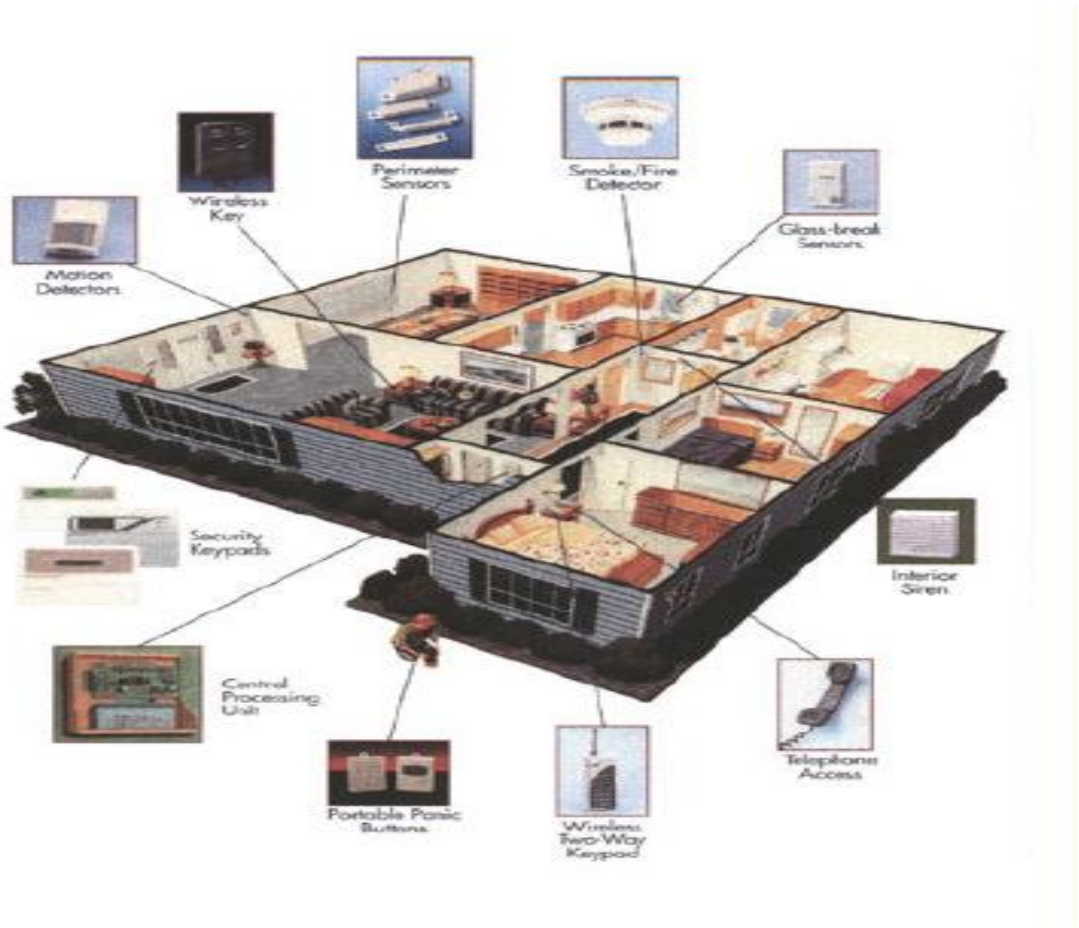
ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή εργασία

«Μελέτη φυσικής, διαχειριστικής και πληροφοριακής ασφάλειας των εγκαταστάσεων ενός βιομηχανικού περιβάλλοντος»



Του Φοιτητή:

Βλισίδη Γεώργιου

Αριθμός Μητρώου: 991359

Επιβλέπων καθηγητής:

Δρ. Δασυγένης Μηνάς

Θεσσαλονίκη 2009

ΠΡΟΛΟΓΟΣ

Η έννοια της ασφάλειας έχει αρχίσει να απασχολεί ένα μεγάλο μέρος της επιχειρηματικής κοινότητας κυρίως λόγο των σύνθετων συνθηκών που διαμορφώνονται σε παγκόσμιο επίπεδο.

Η ασφάλεια μιας βιομηχανίας ήταν πάντα συνυφασμένη με την οικονομική αξία και τη σπουδαιότητα των υλικών αγαθών που ειδικεύεται. Οι κίνδυνοι που διατρέχει μια εταιρία μπορεί να είναι είτε η ανθρώπινη δραστηριότητα, είτε κίνδυνοι από το εξωτερικό περιβάλλον. Και στις δύο περιπτώσεις ο παρονομαστής είναι κοινός. Θέτεται σε άμεσο κίνδυνο η ακεραιότητα και η σωστή λειτουργία της.

Η εξέλιξη της τεχνολογίας είχε αμφίδρομη επιρροή στο ζήτημα του κινδύνου και της αποτελεσματικής του αντιμετώπισης. Από την κάθε πλευρά γίνεται ότι είναι δυνατό για την ανάπτυξη συστημάτων και εργαλείων που να εξυπηρετούν το σκοπό αυτό. Επομένως θα λέγαμε ότι το κίνητρο για κλοπή, βανδαλισμό, ιδιοποίηση και ότι άλλη περίπτωση απειλής υπάρχει τροφοδοτεί με νέες ιδέες και ταχύτερη εξέλιξη της τεχνολογίας για την αντιμετώπιση αυτής και ταυτόχρονα ισχύει και ακριβώς το αντίστροφο. Παράλληλα, η καταστροφική επέμβαση το ανθρώπου στο περιβάλλον, έχει προκαλέσει μια μεγάλη κλιματική αλλαγή την οποία όλο και πιο συχνά την εισπράττει η κοινωνία μας με την μορφή κάποιου ακραίου καιρικού φαινομένου.

Ο πιο σημαντικός παράγοντας που μπορεί να εγγυηθεί την ασφάλεια είναι ο άνθρωπος. Και αυτό γιατί είναι ο νοήμον παράγοντας σε όλη τη διαδικασία της ασφάλειας, που θα εντοπίσει, θα συλλέξει τα στοιχεία, θα πάρει αποφάσεις για να προσαρμόσει τα συστήματα που θα προστατεύσουν αυτόν και την περιουσία του.

Όπως είπαμε προηγουμένως, η εξέλιξη της τεχνολογίας έχει κάνει την έννοια της ασφάλειας πιο περίπλοκη διαδικασία. Πέρα από την συνεχή εκπαίδευση πάνω στις μεθόδους και στην εξέλιξη των συστημάτων ασφαλείας, έχουν δημιουργηθεί ειδικότητες που αντιμετωπίζουν το ζήτημα της ασφάλειας ολοκληρωμένα ενώνοντας όλες τις πτυχές που αυτή περιλαμβάνει.

ΠΕΡΙΛΗΨΗ

Σκοπός αυτής της πτυχιακής εργασίας είναι η ολοκληρωμένη θεωρητική και πρακτική μελέτη των μέτρων ασφαλείας, που χρειάζεται να παρθούν για ένα βιομηχανικό περιβάλλον τόσο σε φυσικό, όσο και σε δικτυακό επίπεδο και να προταθούν τρόποι αποτελεσματικότερης προσέγγισης του θέματος της ασφάλειας.

Η επιλογή γίνεται για μια εταιρία με σημαντικά περιουσιακά και ερευνητικά στοιχεία, ώστε να αντιστοιχούν και τα μέτρα ασφαλείας που μελετώνται. Τα χωροταξικά σχέδια που παρουσιάζονται είναι δημιουργία του συγγραφέα.

Η εργασία δίνει το μεγαλύτερο βάρος στα μέτρα ασφαλείας, που παίρνονται σε κάθε τομέα και λιγότερο στο στήσιμο και την εγκατάσταση τους. Δεν γίνεται παρουσίαση του πως στήθηκε ο δίκτυο, το οποίο σε ένα βαθμό έγινε, αλλά ποιες παραμέτρους ρυθμίσαμε για να αυξήσουμε την ασφάλεια του.

Παρουσιάζονται οι πιθανοί κίνδυνοι, που μπορεί να εκδηλωθούν με διάφορους τρόπους και σε διάφορους στόχους της εταιρίας. Πατώντας πάνω σε αυτούς τους υπαρκτούς κινδύνους, προσαρμόζουμε την ασφάλεια και ταυτόχρονα δίνουμε βάρος στα μέτρα που θα αποτρέψουν τον εισβολέα.

Γίνεται μια παρουσίαση της τεχνολογίας εικονοποίησης (virtualization), των χρήσεων και των ωφελειών της, σαν μια εναλλακτική μέθοδο ασφάλειας. Προσαρμόστηκε στο δίκτυο της εταιρίας και κάναμε μια προσπάθεια να μελετήσουμε μέχρι σε ποιο σημείο μπορεί να εφαρμοστεί.

Επίσης γίνεται μελέτη ενός πλήρους σχεδίου λήψης αντιγράφων ασφαλείας και του σχεδίου, με το οποίο σε πιθανή καταστροφή, βλάβη, ή δυσλειτουργία, θα ανανήψει το σύστημα και θα λειτουργήσει ξανά σωστά.

Τέλος, για την κάθε περίπτωση γίνεται μια προσέγγιση του οικονομικού κόστους που θα έχει το κάθε μέτρο και ένας προϋπολογισμός ολόκληρου του έργου.

ABSTRACT

The scope of the present diploma thesis is a full theoretical and practical study of the security measures needed for an industrial company, with respect to the physical as well as the network security and to propose certain ways of a more effective approach of the security matters.

A company of significant assets was chosen, so that the proposed measures are compatible. All land-planning designs are derived from the author.

The present study concentrates in the several types of measures are taken in the way that they are applied. The network set-up, although done to an extent, is not presented as the present study focuses on the parameters that were controlled in order to increase system security.

All risks that might be present in various ways and at several company targets are presented. Taking into account those risks we adjust the safety measures and at the same time concentrate on prevention of a presumptive system intrusion.

The uses and benefits of the virtualization technology are presented, as an alternative security method. The virtualization technology was adjusted to the network of the theoretic company, and it was attempted to study the limits of its implementation.

Furthermore, a plan of full system back-up, as well as a damage recovery plan that in case of system damage, break-down or malfunction would facilitate system redundancy, were studied.

Finally, the costs of each proposed security measures as well as the total budget of the security plan are estimated.

ΕΥΡΕΤΗΡΙΟ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Η ασφάλεια είναι ένας από τους πιο πολυσυζητημένους τομείς των τελευταίων ετών και αποτελεί αντικείμενο μελέτης για συνεχή εξέλιξη. Η συσσωρευμένη πείρα της τελευταίας 20ετίας, αλλά και η μεγάλη εξέλιξη των αυτόματων συστημάτων έχει επιφέρει μεγάλη πολυπλοκότητα στη διαχείρισή της. Είναι πλέον απαραίτητο όσοι ασχολούνται με την ασφάλεια να είναι ειδικευμένοι σε μια σειρά τομείς, ώστε να μπορούν να ανταπεξέλθουν σε αυτό το σύνθετο χώρο.

Στην παρούσα πτυχιακή εργασία γίνεται μια προσπάθεια να περιγραφούν αναλυτικά οι παράμετροι, που επηρεάζουν την ασφάλεια ενός βιομηχανικού περιβάλλοντος και να καταδείξουμε τρόπους για την αποτελεσματικότερη ασφάλεια αυτού.

Στο πρώτο κεφάλαιο, περιλαμβάνεται η φυσική ασφάλεια του κτιρίου. Αναλύεται η περιμετρική ασφάλεια, μελετούνται μέθοδοι επόπτευσης των εγκαταστάσεών της και προτείνονται διάφορα τεχνολογικά μέσα, το οποία πρέπει να εγκατασταθούν σε συγκεκριμένα σημεία σε όλους τους χώρους της εταιρίας.

Στο δεύτερο κεφάλαιο, μπαίνουν αναλυτικά τα δικαιώματα και οι υποχρεώσεις όσων εργάζονται στην εταιρία. Θέτονται οι κανόνες συμπεριφοράς, χρήσης και αξιοποίηση των πόρων του υπολογιστικού συστήματος. Ξεκαθαρίζεται τι πρέπει και τι δεν πρέπει να πράξει όποιος εργάζεται στην εταιρία.

Στο τρίτο κεφάλαιο, γίνεται η περιγραφή του τοπικού δικτύου, το οποίο είναι απομονωμένο από το διαδίκτυο. Το διαχειριζόμαστε μέσω 2 Windows Server 2003 με τη χρήση τω εργαλείων Active Directory και DFS Replication. Παίρνουμε μέτρα ασφαλείας στις υπόλοιπες συσκευές του δικτύου, όπως είναι το router και τα switches. Τέλος παίρνουμε μέτρα για τη σωστή διαχείριση των φακέλων από τους χρήστες σύμφωνα με την πολιτική ασφαλείας.

Στο τέταρτο κεφάλαιο, αναλύονται σε βάθος οι πολιτικές ασφαλείας των λογαριασμών. Παρουσιάζονται αναλυτικά όλες οι ρυθμίσεις που πρέπει να κάνει ένας διαχειριστής του δικτύου, ώστε να δημιουργήσει ασφαλείς λογαριασμούς χρηστών.

Στο πέμπτο κεφάλαιο, αρχικά γίνεται παρουσίαση των μεθόδων και των μέσων, που χρησιμοποιούνται για τη λήψη αντιγράφων ασφαλείας. Στη συνέχεια,

υλοποιείται ένα αναλυτικό σχέδιο για τα μέσα που θα χρησιμοποιήσει η εταιρία για τη λήψη αντιγράφων ασφαλείας καθώς και ένα χρονοδιάγραμμα που θα γίνεται αυτή η εργασία.

Στο έκτο κεφάλαιο, αναλύεται η σύνδεση στο διαδίκτυο. Παρουσιάζονται οι ρυθμίσεις ασφαλείας που πήραμε στους 3 server που θα χρησιμοποιήσουμε. Στη συνέχεια αναλύουμε το σύστημα τηλεφωνίας μέσω του δικτύου που έχει η εταιρία με τη χρήση των κατάλληλων συσκευών.

Στο έβδομο κεφάλαιο, γίνεται παρουσίαση του virtualization σαν εναλλακτική μέθοδο σε ορισμένες παραμέτρους ασφαλείας. Περιγράφεται αναλυτικά η χρήση του, τα πλεονεκτήματα του σε ένα οργανισμό και η υλοποίησή του. Στη συνέχεια πραγματοποιούμε μια εφαρμογή του για την εταιρία, αξιοποιώντας το υπάρχον υλικό της.

Στο όγδοο κεφάλαιο, δημιουργούμε το σχέδιο αναγνώρισης κινδύνων και ανάκαμψης μετά από καταστροφή. Αναλύουμε τους πιθανούς κινδύνους που μπορεί να εμφανιστούν και καταδεικνύουμε τα περιουσιακά στοιχεία της εταιρίας που μπορεί να προσβληθούν. Τέλος, για την κάθε περίπτωση παρουσιάζουμε το σχέδιο ανάκαμψης και ομαλής λειτουργίας της εταιρίας.

Στο ένατο κεφάλαιο, κάνουμε ανάλυση του κόστους για όλα τα μέσα που θα χρειαστούμε ώστε να δημιουργήσουμε ένα ασφαλές περιβάλλον για την εταιρία.

Τέλος στα παραρτήματα παρουσιάζεται μεταφρασμένο το πρότυπο ISO 17799, το οποίο βάζει τις γενικές κατευθύνσεις που πρέπει να ακολουθεί ένας ειδικός ασφαλείας καθώς επίσης, και μερικές λίστες αναφορών οι οποίες χρησιμοποιούνται από την εταιρία για να αυτοματοποιούν τη λειτουργία της και να βοηθούν στον αποδοτικότερο έλεγχό της.

Για την υλοποίηση της πτυχιακής εργασίας χρησιμοποιήθηκαν πολλά εργαλεία. Το βασικότερο ήταν το VMWARE στο οποίο αναπτύχθηκε ο κορμός της. Από εκεί πάνω δούλεψα με τα λειτουργικά συστήματα Windows Server 2003 R2 για τους βασικούς File Severs, Windows XP Professional για τη βοήθεια και επαλήθευση στις ρυθμίσεις του δικτύου, το FreeBSD για την δημιουργία του Backup PC, το FreeNAS για το NAS, το TrixBox για τον PBX Server το πρόγραμμα Xlite για την Voip τηλεφωνία, το λειτουργικό Ubuntu Linux 8.10 για το στήσιμο των Web, Mail και Proxy Server. Επίσης χρησιμοποίησα τα

προγράμματα Apache2, sendmail και squid για να στήσω τους παραπάνω Server. Τέλος, αξιοποίησα και το πρόγραμμα Office Visio 2007 για να δημιουργήσω την κάτοψη του κτιρίου και του περιμετρικού χώρου της εταιρίας, καθώς και την τοπολογία του τοπικού δικτύου και του διαδικτύου.

Κεφάλαιο 1

ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ ΚΤΙΡΙΟΥ

1.1 Εισαγωγή

Η ασφάλεια εγκαταστάσεων είναι μια ουσιαστική ανάγκη κάθε επιχείρησης η οποία απαιτεί επιτακτικά λύση, τόσο ως προς την επιτήρηση της φυσιολογικής λειτουργίας της, όσο και ως προς την προστασία από μη εξουσιοδοτημένες επεμβάσεις τρίτων. Προκειμένου να αντιμετωπισθεί το σημαντικό αυτό ζήτημα για την εύρυθμη λειτουργία και επιβίωση ενός οργανισμού ή μίας επιχείρησης, πρέπει να υπάρχει ολοκληρωμένη προσέγγιση, θεώρηση και εκτίμηση του κινδύνου και στη συνέχεια θωράκιση με δέσμη μέτρων, διαδικασιών και φυσικά κατάλληλου εξοπλισμού. Στόχος είναι ο σχεδιασμός μίας λύσης παρακολούθησης χώρου που να εγγυάται τον πλήρη έλεγχο της φυλασσόμενης περιοχής.
Οι κίνδυνοι που μια εταιρία διατρέχει χωρίζονται σε:

- **Περιβαλλοντικοί κίνδυνοι**. Πλημμύρες, σεισμοί, καταιγίδες και τυφώνες, πυρκαγιές κλπ.
- **Κίνδυνοι που αφορούν την υποστήριξη του συστήματος**. Διακοπές ρεύματος, διακοπές τηλεπικοινωνιών, κλπ.
- **Κίνδυνοι από ανθρώπινη ενέργεια και πρόθεση**. Μη εξουσιοδοτημένη πρόσβαση(εξωτερική και εσωτερική), δολιοφθορές, λάθη και ατυχήματα υπαλλήλων, βανδαλισμοί, απάτη, κλοπή κλπ.

Η φυσική ασφάλεια, σαν ιδέα, πρέπει να εκλαμβάνεται σαν ένα «κρεμμύδι», ένα σύνολο διαφορετικών επιπέδων ασφαλείας, συνεργαζόμενων μεταξύ τους, ώστε το ένα να συμπληρώνει τα κενά του άλλου. Βασικός σκοπός είναι, όπου αποτυγχάνει το ένα επίπεδο ασφαλείας, αναλαμβάνει το αμέσως επόμενο, ώστε να αποτρέψει τους επίδοξους εισβολείς. Οι άξονες που κινείται η ασφάλεια εγκαταστάσεων χωρίζονται σε 4 κατηγορίες, οι οποίες είναι:

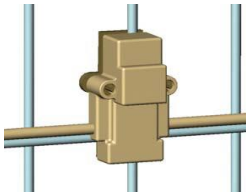
· Περιμετρική ασφάλεια
· Επόπτευση χώρων
· Ψηφιακή καταγραφή εικόνας
· Έλεγχος πρόσβασης

1.2 Περιμετρική ασφάλεια

Η περιμετρική ασφάλεια έχει να κάνει κυρίως με τους χώρους της εταιρίας, που βρίσκονται έξω από το κυρίως κτίριο της. Αφορά τον προαύλιο χώρο, τους φράχτες , την πρόσοψη του κτιρίου και άλλους πιθανούς χώρους που χρησιμοποιεί η εταιρία, πχ. εξωτερικό παρκινγκ.

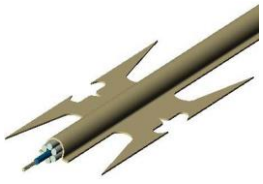
1.2.1 Φράχτες

Αποτελούν την οριογραμμή από την οποία ξεκινάει η δικαιοδοσία της επιχείρησης, καθορίζοντας το τι είναι «μέσα» και τι «έξω» από αυτήν. Η ύπαρξη του δείχνει ότι πίσω από αυτόν υπάρχει μια επιχείρηση, η οποία παίρνει σοβαρά το θέμα της ασφάλειας. Οι φράχτες είναι το πρώτο φυσικό εμπόδιο απέναντι σε αυτούς που έχουν σκοπό να εισβάλουν παράνομα στο χώρο της επιχείρησης μας. Παρόλα αυτά αποτελεί εμπόδιο που θα καθυστερήσει και δεν θα αποτρέψει τον εισβολέα.



Εικόνα 1-1

Για αυτό το λόγο πρέπει να φροντίσουμε, ώστε ο φράχτης να είναι το κατά δυνατόν πιο λειτουργικός σε αυτό που θέλουμε. Δηλαδή, δεν πρέπει να επιτρέπουμε να αναπτύσσονται φυτά πάνω του, γιατί αυτό δυσκολεύει να μπορούμε να βλέπουμε και πέρα από αυτόν, καθώς επίσης δυσκολεύει το γεγονός να εντοπίσουμε τυχόν τρύπες ή γενικότερες φθορές, που μπορεί να έχει υποστεί. Επίσης χρειάζεται να είναι αρκετά ψηλός, τουλάχιστο 2 μέτρα. Για να αυξήσουμε επιπλέον την ικανότητα

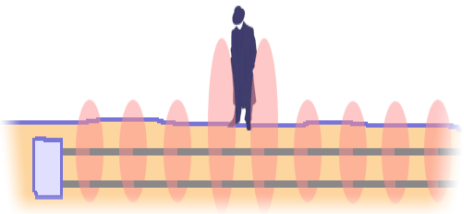


Εικόνα 1-2

αποτροπής, μπορούμε να προσαρμόσουμε και ειδικό συρματόπλεγμα στην κορυφή του με τον αισθητήρα μέσα στο σύρμα (εικόνα 1-2), ώστε να προσδιορίζεται ακριβέστερα το σημείο κοπής ή κάμψης και επιπλέον να τοποθετήσουμε πάνω του ειδικούς αισθητήρες που θα «πιάνουν» οποιοδήποτε κραδασμό του φράχτη. (εικόνα 1-1, 1-3) [1]

Εικόνα 1-3

Σε περίπτωση που κάποιος καταφέρει να περάσει από το φράχτη, μπορούμε να τοποθετήσουμε διαρρέον ομοαξονικό καλώδιο κάτω από το έδαφος. Η ιδιαιτερότητα στην κατασκευή του είναι ότι το φύλλο θωράκισης του έχει μικρές οπές, κατά μήκος του και έτσι το σήμα του εσωτερικού αγωγού διαρρέει ελαφρώς προς το περιβάλλον. Αντιστρόφως, το καλώδιο μπορεί να χρησιμοποιηθεί ως κεραία για να συλλαμβάνει τα ηλεκτρομαγνητικά κύματα από το περιβάλλον. Το σύστημα λειτουργεί ως εξής: δύο καλώδια τοποθετούνται κάτω από το έδαφος, παράλληλα μεταξύ τους και κατά μήκος της περιμέτρου. Το ένα καλώδιο λειτουργεί ως κεραία εκπομπής μιας RF συχνότητας, και το άλλο ως κεραία λήψης της. Έτσι το πεδίο που δημιουργείται, εάν διαταραχθεί στέλνει σήμα συναγερμού. Εκτός από την ανίχνευση της επιφάνειας του εδάφους, μπορεί να ανιχνεύσει και εισβολή και κάτω από αυτό με τη διάνοιξη σήραγγας, βάθους 1 – 1.5 μέτρα. (Εικόνα 1-4) http://www.perimetrica.com/background/tech_buried_coax.html [2]



Εικόνα 1-4

1.2.2 Πύλες εισόδου-εξόδου

Οι πύλες αποτελούν το ελεγχόμενο σημείο εισόδου από τους φράχτες. Είναι το σημείο το οποίο στοχοποιείται πιο συχνά από τους εισβολείς, που θέλουν να εισέλθουν στις εγκαταστάσεις της εταιρίας. Αντικειμενικά, είναι η τρύπα στο φράχτη, για αυτό και πρέπει να παρθούν επιπρόσθετα μέτρα για τον καλύτερο έλεγχο αυτών που τις πλησιάζουν και εισέρχονται.

Είναι απαραίτητη η παρουσία ενός φύλακα, που να μπορεί να εποπτεύει το χώρο. Επίσης μπορούμε να τοποθετήσουμε επιπλέον κάμερες παρακολούθησης στα σημεία εκείνα. Ένα ακόμα μέτρο είναι ο οποιοσδήποτε θέλει να μπει να υπογράφει πρώτα σε βιβλίο επισκεπτών και να κρατούνται κάποια προσωπικά δεδομένα του, πχ στοιχεία ταυτότητας- διπλώματος, από τον φύλακα και στη συνέχεια να υπογράφει και δεύτερη φορά κατά την έξοδό του. [3]

1.2.3 Φωτισμός

Ο φωτισμός παρόλο που είναι μια από τις σημαντικότερες πτυχές της ασφάλειας, συχνά δεν λαμβάνεται υπόψη λόγω του ότι έχουμε συνηθίσει να δουλεύουμε μέρα με επαρκή ηλιακό φωτισμό, ή γενικότερα την έννοια του φωτισμού την έχουμε στο μυαλό μας σαν κάτι βοηθητικό στην καθημερινότητά μας. Ο φωτισμός, όμως, σαν αντικείμενο ασφάλειας είναι κάτι αρκετά διαφορετικό.

Οι προβολείς φωτισμού, που θα χρησιμοποιηθούν, πρέπει να είναι έτσι σχεδιασμένοι ώστε να μην αφήνουν σημεία, εκτός από συγκεκριμένες περιπτώσεις, ακάλυπτα στο σκοτάδι, γιατί τότε αυξάνουν την πιθανότητα και τον κίνδυνο παραβιάσεων, ακόμα και ατυχημάτων.

Πλήρως φωτισμένη πρέπει να είναι η εξωτερική περίφραξη. Ο περιμετρικός φωτισμός πρέπει να είναι ανά περίπου 25 μέτρα, σε σιδηροϊστούς ύψους 7 μέτρων ή ιστούς 4 μέτρων εφόσον στηρίζονται σε σταθερή περίφραξη, με λαμπτήρες 250W και με την εκτυφλωτική δέσμη φωτός των προβολέων προς την εξωτερική πλευρά της περίφραξης προς την κατεύθυνση των πιθανών προσβάσεων και όχι προς το μέρος που είναι οι φύλακες. [3]

Επίσης δυνατό φωτισμό χρειάζεται να προβλέψουμε και στις πύλες εισόδου-εξόδου, καθώς είπαμε και προηγουμένως αποτελούν από τα πιο τρωτά σημεία της εξωτερικής περίφραξης. Αντιθέτως τα σημεία στα οποία υπάρχουν φύλακες, ή κατά μήκος γραμμών περιπολίας από τους κινούμενους φύλακες, ο φωτισμός πρέπει να έχει μικρότερη ένταση. Αυτό το κάνουμε για το γεγονός, ότι δεν πρέπει τα άτομα, που σκοπεύουν να εισέλθουν, να γνωρίζουν που βρίσκονται οι φύλακες.

Αυτό είναι καλό και για να μειώνεται ο κίνδυνος να στοχοποιείται ο φύλακας, αλλά και για να μπορεί το ανθρώπινο μάτι να προσαρμόζεται καλύτερα στο σκοτάδι.

Ο φωτισμός πρέπει να «δένει» αρμονικά και με άλλες επιλογές ασφαλείας που έχουμε πάρει. Πχ με τις κάμερες. Αν δεν υπάρχει επαρκής φωτισμός στα σημεία εστιάσεως των καμερών, τότε ουσιαστικά αχρηστεύεται όλο το σύστημα. Οι κάμερες ασφαλείας, μπορούν κάλλιστα να συνδυαστούν σε κάποια κρίσιμα σημεία τις περιμέτρου, με ειδικούς προβολείς που έχουν αισθητήρες ανίχνευσης κίνησης, έτσι ώστε να αλληλοβοηθούνται στον εντοπισμό οπουδήποτε κινείται στην περιοχή, την οποία έχουμε προσδιορίσει σαν επικίνδυνη.

1.3 Επόπτευση χώρων

1.3.1 Φύλακες

Το ανθρώπινο δυναμικό, σαν οντότητα, είναι από τα πιο σημαντικά στοιχεία της ασφάλειας. Αυτό ισχύει και για τους φύλακες που μπορεί να χρησιμοποιηθούν είτε στην πύλη εισόδου-εξόδου, είτε στην περιπολία γύρω από το κτίριο της εταιρίας.

Το μεγαλύτερο πλεονέκτημα τους, είναι η εύκολη προσαρμοστικότητα σε οποιοδήποτε περιβάλλον και κατάσταση μπορεί να διαμορφωθεί κάποια στιγμή. Χρησιμοποιούν τη λογική για να αντιδρούν σε πιθανές εξωτερικές παρεμβάσεις, παίρνουν αποφάσεις για οτιδήποτε προκύψει και δεν είναι στατικοί.

Για την μέγιστη δυνατή ασφάλεια της εταιρίας, ορίζουμε ότι η παρουσία φυλάκων, θα είναι συνεχής επί 24ώρου βάσεως. Άρα χρειαζόμαστε σε κάθε βάρδια (8 ωρών) 3 φύλακες, έναν για την κεντρική πύλη και δύο που θα κάνουν πεζές περιπολίες σε όλη την περίμετρο των κτιριακών εγκαταστάσεων. [3]

1.3.2 Συστήματα ανίχνευσης εισβολέων (Intrusion Detection Systems-IDSs)

Τα συστήματα ανίχνευσης εισβολέων (IDS), σε αντίθεση με τις κάμερες, που παρακολουθούν για ασυνήθιστη συμπεριφορά, χρησιμοποιούνται για να ελέγχουν μη εξουσιοδοτημένη είσοδο και ειδοποιούν τα υπεύθυνα άτομα να ανταποκριθούν. Αυτά τα συστήματα μπορούν να μαγνητοσκοπούν εισόδους, πόρτες, παράθυρα, συσκευές κ.α.

Ένα IDS μπορεί να χρησιμοποιηθεί για να ανιχνεύει τις παρακάτω μεταβολές:

- Σε φωτοκύτταρα
- Σε ήχους και δονήσεις
- Σε κίνηση
- Σε διάφορους τύπους πεδίων (μαγνητικά, μικροκομματικά, ηλεκτροστατικά)
- Σε διακοπή ρεύματος

Τα IDS μπορούν, επίσης, να ανιχνεύσουν εισβολείς χρησιμοποιώντας ηλεκτρομηχανικά συστήματα, όπως είναι οι μαγνητικοί διακόπτες, μεταλλικά ελάσματα στα παράθυρα, πλάκες πίεσης, ή ηχητικομετρικά συστήματα. Τα τελευταία είναι πολύ πιο ευαίσθητα επειδή ανιχνεύουν αλλαγές σε πολύ «λεπτά»-ανεπαίσθητα περιβαλλοντικά χαρακτηριστικά, όπως οι δονήσεις, τα μικροκύματα, οι υπερηχητικές συχνότητες, υπέρυθρες και φωτοηλεκτρικές αλλαγές.

Τα συστήματα IDS μπαίνουν σε λειτουργία όταν οι εργαζόμενοι έχουν φύγει και μένει πίσω μόνο το προσωπικό. Ουσιαστικά δείχνουν ότι από εκείνη τη στιγμή και μετά κανείς δεν θα πρέπει να κυκλοφορεί στο κτίριο, εκτός από το εξουσιοδοτημένο προσωπικό. [3]

Για αυτό τα παράθυρα και η κεντρική είσοδος θα παρακολουθούνται από αισθητήρες κίνησης προσαρμοσμένους πάνω τους.(εικόνα 1-5).

Επίσης για τον κεντρικό κοινόχρηστο χώρο κατά την είσοδο στο κτίριο μπορούμε να βάλουμε και αισθητήρες κίνησης οροφής για να καλύπτουν μεγαλύτερο εύρος σε σημεία, που δεν φτάνει η εμβέλεια των αισθητήρων στα

παράθυρα (εικόνα 1-6). Ο συγκεκριμένος από 5 μέτρα ύψος έχει εμβέλεια διαμέτρου 18 μέτρων, και κάλυψη 360^{o}.

Στην κεντρική είσοδο, αλλά και στην είσοδο του δωματίου με τους servers τοποθετούμε μπάρες με υπέρυθρες ακτίνες . Στις εισόδους αυτές τοποθετούμε και κάμερες παρακολούθησης για να ελέγχουμε ποιος τις προσεγγίζει, αλλά και σε περιπτώσεις ανάγκης που χρειαστεί κάποιος τεχνικός να εισέλθει, να μπορεί ο υπεύθυνος από το control room να τις απενεργοποιήσει για όσο χρειαστεί (εικόνα1-7).

Στους όλους διαδρόμους θα υπάρχουν αισθητήρες κίνησης (εικόνα 1-8).

Περιμετρικά και σε απόσταση 1-2 μέτρα από τον εξωτερικό τοίχο του κτιρίου θα τοποθετήσουμε εξωτερικούς αισθητήρες κίνησης, οι οποίοι είναι μεγαλύτερης εμβέλειας. Οι αισθητήρες αυτοί έχουν τη δυνατότητα ομαλής λειτουργίας και σε δύσκολες καιρικές συνθήκες -25 έως +60 ^{o} C.(εικόνα 1-9). Επίσης σε κάθε γωνία στο κτιρίου θα τοποθετηθούν κάμερες που θα στέλνουν εικόνα από όλη την περίμετρο του κτιρίου. [4]

Εικόνα 1-5

Εικόνα 1-6

Εικόνα 1-7

Εικόνα 1-8

Εικόνα 1-9

1.3.3 Συστήματα πυρασφάλειας

Μια εταιρία πρέπει να ακολουθεί τα διεθνή πρότυπα για την πρόληψη, ανίχνευση και κατάσβεση πυρκαγιάς.

Η **πρόληψη** έχει να κάνει με την εκπαίδευση των εργαζομένων για το πώς να αντιδράνε σωστά όταν έρχονται αντιμέτωποι με τη φωτιά, την προμήθεια του κατάλληλου εξοπλισμού και την εξασφάλιση ότι αυτός ανά πάσα στιγμή λειτουργεί, το να είναι οι πυροσβεστήρες εύκολα προσβάσιμοι και η χρήση εύφλεκτων υλικών να είναι η ενδεδειγμένη.

Η **ανίχνευση** της φωτιάς γίνεται από μια ποικιλία συστημάτων. Υπάρχουν τα χειροκίνητα μέσα και αυτόματα. Τα δεύτερα έχουν αισθητήρες, οι οποίοι αντιδρούν στην παρουσία καπνού ή φωτιάς.

Η **κατάσβεση** της φωτιάς, μπορεί να επιτευχθεί με τη χρήση πυροσβεστικής μάνικας που πρέπει να έχουν όλοι οι κλειστοί χώροι, ή με τη χρήση των αυτόματων συστημάτων, όπως οι ψεκαστήρες οροφής.

Εικόνα 1-10

Εικόνα 1-11

Επομένως σε κάθε τμήμα και σε διαδρόμους θα πρέπει να υπάρχουν ανιχνευτές καπνού, και πυροσβεστήρες (εικόνα 1-10 και 1-11). **Ο κύριος σκοπός τους σχεδίου πυρασφάλειας είναι όλο το ανθρώπινο δυναμικό να βγει με ασφάλεια από το κτίριο και να μην κινδυνέψει κανένας**. [4]

1.3.4 Συστήματα καταγραφής υγρασίας - θερμοκρασίας

Αυτά τα συστήματα τοποθετούνται συνήθως σε όλους τους εσωτερικούς χώρους του κτιρίου, για να μπορούμε να παρακολουθούμε τις συνθήκες μέσα στις οποίες συνυπάρχουν εργαζόμενοι και εξοπλισμός. Σε κάθε χώρο, πρέπει να παίρνονται τα κατάλληλα μέτρα ανάλογα με τις ιδιαιτερότητες.

Εικόνα 1-12

Λόγου χάρη στο δωμάτιο που θα είναι εγκατεστημένοι οι servers της εταιρίας η θερμοκρασία πρέπει να συγκρατείται σε χαμηλά επίπεδα εξαιτίας της θερμότητας που εκπέμπουν τα μηχανήματα. Επίσης η υγρασία πρέπει να είναι ελάχιστη για να μην προκαλεί φθορές στα υλικά. Αντιθέτως στους χώρους που εργάζονται οι υπάλληλοι, η θερμοκρασία και η υγρασία πρέπει να προσαρμόζονται έτσι ώστε να μπορούν οι εργαζόμενοι να δουλεύουν απρόσκοπτα. Ο συγκεκριμένος μετρητής υγρασίας και θερμοκρασίας της εικόνας 4 μετρητής 608-H2 απεικονίζει Υγρασία Θερμοκρασία & Σημείο Δρόσου, έχει ακρίβεια +- 2%, μπορεί να μετρήσει και να

αποθηκεύσει στη μνήμη θερμοκρασίες από -10 C έως +70C, και αν τα επιθυμητά όρια που έχουμε ορίσει εμείς ξεπεραστούν στέλνει σήμα συναγερμού.(εικόνα 1-12)

1.4 Ψηφιακή καταγραφή εικόνας

1.4.1 Εισαγωγή

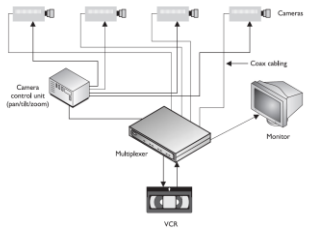
Συνήθως, η εγκατάσταση φραχτών, δεν παρέχει το απαραίτητο επίπεδο προστασίας, το οποίο μια εταιρία χρειάζεται για να προστατέψει τις εγκαταστάσεις της, τον εξοπλισμό και του εργαζόμενούς της. Όλες οι περιοχές θα πρέπει να είναι κάτω από επιτήρηση, ώστε να ενεργήσουμε άμεσα πριν συμβεί κάποιου είδους ζημιά. Η επιτήρηση – επόπτευση χώρων, μπορεί να πραγματοποιηθεί μέσω συσκευών παρακολούθησης. Οι οποίες ανιχνεύουν ασυνήθιστες συμπεριφορές και μη επιθυμητές καταστάσεις. Είναι σημαντικό κάθε εταιρία να έχει το κατάλληλο συνδυασμό από προσωπικό ασφαλείας, φωτισμό, συστήματα ανίχνευσης εισβολέων και να χρησιμοποιεί τεχνολογίες επόπτευσης χώρων. [3]

Από την άλλη, η χρήση καμερών σαν μέτρο ασφαλείας είναι περισσότερο χρήσιμη για εσωτερικούς χώρους παρά για εξωτερικούς λόγω ορισμένων παραγόντων:

- Συνήθης κίνηση εργαζομένων και οχημάτων έσω και έξω περιμετρικά της περιοχής.
- Μη ιδανικές συνθήκες περιβάλλοντος. (Ομίχλη, βροχές, χιονόπτωση, βρώμικοι φακοί)
- Περιορισμένη ανθρώπινη αντοχή για συνεχή παρακολούθηση των monitors.
- Αδυναμία εποπτείας όλων των καμερών ανά πάσα στιγμή.
- Μορφολογία του εδάφους και πιθανή δυσκολία οπτικής κάλυψης κάθε μέτρου περίφραξης.
- Μεγάλο κόστος κάλυψης.
- Μεγάλος αριθμός ψευδών συναγερμών από «έξυπνα» συστήματα λογισμικού.

1.4.2 Κλειστό κύκλωμα παρακολούθησης – Closed-Circuit TV (CCTV)

Επειδή η επόπτευση χώρων βασίζεται στην αισθητήρια αντίληψη, οι συσκευές επόπτευσης συνήθως λειτουργούν σε συνδυασμό με τους φύλακες και άλλους μηχανισμούς απεικόνισης, ώστε να επεκταθούν οι δυνατότητές τους και το εύρος της αντίληψης που διαθέτουν. Ένα κλειστό κύκλωμα τηλεόρασης (CCTV) είναι το πιο ευρέως διαδεδομένο σύστημα καταγραφής και απεικόνισης που χρησιμοποιούν οι οργανισμοί. Αλλά πριν ακόμα αποφασίσουμε τι θα αποκτήσουμε και πως θα εγκαταστήσουμε ένα CCTV, πρέπει να πάρουμε υπόψη μας ορισμένα πράγματα:



Εικόνα 1-13

- Ο σκοπός του καλωδιακού κυκλώματος είναι ο εντοπισμός, η εξακρίβωση και/ή η αναγνώριση των εισβολέων.
- Την ποιότητα του περιβάλλοντος στο οποίο το κλειστό κύκλωμα θα δουλεύει, είτε σε εσωτερικούς είτε σε εξωτερικούς χώρους.
- Το εύρος του πεδίου του οποίου τη θέα θέλουμε να παρακολουθούμε.
- Την ποιότητα φωτισμού του περιβάλλοντος.
- Η αρμονική συνεργασία με τα υπόλοιπα σκέλη της ασφάλειας(φύλακες, συναγερμοί, κ.α.).

Ένα απλό CCTV είναι δομημένο από κάμερες, πομπούς, δέκτες, ένα σύστημα καταγραφής και μια οθόνη. Η κάμερα συλλαμβάνει τα δεδομένα και τα στέλνει στον δέκτη, ο οποίος επιτρέπει την αναπαραγωγή τους στην οθόνη. Τα δεδομένα καταγράφονται ώστε να μπορούμε να τα ξαναδούμε αργότερα αν υπάρξει ανάγκη (εικόνα 1-13). Μπορούμε να έχουμε πολλές κάμερες συνδεδεμένες με ένα πολυπλέκτη, ο οποίος στέλνει την εικόνα, από όλες τις κάμερες, στην οθόνη. [3]

Εικόνα 1-14

Υπάρχουν 2 κύριοι τύποι φακών που χρησιμοποιούνται στις κάμερες ενός CCTV: σταθερής εστίασης βάθους και πλάτους και οι μεταβλητής εστίασης.

Οι **σταθερής εστίασης** (εικόνα 1-14) φακοί χρησιμοποιούνται για να παρατηρούμε σταθερά μια μεγάλη περιοχή, λόγου χάρη την εξωτερική περίμετρο των εγκαταστάσεων. Μπορούμε να τους ρυθμίσουμε, η εικόνα που στέλνουν να έχει μεγαλύτερο βάθος και να καλύπτει περισσότερο χώρο, ή να εστιάζει σε ένα συγκεκριμένο σημείο, που θέλουμε περισσότερη κάλυψη, πχ, πύλες. [5] http://www.chinavasion.com/product_info.php/pName/waterproof-night-vision-security-camera-pal-sony-13-lens/.

Οι **φακοί μεταβλητής** (εικόνα 1-15) εστίασης, μας παρέχουν περισσότερη ευελιξία, λόγω του ότι επιτρέπουν να αλλάζουμε το πεδίο στο οποίο βλέπουν, παίζοντας με τις οπτικές γωνίες και τις αποστάσεις. Το προσωπικό ασφαλείας συνήθως έχει ένα τηλεχειριστήριο, που επικοινωνεί με το κεντρικό σύστημα οθονών του κλειστού κυκλώματος και τους επιτρέπει να περιστρέφουν τις κάμερες και να εστιάζουν σε αντικείμενα, όπου αυτό χρειαστεί. Γενικά, οι φακοί μεταβλητής εστίασης είναι πολύ χρήσιμοι σε περιπτώσεις, που θέλουμε ταυτόχρονα γενική παρακολούθηση και κοντινές εικόνες. Αυτοί οι φακοί επιτρέπουν τη σταθερή εστίαση να αλλάζει από ευρεία γωνία, σε τηλεφωτογραφία, προσαρμόζοντας την εστίαση σε μια συγκεκριμένη εικόνα. [3]

Εικόνα 1-15

Οι φακοί των καμερών ενός CCTV έχουν διάφραγμα, το οποίο ελέγχει την ποσότητα του φωτός, που θα εισχωρήσει στο φακό κατά τη διάρκεια της νύχτας, σε σκοτεινά ή με ελάχιστο φωτισμό σημεία. Η λειτουργία τους είναι ίδια με την ίριδα του ματιού.

Υπάρχουν οι φακοί με χειροκίνητη ρύθμιση του διαφράγματος και οι αυτόματοι. Τους πρώτους τους χρησιμοποιούμε σε μέρη, τα οποία έχουν σταθερό φωτισμό , όπως είναι τα εσωτερικά μέρη της εταιρίας. Οι δεύτεροι, χρησιμοποιούνται σε μέρη τα οποία έχουν ο φυσικός φωτισμός μεταβάλλεται. Το προσωπικό ασφαλείας είναι υπεύθυνο να ρυθμίσει το κύκλωμα, ώστε να έχει μια σταθερή τιμή έκθεσης και με αυτή την τιμή το διάφραγμα να προσαρμόζεται. Πχ σε μια ηλιόλουστη μέρα, το διάφραγμα δεν υπάρχει λόγος να μένει ανοιχτό.

Εικόνα 1-16

Άλλες χρήσιμες λειτουργίες που μπορεί να έχει μια κάμερα είναι η αναγνώριση κίνησης μέσα στο πεδίο εστίασής της, και η καταγραφή ήχου, (εικόνα 1-16). [6]

Για την καλύτερη ασφάλεια από εξωτερικούς παράγοντες, για να μην δεχόμαστε παρεμβολές (θεμιτές ή αθέμιτες), επιλέγουμε όλες οι κάμερες που θα χρησιμοποιήσουμε να είναι ενσύρματες και με αυτόν τον τρόπο να επικοινωνούν με το control room. Το πλεονέκτημα είναι επίσης ότι αυτές οι κάμερες αποδίδουν πολύ καλύτερη ποιότητα εικόνας. Όλες οι καλωδιώσεις πρέπει να είναι καλυμμένες, κυρίως υπεδάφειες ή μέσα σε σωληνώσεις, ή περασμένες μέσα από τους τοίχους, για να προστατεύεται το δίκτυο από εξωγενείς παράγοντες, τις καιρικές συνθήκες και πιθανό σαμποτάζ.

