ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ ΣΕ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΤΗΣ : ΝΤΕΛΕΚΟΥ ΑΙΚΑΤΕΡΙΝΗΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : ΧΑΤΖΙΝΑΣ ΣΠΥΡΙΔΩΝ

ΠΑΤΡΑ 2012

ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ ΣΕ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΤΗΣ : ΝΤΕΛΕΚΟΥ ΑΙΚΑΤΕΡΙΝΗ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : ΧΑΤΖΙΝΑΣ ΣΠΥΡΙΔΩΝ

ΠΑΤΡΑ 2012

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Βασικό αντικείμενο αυτής της πτυχιακής εργασίας αποτελεί η ασφάλεια των Πληροφοριακών Συστημάτων και Δικτύων σε Μικρομεσαίες Επιχειρήσεις. Η παρούσα εργασία γίνεται με σκοπό να διερευνηθεί το επίπεδο ασφαλείας των μικρομεσαίων επιχειρήσεων και σε τι βαθμό λαμβάνουν υπόψη τους, την ασφάλεια των υπολογιστικών τους συστημάτων και πόσο σημαντική είναι γι' αυτές. Η πτυχιακή εργασία είναι οργανωμένη σε 5 κεφάλαια :

Στο 1^{ο} κεφάλαιο αναλύεται η έννοια των πληροφοριακών συστημάτων, τα βασικά συστατικά που τα συνθέτουν και ανάλυση των κατηγοριών στις οποίες υποδιαιρούνται.

Στο 2^{ο} κεφάλαιο αναλύεται η έννοια της ασφάλειας του πληροφοριακού συστήματος, οι παραβάσεις της ασφάλειας, ακόμη οι ευπάθειες και κατηγορίες απειλών των πληροφοριακών συστημάτων καθώς και οι κύριοι τύποι μέτρων προστασίας αυτών και η αναγκαιότητα ύπαρξης πολιτικής ασφάλειας. Έπειτα, ακολουθεί κάποια αναφορά σε κακόβουλα προγράμματα και τεχνικές αντιμετώπισης τους. Επίσης, εκτενέστερη αναφορά σε ορισμένα σημαντικά μέτρα προστασίας. Επιπρόσθετα ορισμένη αναφορά στο διαδίκτυο και στις υπηρεσίες του.

Στο 3^{ο} κεφάλαιο είναι η μεθοδολογία της έρευνας και γίνεται παρουσίαση του ερωτηματολογίου, αναφορά στο σκοπό των ερωτήσεων και συνεντεύξεων αυτού.

Στο 4^{ο} κεφάλαιο περιέχονται οι απαντήσεις από το ερωτηματολόγιο, με τη μορφή διαγραμμάτων και η ανάλυση αυτών.

Στο 5^{ο} κεφάλαιο αναλύονται τα συμπεράσματα, ύστερα από την έρευνα που προέκυψε, όπως και κριτικές και προτάσεις.

ΕΙΣΑΓΩΓΗ

Τα πληροφοριακά συστήματα πραγματοποιούν υψηλής ταχύτητας και μεγάλης ποσότητας αριθμητικούς υπολογισμούς. Παρέχουν, επίσης, γρήγορη, ορθή και χαμηλού κόστους επικοινωνία στο εσωτερικό της επιχείρησης, αλλά και μεταξύ των οργανισμών. Η αυτοματοποίηση των ημι-αυτοματοποιημένων επιχειρηματικών διαδικασιών, αλλά και των χειρωνακτικών καθηκόντων είναι μια ακόμη από τις δυνατότητες των πληροφοριακών συστημάτων. Σε κάθε περίπτωση ο σχεδιασμός ενός πληροφοριακού συστήματος γίνεται για να δώσει λύσεις σε υπάρχοντα επιχειρησιακά προβλήματα. Ορισμένα από τα αυτά τα επιχειρησιακά προβλήματα είναι το λειτουργικό κόστος που προκύπτει και το οποίο έρχεται να το μειώσει. Η χρήση των συστημάτων αυτών αυξάνει την αποτελεσματικότητα και την αποδοτικότητα της ομαδικής εργασίας τόσο σε ένα μέρος όσο και σε περισσότερες τοποθεσίες.

Χαρακτηριστικό των πληροφοριακών συστημάτων είναι η δυνατότητά τους να λειτουργούν και να επικοινωνούν ασύρματα κι έτσι να υποστηρίζουν πρωτοποριακές εφαρμογές. Τα πληροφοριακά συστήματα παρουσιάζουν με οργανωμένο και ζωντανό τρόπο τις πληροφορίες έτσι ώστε να δημιουργούν γνώση και να προκαλούν το ανθρώπινο μυαλό για να λειτουργεί πιο αποτελεσματικά.

Στη σημερινή οικονομική και κοινωνική πραγματικότητα καμία εταιρία ή οργανισμός δεν πρέπει να αγνοήσει τις σύγχρονες τεχνολογίες και ιδιαίτερα τις πληροφορικές και τηλεπικοινωνιακές τεχνολογίες, γιατί σημαίνει ότι αγνοεί μια δύναμη η οποία μπορεί να καλυτερεύσει την παραγωγικότητά της, να διευρύνει τις αγορές της, να αυξήσει τα κέρδη της, να επιτρέψει τη δημιουργία νέων προϊόντων/υπηρεσιών και να θέσει σε κίνδυνο την επιβίωσή της μακροπρόθεσμα.

Τα πληροφοριακά συστήματα είναι οι εφαρμογές των τηλεπικοινωνιακών τεχνολογιών και μπορεί να έχουν επίκεντρο τις εσωτερικές λειτουργίες της επιχείρησης ή τις σχέσεις της με τους επιχειρηματικούς εταίρους, μπορεί να αποβλέπουν στην απλή αυτοματοποίηση των συναλλαγών αλλά και στην ίδια ακόμη την αναδιοργάνωση των λειτουργιών της επιχείρησης. Οποιαδήποτε κι

αν είναι η επικέντρωση, θα πρέπει το management της επιχείρησης να καταλαβαίνει τις επιπτώσεις των Πληροφοριακών Συστημάτων και να συνδέει τις δυνατότητές τους με τους στόχους της επιχείρησης.

Σύμφωνα με τα παραπάνω προκύπτει ότι η ασφάλεια των πληροφοριακών συστημάτων και γενικότερα των δικτύων των επιχειρήσεων αποτελεί εξίσου σημαντικό παράγοντα. Έτσι όλες οι εταιρείες καλούνται να επενδύσουν και στο τομέα της ασφάλειας, με το να λάβουν τα κατάλληλα μέτρα πρόληψης για αντιμετώπιση των ευπαθών σημείων των συστημάτων και των δικτύων τους, ώστε οι πληροφοριακοί πόροι κάθε επιχείρησης να είναι ασφαλής, αφού ολοένα και καινούργιες απειλές από κακόβουλα προγράμματα εισβάλλουν στα συστήματα αυτά και αδίστακτοι hackers υποκλέβουν, καταστρέφουν και παρακολουθούν σημαντικά αρχεία τους. Εάν δεν ληφθούν οι απαραίτητες εργασίες πρόληψης για την ασφάλεια των συστημάτων τα αποτελέσματα αυτής της άγνοιας θα είναι, επιπλέον η απώλεια εμπορικών ευκαιριών και παραγωγικών επενδύσεων των εταιρειών. Για το λόγο αυτό είναι απαραίτητη η ύπαρξη και ανάπτυξη μιας πολιτικής ασφαλείας, η οποία πρέπει να τηρείται αλλά και να αναβαθμίζεται με νέες ακόμα πιο σύγχρονες τεχνολογίες, σε κάθε εταιρεία από τη μικρότερη έως τη πιο μεγάλη, με σκοπό την αντιμετώπιση ακόμα νεότερων απειλών.

ΚΕΦΑΛΑΙΟ 1ο

1.1 ΕΝΝΟΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τα πληροφοριακά συστήματα συγκεντρώνουν, επεξεργάζονται, αποθηκεύουν, αναλύουν και διανέμουν πληροφορίες για ένα συγκεκριμένο σκοπό. Τα πληροφοριακά συστήματα αποτελούνται από οποιαδήποτε δεδομένα ή εντολές εισρέουν στο σύστημα, καθώς επίσης και αναφορές και υπολογισμούς τα οποία εκρέουν από αυτό. Επίσης, αποτελούνται από μηχανισμούς ανατροφοδότησης, οι οποίοι είναι υπεύθυνοι για τον έλεγχο της λειτουργίας του συστήματος. Τέλος, αποτελείται και από το περιβάλλον μέσα στο οποίο λειτουργεί.(Κιουντούζης Ε., 2002, σελ.112)

Ένα πληροφοριακό σύστημα βασισμένο στους υπολογιστές, είναι ένα πληροφοριακό σύστημα το οποίο χρησιμοποιεί τη τεχνολογία των υπολογιστών για να πραγματοποιήσει ορισμένες ή το σύνολο των εργασιών του. Πληροφοριακό σύστημα ονομάζεται κάθε περιβάλλον στο οποίο οι πόροι (πχ άνθρωποι και ηλεκτρονικοί υπολογιστές) συντονίζονται για την εκπλήρωση ενός ευρύτερου σκοπού. Επιμέρους και ανεξάρτητα υποσυστήματα συνεργάζονται ώστε να μετατρέψουν αρχικά δεδομένα υπό τη μορφή στοιχείων εισόδου σε πληροφορίες – στοιχεία εξόδου, που θα είναι χρήσιμες για την επίτευξη των στόχων μια οικονομικής μονάδας. (Τασόπουλος Α., 2005, σελ. 50)

Είναι φανερό λοιπόν ότι ένα Π.Σ. αποτελεί μια ειδική κατηγορία συστήματος, του οποίου τα στοιχεία είναι άνθρωποι, διαδικασίες και μηχανήματα, τα οποία αλληλεπιδρούν και συνεργάζονται για να επεξεργασθούν δεδομένα και να παρέχουν πληροφορία στο χρήστη. Το Π.Σ. είναι επομένως ένα επιχειρησιακό σύστημα, το οποίο επεξεργάζεται δεδομένα από το εσωτερικό και εξωτερικό περιβάλλον της επιχείρησης και παρέχει πληροφορίες στη διοίκηση της, έτσι ώστε να ληφθούν γρήγορα σωστές και έγκυρες αποφάσεις. (Γεωργ.Σ.Οικονόμου–Νικολ.Β.Γεωργοπούλου, 2004, σελ.24)

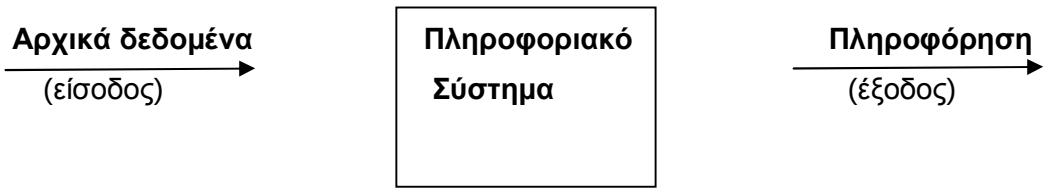
Πιο συγκεκριμένα, μικρότερες υπο-ομάδες συστημάτων αλληλεπιδρούν για να συγκεντρώσουν, επεξεργαστούν, ταξινομήσουν και καταχωρήσουν

πληροφορίες για προγραμματισμό, λήψη αποφάσεων και έλεγχο με τέτοιο τρόπο ώστε να υποστηρίζουν αποτελεσματικά την ομαλή λειτουργία του μεγαλύτερου συστήματος στο οποίο ανήκουν. (Τασόπουλος Α., 2005 σελ.52)

Ένα πληροφοριακό σύστημα είναι ένα σύμπλεγμα δεδομένων και πληροφοριών, δομημένα και επεξεργασμένα σε ένα προκαθορισμένων προδιαγραφών σύστημα. Περιλαμβάνει διαδικασίες αποθήκευσης, ανάκλησης και επεξεργασίας δεδομένων, έχει μηχανισμούς ελέγχου και λειτουργεί εντός του περιβάλλοντός του. (Κιουντούζης Ε., 2002, σελ.80)

Γενικότερα ένα Π.Σ. είτε χειρόγραφο είτε μηχανογραφικό, αποτελείται μεταξύ των άλλων και από τα ακόλουθα τέσσερα στοιχεία.

1. Συλλογή δεδομένων : Τα δεδομένα αφορούν αριθμούς, γεγονότα, συζητήσεις, διαδόσεις, κ.α.
2. Αποθήκευση δεδομένων : Τα δεδομένα είναι δυνατόν να αποθηκευτούν σε καρτελοθήκη, σε αρχείο, ή σε τράπεζα δεδομένων Η/Υ.
3. Επεξεργασία δεδομένων : Η επεξεργασία τους περιλαμβάνει κυρίως την ανάλυση, κωδικοποίηση, ταξινόμηση και σύνθεση τους.
4. Παρουσίαση της πληροφορίας : Η παρουσίαση της πληροφορίας στο χρήστη γίνεται στη μορφή που αυτός τη χρειάζεται.(Γεωργ. Σ.Οικονόμου–Νικολ.Β.Γεωργοπούλου, 2004, σελ.22)



Τα δεδομένα ως αρχικές εισροές προέρχονται από πραγματικά γεγονότα, αριθμούς ή ακόμη και σύμβολα. Στην αρχική τους αυτή μορφή, ενδέχεται να μην έχουν καθόλου νόημα ή ουσία.

Ανάλογα με τις πηγές προέλευσής τους ή τον τρόπο συλλογής τους, μπορούν να διακριθούν στις παρακάτω κατηγορίες:

- Δεδομένα που συλλέγονται με ένα τυποποιημένο και επαναληπτικό ρυθμό ρουτίνας από εξωτερικά γεγονότα.
- Δεδομένα που συλλέγονται με ένα τυποποιημένο και επαναληπτικό ρυθμό ρουτίνας από τις εσωτερικές λειτουργίες της επιχείρησης. Πχ από άλλα τμήματα.
- Πρωτότυπα και διακριτά δεδομένα, που δεν συναντώνται συχνά και προέρχονται από εξωτερικές πηγές, όπως κυβερνητικές αποφάσεις που επηρεάζουν την επιχειρησιακή λειτουργία του οργανισμού ή άλλους κοινωνικούς ή οικονομικούς φορείς.
- Δεδομένα που προέρχονται από αποφάσεις του ανώτερου διοικητικού κλιμακίου της επιχείρησης και δεν συναντώνται σε καθημερινή βάση. (Βασιλακόπουλος Γ., Χρυσικόπουλος Β., 1990, σελ.35)

Όταν προχωρήσουν στο επόμενο στάδιο και διαμέσου του πληροφοριακού συστήματος, τα αρχικά δεδομένα μετατρέπονται σε πληροφορία. Η πληροφορία δηλαδή είναι το προϊόν ενός πληροφοριακού συστήματος όπως προκύπτει από την επεξεργασία των δεδομένων, έχει νόημα και επιχειρησιακή αξία, ενώ βρίσκεται σε μια ορθολογική μορφή ώστε να μπορεί να χρησιμοποιηθεί από τους χρήστες των πληροφοριακών συστημάτων.

Γίνεται κατανοητός ο ρόλος του πληροφοριακού συστήματος στη μετατροπή των δεδομένων σε πληροφορίες, αφού εάν δεν λειτουργεί αποτελεσματικά δύναται να οδηγήσει σε ψευδείς πληροφορίες λανθασμένου περιεχομένου με ό,τι αυτό συνεπάγεται για τη λήψη αποφάσεων.

Για να λειτουργήσει με αποτελεσματικότητα ένα πληροφοριακό σύστημα χρειάζεται διάφορες πηγές, ανεξαρτήτου μεγέθους της εταιρίας ή απαιτήσεων. Οι πηγές θα πρέπει να προέρχονται από τον εξοπλισμό που χρησιμοποιεί η επιχείρηση, τους πόρους με τους οποίους δουλεύει, το προσωπικό που μεσολαβεί στη παροχή δεδομένων από τις πηγές αλλά και τις πηγές χρηματοδότησης όλων των επιπέδων λειτουργίας. (Scriven D.,Scriven J.,Kozoll C., σελ.63)

Στο σημείο αυτό, τονίζουμε πως αυτό που προκύπτει από τη μέχρι τώρα παρουσίαση είναι ότι οι χρήστες, το τμήμα των Π.Σ. και η διοίκηση της επιχείρησης θα πρέπει να έχουν ένα κοινό ορισμό για το Π.Σ., διότι μόνο τότε είναι δυνατό να προσφέρει τα καλύτερα δυνατά αποτελέσματα από τη χρήση

του. Άρα συνάγεται ότι οι κύριες γενικές λειτουργίες ενός Π.Σ. είναι οι ακόλουθες:

- Η αναγνώριση και κάλυψη των πληροφοριακών αναγκών των χρηστών.
- Η επιλογή συναφών δεδομένων από τη μεγάλη ποικιλία των δεδομένων στο εσωτερικό και εξωτερικό περιβάλλον της επιχείρησης.
- Η δημιουργία της πληροφορίας από τα επιλεγμένα δεδομένα με τη χρήση των κατάλληλων εργαλείων.
- Η μεταφορά της δημιουργημένης πληροφορίας στους χρήστες.(Γεωργ.Σ.Οικονόμου–Νικολ.Β.Γεωργοπούλου,2004, σελ.25)

Επιπρόσθετα θα μπορούσαμε να αναφέρουμε σαν Σύστημα τον όρο που σημαίνει μια ορισμένη λειτουργία και να εξυπηρετεί κάποιο συγκεκριμένο σκοπό. Η τεχνική χρήση του όρου σημαίνει ότι αποτελείται από επιμέρους στοιχεία, που αλληλεπιδρούν μεταξύ τους, χαρακτηρίζεται από οργάνωση και εξετάζεται ως μια ενιαία ολότητα, την επιχείρηση ή τον οργανισμό.

Η χρήση του όρου Πληροφοριακό Σύστημα ο οποίος ταυτίζεται λανθασμένα με τον όρο Τεχνολογία Πληροφορικής ή Τεχνολογική Υποδομή, αντιστοιχεί σε ένα οργανωμένο σύνολο από 5 στοιχεία (άνθρωποι, λογισμικό, υλικό, διαδικασίες και δεδομένα).

Καθώς η Τεχνολογία της Πληροφορικής στηρίζεται στις τεχνολογίες των υπολογιστών, τηλεπικοινωνιών, μηχανών γραφείου και ηλεκτρολογικού εξοπλισμού για τη διαχείριση πληροφοριών, που παρέχονται σε ανθρώπους. Οι πληροφορίες μπορεί να είναι κείμενο, εικόνα, δεδομένα (αριθμοί, σύμβολα κ.λ.π.), σήματα, ήχος. Έτσι αυτά τα 5 στοιχεία αλληλεπιδρούν μεταξύ τους και με το περιβάλλον με σκοπό τη παραγωγή και διαχείρισης της πληροφορίας, για την υποστήριξη των ανθρώπινων δραστηριοτήτων στα πλαίσια του οργανισμού.

Συνεπώς ένα πακέτο λογισμικού είναι Τεχνολογική Υποδομή. Ενταγμένο όμως μέσα στο πλαίσιο λειτουργίας ενός γραφείου με τους υπαλλήλους, τις διαδικασίες και το περιβάλλον του οργανισμού, είναι Πληροφοριακό Σύστημα.

διαδικασίες και το περιβάλλον του οργανισμού, είναι Πληροφοριακό Σύστημα.

Πληροφοριακό Σύστημα = Τεχνολογική Υποδομή + Οργανωσιακό Πλαίσιο. (Σωκρ.Κάτσικας-Δημ.Γκρίζαλης-Στεφ.Γκρίτζαλης, 2004, σελ.319)

1.2 ΣΥΣΤΑΤΙΚΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τα συστατικά των πληροφοριακών συστημάτων είναι τα εξής έξι:

- **Εξοπλισμός Η/Υ:** Είναι το σύνολο των εξαρτημάτων, όπως ο επεξεργαστής, η οθόνη, το πληκτρολόγιο και ο εκτυπωτής, τα οποία συνθέτουν έναν Η/Υ και τα περιφερειακά του.
- **Λογισμικό:** Αποτελεί το σύνολο των προγραμμάτων, το οποίο δίνει τη δυνατότητα στον εξοπλισμό του Η/Υ να πραγματοποιήσει την επεξεργασία των δεδομένων
- **Βάση δεδομένων:** Είναι μια συλλογή από σχετικά αρχεία, πίνακες, σχέσεις κλπ, στα οποία ουσιαστικά αποθηκεύονται τα δεδομένα
- **Δίκτυο:** Αποτελεί το σύστημα σύνδεσης, το οποίο επιτρέπει στους υπολογιστές να μοιράζονται τους ίδιους πόρους, όπως περιφερειακά, βάση δεδομένων, κλπ.
- **Διαδικασίες:** Οι διαδικασίες αποτελούν ένα σύνολο από εντολές που αφορούν στον τρόπο με τον οποίο συνδέονται όλα τα παραπάνω συστατικά
- **Άνθρωποι:** Ή αλλιώς ανθρώπινο δυναμικό. Ουσιαστικά, είναι όλα τα άτομα που εργάζονται με το σύστημα ή χρησιμοποιούν τις εκροές του.(Γκίνογλου Δ., Ταχυνάκη Π., Πρωτοψάλτη Ν., 2004, σελ.98)

1.3 ΚΥΡΙΟΤΕΡΕΣ ΔΥΝΑΤΟΤΗΤΕΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τα πληροφοριακά συστήματα είναι σε θέση να πραγματοποιήσουν ορισμένες λειτουργίες με πολύ χαμηλότερο κόστος από αυτό της ανθρώπινης χειρωνακτικής παρέμβασης. Πρώτα απ' όλα τα πληροφοριακά συστήματα πραγματοποιούν υψηλής ταχύτητας και μεγάλης ποσότητας αριθμητικούς υπολογισμούς. Παρέχουν, επίσης, γρήγορη, ορθή και χαμηλού κόστους

επικοινωνία στο εσωτερικό της επιχείρησης, αλλά και μεταξύ των οργανισμών.

Τα πληροφοριακά συστήματα είναι σε θέση να αποθηκεύουν μεγάλο όγκο πληροφοριών σε έναν εύκολα προσβάσιμο και σχετικά μικρό χώρο. Επιτρέπουν, επίσης, γρήγορη και φθηνή πρόσβαση σε μεγάλο πλήθος πληροφοριών, παγκοσμίως. Τα συστήματα αυτά είναι σε θέση να επιταχύνουν τις διαδικασίες εκτύπωσης και σύνταξης, προκειμένου να ελαχιστοποιήσουν το χρόνο που απαιτείται για την ολοκλήρωση αυτών των διαδικασιών. (Παπαθανασίου Α., 2008,σελ. 203)

Η αυτοματοποίηση των ημι-αυτοματοποιημένων επιχειρηματικών διαδικασιών, αλλά και των χειρωνακτικών καθηκόντων είναι μια ακόμη από τις δυνατότητες των πληροφοριακών συστημάτων. Η χρήση των συστημάτων αυτών αυξάνει την αποτελεσματικότητα και την αποδοτικότητα της ομαδικής εργασίας τόσο σε ένα μέρος όσο και σε περισσότερες τοποθεσίες. Χαρακτηριστικό των πληροφοριακών συστημάτων είναι η δυνατότητά τους να λειτουργούν και να επικοινωνούν ασύρματα κι έτσι να υποστηρίζουν πρωτοποριακές εφαρμογές. Τα πληροφοριακά συστήματα παρουσιάζουν με οργανωμένο και ζωντανό τρόπο τις πληροφορίες έτσι ώστε να δημιουργούν γνώση και να προκαλούν το ανθρώπινο μυαλό για να λειτουργεί πιο αποτελεσματικά.(Βασιλακόπουλος Γ., Χρυσικόπουλος Β., 1990, σελ.127)

Σε κάθε περίπτωση ο σχεδιασμός ενός πληροφοριακού συστήματος γίνεται για να δώσεις λύσεις σε υπάρχοντα επιχειρησιακά προβλήματα. Ορισμένα από τα αυτά τα επιχειρησιακά προβλήματα είναι το λειτουργικό κόστος που προκύπτει και το οποίο έρχεται να το μειώσει. (Κιουντούζης Ε., 2002, σελ.85)

Επίσης, βελτιώνει το κομμάτι της εξυπηρέτησης πελατών, αλλά και την επιχειρηματική ανταγωνιστικότητα της οικονομικής μονάδας. Τέλος, σημαντικός σκοπό των πληροφοριακών συστημάτων είναι η συμβολή τους στην ανάπτυξη νέων προϊόντων και υπηρεσιών. (Παπαθανασίου Α., 2008, σελ.232)

Οι προδιαγραφές χρησιμεύουν για την ανάπτυξη οποιουδήποτε συστήματος πριν από την έναρξη της ανάπτυξής του και στην ουσία αποτελούν συγκριτικές μετρήσεις επιδόσεων για την αξιολόγηση της σχεδίασης καθώς και της υλοποίησής της. Διευκολύνουν επίσης τη

διασφάλιση ποιότητας μέσω της επαλήθευσης και την επικύρωση ότι το σύστημα που «χτίζεται» ικανοποιεί τις υπάρχουσες ανάγκες. (Κιουντούζης Ε., 2002, σελ.89)

Για την ανάπτυξη των προδιαγραφών χρησιμοποιούνται πηγές δεδομένων που διακρίνονται σε δύο τύπους:

- *Εξωτερικές*, που είναι τακτικές και επαναλαμβανόμενες (πχ στοιχεία τιμολογίων) ή μη τακτικές (πχ. στοιχεία για ολόκληρο τον κλάδο)
- *Εσωτερικές*, που είναι τακτικές και επαναλαμβανόμενες και δεν απαιτείται η συναλλαγή με τρίτους (πχ ώρες απασχόλησης εργαζομένων) ή μη επαναλαμβανόμενες (πχ ποσοστά εκπτώσεων κτλ) (Παπαθανασίου Α., 2008, σελ.235)

Τα χαρακτηριστικά, όπως αυτά αναλύονται παρακάτω, κάνουν κατανοητές τις πολυπλοκότητες που συνθέτουν την οργάνωση και διοίκηση των πληροφοριακών συστημάτων. Πρώτα απ' όλα, πρέπει να γνωρίζουμε ότι τα πληροφοριακά συστήματα είναι συνδεδεμένα μέσω ηλεκτρονικών δικτύων. (Κιουντούζης Ε., 2002, σελ.93)

Ένα συγκεκριμένο πληροφοριακό σύστημα μπορεί να αποτελείται από αρκετά ξεχωριστά πληροφοριακά συστήματα. Ωστόσο, αρκετά διαφορετικά πληροφοριακά συστήματα μπορούν να υπάρχουν σε έναν οργανισμό. Επίσης, τα διεπιχειρησιακά πληροφοριακά συστήματα συνδέουν τη ροή πληροφοριών σε δύο ή περισσότερους οργανισμούς. (Scriven D., Scriven J., Kozoll C., σελ.102)

Τέλος, ένα enterprise wide σύστημα ή διοργανωσιακό πληροφοριακό σύστημα, αποτελείται από μεγάλους και μικρούς υπολογιστές και λογισμικό συνδεδεμένα με διαφορετικούς τύπους δικτύων. (Κιουντούζης Ε., 2002, σελ.104)

1.4 ΤΑΞΙΝΟΜΗΣΗ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τα πληροφοριακά συστήματα μπορούν να ταξινομηθούν σύμφωνα με:

- ***την οργανωσιακή δομή***
- ***την περιοχή λειτουργίας***
- ***την παρεχόμενη υποστήριξη***
- ***την αρχιτεκτονική συστήματος***
- ***τις ενέργειες/ λειτουργίες που υποστηρίζουν*** (Scriven D.,Scriven J.,Kozoll C., σελ.125)

1.4.1 ΤΑΞΙΝΟΜΗΣΗ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΑΝΑ ΟΡΓΑΝΩΣΙΑΚΗ ΔΟΜΗ

Σύμφωνα με την οργανωσιακή δομή τους, τα πληροφοριακά συστήματα ταξινομούνται σε:

- ***Πληροφοριακά συστήματα τμημάτων/ διευθύνσεων (departmental I.S.).***

  Ένας οργανισμός χρησιμοποιεί αρκετά προγράμματα εφαρμογών σε μία λειτουργική περιοχή ή τμήμα.
- ***Εταιρικά πληροφοριακά συστήματα (enterprise I.S.)***Χρησιμοποιούνται από τα περισσότερα μέρη του οργανισμού, ενώ εμφανίζεται μια ροπή προς συστήματα ERP(Enterprise Resource Planing) ή Συστήματα Σχεδιασμού των Επιχειρησιακών Πόρων, τα οποία υποστηρίζουν μεγάλο μέρος των επιχειρησιακών διαδικασιών.)
- ***Διεπιχειρησιακά πληροφοριακά συστήματα (inter-organisational I.S. – IOS)***

  Είναι τα συστήματα που συνδέουν δύο ή περισσότερους οργανισμούς και είναι κοινά ανάμεσα σε επιχειρηματικούς συνεργάτες και ευρέως χρησιμοποιούμενα για Ηλεκτρονικό εμπόριο, συχνά μέσω extranet (επέκταση του εσωτερικού δικτύου με επιπλέον τοποθεσίες για ασφαλή απομακρυσμένη πρόσβαση μέσω ανασφαλών γραμμών επικοινωνίας (Σωκρ.Κάτσικας-Δημ.Γκρίζαλης-Στεφ.Γκρίτζαλης, 2004, σελ.187)).
  (Scriven D.,Scriven J.,Kozoll C.)

1.4.2 ΤΑΞΙΝΟΜΗΣΗ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΑΝΑ ΠΕΡΙΟΧΗ ΛΕΙΤΟΥΡΓΙΑΣ

Σε κάθε περιοχή λειτουργίας, υπάρχουν κάποια καθήκοντα ρουτίνας και επαναλαμβανόμενα, ουσιώδη για τη λειτουργία του οργανισμού. Επίσης, τα πληροφοριακά συστήματα που υποστηρίζουν αυτά τα καθήκοντα ονομάζονται συστήματα διεκπεραίωσης συναλλαγών.

Ανά περιοχή λειτουργίας έχουμε τα εξής συστήματα:

- Τα λογιστικά πληροφοριακά συστήματα (accounting I.S.)
- Τα οικονομικά πληροφοριακά συστήματα (finance I.S.)
- Τα κατασκευαστικά (λειτουργίες/ παραγωγή) πληροφοριακά συστήματα (manufacturing I.S.)
- Τα πληροφοριακά συστήματα μάρκετινγκ (marketing I.S.)
- Τα πληροφοριακά συστήματα διοίκησης ανθρώπινων πόρων (H.R.M. I.S.) (Laudon, K., Laudon, J, 1998, σελ.146)

1.4.3 ΤΑΞΙΝΟΜΗΣΗ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΑΝΑ ΠΑΡΕΧΟΜΕΝΗ ΥΠΟΣΤΗΡΙΞΗ

Τα πληροφοριακά συστήματα ταξινομούνται σύμφωνα με την παρεχόμενη υποστήριξη στις εξής κατηγορίες:

- ***Συστήματα διεκπεραίωσης συναλλαγών***

  Τα συστήματα διεκπεραίωσης συναλλαγών πραγματοποιούν επαναληπτικά αποστολή και κρίσιμες ενέργειες για το υπαλληλικό προσωπικό.

- ***Πληροφοριακά συστήματα διοίκησης***

  Τα πληροφοριακά συστήματα διοίκησης ασχολούνται με λειτουργικές ενέργειες και διοικητικά θέματα. Ο κύριος σκοπός των συστημάτων αυτών είναι η διατήρηση αρχείων και η ταχύτατη επεξεργασία μεγάλου όγκου δεδομένων, δεν υποστηρίζουν την διαδικασία λήψης αποφάσεων, παρόλο που θεωρούνται ότι είναι επιχειρησιακά εργαλεία. Παρέχουν στα διευθυντικά στελέχη τις πληροφορίες που είναι απαραίτητες στην

διαδικασία λήψης αποφάσεων (Γεωργίου Σ.Οικονόμου–Νικολάου Β.Γεωργοπούλου, 2004, σελ.97).

- ***Συστήματα αυτοματοποίησης γραφείου***

  Τα συστήματα αυτοματοποίησης γραφείου αφορούν κυρίως τους υπάλληλους γραφείου

- ***Συστήματα υποστήριξης αποφάσεων***

  Αντιθέτως, τα συστήματα υποστήριξης αποφάσεων περιλαμβάνουν τη λήψη αποφάσεων από μάνατζερ και αναλυτές. Βοηθούν τα διευθυντικά στελέχη στην επίλυση των προβλημάτων εκείνων στα οποία δεν μπορεί να δοθεί μία άμεση απάντηση, διότι απαιτείται ανθρώπινη παρέμβαση, που είναι η κρίση του διευθυντικού στελέχους και η υποκειμενική του ανάλυση. Έτσι η απάντηση στο πρόβλημα δίνεται από την αλληλεπίδραση του ανθρώπου με τον Η/Υ (Γεωργίου Σ.Οικονόμου–Νικολάου Β.Γεωργοπούλου, 2004, σελ.98).

- ***Πληροφοριακά συστήματα ανώτατης διοίκησης***

  Στα πληροφοριακά συστήματα ανώτατης διοίκησης απευθύνονται οι μάνατζερ υψηλής βαθμίδας

- ***Συστήματα υποστήριξης ομάδων***

  Τα άτομα που δουλεύουν σε ομάδες θα ασχοληθούν με τα πληροφοριακά συστήματα υποστήριξης ομάδων

- ***Συστήματα υποστήριξης νοημοσύνης***

  Υπάλληλοι που χρησιμοποιούν και διαχειρίζονται γνώση, χρησιμοποιούν τα πληροφοριακά συστήματα υποστήριξης νοημοσύνης
  (Τασόπουλος Α., 2005, σελ.69)

1.5 ΤΥΠΟΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Υπάρχουν διάφοροι τρόποι ταξινόμησης των πληροφοριακών συστημάτων, ανάλογα με τις ανάγκες που υπάρχουν κατά την ανάλυση και αξιολόγησή τους:

Α. *Ταξινόμηση με βάση τον τρόπο επεξεργασίας*

- **Συστήματα επεξεργασίας κατά δεσμίδες** (batch): Οι συναλλαγές συλλέγονται καθώς παράγονται, αλλά επεξεργάζονται περιοδικά, για παράδειγμα μια φορά την ημέρα ή την εβδομάδα.
- **Συστήματα κατά δεσμίδες σε απευθείας σύνδεση** (on-line batch): Οι πληροφορίες των συναλλαγών συλλέγονται από τις συσκευές εισαγωγής δεδομένων σε απευθείας σύνδεση και εισάγονται στο σύστημα, αλλά υποβάλλονται σε επεξεργασία περιοδικά όπως στα συστήματα επεξεργασίας κατά δεσμίδες.
- **Συστήματα σε απευθείας σύνδεση πραγματικού χρόνου** (on-line real batch): Η συλλογή των δεδομένων των συναλλαγών καθώς επίσης και η επεξεργασία τους προκειμένου να ενημερωθούν τα αρχεία πραγματοποιούνται σε πραγματικό χρόνο τη στιγμή που πραγματοποιείται η συναλλαγή. (Τασόπουλος Α., 2005)

Β. *Ταξινόμηση με βάση το στόχο*

- **Συστήματα επεξεργασίας συναλλαγών** (Transaction Processing Systems): Χωρίς την επεξεργασία των συναλλαγών πολλές από τις λειτουργίες και τις δραστηριότητες της επιχείρησης θα ήταν αδύνατο να πραγματοποιηθούν, π.χ. δε θα λαμβάνονταν παραγγελίες, δε θα πληρώνονταν λογαριασμοί, δε θα παραγγέλνονταν ανταλλακτικά, κ.α. Με ένα σύστημα επεξεργασίας συναλλαγών αυτοματοποιείται η συλλογή και η επεξεργασία των δεδομένων. Το κύριο χαρακτηριστικό αυτών των Π.Σ. είναι η δυνατότητα τους να αντιμετωπίζουν επαναλαμβανόμενες διαδικασίες. Ο στόχος τους είναι να επεξεργαστούν τις συναλλαγές προκειμένου να ενημερωθούν τα αρχεία και να παραχθούν οι εκθέσεις. Ένα σύστημα επεξεργασίας συναλλαγών υποστηρίζει κυρίως τις δραστηριότητες του λειτουργικού ελέγχου και τις εργασίες ρουτίνας με την παραγωγή αναφορών και την επεξεργασία των συναλλαγών. Με άλλα λόγια την εποχή αυτή οι Η/Υ θεωρούνταν ως μέσα για τη βελτίωση της απόδοσης των λειτουργιών εκείνων, που είχαν σχέση με ‘’διακίνηση εντύπων’’ παρά ως μέσα για

την υποστήριξη των πληροφοριακών αναγκών των διευθυντικών στελεχών (Γ.Σ.Οικονόμου-Ν.Β.Γεωργοπούλου, 2004, σελ.72).

- **Συστήματα στήριξης αποφάσεων** (Decision Support Systems): Ο στόχος τους είναι να υποστηρίξουν διευθυντικές αποφάσεις. Συνήθως, αυτά τα συστήματα είναι βασισμένα σε μοντέλα από το χώρο λήψης αποφάσεων και χρησιμοποιούν τεχνικές από τη διοικητική επιστήμη, τη χρηματοοικονομική ή άλλους λειτουργικούς τομείς της επιχείρησης. Αυτά τα συστήματα χρησιμοποιούνται επίσης συχνά για λόγους εστίασης της προσοχής. Πχ για την εστίαση της προσοχής των διευθυντικών στελεχών σε μια προβληματική πτυχή των διαδικασιών. Το κύριο χαρακτηριστικό των συστημάτων αυτών είναι ότι βοηθούν στη λύση κυρίως προβλημάτων που ένα μέρος τους μπορεί να προγραμματισθεί/δομηθεί και το οποίο λύνεται από τον Η/Υ, και ένα μέρος τους δεν μπορεί να προγραμματισθεί/δομηθεί και για το οποίο χρειάζεται η διαίσθηση και η κρίση του διευθυντικού στελέχους για να δοθεί η λύση (Γ.Σ.Οικονόμου-Ν.Β.Γεωργοπούλου, 2004, σελ.93).
- **Εμπειρογνώμονα συστήματα** (Expert Systems): Αυτά τα συστήματα ενσωματώνουν την πείρα στον οικονομικό τομέα, προκειμένου να βοηθηθούν οι διευθυντές στη διάγνωση ή στην επίλυση των προβλημάτων. Τα συστήματα αυτά δίνουν λύση σε προβλήματα για τα οποία χρειάζεται ανθρώπινη γνώση και εμπειρία. Είναι δηλ. προγράμματα Η/Υ, τα οποία μιμούνται τον τρόπο με τον οποίο τα στελέχη των επιχειρήσεων και οργανισμών λαμβάνουν τις αποφάσεις τους, όπως π.χ. είναι αποφάσεις σχετικές με επιλογή και πρόκριση επενδύσεων, με την διερεύνηση της αξιοπιστίας των πελατών που ζητούν υψηλά δάνεια από τράπεζες κ.α (Γ.Σ.Οικονόμου-Ν.Β.Γεωργοπούλου, 2004, σελ.99).
- **Συστήματα παροχής αναφορών** (Information Reporting Systems): Ο στόχος τους είναι να παρέχουν στους διευθυντές μιας επιχείρησης εκθέσεις και αναφορές που προκύπτουν από την επεξεργασία των συναλλαγών. Για να λειτουργήσουν επικοινωνούν με τα Συστήματα Επεξεργασίας Συναλλαγών.
- **Συστήματα προγραμματισμού επιχειρησιακών πόρων** (Enterprise Resource Planning): Είναι συστήματα που στοχεύουν στον

προγραμματισμό και την υλοποίηση σχεδίων για την επίτευξη υψηλού βαθμού ολοκλήρωσης και ενοποίησης των διαδικασιών του οργανισμού και την αξιόπιστη συντήρηση κοινών βάσεων δεδομένων. (Τασόπουλος Α., 2005, σελ.72)

C. *Ταξινόμηση βασισμένη στη φύση της αλληλεπίδρασης με το περιβάλλον*

- **Μετασχηματιστικά συστήματα**: Τα συστήματα αυτά μετασχηματίζουν τις εισόδους - εισροές που παραλαμβάνονται από το περιβάλλον σε εξόδους - εκροές, πχ εκθέσεις.
- **Διαδραστικά συστήματα**: Αυτά είναι συστήματα που σε μεγάλο βαθμό χαρακτηρίζονται από το ότι οδηγούνται από γεγονότα που πρέπει συνεχώς να αντιδρούν στα εξωτερικά και εσωτερικά ερεθίσματα. (Τασόπουλος Α., 2005, σελ.86)

D. *Ταξινόμηση βασισμένη στην τυποποίησή τους:*

Άτυπο: Χαρακτηρίζεται ένα σύστημα όταν δεν ακολουθούνται κατά την είσοδο σε αυτό ή την έξοδο από αυτό κάποιες προκαθορισμένες τυπικές διαδικασίες, πχ διαδικασίες επιβεβαίωσης μιας παραγγελίας. Χωρίς αυτό να σημαίνει, ότι οι παρεχόμενες από αυτά τα συστήματα πληροφορίες δεν είναι ζωτικής σημασίας για τις λειτουργίες τις επιχείρησης (Γ.Σ.Οικονόμου-Ν.Β.Γεωργοπούλου, 2004,σελ.133).

