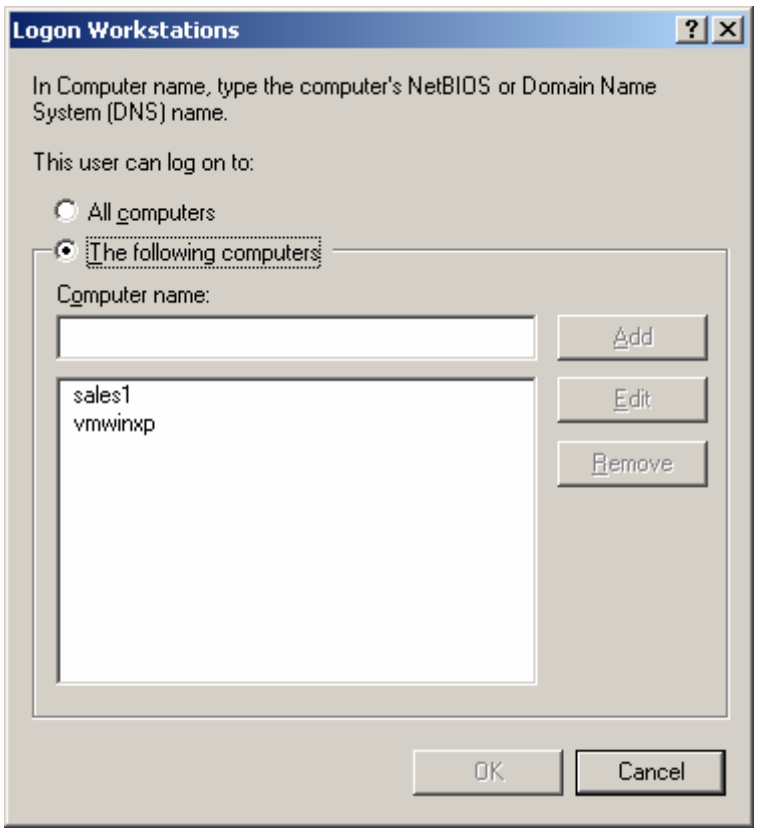


Εικόνα 4-66. User Properties: Η καρτέλα Account.



Εικόνα 44-67. User Properties: Στην καρτέλα Account, η επιλογή Logon Hours.[67]

[67] Επιτρέπεται η πρόσβαση από Δευτέρα μέχρι Παρασκευή από τις 04:00 μέχρι τις 22:00.

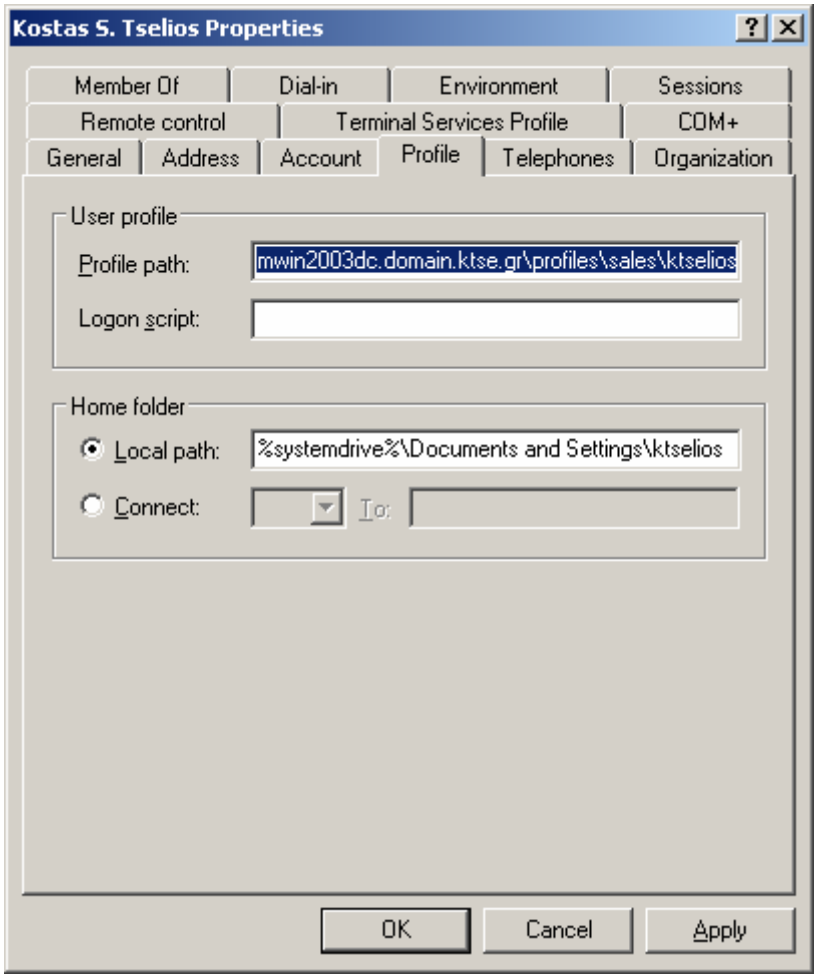


Εικόνα 44-68. User Properties: Στην καρτέλα Account, η επιλογή Log On To.[68]

5. Στην καρτέλα **Profile**[69] μπορούμε να θέσουμε και να χειριστούμε το profile του χρήστη ανάλογα με τη φύση του (Local profile, Roaming profile και Mandatory profile). Στην ομάδα **User Profile** υπάρχουν οι επιλογές **Profile Path**, όπου θέτουμε τον κατάλογο που βρίσκεται το profile του χρήστη και είναι της μορφής *\\server_name\share_name\subfolder\user_name*, και μπορεί να συγχρονίζεται με το local profile, εφόσον η πρόσβαση πραγματοποιείται από διαφορετικούς υπολογιστές, και **Logon Script**, όπου μπορούμε να θέσουμε εναλλακτικά κάποιο Active Directory Service Interfaces [ADSI][70] script για το logon (πχ VBScript ή Jscript). Στην ομάδα **Home Folder** υπάρχουν οι επιλογές **Local Path**, όπου μπορούμε να θέσουμε τον κατάλογο που βρίσκεται το τοπικό profile του χρήστη και είναι της μορφής *%SystemDisk%\Documents and Settings\User_name*[71], και **Connect**, όπου αναθέτουμε κάποιο κατάλογο (σε μορφή εικονικού δίσκου), θέτοντας ένα τυχαίο όνομα δίσκου (πχ Z:\ ), ως roaming profile του χρήστη και είναι της μορφής:
Connect Z:\ To \\server_name\share_name\subfolder\user_name[72].

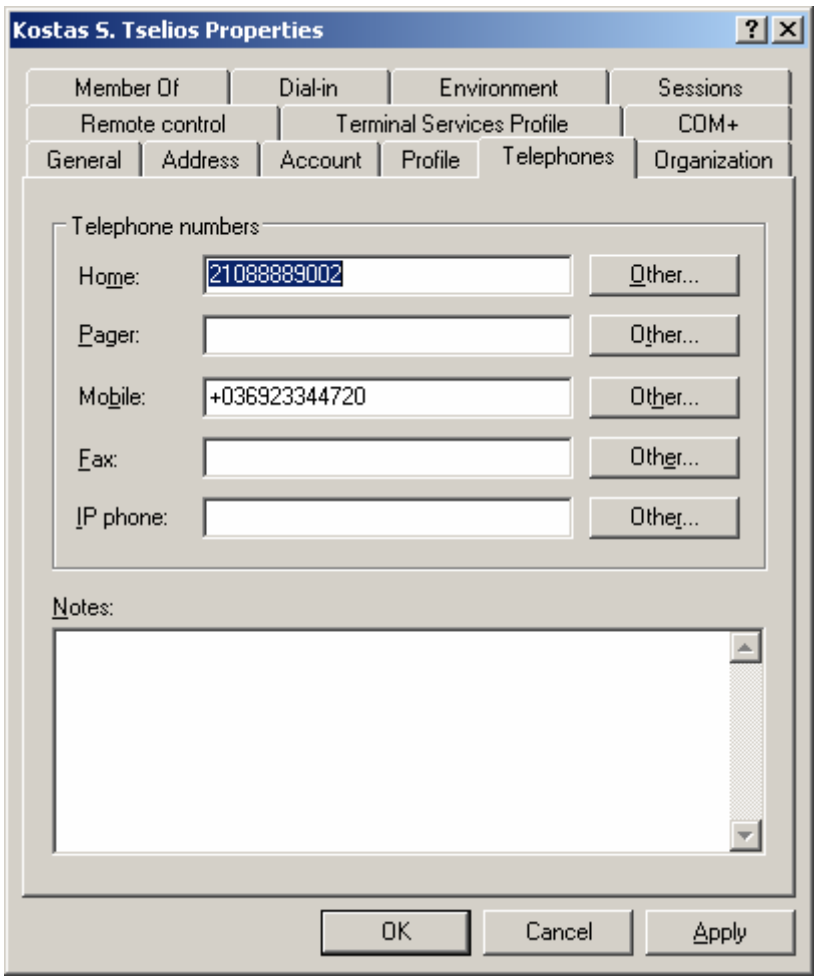
---

[68] Επιτρέπεται η πρόσβαση στους υπολογιστές sales1 και vmwinxp.
[69] Γενικά για τα User Profiles και τη διαχείρισή τους, μπορούμε να συμβουλευτούμε τη Βιβλιοθήκη Τεχνικών Θεμάτων της Microsoft στη διεύθυνση: http://technet.microsoft.com/en-us/library/bb726990.aspxH.
[70] Περισσότερες πληροφορίες μπορούν να αντληθούν από εδώ: http://msdn.microsoft.com/en-us/library/aa772170.aspx.
[71] Εάν δεν θέσουμε κάποιο path, αυτό δημιουργείται αυτόματα κατά την πρώτη είσοδο στον τομέα και έπειτα συγχρονίζεται με το Roaming Profile Path.
[72] Η χρησιμοποίηση ανάθεσης καταλόγου διευκολύνει τον διαχειριστή στη διαδικασία του backup, διότι τα profiles μπορούν να βρίσκονται σε κάποιο απομακρυσμένο server και όχι απαραίτητα στο domain controller.



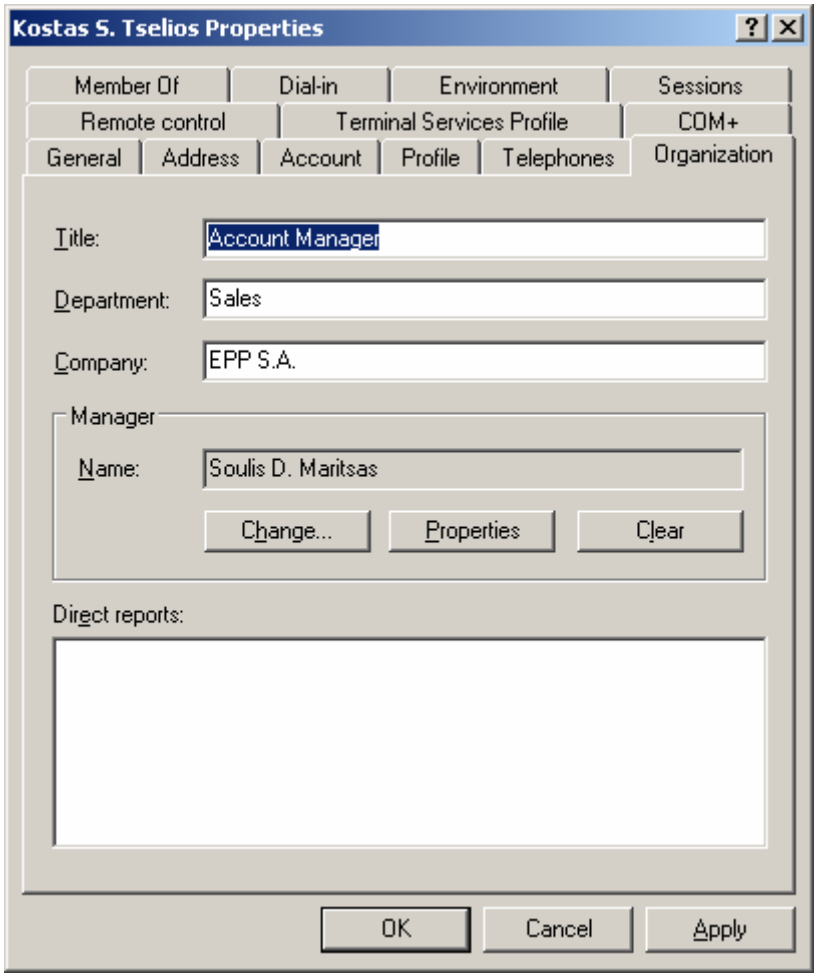
Εικόνα 4-69. User Properties: Η καρτέλα Profile.

6. Στην καρτέλα **Telephones** μπορούμε να παρατηρήσουμε και να τροποποιήσουμε πληροφορίες όσον αφορά την τηλεφωνική επικοινωνία του χρήστη. Στις επιλογές **Other** δίνεται η δυνατότητα να χρησιμοποιηθεί μία τιμή η οποία έχει επαναχρησιμοποιηθεί, κάνοντας ποιο γρήγορη και εύκολη τη συγκεκριμένη διεργασία.



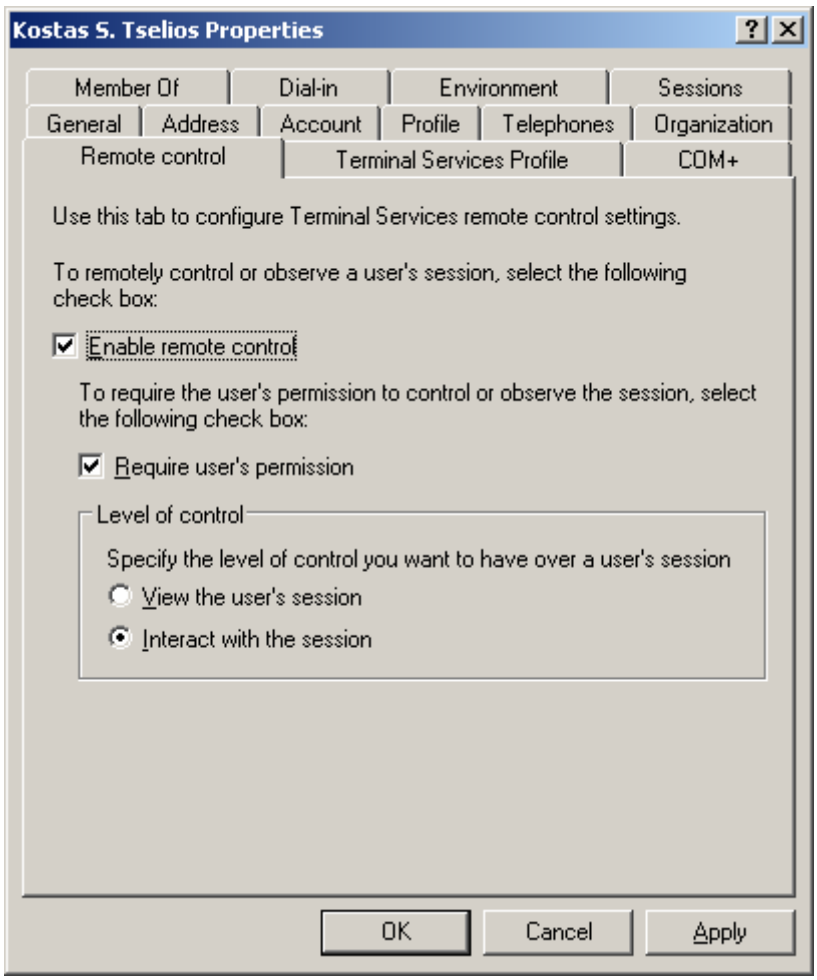
Εικόνα 4-70. User Properties: Η καρτέλα Telephones.

7. Στην καρτέλα **Organization** μπορούμε να παρατηρήσουμε και να τροποποιήσουμε πληροφορίες όσον αφορά τον τίτλο του χρήστη, το τμήμα εργασίας ή την εταιρία εργασίας, καθώς και το όνομα του διαχειριστή του τμήματος εργασίας.



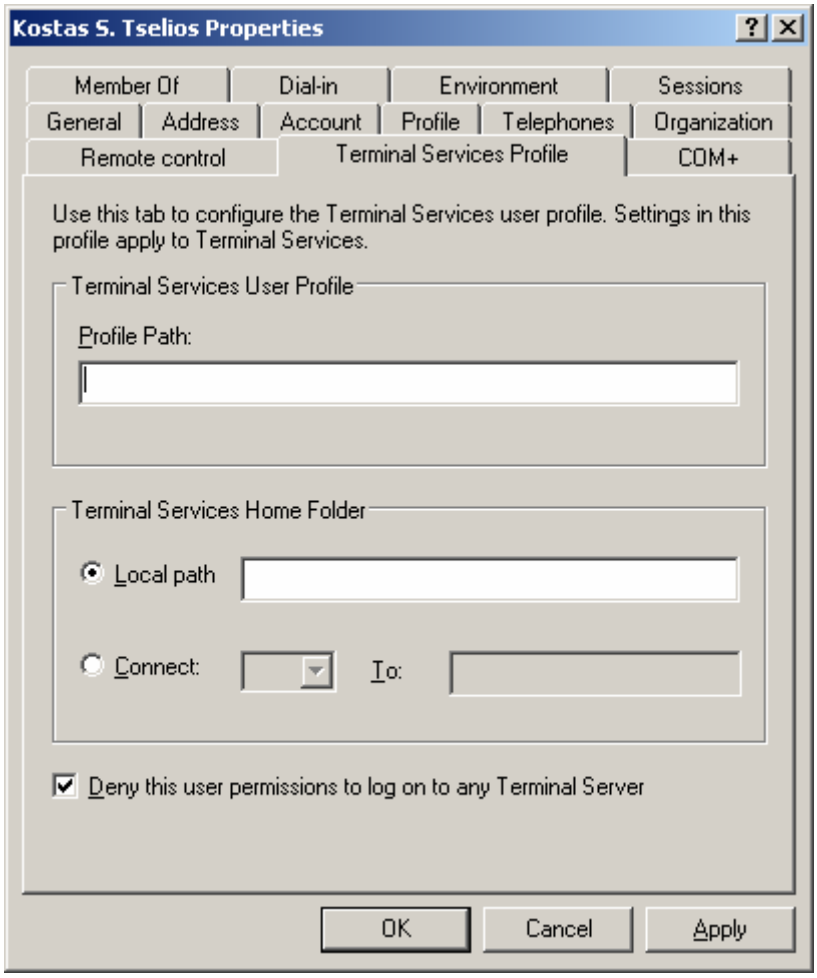
Εικόνα 4-71. User Properties: Η καρτέλα Organization.

8. Στην καρτέλα **Remote Control** μπορούμε να επιλέξουμε εάν θα ενεργοποιήσουμε τον απομακρυσμένο έλεγχο ή όχι (**Enable Remote Control**) και εάν θα απαιτείται η άδεια του χρήστη ή όχι (**Require User's Permission**) για τον απομακρυσμένο έλεγχο. Στην ομάδα **Level of Control**, μπορούμε να ορίσουμε σε ποιό επίπεδο θα υφίσταται αυτός ο έλεγχος, και πιο συγκεκριμένα, μπορούμε να επιλέξουμε **View the User's Session** εάν θα υπάρχει απλή παρατήρηση της συνεδρίας, ή **Interact with the Session** εάν θα υπάρχει αλληλεπίδραση με τη συνεδρία του χρήστη.



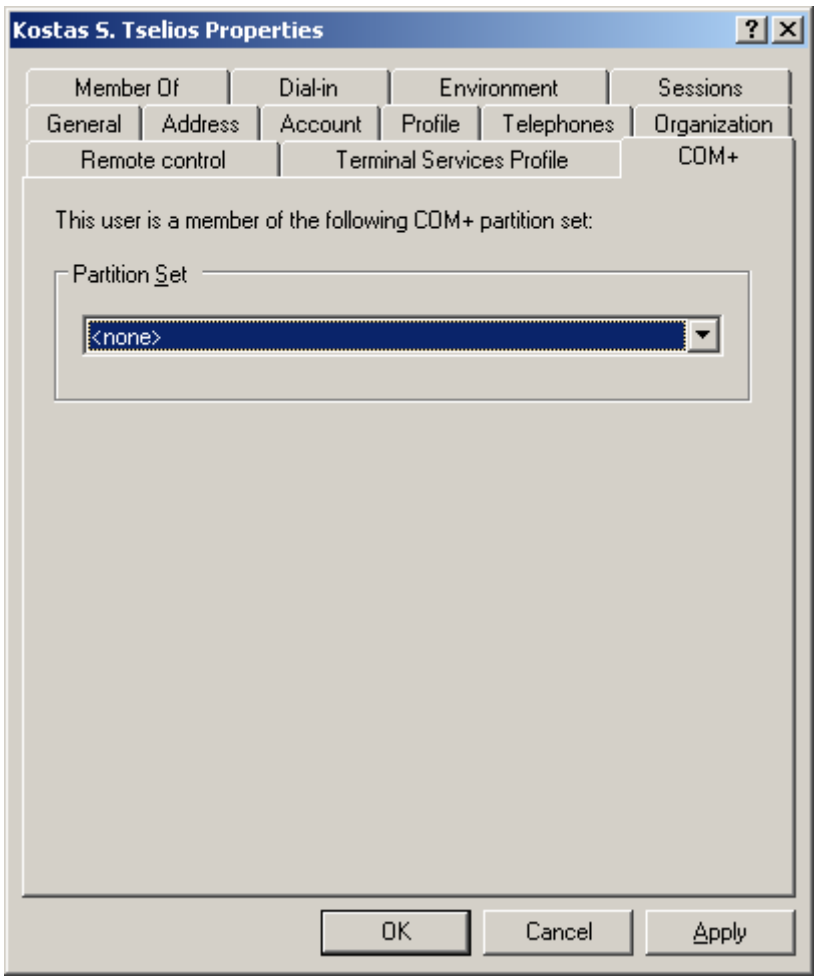
Εικόνα 4-72. User Properties: Η καρτέλα Remote Control.

9. Στην καρτέλα **Terminal Services Profile** θέτουμε τα αντίστοιχα μονοπάτια που των roaming και local profiles του χρήστη που θα τα αντλήσει εφόσον είναι εγγεγραμμένος σε terminal services. Από την επιλογή **Deny this User Permissions to log on to any Terminal Server** μπορούμε να επιλέξουμε εάν θα επιτραπεί η πρόσβαση ή όχι σε οποιοδήποτε terminal server.



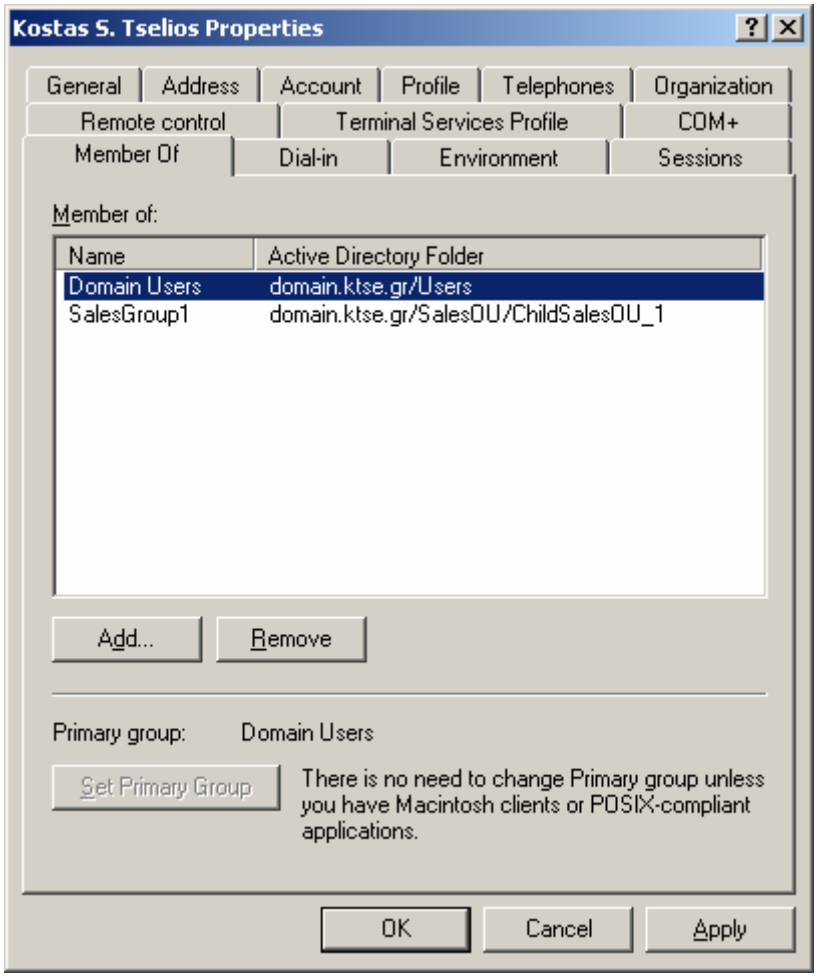
Εικόνα 4-73. User Properties: Η καρτέλα Terminal Services Profile.

10. Στην καρτέλα COM+ μπορούμε να κάνουμε το αντικείμενο μέλος ενός COM+ διαμερίσματος.



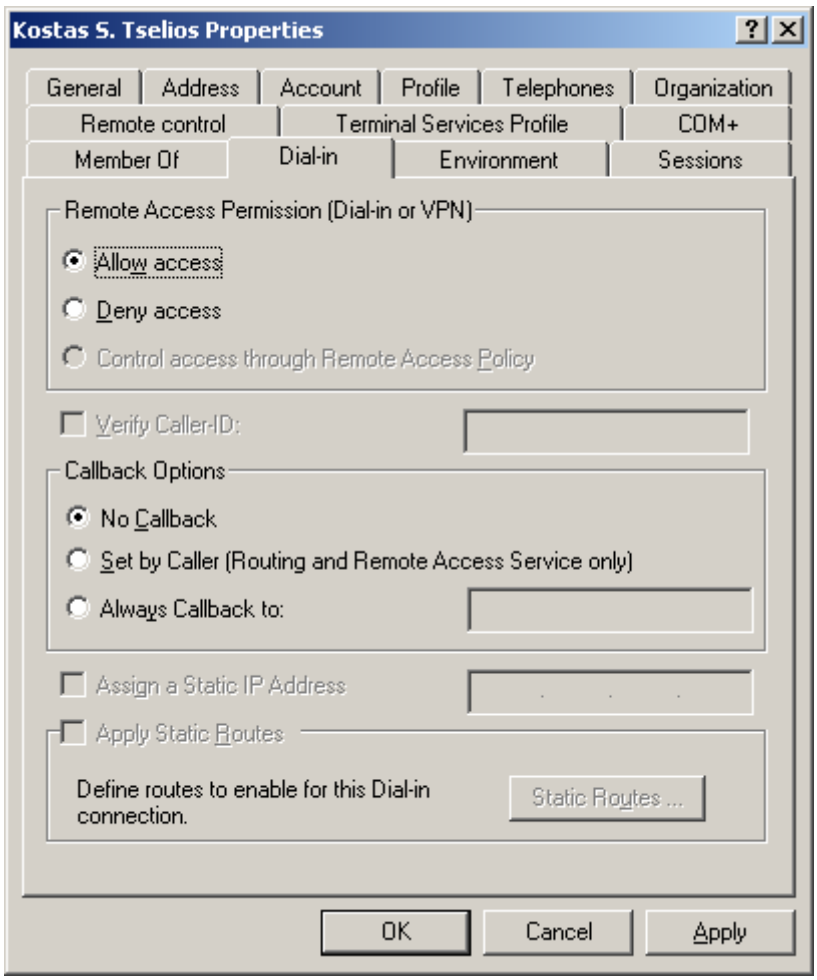
Εικόνα 4-74. User Properties: Η καρτέλα COM+.

11. Στην καρτέλα Member Of μπορούμε να αναθέσουμε το αντικείμενο σε κάποια ομάδα όπως περιγράφηκε πιο πάνω σε αυτή την ενότητα.



Εικόνα 4-75. User Properties: Η καρτέλα Member Of.

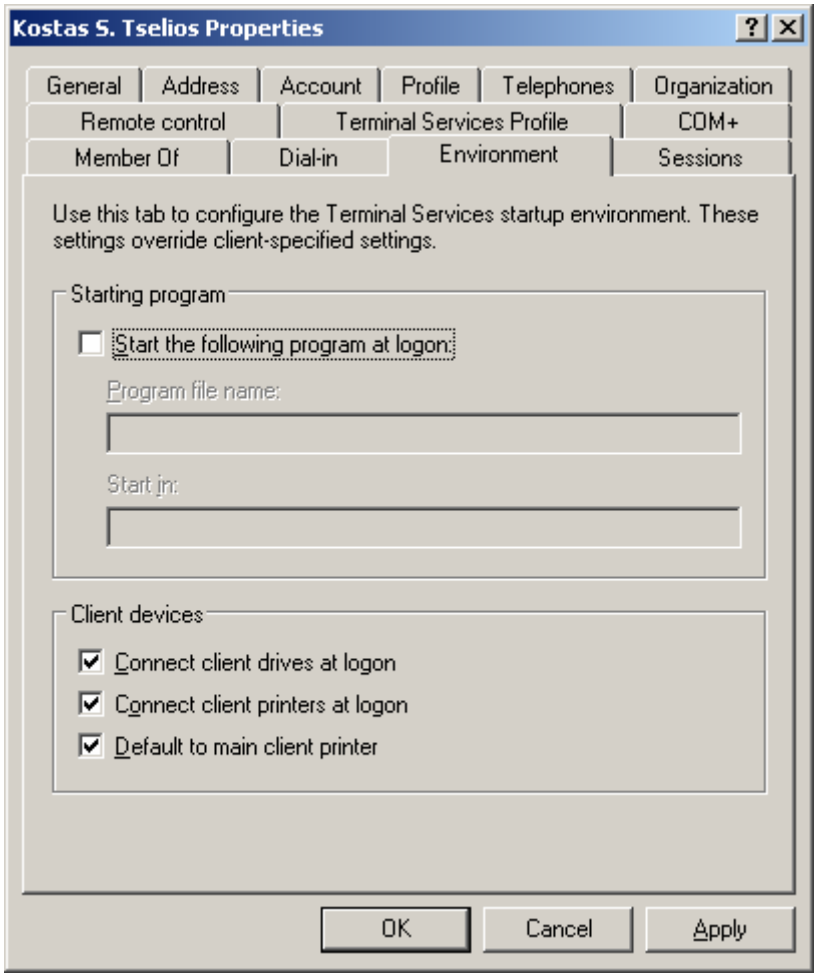
12. Στην καρτέλα **Dial-In** μπορούμε να επιτρέψουμε ή να απαγορεύσουμε την πρόσβαση μέσω Dial-In ή VPN. Οι επιλογές που δίνονται για το callback είναι: **No Callback** (δεν είναι ενεργοποιημένο), **Set by Caller** (για χρήστες που αλλάζουν τοποθεσίες και αριθμούς) και **Always Callback to** (στο πεδίο αυτό θέτουμε τον αριθμό του εξοπλισμού που είναι συνδεδεμένος ο χρήστης και που θα καλεστεί κατά το callback). Στην επιλογή **Assign a Static IP Adress** αναθέτουμε μία στατική IP διεύθυνση στον εξοπλισμό του χρήστη. Στην επιλογή **Apply Static Routes**, στον διάλογο **Static Routes** θέτουμε τις ρυθμίσεις που θέλουμε να έχει ο Dial-In υπολογιστής (Προορισμός [Destination], Μάσκα δικτύου [Network Mask] και Metric [αριθμός αλμάτων]).



Εικόνα 4-76. User Properties: Η καρτέλα Dial-In.

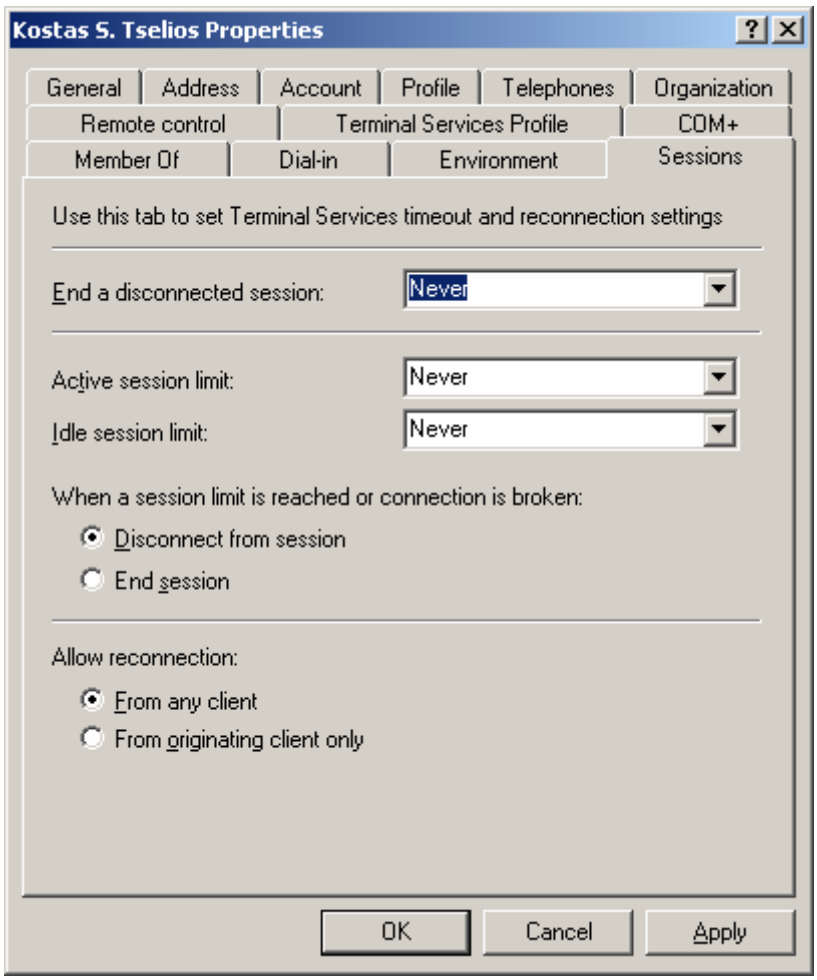
13. Στην καρτέλα **Environment** μπορούμε να ορίσουμε μέσω της ομάδας **Starting Program**, εάν θα εκκινείτε κάποιο πρόγραμμα κατά το logon. Στο πεδίο **Program File Name**, θέτουμε το όνομα του προγράμματος που θα εκτελεστεί και στο πεδίο **Start In** θέτουμε το χωρίο μέσα στο οποίο θα εκτελεστεί το πρόγραμμα.[73] Στην ομάδα **Client Devices** επιλέγουμε **Connect Client Drives at Logon** εάν είναι επιθυμητή η σύνδεση με οδηγούς (πχ δίσκους) που βρίσκονται στο δίκτυο κατά το logon, επιλέγουμε **Connect Client Printers at Logon**, εάν είναι επιθυμητή η σύνδεση με εκτυπωτές που είναι στο δίκτυο και τέλος επιλέγουμε **Default to Main Client Printer**, εάν θα υφίσταται σύνδεση με τον προεπιλεγμένο κεντρικό εκτυπωτή στο δίκτυο.

[73] Για περισσότερες πληροφορίες σχετικά με την αυτόματη εκτέλεση προγραμμάτων κατά το logon απευθυνθείτε εδώ: http://technet.microsoft.com/en-us/library/cc781043.aspxp.



Εικόνα 4-77. User Properties: Η καρτέλα Environment.

14. Στην καρτέλα **Sessions** θέτουμε παραμέτρους που αφορούν τις συνεδρίες του χρήστη με terminal services. Στην επιλογή **End a Disconnected Session** μπορούμε να ορίσουμε σε πόσο χρόνο θα τερματίζεται μία ανενεργή συνεδρία. Στην επιλογή **Active Session Limit** μπορούμε να ορίσουμε τη διάρκεια μίας ενεργής συνεδρίας. Στην επιλογή **Idle Session Limit** μπορούμε να ορίσουμε τη διάρκεια μίας συνεδρίας που βρίσκεται σε αδράνεια. Όταν μία συνεδρία έχει φτάσει τον περιορισμό χρονικής διάρκειας ή έχει χαθεί η σύνδεση με το χρήστη, με την επιλογή **Disconnect From Session** ορίζουμε να αποσυνδεθεί ο χρήστης από τη συνεδρία, ενώ με την επιλογή **End Session** ορίζουμε να τερματιστεί εντελώς η συνεδρία. Τέλος με την επιλογή **Allow Connection From Any Client**, ορίζουμε να μπορεί να γίνεται η επανασύνδεση από οποιοδήποτε πελάτη (πχ υπολογιστή, εξοπλισμό) ενώ με την επιλογή **From Originated Client Only** επιτρέπουμε την επανασύνδεση μόνο από πιστοποιημένο πελάτη.

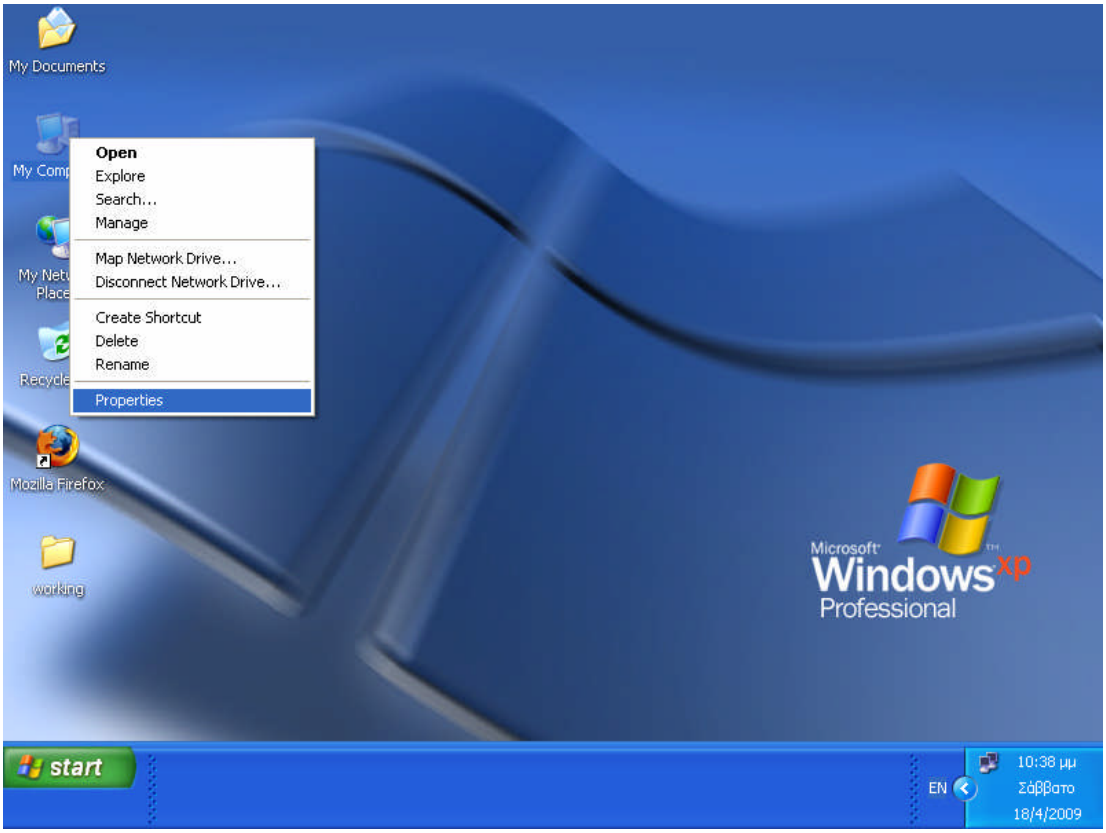


Εικόνα 4-78. User Properties: Η καρτέλα Sessions.

4.3.5 *Καταχώρηση Client σε Τομέα*

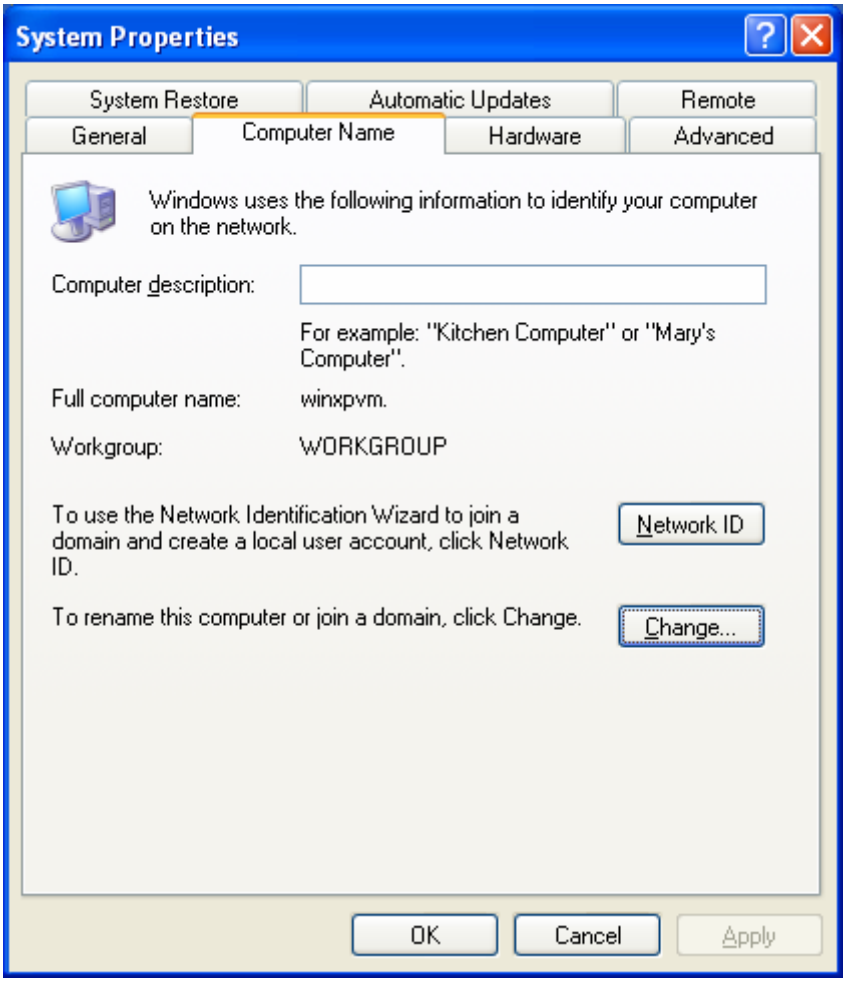
Σε αυτό το σημείο και έχοντας πραγματοποιήσει μία επιτυχή εγκατάσταση και παραμετροποίηση του Active Directory, έχουμε τη δυνατότητα προσθήκης clients σε τομέα. Για να καταχωρηθεί ένας υπολογιστής (client) σε κάποιο τομέα ακολουθούμε τα παρακάτω βήματα:

1. Κάνουμε δεξί κλικ στο **My Computer** και πατάμε **Properties**.



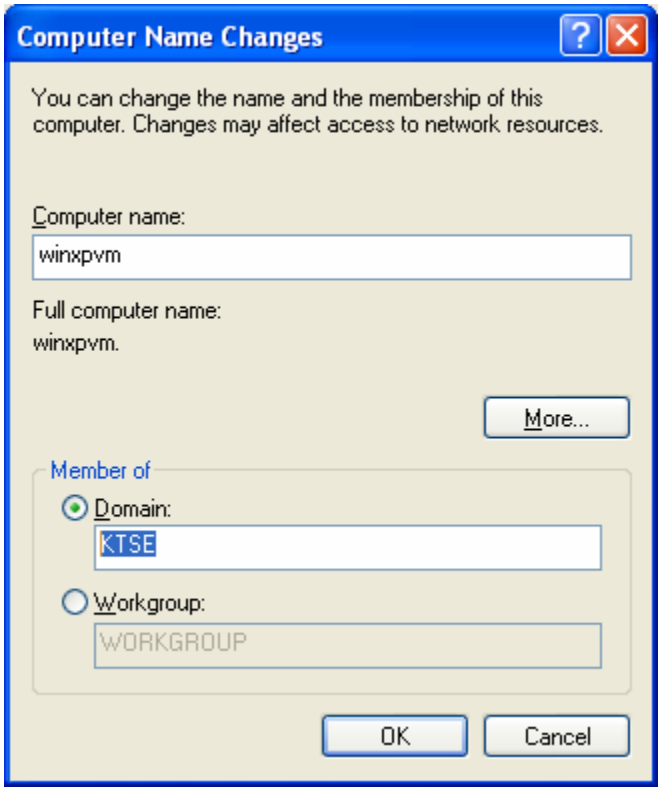
Εικόνα 4-79. My Computer Properties.

2. Στην καρτέλα **Computer Name** πατάμε **Change**.



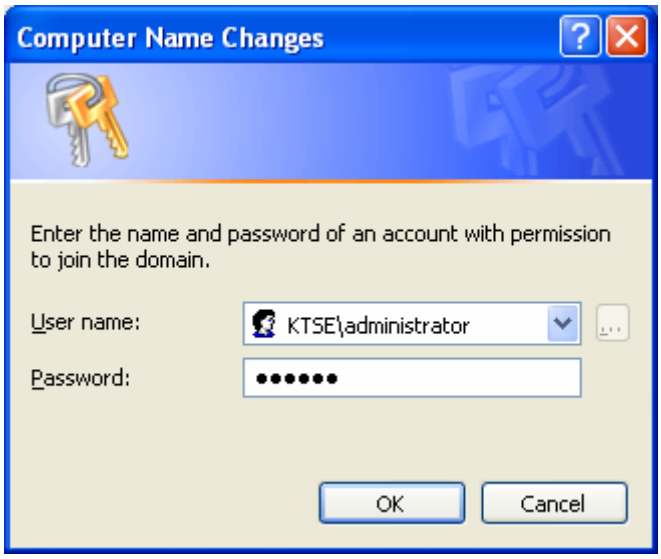
Εικόνα 4-80. System Properties. Στην καρτέλα Computer Name η επιλογή Change.

3. Επιλέγουμε Domain και πληκτρολογούμε στο πεδίο το όνομα του επιθυμητού τομέα.



