ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

Τίτλος Εργασίας: ΑΣΦΑΛΕΙΑ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΕ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Πτυχιακή Εργασία των
Μήτρου Μαρία
Τζόκα Λαμπρινή
Επιβλέπων: **Χατζίνας Σπυρίδων**

ΠΑΤΡΑ 2011

ΠΡΟΛΟΓΟΣ

Αυτή η εργασία έγινε με σκοπό να αποδείξει την άγνοια των μικρομεσαίων επιχειρήσεων για την ασφάλεια των τοπικών δικτύων και των πληροφοριακών συστημάτων.

Στο πρώτο κεφάλαιο αναφέρονται οι βασικές έννοιες για τα τοπικά δίκτυα και τα πληροφοριακά συστήματα. Δίνονται ορισμοί και αναλύονται κάποια βασικά χαρακτηριστικά τους.

Το δεύτερο κεφάλαιο αφιερώθηκε στην ασφάλεια, δηλαδή δίνονται κάποιοι ορισμοί για την ασφάλεια, αναφέρονται οι τρόποι παραβίασης των δικτύων και ποιοί είναι οι τρόποι αντιμετώπισης. Ακόμη σ' αυτό το κεφάλαιο συμπεριλήφθησαν οι χάκερ και η σχέση των Ελλήνων με το χάκινγκ, όπως και το ηθικό χάκινγκ (ethical hacking).

Το τρίτο κεφάλαιο περιλαμβάνει την μεθοδολογία της έρευνας. Είναι το κεφάλαιο που ξεκινάει η έρευνα. Σ' αυτό παραθέτεται το ερωτηματολόγιο που χρησιμοποιήθηκε για την έρευνα, όπως και κάποιες παρατηρήσεις.

Στο τέταρτο κεφάλαιο αναλύονται τα αποτελέσματα της έρευνας. Εξετάζεται κάθε ερώτηση ξεχωριστά και αναλύεται σε διάγραμμα.

Και τέλος υπάρχουν τα συμπεράσματα, δηλαδή γίνεται μια σύγκριση των αποτελεσμάτων με τη θεωρία και αναφέρεται τι ισχύει στις σημερινές μικρομεσαίες επιχειρήσεις.

Στο τέλος της πτυχιακής παρέχεται η σχετιζόμενη με τα θέματα του κειμένου βιβλιογραφία. Σ' αυτή συμπεριλήφθησαν όλες οι πηγές από τις οποίες "αντλήθηκαν" στοιχεία και πληροφορίες.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Τη σημερινή εποχή το διαδίκτυο και οι υπολογιστές είναι πια αναπόσπαστο κομμάτι της ζωής μας. Το διαδίκτυο μέρα με τη μέρα μπαίνει όλο και περισσότερο στην καθημερινότητα μας. Το διαδίκτυο χρησιμοποιείται από όλους αλλά πολύ περισσότερο από τις επιχειρήσεις. Το διαδίκτυο είναι ένα απαραίτητο εργαλείο για κάθε είδους εργασία και ειδικά για τις επιχειρήσεις. Σε λίγο καιρό οι ιδιώτες θα τακτοποιούν τις δουλειές τους με το δημόσιο μέσω διαδικτύου.

Οι επιχειρήσεις με τη βοήθεια του διαδικτύου μπορούν να επικοινωνούν εύκολα και γρήγορα με τους πελάτες τους μέσω e-mail. Επίσης αν διαθέτουν εταιρική ιστοσελίδα αυτό τις βοηθάει ώστε να γίνουν γνωστά τα προϊόντα τους στο καταναλωτικό κοινό και να διαφημιστεί η επιχείρηση τους. Βέβαια υπάρχουν και άλλοι λόγοι για τους οποίους μια επιχείρηση χρησιμοποιεί το διαδίκτυο όπως συναλλαγές με το δημόσιο, επικοινωνία και οικονομικές συναλλαγές με τράπεζες και με ιδιώτες.

Οι επιχειρήσεις επεξεργάζονται μεγάλο όγκο πληροφοριών και πολλές από αυτές διαθέτουν on-line προγράμματα. Όταν κάποια επιχείρηση διαθέτει on-line πρόγραμμα έχει τη δυνατότητα να ξέρει ανά πάσα στιγμή τι συμβαίνει στην επιχείρηση. Για παράδειγμα από την ποσότητα των προϊόντων που διαθέτει η επιχείρηση ή η αποθήκη μέχρι ποιος πελάτης χρωστάει και πόσα. Αυτά τα on-line προγράμματα βοηθούν στην ομαλή λειτουργία της επιχείρησης και κάλο θα ήταν να υπάρχουν σε κάθε επιχείρηση ανεξαρτήτου μεγέθους (μικρή ή μεγάλη επιχείρηση).

Συχνά οι εργαζόμενοι χρειάζεται να ανταλλάσουν δεδομένα μεταξύ τους ή να χρησιμοποιούν παράλληλα τις ίδιες πληροφορίες και ο πιο γρήγορος τρόπος είναι η αποστολή δεδομένων μέσω του δικτύου ή του διαδικτύου. Για αυτό το λόγο οι περισσότερες επιχειρήσεις δημιουργούν τοπικά δίκτυα για την καλύτερη και αποδοτικότερη συνεργασία των εργαζομένων τους.

Το διαδίκτυο όμως δεν είναι ασφαλές γιατί υπάρχουν hackers και crackers οι οποίοι προσπαθούν να δουν αρχεία, να διαγράψουν αρχεία ακόμη και να κλέψουν προσωπικά δεδομένα, για όλους αυτούς τους λόγους πρέπει να είναι ιδιαίτερα προσεκτικοί στην χρήση του διαδικτύου και να χρησιμοποιούν προγράμματα ασφαλείας. Οι επιχειρήσεις πρέπει να χρησιμοποιούν πολιτικές ασφαλείας ώστε τα δεδομένα και οι πληροφορίες τους να προστατεύονται μέσα στο διαδίκτυο άλλα και από αυτό.

Η ασφάλεια των δεδομένων πρέπει να αποτελεί σημαντικό παράγοντα για κάθε επιχείρηση και πρέπει να χρησιμοποιούν εξελιγμένους τρόπους ασφαλείας για να προστατέψουν τα δεδομένα τους.

ΚΕΦΑΛΑΙΟ 1

1.1 ΤΟΠΙΚΑ ΔΙΚΤΥΑ

Τα τοπικά δίκτυα είναι ένα σύνολο υπολογιστών που είναι συνδεδεμένοι μεταξύ τους και μπορούν να ανταλλάσσουν και να μοιράζονται πληροφορίες και να κάνουν χρήση κοινών περιφερειακών μηχανημάτων (όπως εκτυπωτές laser, modem και μηχανήματα fax κ.α.) με γρήγορο, εύκολο τρόπο και με μικρότερο οικονομικό κόστος.

Παρακάτω δίνονται κάποιοι ορισμοί από άλλους συγγραφείς:

«Ένα τοπικό δίκτυο είναι ένα δομημένο δίκτυο υπολογιστών συνδεδεμένων σ' ένα σαφώς καθορισμένο σύστημα που εκτείνεται σε μια τοπική περιοχή που επιτρέπει στους χρήστες την ανταλλαγή εγγράφων, προγραμμάτων, εκτυπωτών και Διαδικτυακών συνδέσεων μέσω υπολογιστών. Μπορεί να περιλαμβάνει πόρους λογισμικού και υλικού και επιτρέπει στους υπολογιστές του δικτύου να κάνουν βέλτιστη χρήση των κοινών πόρων». (1. Annarella Perra, 2010)

«Δίκτυο καλείται μια ομάδα υπολογιστών οι οποίοι είναι συνδεδεμένοι μεταξύ τους, ενσύρματα ή ασύρματα, με σκοπό την ανταλλαγή δεδομένων ή την κοινή χρήση συσκευών. Όταν η εν λόγω ομάδα απαρτίζεται από μικρό αριθμό υπολογιστών που βρίσκονται σε διάμετρο μερικών μέτρων (λ.χ. σε μια μικρή επιχείρηση, σε ένα γραφείο κ.λπ.) τότε κάνουμε λόγο για ένα δίκτυο τοπικής εμβέλειας LAN (Local Area Network)». (2. Άγνωστος, 2010)

1.1.1 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ

Στις σύγχρονες επιχειρήσεις οι πληροφορίες που διακινούνται στο τοπικό της δίκτυο καταλαμβάνουν μεγάλο όγκο. Αυτό σημαίνει ότι για να λειτουργεί η επιχείρηση αποτελεσματικά πρέπει οι υπολογιστικοί πόροι που παρέχονται να είναι επαρκής. Από την πλευρά της διαχείρισης και της λειτουργίας τα χαρακτηριστικά του τοπικού δικτύου είναι τα εξής:

1) Κοινοχρησία των διαθέσιμων υπολογιστικών πόρων: Όλοι οι χρήστες του τοπικού δικτύου έχουν πρόσβαση στους υπολογιστικούς πόρους και στις πληροφορίες, εκτός από τις περιπτώσεις που αφορούν θέματα ασφαλείας και μυστικότητας (εμπιστευτικότητα). Η κοινοχρησία των διαθέσιμων υπολογιστών αξιοποιούν αποτελεσματικά και εξοικονομούν χρήματα.
2) Χωροταξική κατανομή των διαθέσιμων υπολογιστών και πληροφοριών κοντά στους χώρους εργασίας του προσωπικού: Με αυτό τον τρόπο οι χρήστες μπορούν να έχουν πιο γρήγορη πρόσβαση στις πληροφορίες που χρησιμοποιούν πιο συχνά, όπως και τα δεδομένα που αφορούν αποκλειστικά ή χρησιμοποιούνται πιο συχνά από συγκεκριμένο τμήμα.
3) Επικάλυψη των διαθέσιμων υπολογιστών και δεδομένων: Για λόγους αύξησης της διαθεσιμότητας και αποτελεσματικής απόδοσης των

υπολογιστικών πόρων η επένδυση αυτή είναι θετική.

1.1.2 ΤΟΠΟΛΟΓΙΕΣ

«Τοπολογία ενός δικτύου ονομάζεται το γεωμετρικό πρότυπο κατά το οποίο συνδέονται οι κόμβοι μεταξύ τους.» (3. Γ. Βασιλακόπουλος –Β. Χρυσικόπουλος, 1990)

Κάθε τοπικό δίκτυο εκτός από τους κόμβους (υπολογιστές) έχει και έναν υπηρέτη δικτύου δηλ. έναν υπολογιστή που ελέγχει τις πληροφορίες μεταξύ των υπολογιστών και των άλλων συσκευών που συνδέονται. Ακόμη αποθηκεύει τα περισσότερα αρχεία, δεδομένα και προγράμματα που είναι εύκολα να τα προσεγγίσουν οι χρήστες του τοπικού δικτύου. (4. Tilton –Jackson-Rigby, 2001)

Γενικά οι τοπολογίες των δικτύων που συνδέονται οι υπολογιστές μεταξύ τους με φυσικό τρόπο έχουν τις ακόλουθες μορφές:

1) Τοπολογία αστέρα (star): Στην τοπολογία αυτή υπάρχει ένας κεντρικός υπολογιστής μέσω του οποίου γίνονται όλες οι επικοινωνίες δηλ. δέχεται μηνύματα από τους κόμβους αποστολής και τα προωθεί στους κόμβους προορισμού. Σ’ αυτήν την τοπολογία ο κεντρικός υπολογιστής έχει τον έλεγχο των επικοινωνιών του δικτύου.
2) Τοπολογία διαδρόμου (bus): Στα δίκτυα διαδρόμου όλοι οι υπολογιστές του δικτύου συνδέονται πάνω σε μια κοινή ευθύγραμμη γραμμή (καλώδιο) με ανοικτά άκρα. Η γραμμή αυτή επικοινωνίας αποτελεί το μέσο επικοινωνίας και μεταφοράς μηνυμάτων. Στην τοπολογία αυτή μπορεί να δημιουργηθεί και μια επέκτασή της, η τοπολογία bus/tree όπου από την κοινή γραμμή διακλαδίζονται γραμμές και δημιουργούν μικρότερες τοπολογίες bus.
3) Τοπολογία δακτυλίου (ring): Στην τοπολογία δακτυλίου όλοι οι υπολογιστές συνδέονται με ένα καλώδιο που τα άκρα του είναι ενωμένα μεταξύ τους, σχηματίζοντας ένα δακτύλιο. Τα δεδομένα κινούνται σειριακά σε όλο τον δακτύλιο, από κόμβο σε κόμβο. Σ’ αυτήν την τοπολογία κάθε υπολογιστής χρησιμοποιείται ως αναμεταδότης (repeater) επανεκπέμποντας τα δεδομένα προς τον επόμενο υπολογιστή.
4) Μεικτή τοπολογία: Η μεικτή τοπολογία μπορεί να δημιουργηθεί από το συνδυασμό των παραπάνω τοπολογιών δηλ. σ’ ένα δίκτυο υπολογιστών να υπάρχουν συνδεδεμένα υποδίκτυα που χρησιμοποιούν μερικές από τις παραπάνω τοπολογίες.

Ο συνδυασμός τέτοιων τοπολογιών δικτύων ονομάζονται υβριδικές και στόχο έχουν την επίτευξη των πλεονεκτημάτων των συνιστωσών τοπολογιών. (5. Γ. Βασιλακόπουλος –Β. Χρυσικόπουλος, 1990)

Υπάρχουν ακόμη δύο λογικές τοπολογίες που καθορίζονται από τη σύνθεση και αποστολή της πληροφορίας, αυτές οι λογικές τοπολογίες είναι η τοπολογία Ethernet και η Token Ring.

1) Τοπολογία Ethernet: Στην τοπολογία Ethernet χρησιμοποιείται ως μέσο μετάδοσης των πληροφοριών ένα ομοαξονικό καλώδιο και επάνω σ' αυτό βρίσκονται τοποθετημένοι οι υπολογιστές και έχουν την δυνατότητα να εκπέμπουν, να παραλαμβάνουν και να παρακολουθούν το δίκτυο.
2) Τοπολογία Token Ring: Η τοπολογία αυτή είναι μια παραλλαγή της τοπολογίας δακτυλίου (ring). Οι υπολογιστές ενώνονται σ' ένα δακτύλιο και η επικοινωνία μεταξύ τους γίνεται μέσω της διάδοσης του σήματος που συμμετέχουν ενεργά αφού διαθέτουν και δέκτη και πομπό.

Ο σχεδιασμός ενός δικτύου είναι πολύπλοκο έργο αλλά στις σύγχρονες επιχειρήσεις πρέπει να παρέχουν επαρκείς υπολογιστικούς πόρους. Συνεπώς, τα τοπικά δίκτυα υπολογιστών δημιουργούν το κατάλληλο τεχνολογικό υποστήριγμα για την δραστική λειτουργία της επιχείρησης.

1.1.3 ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ

Με την δημιουργία των τοπικών δικτύων που αναπτύχθηκαν με την ενσύρματη σύνδεση παράλληλα υπήρχε και η προσπάθεια για την ανάπτυξη των ασύρματων τοπικών δικτύων.

Τα ασύρματα τοπικά δίκτυα έχουν αλλάξει τον τρόπο επικοινωνίας προσφέροντας λύσεις που θα γίνουν πιο αποδοτικές και θα βελτιώσουν την επικοινωνία, η οποία θα γίνεται πιο άμεση, παρέχει κάλυψη χωρίς περιορισμούς, η επέκταση είναι εύκολη και με αμελητέο κόστος.

Ένα ασύρματο τοπικό δίκτυο μπορεί να χρησιμοποιηθεί από μια επιχείρηση επειδή επιτρέπει τη σύνδεση και την επικοινωνία των υπολογιστών χωρίς καλώδια αλλά με τη χρήση ραδιοκυμάτων.

Τα ασύρματα δίκτυα επιτρέπουν στους εργαζόμενους μιας επιχείρησης να εργάζονται και σε άλλους χώρους, εκτός γραφείου. Οι εργαζόμενοι θα μπορούν να επικοινωνούν με τους συναδέλφους, τους πελάτες και τους συνεργάτες τους. Οι επιχειρήσεις μπορούν να επωφεληθούν από τα ασύρματα δίκτυα με τους εξής τρόπους: (6. Γ. Γεωργίου, 2010)

1) Αυξημένη φορητότητα και συνεργασία: Οι εργαζόμενοι μπορούν να μετακινούνται στο γραφείο τους και σε άλλους χώρους της επιχείρησης και να διατηρείται η σύνδεση τους ώστε να μπορούν να συνεργαστούν πιο αποτελεσματικά.
2) Αυξημένη ανταπόκριση: Με τη βοήθεια των ασύρματων δικτύων οι πελάτες μπορούν να εξυπηρετηθούν όταν ο αρμόδιος εργαζόμενος δεν είναι στο γραφείο του διότι μπορεί να έχει πρόσβαση στις πληροφορίες που χρειάζεται, τη στιγμή που τις χρειάζεται.
3) Καλύτερη πρόσβαση σε πληροφορίες: Τα ασύρματα δίκτυα προσφέρουν σύνδεση σε σημεία που είναι δυσπρόσιτα να συνδεθούν με ενσύρματο

δίκτυο, όπως για παράδειγμα σε μια αποθήκη και με αυτό τον τρόπο βελτιώνονται οι επιχειρησιακές διαδικασίες.

4) Ευκολότερη επέκταση δικτύου: Τα ασύρματα δίκτυα εξυπηρετούν τις επιχειρήσεις που ανακατατάσσουν τα γραφεία τους και που προσλαμβάνουν νέο προσωπικό προσθέτοντας γρήγορα τους νέους χρήστες στο ασύρματο δίκτυο και χωρίς την σύγχυση που προκαλούν τα ενσύρματα δίκτυα (καλώδια).
5) Βελτιωμένη πρόσβαση επισκεπτών: Η επιχείρηση προσφέρει σε πελάτες και επιχειρησιακούς συνεργάτες, που επισκέπτονται το δίκτυο πρόσβαση υψηλής ασφαλείας στο Internet και σε κάποιες επιχειρήσεις μπορούν να προσφέρουν την πρόσβαση στο Internet ως υπηρεσία προστιθέμενης αξίας.

Συνοψίζοντας, τα ασύρματα δίκτυα μπορούν να αυξήσουν την παραγωγικότητα μιας επιχείρησης αφού είναι εύκολα στην χρήση τους, οι εργαζόμενοι είναι συνδεδεμένοι στο δίκτυο και όταν δεν είναι στο γραφείο τους, παρέχει εύκολη πρόσβαση και χρήση των πληροφοριών, εύκολη ρύθμιση αφού δεν υπάρχουν καλώδια, υπάρχει δυνατότητα κλιμάκωσης εφόσον οι επιχειρηματικές δραστηριότητες αυξάνονται, υπάρχει ασφάλεια πρόσβασης στο ασύρματο δίκτυο και το κόστος είναι μικρότερο σε σχέση με το κόστος ενός ενσύρματου δικτύου.

1.2 ΤΙ ΕΙΝΑΙ ΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Στο κεφάλαιο αυτό αναλύονται περαιτέρω τα πληροφοριακά συστήματα, τι είναι πληροφοριακό σύστημα, ποια η χρησιμότητα τους για μια μικρομεσαία επιχείρηση και ποια οφέλη προσφέρουν σε αυτήν.

Υπάρχουν πολλοί ορισμοί διαφόρων συγγραφέων για τα πληροφοριακά συστήματα που έχουν ως σκοπό να κατανοήσουν καλύτερα τι είναι ένα πληροφοριακό σύστημα.

Ένα πληροφοριακό σύστημα μπορεί να είναι χειρόγραφο ή μηχανογραφικό, είτε είναι το ένα είτε είναι το άλλο αποτελείται από κάποια στοιχεία τα οποία είναι τα εξής:

1) Η συλλογή δεδομένων που μπορεί να περιέχει αριθμούς, γεγονότα, συζητήσεις, διαδόσεις.
2) Η αποθήκευση των δεδομένων σε αρχεία του Η/Υ ή σε τράπεζα δεδομένων.
3) Η επεξεργασία των δεδομένων αποτελείται από την ανάλυση, κωδικοποίηση, ταξινόμηση και σύνθεση των δεδομένων.
4) Η παρουσίαση της πληροφορίας γίνεται σε μια μορφή η οποία είναι κατανοητή στο χρήστη. (7. Γ. Οικονόμου-Ν. Γεωργοπούλου, 2004)

Σύμφωνα με το Γ. Βασιλάκοπουλο-Β. Χρυσικόπουλο και στο βιβλίο τους Πληροφοριακά Συστήματα Διοίκησης Ανάλυση και Σχεδιασμός αναφέρουν πως :

«Πληροφοριακό σύστημα διοίκησης είναι ένα ολοκληρωμένο σύστημα χρήστη-μηχανής με σκοπό την υποστήριξη των διοικητικών και λειτουργικών δραστηριοτήτων και διαδικασιών λήψης αποφάσεων σε έναν οργανισμό.» (8. Γ.Βασιλακόπουλος- Β.Χρισικόπουλος, 1990)

Όμως σύμφωνα με τους Γ. Οικονόμου – Ν. Γεωργοπούλου και στο βιβλίο τους Πληροφοριακά Συστήματα για την Διοίκηση των Επιχειρήσεων αναφέρουν πως:

«Το πληροφοριακό σύστημα είναι 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.» (9. Γ.Οικονόμου- Ν. Γεωργοπούλου, 2004)

Επίσης ένας άλλος ορισμός εξίσου σημαντικός είναι ο παρακάτω:

«Πληροφοριακό Σύστημα είναι το μέσο για τη συνεργασία μεταξύ ανθρώπινου δυναμικού, δεδομένων, διαδικασιών, δικτύων υπολογιστών και της τεχνολογίας της πληροφορικής. Αυτή η συνεργασία αποσκοπεί στην υποστήριξη και βελτίωση
καθημερινών λειτουργιών σε επιχειρήσεις, καθώς επίσης και για την υποστήριξη για λύσεις προβλημάτων και για ανάγκες λήψης αποφάσεων.» (10. Ε. Χρίστος-Ε. Ανδρέας, 2003)

1.2.1 ΣΥΣΤΑΤΙΚΑ ΜΕΡΗ ΕΝΟΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Τα συστατικά μέρη ενός πληροφοριακού συστήματος είναι τα εξής: (11. Α.Τσακαλίδης – Δρ.Β.Βασιλειάδης, 2010)

1) Εξοπλισμός υλικό (Hardware)
2) Λογισμικό (Software)
3) Δεδομένα (Data)
4) Ανθρώπινο δυναμικό (Users)
5) Διαδικασίες
6) Δίκτυο (Network)

ΑΝΑΛΥΣΗ (12. Ι.Παπουτσής, 2002)

1) Το hardware είναι ο υπολογιστής, οι περιφερειακές συσκευές και γενικά ο υλικός εξοπλισμός.

2) Το software είναι το λογισμικό, δηλαδή το πρόγραμμα λειτουργίας και διαχείρισης εξοπλισμού και υποστήριξης επιχειρησιακών λειτουργιών.

3) Οι users είναι οι χρήστες, δηλαδή οι άνθρωποι που διαχειρίζονται το πληροφοριακό αυτό σύστημα. Οι χρήστες μπορούν να εισάγουν στοιχεία, να εκτελούν διαδικασίες και να ελέγχουν τα αποτελέσματα.

4) Τα στοιχεία (Data) είναι οι εγγραφές, τα αρχεία, οι πίνακες,

οι κατάλογοι και οι πληροφορίες που περιγράφουν την υπόσταση και τις δραστηριότητες σε μια οντότητα.

5) Τέλος, οι διαδικασίες είναι ένα σύνολο από κανόνες και πολιτικές οι οποίες βοηθούν στην επιτυχία της βέλτιστης λειτουργίας της επεξεργασίας των δεδομένων.

Ένα πληροφοριακό σύστημα αποτελείται από δεδομένα (Data) και πληροφορίες (Information). Τα δεδομένα είναι εισροές και οι πληροφορίες εκροές ενός πληροφοριακού συστήματος.

Δεδομένα είναι τα στοιχεία τα οποία τα έχουν συλλέξει από διάφορες πηγές μέσα και έξω από την επιχείρηση και τα οποία περιγράφουν γεγονότα, πράγματα, πρόσωπα και ιδέες.

Τα δεδομένα έχουν κύκλο ζωής. Ο κύκλος ζωής των δεδομένων βοηθάει στην ανάπτυξη, στο σχεδιασμό και στη λειτουργία του πληροφοριακού συστήματος.

Ο κύκλος ζωής των δεδομένων αποτελείται από τα εξής:

- Δημιουργία
- Αποθήκευση
- Καταστροφή
- Μεταφορά
- Επανάκτηση
- Αναπαραγωγή
- Αξιολόγηση
- Ανάλυση
- Ταξινόμηση
- Σύνθεση
- Δημιουργία πληροφορίας

Τα δεδομένα δεν αποτελούν πληροφορία από μόνα τους χωρίς την απαραίτητη επεξεργασία και την μετατροπή τους ως πληροφορία.

Πληροφορία είναι τα επεξεργασμένα δεδομένα τα οποία αποκτούν νόημα και αξία για τον αποδέκτη, για τις αποφάσεις που παίρνει και για τις δραστηριότητες που εκτελεί.

Υπάρχει μια αλληλεξάρτηση μεταξύ των δεδομένων και των πληροφοριών, όπως της πρώτης ύλης και του έτοιμου προϊόντος.

Τα στάδια μετατροπής των δεδομένων σε πληροφορία είναι τα εξής:

- Δεδομένα
- Επεξεργασία
- Πληροφορίες

Μπορούν να κατηγοριοποιηθούν οι πληροφορίες ως εξής:

Διεθνείς: συναλλαγματικές ισοτιμίες, δημογραφικά στοιχεία κρατών.

Εθνικές: εξέλιξη του πληθωρισμού, επίπεδα απασχόλησης κ.α.

Κλάδου: παραγωγική δυναμικότητα ανταγωνιστικών επιχειρήσεων.

Επιχείρησης: προβλέψεις πωλήσεων, εκτιμήσεις κόστους προϊόντων ή υπηρεσίας.

Τμήματος : πωλήσεις και δαπάνες ενός τμήματος μιας επιχείρησης.

Ατόμου: μισθός με τις ασφαλιστικές και λοιπές κρατήσεις ενός εργαζομένου.

Οι πληροφορίες ανάλογα με το σκοπό για τον οποίο χρησιμοποιούνται μπορούν να διακριθούν σε:

Στρατηγικές πληροφορίες :

«Οι πληροφορίες αυτές αφορούν μακροπρόθεσμο προγραμματισμό της επιχείρησης και χρησιμοποιούνται κυρίως για τη λήψη στρατηγικών αποφάσεων από τα στελέχη της ανώτατης διοίκησης». Οι πληροφορίες αυτές σε εθνικό επίπεδο μπορεί να αφορούν τη διαθεσιμότητα εγχώριων πόρων, τις πληθυσμιακές τάσεις, τις ξένες επενδύσεις και τις εισαγωγές-εξαγωγές. Σε επίπεδο κλάδου και επιχειρήσεων μπορεί να αφορούν οι πληροφορίες αυτές νέες πήγες προμηθειών, επιλογή και τόπου εγκατάστασης, επιλογή μιας νέας τεχνολογίας.

Τακτικές πληροφορίες :

Οι πληροφορίες αυτές αφορούν μεσοπρόθεσμα προγράμματα της επιχείρησης, δηλαδή αυτά που διαρκούν ένα ή δύο χρόνια. Ως τακτικές πληροφορίες μπορούν να χαρακτηριστούν οι προβλέψεις ζήτησης, ο γενικός προγραμματισμός παραγωγής, η αξιολόγηση των προμηθευτών, το πρόγραμμα απασχόλησης και κατανομής του προσωπικού.

Λειτουργικές πληροφορίες :

Οι πληροφορίες αυτές αφορούν βραχυπρόθεσμα προγράμματα και έχουν περισσότερο σχέση με το λειτουργικό προγραμματισμό της επιχείρησης. Οι αποφάσεις αυτές είναι αποφάσεις ρουτίνας. Όπως ανεκτέλεστες παραγγελίες, βραχυπρόθεσμες υποχρεώσεις και απαιτήσεις κ.α.

Για να βοηθήσει μια πληροφορία τα στελέχη μιας επιχείρησης και να μειώσει την αβεβαιότητα, πρέπει η πληροφορία αυτή να έχει συγκεκριμένα χαρακτηριστικά τα οποία είναι τα έξης:

- Ακρίβεια
- Μορφή
- Συχνότητα
- Χρονικός ορίζοντας
- Έκταση
- Προέλευση

Και τα χαρακτηριστικά ενός συνόλου πληροφοριών πρέπει να είναι τα έξης: (13. Γ.Οικονόμου-Ν.Γεωργοπούλου, 2004)

1) Σχετικότητα
2) Πληρότητα
3) Επικαιρότητα

1.2.2 ΑΝΑΠΤΥΞΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

«Στη φάση της ανάπτυξης των προγραμμάτων, των εφαρμογών τα λογικά τμήματα που ορίσθηκαν στη φάση του φυσικού σχεδιασμού κωδικοποιούνται και ολοκληρώνονται μέσα στα πλαίσια του πληροφοριακού συστήματος.»

Για να γίνει η δομημένη προσέγγιση κατά την ανάπτυξη των προγραμμάτων απαιτούνται κάποιοι μέθοδοι οι οποίοι είναι οι έξης:

Top-down υλοποίηση:

Με τη χρήση μιας δομημένης τεχνικής, κωδικοποιούνται σε πρώτη φάση τα λογικά τμήματα των ανωτέρων επιπέδων.

Οι μέθοδοι δομημένου προγραμματισμού:

«Οι μέθοδοι του δομημένου προγραμματισμού αποσκοπούν στη βελτίωση της ποιότητας των προγραμμάτων, στην αύξηση της παραγωγικότητας των προγραμματιστών και στην ελάττωση των χρονικών απαιτήσεων των δοκιμών.»

Υπάρχουν τρεις απλές δομές κατασκευής προγραμμάτων, η ακολουθία, η επιλογή ή εναλλακτική διαδρομή (IF-THEN-ELSE,CASE) και η επανάληψη (DO-WHILE, DO-UNTIL, PERFORM-UNTIL). Υπάρχουν και εντολές όμως που λείπουν από το δομημένο πρόγραμμα, και οι εντολές αυτές είναι οι GO TO.

Η ιεραρχική ομάδα προγραμματιστών:

Τα υπό ανάπτυξη προγράμματα διατηρούνται σε τυποποιημένη μορφή σε μια βιβλιοθήκη, η οποία ονομάζεται βιβλιοθήκη υποστήριξης της διαδικασίας ανάπτυξης προγραμμάτων, που χρησιμοποιείται από την συγκεκριμένη ομάδα. Η ιεραρχική ομάδα προγραμματιστών χρησιμοποιεί δομημένο προγραμματισμό και στάνταρ τεχνικά πρότυπα, που την βοηθούν στην κατασκευή, δοκιμή και συγγραφή προγραμμάτων. Μια ιεραρχική ομάδα προγραμματιστών αποτελείται από ένα προϊστάμενο προγραμματιστών (chief programmer), έναν προγραμματιστή υποστήριξης (back up programmer) και ένα βιβλιοθηκάριο προγραμμάτων (librarian).

- Ο προϊστάμενος προγραμματιστών έχει αναλάβει να γράφει τα σημαντικότερα λογικά τμήματα των εφαρμογών ενός πληροφοριακού συστήματος. Επίσης έχει την εποπτεία της ομάδας του, τεχνικά και διοικητικά.
- Ο προγραμματιστής υποστήριξης έχει μια σφαιρική εικόνα του έργου και σε περιπτώσεις ανάγκης αντικαθιστά τον προϊστάμενο προγραμματιστών.
- Ο βιβλιοθηκάριος συντηρεί την βιβλιοθήκη Υποστήριξης προγραμμάτων και έχει ως σκοπό την εκτέλεση της γραφικής και τεχνικής εργασίας.

Η βιβλιοθήκη αποτελείται από τέσσερα τμήματα, το εξωτερικό τμήμα (external library), το εσωτερικό τμήμα (internal library), τις διοικητικές διαδικασίες γραφείου (office administrative proceduces) και τις διαδικασίες επικοινωνίας με το υπολογιστικό σύστημά (machine iterfaces produces).

Το εξωτερικό τμήμα περιέχει όλο το υλικό που παρήχθη από τη διαδικασία ανάπτυξης του πληροφοριακού συστήματος, ενώ αντίθετα το εσωτερικό τμήμα περιέχει όλα τα μέσα που έχουν παραχθεί από τα προγράμματα υποστήριξης και την διαδικασία ανάπτυξης των προγραμμάτων του πληροφοριακού συστήματος.

Τις διοικητικές διαδικασίες γραφείου (office administrative proceduces) : Οι διοικητικές διαδικασίες γραφείου περιλαμβάνουν τις εξής εργασίες :

⇒ Συντήρηση εσωτερικού τμήματος

⇒ Προετοιμασία εισερχόμενων στο υπολογιστικό σύστημα
⇒ Αρχειοθέτηση εξερχόμενων και εντύπων εξωτερικού τμήματος.

Τις διαδικασίες επικοινωνίας με το υπολογιστικό σύστημα (machine interfaces proceduces): Σε αυτό το τμήμα, καθορίζονται οι αναγκαίες αλληλεπιδράσεις που βοηθούν στη μεταγλώττιση και στην εκτέλεση των προγραμμάτων.

Δομημένη διαδρομή:

Ο αναλυτής παρουσιάζει τα προγράμματα που έχουν κατασκευαστεί στην ομάδα εμπειρογνωμόνων με οργανωμένο και δομημένο τρόπο. Πριν από μια παρουσίαση γίνεται η διανομή του σχετικού τεκμηριωτικού υλικού σε κάθε άτομο που θα έχει συμμέτοχη στη διαδρομή. Με τις παρουσιάσεις αυτές αποκτούν επιπλέον εκπαίδευση όλοι οι συμμετέχοντες και ο αναλυτής, αυτό έχει σαν αποτέλεσμα την αύξηση της παραγωγικότητας και της ποιότητας ολόκληρης της εργασίας. Ένα ολοκληρωμένο λογισμικό εφαρμογών και το τεκμηριωτικό υλικό ενός πληροφοριακού συστήματος είναι το αποτέλεσμα της παραπάνω διαδικασίας.