Τυπικό: Είναι ένα πληροφοριακό σύστημα όταν ακολουθούνται κατά την είσοδο σε αυτό ή την έξοδο από αυτό κάποιες συγκεκριμένες και προκαθορισμένες τυπικές διαδικασίες. Τυπικά συστήματα πληροφοριών είναι εκείνα που βασίζονται σε προκαθορισμένους κανόνες και διαδικασίες για την επεξεργασία των δεδομένων. Με άλλα λόγια ο τρόπος επεξεργασίας των δεδομένων για την παροχή της απαραίτητης πληροφόρησης, είναι γνωστός εκ των προτέρων (Γεωργίου Σ.Οικονόμου–Νικολάου Β.Γεωργοπούλου, 2004, σελ.133).

Όσον αφορά τα λογιστικά πληροφοριακά συστήματα συγκεκριμένα, τα συστατικά τους όπως η μισθοδοσία ή η γενική λογιστική είναι συνήθως συστήματα επεξεργασίας κατά δεσμίδες, επίσης συστήματα επεξεργασίας συναλλαγών που είναι μετασχηματιστικά συστήματα. Ωστόσο, τα συστήματα για τον προσδιορισμό ενός αντιπροσωπευτικού δείγματος για την απόκτηση ελεγκτικών τεκμηρίων και την πραγματοποίηση ενός ελεγκτικού στόχου, μπορούν να είναι συστήματα στήριξης αποφάσεων. Τέλος, τα συστήματα υποβοήθησης της αξιολόγησης του ελεγκτικού κινδύνου και την επιλογής των

κατάλληλων ενεργειών για την εκτέλεση ελεγκτικών διαδικασιών δύναται να είναι εμπειρογνώμονα συστήματα. (Τασόπουλος Α., 2005, σελ.87)

1.6 ΛΕΙΤΟΥΡΓΙΚΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΔΙΟΙΚΗΣΗΣ

Τα λειτουργικά πληροφοριακά συστήματα εγκαθίστανται για να εξασφαλίσουν ότι οι επιχειρηματικές στρατηγικές θα εκπληρωθούν με αποτελεσματικό τρόπο. Ένα λειτουργικό πληροφοριακό σύστημα παρέχει περιοδικές πληροφορίες για θέματα όπως λειτουργική αποδοτικότητα, αποτελεσματικότητα και παραγωγικότητα εξάγοντας πληροφορία από την εταιρική βάση δεδομένων και διεκπεραιώνοντάς τη σύμφωνα με τις ανάγκες των χρηστών. Τα Marketing Information System (M.I.S.) χρησιμοποιούνται επίσης για σχεδιασμό, παρακολούθηση και έλεγχο.

Μια πρόβλεψη πωλήσεων ανά περιοχή μπορεί να βοηθήσει το διευθυντή μάρκετινγκ να πάρει καλύτερες αποφάσεις όσον αφορά στη διαφήμιση και την τιμολόγηση. Οι πληροφορίες ανθρωπίνων πόρων παρέχουν στο διευθυντή ημερήσιες αναφορές με το ποσοστό εργαζομένων σε διακοπές ή σε ανάρρωση σε σύγκριση με προβλεπόμενα ποσοστά. (Γκίνογλου Δ., Ταχυνάκη Π., Πρωτοψάλτη Ν., 2004, σελ.92)

1.6.1 ΧΡΗΣΤΕΣ ΤΩΝ ΛΕΙΤΟΥΡΓΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Οι χρήστες των Λειτουργικών Πληροφοριακών Συστημάτων μπορούν να διακριθούν σε:

- **Εσωτερικούς χρήστες**: Αυτοί που βρίσκονται στο εσωτερικό περιβάλλον της επιχείρησης συμπεριλαμβάνοντας τους managers και τους υπαλλήλους όλης της διοικητικής κλίμακας. Οι βασικότεροι χρήστες μέσα σε μία επιχείρηση διακρίνονται σε τέσσερις κατηγορίες : στο *Υπαλληλικό Προσωπικό*, όπου ασχολείται κυρίως με τις διαδικασίες της εισόδου και του ελέγχου των δεδομένων, παρά με την ερμηνεία των πληροφοριών που παίρνουμε από το Π.Σ. και την εξαγωγή συμπερασμάτων. Τα *Διευθυντικά Στελέχη* πρώτης γραμμής όπου ασχολούνται κυρίως με λειτουργικές αποφάσεις, η υποστήριξη

των οποίων βασίζεται ως επί το πλείστον σε λειτουργική πληροφόρηση. Τις πληροφορίες αυτές μπορούν να τις αποκτήσουν από τα συστήματα επεξεργασίας συναλλαγών και την τράπεζα δεδομένων. Στα *Επιτελικά Στελέχη* τα οποία βοηθούν τους διευθύνοντες ανώτερων βαθμίδων σε συγκεκριμένες λειτουργικές περιοχές της Διοίκησης των επιχειρήσεων. Αυτό γίνεται διότι τα ανώτερα στελέχη ενδέχεται να μην έχουν τον χρόνο και τις γνώσεις να πραγματοποιούν την ανάλυση μόνα τους, καθώς απαιτούνται εξειδικευμένες γνώσεις επεξεργασίας δεδομένων σε πολλά μοντέλα λήψης αποφάσεων. Τέλος, τα *Διευθυντικά Στελέχη* των Ανώτερων Βαθμίδων Διοίκησης εξυπηρετούνται από τα Συστήματα Υποστήριξης Διοίκησης ,τα συστήματα αυτά επεξεργάζονται δεδομένα από το εξωτερικό και εσωτερικό περιβάλλον, έτσι ώστε να διαπιστωθεί τι συμβαίνει στα κατώτερα επίπεδα διοικητικής ιεραρχίας. Έτσι παρέχουν σημαντική βοήθεια στον εντοπισμό των προβλημάτων και των ευκαιριών και στη διαδικασία της λήψης αποφάσεων (Γεωργίου Σ.Οικονόμου–Νικολάου Β.Γεωργοπούλου, 2004, σελ.100).

- **Εξωτερικούς χρήστες**: Αυτοί βρίσκονται στο εξωτερικό περιβάλλον της επιχείρησης, όπως οι πιστωτές, οι προμηθευτές, οι Τράπεζες, οι πελάτες κτλ. (Γκίνογλου Δ., Ταχυνάκη Π., Πρωτοψάλτη Ν., 2004)

Να σημειωθεί ότι οι πληροφορίες που παρέχει ένα Λειτουργικό Πληροφοριακό Σύστημα χρησιμοποιούνται και από τις δύο κατηγορίες χρηστών, με διαφορετικό όμως τρόπο και με διαφορετικό σκοπό. Πχ. ο manager του τμήματος πωλήσεων έχει διαφορετική σκοπιμότητα στη χρήση των πληροφοριών από έναν εξωτερικό προμηθευτή της εταιρίας. (Laudon K., Laudon J., 1998)

1.7 ΔΙΟΙΚΗΤΙΚΑ/ΣΤΡΑΤΗΓΙΚΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Είναι επίσης γνωστά ως τακτικά συστήματα, χειρίζονται ενέργειες μέσω management. Χρησιμοποιούν επίσης κυρίως εσωτερικές πηγές δεδομένων.

Παρέχουν τους ακόλουθους τύπους υποστήριξης, όπως είναι οι στατιστικές περιλήψεις, οι περιοδικές και με συγκεκριμένο στόχο αναφορές, οι

προβλέψεις, οι αποφάσεις ρουτίνας, οι αναφορές εξαίρεσης, η συγκριτική ανάλυση, η πρώιμη ανίχνευση προβλημάτων, καθώς επίσης και η σύνδεση. (Scriven D., Scriven J., Kozoll C., σελ.74)

Τα Στρατηγικά Πληροφοριακά Συστήματα σχετίζονται με αποφάσεις που αλλάζουν σημαντικά τον τρόπο με τον οποίο λειτουργεί ή δραστηριοποιείται μια επιχείρηση. Συνήθως τα Strategic Information Systems, χειρίζονται τον μακροπρόθεσμο σχεδιασμό που σκιαγραφεί στρατηγικές και σχέδια για πέντε χρόνια. (Laudon K., Laudon J., 1998, σελ.96)

Αντιδρούν επίσης προδραστικά σε ενέργεια ενός μείζονος ανταγωνιστή ή σε οποιαδήποτε άλλη σημαντική ενέργεια στο περιβάλλον της επιχείρησης. Ξεκινούν μία αλλαγή σε έναν οργανισμό με έναν πρώιμο (pro-active) τρόπο για να αυξηθεί η ανταγωνιστικότητα. (Τασόπουλος Α., 2005, σελ.71)

Τα Στρατηγικά Πληροφοριακά Συστήματα βοήθησαν επιχειρήσεις να βελτιώσουν τον τρόπο εκτέλεσης των επιχειρηματικών τους δραστηριοτήτων και να επηρεάσουν τόσο την ένταση του ανταγωνισμού όσο και τη θέση τους έναντι των ανταγωνιστών τους. (Γεωργίου Σ.Οικονόμου–Νικολάου Β.Γεωργοπούλου, 2004, σελ.99)

Το ηλεκτρονικό εμπόριο παρέχει στους οργανισμούς καινοτομικά και στρατηγικά πλεονεκτήματα, δίνοντάς τους τη δυνατότητα αύξησης του μεριδίου αγοράς τους, καλύτερης διαπραγμάτευσης με τους προμηθευτές τους ή πρόληψη εισόδου ανταγωνιστών στην περιοχή τους. Υποστηρίζουν και διαμορφώνουν την ανταγωνιστική στρατηγική μιας επιχειρηματικής μονάδας. Αλλάζουν σημαντικά τον τρόπο με τον οποίο λειτουργεί η επιχείρηση ή και ο κλάδος. Βοηθάει έναν οργανισμό να κερδίσει ανταγωνιστικό πλεονέκτημα μέσω της σύνδεσής του με τους στρατηγικούς στόχους ενός οργανισμού και της ικανότητάς του να αυξήσει την απόδοση και την παραγωγικότητα.(Βασιλακόπουλος Γ., Χρυσικόπουλος Β., 1990, σελ.36)

Πολλοί βιομηχανικοί κλάδοι άρχισαν βαθμιαία να αντιλαμβάνονται ότι τα Π.Σ. δεν είναι μόνο απλά εργαλεία υποστήριξης εργασιών ρουτίνας αλλά και στρατηγικά και αποτελεσματικά μέσα για την απόκτηση ανταγωνιστικών πλεονεκτημάτων συμβάλλοντας έτσι σημαντικά στην επέκταση των δραστηριοτήτων των επιχειρήσεων και οργανισμών. (Γεωργίου Σ.Οικονόμου–Νικολάου Β.Γεωργοπούλου, 2004, σελ.99)

Αρχικά, τα Strategic Information Systems θεωρούνταν ότι στόχευαν εξωτερικά κατευθείαν στον ανταγωνισμό της βιομηχανίας. Τα Strategic Information Systems είναι εστιασμένα εσωτερικά προς την ενίσχυση της ανταγωνιστικής θέσης της εταιρίας αυξάνοντας την παραγωγικότητα των εργαζομένων, βελτιώνοντας την ομαδική εργασία, βελτιώνοντας την επικοινωνία.

Τα Strategic Information Systems είναι επίσης μέρη των στρατηγικών συμμαχιών ανάμεσα σε επιχειρηματικούς συνεργάτες. Η ανταγωνιστική στρατηγική ενός οργανισμού είναι η αναζήτηση για ένα ανταγωνιστικό πλεονέκτημα σε μια βιομηχανία, το οποίο της δίνει ένα πλεονέκτημα έναντι των ανταγωνιστών της σε κάποιο μέτρο, όπως κόστη, ποιότητα ή ταχύτητα.(Βασιλακόπουλος Γ., Χρυσικόπουλος Β., 1990, σελ.47)

1.8 ΓΕΩΓΡΑΦΙΚΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Το λογισμικό των γεωγραφικών πληροφοριακών συστημάτων ποικίλλει όσον αφορά τις δυνατότητές τους. Απλά υπολογιστικά συστήματα χαρτογράφησης, εργαλεία ανάλυσης δεδομένων για λήψη αποφάσεων. Τα δεδομένα των γεωγραφικών πληροφοριακών συστημάτων είναι διαθέσιμα από μια μεγάλη ποικιλία πηγών. Οι κυβερνητικές πηγές παρέχουν ορισμένα δεδομένα, καθώς επίσης και οι πωλητές παρέχουν διαφοροποιημένα εμπορικά δεδομένα.(Βασιλακόπουλος Γ., Χρυσικόπουλος Β., 1990, σελ.82)

Κατά τη λήψη αποφάσεων η γραφική μορφή τους καθιστά εύκολο στους manager να ανακαλέσουν δεδομένα και να λάβουν αποφάσεις. Η ολοκλήρωση των γεωγραφικών πληροφοριακών συστημάτων και το παγκόσμιο σύστημα τοποθέτησης έχουν την τάση να υποστηρίζουν τον ανασχεδιασμό της αεροπλοΐας, των μεταφορών και της ναυτιλίας. Παρέχει τη δυνατότητα στα οχήματα να εξοπλίζονται με ένα GPS υποδοχέα, ο οποίος εντοπίζει τη θέση τους καθώς κινούνται. (Κιουντούζης Ε., 2002, σελ.97)

1.9 ΤΑ ΣΤΑΔΙΑ ΑΝΑΠΤΥΞΗΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τα στάδια ανάπτυξης των πληροφοριακών συστημάτων είναι τα έξι ακόλουθα, όπως αναλύονται παρακάτω:

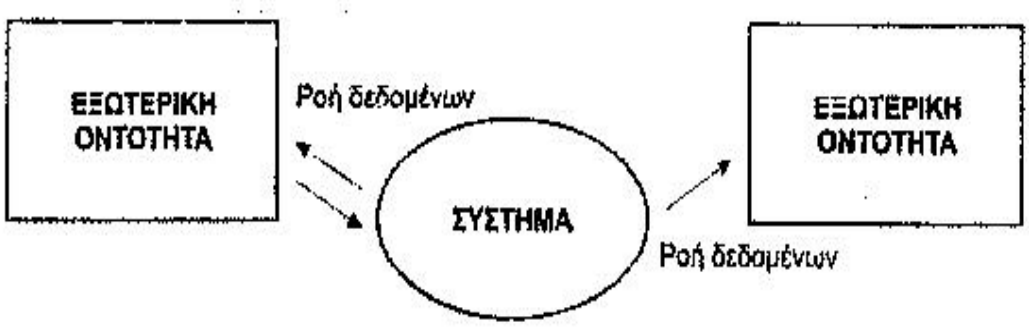
- Έναρξη: εισαγωγή των υπολογιστών στον οργανισμό. Μαζική επεξεργασία προς αυτοματοποίηση υπαλληλικών λειτουργιών για να επιτευχθεί μείωση κόστους, εστίαση στα λειτουργικά συστήματα, έλλειψη διοικητικού ενδιαφέροντος, συγκεντρωτικό πληροφοριακό σύστημα.
- Επέκταση: συγκεντρωμένη ταχεία ανάπτυξη καθώς οι χρήστες απαιτούν περισσότερες εφαρμογές βασισμένες σε υψηλές προσδοκίες ωφελειών, κίνηση προς online συστήματα καθώς το τμήμα Πληροφορικής προσπαθεί να ικανοποιήσει τις απαιτήσεις των χρηστών. Ελάχιστος έλεγχος. Τα έξοδα για την πληροφορική αυξάνονται πολύ γρήγορα.
- Έλεγχος: ανταποκρινόμενο στις ανησυχίες της διοίκησης για τη σύγκριση κόστους-ωφελειών, το σύστημα αναμένεται να παρουσιάσει αποτελέσματα, δημιουργούνται πλάνα και επιβάλλονται μεθοδολογίες και πρότυπα. Συχνά δημιουργείται backlog εφαρμογών και δυσαρεστημένων χρηστών. Εισάγονται ο σχεδιασμός και ο έλεγχος του συστήματος.
- Ενοποίηση: αξιοσημείωτες επενδύσεις στην ενοποίηση (μέσω τηλεπικοινωνιών και βάσεων δεδομένων) των υπαρχόντων συστημάτων. Η ευθύνη του χρήστη για το σύστημα αναγνωρίζεται και το τμήμα Πληροφορικής παρέχει υπηρεσίες στους χρήστες κι όχι απλά λύσεις σε προβλήματα. Στο σημείο αυτό λαμβάνει χώρα μια μετάβαση στη χρήση υπολογιστή και η προσέγγιση από επεξεργασία δεδομένων γίνεται επεξεργασία πληροφορίας και γνώσης
- Διαχείριση δεδομένων: πληροφοριακές απαιτήσεις πέραν της επεξεργασίας καθορίζουν την πορεία του χαρτοφυλακίου εφαρμογών και η πληροφορία μοιράζεται μέσα στον οργανισμό. Οι δυνατότητες της βάσης δεδομένων προωθούνται καθώς οι χρήστες κατανοούν την αξία της πληροφορίας και επιθυμούν να τη μοιραστούν
- Ωριμότητα: ο σχεδιασμός και η ανάπτυξη του στον οργανισμό είναι στενά συντονισμένοι με την ανάπτυξη της επιχείρησης. Λειτουργούν συστήματα που αφορούν ολόκληρη την επιχείρηση. Το τμήμα Πληροφορικής και οι

χρήστες μοιράζονται την ευθύνη αναφορικά με τον επιμερισμό των υπολογιστικών πόρων. Η πληροφορική είναι πλέον στρατηγικός σύμμαχος. (Κιουντούζης Ε., 2002, σελ 99)

1.10 ΟΨΕΙΣ ΕΝΟΣ ΣΥΣΤΗΜΑΤΟΣ

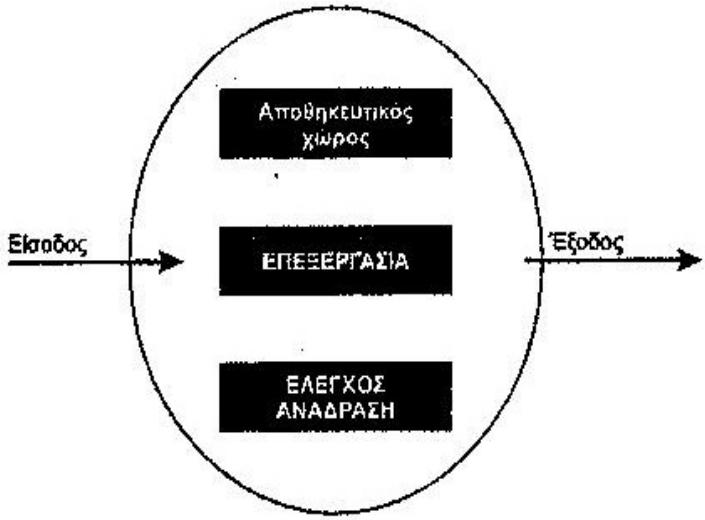
I. Μια όψη βασισμένη στο περιβάλλον:

Κάθε σύστημα λειτουργεί σε αλληλεπίδραση με το περιβάλλον του. Η βασισμένη στο περιβάλλον όψη περιγράφει γραφικά την αλληλεπίδραση του συστήματος με τις διάφορες οντότητες στο περιβάλλον του. Οι αλληλεπιδράσεις αναπαρίστανται ως ροές δεδομένων από και προς τέτοιες οντότητες. Η βασισμένη στο περιβάλλον όψη διευκρινίζει τα όρια του συστήματος και τις αλληλεπιδράσεις με αυτό.



II. Μια όψη βασισμένη στη δραστηριότητα:

Κάθε σύστημα πρέπει να χειριστεί ορισμένες μεταβλητές προκειμένου να επιτευχθούν οι στόχοι του. Η όψη αυτή περιγράφει την επεξεργασία των καταστάσεων και τα αποτελέσματα αυτής της επεξεργασίας σε σχέση με ορισμένες παραμέτρους ελέγχου. (Κιουντούζης Ε., 2002, σελ 100)



1.11 Η ΣΗΜΑΣΙΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΤΗ ΣΗΜΕΡΙΝΗ ΕΠΟΧΗ

Ο όρος «αλλαγή» είναι ένα αναπόφευκτο κομμάτι της σημερινής κοινωνικής ζωής, που επιφέρει οικονομική αστάθεια και αβεβαιότητα όσον αφορά την ομαλή λειτουργία της σύγχρονης επιχείρησης. Σε επιχειρησιακό επίπεδο, λόγω των προβλημάτων που δημιουργούνται από αυτή την αλλαγή και των δυσμενών συνεπειών τους, οι σχεδιαστές των Πληροφοριακών Συστημάτων βρίσκονται μπροστά στην πρόκληση να δημιουργήσουν ένα πληροφοριακό σύστημα αντάξιο των σύγχρονων απαιτήσεων, που θα απλοποιήσει τη διαδικασία αποφάσεων και κυρίως θα εντοπίσει έγκαιρα και θα αντιμετωπίσει τους επιχειρησιακούς κινδύνους.

Οι χρήστες του πληροφοριακού συστήματος είναι οι *τελικοί αποδέκτες* των πληροφοριών που παρέχει, οι άνθρωποι που θα χρησιμοποιήσουν τις πληροφορίες για την επίτευξη των σκοπών που έχει θέσει η οικονομική μονάδα.

Σε αυτούς ανήκουν οι κυρίως χρήστες (end users) και οι προϊστάμενοι τους (user managers), οι οποίοι βέβαια μπορούν να χρησιμοποιούν τις ίδιες λογιστικές πληροφορίες, αλλά και διαφορετικού είδους λόγω των διαφορετικών καθηκόντων και αρμοδιοτήτων που έχουν βάσει κλίμακας

ιεραρχίας. Ανάλογα από το ποιο περιβάλλον της επιχείρησης προέρχονται διακρίνονται σε εσωτερικούς και εξωτερικούς.

Οι χειριστές των μηχανημάτων των Η/Υ, όσοι εισάγουν στοιχεία, όσοι συντηρούν το υλικό ή το λογισμικό κτλ. Είναι οι άνθρωποι που θέτουν ένα Λειτουργικό Πληροφοριακό Σύστημα σε λειτουργία, του δίνουν «σάρκα και οστά». Υπάρχει περίπτωση βέβαια οι χειριστές να είναι και χρήστες του Λειτουργικού Πληροφοριακού Συστήματος ή το αντίστροφο. (Παπαθανασίου Α., 2008, σελ 53)

Η κατηγορία των δημιουργών περιλαμβάνει:

- Τον εκπαιδευτή, που έχει την ευθύνη της εκπαίδευσης στα διάφορα αντικείμενα όλων όσων απαιτείται εκπαίδευση – ενημέρωση.
- Τον προγραμματιστή, δηλαδή εκείνον που συντάσσει, ελέγχει και συντηρεί το λογισμικό του Λειτουργικού Πληροφοριακού Συστήματος.
- Τον αναλυτή που ανακαλύπτει, συμπεραίνει και αναλύει, με τη βοήθεια των χρηστών, τις απαιτήσεις, αξιολογεί εναλλακτικές λύσεις, καθορίζει τις προδιαγραφές σχεδίασης του λογισμικού, υλικού, των διαδικασιών, των δεδομένων κτλ.
- Το σχεδιαστή της βάσης δεδομένων, αν το Πληροφοριακό Σύστημα χρησιμοποιεί βάση δεδομένων.
- Τον ειδικό επί των δικτύων, αν έχουμε δίκτυο υπολογιστών στο σύστημά μας.
- Τον υπεύθυνο της όλης διαχείρισης του έργου, που σχεδιάζει αρμοδιότητες, αναθέτει εργασίες, συντονίζει και διευθύνει την όλη προσπάθεια της ανάπτυξης του Πληροφοριακό Σύστημα.
- Τον υπεύθυνο ασφαλείας, που έχει την ευθύνη της ασφάλειας τόσο των δεδομένων όσο και των μηχανημάτων. (Παπαθανασίου Α., 2008)

1.12 ΛΟΓΙΣΜΙΚΟ- Software

Το λογισμικό αποτελεί ουσιαστικά την άυλη δομή ενός πληροφοριακού συστήματος, με βάση την οποία λειτουργεί και αναπτύσσεται. Ταξινομείται σε τρεις κατηγορίες:

- Λογισμικό συστήματος (system software):

Σε αυτή την ομάδα ανήκουν τα προγράμματα που φτιάχνονται από τον κατασκευαστή του υλικού και αγοράζονται μαζί με αυτό ή χωριστά.

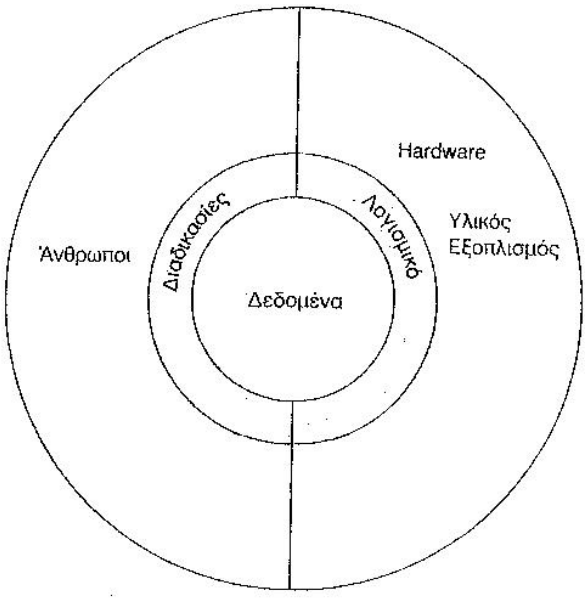
Ü Λογισμικό εφαρμογών (application software)

Σε αυτήν την κατηγορία περιλαμβάνονται τα προγράμματα που γράφονται για να υποστηρίξουν γενικές ή συγκεκριμένες εφαρμογές και απαιτούν το λογισμικό του συστήματος για την εκτέλεσή τους. Πχ μισθοδοσία, έλεγχος αποθήκης, παρακολούθησης προμηθειών, κοστολόγηση κτλ.

Ο λόγος κατασκευής μιας εφαρμογής αποκλειστικά για τις ανάγκες ενός πληροφοριακού συστήματος είναι ότι με αυτό τον τρόπο επιτυγχάνεται η δημιουργία λογισμικού που ικανοποιεί πλήρως τις απαιτήσεις του οργανισμού. Επειδή όμως το κόστος κατασκευής εξειδικευμένου λογισμικού είναι ιδιαίτερα υψηλό, οι επιχειρήσεις ακολουθούν εναλλακτικές επιλογές: ενοικίαση ή αγορά έτοιμου και όχι εξειδικευμένου λογισμικού κτλ. (Βασιλακόπουλος, 1990)

Ü Λογισμικό που αυξάνει την παραγωγικότητα (productivity software)

Σε αυτή την ομάδα ανήκει το λογισμικό εκείνο που διευκολύνει το χρήστη να δημιουργήσει μόνος του νέες εφαρμογές. Για το λόγο αυτό του παρατίθενται κάποια εργαλεία όπως επεξεργαστής κειμένου, εργαλεία διαχείρισης βάσης δεδομένων κτλ. (Κιουντούζης Ε., 2002, σελ 114)



Αναπαράσταση της Δομής ενός Π.Σ.

1.13 ΥΛΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ- Hardware

Computer Hardware όπως διεθνώς ονομάζεται, είναι ο φυσικός εξοπλισμός που χρησιμοποιείται στην ηλεκτρονική επεξεργασία των δεδομένων ενός πληροφοριακού συστήματος. Περιλαμβάνει την κεντρική μονάδα επεξεργασίας και τις περιφερειακές συσκευές, που εξυπηρετούν την εισαγωγή, εξαγωγή, αποθήκευση των δεδομένων καθώς επίσης, επιτρέπουν την επικοινωνία μεταξύ των υπολογιστών.(Βασιλακόπουλος Γ., Χρισικόπουλος Β., 1990 σελ.42)

Η ταχύτητα λειτουργίας και οι δυνατότητες αποθήκευσης είναι κάποια βασικά χαρακτηριστικά του υλικού εξοπλισμού που εξελίσσονται με ταχύτατους ρυθμούς και ταυτοχρόνως διαφέρουν μεταξύ των υπολογιστών ανάλογα με το μέγεθος και το κόστος δημιουργίας τους.

Στην ανάπτυξη ενός πληροφοριακού συστήματος σπάνια απαιτείται η εξ αρχής κατασκευή υλικού hardware, εκτός από τα συστήματα με μεγάλο βαθμό ασφάλειας, όπως τα πληροφοριακά συστήματα διοίκησης και ελέγχου του στρατού, παρουσιάζεται η ανάγκη να μη χρησιμοποιηθεί εξ ολοκλήρου έτοιμος υλικός εξοπλισμός.

Στις περισσότερες περιπτώσεις επιχειρήσεων, απαιτείται η δημιουργία των προδιαγραφών υλικού (hardware specification). Ο υπεύθυνος αναλυτής καλείται όχι μόνο να συντάσσει σωστά τις προδιαγραφές του υλικού και του λογισμικού πάσης φύσης (για τον υπολογιστή, τα μέσα αποθήκευσης, επικοινωνίας κτλ) αλλά επιπλέον να γνωρίζει τις δυνατότητες της αγοράς, να διαπραγματεύεται την προμήθεια, να φτιάχνει τους όρους συμβολαίων αγοράς κτλ. Γιατί σε κάθε περίπτωση ο υλικός εξοπλισμός είναι άμεσα συνδεδεμένος με την επεξεργασία και το είδος των δεδομένων που εισάγονται και επεξεργάζονται, εάν θέλουμε το πληροφοριακό σύστημα να έχει την απόδοση που επιθυμούμε. (Scriven D., Scriven J., Kozoll C., σελ.89)

ΚΕΦΑΛΑΙΟ 2ο

2.1 ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ : ΕΛΕΓΧΟΣ ΚΑΙ ΑΣΦΑΛΕΙΑ

Η ραγδαία ανάπτυξη των πληροφοριακών συστημάτων τα τελευταία χρόνια έχει επιφέρει σημαντικές εξελίξεις στα ηλεκτρονικά συστήματα επεξεργασίας των συναλλαγών και συνεπώς σε ολόκληρη τη δομή και λειτουργία των λογιστικών πληροφοριακών συστημάτων. Η πολυπλοκότητα των συστημάτων και η ανάγκη για πλήρη κατανόηση όλων των δομών που διαθέτουν και των πληροφοριών που παρέχουν, απαίτησε, όχι μόνο συνεχή αξιολόγηση τυχουσών αδυναμιών στο σχεδιασμό τους, αλλά και διαρκή έλεγχο που να εξασφαλίζει ότι η πληροφόρηση πάντα είναι η απαιτούμενη, επαρκής και αληθής ώστε η λήψη αποφάσεων να γίνεται σε ένα ασφαλές περιβάλλον. (Scriven, D., Scriven, J., Kozoll, C., σελ.92)

Για τους παραπάνω λόγους, έχει αναπτυχθεί ένα εξειδικευμένο σύστημα εσωτερικού ελέγχου, το οποίο, ύστερα από προκαθορισμένες διαδικασίες, στόχο έχει να προστατεύσει το λογιστικό πληροφοριακό σύστημα από διάφορες απειλές και κινδύνους. Τόσο ο χρήστης όσο και ο ελεγκτής λογιστικών πληροφοριακών συστημάτων βασικά αξιολογεί την πιθανότητα απώλειας δεδομένων και τους κινδύνους που εμπερικλείονται σε ένα τέτοιο ενδεχόμενο. Οι έλεγχοι που θα εξασφαλίσουν την ασφάλεια λειτουργίας των πληροφοριακών συστημάτων και την εγκυρότητα των πληροφοριών που προσφέρουν.(Βασιλακόπουλος, Γ., Χρισικόπουλος, Β., 1990, σελ.208)

2.2 ΓΕΝΙΚΟΙ ΕΛΕΓΧΟΙ

Επειδή κάθε πληροφοριακό σύστημα σχεδιάζεται με τέτοιο τρόπο ώστε να ικανοποιεί συγκεκριμένες οργανωτικές και λειτουργικές ανάγκες μιας επιχείρησης, διαθέτει ένα μοναδικό σύστημα εσωτερικού ελέγχου που θα το ελέγχει και θα το αξιολογεί. Σαφέστατα, ο έλεγχος γίνεται πάντα υπό τις γενικά παραδεκτές αρχές, αλλά σε κάθε περίπτωση εξειδικεύεται και σχεδιάζεται με τις ιδιαιτερότητες των συναλλαγών και δραστηριοτήτων της επιχείρησης που ελέγχει. (Τασόπουλος Α., 2005, σελ 169)

Οι γενικοί έλεγχοι αποτελούν εκείνους τους ελέγχους που λαμβάνουν χώρα στο γενικό περιβάλλον του οργανισμού και αφορούν την επάρκεια του όλου συστήματος εσωτερικού ελέγχου. Δεν είναι άμεσα συνδεδεμένοι με μια συγκεκριμένη εφαρμογή και έχουν γενική επίδραση στην αποτελεσματικότητα του συνόλου των ελέγχων που εφαρμόζονται στον οργανισμό. Τυχούσες αδυναμίες στους γενικούς ελέγχους μπορούν να αποτρέψουν τους οποιουσδήποτε ελέγχους εφαρμογών, τους ειδικούς ελέγχους, από το να επιφέρουν το επιθυμητό αποτέλεσμα.

Για παράδειγμα:

~ Διοικητικός έλεγχος στη λειτουργία ανάπτυξης και διαχείρισης των λογιστικών πληροφοριακών συστημάτων.

~ Έλεγχοι για τον προσδιορισμό της φυσικής πρόσβασης σε λογιστικά πληροφοριακά συστήματα.

~ Έλεγχοι αποθήκευσης δεδομένων

~ Σχεδιασμός επανάκτησης της λειτουργικής ικανότητας του συστήματος μετά από μια καταστροφή κτλ (Κιουντούζης Ε., 2002, σελ.134)

2.3 ΕΛΕΓΧΟΙ ΕΦΑΡΜΟΓΩΝ

Οι εν λόγω έλεγχοι αναφέρονται σε διαδικασίες αξιολόγησης που εφαρμόζονται σε συγκεκριμένες εφαρμογές. Σχετίζονται δηλαδή με καθορισμένες δραστηριότητες οι οποίες εκτελούνται στο επίπεδο του κάθε ενός συστήματος, όπως επί παραδείγματι η εισαγωγή στοιχείων με βάση την παραγγελία πώλησης. Οι έλεγχοι αυτοί κατατάσσονται σε ελέγχους εισόδου, επεξεργασίας και αναφορών ανάλογα με το στάδιο που αναφέρονται στο κύκλο επεξεργασίας δεδομένων. (Τασόπουλος Α., 2005, σελ 172)

- <u>Έλεγχοι στο στάδιο εισόδου στοιχείων στο σύστημα (input controls)</u>

Οι έλεγχοι εισόδου σχεδιάζονται με τέτοιο τρόπο ώστε να διασφαλίζουν την ακεραιότητα των δεδομένων κατά τη μετατροπή τους σε ψηφιακή μορφή. Κάθε συναλλαγή που εισάγεται στο σύστημα πρέπει να είναι σύμφωνη με τις εγκεκριμένες διαδικασίες διεύθυνσης και τυχόντα λάθη κατά την είσοδο των δεδομένων πρέπει να διορθώνονται έγκαιρα για την ακρίβεια των λογιστικών εγγραφών.

- Έλεγχοι στο στάδιο επεξεργασίας στοιχείων (processing controls)

Κύριος σκοπός αυτών των ελέγχων είναι η διατήρηση της ακρίβειας και της πληρότητας κατά την επεξεργασία των δεδομένων. Παρέχουν λογική επιβεβαίωση ότι η επεξεργασία των δεδομένων και η ενημέρωση των αρχείων είναι ορθή και ολοκληρωμένη. Παράδειγμα: έλεγχοι επαλήθευσης δεδομένων που διατηρούνται στο σύστημα με εξωτερικά στοιχεία.

- Έλεγχοι στο στάδιο εξαγωγής πληροφοριών από το σύστημα (output controls)

Οι έλεγχοι εξόδου υπάρχουν για να διασφαλίζουν ότι οι πληροφορίες θα παρουσιαστούν σωστά και θα φτάσουν μόνο σε εξουσιοδοτημένους χρήστες. Για την επίτευξη των στόχων αυτών, θα πρέπει να καθορίζονται υπευθυνότητες οι οποίες αφορούν τόσο τη λειτουργία ελέγχου δεδομένων όσο και τους ίδιους τους χρήστες των αναφορών οι οποίες εξάγονται από το σύστημα. (Κιουντούζης Ε., 2002, σελ 145)

2.4 ΤΙ ΕΙΝΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Ασφάλεια Πληροφοριακού Συστήματος είναι το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, παραδοχές, διαδικασίες, τεχνικές και (διοικητικά) μέτρα που απαιτούνται για να προστατευθούν όλα τα επιμέρους στοιχεία του Π.Σ. αλλά και το Σύστημα ολόκληρο, από κάθε είδους απειλή (τυχαία ή σκόπιμη). Με τον υπάρχοντα ορισμό αποφεύγουμε τη σύγχυση μεταξύ των εννοιών Ασφάλεια Τεχνολογίας Πληροφορικής όπου σχετίζεται με την Ασφάλεια της Τεχνολογικής Υποδομής του Π.Σ. και την Ασφάλεια Πληροφοριών που έχει να κάνει με την Ασφάλεια Δεδομένων.(Σωκρ.Κάτσικας-Δημ.Γκρίζαλης-Στεφ.Γκρίτζαλης, 2004, σελ.320)

Μπορεί ακόμη η έννοια της ασφάλειας ενός Π.Σ. να σχετιστεί με την ικανότητα ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Σχετίζεται επίσης με την ικανότητά του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη

μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του δικτύου. Συνεπώς η ασφάλεια πληροφοριακών συστημάτων σχετίζεται με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών του συστήματος καθώς και την λήψη μέτρων. Πιο συγκεκριμένα σχετίζεται με : τη λήψη μέτρων για να προληφθούν 'φθορές' των συστατικών ενός πληροφοριακού συστήματος (Πρόληψη), τη λήψη μέτρων για την ανίχνευση του πότε, πώς και από ποιόν προκλήθηκε φθορά σε ένα συστατικό ενός Π.Σ. (Ανίχνευση) και τέλος, την λήψη μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός συστήματος (Αντίδραση).(Γ. Πάγκαλου – Ι. Μαυρίδη, 2002, σελ.16)

2.5 ΘΕΜΕΛΙΩΔΕΙΣ ΚΑΙ ΔΕΥΤΕΡΕΥΟΥΣΕΣ ΕΝΝΟΙΕΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ Π.Σ.

Οι έννοιες Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα συνδέονται στενά με την Ασφάλεια Πληροφοριακών Συστημάτων:

- Η **εμπιστευτικότητα** σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως σημαίνει ότι τα δεδομένα ενός υπολογιστικού συστήματος, καθώς και τα διακινούμενα μεταξύ των υπολογιστών δεδομένα, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Άλλες εκφάνσεις της εμπιστευτικότητας είναι:
    - Είναι η ιδιωτικότητα (privacy) : προστασία των δεδομένων των δεδομένων προσωπικού χαρακτήρα, δηλαδή αυτών που αφορούν συγκεκριμένα πρόσωπα και
    - Η μυστικότητα (secrecy) : προστασία των δεδομένων που ανήκουν σε έναν οργανισμό.
- Στην πληροφορική, **ακεραιότητα** σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων. Επομένως, σημαίνει ότι

η μετατροπή, διαγραφή και δημιουργία των δεδομένων ενός υπολογιστικού συστήματος, γίνεται μόνο από εξουσιοδοτημένα μέρη.