Εικόνα 4-81. Computer Name Changes. Η επιλογή Member Of Domain.

4. Στο διάλογο επιβεβαίωσης θέτουμε στο **User Name** το όνομα του διαχειριστή του τομέα, που είναι της μορφής *Domain_name\Administrator_User_name*, και στο **Password** θέτουμε τον κωδικό του διαχειριστή. Πατάμε **OK**.

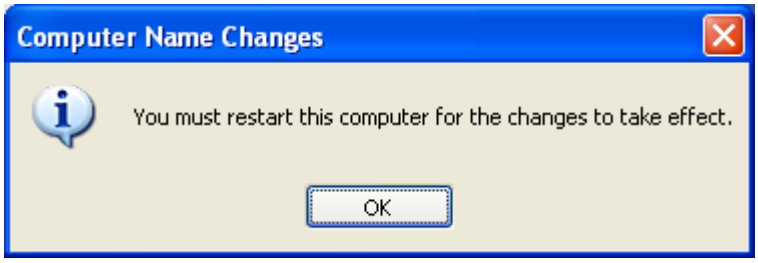


Εικόνα 4-82. Administrator authentication.

5. Πατάμε **OK**.

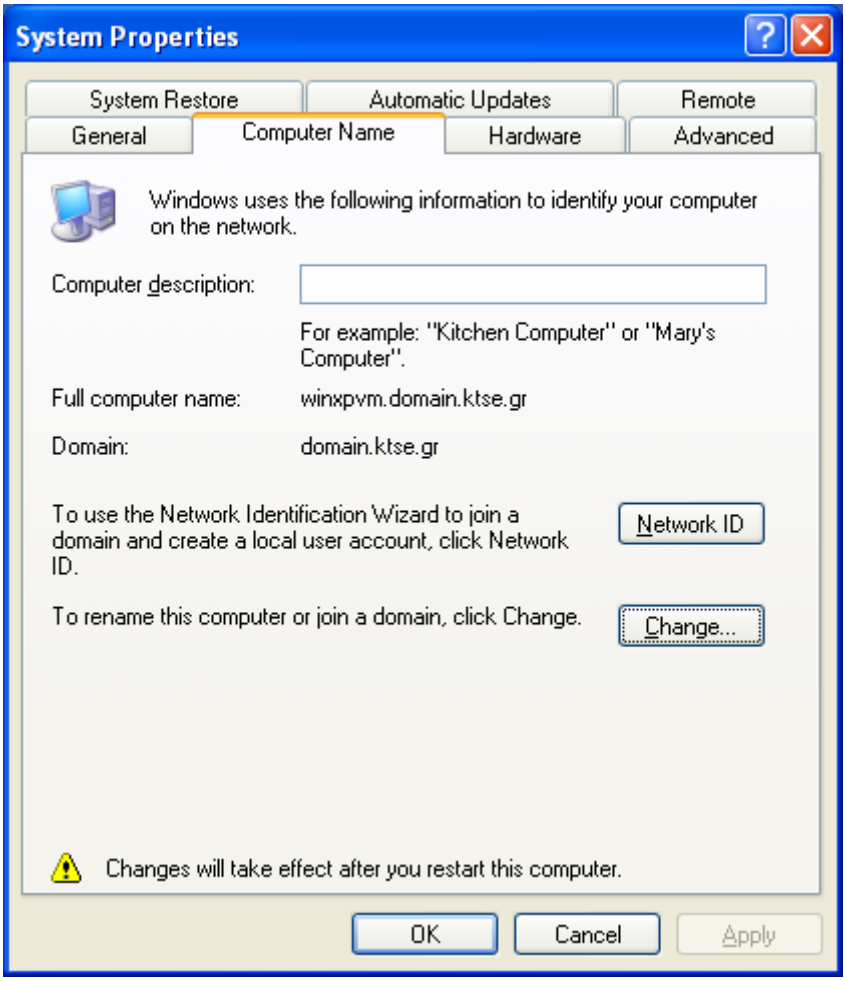
Εικόνα 4-83. Η οθόνη Welcome to domain.

6. Πατάμε **OK**.



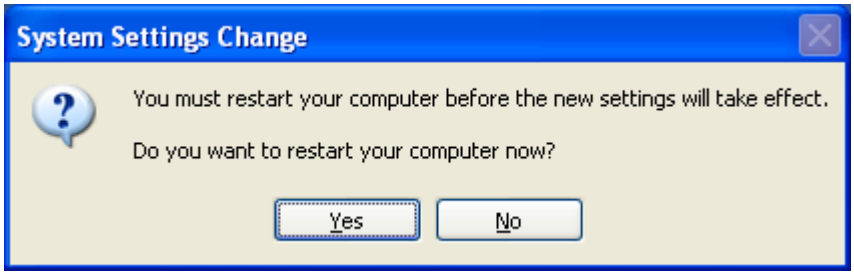
Εικόνα 4-84. Ειδοποίηση για επανεκκίνηση.

7. Πατάμε και πάλι **OK**.



Εικόνα 4-85. System Properties. Η καρτέλα Computer Name με τις αλλαγές.

8. Απαιτείται επανεκκίνηση του υπολογιστή client. Πατάμε **Yes**.



Εικόνα 4-86. Επιβεβαίωση επανεκκίνησης.

9. Στην επιλογή **Log On To** θέτουμε το όνομα του τομέα.

Εικόνα 4-87. Εισαγωγή στον τομέα βήμα 1ο.

10. Θέτουμε **User Name** και **Password** του User που έχει δημιουργηθεί μέσα στο Active Directory.

Εικόνα 4-88. Εισαγωγή στον τομέα βήμα 2ο.

11. Εφόσον έχει οριστεί να αλλάξει ο χρήστης τον κωδικό του κατά την πρώτη είσοδο στον τομέα, πατάμε **OK** για να προχωρήσουμε στη διαδικασία.

Εικόνα 4-89. Εισαγωγή στον τομέα βήμα 3ο.

12. Θέτουμε το παλιό και το νέο κωδικό και πατάμε **OK**.

Εικόνα 4-90. Εισαγωγή στον τομέα βήμα 4ο.

13. Πατάμε **OK**.

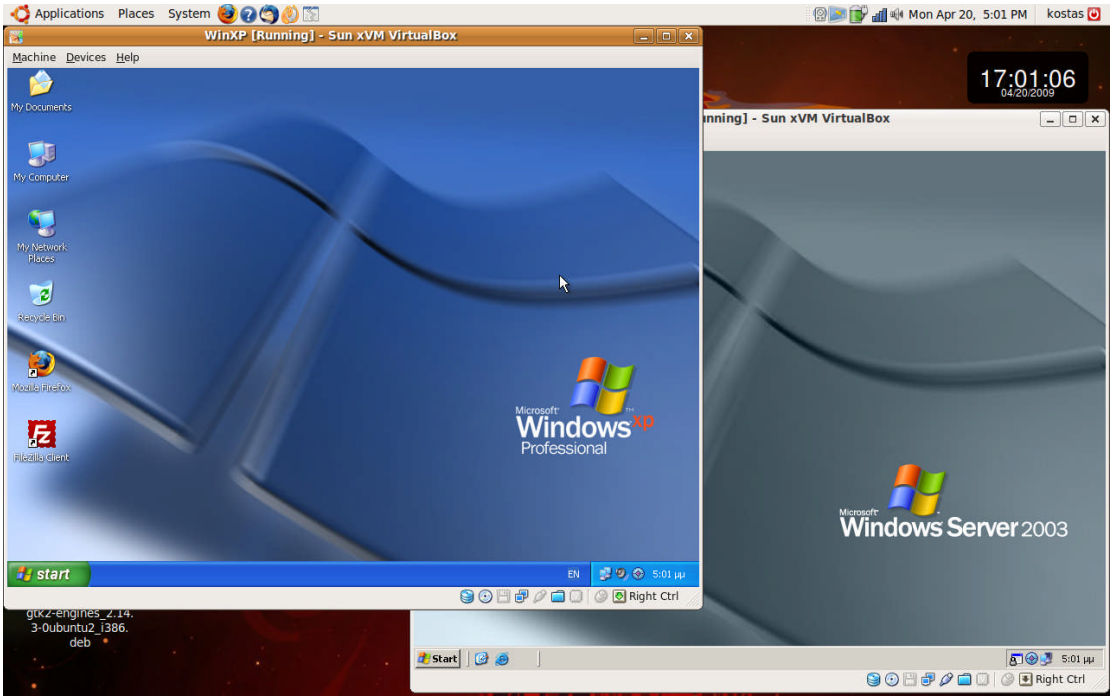
Εικόνα 4-91. Εισαγωγή στον τομέα βήμα 5ο.

14. Έχουμε εισέλθει επιτυχώς στον τομέα.

Εικόνα 4-92. Επιτυχής εισαγωγή στον τομέα.

4.4 Τοπολογία Δικτύου

Δημιουργήθηκε ένα πιλοτικό δίκτυο, το οποίο αποτελείτο από ένα router, ένα host και δύο εικονικές μηχανές (virtual machines [VM]). Το host που χρησιμοποιήθηκε ήταν ένα Ubuntu 8.10 σύστημα και τα εικονικά συστήματα ήταν ένα Windows XP Professional SP2 και ένα Windows Server 2003 SP2 R2.

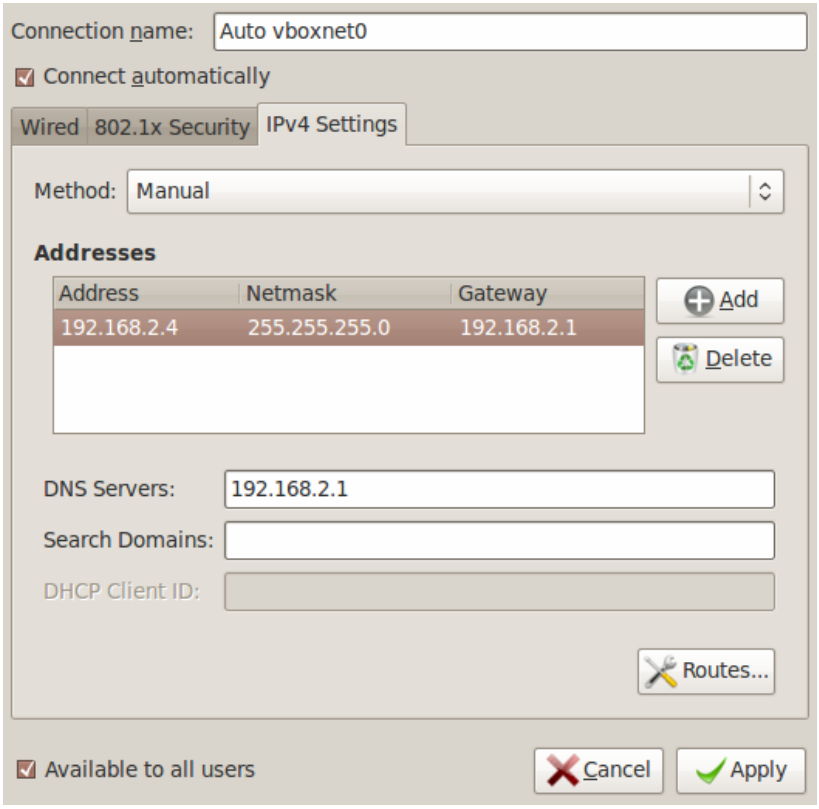


Εικόνα 4-93. VM Host με ενεργά τα δύο Virtual Machines.

Οι IP διευθύνσεις των συντελεστών είναι οι εξής:

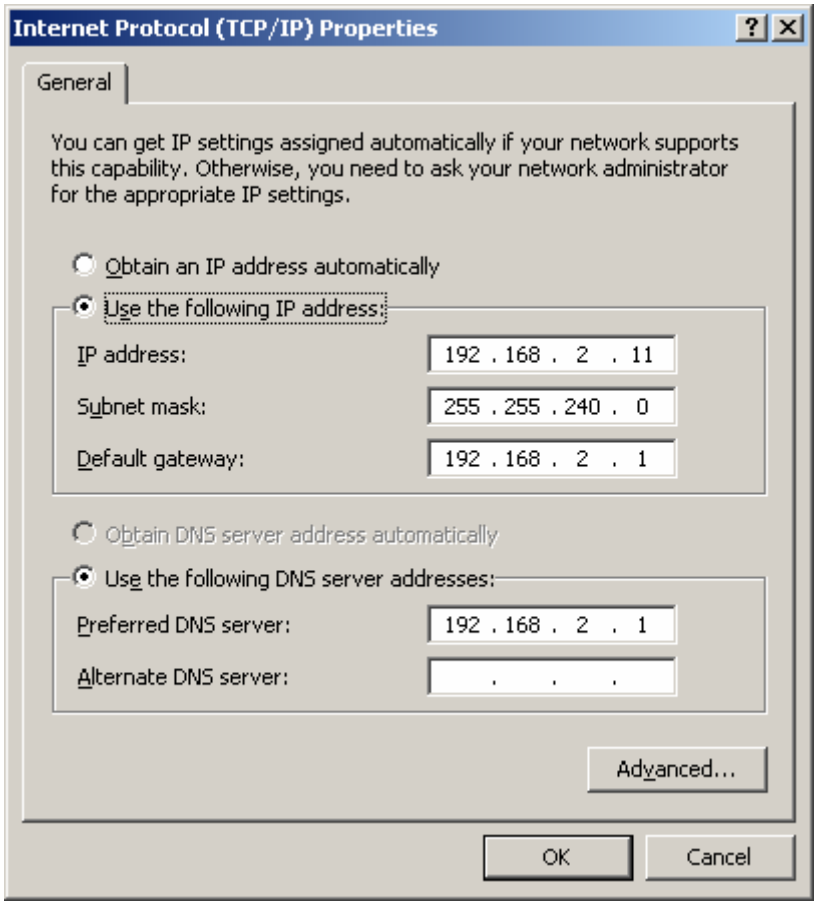
- Router: **192.168.2.1**
- VM Host: **192.168.2.4**
- VM Domain Controller: **192.168.2.11**
- VM Windows XP Client: **192.168.2.5**

1. Το VM Host έχει μία στατική IP, σαν Netmask έχει οριστεί το 255.255.255.0, διότι το ίδιο το σύστημα δεν είναι υπεύθυνο για τον ορισμό της μάσκας του υποδικτύου. Ως Gateway έχει την IP του router, διότι χρειάζεται να βλέπει το internet. Οι DNS Servers είναι ορισμένοι με την IP του router, διότι εξυπηρετείται για τα Domain Name Services από τους Name Servers του παρόχου της σύνδεσης internet.



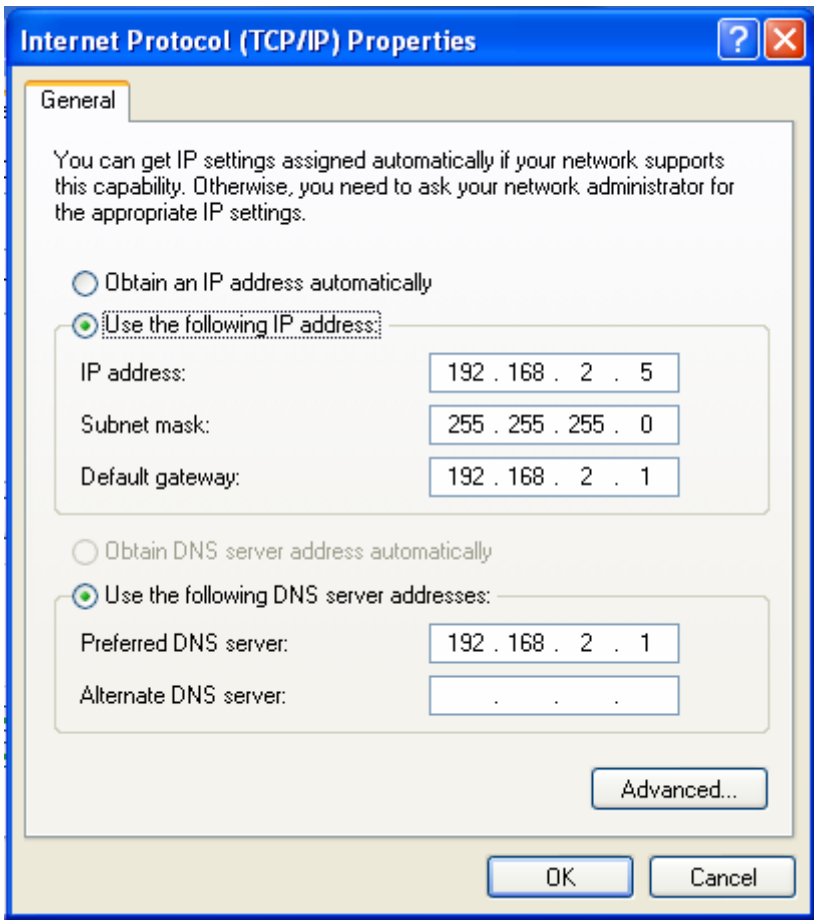
Εικόνα 4-94. Οι ρυθμίσεις δικτύου του VM Host.

2. Το VM Domain Controller έχει Subnet Mask 255.255.240.0, που σημαίνει πως επιτρέπει την πρόσβαση σε 15 συνολικά συστήματα στον τομέα (εκτός του εαυτού του). Το Default Gateway είναι ορισμένο με την IP του router, διότι θα πρέπει να βλεπει το internet, και επειδή δεν υπάρχει ορισμένος ιστότοπος στο Active Directory και το ίδιο το μηχάνημα επειδή είναι πιλοτικό δεν μπορεί να εξυπηρετήσει Domain Name Services (DNS), έχει οριστεί σαν προτιμώμενο DNS server η IP του router, όπου έχει προεπιλεγμένα τους Name Servers του παρόχου της σύνδεσης internet.



Εικόνα 4-95. Οι ρυθμίσεις δικτύου του VM Domain Controller.

3. Το VM Windows XP Client έχει απλά μία στατική IP, Subnet Mask έχει οριστεί το 255.255.255.0, διότι το ίδιο το σύστημα δεν είναι υπεύθυνο για τον ορισμό της μάσκας του υποδικτύου. Default Gateway έχει και αυτό το σύστημα την IP του router, διότι θα πρέπει και αυτό να βλέπει το internet. Οι DNS Servers είναι ορισμένοι με την IP του router, διότι εξυπηρετείται για τα Domain Name Services από τους Name Servers του παρόχου της σύνδεσης internet.



Εικόνα 4-96. Οι ρυθμίσεις δικτύου του VM Client.

Οι εικονικές μηχανές παίρνουνε δίκτυο από το host, συνεπώς είναι απευθείας συνδεδεμένα στο router. Στο δίκτυο του τομέα υπάρχει η δυνατότητα να καταχωρηθούν 15 υπολογιστές με IP διευθύνσεις από 192.168.2.2 μέχρι και 192.168.2.18, εκτός της διεύθυνσης 192.168.2.11 όπου είναι η στατική διεύθυνση του Domain Controller.

Κεφάλαιο 5

5. Επισκόπηση της Διαμόρφωσης και των Προτύπων Πολιτικής Ασφάλειας των Windows XP

Αυτή η ενότητα αποτελεί μία εισαγωγή στην έννοια των προτύπων ασφάλειας των Windows XP και περιγράφει πώς αναπτύχθηκαν τα πρότυπα του NIST. Εν συνεχεία παρέχεται καθοδήγηση για το πώς μπορούν οι οργανισμοί να δουν, να τροποποιήσουν και να εφαρμόσουν τα πρότυπα ασφάλειας, σε ξεχωριστά Windows XP συστήματα ή και σε όλα τα Windows XP συστήματα που βρίσκονται μέσα σε μία ή και περισσότερες Οργανωτικές Ομάδες (OU) ενός Active Directory. Τα Windows XP επίσης παρέχουν ένα μηχανισμό σύγκρισης των ρυθμίσεων που έχει ένα πρότυπο ασφάλειας με τις τρέχουσες ρυθμίσεις του συστήματος. Το αποτέλεσμα αυτής της σύγκρισης μπορεί να χρησιμοποιηθεί για τον εντοπισμό ενδεχόμενων ζητημάτων ασφάλειας, όπως επίσης και συγκεκριμένων χαρακτηριστικών οργανισμών που μπορεί να χρειάζονται να ενσωματωθούν στα πρότυπα.

5.1 Πρότυπα Ασφάλειας Windows XP

Στα Windows XP τα πρότυπα ασφάλειας είναι αρχεία σε μορφή κειμένου τα οποία περιέχουν τιμές σχετικά με ρυθμίσεις σε θέματα ασφάλειας, επομένως αντιπροσωπεύουν μία συγκεκριμένη διαμόρφωση ασφάλειας. Τα πρότυπα μπορούν να δημιουργηθούν και να αναβαθμιστούν χρησιμοποιώντας το snap-in Security Microsoft Management Console (MMC). Μπορούν να εφαρμοστούν σε κάποιο τοπικό υπολογιστή ή να εισαχθούν σε κάποιο Αντικείμενο Πολιτικής Ομάδων ή αλλιώς GPO (Group Policy Object) ή σε κάποια Κονσόλα Διαχείρισης Πολιτικής Ομάδων (Group Policy Management Console) που διευκολύνει στην άμεση επέκταση ρυθμίσεων ασφάλειας κατά μήκος ενός Windows XP περιβάλλοντος. Τα πρότυπα μπορούν επίσης να εφαρμοστούν μέσω διαφόρων εμπορικών διαχειριστικών εργαλείων τροποποίησης και διαμόρφωσης.[74] Το snap-in Security Configuration and Analysis του MMC μπορεί να χρησιμοποιηθεί για να εφαρμοστούν πρότυπα σε ένα σύστημα και να συγκριθούν οι τιμές μέσα σε ένα πρότυπο με τις ρυθμίσεις που υπάρχουν σε ένα σύστημα, για να αναλυθεί η στάση ασφάλειας του συστήματος.

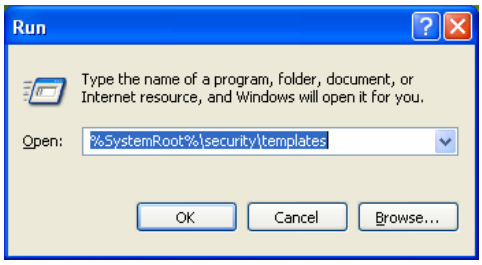
Τα Windows XP διατίθενται με διάφορα προκαθορισμένα πρότυπα ασφάλειας. Παρόλο που αυτά τα πρότυπα εμπεριέχονται στα Windows XP, δεν προτείνονται προς χρήση και εφαρμογή. Η Microsoft αποσκοπεί στην χρησιμοποίησή τους ως βάση για δημιουργία προτύπων συγκεκριμένων περιβαλλόντων (πχ οργανισμού). Σε αυτή την εργασία θα χρησιμοποιηθούν προτεινόμενα πρότυπα του NIST[75]. Αυτά τα πρότυπα αντιπροσωπεύουν τη συνιστώμενη βασική γραμμή ρυθμίσεων που υποστηρίζονται από τις CIS, DISA, NSA, NIST, Microsoft και άλλους ειδικούς σε θέματα ασφάλειας. Επίσης έχουν προσαρμοστεί για χρήση σε υπολογιστές υπηρεσίας Windows XP σε περιβάλλοντα SOHO, enterprise, specialized security-limited functionality και legacy. Προτείνεται προσοχή στην εφαρμογή τους και εάν είναι απαραίτητο θα πρέπει να διαμορφωθούν κατάλληλα έτσι ώστε να συμμορφώνονται με την τοπική πολιτική ασφάλειας και θα πρέπει να καταγράφονται όλες οι

[74] Παραδείγματα διαχειριστικών εργαλείων τροποποίησης και διαμόρφωσης είναι τα Microsoft Systems Management Server (SMS), BindView bv-Control, NetIQ Group Policy Administrator και Configuresoft Enterprise Configuration Manager (ECM).

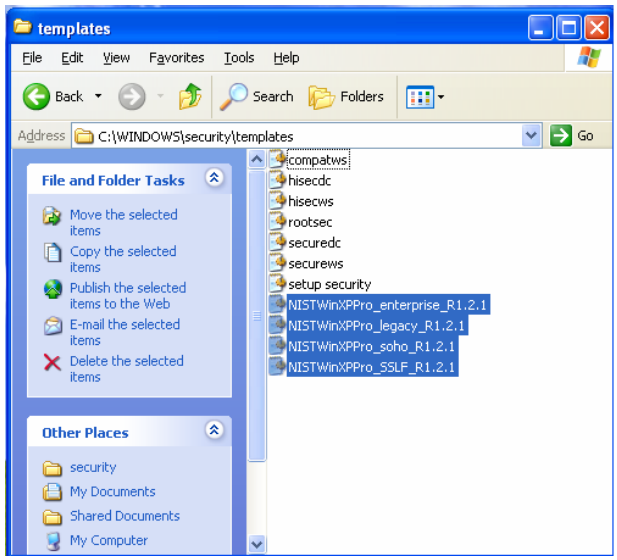
[75] Τα πρότυπα του NIST διατίθενται στην ακόλουθη διεύθυνση: http://csrc.nist.gov/itsec/SP800-68-template-R1.2.1.zip

τροποποιήσεις. Για να παρατηρήσουμε και να τροποποιήσουμε τα πρότυπα της NIST ακολουθούμε τα παρακάτω βήματα[76]:

1. Για να χρησιμοποιηθούν τα πρότυπα του NIST για θέματα ασφάλειας των Windows XP, τα αντιγράφουμε στο φάκελο **%SystemRoot%\Secutiry\Templates**[77] με χρήση του Windows Explorer.



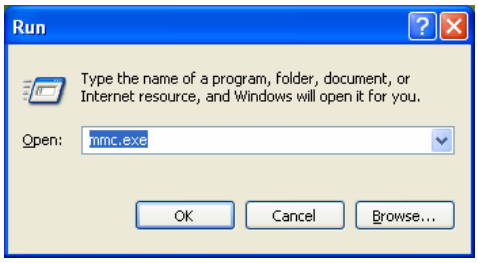
Εικόνα 5-1 Εντολή Run.



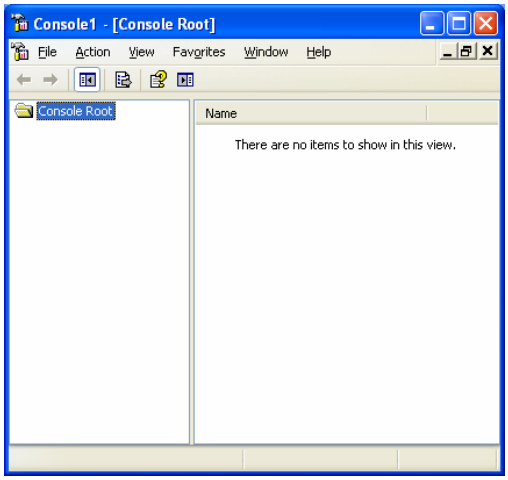
Εικόνα 5-2. Ο φάκελος Templates.

2. Εκκίνηση του MMC χρησιμοποιώντας τη **Run** εντολή του **Start** menu γράφοντας **mmc.exe**.

[76] Αυτή η μέθοδος λειτουργεί για όλες τις ρυθμίσεις προτύπων εκτός από αυτές των τιμών μητρώου (registry values), οι οποίες δεν είναι ορατές από το MMC. Οι ρυθμίσεις των τιμών μητρώου μπορούν να προσαρμοστούν με χειροκίνητη επεξεργασία του προτύπου μέσω κάποιου επεξεργαστή κειμένου.
[77] Το %SystemRoot% αναφέρεται στον κατάλογο Windows που βρίσκεται στον οδηγό του συστήματος (πχ C:\).

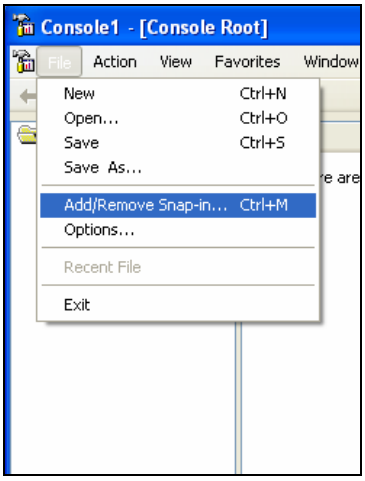


Εικόνα 5-3. Εντολή MMC.

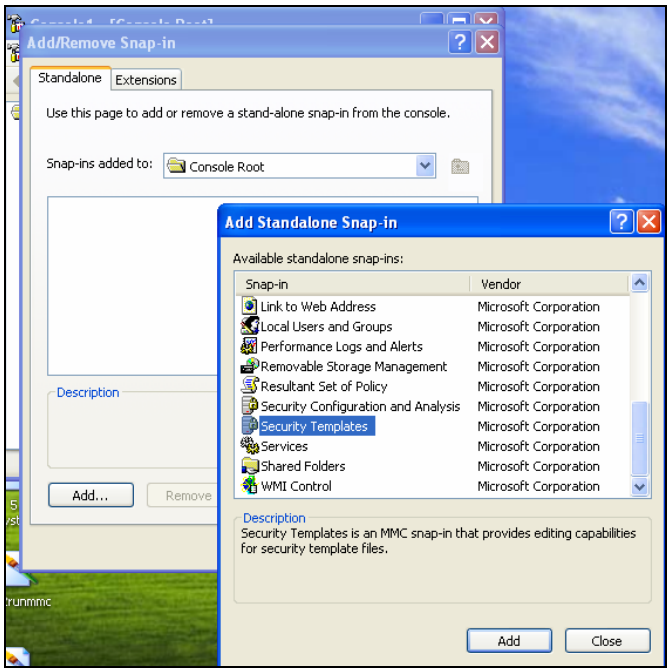


Εικόνα 5-4. Κονσόλα MMC.

3. Πατάμε **File** και έπειτα **Add/Remove Snap-in**. Πατάμε **Add**, επιλέγουμε το **Security Templates** snap-in και πατάμε **Add**. Πατάμε **Close** και **OK**. Μετά την ολοκλήρωση σώζουμε την κονσόλα στο φάκελο **Administrative Tools** για μελλοντική χρήση.

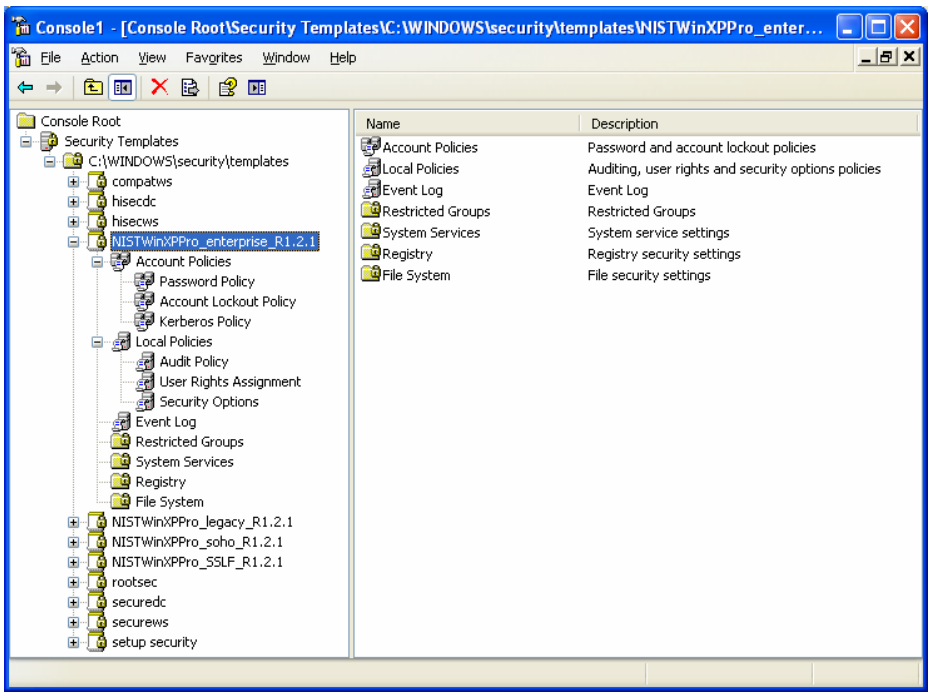


Εικόνα 5-5. Add/Remove Snap-in.

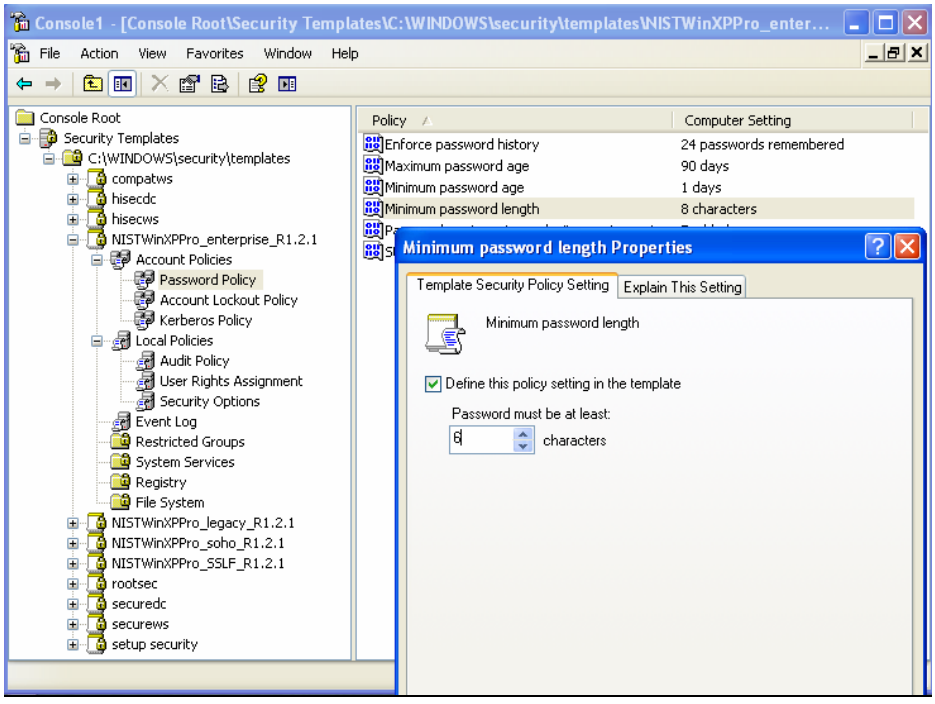


Εικόνα 5-6. Security Templates Snap-in.

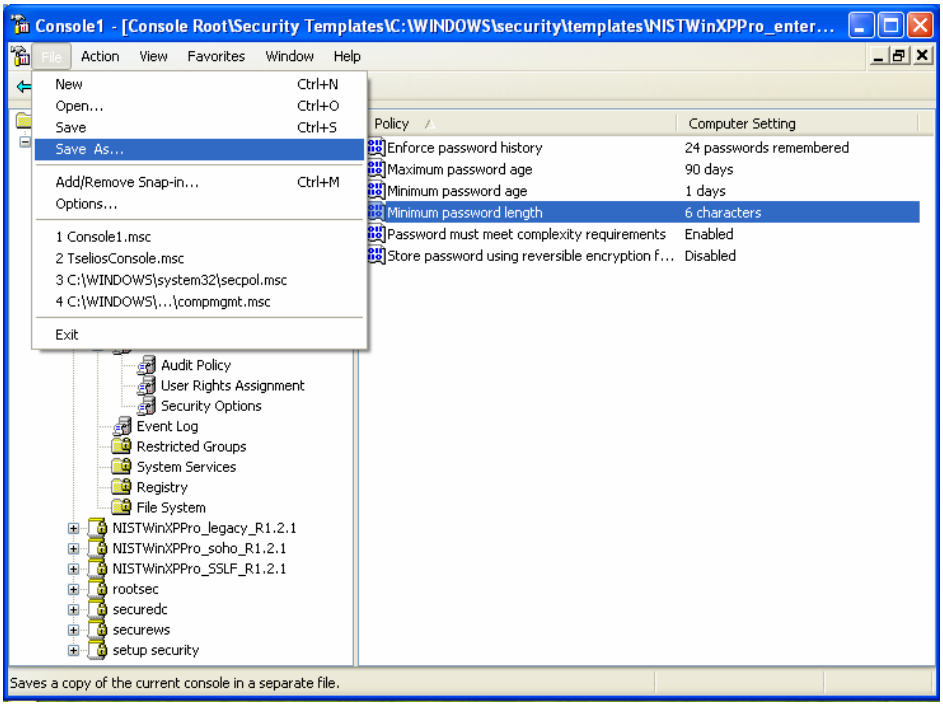
4. Χρησιμοποιούμε το Security Templates snap-in για να επιλέξουμε το πρότυπο που θα εφαρμοστεί στον υπολογιστή υπηρεσίας. Από τις επιλογές που προσφέρονται στις ρυθμίσεις του Security Templates, διαλέγουμε και προσαρμόζουμε αυτές που είναι καταλληλότερες για το σύστημα. Μετά το πέρας των αλλαγών κάνουμε δεξί κλικ στο πρότυπο, επιλέγουμε **Save As** και θέτουμε ένα όνομα. Το αρχείο που μόλις σώσαμε μπορεί να χρησιμοποιηθεί στον τοπικό υπολογιστή ή και στο περιβάλλον κάποιου άλλου υπολογιστή.



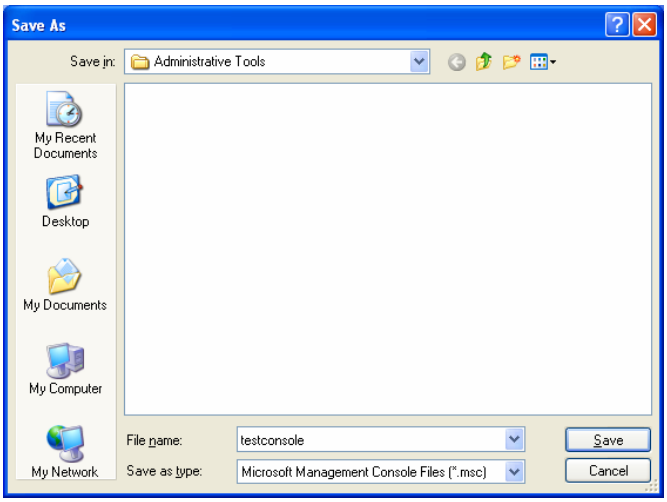
Εικόνα 5-7. Επιλέγουμε το πρότυπο enterprise.



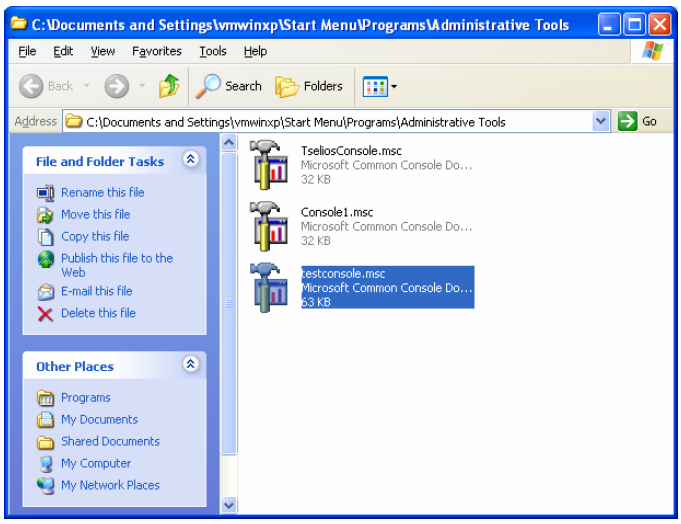
Εικόνα 5-8. Αντικαθιστούμε τον ελάχιστο αριθμό χαρακτήρων του password με την τιμή 6.



Εικόνα 5-9. Έχουμε κάνει τις επιθυμητές αλλαγές και σώζουμε την κονσόλα.



Εικόνα 5-10. Ορίζουμε το όνομα της κονσόλας.



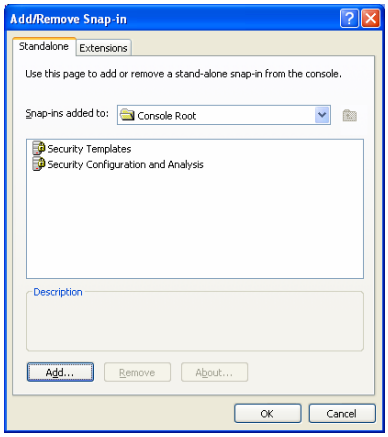
Εικόνα 5-11. Ο Administrative Tools φάκελος που αποθηκεύσαμε την κονσόλα μας.

5.2 Ανάλυση και Διαμόρφωση

Όπως προαναφέρθηκε, το Security Configuration and Analysis snap-in μπορεί να χρησιμοποιηθεί για τη σύγκριση των τρεχόντων ρυθμίσεων ασφάλειας ενός τοπικού υπολογιστή υπηρεσίας με αυτές που έχει το πρότυπο, πριν αυτό να εφαρμοστεί. Αυτό δίνει τη δυνατότητα στους διαχειριστές του συστήματος να εξετάσουν και να πραγματοποιήσουν τις κατάλληλες ρυθμίσεις στις αλλαγές που θα κάνει το πρότυπο ασφάλειας στις ρυθμίσεις του υπολογιστή. Για να χρησιμοποιήσουμε το Security Configuration and Analysis snap-in για να συγκρίνουμε και να εφαρμόσουμε τις ρυθμίσεις ασφάλειας σε τοπικό Windows XP σύστημα ακολουθούμε τα παρακάτω βήματα:

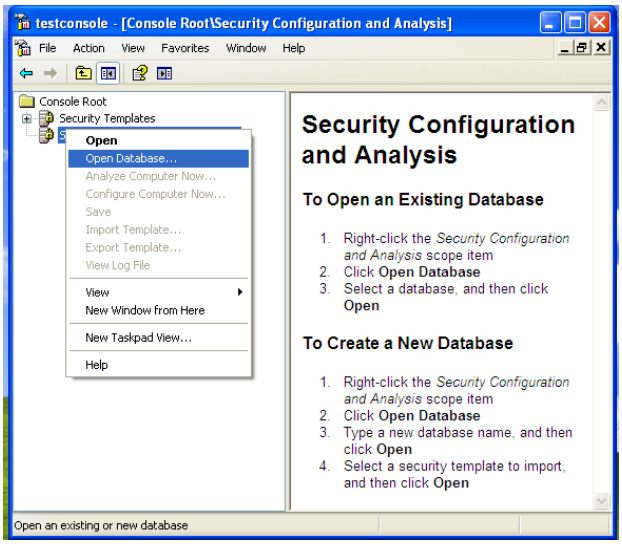
1. Εκκίνηση του MMC χρησιμοποιώντας τη **Run** εντολή του **Start** menu γράφοντας **mmc.exe**.

2. Πατάμε **File** και έπειτα **Add/Remove Snap-in**. Πατάμε **Add**, επιλέγουμε το **Security Configuration and Analysis** snap-in και πατάμε **Add**.



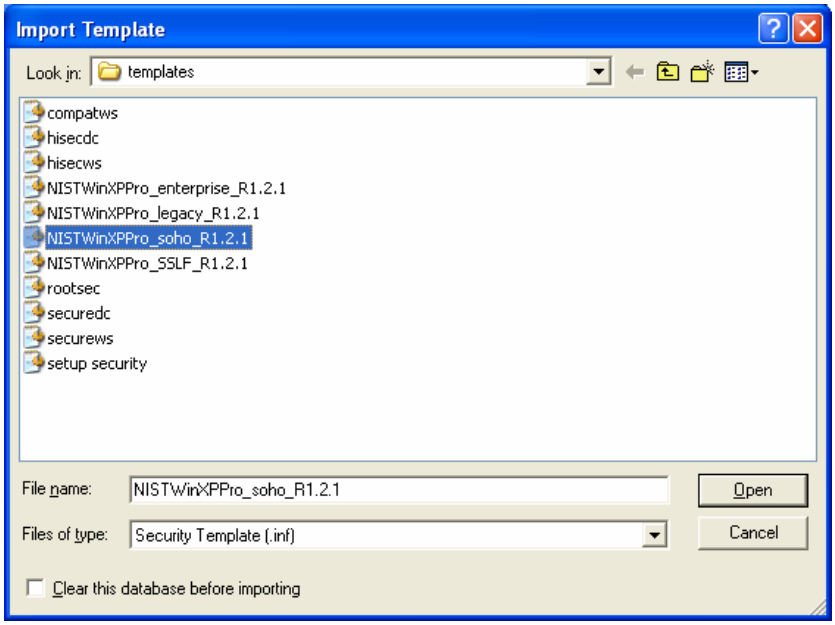
Εικόνα 5-12 Security Configuration and Analysis Snap-in.

3. Ανοίγουμε μια καινούργια βάση δεδομένων κάνοντας δεξί κλικ στο **Security Configuration and Analysis** και επιλέγουμε **Open Database**. Ονομάζουμε τη βάση και πατάμε **Open**.



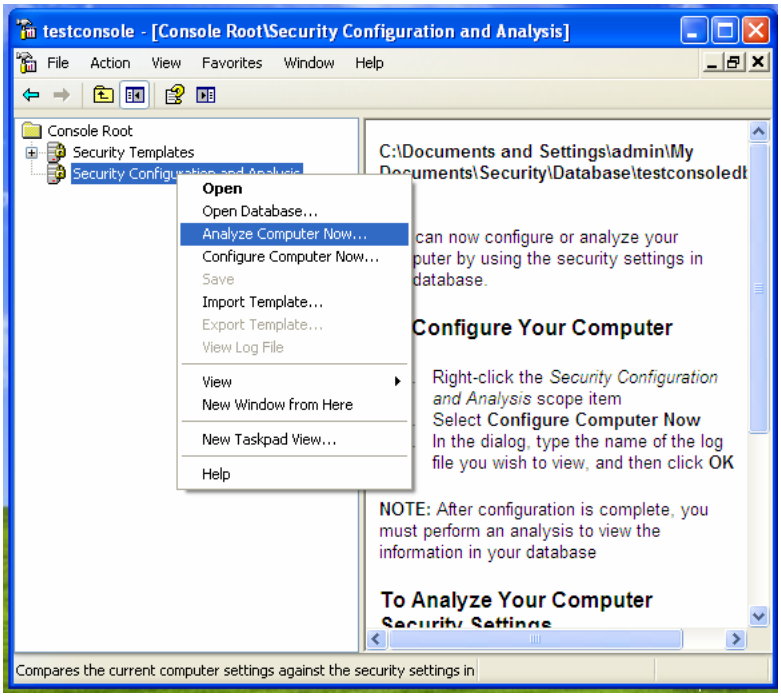
Εικόνα 5-13. Open Database.

