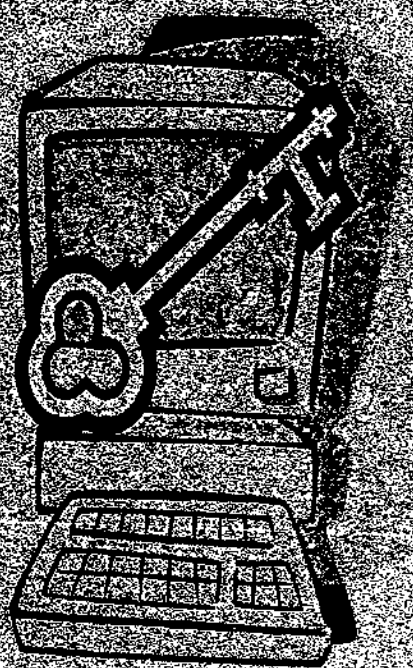
ΑΣΦΑΛΕΙΑ ΛΟΓΙΣΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ



ΣΠΟΥΔΑΣΤΡΙΕΣ:

- ΔΗΜΟΥ ΜΑΡΙΑ
- ΗΛΙΑΔΗ ΔΗΜΗΤΡΑ
- ΚΑΠΠΟΥ ΦΩΤΕΙΝΗ

ΕΙΣΗΓΗΤΗΣ:

- ΟΡΦΑΝΟΣ ΓΕΩΡΓΙΟΣ

ΑΤΕΙ ΠΑΤΡΩΝ 2005

ΑΤΕΙ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

Τμήμα Λογιστικής

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 4°
ΑΣΦΑΛΕΙΑ ΣΤΑ ΛΟΓΙΣΤΙΚΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΚΕΦΑΛΑΙΟ 5°
ΓΕΝΙΚΑ ΠΕΡΙ ΙΩΝ

ΚΕΦΑΛΑΙΟ 6ο
ΤΕΧΝΟΛΟΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

ΚΕΦΑΛΑΙΟ 1°
ΠΡΟΛΟΓΟΣ
ΑΝΤΙΚΕΙΜΕΝΟ ΤΗΣ ΕΡΓΑΣΙΑΣ

Η μελέτη των Λογιστικών Πληροφοριακών Συστημάτων (Λ.Π.Σ) που αποτελεί απόδοση του αγγλικού όρου ACCOUNTING INFORMATION SYSTEM, αποτελεί αντικείμενο τόσο της επιστήμης της Πληροφορικής, όσο και της Λογιστικής επιστήμης.

Η ραγδαία ανάπτυξη των νέων τεχνολογιών και ιδιαίτερα της πληροφορικής επηρεάζει τις επιστημονικές και κοινωνικές εξελίξεις, γι' αυτό και σήμερα, την εποχή της ηλεκτρονικής και του αυτοματισμού η συστηματική επεξεργασία των δεδομένων με σκοπό την παροχή πληροφοριών στη Λογιστική, δεν νοείται χωρίς την παρουσία Η/Υ. Αυτό γιατί η τεράστια ανάπτυξη των Βιομηχανικών και Εμπορικών επιχειρήσεων και αυτών Παροχής Υπηρεσιών με τον έντονα ανταγωνιστικό και αποκεντρωτικό χαρακτήρα, δημιούργησε την ανάγκη για άμεση και γρήγορη πληροφόρηση της Λογιστικής των Οργανισμών αυτών, η οποία δε θα μπορούσε να γίνει χωρίς την εκμετάλλευση της ταχύτητας επεξεργασίας και μεταφοράς πληροφοριών που προσφέρουν οι Ηλεκτρονικοί Υπολογιστές.

