ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ
& ΤΕΧΝΟΛΟΓΙΑΣ

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΤΜΗΜΑ ΧΗΜΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ:

ΕΦΟΔΙΑΣΜΟΣ & ΔΙΑΚΙΝΗΣΗ ΠΡΟΙΟΝΤΩΝ

LOGISTICS

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ηλεκτρονικές Βάσεις Δεδομένων - Απειλές & Μέθοδοι Προστασίας

ΕΠΙΒΛΕΠΩΝ: ΧΟΝΔΡΟΚΟΥΚΗΣ ΓΡΗΓΟΡΗΣ
ΕΠΙΚΟΥΡΟΣ ΚΑΘΗΓΗΤΗΣ

ΚΑΤΡΑΜΑΔΟΣ Σ. ΙΩΑΝΝΗΣ

ΠΕΙΡΑΙΑΣ 2003

Στην Οικογένειά μου,
με αγάπη.

Περίληψη

Η παρούσα διπλωματική εργασία με τίτλο «***Ηλεκτρονικές Βάσεις Δεδομένων - Απειλές & Μέθοδοι Προστασίας***» διεξήχθει στο τμήμα Βιομηχανικής Διοίκησης **&** Τεχνολογίας του Πανεπιστημίου Πειραιώς

Θα ήθελα να ευχαριστήσω θερμά τον κ.Γρηγόρη Χονδροκούκη Επίκουρο Καθηγητή στα Πληροφοριακά Συστήματα του τμήματος Βιομηχανικής Διοίκησης **&** Τεχνολογίας του Πανεπιστημίου Πειραιώς, για την ανάθεση του συγκεκριμένου θέματος καθώς και για την συνεχή επίβλεψή του, τις πολύτιμες συμβουλές και υποδείξεις του καθόλη τη διάρκεια εκπόνησης της διπλωματικής εργασίας.

Θα ήθελα να ευχαριστήσω επίσης τον συνάδελφο Χημικό Μηχανικό κ.Σταύρο Κοντακτσή **Project Manager e-Business Services** της **Contact Solutions** ΕΠΕ καθώς και τον κ.Ιάκωβο Σιγάλα **Cardiovascular Franchise Manager Europe Middle East and Africa (EMEA)** της εταιρείας **Novartis** για τις πολύτιμες συμβουλές τους σχετικά με το θέμα της διπλωματικής αλλά και για την σημαντική βοήθειά τους κατά την συμπλήρωση των ερωτηματολογίων.

Ιδιαίτερες ευχαριστίες θα ήθελα να εκφράσω προς τον κ.Νικόλαο Μπλέσιο Καθηγητή του τμήματος Βιομηχανικής Διοίκησης **&** Τεχνολογίας του Πανεπιστημίου Πειραιώς, για την σημαντική συμβολή του καθόλη τη διάρκεια του μεταπτυχιακού προγράμματος

Τέλος, ευχαριστώ θερμά τα μέλη της τριμελούς επιτροπής: κ.Νικόλαο Μπλέσιο Καθηγητή του τμήματος Βιομηχανικής Διοίκησης **&** Τεχνολογίας του Πανεπιστημίου Πειραιώς, κ.Δημήτριο Καραλέκα Επίκουρο Καθηγητή του τμήματος Βιομηχανικής Διοίκησης **&** Τεχνολογίας του Πανεπιστημίου Πειραιώς και τον κ.Γρηγόρη Χονδροκούκη Επίκουρο Καθηγητή στα Πληροφοριακά Συστήματα του τμήματος Βιομηχανικής Διοίκησης **&** Τεχνολογίας του Πανεπιστημίου Πειραιώς.

ΚΑΤΡΑΜΑΔΟΣ Σ. ΙΩΑΝΝΗΣ
ΧΗΜΙΚΟΣ ΜΗΧΑΝΙΚΟΣ Ε.Μ.Π.
ΠΕΙΡΑΙΑΣ **11/02/2003**

Περίληψη

"Ηλεκτρονικές Βάσεις Δεδομένων - Απειλές & Μέθοδοι Προστασίας"

Εάν η πληροφορία στις μέρες μας δεν ήταν πολύτιμη τότε ασφαλώς και δεν θα αποτελούσε τόσο μεγάλο αντικείμενο συζήτησης. Ωστόσο η πληροφορία όχι μόνο είναι πολύτιμη αλλά με σταθερά βήματα μετατρέπεται σε αξία. Δεν θα ήταν υπερβολή αν λέγαμε πως ζούμε τον αιώνα της πληροφορίας. Είναι επομένως εκ των ουκ άνευ, να τονισθεί η ανάγκη για ανάπτυξη και εφαρμογή προγραμμάτων προστασίας των βάσεων δεδομένων και κυρίως των ηλεκτρονικών βάσεων.

Η ανάπτυξη τέτοιων προγραμμάτων απαιτεί την ορθή απάντηση σε δύο ερωτήσεις που είναι θεμελιώδες τμήμα της ανάλυσης ρίσκου **(Risk Analysis)**. Αφενός οφείλουμε να αντιληφθούμε ποιοί είναι οι εν δυνάμει εχθροί μας, που θα ήθελαν να εισβάλλουν στις βάσεις δεδομένων μας και αφετέρου γιατί θα το έκαναν αυτό. Σημαντικό λοιπόν, είναι να δούμε από τη δική τους σκοπιά, από τη σκοπιά του επιτιθέμενου, την αξία των πληροφοριών μας. Πολλές φορές αυτά που εμείς κρίνουμε ως μικρής σημασίας για κάποιους άλλους μπορεί να έχουν αισθητά μεγαλύτερη αξία. Για παράδειγμα μια απλή ιστοσελίδα μιας εταιρείας μπορεί να θεωρείται από την ίδια την εταιρεία ως μη σημαντική για να προστατευθεί. Για ένα απλό **hacker** όμως, μπορεί να αποτελεί μεγάλο κατόρθωμα να της επιτεθεί. Συνεπώς το γοήτρο της εταιρείας μπορεί να πληγεί ανεπανόρθωτα και αυτό ασφαλώς να έχει μεγαλύτερο κόστος από όσο θα χρειαζόταν προκειμένου να προστατευθεί η ιστοσελίδα.

Το Διαδίκτυο, όχι πολλά χρόνια πριν, αποτελούσε ένα κατά πολύ μικρότερο τόπο συγκριτικά με σήμερα. Οι κόμβοι του ήταν διεσπαρμένοι σε μερικά ακαδημαϊκά ιδρύματα, ερευνητικά εργαστήρια και εταιρείες. Οι χρήστες του ήταν κυρίως φοιτητές, ερευνητές και γενικότερα άνθρωποι που ασχολούνταν κατά τον έναν ή τον άλλο τρόπο με την τεχνολογία και τις επιστήμες. Η υποδομή του, το διάσημο ζεύγος πρωτοκόλλων **TCP/IP**, είχε σχεδιαστεί για να λειτουργεί απλά και αποτελεσματικά, χωρίς να περιλαμβάνει ιδιαίτερους μηχανισμούς ή δικλίδες ασφαλείας.

Η ασφάλεια είναι μία λέξη, ακριβέστερα μια έννοια που δεν απασχολούσε ιδιαίτερα τους πρώτους κυβερνοναύτες. Βεβαίως, σχετικά νωρίς είχαν εκδηλωθεί κάποια ανησυχητικά φαινόμενα, όπως διάδοση ιών, μη εξουσιοδοτημένες προσβάσεις σε συστήματα κ.ά., ωστόσο τα κρούσματα ήταν μεμονωμένα και παρά την ταλαιπωρία που προκαλούσαν στους υπεύθυνους διαχειριστές συστημάτων αντιμετωπίζονταν αποτελεσματικά. Σύντομα, το Διαδίκτυο ξέφυγε από τα στενά ακαδημαϊκά και ερευνητικά πλαίσια, κερδίζοντας τις καρδιές ολοένα και περισσότερων απλών χρηστών, ακόμα και ανθρώπων που δεν είχαν άμεση σχέση με την τεχνολογία και τους υπολογιστές. Η πολυπλοκότητά του ως σύστημα, με την ευρύτερη έννοια, άρχισε να αυξάνει με γοργό ρυθμό, κάνοντας φανερό ότι θα εξαπλωθεί, θα παρεισφρήσει και θα αγκαλιάσει κάθε πλευρά της κοινωνικής και οικονομικής ζωής.

Έτσι και έγινε. Όπως όμως συμβαίνει και με άλλα συστήματα στη φύση αλλά και στις ανθρώπινες κοινωνίες, από την αύξηση της πολυπλοκότητας δεν προέκυψαν μόνον επιθυμητές ιδιότητες. Όταν το σύστημα διαβεί ένα συγκεκριμένο κατώφλι το οποίο, μάλιστα, δύσκολα μπορεί να γίνει διακριτό εκ των προτέρων, οι προκύπτουσες ιδιότητες γίνονται δυνητικά επιβλαβείς για τους συμμετέχοντες **(**και μη**)** στο σύστημα, ακόμα και για την ίδια την υπόστασή του. Εν προκειμένω, κανείς δεν αμφιβάλλει ότι το Διαδίκτυο αποτελεί ένα πολύπλοκο σύστημα. Εκτείνεται σε ολόκληρο τον πλανήτη, μεταβάλλοντας τη σημασία του χώρου και του χρόνου, φέρνοντας κοντά εκατομμύρια ανθρώπους με διαφορετικό πολιτισμικό, οικονομικό και κοινωνικοπολιτικό υπόβαθρο.

Όλοι αυτοί επικοινωνούν, διασκεδάζουν, εκπαιδεύονται, πληροφορούνται, συνεργάζονται και διεξάγουν τις όποιες οικονομικές ή επιχειρηματικές δραστηριότητές τους στο οικουμενικό αυτό μέσο. Μάλιστα, πάρα πολλοί από τους χρήστες του **Internet** έχουν λίγες έως και ελάχιστες τεχνικές γνώσεις, χωρίς αυτό να τους εμποδίζει να χρησιμοποιούν και να επωφελούνται από τα χαρακτηριστικά που τους ενδιαφέρουν. Ποια είναι, λοιπόν, τα αρνητικά ή έστω ανησυχητικά φαινόμενα που προκύπτουν από την εξάπλωση του Διαδικτύου; Από όλα όσα μπορεί να παραθέσει κανείς, εμείς θα επικεντρώσουμε την προσοχή μας σε αυτό που αποτελεί και το θέμα της παρούσας διπλωματικής: Πως θα καταφέρουμε να προστατέψουμε το σύγχρονο αγαθό, τα ηλεκτρονικά δεδομένα.

Περιεχόμενα

Ηλεκτρονικές βάσεις δεδομένων - Απειλές & μέθοδοι προστασίας

Κεφάλαιο 1

Βάσεις Δεδομένων & Χρήστες Βάσεων Δεδομένων

1.1 Τι είναι οι βάσεις δεδομένων

Οι βάσεις δεδομένων και η τεχνολογία βάσεων δεδομένων εξασκούν σημαντική επίδραση τόσο στη χρήση των ηλεκτρονικών υπολογιστών όσο και στην ανάπτυξη των εμπορικών συναλλαγών. Είναι εύλογο να ειπωθεί ότι οι βάσεις δεδομένων διαδραματίζουν κρίσιμο ρόλο σε όλες τις περιοχές όπου χρησιμοποιούνται υπολογιστές, όπως στις επιχειρήσεις, στη μηχανική, στην ιατρική, στα νομικά, στην εκπαίδευση. Η έκφραση βάση δεδομένων βρίσκεται σε καθημερινή χρήση. Ο αρχικός ορισμός που την περιγράφει είναι αρκετά γενικός.

Βάση δεδομένων **(Database)** είναι μία συλλογή από σχετιζόμενα δεδομένα. Με τον όρο δεδομένα εννοούμε γνωστά γεγονότα που μπορούν να καταγραφούν και που έχουν κάποια υπονοούμενη σημασία. Ως παράδειγμα μπορούμε να θεωρήσουμε τα ονόματα, τους αριθμούς τηλεφώνων και τις διευθύνσης ανθρώπων που γνωρίζουμε. Αυτά τα δεδομένα μπορεί να έχουν καταγραφεί σε ένα ευρετήριο διευθύνσεων ή μπορεί να έχουν αποθηκευτεί σε κάποιον υπολογιστή. Έχει συνεπώς δημιουργηθεί μία συλλογή από σχετιζόμενα δεδομένα με υπονοούμενη σημασία και, επομένως, μία βάση δεδομένων.

Μια βάση δεδομένων έχει τις ακόλουθες ιδιότητες.

- Αναπαριστά κάποια άποψη του πραγματικού κόσμου, η οποία μερικές φορές λέγεται μικρόκοσμος. Οι αλλαγές στο μικρόκοσμο αντανακλώνται στη βάση δεδομένων.
- Μια βάση δεδομένων είναι μια λογική συνεκτική συλλογή δεδομένων που έχει κάποια εγγενή σημασία. Μια τυχαία διευθέτηση δεδομένων δεν είναι σωστό να αναφέρεται ως βάση δεδομένων.
- Μια βάση δεδομένων σχεδιάζεται, χτίζεται και γεμίζει με δεδομένα για κάποιο συγκεκριμένο σκοπό. Προορίζεται για μια συγκεκριμένη ομάδα χρηστών και για κάποιες προκαθορισμένες εφαρμογές για τις οποίες οι χρήστες αυτοί ενδιαφέρονται.

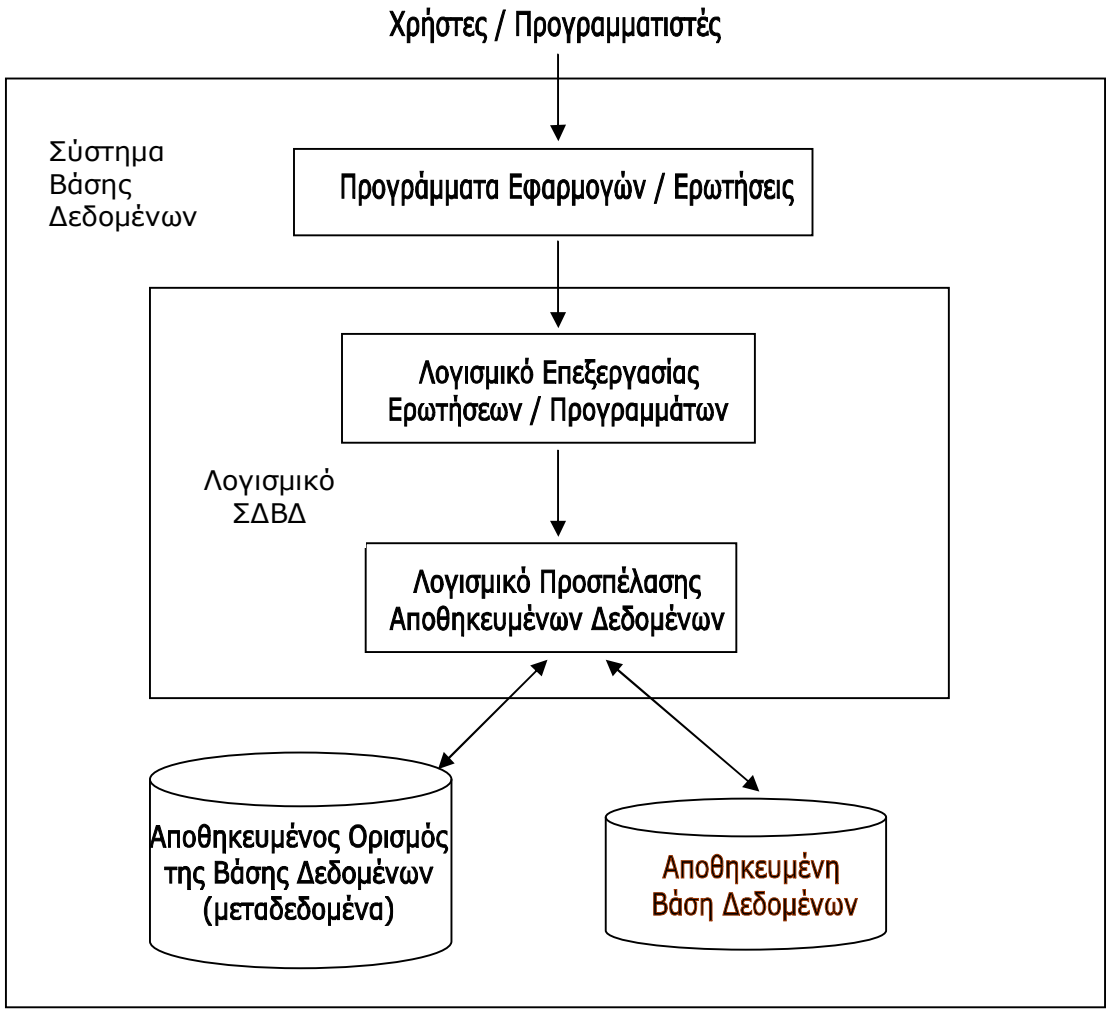
Με άλλα λόγια, μια βάση δεδομένων έχει κάποια πηγή από την οποία παράγονται τα δεδομένα, αλληλεπιδρά σε κάποιο βαθμό με γεγονότα του πραγματικού κόσμου και απευθύνεται σε ένα ακροατήριο που ενδιαφέρεται ενεργά για το περιεχόμενό της.

Μια βάση δεδομένων μπορεί να έχει οποιοδήποτε μέγεθος και κυμαινόμενη πολυπλοκότητα. Για παράδειγμα, η λίστα ονομάτων και διευθύνσεων που αναφέρθηκε προηγουμένως μπορεί να αποτελείται από λίγες μόνο εκατοντάδες εγγραφές, που κάθε μια τους έχει απλή δομή. Από την άλλη πλευρά, ο κατάλογος με τις κάρτες μιας μεγάλης βιβλιοθήκης μπορεί να περιέχει μισό εκατομμύριο κάρτες αποθηκευμένες υπό διαφορετικές κατηγορίες -ως προς το όνομα του συγγραφέα, ως προς το θέμα, ως προς τον τίτλο του βιβλίου- με κάθε κατηγορία οργανωμένη κατά αλφαβητική σειρά.μια βάση δεδομένων ακόμη μεγαλύτερου μεγέθους και πολυπλοκότητας διατηρεί η εφορία για να διαχειρίζεται τις δηλώσεις που υποβάλλουν οι φορολογούμενοι. Έτσι στις Ηνωμένες Πολιτείες αν υποθέσουμε ότι υπάρχουν εκατό εκατομμύρια φορολογούμενοι και ότι κάθε φορολογούμενος συμπληρώνει κατά μέσο όρο πέντε φόρμες με διακόσιους χαρακτήρες πληροφορίας σε κάθε φόρμα, θα έχουμε μια βάση δεδομένων με **$100*(10^6)*200*5$ bytes** πληροφοριών. Υποθέτοντας ότι η εφορία κρατά στοιχεία για τις τελευταίες τρεις δηλώσεις κάθε φορολογούμενου καθώς και για την τρέχουσα δήλωση, θα είχαμε μια βάση δεδομένων με **$4*(10^{11})$ bytes.** Αυτό τον τεράστιο όγκο πληροφοριών πρέπει να τον οργανώσουμε, να τον προστατέψουμε από πιθανές επιθέσεις και να τον διαχειριστούμε κατά τέτοιο τρόπο ώστε οι χρήστες να μπορούν να αναζητήσουν, να ανακτήσουν και να ενημερώσουν τα δεδομένα που χρειάζονται.

Ένα σύστημα διαχείρισης βάσεων δεδομένων **(ΣΔΒΔ) (database management system-DBMS)** είναι μια συλλογή από προγράμματα που επιτρέπουν στους χρήστες να δημιουργήσουν και να συντηρήσουν μια βάση δεδομένων. Επομένως το ΣΔΒΔ είναι ένα γενικής χρήσης σύστημα λογισμικού που διευκολύνει τις διαδικασίες ορισμού, κατασκευής και χειρισμού βάσεων δεδομένων για διάφορες εφαρμογές. Ο ορισμός **(definition)** μιας βάσης δεδομένων περιλαμβάνει την προδιαγραφή των τύπων, των δομών και των περιορισμό των δεδομένων που θα αποθηκευτούν στη βάση. Κατασκευή **(construction)** μιας βάσης δεδομένων είναι η διαδικασία αποθήκευσης των ίδιων των δεδομένων σε ένα μέσο αποθήκευσης που ελέγχεται από το ΣΔΒΔ. Ο χειρισμός **(manipulation)** μιας βάσης δεδομένων περιλαμβάνει λειτουργίες όπως υποβολή ερωτήσεων **(queries)** προς τη

βάση για ανάκτηση συγκεκριμένων δεδομένων, ενημέρωση της βάσης ώστε να αντανακλά αλλαγές στο μικρόκοσμο και παραγωγή αναφορών από τα δεδομένα.

Δεν είναι απαραίτητο να χρησιμοποιήσουμε γενικής χρήσης λογισμικό ΣΔΒΔ για την υλοποίηση μιας βάσης δεδομένων σε υπολογιστή. Θα μπορούσαμε να γράψουμε ένα δικό μας σύνολο προγραμμάτων για τη δημιουργία και τη συντήρηση της βάσης δεδομένων. Σε κάθε περίπτωση -είτε δουλεύουμε με ένα γενικής χρήσης ΣΔΒΔ είτε όχι- πρέπει συνήθως, εκτός από την ίδια τη βάση δεδομένων να χρησιμοποιήσουμε κι ένα μεγάλο όγκο λογισμικού για το χειρισμό της. Μια βάση δεδομένων, μαζί με το αντίστοιχο λογισμικό, ονομάζεται σύστημα βάσης δεδομένων. Το ΣΧΗΜΑ **1** επεξηγεί τα παραπάνω.



ΣΧΗΜΑ 1 : Το απλουστευμένο περιβάλλον ενός συστήματος βάσης δεδομένων

1.2 Χαρακτηριστικά της προσέγγισης βάσεων δεδομένων

Ένα σύνολο διαφορετικών χαρακτηριστικών ξεχωρίζουν την προσέγγιση βάσεων δεδομένων από την παραδοσιακή προσέγγιση του προγραμματισμού με χρήση αρχείων. Στην κλασσική επεξεργασία αρχείων, κάθε χρήστης ορίζει και δημιουργεί τα αρχεία που χρειάζεται για μια συγκεκριμένη εφαρμογή. Ένας χρήστης, στη Γραμματεία για παράδειγμα, μπορεί να τηρεί, ένα αρχείο για τους φοιτητές και τους βαθμούς τους και να έχει κατασκευάσει προγράμματα για να τυπώνει αναλυτικές βαθμολογίες και να εισάγει νέους βαθμούς στο αρχείο. Ένας δεύτερος χρήστης, στο Λογιστήριο, μπορεί να παρακολουθεί τα δίδακτρα και τις πληρωμές των φοιτητών. Ενώ και οι δύο χρήστες ενδιαφέρονται για τα δεδομένα των φοιτητών, κάθε χρήστης τηρεί ξεχωριστά αρχεία -και προγράμματα για το χειρισμό τους- διότι ο καθένας απαιτεί κάποια δεδομένα που δεν είναι διαθέσιμα από τα αρχεία του άλλου. Αυτός ο πλεονασμός στον ορισμό και την αποθήκευση των δεδομένων έχει ως αποτέλεσμα να σπαταλάται αποθηκευτικός χώρος και να καταβάλλεται πρόσθετος κόπος για τη διατήρηση των κοινών δεδομένων σε ενημερωμένη μορφή.

Στην προσέγγιση των βάσεων δεδομένων, διατηρείται ένας και μοναδικός ταμιευτήρας δεδομένων που ορίζεται μία φορά και στη συνέχεια προσπελάζεται από τους διάφορους χρήστες. Οι κύριες διαφορές της προσέγγισης βάσεων δεδομένων από την προσέγγιση επεξεργασίας αρχείων είναι οι ακόλουθες.

1.2.1 Η αυτοπεριγραφική φύση ενός συστήματος βάσης δεδομένων

Ένα θεμελιώδες χαρακτηριστικό της προσέγγισης βάσεων δεδομένων είναι το ότι ένα σύστημα βάσης δεδομένων δεν περιέχει μόνο την ίδια τη βάση αλλά και τον πλήρη ορισμό ή την περιγραφή αυτής. Αυτός ο ορισμός αποθηκεύεται στον κατάλογο του συστήματος, ο οποίος περιέχει πληροφορίες όπως η δομή κάθε αρχείου, ο τύπος και η μορφή αποθήκευσης κάθε στοιχειώδους δεδομένου και διάφοροι περιορισμοί επί των δεδομένων. Οι πληροφορίες που περιέχονται σε αυτόν τον κατάλογο λέγονται μετα-δεδομένα **(meta-data)** και περιγράφουν τη δομή της κυρίως βάσης. Ο κατάλογος χρησιμοποιείται από το λογισμικό του ΣΔΒΔ και περιστασιακά από τους χρήστες της βάσης δεδομένων που χρειάζονται πληροφορίες για τη δομή της βάσης. Στην παραδοσιακή επεξεργασία αρχείων, ο ορισμός των δεδομένων αποτελεί στην τυπική περίπτωση τμήμα των ίδιων των προγραμμάτων εφαρμογών.

1.2.2 Υποστήριξη πολλαπλών όψεων των δεδομένων

Στην τυπική περίπτωση μια βάση δεδομένων έχει πολλούς χρήστες, από τους οποίους κάθε ένας μπορεί να απαιτεί και μια διαφορετική προοπτική ή όψη της βάσης δεδομένων. Μια όψη μπορεί να είναι υποσύνολο της βάσης δεδομένων ή να περιέχει εικονικά δεδομένα που παράγονται από τα αρχεία της βάσης δεδομένων αλλά δεν αποθηκεύονται. Μερικοί χρήστες δεν έχουν ανάγκη να ξέρουν αν τα δεδομένα στα οποία αναφέρονται είναι αποθηκευμένα ή παραγόμενα. Ένα ΣΔΒΔ πολλαπλών χρηστών, του οποίου οι χρήστες χρησιμοποιούν μια ποικιλία εφαρμογών, πρέπει να παρέχει ευκολίες για τον ορισμό πολλαπλών όψεων.

1.2.3 Μοίρασμα των δεδομένων και επεξεργασία δοσοληψιών από πολλούς χρήστες

Ένα ΣΔΒΔ πολλών χρηστών πρέπει να επιτρέπει, όπως υπαινίσσεται και το όνομά του, σε πολλούς χρήστες να προσπελάζουν τη βάση δεδομένω κατά την ίδια χρονική στιγμή. Αυτό το χαρακτηριστικό αποκτά ουσιαστική σημασία αν πρόκειται δεδομένα από πολλαπλές εφαρμογές να ολοκληρωθούν και να συντηρούνται σε μια και μόνο βάση δεδομένων. Το ΣΔΒΔ πρέπει να περιλαμβάνει λογισμικό για έλεγχο ταυτόχρονης προσπέλασης που να εξασφαλίζει, στην περίπτωση που πολλοί χρήστες προσπαθούν να ενημερώσουν τα ίδια δεδομένα, ότι αυτό γίνεται κατά ελεγχόμενο τρόπο ώστε το αποτέλεσμα να είναι σωστό. Ένα παράδειγμα είναι η περίπτωση όπου υπάλληλοι κρατήσεων προσπαθούν να κρατήσουν μία θέση σε μία αεροπορική πτήση. Το ΣΔΒΔ πρέπει να εξασφαλίσει ότι κάθε θέση μπορεί σε κάθε στιγμή να την προσπελάσει μόνο ένας υπάλληλος για να την παραχωρήσει σε ένα επιβάτη. Αυτές οι εφαρμογές γενικά ονομάζονται εφαρμογές επεξεργασίας δοσοληψιών. Βασικός ρόλος του λογισμικού ενός ΣΔΒΔ πολλαπλών χρηστών είναι να εξασφαλίζει ότι οι ταυτόχρονες δοσοληψίες εκτελούνται σωστά χωρίς παρεμβολές.

1.3 Εργαζόμενοι στο προσκήνιο

Για μια μικρή προσωπική βάση δεδομένων, όπως η λίστα των διευθύνσεων, συνήθως ένα άτομο ορίζει, κατασκευάζει και χειρίζεται τη βάση. Αντίθετα, πολλά άτομα αναμειγνύονται στο σχεδιασμό, στη χρήση και στη συντήρηση μιας μεγάλης βάσης δεδομένων με εκατοντάδες χρήστες. Στην ενότητα αυτή περιγράφουμε τα άτομα που η εργασία τους περιλαμβάνει την καθημερινή χρήση μιας μεγάλης βάσης δεδομένων, τους οποίους και ονομάζουμε "εργαζόμενοι στο προσκήνιο". Στην ενότητα **1.4** εξετάζουμε τα άτομα που μπορούν να ονομαστούν "εργαζόμενοι στο παρασκήνιο" -είναι αυτοί που εργάζονται για τη συντήρηση του περιβάλλοντος του συστήματος βάσης δεδομένων, αλλά δεν ενδιαφέρονται ενεργά για την ίδια τη βάση.

1.3.1 Διαχειριστές βάσεων δεδομένων

Σε κάθε οργανισμό όπου πολλά άτομα χρησιμοποιούν τους ίδιους πόρους, υπάρχει ανάγκη για ένα προϊστάμενο διαχειριστή που να επιβλέπει και να διαχειρίζεται τους πόρους αυτούς. Σε ένα περιβάλλον βάσης δεδομένων, ο πρωτεύον πόρος είναι η ίδια η βάση δεδομένων και δευτερεύοντες πόροι είναι το ΣΔΒΔ και το σχετικό λογισμικό. Η διαχείριση αυτών των πόρων είναι υπευθυνότητα του διαχειριστή της βάσης δεδομένων **(**ΔΒΔ**) (Database administrator)**. Ο ΔΒΔ είναι υπεύθυνος να εξουσιοδοτεί την προσπέλαση στη βάση δεδομένων, να συντονίζει και να παρακολουθεί τη χρήση της και να αποκτά πόρους λογισμικού και υλικού σύμφωνα με τις ανάγκες. Ο ΔΒΔ είναι υπεύθυνος για προβλήματα όπως παραβιάσεις ασφάλειας ή χαμηλή απόδοση συστήματος - μεγάλοι χρόνοι απόκρισης. Σε μεγάλους οργανισμούς, ο ΔΒΔ υποβοηθάται από αντίστοιχο προσωπικό για να εκτελέσει όλες αυτές τις λειτουργίες.

1.3.2 Σχεδιαστές βάσεων δεδομένων

Οι σχεδιαστές βάσεων δεδομένων είναι υπεύθυνοι να προσδιορίσουν τα δεδομένα που θα αποθηκευτούν στη βάση και να επιλέξουν κατάλληλες δομές για την αναπαράσταση και την αποθήκευση αυτών των δεδομένων. Αυτές οι εργασίες γίνονται ως επί το πλείστον πριν την υλοποίηση της βάσης δεδομένων. Οι σχεδιαστές είναι υπεύθυνοι να επικοινωνήσουν με όλους τους υποψήφιους χρήστες της βάσης προκειμένου να κατανοήσουν τις απαιτήσεις τους και να δώσουν ένα σχεδιασμό που να καλύπτει τις απαιτήσεις αυτές. Σε πολλές περιπτώσεις, οι σχεδιαστές ανήκουν στους υφισταμένους του ΔΒΔ και μπορεί να

αναλαμβάνουν άλλες ευθύνες μετά την ολοκλήρωση του σχεδιασμού της βάσης. Στην τυπική περίπτωση, οι σχεδιαστές της βάσης δεδομένων επικοινωνούν με κάθε ομάδα ενδεχόμενων χρηστών και αναπτύσσουν μια όψη της βάσης δεδομένων που καλύπτει τις απαιτήσεις δεδομένων και επεξεργασίας αυτής της ομάδας. Οι όψεις αυτές στη συνέχεια αναλύονται και ενοποιούνται με τις όψεις των άλλων ομάδων χρηστών. Ο τελικός σχεδιασμός της βάσης δεδομένων πρέπει να μπορεί να υποστηρίξει τις απαιτήσεις όλων των ομάδων χρηστών.

1.3.3 Τελικοί χρήστες

Αυτοί είναι τα άτομα που η εργασία τους απαιτεί προσπέλαση στη βάση δεδομένων για ερωτήσεις, ενημέρωση και παραγωγή αναφορών. Η βάση δεδομένων υφίσταται κυρίως για δική τους χρήση. Υπάρχουν αρκετές κατηγορίες τελικών χρηστών:

¬ Περιστασιακοί τελικοί χρήστες είναι αυτοί που προσπελάζουν κατά καιρούς τη βάση δεδομένων αλλά μπορεί να χρειάζονται διαφορετικές πληροφορίες κάθε φορά. Χρησιμοποιούν μια περίπλοκη γλώσσα ερωτήσεων και στην τυπική περίπτωση είναι μέσα ή υψηλόβαθμα διοικητικά στελέχη ή άλλοι περιστασιακοί χρήστες.

¬ Οι απλοϊκοί ή παραμετρικοί τελικοί χρήστες αποτελούν ένα μεγάλο τμήμα των τελικών χρηστών μιας βάσης δεδομένων. Η κύρια εργασία τους επικεντρώνεται σε συνεχείς ερωτήσεις και ενημερώσεις που λέγονται προκατασκευασμένες δοσοληψίες και οι οποίες έχουν προγραμματισθεί και ελεγχθεί προσεκτικά. Όλοι έχουμε συνηθίσει να συναλλασσόμαστε με αρκετών ειδών τέτοιους χρήστες. Υπάλληλοι κρατήσεων σε αεροπορικές εταιρείες, ξενοδοχεία και γραφεία ενοικιάσεως αυτοκινήτων ελέγχουν την διαθεσιμότητα για συγκεκριμένες θέσεις ή οχήματα και κάνουν κρατήσεις. Υπάλληλοι υποδοχής δεμάτων σε γραφεία ταχυμεταφορών εισάγουν τα στοιχεία των δεμάτων μέσω ραβδωτού κώδικα και συμπληρωματικές πληροφορίες από το πληκτρολόγιο, ενημερώνοντας μια κεντρική βάση δεδομένων για τα δέματα που φθάνουν ή διέρχονται.

¬ Οι εξειδικευμένοι τελικοί χρήστες περιλαμβάνουν μηχανικούς, επιστήμονες, αναλυτές επιχειρήσεων και άλλους που μαθαίνουν σε βάθος τις δυνατότητες των ΣΔΒΔ για να μπορούν να ανταποκριθούν στις πολύπλοκες απαιτήσεις της δουλειάς τους.

¬ Οι μεμονωμένοι χρήστες διατηρούν προσωπικές βάσεις δεδομένων χρησιμοποιώντας έτοιμα πακέτα προγραμμάτων που παρέχουν εύχρηστες διεπαφές βασισμένες σε μενού ή γραφικά. Ένα παράδειγμα είναι ο χρήστης ενός φορολογικού πακέτου που αποθηκεύει διάφορα προσωπικά οικονομικά δεδομένα για φορολογικούς λόγους.

Ένα τυπικό ΣΔΒΔ παρέχει πολλές ευκολίες για την προσπέλαση μιας βάσης δεδομένων. Οι απλοϊκοί τελικοί χρήστες αρκεί να ξέρουν πολύ λίγα για τις δυνατότητες που παρέχει το ΣΔΒΔ, το μόνο που χρειάζεται να καταλαβαίνουν είναι οι τύποι των τυποποιημένων δοσοληψιών που έχουν σχεδιαστεί και υλοποιηθεί για χρήση από αυτούς. Οι περιστασιακοί χρήστες μαθαίνουν λίγες μόνο δυνατότητες που μπορούν να χρησιμοποιούν κατ' επανάληψη. Οι εξειδικευμένοι χρήστες προσπαθούν να μάθουν τις περισσότερες δυνατότητες ενός ΣΔΒΔ προκειμένου να ικανοποιήσουν τις πολύπλοκες απαιτήσεις τους. Οι μεμονωμένοι χρήστες συνήθως γίνονται ειδήμονες στη χρήση ενός συγκεκριμένου λογισμικού πακέτου.

1.3.4 Αναλυτές συστημάτων & προγραμματιστές

Οι αναλυτές συστημάτων προσδιορίζουν τις απαιτήσεις των τελικών χρηστών, ειδικά των απλοϊκών, και αναπτύσσουν προδιαγραφές για προκαθορισμένες δοσοληψίες που καλύπτουν τις απαιτήσεις αυτές. Οι προγραμματιστές εφαρμογών υλοποιούν τις προδιαγραφές των τυποποιημένων δοσοληψιών σε προγράμματα, τα οποία στη συνέχεια ελέγχουν, διορθώνουν, τεκμηριώνουν και συντηρούν. Για να πετύχουν τους σκοπούς τους οι αναλυτές και οι προγραμματιστές πρέπει να είναι εξοικιωμένοι με την πλήρη γκάμα δυνατοτήτων που παρέχει το ΣΔΒΔ.

1.4 Εργαζόμενοι στο παρασκήνιο

Επί πλέον αυτών που σχεδιάζουν, χρησιμοποιούν και διαχειρίζονται μια βάση δεδομένων, υπάρχουν και άλλοι που σχετίζονται με το σχεδιασμό, την ανάπτυξη και τη λειτουργία του λογισμικού του ΣΔΒΔ και του περιβάλλοντος συστήματος. Αυτά τα άτομα συνήθως δεν ενδιαφέρονται για αυτή καθεαυτή τη βάση. Τους ονομάζουμε εργαζόμενους στο παρασκήνιο και περιλαμβάνουν τις πιο κάτω κατηγορίες.

1.4.1 Άτομα που σχεδιάζουν και υλοποιούν ΣΔΒΔ

Αυτοί είναι άτομα που σχεδιάζουν και υλοποιούν τα τμήματα και τις διεπαφές του ΣΔΒΔ ως πακέτα λογισμικού. Ένα ΣΔΒΔ είναι ένα πολύπλοκο σύστημα λογισμικού που αποτελείται από πολλά συστατικά ή τμήματα, συμπεριλαμβανομένων τμημάτων για την υλοποίηση του καταλόγου, της γλώσσας ερωτήσεων, των επεξεργαστών διεπαφής, της προσπέλασης στα δεδομένα και της ασφάλειας. Το ΣΔΒΔ πρέπει να επικοινωνεί με άλλα συστήματα λογισμικού όπως το λειτουργικό σύστημα και οι μεταγλωττιστές διαφόρων γλωσσών προγραμματισμού.

1.4.2 Κατακευαστές εργαλείων

Τα εργαλεία είναι πακέτα λογισμικού που διευκολύνουν το σχεδιασμό και τη χρήση συστημάτων βάσεων δεδομένων και βοηθούν στη βελτίωση της απόδοσης. Τα εργαλεία είναι προαιρετικά πακέτα που συνήθως αγοράζονται ξεχωριστά. Περιλαμβάνουν πακέτα για σχεδιασμό βάσεων δεδομένων, παρακολούθηση της απόδοσης, διεπαφές φυσικής γλώσσας ή γραφικών, πρωτοτυποποίηση, προσομοίωση και παραγωγή δοκιμαστικών δεδομένων. Κατασκευαστές εργαλείων είναι τα άτομα που σχεδιάζουν και υλοποιούν τέτοια εργαλεία. Σε πολλές περιπτώσεις ανεξάρτητοι κατασκευαστές λογισμικού αναπτύσσουν και εμπορεύονται αυτά τα εργαλεία.

1.4.3 Χειριστές & προσωπικό συντήρησης

Αυτοί είναι το προσωπικό διαχείρισης συστήματος που είναι υπεύθυνο για τη λειτουργία και τη συντήρηση του περιβάλλοντος υλικού και λογισμικού του συστήματος βάσης δεδομένων. Αν και οι πιο πάνω κατηγορίες εργαζομένων στο παρασκήνιο είναι απαραίτητες για να καθιστούν το σύστημα βάσης δεδομένων διαθέσιμο στους τελικούς χρήστες, στην τυπική περίπτωση δε χρησιμοποιούν τη βάση για δικούς τους σκοπούς.

1.5 Σκοποί της χρήσης ενός ΣΔΒΔ

Στην ενότητα αυτή εξετάζουμε τους σκοπούς που έχει η χρήση ενός ΣΔΒΔ και τις δυνατότητες που θα πρέπει να έχει ένα καλό ΣΔΒΔ. Ο ΔΒΔ πρέπει να χρησιμοποιεί τις δυνατότητες αυτές ώστε να επιτυγχάνει διάφορους σκοπούς που έχουν σχέση με το σχεδιασμό, τη διαχείριση και τη χρήση μιας μεγάλης βάσης δεδομένων από πολλούς χρήστες.

1.5.1 Έλεγχος των πλεονασμών

Στην παραδοσιακή ανάπτυξη λογισμικού που χρησιμοποιεί επεξεργασία αρχείων, κάθε ομάδα χρηστών διατηρεί τα δικά της αρχεία για να εξυπηρετεί τις εφαρμογές επεξεργασίας δεδομένων της. Πολλά από τα δεδομένα αποθηκεύονται από μια φορά στα αρχεία της κάθε ομάδας χρηστών. Αυτός ο πλεονασμός στην αποθήκευση πολλές φορές των ίδιων δεδομένων οδηγεί σε αρκετά προβλήματα. Πρώτον, σε πολλαπλασιασμό του μόχθου. Δεύτερον, σε σπατάλη χώρου αποθήκευσης. Τρίτον, αρχεία που αναπαριστούν τα ίδια δεδομένα μπορεί να καταστούν ασύμβατα.

Στην προσέγγιση των βάσεων δεδομένων, οι όψεις των διαφορετικών ομάδων ενοποιούνται κατά το σχεδιασμό της βάσης δεδομένων. Για λόγους συμβατότητας, θα πρέπει να έχουμε ένα σχεδιασμό της βάσης που να αποθηκεύει κάθε λογικό στοιχείο δεδομένων σε μία μόνο θέση στη βάση δεδομένων. Αυτό δεν επιτρέπει ασυμβατότητες και εξοικονομεί χώρο αποθήκευσης. Σε μερικές περιπτώσεις, ο ελεγχόμενος πλεονασμός μπορεί να είναι χρήσιμος. Στις περιπτώσεις αυτές, το ΣΔΒΔ θα πρέπει να έχει τη δυνατότητα να ελέγχει τον πλεονασμό ώστε να αποτρέπει ασυμβατότητες μεταξύ των αρχείων.

1.5.2 Περιορισμός της μη εξουσιοδοτημένης προσπέλασης

Όταν πολλοί χρήστες μοιράζονται μια βάση δεδομένων, είναι πιθανό ότι μερικοί χρήστες δεν θα είναι εξουσιοδοτημένοι να προσπελάζουν όλες τις πληροφορίες της βάσης. Για παράδειγμα, τα οικονομικά δεδομένα συχνά θεωρούνται εμπιστευτικά και επομένως ορισμένα άτομα επιτρέπεται να προσπελάζουν τα δεδομένα αυτά. Επιπλέον, σε μερικούς χρήστες μπορεί να επιτρέπεται μόνο να ανακτήσουν δεδομένα, ενώ σε άλλους και να ανακτήσουν και να ενημερώσουν. Επομένως, το είδος της προσπέλασης πρέπει επίσης να ελέγχεται. Συνήθως οι χρήστες ή οι ομάδες χρηστών παίρνουν λογαριασμούς **(accounts)** που προστατεύονται από κωδικούς χρήσης **(passwords)** και τους

οποίους μπορούν να χρησιμοποιήσουν για να έχουν προσπέλαση στη βάση. Ένα ΣΔΒΔ πρέπει να παρέχει ένα υποσύστημα ασφάλειας και εξουσιοδότησης, το οποίο χρησιμοποιεί ο ΔΒΔ για να δημιουργήσει λογαριασμούς και να προδιαγράψει περιορισμούς για κάθε λογαριασμό. Στη συνέχεια, το ΣΔΒΔ πρέπει αυτόματα να επιβάλει αυτούς τους περιορισμούς. Παρόμοιοι έλεγχοι μπορούν να εφαρμοστούν και στο λογισμικό του ΣΔΒΔ.

1.5.3. Μόνιμη αποθήκευση για αντικείμενα προγραμμάτων και δομές δεδομένων

Μια πρόσφατη εφαρμογή των βάσεων δεδομένων είναι το να παρέχουν μόνιμη αποθήκευση για αντικείμενα προγραμμάτων και για δομές δεδομένων. Αυτός είναι ένας από τους κύριους λόγους για την εμφάνιση των αντικειμενοστρεφών **(object-oriented)** ΣΔΒΔ. Η μόνιμη αποθήκευση αντικειμένων προγραμμάτων και δομών δεδομένων είναι μια σημαντική λειτουργία των συστημάτων βάσεων δεδομένων. Παραδοσιακά συστήματα βάσεων δεδομένων συχνά εμφάνιζαν το λεγόμενο πρόβλημα παρακώλυσης λόγω αναντιστοιχίας. **(impedance mismatch problem),** καθώς οι δομές δεδομένων που παρείχε το ΣΔΒΔ ήταν ασύμβατες προς τις δομές δεδομένων της γλώσσας προγραμματισμού. Τα τυπικά αντικειμενοστρεφή συστήματα βάσεων δεδομένων προσφέρουν συμβατότητα δομών δεδομένων με μία ή περισσότερες αντικειμενοστρεφείς γλώσσες προγραμματισμού.

1.5.4 Παροχή πολλαπλών διεπαφών χρηστών

Επειδή πολλές κατηγορίες χρηστών, με διαφορετικά επίπεδα τεχνικών γνώσεων, χρησιμοποιούν μια βάση δεδομένων, ένα ΣΔΒΔ πρέπει να παρέχει ποικιλία από διεπαφές χρηστών. Αυτές περιλαμβάνουν γλώσσες ερωτήσεων για περιστασιακούς χρήστες, διεπαφές γλωσσών προγραμματισμού για προγραμματιστές εφαρμογών, φόρμες και κωδικούς εντολών για παραμετρικούς χρήστες και διεπαφές βασισμένες σε μενού ή φυσική γλώσσα για μεμονωμένους χρήστες.

1.5.5 Παράσταση πολύπλοκων συσχετίσεων μεταξύ των δεδομένων

Μια βάση δεδομένων μπορεί να περιλαμβάνει μια πληθώρα δεδομένων που αλληλοσχετίζονται κατά πολλούς τρόπους. Ένα ΣΔΒΔ πρέπει να έχει τη δυνατότητα να παριστάνει μια ποικιλία πολύπλοκων συσχετίσεων μεταξύ των δεδομένων καθώς επίσης να ανακτά και να ενημερώνει σχετιζόμενα δεδομένα εύκολα και αποτελεσματικά.

1.5.6 Επιβολή περιορισμών ορθότητας

Οι περισσότερες εφαρμογές βάσεων δεδομένων έχουν διάφορους περιορισμούς ορθότητας που πρέπει να ισχύουν για τα δεδομένα. Ένα ΣΔΒΔ πρέπει να παρέχει δυνατότητες για τον ορισμό και την επιβολή τέτοιων περιορισμών. Ο απλούστερος τύπος περιορισμού ορθότητας συνίσταται στον προσδιορισμό ενός τύπου δεδομένων για κάθε στοιχείο δεδομένων. Είναι ευθύνη των σχεδιαστών της βάσης δεδομένων να αναγνωρίσουν περιορισμούς ορθότητας. Μερικοί περιορισμοί μπορεί να προσδιοριστούν σε επίπεδο ΣΔΒΔ και να επιβληθούν αυτόματα. Άλλοι περιορισμοί μπορεί να να πρέπει να ελέγχονται από τα προγράμματα ενημέρωσης ή κατά την είσοδο των δεδομένων.

Ένα στοιχείο δεδομένων μπορεί να εισαχθεί λανθασμένα αλλά να εξακολουθεί να πληρεί τους περιορισμούς ορθότητας που έχουν τεθεί. Για παράδειγμα, αν ένας φοιτητής πάρει βαθμό Α αλλά εισαχθεί από λάθος στη βάση βαθμός **C**, το ΣΔΒΔ δεν μπορεί να ανακαλύψει αυτό το λάθος αυτόματα, διότι το **C** είναι μια έγκυρη τιμή για τον τύπο δεδομένων του βαθμού. Τέτοια λάθη εισαγωγής μπορούν να ανακαλυφθούν μόνο από τον άνθρωπο **(**όταν ο φοιτητής παραπονεθεί για τη βαθμολογία που πήρε**)** και να διορθωθούν αργότερα ενημερώνοντας τη βάση δεδομένων. Ωστόσο μια τιμή βαθμού **x** μπορεί αυτόματα να απορριφθεί από το ΣΔΒΔ, διότι το **x** δεν είναι έγκυρη τιμή για τον τύπο δεδομένων βαθμός.