1.2.3 ΥΛΟΠΟΙΗΣΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

«Κατά τη φάση της υλοποίησης του πληροφοριακού συστήματος ολοκληρώνεται η δοκιμή του λογισμικού εφαρμογών, γίνεται η εκπαίδευση των χρηστών και εκτελείται η διαδικασία μετάβασης από το υπάρχον πληροφοριακό σύστημα στο νέο.»

Η υλοποίηση ενός πληροφοριακού συστήματος περιλαμβάνει τα παρακάτω:

1. Εγκατάσταση νέου υπολογιστικού συστήματος.
2. Εισαγωγή νέων αυτοματοποιημένων μεθόδων λειτουργίας.
3. Μετατροπή των παλιών αρχείων δεδομένων (χειρόγραφων ή αυτοματοποιημένων), σε μορφή που είναι απαραίτητη για τη λειτουργία του νέου πληροφοριακού συστήματος.

Η δοκιμή του λογισμικού εφαρμογών:

Αποτελείται από τη δημιουργία δοκιμών αποδοχής (acceptance test generation) και την ποιοτική εξασφάλιση (quality assurance). Και χωρίζεται σε δύο φάσεις. Στην πρώτη φάση γίνεται ο καθορισμός των προδιαγραφών των δοκιμών ενώ στη δεύτερη φάση γίνεται ο έλεγχος του λογισμικού εφαρμογών και του τεκμηριωτικού υλικού.

Υπάρχουν τέσσερα επίπεδα ποιοτικής εξασφάλισης :

1. Της δοκιμής (testing)
2. Της επαλήθευσης (verification)
3. Έλεγχου της σωστής λειτουργίας (validation)
4. Πιστοποίηση (certification)

(14. Γ.Βασιλακόπουλος-Β.Χρυσικόπουλος,, 1990)

1.2.4 ΕΙΔΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τα πληροφοριακά συστήματα δημιουργήθηκαν ώστε να καλύπτουν τις ανάγκες πληροφόρησης όσον αφορά την οργάνωση και την διοίκηση μιας επιχείρησης σε όλα τα επίπεδα. Υπάρχει το λειτουργικό και το διοικητικό επίπεδο. Το λειτουργικό επίπεδο έχει σχέση με τις εργασίες ρουτίνας που γίνονται καθημερινά από μια επιχείρηση, όπως για παράδειγμα τιμολόγηση, εισπράξεις, πληρωμές, μισθοδοσία και άλλα. Στο διοικητικό επίπεδο ένα πληροφοριακό σύστημα είναι απαραίτητο όσον άφορα τον έλεγχο, την καθοδήγηση και την λήψη των αποφάσεων.

Τα είδη πληροφοριακών συστημάτων που υπάρχουν είναι τα έξης:

1. Συστήματα που χρησιμοποιούνται κυρίως από το λειτουργικό επίπεδο μιας επιχείρησης και αφορούν την επεξεργασία των δοσοληψιών (Transaction Processing).
2. Τα Πληροφοριακά Συστήματα Διοίκησης - MIS (Management Information System), χρησιμοποιούνται από τα ανώτερα στελέχη μια επιχείρησης και αφορούν κυρίως την πληροφόρηση και τον έλεγχο των δραστηριοτήτων της επιχείρησης.
3. Συστήματα Υποστήριξης Αποφάσεων- DSS (Decision Support Systems), αυτά τα συστήματα βοηθούν στην επίλυση των προβλημάτων τα οποία δεν έχουν μια προκαθορισμένη λύση για να λυθούν.

Υπάρχουν επίσης πληροφοριακά συστήματα τα οποία εφαρμόζονται σε περιοχές μη κλασσικής επεξεργασίας δεδομένων τα οποία είναι τα έξης :

1. Τα Εμπειρικά Συστήματα ή Συστήματα Εμπειρογνωμόνων (Expert Systems), τα οποία αφορούν κυρίως επιστημονικές περιοχές.
2. Τα Πληροφοριακά Συστήματα Πολυμέσων, με τη βοήθεια αυτών των συστημάτων μπορούν να επεξεργαστούν δεδομένα, τα οποία μπορεί να είναι κείμενο, εικόνα, ήχος και video.
3. Τα Γεωγραφικά Πληροφοριακά Συστήματα (GIS). Τα συστήματα αυτά βοηθούν στη δημιουργία των χωροταξικών και γεωγραφικών χαρτών. (15. Ι.Παπουτσής, 2002)

1.3 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

<u>Πλεονεκτήματα και μειονεκτήματα τοπικών δικτύων</u>

Η χρήση των τοπικών δικτύων για μια επιχείρηση έχει τα πλεονεκτήματα και τα μειονεκτήματα της.

1.3.1 ΠΛΕΟΝΕΚΤΗΜΑΤΑ

Πρώτον, γίνεται πιο εύκολη η ανταλλαγή των πόρων και των δεδομένων από έναν υπολογιστή σε έναν άλλον και αυτό γίνεται δυνατό μέσα από διάφορες υπηρεσίες που προσφέρει το internet, μερικές από αυτές είναι οι εξής: (16. Ι. Βογιατζής, 2006)

1) Υπηρεσία ηλεκτρονικού ταχυδρομείου (e-mail): Το ηλεκτρονικό ταχυδρομείο είναι η πιο διαδεδομένη μέθοδος επικοινωνίας μεταξύ των χρηστών του internet και επιτρέπει στους χρήστες να στέλνουν και να λαμβάνουν μηνύματα μέσω της ηλεκτρονικής τους διεύθυνσης (e-mail address).
2) Υπηρεσία Μεταφοράς Αρχείων: Η υπηρεσία μεταφοράς αρχείων έχει ως σκοπό την διακίνηση των αρχείων από έναν υπολογιστή σε έναν άλλον επικοινωνώντας μεταξύ τους με μια κοινή γλώσσα (file transfer protocol). Στο διαδίκτυο υπάρχουν πολλές τοποθεσίες (ftp) ή (ftp sites) από τις οποίες είναι εφικτό οι χρήστες να "κατεβάσουν" και να "ανεβάσουν" αρχεία και να σταλθούν από έναν υπολογιστή σε έναν άλλον.
3) Υπηρεσία συνομιλιών με άλλους χρήστες: Η συνομιλία είναι ένας τρόπος επικοινωνίας σε πραγματικό χρόνο μεταξύ των χρηστών του internet. Το chat γίνεται με την πληκτρολόγηση κειμένου και δίνει την δυνατότητα της εύκολης ανταλλαγής μηνυμάτων μεταξύ των χρηστών οι οποίοι βρίσκονται σε ειδικές ομάδες συνομιλίας (chat rooms). Η υπηρεσία αυτή είναι πολύ διαδεδομένη παγκοσμίως στους χρήστες του διαδικτύου.
4) Υπηρεσία της τηλεδιάσκεψης: Με αυτήν την υπηρεσία επικοινωνούν οι χρήστες μεταξύ τους σε πραγματικό χρόνο και μοιράζονται πληροφορίες κειμένου, φωνής και εικόνας. Ακόμα μπορούν να χρησιμοποιηθούν εφαρμογές όπως είναι η τηλεδιάσκεψη και η τηλεκπαίδευση.

Επίσης άλλες υπηρεσίες που μπορεί να προσφέρει η χρήση του internet είναι οι εξής :

1) Ηλεκτρονικά ΜΜΕ
2) Τηλεφωνία
3) Τηλεομοιοτυπία (telefax ή fax)
4) Υπηρεσία videotex
5) Αλληλεπιδραστική τηλεόραση (interactive t.v)
6) Ηλεκτρονική ανταλλαγή δεδομένων (Electronic Data interchange, EDI)
7) Συστήματα εντοπισμού θέσης (Global Positioning Systems, GPS)
8) Ηλεκτρονικοί πίνακες ανακοινώσεων (Bylletin Board Systems, BBS)
9) On line υπηρεσίες

Δεύτερον, η χρήση των τοπικών δικτύων επιτρέπει την κοινή χρήση του εξοπλισμού των υπολογιστών όπως είναι οι εκτυπωτές, οι σαρωτές, οι σκληροί και οπτικοί δίσκοι κ.α. (17. Άγνωστος, 2010)

Τρίτον, ένα σημαντικό πλεονέκτημα είναι η εξοικονόμηση εργατοωρών για τους εργαζομένους και η μείωση του λειτουργικού κόστους της επιχείρησης .

Αυτό έχει σαν αποτέλεσμα την αύξηση της αποδοτικότητας των υπαλλήλων, γιατί όλα γίνονται αυτόματα μέσω υπολογιστή. Έτσι εξασφαλίζεται η εξοικονόμηση κεφαλαίων και χώρου για μια επιχείρηση.

Τέταρτον, γίνεται από την επιχείρηση κοινή χρήση του λογισμικού και διαχείριση αδειών χρήσης, στα εργαστηριακά περιβάλλοντα τα οποία λειτουργούν μέσω δικτύου. Επίσης η επιχείρηση έχει εύκολη πρόσβαση στην εξωτερική πληροφόρηση μέσω του κοινόχρηστου κόμβου και του λογισμικού.

Πέμπτον, παρέχεται η δυνατότητα ανταλλαγής δεδομένων σε άλλα απομακρυσμένα δίκτυα και υπολογιστές, με τη βοήθεια των επικοινωνιακών μέσων όπως είναι οι δρομολογητές, τα κανάλια και τα modem. Επίσης έχει εξασφαλιστεί η εγκυρότητα ανταλλαγής δεδομένων μεταξύ συστημάτων που απέχουν γεωγραφικά μεταξύ τους.

Έκτον, παρέχεται η δυνατότητα του εύκολου ελέγχου των συνδέσεων των χρηστών και όλων των κοινόχρηστων πόρων. Ο διαχειριστής του δικτύου (network administrator), με ειδικό λογισμικό μπορεί να κατευθύνει τις προσβάσεις των χρηστών και τα δικαιώματα τους και έχει ως μέλημα τη σωστή λειτουργία του δικτυακού περιβάλλοντος.

Έβδομον, με την ύπαρξη των αντιγράφων ασφαλείας και των αποθηκευτικών μέσων επιτυγχάνεται η καταγραφή των κινήσεων των χρηστών και έτσι εξαλείφεται ο κίνδυνος να χαθούν οι πληροφορίες.

Όγδοον, μέσω των τοπικών δικτύων μπορεί να γίνει ο διαμοιρασμός μιας σύνδεσης internet σε όλους τους υπολογιστές του δικτύου. Άρα με μια μοναδική σύνδεση με το Διαδίκτυο, μπορεί να παρέχει πρόσβαση σε όλους τους υπολογιστές του δικτύου. Η δυνατότητα αυτή μειώνει το κόστος της παροχής του internet.

Ένατον, η αξιοποίηση των υπολογιστών περιορισμένων δυνατοτήτων ή παλιότερης τεχνολογίας. Μέσω των τοπικών δικτύων μπορεί να γίνει η αξιοποίηση υπολογιστών παλιότερης τεχνολογίας. (18. Ι. Βογιατζής, 2006)

Ως συμπέρασμα των παραπάνω πλεονεκτημάτων είναι πως τα τοπικά δίκτυα προσφέρουν σε μια επιχείρηση οικονομικά, οργανωτικά, λειτουργικά και χωροταξικά οφέλη.

1.3.2 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΑΣΥΡΜΑΤΩΝ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ

(19. Κ. Γεωργακόπουλος, 2007)

Ευκολία χρήσης: Σήμερα όλοι μπορούν να έχουν πρόσβαση στο internet μέσω των φορητών υπολογιστών και των κινητών τηλεφώνων τους. Τα κινητά τηλέφωνα έχουν υψηλή τεχνολογία και προσφέρουν υψηλές δυνατότητες στους χρήστες τους.
Φορητότητα: Για παράδειγμα, οι συμμετέχοντες σε συσκέψεις έχουν την δυνατότητα να έχουν πρόσβαση στα έγγραφα και τις εφαρμογές τους, μέσω των ασύρματων δικτύων.
Παραγωγικότητα: Μέσα από την πρόσβαση των υπαλλήλων μιας εταιρίας στο

internet καθώς και από τους πελάτες, συνεργάτες και προμηθευτές έχει σαν αποτέλεσμα την γρήγορη διεκπεραίωση των εργασιών και την ενθάρρυνση για συνεργασία μεταξύ των εργαζομένων μιας εταιρίας.
Εύκολη ρύθμιση: Λόγω του γεγονότος του ότι δεν απαιτούνται καλώδια για τη σύνδεση τους, άρα η εγκατάσταση των ασύρματων δικτύων μπορεί να ολοκληρωθεί γρήγορα και οικονομικά.
Δυνατότητα κλιμάκωσης: Τα ασύρματα δίκτυα έχουν την δυνατότητα να επεκταθούν με τον υπάρχοντα εξοπλισμό.
Ασφάλεια: Τα δεδομένα και οι πληροφορίες μπορούν να είναι προσβάσιμα μόνο στους χρήστες που επιτρέπεται η πρόσβαση.
Κόστος: Η οικονομικότερη λύση, η χρήση ασύρματου δικτύου γιατί εξαλείφει ή μειώνει το κόστος καλωδίωσης σε περίπτωση μετακόμισης ή επέκτασης γραφείων.

1.3.3 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΑΣΥΡΜΑΤΩΝ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ

Εκτός από τα πολλά πλεονεκτήματα που προσφέρουν τα τοπικά δίκτυα, υπάρχουν όμως και μερικά μειονεκτήματα τα οποία σχετίζονται περισσότερο με την ασφάλεια των δικτύων αυτών. Αυτά χωρίζονται σε τρεις κατηγορίες:

1) Ταχύτητα: η ταχύτητα στηρίζεται στο πρωτόκολλο που έχει επιλεγεί αλλά δεν είναι το ίδιο σταθερή όπως στα ενσύρματα δίκτυα.
2) Κόστος: το κόστος ενός ασύρματου δικτύου μπορεί να είναι ένας λόγος που δεν ανταποκρίνεται στις ανάγκες μας, παρότι οι τιμές είναι πιο προσιτές για τους καταναλωτές, παραμένουν όμως ακόμη ακριβές.
3) Ασφάλεια: η ασφάλεια είναι ένας σημαντικός παράγοντας. Δίκτυα που δεν είναι σωστά εγκατεστημένα ή που έχουν χαμηλή ασφάλεια, μπορούν εύκολα να παραβιαστούν από τρίτους, άτομα που είναι ειδικά για τις παραβιάσεις (π.χ. χάκερ). (20. Γ. Γεωργίου, 2010)

Τα μειονεκτήματα όσον άφορα την ασφάλεια μπορούν να εξαλειφθούν με:

1) Πιστοποίηση χρήστη
2) Κρυπτογράφηση των δεδομένων.
3) Έλεγχος ταυτότητας χρηστών
4) Πρόσβαση υψηλής ασφαλείας για επισκέπτες και εξωτερικούς χρήστες.
5) Συστήματα ελέγχου (21. Άγνωστος, 2010)

1.4 ΠΩΣ ΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ ΚΑΙ ΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΩΦΕΛΟΥΝ ΜΙΑ ΕΠΙΧΕΙΡΗΣΗ

Στις σύγχρονες επιχειρήσεις χρησιμοποιούν και σύγχρονες μεθόδους διοίκησης και οργάνωσης, με τη βοήθεια της τεχνολογίας είναι πλέον πιο εύκολη. Οι εργαζόμενοι αναλαμβάνουν συγκεκριμένες αρμοδιότητες σε κάθε τμήμα, ακόμη κι αν το τμήμα αυτό αποτελείται από ένα άτομο. Η επιχείρηση θα

έχει αποκτήσει αποτελεσματικές λειτουργικές δομές και θα αυξήσει την εταιρική της ισχύ στην αγορά.

Τα δίκτυα και το Internet εξυπηρετούν και μικρομεσαίες επιχειρήσεις και όχι μόνο βιομηχανίες και μεγάλες επιχειρήσεις. Οι μικρομεσαίες επιχειρήσεις είναι δύσκολο να επιβιώσουν πόσο μάλλον να είναι επικερδείς. Η τεχνολογία όμως βοηθά τον ανταγωνισμό προκειμένου μια επιχείρηση να αντεπεξέλθει στις προκλήσεις της σημερινής εποχής. Ακόμη με τη βοήθεια on line συστημάτων, ενισχύεται η εικόνα της επιχείρησης και συμβάλλουν στην εύρυθμη λειτουργία της. (22. Άγνωστος, 2010)

Αν όμως η επιχείρηση δεν υπολογίσει την τεχνολογία και την συμβολή της, τότε χάνει έναν παράγοντα που θα την βοηθούσε στην διεύρυνση των αγορών της. Οι επιχειρήσεις που συνδυάζουν την τεχνολογία με τη στρατηγική τους, αποσκοπούν σε υψηλά οικονομικά οφέλη (κέρδη), αυτό θεωρείται πλεονέκτημα για την επιχείρηση. Είναι όμως δυνατόν το πλεονέκτημα αυτό να γίνει ανταγωνιστικό μειονέκτημα και αυτό συμβαίνει όταν μπορούν να το αντιγράψουν με ευκολία. Για να αποκτήσει μια επιχείρηση ανταγωνιστικό πλεονέκτημα πρέπει να παρέχει στους αγοραστές μεγαλύτερη αξία σε σχέση με τους ανταγωνιστές της ή ίδια αξία με τους ανταγωνιστές της σε μικρότερο κόστος, σε αυτό μπορεί ένα πληροφοριακό σύστημα να έχει στρατηγική επίδραση. Είναι σαφές ότι οι επιχειρήσεις προσπαθούν να διατηρήσουν τα πλεονεκτήματα που έχουν αποκτήσει και έχει συμβάλλει και η πληροφοριακή τεχνολογία. Τα περισσότερα στελέχη των επιχειρήσεων προσέχουν και παρατηρούν μόνο τις τεχνολογίες του κλάδου τους και δεν παρατηρούν τις νέες τεχνολογίες των υπολογιστών και των τηλεπικοινωνιών που μπορούν να επηρεάσουν όλες τις επιχειρήσεις. (23. Γ.Οικονόμου-Ν.Γεωργόπουλου,2004)

Οι μικρομεσαίες επιχειρήσεις αλλά και μεγαλύτερες έχουν ανάγκη για τη μετάδοση φωνής και δεδομένων, γι’ αυτό δημιουργήθηκε η υπηρεσία Voice over IP (VoIP) - μετάδοση φωνής μέσω του πρωτοκόλλου TCP/IP. Πρόκειται για μια υπηρεσία που μετατρέπει τη φωνή σε πακέτα δεδομένων. Η υπηρεσία VoIP έχει και πρόσθετες εφαρμογές και υπηρεσίες που μπορούν να βοηθήσουν μια επιχείρηση, διότι μέσω του διαδικτύου μπορούν να στέλνουν και να δέχονται ψηφιακά μηνύματα φωνής, να κάνουν και να δέχονται κλήσεις στον υπολογιστή όπως και να στέλνουν γραπτά μηνύματα σε κινητά τηλέφωνα, να κάνουν τηλεδιασκέψεις, να έχουν web phone δηλ. να μπορούν να ανταλλάζουν δεδομένα ήχου, εικόνας, video και κειμένου. (24. Άγνωστος, 2010)

Πολλές εταιρείες τηλεπικοινωνιών και στην Ελλάδα και στην Ευρώπη επενδύουν στο Voice over IP. Στο εξωτερικό η υπηρεσία είναι ευρέως διαδεδομένη. Τα επόμενα χρόνια περιμένουν ότι θα σημειωθεί υψηλή ανάπτυξη της φωνής και θα υπάρχει μεγάλος όγκος κίνησης σε σχέση με την παραδοσιακή τηλεφωνία.

ΚΕΦΑΛΑΙΟ 2

2.1 ΑΣΦΑΛΕΙΑ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

«Ασφάλεια υπολογιστών, είναι η προστασία των προσωπικών ή εμπιστευτικών πληροφοριών και των πόρων του υπολογιστή από άτομα ή οργανισμούς που θα μπορούσαν να τα χρησιμοποιήσουν ή να τα ανακοινώσουν σε άλλους με κακόβουλο τρόπο.» (25. Κ. Γαβριλάκη, 2009)

Η έννοια της ασφάλειας θα πρέπει να απασχολήσει μια επιχείρηση διότι η συλλογή και η διαχείριση πληροφοριών είναι από τους πιο σημαντικούς πόρους μιας επιχείρησης και τα δεδομένα και οι εφαρμογές που χρησιμοποιούν πρέπει να παραμένουν ασφαλείς.

Η ασφάλεια των υπολογιστών και των δικτύων πρέπει να καλύπτουν τις εξής απαιτήσεις: (26. Ι. Ασκοξυλάκης, 2008)

1) Μυστικότητα: Την πληροφορία πρέπει να την προσεγγίζουν μόνο εξουσιοδοτημένοι χρήστες.
2) Ακεραιότητα: Τα δεδομένα και οι διαδικασίες (οι πόροι) του συστήματος μπορούν να τροποποιήσουν μόνο οι εξουσιοδοτημένοι χρήστες.
3) Διαθεσιμότητα: Απαιτείται διαθεσιμότητα των συστημάτων και της πληροφορίας μόνο σε εξουσιοδοτημένους χρήστες ώστε η επιχείρηση να λειτουργεί παρά τις τυχόν διαταραχές (φυσικές καταστροφές, διακοπή τροφοδοσίας, επιθέσεις).

Η περίπτωση απώλειας δεδομένων μπορεί να βλάψει ανεπανόρθωτα την επιχείρηση, όχι μόνο στην ανταγωνιστικότητα και στα κέρδη αλλά και στο εμπορικό της όνομα και τη φήμη της. Οπότε στην παραβίαση της ασφαλείας οι υπεύθυνοι πρέπει να δίνουν μεγάλη σημασία και να την επιβλέπουν.

2.2 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

Τα πλεονεκτήματα που προσφέρει η ασφάλεια είναι τα εξής :

1. Έλεγχος των χρηστών : Με την βοήθεια της ασφαλείας μπορεί να γίνει ο έλεγχος των χρηστών που έχουν πρόσβαση στα δεδομένα και στα αρχεία της επιχείρησης. Με αυτόν τον τρόπο μπορεί ο υπεύθυνος της επιχείρησης να ελέγχει και να ενημερώνεται για το ποιες ιστοσελίδες επισκέπτεται ο κάθε εργαζόμενος της επιχείρησης.
2. Έλεγχος πρόσβασης: Πρέπει η κάθε επιχείρηση να έχει κωδικούς πρόσβασης στα δεδομένα και στα αρχεία της. Όπως επίσης και ο κάθε εργαζόμενος πρέπει να διαθέτει τον δικό του κωδικό πρόσβασης και αυτόν τον κωδικό πρέπει να τον αλλάζει συχνά.

3. Αξιοπιστία δεδομένων: Τα δεδομένα τα οποία λαμβάνουν και στέλνουν πρέπει να είναι αξιόπιστα και προστατευμένα, δηλαδή να μην περιέχουν κάποιου είδους ιό.
4. Διαθεσιμότητα συστήματος: Τα αρχεία και τα δεδομένα της επιχείρησης πρέπει να είναι διαθέσιμα μόνο στους εργαζομένους της επιχείρησης και όχι σε άλλους χρήστες.

Εκτός από τα πλεονεκτήματα που προσφέρει η ασφάλεια, υπάρχουν και μειονεκτήματα τα οποία είναι τα εξής :

1. Περιορίζεται ο χρήστης όσον αφορά την ασφάλεια στη χρήση του Η/Υ: Οι εργαζόμενοι πρέπει να χρησιμοποιούν το διαδίκτυο μόνο για την εργασία τους και όχι για προσωπικούς λόγους.
2. Μπλοκάρισμα των ιστοσελίδων: Επειδή πολλοί εργαζόμενοι στις επιχειρήσεις δεν χρησιμοποιούν το διαδίκτυο μόνο για την εργασία τους αλλά μερικοί και για την διασκέδαση τους. Για αυτό το λόγο, αλλά και για λόγους ασφαλείας οι επιχειρήσεις μπλοκάρουν ιστοσελίδες ώστε να αποφεύγονται τέτοιου είδους προβλήματα, τα οποία βέβαια περιορίζουν την ελευθερία του χρήστη.

2.3 ΕΙΔΗ ΠΑΡΑΒΙΑΣΗΣ ΑΣΦΑΛΕΙΑΣ

Τα βασικότερα είδη παραβίασης ασφαλείας ενός υπολογιστή ή ενός δικτύου είναι τα εξής: (27. Γ. Καρόπουλος, 2010)

1) Υποκλοπή επικοινωνιών: Η υποκλοπή, η αντιγραφή ή η τροποποίηση των δεδομένων μπορεί να βλάψει τόσο το άτομο στην ιδιωτική του ζωή αλλά και να αποτελέσει αντικείμενο εκμετάλλευσης δεδομένων για εμπορικό κέρδος ή δολιοφθορά.
2) Μη εξουσιοδοτημένη πρόσβαση: Η είσοδος κατά λάθος ή με δόλο γίνεται σε ελαττωματικά σημεία των δικτύων με αποτέλεσμα να μπορούν να εκμεταλλευτούν τα δεδομένα /πληροφορίες, με σκοπό να τα αντιγράψουν, να τα τροποποιήσουν ή να τα καταστρέψουν.
3) Κατάρρευση δικτύου: Οι περισσότερες επιθέσεις γίνονται επειδή βρίσκουν αδυναμίες στα στοιχεία του δικτύου. Η κατάρρευση του δικτύου δημιουργεί πρόβλημα σε κάποιες ιστοσελίδες, διότι με την απότομη διακοπή τους μπορεί να χάσουν σημαντικές πληροφορίες. Ειδικά κάποιες επιχειρήσεις που κάνουν τις συναλλαγές τους μέσω Διαδικτύου.
4) Εκτέλεση κακόβουλου λογισμικού: Σ’ αυτήν την περίπτωση η παραβίαση γίνεται από κάποιον ιό, σκουλήκι ή δούρειο ίππο και τροποποιούν ή καταστρέφουν τα δεδομένα. Ο ιός είναι ένα πρόγραμμα και μπορεί να αλλοιώσει ή να καταστρέψει το σύστημα. Ο ιός αναπαράγει τον εαυτό του με απρόβλεπτο ρυθμό και προκαλεί μια ορισμένη ενέργεια. (28.Δ.

Γιαννακόπουλος- Ι. Παπουτσής, 2003)

5) Παραπλάνηση/ψευδής δήλωση: Η παραβίαση αυτή θεωρείται ιδιαίτερα επιζήμια διότι μπορούν να δοθούν εμπιστευτικές πληροφορίες σε λάθος άτομα ή σε κάποια on line συστήματα να είναι αδύνατη η επαλήθευση της ταυτότητας.

Τέλος, η ασφάλεια των δικτύων μπορεί να κινδυνεύει από τα ίδια τα άτομα που διαχειρίζονται το σύστημα δηλ. από ανθρώπινα σφάλματα ή από κακοδιαχείριση του συστήματος ή από βλάβες του εξοπλισμού ή του λογισμικού αλλά και από βλάβες που να οφείλονται σε φυσικές καταστροφές (π.χ. πυρκαγιές, σεισμοί, πλημμύρες).

Όταν είναι γνωστοί οι πιθανοί κίνδυνοι, η ευπάθεια και οι τρόποι λειτουργίας των συστημάτων είναι εφικτό να βρεθούν τα απαραίτητα μέσα και τρόποι για την αντιμετώπιση κάθε πιθανής επίθεσης. Κάθε επιχείρηση δημιουργεί τις πολιτικές ασφαλείας που την καλύπτουν.

2.4 ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

Οι πολιτικές ασφαλείας περιγράφουν ποιες είναι οι ανάγκες ενός δικτύου και ποια μέτρα πρέπει να ληφθούν για να καλυφθούν αυτές οι ανάγκες. Μερικές λύσεις για την ασφάλεια του δικτύου και των δεδομένων παραθέτονται παρακάτω:

1) Κρυπτογράφηση δεδομένων: Η κρυπτογράφηση είναι τρόπος ασφαλείας ώστε ένα μήνυμα να μπορεί να το διαβάσει μόνο ο τελικός αποδέκτης. Υπάρχουν διάφορα επίπεδα κρυπτογράφησης και διάφορα προγράμματα που χρησιμοποιείται. Πλέον τα σύγχρονα προγράμματα κρυπτογράφησης γίνονται πιο ασφαλή.
2) Τείχος προστασίας (firewall): Σε όλες τις συνδέσεις με το Internet ενσύρματες ή ασύρματες απαιτείται τείχος ασφαλείας (Firewall) για να αποτραπεί τυχόν εισβολή μέσω του Διαδικτύου στον υπολογιστή ή στο δίκτυο της επιχείρησης.
3) Κίνδυνος μόλυνσης από κακόβουλο λογισμικό: Το Διαδίκτυο προσφέρει ενημέρωση και πληροφορίες αλλά υπάρχει ο κίνδυνος όταν "κατεβάσουν" κάποιο αρχείο από το Internet να περιέχει ιό. Γι' αυτό πρέπει να υπάρχει εγκατεστημένο στον υπολογιστή κάποιο πρόγραμμα ελέγχου (Antivirus) για να ελέγχει για ιούς και να μπορεί να "καθαρίσει" κάποιο "μολυσμένο" αρχείο. Ακόμη οι χρήστες δεν πρέπει να εκτελούν προγράμματα άγνωστης ή αμφιβόλου προέλευσης ή προγράμματα που στάλθηκαν μέσω ηλεκτρονικού ταχυδρομείου (email) από ανύπαρκτους ή άγνωστους χρήστες.
4) Ψηφιακά πιστοποιητικά: Κατά την κρυπτογράφηση δεδομένων χρησιμοποιούνται τα ψηφιακά πιστοποιητικά για την ασφαλή μεταφορά τους μέσω του Διαδικτύου. Ακόμη χρησιμοποιούνται για τη δημιουργία

ψηφιακής υπογραφής η οποία πιστοποιεί την ταυτότητα του χρήστη. Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται από επιχειρήσεις που κάνουν συναλλαγές και εμπόριο μέσω Internet και τα χρησιμοποιούν για την κρυπτογράφηση των στοιχείων των πιστωτικών καρτών.

5) Προστατευμένες ιστοσελίδες: Είναι οι ιστοσελίδες που επιτρέπουν περιορισμένη χρήση. Σε μερικές προστατευμένες ιστοσελίδες, ο χρήστης πρέπει να εισάγει (το σωστό) κωδικό πρόσβασης για να επιτραπεί στο χρήστη να δει το περιεχόμενο. Πολλές εταιρείες χρησιμοποιούν κωδικούς πρόσβασης στις σελίδες που χρησιμοποιούν οι εργαζόμενοί τους, ώστε να ελέγχεται η χρήση των πληροφοριών.
6) Τακτική διεξαγωγή μηχανισμού ελέγχου: Υπάρχουν συστήματα που μπορούν να ελέγξουν το δίκτυο για τρωτά –αδύναμα σημεία που αποτελούν αντικείμενο εκμετάλλευσης για κάποιον εισβολέα και να αποκτήσει πρόσβαση σε εταιρικά συστήματα. Αυτά τα συστήματα ελέγχουν τους υπολογιστικούς πόρους, εντοπίζουν τα τρωτά σημεία, ενημερώνουν τον διαχειριστή του συστήματος και προτείνουν λύσεις διόρθωσης και για τα κενά ασφαλείας που πιθανώς μπορεί να υπάρχουν.

Κατά την διάρκεια περιαγωγής στο διαδίκτυο θα πρέπει να υπάρχει προσοχή διότι υπάρχουν επιτήδειοι που εξαπατούν χρήστες του Internet και στη σημερινή εποχή το ηλεκτρονικό έγκλημα είναι διαδεδομένο.

2.4.1 ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΕΔΟΜΕΝΩΝ

Η κρυπτογράφηση αποτελεί μια σημαντική τεχνολογία για την ασφάλεια του Internet και για την ασφαλή μεταφορά-ανταλλαγή προσωπικών δεδομένων. «Κρυπτογράφηση (encryption) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.» (29. Π. Αντωνίου, 2011)

Η αντίθετη διαδικασία δηλαδή η επαναφορά του μηνύματος στην αρχική του μορφή ονομάζεται αποκρυπτογράφηση.

Η κρυπτογράφηση είναι μια επιστήμη που βασίζεται στην χρήση των μαθηματικών και γίνεται με την βοήθεια ενός αλγόριθμου κρυπτογράφησης (cipher) και ενός ή δυο κλειδιών κρυπτογράφησης (keys). Το αρχικό κείμενο ονομάζεται απλό κείμενο ενώ το κείμενο που προκύπτει μετά την κρυπτογράφηση ονομάζεται κρυπτογράφημα.

Οι δύο σημαντικότερες μέθοδοι κρυπτογράφησης είναι η Συμμετρική κρυπτογράφηση και η κρυπτογράφηση Δημοσίου Κλειδιού ή Ασύμμετρη κρυπτογράφηση.

Στην συμμετρική κρυπτογράφηση υπάρχει μόνο ένα κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος. Το κλειδί αυτό πρέπει να είναι κρυφό και να γίνει γνωστό μόνο στα εξουσιοδοτημένα μέλη. Για

τη μετάδοση του κλειδιού χρειάζεται ένας ασφαλής τρόπος όπως μια προσωπική συνάντηση για να αποφασίσουν ποιο κλειδί θα χρησιμοποιείται. Αν δεν υπάρχει ασφαλής τρόπος μετάδοσης του κλειδιού, τότε η συμμετρική κρυπτογράφηση δεν είναι αποτελεσματική. (30. Μ. Σιδηρόπουλος, 2009)

Στην κρυπτογράφηση του δημοσίου κλειδιού ή ασύμμετρη κρυπτογράφηση χρησιμοποιούνται δύο κλειδιά, το δημόσιο (public) και το ιδιωτικό (private) κλειδί. Το δημόσιο κλειδί είναι κοινό κλειδί και μπορεί να μεταδοθεί χωρίς να απαιτείται ασφαλής τρόπος. Αντίθετα το ιδιωτικό κλειδί πρέπει να μείνει κρυφό και να το γνωρίζει μόνο ο ιδιοκτήτης του. Τα κλειδιά αυτά έχουν τις εξής ιδιότητες:

- Όταν ένα μήνυμα κρυπτογραφηθεί με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί.
- Το ένα κλειδί δεν προέρχεται από το άλλο. (31. Αδ. Ψαλλιδάκου, 2006)

Κάθε χρήστης έχει το δικό του δημόσιο και ιδιωτικό κλειδί. Υπάρχουν συγκεκριμένοι εξυπηρετητές δημοσίων κλειδιών όπου μπορεί κάποιος να βρει το δημόσιο κλειδί του χρήστη που ζητάει ή μπορεί να δημοσιοποιήσει το δικό του δημόσιο κλειδί ώστε να μπορεί να διατεθεί στο κοινό. (32. Γ. Ξουραφάς –Δ. Σπυροπούλου, 2008)

Η κρυπτογράφηση δημοσίου κλειδιού παρέχει μεγαλύτερη ασφάλεια από τη συμμετρική κρυπτογράφηση.