4. Επιλέγουμε το πρότυπο που θα εφαρμοστεί στον υπολογιστή υπηρεσίας (στη δική μας περίπτωση θέσαμε το SOHO template). Πατάμε **Open** για να φορτωθούν οι ρυθμίσεις από το πρότυπο.

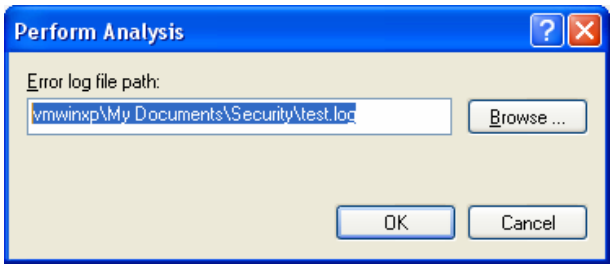


Εικόνα 5-14. Import Teplate.

5. Κάνουμε δεξί κλικ στο **Security Configuration and Analysis** snap-in και επιλέγουμε **Analyze Computer Now**. Δίνουμε όνομα και καθορίζουμε το φάκελο αποθήκευσης του αρχείου log που θα δημιουργηθεί από αυτή τη διεργασία και πατάμε **OK.**[78] Το σύστημα εδώ θα συγκρίνει τις τρέχουσες ρυθμίσεις που είναι ενεργοποιημένες στον υπολογιστή με αυτές του προτύπου.

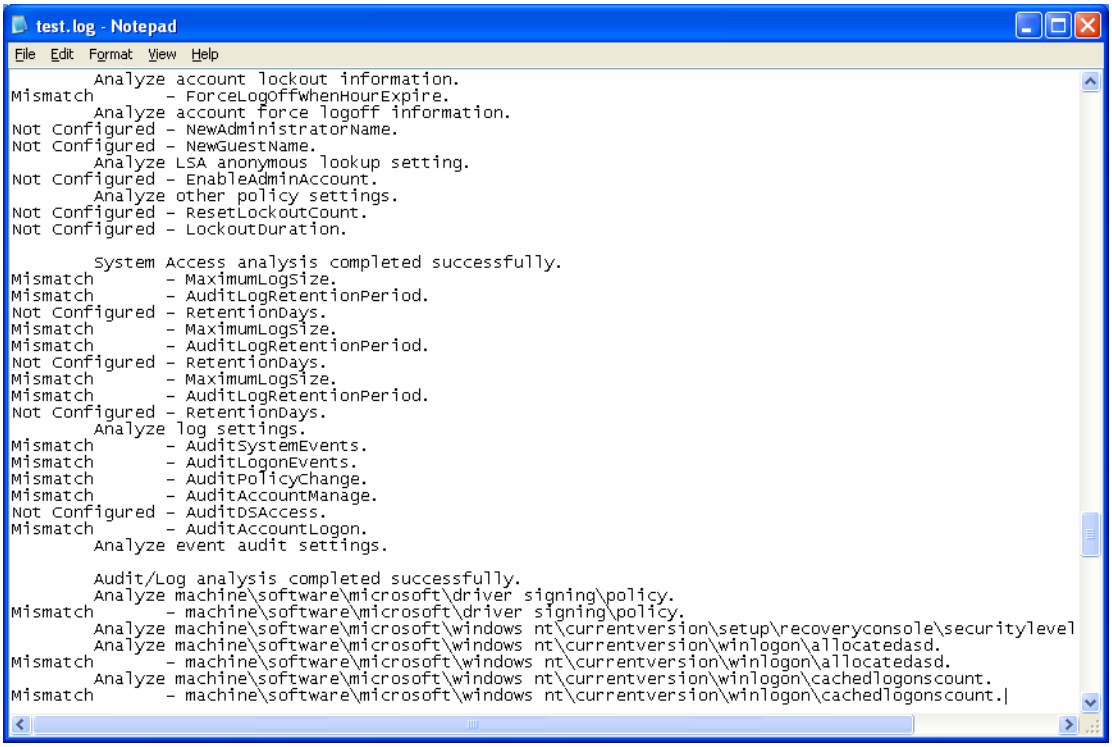


Εικόνα 5-15. Analyze Computer Now.



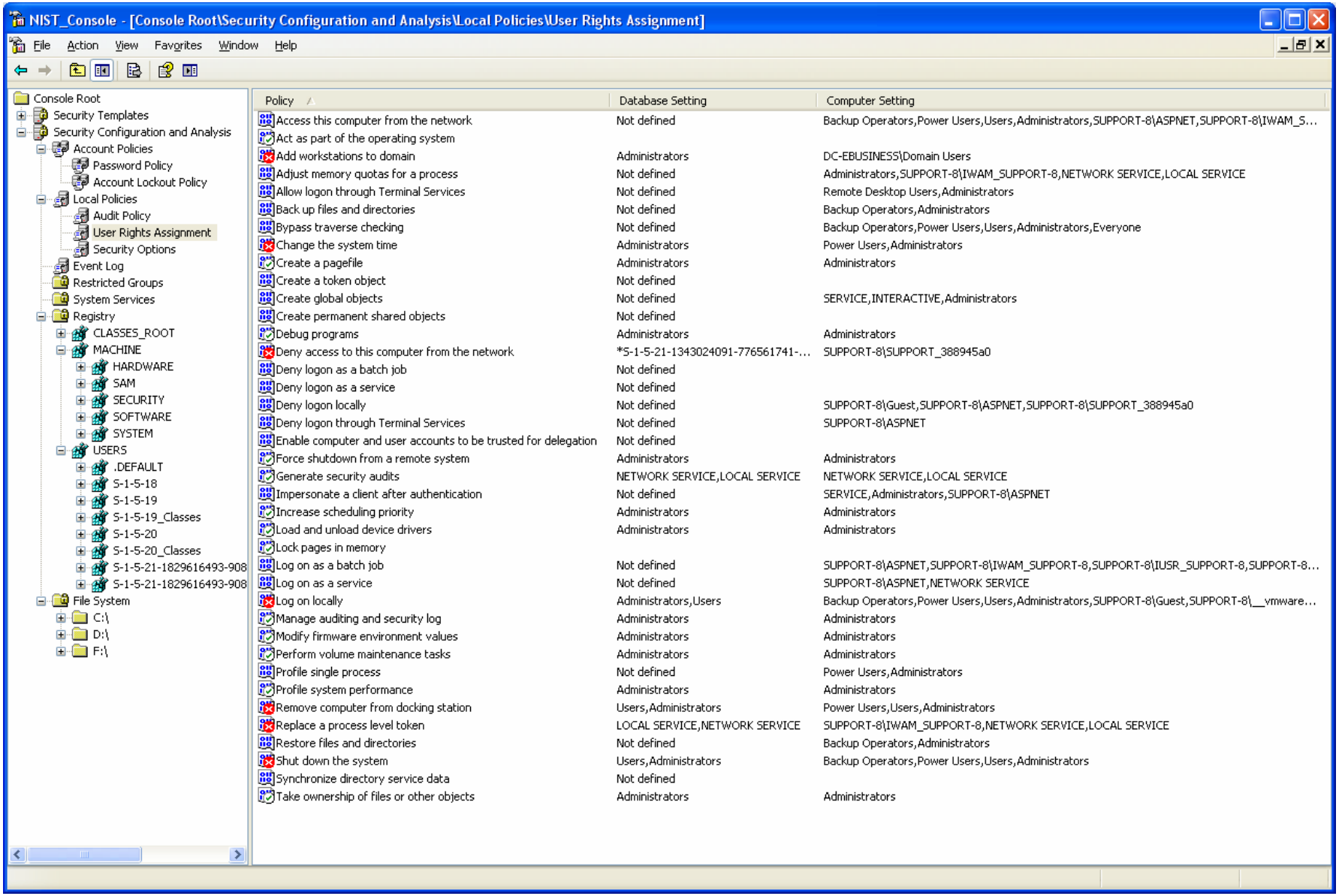
Εικόνα 5-16. Σώζουμε το αρχείο log.

[78] Εξ' ορισμού το αρχείο log ονομάζεται test.log. Στο αρχείο log καταγράφεται κάθε ασυμφωνία και μπορεί να περιέχει εκατοντάδες ή και χιλιάδες καταχωρίσεις για μία και μόνο σάρωση. Το ίδιο log αρχείο χρησιμοποιείται όταν ένα πρότυπο εφαρμόζεται στο σύστημα.



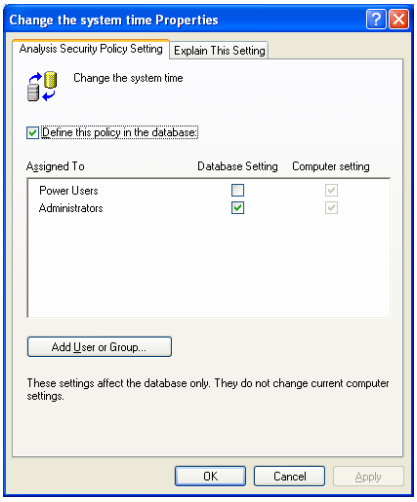
Εικόνα 5-17. Μέρος του log file το οποίο είναι σε μορφή κειμένου και το χρησιμοποιεί η κονσόλα για να εξάγει την αναφορά σύγκρισης ρυθμίσεων.

6. Όταν ολοκληρωθεί ο έλεγχος, παρατηρούμε τις υποκατηγορίες κάτω από το Security Configuration and Analysis snap-in. Παρατηρούμε τις διαφορές ανάμεσα στις ρυθμίσεις των προτύπων και σε αυτές του υπολογιστή. Για παράδειγμα, τα αντικείμενα που έχουν κόκκινο **X** διαφέρουν από το πρότυπο και αυτά που έχουν πράσινο **V** ταυτίζονται με το πρότυπο. Άλλα αντικείμενα μπορεί να μην έχουν αναλυθεί διότι δεν είχε οριστεί κάποια ρύθμιση για αυτά μέσα στο πρότυπο, ή επειδή εξαρτώνται από μια άλλη τιμή η οποία δεν έχει οριστεί. Πέραν του εικονιδίου **V** ή **X** το κάθε αντικείμενο δίνει επίσης μία λεκτική περιγραφή, όπως **Not Analyzed** ή **Not Defined**, ανάλογα με τις περιπτώσεις που προαναφέρθηκαν.



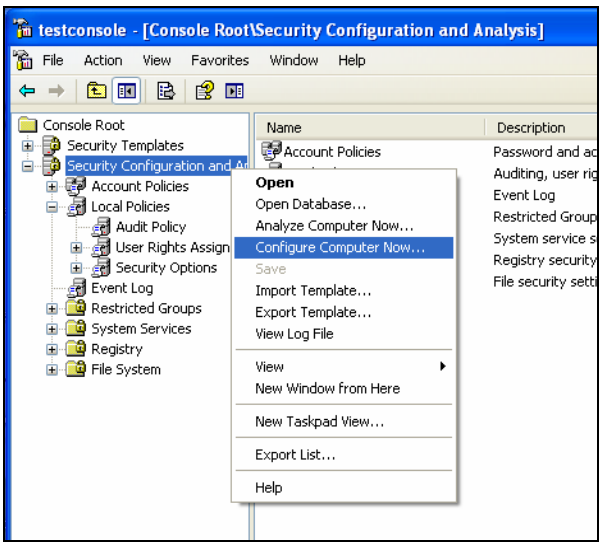
Εικόνα 5-18. Αναφορά της ανάλυσης.

7. Εάν η αναφορά των ρυθμίσεων επισημαίνει ότι οι ρυθμίσεις του συγκεκριμένου προτύπου δεν θα πρέπει να εφαρμοστούν στο σύστημα, μπορούν να ρυθμιστούν κάνοντας τροποποιήσεις στη βάση δεδομένων των ρυθμίσεων που παρατηρούμε στο συγκεκριμένο παράθυρο. Για να καταφέρουμε κάτι τέτοιο κάνουμε διπλό κλικ στη ρύθμιση που θέλει τροποποιήσεις, τις πραγματοποιούμε και πατάμε **OK** για να επιστρέψουμε στην κεντρική οθόνη με τη λίστα των ρυθμίσεων. Επαναλαμβάνουμε τη διαδικασία μέχρι να πραγματοποιηθούν όλες οι επιθυμητές μετατροπές. Εδώ είδαμε, για παράδειγμα, στα δικαιώματα χρηστών, τη ρύθμιση αλλαγής ώρας του συστήματος ότι είναι δυνατή μόνο από τον διαχειριστή. Δίνεται επιπλέον η επιλογή να προσθέσουμε και άλλους χρήστες ή και ομάδες χρηστών που θα έχουν δικαίωμα στην αλλαγή της ώρας του συστήματος (πχ Power Users Group).

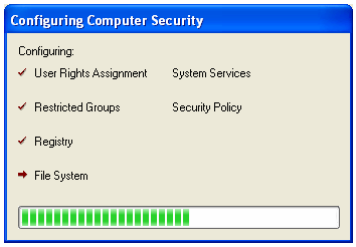


Εικόνα 5-19. Ιδιότητα "Change the system time".

8. Για να εφαρμόσουμε τις ρυθμίσεις της βάσης δεδομένων στο σύστημα κάνουμε δεξί κλικ στο **Security Configuration and Analysis** snap-in και επιλέγουμε **Configure Computer Now**. Καθορίζουμε το όνομα και την τοποθεσία αποθήκευσης του αρχείου log που θα δημιουργηθεί από την διεργασία και πατάμε **OK**. Οι ρυθμίσεις έχουν εφαρμοστεί επιτυχώς στο σύστημα.

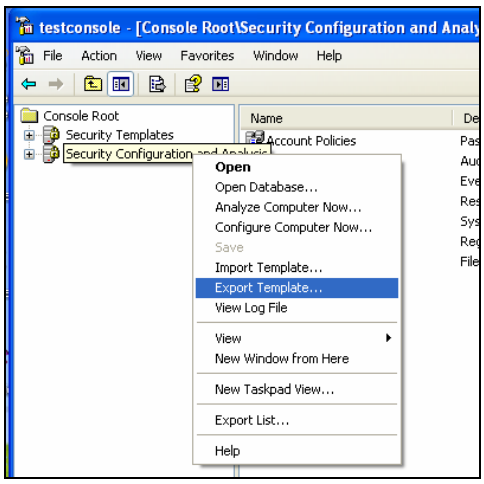


Εικόνα 5-20. Configure Computer Now.

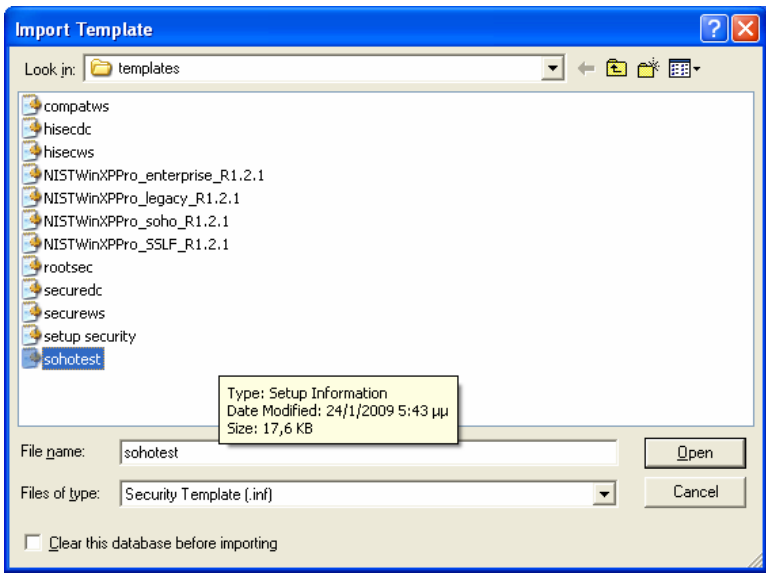


Εικόνα 5-21. Configuring.

9. Όταν η διαμόρφωση ολοκληρωθεί, ο τρόπος διαχείρισης (policy) που χρησιμοποιήθηκε για να εφαρμόσει τη συγκεκριμένη διαμόρφωση μπορεί να εξαχθεί για μελλοντική χρήση σε αυτό τον υπολογιστή ή και σε άλλους. Για να πραγματοποιήσουμε την εξαγωγή του policy κάνουμε δεξί κλικ στο **Security Configuration and Analysis** snap-in και επιλέγουμε **Export Template.**[79] Ονομάζουμε και σώζουμε το πρότυπο για μελλοντική χρήση. Το πρότυπο που εξάγαμε μπορεί επίσης να εισαχθεί για να επαναφέρει τις ρυθμίσεις σε περίπτωση που μελλοντικά κάποιες αλλαγές που θα πραγματοποιηθούν επιφέρουν προβλήματα.



Εικόνα 5-22. Εξαγωγή προτύπου.

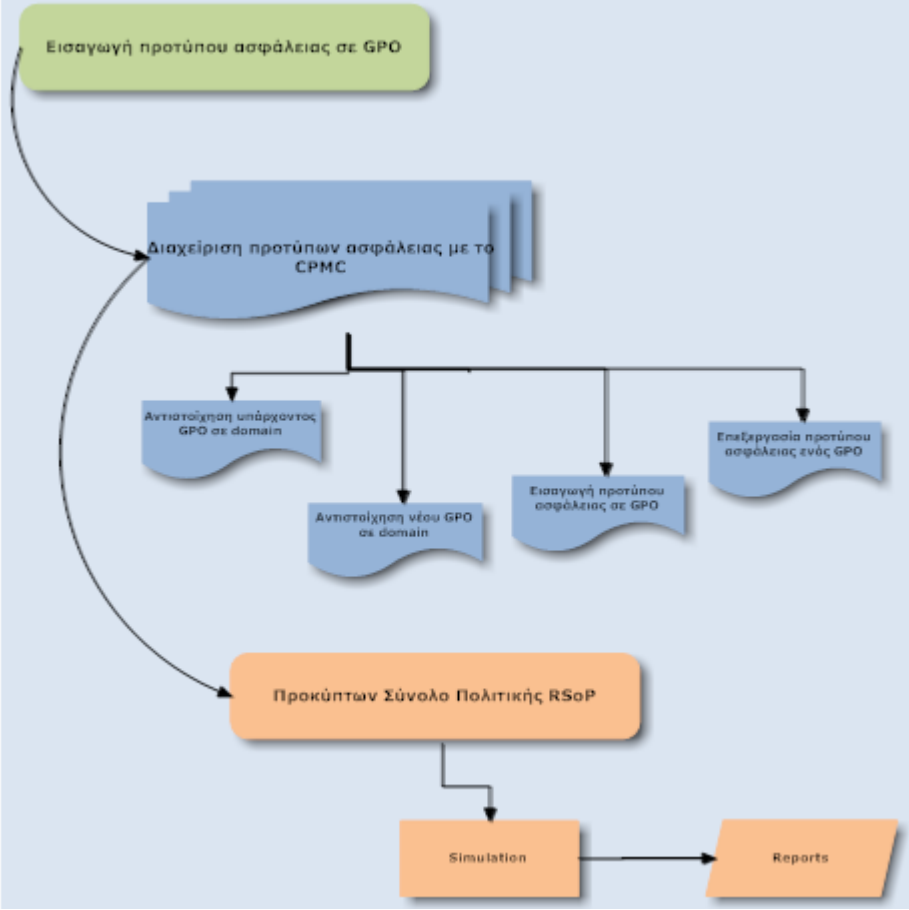


Εικόνα 5-23. Ο φάκελος που αποθηκεύτηκε το πρότυπο.

[79] Εάν η επιλογή **Export Template** δεν είναι διαθέσιμη, εκτελούμε ξανά το βήμα **Analyze Computer Now**. Η επιλογή **Export Template** θα πρέπει πλέον να είναι διαθέσιμη.

5.3 Διανομή Πολιτικής Ομάδων

Σε ένα περιβάλλον τομέα (domain) με Windows XP, μπορούν να χρησιμοποιηθούν GPOs (Group Policy Objects) για να διανεμηθούν ρυθμίσεις ασφάλειας σε όλους τους υπολογιστές σε Οργανωτικές Ομάδες ή αλλιώς OU (Organizational Unit) του Active Directory. Η προτεινόμενη μέθοδος είναι να διαχωρίσουμε τους υπολογιστές ανάλογα με το ρόλο τους μέσα σε OUs. Για παράδειγμα όλοι οι υπολογιστές εργασίας ενός τομέα που είναι όμοια ρυθμισμένοι σε ένα περιβάλλον θα πρέπει να είναι μέσα σε ένα OU.

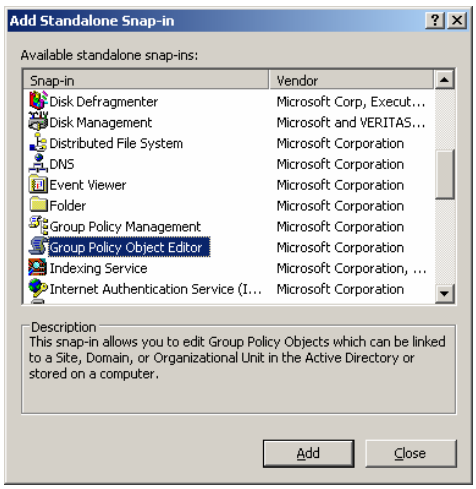


Εικόνα 5-24 Συνοπτικό διάγραμμα διεργασιών της ενότητας 5.3.

Για να εισάγουμε ένα πρότυπο ασφάλειας σε κάποιο GPO ακολουθούμε τα παρακάτω βήματα:

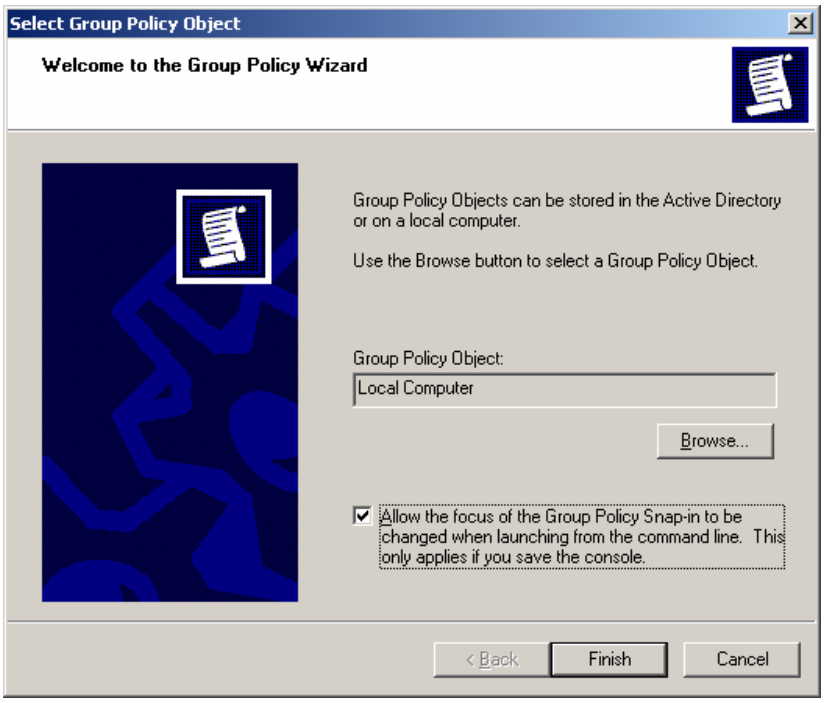
1. Εκκίνηση του MMC χρησιμοποιώντας τη **Run** εντολή του **Start** menu γράφοντας **mmc.exe**.

2. Πατάμε **File** και έπειτα **Add/Remove Snap-in**. Πατάμε **Add**, επιλέγουμε το **Group Policy Object Editor** snap-in και πατάμε **Add**. Επιλέγουμε το κατάλληλο GPO και πατάμε **OK** και τέλος πατάμε **Finish**.



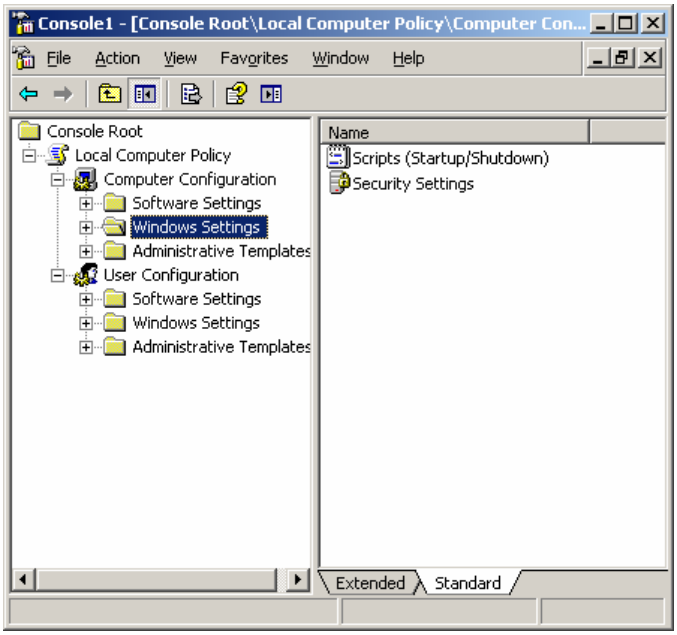
Εικόνα 5-25. Group Policy Object Editor Snap-in.

3. Πατάμε **Next** και **Finish**.



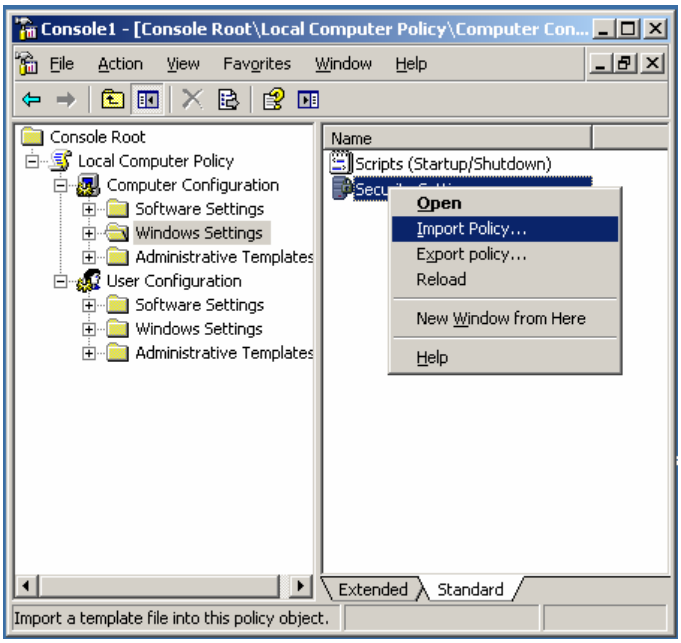
Εικόνα 5-26. Επιλογή GPO.

4. Επεκτείνουμε το Group Policy Object, μετά το **Computer Configuration** και πατάμε το **Windows Settings**.



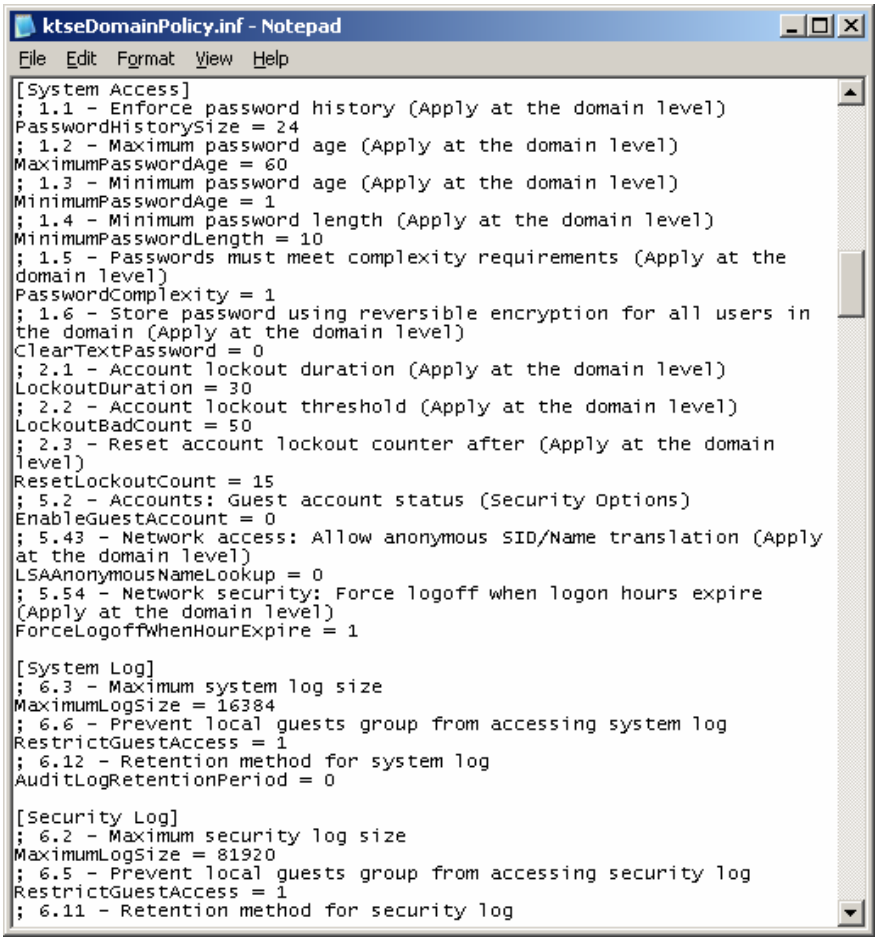
Εικόνα 5-27. Window Settings.

5. Κάνουμε δεξί κλικ στο **Security Settings** και επιλέγουμε **Import Policy**.

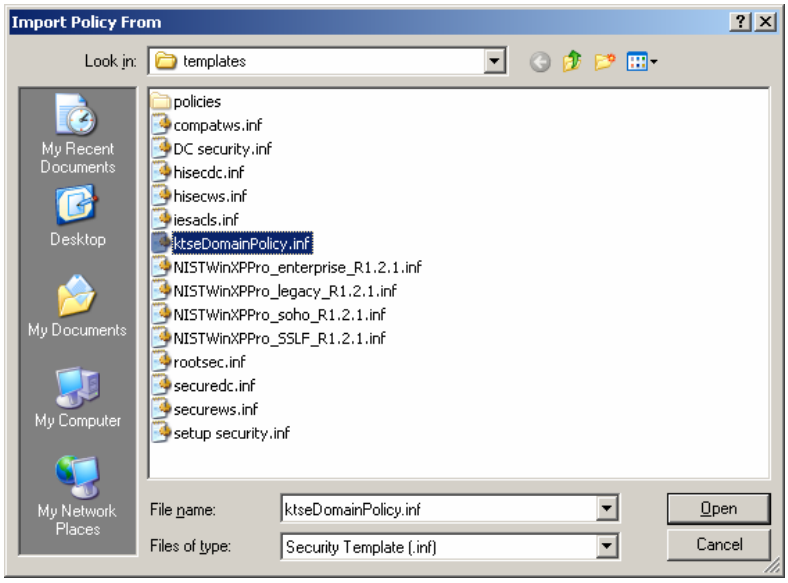


Εικόνα 5-28. Εισαγωγή Policy.

6. Επιλέγουμε το επιθυμητό πρότυπο (εδώ επιλέξαμε ένα δικό μας custom template) και πατάμε **Open**.



Εικόνα 5-29. Κομμάτι ενός custom template.

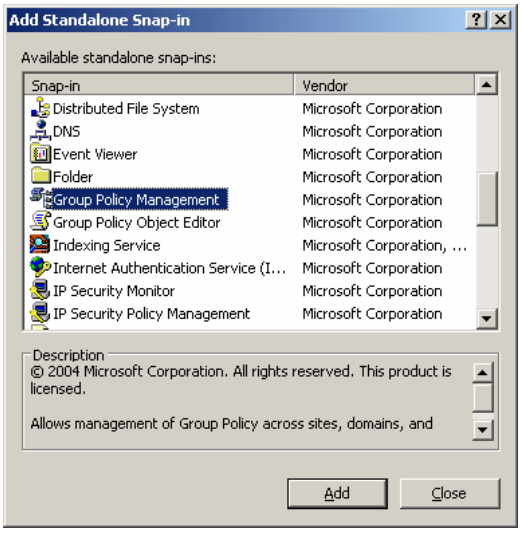


Εικόνα 5-30. Import του custom policy template

Οι ρυθμίσεις ασφάλειας του προτύπου μπορούν από αυτό το σημείο να τοποθετηθούν σε όλους τους υπολογιστές ενός OU. Η πολιτική ομάδων μπορεί να εφαρμοστεί μόνο χρησιμοποιώντας ένα σύστημα Windows 2000 Server ή Windows 2003 Server (στην περίπτωσή μας χρησιμοποιήθηκε Windows 2003 Server με Active Directory) σε ένα Windows XP περιβάλλον τομέα (Active Directory).[80] Η Microsoft προσφέρει επιπλέον το Group Management Console (GPMC) για τη διαχείριση πολιτικής ομάδων για πολλούς τομείς (domains).[81] Το GPMC συνδυάζει τη λειτουργικότητα διάφορων υπαρχόντων εργαλείων σχετικά με τις πολιτικές ομάδων σε μία και μοναδική διεπαφή.[82] Το GPMC μπορεί να χρησιμοποιηθεί για να εισάγουμε, να επεξεργαστούμε και να εφαρμόσουμε πρότυπα ασφάλειας σε συστήματα Windows μέσα σε μία επιχείρηση, το οποίο είναι ιδανικό για ένα διαχειριζόμενο περιβάλλον. Εφόσον το GPMC έχει εγκατασταθεί, μπορούμε να το τρέξουμε απλά εκτελώντας το **gpmc.msc**. Για να καλέσουμε το GPMC snap-in μέσα σε μία κονσόλα MMC ακολουθούμε τα παρακάτω βήματα:

1. Εκκίνηση του MMC χρησιμοποιώντας τη **Run** εντολή του **Start** menu γράφοντας **mmc.exe**.

2. Πατάμε **File** και έπειτα **Add/Remove Snap-in**. Πατάμε **Add**, επιλέγουμε το **Group Policy Management** snap-in και πατάμε **Add**. Πατάμε **Close** και μετά **OK**.

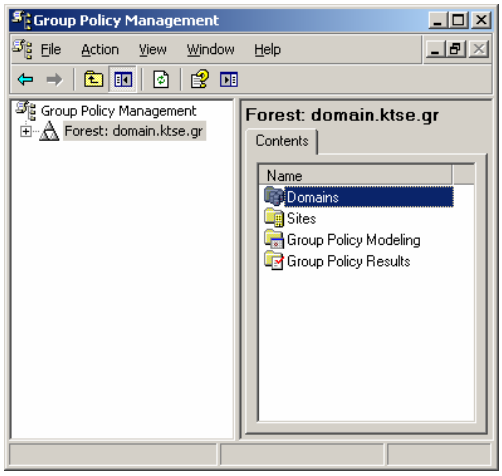


Εικόνα 5-31. Group Policy Management Snap-in.

[80] Περισσότερες πληροφορίες για το Active Directory δίνονται σε επόμενο κεφάλαιο.
[81] Περισσότερες πληροφορίες για το GPMC είναι διαθέσιμες εδώ: http://www.microsoft.com/windowsserver2003/gpmc/default.mspx. Το GPMC μπορεί επίσης να καταφορτωθεί από την ίδια διεύθυνση.
[82] Για περισσότερες πληροφορίες αναφορικά με τη λειτουργικότητα που παρέχεται από το GPMC διάβασε το Microsoft white paper του Jim Lundy, με τίτλο *Administering Group Policy with Group Policy Management Console*, που διατίθεται εδώ: http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx.

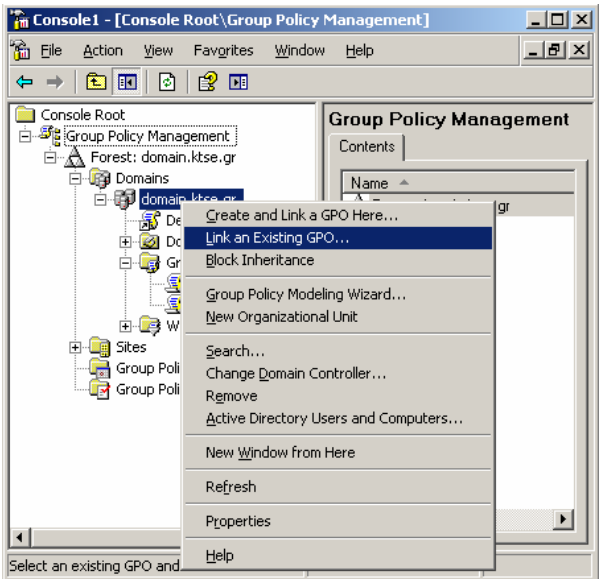
Μέσα στο GPMC ένα GPO θα πρέπει να αντιστοιχηθεί σε κάποιο τομέα, ιστοσελίδα ή σε κάποιο OU για να χρησιμοποιηθεί. Για να αντιστοιχήσουμε ένα υπάρχον GPO σε ένα OU ακολουθούμε τα παρακάτω βήματα.

1. Ανοίγουμε το GPMC.



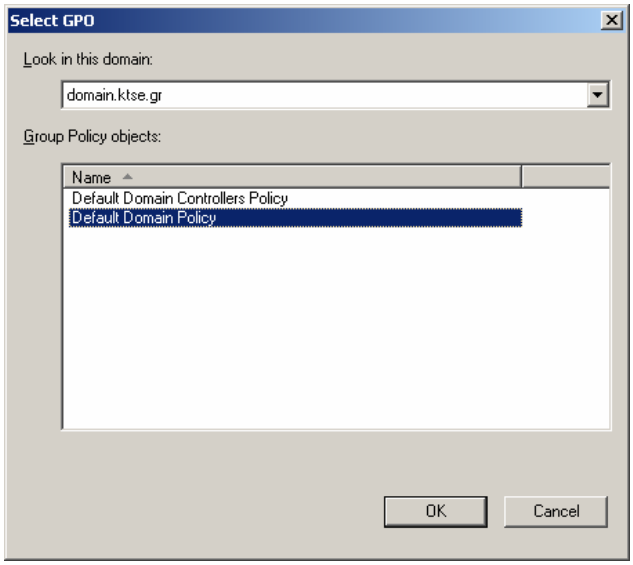
Εικόνα 5-32. GPMC.

2. Κάνουμε δεξί κλικ στο κατάλληλο OU και επιλέγουμε το **Link an Existing GPO**.



Εικόνα 5-33. Link existing GPO.

3. Θα εμφανιστεί μία λίστα από GPOs. Επιλέγουμε αυτό που θα πρέπει να αντιστοιχηθεί στο OU και έτσι η αντιστοίχηση πραγματοποιείται.

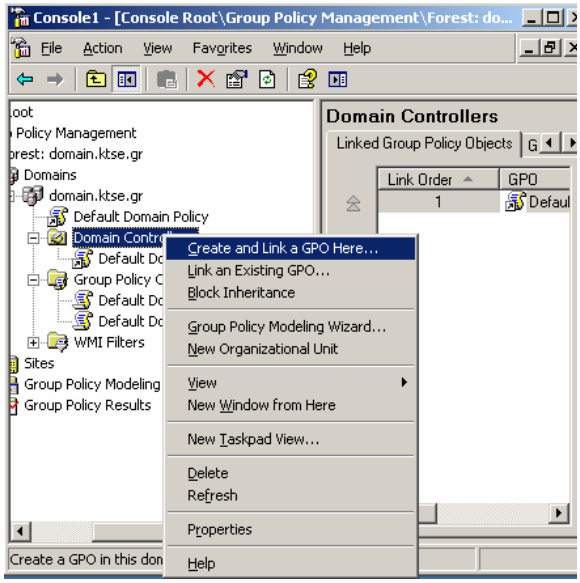


Εικόνα 5-34. Select GPO.

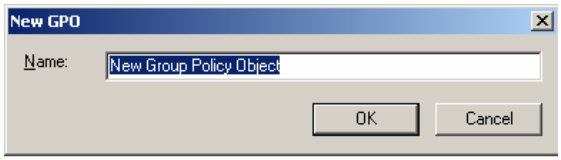
Εναλλακτικά μπορούμε να δημιουργήσουμε ένα νέο GPO το οποίο να είναι αυτομάτως αντιστοιχισμένο σε κάποιο τομέα, ιστοσελίδα ή σε κάποιο OU. Για να δημιουργήσουμε ένα νέο GPO για ένα OU ακολουθούμε τα παρακάτω βήματα:

1. Ανοίγουμε το GPMC.

2. Κάνουμε δεξί κλικ στο κατάλληλο OU και επιλέγουμε **Create and Link a GPO Here**. Αυτό ανοίγει το παράθυρο διαλόγου New GPO.

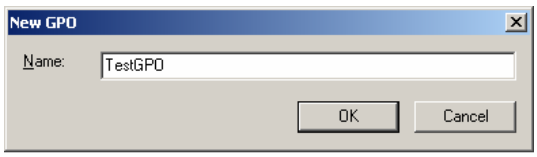


Εικόνα 5-35. Create and Link GPO.



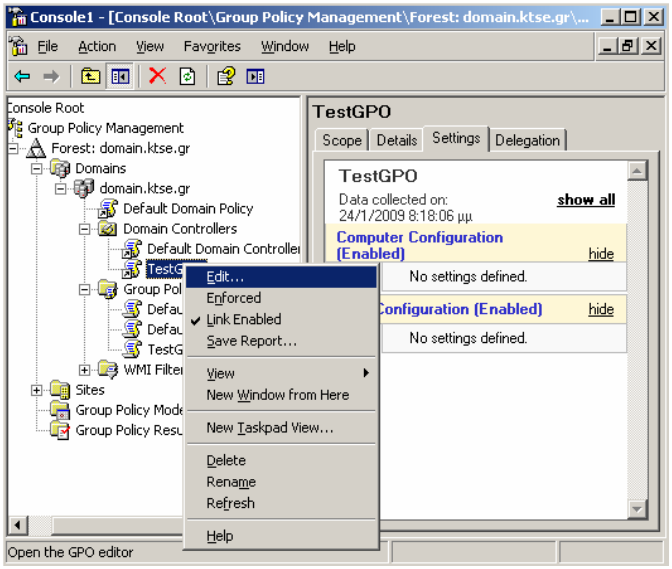
Εικόνα 5-36. New GPO.

3. Δίνουμε ένα όνομα στο GPO. Αυτό θα δημιουργήσει το GPO και θα το αντιστοιχίσει αυτόματα στο OU που επιλέξαμε.

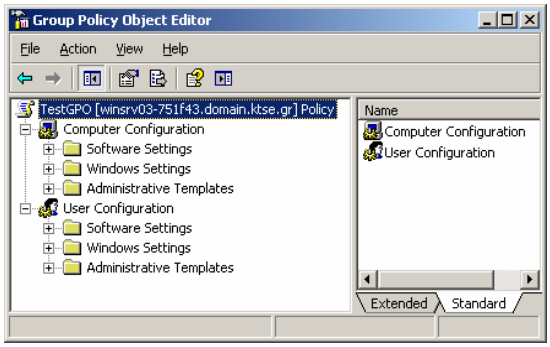


Εικόνα 5-37. Ονοματοδοσία GPO.

4. Κάνουμε δεξί κλικ στο νέο GPO και επιλέγουμε **Edit** για προσδιορίσουμε το GPO με το Group Policy Editor.



Εικόνα 5-38. Edit GPO.



Εικόνα 5-39. Custom GPO.

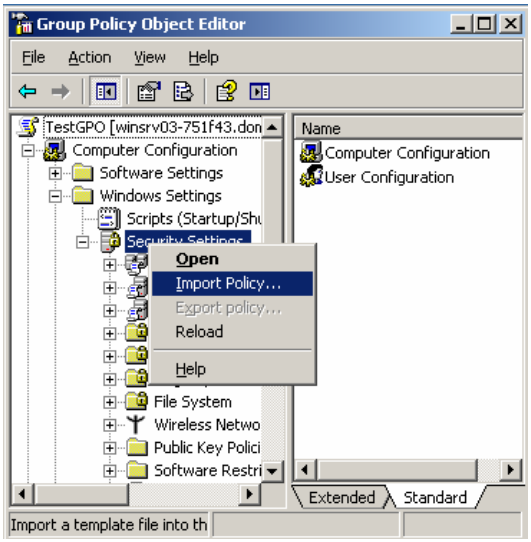
Το GPMC μπορεί να εισάγει πρότυπα ασφάλειας σε κάποιο GPO. Για να κάνουμε κάτι τέτοιο ακολουθούμε τα παρακάτω βήματα:

1. Ανοίγουμε το GPMC.

2. Κάνουμε δεξί κλικ στο κατάλληλο OU και επιλέγουμε **Edit**.

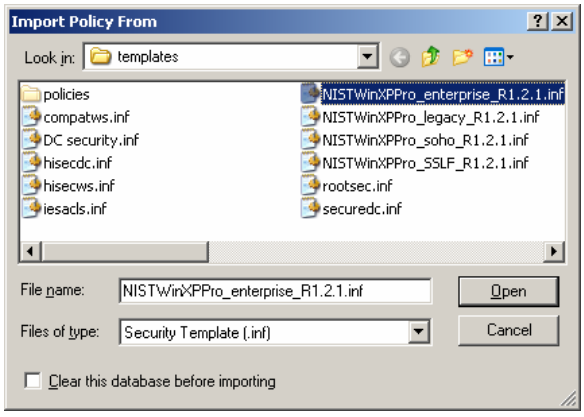
3. Επεκτείνουμε το **Computer Configuration** και πατάμε **Windows Settings**.

4. Κάνουμε δεξί κλικ στο **Security Settings** και επιλέγουμε **Import Policy**.



Εικόνα 5-40. Import Policy.

5. Επιλέγουμε το επιθυμητό πρότυπο (εδώ επιλέξαμε το Enterprise template) και πατάμε **Open.**



Εικόνα 5-41. Import Policy from.