1.5.7 Παροχή μηχανισμών τήρησης εφεδρικών αντιγράφων & ανάκαμψης

Ένα ΣΔΒΔ πρέπει να παρέχει δυνατότητες για ανάκαμψη μετά από βλάβες υλικού ή λογισμικού. Το υποσύστημα τήρησης εφεδρικών αντιγράφων και ανάκαμψης ενός ΣΔΒΔ είναι υπεύθυνο για την ανάκαμψη. Για παράδειγμα, αν το υπολογιστικό σύστημα αποτύχει στο μέσο ενός πολύπλοκου προγράμματος ενημέρωσης, το υποσύστημα ανάκαμψης είναι υπεύθυνο να εξασφαλίσει ότι η βάση δεδομένων θα επανέλθει στην κατάσταση που βρισκόταν πριν αρχίσει να

εκτελείται το πρόγραμμα. Εναλλακτικά, το υποσύστημα ανάκαμψης θα μπορούσε να εξασφαλίσει ότι το πρόγραμμα επανεκκινείται από το σημείο στο οποίο διακόπηκε έτσι ώστε όλη του η επίδραση να καταγραφεί στη βάση δεδομένων.

1.6 Συνέπειες της προσέγγισης βάσεων δεδομένων

Επιπλέον των όσων αναφέρθηκαν στην προηγούμενη ενότητα, άλλα αποτελέσματα της προσέγγισης με χρήση βάσεων δεδομένων μπορούν να ωφελήσουν τους περισσότερους οργανισμούς.

1.6.1 Δυνατότητα επιβολής τυποποίησης

Η προσέγγιση των βάσεων δεδομένων επιτρέπει στον ΔΒΔ να ορίσει και να επιβάλει πρότυπα στους χρήστες μιας βάσης δεδομένων σε ένα μεγάλο οργανισμό. Αυτό διευκολύνει την επικοινωνία και τη συνεργασία μεταξύ διαφόρων τμημάτων, προγραμμάτων και χρηστών μέσα στον οργανισμό. Πρότυπα μπορούν να οριστούν για τα ονόματα και τη μορφή στοιχείων δεδομένων, για τη μορφή της παρουσίασης, για δομές αναφορών, για την ορολογία κ.ο.κ. Ο ΔΒΔ μπορεί να επιβάλει πρότυπα πιο εύκολα σε ένα συγκεντρωτικό περιβάλλον από ότι σε ένα περιβάλλον όπου κάθε ομάδα χρηστών έχει τον έλεγχο των δικών της αρχείων και του λογισμικού.

1.6.2 Μείωση του χρόνου ανάπτυξης των εφαρμογών

Ένα από τα κύρια και εμπορικότερα χαρακτηριστικά της προσέγγισης των βάσεων δεδομένων είναι ότι η ανάπτυξη μιας νέας εφαρμογής χρειάζεται πολύ λίγο χρόνο. Ο σχεδιασμός και η υλοποίηση μιας βάσης δεδομένων από την αρχή μπορεί να απαιτεί περισσότερο χρόνο από το να γραφτεί μια απλή εξειδικευμένη εφαρμογή αρχείων. Όμως, όταν μια βάση δεδομένων εγκατασταθεί και δουλεύει, ο χρόνος που απαιτείται για τη δημιουργία νέων εφαρμογών χρησιμοποιώντας τις δυνατότητες του ΣΔΒΔ είναι σημαντικά μικρότερος. Ο χρόνος ανάπτυξης με τη χρήση ενός ΣΔΒΔ υπολογίζεται ανάμεσα στο ένα έκτο και στο ένα τέταρτο του χρόνου με χρήση παραδοσιακών συστημάτων αρχείων.

1.6.3 Ευελιξία

Μπορεί να είναι απαραίτητο να αλλάξει η δομή μιας βάσης δεδομένων καθώς αλλάζουν οι απαιτήσεις. Για παράδειγμα, μπορεί να προκύψει μια νέα ομάδα χρηστών που χρειάζεται επιπλέον πληροφορίες που δεν βρίσκονται αυτή τη στιγμή στη βάση δεδομένων. Συνεπώς, μπορεί να χρειαστεί να προσθέσουμε ένα νέο αρχείο στη βάση δεδομένων ή να επεκτείνουμε τα στοιχειώδη δεδομένα σε ένα υφιστάμενο αρχείο. Μερικά ΣΔΒΔ επιτρέπουν τέτοιες αλλαγές στη δομή μιας βάσης δεδομένων χωρίς να επηρεάζονται τα αποθηκευμένα δεδομένα και τα υφιστάμενα προγράμματα εφαρμογών.

1.6.4 Διαθεσιμότητα ενημερωμένων πληροφοριών

Μέσω ενός ΣΔΒΔ μια βάση δεδομένων είναι διαθέσιμη σε όλους τους χρήστες. Ευθύς μόλις μια ενημέρωση από ένα χρήστη καταγραφεί στη βάση δεδομένων, όλοι οι άλλοι χρήστες μπορούν αμέσως να δουν αυτή την ενημέρωση. Αυτή η διαθεσιμότητα ενημερωμένων πληροφοριών είναι ουσιώδης για πολλές εφαρμογές επεξεργασίας δοσοληψιών, όπως συστήματα κρατήσεων ή τραπεζικές βάσεις δεδομένων, και επιτυγχάνεται με τα υποσυστήματα ελέγχου συγχρονισμού και ανάκαμψης ενός ΣΔΒΔ.

1.6.5 Οικονομία κλίμακας

Η προσέγγιση των ΣΔΒΔ επιτρέπει την ενοποίηση δεδομένων και εφαρμογών, ελλατώνοντας έτσι τις άχρηστες επικαλύψεις μεταξύ δραστηριοτήτων του προσωπικού επεξεργασίας δεδομένων σε διάφορα προγράμματα ή τμήματα. Αυτό επιτρέπει σε όλο τον οργανισμό να επενδύσει σε πιο ισχυρούς επεξεργαστές, μονάδες αποθήκευσης ή εξοπλισμό επικοινωνιών, από το να αγοράζει κάθε τμήμα ανεξάρτητα το δικό του εξοπλισμό. Έτσι, ελλατώνεται το συνολικό κόστος λειτουργίας και διαχείρισης.

1.7 Πότε δεν πρέπει να χρησιμοποιείται ΣΔΒΔ

Παρόλα αυτά τα πλεονεκτήματα, υπάρχουν μερικές περιπτώσεις όπου η χρήση ενός ΣΔΒΔ μπορεί να επιφέρει άσκοπο επιπλέον κόστος σε σύγκριση με την παραδοσιακή επεξεργασία αρχείων. Το επιπλέον κόστος χρήσης ενός ΣΔΒΔ οφείλεται στους κατωτέρω λόγους:

¬ Υψηλή αρχική επένδυση σε υλικό, λογισμικό και επιμόρφωση.

¬ Η γενικότητα που προσφέρει ένα ΣΔΒΔ για τον ορισμό και την επεξεργασία δεδομένων.

¬ Επιβαρύνσεις για την παροχή λειτουργιών ασφαλείας, ελέγχου συγχρονισμού, ανάκαμψης και ορθότητας.

¬ Πρόσθετα προβλήματα μπορεί να εμφανιστούν αν οι σχεδιαστές της βάσης δεδομένων και ο ΔΒΔ δεν σχεδιάσουν σωστά τη βάση, ή αν οι εφαρμογές του συστήματος βάσης δεδομένων δεν υλοποιηθούν σωστά. Λόγω του επιπλέον κόστους χρήσης ενός ΣΔΒΔ και των ενδεχόμενων προβλημάτων κακής διαχείρισης, ίσως είναι προτιμότερο να χρησιμοποιηθούν συνηθισμένα αρχεία κάτω από τις ακόλουθες συνθήκες:

¬ Η βάση δεδομένων και οι εφαρμογές είναι απλές, καλά ορισμένες και δεν αναμένεται να αλλάξουν.

¬ Υπάρχουν πιεστικές απαιτήσεις λειτουργίας σε πραγματικό χρόνο για κάποια προγράμματα, οι οποίες ίσως δεν μπορέσουν να ικανοποιηθούν λόγω των επιβαρύνσεων του ΣΔΒΔ.

¬ Δεν απαιτείται προσπέλαση πολλών χρηστών στα δεδομένα.

Κεφάλαιο 2

Ηλεκτρονικό Εμπόριο

2.1 Τι είναι το Ηλεκτρονικό Εμπόριο

Ο όρος Ηλεκτρονικό Εμπόριο **(e-commerce)** θα μπορούσε απλά να οριστεί ως η κάθε μορφή επιχειρηματικής συναλλαγής και επικοινωνίας που εκτελείται με την χρήση ηλεκτρονικών μέσων. Είναι προφανές πως ο συγκεκριμένος απλοϊκός ορισμός, παρόλο που είναι ακριβής από τεχνικής άποψης εντούτοις, δεν μπορεί να περιγράψει το πνεύμα του ηλεκτρονικού εμπορίου. Ο βασικός στόχος του δεν είναι η χρήση των ηλεκτρονικών μέσων αλλά η τοποθέτηση σε νέα βάση του οικοδομήματος που ονομάζεται εμπόριο. Επομένως ένας πληρέστερος ορισμός θα μπορούσε να είναι ο ακόλουθος:

> ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ ορίζεται το σύνολο των *επιχειρηματικών στρατηγικών* που μπορούν να υποστηρίξουν συγκεκριμένους *τομείς επιχειρηματικής δραστηριότητας* και συγκεκριμένες *επιχειρηματικές πρακτικές* οι οποίες επιτρέπουν, μέσω της χρήσης *νέων τεχνολογιών*, τη διεκπεραίωση εμπορικών διαδικασιών με ηλεκτρονικά μέσα.

Στο σημείο αυτό και πρωτού αναλυθεί ο ορισμός είναι απαραίτητο να τονισθεί ότι ο όρος "Ηλεκτρονικό Εμπόριο" ή **e-commerce** αποτελεί εννοιολογικά μέρος του **e-business** ή "Ηλεκτρονικού επιχειρείν". Το ηλεκτρονικό επιχειρείν περιγράφει επιχειρήσεις η ύπαρξη και στρατηγική των οποίων στηρίζεται στο διαδίκτυο ή/και επιχειρήσεις που έχουν αναθεωρήσει - προσαρμόσει την αποστολή τους, τη στρατηγικής τους και τις λειτουργίες τους με βάση τα δεδομένα του **Internet.**

Ας δούμε πως αναλύεται ο παραπάνω ορισμός:

Ø Επιχειρηματικές Στρατηγικές: Το Ηλεκτρονικό Εμπόριο **(**Η.Ε.**)** με την εφαρμογή του υποστηρίζει τις επιχειρήσεις στην προσπάθειά τους να σχεδιάσουν

και να εφαρμόσουν στρατηγικές οι οποίες θα τους εξασφαλίσουν ανταγωνιστικό πλεονέκτημα. Έτσι το Η.Ε. δεν αναφέρεται απλά στη χρήση τεχνολογίας για αυτοματοποίηση κάποιων επιχειρηματικών διαδικασιών, αλλά στη στρατηγική εκμετάλλευσή της για επίτευξη επιχειρηματικών στόχων.

Ø Τομείς Επιχειρηματικής Δραστηριότητας: Σημαντικά οφέλη προκύπτουν από την εφαρμογή του Η.Ε. στα διάφορα στάδια λειτουργίας μιας επιχείρησης. Τέτοια στάδια είναι η σύναψη εμπορικής σχέσης, η προώθηση προϊόντων, η παραγγελιοδοσία, η τιμολόγηση, οι πληρωμές κ.α.

Ø Επιχειρηματικές Πρακτικές: Στην πράξη το Η.Ε. απαιτεί μια σειρά επενδύσεων από τις επιχειρήσεις. Πέρα από τις προφανείς επενδύσεις (υλικό, λογισμικό, τηλεπικοινωνιακός εξοπλισμός), το Η.Ε. απαιτεί δέσμευση ανθρώπινων πόρων, εκπαίδευση, κατοχή τεχνογνωσίας και άλλα έμμεσα κόστη που αναφέρονται στην ανάπτυξη κατάλληλης "κουλτούρας" στην επιχείρηση, στον ανασχεδιασμό επιχειρηματικών πρακτικών, κ.α.

Ø Νέες Τεχνολογίες: Το Η.Ε. δεν αποτελεί τεχνολογία από μόνο του. Δεν έγινε δηλαδή κάποια μεμονωμένη τεχνολογική επανάσταση που να κατέστησε δυνατό το Η.Ε. Αντίθετα, αποτελεί μια ολοκληρωμένη και εμπεριστατωμένη προσπάθεια συνδυασμού νέων τεχνολογιών με απώτερο σκοπό την εξυπηρέτηση των επιχειρήσεων. Συνεπώς το Η.Ε. συνδυάζει τεχνολογίες δικτύων υπολογιστών και τεχνολογίες λογισμικού με τέτοιο τρόπο που η χρήση τους να είναι εφικτή αλλά και αποδοτική για τις επιχειρήσεις.

Το Η.Ε μπορεί να αποτελέσει σημαντικό όπλο για τις επιχειρήσεις που επιθυμούν (ή είναι υποχρεωμένες από τις συνθήκες της αγοράς) να προβούν σε αλλαγές στον τρόπο λειτουργίας τους προκειμένου να επιβιώσουν και να ανθίσουν στο σύγχρονο ανταγωνισμό. Μπορεί να βοηθήσει μια επιχείρηση να μεταβάλλει ολοκληρωτικά τη δομή της, περνώντας από πολλά επίπεδα ιεραρχίας σε πιο οριζόντιες δομές και συσφίγγοντας τις σχέσεις της με τους πελάτες και τους προμηθευτές της.

Πρέπει να τονισθεί για μια ακόμη φορά ότι το Η.Ε. είναι ταυτισμένο με τη χρήση τεχνολογίας για υποστήριξη επιχειρηματικών αλλαγών. Οι επιχειρήσεις που αντιμετωπίζουν το Η.Ε. απλώς σαν ένα τρόπο αυτοματοποίησης και επιτάχυνσης

του υπάρχοντος τρόπου λειτουργίας τους δεν μπορούν να αποκομίσουν ιδιαίτερα οφέλη από αυτό. Αντίθετα, η πλήρης εκμετάλλευση των δυνατοτήτων και ευκαιριών που προσφέρει η χρήση μεθόδων Η.Ε. στην κοινωνία των Πληροφοριών επέρχεται μόνο όταν η τεχνολογία συνδυάζεται με (και υποστηρίζει) τον ανασχεδιασμό των επιχειρηματικών διαδικασιών προς την κατεύθυνση της επίτευξης συγκεκριμένων επιχειρηματικών στόχων.

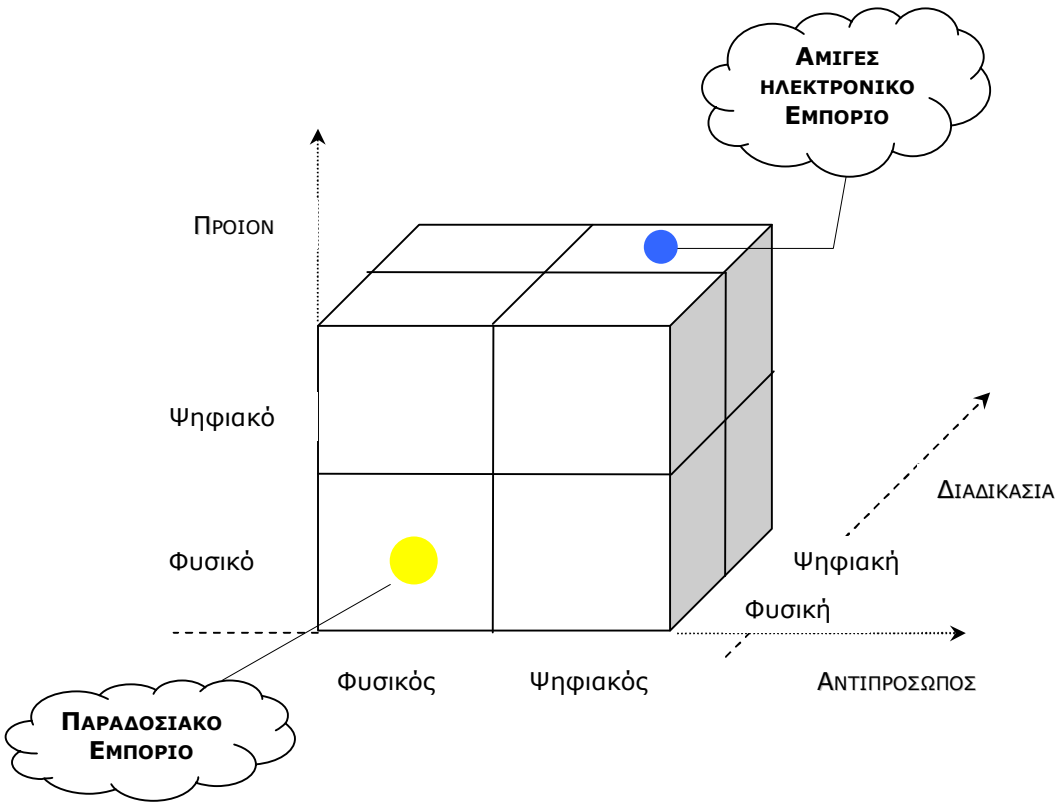
2.2 Μικρό ιστορικό του Ηλεκρονικού Εμπορίου

Οι εφαρμογές του Η.Ε. εμφανίστηκαν στις αρχές της δεκαετίας του **70** με την ηλεκτρονική μεταφορά κεφαλαίων **(Electronic Fund Transfers)**. Ωστόσο αυτές τις εφαρμογές τις χρησιμοποιούσαν μεγάλες εταιρείες, οικονομικά ιδρύματα και λίγες αλλά θαραλέες μικρές επιχειρήσεις. Η εμφάνιση όμως της Ηλεκτρονικής Ανταλλαγής Δεδομένων **(Electronic Data Interchange)** έδωσε τη δυνατότητα στις επιχειρήσεις να ανταλλάσουν με ηλεκτρονικό τρόπο τα εμπορικά τους έγγραφα/παραστατικά. Αυτό είχε ως αποτέλεσμα τη συμμετοχή ολοένα και περισσότερων εταιρειών από διάφορους κλάδους. Το **EDI** ορίζεται ως "η ανταλλαγή δομημένων δεδομένων σε ψηφιακή μορφή μεταξύ των συστημάτων πληροφορικής δύο ή περισσοτέρων εμπορικών εταίρων με την ελάχιστη ανθρώπινη παρέμβαση"

Ακολούθησε η εμφάνιση συστημάτων που περιγράφονται ως τηλεπικοινωνιακές εφαρμογές των οποίων η στρατηγική αξία στην ανάπτυξη του Η.Ε. είναι διεθνώς αναγνωρισμένη. Έτσι στις αρχές του **90** το **internet** εμπορευματοποιείται, ο όρος ηλεκτρονικό εμπόριο κατοχυρώνεται και οι εφαρμογές του εξαπλώνονται με γοργούς ρυθμούς. Σε αυτό συνετέλεσαν αποφασιστικά δύο παράγοντες. Από τη μία η ανάπτυξη της τεχνολογίας και από την άλλη η αύξηση του ανταγωνισμού ανάμεσα στις επιχειρήσεις.

Το Η.Ε. εμφανίζεται σήμερα με διάφορες μορφές ανάλογα με το βαθμό ψηφιοποίησης του προϊόντος ή της υπηρεσίας που πωλείται, της διαδικασίας που ακολουθείται καθώς και του αντιπροσώπου που παραδίδει. Στο ακόλουθο σχήμα παρουσιάζεται ένα μοντέλο που απεικονίζει τις πιθανές μορφές του Η.Ε. με βάση αυτές τις τρεις διαστάσεις (προϊόν, διαδικασία, αντιπρόσωπος), οι οποίες μπορεί να είναι τόσο φυσικές όσο και ψηφιακές. Σχηματικά δημιουργούνται οχτώ κύβοι. Στο παραδοσιακό εμπόριο αντιστοιχεί ο κύβος που οι τρεις διαστάσεις του είναι φυσικές, ενώ στη αμιγής μορφή Η.Ε. ο κύβος που οι τρεις διαστάσεις του είναι ψηφιακές. Οι υπόποιποι κύβοι είναι μια σύνθεση φυσικών και ψηφιακών

διαστάσεων. Η ύπαρξη έστω και μιας ψηφιακής διάστασης δίνει τη δυνατότητα στη συγκεκριμένη μορφή να θεωρείται περίπτωση Η.Ε. Για παράδειγμα, η αγορά βιβλίου από το **Amazon** είναι σαφώς περίπτωση Η.Ε. όχι όμως αμιγής καθώς η πάδοσή του γίνεται από φυσικό αντιπρόσωπο. Η αγορά όμως λογισμικού από την **Egghead**, είναι μία αμιγής περίπτωση Η.Ε. καθώς τα πάντα διεκπεραιώνονται ψηφιακά.



Σχημα 2 : Οι διαστάσεις του Ηλεκτρονικού Εμπορίου

2.3 Συμμετέχοντες στο Ηλεκτρονικό Εμπόριο

Οι συμμετέχοντες σε ένα περιβάλλον Ηλεκτρονικού Εμπορίου μπορεί να είναι επιχειρήσεις, δημόσιοι οργανισμοί και καταναλωτές. Στα πλαίσια αυτά, οι εφαρμογές του Η.Ε. μπορούν να διαχωρισθούν στις ακόλουθες κατηγορίες:

- **Επιχείρηση-προς-επιχείρηση (B2B)**

Ένα παράδειγμα εφαρμογής Η.Ε. μεταξύ επιχειρήσεων είναι η χρήση τηλεπικοινωνιακών δικτύων για να διεκπεραιωθούν ηλεκτρονικά καίριες λειτουργίες, όπως η παραγγελιοδοσία και η τιμολόγηση. Καλύπτει το μεγαλύτερο

μέρος του Η.Ε. σήμερα και γι' αυτό στην παράγραφο **§2.3.1** θα γίνει εκτενέστερη περιγραφή του Β**2**Β.

- **Επιχείρηση-προς-καταναλωτές (B2C)**

Η κατηγορία εφαρμογών επιχείρηση-προς-καταναλωτή παρουσιάζει αυξανόμενη χρήση σε διεθνές επίπεδο, λόγω της ευρείας χρήσης των δυνατοτήτων του **Internet**, το οποίο ενδείκνυται για την αποτελεσματική πρώθηση προϊόντων και υπηρεσιών σε μεγάλο εύρος πιθανών πελατών.

- **Καταναλωτές-προς-καταναλωτές (C2C)**

Η κατηγορία αυτή αφορά τις περιπτώσεις όπου ο καταναλωτής πουλά απευθείας σε καταναλωτή. Στην κατηγορία αυτή ανήκουν και οι δημοπρασίες.

- **Επιχείρηση-προς-Δημόσιους φορείς**

Η κατηγορία εφαρμογών επιχείρηση-προς-Δημόσιους Οργανισμούς καλύπτει κάθε μορφή επικοινωνίας μεταξύ ιδωτικών εταιριών και των αρμόδιων αρχών, τόσο για τη διεκπεραίωση φορολογικών ή άλλων υποχρεώσεων, όσο και για την αυτοματοποίηση της διαδικασίας των Δημοσίων Προμηθειών.

- **Καταναλωτές-προς-Δημόσιους φορείς**

Η κατηγορία εφαρμογών καταναλωτής-προς-Δημόσιους Οργανισμούς δεν έχει ακόμη καμία πρακτική εφαρμογή. Παρ' όλα αυτά, και λόγω της ταχείας ανάπτυξης των προαναφερομένων εφαρμογών, αναμένεται σύντομα η εξάπλωση του Η.Ε. και στη σχέση μεταξύ των κρατικών υπηρεσιών με τους πολίτες.

2.3.1 Τι είναι το B2B

Το Η.Ε. μεταξύ επιχειρήσεων δεν είναι παρά η αυτοματοποίηση ορισμένων συναλλαγών, είτε είναι προμήθειες από μια απλή παραγγελία γραφικής ύλης για μια επιχείρηση εώς διαγωνισμός για την προμήθεια καλωδίων σε μια εταιρεία τηλεπικοινωνιών είτε η σύναψη και η εκτέλεση πολύπλοκων συμβολαίων και συνεργασιών. Βασικός στόχος της μεταφοράς εταιρικών συναλλαγών στο **Internet** είναι η αύξηση της παραγωγικότητας. Επιπλέον, τα δίκτυα Η.Ε. μεταξύ επιχειρήσεων επιτρέπουν σε μικρές και μεγάλες εταιρείες να έχουν πρόσβαση σε πελάτες και προμηθευτές σε όλο τον κόσμο. Στόχος των συστημάτων Β**2**Β είναι να συμβάλλουν στη μείωση του κόστους. Μείωση κόστους που μεταφράζεται σε αύξηση των κερδών.

Η μεταφορά διοικητικών λειτουργιών και η ανάπτυξη του ηλεκτρονικού εμπορίου μεταξύ των επιχειρήσεων ξεκίνησε από τις Ηνωμένες Πολιτείες, αν και

εξαπλώνεται ραγδαία σε ολόκληρο τον κόσμο. Εκτός από τις μεγάλες εταιρείες στους κλαδικούς κόμβους προμηθειών, όπως η **AutoXchange** στην αυτοκινητοβιομηχανία και το **GlobalNetXchange** των **Carrefour** και **Sears Roebuck & Co.** στο λιανεμπόριο, το **2000** έκαναν την εμφάνισή τους διάφορα δίκτυα, όπως το **Covisint**, μέσω του οποίου εκτελούνται παραγγελίες εξαρτημάτων αυτοκινήτου, και το **e2open** από τον κλάδο τεχνολογίας. Το **Covisint**, που άρχισε να λειτουργεί στα τέλη Σεπτεμβρίου, εκτέλεσε μέσα στους δύο πρώτους μήνες περίπου **100** συναλλαγές συνολικής αξίας **350** εκατομμυρίων δολαρίων. Αναμφίβολα σημαντικός παράγοντας στην ανάπτυξη του Η.Ε. μεταξύ επιχειρήσεων είναι οι μεγάλες επιχειρήσεις. Αναγκαστικά, θα ακολουθήσουν και οι άλλες καθώς αυτό είναι το παιχνίδι του ανταγωνισμού.

2.3.2 Ένας κόσμος μία αγορά

Το Η.Ε. μεταξύ επιχειρήσεων είναι ένα από τα πιο ορατά σημάδια της παγκοσμιοποίησης, καθώς καταρρίπτει τους γεωγραφικούς περιορισμούς στην εμβέλεια μιας επιχείρησης. Αναλυτές προβλέπουν ανακατατάξεις στις εξαγωγές από την έκρηξη που αναμένεται ότι θα προκαλέσει η ανάπτυξη του B**2**B στις διασυνοριακές συναλλαγές. Η **Forrester Research** εκτιμά ότι μέχρι το **2004** η αξία των διασυνοριακών συναλλαγών που εκτελούνται μέσω **Internet** θα έχει φτάσει τα τέσσερα τρισεκατομμύρια δολάρια, με την Ευρώπη να προηγείται με εξαγωγές ύψους **692** εκατομμυρίων δολαρίων.

Παράλληλα με τις επενδύσεις σε υποδομές, πολυεθνικές εταιρείες και διεθνείς οργανισμοί προκειμένου να στηρίξουν τις ηλεκτρονικές συναλλαγές, προσπαθούν να διαμορφώσουν ένα νομοθετικό πλαίσιο για την επίλυση εμπορικών διαφορών. Τον Ιανουάριο, ο Αμερικανικός Σύνδεσμος Επίλυσης Διαφορών **(American Arbitration Association, AAA)** παρουσίασε έναν **«**κώδικα συμπεριφοράς**»** που στοχεύει στη φιλική επίλυση εμπορικών διαφορών που αφορούν σε συναλλαγές Η.Ε. μεταξύ επιχειρήσεων. Ήδη, ο κώδικας υιοθετήθηκε από μεγάλες αμερικανικές εταιρείες, όπως η **Microsoft** και η **AT&T**, ενώ αναμένονται νέες συζητήσεις για αυτό το θέμα στο πλαίσιο διαφόρων εμπορικών και διεθνών φορέων.

Εκτός από πρόσβαση σε μια γεωγραφικά διευρυμένη αγορά, οι κόμβοι Η.Ε. μεταξύ επιχειρήσεων έχουν αρχίσει να παρέχουν πρόσθετες υπηρεσίες στις εταιρείες που συμμετέχουν. Καθώς οι εταιρείες αποκτούν μεγαλύτερη εμπειρία στο Η.Ε. μεταξύ επιχειρήσεων, οι **«**ψηφιακές αγορές**»** αναδιαμορφώνονται. Ήδη,

οι κόμβοι Β**2**Β επεκτείνουν τις υπηρεσίες τους πέρα από την απλή παροχή ενός χώρου ανεύρεσης προμηθευτή ή αγοραστή, σε μια πιο ολοκληρωμένη προσέγγιση που περιλαμβάνει τη σύναψη μακρόχρονων συνεργασιών. Σύμβουλοι επιχειρήσεων επισημαίνουν, μάλιστα, ότι μια διαδικτυακή παρουσία δεν θα πρέπει να γίνει αυτοσκοπός για μια επιχείρηση, καθώς πιο σημαντική από την πρόσβαση σε μια ψηφιακή αγορά είναι η πρόσβαση στη σωστή ψηφιακή αγορά. Εν ολίγοις, η συμμετοχή μιας επιχείρησης σε έναν κόμβο Η.Ε. μεταξύ επιχειρήσεων που δεν ταιριάζει στα χαρακτηριστικά και τους στρατηγικούς στόχους της, δεν πρόκειται να επιφέρει θετικά αποτελέσματα και, κατά συνέπεια, είναι χειρότερο από το να μην έχει καθόλου πρόσβαση στην ψηφιακή αγορά.

Αναλυτές εκτιμούν ότι η μεγάλη ανάπτυξη των κόμβων Η.Ε. μεταξύ επιχειρήσεων πρόκειται να επέλθει στον τομέα των υποστηρικτικών λειτουργιών **(back end)** προμηθευτών και αγοραστών που συμμετέχουν στον εκάστοτε κόμβο. Ο τομέας περιλαμβάνει κυρίως την ενσωμάτωση των εφαρμογών παραγγελίας-παράδοσης αγαθών με στόχο τη χρήση της τεχνολογίας για να εξασφαλίσει τη μέγιστη αυτοματοποίηση και παραγωγικότητα. Η ενσωμάτωση προϋποθέτει την ανάπτυξη κατάλληλων εφαρμογών λογισμικού με παράλληλη ανάπτυξη της απαραίτητης πελατειακής βάσης.

Το Η.Ε. δεν θα επιτύχει, αν δεν αναπτύξει τρία σημαντικά και αλληλένδετα χαρακτηριστικά: ασφάλεια, αξιοπιστία, συμβατότητα μεταξύ συστημάτων. Τα αρχικά προβλήματα που σημειώθηκαν στο καταναλωτικό ηλεκτρονικό εμπόριο οδηγούν στο συμπέρασμα ότι τα δύο πρώτα χαρακτηριστικά απαιτούν ακόμα πολύ δουλειά για να διαμορφωθούν. Αλλά το εγχείρημα αυτών που θα πρέπει να λύσουν αυτά τα προβλήματα δεν είναι τίποτα μπροστά στα πολύπλοκα θέματα που πρέπει να αντιμετωπιστούν κατά τη δημιουργία μιας συμβατής ηλεκτρονικής αγοράς. Τίθεται επομένως το κρίσιμο ερώτημα της εποχής ***"Να Β2Β Κανείς Ή..."***

Η ερμηνεία του όρου **«**Νέα Οικονομία**»** έχει εστιαστεί στη μεταφορά του κέντρου του οικονομικού βάρους στο ψηφιακό επιχειρείν. Όμως η ουσιαστική έννοια της Νέας Οικονομίας αναφέρεται στη σταδιακή ανατροπή των όρων της παραγωγής που στηρίζουν την οικονομία, και στη διαμόρφωση μιας οικονομίας που στηρίζεται στην παραγωγή **«**επί παραγγελία**»**. Παράλληλα, το εμπόριο μεταξύ επιχειρήσεων μειώνει την απόσταση μεταξύ του παραγωγού της πρώτης ύλης και του καταναλωτή, καθώς δημιουργεί τις προϋποθέσεις για μια πιο άμεση επικοινωνία μεταξύ προμηθευτή και αγοραστή.

Ένα παράδειγμα είναι ο κόμβος ιχθυοπωλών **GoFish.com** που έχει αναπτυχθεί για την παγκόσμια ψαραγορά. Με την παραδοσιακή μέθοδο, ο ψαράς έπρεπε να επιστρέψει στην ιχθυόσκαλα για να διοχετεύσει την ψαριά του στην αγορά. Τώρα, με σύνδεση δορυφόρου μέσω **Internet**, μπορεί να έχει απευθείας επικοινωνία με την αγορά από τη στιγμή που έχει γεμίσει τα δίχτυα του, και πριν φτάσει στη στεριά, να έχει διαπραγματευτεί και πουλήσει ό,τι έχει πιάσει. Ταυτόχρονα, καθώς ψαράς και αγοραστής έχουν πρόσβαση στην ευρύτερη αγορά, είναι πιο ενημερωμένοι για την προσφορά και τη ζήτηση, και έτσι μπορούν πιο εύκολα να καθορίσουν μια τιμή που αντανακλά τα δεδομένα της αγοράς τη συγκεκριμένη χρονική στιγμή.

Κόμβοι όπως το **GoFish.com** υπάρχουν για όλους τους κλάδους της οικονομικής και της εμπορικής δραστηριότητας. Παράλληλα, λειτουργούν και διακλαδικοί κόμβοι που απευθύνονται σε συγκεκριμένες γεωγραφικές ή εθνικές αγορές.

Αναλυτές πιστεύουν ότι ύστερα από μια έκρηξη στο χώρο, με την ακόλουθη εμφάνιση πολλών κόμβων που είναι οργανωμένοι είτε ανά κλάδο είτε ανά γεωγραφική αγορά, θα υπάρξει ένα στάδιο που θα περιλαμβάνει συμμαχίες, συγχωνεύσεις και εξαγορές. Εκτιμάται μάλιστα ότι από τους **200** και πλέον κόμβους ηλεκτρονικού εμπορίου μεταξύ επιχειρήσεων που λειτουργούν σήμερα, στο τέλος θα επιβιώσουν περίπου **50**, οι οποίοι θα αποτελούν τις νέες, μεγάλες αγορές της παγκόσμιας οικονομίας.

2.4 Προϊόντα που αφορούν το Ηλεκτρονικό Εμπόριο

Υπάρχουν τέσσερις γενικοί τύποι προϊόντων που αφορούν το Ηλεκτρονικό Εμπόριο:

¬ Αγαθά: Πρόκειται για φυσικά αντικείμενα, που έχουν παραχθεί σύμφωνα με κάποιες προδιαγραφές, που συνήθως τις ορίζει ο κατασκευαστής τους. Συνήθως συμπεριλαμβάνεται στην έννοιά τους και η μεταφορά από τον τόπο παραγωγής τους στον τόπο πώλησής τους. Παραδείγματα αυτής της κατηγορίας περιλαμβάνουν: χημικά, φαρμακευτικά προϊόντα, είδη ένδυσης, ανταλλακτικά κάθε είδους, οχήματα κ.λπ.

¬ Εργασίες: Σε αυτή την κατηγορία υπάγονται εργασίες ανάπτυξης ή κατασκευής αγαθών σύμφωνα με προδιαγραφές που θέτει ο πελάτης. Παραδείγματα αποτελούν τα προϊόντα λογισμικού, ηλεκτρικές/υδραυλικές

εγκαταστάσεις, κατασκευές χώρων κ.λπ. Βασικές επιχειρηματικές διαδικασίες που έχουν σχέση με αυτή την κατηγορία αφορούν τη διαπραγμάτευση των προδιαγραφών, τις πληρωμές σύμφωνα με την πρόοδο του έργου κ.λπ.

¬ Υπηρεσίες: Η διάθεση και πώληση υπηρεσιών είναι συνήθως διαδικασίες αλληλοεξαρτώμενες. Παραδείγματα αυτής της κατηγορίας περιλαμβάνουν: δημόσιες, τουριστικές, χρηματοοικονομικές, ψυχαγωγικές, συμβουλευτικές υπηρεσίες και υπηρεσίες υγείας.

¬ Άϋλα αγαθά: Εδώ περιλαμβάνονται προϊόντα των οποίων η αξία δεν συνδέεται άμεσα με το κόστος παραγωγής τους, αλλά με το περιεχόμενο και τη χρήση τους. Επιπλέον, η διανομή τους εξαρτάται άμεσα από κάποιο μέσο επικοινωνίας, ενώ συνδέονται άρρηκτα με την έννοια των δικαιωμάτων χρήσης. Παραδείγματα αυτής της κατηγορίας περιλαμβάνουν τις κινηματογραφικές ταινίες, προϊόντα μουσικής, πακέτα λογισμικού, σχέδια διαφόρων ειδών κ.λπ. Επιχειρηματικές διαδικασίες που σχετίζονται με αυτήν την κατηγορία περιλαμβάνουν την αναπαραγωγή των προϊόντων κατόπιν σχετικής αδείας και όλες τις επικοινωνιακές διεργασίες που πρέπει να συντελεστούν γι' αυτόν τον σκοπό.

Πρέπει να σημειωθεί ότι οι παραπάνω κατηγορίες είναι πολύ γενικού περιεχομένου. Στην πράξη, ένα προϊόν μπορεί να προέλθει από την συνένωση δύο ή περισσότερων από τις παραπάνω γενικές κατηγορίες: για παράδειγμα, ένα βιβλίο είναι ένα προϊόν με στοιχεία άϋλου αγαθού, ενώ αγαθά μπορεί να συνοδεύονται από ένα συμβόλαιο συντήρησης, κάτι που πρακτικά θεωρείται παροχή υπηρεσίας.

2.5 Επιχειρηματικές διαδικασίες του Ηλεκτρονικού Εμπορίου

Οι βασικότερες επιχειρηματικές διαδικασίες που συντελούνται σήμερα στα πλαίσια της εμπορικής διαδικασίας περιλαμβάνουν:

« Προώθηση προϊόντος **(marketing)**: Το **marketing** περιλαμβάνει μια σειρά από δραστηριότητες στην πλευρά του πωλητή προϊόντων και υπηρεσιών **(**π.χ. έρευνα αγοράς, σχεδιασμός προϊόντος, προώθηση και διαφήμιση προϊόντος κ.λπ.**)** όσο και στην πλευρά του πιθανού αγοραστή **(**π.χ. επιλογή κατάλληλου προϊόντος, συλλογή προσφορών, επιλογή βέλτιστης προσφοράς κ.λπ.**)**. Στη διάρκεια των λειτουργιών αυτών, συνήθως υπάρχει ελάχιστη άμεση επαφή μεταξύ του

αγοραστή και του πωλητή αλλά συμμετέχουν σ'αυτές και ενδιάμεσοι φορείς (π.χ. μεταπωλητές, αντιπρόσωποι κ.λπ.)

« Επιβεβαίωση συνεργασίας **(contracting)**: Για τη διεκπεραίωση αυτής της διαδικασίας απαιτούνται: από την πλευρά του αγοραστή η συλλογή των προδιαγραφών του προϊόντος καθώς και άλλων όρων που σχετίζονται με τη συνεργασία με προμηθευτές (π.χ. μεταφοράς, παράδοσης και πληρωμής) και από την πλευρά του πωλητή η διαπραγμάτευση για τους όρους συνεργασίας, η επεξεργασία των παραγγελιών σύμφωνα με τους συμφωνηθέντες όρους συνεργασίας κ.λπ. Στη διάρκεια των λειτουργιών αυτών και ιδιαίτερα κατά τη διάρκεια των διαπραγματεύσεων, διεξάγονται επικοινωνίες μεταξύ των δύο μερών που βασίζονται κυρίως σε αδόμητες πληροφορίες και κείμενα.

« Διαχείριση αποθεμάτων **(logistics)**: Εδώ περιλαμβάνονται όλες οι λειτουργίες που στοχεύουν στη διάθεση των παραγγελθέντων προϊόντων στον αγοραστή σύμφωνα με τους όρους συνεργασίας. Λειτουργίες που περιλαμβάνονται στα πλαίσια αυτά αφορούν την ζήτηση προϊόντων, τη μεταφορά, την υποδοχή και κατηγοριοποίηση των προϊόντων στην αποθήκη κ.λπ. Κατά τη διάρκεια των λειτουργιών αυτών, συνήθως διεξάγονται δομημένες επικοινωνίες μεταξύ των συμμετεχόντων μερών, αγοραστή και πωλητή.

« Διακανομισμός **(settlement)**: Στη διαδικασία αυτή περιλαμβάνεται η αξιολόγηση προϊόντων, υπηρεσιών και η πληρωμή τους. Δεν πρόκειται απλώς για οικονομικό διακανονισμό αλλά για γενικότερο διακανονισμό των όρων συνεργασίας των εμπορικών εταίρων (π.χ. μπορεί να μη συντελείται μια απλή πληρωμή τιμολογίων αλλά και ο αμοιβαίος συμψηφισμός τους).

« Επικοινωνία με δημόσιους φορείς **(interfacing with administration)**: Όλα τα μέρη που συμμετέχουν στα πλαίσια του διεθνούς επιχειρηματικού περιβάλλοντος πρέπει σε κάποια σημεία του εμπορικού κύκλου να έρθουν σε επαφή με δημόσιους φορείς, για διάφορους λόγους (π.χ. διεκπεραίωση εισαγωγών/ εξαγωγών, εξόφληση φόρων κ.λπ.)

2.6 Πεδία εφαρμογής του Ηλεκτρονικού Εμπορίου

Το Η.Ε. μπορεί να εφαρμοστεί σε μια ευρεία γκάμα επιχειρηματικών λειτουργιών που περιλαμβάνουν:

- Ανταλλαγή πληροφοριών για προϊόντα και υπηρεσίες (πριν την πώληση). Η ανταλλαγή πληροφοριών, διαφήμιση και ενημέρωση για προϊόντα και υπηρεσίες είναι ίσως η πλέον διαδεδομένη χρήση του Η.Ε. Για παράδειγμα, πάρα πολλές επιχειρήσεις (ακόμα και στην Ελλάδα) διαθέτουν ηλεκτρονικές σελίδες μέσω των οποίων διαφημίζουν στο **Internet** τα προϊόντα και τις υπηρεσίες που παρέχουν. Οι περισσότερες προσφέρουν παράλληλα και επιπλέον υπηρεσίες στους πελάτες τους και σε κάθε ενδιαφερόμενο, που εμπίπτουν συνήθως σε μια από τις επόμενες κατηγορίες.
- Υποστήριξη πελάτη (πριν και μετά την πώληση). Πολλές επιχειρήσεις δημιουργούν ομάδες συζητήσεων και επαφών με τους πελάτες τους, οι οποίοι με τον τρόπο αυτό μπορούν να επικοινωνούν όχι μόνο με τον προμηθευτή, αλλά και μεταξύ τους, ανταλλάσσοντας ιδέες, ερωτήσεις, συμβουλές, κ.α. Ένα παράδειγμα τέτοιας εφαρμογής είναι το δίκτυο **GEN (Global Engineering Network)** που συντονίζεται από τη **Siemens Nixdorf** και αποτελεί ένα φόρουμ επαφών για μηχανικούς, προμηθευτές και πελάτες μηχανολογικού εξοπλισμού από όλη την Ευρώπη (**http://www.gen.net**).
- Ηλεκτρονική πληρωμή (με την χρήση ηλεκτρονικής μεταφοράς κεφαλαίων, πιστωτικών καρτών ή ηλεκτρονικού χρήματος). Για παράδειγμα, η εταιρεία **Digicash** έχει αναπτύξει ένα σύστημα «ηλεκτρονικών μετρητών» που έχει σχεδιαστεί ειδικά για πληρωμές μέσω του **Internet** και χρησιμοποιεί ειδικούς αλγόριθμους κρυπτογράφησης που εγγυώνται την ανωνυμία και εμπιστευτικότητα των συναλλαγών.
- Ηλεκτρονική διανομή (τόσο σε ότι αφορά τη διαχείριση και παρακολούθηση των φυσικών διανομών, όσο και για την ίδια τη διανομή όπου αυτό είναι εφικτό). Για παράδειγμα, η εταιρεία **Oracle** διαθέτει μια ηλεκτρονική σελίδα στο **Internet** (διεύθυνση **http://www.oracle.com**) μέσω της οποίας οι πελάτες μπορούν να βλέπουν πληροφορίες για τα προϊόντα της εταιρείας, να μεταφέρουν στον υπολογιστή τους δωρεάν δοκιμαστικές εκδόσεις των προγραμμάτων της εταιρείας και αν πληρώσουν μέσω πιστωτικής κάρτας, να μεταφέρουν ολόκληρα

προγράμματα. Λόγω πιθανών νομικών περιορισμών, η τελευταία δυνατότητα είναι διαθέσιμη μόνο σε πελάτες που βρίσκονται στις ΗΠΑ.

- Ένα άλλο παράδειγμα προέρχεται από τον χώρο των εφημερίδων και περιοδικών όπου πολλές εταιρείες παρέχουν τέτοιες υπηρεσίες στους πελάτες τους. Για παράδειγμα, η γνωστή βρετανική εφημερίδα **Times** και **Sunday Times** μπορεί να προσπελαστεί εξ' ολοκλήρου ηλεκτρονικά και δωρεάν από οποιονδήποτε διαθέτει σύνδεση στο **Internet (**στη διεύθυνση **http://www.the-times.co.uk)**.

- Δημιουργία ιδεατών επιχειρήσεων **(virtual enterprises),** δηλαδή ομάδων επιχειρήσεων που συνεργάζονται ηλεκτρονικά δημιουργώντας μια επιχείρηση που προσφέρει προϊόντα και υπηρεσίες που καμία από τις συμμετέχουσες επιχειρήσεις δεν θα μπορούσε να προσφέρει από μόνη της. Έτσι, στο **Internet** μπορεί να βρεθεί η εταιρεία **Virtual Vineyards** που αποτελεί κοινοπραξία μικρών παραγωγών κρασιού στην Καλιφόρνια των ΗΠΑ. Η εταιρεία υπάρχει μόνο στο δίκτυο **(**δεν έχει δηλαδή φυσική υπόσταση**),** στη διεύθυνση **http://www.virtualvin.com**. Οι πελάτες μπορούν να δουν πληροφορίες για τα προϊόντα της εταιρείας και να παραγγείλουν κρασιά πληρώνοντας μέσω πιστωτικής κάρτας ή ηλεκτρονικού χρήματος. Οι παραγγελίες των πελατών μεταφέρονται μέσω δικτύου στον κατάλληλο προμηθευτή και τα προϊόντα αποστέλλονται μέσω ταχυδρομείου. Ο πελάτης έχει τη δυνατότητα να παρακολουθεί κάθε στιγμή ηλεκτρονικά που βρίσκεται η παραγγελία του, ακόμα και όταν αυτή βρίσκεται στο ταχυδρομείο.