2.4.2 ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ

«Στην επιστήμη των υπολογιστών ο όρος firewall ή τείχος προστασίας χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε έναν άλλο.» (33. Μ. Ζιώγα, 2010)

Ένα πρόγραμμα firewall, έχει τη δυνατότητα να ελέγχει και να αναφέρει αν κάποιος ή κάτι προσπαθεί να επικοινωνήσει ή να έχει πρόσβαση στον Η/Υ. Με την αναφορά αυτή που δίνει το firewall, ο χρήστης έχει τη δυνατότητα να απαγορεύσει την είσοδο ή την έξοδο πληροφοριών ή προγραμμάτων από τον Η/Υ σας. Το firewall μπορεί να προστατέψει από τα backdoor προγράμματα (που χρησιμοποιούνται από ερασιτέχνες hackers) και από τα σκουλήκια του Διαδικτύου. Με την τοποθέτηση ενός firewall πετυχαίνουμε την πρόληψη και αντιμετώπιση επιθέσεων στο τοπικό δίκτυο. (34. Χ. Τσομπανίδης, 2010)

Όταν ένα firewall ρυθμίζεται σωστά από τον διαχειριστή του δικτύου (default-deny) τότε απορρίπτει όλες τις συνδέσεις έκτος αυτών που επιτρέπει ο διαχειριστής του δικτύου. Ο διαχειριστής του δικτύου πρέπει να έχει μια ολοκληρωμένη εικόνα του δικτύου και πολύ καλές γνώσεις στα δίκτυα υπολογιστών. (35. Ι. Γκουρτζούνης , 2010)

«Το τείχος προστασίας εμποδίζει εισβολείς ή λογισμικό κακόβουλης

λειτουργίας (όπως ιούς τύπου worm) να αποκτήσουν πρόσβαση στον Η/Υ σας μέσω δικτύου ή μέσω internet. Το τείχος προστασίας εμποδίζει επίσης στον Η/Υ σας να στείλει λογισμικό κακόβουλης λειτουργίας σε άλλους χρήστες.»

Όταν το τείχος προστασίας των windows είναι ενεργοποιημένο, τότε αποκλείει τα περισσότερα προγράμματα. Είναι όμως εφικτό να φτιάχτεί μια λίστα με επιτρεπόμενα προγράμματα, που θα μπορούν να επικοινωνούν με το τείχος προστασίας.

Ένα τείχος προστασίας έχει τη δυνατότητα να αποκλείσει όλες τις εισερχόμενες συνδέσεις ακόμη και εκείνων από τη λίστα επιτρεπόμενων προγραμμάτων, επίσης όταν αποκλείει ένα πρόγραμμα ειδοποιείται ο χρήστης. Υπάρχει και ρύθμιση με την οποία απενεργοποιείται το τείχος προστασίας των windows, άλλα κάλο είναι να αποφεύγεται. Με την απενεργοποίηση του τείχους προστασίας των windows και γενικά ενός τείχους προστασίας (software ή hardware) γίνονται περισσότερο ευάλωτοι σε βλάβες από εισβολείς και κακόβουλο λογισμικό. (36. Ι. Γκουρτζούνης, 2010)

Τα τείχη προστασίας (firewalls) διακρίνονται σε δύο είδη: τα software και τα hardware.

Τα software firewalls είναι ένα λογισμικό πρόγραμμα που εγκαθίστανται σε κάθε υπολογιστή που έχει πρόσβαση στο Internet. Η εγκατάσταση ενός τέτοιου λογισμικού μπορεί να είναι δαπανηρή λύση για μια επιχείρηση (37. Κ. Στυλιάδης, 2010)

Τα hardware firewalls είναι αυτόνομες συσκευές συνδεδεμένες με το δίκτυο ή υπολογιστές, στους οποίους έχουν εγκαταστήσει τα αναγκαία προγράμματα για να λειτουργούν ως τείχη προστασίας στο δίκτυο της επιχείρησης. (38. Κ. Στυλιάδης, 2010)

Υπάρχουν εταιρείες που παρέχουν τέτοια προγράμματα software και hardware. Τέτοιες εταιρείες είναι Cisco, Nokia, Checkpoint, 3Com και Zyxel.

2.4.3 ΚΙΝΔΥΝΟΣ ΜΟΛΥΝΣΗΣ ΑΠΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

Τα κακόβουλα λογισμικά μπορούν να προξενήσουν ζημιά στον υπολογιστή ή στο δίκτυο υπολογιστών. Σήμερα υπάρχει ποικιλία τέτοιων λογισμικών. Αυτά τα κακόβουλα λογισμικά είναι οι ιοί.

«Ο ιός είναι ένα τμήμα ηλεκτρονικού κώδικα ο οποίος προσκολλάται σε ένα πρόγραμμα ή ένα αρχείο, ώστε να μπορεί να μεταδοθεί από υπολογιστή σε υπολογιστή. Προσβάλει καθώς μετακινείται. Οι ιοί μπορούν να καταστρέψουν το λογισμικό σας, το υλικό σας και τα αρχεία σας.

Ιός (ουσ.) Κώδικας ο οποίος έχει γραφτεί με σκοπό να αναπαράγεται. Ο ιός προσκολλάται σε ένα αρχείο "ξενιστή" και προσπαθεί να διαδοθεί από υπολογιστή σε υπολογιστή. Μπορεί να καταστρέψει υλικό, λογισμικό και δεδομένα.» (39. Χ.Κουτσουρελάκης, 2008)

Οι πιο γνωστές κατηγορίες ιών είναι οι εξής: (40. Κ. Στυλιάδης, 2010)

- Ιοί (viruses): Σκοπός του ιού υπολογιστών είναι να προξενεί προβλήματα στον υπολογιστή και κατ' επέκταση στο δίκτυο. Για να μπορέσει ο ιός να βλάψει τον υπολογιστή θα πρέπει να εκτελεστεί ως πρόγραμμα, αυτό γίνεται χωρίς ο χρήστης να το γνωρίζει ή να το εγκρίνει.
  Κάποιοι ιοί δημιουργούνται για να βλάψουν τον υπολογιστή στον οποίο εγκαθίστανται. Ο ιός μπορεί να καταστρέψει ή να τροποποιήσει αρχεία ή να τα διαγράψει ή μπορεί ακόμη να προκαλέσει ζημιά σε ένα τομέα του σκληρού δίσκου και ίσως δεν είναι εφικτό να αποκτηθεί ολόκληρο το περιεχόμενό του. Υπάρχουν όμως και μερικοί ιοί που δεν έχουν σκοπό την καταστροφή, απλά κάνουν γνωστή την ύπαρξή τους παρουσιάζοντας στην οθόνη μηνύματα που τις περισσότερες φορές είναι χιουμοριστικά. Όμως ακόμη και αυτοί οι ιοί μπορούν να προκαλέσουν προβλήματα διότι καταλαμβάνουν μνήμη από τα κανονικά προγράμματα. Πολλοί ιοί μπορεί να προκαλέσουν τη διάλυση των υπολογιστικών συστημάτων και την απώλεια των δεδομένων. (41. Ρ. Αντωνόπουλος – Α. Αγγέλης, 2010)
- Ιοί των e-mail (e-mail viruses): Ο πιο διαδεδομένος τρόπος, σήμερα, για την μετάδοση κάποιου ιού είναι με e-mail. Κάποιοι υποστηρίζουν ότι με την απλή ανάγνωση ενός e-mail δεν είναι δυνατόν να μεταδοθεί ο ιός. Τελευταία όμως, ανακάλυψαν ότι μερικές φορές αρκεί η αποστολή ενός μηνύματος για να προκληθούν ζημιές στον υπολογιστή, χωρίς να διαβαστεί το μήνυμα. Οι ιοί πιο συχνά είναι ως συνημμένα αρχεία τα οποία ενεργοποιούνται όταν το μήνυμα ανοιχθεί και διαβαστεί. (42. Μ.Σαλούστρος -Χ.Παπαδάκης-Δ.Ρεμυλιανάκης, 2010)
- Σκουλήκια (worms): Τα σκουλήκια μοιάζουν με τους ιούς αλλά δεν απαιτείται για την διάδοσή τους ένα πρόγραμμα-φορέας. Τα σκουλήκια χρησιμοποιούν τις επικοινωνίες μεταξύ υπολογιστών και διανέμουν ακριβή και ολοκληρωμένα αντίγραφα του εαυτού τους. Μπορούν και αντιγράφουν τον εαυτό τους από υπολογιστή σε υπολογιστή, ώστε να μεταδίδονται γρήγορα.(43. Κ. Σφούνης, 2010)
- Δούρειοι Ίπποι (Trojan Horses): Ο ιός τύπου Δούρειου ίππου είναι φαινομενικά ένα χρήσιμο πρόγραμμα αλλά προκαλεί ζημιά. Ο Δούρειος ίππος θυμίζει λίγο την ιστορία της μυθολογίας με το ξύλινο άλογο που χρησιμοποιήθηκε για την πολιορκία της Τροίας, με τον ίδιο τρόπο και οι Δούρειοι ίπποι εγκαθίστανται στον υπολογιστή σαν χρήσιμα προγράμματα ενώ στην πραγματικότητα θέτει σε κίνδυνο την ασφάλεια και προκαλεί μεγάλες ζημιές. (44. Χ. Κουτσουρελάκης, 2008)

Οι τρόποι με τους οποίους μεταδίδονται οι ιοί είναι πολλοί, οι πιο συνηθισμένοι τρόποι είναι οι εξής: (45. Κ. Σφούνης, 2010)

1. Ανταλλαγή αρχείων: Μεταφέροντας αρχεία με CD ή USB από έναν μολυσμένο υπολογιστή σε άλλο υπολογιστή.
2. Ηλεκτρονικό Ταχυδρομείο: Από συνημμένα αρχεία που υπάρχουν σε e-mail. Συνήθως προσβάλλεται από σκουλήκια.
3. Παγκόσμιος Πληροφοριακός Ιστός: Με το «κατέβασμα» αρχείων

από το Διαδίκτυο, μπορεί κάποιο αρχείο να εμπεριέχει ιό. Πιο συχνά εδώ συναντιούνται Δούρειοι ίπποι.

Ο κύριος τρόπος προστασίας από τους ιούς είναι η εγκατάσταση αντιϊκού (antivirus), το οποίο θα ελέγχει τα δεδομένα και θα ανιχνεύει οποιαδήποτε "κίνηση" γίνει από ιό. Ακόμη μέσω του Διαδικτύου μπορεί να ενημερώνεται (update) το αντιϊκό πρόγραμμα για την αντιμετώπιση νέων ιών. (46. Ρ. Αντωνόπουλος – Α. Αγγέλης, 2010)

Η χρησιμοποίηση του τείχους προστασίας (firewall) το οποίο είναι ένα λογισμικό που προστατεύει τον υπολογιστή από επιβλαβές περιεχόμενο. (47. Κ. Στυλιάδης, 2010).

Ακόμη μια καλή λύση είναι να κρατιούνται αρχεία back up δηλαδή αντίγραφα ασφαλείας. Σε περίπτωση που χαθούν αρχεία από κάποιο ιό θα είναι εφικτή η αντικατάσταση. Τέλος, δεν πρέπει να ανοίγονται επισυναπτόμενα αρχεία, όταν δεν γνωρίζουν τον αποστολέα. Αλλά αρκετοί ιοί φτάνουν από e-mail γνωστών και φίλων οι οποίοι δεν γνωρίζουν ότι έχουν μολυνθεί από κάποιο ιό. (48. Μ.Σαλούστρος -Χ.Παπαδάκης-Δ.Ρεμυλιανάκης, 2010)

Οι ιοί έχουν εξελιχθεί σε μεγάλο βαθμό με την πάροδο του χρόνου, παρακάτω παρουσιάζονται οι πιο γνωστοί ιοί της ιστορίας του internet: (49. Α. Αυγουστίδης, 2009)

Ο Morris, ο πρώτος ιός τύπου σκουλήκι δημιουργήθηκε το 1988 από τον Robert Morris που έφερε το όνομά του. Το 1992, ο Michelangelo ήταν ο πρώτος ιός και αυτός που υποχρέωσε τις εταιρείες να δημιουργήσουν antivirus προγράμματα. Ο ιός Melissa ήταν από τους πρώτους ιούς e-mail ως συνημμένο αρχείο και δημιουργήθηκε το 1999. Το 2000 ένα e-mail με συνημμένο αρχείο ένα «ερωτικό γράμμα», διαδόθηκε σε μικρό διάστημα σε όλο τον κόσμο προκαλώντας μεγάλη αναστάτωση και κινητοποίηση. Το 2001 εμφανίστηκε το σκουλήκι Red Code, το οποίο αναπαρήγαγε τον εαυτό του πολύ γρήγορα και ελάττωσε την κυκλοφορία του Διαδικτύου. Ο Slammer, το 2003, εξάντλησε το Διαδίκτυο προσβάλλοντας 75 χιλιάδες υπολογιστές. Το 2003 δημιουργήθηκε ο Blaster που μπορούσε να κάνει δίκτυα υπολογιστών να καταρρεύσουν. Το ίδιο έτος εμφανίστηκε και ο ιός Sobig πρόσβαλλε εκατομμύρια υπολογιστές. Το 2004 εμφανίστηκαν οι ιοί My Doom (Η καταδίκη μου) ή όπως ήταν γνωστός Novarg, ο οποίος ήταν από τους πιο καταστροφικούς ιούς. Το ίδιο έτος δημιουργήθηκαν και οι ιοί Sasser και Netski, όπως και οι ιοί «νέας γενιάς» Scob και Mimail οι οποίοι έχουν σκοπό τη συλλογή αριθμών από πιστωτικές κάρτες και απόρρητους κωδικούς.

2.4.4 ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

Με τη βοήθεια του Διαδικτύου υπάρχει η δυνατότητα επικοινωνίας με ανθρώπους και φορείς και η ανταλλαγή πληροφοριών. Για να ανταλλάσσουν πληροφορίες οι άνθρωποι και οι φορείς μεταξύ τους, πρέπει να δημιουργηθεί

ένα κλίμα εμπιστοσύνης. Όμως για τις επιχειρήσεις δεν αρκεί μόνο η εμπιστοσύνη, γιατί πολλές επιχειρήσεις κάνουν διάφορες οικονομικές συναλλαγές μέσω του διαδικτύου. Υπάρχουν hackers και crackers οι οποίοι καραδοκούν και προσπαθούν να κλέψουν τον αριθμό της πιστωτικής κάρτας, προσωπικά και επαγγελματικά δεδομένα.

Για αυτό το λόγο οι επιχειρήσεις πρέπει να γνωρίζουν το πρόσωπο με το οποίο επικοινωνούν, στέλνουν τον αριθμό της πιστωτικής τους κάρτα ή κάνουν διάφορες οικονομικές συναλλαγές μέσω του Διαδικτύου. Πρέπει δηλαδή να είναι σίγουροι πως το πρόσωπο που επικοινωνούν είναι αυτός πραγματικά που δηλώνει ότι είναι και όχι κάποιος άλλος.

Το πρόβλημα αυτό μπορεί να λυθεί με την χρήση των ψηφιακών πιστοποιητικών (digital certificates).

«Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται για να πιστοποιούν ότι το άτομο που στέλνει πληροφορίες ή έναν αριθμό πιστωτικής κάρτας ή ένα μήνυμα ή οτιδήποτε άλλο στο internet, είναι πραγματικά αυτός που δηλώνει ότι είναι.»

Αυτό που κάνουν τα ψηφιακά πιστοποιητικά είναι να τοποθετούν τις πληροφορίες στο σκληρό δίσκο του χρήστη και με τη βοήθεια της τεχνολογίας απόκρυψης δημιουργούν ένα μοναδικό ψηφιακό πιστοποιητικό για κάθε χρήστη.

«Όταν κάποιος που διαθέτει ένα ψηφιακό πιστοποιητικό επισκεφθεί κάποιο site ή στείλει e-mail το πιστοποιητικό αυτό παρουσιάζεται στο site ή επισυνάπτεται στο e-mail και πιστοποιεί ότι ο χρήστης είναι αυτός που ισχυρίζεται ότι είναι.»

Τα ψηφιακά πιστοποιητικά δεν μπορούν να πλαστογραφηθούν, είναι πολύ ασφαλή και αυτό γιατί διαθέτουν πανίσχυρη τεχνολογία απόκρυψης. Οι Digital Authorities είναι ιδιωτικές εταιρείες που εκδίδουν ψηφιακά πιστοποιητικά με χρέωση.

Το ψηφιακό πιστοποιητικό περιλαμβάνει κωδικοποιημένες πληροφορίες οι οποίες είναι μοναδικές για κάθε χρήστη. Οι πληροφορίες αυτές μπορεί να είναι το όνομα του χρήστη, το όνομα της εταιρείας που το εκδίδει, ένας σειριακός αριθμός και πολλά άλλα. (50. Δ. Παπαδάκης, 2010)

Ένας ορισμός για το προσωπικό ψηφιακό πιστοποιητικό είναι ο έξης:

«Τα προσωπικά πιστοποιητικά, τα οποία αποτελούν ένα είδος εγγύησης ότι ο χρήστης είναι αυτός που δηλώνει ότι είναι. Σε αυτά καταχωρούνται προσωπικές πληροφορίες, όπως όνομα χρήστη και κωδικός πρόσβασης. Οι πληροφορίες αυτές αποθηκεύονται σε ένα πιστοποιητικό, το οποίο χρησιμοποιείται όταν στέλνονται προσωπικές πληροφορίες σε ένα διακομιστή ελέγχου ταυτότητας που απαιτεί πιστοποιητικό. Επίσης ένα προσωπικό πιστοποιητικό επιτρέπει στο χρήστη να λαμβάνει κρυπτογραφημένα μηνύματα από τους υπόλοιπους χρήστες.» (51. Ν. Αποστοπούλου - Β. Δαραμούσκας, 2008)

2.4.5 ΠΡΟΣΤΑΤΕΥΜΕΝΕΣ ΙΣΤΟΣΕΛΙΔΕΣ

Οι περισσότερες ιστοσελίδες δεν προστατεύονται, αυτό σημαίνει ότι όλοι μπορούν να δουν το περιεχόμενο αυτών των ιστοσελίδων. Υπάρχουν όμως και οι ιστοσελίδες που προστατεύονται, στις οποίες ιστοσελίδες σου ζητάνε όνομα χρήστη και κωδικό πρόσβασης για να αποκτήσεις πρόσβαση στην ιστοσελίδα. Μερικές ιστοσελίδες περιέχουν παράλληλα και κάποιες προστατευμένες περιοχές, δηλαδή πληρώνεις κάποια συνδρομή και αποκτάς πρόσβαση στις προστατευμένες περιοχές της ιστοσελίδας. (52. Άγνωστος, 2010)

Όλες οι επιχειρήσεις έχουν μια ιστοσελίδα και χρησιμοποιούν το Internet σαν ‘‘εργαλείο’’ τους για την επικοινωνία, την λειτουργία και την ανάπτυξη της επιχείρησής τους. Ακόμη κάποιες επιχειρήσεις κάνουν ηλεκτρονικό εμπόριο. Οι αγορές μέσω Διαδικτύου γίνονται με τη χρήση πιστωτικών καρτών. Για μια ασφαλή συναλλαγή, οι χρήστες-αγοραστές πρέπει να αποφύγουν να δίνουν τα προσωπικά τους στοιχεία σε εταιρείες που δεν χρησιμοποιούν μηχανισμούς ασφαλείας. Αν η ιστοσελίδα είναι ασφαλής πρέπει να προσέξουν τα εξής:

1. Αν η σελίδα είναι προστατευμένη, κατά την είσοδο σε αυτήν θα εμφανιστεί ένα μήνυμα που θα ενημερώνει ότι ο χρήστης επισκέπτεται σελίδα ασφαλείας.
2. Εάν στο πρόγραμμα περιπλάνησης, κάτω δεξιά, υπάρχει ένα λουκετάκι. Αν το λουκετάκι είναι κλειστό η σελίδα είναι ασφαλής. Εάν όμως το λουκετάκι δεν υπάρχει ή είναι ανοικτό, καλύτερα ο χρήστης να αποφύγει τη συναλλαγή.
3. Ο χρήστης πρέπει να παρατηρεί την διεύθυνση του Διαδικτυακού τόπου, Στις κανονικές σελίδες τραπεζών και εταιρειών η διεύθυνση αντί για http:// αρχίζει με https:// και δηλώνει ότι η σελίδα έχει ασφάλεια, επομένως και η συναλλαγή είναι ασφαλής. (53. Άγνωστος, 2010)

Στην εποχή μας το ηλεκτρονικό έγκλημα είναι διαδεδομένο. Οι ηλεκτρονικοί εγκληματίες υποκλέπτουν προσωπικά δεδομένα ανακαλύπτοντας συνεχώς νέους τρόπους παραβίασης λογισμικών ασφαλείας. Οι ηλεκτρονικοί εγκληματίες χρησιμοποιούν το phising, είναι μια μέθοδος «ψαρέματος» προσωπικών στοιχείων με πλαστό e-mail. Οι απατεώνες του κυβερνοχώρου έχουν στρέψει το ενδιαφέρον σου σε ιστοσελίδες που περιλαμβάνουν προσωπικά δεδομένα και δεν έχουν ισχυρά συστήματα ασφαλείας, όπως οι τράπεζες και οι μεγάλες επιχειρήσεις. (54. Π. Δημητρολόπουλος, 2010)

Οι μικρομεσαίες επιχειρήσεις πρέπει να προσαρμοστούν στις νέες τεχνολογίες. Σύμφωνα με τη συνέντευξη που έδωσε ο κ. Αθ. Βαρβάτσικος, Country Manager της Symantec Ελλάδος (55. Χ. Τσομπανίδης, 2010) τονίζει ότι οι μικρομεσαίες εταιρείες πρέπει να υιοθετήσουν τα εξής:

1. Κατανόηση της Έκθεσης της Πληροφορίας: να μπορέσουν να εξισορροπήσουν την ανάγκη για άμεση πληροφόρηση οποιαδήποτε στιγμή με την ανάγκη για επαρκή προστασία. Αναγκαία προϋπόθεση η αξιολόγηση ενός τέτοιου κινδύνου.

2. Πολιτικές Συμμόρφωσης Διαδικτύου: οι αυξημένοι κίνδυνοι που δημιουργεί η κοινωνική δικτύωση επιβάλλει στην επιχείρηση να επανεξετάσει τα πρωτόκολλα τεχνολογίας, ώστε να γίνεται ορθή χρήση του Διαδικτύου.
3. Συσκευές Κινητής Τηλεφωνίας: οι εταιρείες που παρέχουν συσκευές κινητών τηλεφώνων στους εργαζομένους θα πρέπει να ορίσουν τις καλύτερες πρακτικές χρήσης ώστε η πληροφορία να είναι ασφαλής όταν μεταφέρεται και να εξασφαλίσουν ασφαλείς ασύρματες συνδέσεις για τους εργαζομένους.
4. Σωστή Επένδυση Πληροφορικής: Οι σημερινές απειλές είναι πολυμορφικές. Οι μικρομεσαίες επιχειρήσεις πρέπει να αγοράσουν τις λύσεις που ταιριάζουν στις ανάγκες τους και στον προϋπολογισμό τους.
5. Ο Ρόλος του Συμβούλου: οι μικρομεσαίες επιχειρήσεις πρέπει να ανακαλύψουν τον κατάλληλο προμηθευτή λύσεων για την επιχείρησή τους, ώστε να συνεχίσουν τη σωστή εξέλιξη της επιχείρησης.

2.4.6 ΤΑΚΤΙΚΗ ΔΙΕΞΑΓΩΓΗ ΕΛΕΓΧΟΥ

Το τείχος προστασίας (firewall) και οι λίστες ελέγχου πρόσβασης (Access Control Lists-ACL) ανήκουν στην πρώτη γραμμή άμυνας του υπολογιστή. Αν και συμβάλλουν στην ασφάλεια του υπολογιστή, ωστόσο δεν είναι σίγουρο αν προσφέρουν την καλύτερη δυνατή προστασία. Δημιουργήθηκε γι' αυτό το λόγο η δεύτερη γραμμή άμυνας, η οποία περιέχει πολλά επίπεδα άμυνας και είναι γνωστή ως «Defense in Derths», δηλαδή άμυνα σε βάθος.

Με την ενίσχυση της πρώτης γραμμής άμυνας πετυχαίνεται να μην επιτρέπεται η παράνομη πρόσβαση στο δίκτυο. Υπάρχει περίπτωση όμως αυτό να αποτύχει τότε ο ανιχνευτικός μηχανισμός είναι η καλύτερη λύση όσον αφορά το δεύτερο επίπεδο προστασίας.

Το σύστημα ανίχνευσης επιθέσεων (IDS) είναι το κατάλληλο εργαλείο στα χέρια ενός διαχειριστή ασφαλείας γιατί ένα IDS μπορεί να ανιχνεύει άμεσα μια επίθεση και ο διαχειριστής ασφαλείας να αντιδρά στην επίθεση που δέχεται το δίκτυο του.

«Το IDS είναι ένα σύστημα λογισμικού ή ένας συνδυασμός υλικού και λογισμικού το οποίο πραγματοποιεί την ανίχνευση περίεργης δικτυακής κίνησης σε έναν υπολογιστή ή στο δίκτυο.»

Ένα IDS όπως και τα περισσότερα συστήματα ανίχνευσης επιθέσεων λειτουργούν με τη χρήση Signatures, δηλαδή ανιχνεύουν παράνομες ακολουθίες ενεργειών, αναλύουν την περίεργη δικτυακή κίνηση και τέλος αποφασίζουν αν πρόκειται για κάποιο είδος επίθεσης ή όχι. Όταν ένα IDS ανιχνεύει μια επίθεση δεν μπορεί να σταματήσει την εξάπλωση της, μπορεί μόνο να την παρουσιάσει στον διαχειριστή ασφαλείας.

Υπάρχουν δύο είδη συστημάτων ανίχνευσης επιθέσεων:

1. Network-Based IDS (NIDSs): Τα συστήματα αυτά εξετάζουν την διερχόμενη κίνηση για την ύπαρξη ή μη εισβολών.
2. Host-Based IDS (HIDSs): Τα συστήματα αυτά έχουν ακριβή πληροφόρηση για την ύπαρξη ή μη κάποιας επίθεσης και αυτό γίνεται γιατί τα συστήματα αυτά μπορούν να καταλάβουν τι συμβαίνει κάθε φορά στο σύστημα. Και όταν αντιληφθούν μια άγνωστη μορφή επίθεσης η οποία προσπαθεί να πετύχει τη δυσλειτουργία του υπολογιστή, τότε αυτά αναγνωρίζουν την επίθεση ενώ τα Network-based IDS δεν θα την αντιλαμβανόταν. Τα Host-Based IDS είναι πιο αποτελεσματικά από τα Network-Based IDS.

Υπάρχουν 3 είδη μηχανισμών που με την βοήθεια των οποίων μπορεί ένα IDS να αποφασίσει αν επιτίθεται κάποιος στο σύστημα του ή όχι:
1. Ανάλυση με βάση τα γεγονότα ή υπογραφές (events ή signatures): Τα συστήματα αυτά λειτουργούν όπως τα antivirus προγράμματα και βασίζονται σε events ή signatures . Η εταιρεία ανάπτυξης συστήματος IDS φτιάχνει κάθε φορά μια λίστα από signatures. Η λίστα αυτή αποτελείται από ακολουθίες ενεργειών που θεωρεί ύποπτες ή ενδεικτικές επίθεσης. Το IDS μετά ελέγχει το περιβάλλον του για άγνωστες ακολουθίες ενεργειών, και όταν βρει μια τέτοια ακολουθία τότε ενημερώνει το σταθμό ελέγχου για το συμβάν
2. Στατιστική ανάλυση: Τα συστήματα αυτά βασίζονται στη στατιστική ανάλυση, δηλαδή κατασκευάζουν στατιστικά πρότυπα για το περιβάλλον τους. Στατιστικά πρότυπα μπορεί να είναι η μέση διάρκεια μιας συνόδου, ο μέσος αριθμός περιήγησης σε ένα web site, η μέση συχνότητα εμφάνισης μιας IP διεύθυνσης και πολλά άλλα. Τα στατιστικά αυτά πρότυπα μπορούν να καθορίσουν την αποκαλούμενη «Συνήθης Συμπεριφορά» και όταν κάτι αποκλείεται από αυτήν τότε θεωρείται ως ένδειξη περίεργης συμπεριφοράς.
3. Προσαρμόσιμα συστήματα: Τα προσαρμόσιμα συστήματα ξεκινάνε με μια αρχική περίοδο μάθησης, στην οποία το σύστημα μαθαίνει την αλληλεπίδραση ανθρώπων-περιβάλλοντος και ειδοποιεί τους υπευθύνους όταν υπάρχουν ασυνήθιστες δραστηριότητες.

Αυτό που δεν πρέπει να παραλείπεται είναι πως οποιοδήποτε τύπος IDS και αν είναι, θα απολέσει κάποιες πληροφορίες όταν υπάρχει ύποπτη δραστηριότητα και μπορεί να έχει ενδείξεις κινδύνου και όταν όλα είναι φυσιολογικά. Αυτές οι καταστάσεις ονομάζονται false negatives ή false positives. Για αυτό το λόγο η ύπαρξη ενός ανθρώπινου παράγοντα μπορεί να βελτιώσει περισσότερο την αλληλεπίδραση του IDS με το περιβάλλον.

Τα IDS μπορούν να κατηγοριοποιηθούν με βάση την τεχνική την οποία χρησιμοποιούν για την ανίχνευση των εισβολών. Έξι κατηγορίες εισβολών υπάρχουν και είναι οι εξής:
1. Προσπάθεια εισόδου στο σύστημα: η εισβολή αυτή μπορεί να ανιχνευθεί από τα τυπικά προφίλ συμπεριφοράς ή τις παραβιάσεις περιορισμών ασφαλείας.
2. Κρυφή επίθεση: η κρυφή επίθεση μπορεί να ανιχνευθεί από τα τυπικά προφίλ συμπεριφοράς.
3. Διείσδυση στο σύστημα ελέγχου ασφαλείας: η οποία μπορεί να ανιχνευθεί με

την παρακολούθηση συγκεκριμένων πρότυπων δραστηριότητας.
4. Διαρροή: η οποία μπορεί να γίνει αντιληπτή με την χρήση των πόρων του συστήματος.
5.Denial of service (άρνηση εκτέλεση εφαρμογής): η οποία επίσης μπορεί να γίνει αντιληπτή με την χρήση των πόρων του συστήματος.
6. Κακόβουλη χρήση: η οποία μπορεί να ανιχνευθεί από τα τυπικά προφίλ συμπεριφοράς, από τις παραβιάσεις κανόνων ασφαλείας ή από την χρήση ειδικών προνομίων. (56. Ε.Βαλεοντής, 2007)

Συμπερασματικά ένα σύστημα IDS για να εξασφαλίσει την άριστη λειτουργία του πρέπει να ελέγχει συχνά τον εαυτό του και να ελέγχει σε τακτά χρονικά διαστήματα τα δεδομένα που είναι αποθηκευμένα στο εσωτερικό του δικτύου. Ένας άνθρωπος έχει αναλάβει τον έλεγχο του συστήματος ώστε να εξασφαλίζεται περισσότερο η αξιοπιστία του.

«Ένα IDS θα πρέπει να έχει καλή μνήμη και να μην ξεγελιέται από φαινομενικά αθώες ενέργειες. Συχνά μια επίθεση κατανέμεται σε πολλές μικρές ήσσονος σημασίας και φαινομενικά άσχετες μεταξύ τους εργασίες, οι οποίες περνούν απαρατήρητες αλλά τελικά καταφέρνουν να παρακμάσουν τα συστήματα ασφαλείας που επιτρέπουν την είσοδο του εισβολέα.» (57. Γ. Επιτήδειος, 2000)

Εκτός από τα συστήματα πρόσληψης επιθέσεων IDS υπάρχουν και τα IPS. Τα IPS είναι η εξελιγμένη μορφή των IDS. Τα IPS μπορούν να ανιχνεύσουν μια επίθεση και να την αντιμετωπίσουν αυτόματα. Ένα IPS (Intrussion Prevention System) είναι μέρος ενός IDS. Αυτό γίνεται γιατί το IDS κάνει ανίχνευση της επίθεσης και το IPS παίρνει πρωτοβουλία να σταματήσει την επίθεση.

«Στην ουσία ένα IPS συνδυάζει χαρακτηριστικά ενός firewall και ενός IDS, καθώς μπορεί να μπλοκάρει την ανεπιθύμητη κίνηση έχοντας τη βοήθεια ανίχνευσης των κακόβουλων πακέτων που προσφέρει ένα IDS. Η διαφορά του από το firewall είναι ότι έχει καλύτερη και πιο ολοκληρωμένη πληροφορία. Αυτό οφείλεται στην ύπαρξη του IDS, το οποίο παρακολουθεί όλη τη δικτυακή κίνηση.»