Κάμερες θα στήσουμε στις 4 γωνίες της περίφραξης και θα είναι σταθερής εστίασης. Μόνο στην κεντρική ύλη θα έχουμε μεταβλητής εστίασης κάμερα για να μπορεί η ο ομάδα ελέγχου να ελέγχει καλύτερα όποιον μπαίνει. Κάμερες θα τοποθετήσουμε και στις γωνίες εξωτερικά του κτιρίου. Αυτές θα είναι μεταβλητής εστίασης σε περίπτωση που κάποιος καταφέρει να πλησιάσει το κτίριο να γίνεται καθαρά αντιληπτός. Επιπλέον κάμερες περιστροφικές θα τοποθετηθούν και στο ταβάνι στον εκθεσιακό χώρο.(εικόνα 1-17) Μεταβλητής εστίασης κάμερα θα τοποθετηθεί μέσα στο προθάλαμο αναγνώρισης και μέσα στο διάδρομο που είναι το control room και οι servers.

Εικόνα 1-17

1.5 Έλεγχοι πρόσβασης

1.5.1 Κλειδαριές

Οι κλειδαριές είναι ένα φτηνό εργαλείο για έλεγχους πρόσβασης, και χρίζει εκτεταμένης χρησιμοποίησης. Η κύρια δουλειά τους είναι να καθυστερούν τους εισβολείς και να αυξάνουν την πιθανότητα να επέμβει εγκαίρως ο φύλακας, ή η αστυνομία. Τα τελευταία χρόνια με την πρόοδο της τεχνολογίας, οι κλειδαριές δεν

είναι απλά ένα σύστημα κλειδιού-πόρτας, αλλά ένα ολοκληρωμένο σύστημα αναγνώρισης, ταυτοποίησης και πρόσβασης.

1.5.2 Smart Cards

Διεθνώς, κατά την τελευταία δεκαετία οι τεχνολογίες των Έξυπνων Καρτών χρησιμοποιούνται για την προσέγγιση και επίλυση προβλημάτων πρόσβασης, διαχείρισης και διακίνησης πληροφορίας σχεδόν σε όλους τους τομείς της οικονομίας και της κοινωνίας. (εικόνα 1-18)

Εικόνα 1-18

Το ολοκληρωμένο κύκλωμα περιέχει τις επαφές εισόδου-εξόδου και μπορεί να περιέχει μόνο μνήμη ή και μικροεπεξεργαστή. Επίσης παρέχει μία ασφαλή δομή πολλαπλών επιπέδων και να επιτρέπει ιεραρχημένη πρόσβαση, καθιστώντας δύσκολη την πρόσβαση στα στοιχεία και την παραποίηση αυτών, να υπολογίζει κρυπτογραφικές συναρτήσεις (cryptographic functions) και να αντιλαμβάνεται άμεσα προσπάθειες πρόσβασης, οι οποίες δεν είναι έγκυρες.

Μία έξυπνη κάρτα μπορεί να αποθηκεύσει τα στοιχεία αναγνώρισης ενός ατόμου για τον έλεγχο πρόσβασης σε κτίρια υψηλής και μη ασφάλειας-χώρος εργασίας αλλά και σε πανεπιστήμια, σχολεία, βιβλιοθήκες και λέσχες. Για ανάγκες υψηλότερης ασφάλειας και πρόσβαση σε συγκεκριμένες υπηρεσίες ή πληροφορίες, μια έξυπνη κάρτα μπορεί να αποτελέσει μια συσκευή για την αποθήκευση πληροφοριών όπως η εικόνα ή άλλα βιομετρικά χαρακτηριστικά (π.χ. τα δακτυλικά αποτυπώματα, ίριδα του ματιού) του χρήστη (εικόνα 1-19). Η ίδια κάρτα μπορεί στη συνέχεια να διατηρεί στοιχεία για την ταυτοποίηση του ατόμου στα υπολογιστικά συστήματα του οργανισμού. [7]

Εικόνα 1-19

Επομένως, όλοι οι εργαζόμενοι πρέπει να έχουν τη δική τους έξυπνη κάρτα. Μέσω αυτής θα γίνεται η καταγραφή τις κινήσεις τους κατά τη διάρκεια της εργασίας τους. Το σημαντικό εδώ είναι ότι τα συστήματα αυτά κρατάνε αρχείο με ημερομηνίες και ώρες που κάποιος απέκτησε πρόσβαση σε ένα χώρο.

Σε περιπτώσεις όπως η είσοδος στο control room και στο δωμάτιο με τους servers, πρέπει να παρθούν επιπλέον μέτρα. Πρώτον, μόνο ένα άτομο μπορεί να εισέρχεται και να εξέρχεται κάθε φορά από την πόρτα. Δεύτερον, το άτομο που θέλει πρόσβαση θα εισέρχεται πρώτα με την χρήση της έξυπνης κάρτας στον ειδικό προθάλαμο. Εκεί θα γίνεται η αναγνώριση του και από το ηλεκτρονικό σύστημα με βάση βιομετρικές μεθόδους, τα δακτυλικά του αποτυπώματα (εικόνα 5), αλλά και από το προσωπικό ασφαλείας που εργάζεται στο control room μέσω της κάμερας που είναι εγκατεστημένη στον προθάλαμο. Αφού γίνει η ταυτοποίηση του ατόμου τότε μόνο μπορεί να μπει στο δωμάτιο.

1.5.3 Απαγορεύσεις – Περιορισμοί – Συνοδοί

Ένα από τα αρχικά μέτρα, που πρέπει να διευκρινίσουμε, είναι η οριοθέτηση των χώρων και η διαβάθμισή τους, ανάλογα με το τι εργασίες εκτελούνται εκεί και ποιοι είναι οι αρμόδιοι να εισέρχονται σε αυτούς. Παραδείγματος χάριν, δεν μπορεί να μπαίνουν επισκέπτες, ακόμα και απλοί εργαζόμενοι στο δωμάτιο με τους servers, εκτός από τους υπευθύνους δικτύου και ασφαλείας.

Καταρχήν, χρειάζεται να παρθούν κατάλληλες αποφάσεις για το που θα στεγαστούν τα διάφορα τμήματα. Ο εκθεσιακός χώρος, ο χώρος υποδοχής, οι πληροφορίες και η γραμματεία θα πρέπει να είναι ακριβώς όπως εισέρχεται κανείς στο κτίριο. Τα γραφεία θα πρέπει να είναι περιμετρικά του κτιρίου ώστε να μπαίνει φυσικό φως και να αερίζονται καλύτερα. Το δωμάτιο με τους servers και το control room θα πρέπει να βρίσκονται όσο γίνεται κεντρικά στο κτίριο για να μην είναι εύκολη η πρόσβαση του από παράθυρα.

Κατά δεύτερο, χρειάζεται να οριοθετήσουμε τις απαγορευμένες περιοχές και να προσαρμόσουμε ανάλογα τους ελέγχους πρόσβασης. Απαγορευμένες περιοχές είναι το control room και στο δωμάτιο με τους servers. Τα γραφεία, οι

αποθήκες κ.α. είναι ελεγχόμενοι χώροι και ο κεντρικός εκθεσιακός χώρος είναι ελεύθερης πρόσβασης.

Υπάρχουν περιπτώσεις που το χώρο της εταιρίας θα τους επισκεφτούν πελάτες. Σε αυτή την περίπτωση πρέπει να προβλεφτούν ορισμένα πράγματα. 1) Όποιο άτομο θέλει να μπει στο κτίριο, να υπογράφει πρώτα στο βιβλίο επισκεπτών αφήνοντας κάποια προσωπικά του στοιχεία, όπως το ονοματεπώνυμο και ο αριθμός ταυτότητας ή διαβατηρίου. Κατά την έξοδο θα πρέπει να υπογράφει και πάλι την αποχώρηση του. 2) Θα πρέπει να υπάρχουν ειδικές κάρτες με διαφορετικούς χρωματισμούς, ξεχωριστά από τις έξυπνες κάρτες, τις οποίες διαθέτει μόνο το προσωπικό. Αυτές οι κάρτες ανάλογα με το χρώμα τους θα δείχνουν αν το άτομο που τις φέρει είναι σε μέρος που επιτρέπεται. Πχ οι επισκέπτες θα πρέπει να έχουν καρτέλες με μπλε χρώμα, που να δείχνει, ότι μπορούν να κυκλοφορούν μόνο στον εκθεσιακό χώρο. Οι υπάλληλοι θα έχουν κάρτες χρώματος πράσινο, ώστε να μπορούν να κινούνται στα γραφεία και σε άλλους χώρους πχ αποθήκες. Τέλος τα άτομα που έχουν πρόσβαση στο control room και στο δωμάτιο με τους servers, θα πρέπει να έχουν κάρτες χρώματος κόκκινο. Με αυτόν τον τρόπο μειώνεται η πιθανότητα να βρεθούν στους χώρους της εταιρίας μη εξουσιοδοτημένα άτομα. 3) όλοι οι επισκέπτες θα πρέπει να έχουν μαζί τους και ένα συνοδό που να τους ξεναγεί, να φροντίζει να μην περιφέρονται άσκοπα μέσα στο χώρο και να ελέγχει ότι βρίσκονται σε επιτρεπτούς χώρους.

1.5.4 Καταγραφή και σύνταξη αναφορών

Τα συστήματα ελέγχου φυσικής ασφάλειας μπορούν να χρησιμοποιήσουν λογισμικό ειδικό ώστε να καταγράφουν τα διάφορα συμβάντα και τις προσπάθειες πρόσβασης και να δημιουργούν αναφορές για το προσωπικό ασφαλείας. Μερικές από τις πληροφορίες που μπορούν να ελέγχονται είναι:

- Η ημερομηνία και η ώρα που έγινε μια προσπάθεια πρόσβασης
- Το σημείο εισόδου, που πραγματοποιήθηκε η πρόσβαση
- Η ταυτότητα του εργαζομένου που έκανε την προσπάθεια εισόδου

- Τυχόν μη επιτυχημένες προσπάθειες πρόσβασης, ιδιαίτερα σε ώρες που δεν προβλέπεται.

Αυτές οι καταγραφές και οι αναφορές θα είναι άχρηστες να δεν υπάρχει κάποιο άτομο που να της διαβάζει και να τις ελέγχει. Ο υπεύθυνος στο δωμάτιο διαχείρισης ή ένας φύλακας θα πρέπει να βλέπει καθημερινά τις αναφορές, αλλά ο υπεύθυνος ασφαλείας θα πρέπει περιοδικά να κάνει αυτόν τον έλεγχο.

Η διαχείριση του συστήματος μας επιτρέπει να ξέρουμε πόσες θύρες υπάρχουν στις εγκαταστάσεις και ποιοι τις χρησιμοποιούν. Οι καταγραφές και οι αναφορές μας χρησιμεύουν για να ανιχνεύουμε συμπεριφορές και καταστάσεις και όχι να αποτρέπουμε την κακόβουλη ενέργεια. Απλά συνήθως αυτά τα δύο μέρη συνδυάζονται για να αυξήσουν την εμπειρία του συστήματος και του προσωπικού και να δείξουν νέους τρόπους αντιμετώπισης των προβλημάτων.

1.6 Επίλογος

Η φυσική ασφάλεια είναι ένας τεράστιος εξελισσόμενος κλάδος. Αυτό έχει να κάνει με τους κινδύνους και τις προκλήσεις της νέας εποχής. Τα νέα συστήματα που κατασκευάζονται προσφέρουν μεγάλη πολυπλοκότητα στην υλοποίηση ολοκληρωμένων σχεδίων ασφαλείας, για το λόγο ότι ένας επίδοξος εισβολέας με τη χρήση της τεχνολογίας μπορεί να αξιοποιήσει οποιαδήποτε αδυναμία του συστήματος και να πραγματοποιήσει τους στόχους του.

Όση όμως και να είναι η εξέλιξη των συστημάτων και όσο πιο αποτελεσματικά γίνονται, δεν παύουν να είναι μηχανήματα που εξαρτώνται από την ανθρώπινη διαχείριση. Ο άνθρωπος είναι η πιο αξιόπιστη λύση ασφαλείας και όλα τα υπόλοιπα είναι συμπληρωματικά για να του δίνουν τη δυνατότητα να είναι πιο αποτελεσματικός.

Από την άλλη, υπάρχει και η λογική που λέει, ότι ο κακοποιός είναι πάντα ένα βήμα μπροστά από την αστυνομία. Έτσι και με την ασφάλεια εγκαταστάσεων, οι περισσότερες εταιρίας ανάπτυξης τέτοιων συστημάτων μελετάνε περιπτώσεις αποτυχιών δικών τους ή επιτυχιών των εισβολέων και κάνουν διορθώσεις πάνω στο υπάρχον σύστημα, μέχρι την επόμενη φορά που κάποιος θα το υπερνικήσει και θα συνεχιστεί αυτός ο φαύλος κύκλος.

Κεφάλαιο 2

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

2.1 Σύνοψη

Η αποδεκτή πολιτική χρήσης του δικτύου της εταιρίας δεν αποσκοπεί στο να επιβάλει περιορισμούς, που είναι αντίθετης φύσης από αυτούς που έχει θέσει η εταιρία, αλλά για να επιτύχει ένα πνεύμα εμπιστοσύνης και συνεργασίας. Η εταιρία είναι προσηλωμένη να προστατεύει τους εργαζόμενους, τους συνεργάτες και την υλική περιουσία της, από παράνομες ή καταστροφικές ενέργειες, από άτομα, που γίνονται εσκεμμένα ή μη.

Το τοπικό δίκτυο της εταιρίας, το δίκτυο του internet και παρεμφερή συστήματα περιλαμβανομένων του εξοπλισμού των υπολογιστών, των προγραμμάτων, των λειτουργικών συστημάτων, των μονάδων αποθήκευσης, οι λογαριασμοί ηλεκτρονικού ταχυδρομείου, η αναζήτηση στο διαδίκτυο είναι περιουσιακά στοιχεία της εταιρίας. Επιβάλετε να χρησιμοποιείτε αυτά τα συστήματα για τους σκοπούς και τα ενδιαφέροντα της εταιρίας και μόνο.

Η αποτελεσματική ασφάλεια είναι μια ομαδική προσπάθεια, που προϋποθέτει την συμμετοχή κάθε εργαζόμενου στην εταιρία και εντάσσει κάθε νέο εργαζόμενο, που χειρίζεται πληροφορίες ή το πληροφοριακό σύστημα. Είναι υποχρέωση του κάθε εργαζόμενου, σαν χειριστής υπολογιστή να ξέρει όλους τους κανόνες και να συμπεριφέρεται αναλόγως.

Οι χρήστες δεσμεύονται:

- Να μη προβούν σε ενέργειες που συνιστούν προσπάθεια παραβίασης
- Να λαμβάνουν όλα τα ενδεικνυόμενα μέτρα για την διασφάλιση του προσωπικού απόρρητου
- Να μη προβούν σε ενέργειες που συνιστούν παραβίαση του προσωπικού απόρρητου
- Να μην προβούν σε ενέργειες που παραβιάζουν (με παραγωγή, δημοσίευση ή διακίνηση υλικού) των πνευματικών δικαιωμάτων (copyrights) των δικαιούχων.

- Να κάνουν λελογισμένη χρήση των υπολογιστικών και δικτυακών πόρων του δικτύου.
- Να ενημερώνουν αμέσως τους υπεύθυνους του εκάστοτε συστήματος αν υποπέσει στην αντίληψη τους οποιοδήποτε κενό ασφάλειας.
- Να χρησιμοποιούν το δίκτυο για σκοπούς που συνάδουν με το χαρακτήρα και τους στόχους της εταιρίας.
- Να τηρούν τους γραπτούς και άγραφους κανόνες της καλής δικτυακής συμπεριφοράς.
- Να συμμορφώνονται με τους κανονισμούς λειτουργίας των υπηρεσιών που χρησιμοποιούν.

2.2 Πολιτική χρήσης δικτύου

Η πολιτική αποδεκτής χρήσης (acceptable or appropriate use policy) του δικτύου της επιχείρησης καλύπτει κάθε χρήστη του δικτύου δεδομένων της. Η πολιτική αποδεκτής χρήσης περιγράφει τις επιτρεπόμενες και μη επιτρεπόμενες χρήσεις και δραστηριότητες των χρηστών των υπολογιστικών και τηλεπικοινωνιακών συστημάτων του δικτύου δεδομένων της εταιρίας. Σε αυτά τα πλαίσια ο παρόν κανονισμός σκοπό έχει να οριοθετήσει το θεσμικό και κανονιστικό πλαίσιο λειτουργίας των δικτυωμένων υποδομών της εταιρίας. Οι ακόλουθοι ορισμοί είναι χρήσιμοι για τους σκοπούς αυτούς.

1. **Δίκτυο Δεδομένων** της εταιρίας, ονομάζεται το σύνολο των δικτυακών υπηρεσιών και υποδομών που υποστηρίζουν τις απαιτήσεις επικοινωνίας των υπολογιστικών συστημάτων της εταιρίας.
2. **Χρήστης** (δικτύου) ονομάζεται το κάθε τμήμα της εταιρίας (Λογιστήριο, Μάρκετινγκ, R&D, Help Support) ή το φυσικό πρόσωπο (υπάλληλος της εταιρίας), στο οποίο του παρέχονται οι υπηρεσίες.
3. **Κέντρο Λειτουργίας & Διαχείρισης Δικτύου** (ΚΛ&ΔΔ ή απλά για συντομία ΚΛΔ) της εταιρίας, ονομάζεται ο φορέας που προτείνει, υλοποιεί και παρακολουθεί σε τεχνικό επίπεδο τη Δικτυακή πολιτική που χαράσσει η εταιρία.

Ο παρών Κανονισμός Λειτουργίας εφαρμόζεται σε όλες τις κατηγορίες χρηστών δικτύου. Η συμμόρφωση των μελών κάθε διασυνδεδεμένου φορέα με τον παρόντα Κανονισμό αποτελεί ευθύνη του αντίστοιχου φορέα.

2.3 Δραστηριότητες του κέντρου λειτουργίας δικτύου

Οι δραστηριότητες του ΚΛ&ΔΔ μπορούν να καταταχθούν σε έξι κατηγορίες:

1) Εγκατάσταση νέων τμημάτων καλωδιακού συστήματος, ενεργών στοιχείων και λογισμικού συστημάτων δικτύου και εφαρμογών. Όσον αφορά στο καλωδιακό σύστημα οι επεμβάσεις αφορούν την ενσωμάτωση νέων τμημάτων του δικτύου (τα οποία αποτελούν αυτόνομα έργα που εκτελούνται με την επίβλεψη του ΚΛ&ΔΔ από εξωτερικούς εργολάβους) στο υπάρχον δίκτυο. Η εγκατάσταση των ενεργών στοιχείων που κατά καιρούς προμηθεύεται η εταιρία, κατευθύνεται ή εκτελείται από το ΚΛ&ΔΔ, ανάλογα με τις επιμέρους απαιτήσεις για ειδική προσαρμογή και την υπάρχουσα τεχνογνωσία του αναδόχου. Παρόμοια, όσον αφορά στο λογισμικό συστημάτων δικτύου και εφαρμογών, η παραγωγή προστιθέμενης αξίας από το ίδιο το ΚΛ&ΔΔ είναι βασική πολιτική επιλογή, η οποία ενισχύει την αυτοτέλεια και μειώνει τις δαπάνες της εταιρίας.

2) Συντήρηση καλωδιακού συστήματος, ενεργών στοιχείων και λογισμικού. Το ΚΛ&ΔΔ μεριμνά για την καλή κατάσταση του δικτύου με περιοδικές επισκέψεις των στελεχών του στα κομβικά σημεία του δικτύου. Επιβλέπει και πιστοποιεί την καλή εκτέλεση της συντήρησης ενεργών στοιχείων, όπου αυτή έχει ανατεθεί σε εξωτερικούς εργολάβους, και φροντίζει για την έγκαιρη προμήθεια ανταλλακτικών και διεξαγωγή επιδιορθώσεων όπου δεν υπάρχει συμβόλαιο συντήρησης. Το λογισμικό είναι ένας τομέας που απαιτεί μεγάλες και επίπονες προσπάθειες συντήρησης καθώς υπάρχει συχνά ανάγκη για αναβάθμιση τμημάτων ή συνόλων εξειδικευμένων προγραμμάτων τα οποία επιπλέον μπορεί να έχουν διαμορφωθεί ειδικά για τις ανάγκες της εταιρίας. Το συνήθως δωρεάν διαθέσιμο λογισμικό πρέπει να μεταφερθεί από το κατάλληλο σημείο του Internet, ενώ πρέπει να

υπάρχει εύστοχος και έγκαιρος προγραμματισμός αγοράς νέων εκδόσεων προϊόντων λογισμικού.

3) Διαχείριση καλωδιακών κόμβων, ενεργών στοιχείων και εφαρμογών. Σε ένα δίκτυο της κλίμακας της εταιρίας απαιτείται μια ολοκληρωμένη καταγραφή, χαρτογράφηση και διαχείριση του καλωδιακού συστήματος, ώστε να είναι δυνατή η έγκαιρη διάγνωση βλαβών, ο σχεδιασμός επεκτάσεων και η καθημερινή λειτουργία και μικρο-προσαρμογές του δικτύου. Ακόμα πιο κρίσιμος παράγοντας για την αποδοτική λειτουργία του δικτύου είναι η σωστή διαμόρφωση και παρακολούθηση των συνθηκών λειτουργίας (φόρτος, στατιστικά στοιχεία, βλάβες) των ενεργών στοιχείων και βασικών υπολογιστών παροχής δικτυακών εφαρμογών μέσα από μια πλατφόρμα διαχείρισης βασισμένη στο ανοικτά διεθνή πρότυπα (π.χ. SNMP). Σε αυτή τη δραστηριότητα εντάσσονται και οι καθημερινές επισκέψεις τεχνικών του ΚΛ&ΔΔ σε χρήστες που αντιμετωπίζουν δικτυακά προβλήματα μετά από σχετικό τηλεφωνικό ραντεβού.

4) Παροχή δικτυακών υπηρεσιών προστιθέμενης αξίας στην εταιρία. Ενδεικτικά αναφέρονται υπηρεσίες που το ΚΛ&ΔΔ έχει ήδη δώσει:

- Ηλεκτρονικό Ταχυδρομείο (e-mail)
- Υπηρεσίες Παγκόσμιου Ιστού (www)
- Μεταφορά Αρχείων (ftp)
- 'Αρθρα (usenet news)
- Διευθυνσιοδότηση Υπολογιστών (dns)
- Υπηρεσίες Ενδιάμεσου (proxy)
- Αναζήτηση Στοιχείων (directory service)

Για όλες τις υπηρεσίες υπάρχει αναλυτική τεκμηρίωση και παρέχεται υποστήριξη σε όλη την εταιρία.

5) Ανάπτυξη νέων προηγμένων υπηρεσιών δικτύου και ενσωμάτωση τους στο περιβάλλον του δικτύου σε πλήρη κλίμακα. Το Δίκτυο Δεδομένων της εταιρίας, είναι ένα δίκτυο «παραγωγής», με την έννοια ότι υπάρχει υψηλή διαθεσιμότητα των ενεργών στοιχείων (συγκεντρωτές, hubs, δρομολογητές, switches) και των servers του δικτύου και αδιάλειπτη παροχή υπηρεσιών προς όλα τα τμήματα της εταιρίας. Συνεπώς, απαραίτητη προϋπόθεση για την ομαλή εισαγωγή νέων τεχνολογιών και υπηρεσιών είναι η ύπαρξη κάποιας πλατφόρμας

μέσα στο δίκτυο, όπου νέες τεχνολογίες, προϊόντα και υπηρεσίες θα εγκαθίστανται πιλοτικά, θα αναπτύσσονται παρέχοντας προστιθέμενη αξία στην εταιρία και τέλος θα ελέγχονται διεξοδικά πριν παραδοθούν στους χρήστες.

6) Εκπαίδευση των υπαλλήλων της εταιρίας σε θέματα δικτύων και πιο συγκεκριμένα στη χρήση του Δικτύου Δεδομένων της και των προσφερόμενων υπηρεσιών. Επιπλέον παροχή εξειδικευμένων γνώσεων στα στελέχη του ΚΛ&ΔΔ της εταιρίας, όπου κρίνεται σκόπιμο. Η εκπαιδευτική διαδικασία διεξάγεται με οργανωμένα σεμινάρια, διαλέξεις, αλλά και με τη παροχή συμβουλευτικών υπηρεσιών (helpdesk) από τα στελέχη του ΚΛ&ΔΔ.

2.4 Διοίκηση και διαχείριση του δικτύου

- Το πληροφοριακό δίκτυο της εταιρίας διαχειρίζεται από τους υπευθύνους διαχείρισης δικτύου που προσλαμβάνονται με ευθύνη του ΔΣ της εταιρίας. Οι διαχειριστές είναι υπεύθυνοι:
- της διαχείρισης του όλου συστήματος
- της εγκατάστασης του λογισμικού, της ασφάλειας και της τήρησης εφεδρικών αντιγράφων.
- της ασφάλειας και καλής λειτουργίας του εξοπλισμού και του λογισμικού
- της τήρησης της τάξης και της λήψης των αναγκαίων μέτρων για την επιτόπου αντιμετώπιση προβλημάτων
- της συνεργασίας με τους υπεύθυνους της εταιρίας για την εγκατάσταση ειδικών εφαρμογών λογισμικού που απαιτούνται για τη λειτουργία της.
- της τεχνικής διαχείρισης των προσωπικών κωδικών της εταιρίας (διευθυντικών στελεχών, μεσαίων στελεχών, υπαλλήλων)

2.5 Δικαιώματα και υποχρεώσεις χρηστών

Η πρόσβαση των χρηστών στο Δίκτυο Δεδομένων και τα υπολογιστικά συστήματα της εταιρίας διέπεται από τους παρακάτω κανόνες:

1. Οι υποχρεώσεις κατά δικαιώματα των χρηστών ξεκινάνε αμέσως μόλις υπογράψουν το συμβόλαιο τους με την εταιρία.
2. Κάθε χρήστης είναι υπεύθυνος και υπόλογος για κάθε είδους δραστηριότητα η οποία ξεκινάει ή αναπτύσσεται μέσω της πρίζας δεδομένων, του προσωπικού υπολογιστή, ή του λογαριασμού που του έχει παραχωρηθεί
3. Οι χρήστες πρέπει να μη προβούν σε ενέργειες που συνιστούν προσπάθεια παραβίασης (επιτυχή ή μη) της ασφάλειας συστημάτων μέσα από το δίκτυο δεδομένων της επιχείρησης. Στα πλαίσια αυτά εντάσσονται και ενέργειες που υποβαθμίζουν το επίπεδο ασφάλειας ενός συστήματος.
4. Κάθε χρήστης είναι αποκλειστικά υπεύθυνος για την σωστή λειτουργία του προσωπικού υπολογιστή του όσον αφορά τη σύνδεση με το Δίκτυο Δεδομένων και τυχόν προβλήματα που μπορεί να προκαλέσουν στο Δίκτυο ελαττωματικά καλώδια περιοχής εργασίας, κάρτες δικτύου ή λογισμικό. Το ΚΛ&ΔΔ παρέχει τεχνικές συμβουλές και συστάσεις με τις οποίες οι χρήστες υποχρεούνται να συμμορφώνονται.
5. Κάθε χρήστης είναι υπεύθυνος για την επιλογή και τη διαφύλαξη «ασφαλούς» συνθηματικού (password) για πρόσβαση στο λογαριασμό του. Τα συνθηματικά δεν πρέπει ποτέ να γράφονται σε χαρτί ή να φυλάσσονται σε ηλεκτρονική μορφή, ούτε να δίνονται σε τρίτους. Ιδιαίτερη προσοχή πρέπει να δίνεται σε επικοινωνία (ηλεκτρονικό ταχυδρομείο ή τηλέφωνο) από άτομα που ισχυρίζονται ότι είναι υπεύθυνοι συστημάτων και ζητούν να μάθουν συνθηματικά χρηστών (οι πραγματικοί χειριστές συστημάτων ποτέ δεν έχουν ανάγκη κάτι τέτοιο...).
6. Οι κωδικοί αυτοί θα αλλάζουν κάθε έξη μήνες. Σε περίπτωση απώλειας από κάποιο πρόσωπο, θα γίνεται άμεσα έκδοση νέου κωδικού.
7. Οι χρήστες πρέπει να μη προβούν σε ενέργειες που συνιστούν παραβίαση του προσωπικού απόρρητου χρηστών και του απορρήτου των επικοινωνιών μέσω του δικτύου δεδομένων της επιχείρησης. Οι χρήστες δεσμεύονται να αποκτούν πρόσβαση αποκλειστικά σε δεδομένα που αναφέρονται στους ίδιους ή είναι δημοσίως ανακοινώσιμα.

8. Οι χρήστες πρέπει να χρησιμοποιούν το δίκτυο για σκοπούς που συνάδουν με τον επιχειρηματικό – ερευνητικό χαρακτήρα της επιχείρησης. Ενδεικτικά αναφέρεται ότι δεν επιτρέπεται να διακινείται πάνω από το δίκτυο δεδομένων πληροφορία της οποίας τόσο ο αποστολέας όσο και ο παραλήπτης είναι ανταγωνιστικοί εμπορικοί φορείς.
9. Κάθε χρήστης είναι υπεύθυνος για την προστασία των δεδομένων και αρχείων του από λαθραία ανάγνωση ή αλλοίωση από τρίτους. Για το σκοπό αυτό ο χρήστης μπορεί να αξιοποιήσει όποιο μηχανισμό ασφαλείας παρέχει το αντίστοιχο σύστημα του και κρίνει σκόπιμο.
10. Κάθε χρήστης είναι υπεύθυνος να αναφέρει κάθε απόπειρα ή παραβίαση των κανόνων λειτουργίας και της ασφάλειας στους αντίστοιχους υπεύθυνους συστημάτων ή το Κ.Λ.Δ, επώνυμα ή ανώνυμα.
11. Είναι υποχρέωση του κάθε χρήστη να χειρίζεται και να χρησιμοποιεί οτιδήποτε εξοπλισμό συστημάτων ή δικτύου που ανήκει στη εταιρία με προσοχή ώστε να μην προκαλούνται ζημιές ή φθορές. Τυχόν ατυχήματα θα πρέπει να αναφέρονται το ταχύτερο στο ΚΛ&ΔΔ (ή τους αντίστοιχους υπεύθυνους) ώστε να αποκαθίστανται το συντομότερο δυνατό με δαπάνη του υπαιτίου.
12. να ενημερώνουν αμέσως τους υπεύθυνους του εκάστοτε συστήματος αν υποπέσει στην αντίληψη τους οποιοδήποτε κενό ασφάλειας.
13. να μην εκμεταλλευτούν την πρόσβαση που τους παρέχεται σε υπολογιστές, εφαρμογές και κάθε είδους τηλεπικοινωνιακά δίκτυα από το δίκτυο δεδομένων της επιχείρησης, προκειμένου να προβούν σε ενέργειες που παραβιάζουν οποιονδήποτε νόμο του κράτους.
14. Τέλος, κάθε χρήστης οφείλει να σέβεται και να μην παρενοχλεί τους υπόλοιπους χρήστες, να μην σπαταλά άσκοπα πόρους και να μην προβαίνει σε ανήθικες ή παράνομες πράξεις χρησιμοποιώντας τα συστήματα και το Δίκτυο Δεδομένων.

2.6 Δικαιώματα και υποχρεώσεις Κέντρου Δικτύων

Σε γενικές γραμμές οι πράξεις και η συμπεριφορά της ομάδος εργαζομένων του ΚΛ&ΔΔ διέπεται από τις εξής αρχές:

1. Το ΚΛ&ΔΔ παρέχει κάθε δυνατή διευκόλυνση στους χρήστες του δικτύου, ώστε να είναι σε θέση να ανταποκριθούν στα καθήκοντα που τους ανατίθενται από την εταιρία. Για το σκοπό αυτό λειτουργεί υπηρεσία «Υποστήριξης Χρηστών» με εύλογο ωράριο λειτουργίας και μεθόδους επικοινωνίας (επί τόπου, τηλεφωνικά, με e-mail, fax, κτλ.).
2. Το ΚΛ&ΔΔ καταβάλει κάθε δυνατή προσπάθεια ώστε να διασφαλίζεται το απόρρητο των αρχείων, μηνυμάτων ηλεκτρονικού ταχυδρομείου και δεδομένων κάθε χρήστη.
3. Το ΚΛ&ΔΔ απαγορεύεται να εξετάζει αρχεία, μηνύματα ηλεκτρονικού ταχυδρομείου και άλλα δεδομένα χρηστών. Σε εξαιρετικές περιπτώσεις με αποκλειστικό σκοπό τη διάγνωση και αντιμετώπιση προβλημάτων λογισμικού ή όταν υπάρχουν βάσιμες υποψίες για παραβίαση της ασφάλειας του δικτύου, γίνονται οι απαραίτητες τεχνικές ενέργειες. Η διαδικασία αυτή ενεργοποιείται μόνο μετά από ενημέρωση και εντολή του ΔΣ της εταιρίας.
4. Παρομοίως το ΚΛ&ΔΔ απαγορεύεται να παρακολουθεί κατά οποιονδήποτε τρόπο υπολογιστικά συστήματα ή δραστηριότητα χρηστών. Σε εξαιρετικές περιπτώσεις αποκλειστικά και μόνο για την εξακρίβωση τέλεσης παράνομων πράξεων και παραβιάσεων της πολιτικής που καθορίζεται στο παρόν κείμενο, και μόνο εφόσον υπάρχουν βάσιμες υποψίες, γίνονται οι απαραίτητες τεχνικές ενέργειες.
5. Σε όλες τις περιπτώσεις, απαγορεύεται ρητά στα μέλη του ΚΛ&ΔΔ η διαρροή ή δημοσιοποίηση στοιχείων των παραπάνω δύο περιπτώσεων εκτός του ΚΛ&ΔΔ. Μόνοι αρμόδιοι να έχουν πρόσβαση σε τέτοια στοιχεία είναι το ΔΣ της εταιρίας.
6. Το ΚΛ&ΔΔ έχει την υποχρέωση να αναφέρει προβλήματα ασφαλείας στο ΔΣ της εταιρίας το οποίο και εισηγείται περαιτέρω ενέργειες.

7. Το ΚΛ&ΔΔ δικαιούται να ελαττώνει την προτεραιότητα, ή να τερματίζει τη χρήση πόρων του δικτύου σε περίπτωση που χρήστης καταχράται τις δυνατότητες που του παρέχονται και δημιουργεί προβλήματα στην ποιότητα υπηρεσιών που είναι διαθέσιμες στο σύνολο των χρηστών του δικτύου. Ο όρος «χρήστης» στη συγκεκριμένη αυτή περίπτωση περιλαμβάνει και κάθε υπολογιστικό σύστημα που συνδέεται με το Δίκτυο Δεδομένων της εταιρίας.
8. Το ΚΛ&ΔΔ υποχρεούται να ανακοινώνει προγραμματισμένες εργασίες, οι οποίες επιφέρουν διακοπή λειτουργίας σε τμήματα ή υπηρεσίες του Δικτύου Δεδομένων, τουλάχιστον τρεις ημέρες πριν την έναρξη τους. Εξαιρούνται οι περιπτώσεις κατεπειγόντων εργασιών λόγω τεχνικών προβλημάτων.
9. Συμφώνα με την παράγραφο 8, το ΚΛ&ΔΔ φροντίζει για την ομαλή τήρηση λήψης των αντιγράφων ασφαλείας, σύμφωνα πάντα με το σχέδιο που έχει καταρτιστεί.
10. Το ΚΛ&ΔΔ πρέπει να φροντίζει να είναι απενεργοποιημένες όλες οι θύρες USB σε όλους τους υπολογιστών των εργαζομένων. Επίσης παίρνει μέτρα, ώστε οι χρήστες να μην μπαίνουν σε ιστοσελίδες κοινωνικής δικτύωσης, σε ιστοσελίδες πορνογραφικού υλικού.

2.7 Διαβαθμίσεις εγγράφων

Τα έγγραφα θα είναι διαβαθμισμένα σε 4 κατηγορίες, με αρίθμηση από το 1 έως το 4 και με τη σημαντικότητα σε αύξουσα σειρά. Σε κάθε έγγραφο θα πρέπει να αναγράφεται και η διαβάθμισή του στο επάνω δεξί μέρος της πρώτης σελίδας.

Επίπεδο 1: **Κοινά.** Περιλαμβάνει δελτία τύπου και επίσημες ανακοινώσεις της εταιρίας. Δεν έχουν καμιά ασφάλεια.

Επίπεδο 2: **Εσωτερικά.** Περιλαμβάνει τα έγγραφα, που αφορούν λειτουργίες της εταιρίας και μπορούν να κοινοποιούνται σε όλους τους εργαζομένους. Για το κάθε τμήμα της εταιρίας υπάρχει ξεχωριστή υποκατηγορία. Αν το κείμενο

αναφέρεται σε κάποιο τμήμα της εταιρίας τότε πρέπει να φέρει και το όνομα του τμήματος στη θέση διαβαθμίσεως. Έχουν μέτριο επίπεδο ασφάλειας. Υποεπίπεδα:

I) Εσωτερικό Λογιστήριο

II) Εσωτερικό Marketing

III) Εσωτερικό R&D

IV) Εσωτερικό Help Support

Επίπεδο 3: **Εμπιστευτικά.** Περιλαμβάνει έγγραφα, που αφορούν την λειτουργία σε διευθυντικό επίπεδο και σε επίπεδο τμημάτων. Έχουν αυξημένη ασφάλεια και πρέπει απευθύνονται από διευθυντές τμημάτων και πάνω. Πρέπει να κρατούνται σε ξεχωριστό αρχείο από τα κοινά και τα εσωτερικά.

Επίπεδο 4: **Απόρρητα.** Περιλαμβάνει τα έγγραφα που είναι κρίσιμης σημασίας για τη λειτουργία της εταιρίας, όπως είναι τα οικονομικά και τα θέματα ασφάλειας. Τα διαχειρίζεται μόνο το Διοικητικό Συμβούλιο και τα εξουσιοδοτημένα άτομα. Έχουν τη μέγιστη ασφάλεια και φυλάσσονται σε ειδικά διαμορφωμένους χώρους με ασφάλεια(ντουλάπες με κλειδαριές, χρηματοκιβώτια).

2.8 Προτεραιότητα εγγράφων

Είναι χαρακτηρισμός του εγγράφου με έναν όρο που δηλώνει ότι η διεκπεραίωσή του πρέπει να γίνει σε συγκεκριμένο χρόνο, ώστε να μην προκληθεί δυσλειτουργία του συστήματος. Τον βαθμό προτεραιότητας τον επιλέγει ο συντάκτης βάσει των στοιχείων και της φύσης του περιεχομένου του εγγράφου. Την ευθύνη για το βαθμό προτεραιότητας τη φέρει η υπηρεσία.

Οι βαθμοί προτεραιότητας είναι:

α. ***Εξαιρετικά Επείγον*** (Για διεκπεραίωση το συντομότερο δυνατό)

β. ***Επείγον*** (Για διεκπεραίωση σε διάστημα μικρότερο του εύλογου, για να διεκπεραιωθεί, χρόνου)

γ. ***Κοινό*** (Για διεκπεραίωση κατά τη φυσιολογική σειρά βάσει της ημερομηνίας του).

Κεφάλαιο 3

ΤΟ ΤΟΠΙΚΟ ΔΙΚΤΥΟ

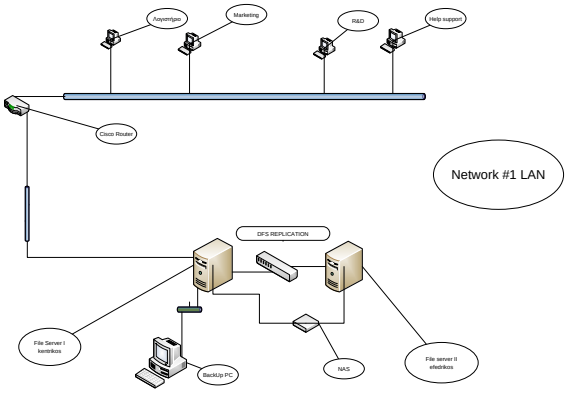
3.1 Εισαγωγή

Το δίκτυο Η/Υ αποτελεί την καρδιά της εταιρίας. Εκεί μέσα βρίσκονται όλα τα κρίσιμα δεδομένα, που χρησιμοποιεί η εταιρία για την καθημερινή λειτουργία της. Εκεί πραγματοποιείται το σύστημα επικοινωνίας τόσο με τον έξω κόσμο, τους πελάτες, τους προμηθευτές, τους συνεργάτες, όσο και στο εσωτερικό της μεταξύ των τμημάτων, των στελεχών και των εργαζομένων της.

Μέσα στο παρόν κεφάλαιο, θα υλοποιήσουμε την κατάλληλη τοπολογία του δικτύου της εταιρίας. Επίσης θα πάρουμε όλα τα απαραίτητα μέτρα, ώστε οι ρόλοι της κάθε οντότητας, που συμμετέχει στο δίκτυο, να είναι πλήρως καθορισμένοι. Επίσης, θα πάρουμε μέτρα για τον καθορισμό των δικαιωμάτων του κάθε ατόμου, ομάδας, τμήματος στα πλαίσια αξιοποίησης των πόρων του δικτύου. Όλα αυτά με γνώμονα το ότι τα μέτρα, που θα παρθούν, θα είναι προς την κατεύθυνση της αυξημένης ασφάλειας και ακεραιότητας τους συστήματος. Θα δημιουργηθούν και θα εξεταστούν δύο είδη δικτύου, ένα τοπικό και ένα δίκτυο σύνδεσης με το διαδίκτυο. Η λογική πάνω σε αυτό είναι να έχουμε απομονώσει τα κρίσιμα αρχεία που διαχειρίζονται οι εργαζόμενοι από το διαδίκτυο και να τα προστατεύουμε από την κοινή θέα σε αυτό. Το διαδίκτυο αποτελεί ένα σημαντικό κομμάτι της επιχείρησης, αλλά θέλουμε η αξιοποίηση του να είναι για λόγους επικοινωνίας με τους πελάτες και να ελαχιστοποιήσουμε την γενική χρήση του από τους χρήστες.

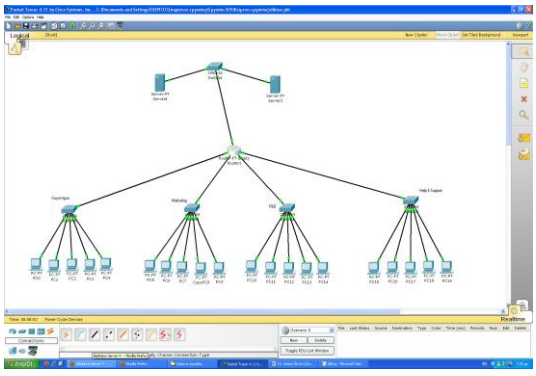
3.2 Περιγραφή του δικτύου

Η εταιρία αποτελείται από 4 τμήματα: το Λογιστικό τμήμα (Financial department), το τμήμα Marketing, το τμήμα Έρευνας και Ανάπτυξης (Research and Deployment department, R&D) και το τμήμα Βοήθειας και Υποστήριξης (Help & Support department). (εικόνα 3-1). Τα γραφεία των τμημάτων βρίσκονται στο 1 όροφο της εταιρίας, μαζί με το δωμάτιο των Servers και το Control Room.



Εικόνα 3-1

Το κάθε τμήμα έχει 5 εργαζόμενους, οι οποίοι έχουν ο καθένας τον προσωπικό του υπολογιστή. Αυτοί οι υπολογιστές είναι απομονωμένοι από το internet, για το οποίο υπάρχει ξεχωριστός υπολογιστής σε κάθε τμήμα που να εξυπηρετεί αυτή την ανάγκη. Κάθε τμήμα έχει το δικό του switch στο οποίο είναι συνδεδεμένοι οι PC των εργαζομένων του τμήματος. Οι switch συνδέονται με το router της εταιρίας και πάνω σε αυτόν είναι τοποθετημένοι και οι 2 Physical Servers, από τους οποίους γίνεται η διαχείριση του δικτύου. (εικόνα 3-2). Στο ισόγειο βρίσκονται τα γραφεία των ανώτερων στελεχών, (πρόεδρος, αντιπρόεδρος, διευθύνον σύμβουλος), στα οποία θα υπάρχουν και εκεί από 2 PC, 1 που θα είναι συνδεδεμένο στο τοπικό δίκτυο και ένα για την επικοινωνία με το internet. Επίσης υπάρχει σε ξεχωριστό γραφείο εγκατεστημένος ένας Print Server τον οποίο τον διαχειρίζονται 2 εργαζόμενοι και κρατάνε το αρχείο με τις εκτυπώσεις που έχουν πραγματοποιηθεί από τα τμήματα.



Εικόνα 3-2

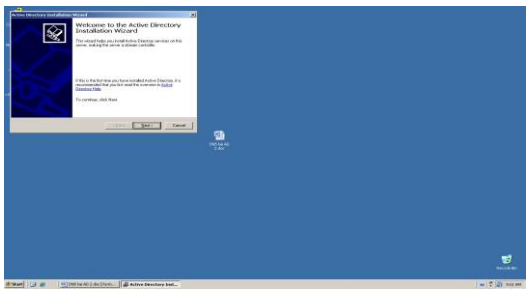
Στο Server Room υπάρχει επίσης, εκτός από τους 2 Server, ένας NAS, στον οποίο γίνεται η αποθήκευση των δεδομένων όλου του τοπικού δικτύου και ένα Backup PC, που γίνεται η λήψη αντιγράφων ασφαλείας, σε κρυπτογραφημένη μορφή.

3.3 Οι Servers

Οι Servers εκτελούν την κύρια διαχειριστική εργασία όλου του δικτύου. Έχουμε εγκατεστημένο λειτουργικό σύστημα Windows Server 2003 Standard Edition R2, το οποίο υποστηρίζει την υπηρεσία ενεργού καταλόγου Active Directory, DFS Replication, χρήση έξυπνων καρτών Smart Cards, δημόσιων και ιδιωτικών κλειδιών κρυπτογράφησης. Προσφέρει επίσης εργαλεία για την ανάλυση ασφαλείας συστημάτων και την εφαρμογή ομοιόμορφων ρυθμίσεων ασφαλείας σε ομάδες συστημάτων και τέλος, προσφέρει ένα περιβάλλον σεναρίων για την αυτοματοποίηση συνηθισμένων εργασιών διαχείρισης.