- Ανάπτυξη κοινών επιχειρηματικών διαδικασιών **(shared business processes)** μεταξύ επιχειρήσεων. Τέτοιες διαδικασίες φέρνουν σε στενή επαφή τους πελάτες με τους προμηθευτές, συσφίγγοντας τους επιχειρηματικούς δεσμούς και δυσχεραίνοντας με αυτόν τον τρόπο την αλλαγή συνεργατών. Για παράδειγμα, η αλυσίδα **super market Tesco** της Μ. Βρετανίας έχει αναπτύξει ένα πολύπλοκο σύστημα ανατροφοδότησης των **540** καταστημάτων που διαθέτει στην χώρα. Κάθε πώληση προϊόντος που καταγράφεται στα ταμεία κάποιου καταστήματος μεταφέρεται ηλεκτρονικά στα κεντρικά γραφεία της εταιρείας. Εκεί υπολογίζεται ποιά προϊόντα χρειάζεται να επανατροφοδοτήσουν κάθε κατάστημα και αυτή η πληροφορία στέλνεται ηλεκτρονικά στην αντίστοιχη αποθήκη της εταιρείας. Εκεί, αν τα προϊόντα δεν υπάρχουν σε στόκ, παραγγέλνονται **(**πάντα ηλεκτρονικά**)** από τον κατάλληλο προμηθευτή. Μετά την παραλαβή από την αποθήκη, τα προϊόντα στέλνονται στο κατάστημα που τα χρειάζεται. Το όλο σύστημα ανατροφοδότησης λειτουργεί με την στενή συνεργασία των

προμηθευτών, οι οποίοι ουσιαστικά είναι συμμέτοχοι σε μια κοινή επιχειρηματική διαδικασία ανατροφοδότησης των ραφιών στα καταστήματα του **super market.**

Βέβαια, η χρήση Η.Ε. για όλες αυτές τις κατηγορίες συναλλαγών δεν είναι το ίδιο εύκολη. Το κόστος χρήσης ηλεκτρονικής επικοινωνίας δεν είναι το ίδιο για κάθε εφαρμογή και εξαρτάται από μια πληθώρα παραγόντων, όπως η εξοικείωση της επιχείρησης με την πληροφορική, η τυχόν ήδη χρήση δικτύων και ηλεκτρονικών μεθόδων επικοινωνίας, ο αριθμός των συναλλασσόμενων εταίρων, κ.α. Γενικά, μια επιχείρηση που χρησιμοποιεί ήδη την πληροφορική σε ικανοποιητικό βαθμό και συναλλάσσεται με άλλους εταίρους που κάνουν το ίδιο, δεν αντιμετωπίζει συνήθως το κόστος επένδυσης για χρήση του Η.Ε. σαν αναχαιτιστικό παράγοντα. Αντίθετα, μια επιχείρηση που πρέπει να επενδύσει από την αρχή σε όλο τον απαραίτητο εξοπλισμό και τεχνογνωσία και ίσως χρειαστεί να "πριμοδοτήσει" κάποιους μικρούς πελάτες ή/και προμηθευτές της να κάνουν το ίδιο, ίσως χρειάζεται να αντιπαραβάλλει προσεκτικά τα κόστη με τα αναμενόμενα (άμεσα και στρατηγικά) οφέλη.

Επιπρόσθετα, η χρήση μεθόδων Η.Ε. σε κάθε ένα από τα προαναφερόμενα είδη επιχειρηματικών λειτουργιών δεν είναι το ίδιο εύκολη λόγω της τυχόν ύπαρξης νομικών ή άλλων κανονιστικών περιορισμών. Έτσι η χρήση του Η.Ε. για διαφήμιση ή για ανταλλαγή πληροφοριών για προϊόντα είναι ίσως εύκολη. Δεν ισχύει όμως το ίδο και για τις ηλεκτρονικές πληρωμές καθώς, παρόλο που οι τεχνολογίες που επιτρέπουν τη διακίνηση "ηλεκτρονικού χρήματος" είναι ήδη αρκετά ώριμες για ευρεία χρήση, οι νομοθεσίες των περισσότερων κρατών θα χρειαστεί να τροποποιηθούν για να επιτρέψουν τέτοιες συναλλαγές, διαφυλάσσοντας παράλληλα τα συμφέροντα των κρατών και διατηρώντας τη δυνατότητα νομικών και φορολογικών ελέγχων από τις αρχές. Είναι αναπόφευκτο βέβαια ότι με την εξάπλωση της χρήσης του Η.Ε. θα δημιουργηθεί η αναγκαία πίεση προς τις κυβερνήσεις για προσαρμογή των εθνικών και διεθνών νομοθεσιών, κάτι που γίνεται ήδη ορατό στις προηγμένες χώρες.

2.7 Επιδράσεις του Ηλεκτρονικού Εμπορίου

Όσο είναι αλήθεια ότι το Η.Ε. μπορεί να είναι ένα πολύτιμο εργαλείο στα χέρια μιας επιχείρησης, άλλο τόσο επίσης αληθεύει το γεγονός ότι η χρήση του δεν μπορεί να προσδώσει τα ίδια οφέλη σε κάθε είδος και τύπο επιχείρησης. Έτσι είναι απαραίτητο για τις επιχειρήσεις, προτού δεσμεύσουν πόρους σε οποιαδήποτε προσπάθειας, να αξιολογήσουν προσεκτικά τα ακόλουθα:

- Μπορεί η χρήση του Η.Ε. να βοηθήσει την επιχείρηση να πετύχει καλύτερα τους στόχους της;
- Σε ποιούς τομείς της επιχειρηματικής λειτουργίας είναι προσφορότερο να χρησιμοποιηθούν τεχνολογίες και πρακτικές Η.Ε.;
- Ποιός συνδυασμός τεχνολογιών μπορεί να επιφέρει τα καλύτερα αποτελέσματα με το μικρότερο δυνατό κόστος επένδυσης και το ελάχιστο ρίσκο;
- Τι είδους και τι έκτασης οργανωτικές αλλαγές θα απαιτήσει η εφαρμογή του Η.Ε. μέσα σε μια επιχείρησης;
- Πως μπορεί το Η.Ε. να μεταβάλλει τις σχέσεις μιας επιχείρησης με τους επιχειρηματικούς της εταίρους;

Είναι αναμφισβήτητο ότι η εφαρμογή μεθόδων Η.Ε. μπορεί να έχει σημαντικές επιδράσεις στη λειτουργία μιας επιχείρησης σε βασικά επιχειρηματικά μεγέθη:

- Λειτουργικό κόστος **(**κόστος διατήρησης αποθέματος**,** κόστος παραγωγής**,** κόστος διαφήμισης και προώθησης κ.α.**)**
- Παραγωγικότητα**,** αποτελεσματικότητα και κερδοφορία
- Στρατηγική θέση της επιχείρησης στην αγορά
- Διαπραγματευτική ικανότητα της επιχείρησης
- Επίδραση πολιτικών **marketing** και προώθησης προϊόντων

Αυτό που σίγουρα απαιτείται είναι μια επιχείρηση να μπορεί να αξιολογήσει σωστά τις ευκαιρίες και τους κινδύνους που μπορεί να συνεπάγεται η υιοθέτησης του Η.Ε.**,** αλλά και να επιλέξει τη σωστή στρατηγική και το πλάνο εφαρμογής του**.** Κάτι τέτοιο όμως είναι εξαιρετικά δύσκολο για πολλούς λόγους**:**

- Το Η.Ε. είναι μια σχετικά καινούρια έννοια και για το λόγο αυτό δεν υπάρχει ακόμη διαθέσιμη**,** σε ευρεία βάση**,** πρακτική εμπειρία που θα βοηθούσε στην αξιολόγηση και ασφαλή εξαγωγή συμπερασμάτων. Έτσι**,** ο πειραματισμός και η επιχειρηματική διαίσθηση είναι τις περισσότερες φορές οι βασικότεροι μηχανισμοί υιοθέτησης του Η.Ε.**,** ειδικά σε τεχνολογικά "ανώριμα" επιχειρηματικά περιβάλλοντα**,** όπως της Ελλάδας**.**
- Η αξιολόγηση των ευκαιριών**,** των δυνατοτήτων αλλά και των κινδύνων που συνεπάγεται η υιοθέτηση μεθόδων Η.Ε. είναι εξαιρετικά δυσχερής γιατί εξαρτάται από μια πληθώρα παραγόντων όπως το είδος επιχειρηματικής δραστηριότητας της επιχείρησης**,** το μέγεθός της**,** ο βαθμός εξοικείωσης της με τη

χρήση νέων τεχνολογιών και μοντέρνων μεθόδων **management**, η γενικότερη στρατηγική και θέση της στην αγορά, και πολλοί άλλοι.

Πρέπει ακόμη να τονιστεί ότι το Η.Ε. δεν είναι (όπως άλλωστε και η Κοινωνία των Πληροφοριών) απλώς μια πρόβλεψη για μια πιθανή μελλοντική πορεία πραγμάτων. Το Η.Ε. αποτελεί ήδη καθημερινή πραγματικότητα σε όλες τις προηγμένες εμπορικά και τεχνολογικά χώρες. Άλλωστε, τα πρώτα (δειλά) παραδείγματα χρήσης του και στην Ελλάδα είναι ήδη γεγονός. Η ραγδαία ανάπτυξη των τεχνολογιών του **EDI** και του **Internet** μέσα στην τρέχουσα δεκαετία, συνέβαλλε αποφασιστικά προς την κατεύθυνση της μετουσίωσης των προβλέψεων κάποιων επιχειρησιακών αναλυτών της προηγούμενης δεκαετίας σε μια απτή, καθημερινή πραγματικότητα που αναμένεται στο μέλλον να αποτελέσει τον κανόνα διεξαγωγής επιχειρηματικών συναλλαγών.

2.8 Οφέλη του Ηλεκτρονικού Εμπορίου

Η χρήση του Η.Ε. είναι από τη φύση της μια έννοια δι-επιχειρησιακή. Παρόλο που το Η.Ε. μπορεί να εφαρμοστεί και μέσα σε μια επιχείρηση, τα πραγματικά οφέλη εμφανίζονται όταν το Η.Ε. εφαρμόζεται μεταξύ επιχειρήσεων, κυρίως μεταξύ επιχειρήσεων που λειτουργούν με σχέσεις προμηθευτή-πελάτη (με την ευρύτερη δυνατή έννοια του όρου). Για το λόγο αυτό και τα οφέλη που αποκομίζουν οι χρήστες είναι σχεδόν πάντα παράλληλα. Κάθε επιχειρηματική ευκαιρία που παρέχει η χρήση Η.Ε. σε έναν προμηθευτή, μπορεί στις περισσότερες περιπτώσεις να μεταφραστεί και σε ένα αντίστοιχο όφελος για τους πελάτες του. Με την έννοια αυτή, το Η.Ε. είναι μια επαναστατική επιχειρηματική καινοτομία, αφού για να αποδώσει καρπούς δεν στηρίζεται στον ανταγωνισμό (**win-lose** επιχειρηματικές σχέσεις), αλλά στη συνεργασία μεταξύ των εμπλεκομένων για το αμοιβαίο τους κέρδος (**win-win** σχέσεις).

Ο παρακάτω πίνακας παρουσιάζει σε αντιστοιχία μερικά μόνο από τα οφέλη και τις ευκαιρίες που μπορεί να δημιουργήσει το Η.Ε., τόσο για τους προμηθευτές όσο και για τους αγοραστές προϊόντων και υπηρεσιών.

ΠΙΝΑΚΑΣ **1:** Τα οφέλη του Ηλεκτρονικού Εμπορίου είναι παράλληλα

ΕΥΚΑΙΡΙΕΣ ΓΙΑ ΤΟΥΣ ΠΡΟΜΗΘΕΥΤΕΣ	ΟΦΕΛΗ ΓΙΑ ΤΟΥΣ ΑΓΟΡΑΣΤΕΣ
«Παγκόσμια**»** παρουσία	**«**Παγκόσμια**»** επιλογή
Βελτιωμένη ανταγωνιστικότητα	Βελτιωμένη ποιότητα υπηρεσιών
Παροχή εξειδικευμένων υπηρεσιών στους πελάτες	Λήψη εξειδικευμένων υπηρεσιών απ τους προμηθευτές
Σμίκρυνση **(**ή και πλήρης απάλειψη**)** τ προμηθευτικής αλυσίδας	Άμεση κάλυψη αναγκών
Ελαχιστοποίηση κόστους παραγωγής	Ελαχιστοποίηση τιμών
Νέες επιχειρηματικές ευκαιρίες	Νέα προϊόντα και υπηρεσίες

- *Παγκόσμια παρουσία / Παγκόσμια επιλογή*

Το Η.Ε. δίνει **(**για πρώτη φορά στην παγκόσμια ιστορία του εμπορίου**)** σε όλους τη δυνατότητα να δραστηριοποιηθούν στην παγκόσμια αγορά, ανεξάρτητα από μέγεθος και τις οικονομικές τους δυνατότητες. Μέχρι σήμερα κάτι τέτοιο ήταν εφικτό μόνο για τις μεγάλες πολυεθνικές επιχειρήσεις, ενώ οι μικρότερες επιχειρηματικές μονάδες ήταν υποχρεωμένες να κινούνται σε μικρές τοπικές αγορές που προσδιορίζονταν από γεωγραφικούς, εθνικούς, χρηματοοικονομικούς ή άλλους περιορισμούς. Σήμερα **(**και ολοένα και περισσότερο στο μέλλον**)** η αγορά-στόχος μιας επιχείρησης που συναλλάσσεται ηλεκτρονικά με τους εταίρους της περιορίζεται μόνο από την ύπαρξη τηλεπικοινωνιακών δικτύων. Με τη συνεχώς αυξανόμενη κάλυψη όλου του πλανήτη με τέτοια δίκτυα, το Η.Ε. δίνει για πρώτη φορά ακόμα και σε μικρού μεγέθους επιχειρήσεις τη δυνατότητα να επιτύχουν την παρουσία τους στην **«**παγκόσμια**»** αγορά. Από την άλλη μεριά, αυτή ακριβώς η δυνατότητα δίνει απεριόριστες δυνατότητες επιλογών στους πελάτες που δεν είναι πλέον υποχρεωμένοι να επιλέξουν προϊόντα και υπηρεσίες μόνο από τους προμηθευτές εκείνους που μπορούν να έρθουν σε φυσική επαφή.

- *Βελτιωμένη ανταγωνιστικότητα/ ποιότητα υπηρεσιών*

Η ηλεκτρονική επικοινωνία επιτρέπει στους προμηθευτές προϊόντων και υπηρεσιών να γίνουν πιο ανταγωνιστικοί, κυρίως προσφέροντας προς τους πελάτες τους υπηρεσίες που πριν ήταν δαδύνατο ή πολύ δύσκολο να προσφερθούν. Για παράδειγμα, η υποστήριξη του πελάτη πριν καιμετά την αγορά

ήταν πολύ κοστοβόρα για πολλές επιχειρήσεις. Αντίθετα, με τη χρήση μεθόδων ηλεκτρονικής επικοινωνίας, ο προμηθευτής έρχεται «κοντά» στον πελάτη του (χωρίς στις περισσότερες περιπτώσεις να χρειαστεί να μετακινηθεί στην πραγματικότητα), προσφέροντάς του έτσι υπηρεσίες υψηλής ποιότητας με πολύ μικρό επιπλέον κόστος.

- *Παροχή και λήψη εξειδικευμένων υπηρεσιών*

Με τη χρήση του Η.Ε., οι προμηθευτές μπορούν να παρακολουθούν πιο αποτελεσματικά το προφίλ του αγοραστικού κοινού τους. Με τον τρόπο αυτό, μπορούν να σχεδιάζουν και να προσφέρουν προϊόντα που να απευθύνονται στους μεμονωμένους πελάτες τους, αλλά σε τιμές της μαζικής αγοράς. Ένα απλό παράδειγμα μπορεί να είναι ένα ηλεκτρονικό περιοδικό που προσφέρει τα άρθρα του στο **Internet** με τέτοιο τρόπο που να δίνει έμφαση στα συγκεκριμένα ενδιαφέροντα κάθε ενός συνδρομητή, προτείνοντάς του συγκεκριμένες πηγές αναζήτησης πληροφοριών στο δίκτυο.

- *Σμίκρυνση προμηθευτικής αλυσίδας/ Άμεση κάλυψη αναγκών*

Ένα από τα πλέον αναφερόμενα οφέλη του Η.Ε. είναι η συμβολή του στην "εξάλειψη" των μη απαραίτητων μεσαζόντων στις εμπορικές συναλλαγές. Κάτι τέτοιο συνεπάγεται αυτόματα τη σμίκρυνση της προμηθευτικής αλυσίδας με τέτοιο τρόπο που ο προμηθευτής έρχεται σε απευθείας επικοινωνία με τον πελάτη χωρίς την παρεμβολή τρίτων (π.χ. αποστολή προϊόντων χωρίς τη χρήση διαμεταφορέων, ενδιάμεσων αποθηκών, κ.α.). Το αντίστοιχο όφελος για τον πελάτη είναι φυσικά η άμεση κάλυψη των αναγκών του, καθώς μπορεί να παραλάβει το προϊόν/ υπηρεσία που επιθυμεί χωρίς τις χρονικές καθυστερήσεις που αναπόφευκτα εισάγουν στον κύκλο διανομής τα ενδιάμεσα μέρη. Η πλέον ακραία περίπτωση σμίκρυνσης της προμηθευτικής αλυσίδας επέρχεται στην περίπτωση που το ίδιο το προϊόν έχει τέτοια φύση που μπορεί να μεταφερθεί ηλεκτρονικά. Στην περίπτωση αυτή μιλάμε πια για πλήρη εξάλειψη της προμηθευτικής αλυσίδας, καθώς δεν χρειάζεται καμία φυσική επαφή για να πραγματοποιηθεί η εμπορική πράξη. Τέτοια παραδείγματα έχουν αρχίσει να εμφανίζονται σε αγορές όπως η βιομηχανία παραγωγής λογισμικού (υπάρχουν οίκοι λογισμικού που δεν έχουν καν γραφεία, αλλά συναλλάσσονται αποκλειστικά μέσω δικτύου), οι τομείς ψυχαγωγίας και ενημέρωσης (π.χ. βίντεο, μουσική, περιοδικά, εφημερίδες) και η εκδοτική βιομηχανία (οι περισσότερες

εγκυκλοπαίδειες που πωλήθηκαν στις ΗΠΑ το **1995** ήταν σε ηλεκτρονική μορφή παρά σε έντυπη μορφή**).**

- *Ελαχιστοποίηση κόστους παραγωγής / Ελαχιστοποίηση τιμών*

Φυσικά η πρώτη ίσως συνεισφορά που θα μπορούσε να αποδώσει κανείς στο Η.Ε. θα ήταν η μείωση του λειτουργικού κόστους για τους προμηθευτές**,** με τα αντίστοιχα οφέλη και για τους πελάτες **(**μείωση του δικού τους κόστους και δυνατότητα απολαβής καλύτερων τιμών**).** Κάθε φυσική επικοινωνία που ήταν απαραίτητη για μια εμπορική συναλλαγή κοστίζει λιγότερο αν πραγματοποιηθεί ηλεκτρονικά **(**π.χ. ηλεκτρονικό ταχυδρομείο αντί για τηλέφωνο ή συναντήσεις**)** και μπορεί να λάβει χώρα σε μικρότερο συνήθως χρόνο. Με την ωρίμανση της τεχνολογίας των δικτύων υπολογιστών**,** η διαφορά κόστους μεταξύ φυσικής και ηλεκτρονικής επικοινωνίας θα γίνεται ολοένα και πιο εμφανής.

- *Νέες επιχειρηματικές ευκαιρίες / Νέα προϊόντα και υπηρεσίες*

Τέλος**,** καθώς το Η.Ε. ανοίγει μια τελείως νέα εποχή στις εμπορικές συναλλαγές**,** προσφέρει παράλληλα την ευκαιρία δημιουργίας εντελώς νέων προϊόντων και υπηρεσιών και μια σειρά από επιχειρηματικές ευκαιρίες στους πρωτοπόρους. Τέτοιες υπηρεσίες περιλαμβάνουν την παροχή δικτύων και δικτυακών υπηρεσιών **(**π.χ. παροχείς πρόσβασης στο **Internet)**, υπηρεσίες ηλεκτρονικών καταλόγων**,** συμβουλευτικές υπηρεσίες σε επιχειρήσεις για υιοθέτηση του Η.Ε. κ.α.

Κεφάλαιο 3

Ασφάλεια

3.1 Γιατί πρέπει να ανησυχούμε!

Η ασφάλεια, θεωρείται ως ένας από τους πιο σημαντικούς σκοπέλους για το Ηλεκτρονικό Εμπόριο και γενικά για την επικοινωνία μέσω του διαδικτύου. Στην ουσία θα το χαρακτηρίζαμε περισσότερο εμπορικό παρά τεχνολογικό πρόβλημα, αφού η επίλυσή του επηρεάζει κυρίως την ανάπτυξη και εξέλιξη των εμπορικών συναλλαγών. Η τεχνολογία από την πλευρά της προσφέρει σημαντικά όπλα για μία γενική αντιμετώπιση του προβλήματος.

Οι κυριότεροι λόγοι για τους οποίους η ασφάλεια οφείλει να μας προβληματίζει είναι οι ακόλουθοι:

- Οι υπολογιστές είναι συνδεδεμένοι.

Μέχρι την ανάπτυξη του **internet** το πρόβλημα της ασφάλειας περιοριζόταν στο χρήστη του υπολογιστή. Από τη στιγμή που χρήστες των βάσεων δεδομένων ήταν άτομα εξουσιοδοτημένα τότε δεν υπήρχε κανένας κίνδυνος για την ασφάλεια των δεδομένων. Στο **internet** όμως δίνεται η δυνατότητα σε οποιονδήποτε να εισέρχεται σε κάθε υπολογιστή που είναι συνδεδεμένος.

- Το δίκτυο είναι ψηφιακό.

Το να αποκτήσει κάποιος πρόσβαση στο τηλεφωνικό δίκτυο για να παρακολουθεί τις τηλεφωνικές συνδιαλέξεις είναι μεν εφικτό, αλλά δεν εγγυάται ευκολία στην απόκτηση πληροφοριών. Αυτό διότι δεν είναι δυνατή η ταυτόχρονη παρακολούθηση διάφορων τηλεφωνικών αριθμών και επίσης απαιτείται χρόνος μέχρι να "ακούσει" την πληροφορία που αναζητά. Μέσα όμως στο δίκτυο των υπολογιστών έχει τη δυνατότητα να παρακολουθεί ταυτόχρονα ένα μεγάλο πλήθος συνομιλιών και το σημαντικότερο ο υπολογιστής μπορεί να αναζητά με μεγάλη ταχύτητα συγκεκριμένες πληροφορίες, χωρίς ο εισβολέας στην ουσία να κάνει τίποτα.

- Οι υπολογιστές συλλέγουν δεδομένα.

Η ίδια η λειτουργία των υπολογιστών είναι τέτοια που καθιστά εφικτά συγκεκριμένα ήδη επιθέσεων. Τα πληροφοριακά συστήματα είναι έτσι χτισμένα ώστε τα επιθυμητά -και ταυτόχρονα άκρως σημαντικά- δεδομένα να είναι εύκολα προσβάσιμα. Συνεπώς αν κάποιος εισέλθει εντός του συστήματος δεν θα δυσκολευτεί να αναζητήσει και να συλλέξει τα δεδομένα που επιθυμεί.

- Οι υπολογιστές μπορούν να προγραμματιστούν.

Ένας εισβολέας είδαμε πως μπορεί να χρησιμοποιήσει τον υπολογιστή προκειμένου να ψάξει ανάμεσα στα δεδομένα για αυτά που τον ενδιαφέρουν. Ταυτόχρονα μπορεί να τον προγραμματίσει ώστε να αναζητά τρόπους για να αποκτήσει πρόσβαση στο σύστημα. Τέλος υπάρχει η δυνατότητα να κατασκευασθούν προγράμματα εισβολών σε συστήματα από ικανούς εισβολείς που θα μετατρέψουν και τους πιο άπειρους σε επικίνδυνους. Αν για παράδειγμα, υπάρχει, απλή σε λειτουργία, συσκευή που να ξεκλειδώνει κλειδαριές τότε δεν απαιτείται έμπειρος κλειδαράς για την ανοίξει.

- Η εισβολή σε πληροφορικά συστήματα μένει ανεξακρίβωτη.

Ένα ανοχύρωτο πληροφοριακό σύστημα δεν διατηρεί πειστήρια παραβίασής του. Τα εγκλήματα στο φυσικό κόσμο συνοδεύονται πάντα από αποδεικτικά: Αποτυπώματα, αυτόπτες μάρτυρες, καταγραφή εικόνας σε κάμερα ασφαλείας, παραβιασμένες πόρτες κ.τ.λ. Η ύπαρξη συστήματος ασφαλείας μας παρέχει ίχνη του τι συνέβει και από ποιόν.

- Υπάρχουν εμπειρίες επιθέσεων.

Πλείστα καθημερινά παραδείγματα έρχονται να επιβεβαιώσουν με τον πιο τρανταχτό τρόπο την ανάγκη θωράκισης των δεδομένων μας. Ακόμη και βάσεις δεδομένων, ιστοσελίδες και πληροφοριακά συστήματα μεγάλων οργανισμών και κυβερνήσεων έπεσαν θύματα εισβολών.

3.2 Τι προσπαθούμε να προστατέψουμε

Όταν συνδεόμαστε στο διαδίκτυο τότε αυτομάτως θέτουμε σε κίνδυνο:

1. Τα δεδομένα: Τις πληροφορίες που φυλάσσονται στις βάσεις δεδομένων μας και αυτά που ανταλλάσονται μέσω του διαδικτύου.

2. Το πληροφοριακό σύστημα **(hardware-software)**

3. Τη φήμη της επιχείρησης.

Ø **ΤΑ ΔΕΔΟΜΕΝΑ**

Τα δεδομένα έχουν τρία κρίσιμα χαρακτηριστικά που πρέπει να προστατευθούν και να εξασφαλιστούν για να μπορεί το διαδίκτυο να είναι αξιόπιστο μέσο:

- Μυστικότητα **(Privacy)**: Να μην διαβάζονται από τρίτους
- Ακεραιότητα **(Integrity)**: Να μην παραποιούνται
- Διαθεσιμότητα **(Availability)**: Να είναι ανά πάσα στιγμή προσβάσιμα.

Οι περισσότεροι επικεντρώνουν την προσοχή τους στους κινδύνους που αφορούν τη μυστικότητα των δεδομένων. Σε μεγάλο βαθμό το γεγονός αυτό είναι απόλυτα φυσιολογικό, καθώς πολλές εταιρείες διατηρούν στους υπολογιστές τα σημαντικότερα δεδομένα τους, όπως για παράδειγμα: Τα σχέδια των προϊόντων τους, οικονομικά αρχεία, αριθμούς πιστωτικών καρτών, πελατολόγιο, προσφορές. Η λύση στο πρόβλημα της μυστικότητας δείχνει απλή ειδικά για τις επιχειρήσεις που δεν απαιτείται να ανταλλάσσουν δεδομένα τους με άλλες επιχειρήσεις ή πελάτες μέσω **Internet.** Απομονώνουν τα μηχανήματα που περιέχουν τα κρίσιμα δεδομένα από εκείνα που συνδέονται με το διαδίκτυο. Επομένως για αυτούς το πρόβλημα της ασφάλειας των βάσεων δεδομένων λύθηκε; Η απάντηση είναι όχι διότι δεν έχει αποκλειστεί ο κίνδυνος για τη διαθεσιμότητα και ακεραιότητα των δεδομένων. Ακόμη και αν τα δεδομένα μιας εταιρείας δεν είναι μυστικά είναι βέβαιο πως το πλήγμα της παραποίησης ή της καταστροφής τους, θα έχει σημαντικό κόστος τόσο οικονομικό όσο και γοήτρου.

Τα περιστατικά που αφορούν την ασφάλεια των βάσεων δεδομένων διαφέρουν από τα τυπικά εγκλήματα γιατί η ανίχνευσή τους είναι δύσκολη. Σε πολλές περιπτώσεις μια βίαιη είσοδος στο πληροφοριακό σύστημα μπορεί να είναι προτιμότερη από μία εισβολή που δεν αφήνει ίχνη και επομένως δεν γνωρίζουμε τι ακριβώς "διαβάστηκε" ή "πειράχτηκε".

Ø **ΤΟ ΠΛΗΡΟΦΟΡΙΑΚΟ ΣΥΣΤΗΜΑ (hardware-software)**

Ένας εισβολέας εκτός από την κλοπή, παραποίηση ή καταστροφή των δεδομένων έχει τη δυνατότητα να χρησιμοποιήσει το συγκεκριμένο σύστημα και να εμφανιστεί στο διαδίκτυο με τη δική μας ταυτότητα, να χρησιμοποιήσει το λογισμικό μας ή ακόμη και να καταστρέψει ολόκληρο ή μέρος του συστήματος μας. Πέρα απο την πιθανότητα καταστροφής που η σημασία της είναι προφανής,

η ενδεχόμενη χρήση του συστήματός μας -χωρίς ασφαλώς την έγκρισή μας- κρύβει εξίσου σημαντικούς κινδύνους. Από τον κίνδυνο να μην μπορούμε να χρησιμοποιήσουμε εμείς το σύστημα μέχρι τον κίνδυνο να θεωρηθούμε υπεύθυνοι για τις πράξεις του εισβολέα στο **internet,** που γίνονται με τη δική μας ταυτότητα. **(**Για παράδειγμα, μπορεί να μην χρησιμοποιούμε το αυτοκίνητό μας από τα μεσάνυχτα μέχρι τις **6**π.μ., αυτό όμως δεν σημαίνει ότι θα χαιρόμασταν να ξέρουμε πως κρυφά κάποιος το χρησιμοποιεί έστω και εκείνες μόνο τις ώρες**)**.

- **Η ΦΗΜΗ ΤΗΣ ΕΠΙΧΕΙΡΗΣΗΣ**

Η φήμη της εταιρείας και το γόητρο της μπορεί να πληγούν ανεπανόρθωτα αν δεν αξιολογηθεί σωστά ο κίνδυνος από τους επίδωξους εισβολείς και αν δεν ληφθούν τα κατάλληλα μέτρα προστασίας. Η χρήση της ταυτότητας της εταιρείας από κάποιον τρίτο στο διαδίκτυο μπορεί να βλάψει σοβαρά την επιχείρηση και να δυσφημιστεί εξαιτίας των πράξεων του. Ταυτόχρονα το γεγονός ότι κλάπηκαν ή παραποιήθηκαν δεδομένα, χτυπήθηκε η ιστοσελίδα της εταιρείας είναι λόγοι για να μειωθεί σημαντικά το κύρος και η αξιοπιστία της εταιρείας τόσο ως προς τους πελάτες της όσο και απέναντι στις συνεργαζόμενες με αυτή επιχειρήσεις.

3.2.1 Από ποιούς & από τι προσπαθούμε να προστατευθούμε

Βασικό τμήμα του σχεδιασμού ενός συστήματος ασφαλείας αποτελεί να εξακριβώσουμε τι επίπεδο ασφάλειας χρειάζεται και ποιές απειλές θα κληθεί να αντιμετωπίσει. Η επιλογή των μέτρων προστασίας γίνεται λαμβάνοντας υπόψη τι κόστος **(**οικονομικό, απόδοσης ή ενόχλησης λόγω της παρουσίας τους**)** έχουν για την εταιρεία.

Το πρώτο λοιπόν, βήμα είναι να εντοπίσουμε τον εχθρό. Συνήθως οι άνθρωποι επικεντρώνονται στο είδος της επίθεσης ξεχνώντας ότι οι επιθέσεις είναι τα εργαλεία. Για παράδειγμα, ένας αποφασισμένος εισβολέας θα επιμείνει πολύ περισσότερο από ένα τυπικό εισβολέα. Έτσι, παρόλο που θα χρησιμοποιηθούν τα ίδια είδη επίθεσης, η επιμονή μπορεί να είναι αυτή που θα αποβεί καταλυτική για την επιτυχία ή μη της επίθεσης. Για το λόγο αυτό είναι σημαντικό να έχουμε προσδιορίσει:

- Ποιοί είναι οι εχθροί μας.
- Ποιές είναι οι προθέσεις τους
- Ποιά είναι τα μέσα τους

Οι εν δυνάμει εχθροί ενός πληροφοριακού συστήματος κατηγοριοποιούνται στις ακόλουθες ομάδες:

- **Hackers - Crackers**

Είναι οι "αναρχικοί" του κυβερνοχώρου που εισβάλουν στα πληροφοριακά συστήματα είτε για διασκέδαση, είτε για να καταστρέψουν, είτε για επίδειξη. Τους ελκύουν όλοι οι απαγορευμένοι χώροι. Πολλές εταιρείες συνηθίζουν να προσλαμβάνουν άτομα που εισέβαλαν στα συστήματά τους με τη λογική "Καλύτερα να δουλεύουν για μας παρά εναντίον μας". Άλλωστε αυτοί που παραβίασαν ένα σύστημα ασφαλείας ξέρουν καλύτερα από τον καθένα που μειονεκτεί και μπορούν να το βελτιώσουν.

- Κλέφτες

Είναι όλοι αυτοί που εισβάλουν σε ένα σύστημα έχοντας ως στόχο την κλοπή δεδομένων που θα τους αποφέρει οικονομικά οφέλη είτε χρησιμοποιώντας τα, είτε πουλώντας τα.

- Ανταγωνιστές

Ένας ανταγωνιστής συνήθως, δεν εισβάλει για να κλέψει χρήματα, ούτε για να καταστρέψει αλλά για να αποκτήσει πληροφορίες που είναι σημαντικές προκειμένου να κυριαρχήσει στον "επιχειρηματικό πόλεμο".

- Εσωτερικοί εχθροί

Δυσαρεστημένοι, αποξενωμένοι και άπληστοι υπάλληλοι μπορούν να αποτελέσουν ένα ιδιαίτερα σοβαρό εκ των έσω κίνδυνο για τις βάσεις δεδομένων μιας εταιρείας

- Ατυχήματα

Πολλές καταστροφές δεν είναι αποτέλεσμα πρόθεσης ούτε οργανωμένης επίθεσης, αλλά πρόκειτα για ατυχήματα ή λάθη από αφέλεια. Δεν είναι καθόλου ασυνήθιστο γεγονός εταιρείες να καταστρέφουν από μόνες τους τις βάσεις δεδομένων τους, ή να τις απελευθερώνουν στο **internet** κατά λάθος.

Έχοντας γνωρίσει τους πιθανούς εισβολείς ενός συστήματος, εν συνεχεία, περιγράφουμε τους τρόπους που έχουν οι **crackers** για να αποκτούν παράνομη ή έστω παράτυπη πρόσβαση σε υπολογιστικά συστήματα, τα εργαλεία που χρησιμοποιούν για να κερδίζουν τον έλεγχο σε υπολογιστές, καθώς και τις διαθέσιμες τεχνικές στις οποίες καταφεύγουν για να προκαλούν ζημιές ή να «γονατίζουν» ένα σύστημα, ανεξαρτήτως της ισχύος του. Στο ξεχωριστό κείμενο στο τέλος της ενότητας περιέχετε ένα σύντομο γλωσσάρι με τεχνικούς όρους, η

γνώση των οποίων βοηθά στην καλύτερη κατανόηση όσων ακολουθούν. Εξάλλου, αν και επικρατεί η αντίληψη ότι οι **crackers** είναι άνθρωποι με υψηλό επίπεδο τεχνογνωσίας, καθώς και με άπειρα αποθέματα υπομονής και επιμονής, δυστυχώς διαπιστώνουμε ότι οι αρετές αυτές δεν είναι απαραίτητη προϋπόθεση για να μπορέσει κάποιος να μας προκαλέσει πονοκεφάλους ακόμα και ζημιές.

- **ΑΝΑΠΑΝΤΕΧΕΣ ΑΡΝΗΣΕΙΣ, ΑΠΡΟΣΜΕΝΗ ΑΝΙΚΑΝΟΤΗΤΑ**

Μία από τις πλέον διάσημες και αποτελεσματικές μεθόδους που χρησιμοποιούν οι **crackers** για να θέτουν εκτός λειτουργίας δικτυωμένους υπολογιστές είναι οι επιθέσεις **DoS (Denial of Service attacks).** Το όνομα της τεχνικής **(**άρνηση εξυπηρέτησης**)** οφείλεται στο γεγονός ότι ο υπολογιστής-θύμα για ένα χρονικό διάστημα δεν είναι σε θέση να εξυπηρετεί αιτήσεις μηχανημάτων-πελατών **(clients),** εξαιτίας του τεράστιου πλήθους κίβδηλων αιτήσεων **(bogus requests)** που δέχεται από τον επιτιθέμενο. Υπάρχουν διάφορα είδη επιθέσεων **DoS,** πολλά από τα οποία εκμεταλλεύονται εγγενείς αδυναμίες του ζεύγους πρωτοκόλλων **TCP/IP.** Για τα περισσότερα από αυτά είναι ήδη γνωστά τα αντίστοιχα μέτρα προστασίας. Συγκεκριμένα, οι διαχειριστές συστημάτων μπορούν να εγκαθιστούν **patches** σε λειτουργικά συστήματα και προγράμματα-διακομιστές, ώστε να αποτρέπουν επιθέσεις **DoS** ή να ελαχιστοποιούν τις συνέπειές τους. Όπως, όμως, συμβαίνει και με τους ιούς υπολογιστών, κατά καιρούς εφευρίσκονται νέα είδη ή παραλλαγές επιθέσεων **DoS.** Παραθέτουμε εν συντομία τέσσερις από τις διασημότερες παραλλαγές, σε αλφαβητική σειρά.

1. ***Ping of Death***

Αίτηση **PING** ή, αλλιώς, αίτηση **ICMP,** προς τον υπολογιστή-στόχο, με άκυρο μέγεθος πακέτου στην κεφαλή **(header)** του τελευταίου **(**πάνω από **64Kb).** Τέτοια **«**παράτυπα**»** πακέτα μπορούν να **«**κρεμάσουν**»** υπολογιστές που τρέχουν λειτουργικά συστήματα ανίκανα να τα μεταχειριστούν.

2. ***Smurf Attack***

Επιτυγχάνεται αποστέλλοντας αιτήσεις **ICMP** σε μια διεύθυνση εκπομπής **(broadcast address)** στο υπό επίθεση δίκτυο ή σε κάποιο άλλο, ενδιάμεσο. Η διεύθυνση επιστροφής **(return address)** των πακέτων **ICMP** πλαστογραφείται, ώστε να είναι ίδια με αυτήν του υπολογιστή-στόχου. Από τη στιγμή που μια διεύθυνση εκπομπής αντιστοιχεί σε όλα τα μηχανήματα ενός υποδικτύου, λειτουργεί ενισχυτικά, δημιουργώντας από μία μόνο αίτηση **ICMP** δεκάδες ή και

εκατοντάδες απαντήσεις, προκαλώντας με τον τρόπο αυτό πληροφοριακό «μποτιλιάρισμα». Ας σημειωθεί ότι μια διεύθυνση εκπομπής αντιστοιχεί το πολύ σε **255** μηχανήματα (ανήκουν όλα στο ίδιο υποδίκτυο), επομένως κατά τη διάρκεια μιας επίθεσης **Smurf**, από κάθε αίτηση **PING** μπορούν να παραχθούν μέχρι και **255** απαντήσεις. Καταλαβαίνουμε, λοιπόν, τον υπέρογκο αριθμό των άχρηστων πακέτων που δημιουργούνται, όταν ο επιτιθέμενος στέλνει εκατοντάδες ή ακόμη και χιλιάδες πακέτα **ICMP**.

3. ***SYN Flood Attack***

Πριν εγκαθιδρυθεί μια συνεδρία μεταξύ ενός πελάτη και ενός διακομιστή, λαμβάνει χώρα μια ακολουθία τριών βημάτων, γνωστή και ως «ακολουθία χειραψίας» **(handshaking sequence)**. Εάν ο πελάτης αγνοήσει την τελευταία απάντηση **SYN-ACK (SYNchronize ACKnowledge)** του διακομιστή, ο τελευταίος θα επιμένει για ένα προκαθορισμένο χρονικό διάστημα. Ένας **cracker** μπορεί να εκμεταλλευτεί τη συγκεκριμένη συμπεριφορά για να υπερφορτώσει το διακομιστή-θύμα ή ακόμα και για να τον «κρεμάσει». Κατά τη διάρκεια μιας τέτοιας επίθεσης, ο θύτης παραποιεί τη δικτυακή του διεύθυνση **(IP address)**, κρύβοντας με τον τρόπο αυτό τα ίχνη του.

4. ***Teardrop Attack***

Ο επιτιθέμενος εκμεταλλεύεται αδυναμίες στην ανασυγκρότηση των πακέτων **IP**. Όταν ένα τέτοιο πακέτο αποστέλλεται στο **Internet**, ενδέχεται να ταξιδεύει σε επιμέρους, μικρότερα τμήματα. Κάθε τμήμα περιλαμβάνει στην κεφαλή του ένα πεδίο, όπου εκεί περιγράφεται η θέση του στο αρχικό πακέτο **IP**. Ο θύτης χρησιμοποιεί ένα πρόγραμμα, ονόματι **«Teardrop»**, το οποίο τεμαχίζει πακέτα **IP** σε τμήματα με λανθασμένες πληροφορίες στο υπό συζήτηση πεδίο. Όταν ο υπολογιστής-στόχος προσπαθήσει να συναρμολογήσει τα «παραπλανητικά» αυτά τμήματα, θα κολλήσει ή θα επανεκκινήσει, εκτός και αν ο διαχειριστής συστήματος έχει φροντίσει να αναβαθμίσει το λειτουργικό με το κατάλληλο **patch** που διορθώνει το πρόβλημα.

Όταν σε μια επίθεση **DoS** συμμετέχουν περισσότερα του ενός μηχανήματα, έχουμε τις λεγόμενες κατανεμημένες επιθέσεις **DoS (Distributed Denial of Service** ή **DDoS attacks)**. Στις επιθέσεις του είδους είναι δυνατόν να συμμετέχουν και προσωπικοί υπολογιστές ακόμα και το **PC** στο σπίτι μας χωρίς να το γνωρίζουν οι χρήστες τους. Ο επιτιθέμενος **cracker** κατορθώνει με κάποιον τρόπο να βάλει ένα μικρό πρόγραμμα σε καθένα από τα μηχανήματα που θα συμμετάσχουν εν αγνοία

τους στην επίθεση. Τη στιγμή που θα την εξαπολύσει, στέλνει μια ειδοποίηση σε ένα από αυτά (διακομιστής **DDoS**). Τότε, εκείνο ειδοποιεί μια συγκεκριμένη χρονική στιγμή καθέναν από τους υπόλοιπους υπολογιστές (πελάτες **DDoS**) και όλοι μαζί αρχίζουν να βάλλουν κατά του στόχου με πλαστές αιτήσεις. Το αποτέλεσμα είναι εκείνος να «πλημμυρίσει» και να μην μπορεί να ανταποκριθεί σε αιτήσεις νομότυπων πελατών. Ένας καλός τρόπος για να προστατεύουμε τους υπολογιστές μας, ώστε να μη χρησιμοποιούνται εν αγνοία μας, είναι να χρησιμοποιούμε κάποιο προσωπικό πρόγραμμα **firewall**.

Αν και ένα μηχάνημα που έχει πέσει θύμα επίθεσης **DoS** ή **DDoS** μπορεί να επανέλθει σε ομαλή λειτουργία σχετικά εύκολα, υπάρχουν έμμεσες αρνητικές συνέπειες. Αναφερόμαστε σε οικονομικές ζημιές που οφείλονται στο χρόνο που ένας κεντρικός διακομιστής μένει εξουδετερωμένος, καθώς και στον τραυματισμό του κύρους της εταιρείας στην οποία ανήκει ο διακομιστής-θύμα. Είναι γνωστό, εξάλλου, ότι στην ιντερνετική εποχή ο ανταγωνισμός βρίσκεται μερικά «κλικ» μακρύτερα.

ΑΠΡΟΣΚΛΗΤΟΙ ΩΤΑΚΟΥΣΤΕΣ

Από τα παλαιότερα εργαλεία που χρησιμοποιούσαν και συνεχίζουν να χρησιμοποιούν οι διαχειριστές συστημάτων για να αναλύουν τη συμπεριφορά δικτύων και να εντοπίζουν (πιθανά) προβλήματα, είναι τα λεγόμενα **«sniffer»**. Έτσι ονομάζεται ένα πρόγραμμα που είναι ικανό να «υποκλέπτει» δεδομένα που ταξιδεύουν σε ένα δίκτυο. Εάν το δίκτυο είναι βασισμένο στο **TCP/IP**, τότε επειδή το **sniffer** παρακολουθεί πακέτα **IP**, ονομάζεται και **packet sniffer**. Εξάλλου, σε ένα δίκτυο τοπολογίας αστέρα, όπως είναι πολλά τοπικά δίκτυα, τα πακέτα που φεύγουν από έναν κόμβο (μηχάνημα) εκπέμπονται προς όλους τους άλλους κόμβους του δικτύου. Ωστόσο, μόνο ο κόμβος για τον οποίο προορίζονται τα πακέτα θα τα χρησιμοποιήσει· οι άλλοι θα τα αγνοήσουν. Εάν, τώρα, ένα πρόγραμμα **sniffer** είναι εγκατεστημένο σε έναν υπολογιστή με κάρτα δικτύου σε «επιδιδόμενη» κατάσταση **(promiscuous mode)**, τότε το μηχάνημα αυτό θα μπορεί να «βλέπει» όλα τα πακέτα που διακινούνται στο δίκτυο.

Οι διαχειριστές συστημάτων κάνουν χρήση των **sniffer** για να αναλύουν την κυκλοφορία των πακέτων σε ένα δίκτυο και να εντοπίζουν εστίες προβλημάτων. Επίσης, συχνά χρησιμοποιούν περισσότερα του ενός **sniffer**, στρατηγικά εγκατεστημένα σε διάφορους κόμβους του δικτύου, ώστε να εντοπίζουν εισβολές

παρείσακτων. Με άλλα λόγια, τα **sniffer** μπορούν να λειτουργήσουν και ως ένα σύστημα ανίχνευσης εισβολών **(intrusion detection systems).**
Βλέπουμε, λοιπόν, ότι τα προγράμματα αυτά αποτελούν πολύτιμο εργαλείο για τους διαχειριστές συστημάτων. Ωστόσο, όπως ήδη θα έχει γίνει προφανές, τις υπηρεσίες τους μπορούν να εκμεταλλευτούν και οι **crackers,** αυτή τη φορά για όχι και τόσο θεάρεστους σκοπούς. Για παράδειγμα, ο **cracker** μπορεί να χρησιμοποιεί ένα **sniffer** για να υποκλέπτει κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών, διάφορα άλλα προσωπικά στοιχεία χρηστών, για να διαβάζει την ηλεκτρονική τους αλληλογραφία κ.λπ..

Ο προφανής τρόπος για να προστατευτεί ένα δίκτυο από την επιβλαβή χρήση των **sniffer** είναι να υπάρχει αυστηρή επίβλεψη στα προγράμματα που εγκαθιστούν οι χρήστες στους υπολογιστές. Εάν ένας **cracker** δεν μπορεί να αποκτήσει φυσική πρόσβαση σε κάποιον υπολογιστή, τότε είναι απλώς ανίκανος να εγκαταστήσει ένα **sniffer.** Αλλος ένας τρόπος για την παρόπλιση των **sniffer** είναι η αποστολή δεδομένων σε κρυπτογραφημένη μορφή. Το **sniffer** θα εξακολουθεί να συλλαμβάνει τα πακέτα, μόνο που τώρα δεν θα μπορεί να εξαγάγει κάποιο νόημα από τα περιεχόμενά τους. Βεβαίως, στην περίπτωση αυτή υπάρχει πάντοτε ο κίνδυνος της αποκρυπτογράφησης. Για το λόγο αυτό, προτείνεται η χρήση ισχυρής κρυπτογραφίας, με το ανάλογο κόστος σε υπολογιστική ισχύ. Το ζητούμενο, λοιπόν, είναι η χρυσή τομή ανάμεσα στη δύναμη των μεθόδων κρυπτογράφησης από τη μία, και στην ευκολία των χρηστών, από την άλλη. Τέλος, υπάρχει μια ολόκληρη κατηγορία προγραμμάτων που μπορούν να εντοπίζουν ποιοι υπολογιστές σε ένα δίκτυο έχουν κάρτα δικτύου σε επιδιδόμενη κατάσταση. Έτσι, ο διαχειριστής συστήματος μπορεί να ελέγξει εάν κάποιος υπολογιστής τρέχει ένα **sniffer,** αν έχει δοθεί επίσημη άδεια για την εγκατάστασή του κ.λπ..