Υπάρχουν τέσσερις τύποι συστημάτων πρόσληψης IPS και είναι οι εξής :
• Host-Based (HIPSs): Αυτό το σύστημα πρόσληψης επιθέσεων βρίσκεται σε ένα συγκεκριμένο μηχάνημα. Σκοπός του είναι η παρακολούθηση της δικτυακής κίνησης και η αποτροπή επιθέσεων.
• Network-Based (NIPSs): Τα συστήματα αυτά σκοπό έχουν να αναλύουν, να βρίσκουν και να αναφέρουν τα συμβάντα που έχουν σχέση με ζητήματα ασφαλείας. Επίσης ελέγχουν την δικτυακή κίνηση.
• Content-Based (CBIPSs): Τα συστήματα αυτά αναλαμβάνουν την παρακολούθηση των περιεχομένων των πακέτων για μοναδικές ακολουθίες οι οποίες ονομάζονται υπογραφές. Και σκοπός τους είναι η αναγνώριση και η αποτροπή γνωστών τύπων επιθέσεων.
• Rate-Based (RBIPSs): Τα συστήματα αυτά παρακολουθούν και μαθαίνουν

φυσιολογικές δικτυακές συμπεριφορές. Παρακολουθούν σε πραγματικό χρόνο το δίκτυο και με την βοήθεια κάποιων στατιστικών στοιχείων έχουν την δυνατότητα να αναγνωρίσουν κάποια μη αποδεκτά όρια για συγκεκριμένους τύπου κίνησης. Όταν οι επιθέσεις ξεπερνούν κάποια φράγματα τότε αναγνωρίζονται. Τα φράγματα αυτά έχουν την δυνατότητα να προσαρμόζονται ανάλογα με την ημέρα, την ώρα, την εβδομάδα και άλλα. Επίσης έχουν ως σκοπό την αποτροπή επιθέσεων τύπου άρνησης εξυπηρέτησης. (58. Ε.Βαλεοντής, 2007)

2.5 ΧΑΚΕΡ ΚΑΙ ΚΡΑΚΕΡ

Υπάρχουν δυο είδη χρηστών που προβαίνουν σε παράνομές πράξεις οι χάκερς (Hackers) και οι κράκερς (Crackers), ας αναλυθεί λοιπόν τι είναι ο καθένας τους:

«Με τον όρο χάκερ χαρακτηρίζεται το άτομο που έχει πολλές τεχνικές γνώσεις για τους υπολογιστές αλλά και προχωρημένες γνώσεις προγραμματισμού, μπορεί να εντοπίσει αδυναμίες σε συστήματα υπολογιστών, να λύνει τεχνικά προβλήματα, να βελτιώνει εφαρμογές αλλά και που συνεργάζεται μ’ άλλους ομοίους για την επίλυση των προβλημάτων των υπολογιστών, χωρίς όμως να προξενεί κάποια ζημιά.» (59. Κ. Στυλιάδης, 2010)

Επίσης «Χάκερ είναι αυτοί που "επιτίθενται" στα computer απλώς από ευχαρίστηση ή περιέργεια, χωρίς όμως να επιδιώκουν κάποιο οικονομικό όφελος. Στην κατηγορία αυτή ανήκουν, οι δράστες που "εισβάλουν" σε υπολογιστή δια της χρήσεως του Διαδικτύου (hackers) για να μάθουν απλώς, κάποια προσωπικά στοιχεία, η για να εντοπίσουν κάποιο πρόβλημα στην πληροφοριακή υποδομή εταιριών, τραπεζών κ.α. (τρύπα συστήματος), και στη συνέχεια να κοινοποιήσουν αυτό με σκοπό την αμοιβή τους η την πρόσληψή τους στην εταιρία.» (60. Κ. Κούρος, 2010)

«Κράκερ είναι οι προγραμματιστές που σπάνε παράνομα την προστασία εφαρμογών και κατά κανόνα δεν είναι χάκερ (software cracker). Το σπάσιμο των κωδικών ενός προγράμματος μπορεί να αποτελεί μια τεχνολογική πρόκληση για τους ειδήμονες των Η/Υ, όμως σε καμιά περίπτωση δεν δικαιολογείται ειδικά αν δημοσιευτούν τα σπασμένα προγράμματα.» (61. Α. Κοσμίδης, 2010)

Ακόμη ένας ορισμός είναι ο εξής: «Τα άτομα που προκαλούν καταστροφές σε υπολογιστές άλλων χρηστών ονομάζονται crackers. Πιο συγκεκριμένα, οι crackers είναι και αυτοί άριστοι γνώστες των υπολογιστών, όπως και οι hackers, αλλά έχουν απώτερο σκοπό το να προκαλέσουν όσο το δυνατόν μεγαλύτερες βλάβες στους υπολογιστές.» (62. Γ. Βασάλος - Δ. Βαφειάδης, 2010)

«Hacking είναι η γνώση που χρησιμοποιείται για καλό σκοπό αλλά και ενίοτε για εκδικητικούς σκοπούς.» (63.Γ. Γκίρτσος, 2007)

Οι χάκερ χωρίζονται σε δύο ομάδες τους καλούς χάκερ και τους κακούς

χάκερ, παρακάτω εξηγείται τι είναι ο καθένας και υπάρχουν διάσημοι καλοί και κακοί χάκερ:

Καλός χάκερ είναι αυτός ο οποίος έχει πολύ καλή γνώση όσον αφορά τα θέματα ασφαλείας ενός λειτουργικού συστήματος. Τα θέματα αυτά μπορεί να είναι από μια απλή σελίδα έως μια ολοκληρωμένη βάση δεδομένων μιας επιχείρησης. Ο χάκερ αυτός λέγεται καλός γιατί όταν βρει μια τρύπα σε ένα σύστημα τότε θα ειδοποιήσει το κατάλληλο πρόσωπο για να την διορθώσει.

2.5.1 ΔΙΑΣΗΜΟΙ ΚΑΛΟΙ ΧΑΚΕΡ

1. Stephen Wozniak: Ο Wos μαζί με το φίλο του το Jobs είναι αυτοί οι οποίοι ίδρυσαν την κορυφαία εταιρεία υπολογιστών Apple.
2. Tim Berners-Lee: είναι αυτός που δημιούργησε το γνωστό σε όλους μας σύστημα World Wide Web (www), που με την βοήθεια του συστήματος αυτού είναι εφικτή η πρόσβαση σε ιστοσελίδες, αρχεία και φακέλους στο διαδίκτυο.
3. Linus Torvalds: είναι αυτός που δημιούργησε το λειτουργικό σύστημα που η βάση του είναι το σύστημα Unix δηλαδή το σύστημα Linux.
4. Richard Stallman: Αυτός δημιούργησε το project GNU με σκοπό να αναπτύξει ένα ελεύθερο λειτουργικό σύστημα.
5. Tsutomu Shimomura: Ο Shimomura έγινε γνωστός γιατί υπέστη hacking από τον Kevin Mitnick.

2.5.2 ΔΙΑΣΗΜΟΙ ΚΑΚΟΙ ΧΑΚΕΡ

Οι κακοί χάκερ είναι αυτοί οι οποίοι όταν βρουν μια τρύπα ή ένα ευάλωτο σημείο ενός λειτουργικού συστήματος, τότε θα προσπαθήσουν να κλέψουν αρχεία, να τα πειράξουν ή να τα καταστρέψουν. Οι κακοί χάκερ διώκονται από την Δίωξη Ηλεκτρονικού εγκλήματος.

Συνήθως αυτού του είδους οι χάκερ εργάζονται για εταιρείες ως υπεύθυνοι ασφαλείας των λειτουργικών συστημάτων. Τα λειτουργικά συστήματα αυτά μπορεί να είναι βάσεις δεδομένων, σελίδες και άλλα. Με την λαθραία εισχώρηση ενός χάκερ σε μια σελίδα ή βάσεις δεδομένων τότε αυτό μπορεί να έχει μεγάλο κόστος για μια εταιρεία. Από την άλλη όμως οι χάκερ βοηθούν στην εξέλιξη του παγκόσμιου ιστού και στην ίδρυση κορυφαίων τεχνολογιών.

1. Jonathan James (κωδικό όνομα «cOmrade»): Μόλις στα δεκάξι του χρόνια ο James καταδικάστηκε σε φυλάκιση για hacking.
2. Adrian Lamo: Ο Lamo είναι αυτός ο οποίος εισέβαλε στους οργανισμούς New York Times και Microsoft.
3. Kevin Mitnick: Ο Kevin είναι ο πιο περιζήτητος εγκληματίας ηλεκτρονικών προγραμμάτων των Ηνωμένων Πολιτειών.

4. Kevin Poulsen: Ο Poulsen έγινε γνωστός από την υποκλοπή που έκανε στις τηλεφωνικές γραμμές του Ραδιοσταθμού Kiss στο Λος Άντζελες. Η υποκλοπή αυτή του απέφερε πολλά δώρα μεταξύ των άλλων και μια ολοκαίνουργια Porche. Επίσης ο Poulsen είναι γνωστός ως Dark Dante.
5. Robbert Tappan Morris: Ο Robert είναι ο γιος ενός πρώην επιστήμονα της Αμερικανικής Κρατικής Υπηρεσίας Πληροφοριών. Αυτός είναι που δημιούργησε το πρώτο worm (σκουλήκι) υπολογιστών του διαδικτύου, το Morris Worm. (64. Η. Κοζιόκος - Σ. Καμήλος, 2010)

2.5.3 ΕΛΛΗΝΕΣ ΧΑΚΕΡΣ ΚΑΙ ΧΑΚΙΝΓΚ

Όλα ξεκίνησαν τα Χριστούγεννα του 1993, εκείνη την εποχή υπήρχαν συγκρούσεις που είχαν σχέση με την διαχείριση του δικτύου Αριάνδη στο Ερευνητικό Κέντρο Δημόκριτος. Τότε άγνωστοι εισέβαλαν στους κεντρικούς του κόμβους, αυτό είχε σαν αποτέλεσμα την απεριόριστη πρόσβαση των χρηστών στις υπηρεσίες του διαδικτύου.

Τον Νοέμβριο του 1998, μια νέα οργάνωση έκανε την εμφάνιση της η οποία ονομάζεται Δικτυακή Πάλη. Η Δικτυακή Πάλη έκανε επίθεση στο Υπουργείο Παιδείας. Στην αρχική ιστοσελίδα του Υπουργείου Παιδείας έκαναν ανάρτηση ενός κειμένου που ήταν καταγγελία εναντίον του Γεράσιμου Αρσένη, της κυβέρνησης, της αντιπολίτευσης, της αστυνομίας και των ακροδεξιών οργανώσεων. Η Δικτυακή Πάλη μετά από λίγους μήνες ξαναχτύπησε, στόχος της αυτή τη φορά οι σελίδες του Υπουργείου Εξωτερικών και του Υπουργείου Περιβάλλοντος, Χωροταξίας και Δημοσίων Έργων (ΥΠΕΧΩΔΕ). Οι επιθέσεις αυτές περιλάμβαναν κείμενα εναντίον των πολιτικών κομμάτων.

Τη 17 Φεβρουαρίου του 1999 έγινε επίθεση στο Υπουργείο Εξωτερικών από άγνωστους χάκερ. Με αυτόν τον τρόπο ήθελαν να διαμαρτυρηθούν οι χάκερ εναντίον της ελληνικής κυβέρνησης και να δείξουν την συμπαράσταση τους στον κουρδικό λαό. Αυτό έγινε λόγω του γεγονότος, ότι είχαν συλλάβει την προηγούμενη μέρα τον Οτζαλάν. Την περιγραφή που έβλεπαν οι επισκέπτες καθώς έμπαιναν στη σελίδα του Υπουργείου Εξωτερικών ήταν «Καλωσορίσατε στο Υπουργείο της Ξεφτίλας».

Οι Έλληνες χάκερ έχουν εκθέσει με τα χτυπήματα τους πολλές φορές και με παρόμοιο τρόπο, όπως τον παραπάνω, υπουργεία, κυβερνητικούς οργανισμούς, πανεπιστήμια, ερευνητικά ιδρύματα, επιχειρήσεις και ιδιώτες. Αυτό που κάνουν οι Έλληνες χάκερ είναι να εισβάλουν σε δίκτυα τα οποία δεν διαθέτουν τα επαρκή μέτρα ασφαλείας, να κάνουν παραμόρφωση της πρώτης σελίδας και να αφήνουν την δικτυακή τους σφραγίδα με το να γράφουν το ψευδώνυμο τους.

Τον Οκτώβριο του 1999 επίθεση δέχτηκε το Γεωδυναμικό Ινστιτούτο του Εθνικού Αστεροσκοπείου Αθηνών.

Τον Ιανουάριο του 2001, έγινε επίθεση στο Υπουργείο Εσωτερικών, το

οποίο μετά την επίθεση των χάκερ μετονομάστηκε σε Υπουργείο Κατασκόπευσης Πολιτών.

Τον Φεβρουάριο του 2000, Έλληνες χάκερς έκαναν επιθέσεις από υπολογιστές των πανεπιστημίων Αθηνών, Θεσσαλονίκης και Κρήτης, στο δίκτυο στρατιωτικών εγκαταστάσεων στην Αριζόνα, το οποίο προκάλεσε τον πανικό του Αμερικανικού Πενταγώνου. Το Ελληνικό Πεντάγωνο μετά από λίγους μήνες δέχτηκε επιθέσεις από υπολογιστές άλλων χωρών χωρίς να υπάρξουν συλλήψεις ή ζημιές.

Η πρώτη σύλληψη έγινε το Σεπτέμβριο του 2000, συνέλαβαν έναν φοιτητή του Πολυτεχνείου Ξάνθης, με την κατηγορία ότι έκανε εισβολή στο κέντρο του Εθνικού Ιδρύματος Ερευνών (ΕΙΕ), έκανε ροζ τηλέφωνα και αυτό είχε σαν αποτέλεσμα να εκτοξευθεί ο τηλεφωνικός λογαριασμός του ΕΙΕ στα ύψη.

Μετά από δύο χρόνια έγινε η σύλληψη δύο Ελλήνων φοιτητών στην Αγγλία με την κατηγορία ότι κατέστρεψαν αρχεία σε συστήματα εταιρείας στην Ελλάδα. (65. Ε. Ελευθεριάδου, 2004)

Υπάρχουν τρεις ομάδες Ελλήνων Χάκερ, οι οποίες είναι οι εξής :

Greek Hacking Scene: Οι Greek Hacking Scene είναι οι λεγόμενοι «αμαρτωλοί και κλέφτες του internet».

«Ξημεροβραδιάζονται μπροστά σε οθόνες, όπλα τους τα πληκτρολόγια. Πυρομαχικά τους, οι δυσνόητοι για το ευρύ κοινό κώδικες. Κίνητρο, το πάθος για το χάκινγκ και την Ελλάδα.»

Οι στόχοι τους είναι εκπαιδευτικοί και πολιτικοί. Οι εκπαιδευτικοί στόχοι είναι οι ιστοσελίδες και τα δίκτυα που προκαλούν ενδιαφέρον για τους νέους χάκερ. Και πολιτικοί στόχοι είναι αυτοί οι στόχοι που έχουν σχέση με τον εχθρό, δηλαδή τουρκικής, αλβανικής, και σκοπιανής ιδιοκτησίας.

Αυτό που κάνουν είναι να αφήνουν ένα μήνυμα, να αλλάζουν την ιστοσελίδα και να αναρτούν τα δικά τους λάβαρα. Η Greek Hacking Scene έχει κάνει τις εξής επιθέσεις :

1) Το καλοκαίρι του 2006 η Greek Hacking Scene έκανε επίθεση στο .tld Top Level Demain του .mk. Το .mk στις ιστοσελίδες του FYROM μεταφράζεται ως «Μακεδονία». Μετά το χτύπημα τους ότι τελείωνε σε .mk έγραφε «Macedonia is Greek» δηλαδή «Η Μακεδονία είναι Ελληνική», συμπεριλαμβανομένων κυβερνητικών, κρατικών και στρατιωτικών σελίδων.
2) Η Greek Hacking Scene έχει χτυπήσει την ιστοσελίδα της NASA, του στρατού των ΗΠΑ και άλλες. Στην ιστοσελίδα http://zone-h.org/archive/defacer=GHS/page=1 υπάρχουν με αποδείξεις τα 1070 χτυπήματα που έχει πραγματοποιήσει η Greek Hacking Scene.
3) Επίσης αναλαμβάνει την ευθύνη για τη δικτυακή επίθεση της 25ης Μαρτίου σε τουρκικά, σκοπιανά και άλλα sites, τα οποία ήταν νόμιμοι στόχοι. Η επίθεση στα 150 sites, τα οποία δεν είχαν σχέση μόνον με τον επετειακό χαρακτήρα της ημέρας.

Η Greek Hacking Scene αποτελείται από έξι άτομα.

«Τους συνδέει η κοινή αγάπη για τους υπολογιστές, τα δίκτυα, τη διασπορά της γνώσης και πάνω από όλα για την Ελλάδα.» Και στόχος τους είναι το κοινό να αντιληφθεί πως στην ομάδα αυτή ανήκουν όλοι οι Έλληνες.
(66. Π. Λιάκος, 2009)

Greek Secuirity Team: Οι Greek Secuirity Team είναι μια ομάδα Ελλήνων χάκερ που πραγματοποίησε δικτυακή επίθεση σε ένα server του CERN, στην Ελβετία, 100 μέτρα κάτω από την επιφάνεια της γης, όπου διεξαγόταν το μεγαλύτερο πείραμα όλων των εποχών. Αυτή η επίθεση μπορεί να έχει σχέση με τις κραυγές κάποιων οι οποίοι πιστεύουν ότι προκαλείται και δημιουργείται μέσω του πειράματος μια μεγάλη τρύπα η οποία θα καταπιεί τα πάντα ή μπορεί να έχει σχέση με τις εμπρηστικές δηλώσεις ταγού και οπαδών διαφωτιστικού χαρακτήρα. Αν και οι hackers αυτοί δεν είναι άτομα που υποστηρίζουν τέτοιες απόψεις.

Πολλά ελληνικά και ξένα μπλοκ, αλλά και ΜΜΕ, ασχολήθηκαν με το θέμα, έκαναν σχόλια στο κείμενο που άφησαν οι Έλληνες χάκερ στο server του CERN. Με το κείμενο στο CERN, αυτό που κάνει η ομάδα GST (Greek Security Team) είναι να γράφει εναντίον μιας άλλης ομάδας χάκερ η οποία ονομάζεται GHT (Greek Hacking Team). (67. Χ. Καρανίκας, 2008)

Οι Greek Secuirity Team (GST) κατάφεραν να παραβιάσουν υπολογιστικά συστήματα του Μεγάλου Επιταχυντή Αδρονίων, επιβεβαιώθηκε από τους αξιωματικούς του CERN.

Με την αποκάλυψη των βρετανικών εφημερίδων Times και Daily Telegraph, οι χάκερ παραποίησαν την ιστοσελίδα του CERN και χλεύαζαν τους υπεύθυνους ασφαλείας των υπολογιστών. Το μόνο που ήθελε η GST είναι να δείξει την μαύρη τρύπα που υπάρχει στην ασφάλεια του δικτύου και όχι να διαταράξουν τα σημαντικά πειράματα του LHC. (68. Α. Μοζ, 2008)

Greek Hacking Team ή (Greek Terrorits Team): Η Greek Hacking Team αποτελείται από τρία άτομα και τα ψευδώνυμα τους είναι ΝΙΚΡΑ, BAGPAPAS και FIRE.

Ο ΝΙΚΡΑ από την Greek Hacking Team πιστεύει πως :
«Hacker είναι αυτός ο οποίος χωρίς εξουσιοδότηση μπαίνει σε συστήματα Η/Υ και αντιγράφει τα αρχεία που έχει ή τα βλέπει.»

Ενώ αντίθετα ο cracker έχει αρκετά μεγάλη γνώση πάνω σε θέματα hacking, αυτό που τους κάνει να διαφέρουν από τους hacker είναι πως οι cracker βρίσκουν έτοιμα tools. Οι cracker εργάζονται για εταιρείες με σκοπό να μπουν στα αρχεία μιας αντίπαλης εταιρείας, να δουν αρχεία, να βρουν κωδικούς ή να καταστρέψουν τα πάντα.

Η Greek Hacking Team έχει κάνει επιθέσεις σε τουρκικά site, αυτό το κάνουν όχι γιατί έχουν κάποιο πρόβλημα με τους Τούρκους ή με τους άλλους γείτονες της Ελλάδας. Επειδή όταν κάνουν επιθέσεις οι γείτονες σε ελληνικά site τα μηνύματα που αφήνουν πίσω τους είναι προσβλητικά για την Ελλάδα και αυτό που κάνει η ομάδα αυτή να δίνει την απάντηση της μέσω των επιθέσεων που κάνει. Έχουν χτυπήσει site μόνο και μόνο για να γράψουν ένα

****TURKEY, ****SCOPIA και άλλα. Δηλώνουν πως το hacking τους αρέσει πολύ για αυτό το λόγο το κάνουν.

«Πιστεύουν επίσης πως το να παραβιάζεις και να μπαίνεις σε συστήματα Η/Υ είναι μέσα στο αίμα του Έλληνα, δηλαδή να θέλει να παραβιάζει και να έχει ότι μπορεί δωρεάν.»

Το hacking δεν θεωρείται για αυτούς παράνομο, γιατί πιστεύουν πως υποστηρίζουν την Ελλάδα μέσω του internet με αυτό που κάνουν.(69. Άγνωστος, 2010)

Μέσα από το http://blogthea.gr/NextStep/cracking-hacking-test-me-software/40490-iaecia-hacking-test-me.html δίνονται κάποιες συμβουλές από το site πως γίνεται το hacking. (70. Άγνωστος, 2010)

2.5.4 ΣΧΟΛΕΙΟ ΓΙΑ "ΧΑΚΕΡΣ"

Το 1997 ξεκίνησε τη λειτουργία της η πρώτη σχολή για χάκερ στο Λος Άντζελες, η σχολή αυτή είναι η Intense School. Σε αυτή τη σχολή οι μαθητές διδάσκονται πως να χρησιμοποιούν τα λειτουργικά συστήματα Microsoft και Cisco.

Η σχολή αυτή έχει δεκαπέντε μαθητές οι οποίοι είναι στελέχη επιχειρήσεων, ακαδημαϊκοί και στρατιωτικοί. Αυτοί κάνουν σεμινάρια για το πως μπορεί κάποιος να σπάσει έναν κωδικό με απόλυτη επιτυχία. Οι μαθητές για να παρακολουθήσουν τα μαθήματα αυτά, να λάβουν μέρος στις εξετάσεις και να γίνουν «Ηθικοί Χάκερ» με δίπλωμα, πλήρωσαν 40.000 δολάρια περίπου.

Οι μαθητές μέσα από τις αναζητήσεις τους σε βάσεις δεδομένων και μηχανές αναζήτησης, προσπαθούν να βρουν πληροφορίες για κάποιες εταιρείες, τα στελέχη και τα συστήματα τους.

Τα σεμινάρια της Intense School έχουν σκοπό την προετοιμασία των μαθητών για τις εξετάσεις, οι οποίες οργανώνονται από το Διεθνές συμβουλίο Ηλεκτρονικού Εμπορίου. Μόνο όταν κάποιος περάσει τις εξετάσεις αυτές τότε παίρνει δίπλωμα που τον ανακηρύσσει Πιστοποιημένο Ηθικό Χάκερ. Τα μαθήματα περιλαμβάνουν ενότητες που έχουν σχέση με το συμμετρικό σύστημα κρυπτογράφησης, η επικοινωνία με κώδικες και οι υπηρεσίες TCP. (71. Δ. Σκότης, 2004)

Η πιστοποίηση για το ηθικό χάκινγκ (ethical hacking) παρέχεται σε περισσότερες από 60 χώρες και αριθμεί χιλιάδες πιστοποιημένους επαγγελματίες. Για το ηθικό χάκινγκ διάφορα πανεπιστήμια έχουν μεταπτυχιακούς τίτλους, όμως το 2006 το πανεπιστήμιο Abertay της Σκωτίας ήταν το πρώτο που δημιούργησε σχολή για το ηθικό χάκινγκ και το πρόσθεσε ως τίτλο πτυχίου. (72. Μ. Μυστακίδου, 2009)

Το ethical hacking έχει κάποιους κώδικες, οι πιο σημαντικοί είναι οι παρακάτω:

1. Οι πληροφορίες πρέπει να είναι ελεύθερες σε όλους .

2. Η πρόσβαση σε πληροφορίες που μπορούν να είναι διδακτέες για το πώς λειτουργεί ο κόσμος πρέπει να είναι απεριόριστες.
3. Έλλειψη εμπιστοσύνης σε όλες τις μορφές εξουσίας.
4. Οι hackers πρέπει να κρίνονται από τις ικανότητες που έχουν στο hacking και όχι με βάση άλλα κριτήρια όπως το πτυχίο ή η ηλικία.
5. Μ' έναν υπολογιστή μπορεί να δημιουργηθεί τέχνη και ομορφιά.
6. Η ζωή μας μπορεί να αλλάξει προς το καλύτερο με τους υπολογιστές.

(73. Γ. Λάζου, 2008)

«Η διεθνής κοινότητα των χάκερ πιστεύει ότι η πρόσβαση στην πληροφορία αποτελεί παγκόσμιο κοινό αγαθό και ότι είναι ηθικό καθήκον τους να μοιράζονται τις ικανότητες τους τόσο δημιουργώντας λογισμικό ανοικτού κώδικα, όσο και διευκολύνοντας την πρόσβαση σε πληροφορίες και υπολογιστικούς πόρους, όπου αυτό είναι εφικτό. Πιστεύουν ότι το σπάσιμο και η εξερεύνηση ενός υπολογιστικού συστήματος, τόσο σε επίπεδο υλικού όσο και κυρίως λογισμικού είναι ηθικά αποδεκτή, εφόσον ο χάκερ δεν διαπράττει κλοπή, βανδαλισμό ή παραβίαση εμπιστευτικότητας. Για τους χάκερ, όποιος αξίζει αυτόν τον τίτλο, είναι στην πραγματικότητα ένας έξυπνος προγραμματιστής ή άτομο με ιδιαίτερες ικανότητες στην κατανόηση και το χειρισμό υπολογιστικών συστημάτων. Δεν αποδέχονται σε καμιά περίπτωση, ότι οι πράξεις ενός χάκερ έχουν κακόβουλους στόχους και αυτή είναι η διαφορά που τους διακρίνει από τους κράκερς.» (74. Χ. Τάππα, 2009).

ΚΕΦΑΛΑΙΟ 3

3.1 ΜΕΘΟΔΟΛΟΓΙΑ ΤΗΣ ΕΡΕΥΝΑΣ

Οι μικρομεσαίες επιχειρήσεις (ΜΜΕ) στη σημερινή εποχή πρέπει να λειτουργούν αποτελεσματικά και να προσαρμόσουν τις λειτουργικές δομές τους στο επιχειρηματικό τοπίο. Προσδιορίζουν τις ανάγκες κάθε τμήματος -έστω κι αν αποτελείται από ένα άτομο- και με τη σωστή αξιοποίηση της τεχνολογίας και του διαδικτύου αυξάνουν την εταιρική ισχύ τους.

Οι ΜΜΕ χρησιμοποιούν το διαδίκτυο (Internet) για την ανάπτυξη της επιχείρησης τους, για καλύτερη εξυπηρέτηση των πελατών τους αλλά και για τη διαφήμιση των προϊόντων και των υπηρεσιών τους. Το μεγαλύτερο μέρος των ΜΜΕ έχουν εταιρική ιστοσελίδα.

Μέσω της εταιρικής ιστοσελίδας το καταναλωτικό κοινό μπορεί να μάθει περισσότερες πληροφορίες για την εταιρεία και τα προϊόντα/υπηρεσίες που παρέχει. Επίσης μέσω της ιστοσελίδας μπορεί να βρει τους τρόπους επικοινωνίας (τηλέφωνα και e-mail) για περαιτέρω πληροφόρηση.

Οι επιχειρήσεις για τη δική τους καλύτερη λειτουργία δημιουργούν τοπικά δίκτυα ώστε να έχουν πρόσβαση σε όλα τα αρχεία και τα δεδομένα, να μπορούν οι εργαζόμενοι να επικοινωνούν και να συνεργάζονται πιο άμεσα, ακόμη κι αν βρίσκονται σε μεγάλες αποστάσεις.

Οι ΜΜΕ παρά το γεγονός ότι χρησιμοποιούν τα τοπικά δίκτυα και το διαδίκτυο για τη διευκόλυνση της λειτουργίας τους, αγνοούν τους κινδύνους και τα προβλήματα που μπορεί να τους προκαλέσουν.

Στο διαδίκτυο υπάρχουν οι hackers και οι crackers, οι οποίοι ελλοχεύουν με σκοπό να υποκλέψουν προσωπικά και επαγγελματικά δεδομένα. Οι παραβιάσεις οι οποίες γίνονται μέσω του διαδικτύου και μπορούν να προκαλέσουν προβλήματα σε μια επιχείρηση είναι τα εξής :

- Υποκλοπές επικοινωνιών
- Μη εξουσιοδοτημένη πρόσβαση στο δίκτυο
- Κατάρρευση του δικτύου, η οποία μπορεί να δημιουργήσει πολλά προβλήματα στην επιχείρηση με την απότομη διακοπή της σύνδεσης με το διαδίκτυο
- Εκτέλεση κακόβουλου λογισμικού, δηλαδή η παραβίαση που γίνεται από κάποιο ιό ή κάποιο σκουλήκι.
- Παραπλάνηση / ψευδής δήλωση, αυτό γίνεται όταν δίνονται εμπιστευτικές πληροφορίες σε λάθος άτομα.

Όλες οι παραπάνω παραβιάσεις του δικτύου μπορούν να αντιμετωπιστούν με τους εξής τρόπους:

- Κωδικοί πρόσβασης, όταν τους αλλάζουν συχνά πετυχαίνουν ως ένα βαθμό την ασφάλεια του δικτύου.

- Αντιϊκά προγράμματα, τα γνωστά σε όλους antivirus, τα οποία μπορούν να προστατέψουν από ιούς ή σκουλήκια του διαδικτύου.
- Κρυπτογράφηση δεδομένων, με την οποία ένα μήνυμα διαβάζεται μόνο από τον τελικό αποδέκτη.
- Τείχος προστασίας (firewall), ένα τείχος προστασίας μπορεί να είναι software ή hardware.
- Ψηφιακά πιστοποιητικά, χρησιμοποιούνται για την πιστοποίηση των ατόμων που στέλνουν διάφορες πληροφορίες μέσω διαδικτύου. Η πιστοποίηση αυτή, βοηθάει να καταλάβει ο χρήστης πως το πρόσωπο που επικοινωνεί μαζί του μέσω διαδικτύου είναι πραγματικά αυτός που δηλώνει ότι είναι και όχι κάποιος άλλος.
- Προστατευμένες σελίδες, αν μια σελίδα είναι προστατευμένη τότε κατά την είσοδο κάποιου στην σελίδα αυτή, ενημερώνεται με μήνυμα πως η σελίδα που επισκέπτεται είναι μια σελίδα ασφαλείας.
- IDS, είναι συστήματα πρόληψης επιθέσεων. Τα συστήματα αυτά έχουν την ικανότητα να ανιχνεύουν τις περίεργες δικτυακές κινήσεις οι οποίες γίνονται σε έναν υπολογιστή ή στο δίκτυο. Τα IDS ανιχνεύουν μια επίθεση και ενημερώνουν τον διαχειριστή ασφαλείας για την επίθεση αυτή, αλλά δεν έχουν την δυνατότητα να την εξουδετερώσουν.
- IPS, είναι και αυτά συστήματα πρόσληψης επιθέσεων. Η διαφορά τους από τα IDS είναι πως με το που θα ανιχνεύσουν μια επίθεση μπορούν να την εξουδετερώσουν αυτόματα.

Οι περισσότερες ΜΜΕ αγνοούν πολλά από τα παραπάνω και είναι λογικό, γιατί δεν υπάρχει ενημέρωση προς τις επιχειρήσεις όσον αφορά την ασφάλεια του δικτύου τους. Επίσης πολλές από αυτές πιστεύουν πως κάτι τέτοιο δεν πρόκειται να συμβεί σε αυτούς και ότι κάνεις δεν θα ασχοληθεί με τα δεδομένα και τις πληροφορίες που διαθέτουν, όμως κάνουν λάθος.

3.2 ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΕΡΕΥΝΑΣ

Η ΑΣΦΑΛΕΙΑ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΕ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

1) Τι είδους επιχείρηση είστε;
   - □ Δικηγορικό γραφείο
   - □ Λογιστικό γραφείο
   - □ Ταξιδιωτικό πρακτορείο
   - □ Άλλο

2) Έχετε πρόσβαση στο Ιντερνέτ σε μόνιμη βάση?
   - □ ΝΑΙ

□ ΟΧΙ

3) Η επιχείρησή σας έχει ιστοσελίδα στο Ίντερνετ;
   □ ΝΑΙ
   □ ΟΧΙ

   Αν ναι, για ποιο λόγο……..
   .....……
   ….
   ……
   ….

4) Η ιστοσελίδα σας είναι προστατευμένη, χρησιμοποιεί το https protocol;
   □ ΝΑΙ
   □ ΟΧΙ
   □ ΔΕΝ ΥΠΑΡΧΕΙ

5) Η επιχείρησή σας αποθηκεύει προσωπικά δεδομένα των πελατών σας (λογαριασμούς κτλ);
   □ ΝΑΙ
   □ ΟΧΙ

6) Η επιχείρησή σας έχει κάνει συμβόλαιο με κάποια εταιρεία προστασίας ιστοσελίδων για ιούς και χάκερς;
   □ ΝΑΙ
   □ ΟΧΙ

7) Χρησιμοποιείται κάποια εξειδικευμένη εφαρμογή;
   □ ΝΑΙ
   □ ΟΧΙ

   Αν ναι, για ποιο σκοπό.....
   ……
   …..……
   ……..

8) Για ποίους λόγους χρησιμοποιείται το Διαδίκτυο;
   □ Επικοινωνία (e-mail)
   □ Συναλλαγές (οικονομικές ή άλλες)
   □ Συναλλαγές με το δημόσιο
   □ Αναζήτηση πληροφοριών

9) Τι είδους προστασία χρησιμοποιείται για το δίκτυο υπολογιστών που έχετε;
   - □ Κωδικοί πρόσβασης
   - □ Αντιϊκά προγράμματα (antivirus)
   - □ Τείχος προστασίας (firewall)
   - □ Ψηφιακά πιστοποιητικά
   - □ Κάτι άλλο……...
…...…….
……
…….

10) Χρησιμοποιείται server (κεντρικό εξυπηρετητή υπολογιστή);
   - □ ΝΑΙ
   - □ ΟΧΙ

   Αν ναι, γιατί…….
   ……
   ….……
   ……..

11) Ο κάθε εργαζόμενος έχει το δικό του κωδικό πρόσβασης;
   - □ ΝΑΙ
   - □ ΟΧΙ

12) Πόσο συχνά αλλάζετε τον κωδικό πρόσβασης;
   - □ Κάθε μήνα
   - □ Κάθε 3 μήνες
   - □ Κάθε 6 μήνες
   - □ Κάθε χρόνο
   - □ Κάτι άλλο…….....