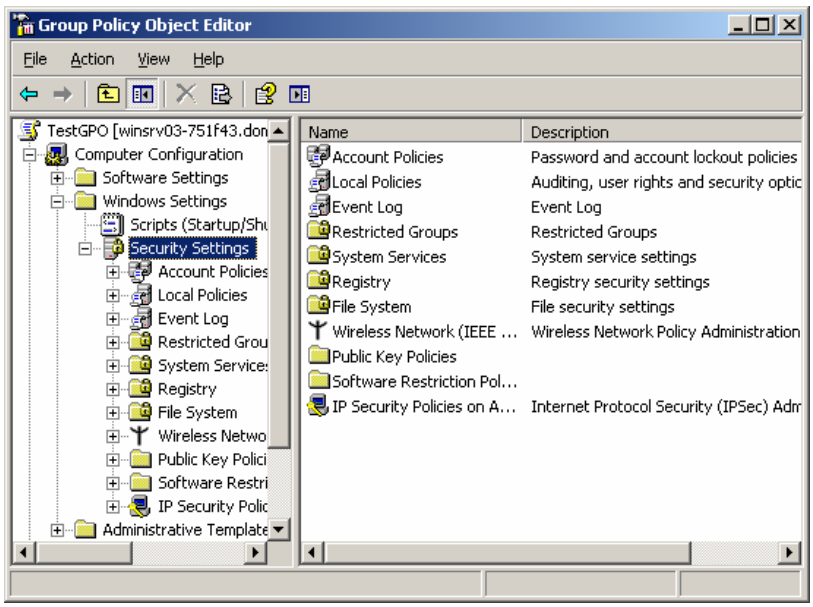
Το GPMC μπορεί επίσης να χρησιμοποιηθεί για να επεξεργαστεί τις ρυθμίσεις ασφάλειας ενός GPO. Για να κάνουμε κάτι τέτοιο ακολουθούμε τα παρακάτω βήματα:

1. Ανοίγουμε το GPMC.

2. Κάνουμε δεξί κλικ στο κατάλληλο GPO και επιλέγουμε **Edit.**

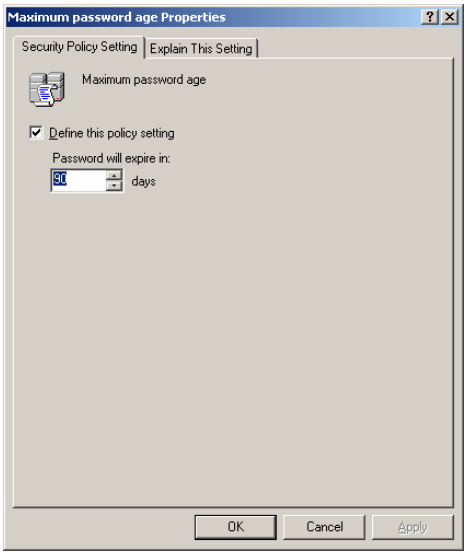
3. Επεκτείνουμε το **Computer Configuration** και πατάμε **Windows Settings**.

4. Πατάμε το **Security Settings** και έπειτα επιλέγουμε την κατάλληλη πολιτική (πχ Account Policies, Password Policy, Maximum Password Age).



Εικόνα 5-42. Security Settings.

5. Πραγματοποιούμε αλλαγές στις ρυθμίσεις ασφάλειας όπως χρειάζεται και πατάμε **OK** μόλις τελειώσουμε.

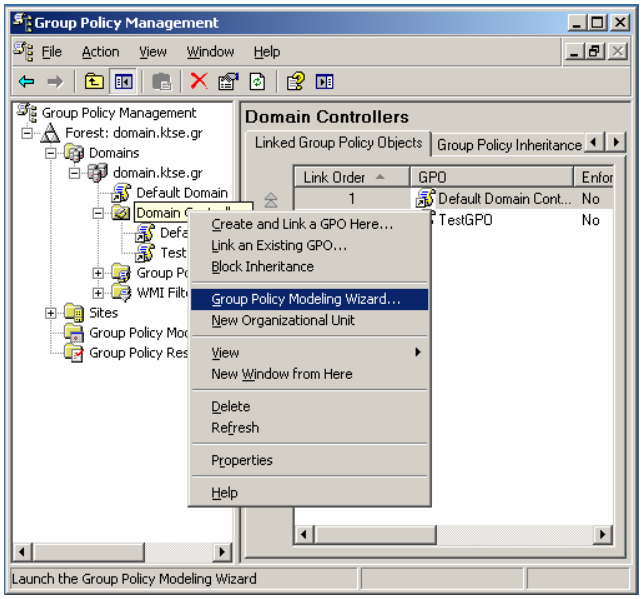


Εικόνα 5-43. Σε 90 ημέρες θα ζητηθεί από το χρήστη να αλλάξει τον κωδικό εξουσιοδότησής του για την εισαγωγή του στον τομέα.

Ένα άλλο χαρακτηριστικό του GPMC είναι το Group Policy Modeling Wizard, το οποίο παρέχει την λειτουργία Προκύπτων Συνόλου Πολιτικής (Resultant set of Policy [RSoP]). Αυτό σημαίνει ότι το εργαλείο wizard μπορεί να καθορίσει τις επιπτώσεις που θα προκύψουν από την εφαρμογή συνδυασμών διαφόρων GPOs (πχ ιστοσελίδες, τομείς και επίπεδα OU) σε ένα συγκεκριμένο υπολογιστή ή χρήστη. Για να χρησιμοποιήσουμε αυτό το χαρακτηριστικό σε ένα OU ακολουθούμε τα παρακάτω βήματα:

1. Ανοίγουμε το GPMC.

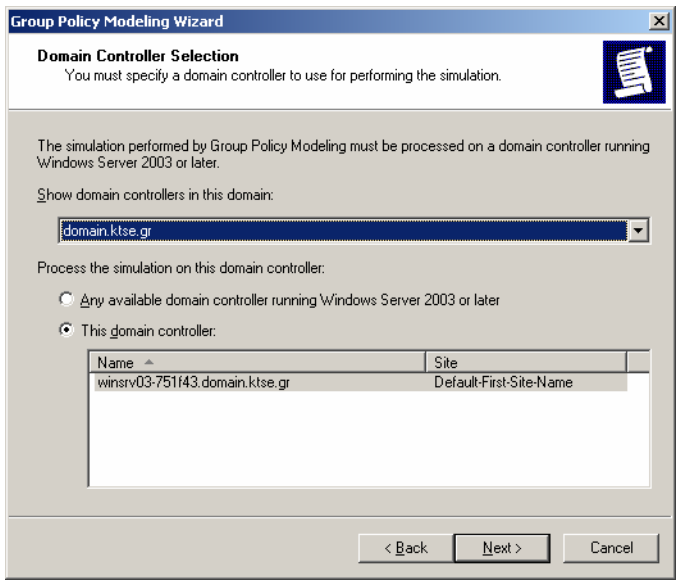
2. Κάνουμε δεξί κλικ στο κατάλληλο OU και επιλέγουμε **Group Policy Modeling Wizard.**



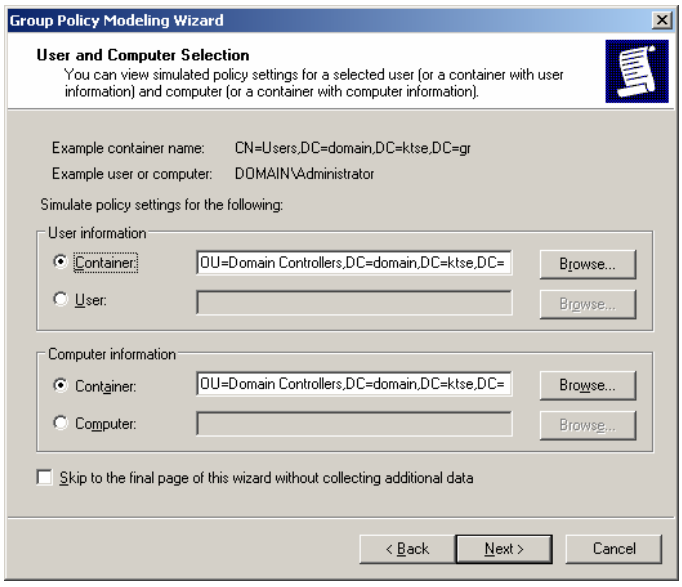
Εικόνα 5-44. Group Policy Modeling Wizard.

3. Κάνουμε τις επιθυμητές επιλογές για την προσομοίωση, πχ καθορίζουμε ένα όνομα χρήστη, ένα όνομα υπολογιστή, μία τοποθεσία χρήστη, μία ιστοσελίδα, μία τοποθεσία υπολογιστή ή ομάδες ασφάλειας.

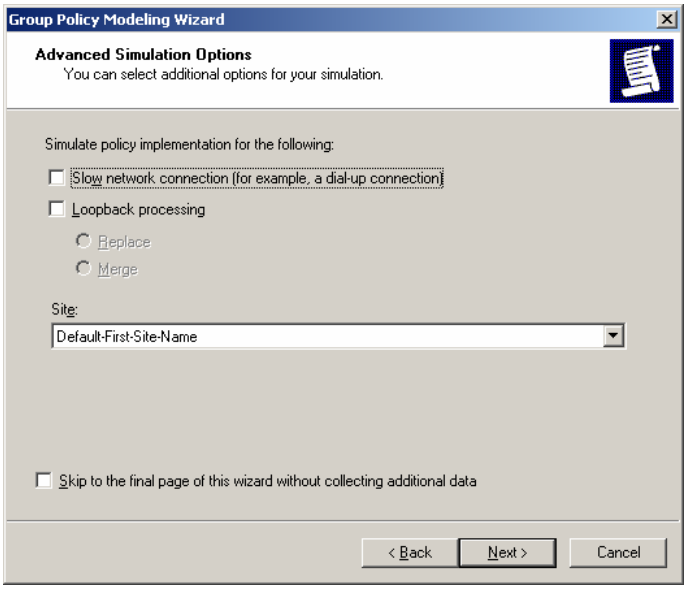
4. Στην οθόνη Summary of Selections κάνουμε μία ανασκόπηση των ρυθμίσεων για να βεβαιώσουμε ότι είναι σωστές και πατάμε Next για να εκκινήσουμε την προσομοίωση.



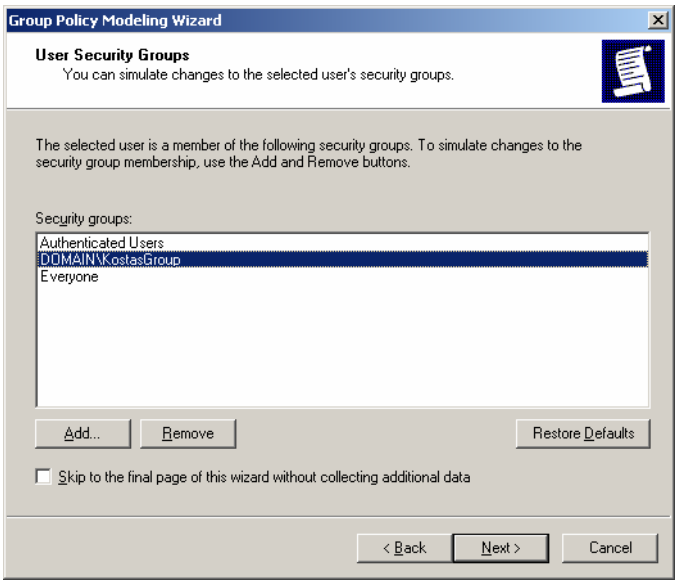
Εικόνα 5-45. Χρησιμοποιήσαμε τον Domain Controller στον τομέα domain.ktse.gr.



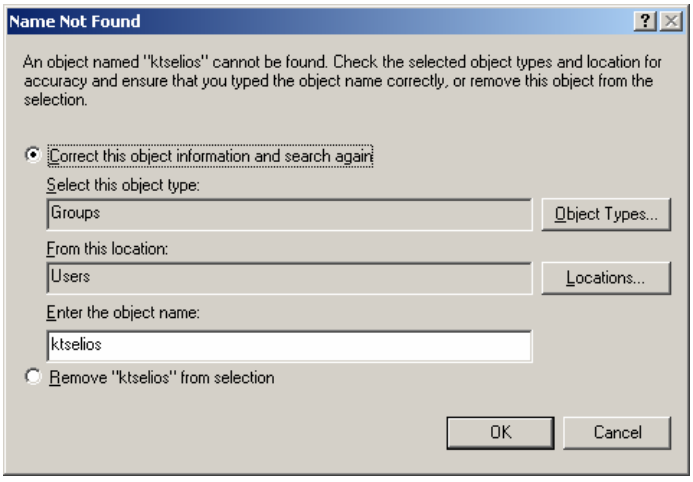
Εικόνα 5-46. Θέσαμε user τον Administrator (διαχειριστής server), και σαν υπολογιστή τον ίδιο τον Domain Controller.



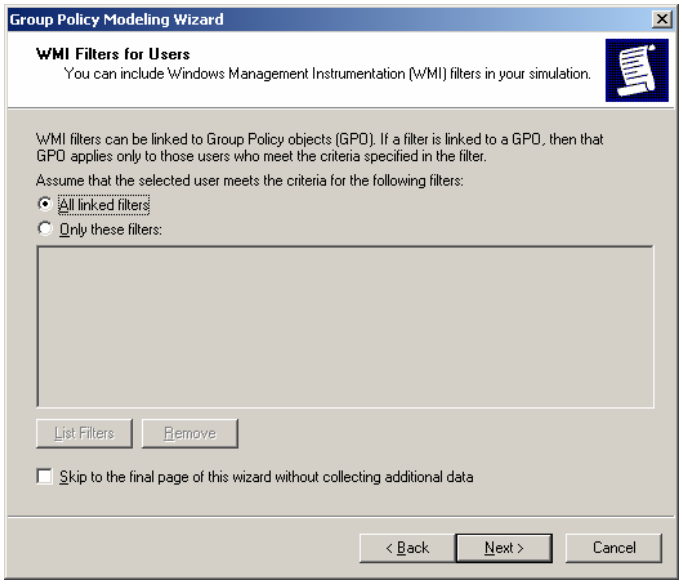
Εικόνα 5-47. Σαν ιστότοπο θέσαμε την default του Domain Controller.



Εικόνα 5-48. Θέσαμε σαν ομάδα το KostasGroup.

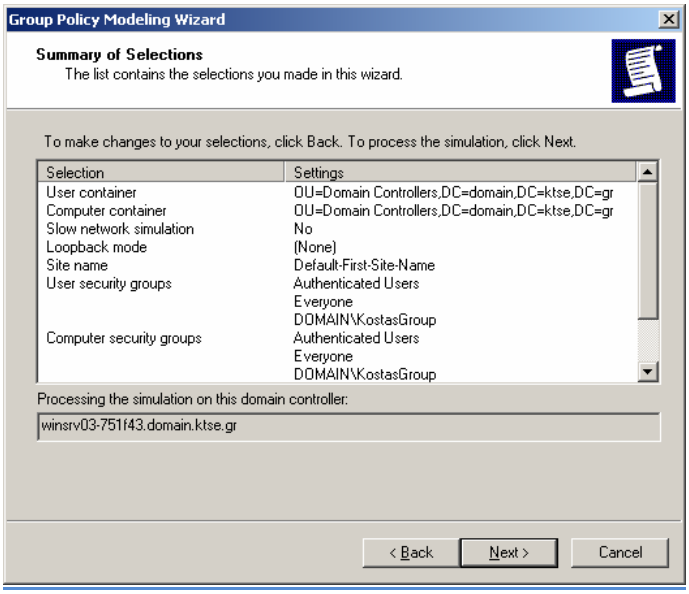


Εικόνα 5-49. Θέσαμε ένα ανύπαρκτο αντικείμενο για να λάβουμε ένα σφάλμα.



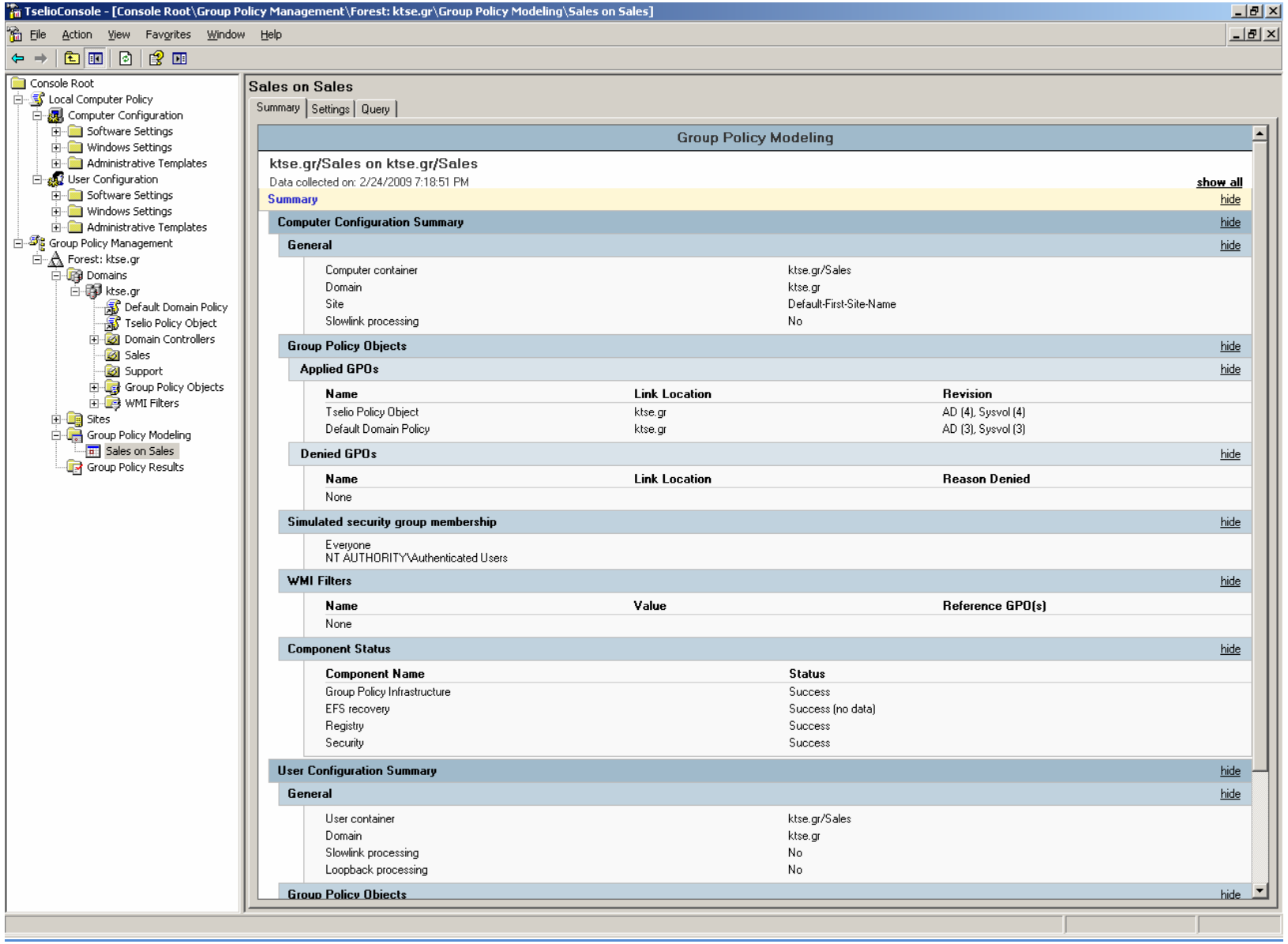
Εικόνα 5-50. Στον συγκεκριμένο Domain Controller δεν θέσαμε WMI filters[83].

[83] Τα WMI φίλτρα επιτρέπουν στο διαχειριστή να καθορίσει δυναμικά το πεδίο των GPOs βάσει των ιδιοτήτων του υπολογιστή-στόχου. Αυτό παρέχει στο διαχειριστή την πιθανότητα να επεκτείνει δραματικά τις δυνατότητες φιλτραρίσματος για τα GPOs σχετικά με παλαιότερους διαθέσιμους μηχανισμούς φιλτραρίσματος ασφάλειας. Το WMI φίλτρο είναι ένα ξεχωριστό αντικείμενο το οποίο μπορεί να αντιστοιχηθεί σε ένα GPO. Όταν το GPO εφαρμοστεί στον υπολογιστή-στόχο, το φίλτρο αξιολογείται σε αυτόν. Τα WMI φίλτρα απαρτίζονται από ένα ή περισσότερα ερωτήματα (queries) που αξιολογούνται ενάντια του WMI repository του υπολογιστή-στόχου. Εάν το σύνολο των ερωτημάτων αξιολογηθεί με την τιμή FALSE, τότε το GPO δεν εφαρμόζεται και, αντιθέτως, εάν όλα τα ερωτήματα αξιολογηθούν με την τιμή TRUE, τότε το GPO εφαρμόζεται. Κάθε ερώτημα γράφεται χρησιμοποιώντας την WMI Query Language (WQL), η οποία είναι μία γλώσσα όμοια με την SQL που χρησιμοποιείται για το querying του WMI repository. Το κάθε GPO μπορεί να έχει μόνο ένα WMI φίλτρο, εντούτοις το ίδιο WMI φίλτρο μπορεί να αντιστοιχηθεί σε πολλαπλά GPOs. Τέλος, όπως και τα GPOs, τα WMI φίλτρα είναι αντικείμενα ανά τομέα (per domain objects).

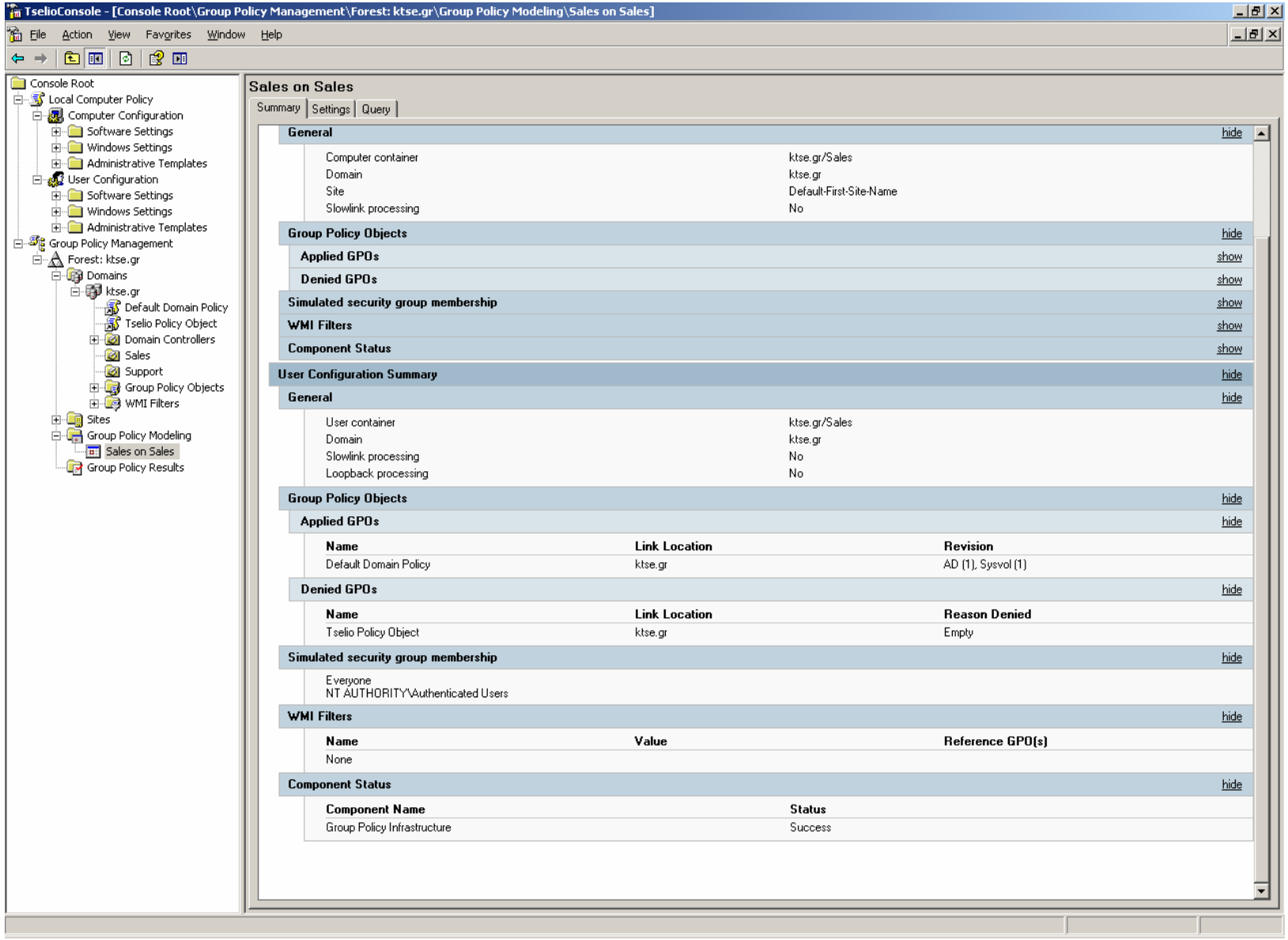


Εικόνα 5-51. Summary of Selection [τελική ανασκόπηση της προσομοίωσης].

5. Μετά το πέρας της προσομοίωσης, το εργαλείο wizard παρουσιάζει τα αποτελέσματα σε μία αναφορά με το όνομα Group Policy Results. Εάν δύο ή περισσότερα GPOs έχουν αντιτιθέμενες ρυθμίσεις για μια συγκεκριμένη πολιτική, η αναφορά παραθέτει το ποια πολιτική εφαρμόστηκε. Αυτό είναι πολύ χρήσιμο για την επίλυση αντιθέσεων ανάμεσα σε GPOs και για την αντιμετώπιση προβλημάτων από απρόσμενες συμπεριφορές των GPOs.



Εικόνα 5-52. Α' μέρος αναφοράς Group Policy Result.



Εικόνα 5-53. Β' μέρος αναφοράς Group Policy Result.

5.4 Πρότυπα Διαχείρισης

Αντιστοίχως με τα πρότυπα ασφάλειας, τα Windows XP υποστηρίζουν και πρότυπα διαχείρισης. Αυτά τα πρότυπα χρησιμοποιούνται για τη διαμόρφωση ρυθμίσεων τόσο σχετικά με την ασφάλεια όσο και άσχετα από αυτή (πχ διαμόρφωση διεπαφής χρήστη) για τα Windows XP και για διάφορες εφαρμογές της Microsoft. Τα πρότυπα διαχείρισης μπορούν να χρησιμοποιηθούν μόνο σε συνεργασία με τα GPOs, οπότε δεν μπορούν να χρησιμοποιηθούν για να ασφαλίσουν συστήματα σε τυπικά SOHO περιβάλλοντα και σε πολλά legacy περιβάλλοντα. Εξαιτίας αυτού, αυτή η εργασία χρησιμοποιεί πρότυπα ασφάλειας αντί προτύπων διαχείρισης.

Οι διαχειριστές συστημάτων σε enterprise και specialized security-limited functionality περιβάλλοντα μπορεί να προτιμήσουν να χρησιμοποιήσουν πρότυπα διαχείρισης τα οποία να περιλαμβάνουν ρυθμίσεις ασφάλειας, από το να χρησιμοποιήσουν και πρότυπα διαχείρισης, με ρυθμίσεις άσχετες με την ασφάλεια, και ξεχωριστά πρότυπα ασφάλειας. Οι διαχειριστές μπορούν να επιλέξουν να ενσωματώσουν τις ρυθμίσεις ασφάλειας που παρουσιάστηκαν μέσα στα δικά τους πρότυπα διαχείρισης. Τα Windows XP SP2 εμπεριέχουν διάφορα προκαθορισμένα πρότυπα διαχείρισης (default administration templates) τα οποία απευθύνονται σε συγκεκριμένους τύπους ρυθμίσεων, περιλαμβανομένου και γενικών ρυθμίσεων των Windows XP, Internet Explorer, Microsoft NetMeeting, Windows Media Player και Microsoft Update. Οι διαχειριστές μπορούν να χρησιμοποιήσουν αυτά τα πρότυπα ως σημείο εκκίνησης για τη δημιουργία προτύπων οργανισμού ή ενός συγκεκριμένου περιβάλλοντος. Τέλος οι διαχειριστές συστημάτων θα πρέπει να διεξάγουν εκτεταμένες δοκιμές σε όλα τα πρότυπα διαχείρισης προτού τα χρησιμοποιήσουν για να διαμορφώσουν και ασφαλίσουν συστήματα παραγωγής.[84]

5.5 Σύνοψη και Υποδείξεις

- ✓ Χρησιμοποίηση των προτύπων ασφάλειας της NIST για τη διαμόρφωση των ρυθμίσεων ασφάλειας πάνω σε Windows XP συστήματα. Μετατροπή των προτύπων όπως χρειαστεί για να συμβαδίζουν με την τοπική πολιτική ασφάλειας και καταγραφή όλων των μετατροπών.

- ✓ Χρησιμοποίηση των snap-ins Security Templates και Security Configuration and Analysis του MMC για δημιουργία, εισαγωγή, τήρηση, διαμόρφωση και εξαγωγή ρυθμίσεων των προτύπων και σύγκριση των ρυθμίσεων των προτύπων με αυτές ενός υποστατού συστήματος.

- ✓ Χρησιμοποίηση των snap-ins Group Policy Object Editor, Group Policy Management Console και Group Policy Modeling Wizard του MMC για την αυτοματοποίηση της επέκτασης των ρυθμίσεων ασφάλειας σε συστήματα των μελών τομέα.

---

[84] Επιπρόσθετες πληροφορίες αναφορικά με τα πρότυπα διαχείρισης, είναι διαθέσιμες από το Κεφάλαιο 4 του *Windows XP Security Guide*, που είναι διαθέσιμο εδώ: http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.mspx

Κεφάλαιο 6

6. Επισκόπηση Προτύπων Ασφάλειας του NIST για τα Windows XP

Αυτή η ενότητα παρέχει μία επισκόπηση των ρυθμίσεων ασφάλειας που θα εφαρμοστούν από τα πρότυπα του NIST, όπως είναι αναρτημένα στο Παράρτημα Α, καθώς και επιπλέον τύποι ρυθμίσεων που θα μπορούσαν να προστεθούν σε αυτά τα πρότυπα. Οι ρυθμίσεις διαχωρίζονται στις εξής κατηγορίες: Πολιτικές Λογαριασμών, Τοπικές Πολιτικές, Πολιτικές Αναφορών Συμβάντων (event logs), Περιορισμένες Ομάδες, Υπηρεσίες Συστήματος, Δικαιώματα Αρχείων, Δικαιώματα Μητρώου (registry permissions) και Τιμές Μητρώου. Αυτή η ενότητα περιγράφει τους σχετικούς ελέγχους ασφάλειας των προτύπων για κάθε κατηγορία και πώς αυτοί οι έλεγχοι μπορούν να χρησιμοποιηθούν για τη βελτιστοποίηση της ασφάλειας του συστήματος.[85] Θα προσπαθήσουμε να δούμε ένα σημαντικό κομμάτι από τις ακριβείς προτεινόμενες παραμέτρους και τιμές των προτύπων ασφάλειας του NIST.

6.1 Πολιτικές Λογαριασμών

Εκτός από την εκπαίδευση των χρηστών όσον αφορά τη χρησιμοποίηση και την επιλογή αποδεκτών κωδικών ασφάλειας, είναι εξίσου σημαντικό να θέσουμε παραμέτρους κωδικών έτσι ώστε αυτοί να είναι αρκετά ισχυροί. Αυτό μειώνει την πιθανότητα ένας επιτιθέμενος να μαντέψει ή να σπάσει τους κωδικούς και να μπορέσει να έχει πρόσβαση στο σύστημα.[86] Όπως περιγράφτηκε και σε προηγούμενο κεφάλαιο, είναι προτιμότερη η χρήση των NTLM v2 ή Kerberos αντί των LM ή NTLM v1 για την πιστοποίηση.[87] Οι ακόλουθοι παράμετροι είναι αυτοί που διευκρινίζονται στα πρότυπα του NIST:

- **Μέγιστη Ηλικία Κωδικών Ασφάλειας:** Εξαναγκάζει τους χρήστες να αλλάζουν τον κωδικό ασφάλειας σε τακτικά χρονικά διαστήματα. Όσο μικρότερη είναι η αξία που θα οριστεί, τόσο μεγαλύτερη είναι η πιθανότητα οι χρήστες να θέτουν ευκολομνημόνευτους κωδικούς (πχ Mypasswd1, Mypasswd2, Mypasswd3). Όσο μεγαλύτερη είναι αυτή η αξία, τόσο μεγαλύτερη είναι η πιθανότητα να γνωστοποιηθούν οι κωδικοί και να χρησιμοποιηθούν από μη-εξουσιοδοτημένα πρόσωπα.

- **Ελάχιστη Ηλικία Κωδικών Ασφάλειας:** Αυτή η ρύθμιση απαιτεί οι χρήστες να περιμένουν ένα συγκεκριμένο αριθμό ημερών προτού αλλάξουν ξανά τους κωδικούς τους. Η ρύθμιση αποτρέπει κάποιο χρήστη από το να αλλάξει ένα

---

[85] Τα Windows XP με SP2 και τα Windows 2003 SP1 συστήνουν ένα μεγάλο αριθμό ρυθμίσεων Πολιτικών Ομάδων που μπορούν να διαμορφωθούν με διαχειριστικά πρότυπα και πρότυπα ασφάλειας. Περισσότερες πληροφορίες για αυτές τις ρυθμίσεις μπορούν να αντληθούν από το άρθρο: http://www.microsoft.com/downloads/details.aspx?FamilyID=7821c32f-da15-438d-8e48-45915cd2bc14&displaylang=en.

[86] Οι κωδικοί θα πρέπει να προστατεύονται και με άλλα μέσα, όπως να μην ενσωματώνονται σε προγράμματα και scripts.

[87] Kerberos and NTLM: http://blogs.msdn.com/sql_protocols/archive/2006/12/02/understanding-kerberos-and-ntlm-authentication-in-sql-server-connections.aspx

κωδικό μόλις αυτός φτάσει τη μέγιστη ηλικία του και αμέσως μετά να τον αλλάξει ξανά με τον ακριβώς προηγούμενο. Δυστυχώς αυτή η ρύθμιση επίσης αποτρέπει τους χρήστες οι οποίοι έχουν αποκαλύψει, από λάθος, τον κωδικό τους σε άλλους, να τον αλλάξουν ξανά άμεσα χωρίς να επέμβει ο διαχειριστής.

- **Ελάχιστο Μήκος Κωδικών Ασφάλειας:** Αυτή η ρύθμιση καθορίζει το ελάχιστο μήκος ενός κωδικού, σε χαρακτήρες. Η λογική πίσω από αυτή τη ρύθμιση είναι ότι όσο μεγαλύτερος είναι ένας κωδικός, συχνά τόσο πιο δύσκολο είναι να τον μαντέψει κάποιος, ή ακόμα και να τον σπάσει, σε σχέση με τους μικρότερους σε χαρακτήρες κωδικούς. Το μειονέκτημα είναι πως οι μεγαλύτεροι σε χαρακτήρες κωδικοί είναι συχνά πιο δύσκολο για τους χρήστες να τους θυμούνται. Οι οργανισμοί που θέλουν να θέσουν ένα σχετικά μεγάλο ελάχιστο μήκος κωδικού, θα πρέπει να παροτρύνουν τους χρήστες να χρησιμοποιούν συνθηματικά (passphrases), ούτως ώστε να τα θυμούνται ευκολότερα από ότι τους συμβατικούς κωδικούς.

- **Οι Κωδικοί Ασφάλειας Πρέπει Να Πληρούν Τις Προϋποθέσεις Πολυπλοκότητας:** Όπως και στη ρύθμιση «Ελάχιστο Μήκος Κωδικών Ασφάλειας», έτσι και αυτή η ρύθμιση κάνει δυσκολότερο το να μαντέψει ή να σπάσει κάποιος τους κωδικούς. Η ενεργοποίηση αυτής της ρύθμισης εφαρμόζει τις προϋποθέσεις πολυπλοκότητας, συμπεριλαμβανομένου και της απόκλισης να εμπεριέχεται το όνομα χρήστη μέσα στον κωδικό ασφάλειάς του και χρησιμοποιεί ένα μίγμα τύπων χαρακτήρων (πεζά, κεφαλαία, ψηφία και ειδικούς χαρακτήρες όπως πχ σημεία στίξης).[88]

- **Επιβολή Ιστορικού Κωδικών Ασφάλειας:** Αυτή η ρύθμιση καθορίζει το πόσους παλαιούς κωδικούς θα θυμάται το σύστημα για ένα χρήστη. Οι χρήστες θα αποτρέπονται από το να επαναχρησιμοποιούν κάποιον από τους παλαιούς κωδικούς. Παραδείγματος χάριν, εάν στη ρύθμιση οριστεί η τιμή 24 το σύστημα δεν θα επιτρέψει στους χρήστες την επαναχρησιμοποίηση των τελευταίων 24 κωδικών τους. Οι παλαιοί κωδικοί μπορεί να έχουν αποκαλυφθεί ή κάποιος επιτιθέμενος είχε αρκετό χρόνο για να σπάσει κωδικοποιημένους κωδικούς. Η επαναχρησιμοποίηση παλαιών κωδικών μπορεί ακούσια να δώσει σε κάποιον επιτιθέμενο πρόσβαση στο σύστημα.

- **Αποθήκευση Κωδικών Χρησιμοποιώντας Αντιστρέψιμη Κρυπτογράφηση Για Όλους Τους Χρήστες Του Τομέα:** Εάν αυτή η ρύθμιση είναι ενεργοποιημένη, οι κωδικοί αποθηκεύονται σε μη κωδικοποιημένη μορφή, βάζοντάς τους σε μεγαλύτερο κίνδυνο να αποκαλυφθούν. Αυτή η ρύθμιση θα πρέπει να απενεργοποιηθεί εκτός εάν είναι απαραίτητη για την υποστήριξη κάποιου συμβατού πρωτοκόλλου επικύρωσης, όπως το CHAP (Challenge Handshake Authentication Protocol), το οποίο αντενδείκνυται.[89]

---

[88] Αυτές οι απαιτήσεις είναι βασισμένες στο εκ προεπιλογής φίλτρο κωδικών (passfilt.dll) που εμπεριέχεται στα Windows XP. Περισσότερες πληροφορίες: http://technet.microsoft.com/en-us/library/bb457114.aspx.

[89] Το NIST δεν προτείνει τη χρησιμοποίηση του CHP ή του MS-CHAP λόγω γνωστών αδυναμιών ασφάλειας.

Συχνά επιτιθέμενοι προσπαθούν να κερδίσουν πρόσβαση σε λογαριασμούς χρηστών, μαντεύοντας τους κωδικούς ασφαλείας τους. Τα Windows XP μπορούν να ρυθμιστούν έτσι, ώστε όταν πραγματοποιηθούν αρκετές αποτυχημένες προσπάθειες πρόσβασης σε κάποιο λογαριασμό για μία χρονική περίοδο, το σύστημα να απενεργοποιεί αυτό το λογαριασμό. Για τον αποκλεισμό ενός λογαριασμού υπάρχουν οι κάτωθι ρυθμίσεις στα πρότυπα του NIST:

- **Κατώφλι Αποκλεισμού Λογαριασμού:** Η τιμή του κατωφλίου καθορίζει το μέγιστο αριθμό αποτυχημένων προσπαθειών που μπορεί να συμβούν, προτού αποκλειστεί ένας λογαριασμός.

- **Διάρκεια Αποκλεισμού Λογαριασμού:** Αυτή η τιμή καθορίζει το χρονικό διάστημα που θα παραμείνει αποκλεισμένος ένας λογαριασμός. Αυτή συχνά είναι ρυθμισμένη να έχει μικρή, αλλά ουσιαστική τιμή (πχ 15 λεπτά) για δύο λόγους. Πρώτον, ένας νόμιμος χρήστης που κατά λάθος αποκλείστηκε από το σύστημα, θα πρέπει να περιμένει 15 λεπτά για να μπορέσει να έχει ξανά πρόσβαση, αντί να ζητήσει από το διαχειριστή να του ξεκλειδώσει αυτός το λογαριασμό του. Δεύτερον, ένας επιτιθέμενος που προσπαθεί να σπάσει ένα κωδικό ασφάλειας χρησιμοποιώντας κάποια μέθοδο ωμής βίας (brute force method), θα μπορεί να δοκιμάζει ένα μικρό αριθμό κωδικών την κάθε φορά και έπειτα θα πρέπει να περιμένει 15 λεπτά για να αρχίσει να χρησιμοποιεί και πάλι τη μέθοδο. Αυτό ελαχιστοποιεί σημαντικά τις πιθανότητες να κατασταθεί επιτυχημένη μία επίθεση ωμής βίας (brute force attack).

- **Επαναφορά Μετρητή Αποκλεισμού Λογαριασμού Μετά Από:** Αυτή η ρύθμιση καθορίζει τη χρονική περίοδο που χρησιμοποιείται μαζί με την τιμή κατωφλίου αποκλεισμού. Για παράδειγμα εάν το κατώφλι είναι ορισμένο στις 10 προσπάθειες και η διάρκεια είναι ορισμένη στα 15 λεπτά, τότε εάν πραγματοποιηθούν πάνω από 10 αποτυχημένες προσπάθειες εισαγωγής ενός συγκεκριμένου λογαριασμού στο σύστημα και σε διάρκεια 15 λεπτών, αυτός ο λογαριασμός θα απενεργοποιείται.

Μία από τις κύριες προκλήσεις όσον αφορά τις ρυθμίσεις πολιτικής των λογαριασμών είναι να επιτευχθεί η ισορροπία ανάμεσα σε ασφάλεια, λειτουργικότητα και χρηστικότητα. Για παράδειγμα αποκλείοντας τους λογαριασμούς χρηστών μετά από λίγες μόνο αποτυχημένες προσπάθειες πρόσβασης και σε μία μεγάλη χρονική περίοδο, μπορεί μεν να καθιστά δυσκολότερη τη μη-εξουσιοδοτημένη πρόσβαση στους λογαριασμούς μαντεύοντας τους κωδικούς τους, αλλά μπορεί να αυξήσει δραματικά τις κλήσεις που θα δεχτεί η μηχανογράφηση για ξεκλείδωμα λογαριασμών που αποκλείστηκαν κατά λάθος από συνεχείς αποτυχημένες προσπάθειες εισόδου σε λογαριασμούς από τους νόμιμους χρήστες τους. Αυτό που θα μπορούσε επίσης να προκληθεί είναι να καταγράφουν οι χρήστες τους κωδικούς τους ή να επιλέγουν ευκολομνημόνευτους κωδικούς. Οι οργανισμοί θα πρέπει να σκεφτούν προσεκτικά τέτοια ζητήματα που μπορεί να τεθούν, πριν ορίσουν την πολιτική των λογαριασμών στα Windows XP.

6.2 Τοπικές Πολιτικές

Η κατηγορία των τοπικών πολιτικών καλύπτει τρείς υποκατηγορίες: πολιτική ελέγχου συστήματος, ανάθεση δικαιωμάτων χρηστών και επιλογές ασφάλειας. Για κάθε μία από αυτές θα εμβαθύνουμε στις ενότητες που ακολουθούν.

6.2.1 *Πολιτική Ελέγχου*

Τα Windows XP έχουν ισχυρές δυνατότητες ελέγχου συστήματος. Σκοπός του ελέγχου είναι η καταγραφή συγκεκριμένου τύπου ενεργειών σε μία αναφορά (log file) ούτως ώστε να μπορούν οι διαχειριστές να επιθεωρούν τις αναφορές αυτές και να εντοπίζουν μη-εξουσιοδοτημένες ενέργειες. Επιπλέον αναφορές ελέγχου (audit logs) μπορούν να φανούν χρήσιμες κατά την έρευνα ενός περιστατικού ασφάλειας που συνέβη. Όπως φαίνεται και στον πίνακα 6.1, ο έλεγχος συστήματος είναι ενεργοποιημένος για τα περιστατικά σύνδεσης (logon events), τη διαχείριση λογαριασμών, την πρόσβαση υπηρεσιών καταλόγου, την πρόσβαση αντικειμένων, την αλλαγή πολιτικής, τη χρήση προνομίων, την παρακολούθηση διεργασιών και τις αναφορές συστήματος. Η κάθε κατηγορία ελέγχου πολιτικής μπορεί να ρυθμιστεί να καταγράφει επιτυχή περιστατικά, ανεπιτυχή περιστατικά, επιτυχή και ανεπιτυχή περιστατικά, ή κανένα από τα δύο.