ΑΔΙΑΚΡΙΤΟΙ ΔΙΑΒΑΤΕΣ

Μια άλλη τεχνική που χρησιμοποιούν διαχειριστές και **crackers,** καθένας για διαφορετικούς σκοπούς, είναι η σάρωση θυρών **(port scanning).** Πρόκειται για μια διαδικασία αποστολής ερωτημάτων σε διακομιστές, με σκοπό να ληφθούν πληροφορίες για τις υπηρεσίες που προσφέρουν, καθώς και για το χρησιμοποιούμενο επίπεδο ασφαλείας. Από τη στιγμή που ο επίδοξος εισβολέας μάθει ποιες υπηρεσίες προσφέρει το μηχάνημα-στόχος, μπορεί στη συνέχεια να σχεδιάσει την επίθεσή του βασιζόμενος σε γνωστές αδυναμίες των περί ου ο λόγος

υπηρεσιών. Επειδή μια διαδικασία **port scanning** αφήνει τα ίχνη της στα αρχεία καταγραφής **(log files)** του λειτουργικού συστήματος, ορισμένοι **crackers** χρησιμοποιούν ορισμένες «ύπουλες» παραλλαγές. Μία από αυτές είναι η λεγόμενη «ημι-ανοιχτή σάρωση **SYN» (half-open SYN scan).** Κατά τη διάρκεια μιας τέτοιας σάρωσης, το πρόγραμμα συνδέεται στα **port**, αλλά τερματίζει καθεμία ακολουθία σύνδεσης, πριν αυτή ολοκληρωθεί. Από τη στιγμή, λοιπόν, που οι ακολουθίες σύνδεσης δεν ολοκληρώνονται, το λειτουργικό σύστημα στο μηχάνημα-στόχος συνήθως δεν τις καταγράφει, θεωρώντας ότι δεν συνέβησαν ποτέ. Ωστόσο, το πρόγραμμα που κάνει τη σάρωση μπορεί να καταλάβει εάν κάποιο **port** είναι «ανοιχτό», κρίνοντας από την απάντηση του λειτουργικού συστήματος. Υπάρχουν διάφορα εργαλεία για το μπλοκάρισμα των **port scan.** Αυτό που προτείνεται στους απλούς χρήστες είναι η χρήση κάποιου προσωπικού προγράμματος **firewall.**

SOCIAL ENGINEERING

Ακούγεται ειρωνικό αλλά αποτελεί μια πραγματικότητα, το γεγονός ότι μία από τις πιο ύπουλες μεθόδους επίθεσης σε ένα σύστημα ασφαλείας δεν βασίζεται στην τεχνολογία αλλά στην ψυχολογία! Ως **"social engineering"** ορίζεται η "τέχνη" του να αποκτάς πρόσβαση σε ένα σύστημα, εξαπατώντας τους χρήστες και τους διαχειριστές του και αποσπώντας τους όλες εκείνες τις πληροφορίες που χρειάζονται.

Σε ένα πείραμα που έγινε, μια ομάδα από **hackers** ξεκίνησαν την προσπάθειά τους να διεισδύσουν σε ένα πληροφοριακό σύστημα μεγάλης εταιρείας. Μοναδικό τους όπλο είχαν τον τηλεφωνικό κατάλογο της εταιρείας. Τηλεφώνησαν στην εταιρεία, ζήτησαν να μιλήσουν με το γραμματεία του δικτύου και κατόρθωσαν μέσα σε εικοσιτέσσερις ώρες η ίδια η εταιρεία να τους δημιουργήσει λογαριασμό, να τους δώσει **ID** και κωδικό μέσω τηλεφώνου και μάλιστα να τους στείλει με **courier** μέσα στη νύχτα το απαιτούμενο, για την είσοδό τους στο δίκτυο, **software.**

ΙΟΙ

Αναμφίβολα το **Internet** έδωσε μεγάλη ώθηση στην εξάπλωση των πάσης φύσεως ιών και... μικροβίων. Στις μέρες της **Amiga** και των **PC XT** ο μόνος τρόπος για να «κολλήσει» κάποιος ένα ειδεχθές πρόγραμμα ήταν να χρησιμοποιήσει μολυσμένες δισκέτες, κυρίως με παιχνίδια. Τότε η μόλυνση με έναν ιό ήταν κάτι το συνηθισμένο μέχρι και γοητευτικό (το γνωστό μπαλάκι που έκανε βόλτες στην

οθόνη). Βέβαια, το αστείο τελείωνε με την οδυνηρή ανακάλυψη ότι οι δισκέτες ή ο σκληρός δίσκος ήταν άχρηστα. Η κατάσταση άλλαξε δραματικά με την είσοδο του **Internet** στη ζωή μας, και συγκεκριμένα με το **e-mail**. Το ηλεκτρονικό ταχυδρομείο εκμηδένισε τις αποστάσεις και έκανε την επικοινωνία ανάμεσα στους εταιρικούς και τους οικιακούς χρήστες πολύ εύκολη και ευχάριστη υπόθεση. Το **e-mail** όμως είναι προς το παρόν το κυριότερο μέσο για τη μετάδοση κάθε είδους ιών και σκουληκιών, μετατρέποντάς τα σε πραγματική επιδημία λόγω της μεγάλης ταχύτητας με την οποία εξαπλώνονται. Στη συντριπτική τους πλειονότητα οι ιοί, τα σκουλήκια και οι δούρειοι ίπποι δεν μπορούν να προκαλέσουν καμία ζημιά, εάν δεν τρέξετε τα εκτελέσιμα αρχεία**/script** που τα μεταφέρουν. Η κακόβουλη αυτή εφαρμογή μπορεί να έχει καλυφθεί κάτω από το μανδύα μιας εικόνας ή ενός κειμένου **word**, παραπλανώντας σας ή κάνοντας πολύ δύσκολο τον εντοπισμό της από το χρήστη. Ας πάρουμε όμως τα πράγματα από την αρχή.

Όταν αναφερόμαστε σε ιούς, εννοούμε προγράμματα τα οποία έχουν δημιουργηθεί για να εισέλθουν στον υπολογιστή χωρίς την έγκρισή μας και να μολύνουν άλλα αρχεία. Είναι μικρά κομμάτια ηλεκτρονικού κώδικα, που έχουν τη δυνατότητα να αντιγράφουν και να εισάγουν τον εαυτό τους σε ένα εκτελέσιμο πρόγραμμα, αρχείο, δισκέτα ή μέρος σκληρού δίσκου. Ανάλογα με τη φύση του ιού, οι συνέπειες από τη μόλυνση μπορεί να είναι μηδαμινές έως και καταστροφικές. Ο ιός θα προσπαθήσει να αναπαραχθεί και να εξαπλωθεί, μολύνοντας όσο το δυνατόν περισσότερα αρχεία ή άλλους υπολογιστές σε τοπικό επίπεδο ή στο **Internet**. Υπάρχουν αρκετά ήδη ιών: α) αυτοί που προσβάλλουν τον τομέα εκκίνησης μιας δισκέτας ή ενός σκληρού δίσκου **(boot sector viruses)** και είναι σχετικά σπάνιοι σήμερα, β) αυτοί που περιέχονται σε εκτελέσιμα αρχεία **(Program/File viruses)**, γ) αυτοί που εκμεταλλεύονται τις γλώσσες μακροεντολών, όπως, π.χ., του **Word** και του **Excel (Macro viruses)**, και δ) οι πολυμορφικοί, οι οποίοι μπορεί να ανήκουν σε μερικές ή όλες τις προαναφερθείσες κατηγορίες. Υπάρχει και μία ειδική κατηγορία ιών, η οποία εκμεταλλεύεται αδυναμίες γνωστών εφαρμογών, όπως, για παράδειγμα, το **Outlook Express**, με αποτέλεσμα ένα απλό **e-mail** κειμένου να μπορεί να κάνει τη ζημιά. Βέβαια, οι ιοί αυτοί είναι σπάνιοι και παροπλίζονται με την εγκατάσταση νεότερων εκδόσεων των προβληματικών εφαρμογών. Σε αυτό το σημείο οι ειδικοί μας προτρέπουν να αναβαθμίζουμε στη νεότερη έκδοση όλες τις εφαρμογές μας, ειδικά αυτές που σχετίζονται με το **Internet**. Με αυτό τον τρόπο μειώνονται αρκετά οι πιθανότητες μόλυνσης.

ΔΟΥΡΕΙΟΙ ΙΠΠΟΙ

Δεν θα ήταν υπερβολή, εάν λέγαμε ότι ο μεγαλύτερος κίνδυνος μετά τους ιούς, για την πλειονότητα των χρηστών **Internet**, προέρχεται από τους δούρειους ίππους **(Trojan horses)**. Πρόκειται για προγράμματα που αποτελούνται από δύο μέρη, τον πελάτη και το διακομιστή. Ο διακομιστής «φωλιάζει» με κάποιον τρόπο στον υπολογιστή του θύματος και ο πελάτης τρέχει στο μηχάνημα του θύτη. Από τη στιγμή που ο χρήστης του υπό επίθεση υπολογιστή συνδεθεί με το **Internet**, το **Trojan**-διακομιστής, που τρέχει σιωπηρά στο υπόβαθρο **(background)**, στέλνει ένα σήμα το οποίο λαμβάνει το **Trojan**-πελάτης (στο μηχάνημα του θύτη). Στη συνέχεια εγκαθιδρύεται μεταξύ τους μια συνεδρία και ο κράκερ αποκτά πρόσβαση στον υπολογιστή-στόχο. Τώρα, ο μακρόθεν έλεγχος του επιτιθέμενου στο άλλο μηχάνημα ποικίλλει, αναλόγως του **Trojan**. Ο πρώτος μπορεί απλώς να παίζει με τα νεύρα του ανυποψίαστου χρήστη, π.χ., ανοιγοκλείνοντας το πορτάκι του οδηγού **CD-ROM** ή εμφανίζοντας γαργαλιστικά μηνύματα στην οθόνη του. Μπορεί όμως και να του διαγράψει αρχεία ή ακόμα και να του προκαλέσει ζημιές στο υλικό του υπολογιστή, όπως, π.χ., να του διαγράψει το **BIOS** ή να «χτυπήσει» τις κεφαλές του σκληρού δίσκου.

Μια άλλη, ύπουλη λειτουργία των δούρειων ίππων είναι η παρακολούθηση και η καταγραφή των πλήκτρων που πιέζει το θύμα. Το **Trojan**-διακομιστής παρακολουθεί συνεχώς τις κινήσεις του χρήστη. Έτσι, όταν εκείνος πληκτρολογεί κωδικούς πρόσβασης ή αριθμούς πιστωτικών καρτών, το πρόγραμμα τα καταγράφει για να τα στείλει αργότερα στο θύτη.

Πώς όμως μπορεί να «μπει» ένα **Trojan** σε έναν υπολογιστή; Ο συνηθέστερος τρόπος είναι να έρχεται ως επισυναπτόμενο σε κάποιο **e-mail** ή να βρίσκεται κρυμμένο μέσα σε κάποιο άλλο πρόγραμμα, π.χ., σε ένα παιχνίδι **freeware** ή **shareware**, σε κάποιο χρήσιμο, διάσημο εργαλείο κ.λπ. Υπάρχουν δύο τρόποι για να αποφεύγουμε τα **Trojan**. Ο πρώτος είναι να χρησιμοποιούμε ένα πρόγραμμα **«Antivirus»** ή **«AntiTrojan»**. Πολλά προγράμματα του είδους μπορούν να τα ανιχνεύουν όταν τα κατεβάζουμε ακόμα και στην περίπτωση που είναι ήδη εγκατεστημένα στο **PC** μας και να τα διαγράφουν. Ο άλλος τρόπος είναι να χρησιμοποιούμε ένα προσωπικό **firewall**. Κάθε φορά που ένα **Trojan**-διακομιστής θα προσπαθεί να «βγει» στο **Internet**, το **firewall** θα μας ειδοποιεί αναλόγως. Είναι προφανές ότι ο συνδυασμός των δύο προηγούμενων μεθόδων παρέχει τη μέγιστη προστασία. Τέλος, καλό είναι να κατεβάζουμε στον υπολογιστή μας μόνο «έμπιστα» προγράμματα, από γνωστούς, επίσημους δικτυακούς τόπους.

- **ΜΑΚΡΟΙΟΙ**

Οι μακροιοί γράφονται σε γλώσσα μακροεντολών ενός επεξεργαστή κειμένου, λογιστικού φύλλου ή άλλων εφαρμογών και εισέρχονται σε οποιοδήποτε τύπο εγγράφου παράγουν οι εφαρμογές. Αυτό τα μολύνει απέναντι σε οποιοδήποτε λειτουργικό σύστημα κι αν εκτελείται η εφαρμογή

- **ΚΟΥΝΕΛΙΑ**

Αυτά είναι προγράμματα, που όταν ξεκινήσουν, κάνουν πολλά αντίγραφα του εαυτού τους. Μπορούν να αντιγράψουν τον εαυτό τους στη μνήμη γεμίζοντας τη **Ram** και πιθανώς να καταρεύσουν τον υπολογιστή. Σε αντίθεση με τους ιούς, τα κουνέλια δεν προσκολλούν τους εαυτούς τους σε υπάρχοντα αρχεία. Παρόλα αυτά, μπορεί να επιχειρήσουν να συγκαλύψουν τους εαυτούς τους υιοθετώντας ένα αθώο όνομα ή ενεργοποιώντας μια ιδιότητα της λίστας κρυφών αρχείων.

- **ΣΚΟΥΛΗΚΙΑ**

Είναι παρόμοια με τα κουνέλια, αλλά είναι ικανά να μεταδοθούν από ένα μηχάνημα στο άλλο επί του δικτύου εκμεταλλευόμενα λογικά κενά σε πρωτόκολλα του διαδικτύου.

Τα σκουλήκια **(worms)** κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται. Συνήθως δεν μολύνουν αρχεία από τον υπολογιστή που περνούν. Πολύ γνωστές περιπτώσεις, όπως αυτές των **Melissa** και **Love Letter**, εξαπλώθηκαν στο δίκτυο με αστραπιαίο ρυθμό. Μάλιστα, το **Melissa worm** έχει αρχίσει ένα νέο γύρ**ο** καλυμμένο αυτήν τη φορά ως έγγραφο του **Office** για **Mac.** Η μέθοδος επίθεσης είναι εξαιρετικά ύπουλη, αφού μόλις καταφέρουν να διεισδύσουν σε έναν υπολογιστή, στέλνουν μολυσμένα και καμουφλαρισμένα **e-mail** σε όλη τη λίστα επαφών του **Outlook.** Έτσι, ο ανυποψίαστος χρήστης λαμβάνει ένα **e-mail** από κάποιον γνωστό του και δείχνοντας εμπιστοσύνη ανοίγει το επισυναπτόμενο αρχείο και μαζί τον ασκό του Αιόλου. Η μαζική αποστολή **e-mail,** εκτός από την κατασπατάληση του ήδη μικρού εύρους ζώνης του **modem** σε ατομικό επίπεδο, επιβαρύνει δραματικά τους κεντρικούς διακομιστές αλληλογραφίας του **Internet,** με αποτέλεσμα να βγαίνουν συχνά εκτός λειτουργίας.

Δυστυχώς, όσα μέτρα προστασίας και αν παίρνουμε, πάντοτε τα προγράμματα που χρησιμοποιούμε θα είναι ατελή, υπό την έννοια ότι θα παρουσιάζουν αδυναμίες τις οποίες ενίοτε θα εκμεταλλεύονται οι αποφασισμένοι κράκερ. Πρόκειται για τα λεγόμενα **«exploits»**, προγραμματιστικές αδυναμίες σε γνωστές και ευρέως χρησιμοποιούμενες εφαρμογές, τα οποία μπορούν να αξιοποιούν καταλλήλως οι **crackers** για να αποκτούν μη εξουσιοδοτημένη πρόσβαση ή έλεγχο σε συστήματα, να προκαλούν ζημιές σε υπολογιστές-στόχους κ.ο.κ. Συχνά, πάντως, οι εταιρείες κυκλοφορούν αναβαθμίσεις ή διορθώσεις **(bug fixes, patches)** προγραμμάτων με γνωστά προβλήματα.

Γλωσσάρι Όρων

- ***Broadcasting***

Μέθοδος αποστολής του ίδιου μηνύματος σε όλους τους υπολογιστές ενός υποδικτύου, ταυτόχρονα. Παρόμοια έννοια είναι το **multicasting**, μόνο που τώρα οι παραλήπτες του μηνύματος είναι προεπιλεγμένοι όχι κατ' ανάγκη όλοι οι υπολογιστές.

- ***Firewall***

Ο διαχωρισμός δύο δικτύων είναι ένας από τους ρόλους του **Firewall**
Μέθοδος που υλοποιείται σε επίπεδο υλικού ή/και λογισμικού και χρησιμοποιείται για να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση από και προς ένα δίκτυο. Συχνά τα **firewall** χρησιμοποιούνται για να εμποδίζουν χρήστες του Διαδικτύου να προσπελάζουν ιδιωτικά δίκτυα, τα οποία είναι και αυτά συνδεδεμένα με το **Internet**. Γενικά, μπορούμε να πούμε ότι ένα **firewall** διαχωρίζει ένα δίκτυο από κάποιο άλλο

- ***Hub***

Κοινό σημείο σύνδεσης για ένα πλήθος υπολογιστών σε ένα τοπικό δίκτυο **(**τοπολογία αστέρα**)**. Ένα **hub** έχει πολλές θύρες **(ports)**. Όταν ένα πακέτο φτάνει σε μία θύρα, αντιγράφεται σε όλες τις άλλες, με αποτέλεσμα όλοι οι υπολογιστές που είναι συνδεδεμένοι με το **hub** να **«**βλέπουν**»** όλα τα διακινούμενα πακέτα. Σε αντιδιαστολή βρίσκονται τα **LAN Switches** ή, αλλιώς, **frame switches**: κάθε φορά που ένα πακέτο φτάνει σε μία θύρα, διαβάζεται η διεύθυνση προορισμού στην κεφαλή του και το πακέτο προωθείται μόνο στη θύρα στην οποία αντιστοιχεί ο υπολογιστής με τη συγκεκριμένη διεύθυνση.

- ***ICMP (Internet Control Message Protocol)***

Επέκταση του πρωτοκόλλου **IP** για την αποστολή μηνυμάτων λαθών και ελέγχου. Χρησιμοποιείται από την εντολή **Ping** για να διαπιστώνεται εάν ένα μηχάνημα είναι **on-line**, από δρομολογητές **(routers)**, κάθε φορά που ειδοποιούν ένα μηχάνημα για τη μη διαθεσιμότητα ενός κόμβου στον οποίο απευθύνονται κ.λπ.

- ***IP Spoofing***

Τεχνική για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε δικτυωμένα μηχανήματα. Ο εισβολέας αποστέλλει μηνύματα με διευθύνσεις **IP** που υποδεικνύουν ότι αυτά προέρχονται από ένα **«**έμπιστο**»** **port**. Ο επίδοξος **cracker** αρχικά καταφεύγει σε ένα πλήθος τεχνικών για να βρει μια διεύθυνση **IP** που αντιστοιχεί σε ένα τέτοιο **port**. Στη συνέχεια, τροποποιεί τα περιεχόμενα της κεφαλής των πακέτων που θα αποστείλει, ώστε να φαίνεται ότι προέρχονται από ένα έμπιστο **port**. Η κατάλληλη ρύθμιση δρομολογητών και **firewall** μπορεί να αποτρέψει τις επιθέσεις του είδους.

- ***PING (Packet InterNet Groper)***

Εργαλείο για να διαπιστώνεται εάν μια δεδομένη διεύθυνση **IP** είναι προσβάσιμη. Το πρόγραμμα στέλνει ένα πακέτο σε μια διεύθυνση και στη συνέχεια αναμένει μια απάντηση από τον υπολογιστή στον οποίο αντιστοιχεί.

- ***Port Number (αριθμός θύρας)***

Αριθμός που αντιστοιχεί σε μια εφαρμογή στο ρόλο διακομιστή, σε ένα δίκτυο βασισμένο στο **TCP/IP (**όπως, π.χ., το **Internet)**. Το **port** μπορεί να θεωρηθεί ως το άκρο μιας λογικής σύνδεσης **(**δηλαδή μιας σύνδεσης όπως τη βλέπει ο χρήστης**)**. Ένα **port number** χρησιμοποιείται ώστε εισερχόμενα δεδομένα να αντιστοιχίζονται στην κατάλληλη υπηρεσία **(service)**. Γνωστά παραδείγματα αποτελούν τα **port 80, 25** και **20,** που χρησιμοποιούνται από διακομιστές ιστοσελίδων, αλληλογραφίας και **FTP,** αντίστοιχα **(**βλ. και www.isi.edu/in-notes/iana/assignments/port-numbers**)**. Ο συνδυασμός μιας διεύθυνσης **IP** ενός μηχανήματος με έναν αριθμό **port** ονομάζεται **Socket.**

- ***Promiscuous Mode (Επιδιδόμενη Κατάσταση)***

Δικτυωμένος υπολογιστής ρυθμισμένος ώστε να αναγνωρίζει και να δέχεται όλα τα πακέτα που φτάνουν ή περνούν από αυτόν, ανεξαρτήτως πρωτοκόλλου ή προορισμού. Κάθε εργαλείο λογισμικού που χρησιμοποιείται για το φιλτράρισμα δικτυακών πακέτων πρέπει να είναι εγκατεστημένο σε έναν υπολογιστή με κάρτα δικτύου και οδηγούς που του επιτρέπουν να βρίσκεται σε κατάσταση **promiscuous**.

- ***Subnet (υποδίκτυο)***

Υποσύνολο ενός δικτύου που περιλαμβάνει υπολογιστές οι οποίοι έχουν διευθύνσεις με ένα κοινό τμήμα. Στα δίκτυα **TCP/IP**, οι υπολογιστές ενός υποδικτύου έχουν διευθύνσεις **IP** με κοινό πρόθεμα, π.χ., **129.129.129**. Η υποδιαίρεση ενός δικτύου σε υποδίκτυα είναι χρήσιμη τόσο για λόγους ευκολίας διαχείρισης όσο και για λόγους ασφαλείας.

3.3 Τι είναι η ασφάλεια του Ιστού

Η ασφάλεια του ιστού είναι διαφορετικά πράγματα για διαφορετικούς ανθρώπους. Για μερικούς είναι η ικανότητα να φυλλομετρούν στον ιστό με ησυχία, γνωρίζοντας ότι κανένας δεν τους παρακολουθεί. Για άλλους είναι η ικανότητα να πραγματοποιούν οικονομικές και διαφημιστικές συναλλαγές με ασφάλεια. Για τους χειριστές χώρων του ιστού, η σιγουριά ότι οι χώροι τους δεν θα βανδαλισθούν ή ότι δεν θα χρησιμοποιηθούν ως πύλες πρόσβασης στο τοπικό τους δίκτυο.

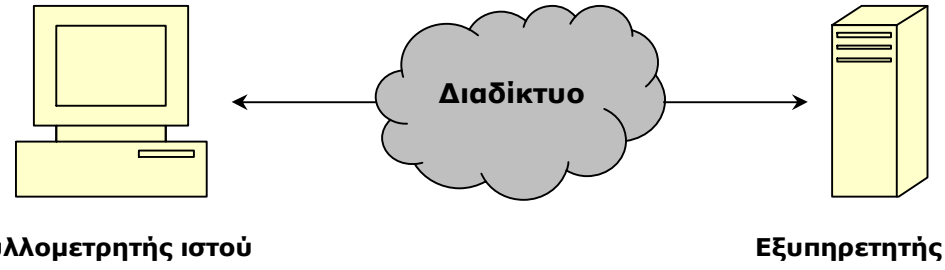
Ένα από τα προβλήματα αναφορικά με την ασφάλεια του ιστού είναι ότι το αντικείμενο έχει διαστρεβλωθεί από κατασκευαστές λογισμικού και τα μέσα ενημέρωσης. Οι κατασκευαστές φυλλομετρητών του ιστού θα σας κάνουν να πιστέψετε ότι η ασφάλεια του ιστού σχετίζεται με τη χρήση κρυπτογραφίας για να προστατευθούν οι αριθμοί των πιστωτικών καρτών. Οι προμηθευτές τοίχων προστασίας προσφέρουν τα συστήματά τους ως το μόνο μέσο για την ασφάλεια. Εν τω μεταξύ τα μέσα ενημερώσης φροντίζουν να δώσουν μια εικόνα για τον ιστό που απέχει από την πραγματικότητα, διογκώντας τους κινδύνους που υπάρχουν για τους χρήστες του χώρου.

Στην πραγματικότητα η ασφάλεια του ιστού είναι πιο απλή και πιο περίπλοκη από ότι οι προμηθευτές θα σας κάνουν να πιστεύετε. Είναι πιο απλή γιατί είναι εύκολο να σπάσετε τον ιστό στα συνθετικά του μέρη και να διαπιστώσετε που βρίσκετε το πρόβλημα. Είναι πιο περίπλοκη γιατί δεν υπάρχουν εύκολες λύσεις, καμία μαγική λύση που να εξουδετερώσει τους κινδύνους και μάλιστα κινδύνους που αναπτύσσονται με την ίδια ταχύτητα που η τεχνολογία προχωρά για να τους αντιμετωπίσει.

3.3.1 Τα τρία μέρη της ασφάλειας του Ιστού

Μια σύνδεση στον ιστό στην πραγματικότητα είναι κάτι πολύ απλό. Τόσο απλό που αποτελείται από τρία μέρη **(**ΣΧΗΜΑ **3)**:

1. Ο φυλλομετρητής του ιστού
2. Ο εξυπηρετής του ιστού
3. Η σύνδεση μεταξύ των δύο



Σχημα 3: Τα μέρη που συνθέτουν μία σύνδεση του ιστού

Ο χρήστης μέσω του φυλλομετρητή, συνδέεται με ένα απομακρυσμένο εξυπηρετητή του ιστού και ζητά ένα έγγραφο. Ο εξυπηρετητής επιστρέφει το έγγραφο και ο φυλλομετρητής το παρουσιάζει. Τι μπορεί να πάει στραβά; θα παρακολουθήσουμε τη συναλλαγή με περισσότερη λεπτομέρεια και θα διαπιστώσουμε ότι η ακεραιότητα του συστήματος βασίζεται σε ένα σύνολο από υποθέσεις.

Από την πλευρά του χρήστη

- Ο απομακρυσμένος εξυπηρετητής ανήκει και λειτουργείται από τον οργανισμό που φαίνεται ότι ανήκει.
- Τα έγγραφα που ο εξυπηρετητής επιστρέφει είναι απαλλαγμένα από επικίνδυνους ιούς ή άλλους σκοπούς.
- Ο απομακρυσμένος εξυπηρετητής δεν θα εγγράψει και δεν θα κατανείμει πληροφορίες που ο χρήστης θεωρεί προσωπικές, όπως οι συνήθειες φυλλομετρήματος του ιστού.

Από τη πλευρά του υπεύθυνου του ιστού

- Ο χρήστης δεν θα επιχειρήσει να εισβάλλει μέσα στο υπολογιστικό σύστημα του εξυπηρετητή του ιστού ή να μεταβάλλει τα περιεχόμενα του χώρου του ιστού.
- Ο χρήστης δε θα προσπαθήσει να αποκτήσει πρόσβαση σε έγγραφα στα οποία δεν επιτρέπεται να εισχωρήσει.
- Ο χρήστης δε θα προσπαθήσει να καταρρύσει τον εξυπηρετητή, κάνοντας τον μη διαθέσιμο για άλλους χρήστες.
- Αν ο χρήστης έχει αποκαλύψει τον εαυτό του είναι πράγματι αυτός που υποστηρίζει ότι είναι.

Από αμφότερες τις πλευρές

- § Η σύνδεση στο δίκτυο είναι ελεύθερη από τρίτα μέρη που παρακολουθούν τη γραμμή επικοινωνίας.
- § Η πληροφορία που αποστέλλεται μεταξύ εξυπηρετητή και φυλλομετρητή μεταφέρεται άθικτη, ελεύθερη από επεμβάσεις από τρίτα μέρη.

Ο σκοπός της ασφάλειας του ιστού είναι να διασφαλίσει ότι αυτές οι υποθέσεις παραμένουν αποδεκτές. Επειδή οι συνδέσεις του ιστού έχουν τρία μέρη, η ασφάλεια του έχει επίσης τρία μέρη.

1. **Ασφάλεια από την πλευρά του πελάτη.** Πρόκειται για μέτρα ασφαλείας που προστατεύουν το απόρρητο και την ακεραιότητα του υπολογιστή του. Οι τεχνολογικές λύσεις περιλαμβάνουν μέτρα προστασίας για να ασφαλίσουν τους χρήστες από ιούς και άλλο μοχθηρό λογισμικό καθώς και μέτρα που περιορίζουν το μέγεθος των προσωπικών πληροφοριών που οι φυλλομετρητές μπορούν να μεταφέρουν χωρίς την έγκριση του χρήστη. Επίσης, σε αυτή την κατηγορία υπάρχουν βήματα που οι οργανισμοί μπορούν να ακολουθήσουν έτσι ώστε οι ενέργειες φυλλομέτρησης του ιστού να εμποδίσουν τους υπαλλήλους από το να διακινδυνεύσουν τη μυστικότητα των απορρήτων της εταιρείας ή την ακεραιότητα του τοπικού δικτύου.

2. **Ασφάλεια από την πλευρά του εξυπηρετητή.** Πρόκειται για μέτρα που προστατεύουν τον εξυπηρετητή του ιστού και τη μηχανή που τρέχει πάνω σε αυτόν από παραβιάσεις, βανδαλισμούς χώρων και άρνηση από επιθέσεις υπηρεσιών (επιθέσεις που κάνουν αδύνατη τη φυσιολογική χρήση του χώρου του ιστού). Η γκάμα των τεχνολογικών λύσεων κυμαίνεται από συστήματα τοίχων προστασίας μέχρι μέτρα ασφαλειάς του λειτουργικού συστήματος.

3. **Απόρρητο εγγράφων.** Πρόκειται για μέτρα που προστατεύουν απόρρητες πληροφορίες από το να ανακαλυφθούν από τρίτες πλευρές. Ένας κίνδυνος στο απόρρητο των εγγράφων είναι αυτοί που κρυφακούν, οι οποίοι υποκλέπτουν έγγραφα καθώς βρίσκονται στο δίκτυο. Ένας άλλος κίνδυνος είναι η απατηλή ταυτότητα, για παράδειγμα ένας χρήστης που παρερμηνεύει τον εαυτό του στον εξυπηρετητή του ιστού σαν κάποιον εξουσιοδοτημένο να κατεβάσει ένα έγγραφο ή ένας εξυπηρετητής του ιστού που ξεγελά το χρήστη και στέλνει εμπιστευτικές πληροφορίες λέγοντάς του ότι πρόκειται για ασφαλή χώρο.

Η βασική τεχνολογική λύση σε αυτή την κατηγορία είναι η κρυπτογραφία, παρόλο που πιο απλά μέτρα, όπως η χρήση κωδικών πρόσβασης **(passwords)** για την αναγνώριση χρηστών, παίζουν επίσης σημαντικό ρόλο.

Κανένα από τα παραπάνω τρία μέρη του ιστού δεν είναι ανεξάρτητο από τα άλλα δύο όταν πρόκειται για την ασφάλεια. Κανένα από τα πιο δυνατά κρυπτογραφικά στον κόσμο δε θα αφήσει ένα χώρο του ιστού ανέπαφο αν ο υπολογιστής στον οποίο αποθηκεύεται παραβιαστεί. Ένας απόρθητος εξυπηρετητής του ιστού δε θα προστατέψει έναν οργανισμό από δημόσια ταπείνωση αν ένας φαρσέρ κατορθώσει να μετατρέψει στοιχεία τόσο όσο να πείσει τον κόσμο ότι η τοποθεσία παραβιάστηκε. Βασικός κανόνας είναι ο ακόλουθος: *"Δεν έχει σημασία ποιοί είστε, πάντα υπάρχει κάποιος στο δίκτυο που δεν θα σας συμπαθεί".* Χώροι που έχουν βανδαλιστεί στο παρελθόν:

- Το υπουργείο δικαιοσύνης των Η.Π.Α.
- Η **C.I.A.**
- Η αεροπορική δύναμη των Η.Π.Α.**(Air Force)**
- Το έθνος του ισλαμ
- **N.A.S.A.**
- Το εργατικό κόμμα της Αγγλίας
- **Telia (**Σουηδική εταιρεία τηλεπικοινωνιών**)**
- **Nesthosting ISP (**βανδαλίστηκαν **1500** σελίδες συνδρομητών**)**

3.3.2 Γιατί οι χώροι του ιστού είναι ευπρόσβλητοι

Τα προβλήματα που ανοίγουν κενά στην ασφάλεια του ιστού είναι ποικίλα αλλά όλα αναπηδούν από λίγες πλην όμως ουσιαστικές αιτίες ¨τα οχτώ θανάσιμα αμαρτήματα" της ασφάλειας του χώρου του ιστού. Ακολουθούν τα οχτώ "αν" που καθιστούν άκρως ανασφαλή τον ιστό.

- ΥΠΑΡΧΟΥΝ ΛΑΘΗ ΣΤΟ ΛΟΓΙΣΜΙΚΟ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

Ένα ασφαλές κομμάτι του λογισμικού είναι αυτό που κάνει αυτά που υποτίθεται ότι πρέπει να κάνει και τίποτε παραπάνω. Οι εισβολείς υπολογιστών συνεχώς έχουν το νου τους για λάθη σε λογισμικό του εξυπηρετητή γιατί κάθε λάθος αναπαριστά μια πιθανή πόρτα εισόδου. Τα λάθη γίνονται πιο συχνά καθώς τα προγράμματα γίνονται πιο μεγαλά και πιο περίπλοκα.

- ΤΟ ΛΟΓΙΣΜΙΚΟ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΕΧΕΙ ΔΙΑΜΟΡΦΩΘΕΙ ΛΑΘΟΣ

Ακόμη και αν ο εξυπηρετητής του ιστού και όλο το λογισμικό που υποστηρίζει δεν έχει λάθη, ο χώρος του ιστού δε θα είναι ασφαλής εκτός αν όλοι οι εξυπηρετητές του δικτύου και το λογισμικό έχουν διαμορφωθεί σωστά. Παρόλο που τα έτοιμα δικτυακά συστήματα έχουν σχεδιαστεί για να είναι ασφαλή, συχνά απαιτείται κάποια προσπάθεια για να επιτευχθεί αυτός ο στόχος.

- ΤΟ ΥΛΙΚΟ ΤΟΥ ΕΞΥΠΗΡΕΤΗΤΗ ΔΕΝ ΕΙΝΑΙ ΑΣΦΑΛΕΣ

Αν κάποιο υλικό του εξυπηρετητή δεν είναι ασφαλές τότε τίποτα δεν είναι! Αν με άλλα λόγια ο εξυπηρετητής δεν είναι φυσικά ασφαλής τότε τα υπόλοιπα μέτρα προστασίας δεν έχουν κανένα νόημα. Αν ο εξυπηρετητής του ιστού βρίσκεται σε ένα εργαστήριο υπολογιστών, σε μία κοινή αίθουσα, σε ένα ξεκλείδωτο τηλεφωνικό γραφείο τότε σίγουρα δεν είναι ασφαλής.

- ΤΑ ΔΙΚΤΥΑ ΔΕΝ ΕΙΝΑΙ ΑΣΦΑΛΗ

Οποιοσδήποτε με πρόσβαση στο δίκτυο και με το κατάλληλο λογισμικό μπορεί να υποκλέψει όλες τις μεταδόσεις στο διαδίκτυο και στα περισσότερα τοπικά δίκτυα που δεν γίνονται κρυπτογραφημένες.

- Η ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΣΥΓΓΡΑΦΗ & ΤΑ ΕΡΓΑΛΕΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΑΝΟΙΓΟΥΝ ΠΡΟΣΒΑΣΕΙΣ

Οι εξυπηρετητές του ιστού απαιτούν φροντίδα και τροφοδότηση. Τα αρχεία ημερολογίου πρέπει να εξετάζονται, οι παράμετροι απόδοσης θέλουν ρύθμιση, νέοι δίσκοι και κατάλογοι πρέπει να προστίθενται κάθε τόσο. Τα περιεχόμενα του χώρου συνεχώς αλλάζουν, αναβαθμίζονται και ανανεώνονται. Μερικοί χώροι αναβαθμίζονται από άλλες μηχανές στο τοπικό δίκτυο, άλλες φορές και μέσω του διαδικτύου. Άλλά όπως γνωρίζουμε τα δίκτυα δεν είναι ασφαλή.

- ΕΣΩΤΕΡΙΚΕΣ ΑΠΕΙΛΕΣ ΠΑΡΑΒΛΕΠΟΝΤΑΙ

Σε καμία περίπτωση δεν πρέπει να υποτιμούνται οι απειλές που προέρχονται από ανθρώπους που έχουν νόμιμο λόγο να χρησιμοποιούν το σύστημα. Υπάρχουν αρκετοί λόγοι που κάποιος χρήστης θα θελήσει να ανακατευθεί με το πληροφοριακό σύστημα ξεκινώντας από επιπόλαιη περιέργεια και καταλήγοντας σε βιομηχανική κατασκοπεία.

- ΑΠΕΙΛΕΣ ΑΡΝΗΣΗΣ ΥΠΗΡΕΣΙΩΝ ΣΥΧΝΑ ΑΓΝΟΟΥΝΤΑΙ

Συνήθως πρόκειται για πρόβλημα που ξεπερνιέται γρήγορα και ανώδυνα, αποδεικνύει όμως την τρωτότητα του συστήματος. Ειδικά για εφαρμογές με σημαντική αποστολή, ο συγκεκριμένος κίνδυνος προκαλεί σοβαρές ανησυχίες.

- ΔΕΝ ΥΠΑΡΧΕΙ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

Αν δεν έχετε πολιτική ασφαλείας τότε δεν μπορείτε να ξέρετε αν ο χώρος σας είναι ασφαλής. Δεν χρειάζεται κάτι υπερβολικό, απλά μια λίστα του τι είναι και τι δεν είναι επιτρεπτό.

3.4 Σχεδιασμός συστήματος ασφαλείας

Ο σχεδιασμός του συστήματος ασφαλείας οφείλει να αποτελεί τμήμα του αρχικού σχεδιασμού του συστήματος και όχι μια διαδικασία που θα εκτελείται μετά την εγκατάσταση του συστήματος. Οι λόγοι είναι απλοί: Αφενός είναι οικονομικότερο να σχεδιάζονται και να υλοποιούνται τατόχρονα το σύστημα και η ασφάλεια του και αφετέρου είναι λειτουργικότερο. Ο σχεδιασμός στηρίζεται σε πέντε βασικά βήματα:

Βήμα 1: Δημιουργία πολιτικής ασφαλείας

Βήμα 2: Προσθήκη των κατάλληλων μεθόδων προστασίας ανάλογα με το πληροφοριακό σύστημα που θα χρησιμοποιήσουμε

Βήμα 3: Σχεδίαση του συστήματος προστασίας που θα καλύπτει το φυσικό, το δικτυακό περιβάλλον και το περιβάλλον του υπολογιστικού συστήματος.

Βήμα 4: Ανάπτυξη διαδικασιών για την παρακολούθηση, τον έλεγχο, την συντήρηση και την αναβάθμιση του συστήματος ασφαλείας.

Βήμα 5: Χρήση των συμπερασμάτων από την παρακολούθηση και τον έλεγχο του συστήματος με στόχο την βελτίωση τόσο του σχεδιασμού, όσο και της υλοποίησης και λειτουργίας του συστήματος.

- **Δημιουργία πολιτικής ασφαλείας**

Στο πρώτο στάδιο πρέπει αρχικά να καθοριστεί η πολιτική ασφαλείας που θα ακολουθηθεί για το σύνολο του συστήματος. Αυτό περιλαμβάνει το πληροφοριακό σύστημα (υπολογιστές και δίκτυα), τα δεδομένα και τους ανθρώπους (διαχειριστές, προσωπικό συντήρησης, χρήστες, πελάτες). Η πολιτική

ασφαλείας δημιουργείται μετά από ανάλυση και αξιολόγηση των αναγκών κάθε οργανισμού για τη διαθεσιμότητα, τους κινδύνους και τις δυνατότητες που πρέπει να διαθέτει το πληροφορικό του σύστημα. Απαρτίζεται από πλάνο που περιέχει τις διαδικασίες λειτουργίας και ελέγχου, τον απαραίτητο εξοπλισμό, αλλά και σενάρια, σχέδια και διαδικασίες αντιμετώπισης κρίσεων. Σε αυτό το έγγραφο υπάρχουν λίγες τεχνικές λεπτομέρειες. Απλά λέει τι πρέπει να γίνει, όχι πως να γίνετε

- **Σχεδιασμός περιβάλλοντος**

Το δεύτερο στάδιο περιλαμβάνει το σχεδιασμό του περιβάλλοντος που θα εγκατασταθεί το πληροφοριακό σύστημα. Με την έννοια περιβάλλον ορίζουμε όλα όσα υπάρχουν έξω από την εφαρμογή. Δηλαδή: οι υπολογιστές, τα λειτουργικά συστήματα, τα δίκτυα, καθώς και η φυσική τοποθεσία της εφαρμογής.

- **Σχεδιασμός μηχανισμού ασφαλείας**

Το τρίτο στάδιο στο σχεδιασμό του συστήματος ασφαλείας αποτελεί η επιλογή των κατάλληλων μεθόδων προστασίας που θα χρησιμοποιηθούν. Γνωρίζοντας το γενικό σχεδιασμό του πληροφοριακού συστήματος, την πολιτική ασφαλείας της εταιρείας, θα πρέπει ήδη να έχουμε καταλάβει ποιές είναι οι ανάγκες μας, τι προστασία θα χρειαστούμε και ποια τεχνολογία είναι η κατάλληλη.

- **Παρακολούθηση και έλεγχος**

Για να είναι επιτυχής ο σχεδιασμός του συστήματος ασφαλείας είναι ιδιαίτερα σημαντικό να έχει ληφθεί υπόψη και να έχουν καθοριστεί οι διαδικασίες μέσα από τις οποίες θα παρακολουθείται καθημερινά η λειτουργία του και θα ελέγχεται σε τακτικά χρονικά διαστήματα η απόδοσή του. Έτσι θα γίνονται οι απαραίτητες βελτιώσεις, προσθήκες και αναβαθμίσεις.

Όσο τεχνολογικά τέλειο κι αν είναι το σύστημα που χρησιμοποιείται, είναι βέβαιο ότι θα αποτύχει, αν δεν ακολουθηθούν τα παραπάνω βήματα κατά το σχεδιασμό του και κυρίως αν δεν υλοποιηθεί η **πολιτική ασφαλείας** καθώς και το τελευταίο βήμα του σχεδιασμού: η **παρακολούθηση** και ο **έλεγχος**.

3.4.1 Βασικές αρχές ασφάλειας δεδομένων

Γενικότερα, τα δεδομένα που δημιουργούνται ή διακινούνται κατά τη διεξαγωγή μιας ηλεκτρονικής συναλλαγής σχετίζονται άμεσα με τους εμπλεκόμενους στη συναλλαγή και θα πρέπει να διασφαλιστούν απέναντι σε όλους τους πιθανούς κινδύνους, όπως υποκλοπή, αλλοίωση, ανεπιθύμητη κοινοποίηση σε τρίτους κλπ. Για το σκοπό αυτό απαιτείται η δημιουργία ενός περιβάλλοντος ηλεκτρονικών συναλλαγών, το οποίο, επιπλέον της ασφάλειας των συστημάτων, θα δίνει έμφαση στην ασφάλεια των ίδιων των δεδομένων και θα διασφαλίζει τις εξής βασικές αρχές:

1. **Επιβεβαίωση ταυτότητας (authentication),** ώστε να αποδεικνύεται η ταυτότητα ενός ατόμου ή μιας εφαρμογής λογισμικού ή ενός μηχανήματος **(**π.χ. **server)**

2. **Εμπιστευτικότητα (confidentiality),** ώστε να εξασφαλίζεται ο ιδιωτικός χαρακτήρας της πληροφορίας.

3. **Ακεραιότητα (integrity),** ώστε να βεβαιώνεται ότι η πληροφορία δεν έχει αλλοιωθεί κατά την μετάδοσή της.

4. **Μη αποκήρυξη (non-repudiation),** ώστε να αποκλειστεί το ενδεχόμενο κάποιος από τους συμμετέχοντες σε μια συναλλαγή να αρνηθεί εκ των υστέρων την εμπλοκή του σ' αυτήν ή τα αποτελέσματά της.

Με βάση τα σημερινά τεχνολογικά δεδομένα, η πλήρης διασφάλιση των πιο πάνω βασικών αρχών είναι δυνατόν να επιτευχθεί μόνο με τη χρήση της κρυπτογραφίας, η οποία επιπλέον θα πρέπει να συνδυάζεται με πολιτικές ασφάλειας, που να καθορίζουν τους κανόνες με τους οποίους λειτουργεί ένα σύστημα κρυπτογράφησης, προϊόντα **(software** και **hardware)** τα οποία να επιτρέπουν την δημιουργία, αποθήκευση και διαχείριση των κλειδιών ασφαλείας, που θα χρησιμοποιούνται κατά την κρυπτογράφηση **/** αποκρυπτογράφηση και τέλος, διαδικασίες που να περιγράφουν τους τρόπους δημιουργίας, διανομής και χρήσης των κλειδιών ασφαλείας.

Η σύγχρονη προσέγγιση στις παραπάνω απαιτήσεις είναι γνωστή με τον όρο Συστήματα Υποδομής Δημοσίου Κλειδιού **(Public Key Infrastructure Systems-** Συστήματα **PKI),** τα οποία ενσωματώνουν ως αναπόσπαστο τμήμα τους και

διάφορες τεχνικές κρυπτογραφίας και επιτρέπουν την ασφαλή διεξαγωγή των εμπορικών συναλλαγών μέσω του **Internet**, επιτυγχάνοντας την τήρηση των τεσσάρων βασικών αρχών που προαναφέρθηκαν.

Πιο συγκεκριμένα και σε σχέση με τις τέσσερις βασικές αρχές, ένα σύστημα PKI λειτουργεί ως εξής:

- **Επιβεβαίωση ταυτότητας (authentication)**

Η επιβεβαίωση ταυτότητας σε ένα ηλεκτρονικό σύστημα είναι απαραίτητη, προκειμένου η πρόσβαση σ' αυτό να επιτρέπεται μόνος σε όσους μπορούν να παράσχουν τα σχετικά διαπιστευτήρια. Στα περισσότερα συστήματα η επιβεβαίωση ταυτότητας διεκπεραιώνεται με τη χρήση ενός κωδικού χρήστη και ενός συνθηματικού **(password)**, τεχνική η οποία παρουσιάζει πλήθος αδυναμιών από πλευράς ασφάλειας. Σε ένα περιβάλλον PKI, για την επιβεβαίωση ταυτότητας χρησιμοποιούνται τα **«**ψηφιακά πιστοποιητικά**» (**ή ψηφιακές ταυτότητες**)**. Τα συνηθέστερα σημείας αποθήκευσης ενός ψηφιακού πιστοποιητικού είναι είτε ο μαγνητικός δίσκος του υπολογιστή του χρήστη, είτε μια ειδική κάρτα **(**έξυπνη κάρτα**)** μικρού μεγέθους, που ο χρήστης έχει πάντα μαζί του. Με ψηφιακά πιστοποιητικά εξάλλου εφοδιάζονται όχι μόνο τα φυσικά πρόσωπα, αλλά και ορισμένα μηχανήματα, π.χ. ο **web server** μιας επιχείρησης, ώστε να μπορεί να **"**αποδείξε**"»** στον εν δυνάμει χρήστη που τον έχει επισκεφθεί μέσω του **Internet** ότι πράγματι εκπροσωπεί μια συγκεκριμένη εταιρεία και έχει κατά συνέπεια το δικαίωμα να προβαίνει σε νόμιμες ηλεκτρονικές συναλλαγές **(**πωλήσεις κλπ.**)**.