……
……
……

13) Τι τείχος προστασίας χρησιμοποιείται;
   - □ Software
   - □ Hardware
   - □ Και τα δύο
   - □ Κανένα από τα δύο

14) Έχετε σύστημα ασφαλείας που ελέγχει/ ανιχνεύει παραβιάσεις από κακόβουλο λογισμικό (ιοί);

□ ΝΑΙ
□ ΟΧΙ

15) Πόσο συχνά κάνετε έλεγχο στο δίκτυό σας για κάποιο κακόβουλο λογισμικό;
□ Ποτέ
□ Κάθε εβδομάδα
□ Κάθε μήνα
□ Κάτι άλλο……...
……
……
…....

16) Πόσο ασφαλή πιστεύετε ότι είναι τα δεδομένα- στοιχεία των πελατών σας;
□ Καθόλου
□ Λίγο
□ Μέτρια
□ Πολύ
□ Πάρα πολύ

17) Πιστεύετε ότι η ασφάλεια των δεδομένων σας που έχετε είναι ικανή να αντιμετωπίσει τους ιούς που ίσως προκύψουν;
□ ΝΑΙ
□ ΟΧΙ
□ Δεν γνωρίζω

18) Σε περίπτωση μόλυνσης από ιό, το κόστος για την επιχείρησή σας ήταν
□ Υψηλό
□ Χαμηλό

19) Η ασφάλεια του δικτύου σας αποτελεί σημαντικό παράγοντα για την επιχείρησή σας;
□ Συμφωνώ
□ Διαφωνώ
□ Δεν γνωρίζω/ Δεν απαντώ

20) Έχετε κάποιο άτομο που ασχολείται με την ασφάλεια;
□ ΝΑΙ
□ ΟΧΙ

21) Έχει συμμετάσχει κάποιος από την επιχείρησή σας έστω σε ένα σεμινάριο περί ασφάλειας;

□ ΝΑΙ
□ ΟΧΙ

Το ερωτηματολόγιο απευθύνεται στις μικρομεσαίες επιχειρήσεις που διαθέτουν τοπικό δίκτυο, on line προγράμματα και σύνδεση στο διαδίκτυο σε μόνιμη βάση. Το ερωτηματολόγιο αυτό θέλει να αποδείξει την άγνοια των περισσότερων μικρομεσαίων επιχειρήσεων όσον αφορά την ασφάλεια τοπικών δικτύων και πληροφοριακών συστημάτων. Επίσης φαίνονται οι πολιτικές ασφαλείας που χρησιμοποιεί η κάθε μικρομεσαία επιχείρηση για να προφυλάξει το δίκτυο της αλλά και τις πολιτικές ασφαλείας που χρησιμοποιεί για να προφυλαχτεί από τους κινδύνους του διαδικτύου.

Η ερεύνα διεξήχθη στα Ιωάννινα και στην Κέρκυρα και σε δείγμα 50 μικρομεσαίων επιχειρήσεων. Οι επιχειρήσεις έδειξαν ενδιαφέρον για την έρευνα. Όταν τους δόθηκε το ερωτηματολόγιο για να το απαντήσουν αρκετές δυσκολεύτηκαν και έκαναν ερωτήσεις ώστε να τους δοθεί κάποια βοήθεια για να απαντήσουν, οι περισσότεροι αφού απαντούσαν το ερωτηματολόγιο παραδεχόταν ότι πολλά απ' όσα αναφερόταν δεν τα γνώριζαν και γι' αυτό το λόγο έκαναν διευκρινιστικές ερωτήσεις. Ακόμη θεωρούσαν ενδιαφέρον το θέμα της έρευνας και ότι ήταν πολλά στοιχεία που αγνοούσαν, τα οποία σχετίζονται με την ασφάλεια μιας επιχείρησης στο διαδίκτυο. Κάποιες επιχειρήσεις που τους ζητήθηκε να απαντήσουν, αρνήθηκαν για δικούς τους λόγους χωρίς να τους αναφέρουν.

Στην αρχή, με την πρώτη ερώτηση γίνεται η γνωριμία με την επιχείρηση, δηλαδή γνωστοποιείται το είδος της μικρομεσαίας επιχείρησης. Η οποία μικρομεσαία επιχείρηση μπορεί να είναι δικηγορικό γραφείο, λογιστικό γραφείο, ταξιδιωτικό πρακτορείο και τελευταία επιλογή το άλλο. Στην θέση του άλλου περιλαμβάνονται όλες οι μικρομεσαίες επιχειρήσεις οι οποίες δεν αναφέρθηκαν παραπάνω. Γιατί στο δείγμα μπορεί να υπάρχουν διαφορετικού είδους μικρομεσαίες επιχειρήσεις, ώστε το αποτέλεσμα που θα βγει από την έρευνα να είναι αντιπροσωπευτικό της πραγματικότητας.

Η δεύτερη ερώτηση είναι αν έχουν πρόσβαση στο internet σε μόνιμη βάση. Η απάντηση που αναμένεται ότι θα δοθεί από τις πιο πολλές μικρομεσαίες επιχειρήσεις είναι πως ναι, έχουν πρόσβαση στο internet σε μόνιμη βάση.

Στην τρίτη ερώτηση ρωτήθηκαν, αν η μικρομεσαία επιχείρηση διαθέτει ιστοσελίδα στο internet. Η απάντηση που αναμένεται πως θα δοθεί είναι ότι οι περισσότερες μικρομεσαίες επιχειρήσεις διαθέτουν εταιρική ιστοσελίδα.

Στην επόμενη ερώτηση ρωτήθηκαν αν οι μικρομεσαίες επιχειρήσεις οι οποίες διαθέτουν εταιρικές ιστοσελίδες, οι ιστοσελίδες τους αυτές είναι προστατευμένες, δηλαδή αν χρησιμοποιούν https protocol. Η απάντηση που αναμένεται ότι θα δοθεί είναι πως η ιστοσελίδα τους δεν είναι προστατευμένη,

δηλαδή δεν χρησιμοποιούν https protocol. Αλλά όμως θα ήταν καλό για τις μικρομεσαίες επιχειρήσεις να χρησιμοποιούν στις εταιρικές τους ιστοσελίδες το https protocol, ώστε να προστατεύουν την εταιρική τους ιστοσελίδα από τους κινδύνους του διαδικτύου.

Η πέμπτη ερώτηση είναι αν η μικρομεσαία επιχείρηση αποθηκεύει προσωπικά δεδομένα των πελατών της. Τα προσωπικά δεδομένα μπορεί να είναι όνομα, επώνυμο, τηλέφωνο, διεύθυνση, ΑΦΜ, λογαριασμοί τραπέζης, και πολλά άλλα. Η απάντηση που αναμένεται από αυτήν την ερώτηση είναι πως οι περισσότερες μικρομεσαίες επιχειρήσεις αποθηκεύουν προσωπικά δεδομένα των πελατών τους. Γιατί σε μία άλλη πιθανή συνάντηση μεταξύ τους, η επιχείρηση να διαθέτει τα απαραίτητα στοιχεία που αφορούν τον πελάτη. Ώστε όταν θα ξανάρθει σε επαφή με έναν συγκεκριμένο πελάτη να ξέρει για παράδειγμα κατά πόσο ο συγκεκριμένος πελάτης είναι φερέγγυος ως προς την επιχείρηση ή όχι.

Στην έκτη ερώτηση ρωτήθηκαν, αν η επιχείρηση έχει κάνει συμβόλαιο με κάποια εταιρεία προστασίας ιστοσελίδων για ιούς και hackers. Βέβαια η απάντηση που αναμένεται ότι θα δοθεί είναι πως δεν έχουν κάνει συμβόλαιο με κάποια εταιρία προστασίας ιστοσελίδων από ιούς και hackers, γιατί οι περισσότερες μικρομεσαίες επιχειρήσεις αγνοούν τους hackers και πιστεύουν πως μια επίθεση ενός hacker δεν θα συμβεί ποτέ στην δικιά τους επιχείρηση, το θεωρούν απίθανο κάτι τέτοιο. Κάθε μικρομεσαία επιχείρηση όπως και κάθε επιχείρηση πρέπει να κάνει συμβόλαιο με κάποια εταιρεία προστασίας ιστοσελίδων για ιούς και hackers, με σκοπό την προστασία του δικτύου τους και πολύ περισσότερο των δεδομένων τους. Αλλά παρ' όλα αυτά ελάχιστές είναι αυτές οι οποίες ενδιαφέρονται για την ασφάλεια του δικτύου τους και την προστασία των δεδομένων τους.

Στην έβδομη ερώτηση ρωτήθηκαν αν η επιχείρηση χρησιμοποιεί κάποια εξειδικευμένη εφαρμογή. Οι εξειδικευμένες εφαρμογές βοηθούν την επιχείρηση ώστε μερικές εργασίες να γίνονται από ένα συγκεκριμένο σύστημα, οι εργασίες αυτές είναι σίγουρες και γίνονται καθημερινά από μία επιχείρηση. Για παράδειγμα το κλείσιμο εισιτηρίων που έχουν τα ταξιδιωτικά πρακτορεία και τα μηχανογραφημένα βιβλία εσόδων εξόδων που έχουν τα λογιστικά γραφεία. Η κάθε μικρομεσαία επιχείρηση μπορεί να έχει την δική της εξειδικευμένη εφαρμογή με σκοπό την ομαλή και γρήγορη διεκπεραίωση των εργασιών της. Η απάντηση που αναμένεται ότι θα δοθεί σε αυτή την ερώτηση είναι πως οι πιο πολλές μικρομεσαίες επιχειρήσεις δεν χρησιμοποιούν κάποια εξειδικευμένη εφαρμογή.

Στην όγδοη ερώτηση, ρωτήθηκαν για ποιους λόγους η μικρομεσαία επιχείρηση χρησιμοποιεί το διαδίκτυο. Οι λόγοι αυτοί μπορεί να είναι επικοινωνία (e-mail), συναλλαγές οικονομικές ή άλλες, συναλλαγές με το δημόσιο και αναζήτηση πληροφοριών. Οι λόγοι για τους οποίους αναμένεται πως μια επιχείρηση χρησιμοποιεί το διαδίκτυο είναι για την επικοινωνία με τους πελάτες ή τους προμηθευτές της και αναζήτηση πληροφοριών. Και λιγότερο ή

και καθόλου οι μικρομεσαίες επιχειρήσεις χρησιμοποιούν τις συναλλαγές (οικονομικές ή άλλες) και τις συναλλαγές με το δημόσιο.

Στην συνέχεια ρωτήθηκαν, τι είδους προστασία χρησιμοποιούν για το δίκτυο υπολογιστών που έχουν. Οι απαντήσεις που αναμένονται στην ερώτηση αυτήν είναι κωδικοί πρόσβασης, αντιϊκά προγράμματα (antivirus), τείχος προστασίας (firewall) και ψηφιακά πιστοποιητικά. Και σε αυτήν την ερώτηση οι μικρομεσαίες επιχειρήσεις είχαν την δυνατότητα να επιλέξουν πάνω από ένα. Η αναμενόμενη απάντηση από τις περισσότερες μικρομεσαίες επιχειρήσεις είναι πως χρησιμοποιούν κωδικούς πρόσβασης και αντιικά προγράμματα (antivirus), είναι οι πιο διαδεδομένοι τρόποι ασφαλείας και πολλές από τις μικρομεσαίες επιχειρήσεις τις χρησιμοποιούν. Από την άλλη, λίγες ή και καμία θα χρησιμοποιεί τείχος προστασίας και ψηφιακά πιστοποιητικά, γιατί αυτές είναι πιο εξελιγμένες πολιτικές ασφαλείας που ελάχιστες επιχειρήσεις γνωρίζουν και χρησιμοποιούν. Υπάρχουν και άλλες πολιτικές ασφαλείας πιο εξελιγμένες από τις παραπάνω, όπως είναι τα IDS και τα IPS. Τα IDS έχουν την δυνατότητα να ανιχνεύουν μια επίθεση και να ειδοποιούν τον τεχνικό ασφαλείας, αλλά δεν μπορούν να την σταματήσουν.

Από την άλλη τα IPS είναι η εξελιγμένη μορφή ενός IDS. Το IPS μόλις ανιχνεύσει μια επίθεση έχει την δυνατότητα να την σταματήσει αυτόματα.

Η δέκατη ερώτηση είναι αν η επιχείρηση χρησιμοποιεί server (κεντρικό εξυπηρετητή υπολογιστή). Τι είναι ο server?

«Εξυπηρετητής (server): Είναι οι υπολογιστές που διαδραματίζουν το σημαντικότερο ρόλο σε ένα δίκτυο, καθώς διαθέτουν τους απαιτούμενους πόρους (εφαρμογές, προγράμματα) και τις τεχνικές προδιαγραφές (γρήγορο επεξεργαστή, ισχυρή μνήμη, μεγάλο αποθηκευτικό χώρο) για να ικανοποιήσουν τις ανάγκες των σταθμών εργασίας και των χρηστών του δικτύου.» (75. Β. Γεωργίου, 2005)

Η απάντηση που αναμένεται είναι πως οι περισσότερες μικρομεσαίες επιχειρήσεις χρησιμοποιούν server (κεντρικό υπολογιστή) γιατί έτσι επιτυγχάνεται η ομαλή λειτουργία της επιχείρησης .

Στην επόμενη ερώτηση ρωτήθηκαν, αν ο κάθε εργαζόμενος έχει το δικό του κωδικό πρόσβασης. Η απάντηση που αναμένεται από τις περισσότερες μικρομεσαίες επιχειρήσεις, είναι πως ο κάθε εργαζόμενος δεν έχει το δικό του κωδικό πρόσβασης και πως υπάρχει ένας κωδικός για όλους τους εργαζομένους της επιχείρησης. Το πιο ασφαλές για μία επιχείρηση θα ήταν ο κάθε εργαζόμενος στην κάθε επιχείρηση να έχει τον δικό του κωδικό πρόσβασης και αυτόν τον κωδικό πρέπει να τον αλλάζει όσο πιο συχνά γίνεται.

Στην συνέχεια ρωτήθηκαν, πόσο συχνά η κάθε μικρομεσαία επιχείρηση αλλάζει τον κωδικό πρόσβασης στα προγράμματα της ή στον Η/Υ. Οι απαντήσεις που υπάρχουν σε αυτήν την ερώτηση είναι κάθε μήνα, κάθε τρεις μήνες, κάθε 6 μήνες, κάθε χρόνο και κάτι άλλο (στο οποίο μπορεί η κάθε επιχείρηση να γράψει οποίο χρονικό διάστημα θέλει και το οποίο δεν αναφέρεται στα παραπάνω). Η απάντηση που αναμένεται από τις περισσότερες

μικρομεσαίες επιχειρήσεις είναι πως αλλάζουν τον κωδικό πρόσβασης κάθε μήνα ή κάθε χρόνο, είναι οι δύο πιο πιθανές απαντήσεις που μπορούν να δοθούν. Η κάθε επιχείρηση θα ήταν ασφαλές να αλλάζει τον κωδικό πρόσβασης όσο πιο συχνά γίνεται, αν είναι εύκολο κάθε εβδομάδα ή και ακόμα και κάθε μήνα.

Στην συνέχεια ρωτήθηκαν, τι τείχος προστασίας χρησιμοποιεί η επιχείρηση. Οι απαντήσεις που υπάρχουν είναι software, hardware, και τα δύο και τέταρτη επιλογή κανένα από τα δύο. Η απάντηση που αναμένεται ότι θα δοθεί από τις περισσότερες επιχειρήσεις είναι πως χρησιμοποιούν software τείχος προστασίας, δηλαδή πρόγραμμα τείχος προστασίας.

Στην συνέχεια ρωτήθηκαν, αν έχουν σύστημα ασφαλείας που ελέγχει/ ανιχνεύει παραβιάσεις από κακόβουλο λογισμικό (ιοί). Η απάντηση που αναμένεται ότι θα δοθεί από τις περισσότερες μικρομεσαίες επιχειρήσεις είναι ότι ναι διαθέτουν σύστημα ασφαλείας που ελέγχει/ανιχνεύει παραβιάσεις από κακόβουλο λογισμικό (ιοί).

Μετά ρωτήθηκαν, πόσο συχνά οι μικρομεσαίες επιχειρήσεις κάνουν έλεγχο στο δίκτυο τους για κάποιο κακόβουλο λογισμικό. Οι επιλεγόμενες απαντήσεις είναι πότε, κάθε εβδομάδα, κάθε μήνα και τέλος κάτι άλλο (που περιέχει χρονικά διαστήματα που δεν αναφέρονται παραπάνω). Αυτό που αναμένεται ότι θα απαντήσουν οι περισσότερες μικρομεσαίες επιχειρήσεις είναι πως ποτέ δεν κάνουν έλεγχο στο δίκτυο τους για κάποιο κακόβουλο λογισμικό, γιατί δεν γνωρίζουν τον τρόπο για να κάνουν τον έλεγχο του δικτύου τους.

Στην επόμενη ερώτηση ζητήθηκε από τις μικρομεσαίες επιχειρήσεις να απαντήσουν πόσο ασφαλή πιστεύουν ότι είναι τα δεδομένα-στοιχεία των πελατών τους. Οι απαντήσεις ανάμεσα στις οποίες μπορούν να επιλέξουν είναι καθόλου, λίγο, μέτρια, πολύ, πάρα πολύ. Αυτό που αναμένεται ότι θα απαντήσουν οι περισσότερες μικρομεσαίες επιχειρήσεις είναι πως τα δεδομένα-στοιχεία των πελατών τους είναι πολύ ασφαλή. Και αυτό γιατί πιστεύουν ότι διαθέτουν τις αναγκαίες πολιτικές ασφαλείας που τους προστατεύουν από τους κινδύνους του διαδικτύου, αλλά όμως κάνουν λάθος. Για να είναι ασφαλή τα δεδομένα τους πρέπει να χρησιμοποιούν εξελιγμένες μορφές ασφαλείας. Άλλα όμως αυτό που λείπει πιο πολύ από τις επιχειρήσεις είναι η ενημέρωση όσον αφορά τις πολιτικές ασφαλείας ώστε να είναι σε θέση να προστατέψουν σωστά το δίκτυο τους.

Η επόμενη ερώτηση είναι αν πιστεύουν πως η ασφάλεια των δεδομένων που έχουν είναι ικανή να αντιμετωπίσει τους ιούς που ίσως προκύψουν. Οι απαντήσεις στην ερώτηση αυτή είναι ναι, όχι και το δεν γνωρίζω. Η απάντηση που αναμένεται ότι θα δώσουν οι περισσότερες μικρομεσαίες επιχειρήσεις είναι πως ναι, δηλαδή ότι η ασφάλεια των δεδομένων που διαθέτουν είναι ικανή να αντιμετωπίσει τους ιούς που ίσως προκύψουν.

Στην επόμενη ερώτηση ρωτήθηκαν, αν στο παρελθόν είχαν μολυνθεί από κάποιο ιό και πόσο ήταν το κόστος για την επιχείρηση, δηλαδή αν ήταν υψηλό ή χαμηλό. Η απάντηση που αναμένεται από τις περισσότερες μικρομεσαίες

επιχειρήσεις είναι πως όταν μολύνθηκαν από ιό, το κόστος για την επιχείρηση τους ήταν υψηλό και αυτό γιατί δεν είχαν τις κατάλληλες πολιτικές ασφαλείας για να προστατέψουν το δίκτυο τους.

Στην συνέχεια ρωτήθηκαν, κατά πόσο η ασφάλεια του δικτύου τους αποτελεί σημαντικό παράγοντα για την επιχείρηση τους. Οι απαντήσεις που τους δόθηκαν να επιλέξουν είναι συμφωνώ, διαφωνώ, και το δεν γνωρίζω/δεν απαντώ. Αυτό που αναμένεται ότι θα απαντήσουν οι περισσότερες μικρομεσαίες επιχειρήσεις, είναι πως συμφωνούν, δηλαδή ότι η ασφάλεια του δικτύου τους αποτελεί σημαντικό παράγοντα για την επιχείρηση τους. Και αυτό συμβαίνει γιατί οι επιχειρήσεις θέλουν να είναι προστατευμένα τα δεδομένα τους από τους ιούς, τους hackers και τους crackers.

Η προτελευταία ερώτηση είναι αν έχουν άτομο στην επιχείρηση τους που να ασχολείται με την ασφάλεια του δικτύου τους. Οι απαντήσεις που μπορούν να επιλέξουν είναι ναι και όχι. Η απάντηση που αναμένεται είναι πως όχι, δηλαδή δεν έχουν άτομο στην επιχείρηση τους που να ασχολείται με την ασφάλεια του δικτύου τους. Παρόλο που στην παραπάνω ερώτηση υποτέθηκε πως για τις περισσότερες μικρομεσαίες επιχειρήσεις η ασφάλεια του δικτύου τους αποτελεί σημαντικό παράγοντα για αυτούς άλλα παρόλα ταύτα όμως δεν έχουν άτομο που να ασχολείται με την ασφάλεια του δικτύου τους.

Η τελευταία ερώτηση είναι αν έχει συμμετάσχει κάποιος από την επιχείρηση τους έστω και σε ένα σεμινάριο περί ασφάλειας. Η αναμενόμενη απάντηση από τις περισσότερες μικρομεσαίες επιχειρήσεις, είναι πως δεν έχει συμμετάσχει κανένας από την επιχείρηση τους σε σεμινάριο περί ασφαλείας και αυτό γιατί αγνοούν τους κινδύνους του διαδικτύου που υπάρχουν και δεν έχουν ενημέρωση όσον άφορα την ασφάλεια του δικτύου τους και των δεδομένων τους.

Στο τέταρτο κεφάλαιο που ακολουθεί περιλαμβάνει τις ερωτήσεις του ερωτηματολογίου και τα αποτελέσματα της έρευνας σε κάθε ερώτηση.

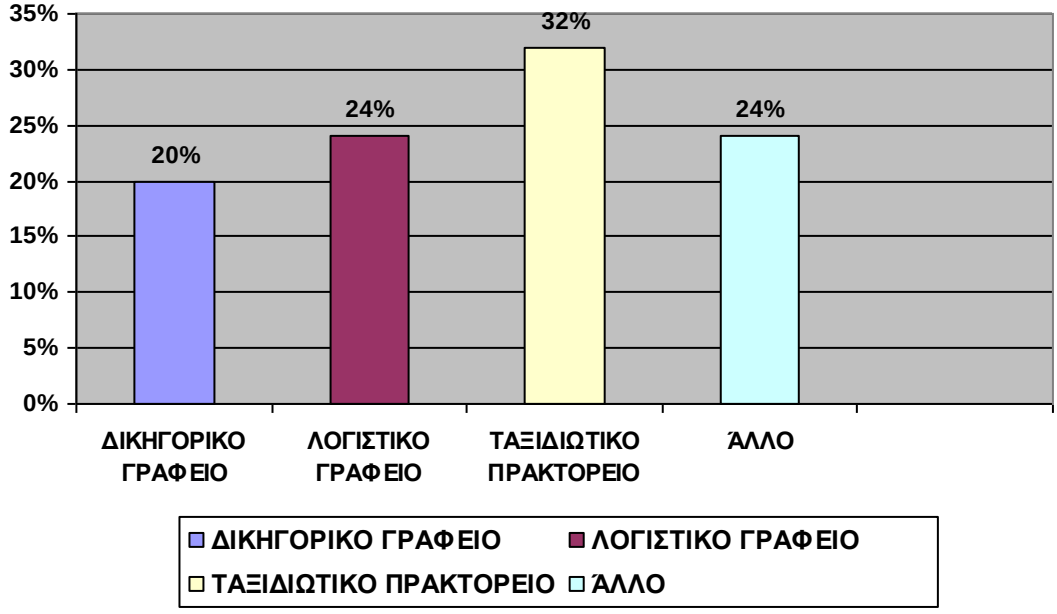
ΚΕΦΑΛΑΙΟ 4

4.1 ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΡΕΥΝΑΣ

Σ' αυτό το κεφάλαιο παρουσιάζονται τα στατιστικά στοιχεία που προέκυψαν από την έρευνα.

1. Τι είδους επιχείρηση είστε;

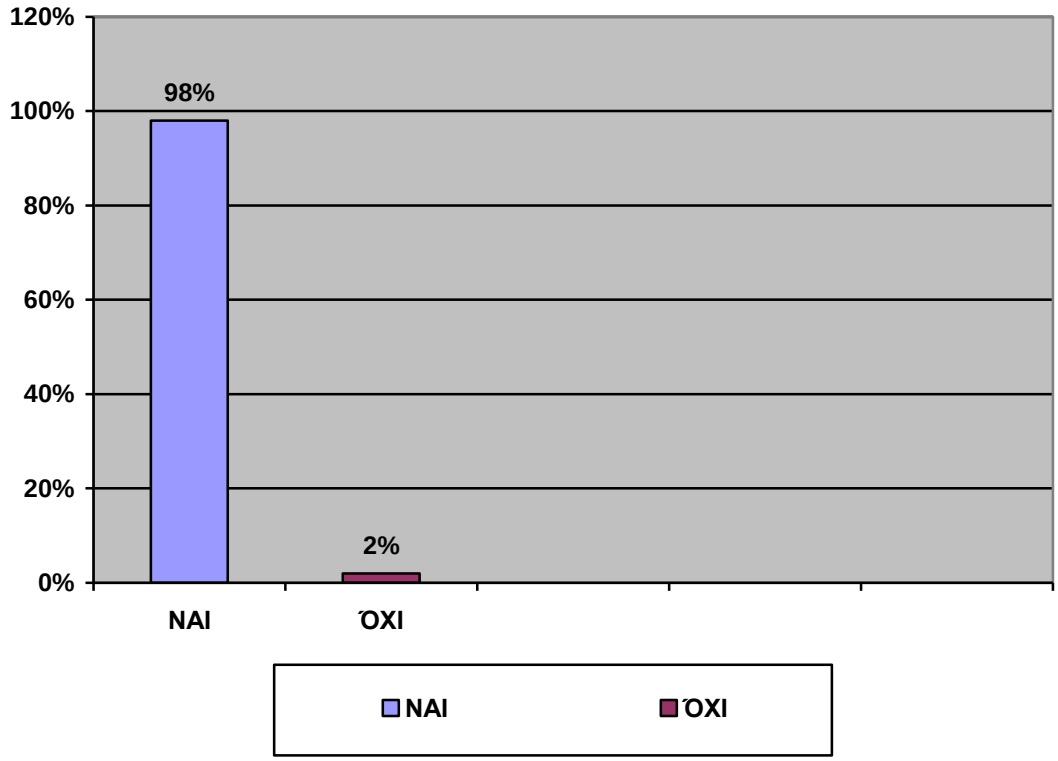
Γράφημα 1: Είδος επιχείρησης



Στην έρευνα αναλύονται τα στοιχεία που δόθηκαν απο 50 μικρομεσαίες επιχειρήσεις οι οποίες βρίσκονται στις περιοχές Ιωάννινα και Κέρκυρα. Από το διάγραμμα φαίνεται ότι το 20% των μικρομεσαίων επιχειρήσεων είναι δικηγορικά γραφεία, το 24 % λογιστικά γραφεία, το 32 % ταξιδιωτικά πρακτορεία και το 24% άλλο, στο οποίο περιλαμβάνονται μικρομεσαίες επιχειρήσεις οι οποίες είναι ασφαλιστικές εταιρίες και εμπορικές και τεχνικές εταιρίες. Αυτό έγινε με σκοπό να υπάρχουν πολλές και διαφορετικού είδους μικρομεσαίες επιχειρήσεις, ώστε το αποτέλεσμα της έρευνας να πλησιάζει περισσότερο στην πραγματικότητα.

2. Έχετε πρόσβαση στο Ιντερνέτ σε μόνιμη βάση;

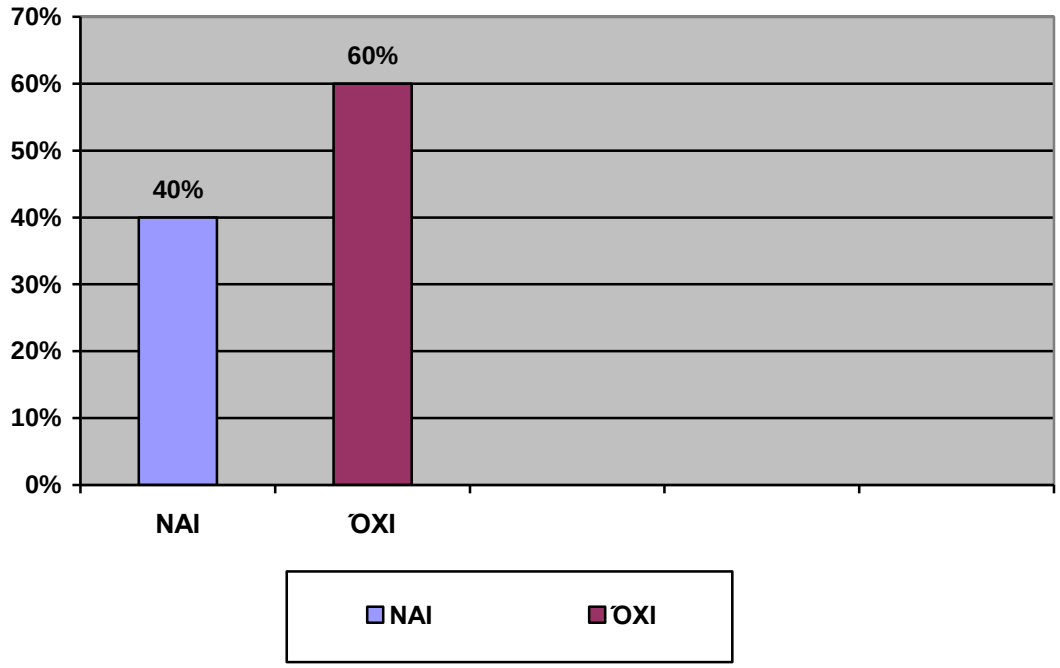
Γράφημα 2: Πρόσβαση στο Ίντερνετ



Σύμφωνα με το διάγραμμα, το 98% των επιχειρήσεων έχει πρόσβαση στο internet σε μόνιμη βάση και μόλις το 2% δεν έχει σύνδεση στο internet σε μόνιμη βάση. Οι επιχειρήσεις που διαθέτουν κυρίως μόνιμη πρόσβαση στο διαδίκτυο είναι τα δικηγορικά γραφεία, τα λογιστικά γραφεία και τα τουριστικά πρακτορεία.

3. Η επιχείρησή σας έχει ιστοσελίδα στο Ίντερνετ;

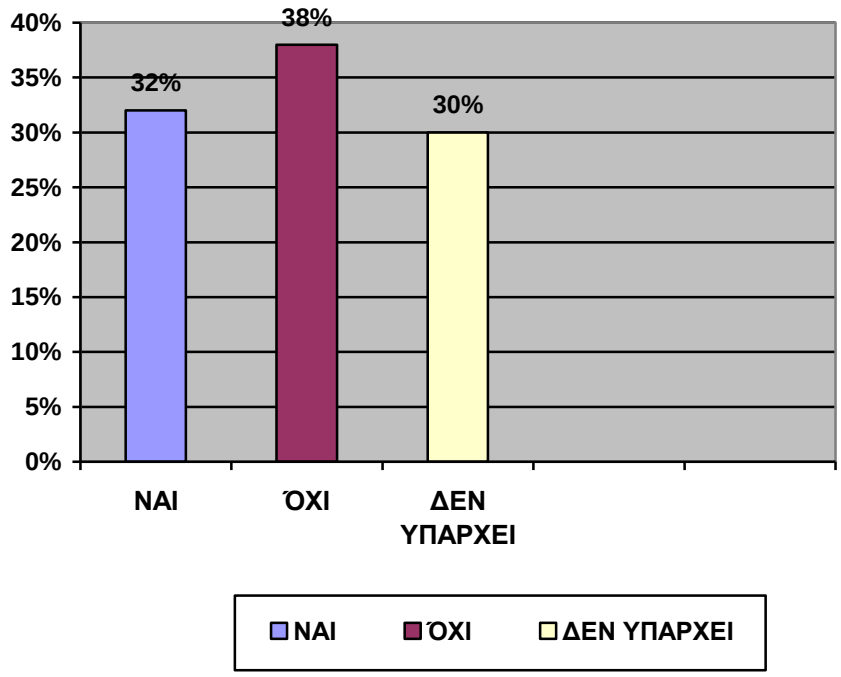
Γράφημα 3: Εταιρική ιστοσελίδα



Στο διάγραμμα φαίνεται πως το 40% των μικρομεσαίων επιχειρήσεων διαθέτουν εταιρική ιστοσελίδα, ενώ ένα μεγάλο ποσοστό το 60% δεν διαθέτουν εταιρική ιστοσελίδα. Οι μικρομεσαίες επιχειρήσεις που διαθέτουν εταιρική ιστοσελίδα είναι κυρίως τα ταξιδιωτικά πρακτορεία, με σκοπό τη διαφήμιση της επιχείρηση τους και την ενημέρωση των πελατών τους όσον αφορά τα πακέτα διακοπών τους άλλα και τις προσφορές τους. Αλλά οι μικρομεσαίες επιχειρήσεις οι οποίες δεν διαθέτουν εταιρική ιστοσελίδα είναι τα δικηγορικά και λογιστικά γραφεία. Οι επιχειρήσεις αυτές προσφέρουν στους πελάτες τους συγκεκριμένες υπηρεσίες και θεωρείται περιττή η ύπαρξη μιας ιστοσελίδας. Ωστόσο θα μπορούσαν να διαθέτουν και αυτές εταιρικές ιστοσελίδες με σκοπό να διαφημιστούν και να αποκτήσουν περισσότερους πελάτες.