3.3.1 Active Directory

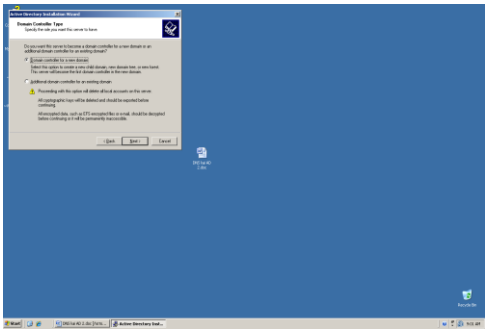
Η υπηρεσία ενεργού καταλόγου (Active Directory) αποτελεί την καρδία των Microsoft Windows Server 2003. Η τεχνολογία Active Directory βασίζεται σε καθιερωμένα πρωτόκολλα του Διαδικτύου και διαθέτει μια σχεδίαση η οποία μας βοηθάει να ορίσουμε τη δομή του δικτύου με σαφή τρόπο. Είναι μια υπηρεσία καταλόγου, που μπορεί να επεκτείνεται και να κλιμακώνεται, και η οποία επιτρέπει την αποδοτική διαχείριση των πόρων του δικτύου. [8]



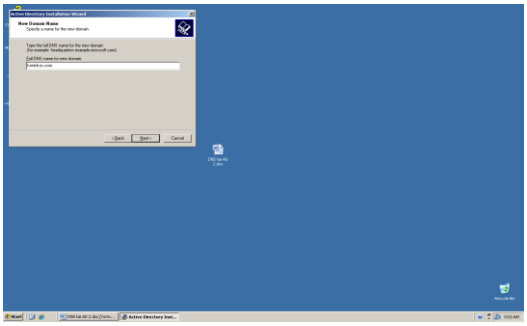
Εικόνα 3-3

Η εγκατάσταση το Active Directory γίνεται εύκολα μέσω του Active Directory Installation wizard (εικόνα 3-3). Μέσα από την διαδικασία εγκατάστασης καθορίζουμε τον το ρόλο που θα παίζει ο

Server. Επιλέγουμε να τον κάνουμε κύριο ελεγκτή τομέα Domain Controller στο νέο τομέα domain που φτιάχνουμε με όνομα kentrikos.com (εικόνες 3-4 και 3-5).

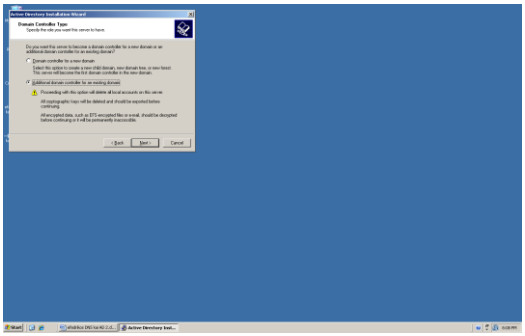


Εικόνα 3-3

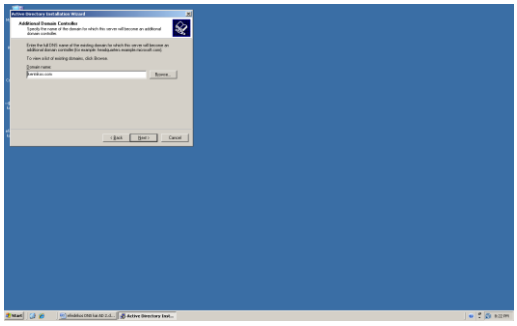


Εικόνα 3-2

Αντίστοιχη εργασία κάνουμε και στον εφεδρικό, 2^{ο} Server, που έχουμε εγκατεστημένο. Η διαδικασία εδώ διαφέρει στο ότι αυτόν τον Server τον δηλώνουμε σαν additional domain controller ώστε και αυτός μαζί με τον πρώτο Server να διαχειρίζονται εξίσου τον τομέα (εικόνα 3-6). Τον δηλώνουμε σαν domain controller του domain kentrikos.com, που δημιουργήσαμε προηγουμένως (εικόνα 3-7).



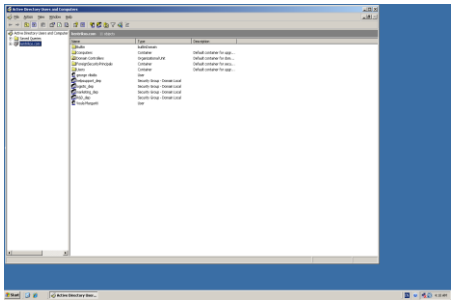
Εικόνα 3-6



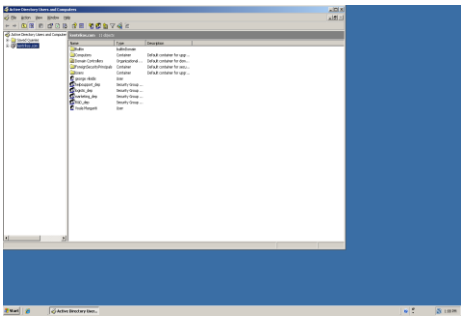
Εικόνα 3-7

Η ουσία της δουλειάς που κάνουμε είναι να εξασφαλίσουμε την απρόσκοπτη λειτουργία και συνέχεια (continuity) του συστήματος. Είναι πάντα υπαρκτός ο κίνδυνος ο ένας από τους 2 server να πέσει, είτε από σφάλμα υλικού, είτε από άλλο εξωγενή παράγοντα. Εμείς θέλουμε στην περίπτωση αυτή να αναλάβει την

αποκλειστική διαχείριση του δικτύου ο εφεδρικός server, χωρίς οι εργαζόμενοι να καταλάβουν τη διαφορά. Από τις εικόνες 3-8 και 3-9 φαίνεται ότι η επικοινωνία μεταξύ των 2 server έχει αποκατασταθεί και στο domain kentrikos.com δημιουργούνται και εμφανίζονται από κοινού οι λογαριασμοί των ομάδων και των χρηστών.



Εικόνα 3-8

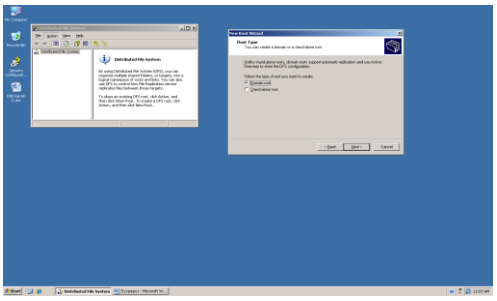


Εικόνα 3-9

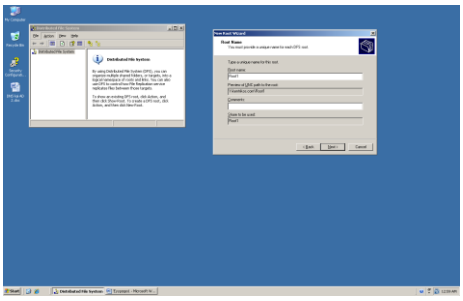
3.3.2 Distributed File System Replication

Το DFS replication είναι μια υπηρεσία, που χρησιμοποιείται για να δημιουργεί πανομοιότυπα αντίγραφα αρχείων από τον ένα server στον άλλο, έτσι ώστε να διατηρούμε πολλαπλές κόπιες αυτών των αρχείων σε διαφορετικές τοποθεσίες. Κάθε αλλαγή που συμβαίνει στο ένα μέλος του replication group αμέσως αντιγράφεται στο άλλο. Χρησιμοποιεί τον φάκελο staging για να καταγράψει ρώτα εκεί τα αρχεία πριν τα παραλάβει ή τα στείλει. Χρησιμοποιεί, επίσης, μια έκδοση πρωτοκόλλου ανταλλαγής για να ορίζει ακριβώς ποια αρχεία χρειάζεται να συγχρονιστούν. Όταν ένας φάκελος αλλάζει, μόνο τα αλλαγμένα μπλοκ αντιγράφονται και όχι ολόκληρο το αρχείο.

Εμείς θα εγκαταστήσουμε το DFS replication στο domain δημιουργώντας αρχικά μια κοινή ρίζα του DFS σε κάθε server. (εικόνες 3-10 και 3-11).

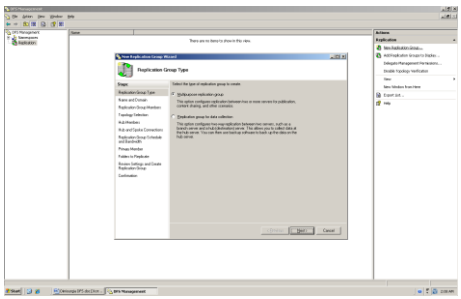


Εικόνα 3-10

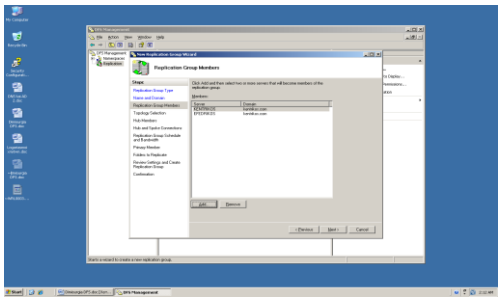


Εικόνα 3-11

Στο DFS Replication επιλέγουμε να εγκαταστήσουμε ένα multipurpose replication group, το οποίο μας δίνει επιπλέον προνόμια μεταξύ 2 ή περισσότερων server, όπως η δημοσίευση, ο διαμοιρασμός περιεχομένου φακέλων και άλλα σενάρια (εικόνα 3-12). Δηλώνουμε το όνομα του group (MAIN_REP), προσθέτουμε τους server (τουλάχιστον 2), οι οποίοι θα γίνουν μέλη του group (εικόνα 3-13) και επιλέγουμε την full mesh topology όπου κάθε μέλος αντιγράφει δεδομένα από κάθε άλλο μέλος της ομάδας (εικόνα 2-14).

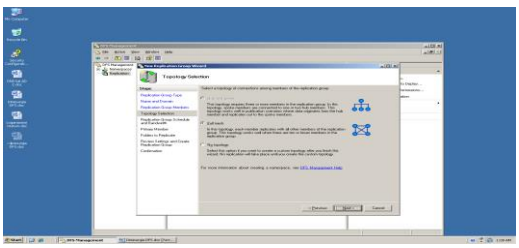


Εικόνα 3-12

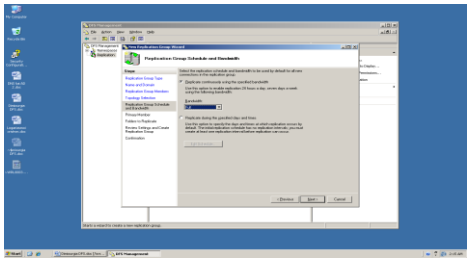


Εικόνα 3-13

Στη συνέχεια επιλέγουμε το replication να είναι συνεχόμενο 24 ώρες το 24ωρο και επί εφτά μέρες την εβδομάδα (εικόνα 3-15) και να γίνεται πάνω σε όλο το σκληρό δίσκο και των 2 servers.



Εικόνα 3-14



Εικόνα 3-15

Με αυτό τον τρόπο έχουμε εξασφαλίσει την συνεχή λειτουργία του δικτύου μας και το ότι ανά πάσα στιγμή τα δεδομένα και τα αρχεία, που χειρίζονται οι υπάλληλοι της εταιρίας, είναι διαθέσιμα. Έχουμε εξασφαλίσει, επίσης, ότι σε περίπτωση βλάβης ενός από τους servers , θα έχουμε τη δυνατότητα και το χρονικό περιθώριο ανάνηψης του συστήματος και λειτουργίας με βάση την αρχική κατάσταση.

3.4 Διαμόρφωση του Cisco router

Για να διαμορφώσουμε και να ασφαλίσουμε ένα Cisco router, χρειάζεται να έχουμε δικαιώματα διαχειριστή, τα οποία παίρνουμε με την εντολή enable. Από εκεί ρυθμίζουμε το όνομα του router, ορίζουμε τους κωδικούς πρόσβασης, διαμορφώνουμε τα interfaces που θα χρησιμοποιηθούν και σώζουμε τις βασικές ρυθμίσεις που κάναμε.

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname LocalRouter
LocalRouter(config)#enable secret gv0393
LocalRouter(config)#line console 0
LocalRouter(config-line)#password ergasia
LocalRouter(config-line)#login
LocalRouter(config-line)#exit
LocalRouter(config)#line vty 0 4
LocalRouter(config-line)#password ptixiaki
LocalRouter(config-line)#login
LocalRouter(config-line)#exit
LocalRouter(config)#
```

Ορίσαμε το όνομα του router, hostname **LocalRouter**, τον κωδικό ασφαλείας ,enable secret **gv0393**, για να μπορεί κάποιος να έχει δικαιώματα διαχειριστή στην κονσόλα, και ορίσαμε τους κωδικούς ασφαλείας για τη χρήση της κονσόλας, password **ergasia** και την υπηρεσία Telnet, password **ptixiaki**.

Στη συνέχεια διαμορφώνουμε τα interfaces του router και δίνουμε ip address, και subnet mask. Για τη σύνδεση με το πρώτο switch έχουμε:

```
LocalRouter(config)#interface FastEthernet0/0
LocalRouter(config-if)#ip address 192.168.1.1
255.255.255.0
LocalRouter(config-if)#description connection1
LocalRouter(config-if)#no shutdown
```

Αντίστοιχα διαμορφώνουμε και τα υπόλοιπα interfaces FastEthernet1/0 ip address 192.168.2.1, FastEthernet2/0 ip address 192.168.3.1, FastEthernet3/0 ip address 192.168.4.1, και την GigabitEthernet4/0 ip address 192.168.5.1 για τη σύνδεση με το switch των 2 server. Σώζουμε την διαμόρφωση που κάναμε σαν την αρχική διαμόρφωση πλέον του router με την εντολή LocalRouter#copy **running-config startup-config** και εκτελούμε την εντολή **show ip route** για να επιβεβαιώσουμε ότι έχουν συνδεθεί και είναι ενεργοποιημένα όλα τα interfaces.

```
LocalRouter#show ip route

C           192.168.1.0/24   is   directly   connected,
FastEthernet0/0
C           192.168.2.0/24   is   directly   connected,
FastEthernet1/0
C           192.168.3.0/24   is   directly   connected,
FastEthernet2/0
C           192.168.4.0/24   is   directly   connected,
FastEthernet3/0
```

```
C            192.168.5.0/24   is   directly   connected,
GigabitEthernet4/0
```

Ενεργοποιούμε την υπηρεσία για να ορίσουμε κρυπτογραφημένα password με την εντολή LocalRouter(config)#service password-encryption και έχουμε στην κονσόλα:

```
line con 0
 password 7 08245E49080A0C16
 login
line vty 0 4
 password 7 083158471110041C1B
 login
```

Τέλος ορίζουμε το μήνυμα της ημέρας banner motd, ώστε να προειδοποιούμε αυτούς που θα επιχειρήσουν μια μη εξουσιοδοτημένη πρόσβαση στο router μας, με την εντολή:
LocalRouter(config)#banner motd # ***** **Unauthorized Access Prohibited** ****** #.

3.4.1 Address Resolution Protocol (ARP)

Το ARP είναι το πρωτόκολλο που μας επιτρέπει να μετατρέπουμε διευθύνσεις IP σε MAC φυσικές διευθύνσεις τοπικού δικτύου.

Όταν ένας router συνδεδεμένος σε ένα τοπικό δίκτυο λάβει ένα πακέτο IP, που προορίζεται για κάποιον από τους σταθμούς του τοπικού δικτύου, για να το αποστείλει θα πρέπει εκτός από τη διεύθυνση IP να γνωρίζει και τη φυσική διεύθυνση MAC address του αποδέκτη. Το ARP βοηθά το router να μάθει την φυσική αυτή διεύθυνση.

Για να το πετύχει ο router, αποστέλλει στο τοπικό δίκτυο μια ερώτηση (ARP request) υπό μορφή broadcast στην οποία έχει περιλάβει και την IP διεύθυνση. Ο σταθμός του δικτύου, που θα αναγνωρίσει την διεύθυνσή του θα απαντήσει με μια

ARP replay. Ο router δέχεται την απάντηση αυτή και ενημερώνεται γι τη φυσική διεύθυνση του σταθμού που απάντησε, την οποία καταγράφει σε ένα πίνακα (ARP cache) σχετίζοντας τη με την αντίστοιχη διεύθυνση IP. [9]

Με τη χρήση του ARP μπορούμε να αποφύγουμε επιθέσεις του τύπου Man-in-the-middle (MITM). Η MITM είναι μια κοινή παραβίαση ασφάλειας. Ο επιτιθέμενος παρεμποδίζει μια νόμιμη επικοινωνία μεταξύ δύο μερών, τα οποία είναι φιλικά μεταξύ τους. Στη συνέχεια, ο κακόβουλος host ελέγχει τη ροή επικοινωνίας και μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες. Οι man-in-the-middle επιθέσεις έχουν δύο κοινές μορφές:

- ο επιτιθέμενος είτε κρυφακούει (eavesdropping)
- είτε και αλλοιώνει κατάλληλα το μήνυμα

Με eavesdropping (κρυφακοή), ένας επιτιθέμενος ακούει απλά ένα σύνολο μεταδόσεων σε και από διαφορετικούς hosts, ακόμα κι αν ο υπολογιστής του επιτιθεμένου δεν είναι συμβαλλόμενο μέρος στη συνδιάλεξη. Πολλοί σχετίζουν αυτόν τον τύπο επίθεσης με διαρροή, κατά την οποία ευαίσθητες πληροφορίες μπορούν να αποκαλυφθούν σε έναν τρίτο, χωρίς αυτό να είναι εν γνώση των νόμιμων χρηστών.

Οι επιθέσεις κατά τις οποίες προκαλείται αλλοίωση του μηνύματος βασίζονται στην ικανότητα του επιτιθέμενου να κρυφακούει. Ο επιτιθέμενος παίρνει αυτή την μη εξουσιοδοτημένη απόκριση, ένα ρεύμα δεδομένων (data stream), αλλάζοντας τα περιεχόμενα ώστε να ικανοποιούν έναν ορισμένο σκοπό - πιθανόν χρησιμοποιώντας ψευδή διεύθυνση IP, αλλάζοντας την διεύθυνση MAC για να μιμηθεί κάποιο άλλο host ή κάνοντας κάποια άλλη τροποποίηση. [10]

Εμείς για τη διαμόρφωση του ARP πρέπει να αντιστοιχήσουμε χειροκίνητα τις διευθύνσεις IP με τις διευθύνσεις MAC, ώστε να δημιουργήσουμε τον ARP πίνακα.

Έτσι πηγαίνουμε στο router και από το CLI δίνουμε την εντολή:

Router(config)# arp 192.168 2.1 000B.BE2D.9801

Και στη συνέχεια αντιστοιχούμε όλες τις θύρες του router με τις φυσικές διευθύνσεις τους.

Έπειτα μας ενδιαφέρει το ίδιο πρωτόκολλο πιστοποίησης να το χρησιμοποιούν και οι 2 server του τοπικού δικτύου. Κάνουμε λοιπόν την ίδια περίπου εργασία και σε αυτή την περίπτωση.

Από το command prompt των server δίνουμε την εντολή:

`arp –s ip_address mac_address`, δηλαδή γα τους server της εταιρίας:

```
arp – s 192.168.5.2  0001.97EA.CE07
```

3.5 Διαμόρφωση των Switch

Όπως και με τον router του δικτύου, έτσι και με τις switch, που είναι σε κάθε τμήμα της εταιρίας, κάνουμε την αντίστοιχη διαμόρφωση. Ασφαλίζουμε την κονσόλα για να εξασφαλίσουμε περιορισμένη πρόσβαση από εξουσιοδοτημένα άτομα μόνο.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret myswitch
S1(config)#line con 0
S1(config-line)#password myswitch2
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#password myswitch3
S1(config-line)#login
S1(config-line)#exit
```

Ενεργοποιούμε την υπηρεσία για την κρυπτογράφηση των κωδικών μας, με την εντολή S1(config)#service password-encryption και έχουμε το παρακάτω μήνυμα:

```
Current configuration : 978 bytes
service password-encryption
hostname S1
line con 0
 password 7 082C555D1E1011141A59
 login
line vty 0 4
 password 7 082C555D1E1011141A58
 login
line vty 5 15
```

Λόγω του ότι μια switch συμπεριφέρεται σαν ένα hub, το οποίο σημαίνει ότι κάθε σύστημα που συνδέεται στο switch, μπορεί εν δυνάμει να δει όλη την κίνηση στο δίκτυο μας από όλες τις συσκευές που είναι συνδεδεμένες σε αυτό. Επιπλέον, ένας εισβολέας μπορεί να συλλέξει πληροφορίες όπως οι κωδικοί πρόσβασης ή τις πληροφορίες με τις οποίες διαμορφώσαμε όλο το δίκτυό μας. Όλες οι θύρες της switch πρέπει να ασφαλιστούν πριν χρησιμοποιηθούν, με ένα αριθμό από κατάλληλες MAC διευθύνσεις που θα επιτρέπονται να συνδέονται με αυτές. Με αυτό τον τρόπο η θύρα αυτή στέλνει όλα τα πακέτα στις MAC διευθύνσεις που έχει αποθηκευμένες και όχι γενικά σε όλο το δίκτυο.

```
S1(config)#interface FastEthernet0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 1
S1(config-if)#switchport    port-security    mac-address
00D0.D308.1BC4
```

```
S1(config-if)#switchport port-security mac-address
sticky
S1(config-if)#exit
S1(config)#end
S1#copy running-config startup-config
S1#show port-security interface FastEthernet0/1
```

Port Security	Enabled
Port Status	Secure-up
Violation Mode	Shutdown
Total MAC Addresses	0 mins
Aging Type	Absolute
SecureStatic Address Aging	Disabled
Maximum MAC Addresses	1
Aging Time	1
Security Violation Count	0
Last Source Address:Vlan	0
Sticky MAC Addresses	0000.0000.0000:0
Configured MAC Addresses	1

Αφού ορίσαμε για τη μια θύρα FastEthernet0/1 ότι μπορεί να συνδέεται μόνο η συγκεκριμένη MAC διεύθυνση, η οποία ανήκει στο πρώτο PC, συνεχίζουμε και κάνουμε το ίδιο σε όλα τα switch, δηλώνοντας κάθε υπολογιστή ξεχωριστά.

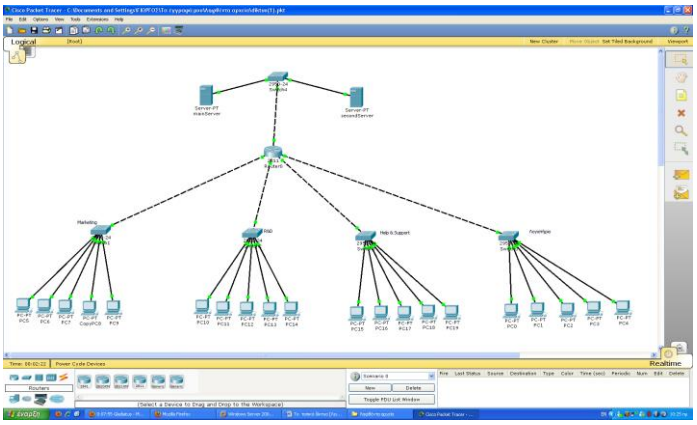
3.5.1 VLANs

Ένα σημαντικό πρόβλημα, που αντιμετωπίζουν τα δίκτυα μεταγωγής/γεφύρωσης, είναι ο μεγάλος φόρτος πακέτων που μπορεί να κυκλοφορεί και να δημιουργεί συνεχή προβλήματα στην ομαλή λειτουργία τους. Ο λόγος είναι και προαναφέρθηκε πιο πριν, ότι οι μεταγωγείς (switches) προωθούν τα πακέτα σε όλο το δίκτυο που είναι συνδεδεμένοι και δεν χρησιμοποιούν τη δρομολόγηση πακέτων.

Μια σημαντική λύση σε αυτό το πρόβλημα είναι και η δημιουργία των VLANs, (Virtual LANs). Ένα VLAN είναι μια ομάδα θυρών ενός ή περισσότερων μεταγωγέων , που ορίζεται από το υλικό ή το λογισμικό του μεταγωγέα ως μια περιοχή εκπομπής. Ο σκοπός των εικονικών δικτύων είναι η ομαδοποίηση συσκευών οι οποίες συνδέονται στο μεταγωγέα σε λογικές περιοχές εκπομπών, για τον έλεγχο τη επίδρασης, που έχουν οι εκπομπές σε άλλες συνδεδεμένες συσκευές. Έτσι ένα VLAN μπορεί να χαρακτηριστεί σαν ένα λογικό δίκτυο. Τα πλεονεκτήματα των VLANs είναι τα εξής:

- Ασφάλεια
- Κατάτμηση
- Ευελιξία

Στην εταιρία, λόγω του ότι έχουμε σε συνεχή λειτουργία τουλάχιστον 30 υπολογιστές, ο φόρτος πακέτων που δημιουργείται μεταξύ ιδιαίτερα των τμημάτων είναι μεγάλος. Για αυτό πρέπει να πάρουμε τα μέτρα μας ώστε τα πακέτα ενός τμήματος να μην δρομολογούνται και στα υπόλοιπα τμήματα, αλλά να πηγαίνουν αποκλειστικά στους Servers και στις μονάδες αποθήκευσης. Επομένως δημιουργούμε 5 εικονικά δίκτυα, ένα για κάθε τμήμα και ένα για τους Servers. (εικόνα 3-16)Οι ονομασίες των VLAN είναι αντίστοιχες με τις ονομασίες των τμημάτων. Πάνω στον Router κάνουμε και τις κατάλληλες επιλογές δρομολόγησης με access list ώστε να μην έχει πρόσβαση το ένα VLAN με το άλλο.



Εικόνα 3-16

Σε κάθε switch δημιουργούμε και ο αντίστοιχο VLAN και δηλώνουμε σε αυτό μόνο τις θύρες που είναι συνδεδεμένοι οι υπολογιστές.

```
Switch(config)#vlan 2
Switch(config)#name Marketing
```

Δημιουργήσαμε στο switch του τμήματος Marketing το VLAN με το ίδιο όνομα. Στη συνέχεια δηλώνουμε τις θύρες των υπολογιστών σαν μέλη αυτού του εικονικού δικτύου.

```
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport access vlan 2
Switch(config-if)#switchport mode access
```

Τον ίδιο κώδικα πληκτρολογούμε και για τις θύρες FastEthernet0/2, 0/3, 0/4, 0/5, 0/6.

Συνεχίζουμε τη διαδικασία και σε όλους τους υπόλοιπους μεταγωγείς δημιουργώντας εικονικά δίκτυα και για αυτούς. Μόλις ολοκληρώσουμε τη διαδικασία πρέπει να πάρουμε τα μέτρα μας ώστε να γεφυρώσουμε τους μεταγωγείς (trunking). Αυτό όμως θα μας εξυπηρετήσει σε μελλοντική χρήση, σε περιπτώσεις που θέλουμε να προσθέσουμε κάποιους υπολογιστές σε ένα μεταγωγέα που δεν θα ανήκουν στο εικονικό δίκτυο των υπόλοιπων υπολογιστών. Εμείς αυτό που θέλουμε είναι να πάρουμε μέτρα αποκλεισμού των εικονικών δικτύων μεταξύ τους.

Το πρώτο πράγμα που κάνουμε είναι δημιουργήσουμε τη ζεύξη μεταξύ των VLAN. Αυτό το κάνουμε στον router, δηλώνοντας τις θύρες, στις οποίες είναι συνδεδεμένοι οι μεταγωγείς, σαν μέρη της ζεύξης.

```
LocalRouter(config)#interface FastEthernet1/0
LocalRouter(config-if)#switchport mode trunk
```

Αντίστοιχη δουλειά κάνουμε και για τις θύρες FastEthernet1/1, 1/2, 1/3, 1/4. Τα vlan που έχουν δηλωθεί αποτελούν πλέον ξεχωριστά interfaces πάνω στον router. Από εκεί θα εξασφαλίσουμε την κίνηση σε όλο το δίκτυο.

Δίνουμε ip address σε όλα τα vlan interfaces. Το vlan 5 είναι το εικονικό δίκτυο των server.

```
interface Vlan5
ip address 192.168.5.1 255.255.255.0
```

Και επιτρέπουμε την κίνηση προς και από του servers

```
ip access-list standard Servers
 permit 192.168.5.0 0.0.0.255
 deny any
```

Συνεχίζουμε με το κάθε vlan και δηλώνουμε ότι α έχει πρόσβαση μόνο στο vlan των servers.

```
LocalRouter(config)#interface Vlan2
```

```
    LocalRouter(config-if)#ip       address       192.168.2.1
255.255.255.0
    LocalRouter(config-if)#ip access-group Servers out
```

Κάνουμε ping από και προς όλα τα vlan για να επαληθεύσουμε ότι οι ρυθμίσεις που κάναμε είναι σωστές. Από τον πρώτο υπολογιστή του τμήματος Marketing κάνουμε ping στο pc με ip 192.168.4.2 και έχουμε την απάντηση

```
    PC>ping 192.168.4.2

    Pinging 192.168.4.2 with 32 bytes of data:

    Reply from 192.168.2.1: Destination host unreachable.
    Reply from 192.168.2.1: Destination host unreachable.
    Reply from 192.168.2.1: Destination host unreachable.
    Reply from 192.168.2.1: Destination host unreachable.

    Ping statistics for 192.168.4.2:
        Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

Βλέπουμε ότι η πρόσβαση στο συγκεκριμένο vlan δεν μας επιτρέπεται. Αντίθετα αν κάνουμε ping στον κεντρικό server, έχουμε:

```
    PC>ping 192.168.5.2

    Pinging 192.168.5.2 with 32 bytes of data:

    Reply from 192.168.5.2: bytes=32 time=110ms TTL=127
    Reply from 192.168.5.2: bytes=32 time=125ms TTL=127
    Reply from 192.168.5.2: bytes=32 time=94ms TTL=127
    Reply from 192.168.5.2: bytes=32 time=110ms TTL=127

    Ping statistics for 192.168.5.2:
        Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
    Minimum = 94ms, Maximum = 125ms, Average = 109ms
```

Βλέπουμε, δηλαδή, ότι εδώ μας επιτρέπεται η πρόσβαση. Αντίθετα παρατηρούμε ότι η επικοινωνία από τους server προς τους υπολογιστές επιτρέπεται.