- **Εμπιστευτικότητα (confidentiality)**

Βασικό χαρακτηριστικό μιας ασφαλούς συναλλαγής μεταξύ δύο μερών είναι το περιεχόμενό της να παραμείνει μυστικό και απροσπέλαστο για οποιονδήποτε τρίτο. Τα προς προστασία δεδομένα μπορεί να αφορούν επιχειρηματικά σχέδια, οικονομικές συναλλαγές, πνευματική ιδιοκτησίας, εμπιστευτικές πληροφορίες σχετικές με το πρόσωπο κλπ. Ένα σύστημα PKI χρησιμοποιεί διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης, στηριζόμενες σε κατάλληλα **«**κλειδιά**»**, προκειμένου να κρατήσει τα ευαίσθητα δεδομένα προστατευμένα από κάθε ανεπιθύμητη πρόσβαση. Έτσι ακόμη και αν τα δεδομένα υποκλαπούν, θα είναι εξαιρετικά δύσκολο έως αδύνατο να αξιοποιηθούν, διότι θα πρέπει προηγουμένως να αποκρυπτογραφηθούν.

- **Ακεραιότητα δεδομένων (data integrity)**

Η αρχή αυτή διασφαλίζει ότι τα δεδομένα που έφθασαν στον παραλήπτη ενός μηνύματος είναι τα ίδια με αυτά που απέστειλε ο αποστολέας και δεν έχουν αλλοιωθεί καθ' οδόν. Η σημασία της ακεραιότητας των δεδομένων μιας ηλεκτρονικής συναλλαγής γίνεται εύκολα αντιληπτή αν σκεφθεί κανείς το παράδειγμα μιας ηλεκτρονικά μεταδιδόμενης οικονομικής προσφοράς για **1.000** μονάδες ενός συγκεκριμένου είδους, προς **5** ευρώ ανά μονάδα. Αν η τιμή μονάδας αλλοιωθεί σε **50** ευρώ, τότε αμφισβητείται η ίδια η υπόσταση της προσφοράς. Ένα σύστημα PKI χρησιμοποιεί τους λεγόμενους αλγόριθμους κατατεμαχισμού και την έννοια του "αποτυπώματος" ενός μηνύματος, σε συνδυασμό με ψηφιακές υπογραφές, προκειμένου να επιτρέψει στον παραλήπτη να βεβαιωθεί ότι το μήνυμα δεν έχει αλλοιωθεί ούτε κατ' ελάχιστον σε σχέση με αυτό που πράγματι απέστειλε ο αποστολέας. Ακόμη και στην περίπτωση που δεν υφίσταται κίνδυνος κακόβουλης ενέργειας εκ μέρους τρίτων, η βεβαιότητα για την ακρίβεια και την πληρότητα ενός ηλεκτρονικού μηνύματος είναι σημαντική.

- **Μη αποκήρυξη (non-repudiation)**

Η αρχή της μη αποκήρυξης σημαίνει ότι εάν προκύψει διαφωνία ή αμφισβήτηση σχετικά με τη διεξαγωγή μιας ηλεκτρονικής συναλλαγής, υπάρχουν διαθέσιμα, αδιάψευστα αποδεικτικά στοιχεία, τα οποία μπορούν να χρησιμοποιηθούν από ένα τρίτο ουδέτερο μέρος, προκειμένου να διαπιστωθεί τι ακριβώς έχει συμβεί. Πρόκειται ουσιαστικά για το συνδυασμό "επιβεβαίωση ταυτότητας- ακεραιότητα δεδομένων", ο οποίος παρέχει στον παραλήπτη την βεβαιότητα ότι ο αποστολέας δεν θα μπορέσει να αρνηθεί (ψευδώς) ότι έχει δημιουργήσει, υπογράψει και αποστείλει ένα ηλεκτρονικό έγγραφο ή έχει συμμετάσχει σε μια συναλλαγή. Αυτό είναι ιδιαίτερα σημαντικό σε οικονομικές ιδίως συναλλαγές, όπου το ένα από τα δυο μέρη θα μπορούσε πιθανόν να αρνηθεί την πληρωμή π.χ. ενός λογαριασμού για παροχή υπηρεσιών, με τον ισχυρισμό ότι οι σχετικές υπηρεσίες δεν είχαν ποτέ ζητηθεί. Σε ένα περιβάλλον PKI, η μη αποκήρυξη χρησιμοποιεί μεν την έννοια των ψηφιακών υπογραφών, προϋποθέτει όμως και ένα γενικότερο πλαίσιο λειτουργίας που καθορίζεται από συγκεκριμένες πολιτικές και διαδικασίες. Φυσικά, σημαντικό ρόλο παίζει στην περίπτωση αυτή και το ισχύον κάθε φορά νομικό πλαίσιο, το οποίο θα πρέπει να ληφθεί σοβαρά υπ' όψη.

Κεφάλαιο 4

Τεχνολογίες Προστασίας

4.1 Βασική Κρυπτογραφία

Η λέξη **Cryptography (**κρυπτογραφία**)** προκύπτει από ελληνικές λέξεις και σημαίνει κρυφό γράψιμο. Η κρυπτογραφία χρησιμοποιούνταν από το στρατό τον καιρό των Ελληνικών πολέμων και αναπτύχθηκε σταθερά με σοφία παράλληλα με μαθηματικά και την τεχνολογία της πληροφορίας. Η κρυπτογραφία **(encryption)** είναι η τέχνη του να κρατάμε ένα μήνυμα κρυμμένο, δηλαδή σε μορφή που το νόημά του να είναι μη αναγνωρίσιμο, ενώ η κρυπτανάλυση **(cryptanalysis)** είναι η τέχνη της αποκάλυψης του κρυπτογραφημένου περιεχομένου χωρίς, και αυτό είναι το σημαντικό, να γνωρίζουμε το κατάλληλο κλειδί.

Η μετατροπή του περιεχομένου ενός μηνύματος σε μη αναγνώσιμη μορφή **(**κρυπτογράφηση**)**, καθώς και η αντίστροφη μετατροπή **(**αποκρυπτογράφηση**)** επιτυγχάνεται με τη χρήση πολύπολοκων μαθηματικών διαδικασιών, που είναι γνωστές ως κρυπτογραφικοί αλγόριθμοι. Οι αλγόριθμοι αυτοί χωρίζονται σε δύο μεγάλες κατηγορίες, τους συμμετρικούς και τους ασύμμετρους. Κατ' επέκταση, τα συστήματα κρυπτογραφίας, ανάλογα με το είδος των αλγορίθμων που χρησιμοποιούν, ανήκουν είτε στη **Συμμετρική** είτε στην **Ασύμμετρη Κρυπτογραφία**, χωρίς να αποκλείεται και η συνδυασμένη χρήση και των δύο κατηγοριών.

4.1.1 Πως λειτουργεί η Κρυπτογραφία

Ας υποθέσουμε ότι θέλουμε να στείλουμε ένα μήνυμα σε κάποιο πρόσωπο, είτε με τον παραδοσιακό τρόπο, είτε ηλεκτρονικά, και επιθυμούμε να μην το διαβάσει κανένας άλλος, εκτός βέβαια από τον επίσημο παραλήπτη. Εντούτοις, υπάρχει πάντοτε η περίπτωση κάποιος να ανοίξει το γράμμα ή να **«**κρυφακούσει**»** το σήμα μετάδοσης. Για το λόγο αυτό στέλνουμε το αρχικό μήνυμα κωδικοποιημένο. Με άλλα λόγια, το μετασχηματίζουμε σύμφωνα με ένα συγκεκριμένο σύνολο κανόνων που ονομάζουμε αλγόριθμο ή σύστημα κρυπτογράφησης. Ο μετασχηματισμός γίνεται με τέτοιο τρόπο, ώστε, για να

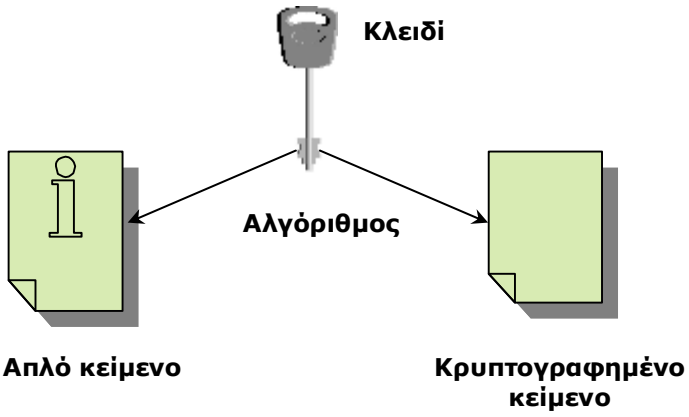
μπορέσει ο παραλήπτης να το αποκωδικοποιήσει, θα πρέπει να γνωρίζει ένα συγκεκριμένο κλειδί, που δεν είναι τίποτα άλλο παρά μια ακολουθία αριθμών.

Όλα τα κρυπτογραφικά συστήματα, ανεξάρτητα πόσο πολύπλοκα είναι, έχουν τα ακόλουθα τέσσερα βασικά μέρη **(**ΣΧΗΜΑ **4).**

1. **Απλό κείμενο.** Αυτό είναι το αρχικό μήνυμα πριν γίνει κάτι πάνω σε αυτό. Είναι είτε αναγνώσιμο από άνθρωπο είτε σε μια μορφή που οποιοσδήποτε με το κατάλληλο λογισμικό να μπορεί να το χρησιμοποιήσει.

2. **Κρυπτογραφημένο κείμενο** Αυτό είναι το απλό κείμενο αφού έχει τροποποιηθεί με κάποιο τρόπο για να συγκαληφθεί, καθιστώντας το μη αναγνώσιμο. Η επεξεργασία της μετατροπής του απλού κειμένου σε κρυπτογραφημένο είναι η ¨κρυπτογράφηση**" (encryption),** ενώ η αντίθετη λειτουργία είναι γνωστή σαν "αποκρυπτογράφηση**" (decryption).**
3. **Κρυπτογραφικός αλγόριθμος** Είναι μια μαθηματική λειτουργία που χρησιμοποιείται για τη μετατροπή απλού κειμένου σε κρυπτογραφημένο και αντίστροφα.

4. **Κλειδί** Είναι το μυστικό κλειδί που χρησιμοποιείται για να κρυπτογραφηθεί και να αποκρυπτογραφηθεί το μήνυμα. Κάθε κλειδί μετατρέπει το ίδιο απλό κείμενο σε διαφορετικό κρυπτογραφημένο κείμενο. Αν το κρυπτογραφικό σύστημα λειτουργεί σωστά, μόνο οι άνθρωποι που γνωρίζουν το σωστό κλειδί μπορούν να αποκρυπτογραφήσουν ένα κομμάτι του κρυπτογραφημένου κειμένου.



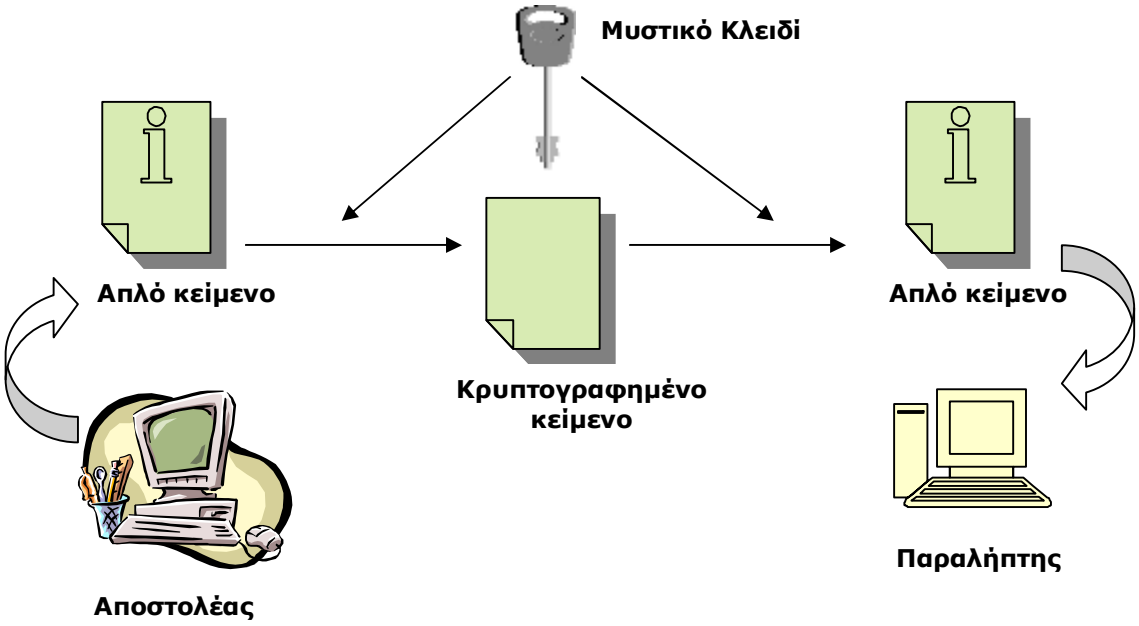
ΣΧΗΜΑ 4 : Τα τέσσερα βασικά μέρη ενός κρυπτογραφικού συστήματος

Το μεγάλο πλεονέκτημα της κρυπτογραφίας είναι ότι μπορεί το κρυπτογραφημένο μήνυμα να μεταδοθεί σε μη ασφαλή, δημόσια κανάλια επικοινωνίας. Ακόμη κι αν αποκτηθεί από κάποιον, του είναι άχρηστο εφόσον δεν έχει και δεν καταφέρει να ανακαλύψει το κλειδί αποκρυπτογράφησης.

Η κρυπτογραφία γενικά περιλαμβάνει δύο επιμέρους κλάδους, την κρυπτολογία και την κρυπτανάλυση. Η κρυπτολογία ασχολείται με την επινόηση νέων και διαρκών ισχυρότερων κρυπτογραφικών αλγορίθμων, ενώ η κρυπτανάληση έχει σαν αντικείμενο την εξέταση των κρυπτογραφικών αλγορίθμων με χρήση ειδικών εργαλείων και τεχνικών, με σκοπό να εντοπίσει πιθανά αδύνατα σημεία τους που θα τους καθιστούσαν ευάλωτους σε επιθέσεις. Κατά συνέπεια, κάθε κρυπτογραφικός αλγόριθμος που επινοείται από τους ειδικούς της κρυπτολογίας, θα πρέπει να τίθεται στη διάθεση των κρυπταναλυτών, προκειμένου να διασφαλιστεί ότι δεν έχει **(**λόγω σχεδιασμού ή εφ' όσον χρησιμοποιηθεί με κάποιο ειδικό τρόπο**)** κενά ή τρόπους παραβίασης. Αν ο πιο πάνω διεξοδικός έλεγχος δεν πραγματοποιηθεί ενδεχομένως τα πιθανά αδύνατα σημεία του να εντοπισθούν από τρίτους, αφού έχει τεθεί σε χρήση, οπότε τα αποτελέσματα για όσους στηρίζονται σ' αυτό να είναι μέχρι και καταστροφικά.

4.1.2 Συμμετρική Κρυπτογραφία

Το κρυπτογραφικό αυτό σύστημα είναι το πλέον γνωστό και χαρακτηρίζεται από την ύπαρξη ενός και μόνο κώδικα ή κλειδιού, το οποίο χρησιμοποιείται τόσο για την κρυπτογράφηση του μηνύματος από τον αποστολέα -πριν την αποστολή- όσο και για την αποκρυπτογράφηση του από τον παραλήπτη -μετά την μεταφορά. Για τον λόγο αυτό άλλωστε ονομάζεται και συμμετρικό. Επίσης είναι γνωστό και με τα ονόματα κρυπτογραφία μυστικού κλειδού **(secret key)** ή διαμοιραζομένου μυστικού **(shared secret)**, δεδομένου ότι το κλειδί θα πρέπει να παραμείνει μυστικό, αλλά και ταυτόχρονα να είναι γνωστό μόνο στα δύο μέρη που ανταλλάσσουν μηνύματα. Για να δουλέψει επομένως το σύστημα, ο αποστολέας και ο παραλήπτης πρέπει, εκ των προτέρων, να συμφωνήσουν σε ένα μυστικό κλειδί **(**ΣΧΗΜΑ **5).**



Σχημα 5 : Συμμετρική Κρυπτογραφία

Τα κρυπτογραφικά κλειδιά παρουσιάζουν πολλές ομοιότητες με τα φυσικά κλειδιά της καθημερινής ζωής, που χρησιμοποιούνται π.χ. για να κλειδώσουν ή να ξεκλειδώσουν μια πόρτα. Για κάθε τύπο κλειδιαριάς, υπάρχει ένα κλειδί ειδικού σχήματος που ταιριάζει σ' αυτήν και το οποίο πρέπει να έχει το σωστό μήκος και τη σωστή μορφολογία. Ένα κλειδί για κλειδαριές συγκεκριμένου κατασκευαστή είναι πολύ πιθανόν να ταιριάζει σε οποιαδήποτε κλειδαριά αντίστοιχου τύπου, αλλά μόνο το σωστό κλειδί, αυτό με το κατάλληλο μήκος και μορφολογία μπορεί να περιστραφεί και να ανοίξει την κλειδαριά.

Κατ' αναλογία, και στα σύγχρονα συστήματα κρυπτογραφίας που λειτουργούν με χρήση υπολογιστών, κάθε κρυπτογραφικός αλγόριθμος χρειάζεται ένα κλειδί με το σωστό μήκος, δηλ. με το σωστό αριθμό **bits.** Ένας κρυπτογραφικός αλγόριθμος μπορεί να λειτουργήσει με οποιοδήποτε κλειδί έχει το κατάλληλο μήκος, αλλά η εφαρμογή του αλγόριθμου θα έχει ως αποτέλεσμα την αποκρυπτογράφηση ενός κρυπτογραφημένου μηνύματος μόνο με το κλειδί που διαθέτει τη σωστή ακολουθία **bits.**

Οι συμμετρικοί αλγόριθμοι κρυπτογράφησης δέχονται σαν είσοδο κανονικό αναγνώσιμο κείμενο **(clear text- plain text)** και με τη χρήση του συμμετρικού κλειδιού παράγουν σαν αποτέλεσμα **(**εξαγόμενο**)** μια κρυπτογραφημένη μορφή του αρχικού κειμένου. Το συμμετρικό κλειδί δεν είναι παρά ένα τυχαίος αριθμος

με το σωστό μέγεθος. Έτσι, αν ο αλγόριθμος είναι συμμετρική κρυπτογράφηση των **40bits,** το συμμετρικό κλειδί θα είναι μήκους **40bits,** ενώ αν πρόκειται για αλγόριθμο συμμετρικής κρυπτογράφησης των **128 bits,** τότε το συμμετρικό κλειδί θα είναι μήκους **128 bits.**

Ένας κρυπτογραφικός αλγόριθμος χαρακτηρίζεται ως ασφαλής εφ' όσον έχει προηγηθεί ο εξαντλητικός έλεγχός του από τους κρυπταναλυτές, χωρίς να εντοπισθούν αδυναμίες. Υπ' αυτές τις προϋποθέσεις ο μόνος τρόπος να παραβιαστεί ένα κρυπτογραφημένο μήνυμα, είναι να δοκιμαστούν όλες οι πιθανές τιμές κλειδιών που αντιστοιχούν στο συγκεκριμένο μέγεθος. Αυτό αποκαλείται επίθεση ωμής βίας **(brute force attack).** Στατιστικά θα χρειαστεί να δοκιμαστούν μόνο οι μισές από τις πιθανές τιμές του κλειδιού, προκειμένου να εντοπισθεί το σωστό κλειδί. Αυτό μπορεί να ακούγεται μη πρακτικό αλλά μη ξεχνάμε πως ένας υπολογιστής υψηλής ταχύτητας μπορεί να προσπαθήσει εκατομμύρια πιθανότητες σε ένα δευτερόλεπτο. Αυτός είναι και ο λόγος που καθιστά το μήκος του κλειδιού σημαντικό.Για παράδειγμα, ένα κλειδί μήκους **16** δυαδικών ψηφίων **(bits)** διαθέτει $\mathbf{2^{16}=65536}$ διαφορετικούς συνδυασμούς και θα υποστεί επίθεση ωμής βίας αμέσως. Ένα κλειδί μήκους **40 bits** διαθέτει περισσότερους από $\mathbf{10^{12}}$ συνδυασμούς. Παρόλο που φαίνονται πολλοί, ένα κλειδί **40 bits** θεωρείται αδύναμο ώστε να του εμπιστευθούν πολύτιμες πληροφορίες. Τα κλειδιά που χρησιμοποιούνται για να κρυπτογραφηθούν ευαίσθητες πληροφορίες είναι συνήθως **128 bits** ή και μεγαλύτερα. **128 bits** σημαίνει $\mathbf{10^{38}}$ συνδυασμοί περισσότεροι από των αριθμό σταγόνων νερού που υπάρχει σε όλους τους ωκεανούς της γης.

Τα μεγέθη των κλειδιών επιλέγονται έτσι ώστε να είναι πρακτικά αδύνατο να δοκιμαστούν έστω και οι μισές πιθανές τιμές του κλειδιού, ακόμη και με χρήση τεράστιου αριθμού υπολογιστών, μέσα στο χρονικό διάστημα κατά το οποίο τα υπό προστασία δεδομένα πρέπει να παραμείνουν ασφαλή. Είναι φυσικά αδύνατο να προβλεφθεί με ακρίβεια η εξέλιξη της τεχνολογίας των υπολογιστών οπότε είναι απαραίτητο να γίνουν κάποιες υποθέσεις σχετικά με την πιθανή αύξηση της επεξεργαστικής τους ισχύος.

Υπάρχουν οι εξής κατηγορίες συμμετρικών αλγορίθμων κρυπτογράφησης:

1. **DES** Οι αλγόριθμοι, οι οποίοι χωρίζουν τα προς κρυπτογράφηση δεδομένα σε πακέτα των **64bits** και είναι γνωστοί ως **"block ciphers".** Ο πιο γνωστός από αυτούς είναι ο **DES (Data Encryption Standard),** ο οποίος έχει σταθερό μήκος

κλειδιού **56bits** και αναπτύχθηκε αρχικά από την **IBM** στην δεκαετία του **1970,** ενώ στη συνέχεια υιοθετήθηκε και από την κυβέρνηση των ΗΠΑ ως το επίσημο πρότυπο κρυπτογράφησης απορρήτων πληροφοριών. Ο **DES** υπήρξε εν χρήσει για μεγάλο διάστημα και χρησιμοποιήθηκε σε πολλά κρυπτογραφικά συστήματα, όπως το σύστημα **Kerberos,** το οποίο αναπτύχθηκε στο MIT. Λόγω όμως της αυξανόμενης ισχύος των υπολογιστών το μήκος **56bits** κλειδί του αρχίζει να γίνεται ευάλωτο σε επιθέσεις τύπου ωμής βίας. Ο **"**κλασσικός**"** αλγόριθμος **DES** είναι πλέον ξεπερασμένος, αφού με τη χρήση ενός σύγχρονου υπολογιστή μπορεί να παραβιαστεί σχετικά εύκολα. Το πρότυπο που αναμένεται να δώσει νέα ζωή στο **DES** είναι το **AES (Advanced Encryption Standard,** Εξελιγμένο Πρότυπο Κωδικοποίησης**).** Στο μεταξύ, εφαρμόζοντας διάφορες τεχνικές επάνω στο **DES,** μπορούμε να αυξήσουμε σημαντικά την ασφάλειά του. Με τη μέθοδο **Triple-DES,** για παράδειγμα, το μήνυμα κωδικοποιείται τρεις φορές, με τρία διαφορετικά κλειδιά. 'Αλλες παραλαγές του **DES** είναι**: DESX, GDES, RDES** όπου χρησιμοποιούνται μεγαλύτερα κλειδιά

2. **RC4.** Στην κατηγορία αυτή ανήκουν οι αλγόριθμοι που δεν εφαρμόζονται σε πακέτα δεδομένων συγκεκριμένου μεγέθους **(64** ή **128bits),** αλλά σε ακολουθίες **bits (stream ciphers).**Ο πιο γνωστός από αυτούς είναι ο **RC4,** με κυριότερα χαρακτηριστικά του την ταχύτητα **(**είναι ταχύτερος από όλους της προηγούμενος κατηγορίας**)** και την υποστήριξη κλειδιών μεταβλητού μήκους.

3. **IDEA Ο** Διεθνής Αλγόριθμος Κρυπτογράφησης Δεδομένων **(International Data Encryption Algorithm),** είναι δημοφιλής στην Ευρώπη αλλά όχι τόσο στην Αμερική. Με ένα μυστικό κλειδί **128 bits,** θεωρείται ότι είναι πιο ασφαλής από τον **DES.** Ο **IDEA** είναι από τους βασικότερους αλγορίθμους στο λογισμικό κρυπτογράφησης του ηλεκτρονικού ταχυδρομείου, του **PGP (Pretty Good Privacy).** Ο άλλος είναι ο **RSA** που αναλύεται παρακάτω.

Τέλος, κοινές σε όλους τους συμμετρικούς αλγόριθμους είναι οι εξής δύο ιδιότητες:

- Είναι γενικά γρήγοροι στην εκτέλεσή τους.
- Είναι συμπαγείς, με την έννοια ότι το παραγόμενο κρυπτογραφημένο μήνυμα έχει γενικά το ίδιο μέγεθος με το αρχικό μήνυμα.

Με βάση τα παραπάνω, εάν δύο πρόσωπα Α και Β θέλουν να επικοινωνήσουν και έστω ότι ο Α επιθυμεί να στείλει ένα μυστικό μήνυμα στον Β, θα πρέπει να κινηθούν ώς εξής:

- Επιλέγεται ένας συμμετρικός αλγόριθμος
- Επιλέγεται το συμμετρικό κλειδί
- Το κλειδί πρέπει να γίνει γνωστό και στους δύο: εάν το έχει επιλέξει ο Α, θα πρέπει να το αποστείλει εκ των προτέρων στον Β
- Ο Α κρυπτογραφεί το μήνυμα με τη χρήση του κλειδιού
- Ο Α αποστέλλει το κρυπτογραφημένο μήνυμα στον Β
- Ο Β αποκρυπτογραφεί το μήνυμα

Η συμμετρική κρυπτογραφία χαρακτηρίζεται από την απλότητά της, δεδομένου ότι απαιτεί την ύπαρξη ενός μόνο κλειδιού. Παρουσιάζει όμως ορισμένα σημαντικά προβλήματα.

Πρέπει να υπάρχει ένας ασφαλής δίαυλος για την αρχική μεταφορά του μυστικού κλειδιού. Αν το μυστικό κλειδί υποκλαπεί, τότε όλες οι επόμενες επικοινωνίες θα είναι επισφαλείς. Βασική προϋπόθεση επιτυχούς λειτουργίας είναι η ύπαρξη αμοιβαίας εμπιστοσύνης μεταξύ των δύο μερών. Όταν ένα συμμετρικό κλειδί αποκαλυφθεί, αυτό και κάθε μήνυμα που το χρησιμοποίησε για να κρυπτογραφηθεί έχει χάσει τα προνόμιά του. Ένα νέο κλειδί πρέπει να επιλεγεί και να διανεμηθεί.

Τα πράγματα γίνονται ακόμη πιο δύσκολα, αν ληφθεί υπ' όψη η αρχή της μη χρησιμοποίησης του ίδιου κλειδιού για παραπάνω από μια επικοινωνίες, έστω και αν αυτές γίνονται με το ίδιο πρόσωπο, δεδομένου ότι τότε αυξάνουν οι κίνδυνοι υποκλοπής του.

Τέλος, σε σχέση με τις βασικές αρχές ασφάλειας που προαναναφέρθηκαν στην εισαγωγή, η συμμετρική κρυπτογραφία δεν διασφαλίζει την επιβεβαίωση ταυτότητας, αλλά ούτε και την μη αποκήρυξη. Κάθε ένα από τα δύο μέρη έχει τη δυνατότητα να τροποποιήσει κακοβούλως τα δεδομένα (ενός μηνύματος ή μιας συναλλαγής), έχοντας συγχρόνως τη βεβαιότητα ότι ένας τρίτος δεν θα είναι σε θέση να προσδιορίσει τον ένοχο.

4.1.3 Ασύμμετρη Κρυπτογραφία

Απάντηση σε πολλά από τα προηγούμενα προβλήματα έρχονται να δώσουν τα συστήματα ασύμμετρης κρυπτογραφίας. Σε αντίθεση με την κρυπτογραφία μυστικού κλειδιού, η ασύμμετρη κρυπτογραφία ή όπως είναι πιο γνωστή, κρυπτογραφία δημοσίου κλειδιού **(Public key cryptography)**, είναι σχετικά πιο πρόσφατη. Οι αλγόριθμοι και τα συστήματα της κατηγορίας αυτής, σχεδιάστηκαν με κύριο σκοπό να δώσουν μια λύση στο πρόβλημα της ασφαλούς διανομής κλειδιού, που παρουσιάζε η συμμετρική κρυπτογραφία. Χαρακτηριστικό τους είναι η ύπαρξη ζεύγους κλειδιών, τα οποία έχουν την ιδιότητα να καθιστούν πρακτικά αδύνατο τον υπολογισμό του ενός κλειδιού γνωρίζοντας το άλλο. Ο πρώτος αλγόριθμος ασύμμετρης κρυπτογραφίας αναπτύχθηκε από τους **Diffie-Hellman** στα μέσα της δεκαετίας του **1970** και στηριζόνταν σε μαθηματικά διακρτών λογαρίθμων.

Σε αντίθεση με τους πολλούς διαθέσιμους συμμετρικούς αλγορίθμους κρυπτογραφίας, υπάρχουν μόνο δύο πρακτικοί αλγόριθμοι δημοσίου κλειδιού με μόνο τον ένα να εφαρμόζεται ευρέως. Αυτός που δεν εφαρμόζεται είναι ο **ElGamal**, ο οποίος είναι μη τυποποιημένος και χρησιμοποιεί μεταβλητά μήκη κλειδιών μεταξύ **512** και**1024.** Η χρήση του έχει περιοριστεί εξαιτίας μιας διαμάχης καταπάτησης του μοτίβου, με τους επινοητές, του **Diffie-Hellman** αλγορίθμου.

Ο πιο διαδεδομένος αλγόριθμος ασύμμετρης κρυπτογραφίας δημιουργήθηκε το **1977** από τους **Rivest, Shamir** και **Adleman,** καθηγητές του MIT,οι οποία βασίστηκαν σε αρχές της θεωρίας των πεπερασμένων πεδίων. Ο αλγόριθμος είναι γνωστός με το όνομα **RSA (**από τα αρχικά των δημιουργών του**)** έχει τύχει ευρείας υλοποίησης, ενώ ταυτόχρονα έχει αποδειχθεί εξαιρετικά ασφαλής, έχοντας αντισταθεί με επιτυχία σε πολλές επιθέσεις. Η ασφάλειά του έγκειται στη δυσκολία της παραγοντοποίησης **(factorization)** πολύ μεγάλων φυσικών αριθμών. Το μέγεθος των κλειδιών διαφέρει σημαντικά σε σχέση με αυτό ενός κλειδιού του συστήματος **DES.** Στο σύστημα **RSA** ένα κλειδί με μήκος **512 bit** θεωρείται αναξιόπιστο. Ένα με μήκος **768 bit** προσφέρει μέση ασφάλεια, ένα με **1.024 bit** καλή, ενώ ένα με μήκος **2.048 bit** θα παραμείνει απαραβίαστο για αρκετές δεκαετίες ακόμα, αν και με το ρυθμό ανάπτυξης της τεχνολογίας ποτέ δεν μπορεί να είναι κανείς σίγουρος.

Σήμερα χρησιμοποιεί κλειδιά μήκους τουλάχιστον **1024bits** και είναι πιθανόν ο πιο πολύπλοκος και απαιτητικός σε υπολογιστική ισχύ από όλους τους εν χρήσει κρυπτογραφικούς αλγορίθμους.

Επίσης πολύ γνωστός είναι ο αλγόριθμος ελλειπτικών καμπυλών **(Elliptic curve cryptography- ECC),** ο οποίος είναι σχετικά πιο πρόσφατος. Είναι λιγότερο πολύπλοκος και απαιτητικός σε σχέση με τον **RSA** και μπορεί να χρησιμοποιήσει μικρότερου μήκους κλειδιά, επιτυγχάνοντας το ίδιο επίπεδο ασφάλειας με τον **RSA.**

Για να γίνει πιο κατανοητή η σημασία του μήκους των κρυπτογραφικών κλειδιών σε σχέση με το επιδιωκόμενο επίπεδο ασφάλειας, παρατίθεται ο πιο κάτω πίνακας, στον οποίο απεικονίζονται συγκριτικά τα μήκη κλειδιών **(**σε **bits)** των διαφόρων αλγορίθμων, σε συνδυασμό με τον χρόνο που απαιτείται προκειμένου να επιτευχθεί η παραβίαση **("**σπάσιμο**")** του κλειδιού. Η υπόθεση που έχει γίνει είναι ότι υπάρχει διαθέσιμο ποσό **10** εκατ. δολλαρίων για αγορά εξοπλισμού **(**υπολογιστών**)** και ότι η μνήμη κοστίζει περίπου **0.5** δολ ανά MB.

Συμμετρικό κλειδί **DES**	Ασύμμετρο κλειδί **ECC**	Ασύμμετρο κλειδί **RSA**	Απαιτούμενος χρόνος	Πλήθος Μηχανών	Μνήμη
56	**112**	**420**	**5** λεπτά	**10.000**	Ελάχιστη
80	**160**	**760**	**600** μήνες	**4.300**	**4 GB**
96	**192**	**1020**	**3** εκατ. έτη	**114**	**170 GB**
128	**256**	**1620**	10^{16} έτη	**0,16**	**120 TB**

Από τον πίνακα αυτό μπορεί να γίνει αντιληπτό γιατί αρχίζει να εγκαταλείπεται ο αλγόριθμος **DES** με υποχρεωτικό σταθερό μήκος κλειδιού **56 bits,** καθώς και γιατί τα προτιμητέα μήκη κλειδιών στον αλγόριθμο **RSA** είναι πλέον **1024** και άνω. Εδώ θα άξιζε να αναφερθεί ότι όλοι οι κατασκευαστές λογισμικού ασύμμετρης κρυπτογράφησης υποστηρίζουν πολλαπλούς αλγόριθμους. Έτσι αν κάποια στιγμή βρεθεί ένα αδύνατο σημείο σε κάποιο αλγόριθμο, το οποίο επιτρέπει την παραβίασή του, υπάρχει πάντα η επιλογή της ενεργοποίησης ενός άλλου εναλλακτικού αλγορίθμου, ο οποίος να είναι ασφαλής.

4.1.4 Δημόσια και Ιδιωτικά κλειδιά

Οι ασύμμετροι αλγόριθμοι διαφέρουν από τους συμμετρικούς κατά ένα πολύ σημαντικό γεγονός. Όταν δημιουργείται ένα συμμετρικό κλειδί, το μόνο που χρειάζεται είναι να επιλεγεί ένας τυχαίος αριθμός με κατάλληλο μήκος **(bits)**. Αντίθετα, η δημιουργία ασύμμετρων κλειδών είναι πιο πολύπλοκη διαδικασία. Οι ασύμμετροι αλγόριθμοι ονομάζονται έτσι επειδή ακριβώς, αντί για τη χρήση ενός και μόνο κλειδιού για την εκτέλεση τόσο της κρυπτογράφησης όσο και της αποκρυπτογράφησης χρησιμοποιούνται δύο διαφορετικά κλειδιά: το ένα για την κρυπτογράφηση και το άλλο για την αποκρυπτογράφηση. Αυτά τα δύο διαφορετικά, αλλά μαθηματικώς συσχετιζόμενα κλειδιά δημιουργούνται πάντοτε μαζί και είναι γνωστά ως ζεύγος δημόσιου/ιδιωτικού κλειδιού **(public/private key-pair)**. Η διαδικασία είναι αρκετά διαφορετική και πιο περίπλοκη από την απλή επιλογή ενός τυχαίου αριθμού, αλλά εμπεριέχει πάντα την έννοια της τυχαιότητας. Όταν ολοκληρωθεί η δημιουργία ενός ασύμμετρου κλειδιού, υπάρχουν δύο κλειδιά: ένα δημόσιο **(public key)** και ένα ιδιωτικό **(private key)**.

Το ιδιωτικό πρέπει να παραμένει κρυφό, φυλασσόμενο με ασφάλεια. Σε κάποιες μάλιστα περιπτώσεις, ούτε ο κάτοχος του κλειδιού δεν έχει τη δυνατότητα να μάθει ποιό ακριβώς είναι το ιδιωτικό του κλειδί. Αντίθετα, το δημόσιο κλειδί είναι επιθυμητό να γίνει ευρέως γνωστό, ώστε να είναι διαθέσιμο σε κάθε ενδιαφερόμενο. Δεδομένου ότι είναι πρακτικά αδύνατος ο υπολογισμός του ιδωτικού κλειδιού, όταν είναι γνωστό το αντίστοιχο δημόσιο, η δημοσιοποίηση αυτή δεν δημιουργεί κινδύνους, ούτε θέτει σε αμφισβήτηση την ασφάλεια του συστήματος.

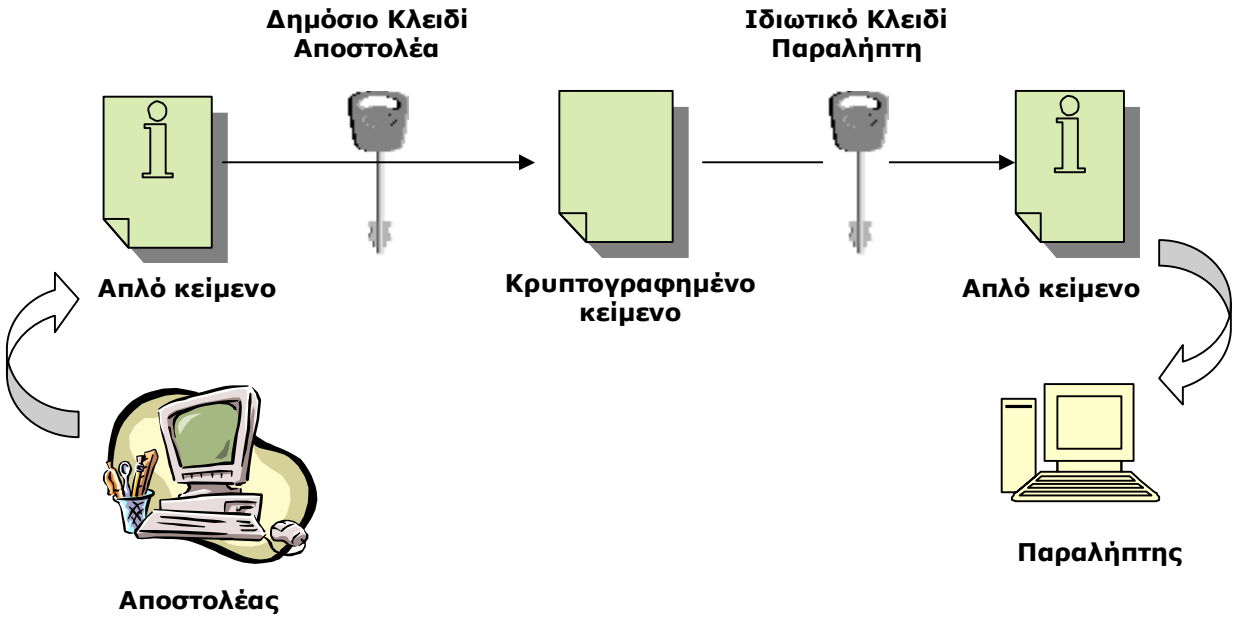
Τα ασύμμετρα κλειδιά έχουν την χαρακτηριστική ιδιότητα πως ότι κρυπτογραφείται με το ένα κλειδί μπορεί να αποκρυπτογραφηθεί με το άλλο, ενώ το ίδιο κλειδί **(**π.χ. το ιδιωτικό**)** δεν μπορεί να αποκρυπτογραφήσει ότι το ίδιο κρυπτογράφησε.

Επιπλέον πρέπει να είναι σαφές πως ότι κρυπτογραφήθηκε με το ένα μέλος του ζεύγους μπορεί να αποκρυπτογραφηθεί **ΜΟΝΟ** με το άλλο μέλος του ίδιου ζεύγους, ενώ οποιοδήποτε τρίτο κλειδί δοκιμαστεί, είναι βέβαιο ότι θα αποτύχει.

Όλα τα προηγούμενα γίνονται πολύ περισσότερο κατανοητά, αν σκεφτούμε ένα κουτί με μία κλειδαριά μέσα στο οποίο υπάρχει κλειδωμένο ένα έγγραφο. Για να διαβάσουμε το περιεχόμενο του εγγράφου, αρκεί να έχουμε το ίδιο κλειδί που χρησιμοποιήθηκε για να κλειδώσει το κουτί **(**συμμετρική κρυπτογραφία**)**. Εξάλλου, εάν το κουτί έχει δύο κλειδαριές, από τις οποίες η μια χρησιμοποιείται για το

κλείδωμα και η άλλη για το ξεκλείδωμα, τότε, για να διαβάσουμε το περιεχόμενο του εγγράφου, θα πρέπει να διαθέτουμε το κλειδί της δεύτερης κλειδαριάς (ασύμμετρη κρυπτογραφία). Ανεξαρτήτως του αριθμού των κλειδαριών (δηλαδή της μεθόδου κρυπτογράφησης), το κλειδί δεν είναι τίποτα άλλο παρά ένα κομμάτι μέταλλο με οδοντώσεις. Υπάρχει μόνο μία διαμόρφωση οδοντώσεων που ανοίγει το κουτί (κατάλληλη ακολουθία αριθμών). Εάν το κλειδί έχει λίγες οδοντώσεις, είναι σχετικά εύκολο να αντιγραφεί (αδύναμη κρυπτογράφηση). Εάν όμως έχει πολλές οδοντώσεις στην ιδανική περίπτωση άπειρες, τότε η αντιγραφή του είναι πολύ δυσκολότερη, έως και ακατόρθωτη (ισχυρή κρυπτογράφηση). Βλέπουμε λοιπόν ότι το πλήθος των αριθμών που αποτελούν ένα «κλειδί» είναι καθοριστικό για την ασφάλεια των πληροφοριών που κλειδώνουμε. Αυτό ακριβώς εκφράζει και το μήκος των κλειδιών που αναφέρεται σε διάφορα συστήματα και εκφράζεται σε **bit**.

Η λειτουργία του ασύμμετρου κλειδιού και γενικότερα της ασύμμετρης κρυπτογραφίας απεικονίζεται στο ΣΧΗΜΑ **6** που ακολουθεί.



ΣΧΗΜΑ 6 : Ασύμμετρη Κρυπτογραφία

Πιο συγκεκριμένα, υποθέτουμε ότι εξετάζουμε την επικοινωνία μεταξύ δύο εμπλεκομένων προσώπων, του Α και του Β, από τα οποία ο Α είναι ο αποστολέας ενός μηνύματος και ο Β ο παραλήπτης.

Ü Εφ' όσον γίνεται χρήση ασύμμετρης κρυπτογραφίας, κάθε ένας από τους δύο εμπλεκόμενους διαθέτει ήδη το δικό του ζεύγους δημόσιου/ ιδιωτικού κλειδιού **(A public/A private** για τον Α, **Bpu/Bpr** για τον Β**).** Η δημιουργία του ζεύγους κλειδιών στα σύγχρονα συστήματα κρυπτογραφημένης επικοινωνίας γίνεται με τη χρήση κατάλληλου λογισμικού.

Ü Ο Α, όπως και ο Β φυλάσει και δεν αποκαλύπτει σε κανέναν το ιδιωτικό **(private)** κλειδί του.

Ü Ο Α, όπως και ο Β δημοσιοποιεί, κοινοποιεί στους ενδιαφερόμενους το δημόσιο **(public)** κλειδί του. Αυτό μπορεί να γίνει είτε με απ' ευθείας αποστολή του **Apu** στον Β είτε μέσω κάποιου συστήματος δημόσιου καταλόγου.

Ü Ο Α αποκτά ένα αντίγραφο του δημόσιου κλειδιού του Β **(Bpu)** με ένα από τους τρόπους που αναφέρθηκαν.

Ü Ο Α κρυπτογραφεί το προς αποστολή μήνυμα, χρησιμοποιώντας το δημόσιο κλειδί του Β και στη συνέχεια αποστέλλει το κρυπτογραφημένο μήνυμα στον Β.

Ü Ο Β παραλαμβάνει το μήνυμα και χρησιμοποιώντας το δικό του ιδιωτικό κλειδί **(Bpr)** το αποκρυπτογραφεί. Σημειώνεται ότι, όπως προαναφέρθηκε, το ιδιωτικό κλειδί του Β είναι το μοναδικό κλειδί παγκοσμίως το οποίο μπορεί να εκτελέσει επιτυχώς αυτήν την αποκρυπτογράφηση.

Αν το ζητούμενο ήταν η αποστολή από τον Β ενός μηνύματος με παραλήπτη τον Α, η παραπάνω διαδικασία θα ακολουθείτο σε αντίστροφη κατεύθυνση, χωρίς ιδιαίτερες διαφοροποιήσεις. Προκύπτει βέβαια από όλα τα παραπάνω ότι για την πλήρη και αμφίδρομη επικοινωνία μεταξύ δύο μερών *απαιτείται η ύπαρξη και χρήση τεσσάρων συνολικά κλειδιών, δύο δημοσίων και δύο ιδιωτικών.*

4.1.5 Πλεονεκτήματα - Μειονεκτήματα

Σε σχέση με τη συμμετρική κρυπτογραφία, η ασύμμετρη παρουσιάζει μια σειρά πλεονεκτημάτων:

- Δεν απαιτείται η ύπαρξη ασφαλούς διαύλου για την αρχική μετάδοση του δημόσιου κλειδιού. Αν κάποιος (π.χ. το πρόσωπο Β παραπάνω) βρει ή υποκλέψει το δημόσιο κλειδί ενός προσώπου Α, μπορεί μεν να το χρησιμοποιήσει για να στείλει στον Α ένα ιδιωτικό μήνυμα, όχι όμως για να προσποιηθεί προς τρίτους ότι είναι ο Α ούτε για να αποκρυπτογραφήσει μηνύματα τρίτων που έχουν σταλεί στον Α κρυπτογραφημένα με το δημόσιου κλειδί του Α. Και τούτο διότι αυτά μπορούν να αποκρυπτογραφηθούν μόνο με τη χρήση του ιδιωτικού κλειδιού του Α, του οποίου μοναδικός κάτοχος και χρήστης είναι ο ίδιος ο Α. Από τα παραπάνω προκύπτει ότι ο Α μπορεί να στείλει στον Β το δημόσιο κλειδί του **(Apu)** είτε μέσω **e-mail** ή ακόμη και να το «δημοσιεύσει» σε ειδικές για το σκοπό αυτό ηλεκτρονικές υπηρεσίες καταλόγου **(public key directories)**.

- Ο Α δεν χρειάζεται να ανησυχεί για το αν ο Β, με τον οποίο επικοινωνεί (και κατά συνέπεια ο Β έχει λάβει γνώση του δημοσίου κλειδιού του Α) είναι «διπλός πράκτορας». Ο Β δεν είναι δυνατόν να επωφεληθεί από την υποκλοπή μηνυμάτων τρίτων προσώπων προς τον Α (αφού για την αποκρυπτογράφηση τους απαιτείται η γνώση του ιδιωτικού κλειδιού του Α), ούτε και να προσποιηθεί ότι είναι ο Α. Εξάλλου η εκχώρηση, από τον Β προς τρίτους του δημόσιου κλειδιού του Α δεν έχει κανένα νόημα, αφού (από τον σχεδιασμό του συστήματος) προορισμός του είναι ακριβώς να είναι γνωστό και διαθέσιμο σε κάθε ενδιαφερόμενο.