4. Η ιστοσελίδα σας είναι προστατευμένη, χρησιμοποιεί το https protocol;

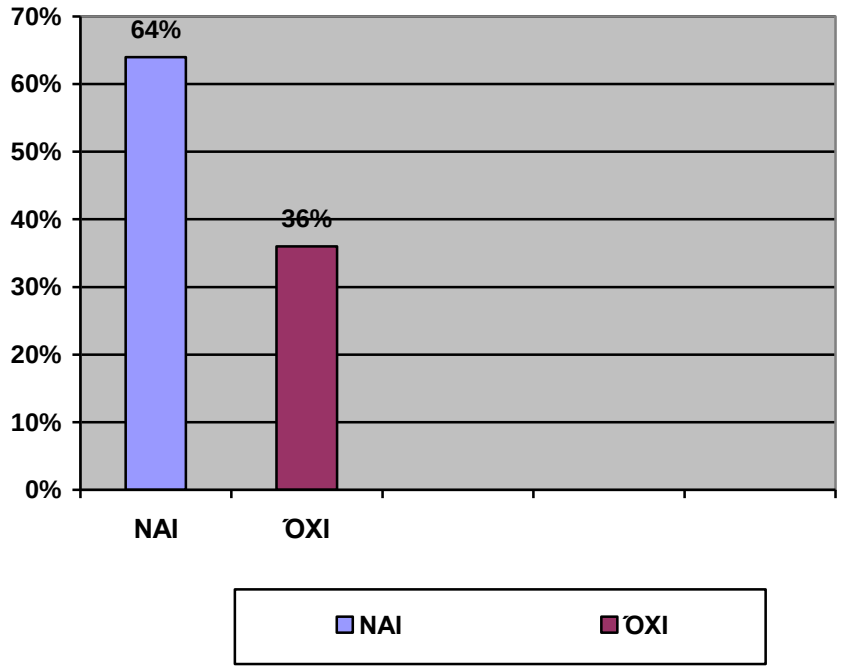
Γράφημα 4: Προστατευμένη ιστοσελίδα



Αυτό που φαίνεται στο διάγραμμα είναι πως το 32% των μικρομεσαίων επιχειρήσεων διαθέτει εταιρική ιστοσελίδα, η ιστοσελίδα τους αυτή είναι προστατευμένη, δηλαδή χρησιμοποιούν https protocol. Αντίθετα το 38% των μικρομεσαίων επιχειρήσεων έχει εταιρική ιστοσελίδα, άλλα η ιστοσελίδα τους αυτή δεν είναι προστατευμένη, δεν χρησιμοποιούν το https protocol. Ενώ το 30% των μικρομεσαίων επιχειρήσεων δεν διαθέτει καθόλου εταιρική ιστοσελίδα άρα δεν χρησιμοποιούν το https protocol. Το 68% των μικρομεσαίων επιχειρήσεων δεν χρησιμοποιεί το https protocol.

5. Η επιχείρησή σας αποθηκεύει προσωπικά δεδομένα των πελατών σας (λογαριασμούς κτλ);

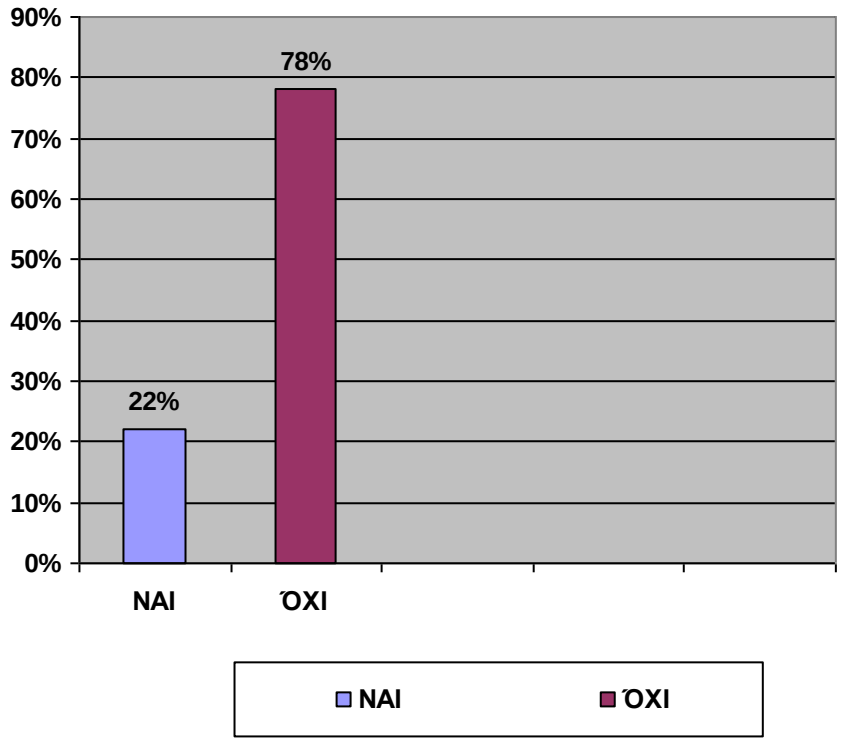
Γράφημα 5: Αποθήκευση προσωπικών δεδομένων



Σύμφωνα με το διάγραμμα, το 64% των μικρομεσαίων επιχειρήσεων αποθηκεύει προσωπικά δεδομένα των πελατών τους. Τα προσωπικά δεδομένα είναι όνομα, επώνυμο, τηλέφωνο (σταθερό και κινητό), διεύθυνση, ΑΦΜ, λογαριασμούς και άλλα. Οι επιχειρήσεις που αποθηκεύουν προσωπικά δεδομένα των πελατών τους είναι τα δικηγορικά και λογιστικά γραφεία. Ενώ το 36% των επιχειρήσεων δεν αποθηκεύει προσωπικά δεδομένα των πελατών τους, οι επιχειρήσεις αυτές είναι τα ταξιδιωτικά πρακτορεία, σε αυτές τις επιχειρήσεις θεωρείται περιττή η αποθήκευση προσωπικών δεδομένων των πελατών τους.

6. Η επιχείρησή σας έχει κάνει συμβόλαιο με κάποια εταιρεία προστασίας ιστοσελίδων για ιούς και χάκερς;

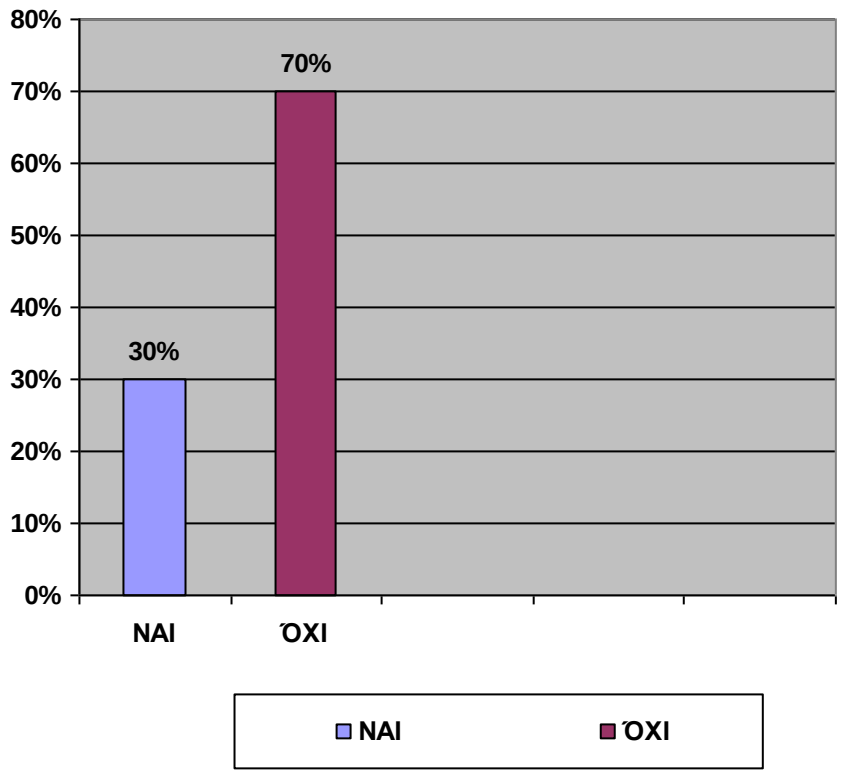
Γράφημα 6: Συμβόλαιο με εταιρεία προστασίας ιστοσελίδων



Σύμφωνα με το διάγραμμα το 22% των μικρομεσαίων επιχειρήσεων έχει κάνει συμβόλαιο με κάποια εταιρεία προστασίας ιστοσελίδων για ιούς και χάκερς ενώ ένα μεγάλο ποσοστό το 78%, δεν έχει κάνει συμβόλαιο με κάποια εταιρεία προστασίας ιστοσελίδων για ιούς και χάκερς. Αυτό συμβαίνει γιατί οι περισσότερες μικρομεσαίες επιχειρήσεις αγνοούν την ασφάλεια και τους κινδύνους του διαδικτύου.

7. Χρησιμοποιείται κάποια εξειδικευμένη εφαρμογή;

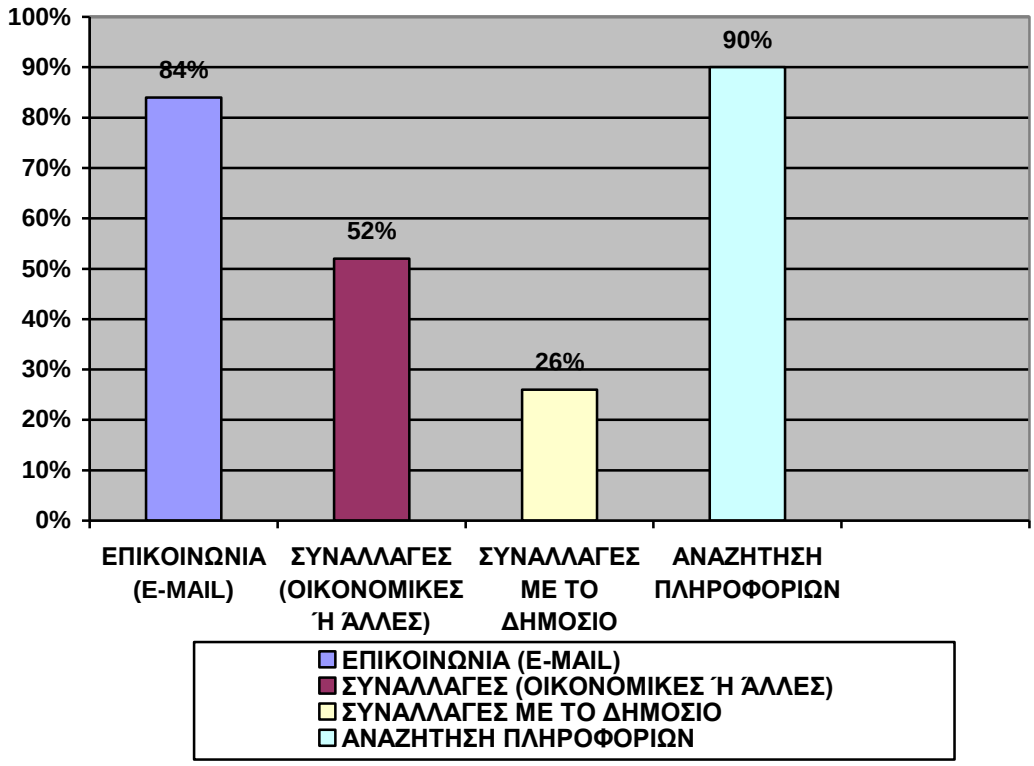
Γράφημα 7: Εξειδικευμένη εφαρμογή



Αυτό που φαίνεται στο διάγραμμα είναι πως το 30% των μικρομεσαίων επιχειρήσεων χρησιμοποιεί κάποια εξειδικευμένη εφαρμογή, όπως για παράδειγμα τα μηχανογραφημένα βιβλία εσόδων-εξόδων που χρησιμοποιούν τα λογιστικά γραφεία, και το πρόγραμμα έκδοσης εισιτήριων που χρησιμοποιούν τα τουριστικά πρακτορεία. Όμως το μεγαλύτερο ποσοστό από τις μικρομεσαίες επιχειρήσεις το 70%, δεν χρησιμοποιούν κάποια εξειδικευμένη εφαρμογή.

8. Για ποίους λόγους χρησιμοποιείται το Διαδίκτυο;

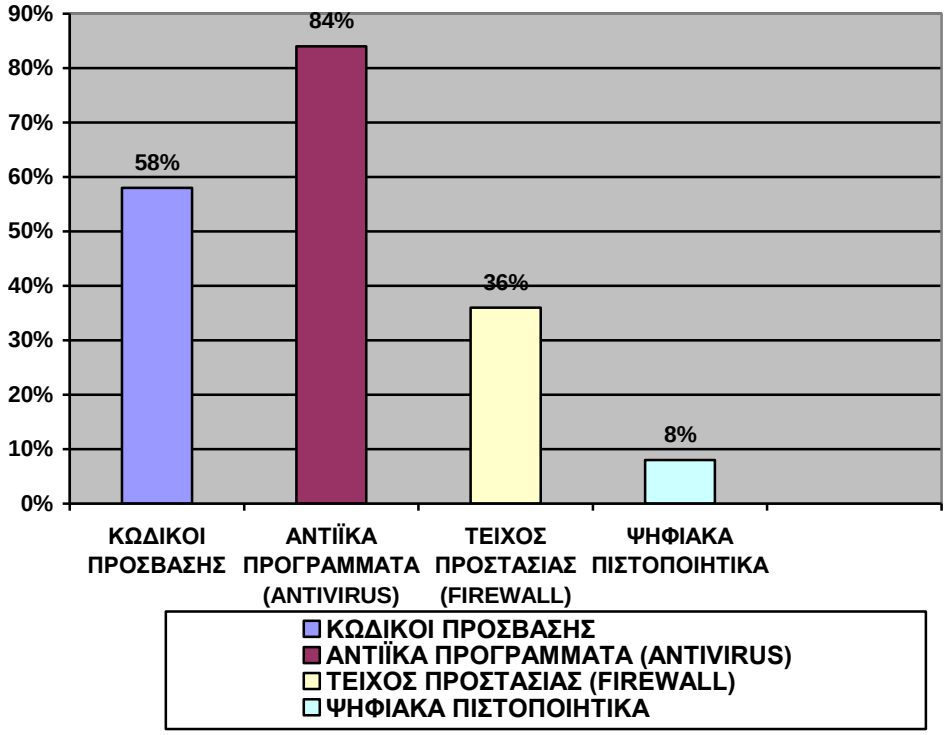
Γράφημα 8: Χρήση διαδικτύου



Σε αυτήν την ερώτηση μπορούσαν οι μικρομεσαίες επιχειρήσεις να επιλέξουν πάνω από ένα. Σύμφωνα με το διάγραμμα, το 84% των μικρομεσαίων επιχειρήσεων χρησιμοποιεί το διαδίκτυο για επικοινωνία (e-mail), με σκοπό να επικοινωνούν με τους πελάτες τους και τους επαγγελματικούς τους συνεργάτες. Το 52% των μικρομεσαίων επιχειρήσεων χρησιμοποιεί το διαδίκτυο για συναλλαγές (οικονομικές ή άλλες). Ενώ μόλις το 26% χρησιμοποιεί το διαδίκτυο για συναλλαγές με το δημόσιο και αυτές οι επιχειρήσεις που χρησιμοποιούν το διαδίκτυο γι' αυτό το λόγο είναι κυρίως τα λογιστικά γραφεία, τα οποία με την βοήθεια του διαδικτύου επικοινωνούν με τις εφορίες μέσω κάποιων κωδίκων που τους δίνονται αλλά και με άλλες δημόσιες υπηρεσίες. Ενώ το μεγαλύτερο ποσοστό των μικρομεσαίων επιχειρήσεων το 90%, δηλαδή όλες σχεδόν οι μικρομεσαίες επιχειρήσεις, χρησιμοποιούν το διαδίκτυο για την αναζήτηση πληροφοριών.

9. Τι είδους προστασία χρησιμοποιείται για το δίκτυο υπολογιστών που έχετε;

Γράφημα 9: Είδος προστασίας

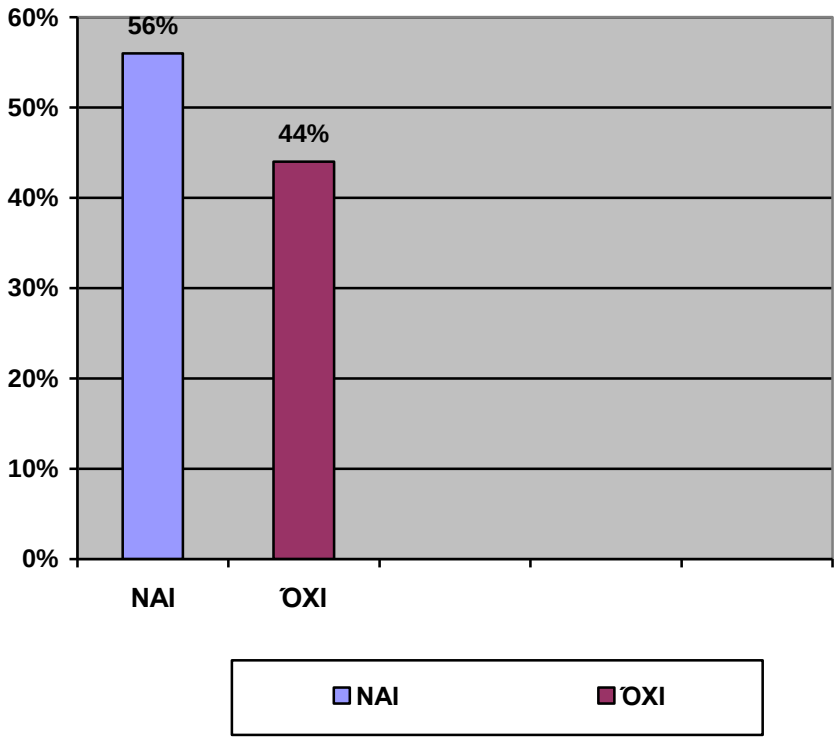


Και σε αυτήν την ερώτηση οι μικρομεσαίες επιχειρήσεις μπορούσαν να επιλέξουν πάνω από ένα. Αυτό που φαίνεται είναι πως το 58% των μικρομεσαίων επιχειρήσεων, δηλαδή λίγο πιο πάνω από τις μισές χρησιμοποιούν για την προστασία του δικτύου υπολογιστών, έχουν κωδικούς πρόσβασης. Ενώ το μεγαλύτερο ποσοστό των μικρομεσαίων επιχειρήσεων δηλαδή το 84% χρησιμοποιεί τα αντιϊκά προγράμματα, τα γνωστά σε όλους antivirus. Το 36% των μικρομεσαίων επιχειρήσεων χρησιμοποιεί για την προστασία του δικτύου υπολογιστών τους, τείχος προστασίας (firewall). Ενώ μόλις το 8% των μικρομεσαίων επιχειρήσεων χρησιμοποιεί ψηφιακά πιστοποιητικά.

Από τα παραπάνω συμπεραίνεται πως οι μικρομεσαίες επιχειρήσεις χρησιμοποιούν περισσότερο για την προστασία του δικτύου υπολογιστών τους κωδικούς πρόσβασης και αντιϊκά προγράμματα (antivirus). Ενώ αυτά που χρησιμοποιούν λιγότερο είναι το τείχος προστασίας (firewall) και τα ψηφιακά πιστοποιητικά.

10.Χρησιμοποιείται server (κεντρικό εξυπηρετητή υπολογιστή);

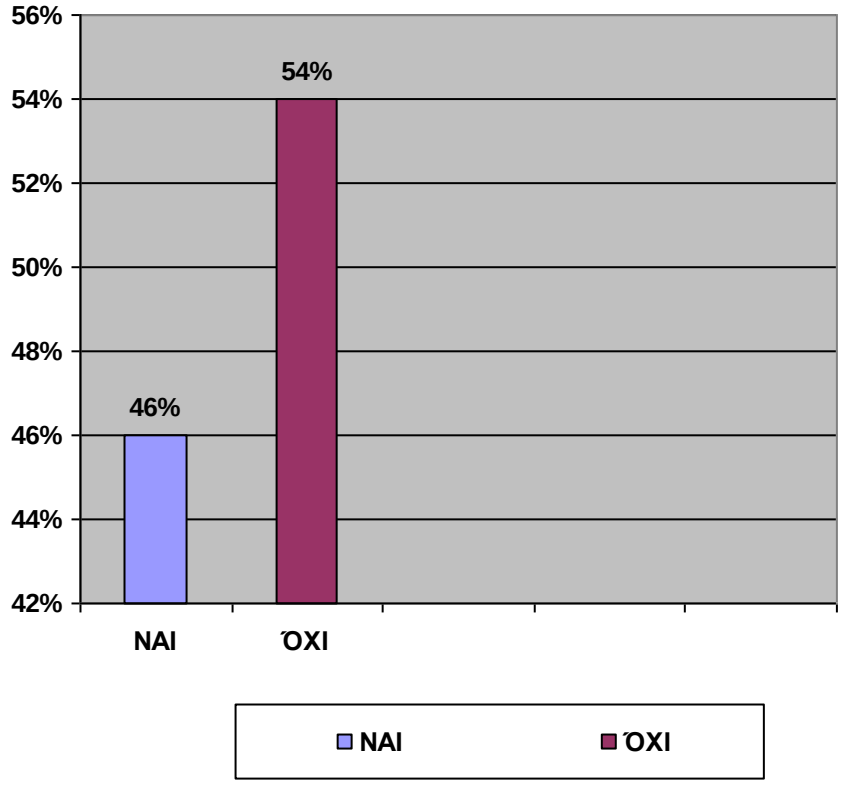
Γράφημα 10: Χρήση server



Αυτό που φαίνεται στο διάγραμμα είναι πως μόλις το 56% των μικρομεσαίων επιχειρήσεων χρησιμοποιεί server (κεντρικό εξυπηρετητή υπολογιστή), ενώ το 44% δεν χρησιμοποιεί καθόλου server. Οι μικρομεσαίες επιχειρήσεις που έχουν server, το χρησιμοποιούν κυρίως για την αποθήκευση των δεδομένων και των αρχείων τους.

11.Ο κάθε εργαζόμενος έχει το δικό του κωδικό πρόσβασης;

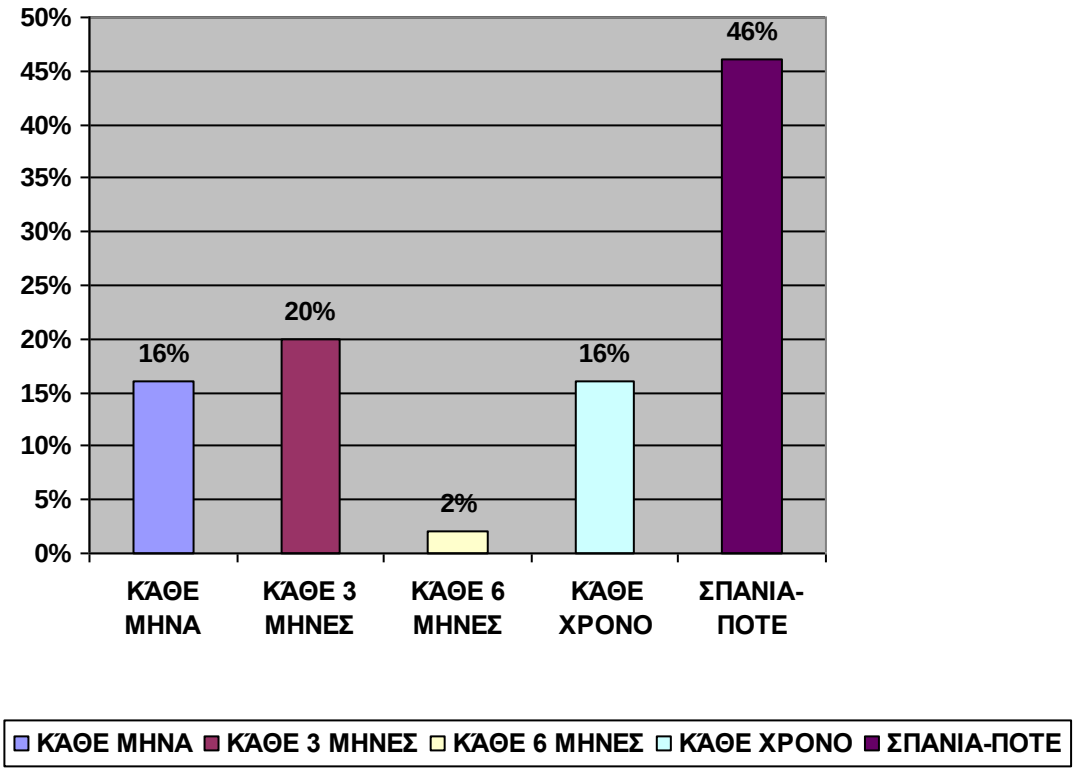
Γράφημα 11: ο κάθε εργαζόμενος έχει δικό του κωδικό πρόσβασης



Στο διάγραμμα φαίνεται πως στο 46% των μικρομεσαίων επιχειρήσεων ο κάθε εργαζόμενος έχει τον δικό του κωδικό πρόσβασης. Ενώ πάνω από τις μισές, δηλαδή στο 54% ο κάθε εργαζόμενος δεν διαθέτει το δικό του κωδικό πρόσβασης και αυτό γίνεται γιατί υπάρχει ένας κωδικός πρόσβασης για όλους τους εργαζόμενους που εργάζονται στην επιχείρηση ή η επιχείρηση δεν χρησιμοποιεί κωδικούς πρόσβασης.

12.Πόσο συχνά αλλάζετε τον κωδικό πρόσβασης;

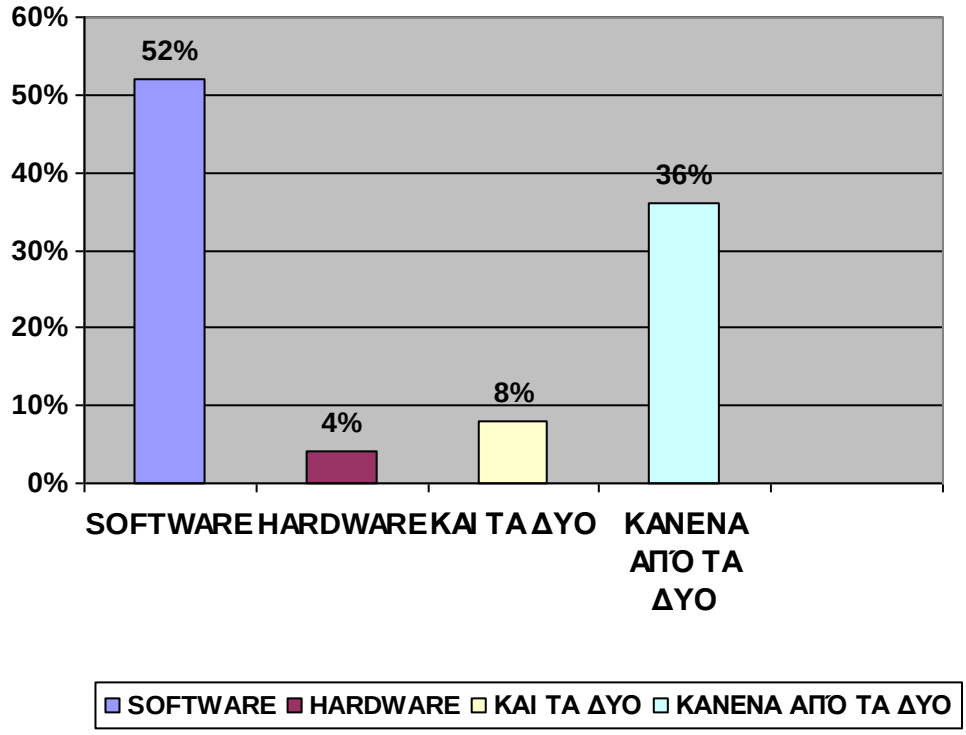
Γράφημα 12: Πόσο συχνά αλλάζετε τον κωδικό πρόσβασης



Όπως διαπιστώνεται από το διάγραμμα, το 16% των μικρομεσαίων επιχειρήσεων αλλάζει τον κωδικό πρόσβασης κάθε μήνα, το 20% κάθε τρεις μήνες, το 2% κάθε έξι μήνες, το 16% κάθε χρόνο και τέλος το 46% αλλάζουν τον κωδικό πρόσβασης σπάνια-ποτέ.
Συμπεραίνεται από τα παραπάνω πως οι περισσότερες μικρομεσαίες επιχειρήσεις αλλάζουν τον κωδικό πρόσβασης τους σπάνια-ποτέ με ποσοστό 46% και ακολουθούν αυτές που αλλάζουν τον κωδικό πρόσβασης κάθε τρείς μήνες με ποσοστό 20%.

13.Τι τείχος προστασίας χρησιμοποιείται;

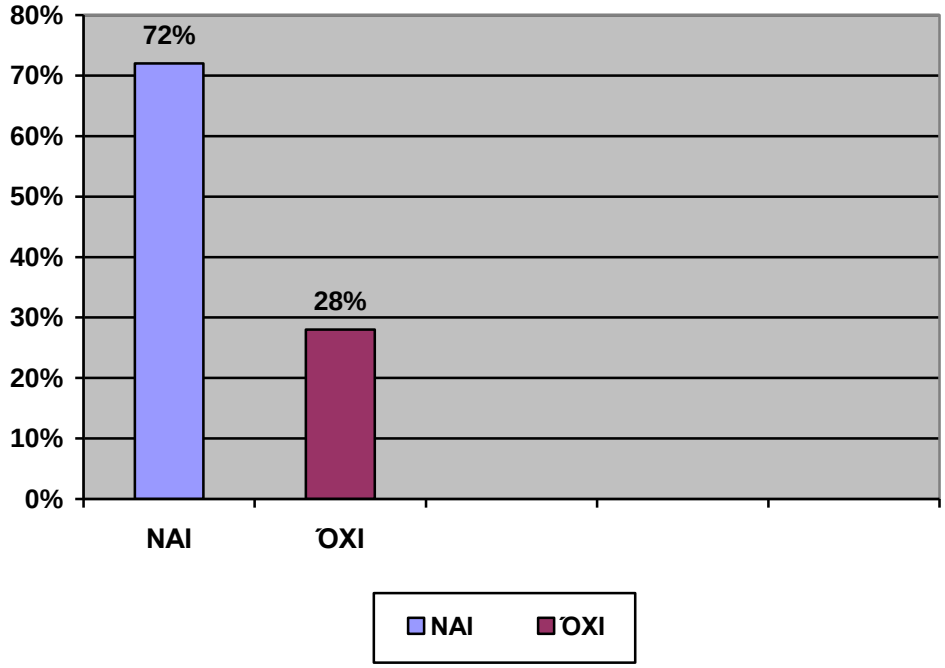
Γράφημα 13: Τείχος προστασίας



Σύμφωνα με το διάγραμμα, το 52% των μικρομεσαίων επιχειρήσεων χρησιμοποιούν software τείχος προστασίας. Ενώ μόλις το 4% χρησιμοποιεί hardware τείχος προστασίας, δηλαδή συσκευή τείχος προστασίας η οποία τοποθετείτε έξω από τον υπολογιστή. Το 8% των μικρομεσαίων επιχειρήσεων χρησιμοποιεί και τα δύο, δηλαδή software και hardware τείχος προστασίας. Ενώ το 36% των μικρομεσαίων επιχειρήσεων δεν χρησιμοποιούν καθόλου τείχος προστασίας, δηλαδή ούτε software ούτε hardware τείχος προστασίας.

14. Έχετε σύστημα ασφαλείας που ελέγχει/ ανιχνεύει παραβιάσεις από κακόβουλο λογισμικό (ιοί);

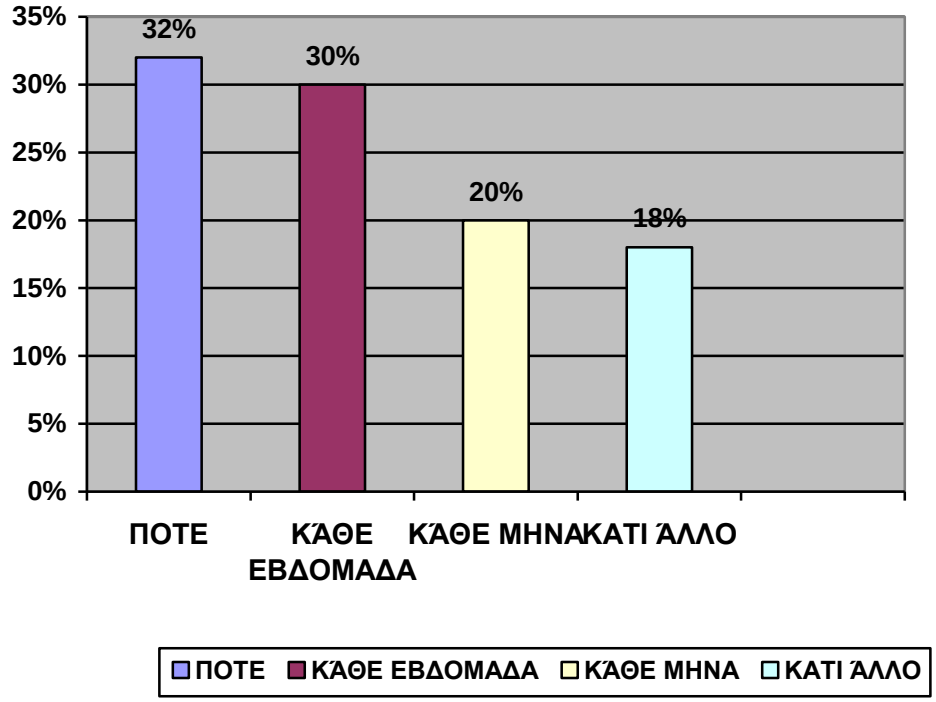
Γράφημα 14: Έχετε σύστημα ασφαλείας



Σύμφωνα με το διάγραμμα το 72% των μικρομεσαίων επιχειρήσεων απάντησε ναι, δηλαδή ότι διαθέτει σύστημα που ελέγχει/ ανιχνεύει παραβιάσεις από κακόβουλο λογισμικό (ιοί) και τα συστήματα που χρησιμοποιούν οι περισσότερες μικρομεσαίες επιχειρήσεις είναι τα γνωστά σε όλους antivirus. Ενώ μόλις το 28% δεν διαθέτει σύστημα ασφαλείας που να ελέγχει/ ανιχνεύει παραβιάσεις από κακόβουλο λογισμικό (ιοί). Και αυτό γίνεται γιατί στις επιχειρήσεις δεν υπάρχει ενημέρωση όσον αφόρα την ασφάλεια, και αυτό είναι κακό γιατί τα δεδομένα και τα αρχεία κάποιων επιχειρήσεων είναι ευάλωτα στους hackers και crackers, οι οποίοι καραδοκούν με σκοπό να κλέψουν προσωπικά και επαγγελματικά δεδομένα.