Πίνακας 6-1 Περιγραφή Ευρέος Ελέγχου Πολιτικής Συστήματος

Έλεγχος Πολιτικής (Audit Policy)	Περιγραφή
Audit account logon events	Ελέγχει πότε ένας χρήστης συνδέεται και αποσυνδέεται σε κάποιο απομακρυσμένο υπολογιστή από το τερματικό του.
Audit account management	Ελέγχει πότε δημιουργήθηκε, άλλαξε, ή διαγράφηκε ένας λογαριασμός χρήστη ή μία ομάδα· πότε μετονομάστηκε, ενεργοποιήθηκε, ή απενεργοποιήθηκε ένας λογαριασμός χρήστη· πότε άλλαξε ένας κωδικός ασφάλειας.
Audit directory service access	Ελέγχει το περιστατικό όπου ένας χρήστης να έχει πρόσβαση σε κάποιο αντικείμενο του active directory, το οποίο έχει ορισμένη τη δική του System Access Control List (SACL). Αυτή η ρύθμιση δεν είναι εφαρμόσιμη στα Windows XP.
Audit logon events	Ελέγχει τις αποσυνδέσεις και τις συνδέσεις των χρηστών, ή το να πραγματοποιήσουν οι χρήστες μία σύνδεση δικτύου σε κάποιο τοπικό υπολογιστή.
Audit object access	Ελέγχει αν κάποιος χρήστης είχε πρόσβαση σε κάποιο αντικείμενο (πχ, ένα αρχείο, φάκελο, registry key ή εκτυπωτή) το οποίο έχει ορισμένη τη δική του SACL. Ο έλεγχος επιτυχίας ή αποτυχίας της ευρείας πρόσβασης αντικειμένων στο σύστημα θα δημιουργήσει πολλές καταχωρίσεις αναφοράς. Συγκεκριμένες αποτυχίες πρόσβασης αντικειμένων μπορεί να είναι φυσιολογικές, σαν αποτέλεσμα απαίτησης κάποιων εφαρμογών σε όλους τους τύπους πρόσβασης για τη σωστή λειτουργία τους. Εφίσταται προσοχή στην χρησιμοποίηση ελέγχου πρόσβασης αντικειμένων.
Audit policy change	Ελέγχει κάθε αλλαγή στην πολιτική ανάθεσης δικαιωμάτων, και επίσης ελέγχει και εμπιστεύεται πολιτικές.
Audit privilege use	Ελέγχει την κάθε περίπτωση άσκησης δικαιώματος κάποιου χρήστη. Αυτό είναι πολύ πιθανό να δημιουργήσει ένα πολύ μεγάλο αριθμό περιστατικών.
Audit process tracking	Ελέγχει λεπτομερείς πληροφορίες παρακολούθησης περιστατικών, όπως ενεργοποίηση προγραμμάτων, διεργασία εξόδου, μεταχείριση

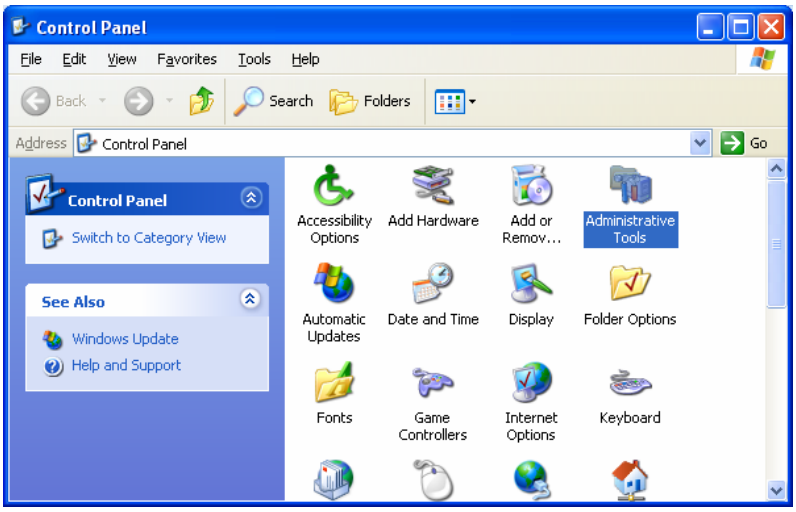
	αναπαραγωγής πανομοιότυπων και έμμεση πρόσβαση αντικειμένων. Ενεργοποιώντας αυτή τη ρύθμιση θα δημιουργηθούν πολλά περιστατικά, οπότε θα πρέπει να χρησιμοποιηθεί μόνο όταν καθίσταται απολύτως απαραίτητο.
Audit system events	Ελέγχει πότε ένας χρήστης πραγματοποιεί επανεκκίνηση ή τερματισμό του υπολογιστή, ή όταν λαμβάνει χώρα ένα περιστατικό που επηρεάζει είτε την ασφάλεια του συστήματος, είτε την αναφορά ασφάλειας (security log).

Οι ρυθμίσεις του παραπάνω πίνακα μπορούν να εφαρμοσθούν ακολουθώντας τα παρακάτω βήματα:

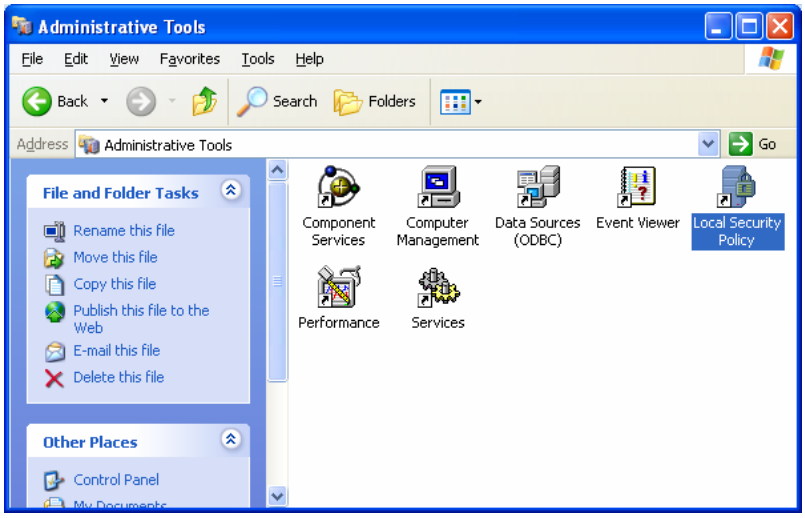
1. Από το μενού εκκίνησης **Start** επιλέγουμε το **Control Panel**.

Εικόνα 6-1. Control Panel.

2. Επιλέγουμε **Administrative Tools** και έπειτα **Local Security Policy**.

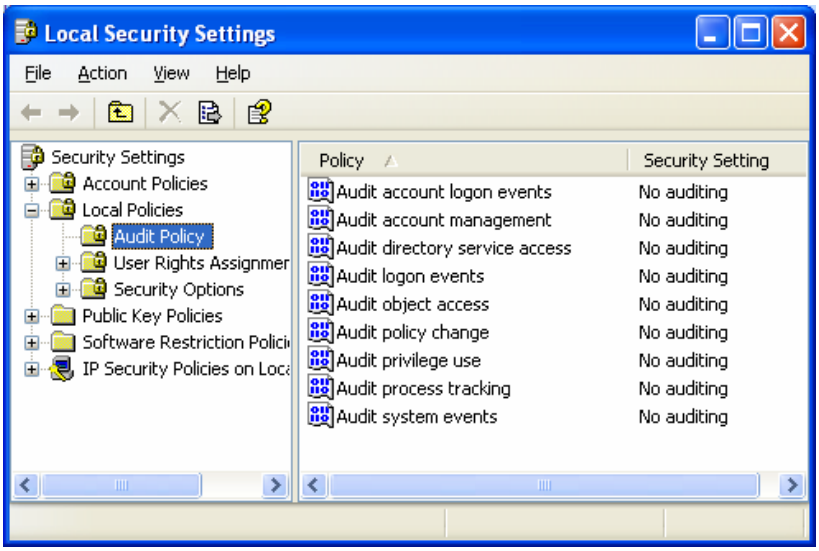


Εικόνα 6-2. Administrative Tools.



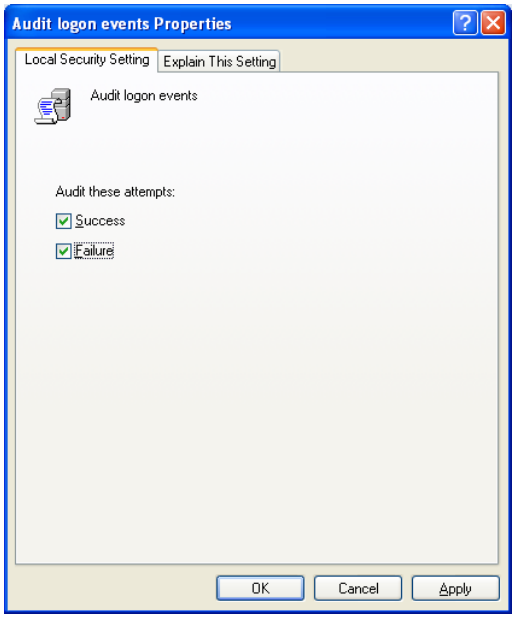
Εικόνα 6-3. Local Security Policy.

3. Επεκτείνουμε το **Local Policies** και κάνουμε κλικ στο **Audit Policy**.



Εικόνα 6-4. Local Security Settings – Audit Policy.

4. Η δεξιά πλευρά απαριθμεί τις τρέχουσες ρυθμίσεις ελέγχου. Πραγματοποιούμε τις επιθυμητές αλλαγές κάνοντας διπλό κλικ στο κατάλληλο αντικείμενο, τροποποιούμε τη ρύθμιση και πατάμε **OK** για να τη σώσουμε.



Εικόνα 6-5. Audit Logon Events Properties.

Εικόνα 6-6. Local Security Settings – Audit Policy Customized.

Τα πρότυπα του NIST δεν ενεργοποιούν τον έλεγχο για συγκεκριμένα αρχεία και registry keys. Οι διαχειριστές θα πρέπει να λάβουν σοβαρά υπόψη την ενεργοποίηση ελέγχου για τους πιο σημαντικούς καταλόγους (πχ, %SystemDrive%, καταλόγους που κρατάνε κρίσιμες πληροφορίες χρηστών) και registry keys (πχ, HKLM\Software, HKLM\System). Επειδή η ενεργοποίηση ελέγχων καταλόγων και registry keys μπορεί να δημιουργήσει ένα μεγάλο αριθμό περιστατικών ελέγχου, οι διαχειριστές θα πρέπει να δοκιμάσουν προσεκτικά όλες αυτές τις ρυθμίσεις προτού τις εφαρμόσουν σε συστήματα παραγωγής.

6.2.2 *Ανάθεση Δικαιωμάτων Χρηστών*

Τα πρότυπα ασφάλειας καθορίζουν ποιές ομάδες έχουν ποια συγκεκριμένα δικαιώματα (πχ, διαχειριστές, χρήστες). Ο στόχος είναι η κάθε ομάδα να έχει μόνο τα απαραίτητα δικαιώματα και όσον αφορά τους χρήστες, να ανήκει ο καθένας μόνο στις απαραίτητες ομάδες. Αυτή είναι η αρχή των ελαχίστων δικαιωμάτων (least privilege principle). Παραδείγματα από δικαιώματα χρηστών που μπορούν να οριστούν είναι τα κάτωθι:

- Τοπική και απομακρυσμένη πρόσβαση στο σύστημα
- Εκτέλεση backup
- Αλλαγή ημερομηνίας και ώρας στο σύστημα
- Διαχείριση των αναφορών
- Τερματισμός του συστήματος

6.2.3 *Επιλογές Ασφάλειας*

Εκτός από τις ρυθμίσεις τοπικής πολιτικής ασφάλειας (Local Security Policy Settings) που προαναφέρθηκαν σε αυτή την ενότητα, επιπρόσθετες ρυθμίσεις, επονομαζόμενες ως Επιλογές Ασφάλειας (Security Options), μπορούν να τροποποιηθούν ούτως ώστε να επιτευχθεί μεγαλύτερη ασφάλεια από ότι με τις προεπιλεγόμενες ρυθμίσεις που παρέχονται. Παραδείγματα από τέτοιους τύπους ρυθμίσεων που είναι διαθέσιμες στα πρότυπα του NIST είναι τα κάτωθι:

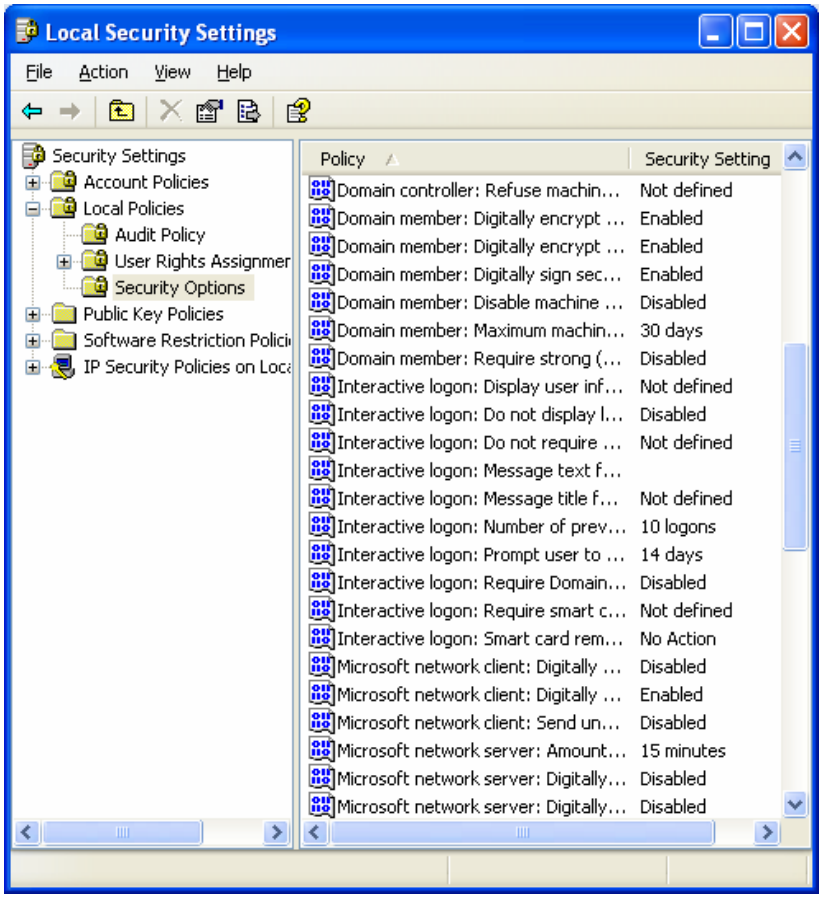
- Περιορισμός της χρήσης κενών κωδικών ασφάλειας
- Μετονομασία των προεπιλεγμένων λογαριασμών Administrator και Guest
- Περιορισμός της απομακρυσμένης πρόσβασης των οδηγών δισκέτας και οπτικού δίσκου
- Κρυπτογράφηση ασφαλούς καναλιού δεδομένων σε κάποιο τομέα
- Ασφάλιση της αλληλεπιδρώσας οθόνης logon (πχ να μη φαίνεται το όνομα του λογαριασμού του προηγούμενου χρήστη, επίδειξη ενός προειδοποιητικού banner, διάλογος προτροπής των χρηστών για αλλαγή των κωδικών πρόσβασης προτού αυτοί λήξουν)
- Περιορισμός σε ποιους τύπους δικτύων μπορεί να εκτελεστεί η πρόσβαση
- Διευκρίνιση των τύπων πιστοποίησης που μπορούν να χρησιμοποιηθούν (πχ NTLM v2)

Οι ρυθμίσεις των επιλογών ασφάλειας μπορούν επίσης να προσεγγιστούν και να διευθετηθούν χειροκίνητα ακολουθώντας τα παρακάτω βήματα:

1. Από το μενού εκκίνησης **Start** επιλέγουμε το **Control Panel**.

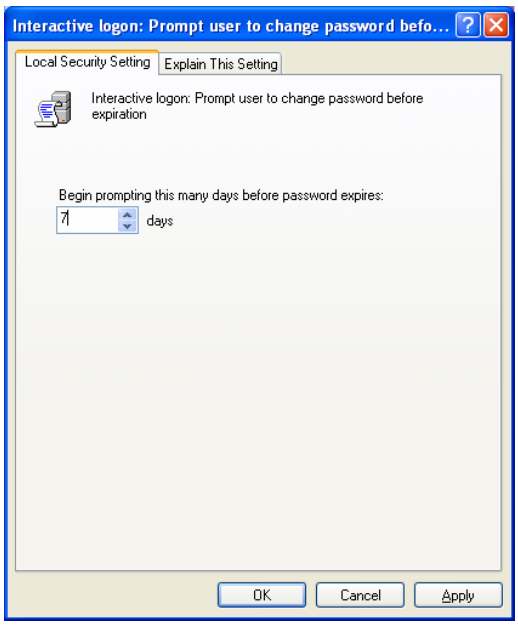
2. Επιλέγουμε **Administrative Tools** και έπειτα **Local Security Policy**.

3. Επεκτείνουμε το **Local Policies** και επιλέγουμε **Security Options**.



Εικόνα 6-7. Local Security Setting – Security Options.

4. Η δεξιά πλευρά απαριθμεί τις επιλογές ασφάλειας και δείχνει τις τρέχουσες ρυθμίσεις της κάθε μίας. Πραγματοποιούμε τις επιθυμητές αλλαγές κάνοντας διπλό κλικ στην κατάλληλη επιλογή ασφάλειας, τροποποιούμε τη ρύθμιση και πατάμε **OK** για να τη σώσουμε (πχ, στο αλληλεπιδρόν logon να προειδοποιείται ο χρήστης 7 ημέρες προτού λήξει ο κωδικός του λογαριασμού του).



Εικόνα 6-8. Interactive Logon – Prompt User to Change Password Before.

6.3 Πολιτικές Αναφορών Συμβάντων

Τα Windows XP καταγράφουν πληροφορίες για αξιοσημείωτα συμβάντα σε τρείς αναφορές: στην Αναφορά Εφαρμογών (Application Log), στην Αναφορά Ασφάλειας (Security Log) και στην Αναφορά Συστήματος (System Log). Η αναφορά περιέχει μηνύματα σφαλμάτων, πληροφορίες ελέγχου και άλλες εγγραφές της δραστηριότητας του συστήματος. Οι αναφορές μπορούν να χρησιμοποιηθούν όχι μόνο στην αναγνώριση ύποπτης και κακόβουλης συμπεριφοράς και στην εξέταση περιστατικών ασφάλειας, αλλά επίσης και να βοηθήσουν στον εντοπισμό και την επισκευή προβλημάτων εφαρμογών. Επομένως είναι σημαντική η ενεργοποίηση της σύνταξης αναφορών και για τους τρείς προαναφερθέντες τύπους. Τα πρότυπα του NIST ενεργοποιούν και τις τρείς αναφορές σε όλα τα περιβάλλοντα και ορίζουν επίσης το μέγιστο μέγεθος της αναφοράς. Αυτό είναι σημαντικό διότι εάν το μέγιστο μέγεθος της αναφοράς έχει πολύ μικρή τιμή, το σύστημα δεν θα έχει αρκετό χώρο για αποθήκευση πληροφοριών όσον αφορά τη δραστηριότητά του. Ορισμένοι οργανισμοί μπορούν να έχουν μία πολιτική αναφορών και ένα κεντρικό εξυπηρετητή αναφορών, έτσι οι ρυθμίσεις των προτύπων θα πρέπει να τροποποιηθούν έτσι ώστε να συμμορφώνονται με την πολιτική αυτή.

6.4 Περιορισμένες Ομάδες

Το NIST συμβουλεύει να αφαιρεθούν όλοι οι χρήστες από την ομάδα Remote Desktop Users, από όλα τα συστήματα, από όλα τα περιβάλλοντα, εκτός από αυτούς τους χρήστες που πρέπει αποκλειστικά να ανήκουν σε αυτή την ομάδα. Αυτό θα μειώσει την πιθανότητα του να κερδίσει κάποιος μη εξουσιοδοτημένη πρόσβαση στο σύστημα μέσω Remote Desktop. Το NIST προτείνει επίσης τον περιορισμό δυνατότητας εγγραφής μέλους στην ομάδα Power Users, διότι είναι σχεδόν ισοδύναμη σε προνόμια με την ομάδα των διαχειριστών. Οι χρήστες δεν θα πρέπει να χρησιμοποιούν ένα λογαριασμό στην ομάδα Power Users για τη λειτουργία του

συστήματος σε καθημερινή βάση˙ τέτοιοι λογαριασμοί θα πρέπει να μεταχειρίζονται ως λογαριασμοί ομάδας διαχειριστών και να χρησιμοποιούνται μόνο όταν αυτό είναι απαραίτητο. Όταν καθίσταται δυνατό, οι χρήστες που χρειάζονται επιπλέον προνόμια, αλλά όχι πλήρη πρόσβαση επιπέδου διαχειριστή, θα πρέπει να τους παραχωρούνται τα συγκεκριμένα προνόμια που χρειάζονται έναντι της έκτασης των προνομίων που παραχωρούνται από την εγγραφή μέλους στην ομάδα Power Users. Εξ' ορισμού, το κάθε πρότυπο ασφάλειας του NIST αφαιρεί όλους τους χρήστες από τις ομάδες Remote Desktop Users και Power Users˙ το πρότυπο ασφάλειας περιβάλλοντος specialized security-limited functionality αφαιρεί επίσης και όλους τους χρήστες της ομάδας Backup Operators.

6.5 Υπηρεσίες Συστήματος

Τα Windows XP λειτουργούν με πολλές υπηρεσίες οι οποίες ξεκινούν αυτόματα κατά την εκκίνηση του συστήματος.[90] Αυτές οι υπηρεσίες καταναλώνουν πόρους και μπορεί να παρουσιάσουν τρωτά σημεία στον υπολογιστή υπηρεσίας. Όλες οι περιττές υπηρεσίες θα πρέπει να απενεργοποιούνται για να μειωθεί ο αριθμός των μέσων επίθεσης εναντίον του συστήματος. Στα διαχειριζόμενα περιβάλλοντα το GPO (Group Policy Object) θα πρέπει να χρησιμοποιηθεί για τη διαμόρφωση των υπηρεσιών στα συστήματα˙ σε άλλα περιβάλλοντα οι υπηρεσίες μπορούν να τερματιστούν μεμονωμένα στο κάθε σύστημα. Και για τις δύο μεθόδους διαμόρφωσης, κάθε υπηρεσία σε κάποιο σύστημα μπορεί να διαμορφωθεί με ένα από τους παρακάτω τρείς τύπους εκκίνησης:

- **Αυτόματος.** Η υπηρεσία ξεκινά αυτομάτως. Αυτό σημαίνει ότι η υπηρεσία τρέχει όποτε το σύστημα είναι σε λειτουργία.

- **Χειροκίνητος.** Η υπηρεσία ξεκινά μόνο από το σύστημα και όταν αυτό είναι απαραίτητο. Στην πράξη πολλές υπηρεσίες που έχουν αναδιαμορφωθεί στο Χειροκίνητο τύπο, δεν θα ξεκινήσουν όταν χρειάζεται˙ για παράδειγμα εάν το Print Spooler είναι ρυθμισμένο στο Χειροκίνητο, δεν θα ξεκινήσει όταν κάποιος χρήστης προσπαθήσει να εκτυπώσει ένα έγγραφο. Επίσης εάν μία υπηρεσία εξαρτάται από κάποια άλλη υπηρεσία η οποία είναι ρυθμισμένη στο Χειροκίνητο, η πρώτη μπορεί λανθασμένα να υποθέσει ότι η δεύτερη τρέχει ήδη.[91]

- **Απενεργοποιημένος.** Το σύστημα δεν μπορεί να εκκινήσει την υπηρεσία.

Το NIST προτείνει την απενεργοποίηση των παρακάτω υπηρεσιών σε όλα τα περιβάλλοντα, εκτός εάν υπάρχει κάποια συγκεκριμένη ανάγκη η οποία απαιτεί την ενεργοποίησή τους:

---

[90]Περισσότερες πληροφορίες για συγκεκριμένες υπηρεσίες, δείτε το έγγραφο *Windows Server 2003 System Services Reference*, στη διεύθυνση http://www.microsoft.com/technet/prodtechnol/windowsserver2003/techref/sptcgsss.mspx.

[91] Εξαιτίας αυτών των ζητημάτων, η NIST προτείνει τον ορισμό του τύπου εκκίνησης υπηρεσίας ενός συστήματος σε Χειροκίνητο, μόνο εάν ο Χειροκίνητος είναι ο εκ προεπιλογής τύπος εκκίνησης της υπηρεσίας.

- Alerter[92]
- ClipBook
- FTP Publishing Service
- IIS Admin Service
- Messenger
- NetMeeting Remote Desktop Sharing
- Routing and Remote Access
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Management Protocol (SNMP) Service
- Simple Network Management Protocol (SNMP) Trap
- Simple Service Discovery Protocol (SSDP) Discovery Service
- Telnet
- World Wide Web Publishing Services

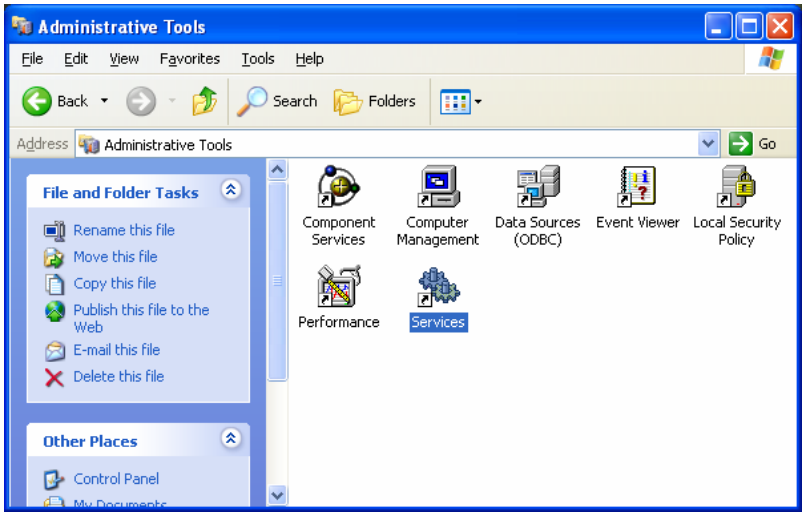
Καθένα από τα πρότυπα ασφάλειας του NIST απενεργοποιεί όλες αυτές τις υπηρεσίες. Επιπρόσθετα τα πρότυπα αυτά απενεργοποιούν και άλλες υπηρεσίες όπως οι Computer Browser, Fax, Indexing Service, Remote Desktop Help Session Manager, Task Scheduler, Terminal Services και Universal Plug and Play Device Host, μόνο για συγκεκριμένα περιβάλλοντα. Μπορεί να αποτελέσει πρόκληση, ιδίως για περιβάλλοντα enterprise, το να διευκρινιστεί ποίες υπηρεσίες μπορούν να απενεργοποιηθούν ασφαλώς. Κάποιες συγκεκριμένες υπηρεσίες μπορεί να χρειάζονται μόνο για κάποιες ειδικές εφαρμογές. Η στρατηγική η οποία υποστηρίζει καλύτερα τη λειτουργικότητα είναι να δοκιμάζεται η κάθε υπηρεσία που φαίνεται να είναι περιττή, ρυθμίζοντάς την σε κατάσταση Απενεργοποιημένης εκκίνησης, και έπειτα να δοκιμάζονται όλες οι εφαρμογές. Στο Παράρτημα Α συμπεριλαμβάνεται λίστα με ενσωματωμένες υπηρεσίες (built-in services) τις οποίες απενεργοποιούν τα πρότυπα του NIST.

Για να αλλάξουμε την κατάσταση εκκίνησης κάποιας συγκεκριμένης υπηρεσίας ακολουθούμε τα παρακάτω βήματα:

1. Από το μενού εκκίνησης **Start** επιλέγουμε το **Control Panel**.

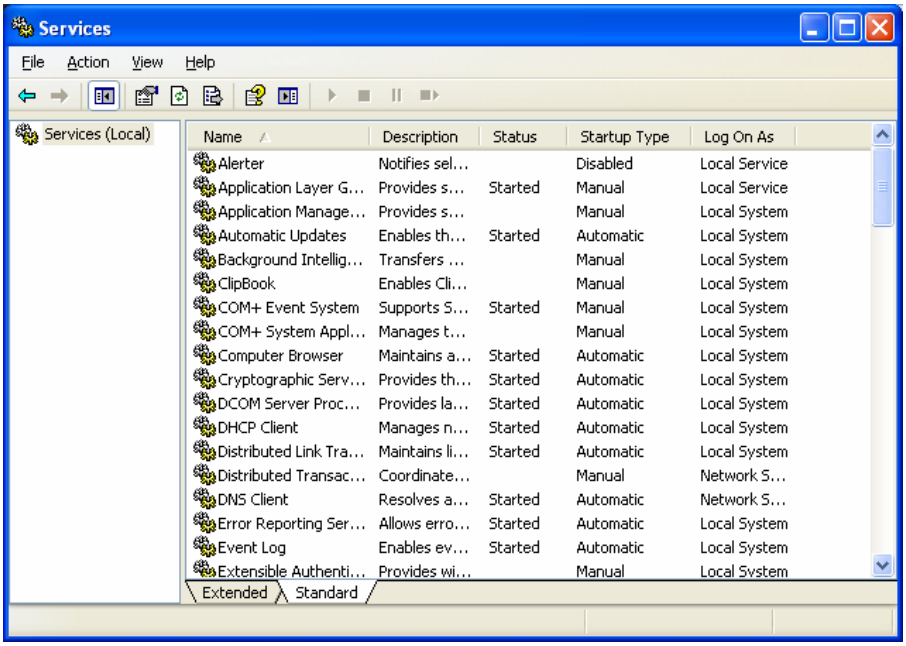
2. Επιλέγουμε **Administrative Tools** και έπειτα **Services**.

[92] Τα Windows XP SP2 απενεργοποιούν αυτή την υπηρεσία εξ' ορισμού. Αυτές οι υπηρεσίες είναι προορισμένες για τη θέαση ειδοποιήσεων και πληροφοριών. Για παράδειγμα κάποιος διαχειριστής θα μπορούσε να στείλει ένα μήνυμα σε όλους τους χρήστες, προειδοποιώντας τους ότι ένας συγκεκριμένος εξυπηρετητής είναι ανενεργός λόγω συντήρησης. Δυστυχώς αυτές οι υπηρεσίες έχουν υποστεί κακή χρησιμοποίηση από επιτιθέμενους και spammers για να παράγουν μηνύματα στις οθόνες των χρηστών. Μία περιγραφή αυτού του ζητήματος είναι διαθέσιμη σε αυτή τη διεύθυνση: http://support.microsoft.com/?id=330904. Το τείχος προστασίας των Windows XP περιορίζει κάποιες από τις πόρτες του Messenger εκ προεπιλογής, έτσι ώστε να μπορούν μόνο να δέχονται πακέτα με διεύθυνση πηγής του τοπικού υποδικτύου, το οποίο μπορεί να βοηθήσει στον κατευνασμό της κακής χρησιμοποίησης αυτών των ζητημάτων εάν οι υπηρεσίες είναι απαραίτητες για διαχειριστικούς σκοπούς σε enterprise περιβάλλον.



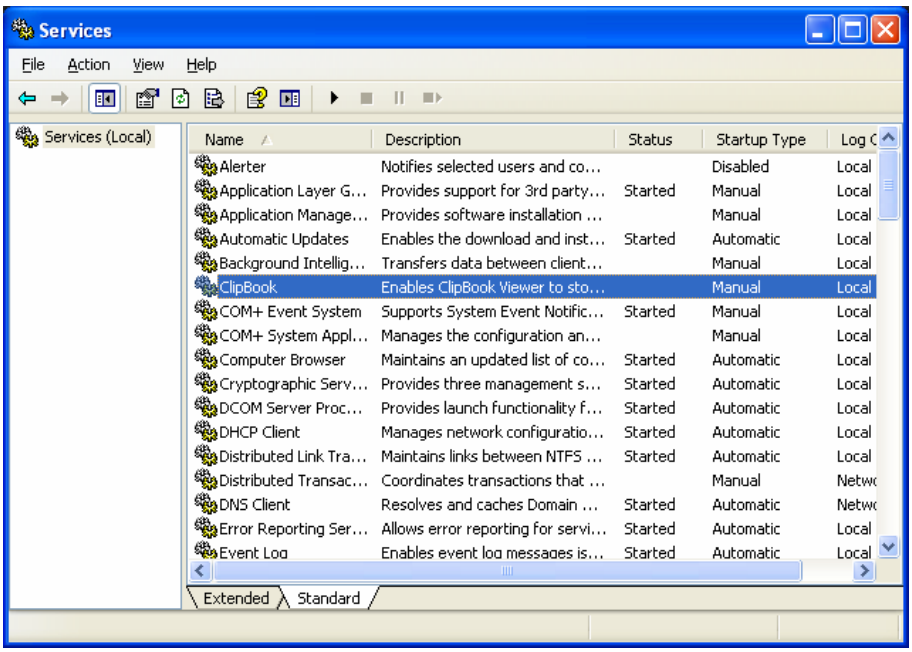
Εικόνα 6-9. Administrative Tools – Services.

3. Κάνουμε κλικ στην καρτέλα θέασης **Standard** που βρίσκεται κάτω αριστερά του παραθύρου.



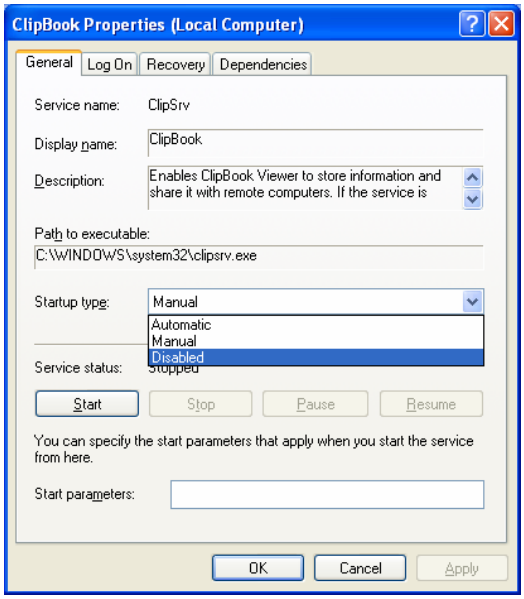
Εικόνα 6-10. Services.

4. Κάνουμε διπλό κλικ στο όνομα της υπηρεσίας (πχ, ClipBook).



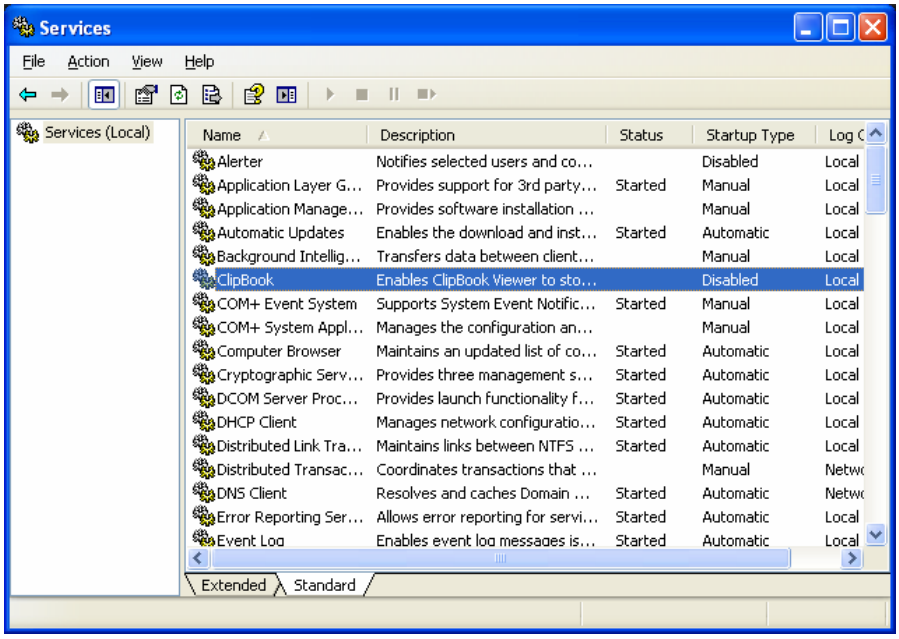
Εικόνα 6-11. Clipbook ορισμένο στο Manual.

5. Εάν η υπηρεσία θα πρέπει να τεθεί στο Manual ή στο Disabled, κάνουμε κλικ στο κουμπί **Stop**, εάν η υπηρεσία έχει ξεκινήσει.



Εικόνα 6-12. Clipbook Properties.

6. Θέτουμε το Startup type σε **Automatic**, **Manual** ή **Disabled** και πατάμε **OK**.



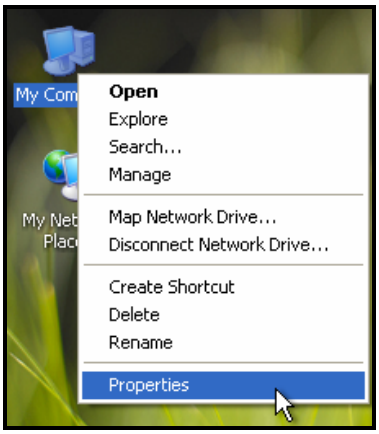
Εικόνα 6-13. Clipbook ορισμένο στο Disabled.

7. Εξερχόμαστε από το εργαλείο **Computer Management**.

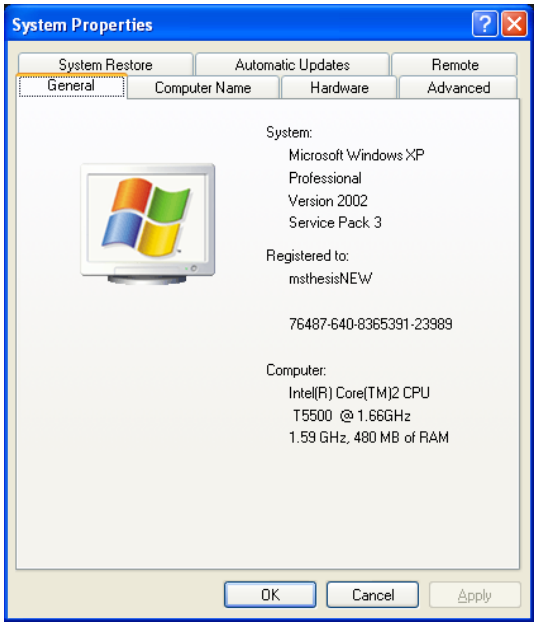
Για την απενεργοποίηση του χαρακτηριστικού Universal Plug and Play, ακολουθούμε τα παραπάνω βήματα για τις υπηρεσίες SSDP Discovery Service και Universal Plug and Play (UPnP) Device Host Service.

Η διαδικασία για την απενεργοποίηση των λειτουργιών Remote Assistance και Remote Desktop είναι διαφορετική από αυτή της απενεργοποίησης άλλων υπηρεσιών. Παρότι αυτές οι λειτουργίες είναι χρήσιμες για υποστήριξη, επιπλέον εκθέτουν τον υπολογιστή σε επιθέσεις βάσει δικτύου. Έτσι, εκτός αν υπάρχει απαίτηση του οργανισμού να τις έχει ενεργοποιημένες, για την διαμόρφωσή τους ακολουθούμε τα παρακάτω βήματα:

1. Κάνουμε δεξί κλικ στο **My Computer** και επιλέγουμε **Properties**.

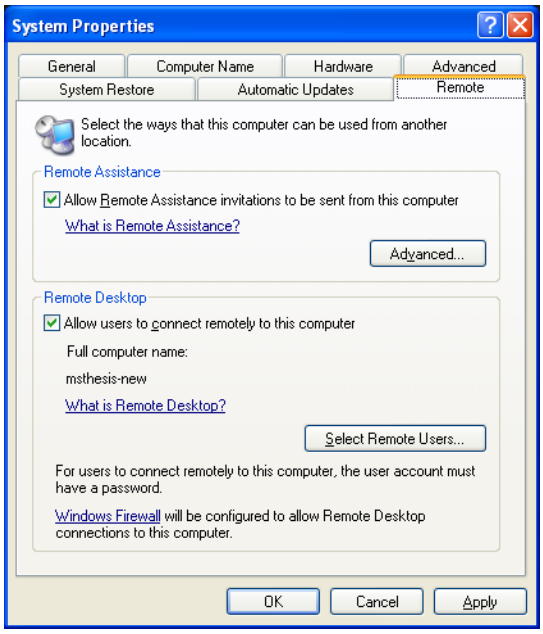


Εικόνα 6-14. My Computer Properties.

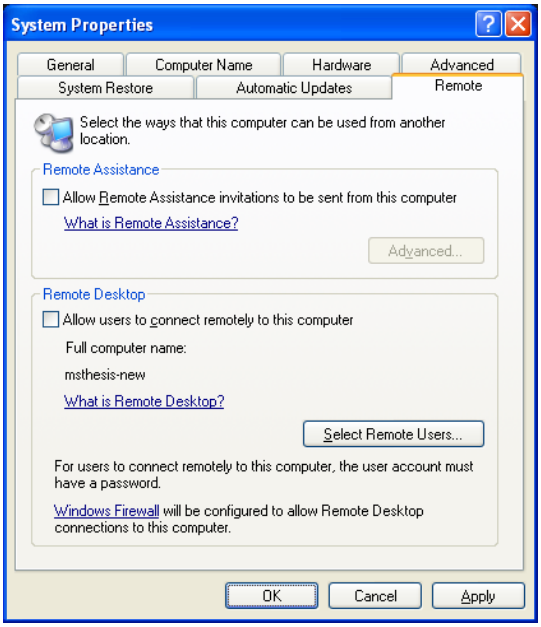


Εικόνα 6-15. System Properties – General.

2. Επιλέγουμε την καρτέλα **Remote** και αφαιρούμε τις επιλογές **Allow Remote Assistance invitations to be sent from this computer** και **Allow users to connect remotely to this computer** από τα αντίστοιχα check boxes. Πατάμε **OK**.



Εικόνα 6-16. System Properties – Remote.



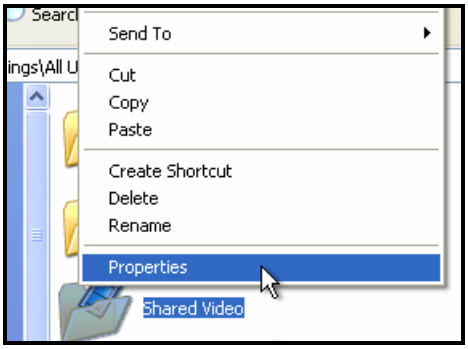
Εικόνα 6-17. System Properties – Remote customized.

6.6 Δικαιώματα Αρχείων

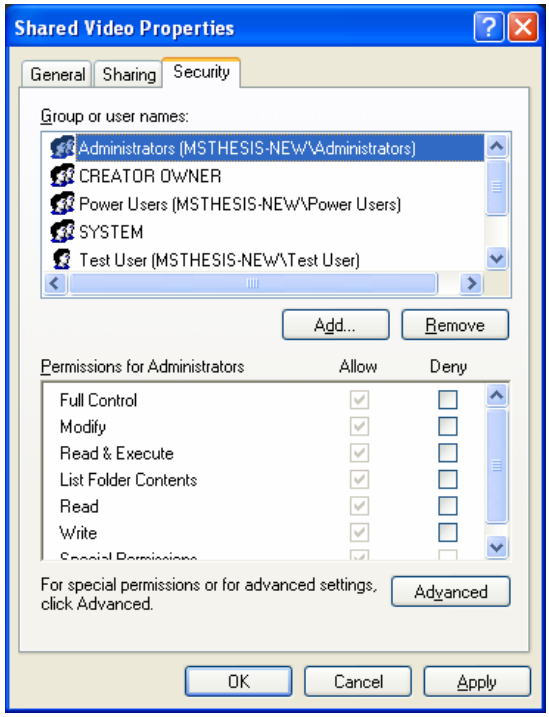
Αυτή η ενότητα παρέχει γενικές οδηγίες όσον αφορά τη ρύθμιση των δικαιωμάτων μέσω του συστήματος αρχείων καταχωρίσεων ελέγχου πρόσβασης (access control entries [ACE]) και λιστών ελέγχου πρόσβασης (access control lists [ACL]) για τα Windows XP.[93] Τα πρότυπα ασφάλειας του NIST περιορίζουν την πρόσβαση σε περισσότερα από 30 εκτελέσιμα αρχεία, προστατεύοντάς τα από μη-εξουσιοδοτημένη διαμόρφωση και χρήση. Επίσης μπορούν να προστεθούν προσαρμοσμένες ρυθμίσεις, οι οποίες είναι σχετικές με το περιβάλλον στο οποίο ανήκει το Windows XP μηχάνημα. Αλλαγές σε κάποιο ACL για κάποια συγκεκριμένη πηγή, όπως ένα αρχείο ή ένας φάκελος, μπορούν να γίνουν χρησιμοποιώντας μία από τις τρείς πιθανές μεθόδους:

- Ανοίγουμε το παράθυρο **Properties** κάποιας πηγής από το περιβάλλον μενού και κάνουμε κλικ στην καρτέλα **Security**. Μας δείχνει τα προνόμια που έχει κάθε χρήστης ή ομάδα σε αυτή την πηγή.

[93] Το ACE είναι μία καταχώριση που δεσμεύει ένα security identifier (SID) με ένα σύνολο από δικαιώματα μέσα σε μία ACL. Περισσότερα: http://msdn.microsoft.com/en-us/library/aa374868.aspx.



Εικόνα 6-18. Shared Folder Properties.



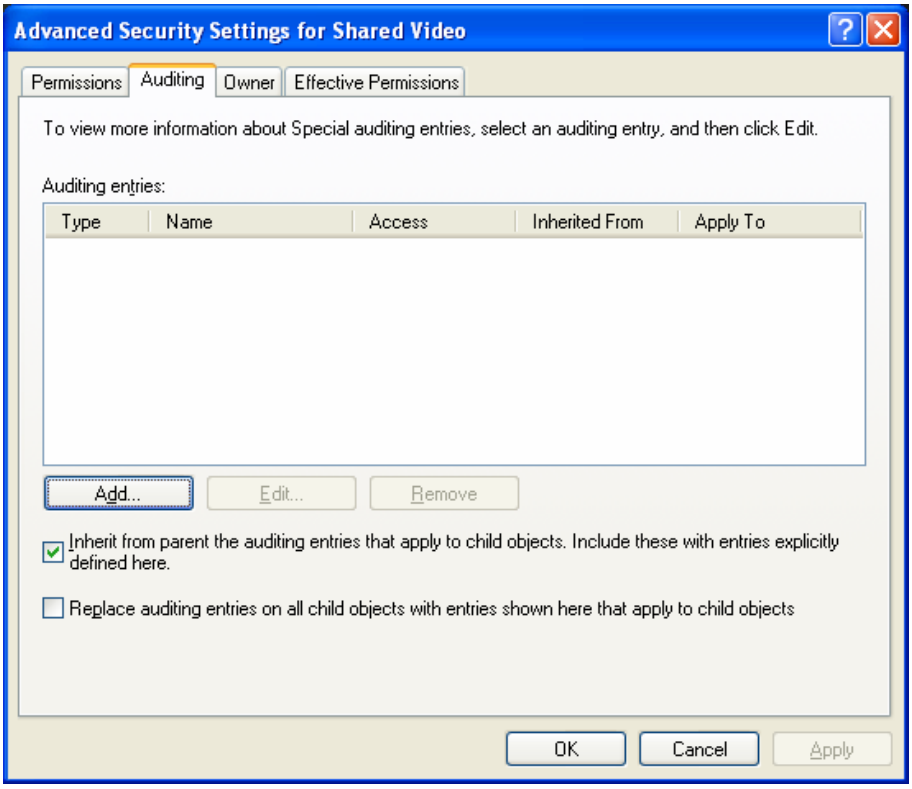
Εικόνα 6-19. Shared Folder Properties – Security.