- Η χρήση των ασύμμετρων κλειδιών μπορεί να επεκταθεί με επιτυχία για να εξυπηρετήσει μεγάλους πληθυσμούς χρηστών. Αυτό οφείλεται στο γεγονός ότι κάθε χρήστης χρειάζεται να μοιραστεί με τους άλλους μόνο ένα κλειδί, το δικό του δημόσιου κλειδί. Το ίδιο ισχύει και για τους υπόλοιπους. Έτσι, για να επικοινωνήσουν τέσσερα πρόσωπα (έστω τα Α, Β, Γ, Δ) μεταξύ τους, χρειάζεται να κοινοποιηθούν μόνο τέσσερα κλειδιά, ενώ για την επικοινωνία μεταξύ **100** προσώπων χρειάζεται να κοινοποιηθούν αντίστοιχα **100** κλειδιά, σε αντίθεση με τα **9.900** κλειδιά που απαιτούνται κατά την χρήση συμμετρικών κλειδιών. Δηλαδή ο αριθμός των χρησιμοποιούμενων κλειδιών είναι ανάλογος του πλήθους των συμμετεχόντων στην επικοινωνία, ενώ στα συστήματα συμμετρικής

κρυπτογραφίας ο αριθμός των κλειδιών είναι ανάλογος του τετραγώνου των συμμετεχόντων. Κατά συνέπεια, οργανισμοί με μεγάλο πλήθος χρηστών δεν έχουν προβλήματα διαχείρισης υπερβολικού πλήθους κλειδιών. Όλοι όσοι χρειάζονται να στείλουν κρυπτογραφημένα μηνύματα σε ένα πρόσωπο Α, χρησιμοποιούν το ίδιο κλειδί: το δημόσιο κλειδί του Α.

- Μια ακόμη μη προφανής ωφέλεια που προκύπτει από τη χρήση συστημάτων δημόσιου / ιδιωτικού κλειδιού είναι ότι δεν απαιτείται να έχει κανείς εκ των προτέρων κάποια σχέση με κάποιον στον οποίο θέλει να απευθύνει ένα μήνυμα. Αυτό ήταν απαραίτητο στα συστήματα συμμετρικού κλειδιού, προκειμένου να καταστεί δυνατή η ανταλλαγή του συμμετρικού κλειδιού, στο οποίο θα βασιστεί στη συνέχεια η κρυπτογράφηση και η αποκρυπτογράφηση. Με το σύστημα δημόσιου / ιδιωτικού κλειδιού, ο αποστολέας απλώς εντοπίζει το δημόσιο κλειδί του παραλήπτη, κρυπτογραφεί το μήνυμα και το αποστέλλει. Ο παραλήπτης διαθέτει ήδη το ιδιωτικό του κλειδί με βάση το οποίο και αποκρυπτογραφεί το μήνυμα.

- Τέλος, λόγω της ασύμμετρης φύσης του συστήματος δημόσιου / ιδιωτικού κλειδιού, κάθε κάτοχος ενός τέτοιου ζεύγους κλειδιών είναι σε θέση να πραγματοποιεί μαθηματικές διεργασίες με το ιδιωτικό του κλειδί, τις οποίες κανείς άλλος παγκοσμίως δεν έχει τη δυνατότητα να εκτελέσει. Η παρατήρηση αυτή αποτελεί τη βάση για τις ψηφιακές υπογραφές **(digital signatures)** και τη διασφάλιση της δυνατότητας της μη-αποκήρυξης **(non-repudiation)**.

Βεβαίως, εκτός απο πλεονεκτήματα, η ασύμμετρη κρυπτογραφία παρουσιάζει και ορισμένα μειονεκτήματα.

- Κατ' αρχήν επειδή οι ασύμμετροι αλγόριθμοι έχουν πολύ μεγαλύτερες απαιτήσεις σε μαθηματικούς υπολογισμούς από ότι οι συμμετρικοί, με αποτέλεσμα να είναι συγκριτικά πιο αργοί και μάλιστα **10** έως **100** φορές πιο αργοί σε σχέση με αντίστοιχης κρυπτογραφικής ισχύος συμμετρικούς. Παρά το γεγονός ότι οι όποιες απαιτούμενες διαδικασίες υπολογισμών διεκπεραιώνονται σήμερα με τη βοήθεια ηλεκτρονικών υπολογιστών και τη χρήση κατάλληλων προγραμμάτων λογισμικού, η παραπάνω διαφορά αποκτά ιδιαίτερη σημασία, ιδίως αν τα προς κρυπτογράφηση (και αποκρυπτογράφηση) δεδομένα δεν είναι τα περιεχόμενα ενός μηνύματος λίγων γραμμών, αλλα πληροφορίες για ένα πολύ μεγάλο έργο,

όπως π.χ. κάποιο έργο γενετικής μηχανής. Οι συμμετρικοί όμως αλγόριθμοι έχουν ένα σοβαρό μειονέκτημα, εάν υποκλαπεί το κλειδί τους, μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση μηνυμάτων από μη εξουσιοδοτημένα άτομα. Από την άλλη, οι ασύμμετροι αλγόριθμοι είναι αρκετά ασφαλείς, εντούτοις πολύ περισσότερο αργοί.

Επιπλέον, με τη χρήση ασύμμετρων αλγόριθμων το μέγεθος του κρυπτογραφημένου μηνύματος είναι μεγαλύτερο από το αντίστοιχο αρχικό. Αυτό μπορεί να αποτελέσει ένα σοβαρό ζήτημα όταν χρησιμοποιούνται πολλαπλά επίπεδα κρυπτογράφησης. Π.χ. μια εφαρμογή λογισμικού κρυπτογραφεί δεδομένα **(**και επομένως διογκώνει το μέγεθός τους**)**, τα οποία στη συνέχεια αποστέλλονται μέσω μιας ασφαλούς σύνδεσης **Web (secure Web session)**, οπότε και πάλι θα διογκωθεί το μέγεθός τους. Εξάλλου είναι πιθανόν η αποστολή να γίνει μέσα από ένα κρυπτογραφημένο δίαυλο **(IPSec tunnel)**, με αποτέλεσμα την παραπέρα διόγκωση του μεγέθους των δεδομένων.

Είναι εμφανές από τα παραπάνω ότι κάθε ένα από τα δύο συστήματα κρυπτογραφίας παρουσιάζει πλεονεκτήματα και μειονεκτήματα. Μάλιστα είναι χαρακτηριστικό ότι υπάρχει μια συμπληρωματικότητα, με την έννοια ότι όπου υπερτερεί το ένα υστερεί το άλλο. Επομένως θα ήταν δυνατό να γίνει ένας συνδυασμός των δύο που να εκμεταλλεύεται τα πλεονεκτήματα του καθενός, χωρίς να κληρονομεί τα αντίστοιχα μειονεκτήματα. Ένας τέτοιος συνδυασμός θα πρέπει να συγκεντρώνει τις εξής ιδιότητες:

- Η προσφερόμενη λύση να είναι ασφαλής
- Η κρυπτογράφηση να είναι ταχεία
- Το κρυπτογραφημένο κείμενο να είναι συμπαγές
- Η λύση να μπορεί να επεκταθεί για την εξυπηρέτηση μεγάλων πληθυσμών
- Η λύση να μην είναι ευάλωτη ως προς την υποκλοπή του κλειδιού
- Η λύση να μην απαιτεί προϋπάρχουσα σχέση μεταξύ των δύο μερών
- Η λύση να μπορεί να υποστηρίξει ψηφιακές υπογραφές και μη-αποκήρυξη

Η συνδυασμένη αυτή χρήση συμμετρικής και ασύμμετρης κρυπτογραφίας περιγράφεται στο ακόλουθο παράδειγμα. Ο αποστολέας **(**έστω Α**)** δημιουργεί ένα τυχαίο συμμετρικό κλειδί, το οποίο και χρησιμοποιείται για την κρυπτογράφηση του μηνύματος. Το ζήτημα είναι πως θα μεταφερθεί το κλειδί αυτό στον

παραλήπτη (έστω Β). Αυτό επιτυγχάνεται με αξιοποίηση της ασύμμετρης κρυπτογραφίας και με εντοπιστμό του δημόσιου κλειδιού του παραλήπτη με τη βοήθεια κάποιου καταλόγου δημοσίων κλειδιών. Το δημόσιο κλειδί του παραλήπτη χρησιμοποιείται για την κρυπτογράφηση του συμμετρικού κλειδιού. Βεβαίως η ασύμμετρη κρυπτογραφία είναι αργή, αλλά δεδομένου ότι το συμμετρικό κλειδί είναι πολύ μικρού μεγέθους **(128bits)**, αυτό δεν αποτελεί πρόβλημα. Το αποτέλεσμα είναι ένα τυχαίο συμμετρικό κλειδί κρυπτογραφημένο (προστατευμένο) με τη βοήθεια ενός ασύμμετρου κλειδιού. Το τελευταίο βήμα είναι η επισύναψη του προστατευμένου συμμετρικού κλειδιού στο κρυπτογραφημένο μήνυμα, έτσι ώστε τα δύο μαζί να αποτελούν ένα αντικείμενο προς αποστολή και το οποίο είναι γνωστό ως ψηφιακός φάκελος **(digital envelope)**.

Στη συνέχει ο ψηφιακός φάκελος αποστέλλεται στον παραλήπτη μέσω του **Internet**. Το πρώτο βήμα μετά την παραλαβή είναι ο διαχωρισμός που περιεχομένου του ψηφιακού φακέλου και η ανάκτηση αφ' ενός του κρυπτογραφημένου μηνύματος και αφ' ετέρου του προστατευμένου συμμετρικού κλειδιού. Ο παραλήπτης χρησιμοποιεί το δικό του ιδωτικό κλειδί για την ανάκτηση/ αποκρυπτογράφηση του συμμετρικού κλειδιού. Τέλος, με τη χρήση του συμμετρικού κλειδιού αποκρυπτογραφεί το κείμενο του μηνύματος. Το συμμετρικό κλειδί δεν είναι πλέον χρήσιμο και μπορεί να αχρηστευτεί.

Κίνδυνος υποκλοπής του μηνύματος δεν υφίσταται, ακόμη και αν κάποιος τρίτος αποκτήσει πρόσβαση στον ψηφιακό φάκελο, ενώ αυτός βρίσκεται καθ' οδόν προς τον παραλήπτη. Ο πιθανός υποκλοπέας δεν μπορεί σε καμμία περίπτωση να επωφεληθεί, δεδομένου ότι θα πρέπει να λάβει γνώση του συμμετρικού κλειδιού, το οποίο όμως είναι κρυπτογραφημένο και είναι δυνατόν να αποκωδικοποιηθεί μόνο με το ιδιωτικό κλειδί του παραλήπτη, το οποίο είναι ούτως ή άλλως απόρρητο.

Παρ' όλα αυτά η μέθοδος αυτή παρουσιάζει το εξής πρόβλημα: Ένας τρίτος μπορεί να εντοπίσει το δημόσιο κλειδί του παραλήπτη Β (μέσω καταλόγου) και στη συνέχεια να δημιουργήσει ένα συμμετρικό κλειδί, με το οποίο να κρυπτογραφήσει ένα τελείως διαφορετικό μήνυμα, το οποίο και να αποστείλλει στον Β με τη μορφή ψηφιακού φακέλου όπως παραπάνω. Ο Β θα παραλάβει τον ψηφιακό φάκελο, θα αποκωδικοποιήσει το συμμετρικό κλειδί με χρήση του δικού του ιδιωτικού κλειδιού και τέλος θα αποκρυπτογραφήσει το μήνυμα με το

συμμετρικό κλειδί. Το μήνυμα όμως αυτό δεν έχει καμμία σχέση με το πραγματικών αναμενόμενο και βεβαίως δεν έχει προέλθει από τον Α.

Προκύπτει επομένως πρόβλημα πιστοποίησης της ταυτότητας του αποστολέα. Η απάντηση στο πρόβλημα αυτό μπορεί να δοθεί με τη βοήθεια των ψηφιακών υπογραφών, οι οποίες προϋποθέτουν τη χρήση των λεγομένων αλγορίθμων κατατεμαχισμού **(hash algorithms).** Τα θέματα αυτά εξετάζονται στη συνέχεια.

4.2 Ψηφιακές υπογραφές (Digital Signatures)

Τα πλεονεκτήματα της ασύμμετρης κρυπτογραφίας είναι προφανή, ωστόσο υπάρχει ένα σοβαρό ζήτημα που χρήζει ιδιαίτερης αντιμετώπισης. Ας υποτεθεί ότι παραλαμβάνουμε ένα μήνυμα ή αρχείο από το χρήστη με ηλεκτρονική διεύθυνση **name@company.com**. Υπό φυσιολογικές συνθήκες δεν έχουμε λόγο να πιστέψουμε ότι ο αποστολέας δεν είναι πράγματι ο αληθινός κάτοχος της συγκεκριμένης διεύθυνσης. Ωστόσο, ένας άλλος, κακόβουλος χρήστης, μπορεί, εάν θέλει, να χρησιμοποιήσει ένα κατάλληλο πρόγραμμα **(e-mail faker)**, για να στείλει αυτό το μήνυμα με διεύθυνση αποστολέα **name@company.com**. Με άλλα λόγια, έχει τη δυνατότητα να προβεί σε ηλεκτρονική πλαστοπροσωπία, για λόγους που μάλλον δεν θα είναι προς το συμφέρον μας (π.χ., μπορεί να είναι ανταγωνιστής και να προσπαθεί να αποσπάσει επιχειρηματικά μυστικά). Πώς μπορούμε να είμαστε βέβαιοι ότι το **e-mail** που λάβαμε το έχει στείλει ο νόμιμος κάτοχος της διεύθυνσης και όχι κάποιος άλλος;

Η αδυναμία που μόλις περιγράψαμε ξεπερνιέται με τη βοήθεια των ψηφιακών υπογραφών **(digital signatures)**, τις οποίες μπορούμε να σκεπτόμαστε ως το ηλεκτρονικό ισοδύναμο των χειρόγραφων υπογραφών. Οι ψηφιακές υπογραφές προσδιορίζουν τον υπογράφοντα και δηλώνουν μια σχέση ανάμεσα σε αυτόν και το υπογεγραμμένο έγγραφο. Ουσιαστικά, μια ψηφιακή υπογραφή είναι ορισμένα δεδομένα που συνοδεύουν ή συσχετίζονται λογικά με ένα ψηφιακά κωδικοποιημένο μήνυμα και τα οποία δεδομένα μπορούν να χρησιμοποιηθούν για να εξακριβωθεί, τόσο ο αποστολέας του μηνύματος, όσο και το ότι το μήνυμα δεν έχει κατά οποιονδήποτε τρόπο αλλοιωθεί, αφ' ότου έπαυσε να είναι υπό τον έλεγχο του αποστολέα. Όπως έχει ήδη προαναφερθεί, μια τέτοια υπογραφή είναι στην ουσία το αποτέλεσμα που παράγεται από μία μαθηματική διαδικασία που έχει κάποια ιδιαίτερα χαρακτηριστικά. Η ασφάλειά της στηρίζεται στη χρήση της ασύμμετρης κρυπτογραφίας, όπου η κρυπτογράφηση και η αποκρυπτογράφηση χρησιμοποιούν διαφορετικά κλειδιά η κάθε μία. Έτσι μια ψηφιακή υπογραφή παρέχει ισχυρή απόδειξη στον παραλήπτη ενός ψηφιακά υπογεγραμμένου μηνύματος ότι το περιεχόμενο του μηνύματος δεν έχει αλλοιωθεί.

Πριν δούμε όμως πως υλοποιείται στην πράξη, είναι σκόπιμο να αναφερθούμε στις συναρτήσεις κατατεμαχισμού **(hash)**. Πρόκειται για μηχανισμούς οι οποίοι στην είσοδό τους δέχονται ένα οσοδήποτε μεγάλο ή μικρό μήνυμα, ενώ στην έξοδο δίνουν ένα αλφαριθμητικό σταθερού μήκους. Το ενδιαφέρον με τις συναρτήσεις **hash** είναι η εξαιρετική **"ευαισθησία"** που έχουν στο περιεχόμενο του μηνύματος

εισόδου. Εάν αυτό μεταβληθεί στο παραμικρό, τότε το αλφαριθμητικό εξόδου διαφέρει σημαντικά από το προηγούμενο. Εφαρμόζοντας, για παράδειγμα, μια γνωστή υλοποίηση συνάρτησης **hash** στο αλφαριθμητικό **"e-banking"** παίρνουμε ως αποτέλεσμα το αλφαριθμητικό **8966f01c4a3f9a06ac 9dc99c658fe0c8**, ενώ της λέξης **"e-Banking" (**κεφαλαίο **"B")** είναι το **4fa944c3c8520f5b6edc0516e7065f08** εντελώς διαφορετικά**!** Αξίζει να παρατηρηθεί ότι, αν και θεωρητικά είναι δυνατόν να δώσουμε σε μια συνάρτηση **hash** δύο διαφορετικά μηνύματα και να πάρουμε το ίδιο αλφαριθμητικό, στην πράξη είναι αστρονομικά απίθανο να βρούμε ένα τέτοιο ζεύγος μηνυμάτων εισόδου.

Οι αλγόριθμοι **hash** που χρησιμοποιούνται στην κρυπτογραφία σχεδιάζονται έτσι ώστε να διαθέτουν ορισμένες ειδικές ιδιότητες:

- Ο αλγόριθμος δεν μπορεί να εκτελεστεί με αντίστροφη κατεύθυνση και να αποκαλύψει έστω και μέρος του αρχικού μηνύματος

- Ο αλγόριθμος δεν παρουσιάζει συγκρούσεις **(collisions):** έτσι είναι υπολογιστικά αδύνατη η ύπαρξη δύο διαφορετικών μηνυμάτων με το ίδιο αποτύπωμα.

- Το προκύπτον αποτύπωμα **(digest)** δεν αποκαλύπτει τίπ**ο**τε σε σχέση με το αρχικό μήνυμα.

- Είναι πρακτικά αδύνατο να δημιουργηθεί **/** ανακαλυφθεί κείμενο, το οποίο να παράγει ένα συγκεκριμένο επιθυμητό αποτύπωμα. Αυτό εμποδίζει οποιονδήποτε τρίτο να υποκαταστήσει ένα μήνυμα χωρίς να προκαλέσει ασυμφωνία στο αποτύπωμα.

Οι συνηθέστερα χρησιμοποιούμενοι αλγόριθμοι είναι ο **MD5** της **RSA,** ο οποίος παράγει αποτύπωμα **(digest)** μεγέθους **128 bits** και προορίζεται για χρήση σε επεξεργαστές **32-bits (**σε αντίθεση με τον παλαιότερο **MD2,** που είχε αναπτυχθεί για χρήση σε επεξεργαστές **8-bits)** και ο **SHA-1 (Secure Hash Algorithm),** με αποτύπωμα **160bits** και ο οποίος απευθύνεται επίσης σε σύγχρονους μεγάλης ισχύος επεξεργαστές.

Πώς όμως υλοποιούνται οι ψηφιακές υπογραφές; Ας υποθέσουμε ότι ο κάτοχος της διεύθυνσης **name@company.com** θέλει να στείλει ένα μήνυμα (έστω ***M***) και ο παραλήπτης να είναι βέβαιος ότι προήλθε από εκείνον και όχι από κάποιον... παραχαράκτη. Τότε ο ιδιοκτήτης της υπό συζήτηση ηλεκτρονικής διεύθυνσης, δεν έχει παρά να υπογράψει το ***M***. Προς τούτο, τροφοδοτεί αρχικά το μήνυμα σε μια συνάρτηση **hash**, έστω ***h***, παίρνοντας στην έξοδο το αλφαριθμητικό ***h(M)***, τη λεγόμενη σύνοψη μηνύματος (**message digest**, μπορούμε να το θεωρούμε ως δακτυλικό αποτύπωμα). Στη συνέχεια, ο αποστολέας κρυπτογραφεί το ***h(M)*** με το μυστικό του κλειδί μ, λαμβάνοντας έτσι το **ciphertext** $s=\mu(h(M))$. Στην ουσία, ο αποστολέας μόλις δημιούργησε την υπογραφή ***s*** του μηνύματος **M** που πρόκειται να αποστείλει, την οποία και θα επισυνάψει στο **e-mail** (θα αποστείλει, δηλαδή, το ζεύγος **<*M*, *s*>**). Όταν ο παραλήπτης το λάβει, για να επικυρώσει την ταυτότητα του αποστολέα, αρχικά βρίσκει το δημόσιο κλειδί του αποστολέα, το δ. Εν συνεχεία, χρησιμοποιώντας την ίδια συνάρτηση **h**, υπολογίζει το ***h(M)*** και το συγκρίνει με το $\delta(s)$, δηλαδή με το $\delta(\mu(h(M)))$, που δεν είναι τίποτα άλλο από τη σύνοψη του μηνύματος που του έστειλε ο αποστολέας (από τη στιγμή που αποστολέας και παραλήπτης χρησιμοποιούν το ίδιο σύστημα κρυπτογράφησης, η συνάρτηση **h** δεν αλλάζει). Εάν ισχύει $h(M)=\delta(s)$, ο παραλήπτης δέχεται την υπογραφή ως έγκυρη. Σε διαφορετική περίπτωση συμπεραίνει ότι η υπογραφή ***s*** δεν είναι του αποστολέα, καθώς και ότι το μήνυμα ***M*** μεταβλήθηκε καθ' οδόν. Με την παραπάνω διαδικασία ο παραλήπτης βεβαιώνεται για τρία πράγματα.

Πρώτον, ότι το **e-mail** προήλθε από τον συγκεκριμένο αποστολέα, αφού μόνο εκείνος θα μπορούσε να υπολογίσει την υπογραφή ***s***, καθώς είναι ο μοναδικός κάτοχος του μυστικού κλειδιού μ.

Δεύτερον, από τη στιγμή που ο αποστολέας υπόγραψε το μήνυμα ***M***, αυτό δεν θα μπορούσε να αλλάξει στο παραμικρό, αφού τότε θα άλλαζε και το ***h(M)*** που θα υπολόγιζε ο παραλήπτης, επομένως η υπογραφή ***s*** θα ήταν άκυρη ($h(M)=\delta(s)$).

Τρίτον, ο αποστολέας δεν μπορεί να ισχυριστεί ότι δεν τα έγραψε, αφού ανά πάσα στιγμή μπορούν να του δείξουν ότι $h(M)=\delta(s)$ (αρκεί, βεβαίως, να έχει φυλάξει ο παραλήπτης κάπου το μήνυμα **M** και την υπογραφή ***s***). Τέλος, περιττό να αναφέρουμε ότι όποτε το επιβάλλουν οι συνθήκες, μπορούμε να κρυπτογραφούμε και ταυτόχρονα να υπογράφουμε μηνύματα.

Μόλις είδαμε πώς μπορούμε με χρήση των ψηφιακών υπογραφών να βεβαιωνόμαστε ότι ένα μήνυμα που λάβαμε από κάποιο χρήστη, προήλθε πράγματι από αυτόν. Αντίστροφα, όταν εμείς στέλνουμε μηνύματα και θέλουμε να βεβαιώνουμε τους παραλήπτες για την ταυτότητά μας, μπορούμε να τα υπογράφουμε, ακολουθώντας την προηγούμενη διαδικασία.

Είναι προφανές ότι η ψηφιακή υπογραφή δεν έχει καμμία σχέση με το όνομα του αποστολέα, αλλά ούτε και με την χειρόγραφη υπογραφή του. Στην πραγματικότητα είναι ένας μετασχηματισμός του ίδιου του μηνύματος, ο οποίος ενσωματώνει ένα "μυστικό" γνωστό μόνο στον αποστολέα. Κατά συνέπεια είναι άρρηκτα συνδεδεμένο και με τον αποστολέα, αλλά και με το μήνυμα το οποίο υπογράφει. Είναι επίσης προφανές ότι, σε αντίθεση με την χειρόγραφη υπογραφή, η ψηφιακή υπογραφή ενός υπογράφοντος θα είναι διαφορετική για κάθε μήνυμα **(**ψηφιακό έγγραφο**)** που υπογράφει. Οι ψηφιακές υπογραφές μπορούν να ανταποκριθούν στις λειτουργικές απαιτήσεις του νόμου εξίσου καλά με τις φυσικές υπογραφές, παρουσιάζουν όμως σε σχέση με αυτές σημαντικές διαφορές.

Κατ' αρχήν, η ίδια η ψηφιακή υπογραφή δεν παρέχει επαρκή μαρτυρία για την ταυτότητα του υπογράφοντος. Για να εξασφαλιστεί αυτό, απαιτείται επιπλέον μαρτυρία, η οποία να συνδέει το κλειδί υπογραφής με τον ίδιο τον υπογράφοντα. Κάτι τέτοιο θα μπορούσε να αποδειχθεί με την επίκληση εξωτερικής μαρτυρίας, όπως συμβαίνει και με τις χειρόγραφες υπογραφές. Συνήθως όμως στην πράξη, ο παραλήπτης ενός ψηφιακά υπογεγραμμένου εγγράφου επιθυμεί να είναι σε θέση να στηριχθεί στην υπογραφή χωρίς επιπλέον ελέγχους. Στο σημείο αυτό υπεισέρχονται οι Αρχές Πιστοποίησης **(**βλέπε **§4.2.1)**, οι οποίες εκδίδουν τα ψηφιακά πιστοποιητικά, τα οποία πληροφορούν για την ταυτότητα του κατόχου και το δημόσιο κλειδί που χρησιμοποιείται, προκειμένου να επαληθευτεί η υπογραφή του σε κάποιο έγγραφο. Έχει ασφαλώς προηγηθεί από την πλευρά της Αρχής Πιστοποίησης ο έλεγχος όλων εκείνων των στοιχείων που διασφαλίζουν την αυθεντικότητα της ταυτότητας του κατόχου του πιστοποιητικού, καθώς και ότι αυτός κατέχει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που περιλαμβάνεται στο πιστοποιητικό. Το πιστοποιητικό χρησιμοποιείται από τον παραλήπτη, προκειμένου αυτός να βεβαιωθεί για την ταυτότητα του υπογράφοντος. Μια άλλη διαφορά είναι ότι στη διαδικασία της φυσικής υπογραφής, ο υπογράφων πρέπει να παρίσταται ο ίδιος και να έχει το προς

υπογραφεί έγγραφο εμπρός του. Αντίθετα, στη διαδικασία της ψηφιακής υπογραφής υπάρχουν οι εξής δύο δυνατότητες:

- Το κλειδί υπογραφής βρίσκεται αποθηκευμένο στον υπολογιστή του υπογράφοντος και η υπογραφή τίθεται με την ενεργοποίηση κάποιας επιλογής σε ένα πρόγραμμα λογισμικού
- Το κλειδί υπογραφής βρίσκεται αποθηκευμένο σε κάποια ειδική συσκευή (π.χ. **Smart Card)** η οποία πρέπει να είναι παρούσα και διαθέσιμη, ώστε το πρόγραμμα λογισμικού να επισυνάψει την υπογραφή.

Εύκολα γίνεται αντιληπτό πως ένας τρίτος που πιθανόν να έχει πρόσβαση, είναι δυνατόν να υπογράψει εκείνος. Κατα συνέπεια, μια ψηφιακή υπογραφή θα έπρεπε ίσως να αντιμετωπιστεί ως κάτι ανάλογο με μια σφραγίδα προτυπωμένης υπογραφής.

Γενικά, προκειμένου ένα μήνυμα να διαβιβαστεί με ασφάλεια από τον αποστολέα στον παραλήπτη και να έχει ο δεύτερος βέβαιη γνώση για την ταυτότητα του αποστολέα, δεν αρκεί το μήνυμα να υπογραφεί ψηφιακά από τον αποστολέα, αλλά θα πρέπει και ο παραλήπτης να είναι σε θέση να επαληθεύσει την ψηφιακή υπογραφή που συνοδεύει το μήνυμα, δηλαδή να μπορεί να βεβαιωθεί για την ταυτότητα του αποστολέα.

Ας δούμε τώρα τι γίνεται στην περίπτωση που ένα άτομο Α συνδιαλέγεται με το άτομο Β σε πραγματικό χρόνο. Πώς μπορεί ο Α να είναι βέβαιος ότι καθ' όλη τη διάρκεια της συνομιλίας τους θα μιλάει στον ίδιο το Β και όχι σε κάποιον άλλο; (Στη θέση του Β θα μπορούσε να ήταν μια τράπεζα, ένα βιβλιοπωλείο **on-line** κ.λπ.). Εάν ο Β του έστελνε ένα υπογεγραμμένο μήνυμα (π.χ., "Ελα Α, εγώ είμαι ο Β"), τότε θα βεβαιωνόταν μόνο για το γεγονός ότι τη στιγμή που του έστειλε το μήνυμα, ήταν όντως εκείνος που το έγραφε. Εάν, όμως, ένας **cracker** κατορθώσει και υποκλέψει ολόκληρο το μήνυμα, καθώς και την υπογραφή, τότε θα μπορέσει να τα χρησιμοποιήσει αργότερα, για να υποδυθεί τον **Β.** Το πρόβλημα, λοιπόν, είναι ότι κάθε φορά που μιλάει ο Α με τον Β σε πραγματικό χρόνο, θέλω να είναι βέβαιος ότι μιλάει μαζί του και όχι με κάποιον **cracker.** Με άλλα λόγια, χρειάζεται έναν τρόπο επικύρωσης του χρήστη **(user authentication)**, κάτι το οποίο δεν μπορεί να γίνει με απλή χρήση ψηφιακών υπογραφών.

Θα δούμε πώς μπορεί να επιτευχθεί. Πριν αρχίσει ο Α να συνομιλεί σε πραγματικό χρόνο με τον Β, παράγει με χρήση ενός κατάλληλου προγράμματος

έναν τυχαίο αριθμό (έστω *τ*) και του τον στέλνει. Στη συνέχεια, εκείνος δημιουργεί ένα μήνυμα που λέει κάτι σαν "Ελα Α, ο Β είμαι και μόλις μου έστειλες το *τ*, τι ακαταλαβίστικα πράγματα είναι αυτά;", το οποίο υπογράφει και του το στέλνει (το σημαντικό εδώ είναι να περιλαμβάνεται στο μήνυμα ο τυχαίος αριθμός *τ*). Όταν ο Α λάβει το μήνυμα με τον τυχαίο αριθμό που μόλις πριν παρήγαγε, μαζί με την ψηφιακή υπογραφή, είναι πλέον βέβαιος ότι μιλάει με τον Β και με κανέναν άλλο. Ο τυχαίος αριθμός *τ* ονομάζεται πρόκληση **(challenge)**. Η μη προβλεψιμότητά του σε συνδυασμό με μια ψηφιακή υπογραφή, παρέχει το ζητούμενο μηχανισμό επικύρωσης χρήστη. Βεβαίως, εννοείται ότι και ο Β μπορεί να χρησιμοποιήσει το μηχανισμό αυτό για να επικυρώσει την ταυτότητά του Α.

Συμπερασματικά ένα σύστημα κρυπτογράφησης και ψηφιακών υπογραφών, εξασφαλίζει σε μεγάλο βαθμό την ασφαλή διακίνηση μηνυμάτων. Δεν παρέχει όμως πλήρη προστασία απέναντι σε κάθε κακόβουλη προσπάθεια τρίτων. Στη σειρά των ενεργειών κατά τη φάση της επαλήθευσης από τον παραλήπτη της ψηφιακής υπογραφής του αποστολέα , παρατηρούμε τα εξής:

1. Ο παραλήπτης εντοπίζει το δημόσιο κλειδί του αποστολέα, μέσω κάποιου καταλόγου δημοσίων κλειδιών
2. Ο παραλήπτης χρησιμοποιεί αυτό το κλειδί για την αποκρυπτογράφηση του κρυπτογραφημένου αποτυπώματος
3. Το κρυπτογραφημένο αποτύπωμα δημιουργήθηκε από τον αποστολέα με χρήση ιδιωτικού του κλειδιού
4. Ο αποστολέας έχει στην κατοχή του το ένα και μοναδικό αντίγραφο του ιδιωτικού του κλειδιού
5. Επομένως αν το κρυπτογραφημένο αποτύπωμα **digest.1** και το επανυπολογισθέν αποτύπωμα **digest.2** ταυτίζονται, τότε το μήνυμα πρέπει να προέρχεται από τον αποστολέα.

Ο κίνδυνος εντοπίζεται στο σημείο (1.): όπου αν ένας τρίτος αποκτήσει πρόσβαση στον κατάλογο, θα μπορούσε να τοποθετήσει το δικό του δημόσιο κλειδί στη θέση του κλειδιού του αποστολέα, δημιουργώντας μια εγγραφή στον κατάλογο, η οποία δίπλα στο όνομα του αποστολέα θα αναφέρει το δημόσιο κλειδί του τρίτου προσώπου (ψευδώς). Στη συνέχεια έχει τη δυνατότητα να δημιουργεί μηνύματα, τα οποία να τα υπογράφει με το δικό του (δηλ. του τρίτου προσώπου)

ιδιωτικό κλειδί και τα οποία μετά να τα αποστέλλει στον παραλήπτη, προσποιούμενος ότι είναι ο αποστολέας.

Όταν ο παραλήπτης προσπαθήσει να αποκρυπτογραφήσει το πλαστό μήνυμα (την πλαστότητα του οποίου αγνοεί), θα ανακτήσει από τον κατάλογο το δημόσιο κλειδί του αποστολέα, λαμβάνοντας όμως ψευδώς το δημόσιο κλειδί του τρίτου προσώπου. Τα υπόλοιπα βήματα θα εκτελεστούν με "επιτυχία" (ταύτιση αποτυπωμάτων **digest1** και **digest2** κλπ), αφήνοντας τον παραλήπτη με την εσφαλμένη εντύπωση ότι έλαβε ένα μήνυμα υπογεγραμμένο από τον αποστολέα.

Επομένως το ζήτημα που ανακύπτει είναι ότι αναμφίβολα απαιτείται ένας μηχανισμός που να διασφαλίζει με απόλυτη βεβαιότητα ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει σε ένα συγκεκριμένο πρόσωπο.

4.2.1 Αρχές Πιστοποίησης

Με δεδομένο το ρόλο του δημόσιου κλειδιού στα πλαίσια της ασύμμετρης κρυπτογραφίας, το κύριο ζητούμενο είναι ένας αξιόπιστος μηχανισμός για τη διανομή των κλειδιών αυτών. Ο μηχανισμός αυτός δεν μπορεί παρά να στηρίζεται στη σύνδεση ενός δημόσιου κλειδιού με ορισμένες πληροφορίες που προσδιορίζουν την ταυτότητα του κατόχου του. Ο συνδυασμός αυτός δημιουργεί τη λεγόμενη "ψηφιακή ταυτότητα" **(digital identity)** ή όπως είναι πιο γνωστό, το "ψηφιακό πιστοποιητικό" **(digital certificate)**. Τα ψηφιακά πιστοποιητικά αποτελούν το ψηφιακό ανάλογο των κλασσικών ταυτοτήτων και αποτελούν τη βάση για τη δημιουργία ενός ασφαλούς ηλεκτρονικού περιβάλλοντος, διότι επιτρέπουν τη διασφάλιση ενός επιπέδου εμπιστοσύνης, σχετικά με το ποιός είναι ο πραγματικός κάτοχος ενός δεδομένου δημοσίου κλειδιού.

Ας υποθέσουμε τώρα ότι παίρνουμε το δημόσιο κλειδί του ατόμου Α από κάποιον κατάλογο **on-line**, ώστε να το χρησιμοποιούμε για να του στέλνουμε κρυπτογραφημένα μηνύματα, τα οποία μόνο εκείνος θα μπορεί να διαβάζει (αφού μόνο εκείνος έχει το αντίστοιχο μυστικό κλειδί). Πώς, όμως, μπορούμε να είμαστε βέβαιοι ότι το κλειδί που πήραμε όντως ανήκει στον Α; Βλέπετε, εάν υποθέσουμε ότι ένας **cracker** γνωρίζει τα στοιχεία του Α, τότε ίσως έχει βάλει το δικό του δημόσιο κλειδί στη θέση του Α. Κάθε φορά, λοιπόν, που εμείς θα στέλνουμε ένα **e-mail** στη διεύθυνση **name@company.com**, ο **cracker** θα μπορεί να το υποκλέπτει και να το διαβάζει, αφού στην ουσία θα το έχουμε κρυπτογραφήσει με το δικό του δημόσιο κλειδί. Το ηθικό δίδαγμα που προκύπτει είναι ότι ένα σύστημα κρυπτογράφησης από μόνο του δεν είναι τόσο χρήσιμο, εάν δεν υπάρχει

και μια υπεύθυνη αρχή (ή αρχές) διαχείρισης των δημόσιων κλειδιών. Μια τέτοια αρχή θα πρέπει να είναι σε θέση να διασφαλίζει ότι το δημόσιο κλειδί ***δ1*** αντιστοιχεί στο χρήστη ***x1***, το δημόσιο κλειδί *δ2* στο χρήστη ***x2*** κ.λπ. Η αντιστοίχηση ενός χρήστη στο δημόσιο κλειδί του παρέχεται από ένα πιστοποιητικό. Τα πιστοποιητικά διανέμει η λεγόμενη Αρχή Πιστοποίησης **(Certification Authority** ή **CA)**, που δεν είναι τίποτα άλλο από έναν έμπιστο οργανισμό ή μια εταιρεία. Μια τέτοια Αρχή έχει την ευθύνη της δημιουργίας, της διανομής, της ανάκλησης και γενικά της διαχείρισης των πιστοποιητικών. Έτσι, εάν ο Α επιθυμεί ένα πιστοποιητικό, αρχικά θα απευθυνθεί σε μια Αρχή Πιστοποίησης, όπως είναι η **VeriSign (**www.verisign.com**)**. Η Αρχή θα ελέγξει με κάποιον τρόπο την ταυτότητα του Α, καθώς και ότι το δημόσιο κλειδί *δ* που προσκομίζει του ανήκει πραγματικά. Ακολουθεί η σύνταξη ενός κειμένου, το οποίο θα περιλαμβάνει στοιχεία που αφορούν τον Α (π.χ., ονοματεπώνυμο, διεύθυνση κατοικίας, **e-mail** κ.λπ.), το κλειδί *δ*, καθώς και άλλα χρήσιμα στοιχεία, όπως, π.χ., η ημερομηνία κατά την οποία η ισχύς του πιστοποιητικού εκπνέει **(expiration date)**. Εν συνέχεια, η Αρχή Πιστοποίησης υπογράφει το έγγραφο με το δικό της μυστικό κλειδί, δημιουργώντας έτσι το πιστοποιητικό του Α. Τώρα, εάν εμείς θέλουμε το δημόσιο κλειδί του Α, καθώς και να επιβεβαιώσουμε ότι είναι δικό του, τότε παίρνουμε πρώτα το πιστοποιητικό του Α από έναν κατάλογο **on-line**. Επαληθεύουμε την ψηφιακή υπογραφή της Αρχής Πιστοποίησης και αν είναι εντάξει, είμαστε πλέον βέβαιοι ότι το κλειδί που πήρα πράγματι ανήκει στον Α. Τέλος, ο λόγος για τον οποίο οι χρήστες εμπιστεύονται μια κάποια Αρχή Πιστοποίησης έγκειται, συνήθως, στο γεγονός ότι κάποιος άλλος φορέας εγγυάται για την αξιοπιστία της. Για τον τελευταίο φορέα μπορεί να εγγυάται κάποιος άλλος κ.λπ. Έχουμε, λοιπόν, μια αλυσίδα εμπιστοσύνης **(chain of trust)**, στη ρίζα της οποίας **(root)** υπάρχει μια καθολικά αποδεκτή Αρχή.

Το **PGP (Pretty Good Privacy)** είναι ένα σύστημα κρυπτογράφησης δημόσιου κλειδιού, το οποίο αναπτύχθηκε το **1991** στις ΗΠΑ από τον τότε μηχανικό λογισμικού, Φιλ Τσίμερμαν. Μέχρι το **1999**, η εξαγωγή κρυπτογραφικού υλικού σε ηλεκτρονική μορφή εκτός της χώρας απαγορευόταν, αφού οι τεχνολογίες του είδους είχαν χαρακτηριστεί "πυρομαχικά". Ωστόσο, χάρη στην εθελοντική πρωτοβουλία **PGP International (**εν συντομία **PGPi)**, το πρόγραμμα διαδόθηκε ευρέως σε ολόκληρο τον κόσμο, ήδη από το **1997**. Κάθε φορά που κυκλοφορούσε στις ΗΠΑ μια νέα έκδοση του **PGP**, οι άνθρωποι που συμμετείχαν στην πρωτοβουλία αγόραζαν από την Αμερική βιβλία με τον πηγαίο κώδικα του

προγράμματος και τα έστελναν στην Ευρώπη. Στη συνέχεια, τα βιβλία σαρώνονταν σελίδα προς σελίδα, περνούσαν από πρόγραμμα **OCR**, και όταν ο πηγαίος κώδικας είχε μεταφερθεί ολόκληρος στον υπολογιστή, μεταγλωττίζονταν.

Σήμερα στις ΗΠΑ έχουν χαλαρώσει οι περιορισμοί εξαγωγών κρυπτογραφικού υλικού, γεγονός που μεταξύ άλλων σημαίνει ότι το **PGP** μπορεί πλέον να εξάγεται και σε ηλεκτρονική μορφή. Ωστόσο, το **project PGPi** συνεχίζει να έχει τον έλεγχο της διανομής των εκδόσεων του προγράμματος στον υπόλοιπο κόσμο, μαζί με τον πηγαίο κώδικα.

Θα πρέπει να επιλέξουμε αν θα στείλουμε το δημόσιο κλειδί μας σε κάποιο διακομιστή κλειδιών, ώστε άλλοι χρήστες να μπορούν εύκολα να το παίρνουν και να μας στέλνουν κρυπτογραφημένα δεδομένα. Εναλλακτικά, για να διανέμουμε το κλειδί στα άτομα που μας ενδιαφέρουν άμεσα, μπορούμε, απλά, να το επισυνάπτουμε στα **e-mail** που τους στέλνουμε. Πάντως, ακόμα και αν δεν στείλουμε άμεσα το δημόσιο κλειδί μας σε κάποιο διακομιστή, μπορούμε να το κάνουμε αργότερα. Το **PGP** για **Windows** έρχεται μαζί με κατάλληλο **plug-in**, ώστε να συνεργάζεται με το **Outlook**. Εδώ είμαστε έτοιμοι να στείλουμε το πρώτο μας **e-mail**, το οποίο θα είναι κρυπτογραφημένο και υπογεγραμμένο. Αφού δημιουργήσουμε το ζεύγος κλειδιών, μια καλή ιδέα είναι να εξαγάγουμε **(export)** το δημόσιο κλειδί μας σε ένα αρχείο κειμένου, ώστε να μπορούμε να το διανέμουμε εύκολα. Αρκεί να επιλέξουμε το χρήστη που μας ενδιαφέρει εν προκειμένω τον εαυτό μας, να κάνουμε δεξί κλικ πάνω του και να πάμε στο **[Export...]**. Την πρώτη φορά που θα κλείσουμε το παράθυρο **"PGPkeys"**, το πρόγραμμα θα μας προτρέψει να αποθηκεύσουμε το ζεύγος κλειδιών που μόλις δημιουργήσαμε σε ένα ασφαλές μέρος: αν έπειτα από "χτύπημα" του δίσκου χάσουμε το ζεύγος κλειδιών, τότε τα δεδομένα που έχουμε σε κρυπτογραφημένη μορφή θα μας είναι παντελώς άχρηστα.

Κατά τη διαδικασία εξαγωγής, θα παρατηρήσουμε να γίνεται λόγος για δύο δακτυλίους κλειδιών **(key ring)**: τον ιδιωτικό και το δημόσιο. Στον ιδιωτικό κρατούνται όλα τα ιδιωτικά κλειδιά που έχουμε στην κατοχή μας, ενώ στο δημόσιο όλα τα δημόσια **(**ανήκουν σε άλλους χρήστες**)**. Σε πολλές περιπτώσεις έχει νόημα να διαθέτουμε περισσότερα από ένα ζεύγη κλειδιών. Το ένα θα το χρησιμοποιούμε, π.χ., για την προσωπική μας αλληλογραφία και το άλλο για την επαγγελματική, όπου κατά πάσα πιθανότητα τα χρησιμοποιούμενα κλειδιά θα έχουν μεγαλύτερο μήκος **(**σε **bit)**, επομένως είναι και δυσκολότερο να παραβιαστούν.

4.3 Τοίχοι Προστασίας (Firewalls)

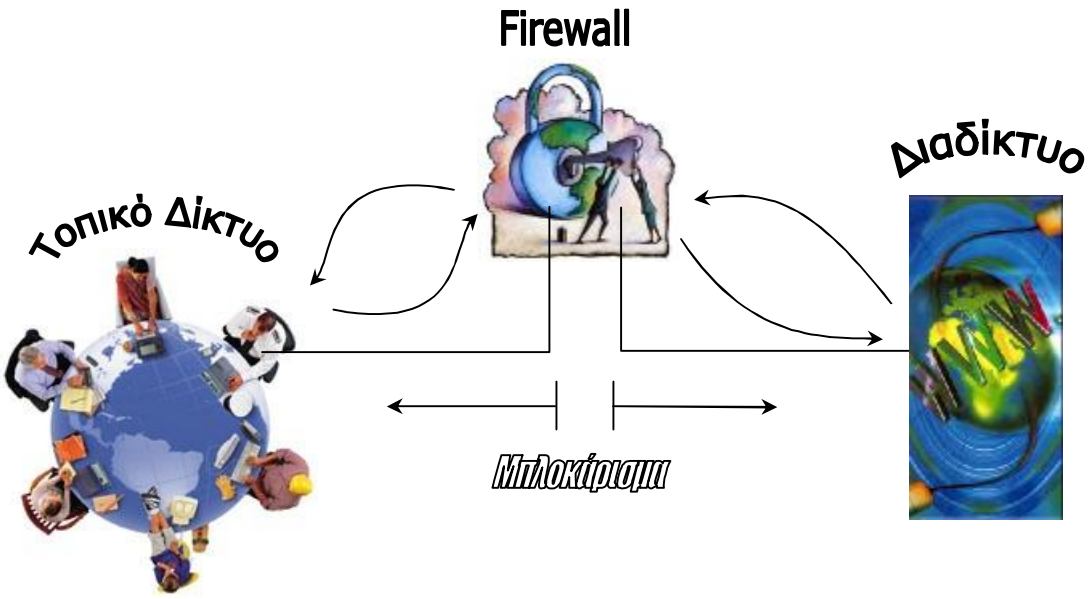
Οι τοίχοι προστασίας **(firewalls)** αποτελούν μία πολύ αποτελεσματική μέθοδο προστασίας δικτύου. Στην ουσία πρόκειται για ένα σύστημα σχεδιασμένο να κάνει το δίκτυο προσβάσιμο με προσεκτικά ελεγχόμενους και παρακολουθούμενους τρόπους. Ένα σύστημα **firewall** επιτυγχάνει δύο στόχους: Παρέχει στους ανθρώπους της εταιρείας πρόσβαση στον παγκόσμιο ιστό, χωρίς ταυτόχρονα να επιτρέπει σε όλο τον κόσμο να κρυφοκοιτά και δεύτερον μπορεί να υψωθεί μεταξύ ενός ανέμπιστου τμήματος λογισμικού, του δημόσιου εξυπηρετητή ιστού και των ευαίσθητων πληροφοριών που ανήκουν στο ιδιωτικό δίκτυο της.

Στις κατασκευές κτιρίων, ο τοίχος προστασίας είναι σχεδιασμένος ώστε να εμποδίζει την εξάπλωση φωτιάς από το ένα μέρος του κτιρίου στο άλλο. Κάτι αντίστοιχο πραγματοποιείται με την τοποθέτησή του ανάμεσα στο εξωτερικό και εσωτερικό δικτυακό περιβάλλον μιας εταιρείας. Η βασική ιδέα ενός **firewall** είναι γενικά απλή. Σε ένα παραδοσιακό ανοιχτό σύστημα, όλοι οι κεντρικοί υπολογιστές στο δίκτυο τοπικής περιοχής **(Local Area Network - LAN)** έχουν άμεση πρόσβαση στο Διαδίκτυο και είναι ισοδύναμα ευάλωτοι σε επιθέσεις από έξω. Η ασφάλεια του τοπικού δικτύου εξαρτάται από την ασφάλεια του πιο αδύναμου κεντρικού υπολογιστή. Ένας απλός ανασφαλής κεντρικός υπολογιστής θα επιτρέψει σε ένα εισβολέα να εισέλθει. Όταν εισέλθει είναι εύκολο κλέβοντας τους λογαριασμούς νομίμων χρηστών, αντικαθιστώντας το λογισμικό του συστήματος με αντίγραφα και με άλλα τέτοια τεχνάσματα,να ανατρέψει άλλους κεντρικούς υπολογιστές στο χώρο. Όχι μόνο είναι δύσκολο να προστατευθεί ένα ανοιχτό σύστημα από επίθεση αλλά είναι δύσκολο να ανιχνευθεί η προσβολή του.