- **Διαθεσιμότητα** ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός πληροφοριακού συστήματος όταν τις χρειάζονται οι εξουσιοδοτημένοι χρήστες. Για τους σκοπούς της ασφάλειας, μας απασχολεί βασικά η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την πρόσβαση των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα. Αυτές οι επιθέσεις ονομάζονται επιθέσεις άρνησης παροχής υπηρεσιών, η οποία σημαίνει παρεμπόδιση της εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων ή πρόκληση καθυστέρησης των λειτουργιών που είναι κρίσιμες στο χρόνο. Παραδείγματος χάρη, οι επιθέσεις «πλημμύρας» στο διαδίκτυο, όπου ο επιτιθέμενος κατακλύζει έναν εξυπηρετητή στέλνοντας του έναν τεράστιο αριθμό αιτήσεων σύνδεσης.

Εκτός από τις παραπάνω τρείς θεμελιώδεις έννοιες, υπάρχουν και δευτερεύουσες έννοιες της ασφάλειας Π.Σ, αυτές είναι :

- *Εξουσιοδοτημένη χρήση* : τα εξουσιοδοτημένα άτομα μόνο μπορούν να χρησιμοποιούν το υπολογιστικό σύστημα ή τις περιφερειακές συσκευές του και σύμφωνα με ένα προκαθορισμένο τρόπο.
- *Αυθεντικοποίηση μηνυμάτων* : η επιθυμία να γνωρίζουμε με βεβαιότητα κατά τη λήψη ενός μηνύματος (μέσω δικτύου) ότι το άτομο που το σύστημα αξιώνει ότι έστειλε το μήνυμα, ότι πράγματι το έστειλε.
- *Μη-απάρνηση* : η επιθυμία να γνωρίζουμε με βεβαιότητα κατά πόσο ένα άτομο παρέλαβε ένα μήνυμα που στάλθηκε, έτσι ώστε να μην μπορεί να απαρνηθεί την παραλαβή του.
- *Απόδοση ευθυνών* : για την αντιμετώπιση πιθανών παραβάσεων της ασφάλειας, πρέπει οι χρήστες να είναι υπεύθυνοι (υπόλογοι) για τις πράξεις τους. Αυτό γίνεται με την ασφαλή αναγνώριση των χρηστών και τη διατήρηση εγγραφών ελέγχου για τα συμβάντα που αφορούν την ασφάλεια. Στην περίπτωση παράβασης της

ασφάλειας του Π.Σ. οι εγγραφές αυτές θα χρησιμοποιηθούν για την εξιχνίαση του προβλήματος και την ανακάλυψη του θύτη.

- *Αξιοπιστία και σιγουριά* : η ασφάλεια σχετίζεται με την αξιοπιστία και την σιγουριά καθώς έχει να κάνει με συστήματα που πρέπει να λειτουργούν κανονικά σε αντίξοες συνθήκες, π.χ. συστήματα πυρηνικών σταθμών και ελέγχου εναέριας κυκλοφορίας.(Γ. Πάγκαλου – Ι. Μαυρίδη, 2002,σελ.18)

2.6 ΠΑΡΑΒΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Στο χώρο της ασφάλειας, έκθεση σε κίνδυνο ονομάζουμε μια μορφή πιθανής απώλειας ή ζημιάς σε ένα υπολογιστικό σύστημα. Παραδείγματα εκθέσεων σε κίνδυνο είναι :

- Η μη εξουσιοδοτημένη αποκάλυψη δεδομένων
- Η μη εξουσιοδοτημένη τροποποίηση δεδομένων
- Η άρνηση θεμιτής προσπέλασης υπολογιστικών πόρων

Ευπάθεια ονομάζεται μια αδυναμία ή ένα ευάλωτο σημείο στο σύστημα ασφαλείας που μπορεί, αν αξιοποιηθεί κατάλληλα, να προκαλέσει απώλειες ή ζημιές. Όταν ένα άτομο εκμεταλλεύεται μια ευπάθεια τότε διαπράττει μια επίθεση στο σύστημα.

Απειλή για ένα υπολογιστικό σύστημα αποτελούν καταστάσεις όπου υπάρχει το ενδεχόμενο πρόκλησης απωλειών ή ζημιών. Παραδείγματα απειλών είναι :

- Ανθρώπινες επιθέσεις
- Φυσικές καταστροφές
- Ακούσια ανθρώπινα λάθη
- Εσωτερικές ατέλειες του εξοπλισμού ή του λογισμικού

Έλεγχος είναι ένα προστατευτικό μέτρο, όπως μία πράξη, συσκευή, διαδικασία ή τεχνική, που μειώνει μια ευπάθεια του συστήματος.(Γ. Πάγκαλου – Ι. Μαυρίδη, 2002, σελ.20)

2.7 ΕΥΠΑΘΕΙΕΣ ΚΑΙ ΑΠΕΙΛΕΣ

Κάθε Π.Σ. είναι ευπαθές σε πιθανές επιθέσεις. Οι πολιτικές και τα προϊόντα ασφάλειας μπορούν να μειώσουν την πιθανότητα του να καταστεί δυνατόν μια επίθεση να διαπεράσει τις άμυνες του συστήματος. Μια κατηγοριοποίηση των τυπικών σημείων *ευπάθειας* σε ένα υπολογιστικό σύστημα θα μπορούσε να περιλαμβάνει τα εξής :

- **Φυσικές Ευπάθειες** : αφορούν το φυσικό περιβάλλον (π.χ. τα κτήρια και τους χώρους των μηχανογραφικών κέντρων (computer rooms)). Μια πρώτη άμυνα γι αυτά, παρέχουν τα κλασικά μέσα προστασίας, όπως ο έλεγχος της φυσικής προσπέλασης, οι φύλακες, οι βιομετρικές συσκευές, οι αντικλεπτικοί συναγερμοί, κ.α.
- **Εκ Φύσεως Ευπάθειες** : Οι υπολογιστές είναι ιδιαίτερα ευπαθείς σε φυσικές καταστροφές και περιβαλλοντικές απειλές, όπως οι πυρκαγιές, οι πλημμύρες, οι σεισμοί, οι κεραυνοί και οι διακοπές ρεύματος. Ακόμη, επηρεάζονται αρνητικά από τη σκόνη, την υγρασία, και τις ακραίες θερμοκρασιακές συνθήκες.
- **Ευπάθειες Υλικού και Λογισμικού** : Πιθανές δυσλειτουργίες του υλικού και του λογισμικού μπορεί να προκαλέσουν την διακοπή παροχής των υπηρεσιών ενός Π.Σ. είτε λόγω ενδογενών σφαλμάτων είτε λόγω εσφαλμένης εγκατάστασης των συστημάτων συστατικών μερών του.
- **Ευπάθειες Μέσων** : Η κλοπή ή η καταστροφή μαγνητικών μέσων και εκτυπωτικών καταστάσεων μπορεί να προκαλέσει την απώλεια ή διαρροή ευαίσθητων δεδομένων.
- **Ευπάθειες Εκπομπών** : Όλες οι ηλεκτρονικές συσκευές εκπέμπουν ηλεκτρομαγνητική ακτινοβολία. Με κατάλληλο εξοπλισμό είναι πιθανή η υποκλοπή των εκπεμπόμενων σημάτων από συστήματα και δίκτυα υπολογιστών και η αποκωδικοποίηση τους με σκοπό την υφαρπαγή κρίσιμων πληροφοριών, ή την παρεμπόδιση της ομαλής λειτουργίας ενός πληροφοριακού συστήματος.
- **Ευπάθειες Επικοινωνιών** : Η σύνδεση ενός Η/Υ σε ένα ανοικτό δίκτυο, όπως το διαδίκτυο (internet), αυξάνει τον κίνδυνο διείσδυσης

από τρίτα μη εξουσιοδοτημένα μέρη. Με αυτό τον τρόπο μηνύματα μπορούν να υποκλαπούν, να αλλάξουν διαδρομή και να χαλκευτούν. Οι γραμμές σύνδεσης των υπολογιστών είναι τα συνηθέστερα σημεία που μπορούν να χρησιμοποιηθούν για υποκλοπή ή ακόμη και για καταστροφή.

- **Ανθρώπινες Ευπάθειες** : Συνήθως, η ασφάλεια ενός Π.Σ. εξαρτάται κατά κύριο λόγο από τους ανθρώπους που το χρησιμοποιούν νόμιμα. Η έλλειψη εκπαίδευσης, ο δόλος, η απροσεξία και η επιπολαιότητα στο χειρισμό ευαίσθητων στοιχείων, όπως για παράδειγμα τα συνθηματικά, καθώς και οι κακοπροαίρετοι ή παραπονεμένοι υπάλληλοι αποτελούν τις μεγαλύτερες απειλές για την ασφάλεια ενός ΠΣ.
  (Γ. Πάγκαλου–Ι. Μαυρίδη, 2002, σελ.21)

Υπάρχει ο κίνδυνος τα δεδομένα που φυλάσσονται σε ένα Λειτουργικό Σύστημα να χαθούν, να καταστραφούν, να σβηστούν, να αλλοιωθούν ή να διαδοθούν χωρίς την απαιτούμενη δικαιοδοσία. Ακόμη το ίδιο το σύστημα μπορεί να χρησιμοποιηθεί χωρίς άδεια ή να γίνει αντικείμενο βανδαλισμού. Απειλές, για ένα υπολογιστικό σύστημα αποτελούν καταστάσεις όπου υπάρχει το ενδεχόμενο πρόκλησης απωλειών ή ζημιών. Μερικές ενδεικτικές Απειλές ακολουθούν :

- *Αποκάλυψη συνθηματικών* : Από τις πιο κοινές απειλές σε ένα ΛΣ. Μη εξουσιοδοτημένοι χρήστες αποκτούν με αυτό τον τρόπο πρόσβαση στο σύστημα και σε ακραίες περιπτώσεις αποκτούν πλήρη διαχειριστικά δικαιώματα.
- *Υποκλοπή* : Κάποιο μη-εξουσιοδοτημένο μέρος έχει καταφέρει να αποκτήσει προσπέλαση σε ένα τμήμα του συστήματος, που έχει ως συνήθεις στόχους την κατασπατάληση των πόρων (π.χ. το υλικό (hardware), το λογισμικό (software), τα δεδομένα (data)) του συστήματος ή την παρακολούθηση του. Ενδεικτικά παραδείγματα είναι η κλοπή εξαρτημάτων, η αθέμιτη αντιγραφή προγραμμάτων ή αρχείων δεδομένων, η καλωδιομένη παρακολούθηση ή υποκλοπή γραμμής με σκοπό την απόκτηση δεδομένων καθώς κυκλοφορούν σε ένα δίκτυο κλπ. Πρόκειται για απειλή κυρίως κατά της εμπιστευτικότητας του συστήματος.

- *Μεταβολή* : Κάποιο μη-εξουσιοδοτημένο μέρος εκτός του ότι έχει καταφέρει να αποκτήσει πρόσβαση, επιπλέον παραποιεί λογισμικό και δεδομένα. Κακόβουλες ενέργειες όπως η τροποποίηση δεδομένων, η τροποποίηση ενός προγράμματος από έναν ιό (virus), η καταστροφή αρχείων συστήματος ή ο φυσικός βανδαλισμός μπορούν να συμβούν συνειδητά ή ασυνείδητα, η αλλαγή των τιμών σε μία βάση δεδομένων κλπ. Πρόκειται για απειλή κυρίως κατά της ακεραιότητας του συστήματος.
- *Συμπτωματικές ασυνέπειες και λάθη* : Προέρχονται από κατασκευαστικές- προγραμματιστικές ατέλειες και από την αμέλεια του διαχειριστή να παρακολουθήσει τις προσθήκες και τις επιδιορθώσεις που ανακοινώνει ο κατασκευαστής.
- *Ιομορφικό λογισμικό* : Μπορεί να είναι δούρειος ίππος ο οποίος εμφανίζεται να εκτελεί άλλη λειτουργία από αυτή που πραγματικά εκτελεί, ιός που λειτουργεί αυτόνομα ή προσκολλάται σε άλλα εκτελέσιμα αρχεία ή σκουλήκι το οποίο εξαπλώνεται πολλαπλασιαζόμενο από σύστημα σε σύστημα.
- *Πλαστογραφία* : Είναι απειλή αποκλειστικά ενάντια στα δεδομένα ενός συστήματος και συμβαίνει όταν κάποιο μη εξουσιοδοτημένο μέρος εισάγει επιπρόσθετα-παραποιημένα δεδομένα σε ένα ΠΣ. Παραδείγματα είναι, η εισαγωγή πλαστών συναλλαγών σε ένα τραπεζικό περιβάλλον, η προσπάθεια αναπαραγωγής παλιών μηνυμάτων (replay), κλπ. Πρόκειται για απειλή κατά της ακεραιότητας και της διαθεσιμότητας του συστήματος.
- *Διακοπή* : Ένα μέρος του συστήματος γίνεται μη-διαθέσιμο, ή άχρηστο ή χάνεται εντελώς. Άρνηση παροχής υπηρεσιών σε τέτοιο βαθμό έτσι ώστε να καθίσταται αδύνατη η χρήση των πόρων του συστήματος. Ενδεικτικά παραδείγματα είναι το σβήσιμο προγραμμάτων ή αρχείων, η κακοήθης καταστροφή μιας συσκευής, κλπ. Πρόκειται κυρίως για απειλή κατά της διαθεσιμότητας του συστήματος.
- *Καταπακτή* : Διάταξη στο κώδικα ενός προγράμματος η οποία επιτρέπει την παράκαμψη ενός μηχανισμού ασφαλείας. Μπορεί να υπάρξει εκ παραδρομής ή εσκεμμένα.

§ *Ο ανθρώπινος παράγοντας* : Συχνά ο ανθρώπινος παράγοντας αποτελεί σημαντικό και δύσκολα αντιμετωπίσιμο πρόβλημα ασφαλείας σε ένα ΛΣ. Ο άνθρωπος μπορεί να αμελήσει κάτι σημαντικό, να παραπλανηθεί, ή να δωροδοκηθεί. (Σωκρ.Κάτσικας-Δημ.Γκρίζαλης-Στεφ.Γκρίτζαλης, 2004, σελ.175)

2.8 ΤΥΠΟΙ ΜΕΤΡΩΝ ΠΡΟΣΤΑΣΙΑΣ

Οι κύριοι τύποι μέτρων για την πρόληψη της εκμετάλλευσης των ευπαθειών ενός πληροφοριακού συστήματος είναι :

- *Κρυπτογράφηση*. Μετασχηματίζοντας τα δεδομένα ώστε να είναι ακατάληπτα από τον εξωτερικό παρατηρητή, η αξία των υποκλοπών και η πιθανότητα για τροποποιήσεις σχεδόν μηδενίζεται.
- *Μέτρα Λογισμικού*. Τα προγράμματα πρέπει να είναι αρκετά ασφαλή και αξιόπιστα ώστε να αποτρέπουν εξωτερικές επιθέσεις. Τα μέτρα προγραμμάτων περιλαμβάνουν :
  - **ü** Μέτρα ανάπτυξης: Πρόκειται για τα πρότυπα σύμφωνα με τα οποία σχεδιάζονται, αποκωδικοποιούνται, ελέγχονται και συντηρούνται τα προγράμματα.
  - **ü** Μέτρα λειτουργικού συστήματος: Πρόκειται για περιορισμούς που επιβάλλονται από το λειτουργικό σύστημα με σκοπό τη προστασία κάθε χρήστη από τους υπόλοιπους χρήστες.
  - **ü** Μέτρα μέσα στα προγράμματα: Πρόκειται για μέτρα που επιβάλλουν περιορισμούς ασφάλειας, όπως για παράδειγμα οι περιορισμοί προσπέλασης σε ένα σύστημα διαχείρισης βάσης δεδομένων (ΣΔΒΔ).
- *Μέτρα υλικού*. Έχουν εφευρεθεί αρκετές συσκευές για να βοηθούν στην ασφάλεια υπολογιστών. Αυτές ποικίλλουν από την υλοποίηση της κρυπτογράφησης με υλικό μέχρι τις συσκευές για επιβεβαίωση της ταυτότητας των χρηστών.
- *Φυσικά μέτρα υλικού.* Είναι από τα πιο εύκολα, πιο αποτελεσματικά και λιγότερο δαπανηρά μέτρα για την ασφάλεια των πληροφοριακών συστημάτων και των συστημάτων βάσεων δεδομένων (για

παράδειγμα, κλειδαριές στις πόρτες, φύλακες, αντίγραφα ασφαλείας, κ.α.).

- *Πολιτικές Ασφάλειας.* Μερικά άλλα μέτρα αποτελούν αντικείμενο πολιτικής, όπως για παράδειγμα ο έλεγχος προσπέλασης. Παρά τα προβλήματα διαχείρισης σε μεγάλους και εξελισσόμενους οργανισμούς, οι πολιτικές ελέγχου προσπέλασης πρέπει να προσαρμόζονται στις επιμέρους συνθήκες και απαιτήσεις ασφάλειας του κάθε πληροφοριακού συστήματος (Γ.Πάγκαλου –Ι.Μαυρίδη, 2002, σελ.27). Όπως επίσης και πολιτικές ασφαλείας που να διασφαλίζουν ότι οι Οργανισμοί προστατεύονται από εσωτερικές και εξωτερικές επιθέσεις, μειώνοντας με αυτόν τον τρόπο τις πιθανότητες διείσδυσής τους στο δίκτυο (www.securitymanager.gr).

2.8.1 ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ

Τα μέτρα προστασίας υποστηρίζουν τη φυσική ασφάλεια και έχουν ως στόχο την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στο χώρο του οργανισμού και της καταστροφής των αγαθών του πληροφοριακού συστήματος. Η προστασία των αγαθών αυτών επιτυγχάνεται με τη δημιουργία επάλληλων περιμέτρων φυσικής ασφάλειας. Οι οδηγίες για τα μέτρα αυτά ασφαλείας περιλαμβάνουν τα εξής :

- *Έλεγχο φυσικής πρόσβασης* σε κρίσιμους χώρους για το πληροφοριακό σύστημα, δηλαδή σε χώρους που βρίσκονται οι εξυπηρετητές των εφαρμογών (server room), χώροι που αποθηκεύονται ευαίσθητα δεδομένα σε ηλεκτρονική ή φυσική μορφή (εφεδρικά αντίγραφα (backup) του λογισμικού συστήματος, προστασία των προγραμμάτων εφαρμογών (βιβλιοθηκών, πακέτων)). Για την προστασία από οποιαδήποτε απειλή, βλάβη, ή ανθρώπινη απροσεξία, τα μέτρα αυτά μπορεί να περιλαμβάνουν τον περιορισμό της κίνησης των επισκεπτών ενός οργανισμού σε συγκεκριμένους χώρους, με τη συνοδεία μελών, τη χρήση μαγνητικών ή έξυπνων καρτών για την είσοδο σε αυτούς τους χώρους κ.λ.π.

- *Εγκατάσταση συστημάτων προστασίας*, όπως για παράδειγμα συστήματος αδιάλειπτης λειτουργίας (U.P.S), συστήματος πυρόσβεσης με αδρανές αέριο, κ.α. (Σωκρ.Κάτσικας-Δημ.Γκρίζαλης-Στεφ.Γκρίτζαλης, 2004, σελ.390)

2.9 ΑΝΑΓΚΑΙΟΤΗΤΑ ΚΑΙ ΣΚΟΠΙΜΟΤΗΤΑ ΑΣΦΑΛΕΙΑΣ

Είναι γεγονός ότι, παρά την προφανή της χρησιμότητα, η λήψη των απαραίτητων μέτρων ασφάλειας δημιουργεί πολλές φορές κάποια πρόσθετη επιβάρυνση στην απόδοση και το κόστος λειτουργίας του πληροφοριακού συστήματος του οργανισμού. Ακόμη θα πρέπει να αποδεχτούμε το κόστος της ασφάλειας και ως κόστος χρόνου αλλά και χρήματος, και είναι αναγκαίο κόστος για την ομαλή και εύρυθμη λειτουργία του οργανισμού. Το κόστος της ασφάλειας εξαρτάται και προκύπτει από την εκάστοτε ακολουθούμενη πολιτική ασφάλειας. Απαιτείται συνεπώς μια πολιτική ασφαλείας η οποία θα πρέπει να εξισορροπεί το κόστος εισαγωγής ασφάλειας από την μία πλευρά και το κόστος ζημιών από πιθανολογούμενο κίνδυνο από την άλλη. Θα πρέπει να δημιουργούνται τέτοιες συνθήκες ασφάλειας ώστε να μη παρεμποδίζεται η ευελιξία και η ανάπτυξη του οργανισμού.

Η αναγκαία πολιτική ασφάλειας καθορίζεται από μία δυναμική εκτίμηση του κόστους των μέτρων ασφάλειας σε σχέση με τις συνέπειες που θα έχει για τον οργανισμό οποιαδήποτε πρόκληση δυσλειτουργίας. Ο βασικός αυτός κανόνας ισχύει για όλους τους τομείς και όλα τα επίπεδα ασφαλείας. Έτσι σε κάθε περίπτωση που απαιτείται η λήψη κάποιου μέτρου ασφάλειας, πρέπει να εξετάζεται η πιθανότητα να συμβεί κάποιο γεγονός/πρόβλημα ασφάλειας, σε σχέση με τις συνέπειες που αυτό θα δημιουργήσει. Εάν η τιμή των δύο αυτών παραμέτρων είναι υψηλή, τότε πρέπει απαραίτητα να ληφθούν μέτρα, ανεξάρτητα από το κόστος πρόληψης.

Τέλος, η ακολουθούμενη πολιτική ασφαλείας θα πρέπει να επανεξετάζεται τακτικά και να διορθώνεται όπου αυτό κρίνεται απαραίτητο, εφόσον η ασφάλεια χαρακτηρίζεται από τη φύση της ως δυναμική παράμετρος και όχι στατική, καθώς η τεχνολογία, ο ανταγωνισμός, η πολυπλοκότητα των

πληροφοριακών συστημάτων και η ολοένα βελτιούμενη επιτηδειότητα των επιτιθέμενων απαιτούν τη λήψη νέων και συνεχώς αυστηρότερων μέτρων ασφάλειας. (Γ. Πάγκαλου – Ι. Μαυρίδη, 2002, σελ.31)

2.10 ΚΑΚΟΒΟΥΛΑ ΠΡΟΓΡΑΜΜΑΤΑ

2.10.1 ΙΟΙ

Ιός (Virus) υπολογιστή είναι ένα πρόγραμμα, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη να "μολύνει" τον υπολογιστή χωρίς τη γνώση ή την άδεια του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν μεταμορφικό ιό. Μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους, παραδείγματος χάριν από ένα χρήστη που στέλνει τον ιό μέσω δικτύου ή του Διαδικτύου, ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως δισκέτα, οπτικό δίσκο ή μνήμη flash USB. (Κιουντούζης Ε., 2002, σελ.209)

Ο ιός δεν είναι μια υπερφυσική οντότητα και δεν γεννιέται από μόνος του : Υπάρχουν κάποιοι που είτε για διασκέδαση είτε για το κέρδος γράφουν αυτού του είδους τα προγράμματα. Μια από τις στρατηγικές με τις οποίες οι ιοί εξαπλώνονται σχετίζεται με τα εκτελέσιμα αρχεία. Η λήψη εκτελέσιμων αρχείων, που διακρίνονται από τις καταλήξεις (exe, com, dll κλπ.), εμπεριέχει το κίνδυνο της μόλυνσης του υπολογιστή από ιούς που μπορεί να κρύβονται μέσα τους.(Silvia Vaccaro, 2007, σελ.133)

Ακόμη μπορούμε να πούμε ότι ιοί υπολογιστών ονομάζονται τα μέρη κώδικα που είναι προσαρτημένα σε ένα κανονικό (ωφέλιμο) πρόγραμμα και αντιγράφονται από μόνα τους. Μπορεί να είναι καταστροφικά (π.χ. να μεταβάλουν και να σβήνουν αρχεία).(Γ. Πάγκαλου – Ι. Μαυρίδη, 2004, σελ.78)

Μερικοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή, είτε με την καταστροφή των προγραμμάτων του είτε με τη διαγραφή αρχείων ή με τη μορφοποίηση (format) του σκληρού δίσκου. Μερικές φορές,

δημιουργούν σε συγκεκριμένο τομέα του σκληρού δίσκου τέτοια καταστροφή, ώστε να είναι αδύνατη η ανάκτηση ολόκληρου του περιεχομένου του. Άλλοι πάλι δεν έχουν ως σκοπό να προκαλέσουν οποιαδήποτε ζημία, (π.χ. παίζουν κάποιο τόνο μουσικής), απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη κειμένου, βίντεο, ή ηχητικών μηνυμάτων, μερικές φορές αρκετά χιουμοριστικών. (Τασόπουλος, Α., 2005, σελ.209)

Όμως, ακόμη και αυτοί οι "καλοκάγαθοι" ιοί μπορούν να δημιουργήσουν προβλήματα στο χρήστη υπολογιστών: Καταλαμβάνουν τη μνήμη που χρησιμοποιείται από τα κανονικά προγράμματα και, κατά συνέπεια, προκαλούν συχνά ασταθή συμπεριφορά του συστήματος και μπορούν να οδηγήσουν σε κατάρρευσή του (system crash). Επιπλέον, πολλοί ιοί είναι, εγγενώς, γεμάτοι προγραμματιστικά σφάλματα, τα οποία πιθανόν να οδηγήσουν στην κατάρρευση των υπολογιστικών συστημάτων και στην απώλεια δεδομένων.

Η «εισβολή» ενός ιού μέσα στο σύστημα της επιχείρησης μπορεί να κάνει πολύ μεγάλη ζημιά, καθώς μπορεί να καταστρέψει σημαντικά αρχεία ή ακόμη και να κλέψει σημαντικά ή απόρρητα έγγραφα της επιχείρησης. Συνεπώς, η ζημιά που μπορεί να προκαλέσει είναι ανυπολόγιστη. (Τασόπουλος Α., 2005, σελ.197)

Υπάρχουν διάφοροι τύποι ιών :

- Ιοί Εκκίνησης : κώδικας που εισάγεται στην διαδικασία εκκίνησης ενός υπολογιστή.
- Παρασιτικούς ιούς : μέρη κώδικα που προσαρτώνται σε εκτελέσιμα προγράμματα (αρχεία .COM. ή .EXE.).
- Συνοδευτικοί ιοί : εναλλακτικά εκτελέσιμα προγράμματα που εισάγονται στην διαδρομή αναζήτησης κανονικών προγραμμάτων.
- Ιοί Μακροεντολών : τμήματα κώδικα που εισάγονται σε αρχεία δεδομένων τα οποία επεξεργάζεται μια εφαρμογή που υποστηρίζει μακροεντολές.

Όσον αφορά τον τρόπο ενεργοποίησης τους, οι ιοί αντιγράφονται από μόνοι τους με δύο βασικούς τρόπους. Όταν εκτελείται ένα μολυσμένο πρόγραμμα :

- Ø Είτε μολύνει άμεσα άλλα μέρη του υπολογιστή, π.χ. άλλες τοποθεσίες στο δίσκο ή άλλα προγράμματα,
- Ø Είτε εγκαθίσταται μόνιμα στη μνήμη από μόνο του και κατόπιν μολύνει άλλα προγράμματα που εκτελούνται ή μέσα αποθήκευσης που εισάγονται για χρήση. (Γ.Πάγκαλου– Ι.Μαυρίδη, 2002, σελ.78)

2.10.2 ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΩΝ ΚΙΝΔΥΝΩΝ ΑΠΟ ΤΟΥΣ ΙΟΥΣ

Οι ιοί εκμεταλλεύονται την έλλειψη προστασίας της ακεραιότητας των συστημάτων και έτσι μια στρατηγική προστασίας από αυτούς συνεπάγεται την εισαγωγή μέτρων διασφάλισης της ακεραιότητας των συστημάτων που αφορούν είτε την αποτροπή της μόλυνσης του συστήματος από ιούς, είτε την ανίχνευση τους και την απομάκρυνση αυτών από το σύστημα. Έτσι έχουμε :

I. **Μέτρα προστασίας από ιούς** που έχουν να κάνουν με *Φυσικά και διαχειριστικά μέτρα προστασίας* :
   - Ÿ Χρήση των διακοπτών ασφαλείας των δισκετών για την προστασία τους από μόλυνση.
   - Ÿ Υιοθέτηση, όπως ήδη κάνουν πολλές επιχειρήσεις, πολιτικών απαγόρευσης χρήσης οποιουδήποτε λογισμικού που δεν έχει εγκριθεί από το τμήμα ασφάλειας της επιχείρησης. Για αυτό όλα τα προϊόντα λογισμικού πρέπει να αποκτώνται με επίσημες διαδικασίες που έχουν ως συνέπεια την ελαχιστοποίηση του κινδύνου μόλυνσης από παρασιτικούς ιούς.
   - Ÿ Εγκατάσταση κλειδαριών στις θήκες των δισκετών και αφαίρεση τους μόνο από το υπεύθυνο προσωπικό, ώστε να εμποδίζεται η εισαγωγή παράνομου λογισμικού στην επιχείρηση.
   - Ÿ Έλεγχος όλων των εισαγόμενων αρχείων (δεδομένων και λογισμικού) σε ειδικές μηχανές που βρίσκονται σε καραντίνα και έχουν εγκαταστημένο λογισμικό ανίχνευσης ιών.

Ακόμη με *Κρυπτογραφικά αθροίσματα* : Αποτελούν έναν κλασικό μηχανισμό προστασίας της ακεραιότητας του συστήματος. Με αυτά υπολογίζεται το κρυπτογραφικό άθροισμα μιας καθαρής ‘έκδοσης’ των προγραμμάτων που θα προστατευθούν, ενώ το άθροισμα αποθηκεύεται κατόπιν σε ένα ασφαλές

μέρος. Πριν από την χρησιμοποίηση κάθε αρχείου επανυπολογίζεται και επικυρώνεται το άθροισμα του, συγκρινόμενο με αυτό που είχε αρχικά αποθηκευθεί.

II. **Ανίχνευση και απομάκρυνση των ιών.** Οι ανιχνευτές ιών ψάχνουν για υπογραφές ιών. Οι υπογραφές τώρα είναι το μέρος του υιικού κώδικα που αποτελείται από μία ακολουθία εντολών και που είναι υπεύθυνο για την διαδικασία αποκρυπτογράφησης και που παραμένει χωρίς κρυπτογράφηση, αφήνοντας έτσι μια υπογραφή που είναι ικανή για τον εντοπισμό του ιού. Οι υπογραφές ιών μπορούν να χρησιμοποιηθούν για την αναγνώριση μολύνσεων από γνωστές οικογένειες ιών και τη μετέπειτα απομάκρυνση τους. Οι ανιχνευτές γνωρίζουν εκ των προτέρων τον ιό που πρόκειται να ανιχνεύσουν και γι αυτό χρειάζονται συνεχή ενημέρωση του μητρώου υπογραφών ταυτοποιημένων ιών σε τακτά χρονικά διαστήματα, κάτι το οποίο αποτελεί μειονέκτημα, καθώς παραμένει η απειλή από τους πολυμορφικούς ιού, οι οποίοι δεν ανιχνεύονται εύκολα καθώς δεν έχουν απλές χαρακτηριστικές υπογραφές. Ακόμη, υπάρχουν ανιχνευτές οι οποίοι αποτελούν τεχνική αντιβιοτικού λογισμικού που θεωρείται απαιτητική σε πόρους για την επιχείρηση.

(Γ. Πάγκαλου – Ι. Μαυρίδη, 2002, σελ.84)

Οι συγγραφείς ιών και κακόβουλου λογισμικού γίνονται εξυπνότεροι μέρα με τη μέρα, καθώς προσπαθούν να αποφύγουν τον εντοπισμό από τα προϊόντα Antivirus. Οι διαχειριστές δικτύων πρέπει να εφαρμόσουν λύσεις ασφαλείας όπως αυτές της ESET, οι οποίες να μπορούν να αντεπεξέλθουν σε νέες και άγνωστες απειλές που εκμεταλλεύονται καινούριες τεχνολογίες, εστιάζοντας κυρίως σε εξελιγμένες λύσεις με μηχανή προληπτικής ανίχνευσης "heuristics", που παρέχει μία ολοκληρωμένη και προηγμένη προστασία, η οποία είναι και απλή στην ανάπτυξη αλλά και στη διαχείρισή της. Επίσης η λύση αυτή παρέχει άμεσα πληροφορίες για την κατάσταση του δικτύου, έτσι ώστε ο διαχειριστής να μπορεί να λάβει τα απαραίτητα μέτρα το ταχύτερο δυνατόν (www.securitymanager.gr).

2.10.3 ΣΚΟΥΛΗΚΙΑ

Τα σκουλήκια (worms) είναι προγράμματα που εξαπλώνονται μέσω των δικτυωμένων υπολογιστών, αντιγράφοντας τα ίδια ανεξέλεγκτα, αλλά δεν προκαλούν άλλου τύπου επιπλοκές. Μοιάζουν πολύ με τους ιούς στο ότι αντιγράφονται από μόνα τους και επιτίθενται σε συστήματα με σκοπό να επιφέρουν βλάβες. Πρόκειται για αυτόνομα προγράμματα τα οποία μολύνουν υπολογιστικά συστήματα μόνο μέσω δικτυακών συνδέσεων.

Πέρα όμως από την συμπεριφορά αναπαραγωγής τους από σύστημα σε σύστημα, τα σκουλήκια συχνά εκτελούν και κακόβουλες πράξεις, που δεν περιορίζονται μόνο στην καταστροφή αρχείων. Έτσι, μέσω των δικτυακών συνδέσεων μπορούν να υποκλέψουν και να μεταφέρουν προς τους συγγραφείς τους πληροφορίες που αφορούν συνθηματικά χρηστών και άλλες ευαίσθητες αλλά και πολύτιμες πληροφορίες. Επιπλέον, μπορούν να επιφέρουν πλήρη αποδιοργάνωση των λειτουργιών ενός συστήματος ώστε να προκαλείται επίθεση άρνησης εξυπηρέτησης. Αυτό συμβαίνει από παράλληλες και ανοργάνωτες επιθέσεις περισσότερων του ενός σκουληκιών στο ίδιο σύστημα.

Για την αποφυγή της μόλυνσης από σκουλήκια επιβάλλεται ο εντοπισμός και η αντιμετώπιση όλων των ευπαθών σημείων του υπολογιστικού συστήματος από τους διαχειριστές του. Αυτό σημαίνει ότι πρέπει να προσεχθούν ιδιαίτερα τα αδύνατα σημεία που μπορούν να εκμεταλλευθούν τα σκουλήκια (όπως εύκολα συνθηματικά ή ανεξέλεγκτες δικτυακές υπηρεσίες). Τρόπος προφύλαξης από τα σκουλήκια είναι η γνώση των μεθόδων που χρησιμοποιούν για τον εντοπισμό και την αξιοποίηση των ευπαθών σημείων του συστήματος. Όπως γίνεται γενικότερα για την πρόληψη εισβολών, η χρήση διατάξεων και ελέγχου προσπέλασης μπορούν να μειώσουν τους κινδύνους επίτευξης των στόχων των σκουληκιών.(Γ. Πάγκαλου – Ι. Μαυρίδη, 2002, σελ.85)

2.10.4 ΔΟΥΡΕΙΟΙ ΙΠΠΟΙ

Οι Δούρειοι Ίπποι (trojan horses) είναι προγράμματα με κρυφές λειτουργίες δηλαδή, ενώ επικαλούνται ότι επιτελούν κάποια εργασία, στην πραγματικότητα εκτελούν και μία/ή διαφορετική λειτουργία. Αυτή η λανθάνουσα δραστηριότητα είναι που συνήθως εκτελεί καλυμμένες ενέργειες, όπως η κλοπή των συνθηματικών των χρηστών. Οι Δούρειοι Ίπποι δεν αναπαράγονται μόνοι τους, ούτε αντιγράφουν τους εαυτούς τους. Πρέπει να βασιστούν στους ίδιους τους χρήστες τους για την εγκατάσταση και την εκτέλεση τους. Κύριες πηγές Δούρειων Ίππων είναι οι διάφοροι εξυπηρετητές αρχείων και διανομής αρχείων (FTPservers). Για την ανίχνευση τους επιβάλλεται η καθιέρωση και η συνεπής εφαρμογή από τους οργανισμούς συγκεκριμένων πολιτικών εγκατάστασης επίσημα αγορασμένου λογισμικού, καθώς κι εκπαίδευσης των χρηστών, έτσι ώστε να αποκτήσουν τα απαραίτητα κίνητρα για να συμμερίζονται τους κινδύνους που αναλαμβάνουν όταν δοκιμάζουν προγράμματα άγνωστης προέλευσης. (Γ. Πάγκαλου – Ι. Μαυρίδη, 2002, σελ.86)

2.10.5 ΤΕΧΝΙΚΕΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

- Επίγνωση σε θέματα Ασφαλείας. Το λογισμικό που οι χρήστες εγκαθιστούν στα υπολογιστικά συστήματα πρέπει να προέρχεται από έμπιστες πηγές. Πρέπει να αποφεύγουν να εγκαθιστούν λογισμικό που μεταφορτώνουν από τυχαίες διευθύνσεις στο Διαδίκτυο. Ακόμη η πολιτική ασφαλείας πρέπει να απαγορεύει στους χρήστες να εγκαθιστούν μη ελεγμένο λογισμικό. Τέλος είναι ιδιαίτερα χρήσιμο οι χρήστες να γνωρίζουν τρόπους επανόρθωσης από προσβολή από Κακόβουλο Λογισμικό καθώς και τρόπους από περιορισμού εξάπλωσης του Κακόβουλου Λογισμικού.
- Αντιβιοτικό Λογισμικό. Αυτά τα προγράμματα ανιχνεύουν τα αρχεία ενός συστήματος προσπαθώντας να εντοπίσουν την ύπαρξη Ιών στο σύστημα.