Το κουμπί **Advanced** μπορεί να χρησιμοποιηθεί για να θέσει περισσότερα δικαιώματα granular permission και επιπρόσθετες ρυθμίσεις όπως τον έλεγχο αρχείου (file auditing) και τον ιδιοκτήτη της πηγής.[94]

Παρακάτω παρατίθεται παράδειγμα απόδοσης δικαιωμάτων για το χρήστη Test User.

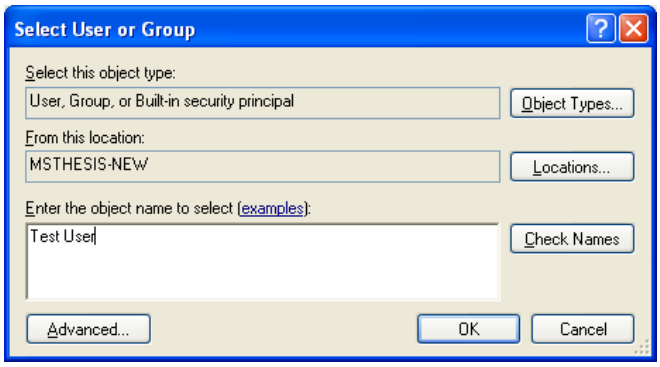
1. Πατάμε **Add** για να προσθέσουμε το χρήστη που επιθυμούμε.

[94] Η μέθοδος αυτή μπορεί να υλοποιηθεί μόνο με ανενεργή την επιλογή Simple File Sharing (Start\My Computer\Folder Options\View\Use Simple File Sharing).



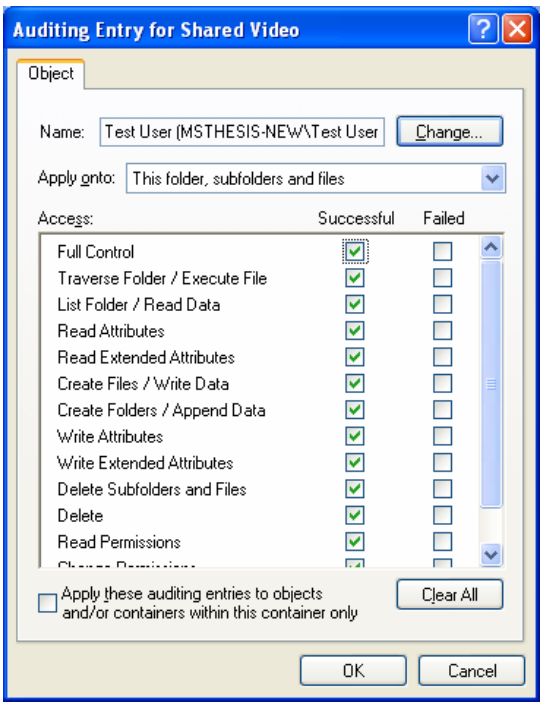
Εικόνα 6-20. Απόδοση δικαιωμάτων βήμα 1ο.

2. Θέτουμε το όνομα του επιθυμητού χρήστη.



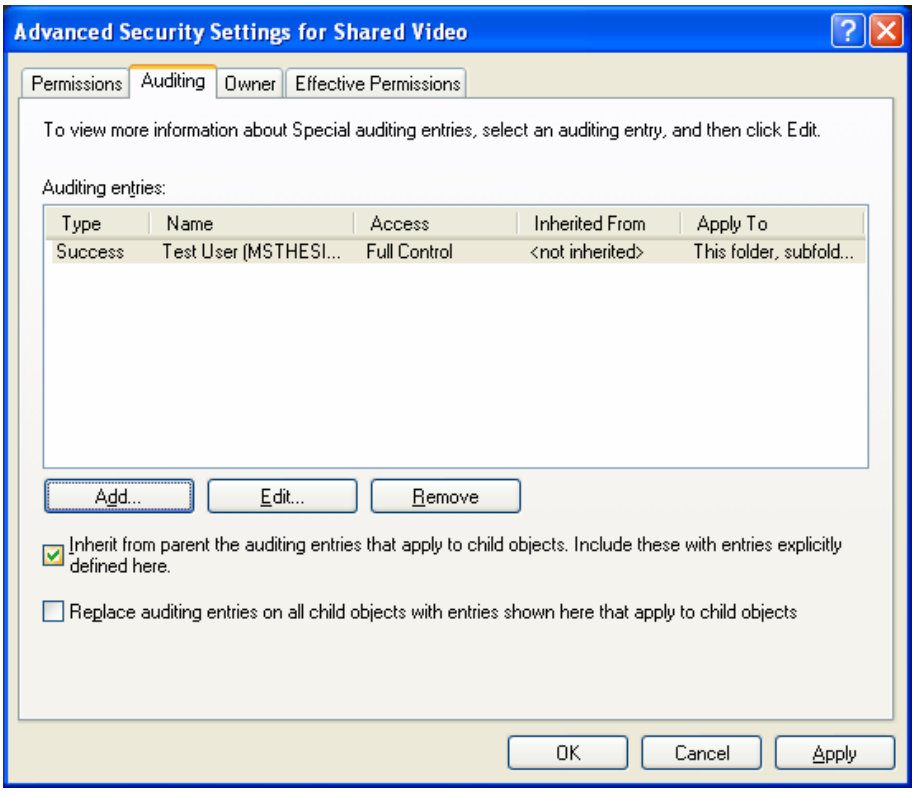
Εικόνα 6-21. Απόδοση δικαιωμάτων βήμα 2ο.

3. Επιλέγουμε τα δικαιώματα που θα του αποδοθούν για τον συγκεκριμένο κατάλογο και πατάμε **OK**.



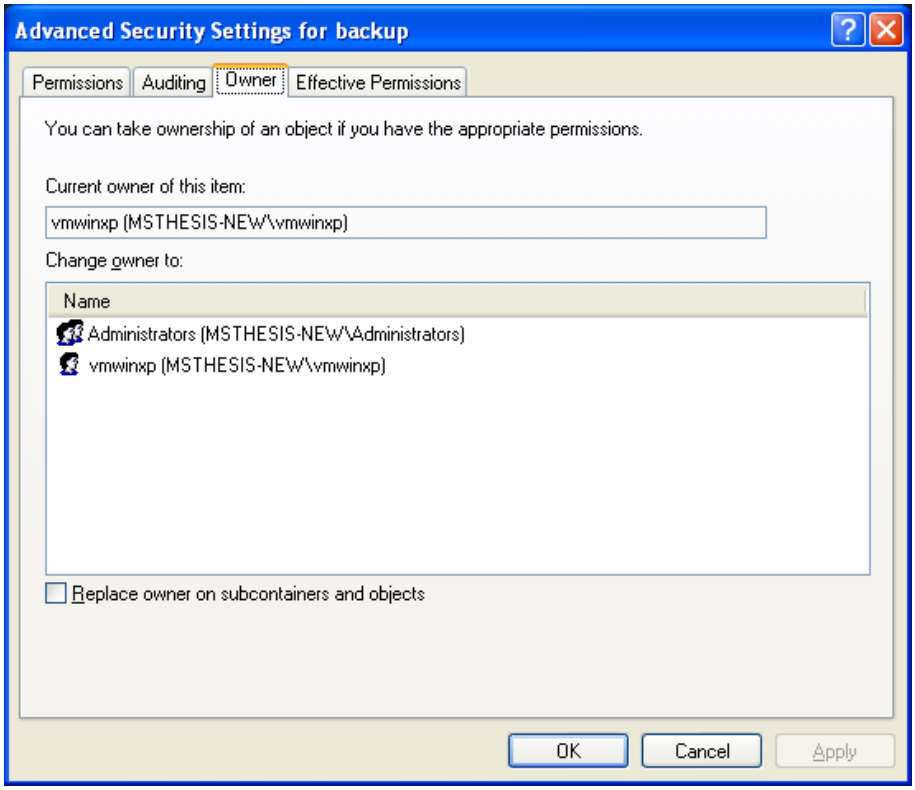
Εικόνα 6-22. Απόδοση δικαιωμάτων βήμα 3ο.

4. Δόθηκε επιτυχώς ο πλήρης έλεγχος στον κατάλογο για το χρήστη Test User.



Εικόνα 6-23. Απόδοση δικαιωμάτων βήμα 4ο.

5. Παρατηρούμε ότι ο ιδιοκτήτης του καταλόγου είναι ο χρήστης vmwinxp.

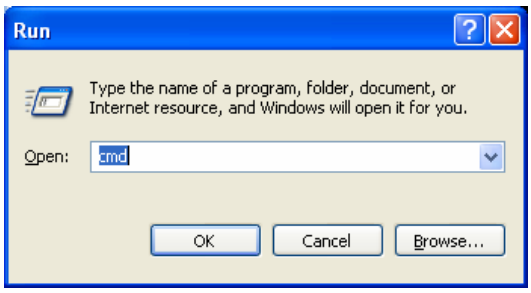


Εικόνα 6-24. Απόδοση δικαιωμάτων βήμα 5ο.

- Χρησιμοποιούμε τη λειτουργία cacls.exe[95] που βρίσκεται στο %SystemRoot%\system32.[96] Αυτή είναι μία διεπαφή γραμμής εντολών που χρησιμοποιείται για να ορίσει τις ACLs κάποιου αρχείου, αλλά δεν ορίζει τα security descriptors[97] των Windows XP.

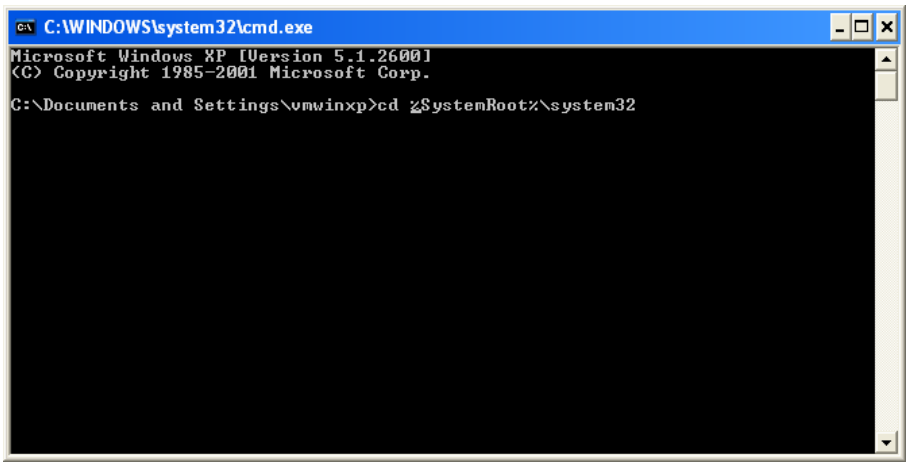
    1. Ανοίγουμε το command prompt των Windows XP. Από το menu **Start** επιλέγουμε **Run** πληκτρολογούμε **cmd**.

[95] Παραδείγματα και διευκρινίσεις για το cacls utility: http://www.ss64.com/nt/cacls.html.
[96] Το **%SystemDrive%** αναφέρεται στο διαμέρισμα του δίσκου στον οποίο έχει γίνει η εγκατάσταση των Windows XP, τυπικά στον δίσκο C:\. Το **%SystemRoot%** αναφέρεται στο φάκελο του **%SystemDrive%** όπου έχουν εγκατασταθεί τα αρχεία των Windows XP, τυπικά το φάκελο **Windows**.
[97] Περισσότερα για τα security descriptors objects μπορείτε να βρείτε εδώ: http://msdn.microsoft.com/en-us/library/aa394577.aspx.



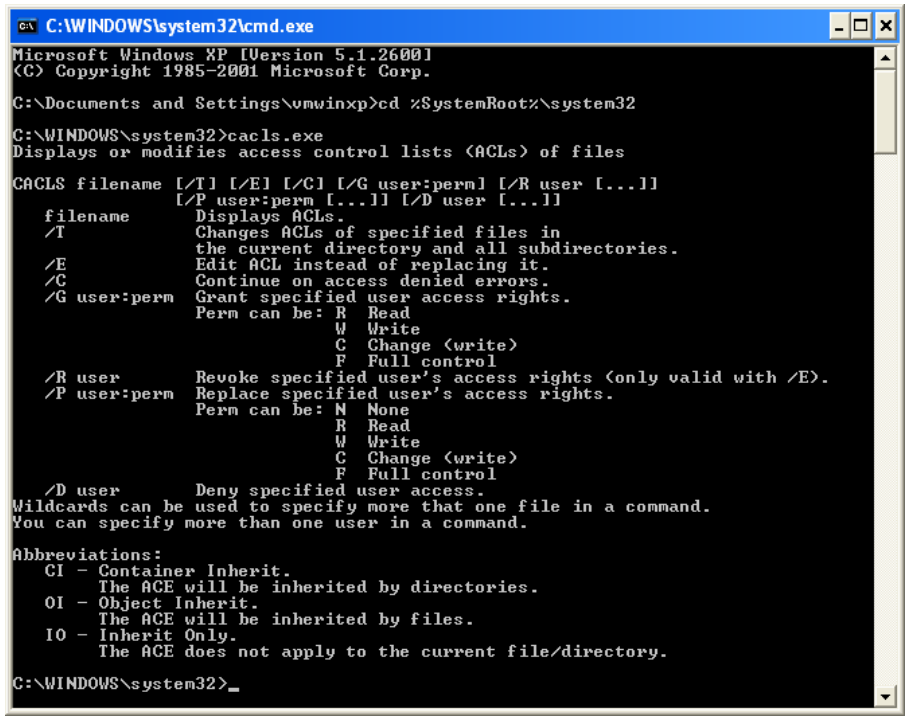
Εικόνα 6-25. Command Prompt.

2. Πάμε στο φάκελο system32 που βρίσκεται στο SystemRoot directory πληκτρολογώντας **cd %SystemRoot%\system32**.



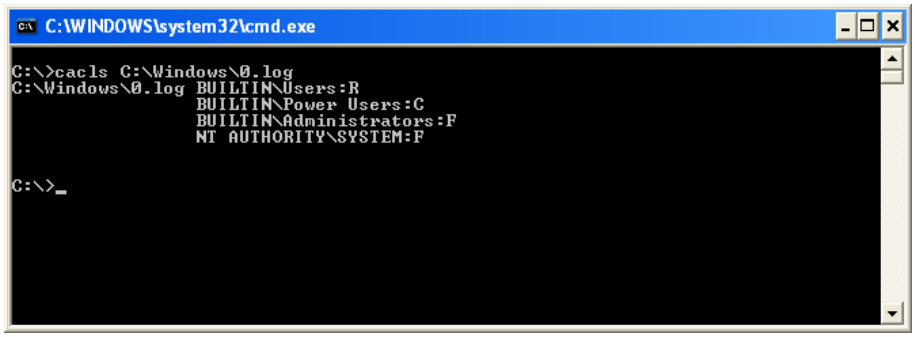
Εικόνα 6-26. Cacls βήμα 1ο.

3. Πληκτρολογούμε cacls.exe και ανοίγουν οι οδηγίες χρησιμοποίησης της λειτουργίας.



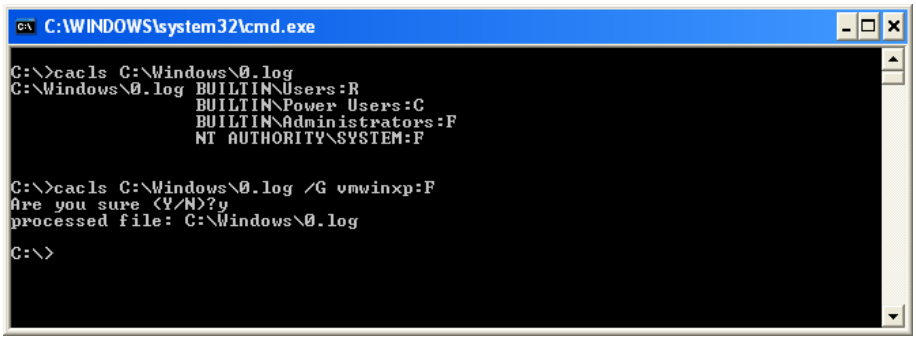
Εικόνα 6-27. Cacls βήμα 2ο.

4. Μπορούμε να δούμε την ACL ενός αρχείου πληκτρολογώντας **cacls filepath**.



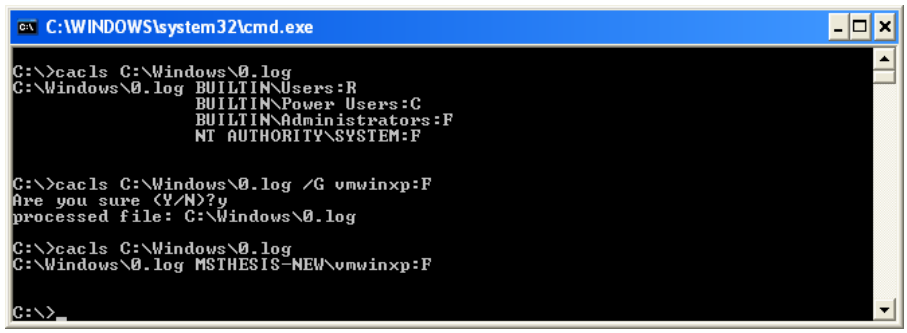
Εικόνα 6-28. Cacls βήμα 3ο.

5. Εδώ δώσαμε πλήρη έλεγχο (perm=F) στο χρήστη vmwinxp στο αρχείο 0.log.



Εικόνα 6-29. Cacls βήμα 4ο.

6. Βλέπουμε ξανά την ACL του ίδιου αρχείου και επιβεβαιώνουμε την αλλαγή της.



Εικόνα 6-30. Cacls βήμα 5ο.

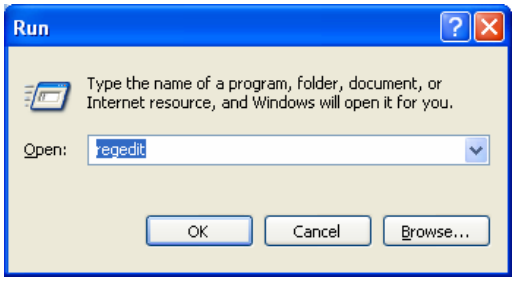
- Χρησιμοποιούμε το snap-in MMC Security Template για να εφαρμόσουμε τις ρυθμίσεις από κάποιο πρότυπο, με τον τρόπο που περιγράφηκε στην ενότητα 5.2.

6.7 Δικαιώματα Μητρώου

Τα Windows XP έχουν επίσης δικαιώματα και για το μητρώο (registry). Τα πρότυπα του NIST δεν περιέχουν καθόλου δικαιώματα μητρώου, αλλά οι διαχειριστές θα πρέπει να θέσουν περιορισμένα δικαιώματα για διάφορα registry keys και values για την προστασία τους από μη-εξουσιοδοτημένη πρόσβαση και τροποποίηση. Η αλλαγή στα δικαιώματα του μητρώου μπορεί να επηρεάσει αρνητικά τη λειτουργικότητα και την ευστάθεια των Windows XP συστημάτων, γι' αυτό οι διαχειριστές θα πρέπει να δοκιμάζουν προσεκτικά κάθε τέτοιο δικαίωμα προτού να τα χρησιμοποιήσουν σε συστήματα παραγωγής.

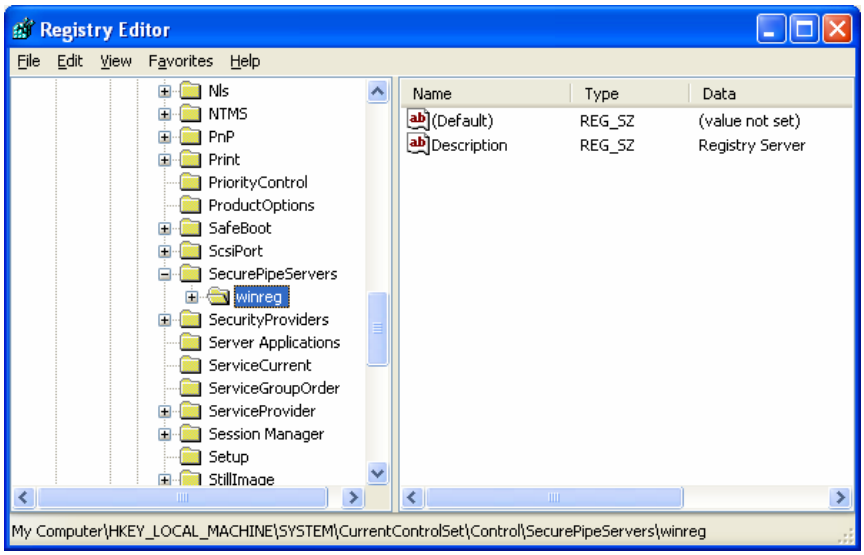
Εξ' ορισμού, το δικαίωμα μεταχείρισης του μητρώου είναι περιορισμένο, αλλά λόγω της αξίας του είναι σημαντικό να επιβεβαιώσουμε ότι είναι προστατευμένο. Για να το κάνουμε αυτό ακολουθούμε τα παρακάτω βήματα:

1. Πατάμε **Start** και επιλέγουμε **Run**. Πληκτρολογούμε **regedit** και πατάμε **OK**.



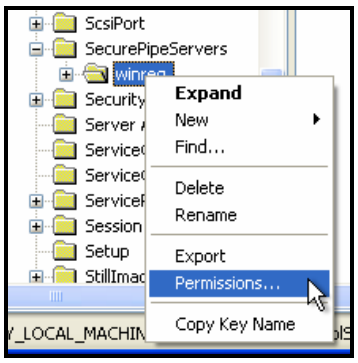
Εικόνα 6-31. Registry Editor.

2. Εντοπίζουμε το key **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg**.

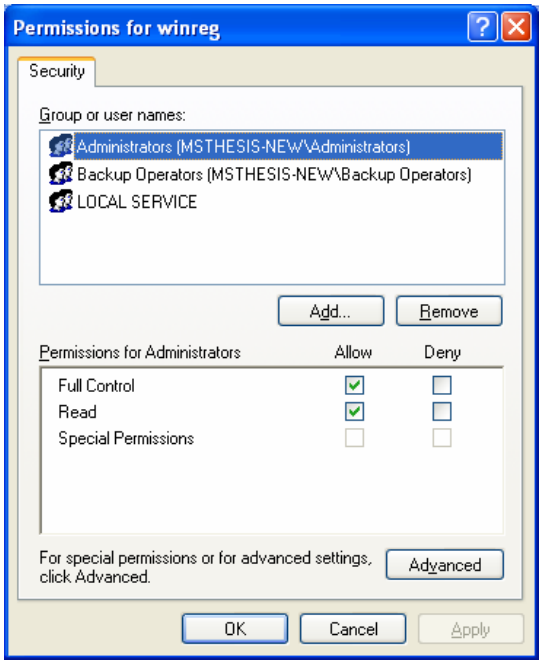


Εικόνα 6-32. Registry Editor – winreg.

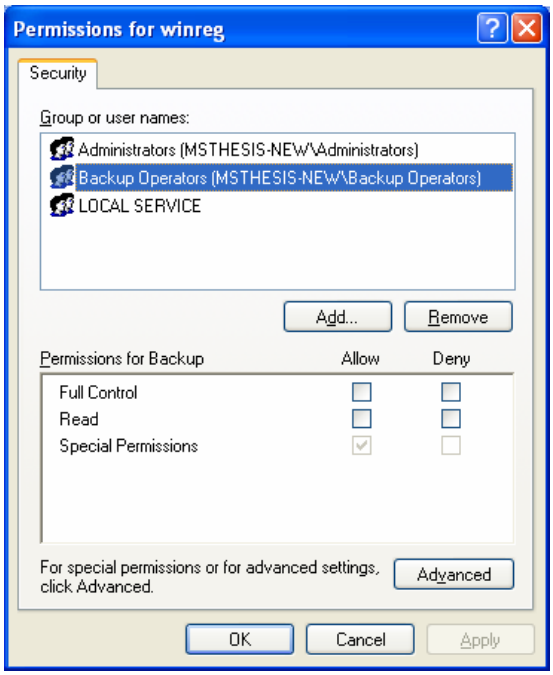
3. Κάνουμε δεξί κλικ στο **winreg** και επιλέγουμε **Permissions**. Επιβεβαιώνουμε ότι μόνο ο διαχειριστής(**Administrator**) έχει πλήρη έλεγχο (**Full Control**), η ομάδα **Backup Operators** δεν έχει κανένα δικαίωμα (εκτός των ειδικών δικαιωμάτων Query Value, Enumerate Subkeys, Notify και Read Control) και το **LOCAL SERVICE** έχει μόνο **Read** δικαιώματα.



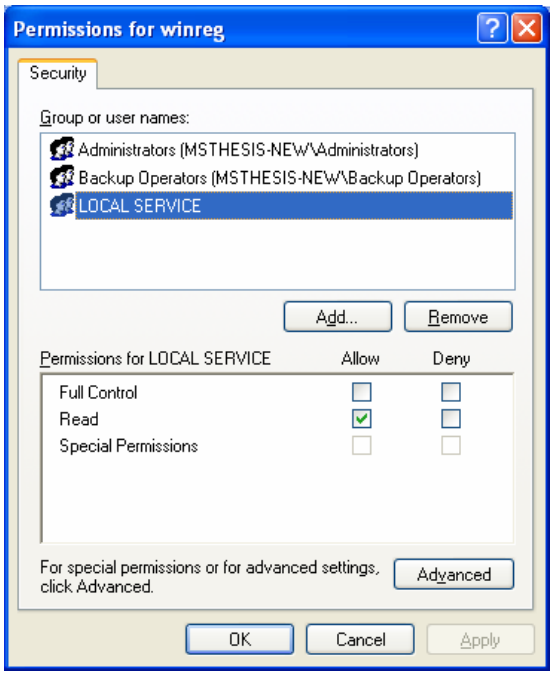
Εικόνα 6-33. Winreg Permissions A.



Εικόνα 6-34. Winreg Permissions B.



Εικόνα 6-35. Winreg Permissions C.



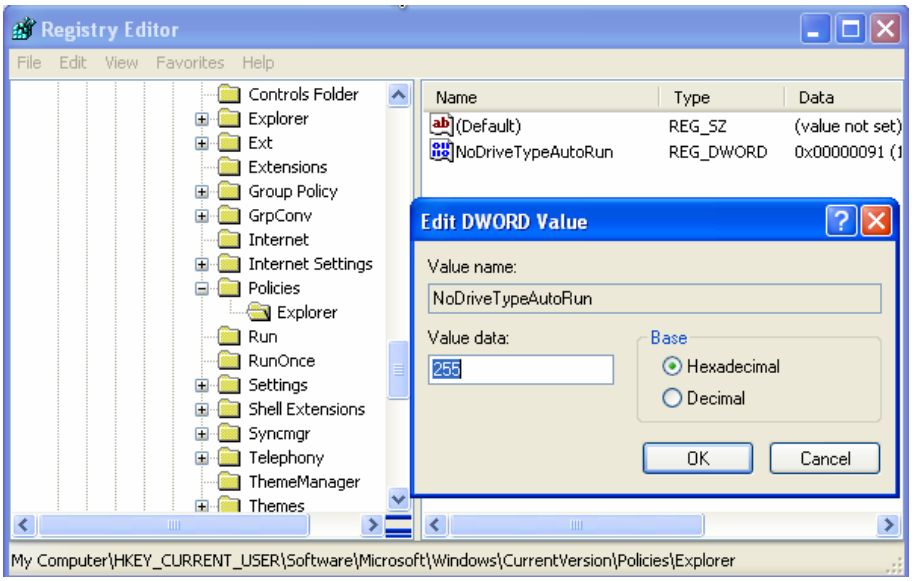
Εικόνα 6-36. Winreg Permissions D.

6.8 Τιμές Μητρώου

Τα πρότυπα του NIST ορίζουν τιμές για διάφορα registry keys που δεν προαναφέρθηκαν σε αυτή την ενότητα. Τα ακόλουθα αντικείμενα παρέχουν το όνομα και το μονοπάτι του registry key, περιγράφουν το σκοπό του και προτείνουν μία κατάλληλη ρύθμιση.

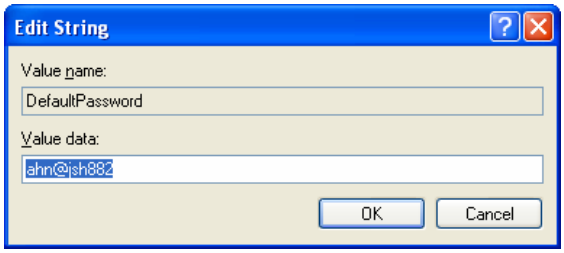
6.8.1 *Αυτόματες Λειτουργίες*

- **HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun**.[98] Η λειτουργία autorun επιχειρεί να εκτελέσει αυτόματα το περιεχόμενο από ένα CD όταν αυτό τοποθετείται μέσα στο σύστημα. Εάν το CD έχει κακόβουλο περιεχόμενο τότε αυτό μπορεί να εκτελεστεί αυτόματα. Θέτοντας το registry value στο 255 απενεργοποιεί τη λειτουργία αυτόματης εκτέλεσης για όλους τους τύπους των οδηγών (drives).



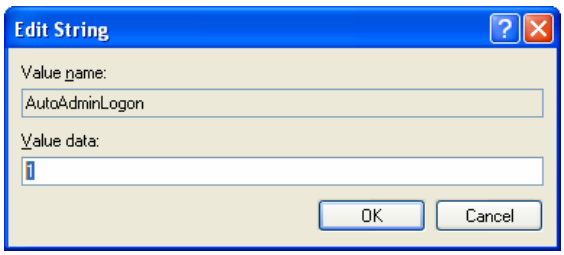
Εικόνα 6-37. NoDriveTypeAutoRun.

- **HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\AutoAdminLogon.**[99] Εάν είναι ενεργοποιημένη αυτή η registry value επιτρέπει την παράκαμψη της πρόσβασης στο σύστημα χρησιμοποιώντας ένα κωδικό πρόσβασης που είναι αποθηκευμένος σε cleartext[100] μέσα στο μητρώο.



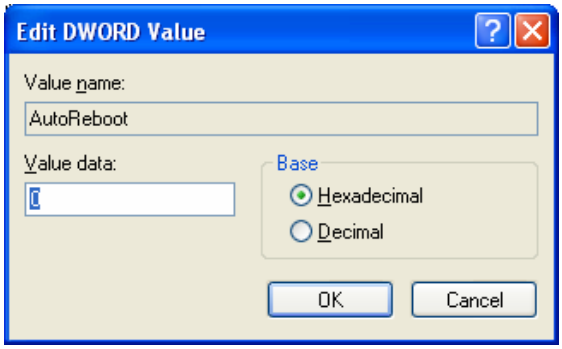
Εικόνα 6-38. AutoAdminLogon cleartext.

[98] Το HKLM είναι συντομογραφία του HKEY_LOCAL_MACHINE.
[99] Εάν δεν υπάρχει αυτή η καταχώριση, τη δημιουργούμε πατώντας Edit\New\String Value και στο value name πληκτρολογούμε AutoAdminLogon. http://support.microsoft.com/kb/315231.
[100] Το cleartext φαίνεται στην Εικόνα6-38. Περισσότερα: http://en.wikipedia.org/wiki/Cleartext.



Εικόνα 6-39. AutoAdminLogon.

- **HKLM\System\CurrentControlSet\Control\CrashControl\AutoReboot.** Η ενεργοποίηση της λειτουργίας AutoReboot, προκαλεί την αυτόματη επανεκκίνηση του συστήματος μετά από αποτυχία ή κλείδωμά του. Κάποιοι αυτό το θεωρούν ανεπιθύμητο από άποψη ασφάλειας και λειτουργικότητας. Για παράδειγμα εάν πραγματοποιηθεί μία αποτυχία συστήματος και το σύστημα προκαλέσει την επανεκκίνησή του, ο χρήστης μπορεί να μην έχει επίγνωση ενός λειτουργικού προβλήματος ή μία παραβίασης ασφάλειας που πραγματοποιήθηκαν. Αυτή η λειτουργία μπορεί να απενεργοποιηθεί θέτοντας την τιμή 0.



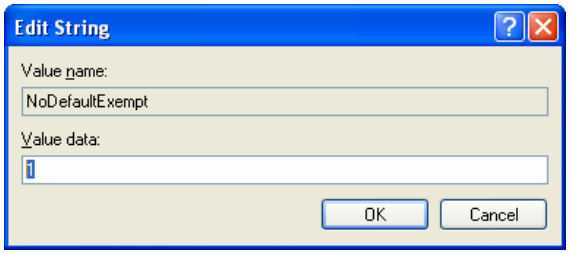
Εικόνα 6-40. AutoReboot.

6.8.2 *Δικτύωση*

Οι ρυθμίσεις που περιγράφτηκαν σε αυτή την ενότητα τροποποιούν τις ρυθμίσεις στοίβας του Microsoft TCP/IP και άλλων πλευρών της δικτύωσης των Windows XP.

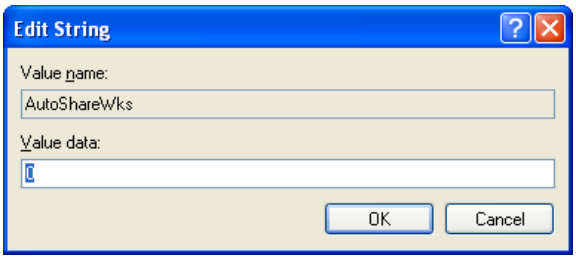
- **HKLM\System\CurrentControlSet\Services\IPSec\NoDefaultExempt.** Στα Windows XP το IPSec έχει ορισμένες εξ' ορισμού εξαιρέσεις στα φίλτρα πολιτικής του. Αυτή η παράμετρος συνήθως θα πρέπει να είναι ορισμένη στην τιμή 1, όπου αφαιρεί τις εξαιρέσεις για τα Kerberos και RSVP traffic.[101]

[101] Περισσότερα για αυτή τη ρύθμιση θα βρείτε εδώ: http://support.microsoft.com/?id=810207.



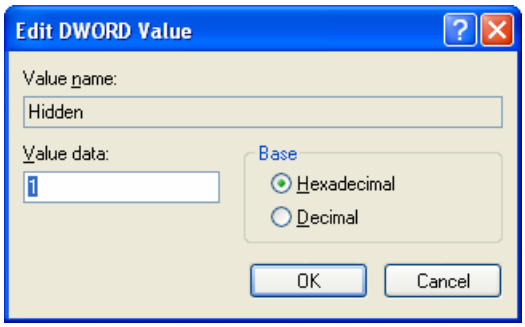
Εικόνα 6-41. NoDefaultExempt.

- **HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\AutoShareWks.** Εάν χρησιμοποιείται η υπηρεσία File and Printer Sharing για τα Microsoft δίκτυα, τα Windows XP θα διαμοιράσουν όλους τους τοπικούς εγκατεστημένους δίσκους, ως κρυμμένες διαχειριστικές πηγές (πχ C$, D$). Προτείνεται η απενεργοποίηση αυτών των διαμοιρασμών εκτός εάν κρίνεται απαραίτητο. Για παράδειγμα κάποιες εφαρμογές λογισμικού μπορεί να εξαρτώνται από την ύπαρξη κάποιου διαμοιρασμού. Επιπρόσθετα σε συστήματα τα οποία συντηρούνται από απόσταση (remote maintenance) οι διαμοιρασμοί μπορεί να είναι απαραίτητοι για τη διευκόλυνση της διαδικασίας συντήρησης. Εάν ο διαμοιρασμός δεν είναι απαραίτητος, θέτοντας την τιμή της registry ίση με 0, αυτός θα κατασταλεί.



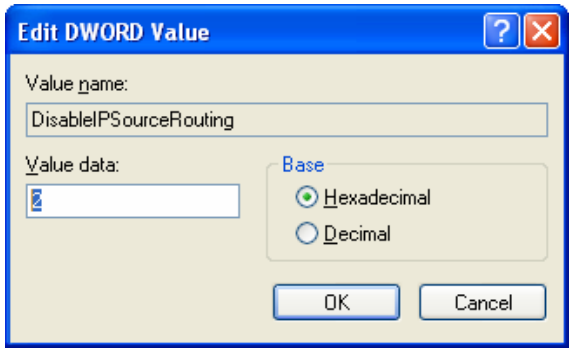
Εικόνα 6-42. AutoShareWks.

- **HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\Hidden.** Θέτοντας σε αυτή την παράμετρο την τιμή 1, εμποδίζεται η υπηρεσία Server του συστήματος από το να στέλνει ανακοινώσεις μέσω browser, το οποίο κάνει το σύστημα κρυφό από τους Browsers των άλλων συστημάτων. Αυτό ελαχιστοποιεί την πιθανότητα κάποιοι άλλοι χρήστης να επιχειρήσουν να πετύχουν πρόσβαση στο σύστημα μέσω Microsoft δικτύωσης.



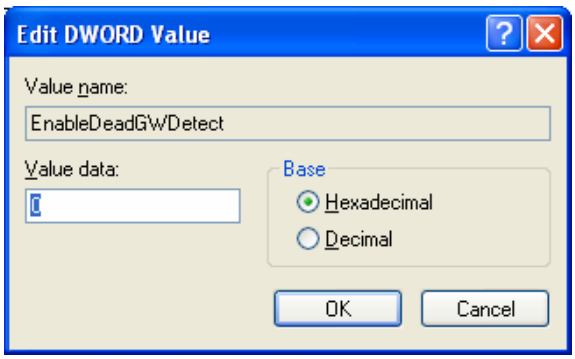
Εικόνα 6-43. Hidden.

- **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting.** Θέτοντας σε αυτή την παράμετρο την τιμή 2, απενεργοποιείται το source routing για το IP πακέτο.[102] Το source routing γενικά δεν έχει κάποιο δικαιολογημένο σκοπό και μπορεί να χρησιμοποιηθεί από επιτιθέμενους για να ανακατευθύνουν πακέτα μέσω κάποιου συγκεκριμένου ενδιάμεσου host. Αυτό θα μπορούσε να επιτρέψει στον επιτιθέμενο να δει και να τροποποιήσει δικτυακές επικοινωνίες.



Εικόνα 6-44. DisableIPSourceRouting.

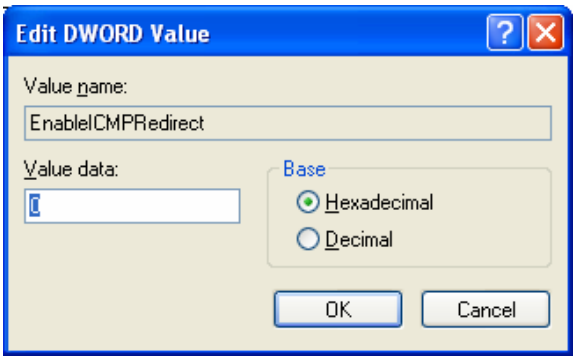
- **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect.** Όταν αυτή η παράμετρος είναι ορισμένη στην τιμή 1, επιτρέπεται στο TCP η δυνατότητα εντοπισμού νεκρού gateway. Με ενεργοποιημένο αυτό το χαρακτηριστικό το TCP μπορεί να ρωτήσει το IP για να αλλάξει σε κάποιο εφεδρικό gateway, εάν κάποιος αριθμός συνδέσεων αντιμετωπίζει δυσκολία. Κάποιος επιτιθέμενος θα μπορούσε να το εκμεταλλευτεί αυτό, εξαπατώντας το σύστημα να χρησιμοποιήσει κακόβουλο gateway και αυτό θα μπορούσε να του επιτρέψει την θέαση και τροποποίηση δεδομένων, ή ακόμα να προκαλέσει την άρνηση της υπηρεσίας (Denial of Service [DoS][103]). Θέτοντας σε αυτή την παράμετρο την τιμή 0, απενεργοποιείται η λειτουργία εντοπισμού νεκρού gateway.



Εικόνα 6-45. EnableDeadGWDetect.

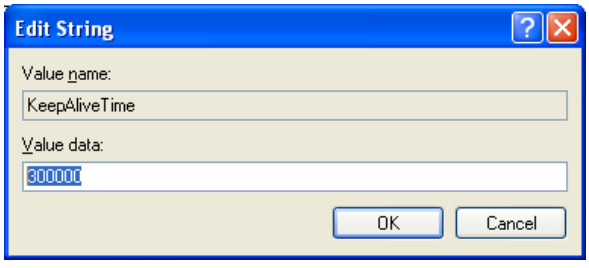
[102]Περισσότερα για το source routing θα βρείτε στη διεύθυνση http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Source_Routing/default.htm.
[103] Επιθέσεις άρνησης υπηρεσίας: http://en.wikipedia.org/wiki/Denial-of-service_attack.

- **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableCMPRedirect.** Εάν είναι ενεργοποιημένη αυτή η λειτουργία, τα Windows XP αλλάζουν τον πίνακα δρομολόγησης τους, σε απάντηση των μηνυμάτων ανακατεύθυνσης ICMP[104] που του αποστέλλονται από συσκευές δικτύου, όπως δρομολογητές. Οι επιτιθέμενοι μπορούν να υποκλέψουν (spoofing) τα μηνύματα ανακατεύθυνσης ICMP για να εξαπατήσουν τα συστήματα να δρομολογήσουν τα πακέτα προς το σύστημα του επιτιθέμενου (ή και αλλού), το οποίο θα μπορούσε να επιτρέψει σε τρίτους να αναχαιτίσουν ευαίσθητες πληροφορίες, να παραβιάσουν το σύστημα, ή να προκαλέσουν την άρνηση της υπηρεσίας [DoS]. Θέτοντας σε αυτή την παράμετρο την τιμή 0, απενεργοποιείται αυτή η λειτουργία.



Εικόνα 6-46. EnableCMPRedirect.

- **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime.** Αυτή είναι μία παράμετρος η οποία ελέγχει το πόσο συχνά το TCP προσπαθεί να επαληθεύσει ότι μία αδρανής σύνδεση είναι ακόμα ανέπαφη, στέλνοντας ένα keep-alive πακέτο.[105] Εάν το απομακρυσμένο σύστημα είναι ακόμα προσπελάσιμο και λειτουργικό, ενημερώνει το keep-alive σύστημα μετάδοσης. Τα keep-alive πακέτα δεν στέλνονται εκ προεπιλογής. Αυτή η λειτουργία μπορεί να ενεργοποιηθεί για μία σύνδεση από κάποια εφαρμογή. Το πρότυπο specialized security-limited functionality του NIST θέτει το χρονισμό του keep-alive στα 300,000 milliseconds (5 λεπτά).



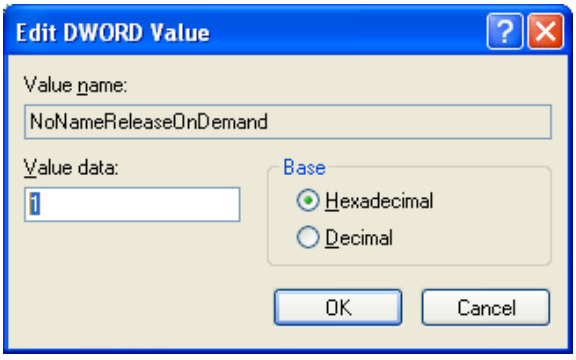
Εικόνα 6-47. KeepAliveTime.

---

[104] Περισσότερα για τα ICMP Redirects θα βρείτε στο άρθρο της CISCO, *When Are ICMP Redirects Sent?*, που είναι διαθέσιμο στη διεύθυνση http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094702.shtml.

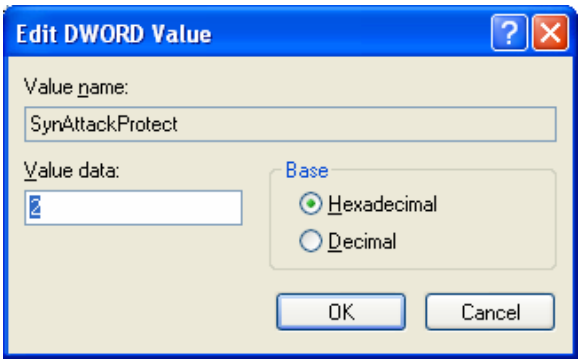
[105] Για τα keep-alive πακέτα δείτε εδώ: http://tldp.org/HOWTO/TCP-Keepalive-HOWTO/overview.html.

- **HKLM\System\CurrentControlSet\Services\Netbt\Parameters\NoName ReleaseOnDemand.** Αυτή η παράμετρος καθορίζει εάν ένας υπολογιστής κοινοποιεί το NetBIOS[106] όνομά του όταν λαμβάνει αιτήσεις κοινοποίησης ονόματος από το δίκτυο. Θέτοντας την τιμή 1, εμποδίζει το σύστημα από το να κοινοποιεί το όνομά του, το οποίο προστατεύει το σύστημα από κακόβουλες επιθέσεις κοινοποίησης ονόματος αλλά μπορεί επίσης να βλάψει και κανονικές εργασίες.



Εικόνα 6-48. NoName ReleaseOnDemand.

- **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect.** Αυτή η λειτουργία ενεργοποιεί την προστασία σε SYN flood επιθέσεις.[107] Εάν οι τιμές της registry TcpMaxHalfOpen και TcpMaxHalfOpenRetried έχουν οριστεί κατάλληλα, αυτή η λειτουργία μειώνει τις προσπάθειες αναμετάδοσης και τη δημιουργία καθυστερημένων καταχωρίσεων λανθάνουσας μνήμης δρομολόγησης (route cache entry [RCE][108]). Θέτοντας αυτή την παράμετρο στην τιμή 1 ή 2 ενεργοποιείται η προστασία σε SYN flood επιθέσεις˙ με την τιμή 2 παρέχεται σθεναρότερη προστασία από όταν θέσουμε την τιμή 1.