Τα **firewalls** αντιμετωπίζουν αυτό το πρόβλημα παρεμβάλλοντας μία ειδικά διαμορφωμένη μηχανή πύλης **(gateway)** ανάμεσα στον έξω κόσμο και στο εσωτερικό δίκυο του χώρου. Η άμεση επαφή μεταξύ των κεντρικών υπολογιστών του εσωτερικού δικτύου και του εξωτερικού κόσμου απαγορεύεται. Αντίθετα όλη η κίνηση πρέπει πρώτα να πάει στην πύλη όπου το λογισμικό αποφασίζει αν η κίνηση μπορεί να επιτραπεί ή να απορριφθεί. Αυτό διαιρεί αποτελεσματικά το δίκτυο σε ένα "εσωτερικό" έμπιστο δίκτυο **(**δηλαδή το τοπικό**)** και σε ένα "εξωτερικό" ανέμπιστο δίκτυο **(**δηλαδή το διαδίκτυο**)**. Η ζώνη συνόρων μεταξύ των εσωτερικών και εξωτερικών δικτύων είναι γνωστή σαν "περίμετρος ασφάλειας". Τώρα η δουλειά προστασίας του τοπικού δικτύου γίνεται πιο απλή καθώς αντί να προστατεύεται ένα ετερογενές σύνολο μεμονωμένων κεντρικών

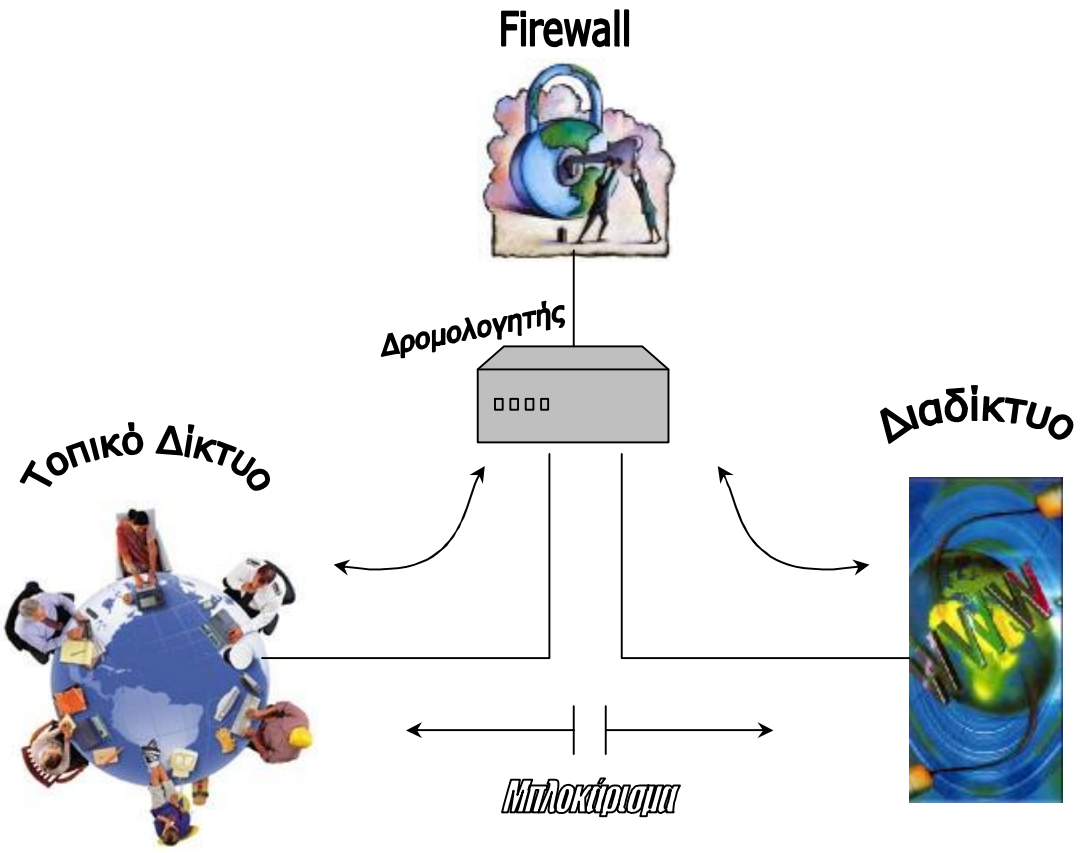
υπολογιστών από προσβολή, οι προσπάθειες επικεντρώνονται στην προστασία της απλής μηχανής πύλης του δικτύου. Αν η πύλη δικτύου είναι ασφαλής, το τοπικό δίκτυο είναι ασφαλές.

Υπάρχουν δύο βασικές υλοποιήσεις για συστήματα **firewalls**. Στην προσέγγιση "πύλη διπλής στέγης" **(**ΣΧΗΜΑ **7)** η μηχανή του **firewall** που ονομάζεται "οχυρή θέση", έχει δύο κάρτες δικτύου, μία που συνδέεται με το εσωτερικό δίκτυο και μία που συνδέεται με το ανέμπιστο δίκτυο. Η μηχανή έχει ρυθμιστεί έτσι ώστε τα πακέτα δικτύου που φθάνουν στη μία κάρτα να μη βασίζονται στην άλλη. Εξ ορισμού τα δύο δίκτυα είναι εντελώς απομονωμένα. Παρόλα αυτά, επειδή υπάρχει πάντα η ανάγκη κάποιας επικοινωνίας μεταξύ των εσωτερικών και των εξωτερικών δικτύων, ειδικά προγράμματα, που ονομάζονται "μεσολαβητές" **(proxies)**, τρέχουν στη μηχανή **firewall**. Η δουλειά ενός μεσολαβητή είναι να προωθήσει επιλεκτικά πληροφορίες από το ένα δίκτυο στο άλλο. Οι μεσολαβητές μπορούν να καθορίσουν ποιά πακέτα δικτύου να προωθήσουν κοιτάζοντας τις διευθύνσεις προέλευσης και προορισμού, εξετάζοντας τον τύπο πακέτου, εξετάζοντας τις θύρες προέλευσης και προορισμού ή ακόμη ελέγχοντας τα περιεχόμενα που υπάρχουν μέσα στο πακέτο. Τα πακέτα δικτύου ποτέ δεν μεταφέρονται άμεσα. Τα δεδομένα τους εξάγονται και ξαναπακετάρονται σε νέα πακέτα πριν μεταφέρουν τις πληροφορίες τους μέσω της πύλης δικτύου.



Σχημα 7 : Firewall σύμφωνα με την προσέγγιση "Πύλη διπλής στέγης"

Στην προσέγγιση ¨διαχωριστικού κεντρικού υπολογιστή πύλης" **(**ΣΧΗΜΑ **8)** ένας δρομολογητής δικτύου χρησιμοποιείται για να ελέγξει την πρόσβαση στο εσωτερικό δίκτυο. Ο δρομολογητής περιορίζει την επικοινωνία μεταξύ των εξωτερικών και εσωτερικών δικτύων διασφαλίζοντας ότι τα δικτυακά πακέτα που ξεκινούν μέσα από το εξωτερικό δίκτυο μπορούν να φτάσουν μόνο όταν η καλά ασφαλισμένη μηχανή της οχυρής θέσης τα εξετάσει και με την παρουσία των μεσολαβητών, που τα ξαναμεταδίδουν στο εσωτερικό δίκτυο. Στις περισσότερες περιπτώσεις, οι μηχανές στο εσωτερικό δίκτυο είναι εντελώς αόρατες στο εξωτερικό. Τα εξωτερικά πακέτα από το εσωτερικό δίκτυο είτε περιορίζονται στη μηχανή τοίχου προστασίας, όπου πάλι πρέπει να συνοδευτούν στο διαδίκτυο μέσω ενός προγράμματος μεσολάβησης ή επιτρέπεται να περάσουν άμεσα μέσω του δρομολογητή, αφού ικανοποιήσουν ορισμένους κανόνες φιλτραρίσματος για να προσδιορίσουν ότι είναι ασφαλή.



Σχημα 8 : Firewall σύμφωνα με την προσέγγιση **"** διαχωριστικού κεντρικού υπολογιστή πύλης"

Σε ένα καλά σχεδιασμένο σύστημα **firewall,** δεν υπάρχει καμία ουσιαστική διαφορά ανάμεσα στα συστήματα διπλής στέγης και διαχωριστικού κεντρικού υπολογιστή. Σε κάθε περίπτωση το εσωτερικό δίκτυο εμφανίζεται στον έξω κόσμο να περιέχει μία απλή καλά προστατευμένη μηχανή, τον κεντρικό υπολογιστή οχυρής θέσης. Όλη η εξερχόμενη κίνηση από το εσωτερικό δίκτυο στον έξω κόσμο εμφανίζεται να ξεκινά από την οχυρή θέση και όλη η εισερχόμενη κίνηση απευθύνεται σε αυτή τη θέση. Το λογισμικό στο οχυρό θέσης ελέγχει κάθε κομμάτι δεδομένων δικτύου που φτάνει, το καταγράφει και του επιτρέπει να περάσει αν ικανοποιεί το σύνολο κανόνων και ρυθμίσεων που έχουν οριστεί από τους διαχειριστές του **firewall.**

Πολλοί οργανισμοί έχουν εγκαταστήσει συστήματα **firewalls** που δεν είναι καθόλου **firewalls.** Είναι δρομολογητές δικτύου που έχουν διαμορφωθεί να σταματούν την επικίνδυνη κυκλοφορία δικτύου ενώ επιτρέπουν να προχωρήσει η ασφαλής κυκλοφορία του δικτύου. Αυτού του είδους το σύστημα μπορεί να είναι δύσκολο να διαχειριστεί αποτελεσματικά λόγω της δυσκολίας του να δημιουργήσει αποτελεσματικούς κανόνες φιλτραρίσματος. Ακόμη και μία φαινομενικά αβλαβής αλλαγή σε ένα πίνακα δρομολόγησης μπορεί να έχει αθέλητες επιδράσεις. Επειδή οι δρομολογητές δεν έχουν σχεδιαστεί βασικά για σκοπούς ασφάλειας, συνήθως δεν καταγράφουν τη δραστηριότητα του δικτύου, κάνοντας δύσκολο το να προσδιοριστεί αν το σύστημα δουλεύει κανονικά ή ακόμη και αν έχει προσβληθεί.

Η ουσία μιας πολιτικής ασφάλειας ενός **firewall** έχει ενσωματωθεί στα φίλτρα που επιτρέπουν ή απαγορεύουν τη δίοδο στην κυκλοφορία δικτύου. Τα προγράμματα μεσολάβησης έρχονται σε δύο εκδόσεις. Υπάρχουν μεσολαβητές **"επιπέδου εφαρμογής",** που έχουν γραφτεί για συγκεκριμένα πρωτόκολλα επικοινωνίας. Για παράδειγμα ένας μεσολαβητής επιπέδου εφαρμογής θα είναι υπεύθυνος για την προώθηση **HTTP** αιτήσεων μπρος και πίσω πάντα μέσω του **firewall,** ένας άλλος υπεύθυνος για **FTP** αιτήσεις και ένας τρίτος υπεύθυνος για το ηλεκτρονικό ταχυδρομείο. Επειδή οι μεσολαβητές επιπέδου εφαρμογής καταλαβαίνουν το νόημα των πληροφοριών τις μεταδίδουν μπρος πίσω και μπορούν να εφαρμόσουν κανόνες φιλτραρίσματος με βάση τα περιεχόμενα των δικτυακών πακέτων. Για παράδειγμα, αν μια εταιρεία αποφασίσει να προστατεύσει τους υπαλλήλους της από πιθανούς κινδύνους **ActiveX** ελέγχων, θα μπορούσε να στήσει ένα **HTTP** μεσολαβητή για να εξετάσει κάθε **HTML** σελίδας που περνά την οχυρή θέση και να διαγράψει αθόρυβα τις αναφορές σε **ActiveX.** Οι μεσολαβητές

επιπέδου εφαρμογής μπορούν επίσης να φιλτράρουν την κυκλοφορία δικτύου από τις **IP** διευθύνσεις των πλευρών αποστολής και παραλαβής, τις θύρες δικτύου σε οποιαδήποτε πλευρά της σύνδεσης και άλλα χαρακτηριστικά των επικεφαλίδων των πακέτων δικτύου.

Σε αντίθεση με τους μεσολαβητές επιπέδου εφαρμογής είναι οι μεσολαβητές "επιπέδου κυκλώματος", προγράμματα γενικού σκοπού που φέρονται στα πακέτα δικτύου σαν σε πολλά μαύρα κουτιά που θα προωθηθούν μέσω της οχυρής θέσης ή όχι. Αυτού του είδους ο μεσολαβητής μπορεί να φιλτράρει μόνο τη βάση της πληροφορίας επικεφαλίδας στα πακέτα δικτύου. Οι μεσολαβητές επιπέδου κυκλώματος μπορούν να απαγορέψουν πακέτα δικτύου που προέρχονται από απαγορευμένες πηγές, αλλά δεν μπορούν να κρυφοκοιτάξουν μέσα στο πακέτο να δουν αν ένα πακέτο, που φαίνεται νόμιμο, κρύβει μια επικίνδυνη δραστηριότητα. Το κύριο πλεονέκτημα των μεσολαβητών επιπέδου κυκλώματος είναι η γενικότητα και η ταχύτητά τους. Ένας μεσολαβητής μπορεί να διαχειριστεί πολλά πρωτόκολλα και είναι πιο γρήγοροι διότι η εργασία τους είναι είναι λιγότερο έντονη υπολογιστικά.

Σε όλους τους τύπους των συστημάτων **firewalls**, η ασφάλεια του εσωτερικού δικτύου εξαρτάται από την ασφάλεια του κεντρικού υπολογιστή οχυρής θέσης. Κάποιος που αποκτά πρόσβαση στον τοίχο προστασίας ή είναι ικανός να επαναδιαμορφώσει τα μέτρα ασφαλείας, το πιο πιθανό είναι να μπορεί να εισέλθει και σε άλλες μηχανές στο τοπικό δίκτυο. Σε συστήματα διαχωριστικού κεντρικού υπολογιστή, ο δρομολογητής είναι επίσης ένας πιθανός αδύνατος σύνδεσμος. Για να εμποδιστεί η έκθεση είτε της οχυρής θέσης είτε του κεντρικού υπολογιστή, τα **firewalls** είναι ειδικά διαμορφωμένα και διαχωρισμένα. Τυπικά, εκτελούν μία "σκληραγωγημένη" έκδοση των **UNIX** και **NT** λειτουργικών συστημάτων, από τις οποίες έχουν αφαιρεθεί διάφορα τρωτά σημεία. Τα **firewalls** δεν εκτελούν αχρείαστες υπηρεσίες, δεν περιέχουν ανέμπιστο λογισμικό και κρατούν μια ασφαλή καταγραφή όλης της δραστηριότητας.

4.3.1 Επιλέγοντας ένα σύστημα Firewall

Αυτό που ακολουθεί είναι μία λίστα με τα σημαντικότερα χαρακτηριστικά που πρέπει να σκεφτεί ένας υποψήφιος αγοραστής ενός συστήματος **firewall.**

- ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ. Τα προϊόντα **firewalls** που είναι διαθέσιμα εκτελούνται και στα δύο συστήματα **UNIX** και **Windows NT.** Κανένα από τα δύο λειτουργικά συστήματα δεν έχει πλεονέκτημα απέναντι στο άλλο. Στις περισσότερες περιπτώσεις οι προμηθευτές **firewalls** έχουν τροποποιήσει το λειτουργικό σύστημα, για να σκληραγωγηθεί και να το κάνουν πιο ανθεκτικό απέναντι στις επιθέσεις. Πρέπει να σημειώσουμε πως δεν είναι απαραίτητο για ένα δίκτυο που είναι αρχικά βασισμένο στα **Windows** να έχει ένα **Windows firewall.** Παρόλα αυτά είναι αναμφίβολα σημαντικό να επιλεγεί ένα τέτοιο σύστημα που ο διαχειριστής του θα νιώθει άνετα να διαχειριστεί.
- ΧΕΙΡΙΣΜΟΣ ΠΡΩΤΟΚΟΛΛΩΝ. Τα συστήματα **firewalls** αναπόφευκτα μένουν πίσω από την αιχμή της τεχνολογίας. Όλα τα **firewalls** θα χειριστούν **FTP,** ηλεκτρονικό ταχυδρομείο, **HTTP, NNTP, TELNET** και άλλα κοινά πρωτόκολλα, αλλά μπορεί να μην είναι ικανά να χειριστούν νέα ή ασυνήθιστα πρωτόκολλα όπως τα **Pointcast, SNMP** ή **RealAudio.** Αν επομένως απαιτείται να περάσετε ένα νέο πρωτόκολλο τηλεσυνδιάσκεψης μέσω του **firewall** πρέπει να έχετε σιγουρευτεί ότι το σύστημα μπορεί να το χειριστεί.
- ΤΥΠΟΙ ΦΙΛΤΡΩΝ. Τα φίλτρα δικτύου, που βασίζονται σε μεσολαβητές επιπέδου εφαρμογής, δίνουν εκτεταμένο έλεγχο σε οτιδήποτε περνά μέσω του **firewall.** Είναι επίσης, ικανά να αναλύσουν τα περιεχόμενα των δεδομένων και να τα τροποποιήσουν αν χρειάζεται. Το μειονέκτημα είναι, ότι αυτή η σε βάθος ανάλυση κουβαλά μια επιβάρυνση απόδοσης, η οποία μπορεί να είναι αξιοσημείωτη σε περιβάλλον που ήδη έχει βαριά κυκλοφορία δικτύου.

Τα συστήματα που βασίζονται σε μεσολαβητές επιπέδου κυκλώματος έχουν καλύτερη απόδοση και τα συστήματα φιλτραρίσματος πακέτων ακόμη καλύτερη. Παρόλα αυτά και τα δύο συστήματα μπορούν να συντονίσουν συνδέσεις μόνο στη βάση των διευθύνσεων προορισμού και αποστολής, τις θύρες προορισμού και άλλους συντελεστές της **TCP/IP** επικεφαλίδας.

- ΚΑΤΑΓΡΑΦΗ ΗΜΕΡΟΛΟΓΙΟΥ. Ένα καλό **firewall** πραγματοποιεί εξαντλητική καταγραφή ημερολογίου. Έρχεται επίσης με εργαλεία που αναλύουν και συνοψίζουν τα αρχεία του ημερολογίου έτσι ώστε να ανιχνεύσουν ασυνήθιστη δραστηριότητα.

Ü ΔΙΑΧΕΙΡΙΣΗ. Τα περισσότερα **firewalls** παρέχουν ένα μηχανισμό απομακρυσμένης διαχείρισης αφού προηγουμένως πιστοποιήσουν προσεκτικά τον διαχειριστή.

Ü ΑΠΛΟΤΗΤΑ. Τα καλά συστήματα **firewalls** είναι απλά. Οι μεσολαβητές είναι μικροί, εύκολοι να κατανοηθούν και μπορούν να επαληθευτούν με επιθεώρηση. Κάποιες εταιρείες κάνουν ακόμη και τον πηγαίο κώδικα του συστήματός τους διαθέσιμο για δημόσια επιθεώρηση, ένα σημάδι της αυτοπεποίθησής τους στο λογισμικό τους.

Ü ΔΙΟΧΕΤΕΥΣΗ ΜΕΣΩ ΚΡΥΠΤΟΓΡΑΦΙΚΟΥ ΚΑΝΑΛΙΟΥ. Μερικά συστήματα **firewalls** παρέχουν την ικανότητα εγκατάστασης ενός κρυπτογραφικού καναλιού μέσω του διαδικτύου για να συνδεθούν με ασφάλεια δύο δίκτυα σε ένα απλό "εικονικό ιδιωτικό δίκτυο". Αυτός μπορεί να είναι ένας χρήσιμος τρόπος να συνδεθούν δύο γραφεία υποκαταστημάτων ή συνεργάτες και μπορεί να είναι πιο φθηνός από τον εναλλακτικό τρόπο της εκμίσθωσης μίας αφοσιωμένης γραμμής τηλεφώνου γι' αυτό το σκοπό.

4.3.2 Αδυναμίες των συστημάτων Firewalls

Τα **firewalls** είναι γεγονός ότι προσφέρουν υψηλού επιπέδου προστασία απέναντι στους κινδύνους που προέρχονται από το διαδίκτυο. Υπάρχουν όμως και κίνδυνοι από τους οποίους τα **firewalls** αδυνατούν να μας προστατέψουν. Μερικές τέτοιες αδυναμίες τους είναι οι επόμενες:

- Το **firewall** δεν μπορεί να εμποδίσει τους εσωτερικούς κινδύνους

Μπορεί να έχει την δυνατότητα να ελέγχει τα δεδομένα που εισέρχονται και εξέρχονται του δικτύου δεν μπορεί όμως να εμποδίσει κάποιον από την εταιρεία (ή κάποιον που κατάφερε να μπει μέσα στα γραφεία της εταιρείας) να αντιγράψει δεδομένα σε δισκέττα, **Cd**, ή ακόμη και σε χαρτί και να τα μεταφέρει τελικά εκτός της εταιρείας. Εάν ο εισβολέας βρεθεί πίσω και από το **firewall** τότε το **firewall** δεν μπορεί να τον ελέγξει, ούτε ασφαλώς να τον εμποδίσει.

- Δεν μπορεί να ελέγξει οτιδήποτε δεν περνάει από μέσα του.

Το **firewall** παρακολουθεί και ελέγχει όλη την κίνηση που διέρχεται από μέσα του αλλά αδυνατεί να κάνει τα ίδια για τα δεδομένα εκείνα που δεν περνούν από το ίδιο.

- Δεν μπορεί να προστατέψει το σύστημα από νέες απειλές.

Κανένα **firewall** δεν έχει τη δυνατότητα να ασφαλίσει το δίκτυο και τα δεδομένα, από καινούργιες απειλές. Η τοποθέτηση του δεν σημαίνει ότι το συγκεκριμένο σύστημα ασφαλείας εξασφαλίζει μόνιμη και διαρκή προστασία. Άλλωστε κανείς δεν μπορεί να γνωρίζει τι μορφή και τι δυνατότητες θα έχουν οι μελλοντικοί κίνδυνοι.

- Δεν μπορεί να προστατέψει το σύστημα από ιούς.

Τα **firewalls** δεν είναι πλέον αποκλειστικό προνόμιο των εταιρικών δικτύων. Ο απλός χρήστης έχει αρκετές επιλογές για να εξασφαλίσει σε ένα μεγάλο βαθμό την ακεραιότητα του υπολογιστή του. Με την εγκατάσταση ενός **Antivirus** στον υπολογιστή σας, μειώνετε δραματικά την πιθανότητα εισβολής κάποιου ιού, σκουληκιού ή δούρειου ίππου. Με κανέναν όμως τρόπο δεν αποτρέπετε κακόβουλους **hacker** ή καλύτερα **cracker** από το να δοκιμάσουν να διεισδύσουν στον υπολογιστή σας χωρίς την έγκρισή σας. Για να εξασφαλιστείτε όσο το δυνατόν περισσότερο, θα πρέπει να εγκαταστήσετε στο **PC** σας κάποιο **firewall.** Θα πρέπει βέβαια να αναφέρουμε ότι δεν προσφέρουν απόλυτη προστασία. Εάν, για παράδειγμα, το πανάκριβο **firewall** της **Microsoft** "τρύπησε", το ίδιο μπορεί να γίνει, αρκετά πιο εύκολα μάλιστα, και στα **PC** μας. Βέβαια, η **Microsoft** και κάθε άλλος εταιρικός δικτυακός τόπος είναι επώνυμοι στόχοι και είναι φυσικό να προσελκύουν το ενδιαφέρον των απανταχού **cracker**, ενώ ο απλός χρήστης είναι στην κυριολεξία σταγόνα μέσα στον ωκεανό. Παρ' όλα αυτά, υπάρχουν δυστυχώς αρκετοί ερασιτέχνες και ημιεπαγγελματίες οι οποίοι "σκανάρουν" το **Internet** για να βρουν "ανοιχτές πόρτες" στους υπολογιστές μας.

Εάν έχετε μόνιμη σύνδεση με το **Internet (**και κατά συνέπεια σταθερό **IP),** εάν τρέχετε κάποιο διακομιστή **(**π.χ., **Web)** στον υπολογιστή σας ή εφαρμογή απομακρυσμένης πρόσβασης **(PC Anywhere-Wingate** κ.λπ.**)** ή απλώς θέλετε να ελέγχετε τι έρχεται και τι φεύγει από το **PC** σας, θα πρέπει να εγκαταστήσετε ένα **firewall.** Μόνο έτσι θα απομονωθεί το σύστημά από το **Internet** και στην ουσία θα "εξαφανιστεί" από τον έξω κόσμο, ακόμα και αν είναι **on-line.** Επιπλέον, με βάση κάποιους συγκεκριμένους κανόνες, ελέγχει και κατά συνέπεια επιτρέπει ή εμποδίζει να εισέλθουν στον υπολογιστή ή να εξέλθουν από αυτόν τα πακέτα δεδομένων του **Internet.**

4.4 Passwords

Τα **passwords** είναι η πιο συνηθισμένη διαδικασία που χρησιμοποιείται σχεδόν παντού για να διασφαλίζει και να επιβεβαιώνει την ταυτότητα του χρήστη, επιτρέποντάς του εν συνεχεία την είσοδο στο κάθε σύστημα. Η συγκεκριμένη μέθοδος εφαρμόζεται για κάθε είσοδο χρήστη σε ένα πληροφοριακό σύστημα ή στο δίκτυο. Από το χρήστη ζητούνται το **user name** και το **password** του, τα οποία εφόσον ταιριάζουν με αυτά που υπάρχουν στο **password file,** θεωρούνται από το σύστημα ως επιβεβαίωση της ταυτότητάς του και έτσι ο χρήστης εισάγεται εντός του συστήματος ή του δικτύου. Τα **passwords** θεωρούνται ως αξιόπιστη και ασφαλής διαδικασία ελέγχου ταυτότητας αλλά όπως σε όλα τα θέματα που αφορούν την ασφάλεια έτσι και εδώ ο κίνδυνος κρύβεται στις λεπτομέρειες**!**

***Λεπτομέρεια 1*:**

Η επιλογή του **password** είναι ίσως το κρισιμότερο σημείο και αυτό διότι οι επιλογές που κάνουν οι χρήστες συνήθως είναι προβλέψιμες. Αν από την άλλη τους δοθεί έτοιμο το **password** τότε επιλέγουν να το σημειώσουν παρά να το αποστηθίσουν. Στη χειρότερη περίπτωση θα ανακαλύψει κάποιος το **password** σε σημείωμα κολλημένο στο πλάϊ της οθόνης του υπολογιστή του χρήστη. Η ορθότερη επιλογή είναι το **password** να αποτελείται από συνδυασμό γραμμάτων και αριθμών.

***Λεπτομέρεια 2*:**

Προκειμένου τα **passwords** να εξασφαλίζουν προστασία πρέπει τακτικά να αντικαθίστανται από νέες επιλογές. Οι χρήστες δυστυχώς αποφεύγουν αυτή την αλλαγή ή επιλέγουν να ανακυκλώνουν ένα μικρό αριθμό από **passwords.** Καλό θα ήταν η τακτική αλλαγή τους να επιβάλλεται από το ίδιο το λογισμικό.

***Λεπτομέρεια 3*:**

Εάν κάποιος έχει λογαριασμούς σε διαφορετικούς υπολογιστές ή **sites** στο **internet** θα πρέπει για λόγους ασφαλείας να χρησιμοποιεί διαφορετικά **passwords** για την είσοδό του σε κάθε σύστημα ή ιστοσελίδα. Ασφαλώς, κάτι τέτοιο είναι ιδαίτερα δύσκολο για τον χρήστη και το πιθανότερο είναι κάπου να τα σημειώσει προκειμένου να μην τα ξεχάσει. Από την άλλη μεριά η ύπαρξη ενός μόνο **password** αυξάνει την πιθανότητα από κάπου να αποκαλυφθεί. Σε κάθε περίπτωση η όσο το δυνατόν συχνότερη αντικατάστασή τους είναι μια καλή και ενδεδειγμένη πρόταση.

Λεπτομέρεια **4:**
Είναι προφανές πως το σημείο που το σύστημα ή το δίκτυο αποθηκεύει τα διάφορα **passwords** είναι σημείο που απαιτεί αυξημένη ασφάλεια αφού αποτελεί βασικό στόχο για εισβολή. Ο συνηθισμένος τρόπος για να περιορίζεται ο κίνδυνος είναι να μην αποθηκεύονται ως κείμενο, ούτε ακόμη και με κρυπτογράφηση **(encrypted),** αλλά με τη μορφή που έχει το καθένα ως συνάρτηση **hash.** Η αντιστροφή της τιμής της συνάρτησης στο αντίστοιχο **password** είναι εξαιρετικά δύσκολη και έτσι τα **passwords,** ναι μεν δεν μπορούν να ανακτηθούν, αλλά εύκολα μπορεί να γίνεται ο έλεγχος ανάμεσα στο αποθηκευμένο **password** και σε αυτό που πληκτρολογείται κατά την είσοδο ενός χρήστη.

Στις μεθόδους για επιβεβαίωση της ταυτότητας κάποιου χρήστη εκτός από τα **passwords,** συμπεριλαμβάνονται ακόμη:

4.4.1 Passwords μιας χρήσης

Ένα πρόβλημα που αντιμετωπίζει η τεχνολογία των **passwords** είναι πως αν μεταδοθεί από μη ασφαλές τηλεπικοινωνιακό κανάλι τότε αυξάνεται αισθητά ο κίνδυνος να έχει υποκλαπεί. Μία λύση στο πρόβλημα είναι ο κάθε χρήστης να έχει ένα σύνολο από **passwords** που το καθένα θα μπορεί να χρησιμοποιηθεί μόνο μια φορά. Ένα τέτοιο σύστημα είναι το **S/Key** το οποίο χρησιμοποιεί μία συνάρτηση η οποία παράγει την αλυσίδα των διαδοχικών **password.** Στην πράξη κάθε έγκυρο **password** αντικαθίσταται στη συνάρτηση και έτσι σχηματίζεται το επόμενο.

4.4.2 Smart Cards

Πρόκειται για μικρές κάρτες -αντίστοιχες με τις πιστωτικές- οι οποίες περιέχουν έναν επεξεργαστή, κάποια μνήμη και μια διασύνδεση με το εξωτερικό περιβάλλον. Χρησιμοποιούνται σε μία σειρά εφαρμογών συμπεριλαμβάνοντας και την ηλεκτρονική πληρωμή. Εκτελούν τρεις βασικές λειτουργίες: Αποθήκευση και διαχείριση πληροφοριών, επιβεβαίωση της ταυτότητας του χρήστη, καθώς και κρυπτογράφηση-αποκρυπτογράφηση. Το πλεονέκτημά της ως προς την ασφάλεια είναι ότι λειτουργεί σε ένα απομονωμένο περιβάλλον.

Σήμερα υπάρχει μία μεγάλη γκάμα από **smart cards,** οι οποίες μεταξύ τους διαφέρουν στην απόδοση και την ικανότητα του επεξεργαστή, το μέγεθος της μνήμης καθώς και την ταχύτητα διασύνδεσης με το εξωτερικό περιβάλλον. Για να λειτουργήσει απαιτείται η ύπαρξη της συσκευής που θα "διαβάσει" την **smart**

card. Υπάρχουν διαφόρων ειδών τέτοιες συσκευές ανάλογα με τι είδους τεχνολογία διαθέτουν. Έτσι έχουμε συσκευές που διαβάζουν την **smart card** όταν αυτή τοποθετηθεί στην ειδική σχισμή και άλλες που είναι χωρίς επαφή και τη "διαβάζουν" με τη βοήθεια υπέρυθρων ακτίνων. Είτε με την πρώτη, είτε με τη δεύτερη μέθοδο, επιτυγχάνεται η απαραίτητη ανταλλαγή δεδομένων ανάμεσα σε κάρτα και συσκευή ανάγνωσης και έτσι γίνεται ο έλεγχος της ταυτότητας του χρήστη.

4.5 Antivirus

Παρά την ύπαρξη περίπου πενήντα χιλιάδων ιών, σύμφωνα με το **Norton Antivirus (**προφανώς πρέπει να είναι ιδιαίτερα διασκεδαστικός ο σχεδιασμός τους, ώστε να δικαιολογείται το πλήθος τους**)**, εάν τηρηθούν μερικοί βασικοί κανόνες, ελαχιστοποιούμε τον κίνδυνο μόλυνσης. Εκτός από την αναβάθμιση των εφαρμογών που σχετίζονται με το **Internet**, είναι πλέον επιβεβλημένη η εγκατάσταση στο πληροφοριακό σύστημα κάποιας εφαρμογής προστασίας από τους ιούς. Μετά την εγκατάσταση θα πρέπει να γίνεται εβδομαδιαία ενημέρωση από τους δημιουργούς του **antivirus (**μέσω **Internet** κατά προτίμηση**)**, ώστε να υπάρχει αυξημένο επίπεδο προστασίας απέναντι και στους νεότερους των ιών. Με την τεράστια εξάπλωση των ιών και των σκουληκιών που χρησιμοποιούν κυρίως το **e-mail** για να εξαπλωθούν, θα πρέπει το **antivirus** να είναι ικανό να ελέγχει και την εισερχόμενη αλληλογραφία της εταιρείας, προστατεύοντας έτσι το σύστημα από τον βασικότερο τρόπο εγκατάστασης των ιών από το εξωτερικό περιβάλλον. Με αυτό τον τρόπο συλλαμβάνονται τα κακόβουλα προγράμματα, προτού φτάσουν στο ηλεκτρονικό γραμματοκιβώτιο της εταιρείας. Βέβαια, οι εφαρμογές προστασίας δεν λειτουργούν πάντα καλά, με συνέπεια να παρουσιάζονται περιστασιακά προβλήματα στη λήψη της αλληλογραφίας, αλλά μπροστά στον υπαρκτό κίνδυνο, τα συγκεκριμένα προβλήματα είναι αποδεκτά. Γενικά, δεν πρέπει να εκτελούνται επισυναπτόμενα αρχεία, εάν δεν υπάρχει βεβαιότητα για την καθαρότητά τους. Ακόμα και αν φαίνονται αθώα **(**μια εικόνα **jpg**, για παράδειγμα**)** ή προέρχονται από γνωστό αποστολέα, δεν αποκλείεται το αρχείο να είναι εκτελέσιμο και να έχει τη μορφή **picture.jpg.exe (**όπως, π.χ., συμβαίνει σε έναν πρόσφατο δούρειο ίππο του **ICQ)**. Να ξεκαθαρίσουμε ότι ελάχιστες είναι οι πιθανότητες να μολυνθεί το σύστημα ανοίγοντας απλώς ένα **e-mail**. Θα πρέπει να εκτελεστεί ο επισυναπτόμενος, καμουφλαρισμένος, κακόβουλος κώδικας. Προσοχή χρειάζεται και με τα αρχεία **word** και **excel** που λαμβάνονται, τα οποία καλό θα είναι να περνούν από έλεγχο για μακροϊούς. Επίσης, πρέπει να προσεχθούν και οι διάφορες εφαρμογές που εγκαθίστανται, ειδικά εάν προέρχονται από αμφιλεγόμενες πηγές.

Η παρουσία του **antivirus** προστατεύει επίσης το σύστημα και από τους εσωτερικούς κινδύνους για την περίπτωση που κάποιος χρήστης είτε εν αγνοία του, είτε εσκεμμένα προσπαθήσει να εγκαταστήσει έναν τέτοιο ιό. Άλλωστε ο κίνδυνος των δολιοφθορών εκ των έσω πρέπει να βρίσκεται ιδιαίτερα ψηλά στην ιεραρχία των κινδύνων, για το σχεδιαστή του συστήματος ασφαλείας.

Όλα τα παραπάνω είναι πολύ καλά για την πρόληψη. Τι πρέπει να γίνεται όμως στην περίπτωση που το πληροφοριακό σύστημα μολυνθεί από κάποιον ιό; Αυτό είναι κάτι που διαπιστώνεται με την παρατήρηση βασικών χαρακτηριστικών και συμπεριφορών του υπολογιστή. Εάν ξαφνικά αρχεία εμφανίζονται ή εξαφανίζονται, το σύστημα γίνεται πιο αργό, μειώνεται η διαθέσιμη μνήμη, εφαρμογές αρνούνται να τρέξουν ή παράξενα μηνύματα εμφανίζονται στην οθόνη, όλα αυτά είναι ενδείξεις που "φωτογραφίζουν" την παρουσία ιού. Η αμέσως επόμενη κίνηση είναι να ελεγχθεί ο υπολογιστής με κάποιο **antivirus.** Αφού εντοπιστεί ο ιός και καθαρίσει το σύστημα, καλό θα ήταν να δημιουργηθούν δισκέτες ασφαλείας, διαδικασία η οποία συνήθως προσφέρεται από το **antivirus** πρόγραμμα που χρησιμοποιείται από το σύστημα. Οι δισκέτες αυτές δίνουν τη δυνατότητα να εκκινηθεί το σύστημα και να γίνει έλεγχος για ιούς, ενώ μπορεί να περιέχουν και αντίγραφα των τομέων εκκίνησης του σκληρού δίσκου σε περίπτωση μόλυνσης του **boot sector.**

Κεφάλαιο 5

Μελέτη περιπτώσεων

5.1 Σύνταξη ερωτηματολογίου

Έχοντας μέχρι τώρα μελετήσει τους περισσότερους και σημαντικότερους κινδύνους που καθημερινά απειλούν το κάθε πληροφοριακό σύστημα και έχοντας δει τις λύσεις που η τεχνολογία προσφέρει, κρίθηκε σκόπιμο, στα πλαίσια της παρούσας διπλωματικής να απευθυνθούμε στους χρήστες του ηλεκτρονικού εμπορίου και να μελετήσουμε τις απόψεις τους. Απόψεις που σαφώς προέρχονται από την εμπειρία και την πράξη. Απόψεις που θα μας δώσουν τη δυνατότητα να αναλύσουμε καλύτερα τα προβλήματα των ηλεκτρονικών συναλλαγών και κυρίως να δούμε πως αυτοί που εφαρμόζουν το Η.Ε. προστατεύουν τα δεδομένα τους.

Προκειμένου να μπορέσουμε να αναλύσουμε όσο γίνετε καλύτερα τις απόψεις τους, συντάξαμε ένα ερωτηματολόγιο το οποίο προσπαθήσαμε να καλύπτει όσο το δυνατόν καλύτερα το χώρο του Η.Ε. και κυρίως τα θέματα που αφορούν την ασφάλειά του. Μέσω του ερωτηματολογίου επιδιώχθηκε να προκύψουν συμπεράσματα για τα ακόλουθα θέματα:

- Πόσο ασφαλές είναι να χρησιμοποιούμε το Η.Ε.
- Αν υπάρχει ανταπόκριση τόσο από επιχειρήσεις όσο και από πελάτες.
- Αν κρίνετε επιβεβλημένη η παρουσία συστήματος ασφαλείας
- Από τι αυτό αποτελείται, με τι κριτήρια επιλέχθηκε, με τι κόστος, ποιός χρόνος χρειάστηκε για να λειτουργήσει
- Αν απαιτούνται και κάθε πότε δοκιμές ελέγχου, συντήρηση, αναβαθμίσεις.
- Αν έχουν διαπιστωθεί επιθέσεις πριν και μετά την εγκατάσταση, τι αποτέλεσμα είχαν και πως το σύστημα ανταποκρίθηκε.
- Αν υπάρχει **security policy**

Με αυτές τις ερωτήσεις διαμορφώθηκε το ακόλουθο ερωτηματολόγιο, με το οποίο απευθυνθήκαμε σε εταιρείες που παρέχουν υπηρεσίες δικτύου, σε τράπεζες, αυτοκινητοβιομηχανίες, φαρμακοβιομηχανίες, εταιρείες κινητής τηλεφωνίας, εταιρείες

που διατηρούν ηλεκτρονικά καταστήματα. Συμπληρώθηκαν τριάντα ερωτηματολόγια αριθμός ικανός για να εξαχθούν χρήσιμα συμπεράσματα.

ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

1. Η εταιρεία σας ασχολείται με Ηλεκτρονικό Εμπόριο Ναι ☐ Όχι ☐

2. Αν ναι με ποιά κατηγορία Ηλεκτρονικού Εμπορίου B2B ☐ B2C ☐

3. Πως θα χαρακτηρίζατε το επίπεδο ασφαλείας του Ηλεκτρονικού Εμπορίου

Πολύ Υψηλό ☐ Υψηλό ☐ Ικανοποιητικό ☐ Μέτριο ☐ Χαμηλό ☐ Πολύ Χαμηλό ☐

4. Πως κρίνετε τη συμμετοχή των πελατών σας στο Ηλεκτρονικό Εμπόριο.

Υψηλή ☐ Ικανοποιητική ☐ Μέτρια ☐ Χαμηλή ☐

5. Οι ιστοσελίδες σας στο δίκτυο έχουν πιστοποιηθεί ως "secure pages" Ναι ☐ Όχι ☐

6. Υπήρχαν επιθέσεις πριν την εγκατάσταση Συστήματος Ασφαλείας στις βάσεις δεδομένων

Ναι ☐ Όχι ☐

7. Με τι είδους δίκτυο είναι συνδεδεμένες οι βάσεις δεδομένων σας

Internet ☐ Intranet ☐ Value Added Networks ☐ Με κανένα ☐

Άλλο

8. Πόσο σημαντική θα ήταν για την εταιρεία σας ενδεχόμενη κλοπή, παραποίηση ή καταστροφή δεδομένων

Εξαιρετικά σημαντική ☐ Πολύ σημαντική ☐ Σημαντική ☐ Ελάχιστα σημαντική ☐ Αδιάφορη ☐

9. Ποιά πιστεύετε πως θα είναι η εξέλιξη του Ηλεκρονικού Εμπορίου.

Ταχύτατη Ανάπτυξη ☐ Αργή Ανάπτυξη ☐ Στασιμότητα ☐ Μείωση ☐ Αποτυχία ☐

Για ποιούς λόγους:

ΠΡΟΣΤΑΣΙΑ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΜΠΟΡΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

10. Πως προστατεύονται οι βάσεις δεδομένων και οι Ηλεκτρονικές Εμπορικές συναλλαγές σας από εσωτερικούς κινδύνους

Passwords ☐ Antivirus ☐ Smart Cards ☐ Διαβαθμισμένη πρόσβαση ☐ Δεν προστατεύονται ☐

Άλλο:

11. Πως προστατεύονται από εξωτερικούς κινδύνους

Passwords ☐ Antivirus ☐ Firewalls ☐ Digital Signatures ☐ Cryptography ☐ Δεν προστατεύονται ☐

Άλλο:

12. Πόσο χρόνο έχει εγκατασταθεί το Σύστημα Ασφαλείας:

13. Η εγκατάσταση του Συστήματος Ασφαλείας έγινε Προληπτικά ☐ Μετά από επίθεση ☐

14. Ποιά κριτήρια υπερίσχυσαν κατά την επιλογή του

Μέγιστη Ασφάλεια ☐ Οικονομικό ☐ Ταχύτητα Εγκατάστασης ☐

Δυνατότητα Αναβάθμισης ☐ Εύχρηστο ☐

Άλλο κριτήριο:

15. Πως κρίνετε το κόστος αγοράς-εγκατάστασης Πολύ Υψηλό ☐ Υψηλό ☐ Μέτριο ☐ Χαμηλό ☐

16. Ποιός ήταν ο χρόνος για την εγκατάστασή του:

17. Απαιτείται συντήρηση του Συστήματος Ασφαλείας Ναι ☐ Όχι ☐

18. Κάθε πότε χρειάζεται συντήρηση και με τι κόστος

19. Πόσες αναβαθμίσεις έχουν γίνει στο Σύστημα Ασφαλείας:

20. Πόσο συχνά γίνονται δοκιμές ελέγχου του Συστήματος Ασφαλείας

1 φορά το μήνα ☐ 1 φορά το εξάμηνο ☐ 1 φορά το χρόνο ☐ Ποτέ ☐

Άλλο:

ΠΡΟΣΤΑΣΙΑ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΜΠΟΡΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

21. Έχουν διαπιστωθεί επιθέσεις στις βάσεις δεδομένων σας Ναι ☐ Όχι ☐

22. Πως ανταποκρίθηκε το Σύστημα Ασφαλείας σε αυτές τις επιθέσεις

Άριστα ☐ Ικανοποιητικά ☐ Μέτρια ☐ Απέτυχε ☐

23. Υπάρχει Security Policy στην εταιρεία σας Ναι ☐ Όχι ☐

24. Πως κρίνετε το βαθμό αφομοίωσής του Security Policy από τους χρήστες.

Υψηλό ☐ Ικανοποιητικό ☐ Μέτριο ☐ Χαμηλό ☐

25. Πως κρίνετε τη λειτουργία του Συστήματος Ασφαλείας μέχρι σήμερα.

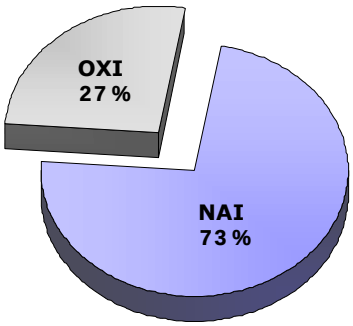
Άριστη ☐ Ικανοποιητική ☐ Μέτρια ☐ Αποτυχημένη ☐

26. Δώστε μία σύντομη περιγραφή του Συστήματος Ασφαλείας:

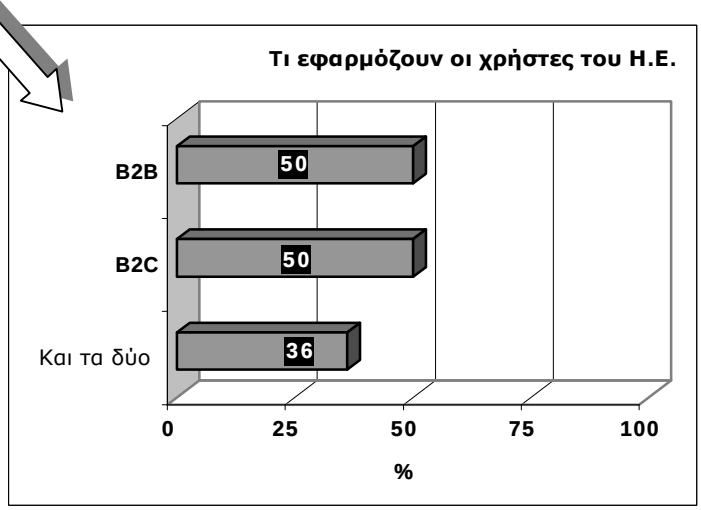
5.2 Αξιολόγηση Ερωτηματολογίων

Οι απαντήσεις που συμπληρώθηκαν στα ερωτηματολόγια δίνουν μια εικόνα του τι συμβαίνει αυτή τη χρονική στιγμή στην ελληνική αγορά ως προς το Η.Ε. Τα συμπεράσματα που προέκυψαν από την ανάλυση των απαντήσεων είναι τα ακόλουθα:

ü Χρήστες του Η.Ε: Το **73%** δήλωσε πως είναι χρήστες των εφαρμογών του.