15. Πόσο συχνά κάνετε έλεγχο στο δίκτυό σας για κάποιο κακόβουλο λογισμικό;

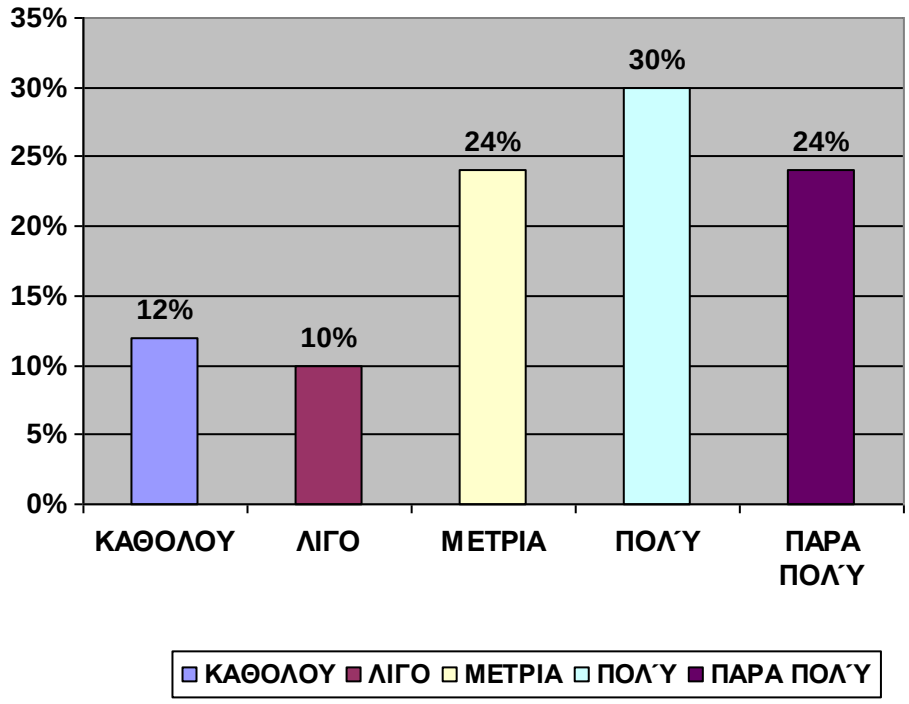
Γράφημα 15: Πόσο συχνά ελέγχετε το δίκτυο σας



Σύμφωνα με το διάγραμμα το 32% των μικρομεσαίων επιχειρήσεων δεν κάνουν έλεγχο στο δίκτυο τους για κάποιο κακόβουλο λογισμικό ποτέ, το 30% των μικρομεσαίων επιχειρήσεων κάνει έλεγχο στο δίκτυο του κάθε εβδομάδα, το 20% κάθε μήνα, και το 18% των μικρομεσαίων επιχειρήσεων επιλέγει το κάτι άλλο (το οποίο περιλαμβάνει χρονικά διαστήματα που δεν αναφέρονται παραπάνω). Όπως φαίνεται οι περισσότερες επιχειρήσεις δεν κάνουν τακτικό έλεγχο στο δίκτυό τους.

16.Πόσο ασφαλή πιστεύετε ότι είναι τα δεδομένα- στοιχεία των πελατών σας;

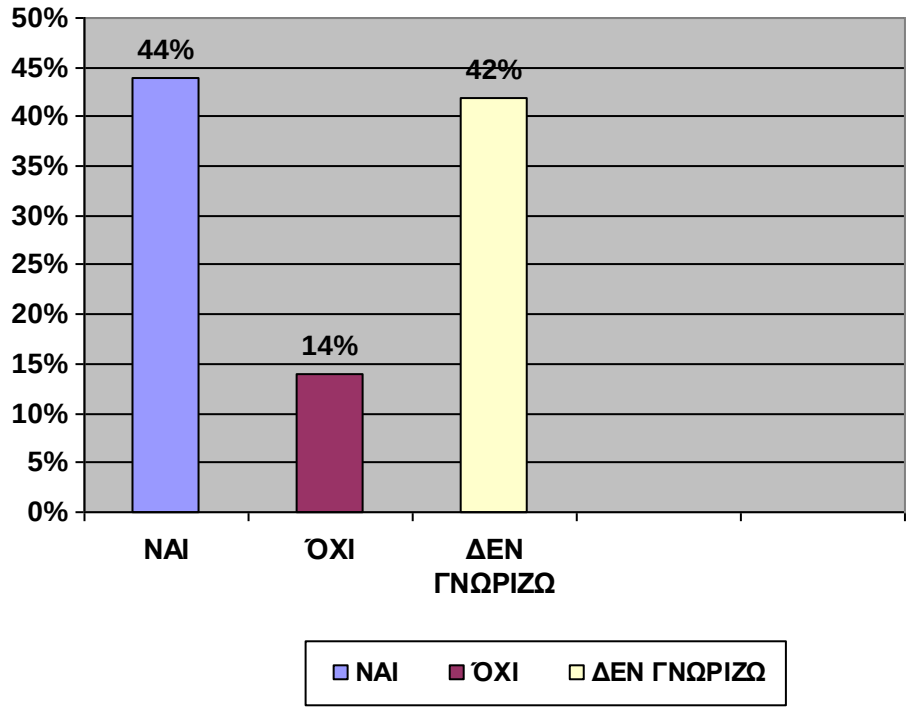
Γράφημα 16: Πόσο ασφαλή πιστεύετε ότι τα δεδομένα-στοιχεία των πελατών σας



Στο διάγραμμα φαίνεται πως το 12% των μικρομεσαίων επιχειρήσεων πιστεύουν πως τα δεδομένα-στοιχεία των πελατών τους δεν είναι καθόλου ασφαλή. Το 10% πιστεύει ότι είναι λίγο ασφαλή, το 24% πιστεύει ότι είναι μέτρια ασφαλή δηλαδή ούτε πολύ ασφαλή ούτε καθόλου ασφαλή, το 30% πιστεύει ότι είναι πολύ ασφαλή και τέλος το 24% πιστεύει ότι δεδομένα-στοιχεία των πελατών τους είναι πάρα πολύ ασφαλή.
Συμπερασματικά, οι περισσότερες μικρομεσαίες επιχειρήσεις με ποσοστό 30% πιστεύουν πως τα δεδομένα-στοιχεία των πελατών τους είναι πολύ ασφαλή, όπως άλλωστε είχε προβλεφτεί, άλλα όμως κάνουν λάθος.

17.Πιστεύετε ότι η ασφάλεια των δεδομένων σας που έχετε είναι ικανή να αντιμετωπίσει τους ιούς που ίσως προκύψουν;

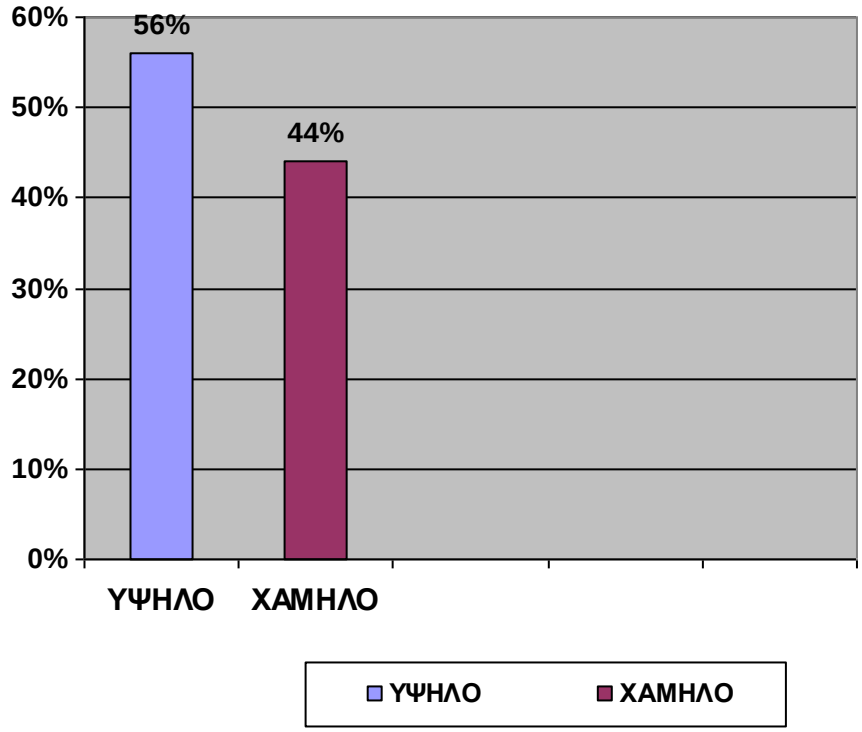
Γράφημα 17: Η ασφάλεια των δεδομένων σας είναι ικάνη να αντιμετωπίσει ιούς



Σύμφωνα με το διάγραμμα το 44% των μικρομεσαίων επιχειρήσεων πιστεύει πως η ασφάλεια των δεδομένων που έχουν είναι ικανή να αντιμετωπίσει τους ιούς που ίσως προκύψουν. Ένα ποσοστό της τάξης του 14% πιστεύει το αντίθετο, δηλαδή ότι η ασφάλεια των δεδομένων που έχουν δεν είναι ικανή να αντιμετωπίσει τους ιούς που ίσως προκύψουν. Ενώ ένα μεγάλο ποσοστό, ένα 42% δηλαδή δεν γνωρίζει κατά πόσο η ασφάλεια των δεδομένων που διαθέτουν είναι ικανή να αντιμετωπίσει τους ιούς που ίσως προκύψουν και είναι πολύ λογικό.

18.Σε περίπτωση μόλυνσης από ιό, το κόστος για την επιχείρησή σας ήταν

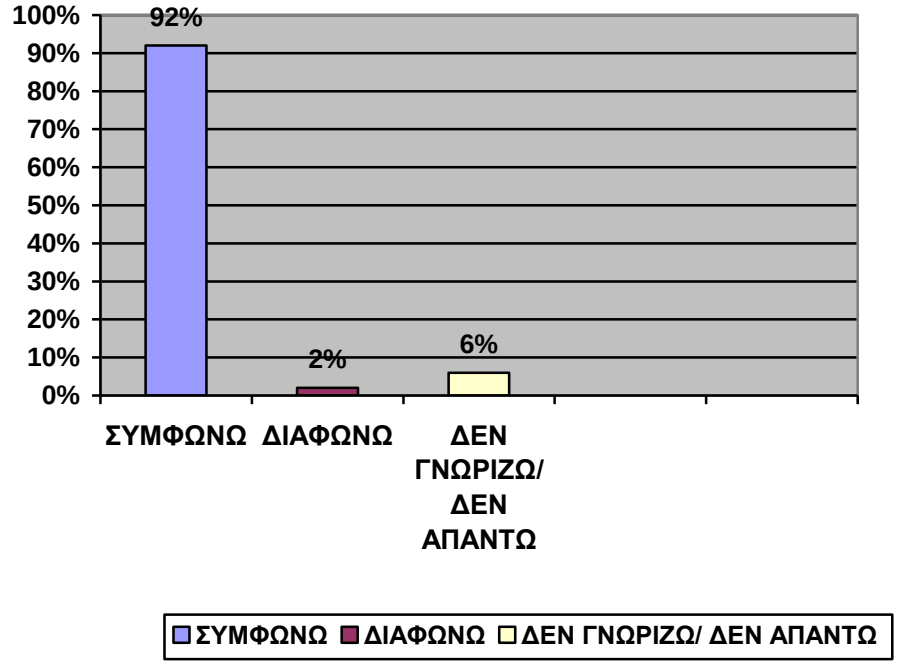
Γράφημα 18: Το κόστος για την επιχείρηση σε περίπτωση μόλυνσης από ιό



Στο διάγραμμα φαίνεται πως όταν οι μικρομεσαίες επιχειρήσεις είχαν μολυνθεί από ιό στο παρελθόν ήταν υψηλό το κόστος για το 56% των μικρομεσαίων επιχειρήσεων ενώ για το 44% το κόστος ήταν χαμηλό. Βέβαια το χαμηλό και υψηλό είναι υποκειμενικό για κάθε επιχείρηση.
Γι' αυτό το λόγο οι επιχειρήσεις πρέπει να χρησιμοποιούν εξελιγμένες μορφές πολιτικών ασφαλείας ώστε να προστατεύονται από τους ιούς και τους hackers του διαδικτύου.

19.Η ασφάλεια του δικτύου σας αποτελεί σημαντικό παράγοντα για την επιχείρησή σας;

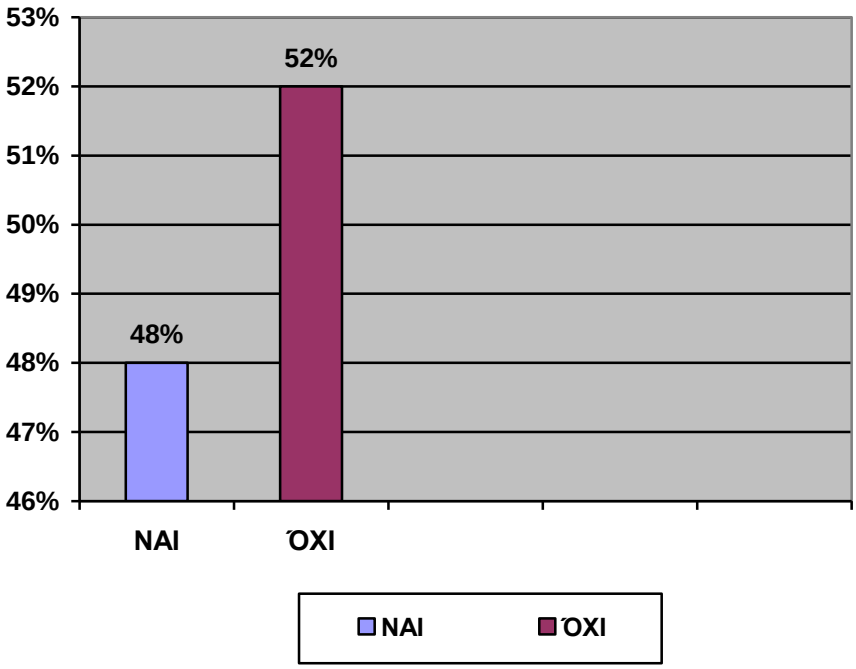
Γράφημα 19: Η ασφάλεια είναι σημαντικός παράγοντας για την επιχείρηση



Αυτό που παρατηρείται στο διάγραμμα είναι πως το 92% των μικρομεσαίων επιχειρήσεων συμφωνεί στο γεγονός πως η ασφάλεια του δικτύου τους αποτελεί σημαντικό παράγοντα για την επιχείρηση τους, όπως άλλωστε είχε προβλεφτεί. Ένα πολύ μικρό ποσοστό, το 2% διαφωνεί με αυτό, δηλαδή πιστεύει πως η ασφάλεια του δικτύου τους δεν αποτελεί σημαντικό παράγοντα για αυτούς και την επιχείρηση τους. Επίσης ένα μικρό ποσοστό, το 6% απαντάει πως δεν γνωρίζει/δεν απαντάει για το αν η ασφάλεια του δικτύου τους αποτελεί σημαντικό παράγοντα για την επιχείρηση τους.
Συμπερασματικά από τα παραπάνω πως για όλες σχεδόν τις μικρομεσαίες επιχειρήσεις η ασφάλεια του δικτύου τους αποτελεί σημαντικό παράγοντα για αυτές, γι' αυτό το λόγο πρέπει να προστατεύουν το δίκτυο τους χρησιμοποιώντας πάντα τις κατάλληλες πολιτικές ασφαλείας.

20.Έχετε κάποιο άτομο που ασχολείται με την ασφάλεια;

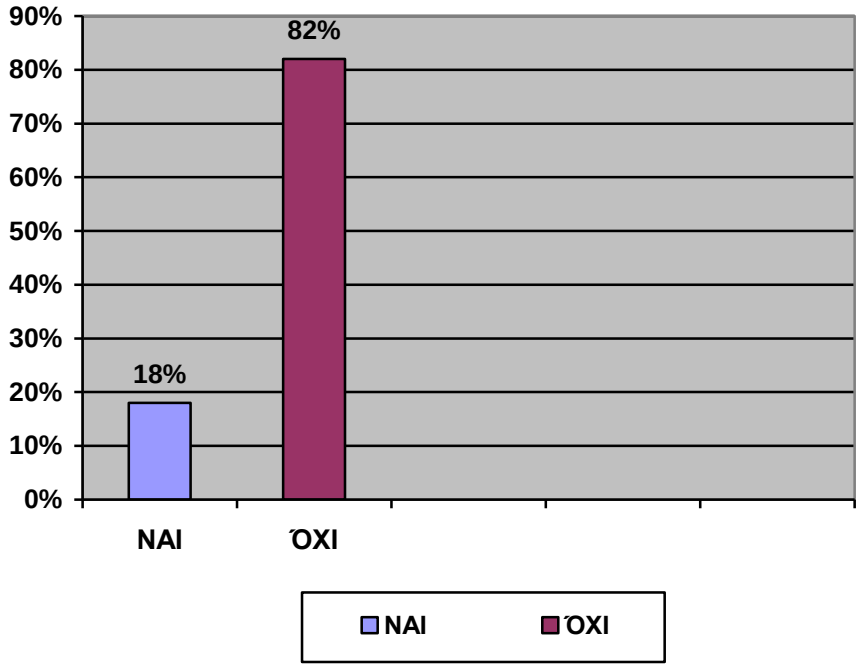
Γράφημα 20: Ασχολείται κάποιο άτομο με την ασφάλεια



Στο διάγραμμα φαίνεται πως το 48% των μικρομεσαίων επιχειρήσεων έχει άτομο που ασχολείται με την ασφάλεια, δηλαδή οι επιχειρήσεις αυτές φροντίζουν για την ασφάλεια των δεδομένων και των αρχείων τους.
Ενώ ένα μεγάλο ποσοστό, το 52% των μικρομεσαίων επιχειρήσεων δεν έχουν άτομο που να ασχολείται με την ασφάλεια. Δηλαδή οι επιχειρήσεις αυτές αγνοούν τους κινδύνους του διαδικτύου και δεν φροντίζουν για την προστασία των δεδομένων και των αρχείων τους, ως αποτέλεσμα να είναι πιο πολύ ευάλωτες από άλλες επιχειρήσεις στους hackers του διαδικτύου.

21. Έχει συμμετάσχει κάποιος από την επιχείρησή σας έστω σε ένα σεμινάριο περί ασφάλειας;

Γράφημα 21: Έχει παρακολουθήσει κάποιος από την επιχείρησή σας σεμινάριο για την ασφάλεια



Στο διάγραμμα φαίνεται πως στο 18% των μικρομεσαίων επιχειρήσεων, έχει συμμετάσχει κάποιος από την επιχείρηση τους έστω και σε ένα σεμινάριο περί ασφαλείας.
Ενώ στο 82% των μικρομεσαίων επιχειρήσεων, κανείς από την επιχείρηση τους δεν έχει συμμετάσχει ούτε σε ένα σεμινάριο περί ασφαλείας. Οι επιχειρήσεις πρέπει να ενδιαφέρονται πιο πολύ για την ασφάλεια του δικτύου τους και να προστατεύουν τα προσωπικά και επαγγελματικά δεδομένα τους.

ΚΕΦΑΛΑΙΟ 5

5.1 ΣΥΜΠΕΡΑΣΜΑΤΑ ΕΡΕΥΝΑΣ

Στα συμπεράσματα της έρευνας γίνεται σύγκριση των αποτελεσμάτων της έρευνας με τη θεωρία και πρέπει να αποδειχτεί τι πραγματικά ισχύει σήμερα στις μικρομεσαίες επιχειρήσεις. Δηλαδή ότι σήμερα οι περισσότερες μικρομεσαίες επιχειρήσεις αγνοούν βασικές πολιτικές ασφαλείας που πρέπει να υπάρχουν σε κάθε επιχείρηση ώστε να προστατευτούν από τους κινδύνους του διαδικτύου. Και από την έρευνα που έγινε, προκύπτουν τα παρακάτω συμπεράσματα :

Για να πραγματοποιηθεί η έρευνα πραγματοποιήθηκαν επισκέψεις σε δικηγορικά γραφεία, λογιστικά γραφεία, ταξιδιωτικά πρακτορεία, εμπορικές και τεχνικές εταιρείες και ασφαλιστικές εταιρείες. Στόχος ήταν από την αρχή ένα δείγμα (50 επιχειρήσεις) αντιπροσωπευτικό της πραγματικότητας. Για αυτό το λόγο ρωτήθηκαν διαφορετικών ειδών μικρομεσαίες επιχειρήσεις, ώστε τα αποτελέσματα στο τέλος να είναι ακριβή και να μην έχουν μεγάλη απόκλιση από την πραγματικότητα.

Οι περισσότερες μικρομεσαίες επιχειρήσεις που ρωτήθηκαν έχουν πρόσβαση στο διαδίκτυο σε μόνιμη βάση και αυτό είναι μια μορφή εξέλιξης για αυτές. Γιατί στο παρελθόν λίγες επιχειρήσεις διέθεταν ηλεκτρονικό υπολογιστή στην επιχείρηση τους και ελάχιστες από αυτές σύνδεση με το διαδίκτυο σε μόνιμη βάση.

Ένα γεγονός που είναι απογοητευτικό είναι πως λιγότερες από τις μισές μικρομεσαίες επιχειρήσεις που ρωτήθηκαν διαθέτουν εταιρική ιστοσελίδα. Και το συμπέρασμα που προκύπτει από αυτό είναι πως δεν βοηθάει τις μικρομεσαίες επιχειρήσεις η μη ύπαρξη εταιρικής ιστοσελίδας. Αν όλες διέθεταν εταιρικές ιστοσελίδες τότε θα μπορούσαν να διαφημιστούν και να γίνουν πιο γνωστοί στο ευρύ καταναλωτικό κοινό που τους ενδιαφέρει.

Επομένως όσες από τις μικρομεσαίες επιχειρήσεις διαθέτουν εταιρική ιστοσελίδα, η ιστοσελίδα τους αυτή δεν είναι προστατευμένη, δηλαδή δεν χρησιμοποιούν https protocol. Πολλές από αυτές δεν γνωρίζουν τι είναι το https protocol. Αυτό που πρέπει να κάνουν οι μικρομεσαίες επιχειρήσεις είναι να διαθέτουν μια προστατευμένη εταιρική ιστοσελίδα.

Ένα μεγάλο ποσοστό μικρομεσαίων επιχειρήσεων αποθηκεύει προσωπικά δεδομένα των πελατών τους. Αυτό είναι καλό για την επιχείρηση γιατί σε μια ενδεχόμενη συνάντηση με τον ίδιο πελάτη, η επιχείρηση θα γνωρίζει πληροφορίες που αφορούν τον πελάτη και αυτό θα έχει σαν αποτέλεσμα την γρήγορη εξυπηρέτηση του πελάτη.

Πολλές μικρομεσαίες επιχειρήσεις δεν έχουν κάνει συμβόλαιο με κάποια εταιρεία προστασίας ιστοσελίδων για ιούς και hackers. Αυτό δείχνει την άγνοια των περισσότερων μικρομεσαίων επιχειρήσεων όσον αφορά την ασφάλεια τοπικών δικτύων και πληροφοριακών συστημάτων. Θα πρέπει όλες οι

επιχειρήσεις να κάνουν συμβόλαιο με κάποια εταιρεία προστασίας ιστοσελίδων για ιούς και hackers, ώστε να προστατεύουν τα δεδομένα και τα αρχεία τους από τους hackers που κυκλοφορούν στο διαδίκτυο.

Λίγες επιχειρήσεις από αυτές που ρωτήθηκαν χρησιμοποιούν κάποια εξειδικευμένη εφαρμογή. Μια εξειδικευμένη εφαρμογή βοηθάει μια επιχείρηση ώστε να γίνονται πιο γρήγορα και πιο απλά οι καθημερινές λειτουργίες της. Όλες οι επιχειρήσεις πρέπει να διαθέτουν κάποια εξειδικευμένη εφαρμογή, ώστε να διευκολύνουν τις συναλλαγές τους.

Οι λόγοι για τους οποίους οι μικρομεσαίες επιχειρήσεις χρησιμοποιούν το διαδίκτυο περισσότερο είναι για επικοινωνία (e-mail) και για αναζήτηση πληροφοριών. Και λιγότερο χρησιμοποιούν το διαδίκτυο για συναλλαγές (οικονομικές ή άλλες) και με συναλλαγές με το δημόσιο.

Οι μικρομεσαίες επιχειρήσεις πρέπει να χρησιμοποιούν το διαδίκτυο για όλους τους παραπάνω λόγους, δηλαδή επικοινωνία (e-mail), συναλλαγές οικονομικές ή άλλες, συναλλαγές με το δημόσιο και αναζήτηση πληροφοριών. Εκτός από τα παραπάνω μια επιχείρηση μπορεί να χρησιμοποιεί το διαδίκτυο για e-banking, σύστημα κρατήσεων, για εκπαίδευση του προσωπικού της επιχείρησης, για ανταλλαγή αρχείων μεταξύ των εργαζομένων της επιχείρησης, τηλεδιάσκεψη και τηλεκπαίδευση.

Οι περισσότερες μικρομεσαίες επιχειρήσεις χρησιμοποιούν περισσότερο για την προστασία του δικτύου τους κωδικούς πρόσβασης και αντιϊκά προγράμματα (antivirus). Ενώ αυτά που χρησιμοποιούν λιγότερο είναι τείχος προστασίας (firewall) και ψηφιακά πιστοποιητικά.

Οι επιχειρήσεις για να προστατέψουν τα δεδομένα και τα αρχεία τους πρέπει να χρησιμοποιούν τις πιο εξελιγμένες μορφές πολιτικών ασφαλείας που υπάρχουν και να έχουν ένα άτομο στην επιχείρηση τους που να ασχολείται αποκλειστικά και μόνο με την ασφάλεια του δικτύου τους. Εκτός από τα παραπάνω είδη προστασίας υπάρχουν και άλλα τα οποία είναι τα IDS και τα IPS.

Ακόμη, ένα μεγάλο ποσοστό από τις μικρομεσαίες επιχειρήσεις χρησιμοποιούν server, δηλαδή κεντρικό εξυπηρετητή υπολογιστή, με σκοπό την αποθήκευση των αρχείων και των δεδομένων της επιχείρησης. Ένας server σε μια επιχείρηση μπορεί να χρησιμοποιηθεί και για άλλους λόγους όπως για πρόσβαση στο διαδίκτυο για όλους τους Η/Υ της επιχείρησης και για πρόσβαση στον δικτυακό εκτυπωτή.

Στις περισσότερες μικρομεσαίες επιχειρήσεις ο κάθε εργαζόμενος δεν έχει τον δικό του κωδικό πρόσβασης. Υπάρχει ένας κοινός κωδικός πρόσβασης για όλους τους εργαζόμενους της επιχείρησης. Ο κωδικός πρόσβασης πρέπει να αλλάζει συχνά και να μην είναι ίδιος για όλους τους εργαζομένους της επιχείρησης. Πολλές από τις μικρομεσαίες επιχειρήσεις αλλάζουν τον κωδικό πρόσβασης σπάνια ή ποτέ. Πρέπει όλες οι επιχειρήσεις να αλλάζουν συχνά τον κωδικό πρόσβασης στα αρχεία τους, ώστε να τα προστατεύουν. Το καλύτερο είναι να αλλάζουν τον κωδικό πρόσβασης οι επιχειρήσεις κάθε μήνα ή έστω

κάθε τρεις μήνες.

Οι περισσότερες μικρομεσαίες επιχειρήσεις χρησιμοποιούν software τείχος προστασίας και ένα επίσης μεγάλο ποσοστό δεν χρησιμοποιούν ούτε software ούτε hardware τείχος προστασίας, δηλαδή κανένα από τα δύο. Θα πρέπει οι επιχειρήσεις να χρησιμοποιούν και hardware τείχος προστασίας, δηλαδή συσκευή τείχος προστασίας.

Πολλές από αυτές διαθέτουν συστήματα ασφαλείας που ελέγχουν/ ανιχνεύουν παραβιάσεις από κακόβουλο λογισμικό (ιοί), και τα συστήματα που χρησιμοποιούν είναι τα antivirus και το τείχος προστασίας (firewall). Όμως υπάρχουν και άλλα συστήματα τα οποία θα μπορούσαν να χρησιμοποιούν και αυτά είναι τα ψηφιακά πιστοποιητικά, τα IDS και τα IPS.

Οι περισσότερες μικρομεσαίες επιχειρήσεις δεν κάνουν ποτέ έλεγχο στο δίκτυο τους για κάποιο κακόβουλο λογισμικό, μερικές από αυτές κάνουν έλεγχο κάθε εβδομάδα και λίγες κάθε μήνα. Επομένως κάνουν έλεγχο όταν καταλάβουν ότι κάτι δεν λειτουργεί σωστά. Όλες οι επιχειρήσεις πρέπει να κάνουν έλεγχο στο δίκτυο τους κάθε εβδομάδα. Κι επειδή αυτόν τον έλεγχο δεν μπορούν να τον πραγματοποιήσουν μόνοι τους οι ιδιοκτήτες των μικρομεσαίων επιχειρήσεων, πρέπει η κάθε επιχείρηση να έχει έναν τεχνικό ασφαλείας που να αναλαμβάνει αυτή τη δουλειά.

Πολλές από τις μικρομεσαίες επιχειρήσεις πιστεύουν ότι τα δεδομένα-στοιχεία των πελατών τους είναι πολύ ασφαλή, άλλα κάνουν λάθος. Επειδή δεν χρησιμοποιούν τις κατάλληλες πολιτικές ασφαλείας γι’ αυτό το λόγο τα αρχεία και τα δεδομένα τους είναι ευάλωτα στους hackers και στους ιούς του διαδικτύου. Γι’ αυτό το λόγο ένα μεγάλο ποσοστό πιστεύει πως η ασφάλεια των δεδομένων που έχουν είναι ικανή να αντιμετωπίσει τους ιούς που ίσως προκύψουν και με το ίδιο ακριβώς ποσοστό απαντάνε πως δεν γνωρίζουν κατά πόσο η ασφάλεια των δεδομένων που έχουν είναι ικανή να αντιμετωπίσει τους ιούς που ίσως προκύψουν, και είναι απόλυτα λογικό.

Επειδή οι μικρομεσαίες επιχειρήσεις δεν χρησιμοποιούν τις κατάλληλες πολιτικές ασφαλείας, στο παρελθόν που είχαν μολυνθεί από ιό το κόστος για την επιχείρηση τους ήταν υψηλό για τις περισσότερες από αυτές.

Ωστόσο για τις περισσότερες ή σχεδόν όλες τις μικρομεσαίες επιχειρήσεις η ασφάλεια του δικτύου τους αποτελεί έναν σημαντικό παράγοντα για αυτούς και την επιχείρηση τους. Παρόλα αυτά δεν κάνουν κάτι για να προστατέψουν το δίκτυο και τα δεδομένα τους.

Ενώ πάλι ένα μεγάλο ποσοστό από αυτές δεν έχει άτομο στην επιχείρηση του που να ασχολείται με την ασφάλεια, διαπιστώθηκε και παραπάνω.

Επίσης σε ένα μεγάλο ποσοστό των μικρομεσαίων επιχειρήσεων κάνεις από την επιχείρηση τους δεν έχει συμμετάσχει ούτε σε ένα σεμινάριο περί ασφαλείας, και αυτό δεν είναι καλό για τις επιχειρήσεις. Οι επιχειρήσεις πρέπει να ενδιαφέρονται περισσότερο για την ασφάλεια του δικτύου τους και των δεδομένων τους.

Ως συμπέρασμα των παραπάνω προκύπτει πως οι περισσότερες

μικρομεσαίες επιχειρήσεις αγνοούν την ασφάλεια τοπικών δικτύων και πληροφοριακών συστημάτων, όπως άλλωστε ήταν αναμενόμενο.