```
SERVER>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=62ms TTL=127
Reply from 192.168.2.2: bytes=32 time=63ms TTL=127
Reply from 192.168.2.2: bytes=32 time=110ms TTL=127
Reply from 192.168.2.2: bytes=32 time=109ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 110ms, Average = 86ms
```

3.6 Διαχείριση συστήματος αρχείων και φακέλων

Η διαχείριση του συστήματος αρχείων είναι από τις πιο σημαντικές παραμέτρους της ασφάλειας του δικτύου. Από εδώ μπορούμε να ορίσουμε τα δικαιώματα και τα απαγορεύσεις πάνω στους χρήστες, να διαχειριστούμε τα αρχεία και να δημιουργήσουμε σενάρια αυτοματοποίησης διεργασιών.

Η ουσία είναι να μπορέσουμε να δημιουργήσουμε μια διαδικασία, η οποία θα εξασφαλίζει, ότι τα δικαιώματα των χρηστών είναι πλήρως αποσαφηνισμένα για το πού έχουν πρόσβαση, αλλά κυρίως για το πού δεν έχουν και ότι δεν θα έχουμε ένα πολύπλοκο σύστημα διαχείρισης των αρχείων, το οποίο θα μπερδεύει τους χρήστες, παρά θα διευκολύνει. Η δομή και η ιεράρχηση των φακέλων και των δικαιωμάτων μπορεί να είναι κάπως έτσι:

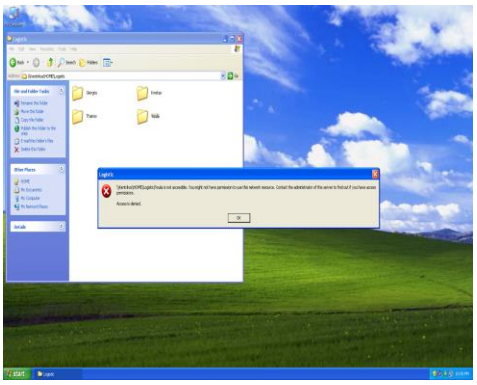
Ο κεντρικός φάκελος που θα περιλαμβάνει όλους τους υποφακέλους των τμημάτων και παρακάτω των εργαζομένων θα είναι ο HOME. Εκεί μέσα δημιουργούμε τους φακέλους των τεσσάρων τμημάτων (Logistic, Marketing, R&D, H&S) και μέσα σε αυτούς δημιουργούμε τους φακέλους των εργαζομένων. Ο φάκελος HOME είναι read-write και επιλέγουμε και όλοι οι υποφάκελοι να κληρονομούν αυτό το δικαίωμα. Επίσης, θα δημιουργήσουμε και ένα φάκελο PUBLIC ο οποίος θα είναι κοινόχρηστος για όλους τους εργαζόμενους της εταιρίας, για ανταλλαγή αρχείων όποτε χρειαστεί. Χρειάζεται προσοχή εδώ, αλλά και όποτε κάνουμε ανάθεση δικαιωμάτων σε χρήστες, να διαγράφουμε από την καρτέλα ασφαλείας την επιλογή Users(Kentrikos0\Users) και να προσθέτουμε την επιλογή Authenticated Users. Κανένας χρήστης δεν θα έχει δικαίωμα μετατροπής των αρχείων σε όλος τους φακέλους εκτός από τον δικό του.

Στον φάκελο του κάθε τμήματος οι μόνοι που θα επιτρέπεται να έχουν πρόσβαση θα είναι οι εργαζόμενοι του τμήματος αυτού και μόνο. Δεν θα επιτρέπεται σε κανέναν άλλο να μπαίνει στους συγκεκριμένους φακέλους. Για αυτό και στον φάκελο του τμήματος και από την καρτέλα Ιδιότητες -> Ασφάλεια διαγράφουμε από τους επιτρεπόμενους χρήστες το Users(Kentrikos0\Users) και προσθέτουμε το τμήμα στο οποίο αντιστοιχεί ο φάκελος. Έτσι πρόσβαση στο φάκελο του κάθε τμήματος θα έχουν οι εργαζόμενοι που έχουμε δηλώσει ότι είναι μέλη του.

Λόγω του ότι κάποιες φορές οι εργαζόμενοι, οι οποίοι ανήκουν στο ίδιο τμήμα, μεταξύ τους θα χρειαστεί να ανταλλάσουν ορισμένα αρχεία, που θα τους εξυπηρετούν στη δουλειά τους, θα δημιουργήσουμε και ένα δημόσιο φάκελο (DropBox) μόνο για το κάθε τμήμα, στον οποίο όλοι οι εργαζόμενοι του εκάστοτε τμήματος θα έχουν δικαιώματα εγγραφής και ανάγνωσης (read-write) και όχι τροποποίησης.

Ο κάθε εργαζόμενος θα έχει τον δικό του προσωπικό φάκελο, στον οποίο θα αποθηκεύονται τα αρχεία του και από όπου θα έχει δικαίωμα ανάγνωσης και εγγραφής και τροποποίησης, αφού είναι τα αρχεία που θα επεξεργάζεται καθημερινά. Σε κάθε προσωπικό φάκελο εργαζομένου δεν θα έχει δικαίωμα πρόσβασης κανένας άλλος παρά μόνο οι διαχειριστές του δικτύου.

Στους φακέλους των χρηστών διαγράφουμε και εδώ από τους επιτρεπόμενους χρήστες το Users(Kentrikos0\Users) και προσθέτουμε τον αντίστοιχο χρήστη στον οποίο θα ανήκει ο φάκελος. Σε αυτόν τον φάκελο δίνουμε δικαίωμα εγγραφής, ανάγνωσης και τροποποίησης από τον χρήστη. Από τον λογαριασμό του χρήστη gvlisidis κάνουμε δοκιμή εγγραφής στον προσωπικό του φάκελο και σε έναν φάκελο άλλου εργαζομένου. Στον προσωπικό η εγγραφή αλλά και η τροποποίηση γίνονται κανονικά, ενώ στον φάκελο άλλου εργαζομένου δεν έχει δικαίωμα πρόσβασης.(εικόνα 3-17).

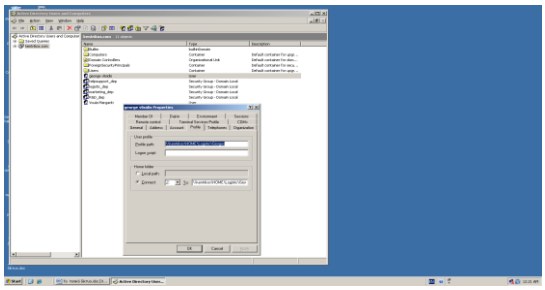


Εικόνα 3-17

3.6.1 Ανάθεση αρχικού φακέλου

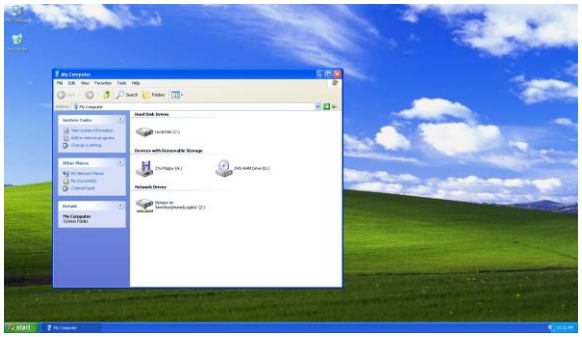
Οι αρχικοί φάκελοι και ο φάκελος "Τα έγγραφά μου" (My Documents) κάνουν ευκολότερη για ένα διαχειριστή τη δημιουργία αντιγράφων ασφαλείας των αρχείων χρήστη και τη διαχείριση λογαριασμών χρήστη, συλλέγοντας τα αρχεία χρήστη σε μία θέση. Εάν αντιστοιχίσουμε έναν αρχικό φάκελο σε ένα χρήστη, μπορούμε να αποθηκεύουμε τα δεδομένα χρήστη σε μια κεντρική θέση και να εκτελούμε δημιουργία αντιγράφων ασφαλείας και επαναφορά δεδομένων ευκολότερα και πιο αξιόπιστα.

Στην εταιρία η αποθήκευση των δεδομένων γίνεται στον NAS, οπότε εκεί δημιουργούμε τους λογαριασμούς και αντιστοιχούμε στους χρήστες τους αρχικούς φακέλους. Αυτό το κάνουμε ως εξής: πηγαίνουμε στους χρήστες τομέα πατάμε ιδιότητας και στην καρτέλα με τα προσωπικά δεδομένα επιλέγουμε το profile. Στον home folder και στο πεδίο **(connect)** καθορίζουμε ένα γράμμα της μονάδας δίσκου που θέλουμε να «βλέπει» ο χρήστης και στη συνέχεια στο πεδίο **(To)** πληκτρολογούμε όλη τη διαδρομή,(εικόνα 3-18) η οποία είναι: \\kentrikos\HOME\Logistic\Giorgos .



Εικόνα 3-18

Αυτόματα στον υπολογιστή του αντίστοιχου χρήστη δημιουργείται η διασύνδεση με τη μονάδα δίσκου που αντιστοιχίσαμε το λογαριασμό του. Από εκεί πλέον έχει άμεση πρόσβαση στον προσωπικό του φάκελο και παράλληλα εξασφαλίσαμε ότι δεν έχει άμεση επαφή με τους φακέλους των άλλων εργαζομένων (εικόνα 3-19). Επειδή όμως όπως είπαμε προηγουμένως, θα υπάρχει ορισμένες φορές η ανάγκη για ανταλλαγή αρχείων, έτσι ο κάθε εργαζόμενος από την καρτέλα entire network θα έχει πρόσβαση στον φάκελο PUBLIC, τον οποίο δημιουργήσαμε για αυτό το λόγο.



Εικόνα 3-19

3.6.2 Σενάρια σύνδεσης (Logon scripts)

Τα logon scripts (ονομάζονται και αρχεία δέσμης) είναι διαταγές που πρέπει να εκτελούνται όταν συνδέεται ο χρήστης. Με τα σενάρια σύνδεσης μπορούμε να ορίσουμε την ώρα του συστήματος, τις διαδρομές των μονάδων του δικτύου, τους εκτυπωτές του δικτύου, και πολλά άλλα. Αν και μπορούμε να τα χρησιμοποιήσουμε ια να εκτελέσουμε διαταγές μια φορά, δεν πρέπει να

χρησιμοποιούνται για ορισμό μεταβλητών περιβάλλοντος, γιατί όλες οι ρυθμίσεις περιβάλλοντος, που χρησιμοποιούνται από τα σενάρια δεν διατηρούνται για μελλοντικές διαδικασίες του χρήστη.

Τα σενάρια σύνδεσης μπορεί να είναι Windows Script Host με προέκταση .vbs .js, αρχεία δέσμης διαταγών με προέκταση .bat, αρχεία διαταγών με προέκταση .cmd και εκτελέσιμα προγράμματα με προέκταση .exe. τα σενάρια σύνδεσης δηλώνονται στην καρτέλα profile από το Active Directory Users And Computers, στο πεδίο logon script. Ένα σενάριο, που θα μπορούσαμε να αντιστοιχίσουμε για τους χρήστες της εταιρίας είναι το εξής:

Echo: OFF

NET USE Z:\\KENTRIKOS\HOME\LOGISTIC\GIORGOS * για να ορίσουμε τη σύνδεση με τον αρχικό φάκελο του κάθε χρήστη.

NET USE [LPT1:] \\KENTRIKOS\LOCAL_PRINTER * για να αντιστοιχίσουμε έναν εκτυπωτή στο χρήστη.

NET TIME \\KENTRIKOS /SET /YES * για να συγχρονίσουμε το ρολόι του υπολογιστή με αυτό του server.

NET SEND MESSAGE * για να στείλουμε ένα μήνυμα στον κάθε χρήστη με την είσοδό του.

Γράφουμε τον κώδικα σε ένα txt αρχείο και το σώζουμε με ως login.cmd στον φάκελο C:\WINDOWS\SYSVOL\domain\scripts.

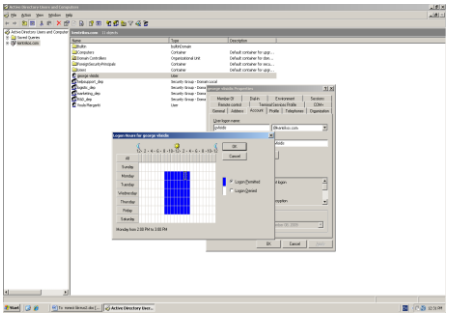
3.6.3 Διαχείριση ωρών σύνδεσης

Μπορούμε να ελέγχουμε επίσης πότε και ποιες ώρες θα συνδέονται οι χρήστες στο δίκτυο. Αυτό γίνεται με τον καθορισμό των έγκυρων ωρών σύνδεσης τους. Τους περιορισμούς αυτούς μπορούμε να τους χρησιμοποιήσουμε και σα μέτρο αύξησης της ασφάλειας και προστασίας από εισβολή ή κακόβουλη χρήση μετά τις συνήθεις ώρες εργασίας. Κατά τη διάρκεια των έγκυρων ωρών σύνδεσης, οι χρήστες μπορούν να εργάζονται όπως συνήθως, να συνδέονται στο δίκτυο και αξιοποιούν τους πόρους του. Κατά τη διάρκεια των απαγορευμένων ωρών δεν μπορούν να εργαστούν.

Δύο περιπτώσεις υπάρχουν στο ενδεχόμενο ένας χρήστης να ξεπεράσει το επιτρεπόμενο όριο σύνδεσης:

1. **Αναγκαστική αποσύνδεση**. Με αυτή την πολιτική οι χρήστες που ξεπερνάνε το όριο σύνδεσης, θα αποσυνδέονται αυτόματα από όλους τους πόρους και από το δίκτυο.
2. **Μη αποσύνδεση**. Σε αυτή την περίπτωση οι χρήστες δεν αποσυνδέονται από το δίκτυο, απλώς δεν μπορούν να κάνουν νέες συνδέσεις δικτύου. [8]

Για λόγους αυξημένης ασφαλείας ορίζουμε την άμεση αποσύνδεση του χρήστη με το πέρας του επιτρεπόμενου χρόνου. Φροντίζουμε στην πολιτική χρήσης του δικτύου να αποσαφηνίσουμε ότι ο εργαζόμενος που θα χρειαστεί παράταση της χρήσης του δικτύου, να έρχεται σε συνεννόηση με τον προϊστάμενο του για να του επιτραπεί από τους διαχειριστές του δικτύου να του δώσουν επιπλέον ώρες. (εικόνα 3-20).



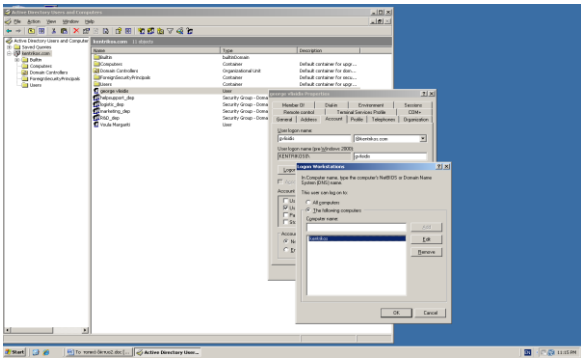
Εικόνα 3-20

Στην εικόνα φαίνεται ότι οι ώρες που θα μπορεί ο χρήστης να συνδέεται είναι μόνο κατά το εργάσιμο της ημέρας και ορίζονται με μπλε χρώμα. Αντίθετα με άσπρο χρώμα ορίζονται οι ώρες και οι ημέρες (Σάββατο, Κυριακή), κατά τις οποίες δεν μπορεί να συνδεθεί.

3.7 Σταθμοί εργασίας επιτρεπόμενης σύνδεσης

Η συγκεκριμένη πολιτική ελέγχει τη δυνατότητα αν ο χρήστης έχει τη δυνατότητα να καθίσει στο πληκτρολόγιο του υπολογιστή και να συνδεθεί στο σύστημα. Το δικαίωμα σύνδεσης των χρηστών από οποιονδήποτε σταθμό εργασίας εμπεριέχει πολλούς κινδύνους από πλευράς ασφαλείας. Αν δεν περιορίσουμε τη χρήση των σταθμών εργασίας, όποιος αποκτήσει ένα όνομα χρήστη και κωδικό πρόσβασης θα μπορεί να τα χρησιμοποιεί για να συνδεθεί σε οποιοδήποτε σταθμό εργασίας της περιοχής. Με τον ορισμό μιας λίστας με

σταθμούς εργασίας από όπου θα επιτρέπεται η σύνδεση, κλείνουμε τις χαραμάδες στην περιοχή και μειώνουμε τους κινδύνους. Δεν αρκεί πλέον για τους εισβολείς να βρουν ένα όνομα χρήστη και τον αντίστοιχο κωδικό πρόσβασης, πρέπει επίσης να βρουν κα τους αντίστοιχους σταθμούς εργασίας από όπου επιτρέπεται η πρόσβαση. Αυτή παράμετρος «δένει» περισσότερο την ασφάλεια του δικτύου με την φυσική ασφάλεια και τους ελέγχους πρόσβασης στις εγκαταστάσεις της εταιρίας.



Εικόνα 3-21

Την επιλογή αυτή τη δημιουργούμε από την καρτέλα Account του χρήστη από το Active Directory Users And Computers. (εικόνα 3-21)Στην επιλογή log on το ενεργοποιούμε τη σύνδεση σε συγκεκριμένους υπολογιστές και τους προσθέτουμε στη λίστα που βρίσκεται παρακάτω.[8]

Κεφάλαιο 4

ΟΡΙΣΜΟΣ ΠΟΛΙΤΙΚΩΝ ΛΟΓΑΡΙΑΣΜΩΝ

4.1 Εισαγωγή

Η πολιτική ομάδων είναι ένα σύνολο κανόνων, που μας βοηθάει να διαχειριζόμαστε χρήστες και υπολογιστές. Οι πολιτικές ομάδων μπορούν να εφαρμόζονται σε πολλές περιοχές, σε μεμονωμένες περιοχές, σε υποομάδες μέσα σε μια περιοχή, ή σε μεμονωμένα συστήματα. Ειδικότερα οι τελευταίες αναφέρονται και ως τοπικές πολιτικές ομάδων (local group policies) και αποθηκεύονται μόνο στο τοπικό σύστημα.

Οι ρυθμίσεις πολιτικής ομάδων αποθηκεύονται σε ένα αντικείμενο πολιτικής ομάδας (Group Policy Object, GPO). Σε μια τοποθεσία, περιοχή, ή οργανωτική μονάδα μπορούμε να εφαρμόζουμε πολλά αντικείμενα GPO. Επειδή οι πολιτικές περιγράφονται με τη χρήση αντικειμένων, ισχύουν πολλά στοιχεία αντικειμενοστρέφειας. Μέσω της κληρονομικότητας, μια πολιτική που εφαρμόζεται σε ένα γονικό αποδέκτη θα κληρονομηθεί και από τους θυγατρικούς του αποδέκτες. Αυτό σημαίνει, ουσιαστικά, ότι κάθε ρύθμιση πολιτικής που εφαρμόζεται σε ένα γονικό αντικείμενο μεταβιβάζεται και στα θυγατρικά αντικείμενα. Η σειρά της κληρονομικότητας είναι η εξής:

Τοποθεσία -> Περιοχή -> Ομάδα εργασίας

Από την άλλη πλευρά, μπορούμε εάν θέλουμε να υποσκελίσουμε την κληρονομικότητα. Για να γίνει αυτό, πρέπει να ορίσουμε ρητά μια ρύθμιση πολιτικής για το θυγατρικό αποδέκτη που να έρχεται σε αντίθεση με τη ρύθμιση πολιτικής του γονέα. [8]

Πότε εφαρμόζονται οι πολιτικές ομάδων;

Οι πολιτικές ομάδων χωρίζονται σε 2 μεγάλες κατηγορίες:

- Σε αυτές που εφαρμόζονται σε υπολογιστές.
- Σε αυτές που εφαρμόζονται σε χρήστες.

4.2 Πολιτικές ονομασίας λογαριασμών

Μια από τις βασικότερες πολιτικές που ορίζουμε είναι αυτή που αφορά το «σχήμα ονομασίας» των λογαριασμών. Κάθε λογαριασμός χρήστη έχει 2 ονόματα: το εμφανιζόμενο όνομα (display name) και το όνομα σύνδεσης (logon name). Το εμφανιζόμενο όνομα (πλήρες όνομα) είναι αυτό που εμφανίζεται στους χρήστες και αυτό με το οποίο γίνονται αναφορές στο λογαριασμό χρήστη κατά τις περιόδους σύνδεσης του χρήστη στο σύστημα. Το όνομα σύνδεσης είναι το όνομα που χρησιμοποιείται για τη σύνδεση στην περιοχή .

Στους λογαριασμούς περιοχής, το εμφανιζόμενο όνομα είναι συνήθως το ονοματεπώνυμο του χρήστη, όμως μπορούμε να χρησιμοποιήσουμε για αυτό το σκοπό οποιοδήποτε αλφαριθμητικό. Τα εμφανιζόμενα ονόματα πρέπει να συμμορφώνονται με τους παρακάτω κανόνες:

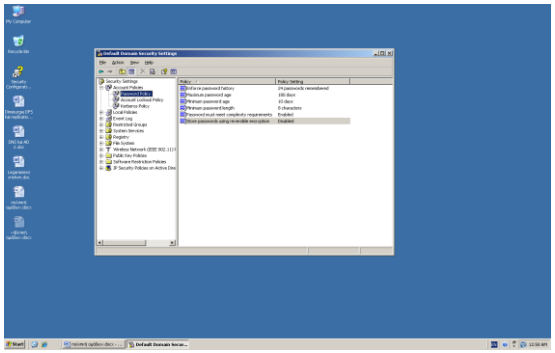
- Τα τοπικά εμφανιζόμενα ονόματα σε κάθε μεμονωμένο υπολογιστή πρέπει να είναι μοναδικά.
- Τα εμφανιζόμενα ονόματα πρέπει να είναι μοναδικά σε ολόκληρη την περιοχή.
- Τα εμφανιζόμενα ονόματα εν πρέπει να υπερβαίνουν σε μήκος ους 64 χαρακτήρες.
- Τα εμφανιζόμενα ονόματα είναι δυνατόν να περιέχουν αλφαριθμητικούς χαρακτήρες.

Τα ονόματα σύνδεσης πρέπει να συμμορφώνονται με τους επόμενους κανόνες:

- Τα ονόματα σύνδεσης πρέπει να είναι μοναδικά σε κάθε υπολογιστή και σε ολόκληρη την περιοχή.
- Τα ονόματα σύνδεσης δεν πρέπει να υπερβαίνουν σε μήκος τους 256 χαρακτήρες.
- Τα ονόματα σύνδεσης δεν επιτρέπεται να περιέχουν ορισμένους χαρακτήρες. Οι μη επιτρεπόμενοι χαρακτήρες είναι οι: “ / \ [ ] ; | = , + * ? < >
- Τα ονόματα σύνδεσης επιτρέπεται να περιέχουν όλους τους άλλους ειδικούς χαρακτήρες – κενά διαστήματα, τελείες, παύλες, και χαρακτήρες υπογράμμισης. [8]

4.3 Καθορισμός πολιτικής των password

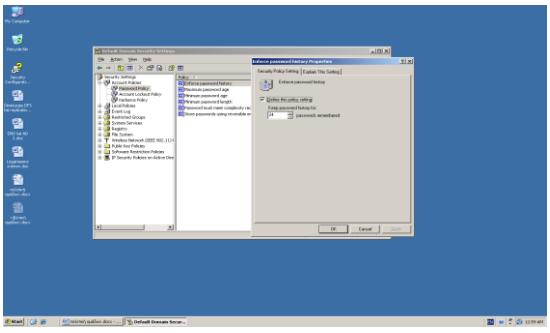
Από το μενού administrative tools επιλέγουμε domain controller security policy και από εκεί πηγαίνουμε στο account policies - > password policy και βλέπουμε την παρακάτω καρτέλα. (εικόνα 4-1) Επιλέγουμε οι ρυθμίσεις για τους κωδικούς να είναι καθολικές σε όλο το διαχειριστή περιοχής και όχι ξεχωριστά για κάθε ομάδα χρηστών, δηλαδή, για κάθε τμήμα.[8]



Εικόνα 4-1

4.3.1 Enforce password history

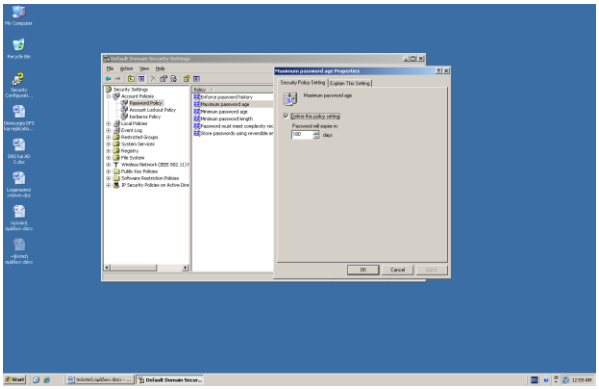
Η πολιτική Enforce password history (επιβολή ιστορικού κωδικών πρόσβασης) καθορίζει τη συχνότητα με την οποία μπορούν να επαναχρησιμοποιούνται οι παλιοί κωδικοί πρόσβασης. Μπορούμε να χρησιμοποιήσουμε αυτήν την πολιτική για να αποθαρρύνουμε τους χρήστες, ώστε να μη χρησιμοποιούν εναλλακτικά ένα μικρό αριθμό κωδικών πρόσβασης. (εικόνα 4-2). Εμείς επιλέγουμε ώστε να κρατείται ιστορικό των τελευταίων 24 κωδικών πρόσβασης του κάθε χρήστη, ώστε αυτός να αποθαρρύνεται να χρησιμοποιεί σε σύντομο χρονικό διάστημα τους παλιότερους κωδικούς.[8]



Εικόνα 4-2

4.3.2 Maximum password age

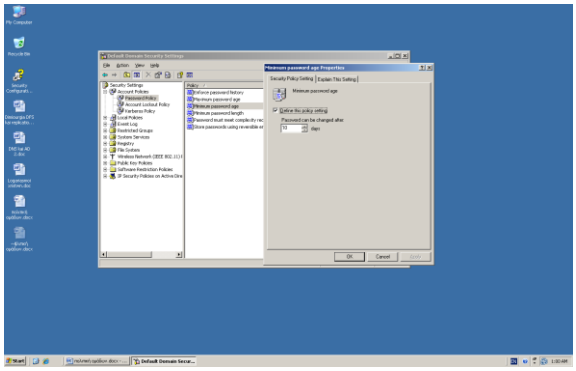
Η πολιτική Maximum password age καθορίζει τη διάρκεια του χρονικού διαστήματος κατά την οποία θα επιτρέπεται στους χρήστες να διατηρούν ένα κωδικό πρόσβασης πριν υποχρεωθούν να τον αλλάξουν. Στόχος μας είναι, οι χρήστες να αλλάζουν από καιρό σε καιρό κωδικό πρόσβασης.(εικόνα 4-3). Επειδή η ασφάλεια παίζει πολύ σημαντικό ρόλο στο δίκτυο μας, επιλέγουμε σύντομο χρονικό διάστημα αλλαγής κωδικού. Επιλέγουμε η χρονική διάρκεια χρήσης των κωδικών να είναι το εξάμηνο. [8]



Εικόνα 4-3

4.3.3 Minimum password age

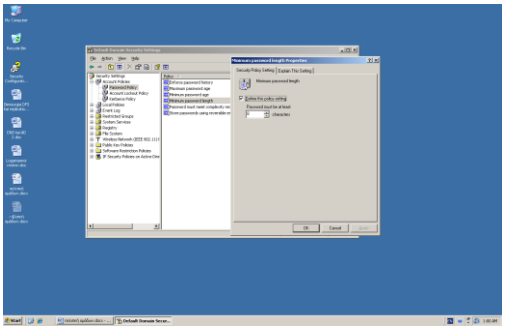
Η πολιτική Minimum password age καθορίζει τη διάρκεια του χρονικού διαστήματος που πρέπει οι χρήστες να διατηρήσουν τον ίδιο κωδικό πρόσβασης πριν τους επιτραπεί να τον αλλάξουν. (εικόνα 4-4). Χρησιμοποιούμε αυτό το πεδίο, ώστε να εμποδίσουμε τους χρήστες να παρακάμπτουν το σύστημα κωδικών πρόσβασης. Έτσι επιλέγουμε σαν ελάχιστο χρονικό όριο τις 10 μέρες και στη συνέχεια άμα θεωρηθεί αναγκαίο, με την βοήθεια του διαχειριστή δικτύου μπορεί να αλλάξει πριν συμπληρωθεί το εξάμηνο που ορίσαμε στο maximum password age. [8]



Εικόνα 4-4

4.3.4 Minimum password length

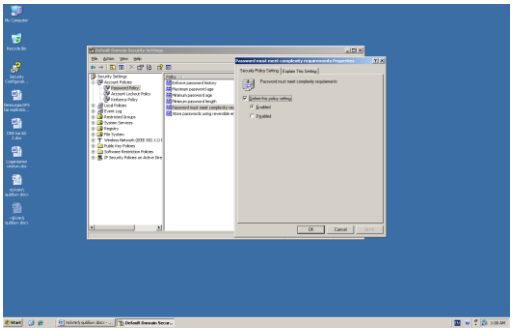
Η πολιτική Minimum password length καθορίζει το ελάχιστο πλήθος των χαρακτήρων από τους οποίους μπορεί να αποτελείται ένας κωδικός πρόσβασης. Σαν ελάχιστη απαίτηση ορίζουμε το μήκος των κωδικών να είναι 8 χαρακτήρες, ενώ όσο μεγαλύτεροι είναι οι κωδικοί, τόσο πιο δύσκολα αποκρυπτογραφούνται.(εικόνα 4-5). [8]



Εικόνα 4-5

4.3.5 Passwords must meet complexity requirements

Η πολιτική αυτή παρέχει τη δυνατότητα γι τον ορισμό πρόσθετων ελέγχων σε ότι αφορά τους κωδικούς πρόσβασης. Οι δυνατότητες αυτές ακολουθούν τις εξής προδιαγραφές:



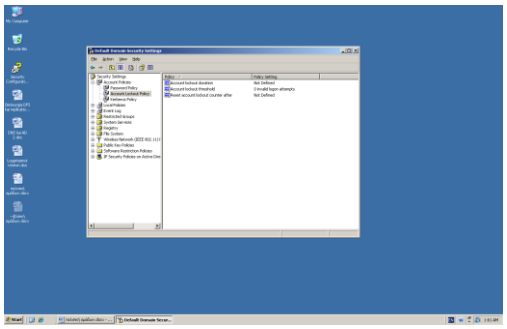
Εικόνα 4-6

- Οι κωδικοί πρόσβασης πρέπει να έχουν μήκος τουλάχιστον έξι χαρακτήρων.
- Οι κωδικοί πρόσβασης δεν επιτρέπεται να περιέχουν το όνομα του χρήστη, ούτε τμήμα του.
- Στους κωδικούς πρόσβασης πρέπει να χρησιμοποιούνται τρεις τουλάχιστον από τους τέσσερις διαθέσιμους τύπος χαρακτήρων : πεζά γράμματα, κεφαλαία γράμματα, αριθμοί, σύμβολα. (εικόνα 4-6).[8]

4.4 Διευθέτηση πολιτικών αποκλεισμού λογαριασμών

Οι πολιτικές αποκλεισμού λογαριασμών καθορίζουν πώς και πότε θα αποκλείονται οι λογαριασμοί από την περιοχή.(εικόνα 4-7). Οι πολιτικές αυτές είναι οι εξής:

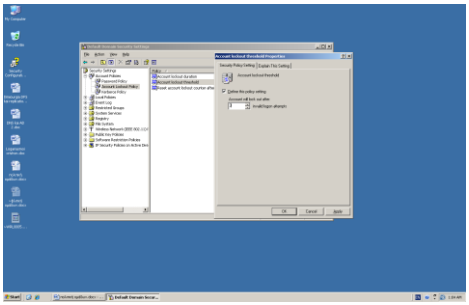
- Account Lockout Threshold
- Account Lockout Duration
- Reset Account Lockout Threshold After



Εικόνα 4-7

4.4.1 Account Lockout Threshold

Η πολιτική Account Lockout Threshold καθορίζει πόσες φορές θα επιτρέπεται να γίνει απόπειρα σύνδεσης πριν αποκλειστεί («κλειδωθεί») ο λογαριασμός. (εικόνα 4-8). Ορίζουμε σαν κατώτατο όριο αποκλεισμού τις 3 προσπάθειες, έτσι ώστε να δίνουμε τη δυνατότητα στους χρήστες, να μην καθυστερούν σε περίπτωση που ξεχάσουν για κάποιο λόγο το κωδικό τους.[8]

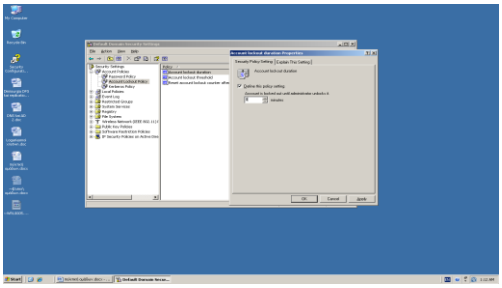


Εικόνα 4-8

4.4.2 Account Lockout Duration

Για την περίπτωση που παραβιαστεί κάποιος από τους ελέγχους αποκλεισμού των λογαριασμών, μπορούμε να χρησιμοποιήσουμε την πολιτική

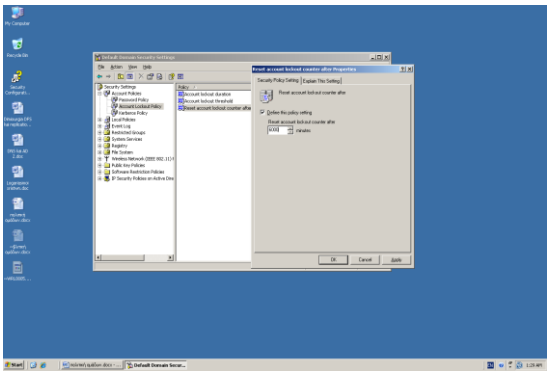
Account Lockout Duration, για να καθορίσουμε τη χρονική διάρκεια, που θα παραμείνει κλειδωμένος ο λογαριασμός. (εικόνα 4-9). Η καλύτερη πολιτική σε ό,τι αφορά την ασφάλεια είναι να κλειδώνουν οι λογαριασμοί επ' αόριστον, ώστε μόνο ο διαχειριστής να μπορεί να τους ξεκλειδώσει. Με αυτόν τον τρόπο οι επίδοξοι εισβολείς δεν θα μπορούν να δοκιμάσουν να προσπελάσουν το σύστημα ξανά και οι χρήστες, οι λογαριασμοί των οποίων κλειδώθηκαν, πρέπει υποχρεωτικά να ζητήσουν βοήθεια από κάποιο διαχειριστή. [8]



Εικόνα 4-9

4.4.3 Reset Account Lockout Threshold After

Κάθε φορά που γίνεται μια αποτυχημένη απόπειρα σύνδεσης, τα Windows Server 2003, αυξάνουν την τιμή του κατώτατου ορίου, με το οποίο παρακολουθούν το πλήθος των αποτυχημένων προσπαθειών σύνδεσης. Η πολιτική Reset Account Lockout Threshold After, καθορίζει για πόσο καιρό θα διατηρούνται οι πληροφορίες σχετικά με τις άστοχες προσπάθειες σύνδεσης, και χρησιμοποιείται για τον μηδενισμό του μετρητή των άστοχων προσπαθειών σύνδεσης μετά από την πάροδο κάποιας συγκεκριμένης χρονικής περιόδου αναμονής. (εικόνα 4-10). Ορίζουμε την τιμή των 100 ωρών ώστε, οι επίδοξοι εισβολείς να χρειαστεί να περιμένουν μεγάλο διάστημα ώστε να δοκιμάσουν πάλι να προσπελάσουν το σύστημα. [8]



Εικόνα 4-10

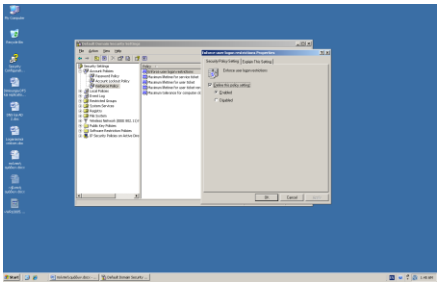
4.5 Διευθέτηση πολιτικών του πρωτοκόλλου Kerberos

Η έκδοση 5 του πρωτοκόλλου Kerberos είναι ο βασικός μηχανισμός πιστοποίηση ταυτότητας, που χρησιμοποιείται σε μια περιοχή ενεργού καταλόγου. Για την επαλήθευση της ταυτότητας χρηστών και υπηρεσιών του δικτύου, το πρωτόκολλο Kerberos χρησιμοποιεί «δελτία υπηρεσιών» (service tickets)και «δελτία χρηστών» (user tickets). Αυτά τα δελτία περιέχουν κρυπτογραφημένα δεδομένα, τα οποία επιβεβαιώνουν την ταυτότητα του συγκεκριμένου χρήστη ή υπηρεσίας. Μπορούμε να ελέγχουμε την διάρκεια, την ανανέωση και την επιβολή αυτών των δελτίων μέσω των εξής πολιτικών:

- Enforce user logon restrictions
- Maximum lifetime for service ticket
- Maximum lifetime for user ticket
- Maximum lifetime for user ticket renewal
- Maximum tolerance for computer clock synchronization

4.5.1 Enforce user logon restrictions

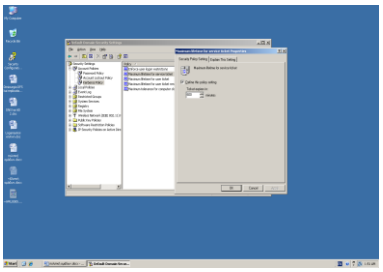
Η πολιτική Enforce user logon restrictions, εξασφαλίζει την επιβολή των τυχών περιορισμών που έχουν επιβληθεί για ένα λογαριασμό χρήστη. (εικόνα 4-11). [8]



Εικόνα 4-11

4.5.2 Maximum lifetime

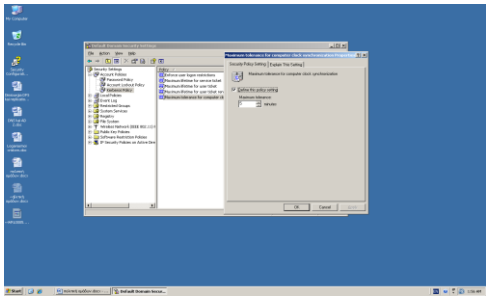
Οι πολιτικές Maximum lifetime for service ticket και Maximum lifetime for user ticket καθορίζουν τη μέγιστη χρονική διάρκεια κατά την οποία θα είναι έγκυρο ένα δελτίο υπηρεσίας ή ένα δελτίο χρήστη.(εικόνα 4-12). [8]



Εικόνα 4-12

4.5.3 Maximum tolerance for computer clock synchronization

Η πολιτική Maximum tolerance for computer clock synchronization, είναι η πολιτική που καθορίζει ότι οι υπολογιστές μιας περιοχής θα πρέπει να συγχρονίζονται μεταξύ τους με απόκλιση ορισμένων λεπτών (συνήθως 5), ώστε να γίνεται σωστά η πιστοποίηση. (4-13). [33]

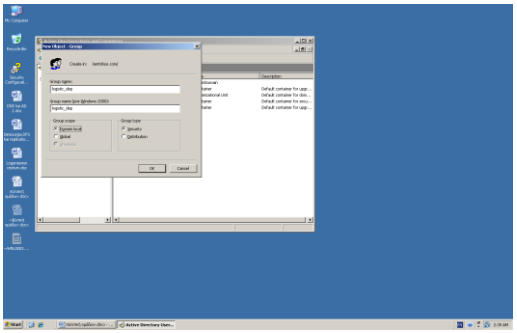


Εικόνα 4-13

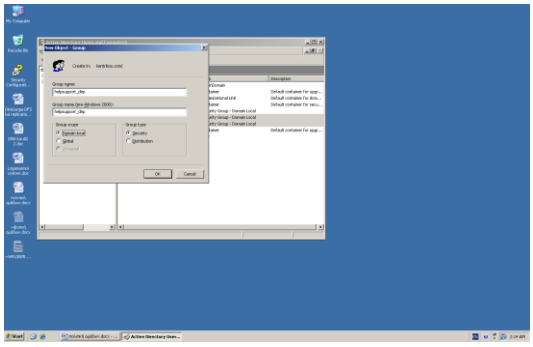
4.6 Δημιουργία ομάδων για τα τμήματα της εταιρίας

Η επιχείρηση αποτελείται από 4 τμήματα για τα οποία θα φτιάξουμε και τις αντίστοιχες ομάδες, στις οποίες θα μπορούμε να διαχειριζόμαστε τα προνόμια πολλών χρηστών, τους εργαζόμενους δλδ. σε κάθε τμήμα. Τα τμήματα αυτά είναι:

Α)Το Λογιστικό τμήμα.
Β)Το τμήμα Marketing.
Γ)Το τμήμα Research & Deployment.
Δ)Το τμήμα Τεχνικής Υποστήριξης(Help Support).

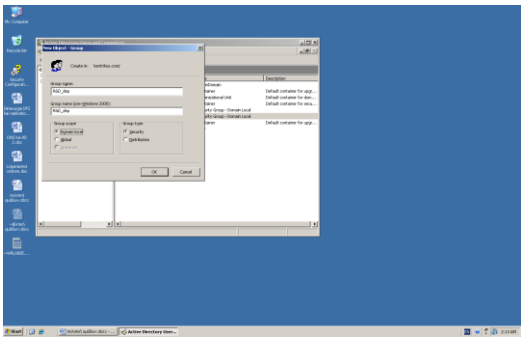


Εικόνα 4-15

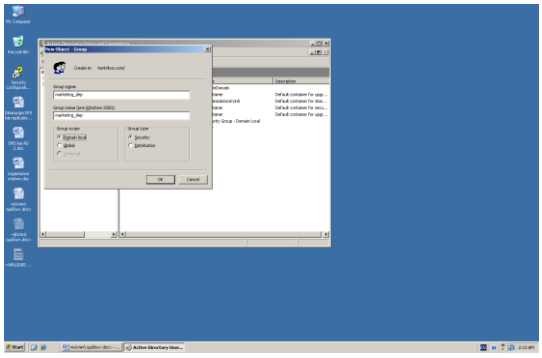


Εικόνα 4-14

Για το κάθε τμήμα δημιουργούμε και τον αντίστοιχο λογαριασμό ομάδας (group account (GA)) στη περιοχή του Active Directory(εικόνες 4-14, 4-15, 4-16, 41-7). Στη συνέχεια μέσα σε κάθε GA δημιουργούμε τους λογαριασμούς χρηστών του κάθε τμήματος.

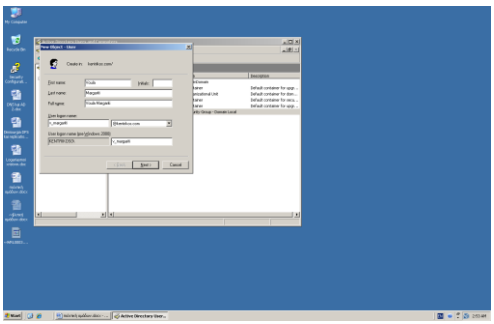


Εικόνα 4-17

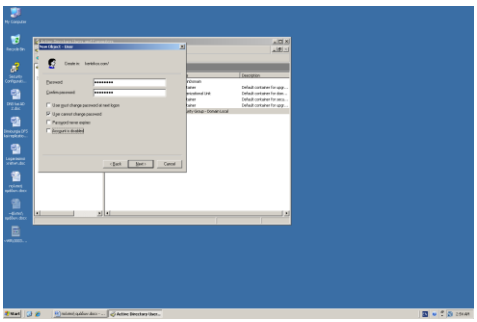


Εικόνα 4-16

Μέσα στους λογαριασμούς των τμημάτων της επιχείρησης δημιουργούμε τους λογαριασμούς των χρηστών. Τα password που καταχωρούμε ακολουθούν τις καθορισμένες πολιτικές που ορίζονται παρακάτω. Ο χρήστης δεν μπορεί να αλλάξει το συνθηματικό του από μόνος του.(εικόνες 4-18, 4-19).



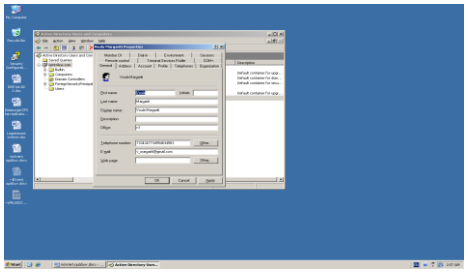
Εικόνα 4-19



Εικόνα 4-18

4.7 Διαχείριση λογαριασμού χρηστών

Δημιουργήσαμε πιο πριν ορισμένους λογαριασμούς χρηστών, τους οποίους και προσθέσαμε στις ομάδες εργασίας στις οποίες ανήκουν. Από την καρτέλα account του λογαριασμού χρήστη διαθέτουμε πολλές επιλογές για να διατηρήσουμε ασφαλές το περιβάλλον του δικτύου.(εικόνες 4-20, 4-21).



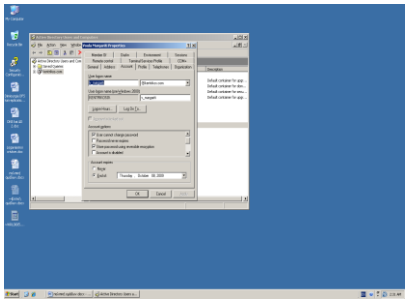
Εικόνα 4-20

1) Ο χρήστης δεν μπορεί να αλλάξει τον κωδικό πρόσβασής του

2) Ο κωδικός χρήστη έχει ημερομηνία λήξης

3) Αποθήκευση κωδικού ως απλό κρυπτογραφημένο κείμενο με τη χρήση αναστρέψιμης κρυπτογράφησης.

4) Καθορίζουμε ότι ο λογαριασμός χρήστη θα χρησιμοποιεί κρυπτογράφηση κατά DES



Εικόνα 4-21

4.8 Επίλογος

Η πολιτική λογαριασμών είναι ένα ισχυρό εργαλείο στα χέρια των διαχειριστών. Θα πρέπει όμως να το αντιμετωπίζουμε με την απαραίτητη σοβαρότητα, ώστε να μην δημιουργούνται καταστάσεις που η μια πολιτική αναιρεί την άλλη και έτσι χαλάει η ομαλή λειτουργία του δικτύου. Πρέπει λοιπόν να διαμορφώσουμε έτσι το σύστημα που να ισορροπεί ανάμεσα στην δυνατή ασφάλεια και στη εύρυθμη λειτουργία του.

Κεφάλαιο 5

ΑΝΤΙΓΡΑΦΑ ΑΣΦΑΛΕΙΑΣ

5.1 Εισαγωγή

Η λήψη αντιγράφων ασφαλείας είναι κάτι σαν ασφαλιστικό συμβόλαιο. Σημαντικά αρχεία μπορεί να διαγραφούν κατά λάθος οποιαδήποτε στιγμή. Δεδομένα κρίσιμα για τη δουλειά μας μπορεί να χαθούν. Επίσης κάποια φυσική καταστροφή μπορεί να προξενήσει υλικές ζημιές στην επιχείρηση. Εδώ χρειάζεται ένας αυστηρός προγραμματισμός για τη λήψη αντιγράφων ασφαλείας και την επαναφορά των δεδομένων, ώστε να αντιμετωπίζουμε όλες τις παραπάνω καταστάσεις. Χωρίς ένα τέτοιο σχέδιο θα μείνουμε απλώς με άδεια χέρια, έχοντας χάσει για πάντα τα κρίσιμα δεδομένα της επιχείρησης μας. [8]

5.2 Σχέδιο λήψης αντιγράφων ασφαλείας

Η κατάστρωση και υλοποίηση ενός σχεδίου για τη λήψη αντιγράφων ασφαλείας απαιτεί κάποιο χρόνο. Για να διευκολυνθούμε στην ανάπτυξή του πρέπει να εξετάσουμε τα παρακάτω:

- Πόσο σημαντικά είναι τα δεδομένα των συστημάτων μας;
- Τι είδους πληροφορίες περιλαμβάνουν τα δεδομένα;
- Πόσο συχνά αλλάζουν τα δεδομένα;
- Μπορούμε να ενισχύσουμε τη λήψη αντιγράφων ασφαλείας με σκιώδη αντίγραφα;
- Διαθέτουμε τον εξοπλισμό για τη λήψη αντιγράφων ασφαλείας;
- Ποιος θα είναι υπεύθυνος για την υλοποίηση του σχεδίου;
- Ποια είναι η καλύτερη στιγμή για τη λήψη αντιγράφων ασφαλείας;

- Είναι απαραίτητη η φύλαξη αντιγράφων ασφαλείας σε άλλο

5.2.1 Βασικοί τύποι αντιγράφων ασφαλείας

Υπάρχουν πολλές τεχνικές γα τη λήψη αντιγράφων ασφαλείας των αρχείων μας. Οι τεχνικές που θα χρησιμοποιήσουμε, εξαρτώνται από το είδος των δεδομένων που αντιγράφουμε, το πόσο εύκολη θέλουμε να είναι η διαδικασία επαναφοράς τους κα. Από τις ιδιότητες ενός αρχείου ή κάποιου φακέλου βρίσκουμε την ιδιότητα Αρχειοθέτηση (archive). Η ιδιότητα αυτή χρησιμοποιείται συχνά για να προσδιοριστεί αν είναι απαραίτητη η δημιουργία αντιγράφου ασφαλείας για ένα αρχείο ή φάκελο. Αν η ιδιότητα είναι ενεργοποιημένη, το αρχείο ή ο φάκελος πρέπει να συμπεριληφθούν στο αντίγραφο ασφαλείας. Οι βασικοί τύποι των αντιγράφων ασφαλείας που μπορούμε να δημιουργήσουμε είναι:

- **Κανονικά/πλήρη αντίγραφα ασφαλείας (normal/full backups)**. Όλα τα επιλεγμένα αρχεία συμπεριλαμβάνονται στο αντίγραφο ασφαλείας, ανεξάρτητα από τη ρύθμιση της ιδιότητας αρχειοθέτησης τους. Όταν δημιουργείται το αντίγραφο ασφαλείας ενός αρχείου, η ιδιότητα αρχειοθέτησης του αρχείου «μηδενίζεται» (απενεργοποιείται). Αν το αρχείο τροποποιηθεί αργότερα, η ιδιότητα αρχειοθέτησης ενεργοποιείται για να δείξει ότι το συγκεκριμένο αρχείο πρέπει να συμπεριληφθεί σε επόμενο αντίγραφο ασφαλείας.
- **Αντίγραφα ασφαλείας απλής αντιγραφής (copy backups)**. Η διαφορά με την προηγούμενη κατηγορία είναι ότι εδώ η ιδιότητα αρχειοθέτησης των αρχείων δεν τροποποιείται. Αυτός ο τρόπος μας επιτρέπει να δημιουργήσουμε και άλλα αντίγραφα ασφαλείας των συγκεκριμένων αρχείων σε επόμενη χρονική στιγμή.
- **Διαφορικά αντίγραφα ασφαλείας (differential backups)**. Επιτρέπουν τη λήψη αντιγράφων ασφαλείας των αρχείων, που έχουν τροποποιηθεί από την τελευταία φορά που τα συμπεριλάβαμε σε ένα κανονικό αντίγραφο ασφαλείας. Η ιδιότητα αρχειοθέτησης δείχνει ποια αρχεία έχουν τροποποιηθεί και μόνο αυτά τα αρχεία συμπεριλαμβάνονται στο αντίγραφο

ασφαλείας. Στην περίπτωση αυτή όμως, η ιδιότητα αρχειοθέτησης δεν τροποποιείται.

- **Αυξητικά αντίγραφα ασφαλείας (incremental backups)**. Αυτή η μέθοδος έχει σχεδιαστεί για τη λήψη αντιγράφων ασφαλείας των αρχείων που έχουν τροποποιηθεί από την τελευταία φορά που πήραμε κάποιο κανονικό ή αυξητικό εφεδρικό αντίγραφό τους. Η ιδιότητα αρχειοθέτησης δείχνει ποια αρχεία έχουν τροποποιηθεί και μόνο αυτά συμπεριλαμβάνονται στο αντίγραφο ασφαλείας. Όταν δημιουργείται το αντίγραφο ασφαλείας ενός αρχείου, η ιδιότητα αρχειοθέτησης του αρχείου μηδενίζεται. Αν το αρχείο τροποποιηθεί αργότερα, η ιδιότητα αρχειοθέτησης ενεργοποιείται για να δείξει ότι το συγκεκριμένο αρχείο πρέπει να συμπεριληφθεί σε επόμενο αντίγραφο ασφαλείας.
- **Ημερήσια αντίγραφα ασφαλείας (daily backups)**. Τα αντίγραφα ασφαλείας δημιουργούνται με βάση την ίδια την ημερομηνία τροποποίησης των αρχείων. Αν το αρχείο τροποποιήθηκε την ίδια ημέρα που δημιουργείται και το αντίγραφο του, τότε το αρχείο αυτό θα συμπεριληφθεί στο αντίγραφο ασφαλείας. Η τεχνική αυτή δεν τροποποιεί την ιδιότητα αρχειοθέτησης των αρχείων. [8]

5.2.2. Επιλογή μέσων αποθήκευσης

Για τη λήψη αντιγράφων ασφαλείας υπάρχουν διαθέσιμα πολλά εργαλεία. Άλλα είναι γρήγορα και ακριβά, άλλα αργά και αξιόπιστα. Η λύση που θα υιοθετήσουμε για την εταιρία εξαρτάται από διάφορους παράγοντες, όπως: [8]

- Χωρητικότητα.
- Αξιοπιστία.
- Επεκτασιμότητα.
- Ταχύτητα.
- Κόστος.

5.2.3 Συνηθισμένες λύσεις

- Μονάδες μαγνητοταινιών. Χαμηλού κόστους αλλά μικρής αξιοπιστίας.
- Μονάδες ψηφιακών μαγνητοταινιών ήχου (DAT).
- Συστήματα αυτόματης φόρτωσης μαγνητοταινιών.
- Οπτικά jukebox.
- Αφαιρούμενοι δίσκοι.
- Σκληροί δίσκοι. Οι σκληροί δίσκοι παρέχουν την ταχύτερη μέθοδο λήψης κι ανάκτησης αντιγράφων ασφαλείας. Μια διαδικασία λήψης αντιγράφων ασφαλείας που χρειάζεται ώρες για να ολοκληρωθεί με μια μονάδα μαγνητοταινίας, για τους σκληρούς δίσκους είναι θέμα μερικών λεπτών. Παλιότερα το κόστος των σκληρών δίσκων ήταν ένας αποτρεπτικός παράγοντας για τη μαζική χρήση τους στη λήψη αντιγράφων ασφαλείας. Πλέον με την κατακόρυφη πτώση των τιμών τους μπορούμε να εξασφαλίσουμε πολλά TerraByte με λίγα ευρώ.
- NAS (Network Attached Storage). Η πτώση των τιμών και η ραγδαία αύξηση της χωρητικότητας των σκληρών δίσκων, οδήγησε στη δημιουργία, πιο ευέλικτων μορφών αποθήκευσης και το σημαντικότερο, πιο αυτόνομων από τον «κλασικό» τρόπο αποθήκευσης μέσα στον Server. Το NAS είναι ένας όρος που χρησιμοποιείται για να περιγράψει ένα πλήρες σύστημα αποθήκευσης το οποίο έχει σχεδιαστεί για να συνδέεται με ένα παραδοσιακό δίκτυο δεδομένων.[8]

5.3 Σχέδιο backup για την εταιρία

Με βάση και όλες τις παραπάνω παραμέτρους καθορίζουμε και το σχέδιο για τα αντίγραφα ασφαλείας που θα κρατάει η εταιρία.

Καταρχήν, οι 2 servers θα είναι συνδεδεμένοι με έναν NAS, πχ. τον LaCie 5TB 5-Bay με τιμή 985

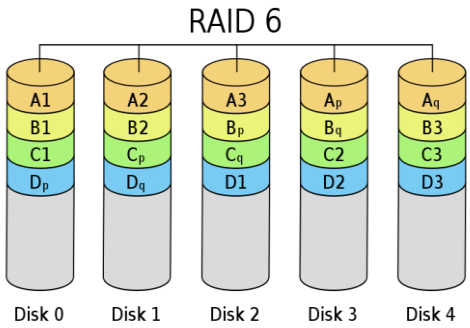
Εικόνα 5-1

Ευρώ. http://www.expansys.com.gr/d.aspx?i=175839. (εικόνα 5-1)

Ο NAS δέχεται μέχρι 5 σκληρούς δίσκους, ο οποίοι έχουν μέγιστη χωρητικότητα 5 TB, σε 5 δίσκους του 1 TB ο καθένας. Διαθέτει, επίσης, διασύνδεση External SATA, η οποία θεωρητικά φτάνει τα 300 MB/s στη μεταφορά δεδομένων, σημαντικά μεγαλύτερη από άλλους τρόπους διασύνδεσης (USB 2.0, Firewire 1394b), κάτι που εξυπηρετεί και τις ανάγκες της εταιρίας για συχνή λήψη αντιγράφων ασφαλείας.

Στον NAS πραγματοποιείται η αποθήκευση των αρχείων που χρησιμοποιούν και δημιουργούν οι χρήστες και είναι αρχεία του office των windows, και αρχεία επιπλέον διάφορων εφαρμογών. Υπάρχει για κάθε τμήμα ξεχωριστός φάκελος, με την αντίστοιχη ονομασία, στους οποίους οι εργαζόμενοι αυτών των τμημάτων, αποθηκεύουν τα δεδομένα.

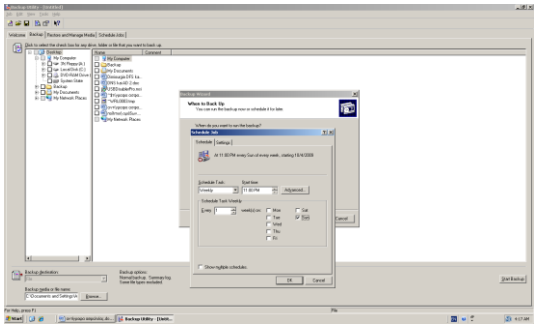
Για την καλύτερη δυνατή ασφάλεια και ακεραιότητα των δεδομένων οι σκληροί δίσκοι είναι σε συστοιχία RAID-6, υλοποίηση την οποία υποστηρίζει το συγκεκριμένο μοντέλο NAS. Η επιλογή αυτή γίνεται κυρίως γιατί το RAID 6 έχει μεγαλύτερη ανοχή σε σφάλματα (fault tolerance) από ότι το RAID 5, λόγω της χρήσης ενός επιπλέον parity block. Το RAID 6 ελαχιστοποιεί τον κίνδυνο για απώλεια δεδομένων σε περίπτωση που και 2^{ος} σκληρός δίσκος καταστραφεί ή ένα ανεπανόρθωτο σφάλμα συμβεί κατά την εγγραφή. (εικόνα 5-2)



Εικόνα 5-2

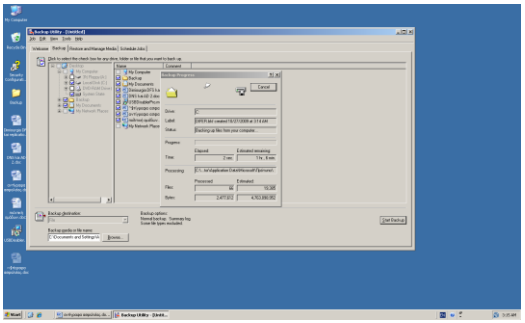
5.3.1 Αντίγραφα ασφαλείας στους servers

Για τον πιο αποτελεσματικό τρόπο διαχείρισης και αξιοποίησης των αντιγράφων ασφαλείας, φροντίζουμε ώστε τα αντίγραφα ασφαλείας των δεδομένων που χρησιμοποιούν οι χρήστες να αποθηκεύονται σε ξεχωριστό μέρος και με διαφορετική συχνότητα από ότι τα αρχεία του συστήματος. Η λογική που ακολουθούμε είναι η προστασία από τα το μεγαλύτερο κακό που μπορεί πιθανά να συμβεί στην εταιρία και τα δεδομένα που κρατάει, δηλαδή μια πλήρη καταστροφή. Επομένως πρέπει να είμαστε έτοιμοι να αντιμετωπίσουμε ανά πάσα στιγμή την περίπτωση επαναφοράς ολόκληρου του συστήματος.



Εικόνα 5-3

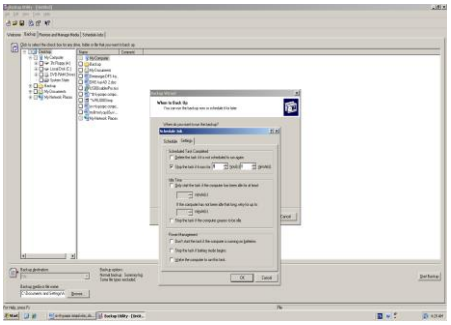
- Για τα δεδομένα θα πραγματοποιούμε καθημερινά αυξητικά (incremental) αντίγραφα ασφαλείας(εικόνα 5-3). Με αυτό τον τρόπο γλιτώνουμε αρκετό αποθηκευτικό χώρο από το να κάναμε καθημερινά διαφορικά (differential) αντίγραφα. (εικόνα 5-4)
- Κάθε Κυριακή του μήνα θα πραγματοποιούμε ένα πλήρες (full) αντίγραφο ασφαλείας.
- Τα αντίγραφα ασφαλείας θα αποθηκεύονται στο βοηθητικό PC που θα έχει λειτουργικό FreeBSD.
- Στο Backup PC τα αρχεία αποθηκεύονται χρησιμοποιώντας κρυπτογράφηση AES 128bit. Επίσης 1 φορά το μήνα θα κρατάμε τα αντίγραφα ασφαλείας του Backup PC, σε εξωτερικούς σκληρούς δίσκους, τους οποίους θα τους αποθηκεύουμε σε διαφορετικό κτίριο μακριά από αυτό της εταιρίας μας. Ο λόγος είναι, ότι σε ενδεχόμενη φυσική



Εικόνα 5-4

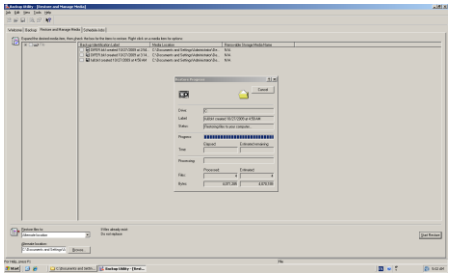
καταστροφή πχ. από καταιγίδες, σεισμούς πυρκαγιές κλπ να μην καταστραφούν και τα 2 κτίρια. Με απλά λόγια, θα ήταν ένα άχρηστο έξοδο να κρατάμε αντίγραφα ασφαλείας λίγα μέτρα ή χιλιόμετρα μακριά από το κτίριο της εταιρίας μας. Η προτεινόμενη απόσταση είναι τα 50 – 100 χιλιόμετρα.

- Η λήψη αντιγράφων ασφαλείας θα γίνεται σε ώρες που οι εργαζόμενοι της εταιρίας έχουν σχολάσει από τη δουλειά τους, δηλαδή από τις 23:00 και μετά. Το ότι το ολικό backup, θα πραγματοποιείται κάθε Κυριακή, μας δίνει την ευχέρεια να έχουμε τον απαραίτητο χρόνο για να το πραγματοποιήσουμε πριν ξεκινήσει η νέα εργάσιμη εβδομάδα. Ενδεικτικά (εικόνα 5-5) ένα full/normal backup με βάση το αρχικό μέγεθος των 8GB κρατάει χρόνο κοντά στα είκοσι (20') λεπτά και ένα incremental backup στα δεδομένα μόνο με μέγεθος των 500 MB διαρκεί λίγα δευτερόλεπτα. Η εταιρία πρέπει να ολοκληρώνει τη λήψη αντιγράφων ασφαλείας πριν αναλάβουν οι εργαζόμενοι το πρωί. Το χρονικό όριο από τις 23:00 μέχρι τις 7:00 (8 ώρες) το πρωί είναι αρκετά μεγάλο για να περιλάβει ένα μεγάλο όγκο αρχείων δεδομένων με την αυξητική μέθοδο.(εικόνα 3) Επίσης επαρκής χρόνος υπάρχει και για το full backup , που θέλουμε να εκτελείται κάθε Κυριακή. Σε περίπτωση που ο όγκος των δεδομένων αυξηθεί πολύ μετά και την πάροδο μεγάλου χρονικού διαστήματος, μπορούμε το full backup να το πραγματοποιούμε και από το Σάββατο. Αυτό όμως προϋποθέτει τα δεδομένα να φτάσουν σε μέγεθος πολλών GB. Επιλέγουμε, ακόμα, κατά τη λήψη των αντιγράφων ασφαλείας να γίνεται επαλήθευση (verification) των δεδομένων ότι αντιγράφηκαν σωστά. Σε εξαιρετικές περιπτώσεις είναι θέμα της εταιρίας να κάνει εκκαθαρίσεις στα δεδομένα που δεν χρειάζεται, ώστε να γλιτώνει επιπλέον επιβάρυνση κόστους και χρόνου κατά τη λήψη αντιγράφων ασφαλείας.



Εικόνα 5-5

- Όλα τα δεδομένα που θα έχουν αντιγραφεί θα κρατούνται για κάθε ενδεχόμενο για ένα χρόνο και στη συνέχεια, με την σύμφωνη γνώμη της εταιρίας θα επιλέγεται ποια από αυτά θα σβήνονται. Μπορούμε όσα δεδομένα επιλεχτούν να σβηστούν να εγγράφονται πρώτα σε DVD και να κρατούνται σε ξεχωριστό μέρος έξω από το κτίριο της εταιρίας.
- Για τα δεδομένα του συστήματος το σχέδιο λήψης αντιγράφων είναι το ίδιο. Απλά επιλέγουμε μόνο τα αρχεία του συστήματος να αντιγράφονται.
- Μπορούμε να κρατάμε και ένα εικονικό αρχείο (image)του συστήματος μας, για το ενδεχόμενο που θέλουμε να το επαναφέρουμε στην κατάσταση που ήταν πριν καταρρεύσει. Με αυτόν τον τρόπο μπορούμε να κρατάμε πολλά διαφορετικά εικονικά αρχεία του συστήματος μας πχ. Ένα όταν εγκαταστήσουμε το λειτουργικό και ρυθμίσουμεντον server και στη συνέχεια όσο γίνεται πιο συχνά, με κριτήριο αν το σύστημα μας είναι σε επιθυμητή κατάσταση τη δεδομένη στιγμή. Μπορούμε επιπλέον το κάθε εικονικό
- Μπορούμε το αρχείο να το αποθηκεύουμε σε DVD, ώστε να μην καταλαμβάνει πολύ χώρο.
- Ένα σωστό και ολοκληρωμένο σύστημα αντιγράφων ασφαλείας, πρέπει απαραίτητα να συνοδεύεται και από ένα σύστημα επαναφοράς δεδομένων, αλλιώς όλη η προηγούμενη δουλειά πάει χαμένη. Επίσης η συχνή δοκιμαστική επαναφορά ορισμένων αρχείων, μας επιβεβαιώνει ότι η διαδικασία, που ακολουθήσαμε είναι σωστή. Επομένως πρέπει να προβλέψουμε, μία φορά το μήνα να δοκιμάζουμε σε εφεδρικούς υπολογιστές την επαναφορά των δεδομένων και τους συστήματος.(εικόνα 5-6).



Εικόνα 5-6

Ημέρα	Είδος Back up	Σχόλια
Δευτέρα	**Αυξητικά αντίγραφα ασφαλείας**	**Τα αυξητικά αντίγραφα ασφαλείας περιλαμβάνουν τις αλλαγές από την Κυριακή**
Τρίτη	**Αυξητικά αντίγραφα ασφαλείας**	**Τα αυξητικά αντίγραφα ασφαλείας περιλαμβάνουν τις αλλαγές από την Δευτέρα**
Τετάρτη	**Αυξητικά αντίγραφα ασφαλείας**	**Τα αυξητικά αντίγραφα ασφαλείας περιλαμβάνουν τις αλλαγές από την Τρίτη**
Πέμπτη	**Αυξητικά αντίγραφα ασφαλείας**	**Τα αυξητικά αντίγραφα ασφαλείας περιλαμβάνουν τις αλλαγές από την Τετάρτη**
Παρασκευή	**Αυξητικά αντίγραφα ασφαλείας**	**Τα αυξητικά αντίγραφα ασφαλείας περιλαμβάνουν τις αλλαγές από την Πέμπτη**
Σάββατο	**Αυξητικά αντίγραφα ασφαλείας**	**Τα αυξητικά αντίγραφα ασφαλείας περιλαμβάνουν τις αλλαγές από την Παρασκευή**
Κυριακή	**Πλήρη/Κανονικά αντίγραφα ασφαλείας**	**Δημιουργία πλήρους σειράς αντιγράφων ασφαλείας**
Κάθε 1η Κυριακή του μήνα	**Επαναφορά δεδομένων**	**Δοκιμαστική επαναφορά των δεδομένων καθώς και των εικονικών αρχείων του συστήματος.**

5.4 Επίλογος

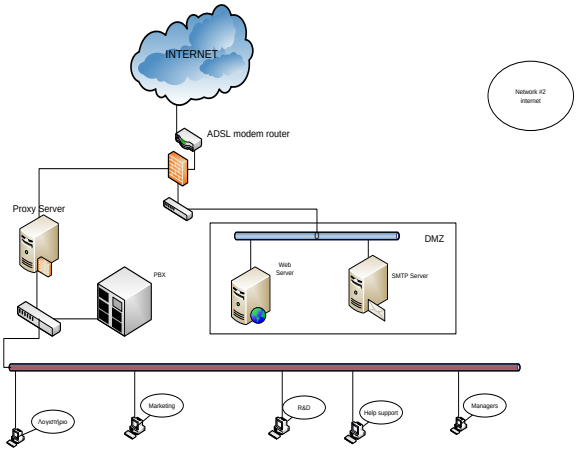
Η λήψη των αντιγράφων ασφαλείας είναι η εργασία η οποία μας εξασφαλίζει την ικανότητα να ανακάμψουμε άμεσα και γρήγορα από μια πιθανή καταστροφή. Θα πρέπει να την έχουμε σε πρώτη προτεραιότητα και να μην την αφήνουμε σε δεύτερη μοίρα για λόγους φόρτου εργασίας. Θα πρέπει με ευθύνη της εταιρίας και της ομάδας ασφαλείας να τηρείται πιστά το πρόγραμμα που έχει καταρτιστεί.

Κεφάλαιο 6

ΤΟ ΔΙΑΔΙΚΤΥΟ

6.1 Εισαγωγή

Το μικρό δίκτυο που θα στήσουμε για την πρόσβαση στο διαδίκτυο από τελείται από έναν υπολογιστή για τα τμήματα Logistic, Marketing, R&D και από το τμήμα Help & Support θα έχουμε τρεις για τις ανάγκες επικοινωνίας με τους πελάτες. Υπολογιστές με σύνδεση στο διαδίκτυο θα έχουν και όλοι οι διευθυντές τμημάτων και τα ανώτερα στελέχη της εταιρίας. Οπότε υπολογίζουμε ότι η εταιρία θα έχει περίπου 15 υπολογιστές συνδεδεμένους με το διαδίκτυο. (εικόνα 6-1)



Εικόνα 6-1

Οι υπολογιστές θα συνδέονται στο internet με έναν proxy server, ο οποίος είναι συνδεδεμένος με το ADSL modem router. Πάνω στο Switch, που συνδέει τους υπολογιστές με τον server τοποθετούμε τον PBX server που θα τρέχει το λειτουργικό TrixBox και με τον οποίο θα συνδέσουμε τα τμήματα με Voip τηλέφωνα για κάθε εργαζόμενο. Επίσης θα έχουμε 2 ακόμα servers έναν SMTP server για τη διαχείριση των email και ένα Web server για το ανέβασμα της ιστοσελίδας της εταιρίας.

6.2 Web Server

Ο Web Server της εταιρίας είναι και αυτός ένα από τα σημαντικά κομμάτια της. Σε αυτό θα στηριχτεί κατά ένα μεγάλο μέρος η προβολή της στο κοινό, μέσα

από την ιστοσελίδα που θα φορτώσουμε. Επομένως θέλουμε να στήσουμε ένα μηχάνημα αξιόπιστο και ασφαλές για να εξυπηρετεί εμάς και τους πελάτες.

Για τον server επιλέγουμε να χρησιμοποιήσουμε λειτουργικό Linux Ubuntu 7.10 και εγκαθιστούμε τα πακέτα: apache 2, mysql-client, mysql-server, php5, php-mysql, phpmyadmin. Χρειάζεται, ταυτόχρονα να ρυθμίσουμε έτσι τον Server ώστε να έχουμε την καλύτερη δυνατή ασφάλεια και να είμαστε προστατευμένοι τόσο από το εξωτερικό του δικτύου, όσο και από τους εσωτερικούς χρήστες. [11]

6.2.1 Διαμόρφωση

Ένα από τα πρώτα πράγματα που πρέπει να κάνουμε είναι να διασφαλίσουμε είναι το ότι ο Apache δεν θα τρέχει έχοντας αρχικό κατάλογο το root, επειδή σε περίπτωση που χακαριστεί από έναν εισβολέα, τότε ο τελευταίος θα μπορούσε να ελέγξει όλο το λογαριασμό από την ρίζα. Για αυτό δημιουργούμε τον φάκελο www-data ώστε ο apache να τρέχει από εκεί. Με την εντολή:

vi /etc/apache2/apache2.conf επεξεργαζόμαστε το αρχείο apache2.conf και κάνουμε την αλλαγή από