Παράλληλα όμως με αυτήν την εκσυγχρόνιση της πληροφορικής, δημιουργείται η ανάγκη για την κατοχύρωση του πολίτη από τις αρνητικές επιπτώσεις της, και την κατοχύρωση αυτή την παρέχει η «ασφάλεια» των πληροφοριακών συστημάτων. Συγκεκριμένα, η Πληροφορική διευκολύνει τη διασταύρωση και τη συνδυασμένη χρήση πληροφοριών που έχουν συγκεντρωθεί σε διαφορετικά μέρη για διαφορετικούς σκοπούς, κι έτσι απεικονίζεται η ανάγκη εξασφάλισης των φυσικών προϋποθέσεων, δηλαδή των μέσων αποθήκευσης των επεξεργασιών και μετάδοσης πληροφοριών. Η ανάπτυξη λοιπόν ασφαλών συστημάτων είναι αυτή που μπορεί να πετύχει αυτή τη τεχνική εξασφάλιση.

Αντικείμενο της εργασίας αυτής είναι να παράσχει τις απαραίτητες γνώσεις και πληροφορίες για τα συστήματα αυτά στον αναγνώστη, προκειμένου να ανταποκριθεί στις απαιτήσεις ενός περιβάλλοντος Πληροφορικής. Ο εν λόγω ενδιαφερόμενος χρήστης, μπορεί επίσης να είναι οποιοσδήποτε ασκεί την Λογιστική επιστήμη σε έναν Οργανισμό και έχει ανάγκη ανά πάσα στιγμή από πληροφορίες που θα τον υποστηρίξουν στο έργο του.

Η εργασία είναι οργανωμένη σε έξι Κεφάλαια:

Στο Πρώτο γίνεται η εισαγωγή και μια γενική αναφορά στο θέμα των πληροφοριακών συστημάτων καθώς και στο αντικείμενο της Πτυχιακής εργασίας.

Το Δεύτερο κεφάλαιο ασχολείται εκτενώς με την έννοια και τα είδη των πληροφοριακών συστημάτων, ενώ παράλληλα αναφέρονται και σαφή παραδείγματα. Επίσης γίνεται αναφορά στην έννοια της πληροφορίας, στα χαρακτηριστικά της και στις ιδιότητές της, στοιχείο που αποτελεί καταλύτη στη ευρύτερη λειτουργία των συστημάτων αυτών.

Ακολουθεί το Τρίτο κεφάλαιο, που ασχολείται πιο συγκεκριμένα με τα Λογιστικά Πληροφοριακά Συστήματα και τον ρόλο των λογιστών στη διαδικασία ανάπτυξής τους. Εδώ επίσης γίνονται αναφορές στη χρήση μεθόδων και διαγραμμάτων που οδηγούν στην έγκυρη ανάλυση των συστημάτων, όπως είναι το γνωστό Μοντέλο του Καταρράκτη.

Στο Τέταρτο κεφάλαιο γίνεται λόγος για την Ασφάλεια των Λογιστικών Πληροφοριακών Συστημάτων, πώς επιτυγχάνεται και τι πλεονεκτήματα παρέχει στον χρήστη.

Το Πέμπτο κεφάλαιο μιλάει για τη μεγάλη απειλή των πληροφοριακών συστημάτων, γίνεται δηλαδή εκτενής ανάλυση της φύσης των ιών, τους λόγους δημιουργίας τους, καθώς και τους τρόπους αντιμετώπισής τους με προληπτικά μέτρα και αμυντικά συστήματα.

Τέλος στο Έκτο κεφάλαιο αναφέρονται γενικά διάφορες τεχνολογίες Ασφάλειας που διασφαλίζουν τις ηλεκτρονικές μας συναλλαγές μέσω διαδικτύου. Χαρακτηριστικά γίνεται λόγος για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων, τις ψηφιακές υπογραφές, καθώς και τα συστήματα προστασίας από επιτήδειους χρήστες – εισβολείς.

Όπως γίνεται κατανοητό, στόχος της παρούσας εργασίας είναι η αναλυτική παρουσίαση του θεωρητικού πλαισίου υποστήριξης της έννοιας και του περιεχομένου των λογιστικών πληροφοριακών συστημάτων καθώς και της σημασίας που έχουν αυτά στην εποχή μας όπου ο αυτοματισμός και η μηχανογράφηση έχουν πλέον εγκαθιδρυθεί.