- Αρχεία Ελέγχου του Λειτουργικού Συστήματος. Είναι ιδιαίτερα χρήσιμα στον εντοπισμό Δούρειων Ίππων που προσπαθούν να στείλουν δεδομένα σε εξωτερικό δίκτυο ή υπολογιστικό σύστημα, ή και για τον εντοπισμό Κακόβουλου Λογισμικού που προσπαθεί να διαβάσει ή να εγγράψει δεδομένα από περιοχή του πληροφοριακού συστήματος στην οποία δεν επιτρέπεται η πρόσβαση.
- Αυστηρά μέτρα ασφαλείας. Είναι αναγκαία για την ελαχιστοποίηση της ζημιάς που μπορεί να επιφέρει το Κακόβουλο Λογισμικό. Τα μέτρα αυτά περιλαμβάνουν την επιβολή ελέγχου πρόσβασης και την εκτέλεση εφαρμογών παραχωρώντας τους τα ελάχιστα απαιτούμενα δικαιώματα στο σύστημα.
- Απομόνωση. Πληροφοριακά συστήματα που περιέχουν πολύτιμη πληροφορία για έναν οργανισμό πρέπει να απομονώνονται δικτυακά, από τα συστήματα που είναι συνδεδεμένα με εξωτερικά ή άλλα μη ελεγχόμενα πληροφοριακά συστήματα.
- Αναχώματα Ασφαλείας(firewalls). Προκειμένου να αποκλεισθεί η δυνατότητα σε Κακόβουλο Λογισμικό που εκτελείται σε εξωτερικό, μη ελεγχόμενο περιβάλλον, να αποκτήσει πρόσβαση σε ένα εσωτερικό δίκτυο.
- Εργαλεία ανίχνευσης Εισβολών. Αυτά τα εργαλεία ανιχνεύουν την κίνηση από και προς συγκεκριμένα σημεία ενός δικτύου, και εντοπίζουν πιθανές ακολουθίες ενεργειών που σηματοδοτούν ενδεχόμενη απόπειρα παραβίασης της πολιτικής ασφαλείας. Με τα εργαλεία αυτά είναι δυνατός ο εντοπισμός Κακόβουλου Λογισμικού με βάση τις ενέργειες που αυτό εκτελεί στο δίκτυο.
- Ενημέρωση των οργανισμών που προσφέρουν προϊόντα και υπηρεσίες προστασίας από κακόβουλο λογισμικό. Σε περίπτωση προσβολής από –νέο- κακόβουλο λογισμικό, ο υπεύθυνος του πληροφοριακού συστήματος που προσβλήθηκε πρέπει να ενημερώνει τους οργανισμούς αυτούς για το συγκεκριμένο πληροφοριακό σύστημα, για την ύπαρξη νέου Κακόβουλου Λογισμικού. Επιπλέον, οι οργανισμοί αυτοί πρέπει να παράγουν ενημερωμένες εκδόσεις του αντιβιοτικού λογισμικού τους. (Σωκρ.Κάτσικας-Δημ.Γκρίζαλης-Στεφ.Γκρίτζαλης, 2004, σελ.252)

2.11 Οι HACKERS ΚΑΙ Οι CRACKERS

- **PHREAKS:** Καθώς το τηλεφωνικό δίκτυο προϋπήρξε του δικτύου υπολογιστών, έτσι και των σύγχρονων hacker προηγήθηκαν οι phone phreaks. Αυτοί ήταν άνθρωποι που χρησιμοποιούσαν το τηλεφωνικό σύστημα κυρίως για επικοινωνία με οποιοδήποτε μέρος του κόσμου με τρόπο φθηνό, γρήγορο και φυσικά μη αντιληπτό, εκμεταλλευόμενοι κλεμμένους τηλεφωνικούς κωδικούς και κάνοντας τροποποιήσεις σε τηλεφωνικά κέντρα. Στα μέσα της δεκαετίας του ’80, η δημοσιοποίηση των κωδικών αυτών για κοινή χρήση αποτελούσε μία βασική προϋπόθεση για να θεμελιωθεί μία bona fides μεταξύ του επίδοξου phreak και της phreaking κοινότητας
- **HACKERS:** Hacker είναι όποιος ενδιαφέρεται για τις μυστικές και κρυφές διεργασίες οποιουδήποτε λειτουργικού συστήματος υπολογιστή. Έχουν εκτενή γνώση λειτουργικών συστημάτων και γλωσσών προγραμματισμού. Προσπαθούν να ανακαλύψουν τα κενά και ρήγματα στα συστήματα υπολογιστών καθώς και τους λόγους ύπαρξης αυτών. Αναζητούν σταθερά πρόσθετη γνώση, τη μοιράζονται ελεύθερα και δεν καταστρέφουν ποτέ και τίποτα σκοπίμως.
- **CRACKERS:** Cracker χαρακτηρίζεται αυτός που διεισδύει ή παραβιάζει την ακεραιότητα συστημάτων (σπάει κωδικούς ασφαλείας κλπ) με πρόθεση τη διάπραξη κακόβουλων πράξεων, όπως καταστροφή δεδομένων, στρέβλωση συστημάτων και παρεμπόδιση λειτουργιών.

Η *πρώτη γενιά* των hackers αποτελείται από μέλη πανεπιστημιακών ομάδων των μεγάλων τεχνολογικών πανεπιστημίων MIT και Stanford.Αυτοί οι επιστήμονες, σχεδόν αποκομμένοι από την υπόλοιπη κοινωνία, ζούσαν εργαζόμενοι στα εργαστήριά τους και ανέπτυξαν τις πρώτες μεθόδους προγραμματισμού κατά το 1950 και 1960 στις υπηρεσίες κυρίως, βέβαια, της Αμερικανικής κυβέρνησης. (Κιουντούζης Ε., 2002, ελ.214)

Η *δεύτερη γενιά* αποτελείται από εμπορικά προσανατολισμένους επιστήμονες που ως σκοπό είχαν την ευρεία διάδοση της πληροφορικής τεχνολογίας στις μάζες. Ήταν αυτοί που δημιούργησαν τους πρώτους

προσωπικούς υπολογιστές. Επιπρόσθετος στόχος της νέας γενιάς αυτής ήταν η μελέτη και ο πειραματισμός για τη βελτίωση της αλληλεπίδρασης ανθρώπου με υπολογιστή, παραδειγματικό επίτευγμα της οποίας ήταν το γνωστό και απαραίτητο σήμερα «ποντίκι».

Η *τρίτη γενιά* αποτελείται από τους προγραμματιστές, οι οποίοι δημιούργησαν τις βασικές δομές στις οποίες στηρίχθηκε μετέπειτα η δημιουργία των ηλεκτρονικών παιχνιδιών. Η γενιά αυτή δείχνει πλέον να αντιλαμβάνεται πλήρως την οικονομική δυναμική του συγκεκριμένου τομέα και εργάζεται δραστικά για να ανταποκριθεί στη ζήτηση που δημιουργεί η ευρεία εξάπλωση της χρήσης προσωπικού ηλεκτρονικού υπολογιστή αλλά και για να διαμορφώσει νέες προοπτικές αγοράς και νέες ανάγκες. (Γκίνογλου Δ., Ταχυνάκη Π., Πρωτοψάλτη Ν., 2004, σελ.168)

Η *τέταρτη* όμως *γενιά* είναι αυτή που συγκρότησε την hacker κοινότητα όπως την ξέρουμε σήμερα. Ενώ με τις προηγούμενες γενιές υπήρχε μια προσήλωση στην επίτευξη μίας εκλαΐκευσης του νέου μέσου και κυρίως μία χρήση αυτού βασισμένη σε ανάγκες και δεδομένα της καθημερινότητας, η νέα αυτή γενιά εμφάνισε για πρώτη φορά μία αντεστραμμένη ψυχολογική συμπεριφορά, μία αναρχική τάση όχι σύνθεσης νέων δεδομένων και προγραμμάτων, αλλά αντίθετα μία αποδημητική και μία ενδοσκοπική εξερευνητική ενέργεια, που εξελίχθηκε στη μοντέρνα μορφή hacking, η οποία προσεγγίζει την εικόνα που έχουμε στο μυαλό μας για τον hacker, εικόνα που άπτεται και εγκληματικών συμπεριφορών. (Κιουντούζης Ε., 2002, σελ.217)

Η εκρηκτική εξέλιξη του διαδικτύου δημιούργησε ένα νέο κοινωνικό μόρφωμα, όπου αναπόφευκτα διάφορες συμπεριφορές αποκτούν μία νέα σημασία, όταν πραγματώνονται εκτός εργαστηρίων και επηρεάζουν την ανθρώπινη καθημερινότητα πλέον. Έτσι, η πρόσβαση σε έναν υπολογιστή δε θεωρείται πλέον ελεύθερη, αλλά απαιτείται μία εξουσιοδότηση. Χωρίς την εξασφάλιση αυτής, εισερχόμεθα πλέον στη νομικά ενδιαφέρουσα περίπτωση της παραβίασης, η οποία θα μπορούσε να αξιολογηθεί ως ανήθικη και εγκληματική. (Τασόπουλος Α., 2005 ελ.197)

2.12 ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΑΣΦΑΛΕΙΑΣ

Όταν αναφερόμαστε στην ασφάλεια χρησιμοποιούμε συχνά τον όρο ψηφιακό πιστοποιητικό, γνωστό και ως Ψηφιακή Ταυτότητα (Digital ID) : Πρόκειται για την ηλεκτρονική μορφή ενός διαβατηρίου ή μιας εμπορικής άδειας, και γενικά μιας εγγύησης, η οποία εκδίδεται από μία έγκυρη Αρχή και η οποία μπορεί να προβάλλεται από πρόσωπα ή οργανισμούς σε ηλεκτρονική μορφή προκειμένου να ελέγχεται η ταυτότητα ή το δικαίωμα πρόσβασης στην πληροφορία. (Silvia Vaccaro, 2007, σελ.87)

Το ψηφιακό πιστοποιητικό χρησιμοποιείται για την κρυπτογράφηση πληροφοριών για την ασφαλή μεταφορά τους μέσα από το internet. Μπορεί να χρησιμοποιείται για την δημιουργία μιας ψηφιακής υπογραφής για ηλεκτρονικό ταχυδρομείο, η οποία πιστοποιεί την ταυτότητα του αποστολέα. Ένα ψηφιακό πιστοποιητικό μπορεί να αγορασθεί από μία αρχή πιστοποίησης, η οποία ελέγχει και πιστοποιεί την ταυτότητα μας. (Ι.Βογιατζής, 2006, σελ.66)

Όταν μία Αρχή Πιστοποίησης (Certification Authority-CA), όπως η καλιφορνέζικη VeriSing (η πιο έγκυρη σε παγκόσμια κλίμακα), εκδίδει μία ψηφιακή ταυτότητα, πιστοποιεί ότι ο κάτοχος δεν έχει κατασκευάσει κάποια πλαστή ταυτότητα και επομένως εγγυάται την αυθεντικότητα της τοποθεσίας. Όταν μια τέτοια Αρχή παρέχει ένα ψηφιακό πιστοποιητικό προκειμένου να προβείτε στις ενέργειες σας, η Αρχή χρησιμοποιεί το όνομα της για να σας δώσει το δικαίωμα να χρησιμοποιήσετε την ονομασία και την ηλεκτρονική διεύθυνση της Εταιρείας σας. (Silvia Vaccaro, 2007, σελ.87)

Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται από τις εταιρείες που κάνουν εμπορία μέσω του internet για το αν κρυπτογραφούν τα στοιχεία των πιστοποιητικών καρτών καθώς αυτά ταξιδεύουν μέσα στο internet. (Ι.Βογιατζής, 2006, σελ.66)

Χρησιμοποιούνται δύο τύποι πιστοποιητικών ασφαλείας :

- Τα «προσωπικά πιστοποιητικά» τα οποία πιστοποιούν την ταυτότητα των χρηστών και στα οποία προσδιορίζονται πληροφορίες όπως το όνομα χρήστη και ο κωδικός πρόσβασης. Τέτοια στοιχεία

χρησιμοποιούνται όταν ο χρήστης αποστέλλει προσωπικές πληροφορίες στο Internet ή σε μια τοποθεσία που απαιτεί τον συγκεκριμένο τύπο πιστοποίησης.

- Τα «πιστοποιητικά των τοποθεσιών Web» τα οποία πιστοποιούν την αυθεντικότητα και την ασφάλεια μιας τοποθεσίας, εγγυώμενα ότι καμία άλλη τοποθεσία δεν μπορεί να λάβει την ταυτότητα της αυθεντικής τοποθεσίας. (Silvia Vaccaro, 2007, σελ.87)

2.12.1 ΥΠΟΦΡΑΦΗ/ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΜΗΝΥΜΑΤΩΝ-EMAIL

Στην ηλεκτρονική μορφή του ταχυδρομείου έχουν αλλάξει οι διαδικασίες μεταφοράς της αλληλογραφίας ως εξής:

Αποστολέας **à** ενδιάμεσοι υπολογιστές **à** διακομιστής αλληλογραφίας αποστολέα (SMTP server) **à** πολλοί ενδιάμεσοι υπολογιστές **à** διακομιστής αλληλογραφίας παραλήπτη (POP server) **à** ενδιάμεσοι υπολογιστές **à** παραλήπτης

Παρατηρούμε ότι ανάμεσα στους δύο που αλληλογραφούν έχουν παρεισφρήσει διάφοροι ενδιάμεσοι υπολογιστές, τους οποίους δεν ελέγχουμε. Αν τώρα λάβουμε υπόψη το γεγονός πως η εποχή που σχεδιάστηκαν τα πρωτόκολλα επικοινωνίας του internet και του email, ήταν αθώα, χωρίς ανάγκη για ασφάλεια, ταυτοποίηση και υπογραφές, αρχίζει να διακρίνεται η διαφορετικότητα αυτής της μορφής του ταχυδρομείου από τα αποτελέσματα που έχει η έλλειψή τους. Καθημερινά όλοι λαμβάνουμε SPAM, διαφημίσεις (για θεμιτά ή μη προϊόντα) και ιούς (virus). Λαμβάνουμε επίσης μηνύματα, με αποστολέα κάποιον γνωστό ή φίλο που στην πραγματικότητα δεν έστειλε ποτέ τίποτα. (Παπαθανασίου Α., 2008)

Σε όλα αυτά τα προβλήματα δεν μπορούμε να εφαρμόσουμε κάποια συνταγή που θα τα εξαφανίσει ως δια μαγείας, αυτό είναι αδύνατο. Το πρόβλημα είναι η δικτυακή υποδομή (underlying network) και σε επίπεδο εφαρμογών αυτό που μπορεί να γίνει, απλά καλύπτει μερικώς το πρόβλημα. Γι' αυτό έχουν δημιουργηθεί φίλτρα ανεπιθύμητης αλληλογραφίας με προσαρμογή (Bayesian filtering) ή χωρίς, για τα προγράμματα email, καθώς

και πολλές ανεξάρτητες ομάδες δημιουργίας μαύρων λιστών (black list) εξυπηρετητών αλληλογραφίας (SMTP servers), τις οποίες προγράμματα αλλά και πάροχοι (ISPs) λαμβάνουν υπόψη τους, σε κάποιες περιπτώσεις.

Υπάρχουν προγράμματα που μπορούν εύκολα να τροποποιήσουν και να πλαστογραφήσουν τις επικεφαλίδες (headers) των μηνυμάτων και να βάλουν για παράδειγμα στη θέση του αποστολέα όποια διεύθυνση επιθυμεί ο χρήστης τους. Με αυτό τον τρόπο λαμβάνετε κάποιες φορές ανεπιθύμητα μηνύματα από τον εαυτό σας! Επιπροσθέτως, η αλληλογραφία, καθώς περνάει από υπολογιστή σε υπολογιστή είναι εντελώς διαφανής (on the clear) και μπορεί να αναγνωστεί από τον οποιονδήποτε το θελήσει, έτσι απλά, σαν μια ταχυδρομική κάρτα που περνά από χέρι σε χέρι. Διαφημιστικές εταιρείες, συστήματα παρακολούθησης πολιτών, κυβερνήσεις, κακοποιοί και περίεργοι ενδιαφέρονται πάντα για αυτά που σκέφτονται οι άνθρωποι και να είστε βέβαιοι πως όλα παρακολουθούνται λιγότερο ή περισσότερο. Στο κλασικό ταχυδρομείο δεν υπήρχαν σε τόσο έντονο βαθμό αυτά τα θέματα. (Παπαθανασίου Α., 2008)

Ένας τρόπος με τον οποίο θα μπορείτε να ελέγχετε την αυθεντικότητα στα μηνύματα που θα ανταλλάσσετε με γνωστούς, συγγενείς, φίλους και όποιον άλλο το επιθυμεί, είναι η ψηφιακή υπογραφή και κρυπτογραφία. Επιπλέον, θα είστε σίγουροι 100% πως είναι πράγματι απ’ αυτούς. Επιπλέον θα έχετε τη δυνατότητα να κρυπτογραφήσετε τα μηνύματα και τις επισυνάψεις τους (attachments), έτσι ώστε κανείς άλλος να μην μπορεί να τα διαβάσει πέρα από εσάς και αυτόν που το έστειλε, ή εσάς και τον παραλήπτη του. Δεν χρειάζεται να είστε μυστικός πράκτορας ή τρομοκράτης για να απαιτείτε το προσωπικό σας απόρρητο.

Η κρυπτογραφία δημόσιου κλειδιού για να εφαρμοστεί, θα πρέπει να δημιουργήσετε ένα ζεύγος δημόσιου-ιδιωτικού κλειδιού (key-pair). Το δημόσιο κλειδί (public) το δίνετε σε όσους θέλετε, το βάζετε στις σελίδες σας, ή ακόμα καλύτερα το στέλνετε και σε εξειδικευμένους εξυπηρετητές (key-servers) που το κρατάνε για όποιον το χρειαστεί. Απ’ την άλλη, το προσωπικό κλειδί (private), το φυλάτε σαν τα μάτια σας. Δεν πρέπει να ξεφύγει ποτέ απ’ τον έλεγχό σας. (Παπαθανασίου Α., 2008)

Προϋπόθεση για την κρυπτογράφηση αποτελεί η κατοχή δημόσιου κλειδιού του παραλήπτη του μηνύματος. Η απόκτηση του δημόσιου κλειδιού τρίτων, γίνεται εύκολα με δύο τρόπους :

- Π.χ. Όταν δεχόμαστε ένα ψηφιακά υπογεγραμμένο μήνυμα, ταυτόχρονα λαμβάνουμε και το δημόσιο κλειδί του αποστολέα.
- Ένας άλλος τρόπος απόκτησης μέσω μιας υπηρεσίας καταλόγου (directory service). (Γ. Πάγκαλου – Ι. Μαυρίδη, 2002, σελ.299)

Τώρα, αν κάποιος θελήσει να σας στείλει ένα μήνυμα, είτε υπογεγραμμένο είτε κρυπτογραφημένο, θα χρησιμοποιηθεί το δημόσιο κλειδί σας και όταν λάβετε μετά το μήνυμα, θα χρησιμοποιηθεί το προσωπικό σας κλειδί για να ελεγχθεί η υπογραφή ή για να αποκρυπτογραφηθεί το κείμενο. Ανάποδα, αν εσείς θελήσετε να στείλετε ένα μήνυμα σε κάποιον, για την κρυπτογράφηση των μηνυμάτων μας θα πρέπει να έχουμε ή να βρούμε το δημόσιο κλειδί του (πχ: από έναν key-server). Με αυτό θα γίνει υπογραφή ή κρυπτογράφηση του κειμένου και ο παραλήπτης θα το διαβάσει με το προσωπικό του κλειδί. (Παπαθανασίου Α., 2008)

2.13 BACK UP

Ένα αντίγραφο **ασφαλείας** ή τη διαδικασία **δημιουργίας αντιγράφων ασφαλείας** αναφέρεται σε λήψη αντιγράφων των δεδομένων, έτσι ώστε αυτά τα πρόσθετα αντίγραφα να χρησιμοποιηθούν για να *επαναφέρουμε* την αρχική, μετά την απώλεια δεδομένων, εκδήλωση. (Παπαθανασίου Α., 2008)

Τα Backups έχουν δύο διαφορετικούς σκοπούς. Πρωταρχικός σκοπός είναι η ανάκτηση των στοιχείων ως αντίδραση στην απώλεια δεδομένων, είτε με τη διαγραφή των δεδομένων ή αλλοιωμένα δεδομένα. Η απώλεια δεδομένων είναι μια πολύ συνηθισμένη «εμπειρία» των χρηστών των υπολογιστών.

Δεδομένου ότι ένα εφεδρικό σύστημα περιέχει τουλάχιστον ένα αντίγραφο όλων των δεδομένων, οι απαιτήσεις για την αποθήκευση των δεδομένων είναι σημαντικές. Η διοργάνωση ενός τέτοιου χώρου αποθήκευσης και η διαχείριση της διαδικασίας δημιουργίας αντιγράφων ασφαλείας είναι μια περίπλοκη επιχείρηση. Στη σύγχρονη εποχή των υπολογιστών, υπάρχουν πολλά διαφορετικά είδη δεδομένων, συσκευές αποθήκευσης που είναι

χρήσιμα για τη δημιουργία αντιγράφων ασφαλείας. Έχουν αναπτυχθεί πολλές διαφορετικές τεχνικές για να βελτιστοποιηθεί η διαδικασία δημιουργίας αντιγράφων ασφαλείας. (Παπαθανασίου Α., 2008)

2.14 ΑΣΦΑΛΕΙΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΠΟΥ ΔΙΑΚΙΝΟΥΝΤΑΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Η διακίνηση των δεδομένων μέσω του διαδικτύου προσφέρει σημαντικά πλεονεκτήματα σε σχέση με τις κλασικές μεθόδους διακίνησης τους. Τα δεδομένα γίνονται διαθέσιμα σε ελάχιστο χρόνο για χρήση και αξιοποίηση, ανεξάρτητα από τον όγκο τους, ενώ το κόστος αποστολής σε οποιαδήποτε απόσταση είναι εξαιρετικά μικρό. Η χρήση του διαδικτύου προσθέτει όμως επιπλέον απειλές κατά της ασφάλειας των πληροφοριών. Ακόμη, οι συνδεδεμένοι στο διαδίκτυο υπολογιστές είναι δυνατόν να αποτελέσουν στόχο διάφορων επιθέσεων.

Κατά την πραγματοποίηση οποιασδήποτε επικοινωνίας ή συναλλαγής μέσω του διαδικτύου θα πρέπει λοιπόν να εξασφαλίζεται για τα δεδομένα που διακινούνται ότι:

- Δεν είναι αναγνώσιμα και αναγνωρίσιμα παρά μόνο από τον νόμιμο αποστολέα και τον αποδέκτη τους.
- Δεν έχουν αλλοιωθεί κατά τη μεταφορά τους μέσω του διαδικτύου. Δηλαδή, το μήνυμα που παραλήφθηκε είναι το ίδιο με αυτό που αποστάλθηκε.
- Ο αποστολέας και ο παραλήπτης είναι πράγματι αυτοί που ισχυρίζονται ότι είναι.
- Ο αποστολέας δεν είναι δυνατόν να αρνηθεί το γεγονός ότι έστειλε το μήνυμα.
- Οι εμπιστευτικές πληροφορίες προστατεύονται από μη εξουσιοδοτημένη αποκάλυψη.
- Οι υπολογιστές διαθέτουν ικανοποιητική προστασία από ιούς που μεταδίδονται μέσω του διαδικτύου.
- Οι ευαίσθητες πληροφορίες (όπως για παράδειγμα, αριθμοί πιστωτικών καρτών, θέματα εξετάσεων, κλπ.) προστατεύονται

επαρκώς όταν διακινούνται μέσω του διαδικτύου (για παράδειγμα, με επαρκή κρυπτογράφηση). (Γ. Πάγκαλος – Ι. Μαυρίδης, 2002, σελ.30)

2.14.1 ΔΙΑΔΙΚΤΥΟ

Το Διαδίκτυο είναι ένα απεριόριστο Παγκόσμιο Δίκτυο το οποίο αποτελείται από πολλά τοπικά δίκτυα. Το Διαδίκτυο γεννήθηκε για να καταστεί δυνατή η επικοινωνία και η ανταλλαγή πληροφοριών. Οι πληροφορίες που ανταλλάσσονται στο Διαδίκτυο δεν αποτελούνται μόνο από ήχους ή κείμενα, αλλά και από εικόνες, έγγραφα και προγράμματα. Το δυνατό σημείο του Διαδικτύου και ταυτόχρονα η αιτία για την ταχύτατη εξάπλωση του είναι ότι 'μιλάει' μια παγκόσμια γλώσσα, που είναι κατάλληλη για όλους σχεδόν τους υπάρχοντες επεξεργαστές.

Το πρώτο πρόβλημα σε κάθε διαδικασία επικοινωνίας είναι φυσικά, ο καθορισμός μιας γλώσσας η οποία να είναι κοινή για όλους τους παράγοντες που συμμετέχουν στην επικοινωνία. Οι παράγοντες αυτοί στην περίπτωση του Διαδικτύου είναι κατά κύριο λόγο οι ηλεκτρονικοί υπολογιστές. Και οι ηλεκτρονικοί υπολογιστές, παρόλο που χρησιμοποιούν όλοι το δυαδικό σύστημα, συχνά 'μιλούν' γλώσσες διαφορετικές και ασυμβίβαστες. Οι διαφορετικοί ηλεκτρονικοί υπολογιστές χρησιμοποιούν στην κυριολεξία εντελώς διαφορετικά λειτουργικά συστήματα, καθώς και διαφορετική κωδικοποίηση χαρακτήρων και διαφορετική δομή δεδομένων. Για να γίνει εφικτή η μεταξύ τους επικοινωνία χρειάζεται να καθοριστούν κοινά αποδεκτοί κανόνες. Τη λειτουργία αυτή εκτελούν τα *πρωτόκολλα*.

Το πρωτόκολλο επικοινωνίας καθορίζει τους κανόνες χειρισμού και της αποστολής των bit (δυαδικά ψηφία που συνθέτουν την πληροφορία) στους ηλεκτρονικούς υπολογιστές που χρησιμοποιούν διαφορετικά λειτουργικά περιβάλλοντα και διαφορετικές αρχιτεκτονικές hardware. Στην περίπτωση του Διαδικτύου το οποίο συνδέει εκατομμύρια ηλεκτρονικούς υπολογιστές και υπο-δίκτυα, το ζήτημα του καθορισμού κοινών πρωτοκόλλων είναι θεμελιώδες. Το πρωτόκολλο που επιτρέπει σήμερα τη λειτουργία αυτής της σύνθετης και πολυεθνικής κοινωνίας συνήθως υποδεικνύεται με τα αρχικά

TCP/IP (Transfer Control Protocol/Internet Protocol. Ένα από τα χαρακτηριστικά του πρωτοκόλλου επικοινωνίας είναι ότι πρόκειται για ένα open standard, τις ιδιότητες του δηλαδή μπορεί οποιοσδήποτε να τις χρησιμοποιήσει ελεύθερα. Αυτό επέτρεψε τη γρήγορη διάδοση εφαρμογών για όλα τα υπάρχοντα λειτουργικά συστήματα και τις πλατφόρμες, εφαρμογές που συχνά διανέμονται δωρεάν ή, όπως συμβαίνει με το λειτουργικό σύστημα Unix, είναι ενσωματωμένες στο ίδιο το σύστημα.

Επιπλέον το TCP/IP είναι ανεξάρτητο από τον τρόπο με τον οποίο έχει δημιουργηθεί το δίκτυο : δηλαδή, ένα TCP/IP είναι δυνατό να στηριχτεί είτε σε ένα τοπικό δίκτυο Ethernet, ή σε μια τηλεφωνική γραμμή, είτε σε ένα καλώδιο οπτικής ίνας(ATM), ή σε ένα δίκτυο δορυφορικής μετάδοσης, κ.τ.λ. Επιτρέπει επίσης την εύκολη ενσωμάτωση διαφορετικών τεχνολογιών hardware σε μια ενιαία λογική δομή επικοινωνίας, όπως ακριβώς συνέβη με το Διαδίκτυο.

Τέλος, το TCP/IP είναι ένα πρωτόκολλο επικοινωνίας το οποίο λύνει πολύ αποτελεσματικά τα συνήθη προβλήματα κάθε πληροφοριακού συστήματος :

- Ÿ Εκμεταλλεύεται με τον καλύτερο δυνατό τρόπο τα διαθέσιμα μέσα επικοινωνίας.
- Ÿ Επιτρέπει την αποτελεσματική και ασφαλή καθοδήγηση των συνδεδεμένων ηλεκτρονικών υπολογιστών, ακόμα και αν ο αριθμός τους ανέρχεται σε πολλά εκατομμύρια.
- Ÿ Εγγυάται την ομαλή έκβαση της επικοινωνίας με τη μέγιστη ασφάλεια.
- Ÿ Επιτρέπει την ανάπτυξη εξελιγμένων και εύκολα χρησιμοποιήσιμων από τον χρήστη μέσων και υπηρεσιών δικτύου. (Silvia Vaccaro, 2007, σελ.2)

2.14.2 ΥΠΗΡΕΣΙΕΣ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ ΔΙΚΤΥΑΚΗ ΕΠΙΚΟΙΝΩΝΙΑ

Τα τελευταία χρόνια ο κόσμος εξοικειώνεται όλο και περισσότερο με το διαδίκτυο. Τα περιεχόμενα και οι μορφές του Ιστού (world wide web) εμπλουτίστηκαν, ο τρόπος πρόσβασης σε αυτόν έγινε πιο απλός και πολυμορφικός.

Τα δίκτυα παρέχουν δυνατότητες καταμερισμού πόρων, είτε μιλάμε για φυσικούς πόρους όπως εκτυπωτές, σαρωτές, μονάδες εγγραφές ,είτε για πληροφορίες που στη σημερινή παγκόσμια κοινωνία αποτελούν κρίσιμο παράγοντα επιτυχίας μίας επιχειρηματικής δραστηριότητας. Με το ευρυζωνικό δίκτυο διαδόθηκαν φαινόμενα όπως τα Blog, η online ανάγνωση εγγράφων διδακτικού περιεχομένου, το home banking και το peer-to-peer (διακίνηση εγγράφων από υπολογιστή σε υπολογιστή, ομότιμη επικοινωνία όχι client-server), το chat. Εντατικοποιήθηκε η επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου, αλλά και μέσω του instant messaging (online ανταλλαγή μηνυμάτων).

Κερδίζουν έδαφος οι μεταδόσεις δεδομένων ήχου/βίντεο και οι τηλεφωνικές επικοινωνίες βρίσκουν ένα νέο μέσο το Voice over IP το οποίο επιτρέπει την εκμετάλλευση των δυνατοτήτων του δικτύου και της ADSL για τηλεφωνικές συνδέσεις χαμηλού κόστους, πρόκειται μία σοβαρή τεχνολογία που πολλοί χρησιμοποιούν για επαγγελματικές κλήσεις.

Ο κόσμος χρησιμοποιεί όλο και πιο συχνά το e-learning, το οποίο είναι μια φόρμα διδασκαλίας στην οποία το δίκτυο χρησιμοποιείται για να έρθουν σε επαφή χρήστες που βρίσκονται μακριά από το τόπο και από τα άτομα που παραδίδουν τα μαθήματα. (Silvia Vaccaro, 2007, σελ.6)

Δυνατότητες Τηλεεργασίας που ήδη έχει αρχίσει να αναπτύσσεται, ιδιαίτερα στην Αμερική. Τα επόμενα χρόνια πρόκειται να επεκταθεί σε πολλές χώρες. Τα πλεονεκτήματα είναι πάρα πολλά και σοβαρά. Μπορεί να επιφέρει αποσυμφόρηση στο κυκλοφοριακό των μεγαλουπόλεων και κέρδος του χρόνου μεταφοράς στο χώρο εργασίας. Οι Σκανδιναβικές χώρες την χρησιμοποιούν εδώ και αρκετά χρόνια στην εκπαίδευση, λόγω συχνών αποκλεισμών περιοχών εξαιτίας των κλιματολογικών συνθηκών. (http://www.ict.plus.gr)

Ακόμη, υποστηρίζονται εφαρμογές ηλεκτρονικού εμπορίου. Εντείνεται, επίσης, η χρήση της Τηλειατρικής, η οποία προσφέρει ιατρικές υπηρεσίες εξ αποστάσεως.

Αυτή η σύντομη αναφορά στις υπηρεσίες που περιγράψαμε πιο πάνω συνθέτει μόνο μερικές από τις πολλές εφαρμογές της χρήσης του

ευρυζωνικού διαδικτύου, το οποίο στο μέλλον θα κερδίζει όλο και περισσότερο έδαφος. (Silvia Vaccaro, 2007, σελ.6)

Στο σημείο αυτό θα πρέπει να σημειωθεί ότι μέσω των ασύρματων δικτύων υποστηρίζεται η κινητικότητα των χρηστών, αφού παρέχεται δυνατότητα πρόσβασης σε πληροφορίες και εφαρμογές σε χρήστες εν κινήσει. Πιο συγκεκριμένα, τα ασύρματα δίκτυα επικοινωνούν με διαμόρφωση ραδιοκυμάτων ή με παλμούς υπέρυθρου φωτός. Τα *Ασύρματα Τοπικά Δίκτυα* (Wireless LAN) είναι μία παραδοσιακή αρχιτεκτονική LAN επεκταμένη με μία ασύρματη διεπαφή ώστε να εξυπηρετούν μικρά χαμηλής-κατανάλωσης φορητά τερματικά ικανά για ασύρματη προσπέλαση. Συνδέονται επιπλέον με πιο εκτεταμένα δίκτυα όπως LAN ή WAN. Έχουν περιορισμένη εμβέλεια και είναι σχεδιασμένα ώστε να χρησιμοποιούνται μόνο σε τοπικά περιβάλλοντα. Υπάρχουν δύο τύποι αρχιτεκτονικών ασύρματων LAN : τα απευθείας δίκτυα και τα δίκτυα διαμέσου υποδομής. Τα *Ασύρματα Δίκτυα Ευρείας-Ζώνης* είναι ειδικά κινητά ραδιοδίκτυα που παρέχουν ευρεία κάλυψη για υπηρεσίες δεδομένων μικρού εύρους μπάντας συχνοτήτων. (Γ. Πάγκαλος – Ι. Μαυρίδης, 2002, σελ.154)

Η τεχνολογία μεταβάλλεται με ραγδαίους ρυθμούς επιτρέποντας την ενσωμάτωση νέων προηγμένων εξατομικευμένων εφαρμογών και χαρακτηριστικών που ακολουθούν 6τις προτιμήσεις, τις απαιτήσεις και τους περιορισμούς των χρηστών για όσο το δυνατόν καλύτερη ποιότητα στο μικρότερο δυνατό κόστος. (Silvia Vaccaro, 2007, σελ.6)

2.14.3 ΤΑ ΔΙΚΤΥΑ ΚΑΙ Η ΔΟΜΗ ΤΟΥΣ

Ένα δίκτυο υπολογιστών είναι ένα σύστημα που αποτελείται από διάφορες συσκευές (δρομολογητές, τερματικά, γέφυρες, εκτυπωτές, αποθηκευτικά μέσα, κ.λ.π.) και υπολογιστές συνδεδεμένους μεταξύ τους ώστε να μπορούν να ανταλλάσουν πληροφορίες. Ένα δίκτυο υπολογιστών αποτελείται από :

- Αυτόνομους υπολογιστές. πρέπει να έχουν δική τους μνήμη και κεντρική μονάδα επεξεργασίας. Οι υπολογιστές που συμμετέχουν σε ένα δίκτυο διακρίνονται σε εξυπηρετητές (servers) και τερματικά ή σταθμούς εργασίας. Οι εξυπηρετητές είναι ισχυροί υπολογιστές που

μοιράζουν τις υπηρεσίες στους άλλους υπολογιστές του δικτύου. Ανάλογα με το είδος της υπηρεσίας οι εξυπηρετητές χωρίζονται σε διάφορα είδη όπως:

- *Εξυπηρετητής βάσης δεδομένων (Database Server)*. Αφορά υπολογιστή με ειδικές προδιαγραφές για τον αποθηκευτικό χώρο του, που είναι αφιερωμένος στην αποθήκευση της βάσης δεδομένων του δικτύου, και η οποία χρησιμοποιείται για την επεξεργασία των στοιχείων της.
- *Εξυπηρετητής αρχείων (File server).* Υπολογιστικό σύστημα που σκοπός του είναι να μοιράζει τα αρχεία και τις εφαρμογές στους υπόλοιπους υπολογιστές του δικτύου.
- *Εξυπηρετητής fax (Fax server).* Υπολογιστής εξοπλισμένος με μηχανήματα fax/modem που επιτρέπει στους χρήστες του δικτύου να τα χρησιμοποιούν για την αποστολή και λήψη fax μέσω των υπολογιστών τους.
- *Εξυπηρετητής ταχυδρομείου (Mail server).* Αναλαμβάνει να αποστείλει, να παραλάβει και να μοιράσει το ηλεκτρονικό ταχυδρομείο στους χρήστες του.
- *Εξυπηρετητής εκτυπωτικών εργασιών (Print server).* Χρησιμοποιείται στον έλεγχο και την διαχείριση των εκτυπωτών και των εκτυπώσεων των χρηστών του δικτύου.
- *Εξυπηρετητής intranet (Intranet server).* Ο εξυπηρετητής αυτός λειτουργεί αυτόνομα σε ένα τοπικό δίκτυο ή είναι συνδεδεμένος με το διαδίκτυο, και παρέχει στους υπολογιστές του τοπικού δικτύου που ανήκει, υπηρεσίες τύπου Internet . (π.χ ανάγνωση ιστοσελίδων, e-mail κ.λ.π).
- Τα είδη των εξυπηρετητών δικτύου είναι τόσα όσες είναι και οι δικτυακές εφαρμογές σήμερα. Όπως για παράδειγμα, ο εξυπηρετητής εφαρμογών, ο εξυπηρετητής απομακρυσμένης σύνδεσης, ο εξυπηρετητής οπτικής βιβλιοθήκης, ο εξυπηρετητής εφαρμογών του Παγκόσμιου ιστού.
- *Κυκλώματα διασύνδεσης*. Πρόκειται για μονάδες υλικού που εξασφαλίζουν την σύνδεση και την μεταφορά των πληροφοριών ανάμεσα στους υπολογιστές. Εκτελούν συνήθως εργασίες

διαμόρφωσης- αποδιαμόρφωσης και ελέγχου ορθότητας μεταφερόμενων δεδομένων. Τοποθετούνται σε κάθε υπολογιστή και τον ενώνουν με τα φυσικά μέσα μετάδοσης, τα οποία είναι τα μέσα όπου θα περάσουν τα σήματα επικοινωνίας και μπορεί να είναι καλώδια, ασύρματες διατάξεις ή και τηλεπικοινωνιακά δίκτυα.

- *Λογισμικό δικτύου.* Πρόκειται για το σύνολο των προγραμμάτων που εξασφαλίζουν τη σύνδεση, πραγματοποιούν και ελέγχουν την επικοινωνία των υπολογιστών –μελών του δικτύου. Ελέγχουν και παραχωρούν δυνατότητες πρόσβασης και δικαιώματα στους χρήστες του δικτύου. Μπορεί να είναι αυτόνομα προγράμματα του λειτουργικού συστήματος ή ακόμα και ολοκληρωμένα λειτουργικά συστήματα δικτύων.
- *Λογισμικό εφαρμογών δικτύου.* Πρόκειται για προγράμματα εφαρμογών που έχουν σχεδιαστεί ειδικά για να εκμεταλλεύονται τις δυνατότητες που προσφέρει ένα δίκτυο υπολογιστών. Μπορεί να είναι επεκτάσεις προγραμμάτων με δικτυακές δυνατότητες, που έχουν αρχικά γραφτεί για περιβάλλον αυτόνομων υπολογιστών (π.χ. ένα πρόγραμμα λογιστικής διαχείρισης για μικροϋπολογιστή). Μπορεί ακόμα η λειτουργία τους ή η φύση της ανάγκης που καλύπτουν να στηρίζεται στην ύπαρξη δικτύου υπολογιστών (π.χ. τα προγράμματα ηλεκτρονικού ταχυδρομείου). (Ι.Βογιατζής, 2006, σελ.13)

Τώρα οι κυριότερες συσκευές διαδικτύωσης - δικτύωσης που χρησιμοποιούνται σε δίκτυα υπολογιστών και εκτελούν λειτουργίες με σκοπό την αύξηση του μεγέθους και την επέκταση των δυνατοτήτων του δικτύου, είναι :

- *Modem :* Συνδυάζεται με μία διαδικτυακή συσκευή όπως ένας δρομολογητής για να επιτευχθεί ολοκληρωμένη σύνδεση των απομακρυσμένων υπολογιστών ή ολόκληρων δικτύων, μέσω του δημόσιου τηλεφωνικού δικτύου. Μετατρέπει τα ψηφιακά σήματα σε αναλογικά (διαδικασία διαμόρφωσης) και η επαναφορά του στο αρχικό ψηφιακό σήμα (αποδιαμόρφωση).
- *Επαναλήπτης (repeater) :* Πρόκειται για συσκευή η οποία δέχεται ένα σήμα σε μία θύρα της και προτού αυτό αλλοιωθεί, το

επαναλαμβάνει/αναπαράγει στις υπόλοιπες θύρες που είναι συνδεμένες στο δίκτυο. Οι επαναλήπτες είναι εγκατεστημένοι στους δορυφόρους και σε κεραίες μετάδοσης σημάτων.