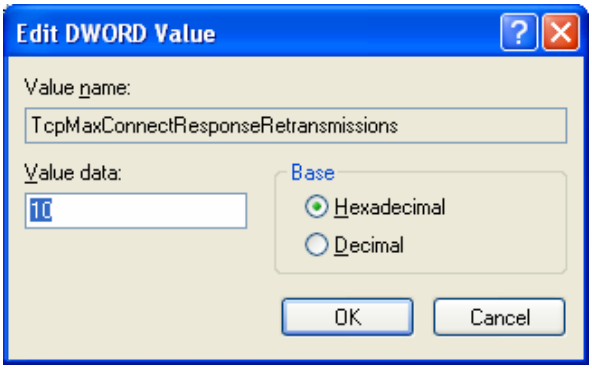


Εικόνα 6-49. SynAttackProtect.

---

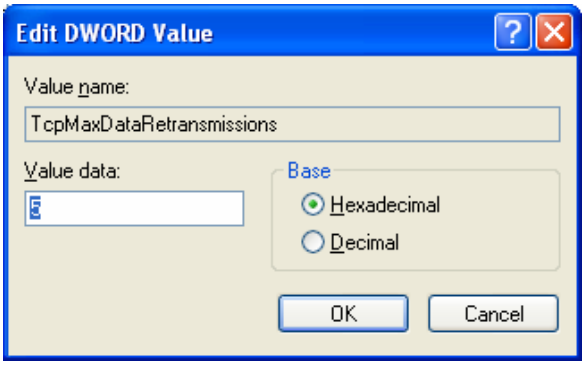
[106] Περισσότερα για το NETBIOS name θα βρείτε εδώ: http://technet.microsoft.com/en-us/library/cc738412.aspx.
[107] Για τις SYN flood attacks μπορείτε να αντλήσετε πληροφορίες από τη διεύθυνση http://www.iss.net/security_center/advice/Exploits/TCP/SYN_flood/default.htm.
[108] Πληροφορίες για τα RCE μπορείτε να αντλήσετε από εδώ: http://freesoft.org/CIE/RFC/1122/55.htm.

- **HKLM\System\CurrentControlSet\Services\Tcpip\TcpMaxConnect ResponseRetransmissions.** Εδώ ορίζεται το πόσες φορές θα αναμεταδίδει το TCP ένα SYN-ACK πακέτο[109] το οποίο δεν έχει επιβεβαιωθεί.



Εικόνα 6-50. TcpMaxConnectResponseRetransmissions.

- **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMax DataRetransmissions.** Εδώ ορίζεται το πόσες φορές θα αναμεταδίδει το TCP ένα πακέτο το οποίο δεν έχει επιβεβαιωθεί από μία πλήρως εγκαθιδρυμένη σύνδεση.



Εικόνα 6-51. TcpMaxDataRetransmissions.

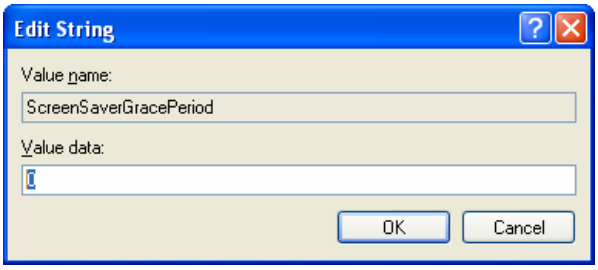
6.8.3 *Άλλες Ρυθμίσεις Προτύπου*

Αυτές οι ρυθμίσεις αντιστοιχούν σε άλλα registry keys που έχουν οριστεί μέσα στα πρότυπα, αλλά δεν εμπίπτουν στις κατηγορίες των ενοτήτων 6.8.1 και 6.8.2.

- **HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\ ScreenSaverGracePeriod.** Αυτή η τιμή ορίζει την περίοδο χάριτος ανάμεσα στην ενεργοποίηση μίας προστασίας οθόνης που απαιτεί κωδικό προστασίας και στην απαίτηση του συστήματος για εισαγωγή του κωδικού για το ξεκλείδωμά του. Ορίζοντας αυτή την τιμή ίση με 0, εξαλείφεται η περίοδος χάριτος.

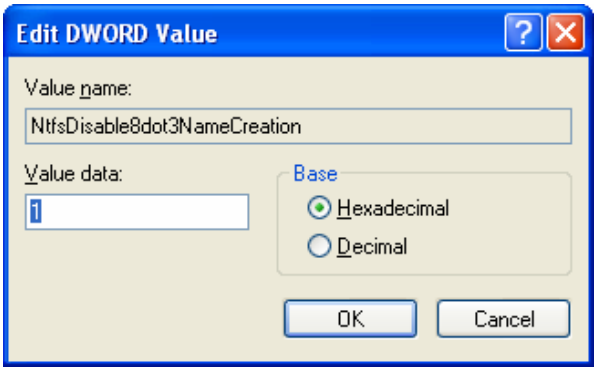
---

[109] Περισσότερες πληροφορίες για τα SYN-ACK πακέτα μπορείτε να βρείτε στη διεύθυνση http://www.faqs.org/docs/iptables/synackandnew.html.



Εικόνα 6-52. ScreenSaverGracePeriod.

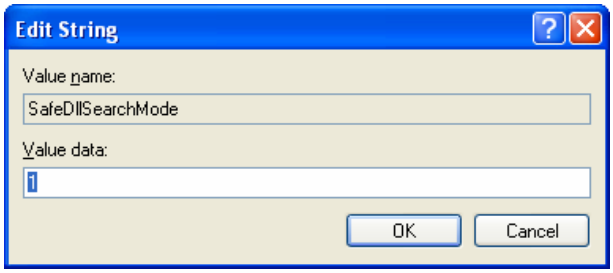
- **HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation.** Ορίζοντας αυτή την τιμή ίση με 1, απενεργοποιείται η αυτόματη δημιουργία συμβατών ονομάτων αρχείων (legacy filenames), σε ntfs 8.3 διαμόρφωση.[110]



Εικόνα 6-53. NtfsDisable8dot3NameCreation.

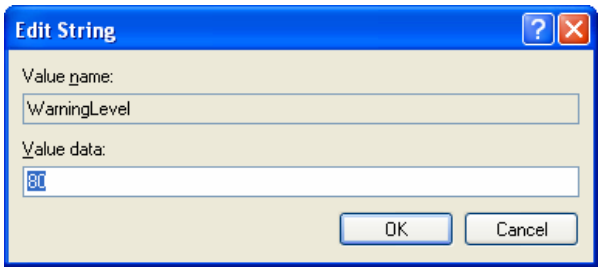
- **HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode.** Τα Windows XP ψάχνουν καταλόγους με μία συγκεκριμένη ιεράρχηση όταν αναζητούν να εκτελέσουν ένα αρχείο. Εκ προεπιλογής τα Windows ψάχνουν τον τρέχοντα κατάλογο, πριν από τον κατάλογο Windows και τους καταλόγους του συστήματος. Θέτοντας σε αυτή την παράμετρο την τιμή 1, τα Windows πλέον θα εκτελούν την αναζήτηση στον κατάλογο Windows και στους καταλόγους του συστήματος, πριν από τον τρέχοντα κατάλογο. Αυτή είναι καλύτερη πρακτική ασφάλειας διότι ο τρέχον κατάλογος μπορεί να είναι πιο περιοριστικό από τους καταλόγους του συστήματος και από αυτόν των Windows. Για παράδειγμα, κάποιος κακόβουλος χρήστης θα μπορούσε να τοποθετήσει σε ένα σύστημα ένα Trojan horse σε έναν διαμοιρασμένο κατάλογο. Εάν χρησιμοποιείται η εκ προεπιλογής ιεραρχία αναζήτησης, κάποιος άλλος χρήστης ο οποίος προσπαθεί να εκτελέσει ένα πρόγραμμα με το ίδιο όνομα, θα μπορούσε ακούσια να εκτελέσει το Trojan horse αντί του επιθυμητού. Εάν χρησιμοποιείται η προτεινόμενη ιεραρχία αναζήτησης το Trojan horse δεν θα μπορέσει να εκτελεστεί.

[110] NTFS 8.3 filenames: http://en.wikipedia.org/wiki/8.3_filename.



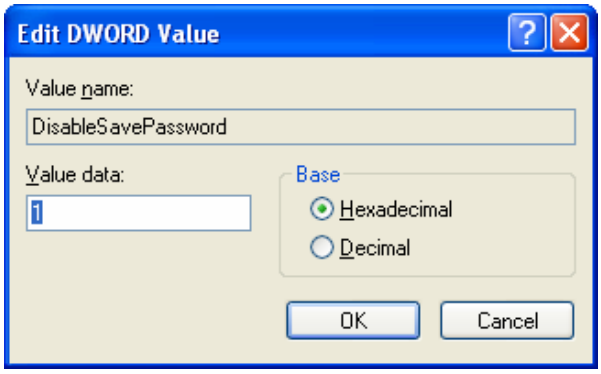
Εικόνα 6-54. SafeDllSearchMode.

- **HKLM\System\CurrentControlSet\Services\EventLog\Security\WarningLevel.** Αυτή η τιμή αντιστοιχεί στο ποσοστό του μέγιστου μεγέθους της αναφοράς γεγονότων ασφάλειας. Όταν αυτό το μέγεθος προσεγγίσει το καθορισμένο ποσοστό, το σύστημα εκδίδει μία προειδοποίηση.



Εικόνα 6-55. WarningLevel.

- **HKLM\System\CurretnControlSet\Services\RasMan\Parameters\DisableSavePassword.** Θέτοντας σε αυτή την παράμετρο την τιμή 1 αποτρέπεται η αποθήκευση των κωδικών ασφάλειας από το Network Connections phone book, που χρησιμοποιούνται για απομακρυσμένη πρόσβαση. [111]



Εικόνα 6-56. DisableSavePassword.

[111] Αναβάθμιση του Connection Manager Phone Book: http://support.microsoft.com/kb/323775.

Για αυτές τις τιμές μητρώου, οι επακριβείς υποδείξεις για τις ρυθμίσεις των προτύπων του NIST είναι προσδιορισμένες στον πίνακα A-5 του Παραρτήματος A.

6.8.4 *Ρυθμίσεις Εκτός των Προτύπων του NIST*

Ο πίνακας 6-2 απαριθμεί επιπρόσθετες τιμές μητρώου σχετικές με την ασφάλεια, οι οποίες δεν είναι ορισμένες στα πρότυπα του NIST.

Πίνακας 6-2. Επιπρόσθετες Registry Values[112]

Αντικείμενο	Όνομα και Μονοπάτι της Τιμής Μητρώου	Προτεινόμενη Τιμή[113]	Περιγραφή
1	HKLM\Software\Microsoft \DrWatson\CreateCrashDump	0	Θέτοντας αυτή την τιμή ίση με 0, απενεργοποιείται η δημιουργία memory dump αρχείων από το πρόγραμμα Dr. Watson debugger.[114] Τα αρχεία memory dump μπορεί να εμπεριέχουν ευαίσθητα δεδομένα όπως κωδικοί ασφάλειας. Αυτή η ρύθμιση μπορεί να ενεργοποιηθεί για επίλυση επαναλαμβανόμενων προβλημάτων.
2	HKLM\Software\Microsoft \Windows NT\CurrentVersion\AEDebug\ Auto	0	Θέτοντας αυτή την τιμή ίση με το 0 απενεργοποιείται το πρόγραμμα Dr. Watson.
3	HKLM\System\CurrentContro lSet \Services\CDrom\Autorun	0	Θέτοντας αυτή την τιμή ίση με 0 απενεργοποιείται η λειτουργία αυτόματης εκτέλεσης για τα CDs.
4	HKLM\System\CurrentContro lSet \Services\MrxSmb\Parameters \RefuseReset	Μη ορισμένη	Θέτοντας σε αυτή την παράμετρο την τιμή 1 προκαλείται η άγνοια του συστήματος για τα πλαίσια ResetBrowser.[115] Αυτά τα πλαίσια μπορούν να χρησιμοποιηθούν για να τερματίσουν το NetBIOS και τους κύριους browsers, και να ανακηρύξουν έναν υπολογιστή σαν νέο κύριο browser. Παλαιότερες εκδόσεις των Windows μπορούσαν να δεχτούν επιθέσεις μέσω των ResetBrowser πλαισίων.
5	HKLM\System\CurrentContro lSet \Services\Tcpip\Parameters \EnablePMTUDiscovery	Μη ορισμένη	Όταν σε αυτή την παράμετρο οριστεί η τιμή 1, το TCP προσπαθεί να ανακαλύψει τη Μονάδα Μέγιστης Μετάδοσης (Maximum Transmission Unit [MTU][116]), το μέγεθος του μεγαλύτερου πακέτου που μπορεί να διατηρηθεί ακέραιο κατά την πορεία του προς κάποιο απομακρυσμένο host. Θέτοντας την

[112] Αυτές οι ρυθμίσεις δεν θα εμφανιστούν στο snap-in του MMC, Security Templates.
[113] Οι προτεινόμενες αυτές τιμές δίνονται και για τα τέσσερα πρότυπα του NIST που περιγράψαμε.
[114] Περιγραφή του Dr. Watson: http://support.microsoft.com/kb/308538.
[115] Σχετικό patch της Microsoft: http://www.microsoft.com/technet/security/bulletin/ms00-036.mspx.
[116] Maximum Transmission Unit: http://en.wikipedia.org/wiki/Maximum_transmission_unit.

			τιμή ίση με 0 απενεργοποιείται αυτή η λειτουργία και προκαλείται τη χρησιμοποίηση μίας MTU των 576 bytes που χρησιμοποιείται από όλες τις συνδέσεις που δεν είναι εγκαθιδρυμένες με τα hosts σε ένα τοπικό υποδίκτυο.
6	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery	0	Αυτή η παράμετρος ελέγχει το κατά πόσο το σύστημα θα προσπαθεί να εκτελέσει την ανακάλυψη δρομολογητών ανά RFC 1256[117] σε βάση ανά-διεπαφών. Αυτό το χαρακτηριστικό θα πρέπει να είναι απενεργοποιημένο θέτοντας την τιμή του ίση με 0.
7	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen	100	Αυτή η ρύθμιση καθορίζει τον αριθμό των επιτρεπτών συνδέσεων στην κατάσταση SYN-RCVD[118] πριν την εφαρμογή των μέτρων SynAttackProtect.
8	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetried	80	Αυτή η ρύθμιση καθορίζει τον αριθμό των επιτρεπτών συνδέσεων στην κατάσταση SYN-RCVD για τις οποίες τουλάχιστον μία αναμετάδοση του πακέτου SYN έχει αποσταλεί πριν την εφαρμογή των μέτρων SynAttackProtect.
9	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TCPMaxPortsExhausted	5	Αυτή η ρύθμιση καθορίζει το πόσες αιτήσεις σύνδεσης μπορούν να απορριφθούν πριν την εφαρμογή των μέτρων SynAttackProtect.

6.9 Σύνοψη και Υποδείξεις

- ✓ Εδραίωση πολιτικών λογαριασμών οι οποίες μειώνουν την πιθανότητα κάποιος επιτιθέμενος να εικάσει ή να σπάσει κωδικούς ασφάλειας και να πετύχει μη-εξουσιοδοτημένη πρόσβαση σε συστήματα. Οι πολιτικές θα πρέπει να εξισορροπούν ασφάλεια, λειτουργικότητα και χρηστικότητα.

- ✓ Διαμόρφωση του ελέγχου πολιτικής για να καταγράφονται σε αναφορές συγκεκριμένοι τύποι δραστηριότητας, έτσι ώστε να μπορούν να επιθεωρούν οι διαχειριστές του συστήματος αυτές τις αναφορές και να εντοπίζουν μη-εξουσιοδοτημένη δραστηριότητα.

- ✓ Ανάθεση δικαιωμάτων χρήστη ακολουθώντας την αρχή των ελαχίστων δικαιωμάτων.

- ✓ Ορισμός επιπρόσθετων επιλογών ασφάλειας για την επίτευξη μεγαλύτερης ασφάλειας απ' ότι παρέχουν οι εξ' ορισμού επιλογές· παραδείγματα εμπεριέχουν τον περιορισμό χρήσης κενών κωδικών ασφάλειας, μετονομασία των εκ

[117] IRDP: ICMP Router Discovery Protocol: http://www.javvin.com/protocolIRDP.html.
[118] Περισσότερα για τις επιτρεπτές συνδέσεις ενός HTTP server μπορείτε να βρείτε στη διεύθυνση http://www.cs.rice.edu/CS/Systems/Web-measurement/paper/node3.html.

προεπιλογής λογαριασμών Administrator και Guest, και καθορισμός των τύπων πιστοποίησης που μπορεί να χρειάζονται.

- ✓ Ενεργοποίηση καταγραφής των αναφορών Εφαρμογών, Ασφάλειας και Συστήματος.

- ✓ Απαλοιφή όλων των χρηστών από τις ομάδες Remote Desktop Users και Power Users που δεν χρειάζονται συγκεκριμένως να είναι μέλη.

- ✓ Απενεργοποίηση όλων των μη απαραίτητων υπηρεσιών.

- ✓ Απενεργοποίηση των χαρακτηριστικών Universal Plug and Play και Remote Assistance, εκτός και αν χρειάζονται να είναι ενεργοποιημένα.

- ✓ Χρησιμοποίηση των ACLs για τον περιορισμό της πρόσβασης σε κρίσιμα εκτελέσιμα αρχεία και σε καταχωρίσεις μητρώου.

- ✓ Ορισμός των τιμών μητρώου που περιορίζουν το debugging και την αυτόματη εκτέλεση περιεχομένου CD-ROM, όπως επίσης και ασφαλέστερη διαμόρφωση δικτύωσης.

- ✓ Επιθεώρηση, προσαρμογή, έλεγχος, τεκμηρίωση και επέκταση των προτύπων του NIST για την ασφάλιση των Windows XP συστημάτων.

Βιβλιογραφία

Έντυπη Βιβλιογραφία

Allen R., Richards J., Lowe-Norris A. G. (2006). *Active Directory*. Η.Π.Α.: Εκδόσεις O'Reilly Media Inc.

Smith J., Nair R. (2005). *Virtual Machines: Versatile Platforms for Systems and Processes*. Η.Π.Α.: Εκδόσεις Elsevier Science & Technology.

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

Ηλεκτρονική Βιβλιογραφία

http://csrc.nist.gov/itsec/SP800-68r1.pdf

http://en.allexperts.com/q/Microsoft-Word-1058/2008/8/Alphabetical-sorting-word-2003.htm

http://en.wikipedia.org/wiki/Active_Directory

http://en.wikipedia.org/wiki/Group_Policy

http://technet.microsoft.com/en-us/library/cc779036(WS.10).aspx

http://www.tech-faq.com/active-directory.shtml

http://www.visualwin.com/AD-Controller/

http://www.visualwin.com/AD-XP/

http://www.visualwin.com/New-Computer-AD/

http://www.visualwin.com/New-User-AD/

http://www.windowsnetworking.com/articles_tutorials/Networking-Basics-Part6.html

Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων

Παραρτήματα πτυχιακής εργασίας

Ασφαλής διαχείριση Microsoft Windows XP Professional σύμφωνα με την μεθοδολογία NIST SP 800-68 (Μέρος 2ο)

Κωνσταντίνος Τσέλιος (ΑΜ: 953)
E-mail: epp953@epp.teiher.gr

Ηράκλειο – 14/07/2009

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

Πίνακας Περιεχομένων Παραρτήματος

Πίνακας Περιεχομένων Παραρτήματος ..... **i**
Πίνακας Πινάκων Παραρτήματος ..... **ii**
Παράρτημα A **1**
A. Διαμόρφωση Ασφάλειας Ομοσπονδιακής Αρχής **1**
Παράρτημα B **3**
B. Ασφάλεια του Windows XP Service Pack 3 ..... **3**
Παράρτημα C **4**
C. Χαρτογράφηση των Ελέγχων των Windows XP με το NIST SP 800-53 ..... **4**
C.1 Διαχειριστικοί Έλεγχοι 4
C.2 Λειτουργικοί Έλεγχοι 6
C.3 Τεχνικοί Έλεγχοι 13
Παράρτημα D **19**
D. Συνήθεις Χρησιμοποιούμενες TCP/IP Πόρτες στα Windows XP Συστήματα **19**
Παράρτημα E **21**
E. Εργαλεία **21**
Παράρτημα F **23**
F. Πηγές **23**
F.1 Βάσεις Δεδομένων Ευπάθειας 23
F.2 Λίστες Ηλεκτρονικού Ταχυδρομείου 23
F.3 Έντυπες Πηγές 23
F.4 Σχετικά Εγχειρίδια και Πηγές του NIST 24
F.5 Διαδικτυακές Πηγές της Microsoft 25
F.5.1 Γενικές Πηγές για τα Windows XP *25*
F.5.2 Γενικές Πηγές Ασφάλειας *26*
F.5.3 ΣΤ. 5.3 Γενικές Πηγές για την Ασφάλεια των Windows XP *26*
F.5.4 Συγκεκριμένες Πηγές για την Ασφάλεια των Windows XP *27*
F.5.5 Άρθρα της Microsoft Knowledge Base *29*
F.5.6 Πηγές Σχετικές με το Windows XP SP3 ..... *31*
F.6 Άλλες Διαδικτυακές Πηγές 31
Παράρτημα G **32**
G. Ακρωνύμια και Συντομογραφίες **32**

Πίνακας Πινάκων Παραρτήματος

Πίνακας C-1. Certification, Accreditation, and Security Assessments (CA) Family Controls. 5
Πίνακας C-2. Planning (PL) Family Controls 5
Πίνακας C-3. Risk Assessment (RA) Family Controls. 5
Πίνακας C-4. System and Services Acquisition (SA) Family Controls. 6
Πίνακας C-5. Awareness and Training (AT) Family Controls. 7
Πίνακας C-6. Configuration Management (CM) Family Controls. 7
Πίνακας C-7. Contingency Planning (CP) Family Controls. 9
Πίνακας C-8. Incident Response (IR) Family Controls. 9
Πίνακας C-9. Maintenance (MA) Family Controls. 9
Πίνακας C-10. Media Protection (MP) Family Controls. 10
Πίνακας C-11. Personnel Security (PS) Family Controls. 10
Πίνακας C-12. Physical and Environmental Protection (PE) Family Controls. 11
Πίνακας C-13. System and Information Integrity (SI) Family Controls. 11
Πίνακας C-14. Access Control (AC) Family Controls. 13
Πίνακας C-15. Audit and Accountability (AU) Family Controls. 16
Πίνακας C-16. Identification and Authentication (IA) Family Controls. 16
Πίνακας C-17. System and Communications Protection (SC) Family Controls. 18
Πίνακας D-1. TCP – UDP Ports. 19
Πίνακας E-1. Tools. 21

Παράρτημα Α

Α. Διαμόρφωση Ασφάλειας Ομοσπονδιακής Αρχής

Όπως συζητήθηκε στην ενότητα 5, η συνεργασία του NIST με πολλούς άλλους οργανισμούς για την παραγωγή ενός συνόλου από πρότυπα ασφάλειας για τα Windows XP ανταποκρίνεται σε τέσσερα περιβάλλοντα — enterprise, SOHO, SSLF και legacy. Το NIST επίσης έχει κάνει τα GPOs διαθέσιμα για τις προδιαγραφές των ρυθμίσεων του FDCC.[1] Τα πρότυπα του NIST και τα GPOs του FDCC καθορίζουν παρόμοιες ρυθμίσεις ασφάλειας, συμπεριλαμβανομένου των ακόλουθων κατηγοριών (απαριθμημένες όπως παρουσιάζονται στο Group Policy Editor[2]):

- Account policies: password policies και account security
- Local policies: system audit policy, user rights assignment και security options
- Event log policies
- System services
- File permissions

Υπάρχουν μερικές διαφορές στους τύπους ρυθμίσεων των προτύπων του NIST και των GPOs του FDCC. Τα πρότυπα καθορίζουν ρυθμίσεις Restricted Groups, αλλά τα GPOs όχι. Άλλη μία σημαντική διαφορά είναι ότι το FDCC περιέχει ρυθμίσεις για το Internet Explorer 7 (IE7) και το Windows Firewall.

Περισσότερες πληροφορίες για τη σπουδαιότητα πολλών εκ των ρυθμίσεων είναι διαθέσιμες από το Threats and Countermeasures Guide: Security Settings in Windows Server 2003 and Windows XP[3] της Microsoft, από την ενότητα 6 αυτού του εγχειριδίου και από μία βάση ρυθμίσεων που δημιουργήθηκε από το NIST. Η βάση, που ονομάζεται NIST Windows Security Baseline Database, περιέχει πληροφορίες για όλες τις ρυθμίσεις από τα πρότυπα του NIST και τα FDCC GPOs.[4] Η βάση είναι αυτάρκης έτσι ώστε να μπορεί να καταφορτωθεί και να τρέξει τοπικά. Επιτρέπει στα ενδιαφερόμενα μέρη να παρατηρήσουν τις ρυθμίσεις ανά βασική γραμμή (πχ, Windows XP, IE7) ή ανά πολιτική (πχ, FDCC), όπως επίσης και να συγκρίνουν

[1] Περισσότερες πληροφορίες για το FDCC, συμπεριλαμβανομένου ενός spreadsheet που περιέχει πλήρη λίστα με όλες τις ρυθμίσεις του FDCC, είναι διαθέσιμο στη διεύθυνση http://nvd.nist.gov/fdcc/index.cfm.

[2] Στο διαχειριστικό περιβάλλον του Active Directory, οι ακόλουθες ρυθμίσεις θα πρέπει να είναι καθορισμένες και εφαρμοσμένες σε επίπεδο τομέα: οι ρυθμίσεις Password Policy· οι ρυθμίσεις Account Lockout Policy· η ρύθμιση "Add workstations to domain" στο User Rights Assignment policy· και οι ρυθμίσεις "Microsoft network server: Disconnect clients when logon hours expire", "Network access: Allow anonymous SID/Name translation", and "Network security: Force logoff when logon hours expire" στο Security Options policy.

[3] http://www.microsoft.com/downloads/details.aspx?FamilyId=1B6ACF93-147A-4481-9346-F93A4081EEA8&displaylang=en.

[4] Η βάση περιέχει ένα αντίγραφο των πληροφοριών του FDCC GPO και δεν προτίθεται να γίνει η επίσημη πηγή των FDCC ρυθμίσεων. Η επίσημη πηγή των πληροφοριών της FDCC διαμόρφωσης συνεχίζει να είναι η http://nvd.nist.gov/fdcc/index.cfm.

βασικές γραμμές αναμεταξύ τους, όπως πχ, να συγκρίνουν τη βασική γραμμή του enterprise προτύπου του NIST με τη βασική γραμμή του FDCC.

Επιπρόσθετα των πραγματικών ρυθμίσεων βασικής γραμμής, η κάθε καταχώρηση στη βάση περιέχει άλλα υποστηρικτικά πεδία δεδομένων, συμπεριλαμβανομένου του αναγνωριστή (identifier) Common Configuration Enumeration (CCE),[5] το μονοπάτι της πολιτικής και το όνομα της ρύθμισης, την περιγραφή της ρύθμισης και το αντικείμενο (όπως πχ, το μονοπάτι ενός registry key).

Η βάση NIST Windows Security Baseline Database διατίθεται ελεύθερα προς κατάβαση στη διεύθυνση http://csrc.nist.gov/itsec/guidance_WinXP.html.

[5] Για περισσότερες πληροφορίες σχετικά με το CCE επισκεφτείτε τη διεύθυνση http://cce.mitre.org/.

Παράρτημα Β

Β. Ασφάλεια του Windows XP Service Pack 3

Το Windows XP Service Pack 3 (SP3) κυκλοφόρησε το Μάιο του 2008.[6] Περιέχει πολλές ενημερώσεις ασφάλειας για τα Windows XP οι οποίες κυκλοφόρησαν αφότου διατέθηκε το SP2 στο 2004. Το SP3 επίσης περιέχει ορισμένα χαρακτηριστικά για τα Windows XP τα οποία προηγούμενα ήταν διαθέσιμα για καταφόρτωση μόνο ως αυτόνομα. Παραδείγματα αυτών των χαρακτηριστικών είναι:

- Το IPSec Simple Policy Update for Windows Server 2003 and Windows XP, το οποίο επηρεάζει την ανάπτυξη των IPSec φίλτρων.

- Το Digital Identity Management Service (DIMS), το οποίο περιλαμβάνει την πρόσβαση χρήστη σε ψηφιακά πιστοποιητικά και ιδιωτικά κρυπτογραφικά κλειδιά.

- Το Wi-Fi Protected Access 2 (WPA2), το οποίο είναι μία πιστοποίηση προϊόντος ασύρματης δικτύωσης.

Όσον αφορά τη νέα ή βελτιωμένη λειτουργικότητα ασφάλειας, το SP3 προσφέρει μερικές αλλαγές από το SP2. Οι πιο αξιοσημείωτες αλλαγές περιέχουν τα ακόλουθα:

- Το Network Access Protection (NAP), το οποίο μπορεί να χρησιμοποιηθεί για την εκτέλεση ελέγχων εξυγίανσης συστήματος σε Windows XP συστήματα προτού επιτραπεί σε αυτά να προσχωρήσουν σε κάποιο δίκτυο ή να διεξάγουν άλλες δραστηριότητες.

- Περισσότερο λεπτομερή κείμενα στις Επιλογές Ασφάλειας (Security Options) του control panel για την καλύτερη επεξήγηση της σπουδαιότητας των ρυθμίσεων ασφάλειας.

- Αναβαθμισμένες κρυπτογραφικές αυτόνομες μονάδες (cryptographic modules). Το Windows XP SP3 υποστηρίζει SHA-256, SHA-384 και SHA-512 για την επικύρωση πιστοποιητικών X.509.[7] Οι κρυπτογραφικές αυτόνομες μονάδες στο SP3 είναι πλέον επικυρωμένες από FIPS.[8]

Αναφορές σε επιπρόσθετες πηγές πληροφόρησης για το Windows XP SP3 είναι διαθέσιμες στο Παράρτημα F.

[6] Όλες οι πληροφορίες που παρουσιάζονται σε αυτό το παράρτημα έχουν αντληθεί από την Επισκόπηση του Windows XP Service Pack 3 από τη Microsoft, όπου είναι διαθέσιμη στη διεύθυνση http://download.microsoft.com/download/6/8/7/687484ed-8174-496d-8db9-f02b40c12982/Overview%20of%20Windows%20XP%20Service%20Pack%203.pdf.
[7] http://en.wikipedia.org/wiki/X.509.
[8] http://www.certicom.com/index.php/fips-validation-what-is-it.

Παράρτημα C

C. Χαρτογράφηση των Ελέγχων των Windows XP με το NIST SP 800-53

Το Παράρτημα C χαρτογραφεί πολλούς ελέγχους ασφάλειας των Windows XP και τις ρυθμίσεις του προτύπου ασφάλειας που αναφέρονται σε αυτό το εγχειρίδιο, με την αντιστοιχία τους στους ελέγχους του NIST SP 800-53 Επανέκδοση 2. Ο κατάλογος των ελέγχων και της χαρτογράφησης δεν προτίθεται να είναι πλήρως περιεκτικός ή επιτακτικός και παραλείπει όλους τους ελέγχους του SP 800-53 που δεν σχετίζονται άμεσα με αυτόνομα Windows XP συστήματα. Οι χαρτογραφήσεις παρατίθενται σύμφωνα με τις κατηγορίες της οικογένειας ελέγχου που θεσμοθετήθηκαν στο SP 800-53. Η κάθε κατηγορία έχει ένα ξεχωριστό πίνακα, με τρεις στήλες που περιέχουν τις ακόλουθες πληροφορίες για κάθε χαρτογράφηση:

- Τον αριθμό και το όνομα του ελέγχου από το SP 800-53
- Τις ενότητες αυτής της δημοσίευσης που χαρτογραφούν τον SP 800-53 έλεγχο και μία συνοπτική περιγραφή του περιεχομένου των ενοτήτων που αντιστοιχούν στον SP 800-53 έλεγχο
- Τις ρυθμίσεις εντός του Παραρτήματος Α αυτής της δημοσίευσης που χαρτογραφούν τον SP 800-53 έλεγχο, εφόσον αυτές υπάρχουν.

Οι πίνακες περιέχουν τις απαιτήσεις και τις βελτιώσεις των ελέγχων που απευθύνονται σε συστήματα χαμηλού, μεσαίου και υψηλού αντικτύπου. (Η ενότητα 2.2 περιέχει ορισμούς για τις κατηγορίες αντικτύπου). Κατόπιν του καθορισμού του επιπέδου αντικτύπου ενός συστήματος, οι διαχειριστές μπορούν να επιλέξουν τους SP 800-53 ελέγχους που αντιστοιχούν στο επίπεδο αντικτύπου ενός συστήματος και έπειτα να αναγνωρίσουν τις ενότητες αυτού του εγχειριδίου και τις ρυθμίσεις των προτύπων που ταιριάζουν με αυτούς τους SP 800-53 ελέγχους. Έτσι παρέχεται μία εναρκτήριος για την αναγνώριση όλων των ελέγχων ασφάλειας που χρειάζονται για την ασφάλιση του συστήματος.

C.1 Διαχειριστικοί Έλεγχοι

Αυτή η ενότητα περιέχει χαρτογραφήσεις για τις ακόλουθες οικογένειες διαχειριστικών ελέγχων:

- Αποτιμήσεις Πιστοποίησης, Διαπίστευσης και Ασφάλειας (Certification, Accreditation, and Security Assessments [CA])
- Σχεδιασμός (Planning [PL])
- Αποτίμηση Κινδύνου (Risk Assessment [RA])
- Απόκτηση Συστήματος και Υπηρεσιών (System and Services Acquisition [SA])

Πίνακας C-1. Certification, Accreditation, and Security Assessments (CA) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
CA-3: Information system connections	• Ενότητα 2.4.5 (Εξουσιοδότηση για σύνδεση σε δίκτυο)	Μ/Δ[9]
CA-7: Continuous monitoring	• Ενότητα 2.6 (Επίβλεψη ελέγχων ασφάλειας και αλλαγών διαμόρφωσης) • Ενότητα 3.1.3 (Επίβλεψη της ιδιότητας των κοινών ελέγχων ασφάλειας)	Μ/Δ

Πίνακας C-2. Planning (PL) Family Controls

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
PL-4: Rules of behavior	• Ενότητα 2.4.5 (Έχοντας ένα εγχειρίδιο κανόνων συμπεριφοράς)	Μ/Δ

Πίνακας C-3. Risk Assessment (RA) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
RA-2: Security categorization	• Ενότητα 2.2 (Περιγράφει τις κατηγορίες ασφάλειας FIPS 199 και τη σχέση τους με τους SP 800-53 ελέγχους)	Μ/Δ
RA-3: Risk assessment	• Ενότητα 2.3 (Καθορίζοντας τις απειλές, διεξαγωγή αποτιμήσεων κινδύνου, εκτέλεση καταπράυνσης κινδύνου)	Μ/Δ
RA-5: Vulnerability scanning	• Ενότητα 2.6 (Εκτέλεση αποτιμήσεων ευπάθειας για την αποτίμηση της στάσης ασφάλειας του συστήματος) • Ενότητα 4.4 (Χρήση σαρωτών ευπαθειών για την αναγνώριση ζητημάτων ασφάλειας)	Μ/Δ

[9] Το Μ/Δ είναι συντομογραφία του «Μη Διαθέσιμες».

Πίνακας C-4. System and Services Acquisition (SA) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
SA-5: Information system documentation	• Ενότητα 2.4.5 (Έχοντας έναν οδηγό διαμόρφωσης ασφάλειας και άλλα εγχειρίδια σχετικά με την ασφάλεια)	Μ/Δ
SA-7: User installed software	• Ενότητα 2.3.2.3 (Μη εγκατάσταση και χρήση μη εγκεκριμένων εφαρμογών) • Ενότητα 3.1.3 (Χρήση πολιτικών περιορισμού λογισμικού για τον περιορισμό του λογισμικού που μπορεί να εκτελεστεί σε ένα σύστημα) • Ενότητα 7.4 (Χρήση πολιτικών περιορισμού λογισμικού για τον περιορισμό του λογισμικού που μπορεί να εκτελεστεί σε ένα σύστημα)	Μ/Δ

C.2 Λειτουργικοί Έλεγχοι

Αυτή η ενότητα περιέχει χαρτογραφήσεις των ακόλουθων οικογενειών λειτουργικών ελέγχων:

- Επίγνωση και Εκπαίδευση (Awareness and Training [AT])
- Διαχείριση Διαμόρφωσης (Configuration Management [CM])
- Σχεδιασμός Απροόπτων (Contingency Planning [CP])
- Απόκριση Περιστατικού (Incident Response [IR])
- Συντήρηση (Maintenance [MA])
- Προστασία Μέσων (Media Protection [MP])
- Ασφάλεια Προσωπικού (Personnel Security [PS])
- Φυσική και Περιβαλλοντική Προστασία (Physical and Environmental Protection [PE])
- Ακεραιότητα Συστήματος και Πληροφορίας (System and Information Integrity [SI])

Πίνακας C-5. Awareness and Training (AT) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
AT-2: Security awareness	• Ενότητα 2.3.2.3 (Εκπαιδεύοντας τους χρήστες προς αποφυγήν μολύνσεων κακόβουλου λογισμικού) • Ενότητα 2.4.5 (Έχοντας επίγνωση ασφάλειας και εκπαίδευση για τερματικούς χρήστες και διαχειριστές)	Μ/Δ
AT-3: Security training	• Ενότητα 2.4.5 (Έχοντας επίγνωση ασφάλειας και εκπαίδευση για τερματικούς χρήστες και διαχειριστές)	Μ/Δ

Πίνακας C-6. Configuration Management (CM) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
CM-1: Configuration management policy and procedures	• Ενότητα 2.4.5 (Έχοντας πολιτική, σχέδιο και διαδικασίες διαχείρισης διαμόρφωσης) • Ενότητα 4 (Έχοντας πολιτική διαχείρισης διαμόρφωσης για το λειτουργικό σύστημα και την εγκατάσταση και τις αλλαγές εφαρμογών)	Μ/Δ
CM-3: Configuration change control	• Ενότητα 2.5 (Τεκμηριώνοντας τις αλλαγές σε εκ προεπιλογής πρότυπα ασφάλειας και ρυθμίσεις) • Ενότητα 2.6 (Καταγράφοντας όλες δραστηριότητες συντήρησης hardware)	Μ/Δ
CM-4: Monitoring configuration changes	• Ενότητα 2.5 (Δοκιμάζοντας τις αλλαγές στους ελέγχους ασφάλειας) • Ενότητα 7 (Εξετάζοντας την επίπτωση της κάθε απόφασης που λαμβάνεται σχετικά με ένα σύστημα που μπορεί να έχει στην ασφάλειά του) • Ενότητα 5.3 (Καθορισμός της επίπτωσης της εφαρμογής ενός προτύπου ασφάλειας σε ένα χρήστη ή υπολογιστή)	Μ/Δ
CM-6: Configuration settings	• Ενότητα 2.4.5 (Έχοντας έναν οδηγό διαμόρφωσης ασφάλειας) • Ενότητα 5 (Χρησιμοποιώντας πρότυπα ασφάλειας για τη θέση	Όλες

	ρυθμίσεων συστήματος σχετικών με την ασφάλεια) • Ενότητα 5.1 (Χρησιμοποιώντας πρότυπα ασφάλειας για τη σύγκριση των υποστατών ρυθμίσεων με των απαιτούμενων ρυθμίσεων) • Ενότητα 5.2 (Χρησιμοποιώντας πρότυπα ασφάλειας για τη σύγκριση των υποστατών ρυθμίσεων με των απαιτούμενων ρυθμίσεων)	
CM-7: Least functionality	• Ενότητα 2.3.1.3 (Απενεργοποιώντας άχρηστες τοπικές υπηρεσίες)	Μ/Δ
	• Ενότητα 2.3.2.1 (Απενεργοποιώντας άχρηστες υπηρεσίες δικτύου)	Μ/Δ
	• Ενότητα 4.1.2.1 (Απενεργοποιώντας μη αναγκαίους clients, υπηρεσίες και πρωτόκολλα δικτύου˙ αφαιρώντας όλες τις μη αναγκαίες εφαρμογές και διεργασίες)	Μ/Δ
	• Ενότητα 6.2.3 (Περιορίζοντας την εκτέλεση συγκεκριμένων ενεργειών)	Ρυθμίσεις Security Options
	• Ενότητα 6.5 (Απενεργοποιώντας αχρείαστες υπηρεσίες)	Ρυθμίσεις System Services
	• Ενότητα 6.8.2 (Αφαιρώντας τις εξαιρέσεις φίλτρανσης της κίνησης των Kerberos και RSVP)	Ρύθμιση 5.79
	• Ενότητα 6.8.4 (Απενεργοποίηση του χαρακτηριστικού Dr. Watson)	Μ/Δ
	• Ενότητα 7.5 (Χρησιμοποιώντας μόνο τα απαραίτητα πρωτόκολλα και συστατικά δικτύου) • Ενότητα 7.6 (Χρησιμοποιώντας το Windows Firewall για την εμπόδιση της πρόσβασης στις πόρτες)	Μ/Δ
	• Ενότητα 7.7 (Αφαιρώντας τις εξαιρέσεις φίλτρανσης της κίνησης των Kerberos και RSVP)	Ρύθμιση 5.79
	• Ενότητα 7.7 (Χρησιμοποιώντας φίλτρα IPsec για τον περιορισμό της κίνησης του δικτύου)	Μ/Δ

Πίνακας C-7. Contingency Planning (CP) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
CP-2: Contingency plan	• Ενότητα 2.3 (Εκτέλεση σχεδιασμού απροόπτων) • Ενότητα 2.4.5 (Έχοντας IT σχέδια απροόπτων)	Μ/Δ
CP-9: Information system backup	• Ενότητα 2.3 (Εκτέλεση διαδικασίας αντιγράφων ασφάλειας, αποθηκεύοντάς τα σε ασφαλή μέρη και ελέγχοντάς τα συχνά) • Ενότητα 4.2 (Εκτέλεση διαδικασίας αντιγράφων ασφάλειας και επαναφορών˙ έλεγχος των αντιγράφων ασφάλειας)	Μ/Δ

Πίνακας C-8. Incident Response (IR) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
IR-1: Incident response policy and procedures	• Ενότητα 2.6 (Έχοντας μία πολιτική απόκρισης περιστατικού οργανισμού)	Μ/Δ
IR-4: Incident handling	• Ενότητα 2.6 (Έχοντας μία επίσημη ικανότητα απόκρισης περιστατικού)	Μ/Δ

Πίνακας C-9. Maintenance (MA) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
MA-1: System maintenance policy and procedures	• Ενότητα 2.3.2.3 (Δημιουργώντας ένα σχέδιο για τη συντήρηση συστημάτων Windows XP)	Μ/Δ
MA-2: Controlled maintenance	• Ενότητα 2.6 (Εκτελεί τακτική συντήρηση ασφάλειας)	Μ/Δ
MA-4: Remote maintenance	• Ενότητα 2.6 (Παροχή απομακρυσμένης διαχείρισης συστήματος και βοήθειας)	Μ/Δ

Πίνακας C-10. Media Protection (MP) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
MP-4: Media storage	• Ενότητα 2.3.1.2 (Φυσική ασφάλιση των αποσπώμενων μέσων) • Ενότητα 2.6 (Προστασία των μέσων) • Ενότητα 4.1.2.2 (Φυσική ασφάλιση εικονικών μέσων) • Ενότητα 4.2 (Αποθήκευση και προστασία μέσων αντιγράφων ασφάλειας) • Ενότητα 7.2.5 (Προστασία δίσκων επαναφοράς κωδικού ασφάλειας)	Μ/Δ
MP-6: Media sanitization and disposal	• Ενότητα 2.6 (Καθαρισμός μέσων) • Ενότητα 7.1.5 (Καθαρισμός όλων των αποσπώμενων και μη μέσων αποθήκευσης, καταστροφή συσκευών αποθήκευσης)	Μ/Δ

Πίνακας C-11. Personnel Security (PS) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
PS-4: Personnel termination	• Ενότητα 2.3.1.2 (Απενεργοποιώντας τους λογαριασμούς αμέσως μετά την αποχώρηση των υπαλλήλων από τον οργανισμό) • Ενότητα 2.3.1.2 (Απενεργοποιώντας τους λογαριασμούς αμέσως μετά την αποχώρηση των υπαλλήλων από τον οργανισμό) • Ενότητα 7.2.1 (Άμεση απενεργοποίηση των λογαριασμών εφόσον δεν είναι πλέον αναγκαίοι, όπως ενός υπαλλήλου που αποχώρισε από τον οργανισμό)	Μ/Δ
PS-5: Personnel transfer	• Ενότητα 7.2 (Άμεση απενεργοποίηση των λογαριασμών εφόσον δεν είναι πλέον αναγκαίοι, όπως ενός υπαλλήλου που άλλαξαν τα καθήκοντά του)	Μ/Δ

Πίνακας C-12. Physical and Environmental Protection (PE) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
PE-1: Physical and environmental protection policy and procedures	• Ενότητα 2.3.1.1 (Έχοντας μία πολιτική φυσικής και περιβαλλοντικής προστασίας)	Μ/Δ
PE-3: Physical access control	• Ενότητα 2.3.1.1 (Εφαρμόζοντας μέτρα φυσικής ασφάλισης για τον περιορισμό της πρόσβασης στα συστήματα) • Ενότητα 2.3.2.3 (Περιορισμός της φυσικής πρόσβασης στα συστήματα)	Μ/Δ
PE-11: Emergency power	• Ενότητα 4.2 (Χρησιμοποίηση UPS για την παροχή προσωρινής ισχύος μπαταρίας έκτακτης ανάγκης)	Μ/Δ

Πίνακας C-13. System and Information Integrity (SI) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
SI-2: Flaw remediation	• Ενότητα 2.3.1.3 (Εγκατάσταση ενημερώσεων εφαρμογών και λειτουργικού συστήματος) • Ενότητα 2.3.2.1 (Έλεγχος και εγκατάσταση ενημερώσεων εφαρμογών και λειτουργικού συστήματος) • Ενότητα 2.6 (Απόκτηση και εγκατάσταση ενημερώσεων λογισμικού) • Ενότητα 4.3 (Απόκτηση και εγκατάσταση ενημερώσεων ασφάλειας) • Ενότητα 4.3.5 (Εκτέλεση patching σε διαχειριζόμενα περιβάλλοντα) • Ενότητα 4.4 (Έλεγχος κατάστασης patch σε υπολογιστές)	Μ/Δ
SI-3: Malicious code protection	• Ενότητα 2.3.2.3 (Προστατεύοντας τα συστήματα από κακόβουλο ωφέλιμο φορτίο· χρησιμοποιώντας λογισμικό antivirus και antispyware· διαμορφώνοντας το λογισμικό των server και client για τη μείωση της έκθεσης σε κακόβουλο λογισμικό)	Μ/Δ