ΠΑΡΑΡΤΗΜΑ

ΑΝΑΦΟΡΕΣ - ΠΗΓΕΣ

1. www.circe.be/content/view/76/332/lang,gr/
2. www.go-online.gr/ebusiness/specials/article.html?article_id
3. Γ. Βασιλακόπουλος –Β. Χρυσικόπουλος, 1990, *Πληροφοριακά Συστήματα Διοίκησης Ανάλυση και Σχεδιασμός*, εκδόσεις Σταμούλη, Πειραιάς, σελ. 220
4. Tilton –Jackson-Rigby, 2001, *Ηλεκτρονικό γραφείο: Μέθοδοι & Διοίκηση*, εκδόσεις 'ΕΛΛΗΝ', Περιστέρι. Σελ. 180
5. Γ. Βασιλακόπουλος –Β. Χρυσικόπουλος, 1990, *Πληροφοριακά Συστήματα Διοίκησης Ανάλυση και Σχεδιασμός*, εκδόσεις Σταμούλη, Πειραιάς, σελ. 231
6. http://webcache.googleusercontent.com/search?q=cache:AabALZT3v5YJ:www.moec.gov.cy/2009_dimiourgikotita_kainotomia/imera_dimiourgikotitas/gym_agiou_pavlou/Diktia_ensirmata_kai_asirmata.ppt+%CF%80%CE%BB%CE%B5%CE%BF%CE%BD%CE%B5%CE%BA%CF%84%CE%B7%CE%BC%CE%B1%CF%84%CE%B1+%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B5%CE%B9%CE%B1%CF%82+%CF%84%CE%BF%CF%80%CE%B9%CE%BA%CF%89%CE%BD+%CE%B4%CE%B9%CE%BA%CF%84%CF%85%CF%89%CE%BD&cd=21&hl=el&ct=clnk&gl=gr&source=www.google.gr
7. Γ. Οικονόμου-Ν. Γεωργοπούλου, 2004, *Πληροφοριακά Συστήματα για τη διοίκηση επιχειρήσεων*, Εκδόσεις Ευγ.Μπένου, Αθήνα ,σ. 87-104 κ σ. 22
8. Γ.Βασιλακόπουλος- Β.Χρισικόπουλος, 1990, *Πληροφοριακά Συστήματα Διοίκησης Ανάλυση και Σχεδιασμός* , Εκδόσεις Σταμούλης , Πειραίας, σ.25
9. Γ.Οικονόμου- Ν. Γεωργοπούλου, 2004, *Πληροφοριακά συστήματα για τη διοίκηση των επιχειρήσεων*, Γ Έκδοση, Εκδόσεις Ευγ.Μπένου, Αθήνα, σ. 24
10. http://sykapcy.com/downloads/sas.pdf
11. mmlab.ceid.upatras.gr/courses/ais_site/files/course/lesson1.ppt
12. Ι.Παπουτσής , 2002, *Βασικά Θέματα Πληροφορικής*, Καλαμάτα, σ.11-12)
13. Γ.Οικονόμου-Ν.Γεωργοπούλου, 2004, *Πληροφοριακά Συστήματα για τη Διοίκηση των επιχειρήσεων*, Εκδόσεις Ευγ.Μπένου, Αθήνα
14. Γ.Βασιλακόπουλος-Β.Χρυσικόπουλος, 1990, *Πληροφοριακά Συστήματα Διοίκησης Ανάλυση και Σχεδιασμός* , Εκδόσεις Α. Σταμούλης, Πειραιάς, σ.60
15. Ι. Παπουτσής, 2002, *Βασικά Θέματα Πληροφορικής*, Καλαμάτα, σ.13-14
16. Ι. Βογιατζής, 2006, *Δίκτυα, Διαδίκτυο και εφαρμογές*, Εκδόσεις TYPOoffest, Πάτρα, σ.54-65
17. http://www.circe.com
18. Ι. Βογιατζής, 2006, *Δίκτυα, Διαδίκτυο και εφαρμογές*, Εκδόσεις

TYPOoffest, Πάτρα, σ. 15 και σ.54-64
19. http://de.teikav.edu.gr/telematics/pdf/3o_Meros_Asyrmata_thlematikh.pdf
20. www.moec.gov.cy/2009.../imera.../Diktia_ensirmata_kai_asirmata.ppt
21. http://www.cisco.com/web/GR/solutions/smb/products/wireless/wireless_primer.html
22. http:// www.go-online.gr
23. Γ.Οικονόμου-Ν.Γεωργόπουλου,2004, *Πληροφοριακά Συστήματα για τη Διοίκηση Επιχειρήσεων*, εκδ. Ευγ. Μπένου, Αθήνα, σελ. 261-265
24. http://www.go-online.gr/ebusiness/specials/article.html
25. http://nefeli.lib.teicrete.gr/browse/stef/epp/2009/GavrilakiKaterina/attached-document-1260438239-880866-12170/Gavrilaki2009.pdf
26. http://www.adae.gr/portal/fileadmin/docs/events/Askoksilakis.pdf
27. http://www.icsd.aegean.gr/website_files/proptyxiako/871591340.pdf
28. Δ.Γιαννακόπουλος- Ι.Παπουτσής, 2003, *Διοικητικά Πληροφοριακά Συστήματα*, εκδ. Σύγχρονη Εκδοτική,Αθήνα, σελ. 327
29. http://www1.cs.ucy.ac.cy/courses/EPL674/labs/lab1/Lab1-Cryptography.pdf
30. http://users.sch.gr/sidmakis/cryptography.php
31. dlib.ionio.gr/ctheses/0506tab575k/Psallidakou_Esignature.ppt
32. http://nefeli.lib.teicrete.gr/browse/stef/epp/2008/Ksourafas,Georgios/attached-document/_____[_____702_____271].pdf
33. http://dspace.lib.uom.gr/bitstream/2159/3781/1/ZiwgaMsc2008.pdf
34. http://oem.gr/main/index.php?option=com_content&view=article&id=1104:sistimata-firewalls-neas-genias&catid=13:diktyaka&Itemid=39
35. http://www.myeasyinternet.net/2010/04/windows_7050.html
36. http://www.myeasyinternet.net/2010/04/windows_7050.html
37. http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Firewalls.html
38. http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Firewalls.html
39. http://www.keplinet-chanion.gr/index.php?option=com_content&view=article&id=268:---&catid=57&Itemid=163
40. http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Viruses.html
41. http://6lyk-n-smyrn.att.sch.gr/ergasies20092010/AntonopoulosAggelis.pdf
42. homepages.pathfinder.gr/lulaby/virus.doc
43. http://dide.flo.sch.gr/Plinet/Tutorials-Sfounis/Tutorials-Sfounis-Worms.html
44. http://www.keplinet-chanion.gr/index.php?option=com_content&view=article&id=268:---&catid=57&Itemid=163
45. http://dide.flo.sch.gr/Plinet/Tutorials-Sfounis/Tutorials-Sfounis-Viruses.html

46. http://6lyk-n-smyrn.att.sch.gr/ergasies20092010/AntonopoulosAggelis.pdf
47. http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Firewalls.html
48. homepages.pathfinder.gr/lulaby/virus.doc
49. http://www.men24.gr/html/ent/647/ent.86647.asp
50. http://www.e-papadakis.gr/ola18.htm
51. http://www.ebusiness-lab.gr/files/dmdocuments/Ptyxiakes-old/PDFs/apostolo_daramou_prostasia_proswpikwn.pdf
52. http://www.bisabled.gr/lib/?p=13350
53. http://www.newinka.gr/consumer.php?id=2738&version=gr
54. http://www.tanea.gr/default.asp?pid=2&artid=4512344&ct=2
55. http://oem.gr/main/index.php?option=com_content&view=article&id=796:apeili_gia_to_33_ton_etairion_oi_istoselides_koinonikis_diktiosis
56. http://docs.google.com/viewer?a=v&q=cache:DZ8BbpMIq1MJ:nemertes.lis.upatras.gr/dspace/bitstream/123456789/768/1/ValeontisThesis.pdf+%CF%83%CF%85%CF%83%CF%84%CE%B7%CE%BC%CE%B1+%CE%B1%CE%BD%CE%B9%CF%87%CE%BD%CE%B5%CF%85%CF%83%CE%B7%CF%82+%CE%B5%CF%80%CE%B9%CE%B8%CE%B5%CF%83%CE%B5%CF%89%CE%BD+(+IDS+)&hl=el&gl=gr&pid=bl&srcid=ADGEEShbkPR6i_cTnfMioNCcgxZeZk5IgKBz2TT6E66WxgNMV9Mb7g6dCtMHAHI4p80cbzTUFhMpoq735BrGvj5McrD20FmYdaCDrfRtZgQUpYGXIEZR9_AzjcERuV5CR55DICmy3Xjy&sig=AHIEtbR5TJ5JAG3QWFekRen5yx9vpYvAAQ
57. http://www.eeei.gr/interbiz/articles/security.htm
58. http://docs.google.com/viewer?a=v&q=cache:DZ8BbpMIq1MJ:nemertes.lis.upatras.gr/dspace/bitstream/123456789/768/1/ValeontisThesis.pdf+%CF%83%CF%85%CF%83%CF%84%CE%B7%CE%BC%CE%B1+%CE%B1%CE%BD%CE%B9%CF%87%CE%BD%CE%B5%CF%85%CF%83%CE%B7%CF%82+%CE%B5%CF%80%CE%B9%CE%B8%CE%B5%CF%83%CE%B5%CF%89%CE%BD+(+IDS+)&hl=el&gl=gr&pid=bl&srcid=ADGEEShbkPR6i_cTnfMioNCcgxZeZk5IgKBz2TT6E66WxgNMV9Mb7g6dCtMHAHI4p80cbzTUFhMpoq735BrGvj5McrD20FmYdaCDrfRtZgQUpYGXIEZR9_AzjcERuV5CR55DICmy3Xjy&sig=AHIEtbR5TJ5JAG3QWFekRen5yx9vpYvAAQ
59. http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Hackers-Crackers.html
60. http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Itemid=0&langEN
61. http://kosmidis-athanasios.pblogs.gr/2008/01/hackers.html
62. http://6lyk-n-smyrn.att.sch.gr/ergasies20092010/VasalosVafeiadis.pdf
63. http://dide.flo.sch.gr/Plinet/Tutorials-Girtsos/Hacking-InternetSecurity.pdf
64. http://6lyk-n-smyrn.att.sch.gr/ergasies20092010/KoziokosKamilos.pdf
65. http://students.ceid.upatras.gr/~akis/jotd23/0358.html
66. http://www.espressonews.gr/default.asp?pid=79&catid=1&artID=973527

67. http://www.tanea.gr/default.asp?pid=2&ct=1&artId=86736
68. http://news.pathfinder.gr/world/news/503916.html
69. http://blogthea.gr/NextStep/cracking-hacking-test-me-software/40490-iaecia-hacking-test-me.html
70. http://news.pathfinder.gr/periscopio/73917.html
71. http://www.5-9report.gr/59report/5-9%20REPORT%20vol32.pdf
72. http://www.enet.gr/?i=news.el.article&id=111458
73. http://archive.enet.gr/online/online_obj?pid=25&tp=T&id=81420156
74. http://www.pcw.gr/Article/News-General-PCs-Notebooks/hacking_tips_legal_hardware_software_gaming/236-4726.html&pbreak=1&pbreak=2&pbreak=3&pbreak=4&pbreak=0&pbreak=1&pbreak=2&pbreak=3&pbreak=4&pbreak=0&pbreak=1&pbreak=2&pbreak=3&pbreak=4&pbreak=0
75. http://mpl.med.uoa.gr/Downloads/PDF/internet.pdf

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Αποστόλου Ν.,1987, *Συστήματα Πληροφορικής στη Διοίκηση*, εκδόσεις Παρατηρητής, Θεσσαλονίκη
2. Βασιλακόπουλος Γ.- Χρυσικόπουλος Β., 1990, *Πληροφοριακά Συστήματα Διοίκησης Ανάλυση και Σχεδιασμός*, εκδόσεις Α. Σταμούλης, Πειραιάς
3. Βογιατζής Ι.,2006, *Δίκτυα, διαδίκτυο και εφαρμογές*, εκδόσεις TYPOoffset, Πάτρα
4. Οικονόμου Γ.- Γεωργόπουλος Ν., 2004, *Πληροφοριακά Συστήματα για τη Διοίκηση Επιχειρήσεων,* εκδόσεις Ε. Μπένου, Αθήνα
5. Παπουτσής Ι., 2002, *Βασικά Θέματα Πληροφορικής*, Καλαμάτα
6. Tilton R.S.- Jackson J.H- Rigby S.C., 2001, *Το ηλεκτρονικό ταχυδρομείο: Μέθοδοι & Διοίκηση*, εκδόσεις "ΕΛΛΗΝ", Αθήνα

ΗΛΕΚΤΡΟΝΙΚΕΣ ΔΙΕΥΘΥΝΣΕΙΣ

1. http://www.go-online.gr/ebusiness/specials/article.html?article_id=1242
2. http://www.go-online.gr/ebusiness/specials/article.html?article_id=1243
3. http://www.go-online.gr/ebusiness/specials/article.html?article_id=1241
4. http://www.go-online.gr/ebusiness/specials/article.html?article_id=841
5. http://www.go-online.gr/ebusiness/specials/article.html?article_id=842
6. http://www.go-online.gr/ebusiness/specials/article.html?article_id=840
7. http://www.cisco.com/web/GR/solutions/smb/products/wireless/wireless_primer.html
8. http://www.cardel.gr/Default.aspx?ID=38
9. http://www.circe.be/content/view/76/332/lang,gr
10. http://el.wikipedia.org/wiki/%CE%A4%CE%BF%CF%80%CE%B9%CE%BA%CF%8C_%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF
11. http://www.neural.uom.gr/Documents/Networks/chapter10.pdf
12. http://el.wikiversity.org/wiki/%CE%95%CE%B9%CF%83%CE%B1%CE%B3%CF%89%CE%B3%CE%AE_%CF%83%CF%84%CE%B1_%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CE%AC_%CF%83%CF%85%CF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1
13. http://2tee-n-smyrn.att.sch.gr/texn_site/texn2.htm
14. http://www.forthnet.gr/templates/viewcontentTmArt.aspx?p=201384
15. http://www.s4u.gr/index.php?option=com_content&view=article&id=5&Itemid=61#bottom

16. http://www.s4u.gr/images/stories/popups/epitheseisasfaleiasitpopup.htm
17. http://www.s4u.gr/images/stories/popups/asfaleiapopup.htm
18. http://www.go-online.gr/ebusiness/specials/article.html?article_id=851
19. http://www.go-online.gr/ebusiness/specials/article.html?article_id=852
20. http://www.go-online.gr/ebusiness/specials/article.html?article_id=853
21. http://www.go-online.gr/ebusiness/specials/article.html?article_id=854
22. http://www.go-online.gr/ebusiness/specials/article.html?article_id=855
23. http://www.go-online.gr/ebusiness/specials/article.html?article_id=719
24. http://www.go-online.gr/ebusiness/specials/article.html?article_id=674
25. http://www.go-online.gr/ebusiness/specials/article.html?article_id=675
26. http://www.go-online.gr/ebusiness/specials/article.html?article_id=675
27. http://www.cnc.uom.gr/services/pdf/security.pdf
28. http://nethellas.gr/internet_intranets.htm
29. http://www.dblad.upatras.gr/download/courses/db1/9_IntergrityConstraints-r.pdf
30. http://www.teiser.gr/icd/staff/chilas/files/D_III/General_intro_to_security.pdf
31. http://www.go-online.gr/ebusiness/specials/article.html?article_id=710
32. http://www.atticatech.com/whats-new-in-15/59-systems/122-data-encryption.html
33. http://www.image.ntua.gr/meleti172KTP/?q=node/23
34. http://www.freshwap.net/forums/el/applications/1169107-folder-lock-6-3-2-full-full-serial-include.html#post1269669
35. http://www.atticatech.com/products/main-systems/systems-security.html
36. http://docs.blackberry.com/ko-kr/smartphone_users/deliverables/14913/About_encrypting_data_in_device_memory_777801_11.jsp
37. http://unothing.blogspot.com/2009/05/blog-post.html
38. http://www.go-online.gr/ebusiness/specials/article.html?article_id=713
39. http://www.axiaplus.gr/Default.aspx?id=213020&nt=108&lang=1
40. www.ece.ucy.ac.cy/courses/ece007/notes/ECE007_lecture18.ppt
41. http://www.it.uom.gr/project/ergaC/Cryptografisi/ERGASIA_C.htm
42. http://office.microsoft.com/el-gr/access-help/HA010096299.aspx
43. http://kallithea.hua.gr/epixeirein/dihm4docs/Richard-Nicolas-Lacroix.pdf
44. http://www.atticatech.com/products/main-systems-security.html
45. http://dide.flo.sch.gr/PLinet/Tutorials-CryptoTerminology.html
46. http://6lyk-n-smyrn.att.sch.gr/ergasies20092010/AntonopoulosAggelis.pdf
47. http://odysonline.gr/2009/10/prostatepse-ta-arxeia-sou-apo-adiakrit/
48. http://www.online-tech-tips.com/computer-tips/decrypt-encrypted-xp-files/el/
49. http://www.el.wikipedia.org/wiki/Κρυπτογραφία
50. http://www.emergingtrends.eul?=1272

51. http://www.securitymanager.gr/it_security/protection_article.php
52. http://library.gnome.org/evolution/stable/encryption.html.el
53. http://www.pi-schools.gr/programs/ktp/previous_version/book2/06_p1.pdf
54. http://www.messaggiano.com/el/internet-tips/52466-computer-viruses-how-to-remove-a-computer-virus-from-your-computer.html
55. http://pacific.jour.auth.gr/articles/article2.htm
56. http://www.microsoft.com//hellas/athome/security/viruses/virus101.mspx.htm
57. http://support.microsoft.com/kb/129972/el
58. http://www.men24.gr/html/ent/647/ent.86647.asp
59. http://www.microsoft.com/hellas/athome/security/viruses/intro_viruses_what.mpsx
60. http://www.capital.gr/News.asp?id=1015912
61. http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-viruses.html
62. http://homepages.pathfinder.gr/Tutorials-viruses.html
63. http://www.computercare.gr/tag/ιοί_υπολογιστών/
64. http://el.wikipedia.org/wiki/Ιός_(υπολογιστές)
65. http://www.adep.gr/adepenet/download.php?itemid=66
66. http://www.pctechnology.gr/vbull/vb/showthread.php?t=873
67. http://www.newinka.gr/consumer.php?id-2738&version=gr
68. http://www.ksemoudania.wikidot.com/copyright
69. http://www.law.uoa.gr/copyright.html
70. http://www.tanea.gr/default.asp?pid=2&artid=4512344&ct=2
71. http://www.sepe.gr/default.aspx?pid=34&la=1&artID=3106
72. http://www.bisabled.gr/lib/?p=13350
73. http://www.infolab.gr/ECDL Core Syllabus V4 7.pdf
74. http://office.microsoft.com/el-gr/excel-help/HP005256149.aspx
75. http://www.format-computers.gr/docs/ECDL_CORE_SYLLABUS_V4D_M.7_GR.pdf
76. http://www.learnsoft.gr/index.php?option=com_contect&view=article&id=52&Itemid=66
77. http://www.it.uom.gr/teaching/open/el/MozillaTrebuchet_win.pdf
78. http://www.lib.uth.gr/LWS/el/ws/lws_edit.asp
79. http://www.hellenicnetbanking.com/gr/generalinfo/problemsconnectining.htm
80. http://www.hellenicnetbanking.com/gr/generalinfo/security.htm
81. http://gsmforum.gr/blog/?p=6898
82. http://windows.microsoft.com/el-GR/windows-vista/what_does_Internet_Explorer_protected_mode_do
83. http://www.novartis.gr/_Privacy/tabid/165/Default.aspx
84. http://www.mondial_assistance.gr/gr/aboutus/condifidentiality.htm

85. http://www.neo2.gr/web/neo2.gr/searchpagebasedontags/-/asset_publisher/Ep0Q/content/%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%B9%CE%B1-%CE%B1%CF%80%CE%BF-%CF%84%CE%B9%CF%82-%CE%B1%CF%80%CE%B5%CE%B9%CE%BB%CE%B5%CF%82-%CF%84%CE%BF%CF%85-%CE%BC%CE%B5%CE%BB%CE%BB%CE%BF%CE%BD%CF%84%CE%BF%CF%82?redirect=%2Fweb%2Fneo2.gr%2Fsearchpagebasedontags%2F-%2Fasset_publisher%2FEp0Q%2Fcontent%2F%25CF%2580%25CF%2581%25CE%25BF%25CF%2583%25CF%2584%25CE%25B1%25CF%2583%25CE%25B9%25CE%25B1-%25CE%25B1%25CF%2580%25CE%25BF-%25CF%2584%25CE%25B9%25CF%2582-%25CE%25B1%25CF%2580%25CE%25B5%25CE%25B9%25CE%25BB%25CE%25B5%25CF%2582-%25CF%2584%25CE%25BF%25CF%2585-%25CE%25BC%25CE%25B5%25CE%25BB%25CE%25BB%25CE%25BF%25CE%25BD%25CF%2584%25CE%25BF%25CF%2582
86. http://oem.gr/main/index.php?option=com_content&view=article&id=796:apeili-gia-to-33-ton-etairion-oi-istoselides-koinonikis-diktiosis&catid=20:epikairotita&Itemid=47
87. http://oem.gr/main/index.php?option=com_content&view=article&id=1104:sistimata-firewalls-neas-genias&catid=13:diktyaka&Itemid=39
88. http://www.microsoft.com/hellas/athome/secuirity/protect/firewall.mspx
89. http://el.wikipedia.org/wiki/firewall
90. http://www.itsecuirity.gr/firewall.html
91. http://help.live.com/Help.aspx?market=el-GK
92. http://project=WL_Messengerv1_2&query=Messenger-TROU_ResolveFirewallissves.htm
93. http://windows.microsoft.com/el-GR/windows7/products/features/windows_firewall
94. http://windows.microsoft.com/el-GR/windows7/firewall-frequently-asked-questions
95. http://windows.microsoft.com/el-GR/windows7/What-is-a-firewall
96. http://windows.microsoft.com/el-GR/windows7/understanding-windows-Firewaall-setting
97. http://www.google.com/support/adsense/bin/answer.py?hl=el&answer=12655
98. http://el.wikipedia.org
99. http://noc.auth.gr/services/personal/sertificates/index.html
100. http://www.ermis.gov.gr/portal/page/portal/ermis/items/pdfs/pkguide_admin.pdf

101. http://www.kep.gov.gr/portal/page/portal/ermis/help?p_topic=4
102. http://www.e-papadakis.gr/ola18.htm
103. http://www.cardel.gr/Default.aspx?ID=38
104. http://pasific.jour.auth.gr/secuirity/page.htm
105. http://pacific.jour.auth.gr/secuirity/page4.htm
106. http://backolas.blogspot.com/2006/02/blog-spot_113960865438587307.html
107. http://www.afpnisis.gr/agora/viewtopic.php?f=648t=323
108. http://www.pc-news.gr/home/publishesarchive/69-greekhackers.html
109. http://news.pathfinder.gr/periscopio/73917.html
110. http://www.thegreekz.com/forum/archive/idex.php/t-391572.html
111. http://www.antidogma.gr/forum/viewtopic.php?f=1668t=4433&p=82576
112. http://www.in2life.gr/features/faces/articles/145191/Face.aspx
113. http://r3104.wordpress.com/2008/04/16/hackers_17_4-2008
114. http://www.go-online.gr/ebusiness/specials/article.html?article_id=683&PHPSESSID=bd57b36e4d144457f061758d39425c6b
115. http://chtsanti.net/firewall.html
116. http://oem.gr/main/index.php?option=com_content&view=article&id=1104:sistimata-firewalls-neas-genias&catid=13:diktyaka&Itemid=39
117. http://www.tekbar.net/el/hackers-and-security/application-firewall-blocking-the-detailed.html
118. http://www.hotstation.gr/article342.html
119. http://datalibrary.wordpress.com/2009/07/24/%CE%BF%CE%B9-%CE%B7%CE%B8%CE%B9%CE%BA%CE%BF%CE%AF-%CE%BA%CF%8E%CE%B4%CE%B9%CE%BA%CE%B5%CF%82-%CF%84%CF%89%CE%BD-%CF%87%CE%AC%CE%BA%CE%B5%CF%81/
120. http://www.infosum.net/el/communication/career-in-ethical-hacking.html
121. http://archive.enet.gr/online/online_obj?pid=25&tp=T&id=81420156
122. http://4lyk-irakl.ira.sch.gr/HACKING.htm
123. http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Firewalls.html
124. http://www.ciscostadium.org/web/GR/solutions/smb/innovators/how_to/articles/secure_my_business/small_business_firewall_software.html
125. http://conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/ergasies/Firewall.pdf
126. http://www.filaderlis.com/ebooks/cookbook15.pdf
127. http://0x3a.wordpress.com/2009/03/01/certified-ethical-hacker-series/

128. http://career.duth.gr/cms/files/fek_a1_120110.pdf
129. http://1kesyp-v.thess.sch.gr/prokyrixeis/100118_eidiko%20prosvpiko%20astynomia.pdf
130. http://www.downeu.com/forum/el/video-tutorials/14496-ec-council-certified-security-analyst-licensed-dvd1-2-a.html
131. http://www.compuservice.gr/products/products-symantec/hardware.htm
132. http://nemertes.lis.upatras.gr/dspace/bistream/123456789/768/1/Valeontisthesis.pdf
133. http://zone-h.org/archive/defacer=GHS/page=1
134. http://www.inout.gr/showthread.php?t=38264
135. http://tetradio.pblogs.gr/tags/greek-hacking-team.html
136. http://helenic-news.blogspot.com/2008/09/cern.html
137. , http://www.games.gr/forum/showthread.php?4244-HACKER-(GREEK-TERRORITS-TEAM
138. http://blogthea.gr/NextStep/cracking-hacking-test-me-software/40490-iaecia-hacking-test-me.html
139. http://blogthea.gr/NextStep/cracking-hacking-test-me-software/40490-iaecia-hacking-test-me.html
140. http://www.go-online.gr/ebusiness/specials/article.html?article_id=680
141. http://www.nokia.gr/support/software
142. http://www.cisco.com/en/US/products/ps5708/Products_Sub_Category_Home.html
143. http://www.odesus.gr/web/index.html
144. http://www.zyxel.com/web/
145. http://h17007.www1.hp.com/us/en/services/index.aspx
146. http://www.ip.gr/el/dictionary/31-server
147. http://athina.cs.unipi.gr/site-ergastirio/asfaleia_diktion/parousiaseis/5-%CE%A3%CF%85%CF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1%20Firewall-%CE%B2%CE%BF%CE%B7%CE%B8%CE%B7%CF%84%CE%B9%CE%BA%CF%8C.pdf.pdf
148. http://www.w-hotspots.gr/documents/Wireless%20Access.pdf
149. http://www.neural.uom.gr/Documents/projects/Thesis08.pdf
150. http://www.cs.uoi.gr/~epap/asurmata/downloads/lect6.pdf
151. www.teiser.gr/icd/staff/vologian/.../Ασύρματα%20δίκτυα.ppt
152. http://17conf.lib.uoi.gr/files/b10.2.Mamma.pdf
153. http://dspace.lib.ntua.gr/bitstream/123456789/3257/3/astyakopoulosa_webgis.pdf
154. mmlab.ceid.upatras.gr/courses/ais_site/files/course/lesson1.ppt

155. http://xrimko.teikoz.gr/xrimatooikonomiko/Shmeioseis%20Mathimatwn%20XR/X4%20-%20Systhmata%20Plhroforiwn%20Dioikhshs%20-%20Tsioras/X4-SysPlhDoi-kef1.pdf
156. http://el.wikiversity.org/wiki/%CE%95%CE%B9%CF%83%CE%B1%CE%B3%CF%89%CE%B3%CE%AE_%CF%83%CF%84%CE%B1_%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CE%AC_%CF%83%CF%85%CF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1
157. http://www.teihal.gr/bus/labs/downloads/kef1MIS.pdf
158. isa.teipir.gr/files/projects/psd_pps.ppt
159. http://www.adae.gr/portal/fileadmin/docs/events/Askoksilakis.pdf
160. http://www.filaderlis.com/ebooks/prostasia%20kai%20asfaleia%20yp.%20sustimaton.pdf
161. http://www.downeu.com/forum/el/video-tutorials/160560-certified-ethical-hacker-v6-training-4dvds-repost.html
162. http://news.bbc.co.uk/2/hi/uk_news/scotland/tayside_and_central/5094044.stm
163. http://www1.cs.ucy.ac.cy/courses/EPL674/labs/lab1/Lab1-Cryptography.pdf
164. http://users.sch.gr/sidmakis/cryptography.php
165. dlib.ionio.gr/ctheses/0506tab575k/Psallidakou_Esignature.ppt
166. http://www.policenet.gr/portal/ext/passwords.html
167. http://nefeli.lib.teicrete.gr/browse/stef/epp/2008/Ksourafas,Georgios/attached-document/_____[_____702_____271].pdf
168. http://de.teikav.edu.gr/telematics/pdf/3o_Meros_Asyrmata_thlematikh.pdf
169. http://sykapcy.com/downloads/sas.pdf
170. http://www.syros.aegean.gr/users/lekkas/pubs/t/dlek_thesis_final.htm
171. http://docs.google.com/viewer?a=v&q=cache:FcLCAl6lXksJ:delab.csd.auth.gr/~dimokas/psd/Pliroforiaka_Systimata_Dioikisis_2.ppt+%CE%BC%CE%B5%CF%81%CE%B7+%CE%B5%CE%BD%CE%BF%CF%82+%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CE%BF%CF%85+%CF%83%CF%85%CF%83%CF%84%CE%B7%CE%BC%CE%B1%CF%84%CE%BF%CF%82+%CE%B4%CE%B9%CE%BF%CE%B9%CE%BA%CE%B7%CF%83%CE%B7%CF%82&hl=el&gl=gr&pid=bl&srcid=ADGEESgpE3WocjTKPRZ3OZONtjt0UAooo-lNQjv2GO2d77DMofbn59arj-dxHgxnzoHQW3TXVcmE8uG0yf_RnV6qjTP5gxjVJmonQljZxg72Q87afj3L2-gTfT-0bTMUEQphU_pXCVLy&sig=AHIEtbSHWUgxBLc-OUMu_IRysu7ycUCJLg
172. http://www.eeei.gr/interbiz/articles/security.htm

173. http://oem.gr/main/index.php?option=com_content&view=article&id=1104:sistimata-firewalls-neas-genias&catid=13:diktyaka&Itemid=39
174. http://webcache.googleusercontent.com/search?q=cache:AabALZT3v5YJ:www.moec.gov.cy/2009_dimiourgikotita_kainotomia/imera_dimiourgikotitas/gym_agiou_pavlou/Diktia_ensirmata_kai_asirmata.ppt+%CF%80%CE%BB%CE%B5%CE%BF%CE%BD%CE%B5%CE%BA%CF%84%CE%B7%CE%BC%CE%B1%CF%84%CE%B1+%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B5%CE%B9%CE%B1%CF%82+%CF%84%CE%BF%CF%80%CE%B9%CE%BA%CF%89%CE%BD+%CE%B4%CE%B9%CE%BA%CF%84%CF%85%CF%89%CE%BD&cd=21&hl=el&ct=clnk&gl=gr&source=www.google.gr
175. http://webcache.googleusercontent.com/search?q=cache:AabALZT3v5YJ:www.moec.gov.cy/2009_dimiourgikotita_kainotomia/imera_dimiourgikotitas/gym_agiou_pavlou/Diktia_ensirmata_kai_asirmata.ppt+%CF%80%CE%BB%CE%B5%CE%BF%CE%BD%CE%B5%CE%BA%CF%84%CE%B7%CE%BC%CE%B1%CF%84%CE%B1+%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B5%CE%B9%CE%B1%CF%82+%CF%84%CE%BF%CF%80%CE%B9%CE%BA%CF%89%CE%BD+%CE%B4%CE%B9%CE%BA%CF%84%CF%85%CF%89%CE%BD&cd=21&hl=el&ct=clnk&gl=gr&source=www.google.gr
176. http://www.myeasyinternet.net/2010/04/windows_7050.html
177. http://dspace.lib.uom.gr/bitstream/2159/3781/1/ZiwgaMsc2008.pdf
178. http://docs.google.com/viewer?a=v&q=cache:DZ8BbpMIq1MJ:nemertes.lis.upatras.gr/dspace/bitstream/123456789/768/1/ValeontisThesis.pdf+%CF%83%CF%85%CF%83%CF%84%CE%B7%CE%BC%CE%B1+%CE%B1%CE%BD%CE%B9%CF%87%CE%BD%CE%B5%CF%85%CF%83%CE%B7%CF%82+%CE%B5%CF%80%CE%B9%CE%B8%CE%B5%CF%83%CE%B5%CF%89%CE%BD+(+IDS+)&hl=el&gl=gr&pid=bl&srcid=ADGEEShbkPR6i_cTnfMioNCcgxZeZk5IgKBz2TT6E66WxgNMV9Mb7g6dCtMHAHI4p80cbzTUFhMpoq735BrGvj5McrD20FmYdaCDrfRtZgQUpYGXIEZR9_AzjcERuV5CR55DICmy3Xjy&sig=AHIEtbR5TJ5JAG3QWFekRen5yx9vpYvAAQ
179. http://www.ebusiness-lab.gr/files/dmdocuments/Ptyxiakes-old/PDFs/lagoutaris-tsoukalas.pdf
180. http://pcex.gr/pc/index.php?option=com_content&task=view&id=30&Itemid=43
181. http://www.pctools.com/gr/internet-security/
182. http://athina.cs.unipi.gr/site-ergastirio/asfaleia_diktion/simeioseis/kefalaio3.pdf
183. http://oem.gr/main/index.php?option=com_content&view=article&id=1104:sistimata-firewalls-neas-genias&catid=13:diktyaka&Itemid=39

184. http://www.keplinet-chanion.gr/index.php?option=com_content&view=article&id=268:---&catid=57&Itemid=163
185. http://www2.e-yliko.gr/htmls/safety/svirus.aspx
186. http://6lyk-n-smyrn.att.sch.gr/ergasies20092010/KoziokosKamilos.pdf
187. http://nefeli.lib.teicrete.gr/browse/stef/epp/2009/GavrilakiKaterina/attached-document-1260438239-880866-12170/Gavrilaki2009.pdf
188. http://nefeli.lib.teicrete.gr/browse/sdo/log/2010/KypriotakisEmmanouel/attached-document-1265706768-212448-16543/Kypriotakis2010.pdf
189. http://dide.flo.sch.gr/Plinet/Tutorials-Girtsos/Hacking-InternetSecurity.pdf
190. http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Itemid=0&langEN
191. http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Hackers-Crackers.html
192. http://www.pcw.gr/Article/News-General-PCs-Notebooks/hacking_tips_legal_hardware_software_gaming/236-4726.html&pbreak=1&pbreak=2&pbreak=3&pbreak=4&pbreak=0&pbreak=1&pbreak=2&pbreak=3&pbreak=4&pbreak=0
193. http://www.kybernografoi.gr/issues/no11/hacking.htm
194. http://nemertes.lis.upatras.gr/dspace/bitstream/123456789/1594/1/Ergasia1.pdf
195. http://www.madata.gr/diafora/technology/34288.html
196. http://www.2600.gr/?page=who/hacker_definition
197. http://6lyk-n-smyrn.att.sch.gr/ergasies20092010/VasalosVafeiadis.pdf
198. http://kosmidis-athanasios.pblogs.gr/2008/01/hackers.html
199. http://i-teacher.gr/files/5o_teyxos_3_2007.pdf
200. http://xakworld.blogspot.com/2009/09/blog-post_181.html
201. http://www.p0wnbox.com/index.php?showtopic=169
202. http://www.5-9report.gr/59report/5-9%20REPORT%20vol32.pdf
203. http://archive.enet.gr/online/online_obj?pid=25&tp=T&id=81420156
204. http://news.kathimerini.gr/4dcgi/_w_articles_economyepix_1_23/08/2006_194922
205. http://www.tanea.gr/default.asp?pid=2&artid=4512344&ct=2
206. http://www.icsd.aegean.gr/website_files/proptyxiako/871591340.pdf
207. http://www.eeei.gr/interbiz/articles/security.htm

208. http://www.espressonews.gr/default.asp?pid=79&catid=1&artID=973527
209. http://www.tanea.gr/default.asp?pid=2&ct=1&artId=86736
210. http://news.pathfinder.gr/world/news/503916.html
211. http://students.ceid.upatras.gr/~akis/jotd23/0358.html
212. http://mpl.med.uoa.gr/Downloads/PDF/internet.pdf
213. http://www.ebusiness-lab.gr/files/dmdocuments/Ptyxiakes-old/PDFs/apostolo_daramou_prostasia_proswpikwn.pdf
214. http://www.keplinet-chanion.gr/index.php?option=com_content&view=article&id=268:---&catid=57&Itemid=163
215. www.moec.gov.cy/2009.../imera.../Diktia_ensirmata_kai_asirmata.ppt