```
User root                          User  www-data
Group root              σε         Group  www-data
```

Στη συνέχεια καθορίζουμε τα δικαιώματα διαχείρισης του server. Ο Apache πρέπει να έχει το δικαίωμα να εκτελεί το αρχείο index.cgi. Από την άλλη, όμως, δεν θέλουμε ο καθένας να διαβάζει και να γράφει στο συγκεκριμένο αρχείο, σε αντίθεση με τον ιδιοκτήτη του αρχείου, στη συγκεκριμένη περίπτωση τον διαχειριστή. Με την εντολή chmod 755 index.cgi παραχωρούμε αυτά τα δικαιώματα. Επιπλέον, τα αρχεία έξω από το λογαριασμό της ρίζαςδεν θα πρέπει να είναι διαθέσιμα, για αυτό είναι σημαντικό να προσθέσουμε, αν δεν υπάρχουν οι παρακάτω γραμμές στο αρχείο apache.conf [12]

```
Options  FollowSymLinks
AllowOverride   None
```

Ο σκοπός των συγκεκριμένων γραμμών είναι να εμποδίσει τον Apache να έχει πρόσβαση σε αρχεία έξω από την web ρίζα.

Δεν θέλουμε οι χρήστες να τρέχουν σενάρια cgi οπουδήποτε στο σύστημα αρχείων, παρά μόνο στην web root. Πραγματοποιούμε λοιπόν τις παρακάτω αλλαγές: στο αρχείο apache2.conf προσθέτουμε τις γραμμές

```
AllowOverride None
Options ExecCGI
Order allow, deny
Allow from 192.168.1.0/24
```

Και με αυτόν τον τρόπο μόνο οι χρήστες του τοπικού δικτύου μας μπορούν να τρέχουν σενάρια .cgi στο "/home/username/public_html/cgi-bin"

Επιπλέον πρέπει να πάρουμε μέτρα για την πιστοποίηση των χρηστών που θα έχουν πρόσβαση στην web root. Όπως είναι λογικό δεν πρέπει να επιτρέψουμε στον καθένα να έχει άμεση πρόσβαση, εκτός από τα εξουσιοδοτημένα άτομα. Βασικές ρυθμίσεις που μπορούμε να κάνουμε είναι:
Η ενεργοποίηση του .htaccess. από το αρχείο apache.conf καιμε τη χρήση του κειμενογράφου vi αλλάζουμε την γραμμή

```
AllowOverride None        σε        AllowOverride AuthConfig
```

Και στη συνέχεια δημιουργούμε ένα αρχείο με το κωδικό πρόσβασης που θα δώσουμε. Μια μέθοδος για πιστοποίηση που μπορούμε να χρησιμοποιήσουμε ονομάζεται digest authentication και χρησιμοποιεί κωδικοποίηση κατά MD5 hash για τα password. Με αυτή τη μέθοδο εξασφαλίζουμε ότι οι κωδικοί πρόσβασης δεν κινούνται στο δίκτυο καθαροί, σε δημόσια θέα και επιπλέον δεν μπορούν να κλαπούν με την μέθοδο sniffing. [12]

Create a password file:

```
# mkdir /var/www/misc
# chmod a+rx /var/www/misc
# cd /var/www/misc
# htdigest -c private.passwords realm username
```

```
Adding password for username in realm realm.
New password:
```

Create .htaccess

```
# cd /home/username/public_html/cgi-bin
# vi .htaccess
```

Add the below in .htaccess

```
AuthName "My Private Area"
AuthType Digest
AuthUserFile /var/www/misc/private.passwords
AuthGroupFile /dev/null require valid-user
```

6.2.2 Απόκρυψη αριθμού έκδοσης - ευαίσθητων πληροφοριών

Από προεπιλογή πολλές εκδόσεις του apache αποκαλύπτουν την έκδοση του server που τρέχουν, την έκδοση του λειτουργικού συστήματος πάνω στο οποίο τρέχει, ακόμα και ποια εργαλεία είναι εγκατεστημένα σε αυτόν. Αυτές οι πληροφορίες μπορεί να αποδειχτούν πολύ χρήσιμες για κάποιον που θέλει να επιτεθεί στο σύστημα. Χρειάζεται λοιπόν δύο οδηγίες που πρέπει να προστεθούν στο αρχείο httpd.conf: [13]

```
ServerSignature Off
ServerTokens Prod
```

Το ServerSignature εμφανίζεται στο κάτω μέρος των σελίδων που δημιουργούνται από τον apache , όπως είναι οι404 σελίδες κλπ. Το ServerTokens χρησιμοποιείται για να προσδιορίσει τι θα βάλει ο server σαν http response header. Με τη δήλωση Prod την ρυθμίζει ως εξής: Server: Apache.

6.2.3 Χρήση του προγράμματος Mod_security

Το mod_security είναι ένα εύχρηστο πρότυπο του apache που το δημιούργησαν οι κατασκευαστές του. Με αυτό μπορούμε να κάνουμε τα ακόλουθα: [13]

- Απλό φιλτράρισμα
- Regular Expression based filtering
- URL Encoding Validation
- Unicode Encoding Validation
- Παρακολούθηση
- Null byte attack prevention
- Upload memory limits
- Server identity masking
- Built in Chroot support

6.2.4 Απενεργοποίηση άχρηστων προτύπων

Ο Apache τυπικά εγκαθίσταται με πολλά πρότυπα, για τα οποία μπορούμε να μάθουμε από το module documentation τι κάνει ο καθένα. Από εκεί καταλαβαίνουμε ότι πολλά από αυτά δεν θα έπρεπε να είναι ενεργοποιημένα. Με την εντολή grep LoadModule httpd.conf μπορούμε να δούμε στο αρχείο httpd.conf ποιες γραμμές περιέχουν τη λέξη LoadModule. Για να τα απενεργοποιήσουμε προσθέτουμε απλώς στην αρχή της κάθε γραμμής το σύμβολο #. Μερικά από τα πρότυπα που δεν χρειαζόμαστε είναι τα : mod_imap, mod_include, mod_info, mod_userdir, mod_status, mod_cgi, mod_autoindex. [13]

6.2.5 Περιορίζουμε τα μεγάλα αιτήματα

Ο Apache έχει πολλές οδηγίες, που μας επιτρέπουν να θέσουμε ένα όριο στο μέγεθος των αιτημάτων που μπορεί να εξυπηρετήσει. Αυτό μπορεί να φανεί πολύ χρήσιμο στην ελαχιστοποίηση των συνεπειών μιας επίθεσης denial of service. Μια αρχή μπορεί να γίνει από την οδηγία LimitRequestBody. Αυτή η εντολή είναι

προκαθορισμένη στο να μην έχει όριο. Ανάλογα με το πόσο φόρτο για upload εξυπηρετούμε μπορούμε να καθορίσουμε μια τιμή όπως αυτή:

LimitRequestBody 2029429

Άλλες εντολές που μπορούμε να καθορίσουμε είναι οι LimitRequestFields LimitRequestFieldSize LimitRequestLine. [13]

6.3 SMTP Server

Για τον SMTP Server θα τον στήσουμε σε μηχάνημα Linux Ubuntu και θα εγκαταστήσουμε το πρόγραμμα SendMail 8.13. Δουλειά του είναι να δέχεται το email από τους Αντιπροσώπους Email Χρήστη (Mail User Agents, MUA) και να το παραδίδει στο κατάλληλο mailer που ορίζεται στο αρχείο ρυθμίσεων του. Το sendmail μπορεί επίσης να δεχθεί συνδέσεις δικτύου και να παραδώσει το mail σε τοπικές θυρίδες ή και σε κάποιο άλλο πρόγραμμα. [14]

Το sendmail χρησιμοποιεί τα ακόλουθα αρχεία ρυθμίσεων:

Όνομα Αρχείου	Λειτουργία
/etc/mail/access	Η βάση δεδομένων πρόσβασης του sendmail.
/etc/mail/aliases	Παρωνύμια (aliases) για τις θυρίδες (Mailboxes)
/etc/mail/local-host-names	Λίστα των υπολογιστών για τους οποίους το sendmail δέχεται mail
/etc/mail/mailer.conf	Ρυθμίσεις του προγράμματος mailer
/etc/mail/mailertable	Πίνακας παραδόσεων του mailer
/etc/mail/sendmail.cf	Το κεντρικό αρχείο ρυθμίσεων του sendmail

/etc/mail/virtusertable	Πίνακας εικονικών χρηστών και περιοχών (domains)

6.3.1 Αναβάθμιση για κλείσιμο τρυπών

Χρειάζεται να κλείσουμε τις γνωστές τρύπες του sendmail, από τις οποίες οι εισβολείς μπορεί να εισχωρήσουν. Η περίπτωση να αποτύχουμε να επιδιορθώσουμε τα γνωστά προβλήματα ασφαλείας αποτελεί τη βασικότερη πηγή κινδύνου για το σύστημα. Οι εισβολείς συχνά κατορθώνουν να καταστρέψουν τα διάφορα συστήματα με το να εκμεταλλεύονται τις αδυναμίες τους.

Για αυτό πρέπει να είμαστε συνεχώς ενημερωμένοι στην mailing list του sendmail ώστε να λαμβάνουμε συνεχώς τις καινούργιες ενημερώσεις για τις πιο σημαντικές αναβαθμίσεις ασφαλείας. Στέλνουμε το email με την παρακάτω γραμμή: subscribe sendmail-announce, στην διεύθυνση majordomo@lists.sendmail.org.

6.3.2 «Μπαλώματα» στις χαραμάδες τους συστήματος

Διορθώνουμε προβλήματα που προκύπτουν με το να εγκαταστήσουμε μπαλώματα (patches) στον πηγαίο κώδικα του sendmail. Κατεβάζουμε το μικρό αρχείο με το patch από το sendmail.org, έπειτα κατεβάζουμε ένα αρχείο με τη υπογραφή, ώστε να επιβεβαιώσουμε τον πηγαίο κώδικα και χρησιμοποιούμε το gpg ή το pgp για να επιβεβαιώσουμε το ότι το αρχείο που κατεβάσαμε είναι το σωστό και δεν έχει κάποιο πρόβλημα. [15]

6.3.3 Disabling Delivery to Programs

Από προεπιλογή το sendmail επιτρέπει τα μηνύματα να έχουν πρόσβαση στα προγράμματα. Για λόγους ασφαλείας εμείς πρέπει να απενεργοποιήσουμε αυτό το δικαίωμα για προγράμματα που δεν πρέπει να έχουν πρόσβαση αυτά τα μηνύματα. Θα υπάρχουν και περιπτώσεις που σε κάποια προγράμματα θα πρέπει να το επιτρέψουμε.

Σε κάθε περίπτωση το sendmail θα παραδώσει μηνύματα σε προγράμματα όταν η ηλεκτρονική διεύθυνση ξεκινάει με την κάθετη γραμμή | . Επομένως μπορούμε να πάμε στο αρχείο sendmail.cf και να αφαιρέσουμε την γραμμή | από τις ρυθμίσεις του mailer, που επιθυμούμε. [15]

6.3.4 Anti-Spam Configuration Control

Οι βασικές ιδιότητες του anti-spam, που είναι διαθέσιμες στο sendmail είναι:

- Η αναμετάδοση (relaying) απαγορεύεται εξαρχής
- Καλύτερος έλεγχος των πληροφοριών του αποστολέα
- Έλεγχος για το ποιος έχει πρόσβαση στη βάση δεδομένων
- Έλεγχος στις κεφαλίδες (headers) των μηνυμάτων [15]

6.3.5 SMTP Authentication

Η χρήση SMTP με πιστοποίηση αυθεντικότητας στον εξυπηρετητή ταχυδρομείου σας, μπορεί να σας προσφέρει μια σειρά από οφέλη. Μπορεί να προσθέσει ένα ακόμα επίπεδο ασφάλειας στο sendmail,

Εγκαθιστούμε το security/cyrus-sasl2 από τη συλλογή των Ports. Το port αυτό υποστηρίζει μια σειρά από επιλογές που μπορούμε να θέσουμε κατά την μεταγλώττιση. Για να μπορέσουμε να χρησιμοποιήσουμε την μέθοδο αυθεντικοποίησης στο SMTP που συζητάμε εδώ, βεβαιωνόμαστε πρώτα ότι είναι ενεργοποιημένη η επιλογή LOGIN.

- Μετά την εγκατάσταση του security/cyrus-sasl2, τροποποιούμε το αρχείο /usr/local/lib/sasl2/Sendmail.conf και προσθέτουμε την παρακάτω γραμμή: pwcheck_method: saslauthd
- Εγκαθιστούμε έπειτα το security/cyrus-sasl2-saslauthd, και προσθέτουμε στο /etc/rc.conf την ακόλουθη γραμμή: saslauthd_enable="YES"

Τέλος, ξεκινάμε το δαίμονα saslauthd: # /usr/local/etc/rc.d/saslauthd start

Ο δαίμονας αυτός δρα ως ενδιάμεσος για το sendmail ώστε να γίνεται πιστοποίηση αυθεντικότητας μέσω της βάσης δεδομένων κωδικών passwd. Με αυτό τον τρόπο απαλλάσσόμαστε από την ανάγκη δημιουργίας νέου σετ από ονόματα χρηστών και κωδικούς για κάθε χρήστη που χρειάζεται να χρησιμοποιήσει πιστοποίηση στο SMTP. Χρησιμοποιείται το ίδιο όνομα και κωδικός, τόσο για είσοδο στο σύστημα, όσο και για το mail. [15]

- Επεξεργαζόμαστε τώρα το /etc/make.conf και προσθέτουμε τις ακόλουθες γραμμές:

```
SENDMAIL_CFLAGS=-I/usr/local/include/sasl -DSASL
SENDMAIL_LDFLAGS=-L/usr/local/lib
SENDMAIL_LDADD=-lsasl2
```

Οι γραμμές αυτές, παρέχουν στο sendmail τις κατάλληλες ρυθμίσεις ώστε να συνδεθεί σωστά με το cyrus-sasl2 κατά τη διάρκεια της μεταγλώττισης.

- Επαναμεταγλωττίζουμε το sendmail εκτελώντας τις παρακάτω εντολές:

```
# cd /usr/src/lib/libsmutil
# make cleandir && make obj && make
# cd /usr/src/lib/libsm
# make cleandir && make obj && make
# cd /usr/src/usr.sbin/sendmail
# make cleandir && make obj && make && make install
```

- Τέλος, εκτελούμε make ενώ βρισκόμαστε στον κατάλογο /etc/mail. Με τον τρόπο αυτό, θα χρησιμοποιηθεί το νέο μας .mc αρχείο και θα δημιουργηθεί

ένα αρχείο .cf. Χρησιμοποιούμε έπειτα την εντολή make install restart, η οποία θα αντιγράψει το αρχείο στο sendmail.cf, και θα επανεκκινήσει σωστά το sendmail.

6.4 Proxy Server

Ένας proxy server είναι ένα πρόγραμμα που δέχεται αιτήσεις για την παρουσίαση σελίδων του World Wide Web από το φυλλομετρητή (browser) ενός χρήστη και αναλαμβάνει να προσκομίσει σε αυτόν τις ζητούμενες σελίδες. Ο proxy server, δηλαδή, παρεμβάλλεται μεταξύ του χρήστη και του WWW server από τον οποίο ζητά πληροφορίες ο χρήστης. Έτσι λοιπόν ο φυλλομετρητής (π.χ. Mozilla, IExplorer κλπ.) αντί να επικοινωνήσει απευθείας με το server που επιθυμεί ο χρήστης ζητά από το proxy server να του προσκομίσει τη σελίδα. Στη συνέχεια ο proxy server ζητά από τον server που ενδιαφέρει το χρήστη τις ζητούμενες σελίδες. Αφού ο server αποστέλλει τις σελίδες στον proxy server, ο proxy server με τη σειρά του στέλνει τις σελίδες που ζητήθηκαν στο φυλλομετρητή του χρήστη, ο οποίος και τις παρουσιάζει.

Τις περισσότερες φορές ένας proxy server είναι και ένας cache server. Ένας cache server αποθηκεύει τις αιτήσεις των φυλλομετρητών και τις αντίστοιχες απαντήσεις των servers με σκοπό να διαχειριστεί νέες αιτήσεις. Έτσι, έχουμε ένα proxy-cache server. Για παράδειγμα, αν έχουμε ένα σύνολο χρηστών που αξιοποιούν τη λειτουργία ενός proxy-cache server, όπως ο proxy server της εταιρίας, τότε αν ένας από αυτούς ζητήσει μια συγκεκριμένη σελίδα από ένα server στην Αμερική ο proxy-cache server θα φέρει τη σελίδα και αφενός θα την παραδώσει στο πρόγραμμα πλοήγησης του χρήστη, αφετέρου θα την αποθηκεύσει για μελλοντική χρήση. Αν τώρα ένας άλλος χρήστης -ή και ο ίδιος- ζητήσει τη ίδια σελίδα τότε ο proxy-cache server θα του προσκομίσει το αντίγραφο που έχει κρατήσει και δε θα αναζητήσει τη σελίδα στην Αμερική. [16]

Επομένως, αν την ίδια σελίδα θέλουν να δουν 100 άτομα, με τη χρήση του proxy-cache server, μόνο ο πρώτος θα χρειαστεί να περιμένει να έρθει η σελίδα

από τον αρχικό server, ενώ οι υπόλοιποι 99 θα δουν τη σελίδα να έρχεται ταχύτερα, αφού θα τους διατεθεί από τον proxy-cache server.

Υπάρχει πραγματικά μεγάλη πληθώρα proxy server στο internet, με τον καθένα από αυτούς να υποστηρίζει περισσότερα ή λιγότερα πρωτόκολλα και δυνατότητες. Εμείς καταλήξαμε στον squid τον οποίο και θα στήσουμε πάνω σε ένα μηχάνημα με λειτουργικό Ubuntu Linux. Είναι ο πιο διαδεδομένος, είναι GPLed, υπάρχει εδώ και πολλά χρόνια, είναι σταθερός, υποστηρίζεται από πληθώρα εφαρμογών και υποστηρίζει τις περισσότερες λειτουργίες από αυτές που μας ενδιαφέρουν.

6.4.1 Διαμόρφωση

Μετά την εγκατάσταση του squid μπορούμε να τον διαμορφώσουμε από το αρχείο squid.conf που βρίσκεται στον κατάλογο /etc/squid. Αυτή η δυνατότητα όμως μπορεί να αποδειχτεί ταυτόχρονα και αδυναμία του συστήματος, εφόσον μπορεί ο καθένας να έχει πρόσβαση σε αυτό ο αρχείο. Επομένως, μια πρώτη δουλειά που μπορούμε να κάνουμε είναι να δημιουργήσουμε ένα αντίγραφο του πρωτότυπου αρχείου διαμόρφωσης και να το προστατέψουμε από την εγγραφή, έτσι ώστε με αυτόν τον τρόπο να έχουμε την αρχικές ρυθμίσεις σαν σημείο αναφοράς.

sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.original
sudo chmod a-w /etc/squid/squid.conf.original

Η εταιρία, όπως έχουμε αναφέρει, δεν έχει ιδιαίτερα μεγάλο αριθμό υπολογιστών συνδεδεμένων με το διαδίκτυο. Αυτό συνεπάγεται και ιδιαίτερα χαμηλό φόρτο για τον proxy server, αφού οι αιτήσεις που θα χρειαστεί να εξυπηρετήσει είναι λίγες. Αυτούς τους υπολογιστές μπορούμε να τους δηλώσουμε στον server για να επιτρέπει την πρόσβαση μόνο σε αυτούς. Αυτό μπορεί να γίνει είτε αυτόματα δηλώνοντας όλο το δίκτυο είτε χειροκίνητα δηλώνοντας κάθε υπολογιστή ξεχωριστά. Εμείς επιλέγουμε τον δεύτερο τρόπο για το λόγο ότι δεν

έχουμε τόσο φόρο εργασίας. Σε διαφορετική περίπτωση θα ήταν ασύμφορο. Επομένως δίνουμε την εντολή [16]

```
acl our_networks src  192.168.111.5
http_access allow our_networks
```

και με αυτό τον τρόπο δηλώσαμε έναν υπολογιστή. Για τους υπόλοιπους αρκεί να προσθέσουμε την ip τους συνεχόμενα στην πρώτη γραμμή που δείξαμε παραπάνω. Στη συνέχεια απαγορεύουμε την πρόσβαση σε οποιονδήποτε άλλο.

```
http_access deny all
```

6.4.2 Έλεγχος πρόσβασης

Μπορούμε να τους απαγορεύσουμε την πρόσβαση στο διαδίκτυο σε μερικούς χρήστες, ή σε όλους τους χρήστες σε συγκεκριμένες ώρες. Αυτό γίνεται μέσω ενός ακόμη κανόνα ACL, του 'time', όπου καθορίζουμε τις ημέρες και τις ώρες απαγόρευσης. Οι ημέρες ορίζονται από ένα λατινικό γράμμα: M για τη Δευτέρα, T για την Τρίτη, W για την Τετάρτη, H για την Πέμπτη, F για την Παρασκευή, A για το Σάββατο και S για την Κυριακή. Το γράμμα D είναι μπαλαντέρ και σημαίνει όλες τις καθημερινές (MTWHF). Μπορούμε να χωρίσουμε τις IP διευθύνσεις σε allow1_computers και allow2_computers, κάπως έτσι: [17]

```
acl allow1_computers src 192.168.111.5 192.168.111.6
acl allow2_computers src 192.168.111.0/24
```

Στη συνέχεια δίνουμε τους κανόνες:

```
http_access deny allow1_computers homework_time
http_access allow allow1_computers
http_access allow allow2_computers
```

Οι δύο τελευταίες γραμμές είναι ευνόητες, αλλά η πρώτη περιλαμβάνει τα allow1_computers και homework_time. Όταν το Squid αποφασίζει αν θα δώσει πρόσβαση ή όχι, δουλεύει με τους κανόνες που εμφανίζονται κατά σειρά στο squid.conf. Στο παράδειγμά μας, θα βρει πρώτα την πρώτη γραμμή και θα απαγορεύσει την πρόσβαση σε όσα μηχανήματα έχουν IP της ομάδας allow1_computers αν η τρέχουσα ημέρα και ώρα συμπεριλαμβάνονται στο homework_time.

Μπορούμε να τους απαγορεύσουμε και την λήψη αρχείων από συγκεκριμένου είδους sites. Πιο συγκεκριμένα, μας ενδιαφέρουν τρία πράγματα: sites που γνωρίζουμε, sites που δεν γνωρίζουμε καθώς και είδη αρχείων που μπορεί να είναι επικίνδυνα για τους υπολογιστές τους.

Το πρώτο γίνεται με έναν ακόμα κανόνα ACL, το dstdomain, με το οποίο καθορίζουμε επακριβώς τα URLs που οι εργαζόμενοι δεν θα μπορούν να επισκέπτονται. Για παράδειγμα:

```
acl banned_sites dstdomain bbc.co.uk
http_access deny allow1_computers homework_time
http_access deny allow1_computers banned_sites
http_access allow allow1_computers
```

Το επόμενο πρόβλημα, ο αποκλεισμός των επικίνδυνων site που δεν γνωρίζουμε, λύνεται με τον καθορισμό "απαγορευμένων" λέξεων. Για παράδειγμα, μπορούμε να μπλοκάρουμε όλες τις ιστοσελίδες που περιέχουν την λέξη 'sex' ή 'windows'. Γι' αυτό πρέπει να χρησιμοποιήσουμε κανονικές εκφράσεις. Μια κανονική έκφραση για παράδειγμα μοιάζει ως εξής: [18]

```
acl noword url_regex -i word
```

Ο διακόπτης -i σημαίνει χωρίς διάκριση πεζών-κεφαλαίων, και έτσι θα περιλαμβάνει κάθε λέξη word, Word, WOrD, κτλ. Έτσι, μπορούμε να μπλοκάρουμε τα ...επίφοβα sites με τους παρακάτω κανόνες:

```
acl nosex url_regex -i sex
acl nowindows url_regex -i windows
```

Το τελευταίο πρόβλημα, η απαγόρευση λήψης επικίνδυνων αρχείων, λύνεται και πάλι με πολύπλοκες κανονικές εκφράσεις, που περιέχουν ^ και $ για την αρχή και το τέλος του ανεπιθύμητου αρχείου. Έτσι μπορούμε να μπλοκάρουμε κάθε URL που τελειώνει σε ".exe" ώστε οι υπολογιστές του δικτύου μας να μην δουν ποτέ εκτελέσιμα Windows, με τον κανόνα: [18]