	• Ενότητα 3.1.3 (Χρήση του χαρακτηριστικού Data Execution Prevention για την ακύρωση επιθέσεων που χρησιμοποιούν buffer overflows) • Ενότητα 7.1.2 (Αλλάζοντας τις εκ προεπιλογής συσχετίσεις αρχείων που χρησιμοποιούνται από κακόβουλο λογισμικό˙ απεικόνιση ολόκληρων των ονομάτων των αρχείων για την αναγνώριση ύποπτων επεκτάσεων που χρησιμοποιούνται από κακόβουλο λογισμικό) • Ενότητα 7.1.3 (Απεικόνιση ολόκληρων των ονομάτων των αρχείων για την αναγνώριση ύποπτων επεκτάσεων που χρησιμοποιούνται από κακόβουλο λογισμικό)	
SI-4: Information system monitoring tools and techniques	• Ενότητα 2.6 (Επίβλεψη των event logs για την αναγνώριση προβλημάτων και ύποπτης δραστηριότητας) • Ενότητα 8.4 (Χρήση personal firewalls για την εμπόδιση εξερχόμενης επικοινωνίας από κακόβουλο λογισμικό)	Μ/Δ
SI-5: Security alerts and advisories	• Ενότητα 2.3.2.3 (Επίβλεψη των mailing lists της Microsoft για σχετικά δελτία ασφάλειας) • Ενότητα 2.6 (Συνδρομή και επίβλεψη ειδοποιήσεων των mailing lists ευπαθειών)	Μ/Δ
SI-6: Security functionality verification	• Ενότητα 3.1.3 (Αναγνώριση και αναφορά αποτυχιών ή σοβαρών κακών διαμορφώσεων ή συγκεκριμένων ελέγχων ασφάλειας από το Windows Security Center) • Ενότητα 4.4 (Αναγνώριση και αναφορά αποτυχιών ή σοβαρών κακών διαμορφώσεων ή συγκεκριμένων ελέγχων ασφάλειας από το Windows Security Center˙ εκτέλεση κεντρικής επίβλεψης των ελέγχων ασφάλειας)	Μ/Δ
SI-7: Software and information integrity	• Ενότητα 2.6 (Επίβλεψη αλλαγών των ρυθμίσεων του λογισμικού και του λειτουργικού συστήματος) • Ενότητα 3.1.3 (Χρήση πολιτικών περιορισμού λογισμικού για την αποτροπή εκκίνησης ανεπιθύμητων εκτελέσιμων αρχείων)	Μ/Δ

	• Ενότητα 7.4 (Χρήση πολιτικών περιορισμού λογισμικού για την αποτροπή εκκίνησης ανεπιθύμητων εκτελέσιμων αρχείων)	
SI-8: Spam protection	• Ενότητα 2.3.2.3 (Προστατεύοντας τα συστήματα από τα κακόβουλα ωφέλιμα φορτία˙ χρήση e-mail clients που υποστηρίζουν spam filtering) • Ενότητα 8.3 (Διαμορφώνοντας τους e-mail clients να χρησιμοποιούν χαρακτηριστικά anti-spam˙ διαμορφώνοντας τους τους e-mail clients να μη φορτώνουν αυτόματα τις απομακρυσμένες εικόνες, οι οποίες μπορούν να είναι spyware) • Ενότητα 8.4 (Χρήση personal firewalls για τον περιορισμό των cookies του φυλλομετρητή, συμπεριλαμβανομένου και των spyware tracking cookies) • Ενότητα 8.6 (Χρήση και ενημέρωση λογισμικού antispyware)	Μ/Δ

C.3 Τεχνικοί Έλεγχοι

Αυτή η ενότητα περιέχει χαρτογραφήσεις για τις ακόλουθες οικογένειες τεχνικών ελέγχων:

- Έλεγχος Πρόσβασης (Access Control [AC])
- Έλεγχος και Υπευθυνότητα (Audit and Accountability [AU])
- Ταυτοποίηση και Πιστοποίηση (Identification and Authentication [IA])
- Προστασία Συστήματος και Επικοινωνιών (System and Communications Protection [SC])

Πίνακας C-14. Access Control (AC) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
AC-2: Account management	• Ενότητα 7.2.1 (Απενεργοποίηση των ανενεργών, αχρείαστων και προσωρινών λογαριασμών˙ διαγραφή των απενεργοποιημένων λογαριασμών)	Μ/Δ

AC-3: Access enforcement	• Ενότητα 2.3.1.1 (Κρυπτογράφηση των τοπικών αρχείων για την αποτροπή πρόσβασης) • Ενότητα 2.3.1.3 (Κρυπτογράφηση ευαίσθητων δεδομένων) • Ενότητα 3.1.2 (Προστατεύοντας προσωπικά δεδομένα και ρυθμίσεις με τη χρήση μεμονωμένων λογαριασμών˙ περιορισμός της απομακρυσμένης πρόσβασης σε λογαριασμούς χρηστών και διαμοιρασμούς) • Ενότητα 3.2.5 (Κρυπτογράφηση των τοπικών αρχείων για την αποτροπή πρόσβασης) • Ενότητα 6.2.2 (Έχοντας του χρήστες να ανήκουν μόνο στις απαραίτητες ομάδες)	Μ/Δ
	• Ενότητα 6.2.2 (Δίνοντας μόνο τα απαραίτητα δικαιώματα στις ομάδες)	Ρυθμίσεις User Rights Assignment
	• Ενότητα 6.2.3 (Θέτοντας ρυθμίσεις ασφάλειας για τον περιορισμό των πράξεων που μπορούν να εκτελέσουν οι χρήστες)	Ρυθμίσεις Security Options
	• Ενότητα 6.4 (Περιορισμός της δυνατότητας μέλους σε ομάδες με συγκεκριμένα προνόμια)	Ρυθμίσεις Restricted Groups
	• Ενότητα 6.6 (Θέτοντας άδειες αρχείων)	Ρυθμίσεις File Permission
	• Ενότητα 6.7 (Θέτοντας άδειες μητρώου) • Ενότητα 7.1.1 (Χρησιμοποιώντας το σύστημα διαχείρισης αρχείων NTFS) • Ενότητα 7.1.4 (Κρυπτογράφηση των τοπικών αρχείων για την αποτροπή πρόσβασης)	Μ/Δ
AC-4: Information flow enforcement	• Ενότητα 2.3.2.1 (Χρήση κάποιου firewall για τον περιορισμό πρόσβασης μέσω δικτύου σε κάποιο host) • Ενότητα 3.1.1 (Χρήση κάποιου personal firewall για τον περιορισμό της κίνησης του δικτύου) • Ενότητα 7.5 (Ασφάλιση διεπαφών δικτύου και απενεργοποίηση αχρείαστων δικτυακών components) • Ενότητα 7.6 (Χρήση κάποιου personal	Μ/Δ

	firewall για τον περιορισμό της κίνησης του δικτύου)	
AC-6: Least privilege	• Ενότητα 2.2 (Ανάθεση δικαιωμάτων χρήστη βάση των ελάχιστων προνομίων) • Ενότητα 6.2.2 (Ανάθεση δικαιωμάτων χρήστη βάση των ελάχιστων προνομίων)	Μ/Δ
AC-7: Unsuccessful login attempts	• Ενότητα 6.1 (Κλείδωμα λογαριασμών μετά από αρκετές αποτυχημένες προσπάθειες εισόδου)	Ρυθμίσεις 2.1 (Lockout duration), 2.2 (Lockout threshold), και 2.3 (Reset counter after x minutes)
AC-8: System use notification	• Ενότητα 2.3.1.2 (Παρουσιάζοντας ένα προειδοποιητικό banner όταν κάποιος χρήστης προσπαθεί να εισέλθει) • Ενότητα 2.3.2.1 (Παρουσιάζοντας ένα προειδοποιητικό banner όταν κάποιος χρήστης προσπαθεί να εισέλθει)	Ρυθμίσεις 5.29 (Banner message text) και 5.30 (Banner message title)
AC-11: Session lock	• Ενότητα 2.3.1.2 (Χρήση screensaver με κωδικό ασφάλειας) • Ενότητα 7.2.4 (Χρήση screensaver με κωδικό ασφάλειας, χειροκίνητο κλείδωμα συνεδριών χρήστη)	Μ/Δ
AC-17: Remote access	• Ενότητα 2.3.2.1 (Χρήση ισχυρών industry-standard πρωτοκόλλων για απομακρυσμένη πρόσβαση) • Ενότητα 3.1.1 (Απενεργοποίηση ενσωματωμένων υπηρεσιών απομακρυσμένης πρόσβασης οι οποίες δεν χρειάζονται)	Μ/Δ
	• Ενότητα 6.4 (Περιορίζοντας τη δυνατότητα μέλους στην ομάδα Remote Desktop Users)	Ρύθμιση 7.3
	• Ενότητα 6.5 (Απενεργοποίηση των υπηρεσιών Remote Assistance και Remote Desktop)	Μ/Δ
AC-18: Wireless access restrictions	• Ενότητα 3.1.1 (Μη αυτόματη σύνδεση σε ασύρματα δίκτυα, χρήση χαρακτηριστικών ασφάλειας wireless) • Ενότητα 7.8 (Χρήση χαρακτηριστικών ασφάλειας wireless)	Μ/Δ

Πίνακας C-15. Audit and Accountability (AU) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
AU-2: Auditable events	• Ενότητα 6.2.1 (Διαμόρφωση ελέγχου συστήματος)	Ρυθμίσεις Audit Policy
	• Ενότητα 7.3.1 (Ελεγχος πρόσβασης σε συγκεκριμένα αρχεία)	Μ/Δ
AU-4: Audit storage capacity	• Ενότητα 6.3 (Ενεργοποίηση αναφορών και καθορισμός του μέγιστου μεγέθους των αναφορών [logs])	Ρυθμίσεις Event Log Policy
AU-6: Audit monitoring, analysis, and reporting	• Ενότητα 2.6 (Επίβλεψη των logs) • Ενότητα 7.3.2 (Ανασκόπηση των logs)	Μ/Δ
AU-8: Time stamps	• Ενότητα 7.3.3 (Εκτέλεση συγχρονισμού ρολογιού)	Μ/Δ

Πίνακας C-16. Identification and Authentication (IA) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
IA-1: Identification and authentication policy and procedures	• Ενότητα 2.3.1.2 (Εχοντας μία πολιτική κωδικού ασφάλειας) • Ενότητα 2.3.2.1 (Εχοντας μία πολιτική κωδικού ασφάλειας)	Μ/Δ
IA-2: User identification and authentication	• Ενότητα 2.3.1.2 (Απαίτηση πιστοποίησης έγκυρου username και password) • Ενότητα 2.3.1.3 (Απαίτηση ισχυρής πιστοποίησης για λογαριασμούς διαχειριστή) • Ενότητα 2.3.2.1 (Απαίτηση ισχυρής πιστοποίησης για τη χρήση υπηρεσιών δικτύου) • Ενότητα 2.3.2.3 (Χρησιμοποιώντας καθημερινά ένα λογαριασμό χρήσης για κανονικές λειτουργίες συστήματος˙ χρήση ενός λογαριασμού επιπέδου διαχειριστή μόνο όταν είναι αναγκαίο για συγκεκριμένα καθήκοντα) • Ενότητα 3.1.2 (Εχοντας ένα μοναδικό λογαριασμό για κάθε άτομο)	Μ/Δ

	• Ενότητα 3.2.1 (Χρήση του Kerberos για πιστοποίηση) • Ενότητα 3.2.2 (Χρήση έξυπνων καρτών για πιστοποίηση)	
	• Ενότητα 6.8.1 (Μην επιτρέποντας την παράκαμψη της εισόδου στο σύστημα)	Ρύθμιση 5.70
	• Ενότητα 7.2 (Απενεργοποιώντας τους εκ προεπιλογής λογαριασμούς, δημιουργώντας ξεχωριστούς λογαριασμούς καθημερινής χρήσης για κάθε χρήστη)	Μ/Δ
IA-4: Identifier management	• Ενότητα 6.1 (Έχοντας ισχυρό κωδικό ασφάλειας για κάθε λογαριασμό χρήστη) • Ενότητα 7.2 (Δημιουργώντας ξεχωριστούς λογαριασμούς καθημερινής χρήσης για κάθε χρήστη)	Μ/Δ
IA-5: Authenticator management	• Ενότητα 2.3.2.2 (Χρήση ενός ασφαλούς συστήματος ταυτοποίησης και πιστοποίησης χρήστη) • Ενότητα 3.1.2 (Αποτρέποντας τα κενά ή μηδενικά passwords από το network login και την υπηρεσία secondary logon˙ αποθηκεύοντας τις πληροφορίες πιστοποίησης για λειτουργικά συστήματα και εφαρμογές) • Ενότητα 4.1.2.1 (Θέτοντας ισχυρούς κωδικούς ασφάλειας για νέους λογαριασμούς) • Ενότητα 6.1 (Χρήση ενός ασφαλούς συστήματος ταυτοποίησης και πιστοποίησης χρήστη)	Μ/Δ
	• Ενότητα 6.1 (Θέτοντας μέγιστη και ελάχιστη ηλικία κωδικών ασφάλειας˙ αποτρέποντας την επαναχρησιμοποίηση κωδικών ασφάλειας μέσω του ιστορικού κωδικών˙ αποθήκευση κρυπτογραφημένων κωδικών ασφάλειας)	Μ/Δ

Πίνακας C-17. System and Communications Protection (SC) Family Controls.

Αριθμός και Όνομα SP 800-53 Ελέγχου	Αντιστοιχία με τις Ενότητες του SP 800-68	Αντιστοιχία με τις Ρυθμίσεις Προτύπου του NIST
SC-4: Information remnants	• Ενότητα 6.8.4 (Απενεργοποιώντας τη δημιουργία memory dump αρχείων) • Ενότητα 7.9 (Απενεργοποιώντας τη δημιουργία memory dump αρχείων· καθαρίζοντας τα αρχεία σελίδων κατά την απενεργοποίηση του συστήματος· απενεργοποιώντας τη χρήση αρχείων hibernation)	Μ/Δ
SC-5: Denial of service protection	• Ενότητα 6.8.2 (Διαμορφώνοντας τις ρυθμίσεις δικτύου για την αποτροπή ή τον περιορισμό συγκεκριμένων επιθέσεων άρνησης υπηρεσίας)	Ρυθμίσεις Security Options
SC-8: Transmission integrity	• Ενότητα 3.2.4 (Χρήση του IPsec για την προστασία των επικοινωνιών δικτύου) • Ενότητα 7.7 (Χρήση του IPsec για την προστασία των επικοινωνιών δικτύου)	Μ/Δ
SC-9: Transmission confidentiality	• Ενότητα 2.3.2.2 (Κρυπτογράφηση των επικοινωνιών δικτύου) • Ενότητα 3.2.4 (Χρήση του IPsec για την προστασία των επικοινωνιών δικτύου) • Ενότητα 7.7 (Χρήση του IPsec για την προστασία των επικοινωνιών δικτύου)	Μ/Δ
SC-13: Use of cryptography	• Ενότητα 7.8 (Χρήση αλγόριθμων κρυπτογράφησης εγκεκριμένων από το FIPS)	Μ/Δ
SC-18: Mobile code	• Ενότητα 2.3.2.3 (Διαμορφώνοντας τα συστήματα έτσι ώστε οι εκ προεπιλογής συσχετίσεις αρχείων να αποτρέπουν την αυτόματη εκτέλεση αρχείων ενεργού περιεχομένου)	Μ/Δ

Παράρτημα D

D. Συνήθεις Χρησιμοποιούμενες TCP/IP Πόρτες στα Windows XP Συστήματα

Το παράρτημα D απαριθμεί συνήθεις χρησιμοποιούμενες TCP/IP πόρτες στα Windows XP συστήματα.[10]

Πίνακας D-1. TCP – UDP Ports.

Πόρτα	Πρωτόκολλο	Υπηρεσία	Περιγραφή
21	TCP	FTP	File Transfer Protocol server
23	TCP	Telnet	Υπηρεσία Telnet
68	UDP	DHCP	Dynamic Host Configuration Protocol client
80	TCP	HTTP	HyperText Transfer Protocol server
123	UDP	NTP	Network Time Protocol client (Windows Time)
135	TCP	epmap	DCE Endpoint Resolution (remote procedure call)
137	UDP	NetBIOS-ns	Υπηρεσία NetBIOS Name
138	UDP	NetBIOS-dgm	Υπηρεσία NetBIOS Datagram
139	TCP	NetBIOS-ssn	Υπηρεσία NetBIOS Session
161	UDP	SNMP	Simple Network Management Protocol
213	UDP	IPX Over IP	Client Service για Netware service
443	TCP	HTTPS	HTTP over SSL server
445	TCP, UDP	microsoft-ds (SMB)	Microsoft Common Internet File System (CIFS)
500	UDP	IKE	Internet Key Exchange (συχνά χρησιμοποιούμενο με IPsec)
515	TCP	LPR	Υπηρεσία Print Spooler
522	TCP		NetMeeting client[11]

[10] Για περισσότερες πληροφορίες στις πόρτες που χρησιμοποιούνται από τις υπηρεσίες των Windows XP δείτε το άρθρο με τίτλο *Windows Server 2003 System Services Reference* που είναι διαθέσιμο στη διεύθυνση http://www.microsoft.com/downloads/details.aspx?FamilyID=b38a0682-2997-4678-9d9e-a07cc66a3bba&displaylang=en και το MSKB άρθρο 832017, *Service overview and network port requirements for the Windows Server system*, στη διεύθυνση http://support.microsoft.com/?id=832017. Επίσης το MSKB άρθρο 308127, *How to manually open ports in Internet Connection Firewall in Windows XP*, περιέχει πληροφορίες σε κάποιες γηγενής Windows XP πόρτες, καθώς και σε πόρτες που χρησιμοποιούνται από διάφορα λογισμικά εξωτερικών παραγόντων. Αυτό το άρθρο είναι διαθέσιμο στη διεύθυνση http://support.microsoft.com/?id=308127.

[11] Επιπρόσθετες πληροφορίες για τις πόρτες του NetMeeting είναι διαθέσιμες από το Technet της Microsoft στη διεύθυνση http://www.microsoft.com/technet/security/secnews/asktheexperts/ask2.mspx.

1503	TCP		NetMeeting client
1701	UDP	L2TP	Layer 2 Tunneling Protocol client
1720	TCP		NetMeeting client
1723	TCP/UDP	PPTP	Point-to-Point Tunneling Protocol client
1731	TCP		NetMeeting client
1900	UDP	SSDP	Simple Service Discovery Protocol
2001-2120	UDP		Φωνητικές κλήσεις του Windows Messenger[12]
2869	TCP	UPnP	Universal Plug and Play
3002	TCP		Windows Firewall/Sharing
3003	TCP		Windows Firewall/Sharing
3389	TCP	RDP	Υπηρεσία Remote Desktop Protocol
4500	UDP	L2TP/IPsec	NAT-T L2TP/IPSec
5000	TCP	UPnP	Universal Plug and Play
6801	UDP		Φωνητικές κλήσεις του Windows Messenger
6891-6900	TCP		Μεταφορές Αρχείων του Windows Messenger
6901	TCP/UDP		Φωνητικές κλήσεις του Windows Messenger

[12] Περισσότερες πληροφορίες για τις πόρτες του Windows Messenger είναι διαθέσιμες από το άρθρο του Barb Bowman, *Don't Let the Defence Rest*, που είναι διαθέσιμο στη διεύθυνση http://www.microsoft.com/windowsxp/using/networking/expert/bowman_november12.mspx.

Παράρτημα Ε

Ε. Εργαλεία

Το Παράρτημα Ε συνοψίζει διάφορα εργαλεία που αναφέρθηκαν στο εγχειρίδιο τα οποία μπορούν να χρησιμοποιηθούν για να διαμορφώσουν, να διαχειριστούν και να επιβλέπουν τις ρυθμίσεις ασφάλειας των Windows XP.

Πίνακας Ε-1. Tools.

Όνομα Εργαλείου	Συνάφεια	Αναφορά
Automatic Updates	Ελέγχει τον Microsoft update server για νέες ενημερώσεις˙ τις καταφορτώνει και τις εγκαθιστά	Εμπεριέχεται με τα Windows XP
Cipher	Καθαρίζει δεδομένα από αχρησιμοποίητα τμήματα δίσκων	cipher.exe Εμπεριέχεται με τα Windows XP
Enterprise Scan Tool	Σαρώνει υπολογιστές για την αναγνώριση ζητημάτων ασφάλειας που δεν είναι ανιχνεύσιμα από το MBSA	http://support.microsoft.com/?id=894193
Event Viewer	Παρουσιάζει τις καταχωρίσεις των logs για τις εφαρμογές, την ασφάλεια και το σύστημα	eventvwr.exe Εμπεριέχεται με τα Windows XP
Group Policy Management Console (GPMC) MMC snap-in	Διαχειρίζεται το Group Policy για πολλαπλούς τομείς	http://www.microsoft.com/windowsserver2003/gpmc/default.mspx
Group Policy Modelling Wizard MMC snap-in	Καθορίζει τις επιπτώσεις της εφαρμογής συνδυασμών από GPOs σε κάποιο συγκεκριμένο χρήστη ή υπολογιστή	http://www.microsoft.com/windowsserver2003/gpmc/default.mspx
Group Policy Object Editor MMC snap-in	Εισάγει κάποιο πρότυπο ασφάλειας μέσα σε ένα GPO	Εμπεριέχεται με τα Windows XP
Local Security Policy	Παρουσιάζει τις τοπικές ρυθμίσεις ασφάλειας και επιτρέπει στο διαχειριστή να τις αλλάξει	Εμπεριέχεται με τα Windows XP (Control Panel / Administrative Tools)
Microsoft Baseline Security Analyzer (MBSA)	Σαρώνει υπολογιστές για την αναγνώριση ζητημάτων ασφάλειας	http://technet.microsoft.com/en-us/security/cc184924.aspx
Microsoft Management Console	Λειτουργεί ως container για τα snap-ins	mmc.exe Εμπεριέχεται με τα Windows XP
Microsoft Update	Ελέγχει για διαθέσιμες ενημερώσεις, τις μεταφέρει στο σύστημα και τις εγκαθιστά	http://update.microsoft.com/
Port Reporter	Καταγράφει πληροφορίες για τη χρήση των TCP και UDP πορτών	http://www.microsoft.com/downloads/details.aspx?amp;displaylang=en&familyid=69BA779B-BAE9-

		4243-B9D6-63E62B4BCD2E&displaylang=en
Qchain.exe	Επιτρέπει την ταυτόχρονη εγκατάσταση πολλών hotfixes	http://www.microsoft.com/downloads/details.aspx?amp;displaylang=en&familyid=3C64D889-74F1-490B-A2FB-F15671A3B60C&displaylang=en
Qfecheck.exe	Εντοπίζει και επαληθεύει εγκατεστημένα hotfixes	http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=155C7C58-102E-47B0-A12A-BFAB8CFCCC03
Registry Editor	Παρέχει στους διαχειριστές ένα τρόπο γραφικής παρουσίασης και προσαρμογής για τις καταχωρήσεις μητρώου (registry entries)	regedit.exe και regedt32.exe Εμπεριέχονται με τα Windows XP
Remote Installation Services	Επιτρέπει την αυτόματη εγκατάσταση των Windows XP σε απομακρυσμένα συστήματα	Εμπεριέχεται με τα Windows 2000 και Windows 2003
Security Configuration and Analysis MMC snap-in	Συγκρίνει τις τρέχουσες ρυθμίσεις ασφάλειας του συστήματος με τις ρυθμίσεις ενός προτύπου	Εμπεριέχεται με τα Windows XP
Security Templates MMC snap-in	Επιτρέπει στο διαχειριστή να ανασκοπήσει, να τροποποιήσει και να εφαρμόσει πρότυπα ασφάλειας	Εμπεριέχεται με τα Windows XP
Sysprep	Κλωνοποιεί μία εικόνα των XP σε άλλα συστήματα	sysprep.exe Εμπεριέχεται με τα Windows XP
Windows Malicious Software Removal Tool	Ελέγχει για συγκεκριμένες συνήθεις απειλές κακόβουλου λογισμικού και επιχειρεί να τις αφαιρέσει	Εγκαθίσταται αυτόματα μέσω των Automatic Updates και Microsoft Update. Μπορούν να καταφορτωθούν απευθείας από τη διεύθυνση http://www.microsoft.com/security/malwareremove/default.mspx

Παράρτημα F

F. Πηγές

F.1 Βάσεις Δεδομένων Ευπάθειας

- National Vulnerability Database (NVD)
  http://nvd.nist.gov/
- Open Source Vulnerability Database
  http://www.osvdb.org/
- SecurityFocus Vulnerability Database
  http://www.securityfocus.com/bid/
- United States Computer Emergency Readiness Team (US-CERT) Vulnerability Notes Database
  http://www.kb.cert.org/vuls/

F.2 Λίστες Ηλεκτρονικού Ταχυδρομείου

- Microsoft Security Notification Service
  http://www.microsoft.com/technet/security/bulletin/notify.mspx
- SecurityFocus - BugTraq
  http://www.securityfocus.com/archive/1
- US-CERT National Cyber Alert System
  http://www.us-cert.gov/cas/

F.3 Έντυπες Πηγές

Allen, Robbie and Gralla, Preston, *Windows XP Cookbook*, O'Reilly, 2005.

Bott, Ed, et al., *Microsoft Windows XP Inside Out, Second Edition*, Microsoft Press, 2004.

Bott, Ed and Siechert, Carl, *Microsoft Windows Security Inside Out for Windows XP and Windows 2000*, Microsoft Press, 2002.

Boyce, Jim, *Windows XP Power Tools*, Sybex, 2002.

Honeycutt, Jerry, *Microsoft Windows XP Registry Guide*, Microsoft Press, 2002.

Moskowitz, Jeremy, *Group Policy, Profiles, and IntelliMirror for Windows 2003, Windows XP, and Windows 2000*, Sybex, 2004.

Moulton, Pete, SOHO Networking: *A Guide to Installing a Small-Office/Home-*

Office Network, Prentice Hall PTR, 2002.

Russel, Charlie and Crawford, Sharon, *Microsoft Windows XP Professional Resource Kit, Third Edition*, Microsoft Press, 2005.

Simmons, Curt and Causey, James, *Microsoft Windows XP Networking Inside Out*, Microsoft Press, 2002.

Thurrott, Paul, *Windows XP Home Networking, 2nd Edition*, John Wiley and Sons, 2004.

F.4 Σχετικά Εγχειρίδια και Πηγές του NIST

- Computer Security Resource Center Special Publications
  http://csrc.nist.gov/publications/PubsSPs.html
  - SP 800-28 Version 2, *Guidelines on Active Content and Mobile Code*
  - SP 800-30, *Risk Management Guide for Information Technology Systems*
  - SP 800-34, *Contingency Planning Guide for Information Technology Systems*
  - SP 800-40 Version 2.0, *Procedures for Handling Security Patches*
  - SP 800-43, *Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System*
  - SP 800-46, *Security for Telecommuting and Broadband Communications*
  - SP 800-48 Revision 1, *Guide to Securing Legacy IEEE Wireless Networks*
  - SP 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems*
  - SP 800-61 Revision 1, *Computer Security Incident Handling Guide*
  - SP 800-63, *Electronic Authentication Guideline*
  - SP 800-70, *Security Configuration Checklists Program for IT Products*
  - SP 800-70 Revision 1 (Draft), *National Checklist Program for IT Products*
  - SP 800-77, *Guide to IPsec VPNs*
  - SP 800-83, *Guide to Malware Incident Prevention and Handling*
  - SP 800-88, *Guidelines for Media Sanitization*
  - SP 800-92, *Guide to Computer Security Log Management*

- SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*
- SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*
- SP 800-115, *Technical Guide to Information Security Testing and Assessment*

- Δημοσιεύσεις του FIPS
  http://csrc.nist.gov/publications/PubsFIPS.html
  - FIPS 140-2, *Security Requirements for Cryptographic Modules*
  - FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
  - FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FISMA Implementation Project
  http://csrc.nist.gov/groups/SMA/fisma/index.html
- National Checklist Program and Checklist Repository
  http://checklists.nist.gov/
- Security Content Automation Protocol (SCAP)
  http://nvd.nist.gov/scap.cfm

F.5 Διαδικτυακές Πηγές της Microsoft

Η ιστοσελίδα της Microsoft περιέχει πληθώρα πληροφοριών σχετικά με τα Windows XP και με την ασφάλεια των Windows. Αυτή η ενότητα απαριθμεί πολλές από αυτές τις πηγές, διαχωρίζοντάς τις σε έξι κατηγορίες: γενικές πηγές για τα Windows XP, γενικές πηγές ασφάλειας (πχ, άσχετες με τα XP), γενικές και συγκεκριμένες πηγές για την ασφάλεια των Windows XP, άρθρα της Microsoft knowledge base και πηγές σχετικές με το Windows XP SP3.

F.5.1 *Γενικές Πηγές για τα Windows XP*

- Microsoft Technet
  http://technet.microsoft.com/en-us/default.aspx
- Microsoft Windows XP Professional Resource Kit Documentation
  http://technet.microsoft.com/en-us/library/bb968968.aspx
- Windows Application Compatibility and User Account Control
  http://technet.microsoft.com/en-us/windows/aa905066.aspx
- Windows XP Home Page
  http://www.microsoft.com/windows/windows-xp/default.aspx

- Windows XP Professional Features
  http://technet.microsoft.com/en-us/library/bb457058(TechNet.10).aspx

- Windows XP Service Pack 2 – Step by Step
  http://support.microsoft.com/kb/889735/EN-US/

- *Administering Group Policy with Group Policy Management Console*
  http://technet2.microsoft.com/WindowsServer/f/?en/library/b9cb929b-4c2f-4754-ad31-d154bb8105771033.mspx

- Enterprise Management with the Group Policy Management Console
  http://www.microsoft.com/windowsserver2003/gpmc/default.mspx

F.5.2 *Γενικές Πηγές Ασφάλειας*

- Microsoft Download Center
  http://www.microsoft.com/downloads/search.aspx?displaylang=en

- Microsoft Security Central
  http://www.microsoft.com/security/

- Microsoft TechNet Security TechCenter
  http://technet.microsoft.com/en-us/security/default.aspx

- Microsoft Technical Security Notifications
  http://www.microsoft.com/technet/security/bulletin/notify.mspx

- Microsoft Windows Update Web site
  http://windowsupdate.microsoft.com/

- Security Bulletins
  http://signup.alerts.live.com/brochure/index.jsp

- Windows Server Update Services
  http://technet.microsoft.com/en-us/wsus/default.aspx

F.5.3 *ΣΤ. 5.3 Γενικές Πηγές για την Ασφάλεια των Windows XP*

- *Group Policy Settings Reference for Windows Server 2003 with Service Pack 1*
  http://www.microsoft.com/downloads/details.aspx?FamilyID=7821c32f-da15-438d-8e48-45915cd2bc14&displaylang=en

- *Home and Small Office Network Topologies*
  http://technet.microsoft.com/en-us/library/bb457037.aspx

- *Securing Mobile Computers with Windows XP Professional*
  http://technet.microsoft.com/en-us/library/bb457043.aspx

- *Step-by-Step Guide to Securing Microsoft Windows XP Professional with Service Pack 2 in Small and Medium Businesses*
  http://www.microsoft.com/windowsxp/using/security/learnmore/smbsecurity.mspx

- *Threats and Countermeasures Guide: Security Settings in Windows Server 2003 and Windows XP*
  http://www.microsoft.com/downloads/details.aspx?FamilyId=1B6ACF93-147A-4481-9346-F93A4081EEA8&displaylang=en

- *What's New in Security for Windows XP Professional and Windows XP Home Edition*
  http://technet.microsoft.com/en-us/library/bb457059.aspx

- *Windows XP Baseline Security Checklists*
  http://www.microsoft.com/technet/archive/security/chklist/xpcl.mspx?mfr=true

- *Windows XP Security Guide v2.2*
  http://www.microsoft.com/downloads/details.aspx?familyid=2D3E25BC-F434-4CC6-A5A7-09A8A229F118&displaylang=en

- *Windows XP Service Pack 2 (SP2) Solution Center*
  http://support.microsoft.com/ph/6794

F.5.4 *Συγκεκριμένες Πηγές για την Ασφάλεια των Windows XP*

- *Configuring Windows XP IEEE 802.11 Wireless Networks for the Home and Small Business*
  http://www.microsoft.com/technet/network/wifi/wifisoho.mspx

- *Data Protection and Recovery in Windows XP*
  http://technet.microsoft.com/en-us/library/bb457020.aspx

- *Don’t Let the Defense Rest: Securing Home Networks with Windows XP*
  http://www.microsoft.com/windowsxp/using/networking/expert/bowman_november12.mspx

- *Encrypting File System in Windows XP and Windows Server 2003*
  http://technet.microsoft.com/en-us/library/bb457065.aspx

- *Get Started Using Remote Desktop with Windows XP Professional*
  http://www.microsoft.com/windowsxp/using/mobility/getstarted/remoteintro.mspx

- *Guide for Installing and Deploying Updates for Microsoft Windows XP Service Pack 2*
  http://technet.microsoft.com/en-us/library/bb457071.aspx

- *How NTFS Works*
  http://technet.microsoft.com/en-us/library/cc781134.aspx

- *How to Set Up and Use Automated System Recovery in Windows XP*
  http://technet.microsoft.com/en-us/library/bb456980.aspx

- *How to Share Files Using Encrypting File System*
  http://www.microsoft.com/windowsxp/using/security/expert/sharefilesefs.mspx

- *How to Use Sysprep: An Introduction*
  http://technet.microsoft.com/en-us/library/bb457073.aspx

- *Manage Your Computer's Security Settings in One Place*
  http://www.microsoft.com/windowsxp/using/security/internet/sp2_wscintro.mspx

- *NTFS vs. FAT: Which Is Right for You?*
  http://www.microsoft.com/windowsxp/using/setup/expert/russel_october01.mspx

- *Predefined Security Templates*
  http://technet.microsoft.com/en-us/library/cc787720.aspx

- *Remote Installation Services*
  http://technet.microsoft.com/en-us/library/cc786442.aspx

- *Securing Wireless LANs with Certificate Services*
  http://www.microsoft.com/technet/security/prodtech/windowsserver2003/pkiwire/swlan.mspx?mfr=true

- *Securing Wireless LANs with PEAP and Passwords*
  http://www.microsoft.com/downloads/details.aspx?FamilyID=60c5d0a1-9820-480e-aa38-63485eca8b9b&displaylang=en

- *Set Up a Wired Network*
  http://www.microsoft.com/windowsxp/using/networking/setup/wired.mspx

- *Step-by-Step Guide to Internet Protocol Security (IPSec)*
  http://technet.microsoft.com/en-us/library/bb742429.aspx

- *Stored User Names and Passwords Overview*
  http://technet.microsoft.com/en-us/library/cc786845.aspx

- *Universal Plug and Play in Windows XP*
  http://technet.microsoft.com/en-us/library/bb457049.aspx

- *Using Software Restriction Policies to Protect Against Unauthorized Software*
  http://technet.microsoft.com/en-us/library/bb457006.aspx

- *Wireless Networking*
  http://technet.microsoft.com/en-us/network/bb530679.aspx

- *Windows Server 2003 System Services Reference*

http://www.microsoft.com/downloads/details.aspx?FamilyID=b38a0682-2997-4678-9d9e-a07cc66a3bba&displaylang=en

- *Wireless Deployment Technology and Component Overview*
  http://technet.microsoft.com/en-us/library/bb457015.aspx

- *The Wireless XP Wireless Zero Configuration Service: The Cable Guy, November 2002*
  http://technet.microsoft.com/en-us/library/bb878124.aspx

F.5.5 *Άρθρα της Microsoft Knowledge Base*

- Άρθρο 143475, *Windows NT System Key Permits Strong Encryption of the SAM*
  http://support.microsoft.com/?id=143475

- Άρθρο 217098, *Basic Overview of Kerberos User Authentication Protocol in Windows 2000*
  http://support.microsoft.com/?id=217098

- Άρθρο 243330, *Well-known security identifiers in Windows operating systems*
  http://support.microsoft.com/?id=243330

- Άρθρο 254649, *Overview of memory dump file options for Windows Server 2003, Windows XP, and Windows 2000*
  http://support.microsoft.com/?id=254649

- Άρθρο 279765, *How to Use the Fast User Switching Feature in Windows XP*
  http://support.microsoft.com/?id=279765

- Άρθρο 282784, *Qfecheck.exe verifies the installation of Windows 2000 and Windows XP hotfixes*
  http://support.microsoft.com/?id=282784

- Άρθρο 294739, *A discussion about the availability of the Fast User Switching feature*
  http://support.microsoft.com/?id=294739

- Άρθρο 296861, *How to install multiple Windows updates or hotfixes with only one reboot*
  http://support.microsoft.com/?id=296861

- Άρθρο 304040, *How to configure file sharing in Windows XP*
  http://support.microsoft.com/?id=304040

- Άρθρο 307973, *How to configure system failure and recovery options in Windows*
  http://support.microsoft.com/?id=307973

- Άρθρο 308422, *How to use the Backup utility that is included in Windows XP to back up files and folders*
  http://support.microsoft.com/?id=308422

- Άρθρο 309340, *How to use Backup to protect data and restore files and folders on your computer in Windows XP and Windows Vista*
  http://support.microsoft.com/?id=309340

- Άρθρο 310749, *New Capabilities and Features of the NTFS 3.1 File System*
  http://support.microsoft.com/?id=310749

- Άρθρο 314343, *Basic Storage Versus Dynamic Storage in Windows XP*
  http://support.microsoft.com/?id=314343

- Άρθρο 314834, *How to Clear the Windows Paging File at Shutdown*
  http://support.microsoft.com/?id=314834

- Άρθρο 314984, *How to create and delete hidden or administrative shares on client computers*
  http://support.microsoft.com/?id=314984

- Άρθρο 320820, *How to Use the Backup utility to back up files and folders in Windows XP Home Edition*
  http://support.microsoft.com/?id=320820

- Άρθρο 322389, *How to obtain the latest Windows XP service pack*
  http://support.microsoft.com/?id=322389

- Άρθρο 330904, *Messenger Service window that contains an Internet advertisement appears*
  http://support.microsoft.com/?id=330904

- Άρθρο 810207, *IPSec default exemptions are removed in Windows Server 2003*
  http://support.microsoft.com/?id=810207

- Άρθρο 837243, *Availability and description of the Port Reporter tool*
  http://support.microsoft.com/?id=837243

- Άρθρο 832017, *Service overview and network port requirements for the Windows Server system*
  http://support.microsoft.com/?id=832017

- Άρθρο 875352, *A detailed description of the Data Execution Prevention (DEP) feature in Windows XP Service Pack 2, Windows XP Tablet PC Edition 2005, and Windows Server 2003*
  http://support.microsoft.com/?id=875352

- Άρθρο 890830, *The Microsoft Windows Malicious Software Removal Tool helps remove specific prevalent malicious software from computers that are running Windows Vista, Windows Server 2003, Windows XP, or Windows 2000*
  http://support.microsoft.com/?id=890830

- Άρθρο 893357, *The Wi-Fi Protected Access 2 (WPA2)/Wireless Provisioning Services Information Element (WPS IE) update for Windows XP with Service Pack 2 is available*
  http://support.microsoft.com/?id=893357

- Άρθρο 894193, *How to obtain and use the Enterprise Scan Tool*
  http://support.microsoft.com/?id=894193

F.5.6 *Πηγές Σχετικές με το Windows XP SP3*

- *Overview of Windows XP Service Pack 3*
  http://download.microsoft.com/download/6/8/7/687484ed-8174-496d-8db9-f02b40c12982/Overview%20of%20Windows%20XP%20Service%20Pack%203.pdf

- Άρθρο της Knowledge Base 936929, *Information about Windows XP Service Pack 3*
  http://support.microsoft.com/?id=936929

- Windows XP Service Packs
  http://technet.microsoft.com/en-us/windows/bb410118.aspx

F.6 Άλλες Διαδικτυακές Πηγές

- *How Windows Server 2003's Software Restriction Policies Improve Security*
  http://www.windowsecurity.com/articles/windows_2003_restriction_policies_security.html

- *National Industrial Security Program Operating Manual*, DoD 5220.22-M, by the Department of Defense
  http://www.dtic.mil/whs/directives/corres/html/522022m.htm

- National Security Agency Security Recommendation Guides for Windows XP
  http://www.nsa.gov/snac/downloads_winxp.cfm

- *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, by the Department of Justice
  http://www.cybercrime.gov/s&smanual2002.htm

- Windows XP Resource Center
  http://labmice.techtarget.com/windowsxp/default.htm

- WinXPnews
  http://www.winxpnews.com/

Παράρτημα G

G. Ακρωνύμια και Συντομογραφίες

Τα ακρωνύμια και οι συντομογραφίες που χρησιμοποιήθηκαν στον οδηγό, ορίζονται παρακάτω.

0-9	**3DES**	Triple Data Encryption Standard
A	**ACE**	Access Control Entry
	ACL	Access Control List
	AD	Active Directory
	AES	Advanced Encryption Standard
	AP	Access Point
	AS	Authentication Service
B	**BIOS**	Basic Input/Output System
C	**CCE**	Common Configuration Enumeration
	CD	Compact Disk
	CHAP	Challenge Handshake Authentication Protocol
	CIFS	Common Internet File System
	CIS	Center for Internet Security
	CS	Client/Server
D	**DCOM**	Distributed Component Object Model
	DEP	Data Execution Prevention
	DES	Data Encryption Standard
	DESX	Extended Data Encryption Standard
	DHCP	Dynamic Host Configuration Protocol
	DHS	Department of Homeland Security
	DIMS	Digital Identity Management Service
	DISA	Defense Information Systems Agency
	DLL	Dynamic Link Library
	DNS	Domain Name System
	DoS	Denial of Service
	DRA	Data Recovery Agent
	DTC	Distributed Transaction Coordinator
E	**ECM**	Enterprise Configuration Manager
	EFS	Encrypting File System
	e-mail	Electronic mail
F	**FAT**	File Allocation Table
	FDCC	Federal Desktop Core Configuration
	FEK	File Encryption Key
	FIPS	Federal Information Processing Standards
	FISMA	Federal Information Security Management Act
	FTP	File Transfer Protocol

	FUS	Fast User Switching
G		
	GB	Gigabyte
	GINA	Graphical Identification and Authentication
	GPMC	Group Policy Management Console
	GPO	Group Policy Object
	GUI	Graphical User Interface
H		
	HKLM	HKEY_Local_Machine
	HTML	Hypertext Markup Language
	HTTP	HyperText Transfer Protocol
	HTTPS	HTTP Over SSL
I		
	ICF	Internet Connection Firewall
	ICMP	Internet Control Message Protocol
	ICS	Internet Connection Sharing
	IE	Internet Explorer
	IE7	Internet Explorer version 7
	IETF	Internet Engineering Task Force
	IIS	Internet Information Services
	IKE	Internet Key Exchange
	IM	Instant Messaging
	IP	Internet Protocol
	IPsec	IP Security
	IRC	Internet Relay Chat
	IT	Information Technology
	ITL	Information Technology Laboratory
L		
	L2TP	Layer 2 Tunneling Protocol
	LAN	Local Area Network
	LM	LanManager
M		
	MBSA	Microsoft Baseline Security Analyzer
	MMC	Microsoft Management Console
	MS	Microsoft
	MTU	Maximum Transmission Unit
N		
	NAP	Network Access Protection
	NAT	Network Address Translation
	NetBT	NetBIOS over TCP/IP
	NIC	Network Interface Card
	NIST	National Institute of Standards and Technology
	NSA	National Security Agency
	NTFS	NT File System
	NTLM	NT LanManager
	NTP	Network Time Protocol
	NVD	National Vulnerability Database
	NX	No Execute

O	**OMB**	Office of Management and Budget
	OS	Operating System
	OU	Organizational Unit
P	**P2P**	Peer-to-Peer
	PIN	Personal Identification Number
	PKI	Public Key Infrastructure
	PPTP	Point-to-Point Tunneling Protocol
Q	**QoS**	Quality of Service
R	**RA**	Remote Assistance
	RC	Release Candidate
	RCE	Route Cache Entry
	RDP	Remote Desktop Protocol
	RFC	Request for Comment
	RIS	Remote Installation Service
	RPC	Remote Procedure Call
	RSVP	Resource Reservation Protocol
S	**SACL**	System Access Control List
	SAM	Security Accounts Manager
	SCAP	Security Content Automation Protocol
	SID	Security Identify
	SMB	Server Message Block
	SMS	Systems Management Server
	SMTP	Simple Mail Transport Protocol
	SNMP	Simple Network Management Protocol
	SOHO	Small Office Home Office
	SP	Service Pack
	SP2	Service Pack 2
	SP3	Service Pack 3
	SQL	Structured Query Language
	SR	Service Release
	SSDP	Simple Service Discovery Protocol
	SSH	Secure Shell
	SSID	Service Set Identifier
	SSL	Secure Sockets Layer
	SUS	Software Update Services
T	**TCP**	Transmission Control Protocol
	TCP/IP	Transmission Control Protocol/Internet Protocol
	TGS	Ticket-Granting Service
	TLS	Transport Layer Security
U	**UDP**	User Datagram Protocol
	UI	User Interface
	UPnP	Universal Plug and Play
	UPS	Uninterruptible Power Supply
	URL	Uniform Resource Locator

	US-CERT	United States Computer Emergency Readiness Team
V	**VBS**	Visual Basic Script
	VoIP	Voice over IP
	VPN	Virtual Private Network
W	**WebDAV**	Web Distributed Authoring and Versioning
	WEP	Wired Equivalent Privacy
	Wi-Fi	Wireless Fidelity
	WPA	Wi-Fi Protected Access
	WPA2	Wi-Fi Protected Access Version 2
	WUS	Windows Update Services
	WSUS	Windows Server Update Services