- *Γέφυρα (Bridge) :* Μια γέφυρα οδηγεί τα πακέτα στην κατεύθυνση του προορισμού τους, χωρίς να τα προωθεί σε τμήματα του δικτύου στα οποία δεν βρίσκεται καθορισμένος παραλήπτης για τα πακέτα αυτά. Χωρίζει ένα δίκτυο σε μικρότερα δίκτυα /μικρότερα τμήματα, και έτσι βελτιώνεται η απόδοση του δικτύου, καθώς περιορίζεται η κίνηση στα τμήματα αυτά.
- *Δρομολογητής (Router) :* Πρόκειται για μια ακόμα πιο εξελιγμένη συσκευή. Διαθέτουν εξελιγμένο λογισμικό που μπορεί να εξετάζει το βέλτιστο μονοπάτι για την αποστολή κάποιου πακέτου, κάνοντας χρήση ενός πίνακα δρομολόγησης που προωθεί τα πακέτα στο προορισμό τους, δηλαδή στο κατάλληλο δίκτυο. Τώρα το βέλτιστο μονοπάτι είναι αυτό με το λιγότερο κόστος, πιο συγκεκριμένα ο δρομολογητής διαλέγει το καλύτερο δρόμο για τα πακέτα με βάση το κόστος, εκείνο με το λιγότερο κόστος.
- *Κεντρικός σταθμός (Hub) :* Κεντρικοί σταθμοί ή αλλιώς συγκεντρωτές καλωδίων και παρέχουν στην καλωδίωση του δικτύου ένα κεντρικό σημείο σύνδεσης. Συνδέουν ομάδες υπολογιστών επιτρέποντας στα συστήματα να επικοινωνούν μεταξύ τους.
- *Μεταγωγέας (Switch) :* Είναι μια συσκευή που συνδέει με ένα κλειστό κύκλωμα, έναν υπολογιστή με έναν άλλον για όλη τη διάρκεια της συνομιλίας τους. Η κάθε θύρα του είναι ένα απομονωμένο δίκτυο. Η συσκευή αυτή μπορεί να δημιουργήσει μία γέφυρα ανάμεσα σε δύο θύρες σε πολύ μεγάλη ταχύτητα. Έτσι πλεονέκτημα του είναι ότι διαθέτει πολλές υποδοχές, συγκριτικά με μία γέφυρα και οι οποίες του παρέχουν διασυνδέσεις με διαφορετικούς ρυθμούς, με αποτέλεσμα την αποφυγή καθυστέρησης κατά τη μεταφορά δεδομένων. (Ι.Βογιατζής, 2006, σελ.33)

2.14.4 ΤΑΞΙΝΟΜΗΣΗ ΔΙΚΤΥΩΝ

Θα επιχειρήσουμε να κατηγοριοποιήσουμε τα δίκτυα όσον αφορά τη γεωγραφική τους κάλυψη και την τοπολογία τους. Σύμφωνα με την **Γεωγραφική τους Κάλυψη** τα δίκτυα μπορούν να διακριθούν στις ακόλουθες τρείς κατηγορίες :

- ü *Δίκτυα Προσωπικής Περιοχής (Personal Area Network- PAN)*
  Αναφέρεται σε δίκτυα που προορίζονται για ένα άτομο. Ως παράδειγμα για το δίκτυο προσωπικής περιοχής μπορούμε να αναφέρουμε ένα ασύρματο δίκτυο που συνδέει έναν υπολογιστή με το ποντίκι, το πληκτρολόγιο και τον εκτυπωτή.
- ü *Τοπικά Δίκτυα (Local Area Network- LAN)*
  Τα τοπικά δίκτυα είναι δίκτυα τα οποία εκτείνονται σε ένα μόνο κτίριο ή κτιριακό συγκρότημα ή σε μία έκταση μέχρι λίγα χιλιόμετρα. Είναι κυρίως ιδιωτικής χρήσης δίκτυα. Χρησιμοποιούνται ευρέως για την διασύνδεση προσωπικών υπολογιστών και σταθμών εργασίας. Κλασικά παραδείγματα αποτελούν το Ethernet και το Token Ring.
- ü *Αστικά/Μητροπολιτικά Δίκτυα (Metropolitan Area Network- MAN)*
  Τα αστικά Δίκτυα δεν ξεπερνούν τα σύνορα μιας πόλης. Καλύπτουν τις ανάγκες επικοινωνίας μέσα στην ίδια πόλη. Κύρια χρήση τους είναι η διασύνδεση τοπικών δικτύων. Δίκτυο της μορφής αυτής θεωρείται ένα τοπικό τηλεφωνικό δίκτυο και το Fiber Distributed Data Interface (FDDI).
- ü *Δίκτυα Ευρείας Περιοχής (Wide Area Network- WAN)*
  Τα δίκτυα ευρείας περιοχής εκτείνονται σε μεγάλη γεωγραφική περιοχή, όπως μία χώρα ή μια ήπειρο. Χρησιμοποιούν διάφορες συσκευές, όπως είναι οι δορυφόροι, ακόμα και κάποια υπάρχοντα τηλεφωνικά δίκτυα. Ένα τέτοιο δίκτυο μπορεί να ενώνει άλλα μικρότερα δίκτυα ευρείας περιοχής, τοπικά δίκτυα, και αυτόνομους υπολογιστές. Παραδείγματα τέτοιων δικτύων αποτελούν τα δίκτυα των τραπεζών που εκτείνονται σε όλη την Ελλάδα και στο εξωτερικό, τα δίκτυα των αεροπορικών εταιρειών, το διαδίκτυο κ.λ.π.

Θεωρώντας ως κριτήριο κατηγοριοποίησης των δικτύων την **Τοπολογία** τους, τα δίκτυα μπορούν να διακριθούν στις ακόλουθες κατηγορίες :

- ***Ακτινωτά Δίκτυα ή Δίκτυα Τοπολογίας Αστέρα***

  Σε αυτήν την τοπολογία, υπάρχει ένας κεντρικός κόμβος (Hub) για τον έλεγχο της κυκλοφορίας, κάθε σταθμός είναι απευθείας συνδεδεμένος στον κεντρικό αυτό κόμβο, μία για μετάδοση και μία για λήψη. Πλεονεκτήματα ενός ακτινωτού δικτύου είναι η εύκολη σχεδίαση και υποστήριξη, ο μικρός χρόνος απόκρισης και η πολύ καλή αξιοπιστία του. Ως μειονεκτήματα μπορούμε να αναφέρουμε την υποχρεωτική διέλευση από το κέντρο των συνδέσεων μεταξύ των σταθμών εργασίας. Τέτοια δίκτυα αποτελούν τμήματα μεγαλύτερων δικτύων ή υποστηρίζουν μικρές και μεσαίες εφαρμογές.

- ***Δίκτυα Αρτηρίας***

  Σε ένα δίκτυο αρτηρίας όλοι οι σταθμοί συνδέονται απευθείας σε ένα γραμμικό μέσο μετάδοσης ή αρτηρία με χρήση κατάλληλων συνδετήρων. Τα δεδομένα μεταδίδονται στην αρτηρία επιτρέποντας την πλήρως αμφίδρομη λειτουργία μεταξύ των σταθμών και των συνδετήρων. Η μετάδοση από οποιοδήποτε σταθμό διαδίδεται κατά μήκος του μέσου και προς τις δύο κατευθύνσεις και μπορεί να ληφθεί από όλους τους υπόλοιπους σταθμούς. Σε κάθε άκρη της αρτηρίας υπάρχει μία τερματική αντίσταση, η οποία απορροφά το σήμα.

- ***Δίκτυα Δένδρου***

  Η τοπολογία δένδρου είναι γενίκευση της τοπολογίας αρτηρίας. Το μέσο μετάδοσης είναι ένα διακλαδούμενο καλώδιο χωρίς κλειστούς βρόχους. Ένα ή περισσότερα καλώδια ξεκινούν από την κορυφή και καθένα από αυτά μπορεί να έχει κλάδους. Οι κλάδοι μπορούν να έχουν περισσότερους κλάδους, επιτρέποντας πολύπλοκες διατάξεις.

- ***Δίκτυα Δακτυλίου (ring)***

  Στην τοπολογία δακτυλίου, το δίκτυο αποτελείται από ένα σύνολο επαναληπτών που συνδέονται με σημείο προς σημείο ζεύξεις σε ένα κλειστό βρόχο. Όλοι οι υπολογιστές είναι συνδεδεμένοι σε έναν πλήρη κλειστό δακτύλιο. Ο επαναλήπτης είναι μία συσκευή που επαναμεταδίδει τα bit που λαμβάνει από μία σύνδεση προς μία άλλη σύνδεση με την ίδια ταχύτητα που αυτά λαμβάνονται. Οι συνδέσεις

είναι μονοκατευθυντικές, δηλαδή δεδομένα μεταδίδονται σε μία κατεύθυνση μόνο.

- ***Δίκτυα Βρόχου*** *(Mesh Networks)*

  Στα Δίκτυα βρόχου, κάθε σταθμός εργασίας είναι συνδεδεμένος με άλλους δύο τουλάχιστον δρόμους, έτσι ώστε να σχηματίζονται βρόχοι. Αυτό μεταφράζεται στο γεγονός ότι υπάρχουν εναλλακτικοί δρόμοι για την επικοινωνία μεταξύ δύο σταθμών, το οποίο αποτελεί και το βασικό πλεονέκτημα των δικτύων βρόχου, ειδικά σε περιπτώσεις υπερφορτώσεων ή διακοπών των συνδέσεων. Οι κόμβοι στα δίκτυα βρόχου πρέπει να υποστηρίζουν διαδικασίες αποθήκευσης δεδομένων, δρομολόγησης καθώς και χρήσης του δικτύου. Το κόστος ενός τέτοιου δικτύου είναι μεγάλο, καθώς απαιτούνται πολλαπλές τηλεπικοινωνιακές γραμμές και έξυπνοι κόμβοι. Η απόδοση του δικτύου εξαρτάται από την αξιοπιστία των κόμβων, τις μεθόδους δρομολόγησης, τους ρυθμούς μετάδοσης, την αποθηκευτική ικανότητα των κόμβων κλπ. Τα δίκτυα βρόχου χρησιμοποιούνται για τη σύνδεση τηλεπικοινωνιακών κόμβων μεταξύ τους, σε αντίθεση με τα ακτινωτά δίκτυα που χρησιμοποιούνται για τη σύνδεση των υπολογιστών σε ένα τερματικό σταθμό.

- ***Κομβικά Δίκτυα*** *(bus)*

  Το κομβικό δίκτυο είναι σύνθεση πολλών ακτινωτών σε ένα δίκτυο κορμού, με κόμβους που αναλαμβάνουν τη δρομολόγηση των μηνυμάτων. Όλοι οι υπολογιστές συνδέονται κατά μήκος ενός κεντρικού αγωγού. Τα δίκτυα αυτά παρέχουν λύσεις σε περιπτώσεις διακοπής ή υπερφόρτωσης γραμμών του δικτύου κορμού και κάνουν αποδοτική χρήση των γραμμών. (Μαλαμάτη Δ. Λούτα, 2006, σελ.14)

2.15 FIREWALL

Το *firewall*, που μπορεί να αποδοθεί στα ελληνικά με τον όρο *πύρινο τείχος προστασίας* ή και *ηλεκτρονική πύλη ασφαλείας,* ένα είδος μοντέρνου ‘αντικλεπτικού’ που φροντίζει για την ασφάλεια του υπολογιστή. Αποτελείται από λογισμικό και υλικό εξοπλισμό και είναι ένα πρόγραμμα ή μία συσκευή hardware που φιλτράρει τις πληροφορίες που έρχονται από τη σύνδεση του

Internet μέσα στο ιδιωτικό μας δίκτυο ή στον προσωπικό μας υπολογιστή. (http://dide.flo.sch.gr)

Ως ένα σύστημα firewall μπορεί να θεωρηθεί μία διάταξη δρομολόγησής (router), ένας προσωπικός υπολογιστής, ένας διανομέας ή διακομιστής (server), ή ένα σύνολο εξοπλισμού και λογισμικού που παρέχει ασφάλεια στα δίκτυα δηλαδή ένα σύνολο από διακομιστές διαμορφώμενοι με τέτοιο τρόπο ώστε να κατοχυρώνουν μία δικτυακή τοποθεσία (site) ή ένα υποδίκτυο από πρωτόκολα και υπηρεσίες (π.χ. υπηρεσίες FTP, HTTP, e-mail κ.λ.π.) (Γ. Πάγκαλου – Ι. Μαυρίδη, 2002, σελ.248)

Παρεμβάλλεται ανάμεσα σε δύο διαφορετικά δίκτυα υπολογιστών και φιλτράρει τα διακινούμενα πακέτα πληροφοριών, θεωρείται ως ένας συνδετικός κρίκος ανάμεσα σε δύο δίκτυα υπολογιστών ή ως ένα φίλτρο δεδομένων. Στην ουσία πρόκειται για έναν ελεγκτή κυκλοφορίας δεδομένων στο Internet. Αν δεν επιτρέψει την κυκλοφορία ενός πακέτου δεδομένων, η ενέργεια αυτή χαρακτηρίζεται ως *block traffic*, ενώ αν η κυκλοφορία επιτραπεί χαρακτηρίζεται ως *permit traffic*. Το firewall κατά τη λειτουργία του (φιλτράρισμα) βασίζεται σε ένα σύνολο κανόνων (κριτήρια) που ορίζονται από τον χρήστη (διαχειριστή firewall) και με βάση αυτούς τους κανόνες επιτρέπει ή απορρίπτει την κυκλοφορία (διακίνηση) των δεδομένων ανάμεσα στα δύο δίκτυα υπολογιστών. (http://dide.flo.sch.gr)

Οι Κατηγορίες των Firewalls

Οι δύο μεγάλες κατηγορίες των firewalls είναι οι εξής :

- *Hardware Firewalls*: είναι είτε συσκευές που είναι αυτόνομες (stand alone) και συνδέονται αμέσως με το δίκτυο, είτε υπολογιστές που η μόνη τους δουλειά είναι ο ρόλος του firewall σ’ ένα δίκτυο και που έχουν εγκατεστημένα τα απαραίτητα προς τον σκοπό αυτό προγράμματα.
- *Software Firewalls:* αυτά είναι προγράμματα υπολογιστών που μπορούμε να βρούμε στο εμπόριο ή στο Internet και που μπορούμε να εγκαταστήσουμε στον υπολογιστή μας. Είναι γνωστά και με τον όρο *Personal Firewall.* (http://dide.flo.sch.gr)

2.15.1 ΤΙ ΚΑΝΕΙ ΕΝΑ FIREWALL

- Μπορεί να εμποδίσει ιούς (viruses), σκουλήκια (worms), δούρειους ίππους (trojan horses) και άλλα προγράμματα τύπου spyware από το να εγκατασταθούν στον υπολογιστή μας και να κάνουν ζημιά.
- Εμποδίζει την πρόσβαση στον υπολογιστή μας σε άγνωστους ή ανεπιθύμητους επισκέπτες.
- Ειδοποιεί τον χρήστη ότι ο υπολογιστής δέχεται κάποια επίθεση.
- Παρουσιάζει αναλυτικά στατιστικά στοιχεία σχετικά με την κίνηση από και προς τον υπολογιστή μας.
- Μπορεί να εμποδίσει κάποιο πρόγραμμα τύπου dialer από το να πραγματοποιήσει τηλεφωνικές κλήσεις χωρίς τη θέλησή μας.
- Ένα firewall μπορεί να ελέγξει την κίνηση (traffic) των πακέτων του Internet από και προς τον υπολογιστή μας.

- Μπορεί να εντοπίσει τις πιθανές επιθέσεις στον υπολογιστή μας, να αναλύσει την κίνηση και τα αρχεία που ανταλλάσσονται, να διακρίνει τις ύποπτες δραστηριότητες και να εμποδίσει την ολοκλήρωσή τους.
- Ένα firewall προστατεύει ένα δίκτυο από κάποιο άλλο δίκτυο και γενικότερα από την παράνομη πρόσβαση, υποβάλλοντας τα διερχόμενα πακέτα πληροφοριών (εισερχόμενα και εξερχόμενα) σε μια σειρά από ελέγχους, λαμβάνει την απόφαση να τα αφήσει να διέλθουν ή να τα εμποδίσει, ανάλογα με το αν περνούν κάποια τεστ ή όχι.
- Μπορεί επίσης να ελέγξει τα προγράμματα που είναι εγκατεστημένα στον ίδιο τον υπολογιστή μας και συνδέονται στο Internet και τα οποία στέλνουν προς τα έξω ευαίσθητα προσωπικά μας δεδομένα ή αφήνουν ανοικτή μια κερκόπορτα (είναι σημεία εισόδου που επιτρέπουν την πρόσβαση σε ένα σύστημα, παρακάμπτοντας την συνηθισμένη διαδικασία πρόσβασης ασφαλείας. Αποτελεί σημείο ευπάθειας, αν γίνει γνωστή από επίδοξους εισβολείς (Σωκρ.Κάτσικας-Δημ.Γκρίζαλης-Στεφ.Γκρίτζαλης, 2004, σελ.244)) για να μπορούν οι πιθανοί hackers να ελέγξουν τον υπολογιστή μας. Ένα firewall μπορεί να κρατήσει κλειστές αυτές τις πόρτες και να μας ενημερώνει για κάθε ύποπτη κίνηση.

Τα firewalls χρησιμοποιούν μια ή περισσότερες από τις εξής τρεις μεθόδους για να ελέγξουν την κυκλοφορία (traffic) που διέρχεται μέσα και έξω από το δίκτυο :

1. *Φιλτράρισμα Πακέτων (Packet Filtering)-Πύλες φιλτραρίσματος Πακέτων*. Τα πακέτα (packets), που είναι μικρά κομμάτια δεδομένων, αναλύονται (διέρχονται) μέσα από κάποια φίλτρα. Τα πακέτα που κατορθώνουν να περάσουν μέσα από τα φίλτρα στέλνονται στο σύστημα που τα ζήτησε και όλα τα άλλα πακέτα απορρίπτονται.
2. *Υπηρεσία Μεσολάβησης (Proxy Service)-Πύλες εφαρμογών*. Οι πληροφορίες από το Internet αναχαιτίζονται από το firewall και στέλνονται μετά στο σύστημα που τις ζήτησε και το αντίστροφο.
3. *Αυστηρή Επιθεώρηση (Τεχνολογία Stateful Inspection)*. Είναι μια καινούργια μέθοδος που δεν εξετάζει τα περιεχόμενα του κάθε πακέτου αλλά αντίθετα συγκρίνει συγκεκριμένα κομμάτια κλειδιά του πακέτου με μια βάση δεδομένων εμπιστευτικών πληροφοριών (που έχουν αποθηκευτεί και προέρχονται από προηγούμενα πακέτα πληροφοριών, η βάση αυτή συνεχώς ενημερώνεται (Γ. Πάγκαλου – Ι. Μαυρίδη, 2002 σελ.253)). Οι πληροφορίες που ταξιδεύουν μέσα από το firewall προς τα έξω καταγράφονται για συγκεκριμένα χαρακτηριστικά που έχουν και μετά οι εισερχόμενες πληροφορίες συγκρίνονται μ' αυτά τα χαρακτηριστικά. Αν από την σύγκριση προκύψει ένα λογικό ταίριασμα, επιτρέπεται στις πληροφορίες να διέλθουν. Αλλιώς, απορρίπτονται. (http://dide.flo.sch.gr)

   Ο συνδυασμός αυτός υπερέχει αφού συνδυάζει όλα τα πλεονεκτήματα των δύο βασικών τύπων τεχνολογιών : Πύλες Φιλτραρίσματος Πακέτων και Πύλες Εφαρμογών. (Γ. Πάγκαλου – Ι. Μαυρίδη, 2002 σελ.253)

ΓΕΝΙΕΣ FIREWALL

- **1η γενιά - Φίλτρα πακέτων**

Το πρώτο ερευνητικό δημοσίευμα πάνω στην τεχνολογία firewall προέκυψε το 1988 όταν οι μηχανικοί της DEC (Digital Equipment Corporation)

ανέπτυξαν φίλτρα πακέτων δεδομένων (data packet filters). Τα φίλτρα αυτά θεωρούνται ως η πρώτη γενιά firewall. Τα φίλτρα πακέτων δρουν ως εξής: Διαβάζουν τα πακέτα δεδομένων που διακινούνται από το ένα δίκτυο στο άλλο και, εάν κάποιο πακέτο ταιριάζει με κάποιο συγκεκριμένο κανόνα, τότε το απορρίπτουν. (Παπαθανασίου Α., 2008, σελ.96)

Ο διαχειριστής του δικτύου είναι σε θέση να ορίσει τους κανόνες βάσει των οποίων θα απορρίπτονται τα πακέτα. Αυτός ο τύπος firewall δεν ενδιαφέρεται για το εάν κάποιο πακέτο ανήκει σε μία σύνδεση, δηλαδή δεν αποθηκεύει πληροφορίες σχετικά με την κατάσταση των διαφόρων συνδέσεων από το ένα δίκτυο στο άλλο. Αντιθέτως, φιλτράρει κάθε πακέτο με βάση την πληροφορία που περιέχεται στο ίδιο το πακέτο. Επειδή τα πρωτόκολλα TCP και UDP χρησιμοποιούν τις ευρέως διαδεδομένες θύρες, ένα firewall πρώτης γενιάς μπορεί να ξεχωρίσει τα πακέτα που αφορούν διάφορες λειτουργίες, όπως για παράδειγμα το email, την μεταφορά αρχείων, την περιήγηση στο Διαδίκτυο κ.ο.κ. (Παπαθανασίου Α., 2008, σελ.304)

- **2η γενιά - Φίλτρα κατάστασης**

Η δεύτερη γενιά firewall αναπτύχθηκε από τρεις ερευνητές στα εργαστήρια της AT&T Bell: Dave Presetto, Howard Trickey και Kshitij Nigam. Τα firewall της δεύτερης γενιάς δρουν όπως τα firewall πρώτης γενιάς με κάποιες επιπρόσθετες λειτουργίες. Μία από αυτές είναι το γεγονός ότι πλέον εξετάζουν και την κατάσταση του κάθε πακέτου, δηλαδή την σύνδεση από την οποία προήλθε. Για τον λόγο αυτό και αναφέρονται ως φίλτρα κατάστασης. Τα φίλτρα αυτά κρατούν ανά πάσα στιγμή πληροφορίες για τον αριθμό και το είδος των συνδέσεων μεταξύ των δύο δικτύων και επιπλέον μπορούν να ξεχωρίσουν εάν ένα πακέτο αποτελεί την αρχή ή το τέλος μία νέας σύνδεσης ή μέρος μίας ήδη υπάρχουσας. Οι διαχειριστές τέτοιων firewalls μπορούν να ορίσουν τους κανόνες βάσει των οποίων θα επιτρέπεται η δημιουργία συνδέσεων από το εξωτερικό δίκτυο (Διαδίκτυο) προς το τοπικό/εταιρικό δίκτυο. (Παπαθανασίου Α., 2008,σελ.267)

- **3η γενιά - Επίπεδο εφαρμογών**

Η τρίτη γενιά firewall βασίζεται πλέον στο επίπεδο εφαρμογών σύμφωνα με το μοντέλο αναφοράς OSI (Open Systems Interconnection). Το κύριο χαρακτηριστικό αυτής της γενιάς firewall είναι ότι μπορεί να αντιλαμβάνεται ποια προγράμματα και πρωτόκολλα προσπαθούν να δημιουργήσουν μία νέα σύνδεση. Με τον τρόπο αυτό μπορούν να εντοπιστούν εφαρμογές που προσπαθούν να δημιουργήσουν ανεπιθύμητες συνδέσεις ή καταχρήσεις ενός πρωτοκόλλου ή μιας υπηρεσίας. (Παπαθανασίου Α., 2008 σελ.298)

Σήμερα σιγά σιγά εδραιώνονται τα firewalls **4ης γενιάς**, τα οποία διαθέτουν γραφικό περιβάλλον μέσω του οποίου μπορεί ο χρήστης να κάνει τις επιλογές του όσον αφορά την ασφάλεια του δικτύου του και να θέσει τους κανόνες βάσει τον οποίων θα απορρίπτονται κάποια πακέτα ή συνδέσεις. Τα firewalls 4ης γενιάς μπορούν πλέον να ενσωματωθούν στο λειτουργικό σύστημα και συνεργάζονται στενά με άλλα συστήματα ασφαλείας, όπως για παράδειγμα το **IPS - Intrusion Prevention System**. (Παπαθανασίου Α., 2008 σελ.247)

Μερικά firewalls επιτρέπουν μόνο την κυκλοφορία ηλεκτρονικού ταχυδρομείου, προστατεύοντας το δίκτυο από οποιεσδήποτε επιθέσεις εκτός από τις επιθέσεις ενάντια στην υπηρεσία ηλεκτρονικού ταχυδρομείου. Άλλα firewalls παρέχουν τη λιγότερο ακριβή προστασία και τις υπηρεσίες φραγμών που είναι γνωστά προβλήματα. Γενικά, οι αντιπυρικές ζώνες διαμορφώνονται για να προστατεύσουν από τα πλαστά διαλογικά logins από τον κόσμο «εξωτερικών όψεων». Αυτό περισσότερο από τίποτα, αποτρέπει τους βανδάλους από την αναγραφή στις μηχανές στο δίκτυό σας. Τα firewalls δεν μπορούν να προστατεύσουν από τις επιθέσεις που δεν περνούν από την αντιπυρική ζώνη. Πολλές εταιρίες που συνδέουν με το Διαδίκτυο ανησυχούν πολύ για τα ιδιόκτητα στοιχεία που διαρρέουν από την επιχείρηση μέσω εκείνης της διαδρομής. (Γκίνογλου Δ., Ταχυνάκη Π., Πρωτοψάλτη Ν., 2004, σελ.234)

ΣΥΓΧΡΟΝΗ ΤΕΧΝΟΛΟΓΙΑ FIREWALL-ΥΒΡΙΔΙΚΗ ΠΥΛΗ

Για μια ολοκληρωμένη προστασία απαιτείται η συνδυασμένη δράση των τεχνολογιών Επιπέδου Πακέτων και Επιπέδου Εφαρμογής. Έτσι παρατηρείται μία τάση υιοθέτησης της σύγκλισης αυτών των τεχνολογιών ως ο ιδανικός τρόπος υλοποίησης συστημάτων firewall για περιβάλλοντα μεσαίας έως και υψηλής επικινδυνότητας. Ο όρος υβριδικές ή σύνθετες πύλες χρησιμοποιείται για να περιγράψει τα σύγχρονα συστήματα firewall που συνδυάζοντας τα πλεονεκτήματα των προηγούμενων τεχνολογιών/τύπων, προχωρούν ακόμη ένα βήμα πιο πέρα. Η σύγχρονη εναλλακτική υλοποίησης είναι ο Συνδυασμός φιλτραρίσματος πακέτων με πύλες εφαρμογών. Έχει ήδη τονιστεί ότι ο σχετικά πρωτόγονος έλεγχος αποκλειστικά των IP-επικεφαλίδων, είναι μια λειτουργία που κάθε firewall χρειάζεται, γιατί σε αρκετές περιπτώσεις αυτός είναι ο πιο κατάλληλος και πιο γρήγορος τρόπος ελέγχου. Τα καθαρά proxy firewalls διαθέτουν λογισμικό που προσομοιώνει ένα δρομολογητή φιλτραρίσματος. Επειδή όμως η ασφάλεια ενός συστήματος αυξάνει κατά πολύ όταν δεν είναι συγκεντρωμένη η άμυνα του σε ένα μοναδικό σημείο, πολλές φορές ένα proxy σύστημα firewall συνδυάζεται με μία επιπλέον διάταξη φίλτρου πακέτων. Το υβριδικό αυτό σύστημα αποκτά παράλληλα ακόμη πιο γρήγορο και πιο αξιόπιστο φιλτράρισμα πακέτων, αφού είναι επιπέδου hardware. Ακόμη, σ' αυτή την κατηγορία μπορεί να ενταχθεί και η προαναφερόμενη τεχνολογία Stateful Inspection (Γ. Πάγκαλου – Ι. Μαυρίδη, 2002, σελ. 253)

Τι δεν Μπορεί να Κάνει Ένα Firewall

- Να διαγράψει ιούς (viruses), δούρειους ίππους (trojan horses) και άλλα προγράμματα τύπου spyware. Για τέτοιες επιθέσεις χρειάζονται επιπλέον μέτρα προστασίας.
- Να εμποδίσει την μη ζητηθείσα εμπορική ηλεκτρονική αλληλογραφία, γνωστή και με τον όρο spam e-mail.
- Να μας προστατεύσει από επιβλαβή προγράμματα τα οποία είτε δεν μπόρεσε να εντοπίσει ή εμείς οι ίδιοι επιτρέψαμε την εγκατάστασή τους, όπως είναι συνήθως τα προγράμματα συνομιλίας (chat) ή ανταλλαγής αρχείων (peer-to-peer). Να μας προστατεύσει από τις

εσωτερικές απειλές, δηλ. από τους κακόβουλους χρήστες που έχουν φυσική πρόσβαση στο εσωτερικό του τοπικού δικτύου μας (π.χ. από τους υπαλλήλους του οργανισμού). (http://dide.flo.sch.gr)

Εφόσον ένα εσωτερικό μηχάνημα μπορεί να επικοινωνήσει με ένα άλλο χωρίς να περάσει μέσα από το firewall,οποιαδήποτε ζημιά μπορεί να προκληθεί χωρίς να γίνει αντιληπτό από αυτό. Απαιτούνται επιπλέον μηχανισμοί πιστοποίησης και ελέγχου προσπέλασης για τους χρήστες, τα intranet firewalls ελαχιστοποιούν ανάλογους κινδύνους (Γ. Πάγκαλου – Ι. Μαυρίδη, 2002, σελ.260).

2.15.2 ΡΥΘΜΙΖΟΝΤΑΣ ΕΝΑ FIREWALL

Τα firewalls μπορούν να προσαρμοστούν. Δηλαδή να προσθέσουμε ή να αφαιρέσουμε φίλτρα με βάση κάποιες συνθήκες, από τις οποίες είναι οι εξής :

- *IP Διευθύνσεις (IP Addresses)*. Το κάθε μηχάνημα που συνδέεται στο Internet αποκτά μια μοναδική διεύθυνση που είναι γνωστή ως IP διεύθυνση (IP address). Οι IP διευθύνσεις είναι αριθμοί που αποτελούνται από 32 bits και μπορούν να παρουσιασθούν ως τέσσερις δεκαδικοί αριθμοί χωρισμένοι με τελείες. Μια τυπική IP διεύθυνση είναι σαν την εξής : 212.24.52.118. Για παράδειγμα, αν μια συγκεκριμένη IP διεύθυνση που βρίσκεται εκτός της εταιρείας διαβάζει υπερβολικά μεγάλο αριθμό αρχείων από έναν server, το firewall θα μπορεί να εμποδίσει όλη την κυκλοφορία προς ή από αυτήν την IP διεύθυνση.
- *Ονόματα Χώρου (Domain Names)*. Επειδή είναι δύσκολο να θυμάται κανείς όλη τη σειρά των αριθμών που συγκροτούν μια IP διεύθυνση και επειδή οι IP διευθύνσεις ενδέχεται να αλλάζουν μερικές φορές, όλοι οι servers που υπάρχουν στο Internet διαθέτουν και ονόματα που είναι κατανοητά από τους ανθρώπους, τα οποία είναι γνωστά με τον όρο ονόματα χώρου (domain names). Για παράδειγμα, είναι πολύ ευκολότερο για όλους μας να θυμόμαστε το www.mycompany.com παρά το 212.24.52.118. Μια εταιρεία έχει τη δυνατότητα να μπλοκάρει

την πρόσβαση σε συγκεκριμένα domain names ή να επιτρέψει την πρόσβαση μόνο σε συγκεκριμένα domain names.

- *Θύρες (Ports)*. Όλα τα μηχανήματα server κάνουν τις υπηρεσίες τους να είναι διαθέσιμες στο Internet χρησιμοποιώντας αριθμημένες θύρες (ports), από μία για κάθε υπηρεσία που υπάρχει διαθέσιμη στον server. Για παράδειγμα, αν ένα μηχάνημα server τρέχει έναν Web (HTTP) server και έναν FTP server, ο Web server θα είναι διαθέσιμος στη θύρα (port) 80 και ο FTP server θα είναι διαθέσιμος στη θύρα (port) 21. Μια εταιρεία μπορεί να μπλοκάρει την πρόσβαση στη θύρα 21 σ' όλα τα μηχανήματα εκτός από ένα μέσα στην εταιρεία.
- *Συγκεκριμένες Λέξεις και Φράσεις*. Μπορεί να είναι ο,τιδήποτε. Το firewall θα ψάξει παντού (λειτουργία sniff) σε κάθε πακέτο δεδομένων για να βρει ένα ακριβές ταίριασμα του κειμένου που υπάρχει στο φίλτρο. Για παράδειγμα, μπορούμε να καθοδηγήσουμε το firewall ώστε να μπλοκάρει όλα τα πακέτα που περιέχουν τη λέξη "go on". Το σημαντικό είναι ότι οι λέξεις θα πρέπει να ταιριάζουν ακριβώς, δηλ. το φίλτρο δεν θα εντοπίσει τη λέξη "goon", που δε περιέχει τον κενό χαρακτήρα. Μπορούμε, όμως, να συμπεριλάβουμε όσες λέξεις, φράσεις και παραλλαγές αυτών θέλουμε.
- *Πρωτόκολλα (Protocols)*. Το πρωτόκολλο είναι ο προκαθορισμένος τρόπος που κάποιος που επιθυμεί να χρησιμοποιήσει μια υπηρεσία, επικοινωνεί μαζί της. Ο «κάποιος» μπορεί να είναι ένα άτομο, αλλά πιο συχνά είναι ένα πρόγραμμα υπολογιστή, όπως είναι ένας φυλλομετρητής (Web browser). Τα πρωτόκολλα αποτελούνται συνήθως από κείμενο και απλά περιγράφουν το πώς ο πελάτης (client) και ο διακομιστής (server) θα κάνουν τη συνομιλία τους. Το http είναι το πρωτόκολλο του Web.

Μερικά κοινά πρωτόκολλα για τα οποία μπορούμε να ορίσουμε φίλτρα firewall είναι τα εξής :

§ *IP (Internet Protocol)*, αποτελεί το κύριο σύστημα διανομής για τις πληροφορίες που διακινούνται στο Internet.

- *TCP (Transmission Control Protocol)*, χρησιμοποιείται για τη διάσπαση και την επανένωση των πληροφοριών (πακέτων) που ταξιδεύουν στο Internet.
- *HTTP (Hyper Text Transfer Protocol)*, χρησιμοποιείται στις ιστοσελίδες (Web pages).
- *FTP (File Transfer Protocol)*, χρησιμοποιείται για το κατέβασμα (download) και το ανέβασμα (upload) αρχείων.
- *UDP (User Datagram Protocol)*, χρησιμοποιείται για τις πληροφορίες που δεν απαιτούν απόκριση (response), όπως είναι ο ήχος και το βίντεο ροής (streaming audio και video).
- *ICMP (Internet Control Message Protocol)*, χρησιμοποιείται από έναν δρομολογητή (router) για την ανταλλαγή πληροφοριών μ' άλλους δρομολογητές.
- *SMTP (Simple Mail Transport Protocol)*, χρησιμοποιείται στην αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail).
- *SNMP (Simple Network Management Protocol)*, χρησιμοποιείται για τη συλλογή πληροφοριών συστήματος από έναν απομακρυσμένο υπολογιστή (remote computer).
- *Telnet*, χρησιμοποιείται για να εκτελούμε εντολές σ' έναν απομακρυσμένο υπολογιστή (remote computer).

Η εταιρεία μπορεί να ορίσει μόνο ένα ή δύο μηχανήματα για να χειρισθούν ένα συγκεκριμένο πρωτόκολλο και να καταργήσει αυτό το πρωτόκολλο σ' όλα τα άλλα μηχανήματα.

Ένα software firewall μπορεί να εγκατασταθεί στον υπολογιστή του σπιτιού μας, όπου υπάρχει σύνδεση με το Internet. Αυτός ο υπολογιστής θεωρείται ότι είναι μια πύλη (gateway) επειδή παρέχει το μοναδικό σημείο πρόσβασης ανάμεσα στο δίκτυο του σπιτιού μας και το Internet.

Μ' ένα hardware firewall, η μονάδα του firewall αποτελεί κανονικά την πύλη (gateway) και ένα καλό παράδειγμα είναι ένας δρομολογητής (router) που διαθέτει μια ενσωματωμένη κάρτα Ethernet και ένα hub. Οι υπολογιστές στο δίκτυο του σπιτιού μας συνδέονται στον δρομολογητή (router), ο οποίος με τη σειρά του συνδέεται σ' ένα καλωδιακό modem ή σ' ένα DSL modem.

Μπορούμε να ρυθμίσουμε (configure) τον router μέσω ενός Web interface από τον φυλλομετρητή του υπολογιστή μας και εκεί μπορούμε να ορίσουμε τα φίλτρα ή και άλλες ρυθμίσεις. (http://dide.flo.sch.gr)

2.15.3 ΑΠΟ ΤΙ ΜΠΟΡΕΙ ΝΑ ΜΑΣ ΠΡΟΣΤΑΤΕΥΣΕΙ ΕΝΑ FIREWALL

Υπάρχουν πολλοί τρόποι που μπορεί να χρησιμοποιήσει κάποιος ασυνείδητος για να κάνει ζημιά σε μη προστατευμένους υπολογιστές, όπως :

- *Απομακρυσμένη Πρόσβαση (Remote Login)*. Συμβαίνει όταν κάποιος έχει τη δυνατότητα να συνδεθεί στον υπολογιστή μας και να τον ελέγξει κατά κάποιον τρόπο. Αυτό μπορεί να κυμαίνεται από το να μπορεί να δει απλά ή να έχει πρόσβαση σε αρχεία έως το να μπορεί να τρέχει προγράμματα στον υπολογιστή μας.
- *Κερκόπορτες Εφαρμογής (Application Backdoors)*. Μερικά προγράμματα έχουν ιδιαίτερα χαρακτηριστικά που επιτρέπουν την απομακρυσμένη πρόσβαση (remote access), ενώ άλλα περιέχουν σφάλματα (bugs) τα οποία δίνουν τη δυνατότητα για την ύπαρξη κερκόπορτας ή πίσω πόρτας (backdoor), δηλ. μιας κρυφής πρόσβασης, με την οποία μπορεί να έχει κάποιος κάποιο επίπεδο ελέγχου του προγράμματος.
- *SMTP Session Hijacking*. Το SMTP αποτελεί την πιο κοινή μέθοδο αποστολής ηλεκτρονικού ταχυδρομείου (e-mail) στο Internet και αποκτώντας πρόσβαση σε μια λίστα από διευθύνσεις e-mail, κάποιος μπορεί να στείλει αυτόκλητα e-mail (spam) σε χιλιάδες χρήστες.
- *Σφάλματα στο Λειτουργικό Σύστημα*. Όπως και οι εφαρμογές, μερικά λειτουργικά συστήματα έχουν backdoors, ενώ άλλα παρέχουν απομακρυσμένη πρόσβαση με ανεπαρκείς ελέγχους ασφαλείας ή έχουν ελαττώματα (bugs) που μπορεί να εκμεταλλευθεί ένας έμπειρος hacker.
- *Άρνηση Υπηρεσίας (Denial of Service)*. Αυτό το είδος επίθεσης είναι σχεδόν αδύνατο να αντιμετωπισθεί. Αυτό που συμβαίνει είναι ότι ο hacker στέλνει μια αίτηση (request) στον server για να συνδεθεί σ' αυτόν. Όταν ο server απαντήσει με μια αναγνώριση (acknowledgement) και προσπαθήσει να κάνει μια σύνοδο (session),

δεν θα μπορεί να βρει το σύστημα που έκανε την αίτηση (request). Κατακλύζοντας έναν server με τέτοιες αναπάντητες αιτήσεις session, ένας hacker αναγκάζει τον server να δουλεύει πολύ αργά (σέρνεται) έως ότου καταρρεύσει.

- *Βόμβες e-mail (e-mail Bombs)*. Μια βόμβα e-mail είναι συνήθως μια προσωπική επίθεση όπου κάποιος μάς στέλνει το ίδιο e-mail εκατοντάδες ή και χιλιάδες φορές μέχρις ότου το σύστημά μας να μην μπορεί να δεχθεί άλλα μηνύματα.
- *Μακροεντολές (Macros)*. Για να απλοποιήσουν περίπλοκες διαδικασίες ή εργασίες, πολλές εφαρμογές (applications) μάς δίνουν τη δυνατότητα να δημιουργήσουμε ένα μικρό πρόγραμμα (σενάριο εντολών, script) από εντολές που η εφαρμογή μπορεί να εκτελέσει. Αυτό το script είναι γνωστό ως μακροεντολή (macro). Οι hackers μπορούν να εκμεταλλευθούν αυτή τη δυνατότητα και να δημιουργήσουν τα δικά τους macros, τα οποία, ανάλογα με την εφαρμογή, μπορούν να καταστρέψουν τα δεδομένα ή και να προκαλέσουν την κατάρρευση του υπολογιστή μας.
- ***Ιοί** (Viruses)*. Πιθανώς η πιο γνωστή απειλή είναι οι ιοί των υπολογιστών (computer viruses). Ένας ιός (virus) είναι ένα μικρό πρόγραμμα που μπορεί να αντιγράψει τον εαυτό του σ' άλλους υπολογιστές. Μ' αυτόν τον τρόπο μπορεί να διαδοθεί ταχύτατα από το ένα σύστημα στο άλλο. Το αποτέλεσμα ενός ιού μπορεί να κυμαίνεται από την εμφάνιση ενός αβλαβούς μηνύματος έως και τη διαγραφή όλων των αρχείων του υπολογιστή μας.
- *Spam e-mail*. Μπορεί να μην κάνει ζημιά αλλά είναι πάντα ενοχλητική, η μη ζητηθείσα ή αυτόκλητη εμπορική αλληλογραφία (spam e-mail), που αποτελεί το ηλεκτρονικό ισοδύναμο της άχρηστης διαφημιστικής αλληλογραφίας (junk mail). Το spam e-mail μπορεί να είναι και επικίνδυνο καθώς αρκετά συχνά περιέχει συνδέσμους (links) σε Web sites, τα οποία ενδέχεται να στέλνουν cookies (Είναι απλά, μικρά αρχεία κειμένου, τα οποία ορισμένες τοποθεσίες στο Internet αποθηκεύουν στον υπολογιστή μας, συγκεκριμένα στο σκληρό δίσκο. Έτσι κάθε φορά που επισκεπτόμαστε κάποια ηλεκτρονική διεύθυνση, οι προσωπικές μας πληροφορίες θα ανακτούνται αυτόματα, μέσω των

cookies (Ι. Βογιατζής, 2006, σελ.65).) για να ανοίξουν έτσι μια κερκόπορτα (backdoor) στον υπολογιστή μας.