ΚΕΦΑΛΑΙΟ 2°
Η ΕΝΝΟΙΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

2.1 Η έννοια του συστήματος

Με τον όρο Σύστημα νοείται ένα σύνολο στοιχείων, διαρθρωμένων με κάποια συγκεκριμένη οργανωτική δομή που επιτελεί μια σειρά δραστηριοτήτων και επιδιώκει την επίτευξη ενός προκαθορισμένου σκοπού.

Ο ορισμός αυτός υπονοεί ότι όλοι οι παράγοντες που σχετίζονται με ένα σύστημα, τόσο σε επίπεδο στοιχείων όσο και σε επίπεδο συνόλου, είναι καθορισμένοι και κανείς δεν αφήνεται στην τύχη. Έτσι, τα στοιχεία που απαρτίζουν το σύστημα είναι σαφώς καθορισμένα, όπως επίσης καθορισμένη είναι η λειτουργία του καθενός από αυτά και ο επιμέρους αντικειμενικός σκοπός του. Επίσης η αλληλεξάρτηση, η αλληλεπίδραση και η συνοχή όλων των στοιχείων του συστήματος είναι καθορισμένη από ένα σχέδιο εσωτερικής οργάνωσης και δομής με κάποιο συγκεκριμένο τελικό αντικειμενικό σκοπό σε επίπεδο συνόλου.

2.2 Διαχωρισμός συστημάτων

Γενικά, τα συστήματα χωρίζονται σε μεικτά, φυσικά και τεχνητά:

Μεικτά είναι αυτά των οποίων τα στοιχεία είναι άνθρωποι και υλικά μέσα. Χαρακτηριστικά παραδείγματα αποτελούν μια Βιομηχανική Μονάδα, ένας Οργανισμός Παροχής Υπηρεσιών, καθώς και ένα Πληροφοριακό Σύστημα – μιας και σημαντικό του στοιχείο είναι οι χρήστες.

Φυσικό Σύστημα θα μπορούσε να είναι ένας οποιοσδήποτε ζωντανός (φυσικός) οργανισμός, και τελειότερο παράδειγμα αυτού είναι ο άνθρωπος.

Τεχνητό Σύστημα αποτελεί ένα μηχάνημα που είναι κατασκευασμένο μόνο από υλικά μέσα, όπως για παράδειγμα ένα ρομπότ ή ένας Ηλεκτρονικός Υπολογιστής. («Διοικητικά Πληροφοριακά Συστήματα», Δ.Γιαννακόπουλος, Ι.Παπουτσής).

2.3 Τι είναι Πληροφοριακό Σύστημα

Πληροφοριακό σύστημα είναι ένα σύνολο αλληλοσυνδεόμενων υποσυστημάτων που δουλεύουν μαζί για να συγκεντρώσουν, να επεξεργαστούν, να αποθηκεύσουν, να μετατρέψουν και να διανείμουν πληροφορίες για σχεδιασμό, λήψη αποφάσεων και έλεγχο.

Αναφέρεται στη χρήση της τεχνολογίας των υπολογιστών με σκοπό την παροχή των κατάλληλων πληροφοριών στους χρήστες. Επομένως πληροφοριακό σύστημα είναι μια συλλογή από υλικό (hardware) και λογισμικό (software) υπολογιστών που είναι σχεδιασμένα να μετατρέπουν δεδομένα σε χρήσιμη πληροφορία

Κάθε σύστημα επικοινωνεί με το περιβάλλον του δεχόμενο εισροές από αυτό, τις οποίες μετασχηματίζει στο εσωτερικό του και αποδίδει με τη σειρά του τα αποτελέσματα του μετασχηματισμού αυτού στο περιβάλλον, παράγοντας έτσι εκροές από αυτό. Η λειτουργίας της εισροής στο σύστημα είναι γνωστή ως είσοδος (INPUT), το σύνολο των εκροών από το σύστημα ως έξοδος (OUTPUT), και τέλος, η διαδικασία του μετασχηματισμού των εισροών στο εσωτερικό του συστήματος καλείται επεξεργασία.