```
acl noexes url_regex -i exe$
```

Το δολάριο στο τέλος σημαίνει ότι τα γράμματα exe πρέπει να εμφανίζονται στο τέλος του URL. Δηλαδή το www.hexen.com θα επιτρέπεται, ενώ το http://evil.com/virus.exe θα απαγορεύεται. [18]

6.5 Voip τηλεφωνία

Το Voice over IP (γνωστό και ως VoIP, Τηλεφωνία IP και Τηλεφωνία μέσω Διαδικτύου) αφορά μία τεχνολογία που καθιστά δυνατή τη δρομολόγηση φωνητικών συνδιαλέξεων μέσω του Διαδικτύου ή ενός δικτύου υπολογιστών. Για την πραγματοποίηση κλήσεων μέσω VoIP, ο χρήστης χρειάζεται ένα πρόγραμμα τηλεφώνου SIP με βάση λογισμικό ή ένα τηλέφωνο VoIP. Οι τηλεφωνικές κλήσεις μπορούν να πραγματοποιηθούν προς οποιοδήποτε προορισμό/άτομο: προς αριθμούς VoIP, καθώς και προς άτομα που διαθέτουν κανονικούς αριθμούς τηλεφώνου. [19]

6.5.1 Τι είναι τα τηλέφωνα SIP

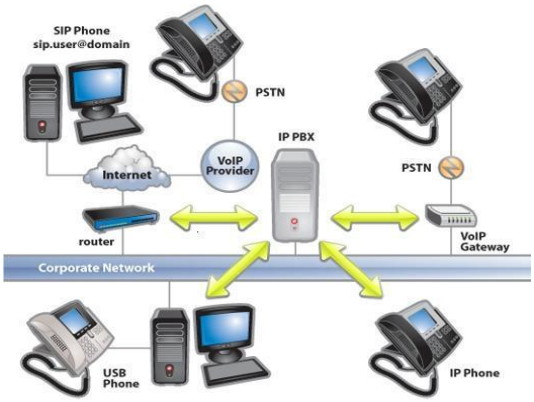
Τα τηλέφωνα SIP είναι ίδια με τα τηλέφωνα VoIP ή τα λογισμικά τηλεφώνου. Είναι τηλέφωνα που σας επιτρέπουν να κάνετε τηλεφωνικές κλήσεις χρησιμοποιώντας την τεχνολογία VoIP (φωνή μέσω πρωτοκόλλου internet).

Υπάρχουν δύο τύποι τηλεφώνων SIP. Ο πρώτος τύπος είναι το τηλέφωνο SIP με λογισμικό. Μοιάζει με την κοινή τηλεφωνική συσκευή, αλλά μπορεί να δεχτεί και να πραγματοποιήσει κλήσεις χρησιμοποιώντας το διαδίκτυο αντί για το παραδοσιακό σύστημα PSTN.

Τα τηλέφωνα SIP μπορεί επίσης να βασίζονται σε λογισμικό. Στην περίπτωση αυτή, επιτρέπουν να χρησιμοποιήσετε οποιονδήποτε υπολογιστή ως τηλέφωνο μέσω ακουστικών με μικρόφωνο ή/και κάρτας ήχου. Επίσης απαιτούν ευρυζωνική σύνδεση και σύνδεση με πάροχο υπηρεσιών VOIP ή διακομιστή SIP. [20]

6.5.2 Τι είναι το τηλεφωνικό σύστημα PBX

PBX είναι τα αρχικά των λέξεων Private Branch Exchange (ιδιωτικό κέντρο), δηλαδή ιδιωτικό τηλεφωνικό σύστημα που χρησιμοποιείται μέσα σε μια εταιρεία. Οι χρήστες του τηλεφωνικού συστήματος PBX τηλεφωνούν εκτός εταιρείας με κοινή χρήση μιας σειράς εξωτερικών γραμμών. (εικόνα 6-2)



Εικόνα 6-2

Το PBX συνδέει τα εσωτερικά τηλέφωνα μέσα σε μια επιχείρηση μεταξύ τους αλλά και με το δημόσιο τηλεφωνικό δίκτυο μεταγωγής (public switched telephone network (PSTN)). Μία από τις τελευταίες τάσεις στην εξέλιξη των τηλεφωνικών συστημάτων PBX είναι το VoIP PBX, επίσης γνωστό ως IP PBX, που χρησιμοποιεί το πρωτόκολλο internet για τη μετάδοση κλήσεων. [21]

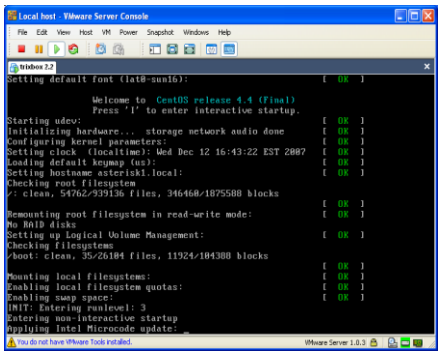
6.5.3 Διαθέσιμα IP PBX που βασίζονται σε SIP

- Asterisk – ένα IP PBX που βασίζεται στο Linux
- SIPX – ένα άλλο IP PBX που βασίζεται στο Linux
- 3CX Phone System – ένα IP PBX που βασίζεται στα Windows [22]

6.5.4 Πως λειτουργεί ένα IP PBX / Τηλεφωνικό σύστημα VoIP

Ένα Τηλεφωνικό Σύστημα VoIP / Σύστημα IP PBX αποτελείται από ένα ή περισσότερα τηλέφωνα SIP / τηλέφωνα VoIP, ένα διακομιστή IP PBX και περιλαμβάνει προαιρετικά μια Πύλη VoIP.

Ο διακομιστής του IP PBX είναι παρόμοιος με ένα διακομιστή μεσολάβησης: οι πελάτες SIP, είτε πρόκειται για τηλέφωνα με βάση λογισμικό, είτε για τηλεφωνικές συσκευές, καταχωρούνται στο διακομιστή του IP PBX, και όταν θέλουν να πραγματοποιήσουν μια κλήση, ζητούν από το IP PBX να δημιουργήσει τη σύνδεση.



Εικόνα 6-3

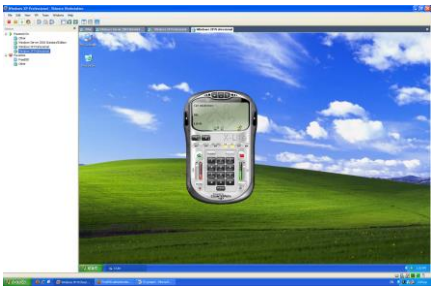
Το IP PBX διαθέτει ένα κατάλογο με όλα τα τηλέφωνα/χρήστες και τις αντίστοιχες SIP διευθύνσεις τους, και είναι επομένως σε θέση να συνδέσει μία εσωτερική κλήση ή να δρομολογήσει μία εξωτερική κλήση μέσω μίας πύλης VoIP ή ενός παροχέα υπηρεσιών VoIP.(εικόνα 6-3).

6.5.5 Η χρήση Voip τηλεφωνίας στην εταιρία

Με βάση τα παραπάνω, χρησιμοποιούμε για την εταιρία μας, ένα PBX server ο οποίος μπορεί να είναι ο INNOVVI BOXX SMB-BR (http://allvoip.gr/product_info.php?cPath=21&products_id=124) και εγκαθιστούμε το λειτουργικό TrixBox, το οποίο είναι βασισμένο σε Linux. Σε κάθε υπολογιστή εγκαθιστούμε το πρόγραμμα X lite το οποίο είναι ένα SIP τηλέφωνό.

Η χρήση του συγκεκριμένου προγράμματος γίνεται μόνο για λόγους ευκολίας της εργασίας. Την πραγματικότητα η εταιρία μπορεί να εξοπλιστεί με μια σειρά Voip τηλεφωνικών συσκευών. Τέτοιες συσκευές υπάρχουν στο εμπόριο και σε πολύ προσιτές τιμές, πχ η Crypto VPE 200 με τιμή 70 ευρώ. (http://allvoip.gr/product_info.php?cPath=22_23&products_id=183)

Από την ip PBX server μπαίνουμε στην ιστοσελίδα διαμόρφωσης σε administrator mode και από την καρτέλα FreePBX και στη συνέχεια στην καρτέλα extensions. Από εκεί επιλέγουμε το Generic SIP device και δημιουργούμε ένα λογαριασμό (extension) με User extension: τον κωδικό αριθμό που θα αντιστοιχεί και στον αριθμό κλήσης π.χ. 201 και 202, display name: το όνομα του εργαζόμενου, και secret: ένα συνθηματικό. (εικόνες 6-4, 6-5)



Εικόνα 6-4

Εικόνα 6-5

Στη συνέχεια πηγαίνουμε σε κάθε X lite στους υπολογιστές των εργαζομένων και περνάμε τα δεδομένα που θέσαμε πιο πριν, έτσι ώστε να φτιάξουμε τους λογαριασμούς τους. Από εκεί μόλις δημιουργήσουμε τους λογαριασμούς κάνουμε μια δοκιμαστική κλήση και παρατηρούμε ότι κάθε Voip τηλέφωνο καλεί κανονικά.

6.6 Επίλογος

Η ασφάλεια του διαδικτύου μας δεν μπορεί να εξαντληθεί απλά με τεχνικές και προγράμματα. Δεν υπάρχει ασφαλής τρόπος ή πρόγραμμα που να εξασφαλίζει την 100% προστασία από εξωγενείς παράγοντες. Μάλιστα πρέπει να θεωρούμε δεδομένο την πιθανότητα παραβίασης κάποια στιγμή του συστήματος μας, αφού η χρήση τεχνικών και προγραμμάτων ασφαλείας έπεται των εισβολών και των επιθέσεων. Το πιο σημαντικό είναι η επιτήρηση από το προσωπικό για να προλαμβάνονται όλα τα μέτρα εκείνα, που θα μας βοηθήσουν να ανακάμψουμε.

Κεφάλαιο 7

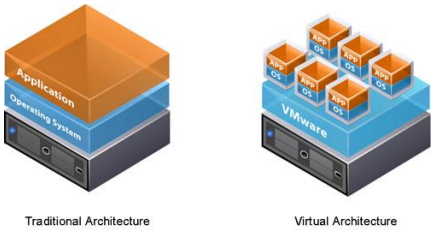
VIRTUALIZATION

7.1 Εισαγωγή

Η ιδεατοποίηση (Virtualization) ηλεκτρονικών υπολογιστών είναι μία έννοια που αναπτύχθηκε για πρώτη φορά στη δεκαετία του 1960 για τον διαμερισμό των μεγάλων κεντρικών μονάδων υπολογιστών. Είναι η πιο εξεζητημένη τεχνολογία, όχι μόνο γιατί αναπτύσσεται με γοργούς ρυθμούς αλλά και η εφαρμογή της αυξάνεται επιτακτικά. Δεν είναι ακραίο να πούμε πως τα πάντα πάνε προς Virtualization. Το virtualization έχει πάμπολλες εφαρμογές ενοποίηση (Consolidation), ισοκατανομή φόρτου (Load Balancing), δοκιμή λογισμικού (Software testing), επανάκαμψη μετά από καταστροφή (Disaster recovery).

7.2 Τί είναι το Server Virtualization

Το Server Virtualization είναι ένα πλαίσιο, μεθοδολογία ή τεχνική που επιτυγχάνει τον διαμερισμό των φυσικών πόρων ενός υπολογιστή σε πολλαπλά περιβάλλοντα εκτέλεσης, εφαρμόζοντας μία ή περισσότερες τεχνολογίες όπως διαμερισμό σε επίπεδο υλικού ή σε επίπεδο λογισμικού, διαμερισμό σε επίπεδο χρόνου, μερική ή ολική προσομοίωση μηχανής, εξομοίωση, ποιότητα υπηρεσιών, και άλλες.



Εικόνα 7-1

Είναι η μέθοδος εκτέλεσης πολλαπλών ανεξάρτητων ιδεατών λειτουργικών συστημάτων σε έναν φυσικό υπολογιστή. Είναι η απόκρυψη των φυσικών υπολογιστικών πόρων, συμπεριλαμβανομένων του αριθμού και της ταυτότητας

των μεμονωμένων φυσικών εξυπηρετητών, επεξεργαστών και λειτουργικών συστημάτων από τους χρήστες του «ιδεατού» εξυπηρετητή.

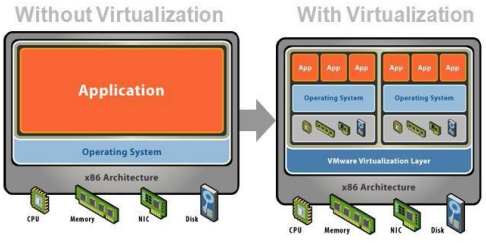
Το Virtualization, είναι ο διαμερισμός ενός φυσικού συστήματος σε πολλαπλά απομονωμένα μεταξύ τους εικονικά περιβάλλοντα. Τα εικονικά αυτά περιβάλλοντα συνήθως ονομάζονται virtual private servers, αλλά μπορεί κανείς να τα συναντήσει και με το όνομα partitions, guests, instances, containers ή emulations ή virtual machines.

Είναι ένα αφαιρετικό ενδιάμεσο στρώμα που επιτρέπει σε πολλαπλά ιδεατά μηχανήματα, με ετερογενή λειτουργικά συστήματα να λειτουργούν το καθένα ξεχωριστά μέσα σε ένα απομονωμένο περιβάλλον, το ένα δίπλα στο άλλο, πάνω στο ίδιο φυσικό μηχάνημα.

7.3 Τι είναι ένα Virtual Machine

Ένα εικονικό Μηχάνημα (Virtual Machine) είναι όπως ένα Φυσικό Μηχάνημα (Physical Machine), αλλά αντί για ηλεκτρονικά στοιχεία, αποτελείται από ένα σύνολο αρχείων λογισμικού. Κάθε εικονική μηχανή (virtual machine) αντιπροσωπεύει ένα ολοκληρωμένο σύστημα με επεξεργαστές, μνήμη, υποδομή για δικτυακή επικοινωνία, αποθηκευτικό χώρο, και BIOS. Ένα ιδεατό μηχάνημα τρέχει ένα ξεχωριστό λειτουργικό σύστημα και αντίστοιχες εφαρμογές, χωρίς καμία τροποποίηση, όπως ένα φυσικός εξυπηρετητής (physical server). [23]

7.4 Πώς λειτουργεί το Server Virtualization



Εικόνα 7-2

Στην ουσία, το Virtualization μας επιτρέπει να μετατρέψουμε το hardware σε software. Μπορούμε να χρησιμοποιήσουμε λογισμικό, όπως το VMware ESX Server, για να μετατρέψουμε ή αλλιώς να κάνουμε εικονοποίηση - «virtualize» τους φυσικούς πόρους ενός x86-based υπολογιστή,

συμπεριλαμβανομένων των ΚΜΕ (CPU), Μνήμη (RAM), σκληρό δίσκο (hard disk) και ελεγκτή δικτύου (network controller), προκειμένου να δημιουργήσουμε ένα πλήρως λειτουργικό ιδεατό μηχάνημα (virtual machine) που μπορεί να «τρέχει» το δικό του λειτουργικό σύστημα και τις δικές του εφαρμογές ακριβώς όπως ένας «πραγματικός» υπολογιστής.

Πολλαπλά virtual machines μπορούν να μοιράζονται τους φυσικούς πόρους χωρίς να επηρεάζουν το ένα το άλλο έτσι ώστε να μπορούμε με ασφάλεια να τρέξουμε πολλαπλά λειτουργικά συστήματα και εφαρμογές παράλληλα σε έναν υπολογιστή, μοιράζοντάς τον ουσιαστικά σε πολλούς ιδεατούς υπολογιστές (virtual machines), όπως φαίνεται και στην εικόνα 7.2. [23]

7.5 Οφέλη ενός οργανισμού από το Virtualization

1. **Ενοποίηση Εξυπηρετητών (Server Consolidation) & Βελτιστοποίηση Υποδομής (Infrastructure Optimization):**

Το Virtualization κάνει εφικτή την σημαντικά υψηλότερη αξιοποίηση πόρων συγκεντρώνοντας πόρους κοινής υποδομής (common infrastructure resources) και καταργώντας το παραδοσιακό μοντέλο “μία εφαρμογή σε έναν εξυπηρετητή”.

2. **Μείωση Κόστους Φυσικής Υποδομής**:

Με το Virtualization, μπορούμε να μειώσουμε τον αριθμό των servers και το σχετιζόμενο IT hardware στο κέντρο δεδομένων. Αυτό οδηγεί σε μείωση στις απαιτήσεις σε ακίνητη περιουσία (real estate), ισχύ και ψύξη, οδηγώντας σε σημαντικά χαμηλότερο IT κόστος.

3. **Βελτιωμένη Ευελιξία Λειτουργιών & Ανταπόκριση**:

Το Virtualization προσφέρει έναν νέο τρόπο διαχείρισης της IT υποδομής και μπορεί να βοηθήσει τους IT διαχειριστές να δαπανούν λιγότερο χρόνο σε επαναλαμβανόμενες διαδικασίες όπως το provisioning (προμήθειες), η παραμετροποίηση, η παρακολούθηση και η συντήρηση.

4. **Αυξημένη Διαθεσιμότητα Εφαρμογών & Βελτιωμένο Business Continuity**:

Εξαλείφεται το προγραμματισμένο downtime και γίνεται εφικτή η γρήγορη ανάκαμψη από απρόσμενες διακοπές λειτουργίας με την δυνατότητα για ασφαλές backup και μετακίνηση ολόκληρων virtual environments, χωρίς καμία διακοπή στην υπηρεσία.

5. **Βελτιωμένη Διαχειρισιμότητα και Ασφάλεια των Σταθμών Εργασίας (Desktops)**:

Παρέχεται η δυνατότητα για δημιουργία, διαχείριση και παρακολούθηση ασφαλούς περιβάλλοντος με desktops το οποίο οι χρήστες μπορούν να προσπελάσουν τοπικά ή από απομακρυσμένη τοποθεσία, με ή χωρίς δικτυακή σύνδεση, από σχεδόν οποιοδήποτε standard desktop, laptop ή tablet PC. [23]

7.6 Πλεονεκτήματα των Virtual Machines

Γενικά, τα virtual machines διαθέτουν τέσσερα σημαντικά χαρακτηριστικά που ωφελούν τον χρήστη:

- **Απομόνωση**: Τα virtual machines είναι απομονωμένα το ένα από το άλλο σαν ήταν φυσικά διαχωρισμένα.
- **Ενθυλάκωση**: Τα virtual machines ενθυλακώνουν ένα ολόκληρο υπολογιστικό περιβάλλον
- **Συμβατότητα**: Τα virtual machines είναι συμβατά με όλους τους προτυποποιημένους (standard) x86 υπολογιστές
- **Ανεξαρτησία από το Hardware**: Τα virtual machines τρέχουν ανεξάρτητα από το υποκείμενο hardware

7.7 Πλεονεκτήματα του Server Virtualization

Η τεχνολογία Server Virtualization παρουσιάζει μια σειρά από πλεονεκτήματα που μπορούν να ωφελήσουν σημαντικά ένα τμήμα IT και συνολικότερα έναν οργανισμό. Ακολούθως παρατίθεται μια λίστα από αντιπροσωπευτικούς λόγους για τους οποίους μπορούμε να αξιοποιήσουμε το Server Virtualization:

- Οι Ιδεατές Μηχανές (Virtual Machines) μπορούν να χρησιμοποιηθούν για την συνένωση του φορτίου εργασίας πολλαπλών υποαπασχολούμενων εξυπηρετητών σε λιγότερα μηχανήματα, ίσως και σε ένα μηχάνημα (server consolidation). Τα σχετιζόμενα οφέλη είναι η εξοικονόμηση σε υλικό εξοπλισμό (hardware), σε περιβαλλοντικό κόστος, σε διοίκηση και διαχείριση της υποδομής εξυπηρετητών.
- Τα virtual machines μπορούν να χρησιμοποιηθούν για να παρέχουν ασφαλή, απομονωμένα περιβάλλοντα για την λειτουργία εφαρμογών που δεν μπορούμε να εμπιστευτούμε. Το Virtualization αποτελεί ένα σημαντικό πλαίσιο για την δημιουργία ασφαλών υπολογιστικών πλατφορμών.
- Οι ιδεατές μηχανές μπορεί να χρησιμοποιηθούν για την εκτέλεση πολλαπλών λειτουργικών συστημάτων ταυτόχρονα: διαφορετικές εκδόσεις ή ακόμη και εντελώς διαφορετικά συστήματα, που μπορεί να είναι σε αναμονή. Κάποια τέτοια συστήματα ίσως να είναι δύσκολο ή αδύνατον να τρέξουν σε νέο πραγματικό hardware.
- Τα virtual machines επιτρέπουν με μεγάλη ευκολία το debugging και το performance monitoring. Για παράδειγμα, τέτοια εργαλεία μπορούν να τοποθετηθούν στο virtual machine monitor. Η εξουδετέρωση σφαλμάτων (debugging) μπορεί να γίνει σε λειτουργικά συστήματα χωρίς να διακοπεί η παραγωγική τους λειτουργία, η ακόμα μπορούν να δημιουργηθούν πιο σύνθετα σενάρια εξουδετέρωσης σφαλμάτων.
- Τα virtual machines εκτελούνται απομονωμένα με αποτέλεσμα να μην επηρεάζουν το περιβάλλον τους (άλλες ιδεατές μηχανές που εκτελούνται ταυτόχρονα στο ίδιο φυσικό σύστημα), οποιαδήποτε σφάλματα και αν εμφανίζονται μέσα στο κάθε virtual machine. Δύναται να δημιουργούμε

λάθη σκόπιμα στο λογισμικό μια ιδεατής μηχανής για να μελετήσουμε τις επακόλουθες συνέπειες.

- Το Virtualization μπορεί να κάνει ευκολότερες και καλύτερα διαχειρίσιμες, λειτουργίες όπως η αλλαγή συστημάτων (system migration), η δημιουργία αντιγράφων ασφαλείας (backup), και η ανάκαμψη από σφάλματα (recovery).

7.8 Εφαρμογές της τεχνολογίας Server Virtualization

7.8.1 Server Consolidation

Εξάπλωση/Διασπορά διακομιστών (Server Sprawl) λέγεται η κατάσταση στην οποία πολλαπλοί, υποαπασχολούμενοι servers καταλαμβάνουν χώρο και καταναλώνουν περισσότερους πόρους από ότι μπορεί να δικαιολογηθεί από το φόρτο εργασίας τους. Συχνές αιτίες του server sprawl (εξάπλωσης υπολογιστών) είναι η αγορά μεγάλου αριθμού από χαμηλού κόστους (low-end) servers και η πρακτική της αφιέρωσης διακομιστών σε μεμονωμένες εφαρμογές. Η εξάπλωση των διακομιστών μπορεί να περιορίζεται σε ένα δωμάτιο υπολογιστών, αλλά σε κάποιες περιπτώσεις μπορεί να εξαπλώνεται σε πολλαπλές εγκαταστάσεις σε ευρύτατα εκτεταμένες γεωγραφικές περιοχές, ειδικά σε περιπτώσεις που μια επιχείρηση έχει εξαγοράσει μια άλλη ή όπου δύο εταιρείες έχουν συγχωνευθεί.[24]

7.8.2 Disaster Recovery

Ένα σχέδιο ανάκαμψης από καταστροφή (disaster recovery plan – DRP), που μερικές φορές αναφέρεται ως business continuity plan (BCP) ή σαν business process contingency plan (BPCP), περιγράφει πώς ένας οργανισμός θααντιμετωπίσει πιθανές καταστροφές. Όπως μια καταστροφή είναι ένα γεγονός που κάνει αδύνατη την συνέχιση των κανονικών λειτουργιών, ένα πλάνο ανάκαμψης από καταστροφή αποτελείται από προληπτικά μέτρα που λαμβάνονται

προκειμένου οι επιδράσεις μια καταστροφής να ελαχιστοποιηθούν και ο οργανισμός να είναι σε θέση είτε να διατηρήσει είτε γρήγορα να αρχίσει εκ νέου τις πιο κρίσιμες επιχειρησιακά (mission-critical) λειτουργίες. Συνήθως, ο σχεδιασμός ανάκαμψης από καταστροφές περιλαμβάνει ανάλυση των επιχειρησιακών διαδικασιών και των αναγκών για συνέχιση των λειτουργιών. Μπορεί επίσης να περιλαμβάνει επικέντρωση σε σημαντικό βαθμό στην αποφυγή καταστροφής.

Το Disaster Recovery γίνεται μία ολοένα σημαντικότερη πλευρά του enterprise computing. Καθώς οι συσκευές, τα συστήματα και τα δίκτυα γίνονται όλο και πιο σύνθετα, υπάρχουν περισσότερα πράγματα που μπορούν να παρουσιάσουν προβλήματα. Σαν συνέπεια, τα πλάνα ανάκαμψης έχουν επίσης γίνει πιο σύνθετα. [24]

7.8.3 Network Virtualization

Network Virtualization είναι η μέθοδος συνδυασμού των διαθέσιμων πόρων σε ένα δίκτυο χωρίζοντας το διαθέσιμο bandwidth σε κανάλια (chanels), κάθε ένα από τα οποία είναι ανεξάρτητο από τα άλλα, και κάθε ένα από τα οποία μπορεί να ανατεθεί (ή να επανατεθεί) σε έναν συγκεκριμένο server ή συσκευή σε πραγματικό χρόνο. Κάθε κανάλι ασφαλίζεται ανεξάρτητα. Κάθε συνδρομητής έχει κοινή πρόσβαση σε όλους τους πόρους στο δίκτυο από έναν υπολογιστή. Η διαχείριση του δικτύου μπορεί να είναι μια κουραστική και χρονοβόρα εργασία για έναν διαχειριστή.

Το Network Virtualization προορίζεται για να βελτιώσει την παραγωγικότητα, την αποδοτικότητα, και την ικανοποίηση από την εργασία του διαχειριστή επιτρέποντάς του να εκτελεί πολλές από αυτές τις εργασίες αυτόματα, κι έτσι να παραλλάσσει την πραγματική πολυπλοκότητα του δικτύου. Αρχεία, εικόνες, προγράμματα και φάκελοι δύναται να είναι κεντρικά διαχειρίσιμα, από ένα μόνο φυσικό site.

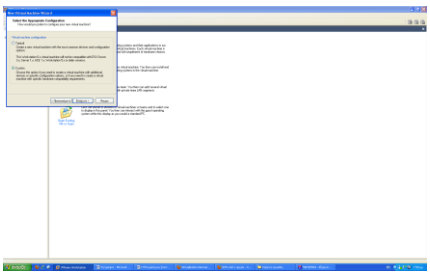
Μέσα αποθήκευσης όπως σκληροί δίσκοι και οδηγοί ταινίας (tape drives) μπορούν εύκολα να προστεθούν ή να επανατεθούν. Αποθηκευτικός χώρος μπορεί να μοιραστεί ή να επανατεθεί ανάμεσα στους servers. Το Network Virtualization

προορίζεται για να βελτιστοποιήσει την ταχύτητα του δικτύου, την αξιοπιστία, την ευελιξία, την επεκτασιμότητα, και την ασφάλεια. [65]

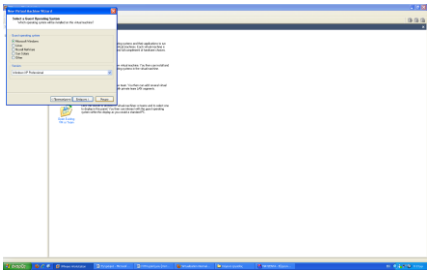
7.9 Παρουσίαση VMware

Για να φτιάξουμε ένα πραγματικό ηλεκτρονικό υπολογιστή (physical computer) παίρνουμε μητρική κάρτα (motherboard), επεξεργαστή (cpu), μνήμη (ram), αποθηκευτικά μέσα – σκληρό δίσκο (hdd), κάρτα δικτύου (network card), τροφοδοτικό (power supply).

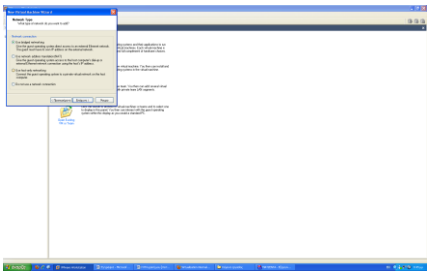
Για να φτιάξουμε ένα εικονικό υπολογιστή, ξεκινάμε από File -> New -> Virtual Machine -> New Virtual Machine Wizard (εικόνα 7-3) και στη συνέχεια επιλέγουμε να δημιουργήσουμε μια custom εικονική μηχανή διαλέγοντας το λειτουργικό σύστημα που θα εγκαταστήσουμε και την κατάλληλη έκδοσή του (εικόνα 7-4). Έπειτα δίνουμε στοιχεία για το πόσους επεξεργαστές ή πόσους πυρήνες στον επεξεργαστή έχει ο υπολογιστής οικοδεσπότης και τους οποίους εμείς θα τους διαθέσουμε και στην εικονική μηχανή. Μετά καθορίζουμε τη μνήμη RAM που θα χρησιμοποιεί. Εδώ θέλει μια προσοχή διότι η RAM που θα δώσουμε στο εικονικό μηχάνημα δεσμεύεται πλήρως από αυτό και ουσιαστικά την χάνουμε από τον υπολογιστή οικοδεσπότη. Στη συνέχεια επιλέγουμε τον τρόπο διασύνδεσης της εικονικής μηχανής (εικόνα 7-5), τι τύπο σκληρού δίσκου θα χρησιμοποιήσουμε και τέλος πόσο μέγεθος σκληρού δίσκου θα χρησιμοποιήσουμε (εικόνα 7-6).



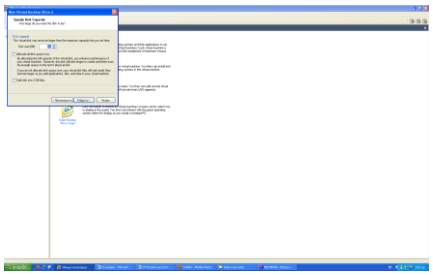
Εικόνα 7-3



Εικόνα 7-4

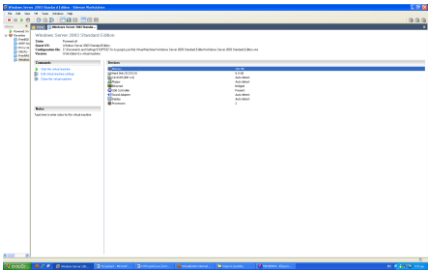


Εικόνα 7-5

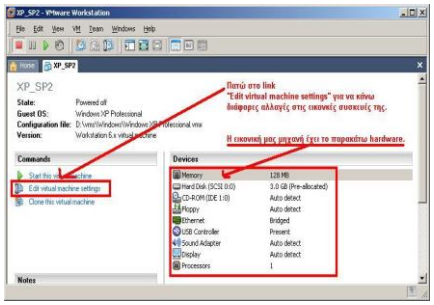


Εικόνα 7-6

Σε κάθε εικονική μηχανή το Virtualization layer δίνει από ένα set εικονικών συσκευών hardware. Η κάθε εικονική μηχανή δεν έχει απ' ευθείας πρόσβαση στο hardware layer. Επίσης στέλνει τα αιτήματά της για πρόσβαση στο εικονικό hardware. Το virtualization layer, όλα αυτά τα αιτήματα προς το εικονικό hardware, τα μαρκάρει με κατάλληλη προτεραιότητα και τα στέλνει μέσω μιας σειράς στο πραγματικό hardware του υπολογιστή. Το εικονικό hardware κάθε εικονικής μηχανής άλλες φορές είναι προκαθορισμένο από την VMWare και άλλες πάλι φορές εξαρτάται από το υποκείμενο hardware του physical host. (εικόνα 7-7)



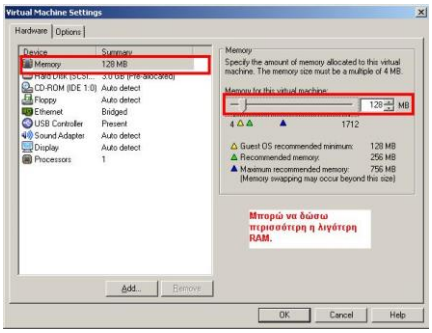
Εικόνα 7-7



Εικόνα 7-8

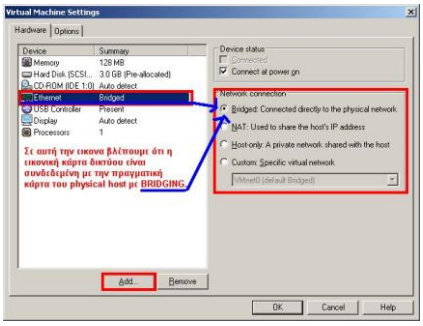
Όπως σε ένα πραγματικό ηλεκτρονικό υπολογιστή μπορούμε να προσθέσουμε επιπλέον ram, σκληρό δίσκο, έτσι και οι εικονικές μηχανές επιδέχονται τροποποιήσεων. Μπορούμε δηλαδή και σε αυτές να προσθαφαιρέσουμε οποιοδήποτε κομμάτι υλικού, (εικόνα 7-8). Παραδείγματος χάρη:

Μνήμη



Εικόνα 7-9

Δίκτυο



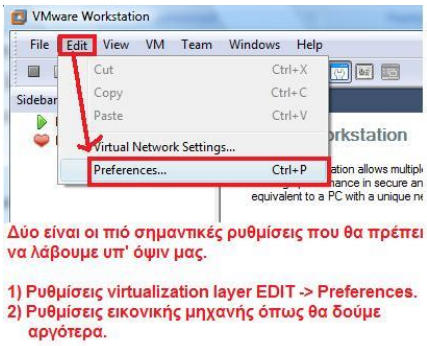
Εικόνα 7-10

Δύο είδη ρυθμίσεων θα πρέπει να έχουμε υπ' όψιν μας.

1) Ρυθμίσεις που αφορούν ως προς το σύνολο την συμπεριφορά του virtualization layer.

2) Ρυθμίσεις που αφορούν την συμπεριφορά των εικονικών μηχανών.

Οι ρυθμίσεις που αφορούν το virtualization layer γίνονται από Edit -> Preferences.(εικόνα 7-11)



Εικόνα 7-11

Στην καρτέλα Workspace (εικόνα 7-12) οι σπουδαιότερες ρυθμίσεις είναι:

1) Default location of virtual machines and teams.

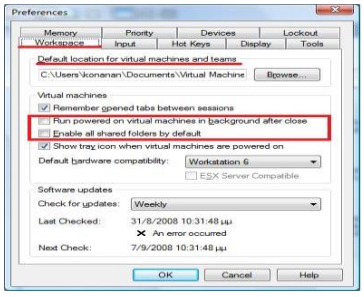
Εδώ ορίζουμε το σημείο που θα αποθηκεύονται οι εικονικές μηχανές που θα δημιουργούμε. Teams είναι ομάδες εικονικών μηχανών.

2) Run powered on virtual machines in background after close.

α) Ξεκινάμε το vmware workstation,

β) ξεκινάμε τις εικονικές μηχανές και

γ)κλείνουμε το vmware workstation έχοντας τις εικονικές μηχανές να τρέχουν σαν services.



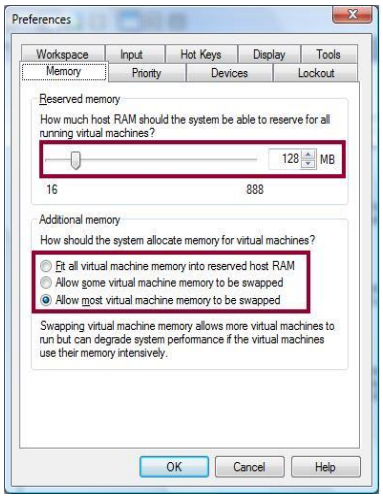
Εικόνα 7-12

3) Enable all shared folders by default. Ενεργοποιώ τα κοινόχρηστα στοιχεία ανάμεσα στο host / guest λειτουργικό.

Από τη καρτέλα memory (εικόνα 7-13) καθορίζουμε :

Το σύνολο της ram που θα δεσμεύσουμε για όλες τις εικονικές μηχανές. Ο πραγματικός ηλεκτρονικός υπολογιστής, έχει ας υποθέσουμε N ram, από αυτή την ram δεσμεύουμε ένα ποσό για να την χρησιμοποιούν αποκλειστικά οι εικονικές μηχανές.

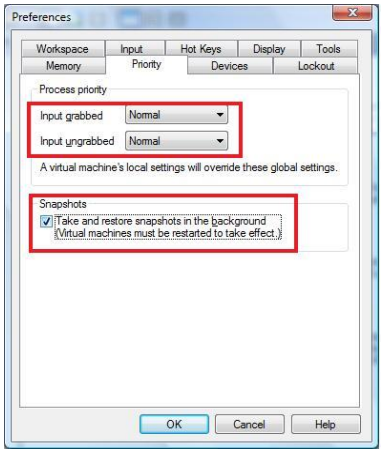
Πως θα διαχειρίζεται το virtualization layer την RAM;



Εικόνα 7-13

Αν έχω αρκετή RAM τότε για λόγους απόδοσης, δεσμεύσω αυτή που χρειάζονται οι εικονικές μηχανές. Αν π.χ έχω ένα σύστημα με 4GB RAM και δεσμεύσω (από εδώ) τα 3GB, τότε το host OS θα βλέπει μόνο το 1GB ενώ οι εικονικές μηχανές θα έχουν στην διάθεσή τους 3GB.

Εδώ καθορίζουμε τι θα γίνεται σε περίπτωση που επιλέγουμε μια εικονική μηχανή. Τι προτεραιότητα θα έχει αυτή. Την εικονική μηχανή ,επίσης, μπορώ να την παγώσω και να φωτογραφήσω την κατάστασή της μια συγκεκριμένη στιγμή. Η διαδικασία παγώματος και φωτογράφισης είναι πολύ εύκολη μόνο που παίρνει αρκετό χρόνο. Γι αυτό στην καρτέλα Priority μπορούμε να καθορίσουμε αν το snapshot θα γίνεται σε background ή όχι.(εικόνα 7-14)

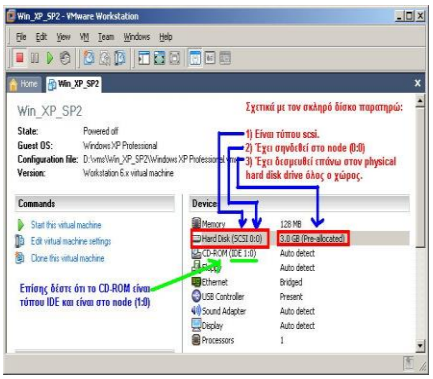


Εικόνα 7-14

7.9.1 Εικονικός σκληρός δίσκος

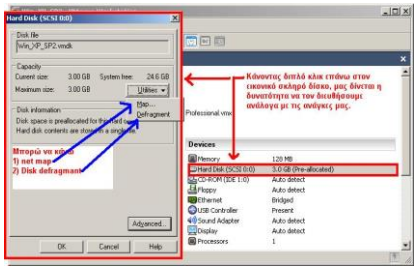
Ο δυναμικός σκληρός δίσκος δεν δεσμεύει όλο το μέγεθος του, αλλά ξεκινά δεσμεύοντας ένα μικρό μέρος αυτού και στην συνέχεια μεγαλώνει ανάλογα με τις απαιτήσεις. Σε αυτή την περίπτωση δεσμεύουμε τόσο physical hard disk space όσο χρειαζόμαστε. (εικόνα 7-15).

Τα μειονεκτήματα των δυναμικών δίσκων είναι :
1) χαμηλότερη επίδοση του συστήματος,
2) μελλοντικός πιθανός κερματισμός του σκληρού δίσκου.
Τέλος ο εικονικός δίσκος μπορεί να είναι
1) μονολιθικός να αποτελείται από ένα αρχείο.
2) split file δηλαδή να αποτελείται από πολλά αρχεία των 2GB το κάθε ένα. Η χρήση εικονικού δίσκου τύπου split file έχει πολλά πλεονεκτήματα, για να κάνουμε π.χ. disk backup, disk defragmentation, disk shring χρειαζόμαστε μόνο 2GB ελεύθερο σκληρό.



Εικόνα 7-15

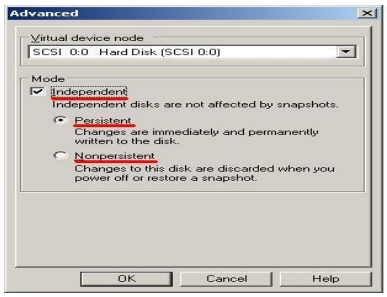
Από το κεντρικό interface του VMWare server/workstation, κάνοντας διπλό κλικ στον σκληρό δίσκο μπορούμε να τον παραμετροποιήσουμε ανάλογα με τις ανάγκες μας.(εικόνα 7-16)



Εικόνα 7-16

Όπως βλέπουμε παραπάνω μέσα από το utilities μπορούμε να
1) τον αντιστοιχίσουμε σε ένα network drive (mapping)
2) να του κάνουμε defragment.

Τέλος από αυτό το σημείο καθορίζουμε το τρόπο πρόσβασης στον εικονικό δίσκο. (εικόνα 7-17).



Εικόνα 7-17

1) Independent mode (Δεν μπορούμε να πάρουμε snapshot)
2) Persistent mode
Οι εγγραφές (μεταβολές) στον εικονικό δίσκο σώζονται ΑΜΕΣΩΣ την στιγμή που λαμβάνουν χώρα σε αυτόν.
3) Non Persistent.

7.9.2 Network

Το περιβάλλον VMware workstation / server χρησιμοποιεί τις ίδιες δικτυακές συσκευές (παρόμοια πράγματα ισχύουν και στον χώρο της MS). Το κλειδί στα εικονικά δίκτυα είναι το εικονικό switch. Όπως ένα πραγματικό switch έτσι και το εικονικό μας επιτρέπει να συνδέσουμε διάφορες IP συσκευές μεταξύ τους. Στο περιβάλλον workstation / server έχουμε 10 windows εικονικά switch. Σε κάθε ένα από αυτά μπορούμε να συνδέσουμε μια ή περισσότερες εικονικές μηχανές. (εικόνα 7-18)

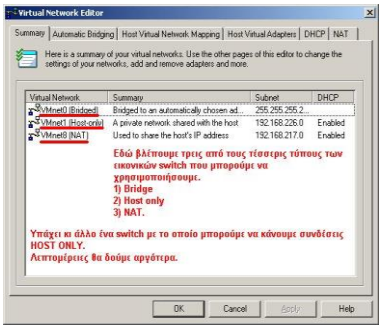
Εξ' ορισμού, τρία από αυτά τα εικονικά switch χρησιμοποιούνται για συγκεκριμένα είδη δικτύων.

VMNET0 = Bridged Networking
VMNTE1 = Host-Only Networking
VMNTE 8 = NAT Networking

Εικόνα 22

Ας περάσουμε λοιπόν από το επίμαχο σημείο για να δούμε καλύτερα περί τίνος πρόκειται. Από το κεντρικό μενού FILE -> VIRTUAL NET SETTINGS

Στην παρακάτω καρτέλα βλέπουμε τα είδη των εικονικών switch καθώς και το σημείο από το οποίο μπορούμε να προβούμε σε τυχόν διευθετήσεις. Network Adaptor (NIC). Κάθε φορά που δημιουργούμε μια εικονική μηχανή με τον New Virtual Machine Wizard, δημιουργούμε σε αυτή την εικονική μηχανή και μια εικονική κάρτα δικτύου. Αυτή η εικονική κάρτα δικτύου, εμφανίζεται (στο guest λειτουργικό) σαν AMD PCNET PCI (ή σαν Intel Pro/1000 MT αν πρόκειται για Vista guest OS). (εικόνα 7-19)



Εικόνα 7-19

7.9.3 Snapshots

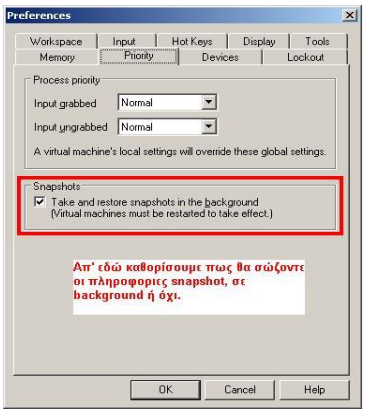
Με το snapshot σώζουμε ολοκληρωτικά την κατάσταση που βρίσκεται η εικονική μας μηχανή σε μια χρονική στιγμή.

Πληροφορίες που σώζονται είναι:

1) οτιδήποτε πληροφορίες βρίσκονται στην εικονική RAM,

2) Κατάσταση όλων των εικονικών σκληρών δίσκων,

3) Ρυθμίσεις διευθέτησης της εικονικής μηχανής.



Εικόνα 7-20

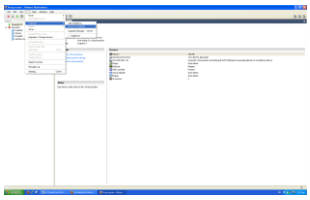
Έτσι, όταν επιστρέφουμε σε ένα snapshot, γυρνάμε στις ρυθμίσεις που είχε εκείνη την στιγμή η μηχανή μας. Με τις εργοστασιακές ρυθμίσεις του workstation, το σώσιμο των πληροφοριών γίνεται σε background mode για να μπορούμε παράλληλα να εργαζόμαστε. Αυτό μπορεί να πραγματοποιηθεί πό το κεντρικό μενού EDIT -> PREFERENCES -> PRIORITY. (εικόνα 7-20)

Παραπάνω είπαμε ότι παίρνοντας ένα snapshot, σώζουμε ολοκληρωτικά την κατάσταση μιας εικονικής μηχανής την δεδομένη στιγμή εκτός των άλλων και την “Κατάσταση όλων των εικονικών σκληρών δίσκων ”. Σε περίπτωση που δεν επιθυμούμε να συμπεριλαμβάνονται πληροφορίες από ένα σκληρό έχουμε την

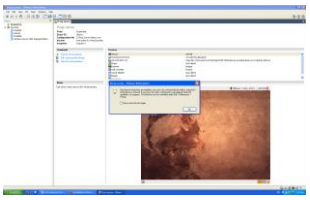
δυνατότητα να τον αποκλείσουμε. Αυτή η ρύθμιση γίνεται από VM->SETTINGS, επιλέγω τον σκληρό δίσκο και πατώ το κουμπί advanced.

Παράδειγμα snapshot παίρνουμε από τον proxy server. Στη συνέχεια κλείνουμε την εικονική μηχανή και την επανεκκινούμε από τη ρύθμιση. (εικόνες 7-21, 7-22, 7-23)

Εικόνα 7-21



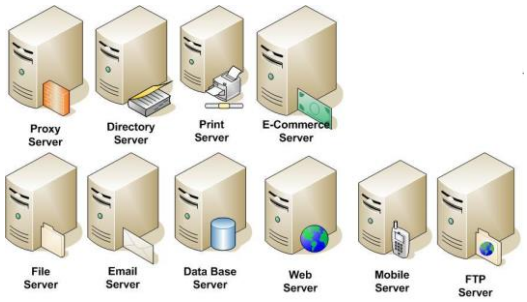
Εικόνα 7-22



Εικόνα 7-23

7.10 Παράδειγμα εφαρμογής

Ας υποθέσουμε πως ένας server υπολογιστής που ταιριάζει στις ανάγκες μας, κοστίζει 5000 ευρώ και ας υποθέσουμε πως χρειαζόμαστε 10 τέτοιους υπολογιστές, πρέπει δηλαδή να επενδύσουμε 50.000 ευρώ. Σε αυτήν την περίπτωση θα μπορούσαμε να αγοράζαμε ένα τέτοιο υπολογιστή server και πάνω σε αυτόν συμπυκνώναμε τους υπόλοιπους. Δηλαδή, θα αγοράσουμε ένα physical server (με τα αναγκαία hardware resources) και μέσα σε αυτόν θα εγκαταστήσουμε 10 εικονικές μηχανές, (εικόνα 7-24, 7-25)η κάθε μια από τις οποίες θα τρέχει το αντίστοιχο software server (ταυτόχρονα). Έτσι, όσο περισσότερους server συμπυκνώναμε τόσο καλύτερη απόδοση χρημάτων θα είχαμε.



Εικόνα 7-24

Φυσικά αυτή η συμπύκνωση δεν μπορεί να γίνεται απερίσκεπτα, ούτε μπορούμε να εικονικοποιήσουμε τα πάντα.

Το σύνηθες windows server utilization κυμαίνεται από 3-5%. Για κάποιους λόγους αυτό είναι το INDUSTRY STANDARD απόδοσης των windows Server.

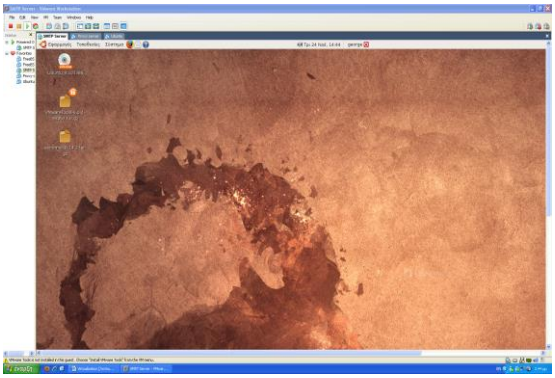
Εικόνα 7-25

Την συμπύκνωση, την κάνουμε υπό την προϋπόθεση οι εικονικοί μας servers έχουν μικρό server utilization. Έτσι αντί να αγοράσουμε 10 servers που θα εργάζονται με χαμηλή απόδοση, προτιμούμε να αγοράσουμε 1 physical server ανεβάζοντας την απόδοσή του 10 X (3% - 5%) βάζοντας μέσα σε αυτόν τους 10 εικονικούς servers (εικόνα 3). Τώρα έχουμε ένα physical server ο οποίος δεν εργάζεται με 3-5% απόδοση αλλά 30-50%.

Οικονομία: σε έξοδα αγοράς, λειτουργικά έξοδα (κατανάλωση ρεύματος, power-cooling).

Κόστος αγοράς: Το κόστος ενός server σίγουρα δεν συγκρίνεται με αυτό ενός workstation. Επειδή ένας υπολογιστής server πρέπει να είναι αξιόπιστος και απαιτούμε πολλά από αυτόν, όπως είναι η ανοχή σε σφάλματα (fault tolerance) σε πολλά επίπεδα, για αυτό όλο του το hardware είναι ακριβότερο. Παρόλα αυτά όμως τα έξοδα για την αγορά ενός τέτοιου μηχανήματος ισοσταθμίζονται από το κέρδος που έχουμε με την συμπύκνωση των server της εταιρίας.

Ουσιαστικά θα χρειαστούμε 2 μηχανήματα. Στο ένα θα είναι εγκατεστημένοι οι δύο sever του τοπικού δικτύου και στον άλλο εγκαθιστούμε τον Web Server, τον Mail Server, τον Proxy Server, και τον PBX Server. (εικόνα 7-26). Βέβαια, ειδικά στον 2^{ο} server θα πρέπει να προβλέψουμε και το φόρτο του δικτύου που θα αναπτυχθεί. Όμως οι υπολογιστές που θα έχουν πρόσβαση στο διαδίκτυο δεν είναι πολλοί σε αριθμό και δεν απαιτείται να είναι συνεχώς online. Το μόνο που σίγουρα θα δημιουργεί το μεγαλύτερο φόρτο είναι ο PBX sever και η Voip τηλεφωνία που χρησιμοποιήσουμε, αλλά εδώ μπορούμε να



Εικόνα 7-26

χρησιμοποιήσουμε μια μισθωμένη γραμμή και να ορίσουμε το μεγαλύτερο εύρος της να το χρησιμοποιεί ο PBX.

Επομένως ένα μηχάνημα με 8 GB μνήμη και ένα επεξεργαστή 4 πυρήνων μπορεί να ανταπεξέλθει με μεγάλη ευκολία. Για να το καταφέρουμε αυτό μοιράζουμε την μνήμη ανάλογα με τις αιτήσεις. Ο proxy, ο web και ο SMTP server μπορούν να δουλέψουν με μνήμη της τάξης των 512 MB έως 1 GB. Αυτό μας δίνει το δικαίωμα να διαθέσουμε περίπου 5 έως 3 GB μνήμης για το PBX server, οποίος σε ορισμένες περιπτώσεις θα χειρίζεται μεγάλο φόρτο λόγω των κλήσεων που θα γίνονται.

Αντίστοιχα με ένα ίδιο μηχάνημα μπορούμε να αντικαταστήσουμε τους 2 server του τοπικού δικτύου. Με αυτόν τον τρόπο πέρα από τον ένα υπολογιστή που γλυτώνουμε, μπορούμε ταυτόχρονα να μοιράσουμε και το βάρος της διαχείρισης του δικτύου καλύτερα μεταξύ των 2 server

Λειτουργικό κόστος: Οι server, συνήθως βρίσκονται σε συνεχή λειτουργία, αυτός άλλωστε είναι και ο σκοπός, να δουλεύουν 24 ώρες, 360 ημέρες τον χρόνο. Έξοδα λοιπόν όχι μόνο για την τροφοδοσία τους αλλά και για την ψύξη τους. Χρησιμοποιώντας λιγότερους physical servers, ελαττώνουμε και τα έξοδα λειτουργίας, συντήρησης.

Disaster recovery. Η εταιρία με τη χρήση του virualization, έχει το πλεονέκτημα να δημιουργεί αντίγραφα ασφαλείας του συστήματος, ώστε σε περίπτωση καταστροφής να μπορεί να ανακάμψει το σύστημα το ταχύτερο δυνατό και να μην διακοπεί η λειτουργία της.

Χαμηλότερο κόστος για server refreshing. Με την εμφάνιση του virtualization, η Microsoft έχει αλλάξει την πολιτική των αδειών π.χ. με κάθε Server 2003 παίρνεις επιπλέον virtual licenses (4 άδειες). Έτσι κάθε φορά που επιβάλλεται να προσθέσουμε ένα server, να αντικαταστήσουμε ένα server, να αναβαθμίσουμε ένα server, χρειαζόμαστε μικρότερο προϋπολογισμό αφού δεν θα φρεσκάρουμε πολλούς physical servers (μοιραζόμαστε το ίδιο hardware).