- *Βόμβες Ανακατεύθυνσης (Redirect Bombs)*. Οι hackers μπορούν να χρησιμοποιήσουν το πρωτόκολλο ICMP για να αλλάξουν (ανακατευθύνουν) τη διαδρομή που ακολουθούν οι πληροφορίες, στέλνοντάς τες σ' έναν διαφορετικό δρομολογητή (router). Αυτός είναι κι ένας από τους τρόπους που γίνεται μια επίθεση άρνησης υπηρεσίας (denial of service attack).
- *Source routing*. Στις περισσότερες περιπτώσεις, η διαδρομή που ακολουθεί ένα πακέτο στο Internet (ή σ' ένα άλλο δίκτυο) καθορίζεται από τους δρομολογητές (routers) που υπάρχουν κατά μήκος της διαδρομής. Αλλά η πηγή (source), δηλ. ο αρχικός υπολογιστής, που παρέχει το πακέτο μπορεί αυθαίρετα να καθορίσει τη διαδρομή (route) που θα πρέπει να ακολουθήσει το πακέτο. Οι hackers το εκμεταλλεύονται αυτό μερικές φορές για να κάνουν τις πληροφορίες να φαίνονται ότι προέρχονται από μια έγκυρη πηγή ή ακόμη και μέσα από το ίδιο το δίκτυο. Τα περισσότερα firewalls μπορούν και εξουδετερώνουν το source routing.

Πρέπει να έ/χουμε υπόψη μας ότι κάθε σύνδεση στο Internet παραμένει επισφαλής ακόμα και αν είναι εγκατεστημένο κάποιο firewall. Οι επίδοξοι hackers μπορούν να βρουν εργαλεία και τεχνικές ώστε να δημιουργήσουν μια σύνδεση με το εσωτερικό δίκτυο της εταιρείας και να παρακάμψουν έτσι, στην ουσία να ξεγελάσουν, το firewall. Για τον εντοπισμό και την αντιμετώπιση αυτών των διαρροών βοηθούν τα ***συστήματα διάγνωσης εισβολής***, γνωστά και ως ***IDS (Intrusion Detection Systems)***. (http://dide.flo.sch.gr)

Με τον όρο Συστήματα –Διάγνωσης/Ανίχνευσης Εισβολών αναφερόμαστε στο λογισμικό και υλικό για την παρακολούθηση και ανάλυση των συμβάντων που λαμβάνουν χώρα σε υπολογιστές ή δίκτυα, με απώτερο σκοπό να εντοπιστούν ενδείξεις προσπαθειών εισβολής. Οι απόπειρες εισβολής περιλαμβάνουν ίχνη από απόπειρες για παραβίαση της ακεραιότητας, εμπιστευτικότητας, ή διαθεσιμότητας των πληροφοριακών πόρων. Τέτοιου είδους εισβολές προέρχονται από : εξωτερικούς προς το

εσωτερικό δίκτυο χρήστες, από εσωτερικούς χρήστες που έχουν περιορισμένα δικαιώματα πρόσβασης αλλά επιχειρούν ενέργειες που απαγορεύονται από την πολιτική ασφαλείας, από εσωτερικούς χρήστες οι οποίοι έχουν κατάλληλα δικαιώματα πρόσβασης για τις πράξεις στις οποίες προβαίνουν, αλλά ασκούν τα δικαιώματα αυτά με καταχρηστικό τρόπο (Μαλαμάτη Δ. Λούτα, 2007, σελ.47).

2.15.4 Οι PROXY SERVERS ΚΑΙ Η DMZ

Μια λειτουργία που συνδυάζεται συχνά μ' ένα firewall είναι ο proxy server (διακομιστής μεσολάβησης). Ο *proxy server* χρησιμοποιείται για να υπάρχει πρόσβαση στις ιστοσελίδες από τους άλλους υπολογιστές. Όταν κάποιος άλλος υπολογιστής ζητάει μια ιστοσελίδα, αυτή ανακτάται (retrieved) από τον proxy server και μετά στέλνεται στον υπολογιστή που την ζήτησε. Το αποτέλεσμα αυτής της ενέργειας είναι ότι ο απομακρυσμένος υπολογιστής που περιέχει την ιστοσελίδα δεν έρχεται ποτέ σε άμεση επαφή με τους υπολογιστές του δικτύου μας, παρά μόνο με τον proxy server.

Οι proxy servers μπορούν επίσης να κάνουν την πρόσβασή μας στο Internet να εργάζεται πιο αποδοτικά. Αν κατεβάσουμε μια ιστοσελίδα από ένα Web site, αυτή αποθηκεύεται στον proxy server. Αυτό σημαίνει ότι την επόμενη φορά που θα επανέλθουμε σ' αυτήν την ιστοσελίδα, δεν θα χρειασθεί να φορτωθεί εκ νέου από το Web site, αλλά θα φορτωθεί αμέσως από τον proxy server. Υπάρχουν περιπτώσεις που μπορεί να θέλουνε κάποιοι απομακρυσμένοι χρήστες να έχουν πρόσβαση σε στοιχεία του δικτύου μας, όπως για παράδειγμα :

- Web site
- Online συναλλαγές
- Περιοχή FTP για download και upload

Στις περιπτώσεις αυτές, μπορούμε να δημιουργήσουμε μια *DMZ (Demilitarized Zone, Αποστρατιωτικοποιημένη Ζώνη)*. Αν και ακούγεται πολύ

σοβαρό, πρόκειται στην πραγματικότητα για μια περιοχή που βρίσκεται εκτός του firewall. Η εγκατάσταση μιας DMZ είναι πολύ εύκολη. Αν έχουμε πολλούς υπολογιστές, μπορούμε να επιλέξουμε να τοποθετήσουμε έναν υπολογιστή ανάμεσα στη σύνδεση με το Internet και το firewall. Τα περισσότερα από τα software firewalls μάς δίνουν τη δυνατότητα να καθορίσουμε έναν κατάλογο (directory) στον υπολογιστή αυτόν ως DMZ.

[Μπορούμε να φανταστούμε την DMZ σαν την μπροστινή αυλή του σπιτιού μας. Ανήκει σε μας και μπορούμε να τοποθετήσουμε κάποια πράγματα εκεί, αλλά θα τοποθετήσουμε τα πολύτιμα πράγματα μέσα στο σπίτι μας όπου και θα είναι περισσότερο ασφαλή.] (http://dide.flo.sch.gr)

2.15.5 ΕΤΟΙΜΑ ΠΡΟΓΡΑΜΜΑΤΑ FIREWALL

Το ενσωματωμένο firewall των Windows XP ενώ προσφέρει ικανοποιητική προστασία και έλεγχο για την κίνηση που γίνεται από έξω προς τα μέσα (inbound traffic), αγνοεί την προστασία και τον έλεγχο για την κίνηση που γίνεται από μέσα προς τα έξω (outbound traffic). Αν αυτό δεν μας είναι αρκετό, προγράμματα τύπου firewall προσφέρονται και από γνωστές εταιρείες που εξειδικεύονται στην ασφάλεια των υπολογιστικών συστημάτων, όπως είναι τα εξής :

- *Norton Personal Firewall* της εταιρείας Symantec,
- *Personal Firewall Plus* της εταιρείας McAfee,
- *Panda Platinum* της εταιρείας Panda,
- *Norman Personal Firewall* της εταιρείας Norman,
- *Sygate Personal Firewall* της εταιρείας Sygate,
- *eSafe Desktop Firewall*,
- *Tiny Personal Firewall* της εταιρείας Tiny,
- *F-Secure Firewall* της εταιρείας F-Secure,
- *Lockdown Millennium* της εταιρείας Lockdown και
- *Bit Defender* της εταιρείας AVX.

Το *Kerio Personal Firewall* της εταιρείας Kerio αποτελεί ένα από τα ασφαλέστερα προγράμματα της κατηγορίας του και μπορεί να κάνει και έλεγχο για ιούς τύπου dialer. Όμως, το πιο δημοφιλές πρόγραμμα firewall είναι το *Zone Alarm* της εταιρείας Zone Labs, καθώς καταφέρνει και συνδυάζει αρμονικά την ασφάλεια με την ευκολία χρήσης. Αυτό που κάνει στην ουσία το πρόγραμμα Zone Alarm είναι να επιτρέπει ή όχι την πρόσβαση σε προγράμματα που κάνουν χρήση του Internet.

Ο καλύτερος τρόπος για να δοκιμάσουμε κατά πόσο λειτουργεί σωστά και αποδοτικά ένα firewall, είναι να επισκεφθούμε ένα από τα sites του Internet που αναλαμβάνουν να κάνουν εικονικές εισβολές στον υπολογιστή μας και να μας δείξουν τις τυχόν αδυναμίες του, όπως είναι τα http://grc.com και http://www.pcinternetpatrol.com (http://dide.flo.sch.gr)

2.15.6 ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΜΕ ΤΗ ΧΡΗΣΗ FIREWALL

Η πολιτική ασφαλείας του δικτύου μιας εταιρείας, η οποία χρησιμοποιεί firewall, θα πρέπει σε γενικές γραμμές να έχει υπόψη της τα εξής :

- Θα πρέπει να περνάνε μέσα από το firewall όλες οι συνδέσεις που γίνονται από το δίκτυο της εταιρείας προς το Internet. (http://dide.flo.sch.gr)
- Θα πρέπει να ορισθεί ένας τεχνικός υπεύθυνος για την εγκατάσταση, τη ρύθμιση και τη διαχείριση του firewall, ο οποίος θα πρέπει να ακολουθεί και τακτική εκπαίδευση και ενημέρωση. Οφείλει να έχει πολύ καλή εμπειρία στη σχεδίαση και υλοποίηση firewalls, για τη σωστή χρήση και εγκατάσταση του. (Γ.Πάγκαλου– Ι.Μαυρίδη, 2002, σελ.257)
- Να δημιουργούνται σε καθημερινή, εβδομαδιαία και μηνιαία βάση ασφαλή (εφεδρικά) αντίγραφα (backups) του λογισμικού και των δεδομένων του συστήματος firewall, δηλαδή του λογισμικού συστήματος, των αρχείων ρυθμίσεων, των αρχείων της βάσης δεδομένων, των αρχείων καταγραφής, κ.α., ώστε έτσι σε περίπτωση αποτυχίας του συστήματος (system failure) να υπάρχει η δυνατότητα αποκατάστασης της λειτουργίας του χωρίς σημαντικές απώλειες. Τα εφεδρικά να φυλάσσονται σε αξιόπιστα μέσα, για να αποφευχθεί η

ακούσια καταστροφή/διαγραφή τους. Μόνο το κατάλληλο προσωπικό να έχει φυσική πρόσβαση σε αυτά. (Γ. Πάγκαλου – Ι. Μαυρίδη, 2002, σελ.257)

- Τουλάχιστον ένα ακόμη firewall, έτοιμο προς χρήση και με τις σωστές ρυθμίσεις να κρατείτε εκτός λειτουργίας ως εφεδρεία. (Γ. Πάγκαλου – Ι. Μαυρίδη, 2002, σελ.257)
- Το εγκατεστημένο firewall θα πρέπει να παρακολουθείται και να ελέγχεται σε τακτά χρονικά διαστήματα.
- Θα πρέπει να απενεργοποιηθούν όλες οι εφαρμογές που δεν είναι απαραίτητες.
- Το firewall θα πρέπει να είναι διαθέσιμο 24 ώρες το 24ωρο. (http://dide.flo.sch.gr)

ΚΕΦΑΛΑΙΟ 3ο

3.1 ΣΚΟΠΟΣ ΤΗΣ ΕΡΕΥΝΑΣ

Το πρακτικό αυτό μέρος, αναφέρεται στο σκοπό των ερωτήσεων και των συνεντεύξεων, του ερωτηματολογίου που ακολουθεί, και οι οποίες προέρχονται από τον υπεύθυνο ασφαλείας των πληροφοριακών συστημάτων της κάθε επιχείρησης. Επιπρόσθετα, το ερευνητικό αυτό μέρος δημιουργείται με το σκοπό οι υπόλοιποι φοιτητές να :

- εμπεδώσουν και να εμβαθύνουν τις θεωρητικές γνώσεις που έχουν αποκτήσει
- να γνωρίσουνε και από την πρακτική πλευρά το κομμάτι της ασφάλειας
- να κατανοήσουν το μέγεθος και την έκταση των προβλημάτων που αντιμετωπίζει η ασφάλεια πληροφοριακών συστημάτων
- να γνωρίσουν/διδαχθούν σύγχρονες τεχνικές ασφαλείας

Ο σκοπός της παρούσας εργασίας είναι να διερευνηθεί το επίπεδο ασφαλείας των μικρομεσαίων επιχειρήσεων. Με άλλα λόγια, πόσο σημαντικό είναι για μια Μικρομεσαία Επιχείρηση το θέμα της ασφάλειας, τα αντιβιοτικά (antivirus), οι δυνατοί κωδικοί των χρηστών, το τείχος προστασίας για τους hackers/ crackers, τα αντίγραφα ασφαλείας (back up), κλπ.

Πιο συγκεκριμένα, οι ΜΜΕ δεν λαμβάνουν σοβαρά υπόψη τους την ασφάλεια του υπολογιστικού τους συστήματος και έτσι δέχονται τις συνέπειες των κινδύνων που τους εμφανίζονται, ανήμπορες να αντιδράσουν κατάλληλα στις ζημιές που θα προκληθούν όπως **:**

Αθέμιτη προσπέλαση υπολογιστικών πόρων/παράνομη πρόσβαση (hacking),

Δημοσιευμένα έγγραφα-δεδομένα τους και καταστροφή χρήσιμων αρχείων,

Αποκάλυψη συνθηματικών,

Αλλοίωση/τροποποίηση δεδομένων,

Υποκλοπή λογαριασμών,

Δυσλειτουργία-κατάρρευση ολόκληρου του υπολογιστικού συστήματος,

Μόλυνση συστημάτων (worms) και εκτέλεση κακόβουλου κώδικα (ιοί) και πληθώρα ενοχλητικά μηνύματα Spam (και συχνά ακατανόητα) e-mail που δεν

έχουν ζητηθεί και που επιβαρύνουν τις θυρίδες ηλεκτρονικού ταχυδρομείου, υπερφορτώνουν τα δίκτυα, μας καθυστερούν και μας χαλούν την διάθεση.

Έτσι λοιπόν για την αντιμετώπιση αυτών των απωλειών/ζημιών, είναι απαραίτητο να παρθούν για κάθε επιχείρηση προστατευτικά μέτρα όπως :

Η *Κρυπτογράφηση*, που καταστεί αδύνατη την ανάγνωση των αρχείων και email από κάποιον μη εξουσιοδοτημένο,

Αντίγραφα ασφαλείας (Back up), για την προστασία των πιο σημαντικών δεδομένων-πληροφοριών της επιχείρησης,

Ψηφιακά Πιστοποιητικά που προβάλλονται από οργανισμούς, για την πιστοποίηση της ταυτότητας των χρηστών κατά την αποστολή προσωπικών πληροφοριών/στοιχείων διαμέσου του internet, σε συγκεκριμένες αυθεντικές διαδικτυακές τοποθεσίες.

Δυνατοί κωδικοί πρόσβασης είναι σημαντικοί για την προστασία των χρηστών, ώστε να γίνονται πιο ασφαλείς online συναλλαγές, για εξουσιοδοτημένη εκτέλεση εφαρμογών, καθώς και να πραγματοποιείται η τακτική αλλαγή τους. Ένας ιδανικός κωδικός πρόσβασης πρέπει να έχει αρκετούς χαρακτήρες, ενώ πρέπει να περιλαμβάνει γράμματα, σύμβολα και αριθμούς,

Αντιβιοτικά λογισμικά για τον εντοπισμό κακόβουλου λογισμικού (ιοί, σκουλήκια, δούρειοι ίπποι κλπ) και την απομάκρυνση του.

Firewalls, ένα είδος μοντέρνου 'αντικλεπτικού' που φροντίζει για την ασφάλεια του υπολογιστή, προκειμένου να εμποδιστεί η εισχώρηση κακόβουλου λογισμικού και η μη εξουσιοδοτημένη πρόσβαση σε εσωτερικό δίκτυο,

Και γενικότερα ο κάθε οργανισμός πρέπει να έχει επίγνωση σε θέματα ασφαλείας του δικτύου του και των υπολογιστικών του συστημάτων, να τηρεί την πολιτική ασφαλείας του, να φροντίζει να ενημερώνεται και να εφαρμόζει νέες προηγμένες πολιτικές ασφαλείας όπως τα *συστήματα διάγνωσης εισβολής (IDS)* για παρακολούθηση και ανάλυση κάθε απόπειρα εισβολής, με σκοπό παραβιάσεις, της ακεραιότητας, εμπιστευτικότητας, ή διαθεσιμότητας των πληροφοριακών πόρων.

Παρακάτω ακολουθεί ερωτηματολόγιο, το οποίο έχει δοθεί σε μικρομεσαίες επιχειρήσεις στο σύνολο τους 36 στη περιοχή της Χαλκίδας, σύμφωνα με το οποίο θα φανεί το επίπεδο ασφαλείας των πληροφοριακών συστημάτων και δικτύων τους.

3.2 ΠΑΡΟΥΣΙΑΣΗ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ

1. **Τι είδους επιχείρηση είναι;**
    a. **Τεχνικά γραφεία**
    b. **Μεταφορικά και Λογιστικά γραφεία**
    c. **Δικηγορικά και Ασφαλιστικά γραφεία**
    d. **Άλλο……..**
2. **Ποια/ες υπηρεσίες χρησιμοποιείται σε καθημερινή βάση; (μπορείτε να επιλέξετε παραπάνω από μία απαντήσεις)**
    a. **Internet**
    b. **Email**
    c. **Συναλλαγές**
    d. **MS Office**
    e. **Άλλο……....**
3. **Στους Η/Υ της επιχείρησής σας χρησιμοποιείται αντιβιοτικά (antivirus) ;**
    a. **ΝΑΙ**
    b. **ΟΧΙ**
4. **Ποιούς τρόπους προστασίας χρησιμοποιείται για την αντιμετώπιση κακόβουλων ενεργειών;**
   (μπορείτε να επιλέξετε παραπάνω από μία απαντήσεις)
    a. **Κρυπτογράφηση (σε e-mail)**
    b. **Αντίγραφα Ασφαλείας (buck up)**
    c. **Αναχώματα ασφαλείας (Firewalls)**
    d. **Πιστοποιητικά Ασφαλείας**
    e. **Άλλο…….**
5. **Έχετε κολλήσει ποτέ ιό (virus);**
    a. **ΝΑΙ**
    b. **ΟΧΙ**
6. **Η ζημιά που προέκυψε, από την παραβίαση αυτή, σαν κόστος ήταν :**
    a. **Χαμηλό**
    b. **Υψηλό**

7. **Υποβάλλεται σε έλεγχο το λειτουργικό σας σύστημα για την ύπαρξη κακόβουλων προγραμμάτων (σκουλήκια, ιοί, κλπ) ;**
    a. **ΝΑΙ**
    b. **ΟΧΙ**
8. **Γνωρίζετε τι σημαίνει η έννοια hacker/cracker;**
    a. **ΝΑΙ**
    b. **ΟΧΙ**
9. **Έχετε σπουδάσει κάτι σχετικό με την ασφάλεια των Η/Υ;**
    a. **ΝΑΙ**
    b. **ΟΧΙ**
10. **Οι χρήστες στην επιχείρηση σας, γνωρίζουν τρόπους επανόρθωσης από προσβολή από κακόβουλο λογισμικό καθώς και τρόπους περιορισμού εξάπλωσης του;**
    a. **ΝΑΙ**
    b. **ΟΧΙ**
    c. **Ελάχιστα**
11. **Από πού προμηθεύεται το λογισμικό που εγκαθιστά η εταιρεία σας;**
    a. **Έμπιστες πηγές (από κάποια εταιρεία παροχής λογισμικού)**
    b. **Διευθύνσεις στο διαδίκτυο (π.χ. δωρεάν παροχή)**
12. **Διαθέτετε στην εταιρεία σας εξυπηρετητή δικτύου (server);**
    a. **ΝΑΙ**
    b. **ΟΧΙ**
13. **Ποιό είδος Τείχου Προστασίας (Firewall) χρησιμοποιείτε ;**
    a. **Software**
    b. **Hardware**
    c. **Και τα δύο παραπάνω**
    d. **Δεν γνωρίζετε**
14. **Χρησιμοποιείται κωδικούς (passwords-συνθηματικά) ώστε να αποφεύγεται την πρόσβαση κακόβουλων χρηστών στο σύστημά σας;**
    a. **ΝΑΙ**
    b. **ΟΧΙ**

15. **Κάθε πότε αλλάζετε τους κωδικούς πρόσβασης ;**
    a. **Ποτέ**
    b. **Κάθε 3μηνο**
    c. **Κάθε 6μηνο**
    d. **Κάθε χρόνο**
    e. **Άλλο……**
16. **Χρησιμοποιείται προηγμένες τεχνολογίες-εργαλεία, στη πολιτική ασφαλείας σας για τον εντοπισμό και την αποτροπή κακόβουλων εισβολών ;**
    a. **ΝΑΙ**
    b. **ΟΧΙ**
17. **Τι θα βελτιώνατε στα προηγμένα συστήματα ασφαλείας ;**
    a. **Το κόστος**
    b. **(Μείωση) της τεχνολογικής πολυπλοκότητας τους για την καλύτερη διαχείριση τους**
    c. **Την ανάλυση επιθέσεων**
18. **Παρακολουθούνται επιμορφωτικά/εκπαιδευτικά προγράμματα για την εταιρεία σας, σε θέματα ασφάλειας των Η/Υ της ;**
    a. **ΝΑΙ**
    b. **ΟΧΙ**
19. **Πιστεύετε ότι το επίπεδο ασφάλειας του υπολογιστικού σας συστήματος του δικτύου σας για τα αποθηκευμένα/ες δεδομένα-πληροφορίες σας, είναι ικανοποιητικό ;**
    a. **ΝΑΙ**
    b. **ΟΧΙ**
    c. **Δεν γνωρίζετε**

Αρχικά στην πρώτη ερώτηση, γίνεται αναφορά στο είδος των επιχειρήσεων που απευθύνεται το ερωτηματολόγιο, οι οποίες μπορεί να είναι σύμφωνα με αυτό τεχνικές, μεταφορικές εταιρείες, λογιστικά, δικηγορικά, ασφαλιστικά γραφεία και άλλες διάφορων ειδών εμπορικές μικρομεσαίες επιχειρήσεις.

Στην δεύτερη ερώτηση, εμπεριέχονται ερωτήσεις όπου έχουν να κάνουν με τις υπηρεσίες που επαναλαμβάνονται καθημερινά από τους χρήστες και που είναι απαραίτητες για την διεκπεραίωση των εργασιών/διαδικασιών τους, και έχουν να δείξουν, μέσω ποιών οδών μπορεί να είναι επιρρεπής σε κινδύνους το πληροφοριακό σύστημα της κάθε εταιρείας, όπως και περιμένουμε αρκετές από τις ΜΜΕ να έχουν πρόσβαση στις περισσότερες από τις αναγραφόμενες υπηρεσίες. Σαν επιλογές είναι το Internet, τα Email που χρησιμοποιούνται σχεδόν από όλες τις επιχειρήσεις για αναγκαία καθημερινή χρήση και επικοινωνία, οι Συναλλαγές δια μέσου του διαδικτύου απαραίτητες κι αυτές με τη σειρά τους για ταχύτατη διεκπεραίωση πληρωμών, όπως εκτελούν κυρίως τα λογιστικά γραφεία για υποχρεωτικές πληρωμές διαφόρων φόρων (π.χ. ΦΠΑ), οι οποίες αναμένεται να διενεργούνται από ένα μικρό ποσοστό εμπορικών επιχειρήσεων που ανταλλάσουν σημαντικές πληροφορίες με τους πελάτες και προμηθευτές τους, τέλος η χρησιμοποίηση του MS Office.

Η τρίτη ερώτηση γίνετε με σκοπό να καταγραφεί το επίπεδο ασφαλείας των Η/Υ όταν πρόκειται για ιούς (viruses). Τα συγκεκριμένα προγράμματα-εργαλεία (antivirus) ανιχνεύουν την ύπαρξη ιών στο υπολογιστικό σύστημα. Οι απαντήσεις από την ερώτηση αυτή που αναμένονται να παρθούν είναι πως, η πλειοψηφία των ΜΜΕ χρησιμοποιεί αυτού του είδους προστασίας, για την ανίχνευση ιών μιας και είναι πλέον το πιο γνώριμο μέτρο προστασίας.

Η τέταρτη ερώτηση αναφέρεται στα μέτρα προστασίας, που ενδεχομένως να χρησιμοποιεί η κάθε επιχείρηση, έναντι κακόβουλων λογισμικών/επιθέσεων. Όπως η Κρυπτογράφηση που έχει να κάνει με την γνησιότητα των μηνυμάτων (e-mail) στο ηλεκτρονικό ταχυδρομείο, δηλαδή το μήνυμα το οποίο δέχεται ο παραλήπτης να είναι όντως του αποστολέα από τον οποίο περιμένει και όχι κάποιου άλλου. Τα (Back up) είναι η διαδικασία δημιουργίας αντιγράφων ασφαλείας για την αποθήκευση των δεδομένων σε

περίπτωση απώλειας/αλλοίωσης τους. Η δημιουργία των Backup, μπορεί να πραγματοποιηθεί (π.χ. σε δεύτερο εξωτερικό σκληρό δίσκο, DVD, CD-ROM, ή και με τη βοήθεια εύχρηστων προγραμμάτων λήψης αντιγράφων ασφαλείας καθώς αναβαθμίζεται η τεχνολογία). Τα (Firewalls) που τοποθετούνται για πρόληψη επιθέσεων (hacker) αλλά και για την εμπόδιση αυτών. Φιλτράρουν τα διακινούμενα πακέτα πληροφοριών από και προς τον υπολογιστή. Τα Πιστοποιητικά Ασφαλείας τα οποία χρησιμοποιούνται, για την ασφαλή μεταφορά προσωπικών πληροφοριών διαμέσου του internet, από εταιρείες που εμπορεύονται τα προϊόντα τους μέσω του διαδικτύου και θέλουν να διαφυλάξουν τα στοιχεία των πιστωτικών καρτών και γενικότερα για την αυθεντικότητα/ασφάλεια τοποθεσιών στο διαδίκτυο καθώς και για την πιστοποίηση της ταυτότητας των χρηστών. Σ' αυτό το σημείο, ο τρόπος αυτός αναμένεται να υιοθετείτε από ελάχιστες επιχειρήσεις. Γενικότερα, οι απαντήσεις που αναμένουμε να λάβουμε είναι πως οι περισσότερες ΜΜΕ δεν δίνουν ιδιαίτερη βάση στην ασφάλεια των υπολογιστικών τους συστημάτων και γι αυτό δεν υιοθετούν εξίσου όλους αυτούς τους τρόπους προστασίας παρά τους πιο γνωστούς.

Η πέμπτη ερώτηση αναφέρετε στην ενδεχόμενη ύπαρξη ιών, οι οποίοι μπορούν να εισέλθουν στον Η/Υ μέσω του διαδικτύου ή από εκτέλεση άγνωστης προέλευσης προγραμμάτων στα οποία δεν γνωρίζεται ο κατασκευαστής τους. Όσο και να τηρούνται οι τρόποι προστασίας από ένα μέρος των ΜΜΕ αλλά και εκείνες οι οποίες δεν τους τηρούν αυστηρά και αναμένεται να είναι αρκετές, δεν μπορούν να αποφύγουν την εισβολή ιών στα υπολογιστικά συστήματα τους.

Στην έκτη ερώτηση, οι ιοί αποτελούν κακόβουλα προγράμματα που μπορούν να προκαλέσουν σημαντικές ζημιές στη λειτουργία των υπολογιστικών συστημάτων μιας εταιρείας και να είναι η αιτία απώλειας δεδομένων καθώς μπορούν και προκαλούν καταστροφές π.χ. σε ολόκληρο το σκληρό δίσκο ή και κατάρρευση των Η/Υ. Οι απαντήσεις που αναμένονται να ληφθούν είναι πως οι ΜΜΕ φροντίζουν να αποφεύγουν τις καταστροφές στα λειτουργικά τους συστήματα, παρόλο αυτά δεν μπορούν να αποφύγουν εντελώς την ύπαρξη ιών και έτσι αναμένεται να επικρατήσει μια παραπάνω δαπάνη για την επιδιόρθωση βλαβών.

Η έβδομη ερώτηση στοχεύει στην επιβολή ελέγχου των Υπολογιστικών συστημάτων από τις ΜΜΕ για την αποφυγή κακόβουλων ενεργειών, κάτι το οποίο αναμένεται να μην πραγματοποιείτε κατά εξακολούθηση γι' αυτό το λόγο αρκετές επιχειρήσεις να μην υποβάλλουν τον έλεγχο, για το λόγο ότι οι ΜΜΕ συμβαίνει να αδιαφορούν για την ασφάλεια των Η/Υ τους.

Η όγδοη ερώτηση εμπεριέχεται με σκοπό να δείξει κατά πόσο οι ΜΜΕ έχουν υπόψη τους την σημασία των εννοιών Hacker/Cracker και τι ακριβώς είναι ικανοί αυτοί να προκαλέσουν. Αυτό που αναμένεται να απαντηθεί κυρίως, είναι πως η πλειοψηφία γνωρίζει τις συγκεκριμένες έννοιες.

Στην ένατη ερώτηση ερωτάται για το αν οι ΜΜΕ έχουν κάποιο υπεύθυνο μέλος το οποίο να είναι εξειδικευμένο στο τομέα της ασφάλειας των Η/Υ. Οι απαντήσεις που αναμένονται να παρθούν από τις περισσότερες είναι πως δεν έχουν και πως μόνο ελάχιστες είναι εκείνες οι οποίες ενδιαφέρονται πραγματικά για την ασφάλεια των λειτουργικών συστημάτων τους.

Η δέκατη ερώτηση αναφέρεται στο αν οι χρήστες μιας επιχείρησης γνωρίζουν να επαναφέρουν τα υπολογιστικά τους συστήματα όταν έχουν προσβληθεί από κάποιον ιό ή από δούρειους ίππους ή από άλλες κακόβουλες ενέργειες. Καθώς επίσης αν γνωρίζουν και τρόπους εμπόδισης αυτών των κακόβουλων ενεργειών από ενδεχόμενα επανειλημμένα τέτοια χτυπήματα. Οι απαντήσεις που αναμένονται να παρθούν είναι πως η πλειοψηφία δεν γνωρίζει.

Η ενδέκατη ερώτηση αναφέρεται στη παροχή λογισμικού των ΜΜΕ, με προγράμματα εγκατάστασης άγνωστης λειτουργικότητας, προέλευσης (δωρεάν καθώς και από το internet) ή με προγράμματα εμπορεύσιμα από εταιρείες ειδικευμένες στην ασφάλεια των Η/Υ. Οι απαντήσεις που αναμένουμε να λάβουμε από τη πλειοψηφία των εταιριών είναι πως προμηθεύονται λογισμικό από έμπιστες πηγές λογισμικού.

Η δωδέκατη ερώτηση εμπεριέχεται για να δείξει πόσες ΜΜΕ έχουν τουλάχιστον έναν εξυπηρετητή για το δίκτυο τους, όπου θα αποθηκεύονται τα αρχεία- εφαρμογές τους, που αποτελούν απαραίτητους πόρους για κάθε εταιρεία, έτσι ώστε να διενεργούνται πιο αποτελεσματικά οι διαδικασίες στους υπόλοιπους υπολογιστές μέσα στην επιχείρηση. Οι απαντήσεις που

αναμένονται να ληφθούν είναι πως ελάχιστες είναι αυτές που δεν έχουν κεντρικό εξυπηρετητή.

Η δέκατη τρίτη ερώτηση αναφέρεται στο είδος τείχου προστασίας (Firewall) που χρησιμοποιούν, για την ασφάλεια των λειτουργικών τους συστημάτων από μη εξουσιοδοτημένες εισβολές, από ιούς, από hackers και γενικότερα για την προστασία/ασφάλεια των διερχόμενων πακέτων πληροφόρησης από και προς τα δίκτυα των μικρομεσαίων επιχειρήσεων. Η πλειοψηφία των μικρομεσαίων επιχειρήσεων αναμένεται να διαθέτει Software Firewall, που είναι προστασία με προγράμματα σε αντίθεση με το Hardware Firewall προστασία με υλικό εξοπλισμό που αναμένεται να έχουν οι λιγότερες. Τέλος ένα μικρό ποσοστό των ΜΜΕ, αναμένεται να απαντήσουν ότι χρησιμοποιούν και τα δύο είδη Firewall αλλά και ότι υπάρχει ποσοστό που δεν γνωρίζει γι αυτό τον τρόπο προστασίας.

Η δέκατη τέταρτη ερώτηση αναφέρεται στην επιβολή ελέγχου πρόσβασης στα υπολογιστικά συστήματα με την χρησιμοποίηση (ισχυρών) κωδικών αποκλειστικά από τους χρήστες, για την εκτέλεση εφαρμογών στον κάθε υπολογιστή. Η πλειοψηφία των απαντήσεων που αναμένουμε να λάβουμε είναι πως αρκετές επιχειρήσεις κάνουν χρήση κωδικών πρόσβασης για την αποφυγή μη εξουσιοδοτημένης χρήσης στον Η/Υ του κάθε χρήστη, καθώς είναι ένα γνώριμο/οικείο μέτρο ασφάλειας.

Η δέκατη πέμπτη ερώτηση εμπεριέχεται με σκοπό να φανούν τα χρονικά διαστήματα που μεσολαβούν κατά την πραγματοποίηση αλλαγής των κωδικών πρόσβασης από επιχειρήσεις που χρησιμοποιούν αυτό το είδος προστασίας, που αναμένεται να μην πραγματοποιούν τη συχνή αλλαγή τους.

Στην δέκατη έκτη ερώτηση γίνεται αναφορά στην υιοθέτηση εξελιγμένων τεχνολογιών ασφαλείας από της μικρομεσαίες επιχειρήσεις που κύριο στόχο έχουν να παρέχουν αυξημένη προληπτική ασφάλεια από μη εξουσιοδοτημένες εισβολές στα λειτουργικά συστήματα καθώς και αντιμετώπιση από τέτοιου είδους κακόβουλες ενέργειες, με την χρήση προηγμένων τεχνολογιών/εργαλείων. Οι περισσότερες απαντήσεις αναμένονται να είναι θετικές.

Η δέκατη έβδομη ερώτηση που απευθύνεται στους ερωτηθέντες είναι για το τι θα επέλεγαν εάν είχαν τη δυνατότητα να βελτιώσουν ακόμα περισσότερο τα συστήματα ασφαλείας που θα μπορούσαν να αποκτήσουν

εγκατεστημένα στην επιχείρηση τους ή που ήδη έχουν. Οι απαντήσεις είναι το κόστος, τη μείωση της τεχνολογικής πολυπλοκότητας τους για ευκολότερη διαχείριση τους και τέλος η ανάλυση των επιθέσεων.

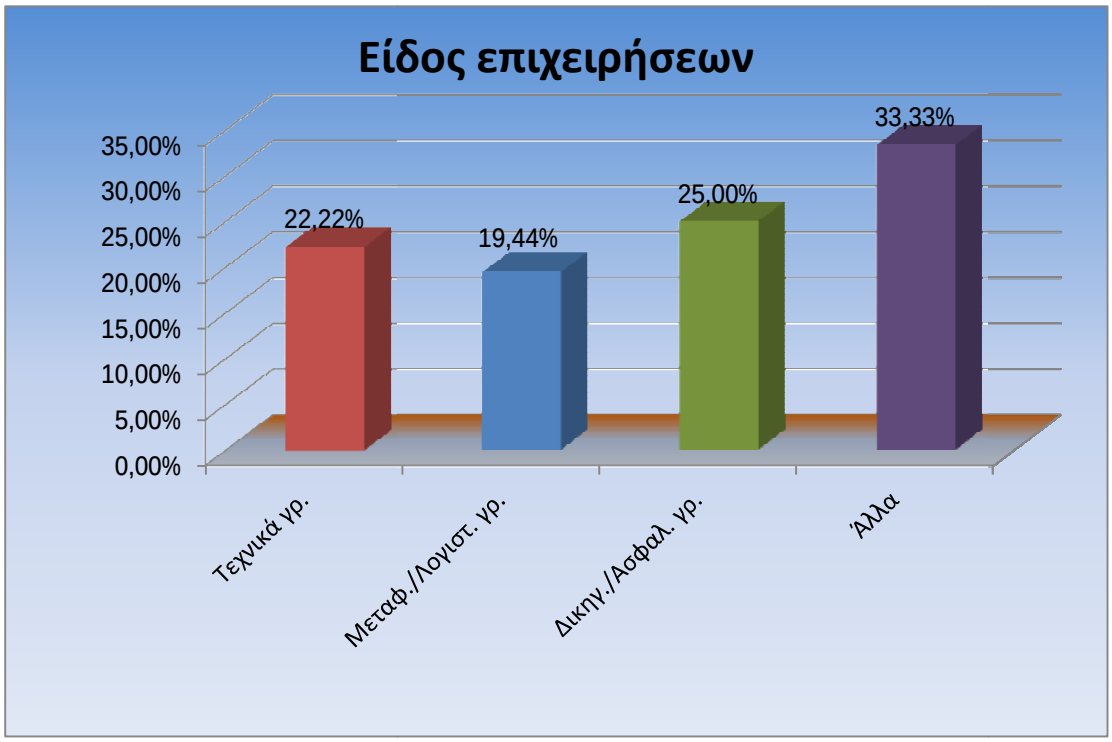
Η δέκατη όγδοη ερώτηση αναφέρεται με το σκοπό να φανεί κατά πόσο οι μικρομεσαίες επιχειρήσεις ενδιαφέρονται για την παρακολούθηση επιμορφωτικών σεμιναρίων επάνω σε θέματα ασφαλείας των υπολογιστικών συστημάτων τους, κάτι το οποίο επιπλέον θα δείξει κατά πόσο ενημερωμένοι είναι και οι χρήστες των μικρομεσαίων επιχειρήσεων, για να είναι έγκαιρα αντιμέτωποι με την ύπαρξη τυχόν κακόβουλων προγραμμάτων. Οι περισσότερες από τις μικρομεσαίες επιχειρήσεις αναμένεται να μην παρακολουθούν τέτοια προγράμματα.

Τέλος, στην δέκατη ένατη ερώτηση αναγράφεται αν το επίπεδο ασφάλειας των πληροφοριακών συστημάτων θεωρείται ικανοποιητικό από τις ΜΜΕ. Τα αποτελέσματα των απαντήσεων είναι : ναι, όχι και δεν γνωρίζεται. Οι περισσότερες απαντήσεις κλείνουν στο ότι οι μικρομεσαίες επιχειρήσεις θεωρούν ικανοποιητικό το επίπεδο ασφαλείας των υπολογιστικών τους πόρων.