Το input ενός πληροφοριακού συστήματος μπορεί να είναι δεδομένα ή πληροφορίες. Τα δεδομένα είναι πρώτες πληροφορίες (raw facts) για γεγονότα που δεν έχουν οργάνωση ή νόημα, τα οποία μπορούν ωστόσο να οργανωθούν με τέτοιο τρόπο ώστε να είναι χρήσιμα και να έχουν νόημα για τον κόσμο.

Όταν τα δεδομένα εκθέτουν αυτά τα χαρακτηριστικά, τότε είναι πληροφορίες. Τα πληροφοριακά συστήματα επεξεργάζονται αυτά τα δεδομένα ή τις πληροφορίες κατατάσσοντάς τα, οργανώνοντάς τα, ή επεξεργάζοντάς τα με τέτοιο τρόπο ώστε να είναι αποτέλεσμα ως πληροφορίες.

Οι managers χρησιμοποιούν τις πληροφορίες για να σχεδιάσουν, να πάρουν αποφάσεις και να ελέγξουν τους οργανισμούς. Οι λογιστές παράγουν προϋπολογισμούς (budgets) έτσι ώστε οι managers να μπορούν να συγκρίνουν την πραγματική και υπάρχουσα κατάσταση με τους στόχους τους και να ελέγχουν τις κινήσεις τους ώστε να αποφύγουν τυχόν λάθη.

2.3.1 Είδη πληροφοριακών συστημάτων

Παρατίθενται ορισμένα είδη πληροφοριακών συστημάτων για μεγαλύτερη κατανόηση:

I) «Συστήματα επεξεργασίας και υποστήριξης δοσοληψιών και δεδομένων» :

Επεξεργάζονται σε πρώτο επίπεδο τα δεδομένα που προκύπτουν από τις δοσοληψίες μιας επιχείρησης ή ενός οργανισμού. Αυτά τα συστήματα μέσα σε μια επιχείρηση διαχειρίζονται λογιστικά τις παραγγελίες των πελατών, την προμήθεια των πρώτων υλών από τους προμηθευτές, την κίνηση αποθήκης, την μισθοδοσία κλπ. Τα απλά Λογιστικά Πληροφοριακά Συστήματα θεωρούνται πως ανήκουν σε αυτήν την κατηγορία.

2) «Διοικητικά πληροφοριακά Συστήματα» :

Προσφέρουν τις κατάλληλες πληροφορίες για την διοίκηση ενός οργανισμού. Συνεργάζονται με τα υπόλοιπα πληροφοριακά συστήματα της επιχείρησης από τα οποία αποσπούν τις κατάλληλες πληροφορίες που είναι χρήσιμες για τη διοίκηση.

Το Διοικητικό Πληροφοριακό Σύστημα αποτελείται από τρία υποσυστήματα*:

- Το πληροφοριακό σύστημα *Marketing* που υποστηρίζει τις πωλήσεις, συνεργάζεται και χρησιμοποιεί πληροφορίες από το Λογιστικό Πληροφοριακό Σύστημα. Χρησιμοποιεί επίσης κι άλλες πληροφορίες όπως το προφίλ και τις προτιμήσεις των πελατών, πληροφορίες για τους ανταγωνιστές κλπ.

- Το πληροφοριακό σύστημα *παραγωγής* που χρησιμοποιείται στην παραγωγική διαδικασία, συνεργάζεται με το Λογιστικό Πληροφοριακό Σύστημα και αντλεί δεδομένα απ' αυτό, όπως σύνολα απογραφών και πληροφορίες κοστολόγησης. Επίσης χρησιμοποιεί δεδομένα για τις πρώτες ύλες, τις νέες τεχνικές παραγωγής κλπ.

- Το *οικονομικό* πληροφοριακό σύστημα που συνεργάζεται άμεσα με το Λογιστικό Πληροφοριακό Σύστημα και αντλεί δεδομένα όπως σύνολα ταμειακών ροών και πληροφορίες πληρωμών. Άλλες πληροφορίες που χρησιμοποιεί αναφέρονται στο προφίλ των δανειστών, την πιστωτική αγορά κλπ.