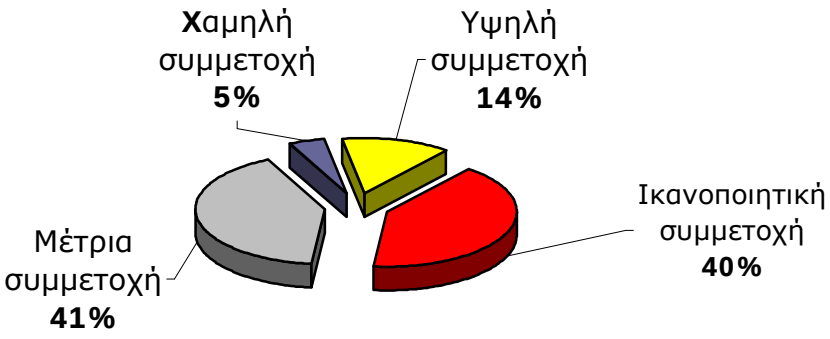


Το ποσοστό **73%** αντιστοιχεί σε **22** χρήστες από τους **30** που ερωτήθηκαν και οι οποίοι επιλέγουν και εφαρμόζουν:



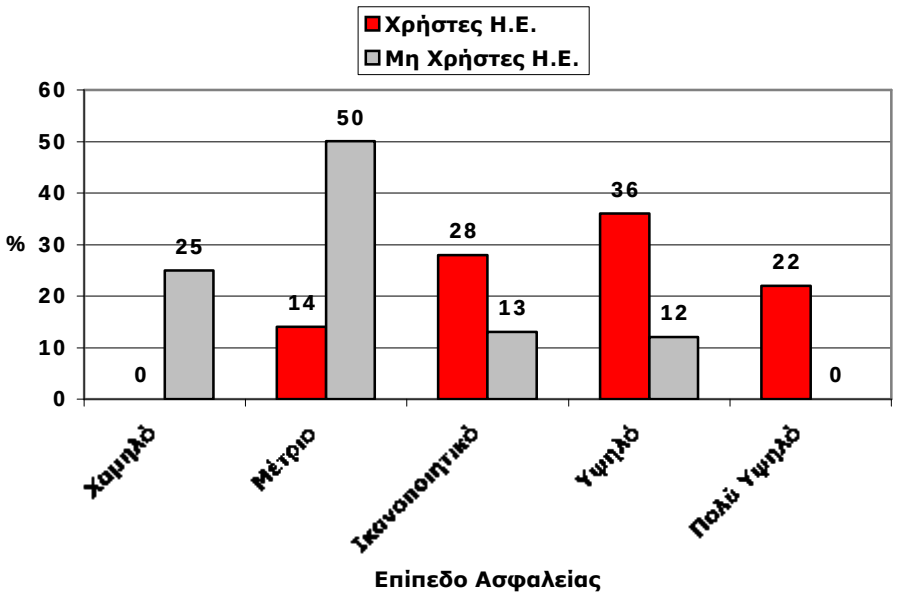
ü Οι εταιρείες που δραστηριοποιούνται στο χώρο του Η.Ε. εμφανίζονται στην πλειοψηφία τους ικανοποιημένες από την ανταπόκριση των πελατών τους κάτι που τους ενθαρρύνει να επενδύσουν στο Η.Ε. Στο ακόλουθο γράφημα φαίνονται αναλυτικά τα αποτελέσματα

Συμμετοχή πελατών στο Η.Ε.



ü Μεγάλο ενδιαφέρον παρουσίαζει το γεγονός ότι το **75%** των εταιρειών που δηλώνει ότι δεν ασχολείται με το Η.Ε. πιστεύει πως το επίπεδο ασφαλείας και επομένως αξιοπιστίας του είναι από χαμηλό εώς μέτριο. Οι ίδιοι τατόχρονα προβλέπουν κατά **70%** στασιμότητα στην ανάπτυξη του Η.Ε. Από αυτά αποδεικνύεται πως οι μη χρήστες του Η.Ε. έχουν την εικόνα ότι πρόκειται για ένα χώρο που εγκυμονεί σημαντικούς κινδύνους και έτσι αποφεύγουν την είσοδό τους. Φοβούνται ότι θα κινδυνεύσουν περισσότερο από όσο θα ωφεληθούν. Είναι όμως έτσι τα πράγματα; Πιστεύουν το ίδιο και όσοι καθημερινά συναλλάσονται μέσω του Η.Ε.;

Στο ακόλουθο γράφημα αντιπαραβάλονται οι απόψεις για το επίπεδο ασφαλείας όσων συμμετέχουν, με τις απόψεις εκείνων που δεν χρησιμοποιούν τις ηλεκτρονικές συναλλαγές.



Οι παραπάνω απαντήσεις έδειξαν πως όσοι συμμετέχουν έχουν ακριβώς την αντίθετη άποψη από αυτούς που δεν είναι χρήστες. Θεωρούν ότι το επίπεδο ασφαλείας του Η.Ε. είναι υψηλό εώς πολύ υψηλό σε ποσοστό **58%** και ταυτόχρονα εκτιμούν πως η ανάπτυξη του είναι βέβαιη είτε με αργά είτε με γοργά βήματα. Οι λόγοι για τους οποίους πιστεύουν στην εξέλιξη του Η.Ε. είναι:

- « Ελαχιστοποίηση χρόνου, κόστους, λάθους
- « Αξιοπιστία στην περιγραφή του προϊόντος

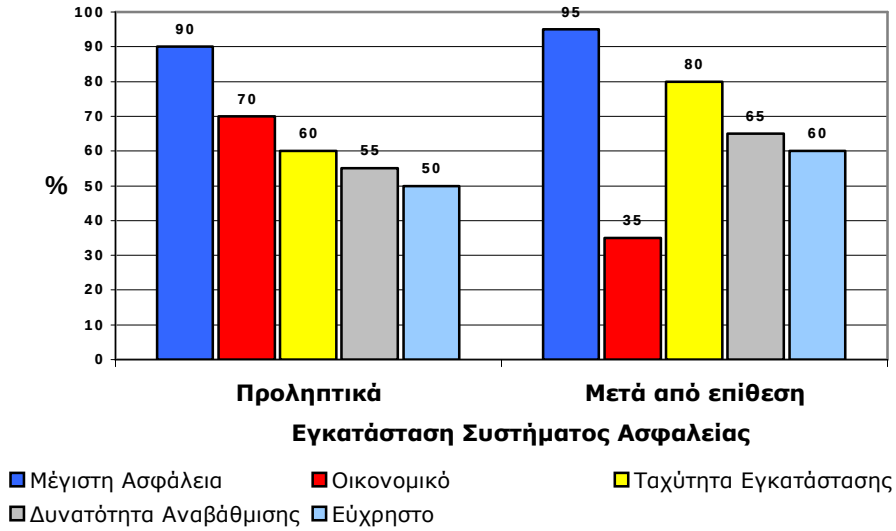
Υπογραμμίζουν όμως την ανάγκη για τη δημιουργία υποδομών που θα βοηθήσουν στην ανάπτυξη του Η.Ε., την ανάγκη "παιδείας" τόσο των **on-line** καταναλωτών όσο και των ίδιων των εμπόρων ώστε να αποτραπούν γεγονότα που θα δυσφημίσουν το Η.Ε. και θα αποθαρρύνουν επίδοξους χρήστες του. Τέλος πιστεύουν στην ανάγκη κινήτρων προκειμένου να αυξηθούν οι εταιρείες που θα εφαρμόζουν το Η.Ε. αλλά και οι χρήστες του **internet**.

Καταλήγουμε επομένως στο συμπέρασμα πως υπάρχει μεγάλη διάσταση απόψεων ανάμεσα στις δύο πλευρές. Είναι φανερό πως όσοι μετέχουν και ζουν καθημερινά το Η.Ε. μπορούν να έχουν μια πιο ξεκάθαρη εικόνα της κατάστασης όπως επίσης είναι φανερό πως η "φήμη" που συνοδεύει το Η.Ε. δεν είναι η καλύτερη δυνατή γι'αυτό και αντιμετωπίζεται με καχυποψία.

Όλοι όμως συμφωνούν και μάλιστα σε ποσοστό **100%** πως ενδεχόμενη κλοπή, παραποίηση ή και καταστροφή δεδομένων είναι εξαιρετικά σημαντική για την εταιρεία τους. Δίνουν επομένως τεράστια σημασία στα θέματα που αφορούν την προστασία των βάσεων δεδομένων τους και γενικότερα του πληροφοριακού τους συστήματος. Δεν είναι τυχαίο άλλωστε πως η πλειοψηφία των ερωτηθέντων έχουν εγκαταστήσει το σύστημα ασφαλείας τους είτε παράλληλα με την αρχική εγκατάσταση του πληροφοριακού συστήματος είτε αργότερα για λόγους προληπτικούς. Με απλά λόγια αυτό σημαίνει, πως όσοι ασχολούνται με τα **e-** γνωριζουν όχι μόνο τους κινδύνους που κρύβουν αλλά και τις μεθόδους προστασίας. Μικρό ποσοστό των ερωτηθέντων **(<10%)** εγκατέστησε το σύστημα προστασίας αφού δέχθηκε επίθεση στις βάσεις δεδομένων του. Ταυτόχρονα αναγνωρίζοντας πως για το ευρύ κοινό οι αγορές **on-line**, καλύπτονται από τον φόβο εξαπάτησης ή ακόμη και κλοπής προσωπικών δεδομένων τους έχουν φροντίσε να πιστοποιήσουν τις σελίδες τους ως **"secure pages"** προσπαθώντας να μεταδόσουν ένα αίσθημα ασφάλειας και κυρίως αξιοπιστίας στους πελάτες τους.

ü Ιδιαίτερο ενδιαφέρον έχει να δούμε με ποιά κριτήρια έγινε η επιλογή των συστημάτων ασφαλείας. Χωρίσαμε τους ερωτηθέντες σε δύο κατηγορίες. Στην πρώτη βρίσκονται όσοι εγκατέστησαν το σύστημα ασφαλείας προληπτικά και στη δεύτερη όσοι αφού πρώτα δέχθηκαν επίθεση. Σημαντικότερο κριτήριο για την επιλογή -και για τις δύο κατηγορίες- είναι, όπως άλλωστε αναμενόταν, η μέγιστη ασφάλεια που πρέπει να εξασφαλίζει το επιλεχθέν σύστημα ασφαλείας. Οι δύο όμως κατηγορίες διαφοροποιούνται ως προς το οικονομικό κριτήριο. Για αυτούς που η εγκατάσταση γίνεται προληπτικά αποτελεί το δεύτερο από πλευράς σπουδαιότητας κριτήριο και όχι άδικα όπως θα διαπιστώσουμε στη συνέχεια. Δεν

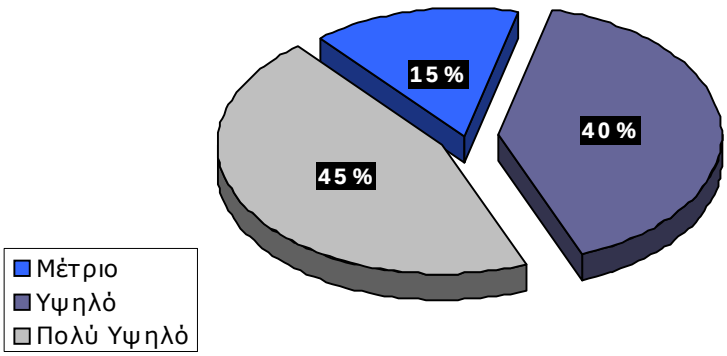
συμβαίνει όμως το ίδιο με την άλλη κατηγορία για την οποία το οικονομικό κριτήριο βρίσκεται τελευταίο στη λίστα κριτηρίων. Η εξήγηση βρίσκεται στο ότι αυτοί που έχουν υποστεί επίθεση είναι σε θέση να γνωρίζουν τη ζημιά που τους προξένησε και προφανώς ήταν τόσο σημαντική που αποδυνάμωσε το κριτήριο του κόστους και στη θέση του έφερε το κριτήριο του χρόνου εγκατάστασης του συστήματος. Αναζητούν συνεπώς ένα σύστημα που θα μπορέσει να εγκατασταθεί και να λειτουργήσει άμεσα αποτρέποντας νέα επίθεση εναντίον τους. Αναλυτικά τα κριτήρια και η ιεράρχησή τους από την κάθε ομάδα, απεικονίζεται στο επόμενο γράφημα.



ü Το κόστος, η συντήρηση και οι αναβαθμίσεις του συστήματος ασφαλείας είναι παράμετροι που όπως προέκυψε από την έρευνα απασχολούν ιδιαίτερα τον διαχειριστή του συστήματος. Η άποψη που κυριαρχεί για το κόστος αγοράς και εγκατάστασης φανερώνει πως πρόκειται για υψηλή εώς πολύ υψηλή δαπάνη. Παράλληλα ο χρόνος εγκατάστασης του συστήματος ασφαλείας ποικίλει από δύο εώς έξι μήνες. Μεγάλες διαφορές εντοπίζονται στη συντήρηση του συστήματος αλλά και στις αναβαθμίσεις του. Τόσο η συντήρηση όσο και οι αναβαθμίσεις είναι άμεσα εξαρτόμενες από το είδος του συστήματος που χρησιμοποιείται για αυτό και συναντήσαμε διαφορετικές απαντήσεις ως προς το πότε πρέπει να εκτελούνται οι παραπάνω διαδικασίες. Γενικά πρέπει να διενεργείται ένας ετήσιος έλεγχος του συστήματος όπου εκεί θα αξιολογείται το σύστημα και θα κρίνεται κατά πόσο απαιτείται συντήρηση ή αναβάθμιση. Ακριβώς για το λόγο ότι οι απειλές καθημερινά αυξάνονται ως προς το πλήθος αλλά και ανανεώνονται ως προς τις

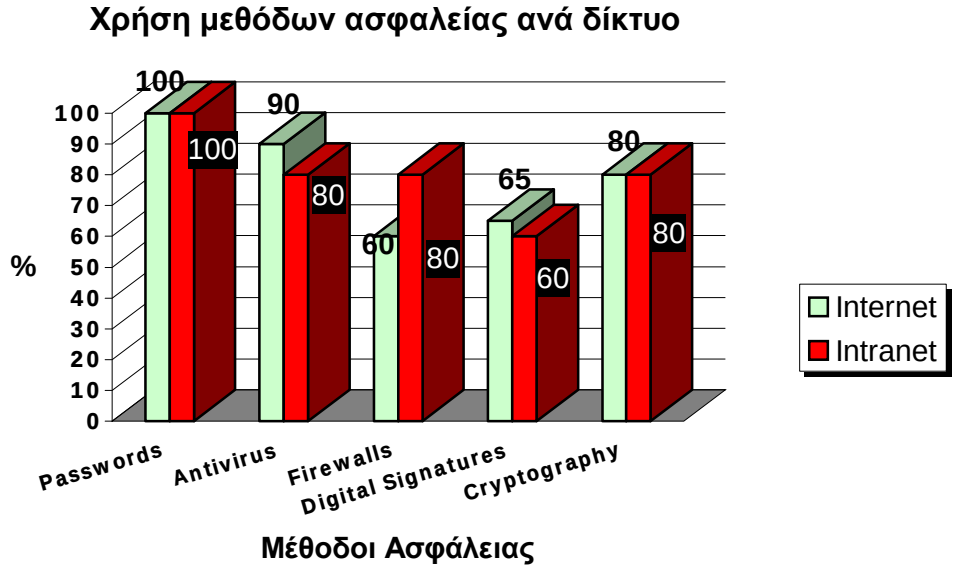
μεθόδους τους θα πρέπει το σύστημα ασφαλείας να τις παρακολουθεί και να προσαρμόζεται ούτως ώστε να μπορέσει να τις αντιμετωπίσει.

Πως κρίνετε το κόστος Αγοράς-Εγκατάστασης του Συστήματος Ασφαλείας



ü Το σύστημα ασφαλείας επιλέγεται με κριτήριο το πόσο σημαντική είναι η βάση δεδομένων που θα προστατέψει. Ταυτόχρονα οι κίνδυνοι που τις απειλούν ταξινομούνται σε δύο κατηγορίες. Τους εσωτερικούς κινδύνους όπου η επίθεση προέρχεται από κάποιον υπάλληλο **(**από λάθος ή εσκεμμένα**)** ή από κάποιον τρίτο που κατάφερε όμως να διεισδύσει εντός της εταιρείας. Και τους εξωτερικούς κινδύνους όπου η επίθεση προέρχεται από το διαδίκτυο. Διαπιστώσαμε πως όλες οι εταιρείες έχουν λάβει μέτρα και για τα δύο είδη απειλών. Η χρήση **passwords, antivirus,** και η διαβαθμισμένη πρόσβαση είναι συνήθως η βάση του συστήματος ασφαλείας και μέθοδοι που υιοθετούνται από την πλειοψηφία των επιχειρήσεων. Όσοι χρησιμοποιούν το **Internet** για το Η.Ε. συνήθως επιλέγουν να συναλλάσονται σε περιβάλλον **SSL** με **128bit** κρυπτογραφία και αν χρησιμοποιούν πιστωτικές κάρτες σε περιβάλλον **SET.** Από την άλλη μεριά οι χρήστες **Intranet** διαλέγουν την προστασία που προσφέρει κάποιο από τα είδη των **firewalls.** Οι ψηφιακές υπογραφές χρησιμοποιούνται με ολοένα και αυξανόμενο ρυθμό. Στο ακόλουθο γράφημα φαίνονται οι επιλογές στις μεθόδους ασφαλείας που έχουν κάνει οι εταιρείες σε σχέση με το δίκτυο που χρησιμοποιούν. Σε πολύπλοκα και ανεπτυγμένα συστήματα ασφαλείας παρουσιάζεται η χρήση **Smart card** για επιβεβαίωση ταυτότητας του χρήστη. Ένα τέτοιο ανεπτυγμένο σύστημα ασφάλειας είναι το ακόλουθο:

- Ø Διπλό **Firewall** ένα εσωτερικό και ένα εξωτερικό
- Ø Υλοποίηση **antivirus** φίλτρων πάνω στα **Firewalls**
- Ø Περιορισμένη πρόσβαση στις βάσεις δεδομένων με υλοποίηση **Security Policy**
- Ø **Ε**ίσοδος σε κρίσιμους χώρους με **Smart Card**
- Ø **Administration** από προκαθορισμένους χώρους εργασίας με χρήση **Password** και **Smart Card**



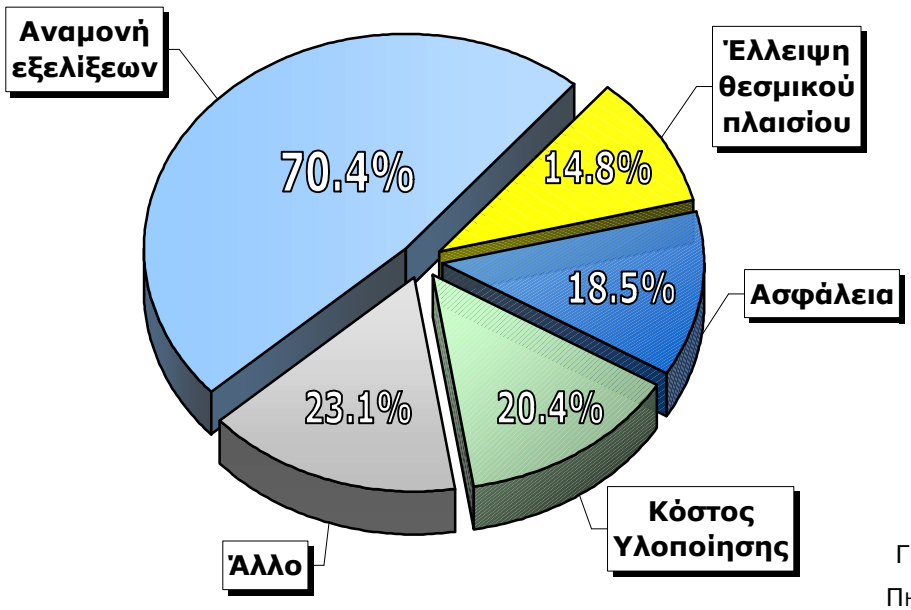
ü Αξίζει τέλος, να σταθούμε στο γεγονός πως το **80%** όσων χρησιμοποιούν το Η.Ε. δηλώνει πως έχει διαπιστώσει επιθέσεις στο σύστημα του. Τα συστήματα ασφαλείας ανταποκρίθηκαν άριστα σε αυτές τις επιθέσεις σε ποσοστό **70%** ενώ ικανοποιητικά σε ποσοστό **20%** και μόνο το **10%** δηλώνει πως υπέστησαν μικρής έκτασης ζημιές από τις επιθέσεις. Το συμπέρασμα που προκύπτει είναι ιδιαίτερα ενθαρρυντικό για την εξέλιξη του Η.Ε. Από τη μία μεριά διαπιστώνεται πως, απέναντι στους κινδύνους που περιγράφηκαν στις πρώτες ενότητες, η τεχνολογία έχει τις λύσεις και από την άλλη οι χρήστες, έχοντας κατανοήσει τις πραγματικές τους ανάγκες, έχουν επιλέξει τα κατάλληλα συστήματα προστασίας. Απόδειξη του γεγονότος ότι οι χρήστες αντιλαμβάνονται πλήρως πως οι κίνδυνοι όχι μόνο είναι υπαρκτοί αλλά και "προοδεύουν" αποτελεί το ότι η πλειοψηφία τους πραγματοποιεί δοκιμές ελέγχου στα συστήματά ασφαλείας. Παράλληλα, όλες σχεδόν οι εταιρείες διαθέτουν **Security Policy** αν και ο βαθμός αφομοίωσής του

από τους υπαλλήλους γενικά κυμαίνεται σε μέτριο εώς ικανοποιητικό επίπεδο. Στο επόμενο γράφημα παρουσιάζεται η άποψη των διαχειριστών συστημάτων ασφαλείας ως προς την μέχρι σήμερα λειτουργία τους, όπου και φαίνεται πως τα υπάρχοντα συστήματα ασφαλείας είναι σε θέση να προστατέψουν τις πολύτιμες βάσεις δεδομένων μιάς εταιρείας.

5.3 Το Ηλεκτρονικό Εμπόριο σήμερα

Σημαντικές δυνατότητες παρουσιάζει η ανάπτυξη του Ηλεκτρονικού Εμπορίου στην Ελλάδα, παρά την καθυστέρηση η οποία παρατηρείται στην υιοθέτηση των σχετικών τεχνολογιών, συγκριτικά με τα υπόλοιπα κράτη-μέλη της Ευρωπαϊκής Ένωσης. Το συμπέρασμα αυτό προκύπτει από πρωτογενή έρευνα, την οποία διεξήγαγε το ΙΔΡΥΜΑ ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΩΝ ΕΡΕΥΝΩΝ **(**ΙΟΒΕ**).** Σύμφωνα με τα αποτελέσματα της έρευνας η διετία **2000-2001** υπήρξε ιδιαίτερα καθοριστική για την ανάπτυξη του κλάδου, καθώς το ***76.6%*** των επιχειρήσεων στη βιομηχανία, το ***60%*** των επιχειρήσεων στο εμπόριο και το ***61.5%*** των επιχειρήσεων που δραστηριοποιούνται στον τομέα των υπηρεσιών ξεκίνησαν την εφαρμογή του Η.Ε.. Εώς το τέλος του **2001** η χρήση των εν λόγω υπηρεσιών είχε ανέλθει σε ποσοστό ***100%*** για τις μεγάλες επιχειρήσεις του κλάδου των υπηρεσιών και ***60%*** για τις μεγάλες επιχειρήσεις του εμπορίου. Στις μεσαίες επιχειρήσεις του κλάδου των υπηρεσιών, το αντίστοιχο ποσοστό διαμορφωνόταν σε ***56.3%*** και για τις μικρές επιχειρήσεις που δραστηριοποιούνται στο εμπόριο στο ***45.5%***. Πάντως υψηλά ποσοστά για τη μελλοντική χρήση εφαρμογών ηλεκτρονικού εμπορίου παρουσιάζουν και οι τρεις τομείς με ποσοστό ***64.7%*** για τις επιχειρήσεις του εμπορίου, ***59.6%*** για τις βιομηχανικές επιχειρήσεις και ***56.5%*** για τον κλάδο των υπηρεσιών. Στο ακόλουθο γράφημα παρουσιάζονται τα εμπόδια για την εφαρμογή του Η.Ε.

Εμπόδια στην υιοθέτηση του Ηλεκτρονικού Εμπορίου



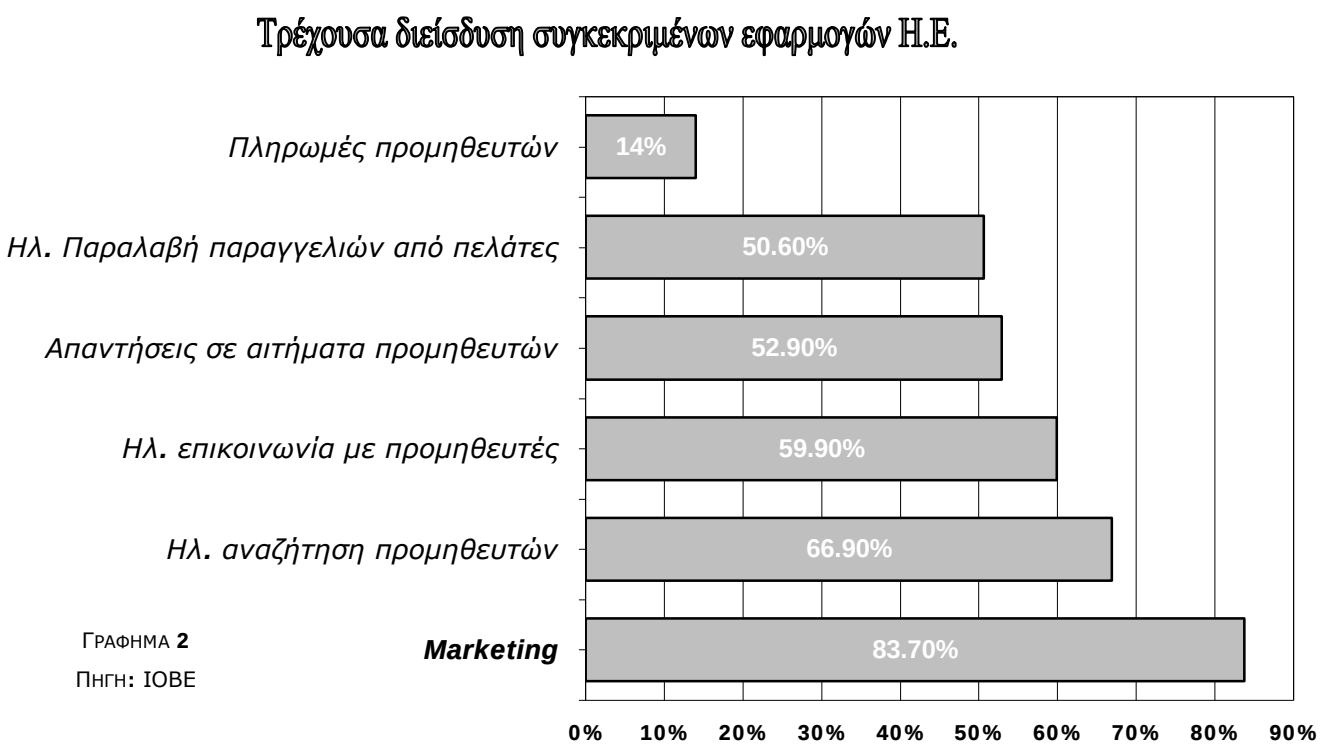
ΓΡΑΦΗΜΑ **1**

ΠΗΓΗ: ΙΟΒΕ

Θα πρέπει να σημειωθεί ότι σύμφωνα με το ***23.1%*** των ερωτηθέντων τα βασικότερα εμπόδια εντοπίζονται σε άλλους τομείς όπως το μικρό μέγεθος των επιχειρήσεων**,** η ικανοποίηση από το υπάρχον δίκτυο**,** η ανάγκη τυποποίησης του προϊόντος**,** η έλλειψη υποδομής των πελατών**,** η έλλειψη ενδιαφέροντος και η λήψη των αποφάσεων από τη μητρική εταιρεία**.**

Τη μεγαλύτερη διείσδυση παρουσιάζουν οι εφαρμογές **marketing *83.7%*,** η ηλεκτρονική αναζήτηση προμηθευτών ***66.9%*** και η ηλεκτρονική επικοινωνία με τους προμηθευτές ***59.9%.*** Η χαμηλότερη παρατηρείται πως είναι το ***14%*** στις πληρωμές προμηθευτών γεγονός το οποίο αποδίδεται στο τρέχον επίπεδο ασφαλείας των συναλλαγών και στη χαμηλή εξοικείωση με ανάλογα συστήματα πληρωμών **(**ΓΡΑΦΗΜΑ **2).**

Ευοίωνες**,** πάντως είναι και οι προοπτικές ανάπτυξης στο σύνολο της αγοράς της Δυτικής Ευρώπης καθώς οι επενδύσεις για εταιρική παρουσία στο διαδίκτυο αναμένεται να ανέλθουν σε **60.7** δις ευρώ για το **2003,** από **22** δις ευρώ το **2000.** Αναμφίβολα τα ηνία στην κατηγορία Η.Ε**.** από επιχειρήσεις προς καταναλωτές διατηρούν οι Η.Π.Α**.** με αξία συναλλαγών που για το **2000** αντιπροσώπευε περισσότερο από τα **3/4** της παγκόσμιας αγοράς**.** Η αναπτυσσόμενη αγορά αυτού του είδους Η.Ε**.** στην Ευρωπαϊκή Ένωση αναμένεται να φτάσει περίπου το **1/3** των Η.Π.Α**.** στα επόμενα δύο με τρία χρόνια**.**



ΓΡΑΦΗΜΑ **2**
ΠΗΓΗ: ΙΟΒΕ

5.4 Μελλοντικές εξελίξεις - Προοπτικές

Ρυθμοί Ανάπτυξης του Η.Ε.

Στα **2.3** τρις δολ. εκτιμάται ότι θα ανέλθουν οι πωλήσεις του Η.Ε. μεταξύ επιχειρήσεων **(B2B)** στην Ευρώπη μέχρι το **2005,** από **500** δις δολ. που είναι σήμερα. Η αυξητική αυτή τάση φαίνεται να είναι παγκόσμια καθώς οι πωλήσεις B**2**B παγκοσμίως αναμένεται να αυξηθούν σε **8.5** τρις δολ. μέχρι το **2005** έναντι **1.9** τρις που είναι σήμερα. Σύμφωνα με πρόσφατη έρευνα της εταιρείας **Gartner,** το **2005** μέσω του B**2**B θα πραγματοποιείται το ***8%*** των συνολικών συναλλαγών μεταξύ επιχειρήσεων στην Ευρώπη. Παρόλα αυτά μέχρι σήμερα, μόλις το **18.5%** των ευρωπαϊκών επιχειρήσεων έχουν υιοθετήσει το συγκεκριμένο τρόπο προμηθειών, ενώ στα τέλη του **2003** το ποσοστό αυτό αναμένεται να εκτιναχθεί στο ***73.6%***. Είναι πλέον σαφές ότι το διεπιχειρησιακό Η.Ε. έχει ξεπεράσει κάθε προσδοκία και συνεχίζει την ανάπτυξή του αφήνοντας πολύ πίσω, από πλευράς πωλήσεων, το Η.Ε. που απευθύνεται σε καταναλωτές **(B2C).**

Σύμφωνα με νέα έρευνα της **Forrester Research,** το **on-line** εμπόριο στην Ευρωπαϊκή Ένωση θα εκτοξευθεί από μόλις **77** δις ευρώ το **2001** σε περισσότερο από **2.2** τρις ευρώ εώς το **2006** αριθμός που αντιστοιχεί στο ***22%*** του συνολικού εμπορίου.

Το ηλεκτρονικό εμπόριο ηλεκτρολογικού εξοπλισμού, χημικών και **Logistics** θα γνωρίσει πολύ μεγάλη ανάπτυξη μέσα στο **2003.** Για τον ηλεκτρολογικό εξοπλισμό αναμένεται αύξηση των **on-line** πωλήσεων από ***4.3%*** σε περισσότερο από ***11%***. Στον τομέα των χημικών και των **Logistics** περισσότερο από **7%** προβλέπεται να διεκπεραιωθεί μέσω διαδικτύου. Εξίσου γοργά θα προχωρήσει και σε τομείς της βιομηχανίας. Αντίθετα με βραδύτερους ρυθμούς αναμένουμε ότι θα προχωρήσει η διείσδυση του Η.Ε. σε τομείς όπως τα τρόφιμα, τα υφάσματα και τα είδη σπιτιού, που θα αρχίσουν να εμφανίζουν ικανοποιητικούς ρυθμούς ανάπτυξης από το **2005.**

Ρυθμοί Ανάπτυξης του Η.Ε. στην Ελλάδα

Η Ελλάδα προσπαθεί να γεφυρώσει με ταχύτερους ρυθμούς το "ψηφιακό χάσμα" που την χωρίζει από τους υπόλοιπους εταίρους στην Ευρωπαϊκή Ένωση. Η αναμενόμενη ετήσια αύξηση των δαπανών για **online** αγορές στην Ελλάδα είναι πολύ υψηλότερη από τον αντίστοιχο μέσο όρο στην Ευρώπη. Σε αυτή την κατεύθυνση σημαντική αναμένεται να είναι η συμβολή των μεγάλων έργων που θα υλοποιηθούν υπό το πλαίσιο του προγράμματος "Κοινωνία της Πληροφορίας",

το οποίο περιλαμβάνει έργα για την ηλεκτρονική διακυβέρνηση καθώς και δράσεις για το **e-procurment.** Σύμφωνα με μελέτη της **Forrester Research** οι **online** πωλήσεις αναμένεται να σημειώσουν σημαντική αύξηση όπως φαίνεται και στον επόμενο πίνακα.

ΠΙΝΑΚΑΣ: Προβλέψεις της **Forrester Research** για **online** πωλήσεις τα επόμενα έτη

Έτη	Εκατομμύρια Ευρώ
2003	**125**
2004	**262**
2005	**476**
2006	**772**

Ταχείς ρυθμούς ανάπτυξης για τις **online** αγορές των Ελλήνων χρηστών προβλέπει και η **Jupiter Research,** σύμφωνα με την οποία οι δαπάνες για ηλεκτρονικές αγορές θα αυξάνονται ετησίως κατά ***42%*** εώς το **2007.**

Προοπτική για την αγορά συστημάτων ασφαλείας

Διπλασιασμό της αξίας της αγοράς συστημάτων ασφαλείας για τα πληροφοριακά συστήματα μέχρι το **2006** προβλέπουν οι αναλυτές. Σύμφωνα με έρευνα της **IDC,** στο διάστημα αυτό η αγορά θα ανέλθει σε **155** δις δολ. από **66** δις δολ. το **2001.** Τα αποτελέσματα της έρευνας δεν αποτελούν έκπληξη, ιδιαίτερα μετά τα γεγονότα της **11**ης Σεπτεμβρίου. "Η ασφάλεια δεν είναι πλέον μιά εναλλακτική ή επιπρόσθετη δραστηριότητα, αλλά μια βασική προτεραιότητα" τονίζει ο Αλαν Μπριλ διευθύνων σύμβουλος του τομέα τεχνικών υπηρεσιών της **Kroll.** Μετά την **11**η Σεπτεμβρίου πολλές εταιρείες καθυστέρησαν τις αγορές τους επειδή δεν γνώριζαν τι ακριβώς χρειάζονταν. Το θέμα της ασφάλειας παρέμεινε πρώτη προτεραιότητα για μεγάλο ποσοστό **(40%)** των επαγγελματιών της τεχνολογίας. Επίσης, ο τομέας της ασφάλειας ήταν ο μοναδικός για τον οποίο οι περισσότεροι ερωτηθέντες αύξησαν τις δαπάνες τους το τελευταίο εξάμηνο. Τέλος οι ερευνητές της **IDC** προβλέπουν για φέτος ότι η αξία των συστημάτων ασφάλειας θα φτάσει τα **80** δις δολ.

Κι όλα αυτά τη στιγμή που αυξάνονται με εκρηκτικό ρυθμό, οι απαιτήσεις για αποθήκευση πληροφοριών. Το αντιφατικό στοιχείο είναι πως αν και οι απαιτήσεις πολλαπλασιάζονται δε συμβαίνει το ίδιο και με τις αγορές συστημάτων αποθήκευσης. Οι εταιρείες είναι επιφυλακτικές στο που θα πρέπει να επενδύσουν. Σε αυτό το "ασφυκτικό" περιβάλλον, εταιρείες οι οποίες παρέχουν λύσεις αποθήκευσης, όπως είναι η **EMC, Network Appliance, IBM,** προσπαθούν να πείσουν τους πελάτες τους να αγοράσουν εντελώς νέα δίκτυα αποθήκευσης. Μπορούν άραγε οι εταιρείες να πείσουν τους επιφυλακτικούς διευθυντές των επιχειρήσεων να εφαρμόσουν μια πρωτοπόρα αλλά δαπανηρή αρχιτεκτονική δικτύου; Ποιά είναι η καλύτερη επιλογή αποθήκευσης από οικονομικής και τεχνολογικής άποψης;

Αυτή τη στιγμή, κυκλοφορούν στην αγορά πολλά και διαφορετικά είδη λύσεων αποθήκευσης συμπεριλαβανομένων των δικτύων περιοχής αποθήκευσης **(SANs, storage area networks),** της συνδεδεμένης με δίκτυο αποθήκευσης **(NAS, network-attached storage)** και των μέσων αποθήκευσης περιεχομένου **(CAS, content-attached storage).**

Η πλέον σημαντική εξέλιξη είναι η αποθήκευση αρχείων σε δικό τους ξεχωριστό δίκτυο. Τα πρακτικά οφέλη είναι τα ακόλουθα:

- Εξαιρετικά εκτεταμένος χώρος αποθήκευσης
- Προστασία των δεδομένων, εφόσον και όταν "κρασάρει" το δίκτυο
- Απρόσκοπτη επέκταση του χώρου αποθήκευσης
- Ταχύτερη πρόσβαση στις πληροφορίες
- **Backup** με μεγαλύτερη διαφάνεια.

Η άποψη που δείχνει να εδραιώνεται είναι πως η αποθήκευση πρέπει να καταστεί ξεχωριστή οντότητα για να γίνεται πιο εύκολη η μεταφορά, η ανάκτηση και η επεξεργασία των δεδομένων. Είναι αυτονόητο ότι, στην αρχή, θα προκληθούν επιπλέον έξοδα, όμως μόλις μια εταιρεία εδραιώσει την αρχιτεκτονική της **online** αποθήκευσης, θα επωφεληθεί από τις οικονομίες κλίμακος που θα επιτευχθούν, καθώς τα αρχειοθετημένα αρχεία σταδιακά θα αυξάνουν.
Το μέλλον θα δείξει...

Τρομοκράτες οι Crackers στη Μ. Βρετανία

Τρομοκράτες θεωρούνται οι **crackers,** σύμφωνα με νόμο περί τρομοκρατίας που έχει ψηφιστεί από τη βρετανική κυβέρνηση. Ο συγκεκριμένος νόμος βάλλει κατά αυτών που πραγματοποιούν ηλεκτρονικές επιθέσεις σε κυβερνητικά και άλλα δίκτυα έχοντας ιδεολογικά κίνητρα.

Ο βρετανικός νόμος διευρύνει την έννοια της τρομοκρατίας, έτσι ώστε αυτή να συμπεριλαμβάνει τους **crackers** που πραγματοποιούν επιθέσεις σε κυβερνητικά συστήματα υπολογιστών ή δικτυακούς τόπους επιχειρήσεων. Στο εξής, όποιος προσπαθεί να «παρακωλύσει τη λειτουργία ενός ηλεκτρονικού συστήματος» με πρόθεση να απειλήσει και να επηρεάσει την κυβέρνηση ή το κοινό, για να προωθήσει "έναν πολιτικό, θρησκευτικό ή ιδεολογικό στόχο", θεωρείται τρομοκράτης.

Οι υπέρμαχοι της νομοθεσίας, πάντως, υποστηρίζουν ότι αυτή αποτελεί ένα σημαντικό βήμα για την προάσπιση των δικαιωμάτων των πολιτών απέναντι σε επιθέσεις κακόβουλων **crackers.**

Δεκτή η Ψηφιακή Υπογραφή στις ΗΠΑ

Η ψηφιακή υπογραφή έχει αποκτήσει την ισχύ της χειρόγραφης στις Ηνωμένες Πολιτείες με ένα νόμο που εκτιμάται ότι θα δοκιμαστεί στην αρένα του Διαδικτύου. Ωστόσο, η υιοθέτηση της ψηφιακής υπογραφής μπορεί να σημαίνει για τους χρήστες τόσο διευκολύνσεις όσο και κινδύνους.

Ο νόμος για την καθιέρωσή της στις ΗΠΑ **(The Electronic Signatures in Global National Commerce Act)** έχει στόχο να διευκολύνει τις εμπορικές και οικονομικές συναλλαγές. Σε ορισμένες περιπτώσεις, όπως στη σύναψη συμβολαίων, όταν χωρίζουν τα ενδιαφερόμενα μέρη μεγάλες γεωγραφικές αποστάσεις, οι νέες δυνατότητες μπορούν να τους εξοικονομήσουν πολύτιμο χρόνο.

Εντούτοις, η νέα αυτή τεχνολογική πρόοδος δεν είναι απαλλαγμένη από προβλήματα και κινδύνους για το χρήστη. Ο συγκεκριμένος νόμος, για παράδειγμα, δεν καθορίζει τι είδους τεχνολογίες θα χρησιμοποιούνται κατά την ψηφιακή υπογραφή ενός ηλεκτρονικού εγγράφου. Μπορούν να χρησιμοποιούνται σχετικά ασφαλείς διαδικασίες, όπως η χρήση κωδικών πρόσβασης ή δακτυλικών αποτυπωμάτων, αλλά και εξαιρετικά αβέβαιες, όπως το πάτημα ενός κουμπιού σε μία ιστοσελίδα. Επίσης, τα συστήματα τα οποία φιλοξενούν τις ψηφιακές υπογραφές είναι δυνατόν να δεχτούν επιθέσεις από **hacker,** με αποτέλεσμα η

ταυτότητα του χρήστη να υπόκειται στον κίνδυνο να γίνει αντικείμενο εκμετάλλευσης.

Συμπερασματικά:

Σε ένα συνεχώς διευρυνόμενο μέσο όπως το Διαδίκτυο, με τα κεφάλαια για επενδύσεις στην ιδέα του ηλεκτρονικού επιχειρείν να ρέουν άφθονα και συνεχώς, υπάρχει μεγάλο περιθώριο για κέρδος αλλά και για... χάσιμο. Μέσα σε αυτό το κλίμα, αυξάνονται και οι ευκαιρίες για ηλεκτρονική απάτη, άλλωστε οι επιτήδειοι δεν λείπουν ποτέ. Μία από τις απαραίτητες προϋποθέσεις για την άνθηση του ηλεκτρονικού εμπορίου είναι η ασφάλεια των συναλλαγών. Ο χρήστης που κάνει μια αγορά **on-line** πρέπει να είναι σίγουρος ότι ο αριθμός της πιστωτικής κάρτας του δεν θα υποκλαπεί. Κάθε φορά που συνδιαλέγεται δικτυακά με την τράπεζά του θέλει να γνωρίζει ότι όντως έρχεται σε επαφή με την ίδια την τράπεζα και όχι με κάποιον εικονικό τόπο. Όταν αποστέλλει στο **Internet** ευαίσθητα δεδομένα, θέλει να ξέρει ότι είναι "για τα μάτια" του θεμιτού παραλήπτη και μόνο αυτού και πάει λέγοντας. Τα προηγούμενα μπορεί να ακούγονται υπερβολικά (το πολύ να συμβαίνουν μόνο στους άλλους), ωστόσο, για να το θέσουμε όσο πιο απλά γίνεται, το θέμα είναι να μαθαίνεις πριν "την πάθεις", διότι ο κίνδυνος είναι υπαρκτός. Πράγματι, δεν έχει κανείς παρά να παρακολουθήσει για μικρό χρονικό διάστημα την επικαιρότητα γύρω από τα τεκταινόμενα στο Διαδίκτυο. Θύματα επιθέσεων ενοχλητικών έως και επικίνδυνων **crackers** πέφτουν από καιρού εις καιρόν μεγάλοι δικτυακοί τόποι, όπως το **Yahoo!**, το **Amazon**, το **eBay** ακόμα και το δίκτυο της **Microsoft**. Εάν, όμως, τόποι με διαμέτρημα παρόμοιο με αυτό των προαναφερθέντων, καθώς επίσης και μεγάλοι χρηματοπιστωτικοί οργανισμοί ή θωρακισμένοι τραπεζικοί λογαριασμοί "λυγίζουν" στις ύπουλες επιθέσεις των **cracker**, πώς μπορούμε να είμαστε ήσυχοι για την ασφάλεια του **PC** και των δεδομένων μας, κάθε φορά που σερφάρουμε;

Αποτελεί ειρωνεία το γεγονός ότι το ταπεινό **PC** στο σπίτι μας μπορεί στην πράξη να είναι περισσότερο ασφαλές όσον αφορά σε εξωτερικούς κινδύνους σε σύγκριση, π.χ., με τους διακομιστές της **Microsoft**.

Το Διαδίκτυο είναι εδώ, παντού, τριγύρω μας. Είναι ένα θαυμάσιο μέρος, αρκεί να είναι κανείς οπλισμένος με βασικές γνώσεις και να επαγρυπνεί, όσο χρειάζεται. Διαφορετικά, όρεξη να έχουμε για (δυσάρεστες) περιπέτειες.-

Βιβλιογραφία

(1) **Efraim Turban, Jae Lee, David King, H.Michael Chung "Electronic commerce. A managerial Perspective" Prentice-Hall Editions 1999**

(2) **K.C.Laudon, J.P.Laudon "Management Information Systems" Prentice-Hall Editions, Seventh Edition 2002**

(3) **G.Winfield Treese, Lawrence C. Stewart "Designing Systems for Internet Commerce" Addison-Wesley 1998**

(4) **B.Schneier "Applied Cryptography" J. Wiley and Sons Inc. Second Edition 1996**

(5) **J.c.GRAFF "Cryptography and e-commerce" J. Wiley and Sons Inc. 2001**

(6) **Richard E. Smith "internet Cryptography" Addison-Wesley 1997**

(7) **B. Chapman, E. Zwincky "Building Internet Firewalls" O'Reilly & Associates Inc. 1995**

(8) **Randall K. Nichols, Daniel J. Ryan, Julie Ryan "Defending your digital assets against hackers, crackers, spies & thieves" McGraw Hill 2000**

(9) **Janczewski, Lech "Internet and Intranet security management" Idea Group Publishing 2000**

(10) **Karanjit S. &Chris Hare "Internet Firewalls and Network Security" New Riders Publishing 1995**

(11) **Marcus Goncalves "Firewalls a complete guide" McGraw Hill 2000**

(12) **F.J.Cooper, Chris Goggans, J.K.Halvey, L.Hughes, Karanjit S. "Implementing Internet Security" New Riders Publishing 1995**

(13) **S Castano, G.Martelli, M.Fugini, "Database Security" Addison Wesley**

(14) **L.Klander "Hacker Proof" Jamsa Press 1997**

(15) **R.Elmarsi-S.B.Navathe** "Θεμελιώδεις Αρχές Συστημάτων Βάσεων Δεδομένων" Εκδόσεις Δίαυλος **1996** Μετάφραση Επιμέλεια Μ.Χατζόπουλος

(16) **L.D.Stein** "Ασφάλεια Δικτύων **Web**" Εκδόσεις Ίων, Επιμέλεια Δ.Γκαρμπολάς

(17) Γ.Δουκίδης, Γ.Γιαγλής, Γ.Παππάς, Β.Ζαρογιάννη, Β.Περγιουδάκης "Ηλεκτρονικό Εμπόριο και Ηλεκτρονική Ανταλλαγή Δεδομένων **(EDI)**" Οικονομικό Πανεπιστήμιο Αθηνών **1996** εκδόσεις Νέων Τεχνολογιών

(18) Επιχειρησιακό Πρόγραμμα Βιομηχανίας Πρόγραμμα Κλαδικά Έργα **EDI** "Οδηγός Ηλεκτρονικού Εμπορίου για επιχειρήσεις μόδας" Αθήνα Ιούλιος **2000**

(19) "Ψηφιακές Υπογραφές και Συστήματα **PKI**" Διπλωματική Εργασία Σακαρίδη Σαράντη Τμήμα Βιομηχανικής Διοίκησης & Τεχνολογίας, Μεταπτυχιακό Πρόγραμμα: Εφοδιασμός & Διακίνηση Προϊόντων, Κατεύθυνση **LOGISTICS** Πειραιάς **2002**

(20) **Marvin Zim "The Paranoid's Guide to safe Internet Communicating", Harvard Management Communication Letter July 1999**

(21) **Harvard Bussiness School 9-799-087 Rev. May 10, 1999 "Network Associates: Securing Internet"**

(22) **"How to create an E-commerce Web Site" Verisign Guide**