ΚΕΦΑΛΑΙΟ 4ο

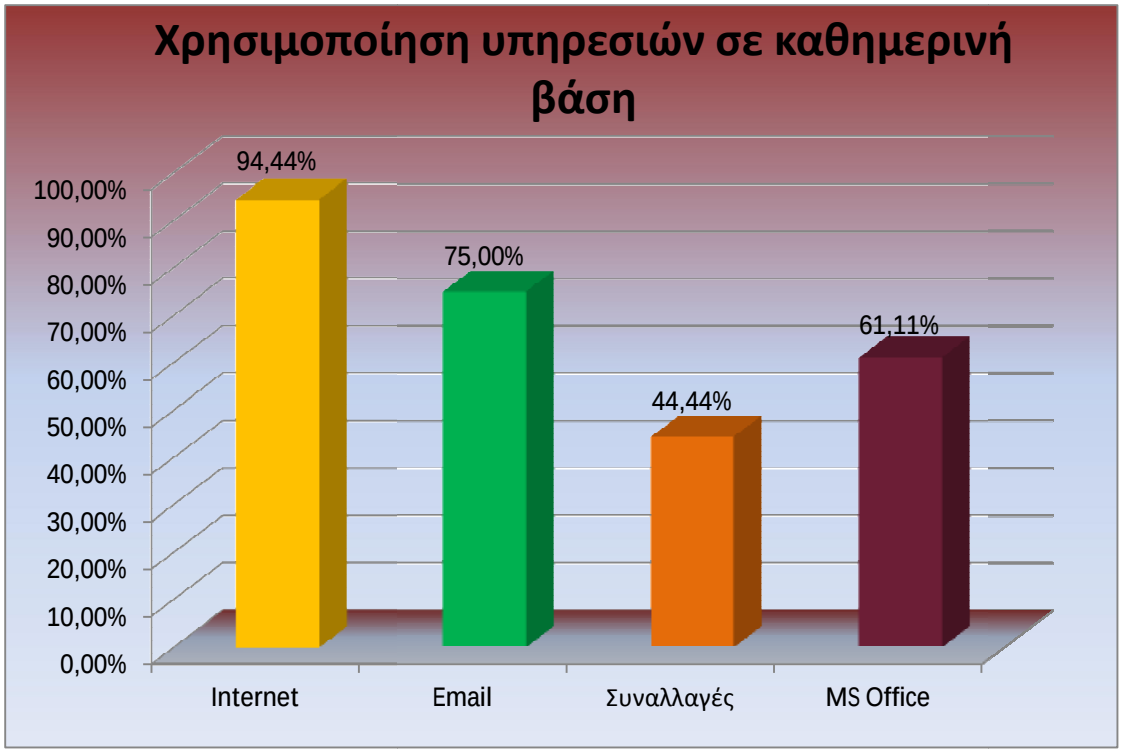
4.1 ΑΝΑΛΥΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ

1. Τι είδους επιχείρηση είναι;



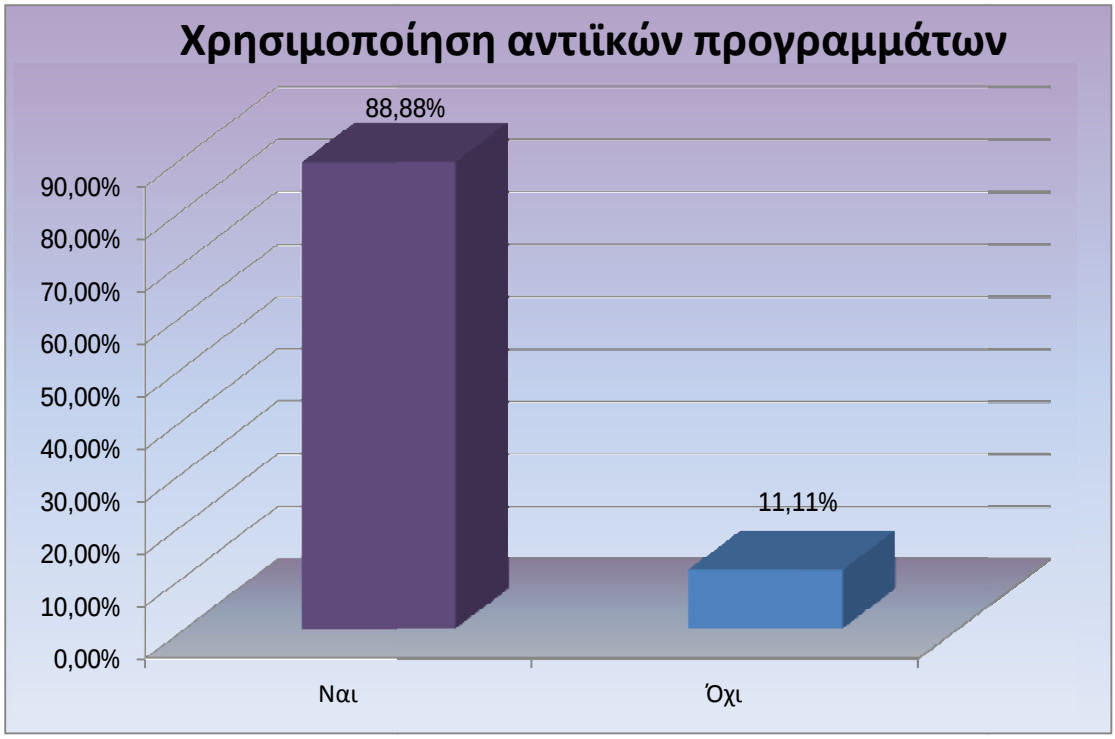
Στο παραπάνω γράφημα απεικονίζεται το είδος των επιχειρήσεων που συμμετέχουν στα αποτελέσματα των ερωτήσεων συνολικά του ερωτηματολογίου. Όπως φαίνεται το 22,22% είναι τεχνικά γραφεία, το 19,44% μεταφορικές εταιρείες και λογιστικά γραφεία, το 25,00% δικηγορικά μαζί με ασφαλιστικά γραφεία και τέλος απεικονίζονται με τη μορφή ‘’άλλα’’ διαφόρων ειδών εμπορικές/παραγωγικές επιχειρήσεις που αγγίζουν το ποσοστό των 33,33%.

2. Ποια/ες υπηρεσίες χρησιμοποιείται σε καθημερινή βάση; (μπορείτε να επιλέξετε παραπάνω από μία απαντήσεις)



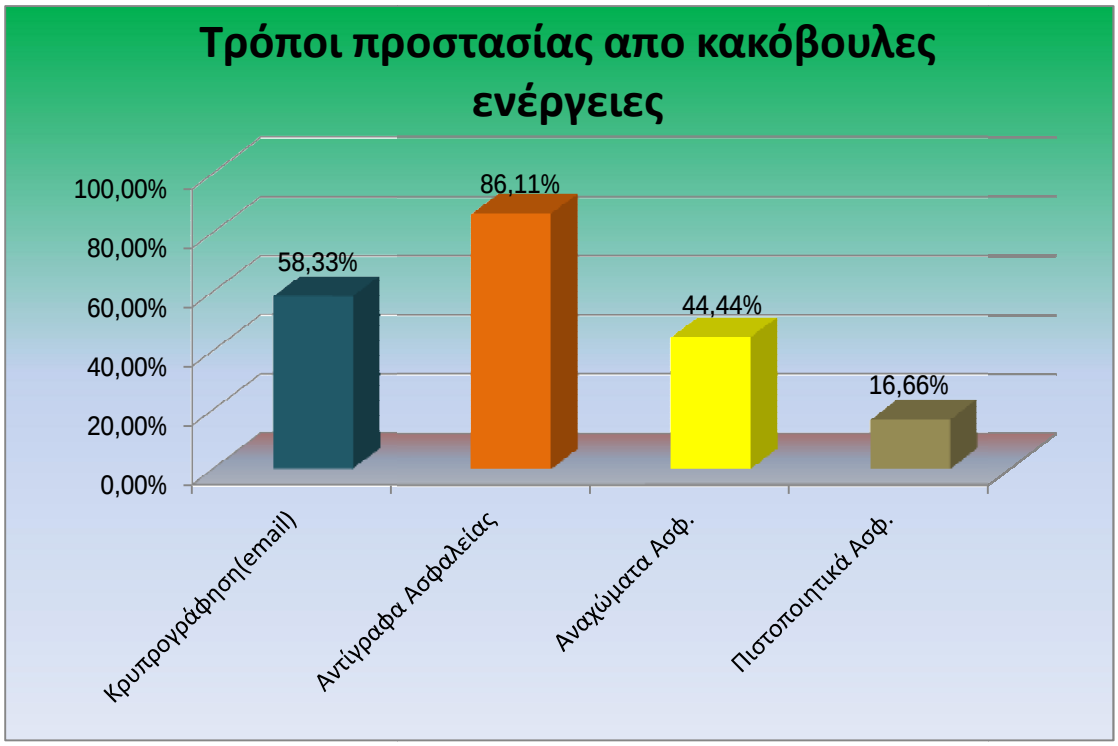
Σύμφωνα με το διάγραμμα, φαίνεται ότι το 94,44% των επιχειρήσεων να χρησιμοποιούν το internet σε καθημερινή βάση για αναζήτηση πληροφοριών κ.α., το 75,00% χρησιμοποιεί συχνά email για επικοινωνία, όπως με προμηθευτές, πελάτες κ.α. Το 44,44% των επιχειρήσεων μέσα στις καθημερινές τους υπηρεσίες εντάσσονται οι συναλλαγές, για την ταχύτατη διεκπεραίωση πληρωμών μέσω του διαδικτύου που εκτελούνται κυρίως από τα λογιστικά γραφεία για υποχρεωτικές πληρωμές διαφόρων φόρων, όπως ο ΦΠΑ, φόρο μισθωτών υπηρεσιών(ΦΜΥ), φόρο φορολογίας εισοδήματος, και εργοδοτικών εισφορών (ΙΚΑ). Ακόμη, διάφορες άλλες συναλλαγές εκτελούνται και από εμπορικές εταιρείες που ανταλλάσουν σημαντικές πληροφορίες/στοιχεία με τους πελάτες, προμηθευτές τους. Έπειτα το 61,11% χρησιμοποιεί σε καθημερινή βάση MS Office.

3. Στους Η/Υ της επιχείρησής σας χρησιμοποιείται αντιβιοτικό λογισμικό (antivirus) ;



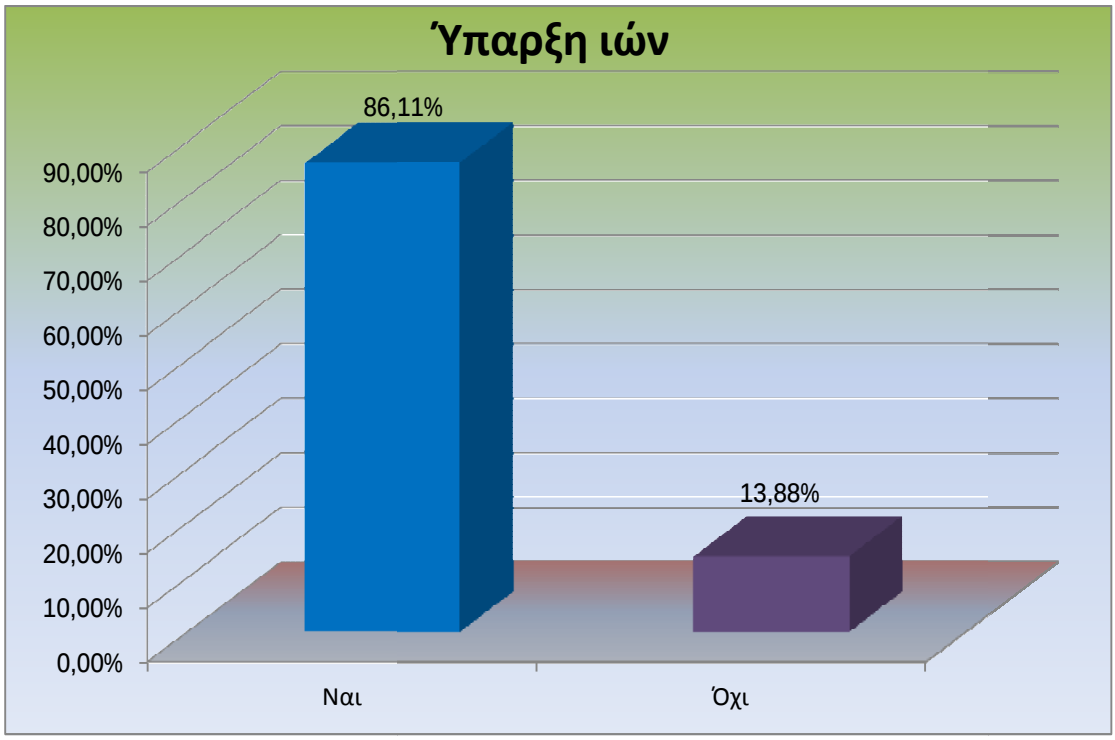
Στο παραπάνω διάγραμμα φαίνεται ότι το 88,88% των επιχειρήσεων κάνει χρήση αντιβιοτικών λογισμικών τα ονομαζόμενα ως (antivirus), για την ανίχνευση ιών στα υπολογιστικά τους συστήματα με σκοπό την εμπόδιση τους. Ενώ το 11,11% των επιχειρήσεων δεν χρησιμοποιεί, με αποτέλεσμα οι Η/Υ να είναι επιρρεπής στα κακόβουλα προγράμματα και στην απώλεια δεδομένων.

4. **Ποιούς τρόπους προστασίας χρησιμοποιείται για την αντιμετώπιση κακόβουλων ενεργειών; (μπορείτε να επιλέξετε παραπάνω από μία απαντήσεις)**



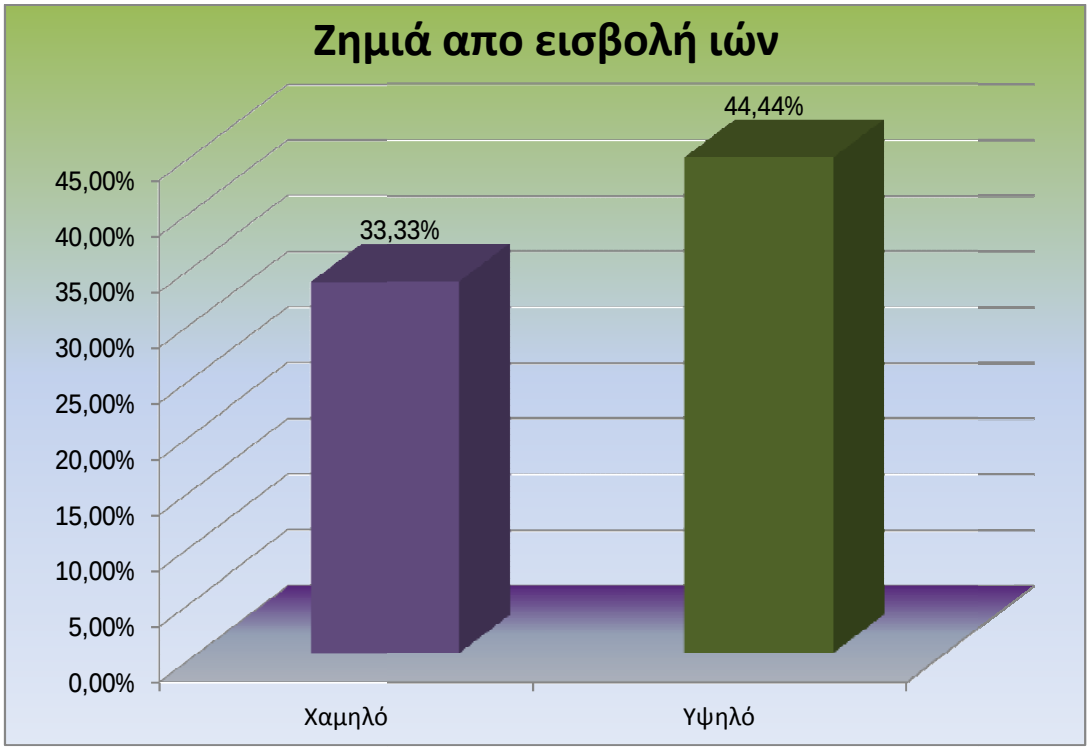
Σύμφωνα με το διάγραμμα αυτό που φαίνεται είναι πως το 58,33% των επιχειρήσεων χρησιμοποιεί ως τρόπο προστασίας από κακόβουλες ενέργειες, την κρυπτογράφηση στα email για την γνησιότητα των μηνυμάτων ηλεκτρονικού ταχυδρομείου. Το μεγαλύτερο ποσοστό των επιχειρήσεων όπως φαίνεται και στο διάγραμμα υιοθετεί σαν τρόπο προστασίας των ευαίσθητων δεδομένων τους, τα αντίγραφα ασφαλείας (backup) για την αποθήκευση των αρχείων/δεδομένων που διαθέτουν και είναι ποσοστό της τάξεως 86,11%. Έπειτα το ποσοστό 44,44% των επιχειρήσεων χρησιμοποιεί ως τρόπο προστασίας τα αναχώματα ασφαλείας (Firewall) για πρόληψη κακόβουλων προγραμμάτων (trojan horses, viruses, κ.α.) αλλά και για απομάκρυνση επιθέσεων (hacker). Τέλος, το 16,66% χρησιμοποιεί πιστοποιητικά ασφαλείας για τη διαφύλαξη προσωπικών πληροφοριών με την πιστοποίηση της ταυτότητας των χρηστών σε ασφαλής/αυθεντικές τοποθεσίες του διαδικτύου, καθώς και για ασφαλής συναλλαγές. Αυτό τον τρόπο υιοθετούν κυρίως λογιστικά γραφεία και ορισμένες εμπορικές εταιρείες που χρησιμοποιούν σημαντικά στοιχεία στις συναλλαγές τους με διάφορες δημόσιες ή μη υπηρεσίες, προμηθευτές κ.α. καθώς, παρατηρείται να είναι ο λιγότερο διαδεδομένος τρόπος πρόληψης.

5. Έχετε κολλήσει ποτέ ιό (virus);



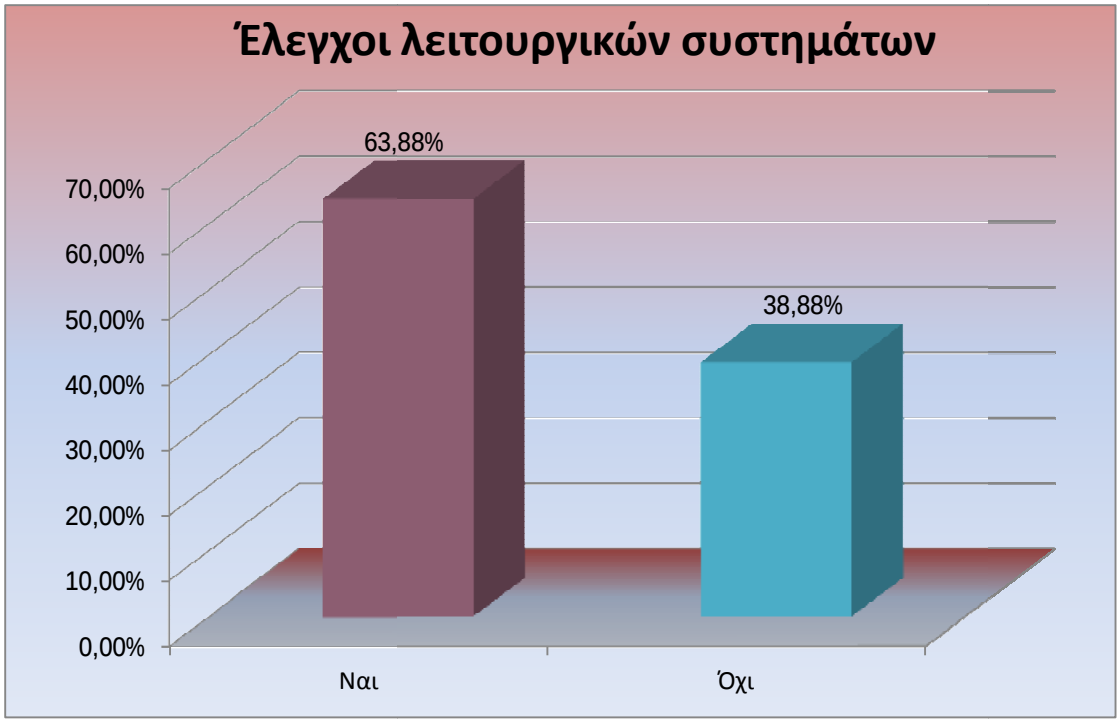
Στο παραπάνω διάγραμμα φαίνεται ότι, το 86,11%% των επιχειρήσεων δείχνει να έχει κολλήσει ιό συχνά κατά το παρελθόν, για το λόγο ότι δεν φροντίζουν οι περισσότερες σταδιακά για την ασφάλεια του δικτύου τους αλλά και γιατί υπάρχουν επιχειρήσεις που δεν είναι καθόλου ενήμερες για το πόσο εύκολα μπορεί να προκύψει μια παραβίαση στα υπολογιστικά τους συστήματα. Ενώ, ποσοστό της τάξεως 13,88% δείχνει πως δεν έχουν κολλήσει ιό για χρονικό διάστημα μικρότερο του ενός εξαμήνου.

6. Η ζημιά που προέκυψε, από την παραβίαση αυτή, σαν κόστος ήταν :



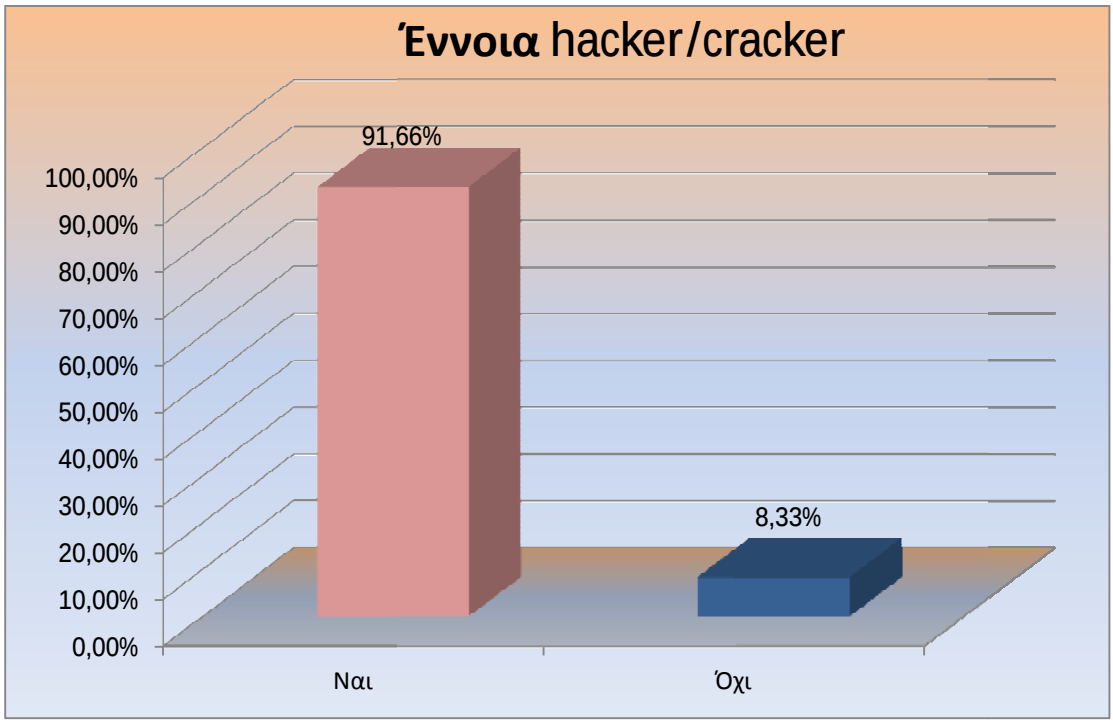
Όπως φαίνεται στο διάγραμμα το 33,33% των επιχειρήσεων η ζημιά που προκλήθηκε από παραβιάσεις κακόβουλων ενεργειών (ιών), ανέρχεται σε χαμηλό κόστος, ενώ αυτό που δείχνει να υπερισχύει είναι το 44,44% των επιχειρήσεων, στις οποίες η ζημιά από τέτοιου είδους παραβίαση ανέρχεται σε υψηλό ποσό.

7. Υποβάλλεται σε έλεγχο το λειτουργικό σας σύστημα για την ύπαρξη κακόβουλων προγραμμάτων (σκουλήκια, ιοί, κλπ) ;



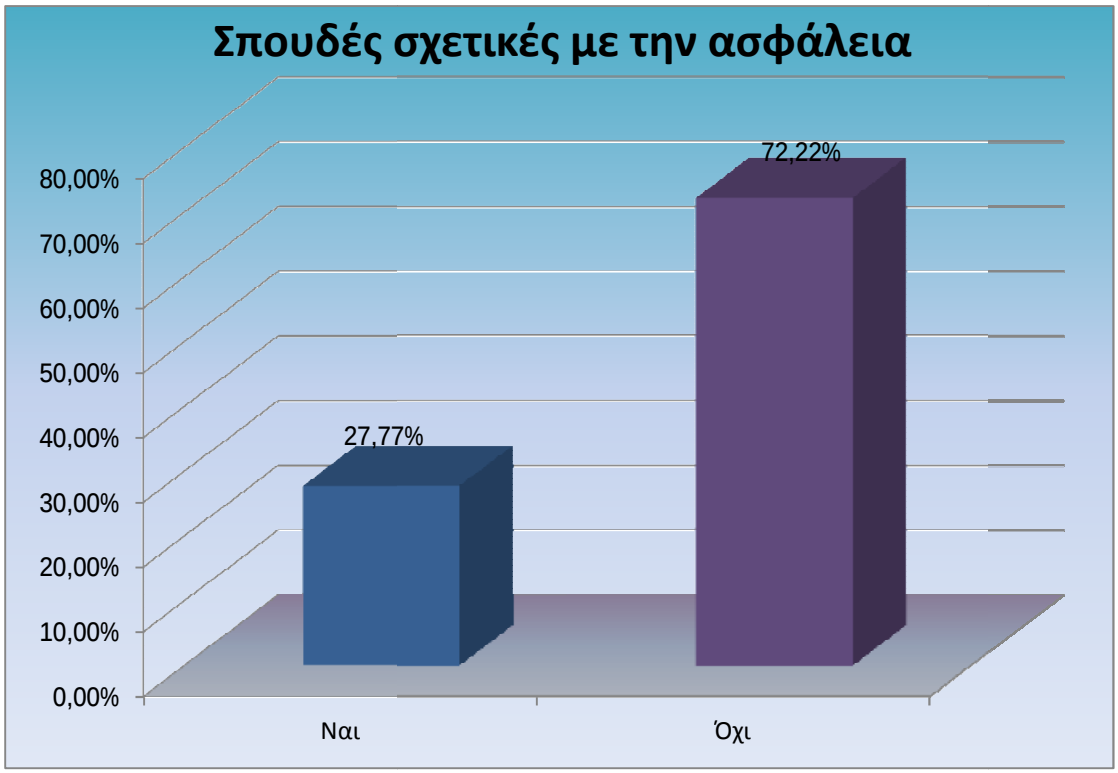
Στο παραπάνω διάγραμμα φαίνεται πως το 63,88% των επιχειρήσεων, ισχυρίζεται πως υποβάλλει σε έλεγχο τα λειτουργικά συστήματα, σε ή μη τακτά (εβδομάδας, μηνός) χρονικά διαστήματα. Αντίθετα, ένα σημαντικός αριθμός ποσοστού επιχειρήσεων 38,88%, δεν πραγματοποιεί ελέγχους όπως θα έπρεπε, με αποτέλεσμα τα πληροφοριακά τους συστήματα να είναι περισσότερο ευάλωτα σε κακόβουλες εισβολές και έτσι να έρχονται αντιμέτωπες με τα όποια κόστη για επιδιορθώσεις βλαβών.

8. Γνωρίζετε τι σημαίνει η έννοια hacker/cracker;



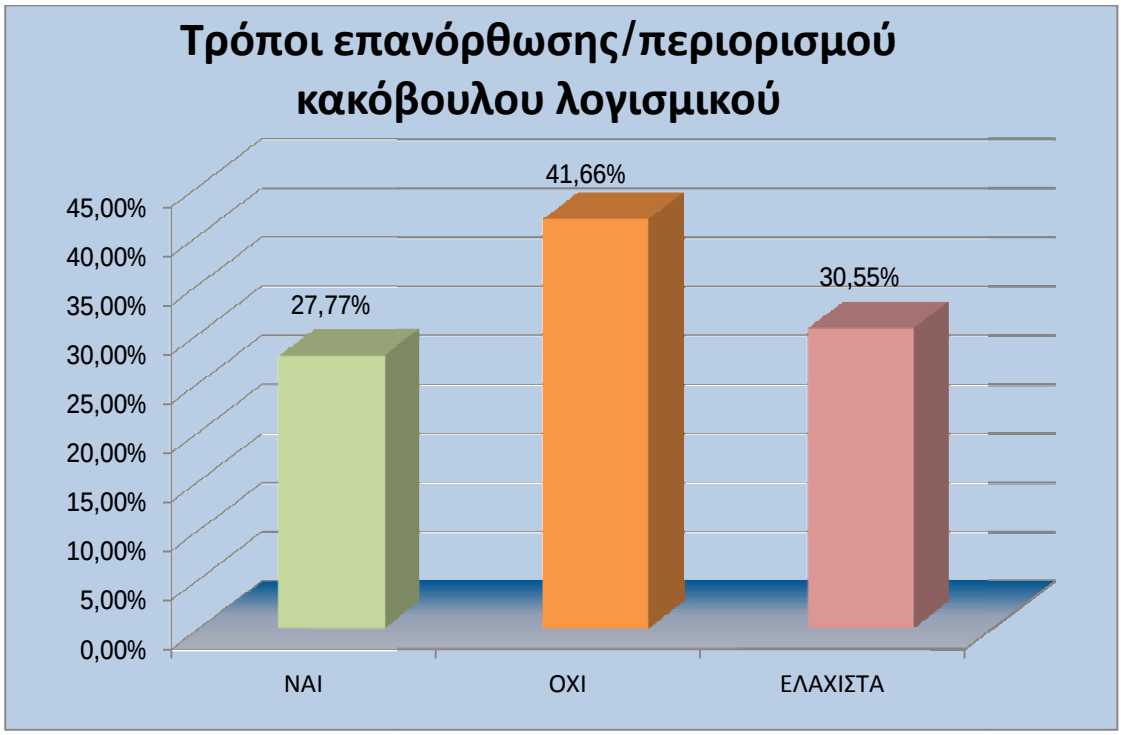
Σύμφωνα με το διάγραμμα, αυτό που φαίνεται είναι ότι το 91,66% των ΜΜΕ ισχυρίζεται ότι γνωρίζει τις έννοιες hacker/cracker, ενώ το 8,33% των ΜΜΕ ισχυρίζεται ότι δεν γνωρίζει την ουσιαστική έννοια τους και για το τι καταστροφές μπορούν να προκαλέσουν.

9. Έχετε σπουδάσει κάτι σχετικό με την ασφάλεια των Η/Υ;



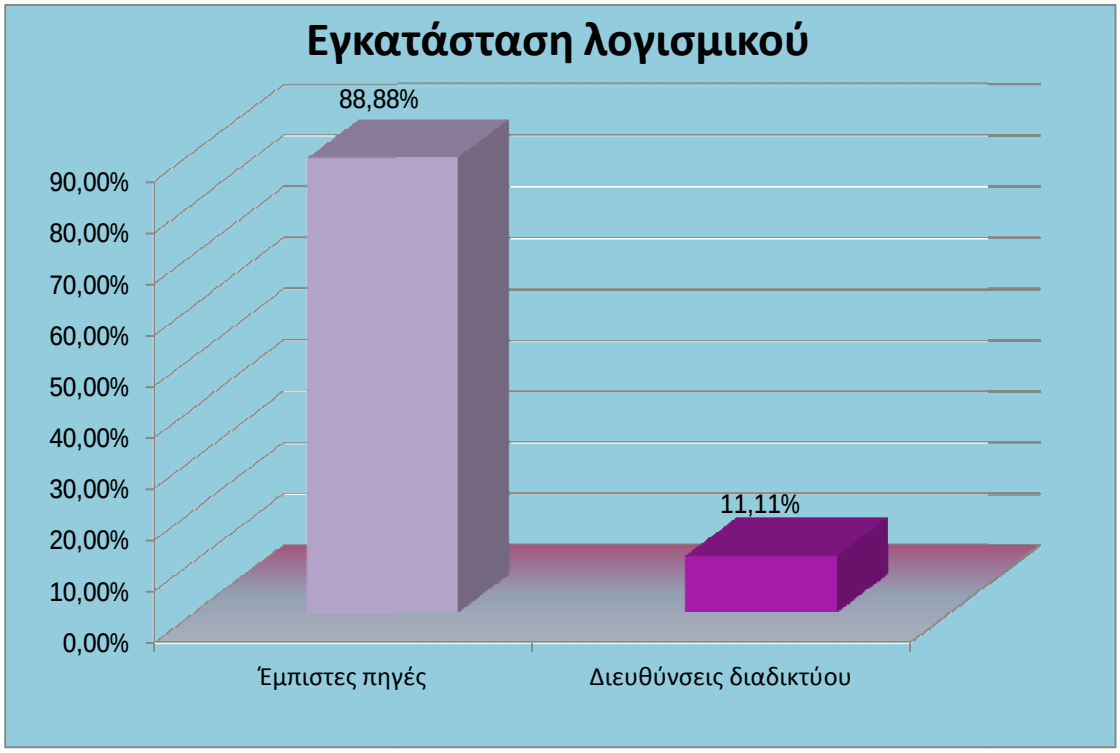
Στο παραπάνω διάγραμμα, με ποσοστό 27,77% των επιχειρήσεων, έχει φροντίσει για την ασφάλεια του δικτύου του και αφορά κυρίως επιχειρήσεις που κατέχουν άτομα τα οποία και δουλεύουν μόνιμα σε αυτές καθώς παράλληλα φροντίζουν και ασχολούνται για την ασφάλεια των υπολογιστικών τους συστημάτων και των δικτύων τους, παρέχοντας τις εξειδικευμένες γνώσεις τους. Αντίθετα, ακολουθεί ποσοστό 72,22% το οποίο δεν περιέχει άτομα που να έχουν ακολουθήσει σχετικές σπουδές με την ασφάλεια των υπολογιστικών συστημάτων/δικτύων, με αποτέλεσμα οι μικρομεσαίες αυτές επιχειρήσεις να είναι περισσότερο ευάλωτες σε κακόβουλες εισβολές.

10. Οι χρήστες στην επιχείρηση σας, γνωρίζουν τρόπους επανόρθωσης από προσβολή από κακόβουλο λογισμικό καθώς και τρόπους περιορισμού εξάπλωσης του;



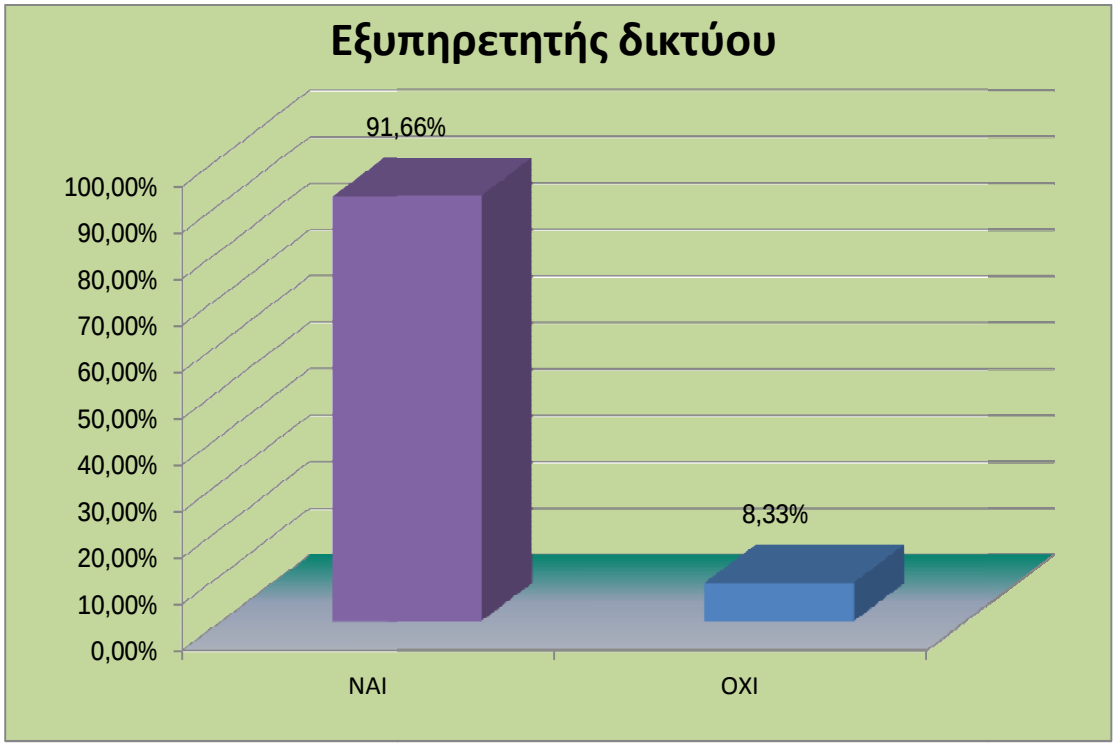
Στο παραπάνω διάγραμμα βλέπουμε ότι, οι χρήστες που αντιστοιχούν στο ποσοστό 27,77% των ΜΜΕ, γνωρίζουν τρόπους επανόρθωσης από άγνωστες απειλές/επιθέσεις. Στη συνέχεια, χρήστες που αντιστοιχούν σε ποσοστό 41,66% των ΜΜΕ ισχυρίζονται ότι δεν γνωρίζουν τρόπους επανόρθωσης και αποτροπής κακόβουλων ενεργειών και αυτό στηρίζεται κυρίως στο, ότι οι συγκεκριμένες επιχειρήσεις δεν διαθέτουν αξιόπιστα συστήματα/λύσεις ασφαλείας που να εμποδίζουν ολοένα νεότερες απειλές καθώς ο παράγοντας της ασφάλειας δεν είναι στατικός, το επίπεδο ασφαλείας τους δεν είναι κατάλληλο. Ακόμη, ποσοστό 30,55% ισχυρίζεται πως ελάχιστα γνωρίζει τρόπους επανόρθωσης των υπολογιστικών τους συστημάτων από άγνωστες επιθέσεις.