Μια ακόμα σημαντική παράμετρος του virtualization, είναι η λήψη **snapshots**. Η λειτουργία αυτή είναι σημαντική, διότι πατώντας ένα κουμπί παγώνουμε τον server την συγκεκριμένη χρονική στιγμή. Αν αργότερα αντιμετωπίσουμε κάποιο πρόβλημα και θελήσουμε να επιστρέψουμε σε αυτήν την

κατάσταση μπορούμε πολύ εύκολα. Όταν ο μηχανισμός snapshot είναι ενεργοποιημένος, τότε το όλο σύστημα δουλεύει πιο αργά. Snapshot μπορούμε να πάρουμε σε μια ή περισσότερες εικονικές μηχανές (ένα snapshot σε κάθε εικονική μηχανή) ή αν πρόκειται για team να πάρουμε το snapshot του team (ένα snapshot ανεξάρτητα από τον αριθμό των εικονικών μηχανών που έχει το team). Το πόσο μεγάλο πλεονέκτημα είναι το καταλαβαίνουμε σε περιπτώσεις που έχουμε κατάρρευση τους συστήματος και χρειαστούμε να κάνουμε disaster recovery.

7.11 Λογισμικό Server Virtualization

Μεγάλοι κατασκευαστές αναπτύσσουν λογισμικό Virtualization. Μερικοί παρατίθενται στην ακόλουθη λίστα:

1. VMware (http://www.vmware.com)
2. Microsoft (http://www.microsoft.com)
3. Citrix Systems (http://www.citrix.com)
4. XenSource (http://www.xensource.com)
5. Virtual Iron (http://www.virtualiron.com)
6. Parallels (http://www.parallels.com)
7. Sun Microsystems (http://www.sun.com/)
8. InnoTek (http://www.virtualbox.org)
9. Amazon EC2 (http://aws.amazon.com/ec2)

Οι πιο σημαντικοί από τους παραπάνω κατασκευαστές στο χώρο του Virtualization, σύμφωνα και με το μερίδιό τους στην αγορά, είναι η Microsoft με το λογισμικό πακέτο «Microsoft Virtual Server» και η VMware με την πλατφόρμα Virtualization «ESX Server». Ωστόσο, παγκόσμιος ηγέτης στο χώρο του x86 Virtualization τα τελευταία 10 χρόνια παραμένει η VMware.

7.12 Επίλογος

Η εικονοποίηση των συστημάτων είναι μια τεχνολογία που εξελίσσεται ραγδαία και όπως είδαμε προηγουμένως προσφέρει πολλές εναλλακτικές εφαρμογές. Αλλά δεν πρέπει να αντιμετωπίζεται σαν το χρυσό χάπι που θα λύσει όλα τα προβλήματα. Οι περιορισμοί στο υλικό που θα χρησιμοποιηθεί είναι μεγάλοι, κυρίως όσον αφορά τη RAM. Από την άλλη σίγουρα μπορεί να δώσει λύσεις που έχουν να κάνουν με την αυτοματοποίηση την καλύτερη αποδοτικότητα του συστήματος και την εξοικονόμηση πολλών χρημάτων, για αυτό και μεγάλες εταιρίες πληροφορικής κάνουν μεγάλο αγώνα ανάπτυξης του, όχι μόνο για τον μεταξύ τους επιχειρηματικό ανταγωνισμό, αλλά και για τα δικά τους οφέλη από αυτή την τεχνολογία.

Κεφάλαιο 8

Ανάλυση Κινδύνων & Σχέδιο Συνέχισης Λειτουργίας

8.1 Εισαγωγή

Η **ανάλυση κινδύνων (risk analysis)**, η οποία είναι ένα εργαλείο για την συνολικότερη διαχείριση κινδύνων, είναι μια μέθοδος που αναγνωρίζει τις αδυναμίες και τους κινδύνους που διατρέχει μια εταιρία, υπολογίζει την πιθανή ζημιά και δείχνει σε ποιους τομείς πρέπει να δοθεί βάρος στην ασφάλεια. Η ανάλυση κίνδυνων χρησιμοποιείται για διασφαλίσει ότι η ασφάλεια, που δημιουργήσαμε, είναι ανταποκρίνεται στα χρήματα που επενδύσαμε, είναι συναφή με το αντικείμενο και ανταποκρίνεται στους κινδύνους.

Η υπόθεση της ασφάλειας δεν είναι εύκολο πράγμα, ακόμα και για τους πιο πεπειραμένους και είναι εύκολο να χρησιμοποιήσουμε «πολλή» ασφάλεια ξοδεύοντας περιττά χρήματα ή ανεπαρκή, χωρίς ουσιαστικά να εξυπηρετεί τον στόχο μας. Η ανάλυση του ρίσκου ή των πιθανών κινδύνων βοηθάει τις εταιρίες να ιεραρχήσουν τους πιθανούς κινδύνους με βάση την αξία των δικών τους περιουσιακών στοιχείων και να υπολογίσουν το κόστος για την πραγματοποίηση ενός σχεδίου αποφυγής αυτών.

Παράλληλα, ο στόχος της **ανάνηψης συστήματος (System redundancy)** από καταστροφή είναι να ελαττώσει τις συνέπειες μιας καταστροφής και να πάρει τα απαραίτητα μέτρα ώστε να εξασφαλίσει ότι οι εγκαταστάσεις, το προσωπικό και η παραγωγική διαδικασία είναι ικανά να επανέλθουν σε λειτουργία σε ένα συγκεκριμένο χρονικό διάστημα. Διαφέρει από το **σχέδιο συνέχισης της λειτουργίας (Business Continuation plan)**, που περιλαμβάνει μεθόδους και διαδικασίες με τις οποίες θα πρέπει να αντιμετωπίσουμε ένα ενδεχόμενο μεγάλης διακοπής ή καταστροφής. [3]

Κάθε εταιρία έχει τη δική της ομάδα ανάλυσης κινδύνων, προσαρμοσμένη στη δική της λειτουργία, τις πηγές και τους στόχους. Για να είναι πιο αποτελεσματική μια ομάδα τέτοια, πρέπει να περιλαμβάνει άτομα, που να εργάζονται σε όλα τμήματά της, για να διασφαλίσει ότι όλες οι παράμετροι θα ληφθούν υπόψη και θα εξεταστούν.

8.2 Στόχοι της ανάλυσης κινδύνου

Οι στόχοι της ανάλυσης κινδύνων είναι τέσσερις:

- Αναγνώριση των περιουσιακών στοιχείων και της αξίας τους
- Αναγνώριση των αδυναμιών και των απειλών
- Ποσοτικοποίηση της πιθανότητας και του αντίκτυπου για την εταιρία από αυτούς τους κινδύνους.
- Παροχή ενός οικονομικού σχεδίου ισορροπημένου μεταξύ του αντίκτυπου του κινδύνου και του κόστους των μέτρων ασφαλείας [3]

8.3 Η διαδικασία της ανάλυσης κινδύνου

Για τη διαδικασία της ανάλυσης κινδύνων έχουν αναπτυχθεί πολλές τεχνικές από ειδικούς και η κάθε μια έχει τη χρησιμότητά της. Το σημαντικό σε όλη την υπόθεση είναι να μπορούμε να πραγματοποιήσουμε μια πλήρη καταγραφή όλων των πιθανών κινδύνων, χωρίς παραλείψεις, και να συντάξουμε ένα σαφές και κατανοητό σχέδιο αντιμετώπισης του.

Πρώτα, προσδιορίζουμε τον κίνδυνο δίνοντας ένα ορισμό τον οποία ένας τρίτος μπορεί να καταλάβει. Δεύτερον, προσδιορίζουμε την πιθανότητα να συμβεί, δημιουργώντας μια κλίμακα πιθανοτήτων. Τρίτον, προσδιορίζουμε τη σοβαρότητα του κινδύνου σε περίπτωση που συμβεί. Και εδώ δημιουργούμε μια αντίστοιχη κλίμακα. Όταν έχουμε ξεκαθαρισμένο την πιθανότητα και τη σοβαρότητα του κινδύνου μπορούμε να συνδυάσουμε αυτές τις δύο διαδικασίες. Τέταρτον,

προσδιορίζουμε την ημερομηνία που πρέπει να μετριάσουμε των κίνδυνο ή την πλήρους χειραγώγησής του.

Στη συνέχεια αναλαμβάνει το σχέδιο ανάνηψης συστήματος και το σχέδιο συνέχισης της λειτουργίας της εταιρίας, ώστε να περιγραφεί η διαδικασία επαναλειτουργίας.

Για την πιθανότητα να συμβεί η κλίμακα που θα χρησιμοποιήσουμε είναι:

Εξαιρετικά πιθανό

Πολύ πιθανό

Πιθανό

Σχετικά πιθανό

Απίθανο

Η κλίμακα για την σοβαρότητα του κινδύνου είναι η εξής:

Βαθμός 9 - 10	κρίσιμη ζημιά
Βαθμός 6 – 8	σοβαρή ζημιά
Βαθμός 3 – 5	μέτρια ζημιά
Βαθμός 1 – 2	μικρή ζημιά

8.4 Παράμετροι υπολογισμού του κόστους

Όλα τα περιουσιακά στοιχεία της εταιρίας έχουν ποσοτική και ποιοτική αξία που πρέπει να υπολογιστεί, αλλά και να διαχωριστεί. Το πραγματικό κόστος ενός περιουσιακού στοιχείου είναι η απόκτηση του, η ανάπτυξη του και η συντήρηση του. Η αξία του διαμορφώνεται από το πόσο σημαντικό είναι για τους χρήστες, τους ιδιοκτήτες του και τους μη εξουσιοδοτημένους χρήστες. Οι παρακάτω κανόνες πρέπει να λαμβάνονται υπόψη όταν υπολογίζουμε την αξία των περιουσιακών στοιχείων: [3]

- Το κόστος για την απόκτηση και ανάπτυξη του περιουσιακού στοιχείου
- Κόστος συντήρησης και προστασίας
- Αξία για τους ιδιοκτήτες και αυτούς που θα το χρησιμοποιήσουν
- Αξία για τους αντίπαλους της εταιρίας

- Αξία των πνευματικών δικαιωμάτων
- Η τιμή που έχει αν είναι προς πώληση
- Κόστος αντικατάστασής του
- Την επίδραση που θα έχει αν δεν είναι άμεσα διαθέσιμο στη λειτουργία της εταιρίας
- Από την χρησιμότητα και τον ρόλο που παίζει για την εταιρία

8.5 Ανάλυση για την εταιρία

Με βάση τα παραπάνω, μπορούμε να προχωρήσουμε στην ανάλυση των κινδύνων, που πιθανά θα αντιμετωπίσουμε στην εταιρία. Καταρχήν κάνουμε ένα πίνακα με τα είδη των κινδύνων που μπορεί να αντιμετωπίσουμε, τι μπορεί να αποτελεί αδυναμία μας, που να τους επιτρέψει την εμφάνιση και τι μπορεί να προκαλέσει η ύπαρξη τους.

Είδος κινδύνων	Τι μπορεί να τον προκαλέσει	Αποτέλεσμα αυτού του κινδύνου
Ιός	Έλλειψη αντιικού λογισμικού	Προσβολή από ιό
Χάκερ	Υπηρεσίες που τρέχουν στους server	Μη εξουσιοδοτημένη πρόσβαση σε εμπιστευτικές πληροφορίες
Χρήστες	Παρερμηνεία των παραμέτρων του λειτουργικού συστήματος	Δυσλειτουργία του συστήματος
Πυρκαγιά	Έλλειψη συστημάτων πυρόσβεσης	Πιθανή απώλεια ανθρώπινης ζωής και κτιριακή και υπολογιστική καταστροφή
Εργαζόμενοι	Έλλειψη εκπαίδευσης ή έλλειψη επιτήρησης	Μοίρασμα εμπιστευτικών πληροφοριών, χρησιμοποίηση επικινδύνων προγραμμάτων
Εργολάβος συστημάτων	Έλλειψη μηχανισμών ελέγχου	Κλοπή εμπορευμάτων

ασφαλείας		
Εισβολέας στο σύστημα	Αδύναμα firewalls	Buffer overflow Denial of service
Εισβολέας στα κτίρια	Έλλειψη φύλαξης	Είσοδος στο κτίριο και κλοπή συσκευών

8.5.1 Ανάλυση κινδύνων

8.5.1.1 Κίνδυνος 1. Ιοί στο σύστημα

Πιθανότητα να συμβεί: εξαιρετικά πιθανό

Σοβαρότητα αποτελέσματος: 5 (μέτρια ζημιά)

Για την αντιμετώπιση των ιών χρειάζεται να είμαστε καταρχήν εξοπλισμένοι με ενημερωμένα antivirus στους υπολογιστές. Όπου έχουμε προσβολή από ιό τότε πραγματοποιούμε scan με το antivirus. Αν το πρόβλημα συνεχίσει δοκιμάζουμε να καθαρίσουμε με ένα Live cd που θα έχει ενημερωμένα περισσότερα antivirus και malware προγράμματα. Αν το Live cd δεν μπορεί να ανταποκριθεί, αφαιρούμε τον σκληρό δίσκο και τον πηγαίνουμε στο τμήμα τεχνικής υποστήριξης όπου και από εκεί μπορούν να αξιοποιηθούν οι τελευταίες ενημερώσεις των προγραμμάτων μας. Ο χρόνος αντιμετώπισης κυμαίνεται από μία έως 3 ώρες, ανάλογα και με τον όγκο των δεδομένων που πρέπει να σαρωθούν.

8.5.1.2 Κίνδυνος 2. Εισβολείς – Hacker

Πιθανότητα να συμβεί: Πιθανό

Σοβαρότητα αποτελέσματος: 8 έως 10

Όταν αναφερόμαστε σε εισβολέα, αναφερόμαστε σε πρώτα και κύρια σε ανθρώπινη δραστηριότητα. Αυτό είναι σημαντικό στοιχείο για να κατανοήσουμε το πόσο σημαντικό είναι να μην πάθουμε αυτή τη ζημιά. Σε περίπτωση εισβολέα στο σύστημα αν είναι στο τοπικό δίκτυο σημαίνει ότι βρίσκεται πιθανά και εντός του κτιρίου της εταιρίας, σύμφωνα με τους κανόνες ασφαλείας, που έχουμε θέσει. Επομένως χρειάζεται άμεσος εντοπισμός του από τους πόρους που χρησιμοποιεί

για την επίθεση, ώστε να προσδιοριστεί και η θέση του. Σε περίπτωση που ο εισβολέας επιτεθεί από το διαδίκτυο, πρέπει οι διαχειριστές τους συστήματος να είναι πάντα σε εγρήγορση να τον προσδιορίσουν και να τον απομονώσουν. Συνήθως μόλις εντοπιστεί ο εισβολέας παραιτείται και από την προσπάθεια. Ο χρόνος που θα χρειαστούμε για να επανέλθουμε από αυτό τον κίνδυνο είναι ανάλογος με την επιμονή και τα κίνητρα του εισβολέα και την ζημιά που μπορεί να προκαλέσει.

8.5.1.3 Κίνδυνος 3. Πυρκαγιά

Πιθανότητα να συμβεί: Σχετικά πιθανό

Σοβαρότητα αποτελέσματος: 9 έως 10

Σε περίπτωση πυρκαγιάς αν αυτή είναι περιορισμένη πρέπει το προσωπικό να είναι εκπαιδευμένο στην αντιμετώπισή της, με τη χρήση των πυροσβεστήρων που υπάρχουν σε όλους τους χώρους του κτιρίου. Σε περίπτωση που η πυρκαγιά είναι εκτεταμένη πρέπει να γίνει άμεση εκκένωση του κτιρίου της εταιρίας για τη αποφυγή ανθρώπινης απώλειας και να γίνει κλήση στην πυροσβεστική. Για το λόγο αυτό χρειάζεται και συχνός έλεγχος του συστήματος αυτόματης πυρόσβεσης για να είμαστε σίγουροι ότι θα λειτουργήσει όταν θα το χρειαστούμε. Η ανάκαμψη από μια τέτοια ζημιά είναι ανάλογη της καταστροφής που μπορεί να επέλθει. Αν η πυρκαγιά είναι περιορισμένη η ζημιά μπορεί να είναι κάποια μηχανήματα τα οποία εύκολα μπορούν να αντικατασταθούν και να εξοπλιστούν από τα αντίγραφα ασφαλείας που κρατάμε. Σε περίπτωση, όμως μεγάλης πυρκαγιάς μπορεί να έχουμε ολοκληρωτική καταστροφή και να διακοπεί η λειτουργία της εταιρίας για μέρες.

8.5.1.4 Κίνδυνος 4. Πλημύρα

Πιθανότητα να συμβεί: Σχετικά πιθανό

Σοβαρότητα αποτελέσματος: 2 έως 5

Η περίπτωση πλημύρας έχει να κάνει με τη στεγανότητα και την καλή συντήρηση του κτιρίου κυρίως στη στέγη. Όταν αντιληφθούμε την ύπαρξη νερών

αμέσως απομακρύνουμε από εκείνο το μέρος οποιαδήποτε ηλεκτρική συσκευή υπάρχει κοντά. Αν αυτό δεν είναι δυνατό τότε κατεβάζουμε τις κατάλληλες ασφάλειες από τον ηλεκτρολογικό πίνακα. Στη συνέχεια φροντίζουμε με οποιοδήποτε μέσο να περιορίσουμε τη διασπορά των νερών και τέλος καλούμε την τεχνική εταιρία να κλείσει τις εισόδους του νερού.

8.5.1.5 Κίνδυνος 5. Σεισμός

Πιθανότητα να συμβεί: Σχετικά πιθανό

Σοβαρότητα αποτελέσματος: 2 έως 6

Η Ελλάδα είναι μια σεισμογενής χώρα με μεγάλο ιστορικό σε πολλές περιοχές της. Η αντιμετώπιση ενός σεισμού έχει να κάνει πρώτα και κύρια με την αντισεισμική θωράκιση του κτιρίου. Από εκεί και ύστερα όταν γίνει σεισμός, λαμβάνουμε τα απαραίτητα μέτρα προστασίας κατά τη διάρκειά του και στη συνέχεια εκκενώνουμε το κτίριο για να μην έχουμε τραυματισμό ανθρώπων. Οι υλικές ζημιές δεν θα είναι εκτεταμένες εφόσον έχουμε πάρει όλα τα μέτρα ασφαλείας που απαιτούνται. Ο χρόνος ανάκαμψης είναι ανάλογος με τη ζημιά που θα προκληθεί.

8.5.1.6 Κίνδυνος 6. Διακοπή ρεύματος – black out

Πιθανότητα να συμβεί: Πιθανό

Σοβαρότητα αποτελέσματος: 2

Μια διακοπή ρεύματος όταν συμβεί δεν έχει σημαντικές επιπτώσεις στο σύστημα. Αν αυτή προέρχεται από την εταιρία παροχής ρεύματος, τότε η βλάβη δεν θα διαρκέσει παρά μόνο λίγες ώρες και αυτό θα έχει ως συνέπεια τη διακοπή της λειτουργίας της εταιρίας για εκείνο το χρονικό διάστημα. Σε περίπτωση που η διακοπεί προκληθεί από εσωτερικό παράγοντα τότε πρέπει να αναλάβει αμέσως η ομάδα ηλεκτρολογικού της εταιρίας για την άμεση αποκατάσταση . το κόστος σε αυτή την περίπτωση δεν είναι υψηλό αφού στη χειρότερη περίπτωση θα χρειαστούμε κάποια αλλαγή του ηλεκτρολογικού υλικού.

8.5.1.7 Κίνδυνος 7. Υπάλληλοι της εταιρίας

Πιθανότητα να συμβεί: Εξαιρετικά πιθανό

Σοβαρότητα αποτελέσματος: 5 έως 10

Οι υπάλληλοι της εταιρίας είναι ένας σημαντικός παράγοντας δημιουργίας κινδύνων. Η ζημιά που μπορεί να προκαλέσουν ποικίλει από το εάν έχουν πρόθεση (σαμποτάζ) ή όχι. Αν συμβεί κάποια ενέργεια τους που προκαλέσει δυσλειτουργία τότε οι διαχειριστές πρέπει να αναλάβουν την άμεση εξομάλυνση του συστήματος. Αν έχουμε απώλεια δεδομένων πρέπει να επαναφέρουμε τα δεδομένα από τα αντίγραφα ασφαλείας που κρατάμε. Πιθανή χρονική διάρκεια είναι οι 2 ώρες. Αν έχουμε ανεπιθύμητη χρήση και προσπάθεια μη εξουσιοδοτημένης πρόσβασης πρέπει άμεσα οι διαχειριστές να εντοπίσουν σε ποιο σημείο πάει να γίνει η παραβίαση και να επέμβουν αμέσως.

8.5.1.8 Κίνδυνος 8. Διάρρηξη

Πιθανότητα να συμβεί: Σχετικά πιθανό

Σοβαρότητα αποτελέσματος: 3 έως 8

Η διάρρηξη έχει να κάνει και αυτή με ανθρώπινη δραστηριότητα και ποικίλει ανάλογα με τα κίνητρα του διαρρήκτη. Σε περίπτωση που συμβεί, πρέπει άμεσα να γίνει κλήση στην αστυνομία από τους φύλακες ή όποιον την αντιληφθεί. Στη συνέχεια, πρέπει να γίνει καταγραφή από την εταιρία ποιες ήταν οι επιπτώσεις μιας διάρρηξης και τι συνέπειες έχει στη λειτουργία της. Ανάλογα με τις συνέπειες και το πόσο κατάφερε να διεισδύσει ο διαρρήκτης και σε ποιο ποσοστό πέτυχε το στόχο του, θα εξαρτηθεί και ο χρόνος, με τον οποίο θα επανέλθει η κανονική λειτουργία της εταιρίας.

8.5.1.9 Κίνδυνος 9. Επιδημίες

Πιθανότητα να συμβεί: Πολύ πιθανό

Σοβαρότητα αποτελέσματος: 2 έως 6

Οι επιδημίες και γενικότερα οι αρρώστιες προσβάλουν το προσωπικό. Σε περιπτώσεις έξαρσης ιώσεων υπάρχει πιθανότητα ένα μεγάλο μέρος του

εργατικού δυναμικού της εταιρίας να προσβληθεί και καταστεί αδύνατο να εργαστεί για ένα χρονικό διάστημα μερικών ημερών. Σε αυτή την περίπτωση η εταιρία πρέπει να έχει πάρει τα μέτρα της ώστε η δουλειά που ήταν να γίνει από τους εργαζόμενους που λείπουν να μπορέσει να βγει από το υπόλοιπο προσωπικό στο βαθμό, που από τη μία θα περιορίσει όσο μπορεί την απώλεια της δουλειάς και από την άλλη να μην πέσει το βάρος όλο στους υπόλοιπους εργαζόμενους.

8.5.2 Μελέτη περιπτώσεων

Η κάθε περίπτωση κινδύνου μπορεί να εξεταστεί ξεχωριστά ανάλογα και με τα περιουσιακά στοιχεί που προσβάλει. Πάντα ακολουθούμε συγκεκριμένα βήματα για το πώς κινούμαστε.

8.5.2.1 Περίπτωση 1. Το τοπικό δίκτυο

Το τοπικό δίκτυο είναι η καρδιά της εταιρίας και περιλαμβάνει τα κρίσιμα αρχεία, που διαχειρίζονται οι χρήστες. Πάνω σε αυτό δουλεύουν πολλές ώρες εργαζόμενοι και μέσα από αυτό εξελίσσονται τα προϊόντα τα οποία η εταιρία διαθέτει στη αγορά.

Το τοπικό δίκτυο περιλαμβάνει το υλικό μέρος του δικτύου μας. Είναι οι υπολογιστές, τα καλώδια, οι router, τα switches. Αν κάποιο από αυτά δεν λειτουργεί έχουμε τη δυνατότητα άμεσης αντικατάστασης του με ένα καινούργιο και επαναλειτουργία του συστήματος. Γενικά δεν επιβαρύνει σημαντικά τον προϋπολογισμό της εταιρίας, αφού ένας μέσος καλός υπολογιστής έχει κόστος 700 ευρώ.

Κίνδυνος, όμως μπορεί να δημιουργηθεί και από τα μέσα. Υπάρχει η πιθανότητα λανθασμένου χειρισμού κάποιου εργαζόμενου, είτε άθελα , είτε με σκοπιμότητα. Με αυτό τον τρόπο ίσως να κινδυνέψει η ακεραιότητα των δεδομένων και ολόκληρου του δικτύου της εταιρία.

Άρα τα μέτρα που παίρνουμε για την προστασία είναι:

1) Να υπάρχει κανονισμός με τη σωστή χρήση και συντήρηση των μηχανημάτων, καθαριότητα των υπολογιστών από σκόνες, τοποθέτηση σε σημεία που δεν θα κινδυνεύουν με χτύπημα τα tower boxes, η καλωδίωση να είναι εσωτερική για μεγαλύτερη προστασία.
2) Οι εργαζόμενοι να εκπαιδεύονται για ένα διάστημα μόλις προσλαμβάνονται, πάνω στα συστήματα που χρησιμοποιεί η εταιρία.
3) Να είναι απόλυτα καθορισμένοι οι ρόλοι και τα δικαιώματα του κάθε εργαζόμενου στην επιχείρηση, από τον ανώτερο μέχρι τον απλό υπάλληλο, ώστε να μην επιδέχονται παρερμηνείες.
4) Οι συνθήκες περιβάλλοντος να είναι κατάλληλες. Να μην έχει πολύ υγρασία ούτε ζέστη.
5) Τα towers να είναι κλειδωμένα με λουκέτο μέσα σε ειδικές θήκες
6) Να υπάρχουν πάντα εφεδρικοί υπολογιστές, routers, switches και καλώδια έτσι ώστε σε απώλεια κάποιου να μπορούν άμεσα να αντικατασταθούν.
7) Εφοδιασμός με antivirus προγράμματα και συνεχής ενημέρωση αυτών.

8.5.2.2 Περίπτωση 2. Οι Server

Οι file servers είναι από τα ποιο σημαντικά στοιχεία του τοπικού δικτύου για αυτό και τους εξετάζουμε ξεχωριστά από το υπόλοιπο υλικό.

Με αυτούς γίνεται η κεντρική διαχείριση του δικτύου, από αυτούς καθορίζονται τα δικαιώματα των χρηστών όλων των κατηγοριών μέσα στο δίκτυο και από αυτούς γίνεται η διαχείριση του συστήματος. Η πιο σημαντική πηγή κινδύνου για αυτούς είναι η υλική καταστροφή και η πρόσβαση μέσω του δικτύου από μη εξουσιοδοτημένα άτομα, με σκοπό την κλοπή ή την αλλοίωση των δεδομένων. Οπότε για τους Servers πρέπει να προβλέψουμε:

1) Την αλληλένδετη και συμπληρωματική λειτουργία τους, ώστε αν ο ένας «πέσει» για τον οποιοδήποτε λόγο, ο άλλος να αναλαμβάνει όλη τη δουλειά, χωρίς οι χρήστες να καταλαβαίνουν κάποιο πρόβλημα
2) Η εγκατάσταση antivirus

3) Την συνεχή παρουσία των διαχειριστών του δικτύου μέσα στο server room.

4) Την παρακολούθηση του server room από CCTV και συστήματα IDS

5) Λήψη αντιγράφων εικόνας του συστήματος μια συγκεκριμένη στιγμή και πάντα όταν έχουμε επιθυμητή λειτουργία. Έτσι σε περίπτωση δυσλειτουργίας να μπορούμε άμεσα να τον αντικαταστήσουμε και να μη χάσουμε χρόνο από την διαμόρφωση του.

8.5.2.3 Περίπτωση 3. Το NAS

Είναι το μέρος που αποθηκεύονται όλα τα δεδομένα, που δημιουργούνται και διακινούνται μέσα στην εταιρία. Αυτά τα δεδομένα μπορεί να είναι απλές αναφορές, αλλά και διαβαθμισμένα έγγραφα μεγάλης κρισιμότητας. είναι η βασική αποθηκευτική μονάδα και πρέπει να επιβλέπεται ιδιαίτερα. Το πλεονέκτημα είναι ότι βρίσκεται στο ίδιο δωμάτιο με τους Servers και ότι ισχύει για αυτούς περιλαμβάνει και αυτό. Από την άλλη ένα NAS είναι πολύ πιο ευαίσθητο στην συνεχή χρήση και μπορεί να χαλάσει πιο εύκολα. Το κόστος του NAS, που επιλέξαμε είναι 1000 ευρώ περίπου. Η εταιρία πρέπει καταρχήν να έχει ένα εφεδρικό για την περίπτωση που έχουμε ολική ζημιά, μια και είναι ίσως το πιο σημαντικό μηχάνημά μας. Επίσης τους σκληρούς δίσκους τους έχουμε σε συστοιχία RAID 5 για μεγαλύτερη ανοχή σε σφάλματα, αφού και ένας δίσκος να πέσει, το σύστημα λειτουργεί με τους άλλους 4 και μπορεί εύκολα να αντικατασταθεί ο κατεστραμμένος.

8.5.2.4 Περίπτωση 4. Το Backup PC

Το Backup PC αποτελεί την τρίτη περίπτωση περιουσιακού στοιχείου, που η σημαντικότητά του για την εταιρία, είναι αντίστοιχη με τους Server και το NAS. Και σε αυτή την περίπτωση έχουμε το πλεονέκτημα ότι στεγάζεται με τους υπόλοιπους Servers. Το Backup PC, όμως είναι το τελευταίο προπύργιο μαζί με τους αποσπώμενους δίσκους, σε περίπτωση που πάθουμε σημαντική ζημιά στους Server και το NAS, με το οποίο θα μπορέσουμε να επαναφέρουμε το σύστημα. Οι

αποσπώμενοι δίσκοι αποτελούν ταυτόχρονα και ένα πρόσθετο μέτρο ενάντια στους κινδύνους που αναφέραμε πιο πριν.

8.5.2.5 Περίπτωση 5. Web, SMTP, Proxy Server

Οι Servers αυτοί αποτελούν ένα ξεχωριστό περιουσιακό στοιχείο, αφού είναι και διαχωρισμένοι από το υπόλοιπο δίκτυο τη εταιρίας. Εκεί έχουμε ρίξει το βάρος της επικοινωνίας με τους πελάτες της εταιρίας και σε ένα μεγάλο βαθμό την προβολή και προώθηση των προϊόντων μας. Το διαδίκτυο δεν έχει τόση μεγάλη πληροφοριακή αξία όσο το τοπικό δίκτυο αφού εκεί δεν χρειάζεται να αποθηκεύσουμε στοιχεία απαραίτητα για τη λειτουργία της εταιρίας. Ούτε αν έχουμε καταστροφή ή κάποια βλάβη θα σταματήσει η συνολική παραγωγική διαδικασία. Θα έχει όμως μεγαλύτερο αντίκτυπο στο προφίλ απέναντι στο κοινό και στο γόητρο της.

Από υλικής άποψης, οι απαιτήσεις κινούνται σε φυσιολογικά επίπεδα, εφόσον δεν χρειάζεται να έχουμε ιδιαίτερα ακριβά μηχανήματα, μιας και αυτή τη δουλειά μπορούν να την πραγματοποιήσουν απλοί υπολογιστές.

Άρα τα μέτρα που πρέπει να πάρουμε είναι:

1) Λήψη αντιγράφων ασφαλείας στον Web και τον SMTP Server.
2) Εφεδρικά pc για άμεση αντικατάσταση σε περίπτωση μηχανικής βλάβης.
3) Αξιοποίηση του Virtualization σαν τρόπο εξοικονόμησης χρημάτων και χρόνου αποκατάσταση. Μπορούμε να έχουμε έτοιμο σαν εφεδρεία ένα δυνατό μηχάνημα που θα τρέχει 3 εικονικές μηχανές για τους Servers. Έτσι σε περίπτωση ολικής καταστροφής θα έχουμε τη δυνατότητα άμεσης ανάνηψης του συστήματος.
4) Εφοδιασμός με antivirus προγράμματα
5) Συνεχής παρακολούθηση από τους διαχειριστές

8.5.2.6 Περίπτωση 6. Control Room

Το Control Room θα μπορούσε να χαρακτηριστεί το κέντρο ασφάλειας της εταιρίας. Από εδώ, αυτός που έχει πρόσβαση αποκτάει ταυτόχρονα και την δυνατότητα να επεξεργάζεται όλη τη φυσική, την περιμετρική ασφάλεια και τους ελέγχους πρόσβασης της εταιρίας. Είναι από τους πιο κρίσιμους στόχους για την συνολική ασφάλεια και όχι μόνο για ένα συγκεκριμένο περιουσιακό στοιχείο. Επίσης η αξία εγκατάστασης ενός τέτοιου κέντρου είναι και χρονοβόρα αλλά και δαπανηρή και απαιτεί ειδικευμένο προσωπικό. Η καταστροφή ή η δυσλειτουργία του θα αφήσει γυμνή από θέμα εξωτερικής επίθεσης την εταιρία για μεγάλο χρονικό διάστημα, αφού η επισκευή και επαναλειτουργία ενός τέτοιου συστήματος είναι εξαιρετικά δύσκολο να γίνει άμεσα από το προσωπικό που εργάζεται εκεί. Από τη στιγμή που κάποιος αποκτήσει τον έλεγχο του control room ή καταφέρει να το θέσει σε μη λειτουργία, τότε η ζημιά που μπορεί να προκαλέσει εξαρτάται πλέον από τις προθέσεις του και δεν μπορεί να υπολογιστεί.

Επομένως η εξασφάλιση ότι αυτό θα δουλεύει ανά πάσα στιγμή , είναι το μεγάλο στοίχημα του σχεδίου ασφαλείας. Τα μέτρα προστασίας που παίρνουμε είναι συνδυασμένα με την φυσική ασφάλεια του κτιρίου. Πυροπροστασία, έλεγχος πλημυρών και καπνού είναι από τα απαραίτητα αισθητήρια που πρέπει να υπάρχουν μέσα στο δωμάτιο. Έλεγχοι πρόσβασης με την αυστηρότερό δυνατό έλεγχο. Εξειδικευμένο προσωπικό που να εκπαιδεύεται συχνά. Επίσης, ένα καλό μέτρο θα ήταν η συμφωνία με την εταιρία που εγκατέστησε το σύστημα ασφαλείας, να έχει πάντα διαθέσιμο προσωπικό, το οποίο θα χρειαστεί να επέμβει άμεσα για να διορθώσει μια πιθανή βλάβη. Επίσης σύμφωνα με την ιεραρχία των περιουσιακών στοιχείων, στο δωμάτιο με τους server και στην αίθουσα παραγωγής θα πρέπει άμεσα να βρεθεί το προσωπικό φύλαξης για όσο χρονικό διάστημα χρειαστεί να έρθει η αστυνομία, ή το συνεργείο επιδιόρθωσης.

8.5.2.7 Περίπτωση 7. Οι εγκαταστάσεις

Οι εγκαταστάσεις της εταιρίας αποτελούν ένα σύνθετο περιουσιακό στοιχείο ως προς την αξία που έχει για την αυτή.

Πρώτον, από μόνες τους είναι ένα σημαντικό περιουσιακό στοιχείο. Το κτίριο, οι φράχτες, το υλικό που υπάρχει μέσα είναι η μεγαλύτερη χρηματική επένδυση της εταιρίας. Βέβαια αυτή η αξία είναι σταθερή και πιο σπάνια μεταβάλλεται, όπως αυτή του προϊόντος, δεν παύει να έχει όμως τεράστιο κόστος για την εταιρία.

Δεύτερον, οι κτιριακές εγκαταστάσεις είναι ταυτόχρονα και ένα μέτρο προστασίας των υπόλοιπων περιουσιακών στοιχείων, που βρίσκονται μέσα σε αυτές. Επομένως η πραγματική τους αξία είναι πιο μεγάλη και πιο περίπλοκη.

Κίνδυνοι, όπως οι πλημύρες, οι πυρκαγιές και οι βανδαλισμοί μπορεί να εκτινάξουν το κόστος μιας ζημιάς σε τεράστια μεγέθη. Το θέμα διαρρηκτών, που αναφέρθηκε και στην περίπτωση 7, είναι ένα άλλο σημαντικό ζήτημα και έχει να κάνει με τους σκοπούς του καθενός. Για την εταιρία, οι βασικοί στόχοι, που θα μπορούσε κάποιος να έχει κέρδος είναι ο τομέας παραγωγής και το δίκτυο με τα αρχεία που κρατούνται εκεί. Όμως για να φτάσει κάποιος εκεί πρέπει να παραβιάσει το κτίριο. Μια τέτοια παραβίαση μπορεί να σημαίνει σημαντική καταστροφή.

Επομένως, σημαντικό είναι να πάρουμε τέτοια μέτρα, τα οποία θα λειτουργούν αποτρεπτικά για τον επίδοξο εισβολέα. Κάμερες, συναγερμοί, έλεγχοι πρόσβασης και κάθε ηλεκτρονικό μέσο είναι επιθυμητά και αυξάνουν την ικανότητα προστασίας του κτιρίου. Επιπλέον, όπως και με το control room έτσι και εδώ πρέπει να υπάρχει ένα σχέδιο άμεσης επέμβασης από ανθρώπινο δυναμικό που να εξασφαλίζει με την παρουσία του την ασφάλεια του κτιρίου μέχρι να λήξει ο συναγερμός. Η εταιρία πρέπει να είναι σε ετοιμότητα άμεσης επισκευής και αντικατάστασης ζημιών, είτε με τη βοήθεια των εταιριών που συνεργάζεται, είτε έχοντας δικό της συνεργείο τεχνικών.

8.5.2.8 Περίπτωση 8. Το ανθρώπινο δυναμικό

Το ανθρώπινο δυναμικό είναι και για ευνόητους λόγους το πιο σημαντικό περιουσιακό στοιχείο της εταιρίας. Είναι μεγάλη η ευθύνη της εταιρίας να παρέχει όλα τα μέτρα ασφαλείας που απαιτούνται ώστε να μην δημιουργηθεί κίνδυνος για τη σωματική ακεραιότητα και τη ζωή των εργαζομένων.

Το σημαντικότερο στοιχείο που πρέπει να παρθεί υπόψη από την εταιρία, είναι ότι εδώ οι δυνατότητες για ανάνηψη συστήματος είναι από ελάχιστες έως και καθόλου. Το πρώτο πράγμα που πρέπει να είναι ξεκάθαρο, είναι ότι οι άνθρωποι που εργάζονται εκεί δεν μπορούν αντιμετωπίζονται όπως τα υλικά μέρη της, δηλαδή σαν αναλώσιμα και αντικαταστάσιμα.

Οι κίνδυνοι που διατρέχει κάποιος σε ένα χώρο εργασίας, ακόμα και στο σπίτι του, είναι υπερβολικά πολλοί. Η εταιρία, όμως πρέπει να έχει πάρει από πριν όλα τα απαραίτητα μέτρα για τν αποτροπή τους.

1) Πρέπει να υπάρχουν ξεκάθαροι και σαφείς κανόνες συμπεριφοράς σε περιπτώσεις πυρκαγιάς, πλημύρας, σεισμού και γενικότερα οποιασδήποτε κατάστασης απαιτεί την εκκένωση του κτιρίου.
2) Σε εξαμηνιαία βάση θα πρέπει να γίνονται ασκήσεις ετοιμότητας και σωστής αντίδρασης στους εργαζόμενους με μέριμνα της εταιρίας.
3) Κανόνες αντίδρασης σε εξωτερική απειλή
4) Σαφείς κανόνες και μέτρα ασφαλείας σε μέρη όπως ηλεκτρικοί πίνακες, πρίζες κλπ.
5) Κατάλληλες συνθήκες εξαερισμού και θερμοκρασίας των χώρων.
6) Δημιουργία σταθερού μικρού ιατρείου
7) Ασφαλιστική κάλυψη των εργαζομένων

8.6 Επίλογος

Ανάλυση κινδύνων, η ανάνηψη συστήματος και το σχέδιο συνέχισης της λειτουργίας της επιχείρησης είναι διαδικασίες οι οποίες προϋποθέτουν μεγάλη διοικητική υποστήριξη και αυξημένη ανησυχία από το διοικητικό προσωπικό . Το συνεχώς εξελισσόμενο επιχειρηματικό περιβάλλον, η αξία της πληροφορίας, η χρήση νέων τεχνολογιών στα χέρια ανθρώπων που σκοπός τους είναι να προβάλλουν την ακεραιότητα μιας επιχείρησης, οι κλιματικές αλλαγές, καθιστούν αναγκαία την προετοιμασία της επιχείρησης για το χειρότερο δυνατό ενδεχόμενο. Είναι αναγκαία, επίσης, η προώθηση από την ίδια την δομή και τη λειτουργία της εταιρίας, μιας κουλτούρας-αντίληψης επαγρύπνησης και αλληλοβοήθειας όλων των εργαζομένων. Σε κάθε περίπτωση πάντως απαιτείται σωστός σχεδιασμός και συντονισμός όλων των εμπλεκομένων στην εταιρία.

Κεφάλαιο 9

ΕΚΤΙΜΗΣΗ ΚΟΣΤΟΥΣ

9.1 Εισαγωγή

Στο συγκεκριμένο κεφάλαιο θα κάνουμε μια όσο το δυνατόν καλύτερη και πιο εύστοχη προσέγγιση τους συνολικού κόστους πάνω στα μέτρα που αποφασίσαμε ότι θα χρησιμοποιήσουμε για την ασφάλεια της εταιρίας. Η εκτίμηση, όπως είναι προφανές, θα περιοριστεί σε αυτά τα μέτρα και όχι γενικά στα λειτουργικά έξοδα της εταιρίας. Θα δείξουμε λοιπόν ότι υπάρχει ένα εύρος τιμών που μπορεί να μας προσφέρει αυξημένη ασφάλεια ενώ ταυτόχρονα μπορεί να προσαρμόζεται και στις ανάγκες της κάθε εταιρίας, χωρίς να επιφέρει κόστος δυσανάλογο από αυτό που μπορεί να αντέξει η εταιρία.

Η εκτίμηση που θα κάνουμε, χωρίζεται σε δύο κατηγορίες. Στην φυσική και περιμετρική ασφάλεια και στο υλικό που θα χρησιμοποιηθεί για το στήσιμο του εσωτερικού δικτύου.

9.2 Εκτίμηση για την περιμετρική ασφάλεια

9.2.1 Φράχτες

Ο φράχτης της εταιρίας έχει προσαρμοσμένα πάνω του και κατά μήκος αισθητήρες κραδασμών, ενώ στο έδαφος ακριβώς δίπλα από αυτόν έχει προσαρμοστεί διαρρέον ομοαξονικό καλώδιο που δημιουργεί ένα μικρό πεδίο γύρω του. Οι αισθητήρες θα πρέπει να τοποθετηθούν σε απόσταση 5 μέτρα ο ένας από τον άλλο. Αν υποθέσουμε ότι η περίμετρος του φράχτη είναι 360 μέτρα

θα χρειαστούμε συνολικά 72 τέτοιους αισθητήρες. 72 * 14 Ε = 1008 ευρώ. Αντίστοιχα το διαρρέον ομοαξονικό καλώδιο μας κοστίζει με 4 ευρώ το μέτρο. Λόγω του ότι είναι διπλό σύρμα θα χρειαστούμε συνολικό μήκος 720 μέτρα. Άρα το κόστος του είναι 720 * 4 Ε = 2880 ευρώ.

Σύνολο 3888 ευρώ.

9.2.2 Φύλακες

Ένας φύλακας σαν φυσικό πρόσωπο και εργαζόμενος, αποτελεί ένα πάγιο έξοδο είτε το υπολογίζουμε μηνιαίως είτε σε βάθος χρόνου. Από τη στιγμή που έχουμε συνολικά 15 άτομα. Οι 9 είναι σε βάρδιες των τριών για την περίμετρο και οι 6 σε βάρδιες των 2, για το control room και το server room. Αν υποθέσουμε ότι ο μέσος μισθός τους είναι 1000 ευρώ το μήνα μιλάμε για ένα έξοδο 15.000 ευρώ μηνιαίως. **Σύνολο 15.000 ευρώ.**

9.2.3 Intrusion Detection Systems

Σύμφωνα με το σχέδιο που αναφέραμε προηγουμένως, θα τοποθετήσουμε πολλά συστήματα IDS στο χώρο της εταιρίας. Αυτά είναι οι ανιχνευτές κίνησης εξωτερικά και περιμετρικά του κτιρίου, ανιχνευτές δέσμης για την κύρια είσοδο κγια το διάδρομο του control room και ανιχνευτές σπασίματος τζαμιών που τοποθετούνται στα παράθυρα. Για την εταιρία θα χρειαστούμε:

7 αισθητήρες κίνησης εξωτερικούς. 7 * 171 Ε = 1197 ευρώ

8 αισθητήρες τζαμιών. 8 * 64 Ε = 512 ευρώ

2 ανιχνευτές δέσμης, 2 * 595 Ε = 1190 ευρώ

Σύνολο 2899 ευρώ.

9.2.4 Πυρασφάλεια

Σε κάθε δωμάτιο θα χρειαστούμε και από έναν αισθητήρα πυρκαγιάς και 2 ειδικούς ψεκαστήρες νερού από το ταβάνι. Επίσης θα πρέπει να υπάρχει και 1 πυροσβεστήρας στα δωμάτια αυτά. Στους κοινόχρηστους χώρους και διαδρόμους θα πρέπει να υπάρχουν αισθητήρες φωτιάς ανά 8 μέτρα και ανά 20 μέτρα πυροσβεστήρες. Αντίστοιχα πρέπει να υπάρχουν και σε αυτούς τους χώρους συστήματα ψεκασμού.

Επομένως σύμφωνα με μια απλή εκτίμηση θα χρειαστεί να τοποθετήσουμε 30 αισθητήρες φωτιάς, 60 ψεκαστικά μπεκ και 30 πυροσβεστήρες στους 2 ορόφους της εταιρίας. Κάτι που σημαίνει ότι θα κοστίσει:

30 * 35 E = 1.050 E

60 * 10 E = 600 E

30 * 90 E = 2.700 E

Σύνολο = 4.350 E

9.2.5 Συστήματα καταγραφής υγρασίας θερμοκρασίας

Τα συστήματα καταγραφής υγρασίας και θερμοκρασίας, που απαιτούνται είναι σαφώς λιγότερα από ότι αυτά της πυρασφάλειας. Για το σύνολο του κτιρίου θα χρειαστούμε 10 τέτοιους ανιχνευτές οι οποίοι κοστίζουν από 35 ευρώ ο καθένας. **Σύνολο 350 Ευρώ.**

9.2.6 Συστήματα καταγραφής πλημμύρας

Αισθητήρες πλημμύρας θα εγκαταστήσουμε σε αρκετά σημεία του κτιρίου και σίγουρα σε κάθε δωμάτιο. Θα χρειαστούμε περίπου 30 αισθητήρες για να καλύψουμε επαρκώς τους χώρους που θέλουμε. **Σύνολο 30 * 48 E = 1440 ευρώ.**

9.2.7 Σύστημα ψηφιακής καταγραφής – κάμερες

Οι κάμερες είναι αυτές που βοηθούν κυρίως στην παρακολούθηση και επόπτευση των κοινόχρηστων χώρων, αφού η χρήση τους δεν επιτρέπεται σε χώρους που εργάζονται άνθρωποι. Έχουμε ξεχωρίσει τις περιπτώσεις για το που θα χρησιμοποιηθούν οι διάφοροι τύποι καμερών. Θα χρειαστούμε:

8 κάμερες σταθερής εστίασης για την εξωτερική περίφραξη. 8 * 37 E = 296 ευρώ.

2 κάμερες μεταβλητής εστίασης για την κεντρική πύλη της περίφραξης.

2 * 77 E = 144 ευρώ.

5 κάμερες μεταβλητής εστίασης εξωτερικά του κυρίως κτιρίου. 5 * 53 E = 265 ευρώ.

1 κάμερα μεταβλητής εστίασης για τον διάδρομο που οδηγεί στο control room και στο server room. 1 * 74 E = 74 ευρώ.

5 περιστροφικές κάμερες ταβανιού για τον εκθεσιακό χώρο και για τους κοινόχρηστους χώρους. 5 * 24 E = 120 ευρώ.

Σύνολο 899 ευρώ.

9.2.8 Smart Cards

Οι έξυπνες κάρτες θα χρησιμοποιηθούν στις εισόδους των δωματίων για τον έλεγχο της πρόσβασης και την καλύτερη παρακολούθηση της κίνησης σε αυτά. Εμεί για την εταιρία χρειαζόμαστε: 10 ειδικά μηχανήματα ανάγνωσης καρτών και 1 που θα χρησιμοποιεί βιομετρικές μεθόδους, όπως είναι τα αποτυπώματα.

10 * 69 E = 690 ευρώ

1 * 220 E = 220 ευρώ

Σύνολο 910 ευρώ.

Γενικό σύνολο περιμετρικής ασφάλειας : 29.736 ευρώ

9.3 Εκτίμηση κόστους δικτύου

Το κυριότερο έξοδο του δικτύου μας έχει να κάνει κυρίως με τους υπολογιστές που θα χρησιμοποιηθούν και το υλικό διασύνδεσης και αποθήκευσης.

9.3.1 Υπολογιστές χρηστών

Υπολογίσαμε ότι οι υπολογιστές των χρηστών, συνυπολογίζοντας αυτούς του τοπικού δικτύου και αυτούς που θα είναι συνδεδεμένοι στο διαδίκτυο, θα είναι περίπου 60. Αν η μέση τιμή του κάθε υπολογιστή με την οθόνη και τα υπόλοιπα περιφερειακά είναι 1000 ευρώ τότε έχουμε : **σύνολο 60.000.**

9.3.2 Servers

Οι server της εταιρίας είναι συνολικά εφτά. Δύο για το τοπικό δίκτυο, ένας print server και τέσσερις για το διαδίκτυο (Web, SMTP, Proxy, PBX). Αυτοί οι server θα είναι υπολογιστές που θα τρέχουν και το αντίστοιχο λειτουργικό. Επειδή τους χρειαζόμαστε για συγκεκριμένη δουλειά, μπορούμε να δώσουμε βάρος στον εξοπλισμό που μας χρειάζεται και να αφήσουμε πιο χαμηλά κάποιον άλλο πχ την κάρτα γραφικών. Επίσης οι server του διαδικτύου δεν χρειάζεται να εξυπηρετούν κάποιο ιδιαίτερα μεγάλο φόρτο, άρα δεν υπάρχει ανάγκη για αγορά μηχανημάτων ιδιαίτερα δαπανηρών.

2 server του τοπικού δικτύου 1800 ευρώ έκαστος. **Σύνολο 3600 ευρώ**.

1 print server του τοπικού δικτύου με κόστος 1000 ευρώ.

3 server του διαδικτύου 1200 ευρώ έκαστος. **Σύνολο 3600 ευρώ**.

1 PBX server με κόστος 1000 ευρώ.

Σύνολο 9200 ευρώ.

9.3.3 VoIP τηλέφωνα

Τα VoIP τηλέφωνα είναι και αυτά ένα σημαντικό κεφάλαιο της εταιρίας. Αυτά είναι εγκατεστημένα από ένα σε κάθε τμήμα και από ένα στα ανώτερα στελέχη της εταιρίας. Χρειαζόμαστε :

15 SIP VoIP τηλέφωνα 89 ευρώ έκαστο. **Σύνολο 1335 ευρώ.**

9.3.4 Backup PC

Το Backup PC είναι μηχάνημα που θα γίνεται μόνο το Backup των δεδομένων. Σε αυτό θα τρέχει το λειτουργικό FreeBSD που είναι βασισμένο σε UNIX. Για το λόγο αυτό οι απαιτήσεις δεν είναι πολύ μεγάλες. **1 pc με κόστος 1000 ευρώ.**

9.3.5 NAS

Το NAS στο οποίο θα στηρίζεται η εταιρία για την κεντρική αποθήκευση των δεδομένων της έχει κόστος 989 Ευρώ

9.3.6 Switches

Για τις ανάγκες του τοπικού δικτύου και του διαδικτύου θα χρησιμοποιήσουμε έξι switches, οι οποίες θα είναι του τύπου Cisco Catalyst 2950 Series, με κόστος:

6 * 1415 E = 8490.

9.3.7 Router

Επίσης θα εγκαταστήσουμε ένα cisco router για το τοπικό δίκτυο, το Cisco 2851 Router που υποστηρίζει GBit Ethernet. Και για το διαδίκτυο θα χρησιμοποιήσουμε το cisco 877 ADSL router. Άρα έχουμε:

1 Cisco router * 1595 E = 1595 ευρώ

1 cisco adsl modem router *289 E = 289 ευρώ

Σύνολο 1884 ευρώ.

Γενικό σύνολο δικτύου : 82.898 Ευρώ

ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΡΑΡΤΗΜΑ Α

ΑΠΑΙΤΗΣΕΙΣ ΤΟΥ ΠΡΟΤΥΠΟΥ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ISO 17799

Η ανάγκη για όλο και πιο αυξημένη ασφάλεια οδήγησε στην δημιουργία κανόνων που διέπουν την χρήση και την εφαρμογή της στον τομέα των πληροφοριών . Όλες οι τεχνικές που είχαν χρησιμοποιηθεί κατά καιρούς έπρεπε να συγκεντρωθούν ώστε να αναπτυχθεί ένα διεθνές πρότυπο που να κατευθύνει σωστά την ανάπτυξη της ασφάλειας. Τέτοια πρότυπα πλέον έχουμε πολλά και τα οποία συνεχώς εξελίσσονται.

Το ISO 17799 χρησιμοποιείται για να περιγράψει 2 διαφορετικά κείμενα: το ISO 27002 το οποίο είναι ένα σύνολο από ελέγχους ασφαλείας και το ISO 27001 (παλιό BS7799) το οποίο είναι ένας προσδιορισμός για τα συστήματα διαχείρισης πληροφοριακής ασφάλειας (Information Security Management System - ISMS). Οι κανόνες που βάσει αυτό το πρότυπο είναι:

1. Πολιτική Ασφάλειας

1.1 Δημιουργία πολιτικής πληροφοριακής ασφάλειας

1.2 Αναπτύξτε ένα κείμενο με την πολιτική πληροφοριακής ασφάλειας

1.3 Επαναλάβετε και αξιολογήστε τους κανόνες της πληροφοριακής ασφάλειας που δημιουργήσατε.

2. Συστηματοποίηση της ασφάλειας

2.1 Δημιουργήστε μια υποδομή ασφάλειας

2.1.1 Ξεκινήστε ένα forum σχετικό με την διαχείριση της πληροφοριακής ασφάλειας.

2.1.2 Καθορίστε τα μέρη, τους φυσικούς χώρους, που θα εφαρμοστεί η πληροφοριακή ασφάλεια

2.1.3 Αναθέστε τις κατάλληλες αρμοδιότητες της πληροφοριακής ασφάλειας, στα κατάλληλα άτομα .

2.1.4 Δημιουργήστε μια εξουσιοδοτημένη διαδικασία με την οποία θα γίνονται νέες εγκαταστάσεις.

2.1.5 Προσδιορίστε τους ειδικούς που θα ασχοληθούν με την πληροφοριακή ασφάλεια.

2.1.6 Να κρατάτε ξεχωριστά βοηθητικά κείμενα σχετικά με την πολιτική ασφάλειας

2.2 Ελέγξτε την πρόσβαση τρίτων προσώπων στις εγκαταστάσεις.

2.2.1 Αναγνωρίστε και προσδιορίστε τους κινδύνους που δημιουργούνται από πρόσβαση τρίτων προσώπων.

2.2.1.1 Μελετήστε εις βάθος την πρόσβαση από τρίτους

2.2.1.2 Επιβάλετε ειδικούς πληροφοριακούς ελέγχους.

2.2.1.3 Ελέγξτε την πρόσβαση του ανάδοχου των έργων σε πληροφορίες της εταιρίας

2.2.2 Χρησιμοποιήστε συμβόλαια για να ελέγξετε την πρόσβαση από τρίτους

2.3 Ελέγξτε την διαδικασία εισαγωγής εξωτερικών πληροφοριών

2.3.1 Χρησιμοποιήστε συμβόλαια για να ελέγξετε εξωτερικές υπηρεσίες

3. Ταξινόμηση και έλεγχος πόρων

3.1 Λογοδοσία-έλεγχος από αυτούς που αξιοποιούν τους πόρους

3.1.1 Καταρτίστε ένα χώρο αποθήκευσης όλων των πληροφοριακών πόρων

3.2 χρησιμοποιήστε ένα σύστημα ταξινόμησης των πληροφοριών

3.2.1 Αναπτύξτε οδηγούς για την ταξινόμηση των πληροφοριών

3.2.2 Χρησιμοποιήστε διαδικασίες για την διαχείριση και ονοματοποίηση των πληροφοριών

4. Προσωπικό διαχείρισης τα ασφάλειας

4.1 Ελέγξτε την διαδικασία πρόσληψης του προσωπικού σας

4.1.1 Περιλάβετε την ασφάλεια σε κάθε είδους δουλειά

4.1.2 Ελέγξτε το παρελθόν αυτών που κάνουν αίτηση για πρόσληψη

4.1.3 Χρησιμοποιήστε εμπιστευτικότητα ή συμφωνίες μη αποκάλυψης στοιχείων

4.1.4 Συνάψτε συμβόλαια με τους εργαζόμενους ώστε να προστατέψετε τις πληροφορίες

4.2 Εφοδιαστείτε με εξάσκηση στη πληροφοριακή ασφάλεια

4.2.1 Ελέγξτε την εξάσκηση στην πληροφοριακή ασφάλεια

4.3 Άμεση ανταπόκριση σε συμβάντα που σχετίζονται με την πληροφοριακή ασφάλεια.

4.3.1 Αναφέρετε όλα τα γεγονότα της πληροφορικής ασφάλειας.

4.3.2 Αναφέρετε όλες τις αδυναμίες και τους κίνδυνους της ασφάλειας σας.

4.3.3 Ελέγξτε όλες τις δυσλειτουργίες λογισμικού

4.3.4 Να μαθαίνετε από όλα τα γεγονότα που έχετε αντιμετωπίσει μέχρι τώρα

4.3. Αναπτύξτε μια πειθαρχημένη διαδικασία

5. Φυσική και περιβαλλοντική ασφάλεια

5.1 Χρησιμοποιήστε ασφαλείς περιοχές για την καλύτερη προστασία τ ων εγκαταστάσεων

5.1.1 Χρησιμοποιήστε περιμετρικές ζώνες περίφραξης για να προστατέψετε τις εγκαταστάσεις.

5.1.2 Χρησιμοποιήστε ελέγχους εισόδων για να προστατέψετε τις ασφαλείς περιοχές

5.1.3 Χρησιμοποιήστε σχεδιασμένες στρατηγικές – πρότυπα για να προστατέψετε τις ασφαλείς περιοχές σας.

5.1.4 Χρησιμοποιήστε οδηγίες εργασιών

5.1.5 Χρησιμοποιήστε περιοχές απομόνωσης για την προστασία των υψίστης ασφαλείας περιοχών

5.2 Προστατέψτε το εξοπλισμό σας από κινδύνους

5.2.1 φυλάξτε τον εξοπλισμό

5.2.2 προστατέψετε τι βασικές σας προμήθειες.

5.2.3 Ασφαλίστε τα καλώδια

5.2.4 Συντηρήστε τον εξοπλισμό

5.2.5 Ελέγξτε τον off-site (απομακρυσμένο) εξοπλισμό

5.2.6 Ελέγξτε όλο το διαθέσιμο εξοπλισμό

5.3 Ελέγξτε την πρόσβαση στις πληροφορίες και στην ιδιοκτησία

5.3.1 Καθορίστε μια ξεκάθαρη πολιτική προστασίας.

5.3.2 Ελέγξτε την απομάκρυνση των περιουσιακών στοιχείων

6. Διαχείριση επικοινωνιών και χειρισμών

6.1 Δημιουργήστε διαχειρίστηκες διαδικασίες.

6.1.1 Εγγράψτε τις σε κείμενα

6.1.2 Ελέγξτε τις αλλαγές σε εγκαταστάσεις και στο συνολικό σύστημα

6.1.3 Εφαρμόστε συνυφασμένες διαδικασίες διαχείρισης.

6.1.4 Ξεχωρίστε τους ελέγχους και τις αρμοδιότητες

6.1.5 Ξεχωρίστε την ανάπτυξη του συστήματος από την βελτίωσή του.

6.1.6 Ελέγξτε τη διαχείριση των εξωτερικών εγκαταστάσεων

6.2 Αναπτύξτε σχέδια για να εξασφαλίσετε μελλοντική αύξηση χωρητικότητας.

6.2.1 Καταγράψτε τη χρήση και εξετάστε μελλοντικές απαιτήσεις.

6.2.2 Χρησιμοποιήστε αποδεκτά κριτήρια για να τεστάρετε το σύστημα σας.

6.3 Προστατευτείτε από το κακόβουλο λογισμικό

6.3.1 Ανιχνεύστε και εμποδίστε το κακόβουλο λογισμικό

6.4 Δημιουργήστε διαδικασίες φύλαξης – τακτοποίησης

6.4.1 Κάντε λήψη αντιγράφων ασφαλείας τις πληροφορίες και το λογισμικό που χρησιμοποιείτε

6.4.2 Διατηρήστε αρχείο για τις διαχειριστικές ενέργειες σας.

6.4.3 Αναφέρετε και καταγράψτε τα σφάλματα του δικτύου

6..5 Ασφαλίστε τα δίκτυα υπολογιστών

6.5.1 Εγκαταστήστε ελέγχους ασφαλείας του δικτύου

6.6 Προστατέψτε και ελέγξτε την τα μέσα επικοινωνίας των υπολογιστών

6.6.1 Χειριστείτε τα αφαιρούμενα μέσα επικοινωνίας

6.6.2 ελέγξτε τα διαθέσιμα μέσα επικοινωνίας.

6.6.3 Ελέγξτε τον χειρισμό των πληροφοριών και τους χώρους αποθήκευσης της

6.6.4 Προστατέψτε τα έγγραφα τους συστήματος

6.7 Ελέγξτε τις συναλλαγές με άλλους εξωτερικούς οργανισμούς

6.7.1 Αναπτύξτε συμφωνίες για την ανταλλαγή των πληροφοριών

6.7.2 Ασφαλίστε την μεταφορά πληροφοριών μεταξύ των μέσων επικοινωνίας

6.7.3 Δημιουργήστε ελέγχους για να προστατέψετε τις ηλεκτρονικές οικονομικές συναλλαγές

6.7.4 Εγκαταστήστε ελέγχους για να προστατέψετε τα email.

6.7.4.1 Ελέγξτε τη χρήση των email.

6.7.4.2 Αναπτύξτε μια πολιτική χρήσης των email

6.7.5 Προστατέψτε τα συστήματα ηλεκτρονικού γραφείου

6.7.6 Ελέγξτε τα συστήματα που χρησιμοποιούν δημόσιες πληροφορίες

6.7.7 Ελέγξτε τις εξωτερικές επικοινωνίες

7. Διαχείριση ελέγχου και πρόσβασης των πληροφοριών

7.1 Έλεγχος πρόσβασης στην πληροφορία

7.1.1 Αναπτύξτε μια πολιτική και κανόνες ώστε να ελέγξετε την πρόσβαση

7.1.1.1 Αναπτύξτε μια πολιτική ώστε να ελέγξετε την πρόσβαση στις πληροφορίες.

7.1.1.2 Αναπτύξτε κανόνες ελέγχου της πρόσβασης στις πληροφορίες

7.2 Χειριστείτε την κατανομή των δικαιωμάτων πρόσβασης

7.2.1 Επιβάλλετε διαδικασία εγγραφής των χρηστών

7.2.2 Ελέγξτε την εξουσιοδότηση των προνομίων του συστήματος

7.2.3 Επιβάλλετε μια διαδικασία για να χειρίζεστε τους κωδικούς των χρηστών

7.2.4 Επαναλάβετε τον έλεγχο για τα δικαιώματα πρόσβασης των χρηστών και των προνομίων τους

7.3 Ενθαρρύνετε την υπευθυνότητα στους τρόπους πρόσβασης

7.3.1 Ενθαρρύνετε τους χρήστες ώστε να προστατεύουν τους κωδικούς τους.

7.3.2 Ενθαρρύνετε τους χρήστες να προστατεύουν τον εξοπλισμό

7.4 Ελέγξτε την πρόσβαση στο δίκτυο υπολογιστών

7.4.1 Διαμορφώστε μια πολιτική χρήσης του δικτύου

7.4.2 Χρησιμοποιήστε υποχρεωτικά βήματα για τον έλεγχο της πρόσβασης

7.4.3 Εξακριβώστε τις απομακρυσμένες συνδέσεις των χρηστών

7.4.4 Χρησιμοποιήστε κόμβους πιστοποίησης για να ελέγξετε απομακρυσμένους χρήστες.

7.4.5 Ελέγξτε την απομακρυσμένη πρόσβαση σε διαγνωστικά ports

7.4.6 Ξεχωρίστε εσωτερικά και εξωτερικά δίκτυα

7.4.7 Περιορίστε τις συνδέσεις σε κοινά δίκτυα

7.4.8 Εγκαταστήστε ελέγχους δρομολόγησης στα κοινά δίκτυα

7.4.9 Επαληθεύστε την ασφάλεια των διαδικτυακών υπηρεσιών

7.5 Περιορίστε την πρόσβαση στο επίπεδο της διαχείρισης του συστήματος

7.5.1 Χρησιμοποιήστε αυτόματες τεχνικές αναγνώρισης των τερματικών

7.5.2 Εγκαταστήστε διαδικασίες (terminal) εγγραφής

7.5.3 Αναγνωρίστε και πιστοποιήστε όλους τους χρήστες
7.5.4 Δημιουργήστε ένα σύστημα διαχείρισης των κωδικών πρόσβασης
7.5.5 Ελέγξτε τη χρήση όλων των λειτουργιών του συστήματος
7.5.6 Εφοδιαστείτε με συναγερμούς ώστε να προστατέψετε τους χρήστες
7.5.7 Χρησιμοποιήστε διακοπές για να προστατέψετε ανενεργά τερματικά.
7.5.8 Περιορίστε τις φορές που ένα τερματικό προσπαθεί να συνδεθεί στο δίκτυο
7.6 Χειριστείτε την πρόσβαση στα συστήματα εφαρμογών
7.6.1 Ορίστε κανόνες για την πρόσβαση στις εφαρμογές και τις πληροφορίες
7.6.2 Απομονώστε ευαίσθητα συστήματα πληροφοριών
7.7 Καταγράψτε τη πρόσβαση στο σύστημα και τη χρήση του.
7.7.1 Εγκαταστήστε και συντηρήστε τις εγγραφές στο σύστημα
7.7.2 Καταγραφή της κίνησης στις εγκαταστάσεις
7.7.2.1 Εγκαταστήστε διαδικασίες για τα μέσα καταγραφής
7.7.2.2 Επαληθεύστε τα αποτελέσματα από τις δραστηριότητες καταγραφής
7.7.2.3 Μελετήστε τις εγγραφές για να αναγνωρίσετε γεγονότα που σχετίζονται με την ασφάλεια
7.8 Προστατέψτε κινητούς και ηλεκτρονικούς πόρους
7.8.1 Προστατέψτε κινητό εξοπλισμό και πληροφορία
7.8.2 Προστατέψτε ηλεκτρονικό εξοπλισμό και πληροφορία

8. Συστήματα ανάπτυξης και συντήρησης

8.1 Αναγνωρίστε τις απαιτήσεις ασφαλείας του συστήματος
8.1.1 Προσδιορίστε τις απαιτήσεις και ους ελέγχους ασφαλείας
8.2 Αναπτύξτε την ασφάλεια μέσα στα συστήματα εφαρμογών σας
8.2.1 Δημιουργήστε εσωτερική επικύρωση των δεδομένων στο σύστημα σας
8.2.2 Δημιουργήστε διαδικαστικούς ελέγχους μέσα στο σύστημα
8.2.2.1 Σχεδιάστε διαδικαστικούς ελέγχους για να ελαχιστοποιήσετε τους κινδύνους
8.2.3 Δημιουργήστε μηνύματα πιστοποίησης μέσα στο σύστημα
8.2.4 Δημιουργήστε επικύρωση εξωτερικών δεδομένων στο σύστημα
8.3 Χρησιμοποιήστε κρυπτογραφία για να προστατέψετε τις πληροφορίες
8.3.1 Αναπτύξτε μια πολιτική για τη χρήση της κρυπτογράφησης
8.3.2 Κωδικοποιήστε ευαίσθητη ή κρίσιμη πληροφορία
8.3.3 Προστατέψτε τα κείμενα που έχουν ηλεκτρονικές υπογραφές

8.3.4 Χρησιμοποιήστε υπηρεσίες αναγνώρισης ευθυνών για να επιλύσετε προβλήματα διαφωνιών

8.3.5 Εγκαταστήστε ένα σύστημα διαχείρισης κλειδιών

8.3.5.1 Προστατέψτε τα κλειδιά κρυπτογράφησης.

8.3.5.2 Χρησιμοποιήστε ασφαλείς μεθόδους για το χειρισμό των κλειδιών

8.4 Προστατέψτε τα συστήματα αρχείων της επιχείρησης σας

8.4.1 Ελέγξτε την εφαρμογή του λογισμικού

8.4.2 Ελέγξτε τη χρήση των δεδομένων του συστήματος

8.4.3 Ελέγξτε την πρόσβαση στις βιβλιοθήκες των πηγαίων προγραμμάτων

8.5 Ελέγξτε την ανάπτυξη και την υποστήριξη

8.5.1 Εγκαταστήστε διαδικασίες αλλαγής του ελέγχου

8.5.2 Επαληθεύστε αλλαγές στο λειτουργικό σύστημα

8.5.3 Περιορίστε τις αλλαγές στα πακέτα λογισμικού

8.5.4 Πάρτε μέτρα ασφάλειας απέναντι σε αφανή κανάλια και ιούς

8.5.5 Ελέγξτε την ανάπτυξη λογισμικού από εξωτερικές πηγές

9. Διαχείριση συνέχισης της επιχείρησης

9.1 Σχεδιάστε μια διαδικασία διαχείρισης της συνέχειας

9.1.1 Εγκαταστήστε – επιβάλετε αυτή τη διαδικασία

9.1.2 Διενεργήστε ανάλυση κινδύνων και ανάλυση του αντίκτυπου που θα έχει

9.1.3 Αναπτύξτε τα σχέδια συνέχισης της λειτουργίας της επιχείρησης

9.1.4 Συντηρήστε ένα σχέδιο συνέχισης

9.1.5 Τεστάρετε και αναβαθμίστε το σχέδιο συνέχισης

9.1.5.1 Τεστάρετε τα σχέδια συνέχισης της επιχείρησης

9.1.5.2 Αναβαθμίστε αυτά τα σχέδια

10. Διαχείριση συμμόρφωσης με τους κανόνες

10.1 Συμμόρφωση με τις νόμιμες απαιτήσεις

10.1.1 Αναγνώριση όλων των σχετικών νόμιμων απαιτήσεων

10.1.2 Σεβασμός στα πνευματικά περιουσιακά στοιχεία

10.1.2.1 Δημιουργήστε πνευματικά δικαιώματα

10.1.2.2 Συμμόρφωση με αυτά

10.1.3 Ασφαλίστε όλες τις εγγραφές του οργανισμού σας

10.1.4 Προστατέψτε τις ιδιωτικές πληροφορίες του προσωπικού σας

10.1.5 Αποτρέψτε κακή χρήση στη επεξεργασία των δεδομένων

10.1.6 Ελέγξτε τη χρήση κρυπτογραφικών ελέγχων

10.1.7 Συλλέξτε στοιχεία για να υποστηρίξετε τις ενέργειές σας

10.1.7.1 Συμμορφωθείτε με τους επιτρεπτούς κανόνες των στοιχείων

10.1.7.2 Συλλέξτε στοιχεία που θα είναι αποδεκτά στο δικαστήριο

10.1.7.3 Προστατέψτε την ποιότητα των στοιχείων σας

10.2 Εκτελέστε επαληθευτικούς ελέγχους συμμόρφωσης με την ασφάλεια

10.2.1 Επαληθεύστε τη συμμόρφωση με την πολιτική ασφάλειας

10.2.2 Επαληθεύστε τη συμμόρφωση με την τεχνική ασφάλεια

10.3 Εκτελέστε ελέγχους του λειτουργικού συστήματος

10.3.1 Σχεδιάστε τους ελέγχους του ΛΣ

10.3.2 Προστατέψτε τα εργαλεία του συστήματος σας.

ΠΑΡΑΡΤΗΜΑ Β

Checklists για λήψη αντιγράφων ασφαλείας

No.	Αντικείμενο ελέγχου	Διαδικασία	Αποτέλεσμα	Ημερομηνία ελέγχου
1	Διαδικασία λήψης αντιγράφων ασφαλείας	Καλύπτει η πολιτική λήψης αντιγράφων ασφαλείας τις παρακάτω ελάχιστες απαιτήσεις; Αντίγραφα ασφαλείας στους Servers . Αντίγραφα ασφαλείας για κάθε χρήστη ξεχωριστά Χρονοδιάγραμμα Χειριστές των αντιγράφων ασφαλείας Κλειδί ασφαλείας Τοποθεσία των αντιγράφων ασφαλείας Χρήστες με δικαιώματα επαναφοράς δεδομένων Διαδικασία επαναφοράς		
2	Ρύθμιση του σχεδίου λήψης αντιγράφων ασφαλείας	Αναγνωρίζονται τα πιο σημαντικά αρχεία που πρέπει να γίνουν κόπιες. Για κάθε περίπτωση να γίνεται προσδιορισμός του είδους των αντιγράφων ασφαλείας. Κατά τη λήψη παίρνουμε screenshots τα οποία μας δείχνουν: -την επιλογή των αρχείων που θα τους γίνει backup. -το πρόγραμμα που έχει καταρτιστεί -ένα αρχείο επιβεβαίωσης επιτυχούς λήψης των αντιγράφων. -ένα αρχείο επιβεβαίωσης επιτυχούς επαναφοράς		
3	Απόσταση απομακρυσμένων αποθηκευτικών μέσων	Επίσκεψη από εξουσιοδοτημένο άτομο των εγκαταστάσεων που κρατούνται τα απομακρυσμένα αντίγραφα ασφαλείας		

Checklist: Ασφάλεια του δικτύου μας

Router

Έλεγχος	Περιγραφή
☐	Ενημερωμένο με τα τελευταία updates και patches
☐	Είμαστε εγγεγραμμένοι στην υπηρεσία εξυπηρέτησης τοθ κατασκευαστή
☐	Οι γνωστές θύρες που αποτελούν αδυναμία είναι κλειστές
☐	ενεργοποιημένο φίλτρο εισόδου και εξόδου. Εισερχόμενα και εξερχόμενα πακέτα επιβεβαιώνονται ως ασφαλή κατά την κίνησή τους στο δίκτυο
☐	Η ICMP κυκλοφορία παρακολουθείται από οθόνες.
☐	Οι διασυνδέσεις είναι καταμετρημένες και ασφαλισμένες
☐	Η απευθείας εκπομπή δεν επιτρέπεται
☐	Άχρηστες εφαρμογές είναι απενεργοποιημένες (TFTP).
☐	Χρήση δυνατών κωδικών ασφαλείας

Firewall

Έλεγχος	Περιγραφή
☐	Ενημερωμένο με τα τελευταία updates και patches
☐	Αποτελεσματικά φίλτρα πρέπει να είναι εγκατεστημένα για να εμποδίζουν την κακόβουλη κυκλοφορία να εισέλθει στην περίμετρο του δικτύου
☐	Θύρες που δεν χρησιμοποιούνται πρέπει να κλειδώνονται
☐	Πρωτόκολλα που δεν χρησιμοποιούνται πρέπει να μπλοκάρονται εξαρχής
☐	Ενεργοποιημένο σύστημα ανίχνευσης εισβολέων

Switch

Έλεγχος	Περιγραφή
☐	Ενημερωμένο με τα τελευταία updates και patches
☐	Οι διασυνδέσεις είναι καταμετρημένες και ασφαλισμένες
☐	Διασυνδέσεις που δεν χρησιμοποιούνται είναι απενεργοποιημένες
☐	Υπηρεσίες που δεν χρησιμοποιούνται είναι απενεργοποιημένες
☐	Οι διαθέσιμες υπηρεσίες είναι ασφαλισμένες

Checklist για τους εργοδότες

1. Γνωρίζεις ότι σύμφωνα με τη νομοθεσία ο εργοδότης είναι ο υπεύθυνος για να εξασφαλίζει τη λήψη και την τήρηση των απαραίτητων μέτρων για την ασφάλεια και την υγεία των εργαζομένων ή και ακόμη και τρίτων που βρίσκονται στους χώρους εργασίας;	**ΝΑΙ**☐	**ΟΧΙ**☐
2. Έχεις μεριμνήσει για τη σύνταξη γραπτής εκτίμησης κινδύνου;	**ΝΑΙ**☐	**ΟΧΙ**☐
3. Φροντίζεις για την προσαρμογή της εκτίμησης κινδύνου στις ουσιαστικές αλλαγές που γίνονται στις εγκαταστάσεις και στην παραγωγική διαδικασία;	**ΝΑΙ**☐	**ΟΧΙ**☐
4. Πραγματοποιείται εκπαίδευση των εργαζομένων αμέσως μετά την πρόσληψή τους και σε τακτικά χρονικά διαστήματα με έμφαση στα μέτρα ασφάλειας και υγείας;	**ΝΑΙ**☐	**ΟΧΙ**☐
5. Ενημερώνεις τους εργαζόμενους για τους κινδύνους που αντιμετωπίζουν και για τον τρόπο προστασίας τους;	**ΝΑΙ**☐	**ΟΧΙ**☐
6. Προβαίνεις σε διαβούλευση με τους εργαζόμενους για τα μέτρα που πρέπει κάθε φορά να λαμβάνονται για την ασφάλεια και την υγεία τους;	**ΝΑΙ**☐	**ΟΧΙ**☐
7. Υπάρχει συγκεκριμένο σύστημα ή διαδικασία για την ανάθεση εργασιών σε εργαζόμενους;	**ΝΑΙ**☐	**ΟΧΙ**☐
8. Υπάρχει τεχνικός ασφάλειας στην επιχείρηση;	**ΝΑΙ**☐	**ΟΧΙ**☐
9. Υπάρχει γιατρός εργασίας στην επιχείρηση;	**ΝΑΙ**☐	**ΟΧΙ**☐
10. Υπάρχει Επιτροπής Υγιεινής και Ασφάλειας στην επιχείρηση;	**ΝΑΙ**☐	**ΟΧΙ**☐
11. Υπάρχουν εκπρόσωποι-αντιπρόσωποι των εργαζομένων με αρμοδιότητα την ασφάλεια και υγεία των εργαζομένων;	**ΝΑΙ**☐	**ΟΧΙ**☐
12. Γίνονται συναντήσεις του εργοδότη, των εκπροσώπων των εργαζομένων, του τεχνικού ασφάλειας (και του γιατρού εργασίας) όπως προβλέπεται από τις σχετικές διατάξεις;	**ΝΑΙ**☐	**ΟΧΙ**☐
13. Υπάρχει επίβλεψη κατά τη διάρκεια των εργασιών προκειμένου να τηρούνται τα απαραίτητα κατά περίπτωση μέτρα ασφάλειας και υγείας;	**ΝΑΙ**☐	**ΟΧΙ**☐
14. Οι εργασίες οργανώνονται ώστε να τηρούνται τα απαραίτητα μέτρα ασφάλειας και υγείας;	**ΝΑΙ**☐	**ΟΧΙ**☐
15. Υπάρχει πρόβλεψη για μηχανισμό επιτήρησης της εφαρμογής των μέτρων αυτών;	**ΝΑΙ**☐	**ΟΧΙ**☐
16. Λαμβάνονται μέτρα για εργονομικές διευθετήσεις ώστε να μην καταπονούνται άσκοπα ή υπερβολικά οι εργαζόμενοι;	**ΝΑΙ**☐	**ΟΧΙ**☐
17. Προβλέπονται μέτρα για τον έλεγχο της "επαγγελματικής" υγείας των εργαζομένων;	**ΝΑΙ**☐	**ΟΧΙ**☐

18. Γίνεται έλεγχος των εργαζομένων σύμφωνα με τις σχετικές διατάξεις υγιεινής; **ΝΑΙ**☐ **ΟΧΙ**☐
19. Υπάρχει πρόβλεψη για την παροχή Α΄ Βοηθειών σε περίπτωση ανάγκης; **ΝΑΙ**☐ **ΟΧΙ**☐
20. Υπάρχουν εντεταλμένοι εργαζόμενοι για την παροχή πρώτων βοηθειών; **ΝΑΙ**☐ **ΟΧΙ**☐
21. Έχουν ενημερωθεί οι εργαζόμενοι τι ενέργειες πρέπει να κάνουν στις περιπτώσεις αυτές; **ΝΑΙ**☐ **ΟΧΙ**☐
22. Έχει τοποθετηθεί η προβλεπόμενη σήμανση στους χώρους εργασίας; **ΝΑΙ**☐ **ΟΧΙ**☐
23. Υπάρχει στα δοχεία, σάκους κλπ. η προβλεπόμενη από τις κείμενες διατάξεις σήμανση; **ΝΑΙ**☐ **ΟΧΙ**☐
24. Υπάρχουν στους χώρους εργασίας πινακίδες με συγκεκριμένες οδηγίες για τους εργαζόμενους; **ΝΑΙ**☐ **ΟΧΙ**☐

ΦΥΣΙΚΟΙ ΠΑΡΑΓΟΝΤΕΣ

25. Λαμβάνονται τεχνικά και οργανωτικά μέτρα για την προστασία των εργαζομένων από τη "θερμική καταπόνηση"; **ΝΑΙ**☐ **ΟΧΙ**☐
26. Τους χορηγούνται τα απαραίτητα μέσα ατομικής προστασίας; **ΝΑΙ**☐ **ΟΧΙ**☐
27. Έχει προκαθοριστεί ο μέγιστος χρόνος συνεχούς εργασίας των εργαζομένων που εκτίθενται σε ακτινοβολία; **ΝΑΙ**☐ **ΟΧΙ**☐
28. Λαμβάνονται μέτρα για την προστασία των εργαζομένων από θόρυβο; **ΝΑΙ**☐ **ΟΧΙ**☐

ΒΙΟΛΟΓΙΚΟΙ ΠΑΡΑΓΟΝΤΕΣ

29. Λαμβάνονται μέτρα για την προστασία των εργαζομένων έναντι των βιολογικών παραγόντων; **ΝΑΙ**☐ **ΟΧΙ**☐
30. Υποβάλλονται οι εργαζόμενοι σε προληπτικό ιατρικό έλεγχο; **ΝΑΙ**☐ **ΟΧΙ**☐
31. Λαμβάνονται ιδιαίτερα μέτρα για την πρόληψη μόλυνσης των ουσιών από τρωκτικά κλπ.; **ΝΑΙ**☐ **ΟΧΙ**☐

ΜΕΣΑ ΑΤΟΜΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ

32. Χορηγούνται στους εργαζόμενους μέσα ατομικής **ΝΑΙ**☐ **ΟΧΙ**☐

προστασίας;

33. Οι εργαζόμενοι χρησιμοποιούν τα μέσα αυτά; **ΝΑΙ**☐ **ΟΧΙ**☐
34. Υπάρχει παρότρυνση και επιτήρηση των εργαζομένων για τη χρήση των μέσων αυτών; **ΝΑΙ**☐ **ΟΧΙ**☐
35. Έχουν ενημερωθεί οι εργαζόμενοι για τη αναγκαιότητα χρησιμοποίησης των μέσων ατομικής προστασίας; **ΝΑΙ**☐ **ΟΧΙ**☐

ΑΛΛΟΙ ΠΑΡΑΓΟΝΤΕΣ

36. Επισημαίνονται επαρκώς οι χώροι όπου τα δάπεδα είναι ολισθηρά; **ΝΑΙ**☐ **ΟΧΙ**☐
37. Προβλέπονται ειδικά μέτρα για τη μείωση των κινδύνων από την ολισθηρότητα; **ΝΑΙ**☐ **ΟΧΙ**☐
38. Έχουν τοποθετηθεί αντιολισθητικά δάπεδα; **ΝΑΙ**☐ **ΟΧΙ**☐
39. Έχουν προκαθοριστεί οι ενέργειες σε περίπτωση ανάγκης; **ΝΑΙ**☐ **ΟΧΙ**☐
40. Διατίθεται στους εργαζόμενους σε όλες τις θέσεις εργασίας πόσιμο νερό; **ΝΑΙ**☐ **ΟΧΙ**☐
41. Πραγματοποιούνται κατά τακτά χρονικά διαστήματα ασκήσεις ετοιμότητας; **ΝΑΙ**☐ **ΟΧΙ**☐
42. Ζητείται από τους εργαζόμενους να μη αναλαμβάνουν εργασία εάν δεν αισθάνονται πλήρως υγιείς οπότε και ενημερώνουν σχετικά; **ΝΑΙ**☐ **ΟΧΙ**☐
43. Υπάρχουν τα κατάλληλα μέσα πυρόσβεσης; **ΝΑΙ**☐ **ΟΧΙ**☐
44. Οι θέσεις που βρίσκονται επισημαίνονται με σαφήνεια; **ΝΑΙ**☐ **ΟΧΙ**☐
45. Υπάρχουν οδηγίες για τη χρήση φορητού εξοπλισμού κατάσβεσης; **ΝΑΙ**☐ **ΟΧΙ**☐
46. Υπάρχουν εκπαιδευμένοι εργαζόμενοι για τη χρήση των μέσων πυρόσβεσης; **ΝΑΙ**☐ **ΟΧΙ**☐
47. Σε περίπτωση φθορών υπάρχουν συγκεκριμένες οδηγίες για τον ασφαλή τρόπο επισκευής τους; **ΝΑΙ**☐ **ΟΧΙ**☐
48. Έχει εκτιμηθεί η καταπόνηση των εργαζομένων από μυοσκελετικά προβλήματα λόγω της στάσης του σώματος, των μεταφερόμενων φορτίων, του χρόνους εργασίας κλπ. ; **ΝΑΙ**☐ **ΟΧΙ**☐
49. Λαμβάνονται μέτρα για τη μείωση της έκθεσης των εργαζομένων στους παράγοντες αυτούς; **ΝΑΙ**☐ **ΟΧΙ**☐
50. Όταν γίνονται εργασίες σε ηλεκτρικά κυκλώματα ή εργαλεία λαμβάνεται μέριμνα να έχει απαραίτητα προηγηθεί διακοπή της ηλεκτρικής παροχής; **ΝΑΙ**☐ **ΟΧΙ**☐
51. Τοποθετούνται σχετικές προειδοποιητικές πινακίδες; **ΝΑΙ**☐ **ΟΧΙ**☐

52. Λαμβάνονται μέτρα για τη διατήρηση καθαρών των χώρων εργασίας; **ΝΑΙ☐** **ΟΧΙ☐**
53. Λαμβάνεται πρόνοια για τη διατήρηση των διαδρόμων κυκλοφορίας ελεύθερων χωρίς εμπόδια, υλικά κλπ; **ΝΑΙ☐** **ΟΧΙ☐**
54. Υπάρχουν συγκεκριμένες και σαφείς οδηγίες πότε διακόπτεται η εργασία τους για λόγους ασφαλείας και σε τι ενέργειες πρέπει κάθε φορά να προβούν; **ΝΑΙ☐** **ΟΧΙ☐**

Checklist για την ασφάλεια του κτιρίου

1	Όλες οι είσοδοι φωτίζονται επαρκώς	ΝΑΙ	ΟΧΙ
2	Οι βάρδιες των φυλάκων γίνονται στην ώρα τους	ΝΑΙ	ΟΧΙ
3	Οι φύλακες είναι εξοπλισμένοι με φακό και ασύρματο	ΝΑΙ	ΟΧΙ
4	Γίνεται μηνιαίος έλεγχος στην περίφραξη	ΝΑΙ	ΟΧΙ
5	Γίνεται μηνιαίος έλεγχος στα συστήματα ανίχνευσης εισβολέων	ΝΑΙ	ΟΧΙ
6	Γίνεται μηνιαίος έλεγχος στο κλειστό κύκλωμα παρακολούθησης	ΝΑΙ	ΟΧΙ
7	Έχει αναφερθεί περίεργη κίνηση ατόμων συστηματικά έξω και γύρω από την περίφραξη	ΝΑΙ	ΟΧΙ
8	Κρατείται βιβλίο επισκεπτών	ΝΑΙ	ΟΧΙ
9	Το σύστημα πιστοποίησης των εργαζομένων ελέγχεται μηνιαίως	ΝΑΙ	ΟΧΙ

Checklist για το προσωπικό

1	Κρίθηκε ικανός για τη δουλειά	ΝΑΙ	ΟΧΙ
2	Διάβασε και υπέγραψε ότι αποδέχεται την πολιτική ασφαλείας	ΝΑΙ	ΟΧΙ
3	Έχει καθαρό ποινικό μητρώο	ΝΑΙ	ΟΧΙ

4	Δεν έχει οικονομικά προβλήματα	ΝΑΙ	ΟΧΙ
5	Έγινε εκπαίδευση σε θέματα ασφαλείας	ΝΑΙ	ΟΧΙ
6	Συμφωνεί με τους κανόνες συμπεριφοράς της εταιρίας	ΝΑΙ	ΟΧΙ

Checklist για καταγραφή για ανάνηψη μετά από καταστροφή

1	Διασφαλίστε ότι η ανάνηψη του υλικού θα είναι πλήρης όταν χρειαστεί	
3	Επιβεβαίωση αντιγράφων ασφαλείας	
4	Επιβεβαίωση της σωστής επαναφοράς δεδομένων	
5	Επιβεβαίωση άμεσης ανάκτησης των απομακρυσμένων αντιγράφων ασφαλείας	
6	Επιβεβαίωση για την εγκυρότητα του σχεδίου ανάνηψης και ότι οι εργαζόμενοι σε θέσεις κλειδιά είναι σε ετοιμότητα	
7	Επιβεβαιώστε ότι το σχέδιο ανάνηψης είναι προσαρμοσμένο στις σύγχρονες απαιτήσεις	
9	Επιβεβαιώστε ότι το σχέδιο ανάνηψης και έκτακτης ανάγκης περιλαμβάνει όλα τα πιθανά σενάρια	

Checklist την παρακολούθηση Web Servers

1	Διασφαλίστε ότι ο web server τρέχει σε ένα αυτόνομο σύστημα και δεν εξαρτάται από άλλες εφαρμογές	
2	Επιβεβαιώστε ότι ο web server είναι πλήρως ενημερωμένος με τις τελευταίες ενημερώσεις	
3	Προσδιορίστε αν ο web server θα πρέπει να τρέχει επιπλέον εργαλεία για τη δική του προστασία.	
4	Επιβεβαιώστε ότι μη χρήσιμες υπηρεσίες και εργαλεία είναι απενεργοποιημένα.	
5	Επιβεβαιώστε ότι μόνο τα κατάλληλα πρωτόκολλα και οι θύρες επιτρέπεται να έχουν πρόσβαση στο web server.	
6	Επιβεβαιώστε ότι οι λογαριασμοί που έχουν πρόσβαση στον ςεβ ερωερ έχουν ισχυρούς κωδικούς πρόσβασης	
7	Εξασφαλίστε ότι οι κατάλληλοι έλεγχοι υπάρχουν για τα δεδομένα	
8	Επιβεβαιώστε ότι άχρηστα ή μη χρήσιμα ISAPI φίλτρα έχουν απομακρυνθεί από τον server	
9	Επιβεβαιώστε την εγκυρότητα όλων των πιστοποιητικών που χρησιμοποιεί ο server	

10	Επιβεβαιώστε ότι οι κατάλληλοι έλεγχοι για την πιστοποίηση είναι επιβεβλημένοι	
11	Επαληθεύστε αν υπάρχουν script στην ιστοσελίδα που αποτελούν αδυναμία του συστήματος	
12	Εξασφαλίστε ότι οι εφαρμογές που τρέχουν προστατεύονται από επιθέσεις.	

Βιβλιογραφία

[1] http://www.perimetrica.com
[2] http://www.perimetrica.com/background/tech_buried_coax.html
[3] McGraw Hill - CISSP Certification All in One Exam Guide 4th Edition Nov 2007 eBook-BBL
[4] http://www.smarthome.gr/category_products.asp?scid=9000J&lang=1
[5]http://www.chinavasion.com/product_info.php/pName/waterproof-night-vision-security-camera-pal-sony-13-lens/.
[6] http://www.chinavasion.com/product_info.php/pName/mini-security-camera-13-sony-ccd-night-vision-waterproof/
[7] http://e-businessforum.gr/omades_new/content/paradoteo_g3V4.0.pdf
[8] Stanek R. William, Ο βοηθός το διαχειριστή των Microsoft Windows server 2003, εκδόσεις Κλειδάριθμος
[9] Αλεξόπουλος Άρης, Τηλεπικοινωνίες και Δίκτυα υπολογιστών
[10] http://el.wikipedia.org/wiki/ARP
[11] http://www.lullabot.com/node/289/play
[12] http://www.linuxsecurity.com/content/view/133913/171/
[13] http://www.petefreitag.com/item/505.cfm
[14] http://www.freebsd.org/doc/el/books/handbook/sendmail.html
[15] http://www.codewalkers.com/c/a/Server-Administration/sendmail-Security-Options/
[16] http://magaz.hellug.gr/33/03_qos1-3.html
[17] http://shibuvarkala.blogspot.com/2008/11/howto-block-port-in-squid-proxy-ubuntu.html
[18] http://www.postokano.gr/proxy-server-egkatastasi-parametropoiisi-debian
[19] http://www.3cx.gr/voip-sip/voip-definition.php
[20] http://www.3cx.gr/voip-sip/sip-phones.php
[21] http://www.3cx.gr/voip-sip/ip-pbx-benefitfaq.php
[22] http://www.3cx.gr/voip-sip/ip-pbx-examples.php
[23] Γεώργιος Ν. Ράπτης, Server Virtualization, ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
[24] http://www.adslgr.com/forum/showthread.php?t=252178