11. Από πού προμηθεύεται το λογισμικό που εγκαθιστά η εταιρεία σας;



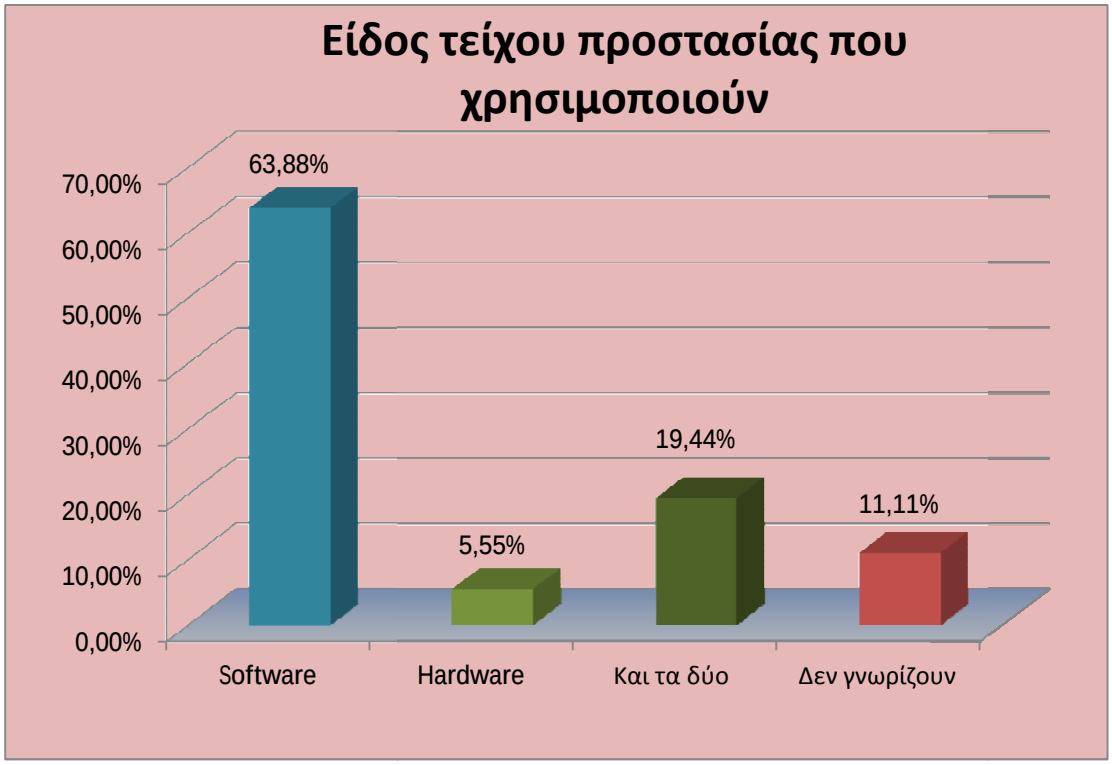
Από το διάγραμμα παραπάνω προκύπτει πως, οι επιχειρήσεις που εγκαθιστούν έτοιμα προγράμματα/λογισμικό για τα πληροφοριακά τους συστήματα αγγίζουν το ποσοστό του 88,88%, τα οποία προέρχονται από έμπιστες εταιρείες παροχής λογισμικών. Ενώ σε ποσοστό μικρότερο μόλις 11,11% των ΜΜΕ, προτιμούν να προμηθεύονται το λογισμικό τους από το διαδίκτυο ελεύθερα/δωρεάν, πράγμα που δεν είναι έμπιστο καθώς μπορεί να είναι άγνωστου κατασκευαστή ή και εσφαλμένα εξαρχής και δεν γίνεται να παρέχουν την προαπαιτούμενη υποστήριξη σε περιπτώσεις ανάγκης, σημαντική η αιτία αυξημένων δαπανών (σε αντίθετη περίπτωση, αν είχαν φροντίσει προληπτικά) των επιχειρήσεων, που προκύπτουν έπειτα από ανεπιθύμητες εισβολές στα πληροφοριακά τους συστήματα.

12. Διαθέτετε στην εταιρεία σας εξυπηρετητή δικτύου (server);



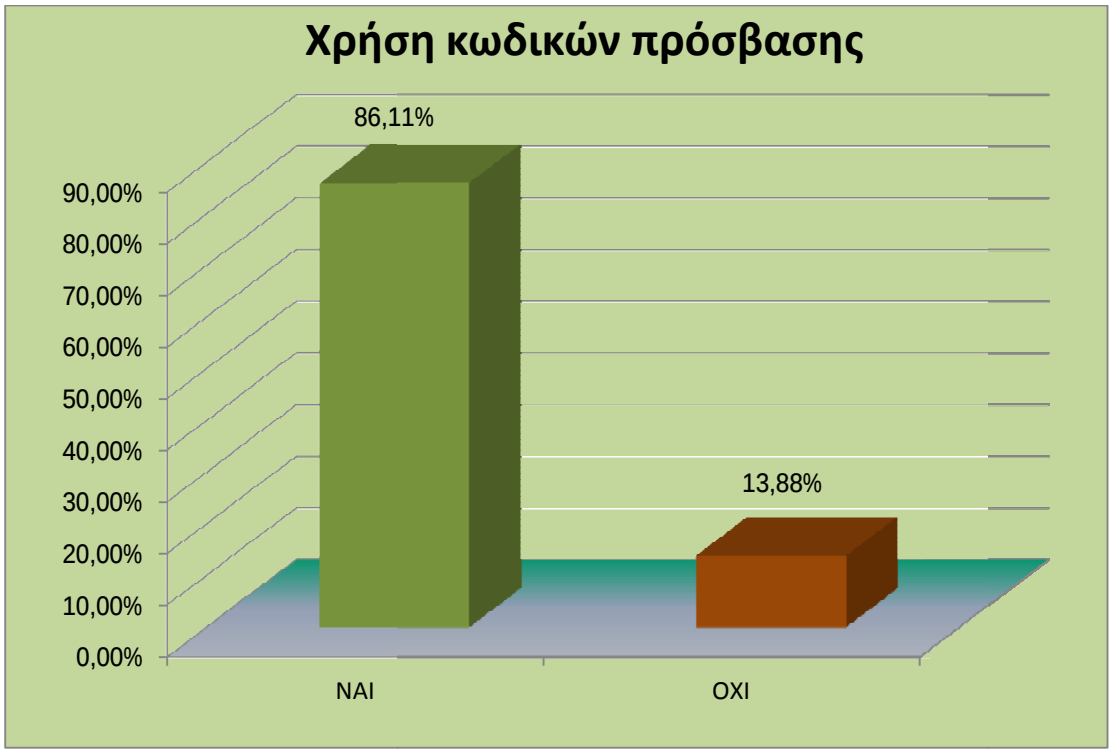
Στο διάγραμμα φαίνεται πως, το 91,66% των επιχειρήσεων χρησιμοποιεί ένα τουλάχιστον Server για την καλύτερη διεκπεραίωση των διαδικασιών στο δίκτυο τους, συνδεδεμένοι με τους υπόλοιπους υπολογιστές, όπου αποθηκεύονται ευαίσθητα αρχεία και δεδομένα που κατά τη διάρκεια τα ανακτούν οι χρήστες. Αντίθετα, το 8,33% δεν διαθέτει εξυπηρετητή δικτύου.

13. Ποιό είδος Τείχου Προστασίας (Firewall) χρησιμοποιείτε ;



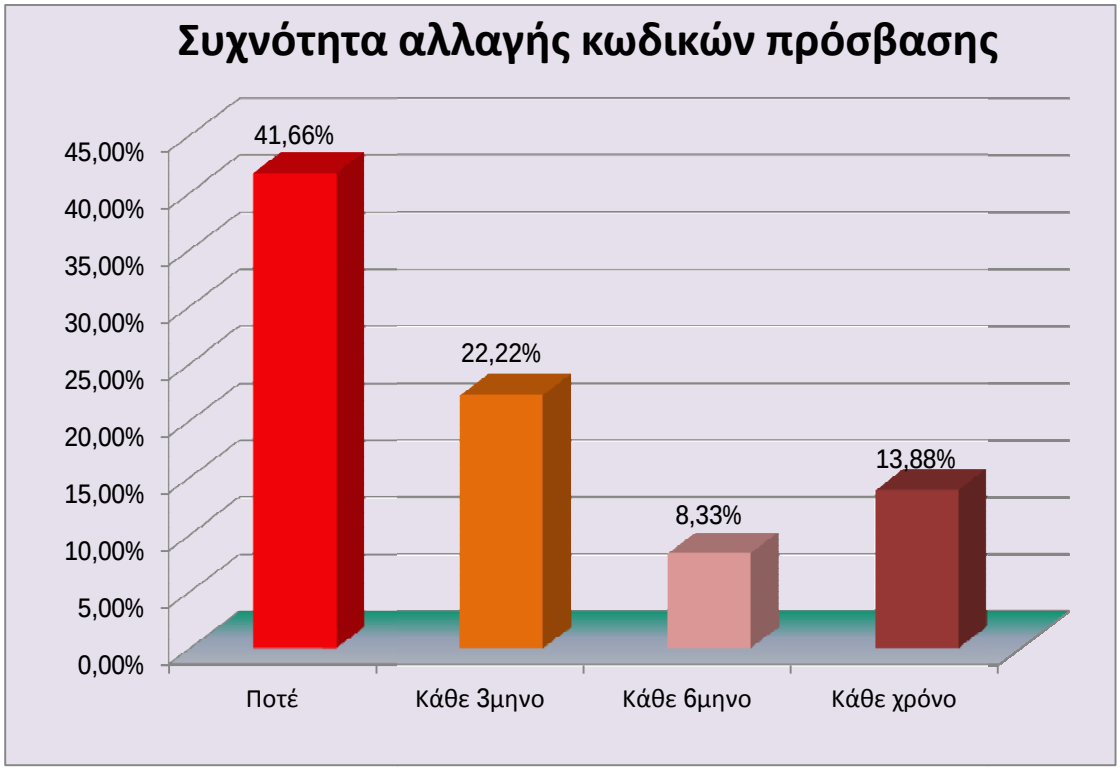
Όπως φαίνεται στο διάγραμμα με μεγάλη διαφορά το 63,88% των μικρομεσαίων επιχειρήσεων χρησιμοποιεί software firewall για την προστασία των διακινούμενων πακέτων πληροφοριών από και προς το δίκτυο τους. Στη συνέχεια ένα μικρό ποσοστό χρησιμοποιεί hardware firewall για την προστασία των δεδομένων τους. Ακολουθεί ποσοστό με 19,44% που κάνει χρήση και λογισμικού αλλά και υλικού εξοπλισμού για πρόληψη από άγνωστες επιθέσεις, καθώς παρατηρείται να είναι μικρό το ποσοστό στην εφαρμογή και των δύο αυτών μέτρων ασφαλείας από τις επιχειρήσεις. Τέλος, το 11,11% απαντά πως δεν γνωρίζει γι' αυτό το είδος προστασίας λόγο της άγνοιας που έχουν για την ασφάλεια.

14. Χρησιμοποιείται κωδικούς (passwords-συνθηματικά) ώστε να αποφεύγεται την πρόσβαση κακόβουλων χρηστών στο σύστημά σας;



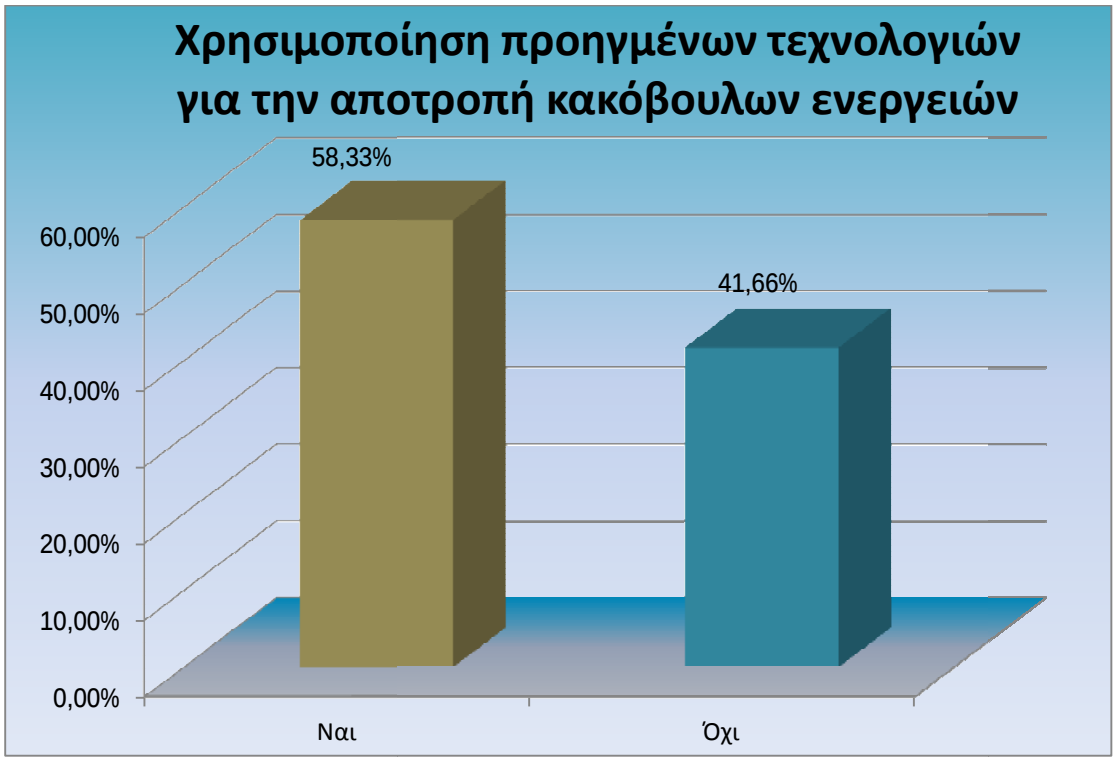
Όσον αφορά την ερώτηση για χρησιμοποίηση ισχυρών κωδικών στα υπολογιστικά συστήματα της κάθε ΜΜΕ, που αποτελεί ένα ακόμη μέτρο προστασίας, όπως παρουσιάζεται και παραπάνω το 86,11% κάνει χρήση αυτού του μέτρου, ενώ ποσοστό 13,88% δεν δείχνει να ενδιαφέρεται για το συγκεκριμένο είδος προστασίας γι' αυτό και δεν πραγματοποιεί χρήση αυτών.

15. Κάθε πότε αλλάζετε τους κωδικούς πρόσβασης ;



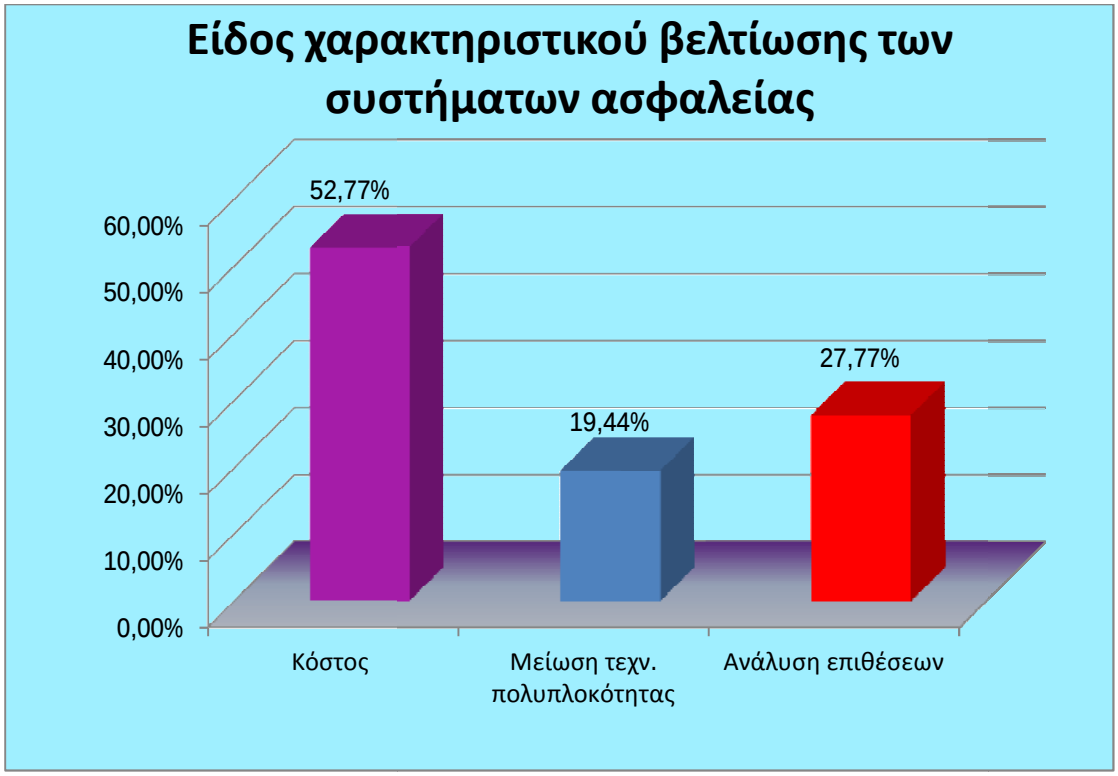
Όπως παρουσιάζεται στο επάνω διάγραμμα, οι απαντήσεις των ερωτηθέντων όσον αφορά την συχνότητα αλλαγής των κωδικών πρόσβασης στους Η/Υ που χρησιμοποιούν, αυτή είναι ανύπαρκτη για το μεγαλύτερο ποσοστό που είναι 41,66% αν και θα έπρεπε να ήταν συχνότερη η πραγματοποίηση αλλαγής, ακολουθεί ένα 22,22% το οποίο αλλάζει κάθε 3 μήνες, ένα 8,33% το οποίο πραγματοποιεί κάθε 6 μήνες και τέλος σε ένα 13,88% η συχνότητα σημειώνεται ότι πραγματοποιείται κάθε χρόνο.

16. Χρησιμοποιείται προηγμένες τεχνολογίες/συστήματα, στη πολιτική ασφαλείας σας για τον εντοπισμό και την αποτροπή κακόβουλων εισβολών ;



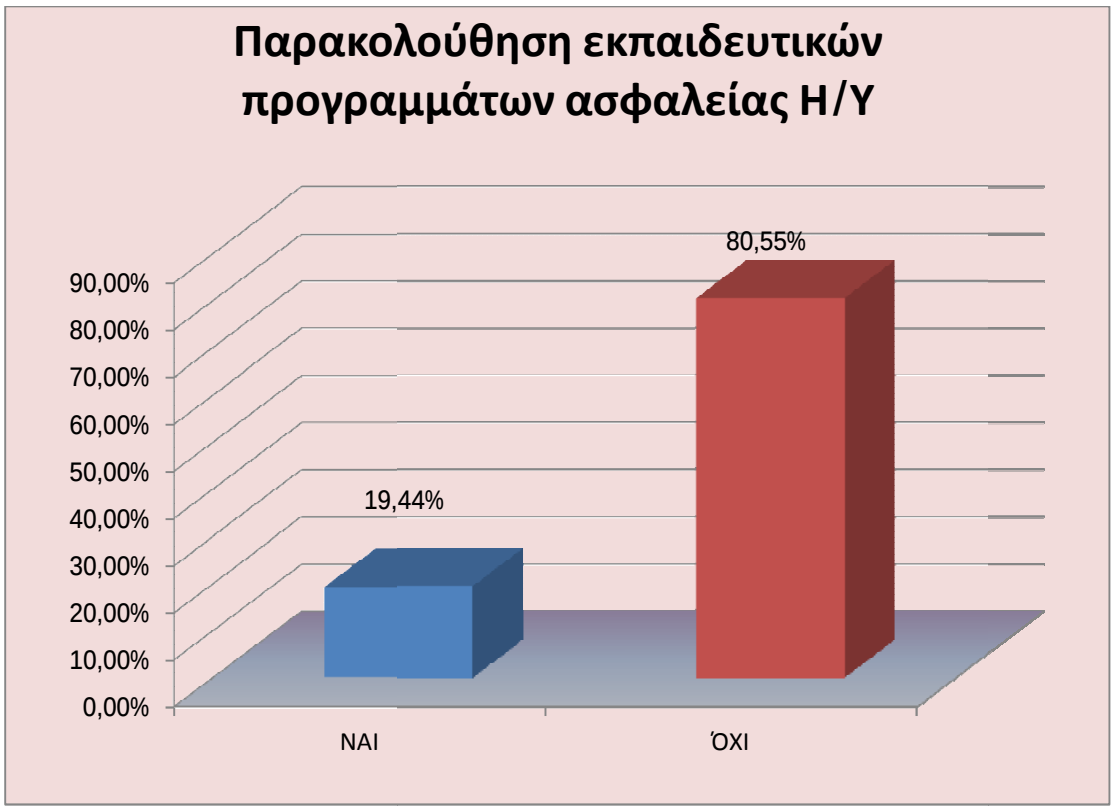
Σύμφωνα με το διάγραμμα, βλέπουμε ότι το 58,33% των επιχειρήσεων χρησιμοποιεί εξελιγμένες τεχνολογίες/συστήματα ασφαλείας στα υπολογιστικά τους συστήματα, με σκοπό την αποφυγή και αντιμετώπιση νέων/άγνωστων απειλών (ιών, hacker, κ.α.). Στο προαναφερόμενο ποσοστό, οι περισσότερες από τις ΜΜΕ θεωρούν ως προηγμένες τεχνολογίες που χρησιμοποιούν, τα ήδη γνωστά υπάρχοντα αντιϊκά προγράμματα που διαθέτουν (antivirus), λίγες τα αναχώματα ασφαλείας (Firewall), ενώ ελάχιστες θεωρούν ως εξελιγμένα συστήματα ασφαλείας, που διαθέτουν τα IDS - συστήματα ανίχνευσης εισβολών. Στη συνέχεια ακολουθεί ποσοστό επιχειρήσεων της τάξεως 41,66% το οποίο ισχυρίζεται πως δεν χρησιμοποιεί προηγμένες τεχνολογίες ασφαλείας.

17. Τι θα βελτιώνατε, αν ήταν αυτό δυνατό, στα προηγμένα συστήματα ασφαλείας ;



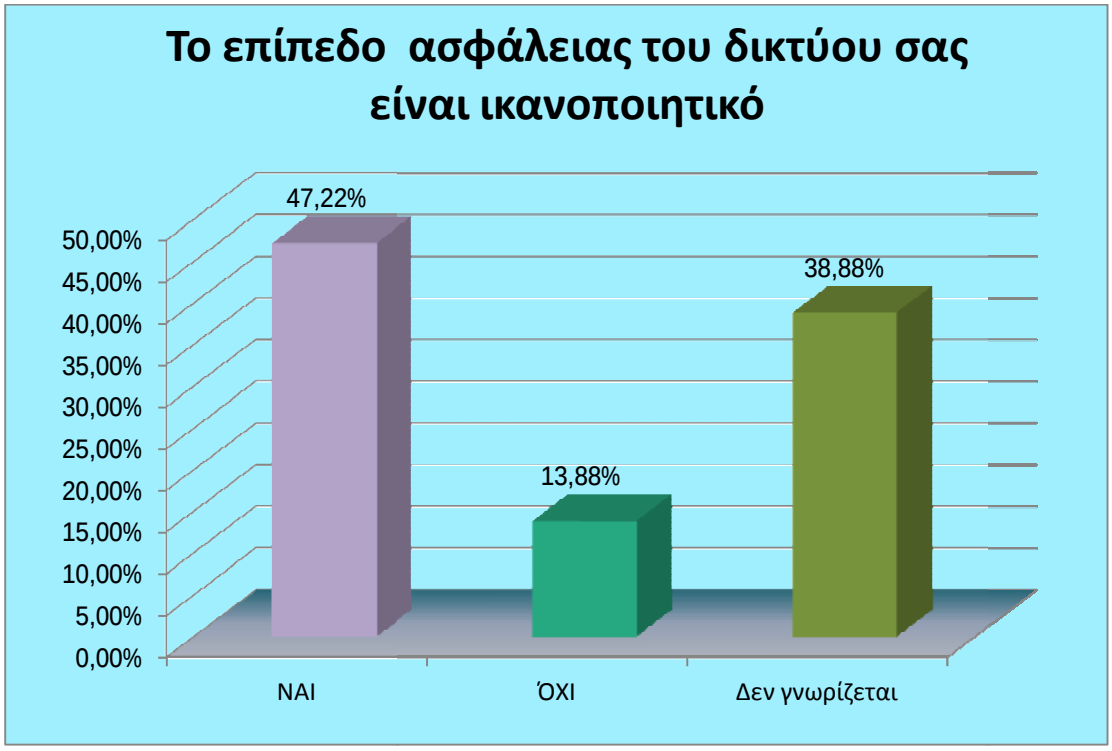
Όπως απεικονίζεται στο επάνω διάγραμμα, οι περισσότερες επιχειρήσεις, θα βελτίωναν το κόστος για μη δαπανηρή εγκατάσταση τέτοιων προηγμένων μηχανών όπως ισχυρίζονται, σε ποσοστό που αγγίζει το 52,77%. Έπειτα ποσοστό 19,44% θα πετύχαινε μείωση της τεχνολογικής πολυπλοκότητας των συστημάτων αυτών για την καλύτερη διαχείριση τους, με σκοπό την ευκολότερη παροχή πληροφοριών της κατάστασης του δικτύου, σε περιπτώσεις προβλημάτων για την έγκαιρη αντιμετώπιση τους. Ακόμη, ένα ποσοστό 27,77% των ερωτηθέντων, θα επέλεγε ακόμη πιο βέλτιστη ανάλυση κάθε πιθανής εισβολής.

18. Παρακολουθούνται επιμορφωτικά/εκπαιδευτικά προγράμματα για την εταιρεία σας, σε θέματα ασφάλειας των Η/Υ της ;



Όπως φαίνεται παραπάνω το 19,44% των επιχειρήσεων μόνο, παρακολουθούν εκπαιδευτικά προγράμματα/σεμινάρια για την ασφάλεια των Η/Υ, πράγμα που δείχνει ότι ελάχιστες μόνο ενδιαφέρονται πραγματικά για την ασφάλεια του δικτύου τους και φροντίζουν γι' αυτό και για την συνεχή ενημέρωση τους επί του θέματος. Ενώ, ποσοστό 80,55% δεν φροντίζει να παρακολουθεί τέτοιου είδους σεμινάρια.

19. Πιστεύετε ότι το επίπεδο ασφάλειας του υπολογιστικού σας συστήματος του δικτύου σας για τα αποθηκευμένα/ες δεδομένα-πληροφορίες σας, είναι ικανοποιητικό ;



Σύμφωνα με το διάγραμμα, το 47,22% των μικρομεσαίων επιχειρήσεων θεωρεί ότι το επίπεδο ασφάλειας των υπολογιστικών τους συστημάτων να είναι ικανοποιητικό για πρόληψη αλλά και αντιμετώπιση κακόβουλων ενεργειών (ιών, μη εξουσιοδοτημένων εισβολών), και φαίνεται να επικρατεί παρόλο την άγνοια πολλών επιχειρήσεων σε βασικές πτυχές του θέματος. Το 13,88% ισχυρίζεται ότι δεν έχουν την ασφάλεια που θα έπρεπε, για το λόγο αυτό απαντούν ότι το επίπεδο ασφαλείας τους δεν είναι ικανοποιητικό. Τέλος, ποσοστό της τάξεως 38,88% σύμφωνα με το διάγραμμα, δεν μπορεί να κρίνει αν το επίπεδο ασφάλειας του δικτύου τους είναι λίγο ή πολύ ασφαλές, με την έννοια ότι ποτέ δεν μπορεί κανείς να είναι σίγουρος για την ασφάλεια του δικτύου του από κακόβουλες ενέργειες, καθώς ο τομέας της ασφάλειας δεν είναι στατικός αλλά δυναμικός με απώτερο σκοπό την συνεχή εξέλιξη της.

ΚΕΦΑΛΑΙΟ 5ο

5.1 ΣΥΜΠΕΡΑΣΜΑΤΑ - ΚΡΙΤΙΚΗ - ΠΡΟΤΑΣΕΙΣ

Έπειτα από την ανάλυση των ερωτήσεων που προηγήθηκαν στο προηγούμενο κεφάλαιο και σύμφωνα με τις συνεντεύξεις των υποψήφιων υπεύθυνων ασφαλείας δικτύων των επιχειρήσεων που συμμετείχαν στην έρευνα, αυτά που προκύπτουν είναι τα εξής :

Συγκεκριμένα, τα δίκτυα των επιχειρήσεων πλέον είναι μόνιμα συνδεδεμένα με το internet, και όπως έχει γίνει αντιληπτό, να είναι αρκετά ευάλωτα και εκτεθειμένα σε έναν μεγάλο αριθμό κινδύνων. Έτσι, κατά την διεκπεραίωση των καθημερινών υπηρεσιών τους θα πρέπει, να φροντίζουν να επισκέπτονται, για την ασφάλεια του δικτύου τους, αυθεντικές διαδικτυακές τοποθεσίες αλλά και να εφαρμόζουν απαραίτητα μέτρα προστασίας (όπως η κρυπτογράφηση σε e-mail, τα πιστοποιητικά ασφαλείας, χρήση ισχυρών κωδικών καθώς και συχνή αλλάγη αυτών). Ακόμη, τακτική λήψη αντιγράφων ασφαλείας (backup), ιδιαίτερα των κρίσιμων και χρήσιμων αρχείων, που οφείλει κάθε χειριστής ενός Η/Υ να πραγματοποιεί, καθώς παρατηρείται να χρησιμοποιούν κυρίως για την αποθήκευση των δεδομένων, πληροφοριών τους, εξυπηρετητές αρχείων (Server).

Επιπλέον, η πλειοψηφία των επιχειρήσεων σήμερα χρησιμοποιεί αντιϊκά προϊόντα (antivirus) παρόλ' αυτά, δεν γίνεται να αποφύγουν εντελώς τις μολύνσεις από κακόβουλα προγράμματα, καθώς όλο και καινούργιοι ιοί (όπως π.χ. οι πολυμορφικοί ιοί) εμφανίζονται και προσβάλλουν τα πληροφοριακά συστήματα. Αποτέλεσμα αυτών των μολύνσεων, είναι οι δαπάνες μεγάλων χρηματικών ποσών για επιδιορθώσεις προβλημάτων, ανακατασκευή κατεστραμμένων δεδομένων και λοιπών ενεργειών.

Επιπρόσθετα, οι χρήστες των μικρομεσαίων επιχειρήσεων θα πρέπει να φροντίζουν να είναι ενήμεροι και να γνωρίζουν πάντοτε τρόπους αποκατάστασης των υπολογιστικών συστημάτων από τέτοιου είδους εισβολές για να συμμερίζονται τους κινδύνους που αναλαμβάνουν όταν δοκιμάζουν προγράμματα άγνωστης προέλευσης, κάτι το οποίο φάνηκε να μην ισχύει. Έτσι λοιπόν καλό θα είναι να εκπαιδεύονται γι' αυτό, με το να παρακολουθούν

ανάλογα επιμορφωτικά προγράμματα, πράγμα που δεν συνηθίζεται, όπως διαπιστώθηκε από την έρευνα και να μην υιοθετούν μόνο τους πιο γνωστούς τρόπους προστασίας για τα ευαίσθητα δεδομένα τους, που είναι κυρίως κωδικοί πρόσβασης, αντίγραφα ασφαλείας, κρυπτογράφηση στα email, αντιβιοτικά λογισμικά. Ακόμη, θα έπρεπε όλες οι επιχειρήσεις στο εσωτερικό τους να διαθέτουν μόνιμα εξειδικευμένο προσωπικό, που θα παρέχει μόνιμη υποστήριξη για την ασφάλεια των δικτύων τους και όχι μόνο ελάχιστες να διαθέτουν και να προσπαθούν να διατηρούν καλό επίπεδο ασφάλειας των δεδομένων τους, ή κάθε ΜΜΕ να διαθέτει ένα τουλάχιστον άτομο που να έχει πραγματοποιήσει σπουδές σχετικές με την ασφάλεια. Ακόμη όλα τα προγράμματα λογισμικού, θα πρέπει να προέρχονται από έμπιστες πηγές και να παρέχουν κατάλληλη υποστήριξη στους διαχειριστές δικτύων για απαραίτητη βοήθεια όταν την χρειάζονται. Επιπρόσθετα, θα πρέπει όλα τα τερματικά στο δίκτυο να είναι πλήρως ενημερωμένα ως προς τις εφαρμογές τους και τη λειτουργικότητα τους (όπως συνεχή ανανέωση του μητρώου ταυτοποιημένων ιών και όλων των προγραμμάτων λογισμικού), ώστε να είναι λιγότερο ευάλωτα σε πιθανές επιθέσεις, εφόσον η διαδικασία της ασφάλειας παραμένει μία δυναμική και όχι στατική υπόθεση. Καθώς όλες οι μικρομεσαίες επιχειρήσεις θα πρέπει να πραγματοποιούν συνεχής ελέγχους των λειτουργικών τους συστημάτων σε τακτά χρονικά διαστήματα οι οποίοι δεν τηρούνται με τέτοια συχνότητα.

Παρατηρείται ότι, πολλές από τις μικρομεσαίες επιχειρήσεις δεν γνωρίζουν τις δυνατότητες των firewalls σαν βασική 1^{η} γραμμή άμυνας, που απαραίτητα πρέπει να υπάρχουν σε κάθε ΜΜΕ, και ότι πάνω σ’ αυτά βασίζονται κι άλλα εξελιγμένα συστήματα ασφαλείας (π.χ. IDS, IPS) για ουσιαστικότερη αντιμετώπιση άγνωστων απειλών, κάτι το οποίο παρατηρήθηκε να μην πραγματοποιείτε, παρά να τα εγκαθιστούν ελάχιστες μόνο επιχειρήσεις. Επιπλέον, αρκετές στα παραπάνω, φάνηκε να μην συνδυάζουν υλικό και λογισμικό εξοπλισμό, για την αποτελεσματικότερη αντιμετώπιση κακόβουλων εισβολών. Η πλειοψηφία δηλαδή των ΜΜΕ όπως έδειξε η έρευνα, χρησιμοποιεί κυρίως Software Firewall, αντί να χρησιμοποιεί και επιπλέον Hardware Firewall, η οποία μπορεί είναι συσκευή αυτόνομη (όπως ένας δρομολογητής-router). Για το λόγο αυτό στην πολιτική ασφαλείας της κάθε ΜΜΕ θα πρέπει, να χρησιμοποιεί σύγχρονα-προηγμένα συστήματα

ασφαλείας (υβριδικά Firewall :συνδυασμός φιλτραρίσματος πακέτων με πύλες εφαρμογών-υβριδική τεχνολογία Stateful Inspection, IDS) για την αυξανόμενη προληπτική ασφάλεια του συστήματος και την αντιμετώπιση σοβαρών κινδύνων.

Η έρευνα έδειξε, πως οι περισσότερες μικρομεσαίες επιχειρήσεις θεωρούν και χρησιμοποιούν προηγμένα συστήματα ασφαλείας τα antivirus (antivirus), λίγες τα αναχώματα ασφαλείας (firewalls) και ελάχιστες τα (IDS). Αυτό κατ' επέκταση δείχνει για ακόμη μια φορά το μη ικανοποιητικό επίπεδο ασφάλειας των ΜΜΕ, που σημαίνει ότι τα δεδομένα, αρχεία που διαθέτουν μπορούν εύκολα να υποκλαπούν και καταστραφούν από hackers και να κινδυνεύουν στο έπακρο από κακόβουλα λογισμικά (viruses, worms, Trojan horses). Παρατηρήθηκε λοιπόν, οι περισσότερες από τις ΜΜΕ να μην υιοθετούν προηγμένες λύσεις/τεχνολογίες προστασίας στην πολιτική ασφαλείας τους, κατά της εισβολής άγνωστων και καινούργιων απειλών (ιών, hackers), λόγο κυρίως του υψηλού χρηματικού ποσού για την εγκατάσταση τους. Για το λόγο αυτό η πλειοψηφία απαντά, πως ένα χαρακτηριστικό που θα βελτίωνε στα συστήματα ασφαλείας, είναι το κόστος απόκτησης τους, ακολουθεί η καλύτερη ανάλυση των επιθέσεων και τέλος οι λιγότερες επιχειρήσεις απάντησαν η τεχνολογική πολυπλοκότητα αυτών για καλύτερη διαχείριση τους και κατάλληλη πληροφόρηση της κατάστασης του δικτύου τους.

Άρα το επίπεδο ασφαλείας των πληροφοριακών συστημάτων και δικτύων στις Μικρομεσαίες Επιχειρήσεις παρατηρείται ότι δεν είναι ικανοποιητικό, λόγο άγνοιας πολλών επιχειρήσεων σε θέματα ασφαλείας δικτύων και πολλών σφαλμάτων του υλικού αλλά και του λογισμικού που χρησιμοποιούνται στο δίκτυο τους, με αποτέλεσμα την εύκολη παραβίαση τους από κακόβουλα προγράμματα αλλά και από κακόβουλους εισβολείς (Hackers) οι οποίοι εντοπίζουν εύκολα τις ευπάθειες κάθε δικτύου και εκμεταλλεύονται τέτοιες καταστάσεις προς όφελος τους, με την υποκλοπή και διαρροή σημαντικών-ευαίσθητων αρχείων ή την καταστροφή τους και την δυσλειτουργία εφαρμογών. Γι' αυτό το λόγο οι επιχειρήσεις θα πρέπει πάντα να εφαρμόζουν και να εξελίσσουν, βελτιώνουν τις πολιτικές ασφαλείας τους.

Ακόμη, σαν αποτέλεσμα όλων αυτών των παραμέτρων, θα πρέπει η κάθε επιχείρηση να εφαρμόζει στη πολιτική ασφαλείας της, όχι μόνο μία

τεχνική ασφαλείας σαν αντιμετώπιση από κακόβουλες ενέργειες/εξωτερικών επιθέσεων αλλά ένα σύνολο από τέτοιες ενέργειες για καλύτερη πρόληψη και προστασία στην οποιαδήποτε νέα απειλή. Όπως παραδείγματος χάριν, όχι μόνο συστήματα Firewall ή μόνο αντιϊκά προγράμματα διότι το κάθε ένα από αυτά τα μέτρα ασφαλείας είναι μία μόνο πτυχή της ασφάλειας σαν $1^{η}$ γραμμή άμυνας, χωρίς να θεωρούνται ικανά από μόνα τους για την εξασφάλιση της απόκρουσης τέτοιων επιθέσεων. Είναι καλύτερα μία επιχείρηση να επενδύσει στην ασφάλεια του δικτύου της πρόωρα, παρά να χρειαστεί να αντιδράσει μετά από μία επίθεση.

Εν κατακλείδι, με σκοπό την καλύτερη εμβάθυνση επί του θέματος, θα ήταν να πραγματοποιηθεί έρευνα σε μεγάλες σύγχρονες επιχειρήσεις που διαθέτουν πολυάριθμα υποκαταστήματα ανά τον κόσμο. Ο έλεγχος, σε τέτοιου είδους δίκτυα (ευρείας εμβέλειας) που εντάσσονται οι συγκεκριμένες, είναι πολύ δύσκολη υπόθεση, η εγκληματικότητα παραμένει μία μόνιμη απειλή εκφραζόμενη με την σύγχρονη έννοια το Hacking με σκοπό την μετάδοση ιών, υποκλοπή προγραμμάτων, σημαντικών αρχείων και δεδομένων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Laudon K., Laudon J., Πληροφοριακά συστήματα διοίκησης, Αθήνα 1998.

- Scriven D., Scriven J., Kozoll C., Πολιτικές και διαδικασίες πληροφοριακών συστημάτων διοίκησης, εκδόσεις Κριτήριον, Αθήνα.

- Βασιλακόπουλος Γ., Χρυσικόπουλος Β., Πληροφοριακά συστήματα διοίκησης, εκδόσεις Α. Σταμούλης, Πειραιάς 1990.

- Γκίνογλου Δ., Ταχυνάκη Π., Πρωτοψάλτη Ν., Λογιστικά πληροφοριακά συστήματα, Αθήνα 2004.

- Κιουντούζης Ε., Μεθοδολογίες ανάλυσης και σχεδιασμού πληροφοριακών συστημάτων, εκδόσεις Μπένου, Αθήνα 2002.

- Παπαθανασίου Α., Θέματα επιχειρηματικών πληροφοριακών συστημάτων», Αθήνα 2008.

- Τασόπουλος Α., Πληροφοριακά συστήματα: οργάνωση, μεθοδολογία, εφαρμογές, εκδόσεις Σταμούλης, Αθήνα 2005.

- Γ. Σ. Οικονόμου - Ν. Β. Γεωργοπούλου, Πληροφοριακά συστήματα για τη Διοίκηση Επιχειρήσεων, Εκδόσεις Ευγ. Μπένου, Αθήνα 2004.

- Σωκρ.Κάτσικας-Δημ.Γκρίζαλης-Στεφ.Γκρίτζαλης, Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών, Αθήνα2004.

- Γ. Πάγκαλος – Ι. Μαυρίδης, Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων, Εκδόσεις ΑΝΙΚΟULA, Θεσσαλονίκη 2002.

- Silvia Vaccaro,., Περιηγηθείτε με ασφάλεια στο διαδίκτυο, Εκδόσεις Ημερησία Α.Ε.Ε, Αθήνα 2007.

- http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Firewalls.html

- Ι. Βογιατζής, Δίκτυα, Διαδίκτυο και Εφαρμογές, Εκδόσεις TYPOoffset, Πάτρα 2006.

- Μαλαμάτη Δ. Λούτα, Ασφάλεια Συστημάτων, Κοζάνη 2007.

- http://www.ict.plus.gr: Διαδικτυακή πύλη για την πληροφορική, τις τηλεπικοινωνίες, την τεχνολογία και τις επιχειρήσεις στην Ελλάδα και στον κόσμο

- Μαλαμάτη Δ. Λούτα, Τηλεπικοινωνίες-Δίκτυα, Κοζάνη 2006.

- http://www.securitymanager.gr/it_security/contents_article.php?id=135&category=INTERVIEW&month=%C9%C1%CD%CF%D5%C1%D1%C9%CF%D3-%D6%C5%C2%D1%CF%D5%C1%D1%C9%CF%D3&year=2011&issue=19&PHPSESSID=f745eb4872a309edea76ff63beebb7fb