*Τα τρία υποσυστήματα που αναφέρθηκαν είναι τα βασικά, τα οποία συναντώνται σε χρήση σε πολλές επιχειρήσεις, αλλά δεν είναι τα μοναδικά. Καθένας τομέας ή τμήμα μιας επιχείρησης που παρουσιάζει ιδιαίτερο ενδιαφέρον για την επιχείρηση μπορεί να υποστηριχτεί από το δικό του πληροφοριακό σύστημα. Για παράδειγμα, μπορούν να χρησιμοποιηθούν «συστήματα διαχείρισης αναφορών» ή πληροφοριακά συστήματα εσωτερικού ελέγχου για τον εσωτερικό έλεγχο της επιχείρησης.

Είναι σημαντικό να κατανοηθεί πως όλα αυτά τα υποσυστήματα δεν είναι φυσικώς ανεξάρτητα αλλά κυρίως πρόκειται για ένα λογικό διαχωρισμό. Αντίθετα όλα διαμοιράζονται τους ίδιους πληροφοριακούς πόρους της επιχείρησης και κυρίως όλα εξαρτώνται από το Λογιστικό Πληροφοριακό Σύστημα της επιχείρησης από το οποίο αντλούν τα αποτελέσματα των διαφόρων δραστηριοτήτων της επιχείρησης αλλά και άλλες πληροφορίες.

3) «Συστήματα υποστήριξης αποφάσεων» :

Προσφέρουν κυρίως στο διευθυντικό προσωπικό τη δημιουργία πληροφοριών με σκοπό την υποστήριξη των αποφάσεων που κάθε φορά πρέπει να ληφθούν. Σε αντίθεση με τα συστήματα διαχείρισης αναφορών, τα οποία αρκούνται να προσφέρουν συγκεκριμένο είδος πληροφοριών με συγκεκριμένο τρόπο, τα συστήματα υποστήριξης αποφάσεων προσφέρουν πολύ μεγαλύτερη ελευθερία στη δημιουργία 'προσωπικών' μοντέλων αποφάσεων, βάσεων δεδομένων και τύπο αναφορών. Στενά συνδεδεμένα είναι τα συστήματα βάσεων γνώσης που βασίζονται στα έμπειρα συστήματα, την τεχνητή νοημοσύνη και τα νευρωνικά δίκτυα.

2.4 Η Έννοια της Πληροφορίας

Πληροφορία (information) λέγεται το σύνολο των γεγονότων ή δεδομένων (data), τα οποία έχουν συλλεχθεί και δομηθεί με τέτοιο τρόπο, ώστε να έχουν συγκεκριμένη σημασία.

Σε γενικά πλαίσια τα δεδομένα είναι λίγο – πολύ ακατέργαστα και ασύνδετα γεγονότα μεταξύ τους. Η πληροφορία αναφέρεται σε δεδομένα που έχουν συστηματικοποιηθεί και ταξινομηθεί σε κατηγορίες και σχήματα, τα οποία όταν εφαρμόζονται στην πράξη

μετατρέπονται σε γνώση που παράγει καινούρια δεδομένα. («Λογιστικά Πληροφοριακά Συστήματα – Σύγχρονες Υπηρεσίες», Β.Ταμπακάς - Γ.Ορφανός, σημειώσεις ομώνυμου μαθήματος)

2.4.1 Χαρακτηριστικά Πληροφορίας

Η χρησιμότητα και η αξία της πληροφορίας εξαρτάται από τον βαθμό στον οποίο ικανοποιούνται τα παρακάτω χαρακτηριστικά της:

- ***Σχετικότητα (Relevance):*** Ο χρήστης συλλέγει πληροφορίες προκειμένου να τις χρησιμοποιήσει σε μια τρέχουσα κατάσταση.
- ***Πληρότητα (Completeness):*** Εδώ έχει τη δυνατότητα πρόσβασης σε όλες τις αναγκαίες πληροφορίες.
- ***Ακρίβεια (Accuracy):*** Η απουσία υπολογιστικών σφαλμάτων μιας πληροφορίας τον βοηθά στην εξαγωγή συμπερασμάτων με μεγάλη ακρίβεια, εκφράζοντας την κατάσταση ενός γεγονότος όπως αυτό είναι στην πραγματικότητα.
- ***Επικαιρότητα (Timeliness):*** Η αξία μιας πληροφορίας σε ένα συνεχώς μεταβαλλόμενο περιβάλλον μειώνεται, όσο μεγαλώνει ο χρόνος διάθεσής της. Η άμεση μετάδοση της πληροφορίας

στους σωστούς αποδέκτες της προσδίδει προστιθέμενη αξία, μιας και οι πληροφορίες θα πρέπει να δίνονται στον χρήστη τη στιγμή που τις χρειάζεται.

- ***Ταχύτητα (Speed):*** Η δυνατότητα πρόσβασης στην πληροφορία μέσα στα απαιτούμενα χρονικά πλαίσια.
- ***Αντικειμενικότητα:*** Μια πληροφορία όταν προκύπτει μέσω σαφών και προσδιορισμένων διαδικασιών, τότε μειώνει αισθητά τις πιθανότητες να εμπεριέχει υποκειμενικά σφάλματα.

Αναφέρονται ονομαστικά και τα χαρακτηριστικά:

- ***Αποτελεσματικότητα Κόστους (Cost effectiveness)***
- ***Ελεγξιμότητα (Audibility).***

Συνοψίζοντας λοιπόν, όταν η πληροφορία έχει όλα τα παραπάνω, θεωρείται *αξιόπιστη (Reliable).*

Η επεξεργασία πληροφοριών είναι μια σημαντική λειτουργία στον χώρο της επιχείρησης με ευρύτερες κοινωνικές διαστάσεις. Ένα μεγάλο μέρος της εργασίας και του προσωπικού χρόνου κάθε χρήστη καταναλώνεται στην καταγραφή, αναζήτηση και απορρόφηση πληροφοριών, με τη βοήθεια πάντα των Η/Υ οι οποίοι έχουν εξελιχθεί σε αναπόσπαστο κομμάτι της οργανωμένης αυτής διαδικασίας, λόγω των μεγάλων δυνατοτήτων τους.

2.4.2 Ιδιότητες της Πληροφορίας

- Το περιεχόμενο μιας πληροφορίας δεν αλλάζει αν αλλάξει η μορφή της.
  Πολλές φορές επιβάλλεται κάτι τέτοιο, προκειμένου να είναι επεξεργάσιμη από διάφορα ηλεκτρονικά συστήματα και μεταδόσιμη από τα μέσα ηλεκτρονικής μετάδοσης.

- Η λήψη και η μετατροπή των πληροφοριών αποτελεί βασική προυπόθεση για την ύπαρξη και προσαρμοστικότητα των ζωντανών οργανισμών.

- Η πληροφορία ακολουθεί έναν δικό της κύκλο αναπαραγωγής και χρήσης ανάλογα με τη δραστηριότητα στην οποία αναφέρεται.

- Η πληροφορία μειώνει την αοριστία, καθώς είναι αποτέλεσμα επεξεργασίας δεδομένων κατωτέρου επιπέδου.

- Η πληροφορία παίζει το ρόλο της αναδραστικής σύνδεσης στα συστήματα που έχουν δυνατότητα αυτορρύθμισης και αυτοοργάνωσης. («Τα Πληροφοριακά Συστήματα Διοίκησης Στη Νέα Οικονομία», Παν.Σ.Αναστασιάδης)

2.4.3 Κρισιμότητα, Εμπιστευτικότητα των Πληροφοριών

Διαπιστώνεται ότι υπάρχει διαφορά ανάμεσα στα δεδομένα και στις πληροφορίες καθώς, ο ρόλος του Η/Υ συνίσταται στη μετατροπή των δεδομένων σε κάποιο ιστόγραμμα ή καμπύλη που να δίνει όσο γίνεται πιο περιεκτικά και παραστατικά τις απαραίτητες πληροφορίες στο λογιστικό στέλεχος.

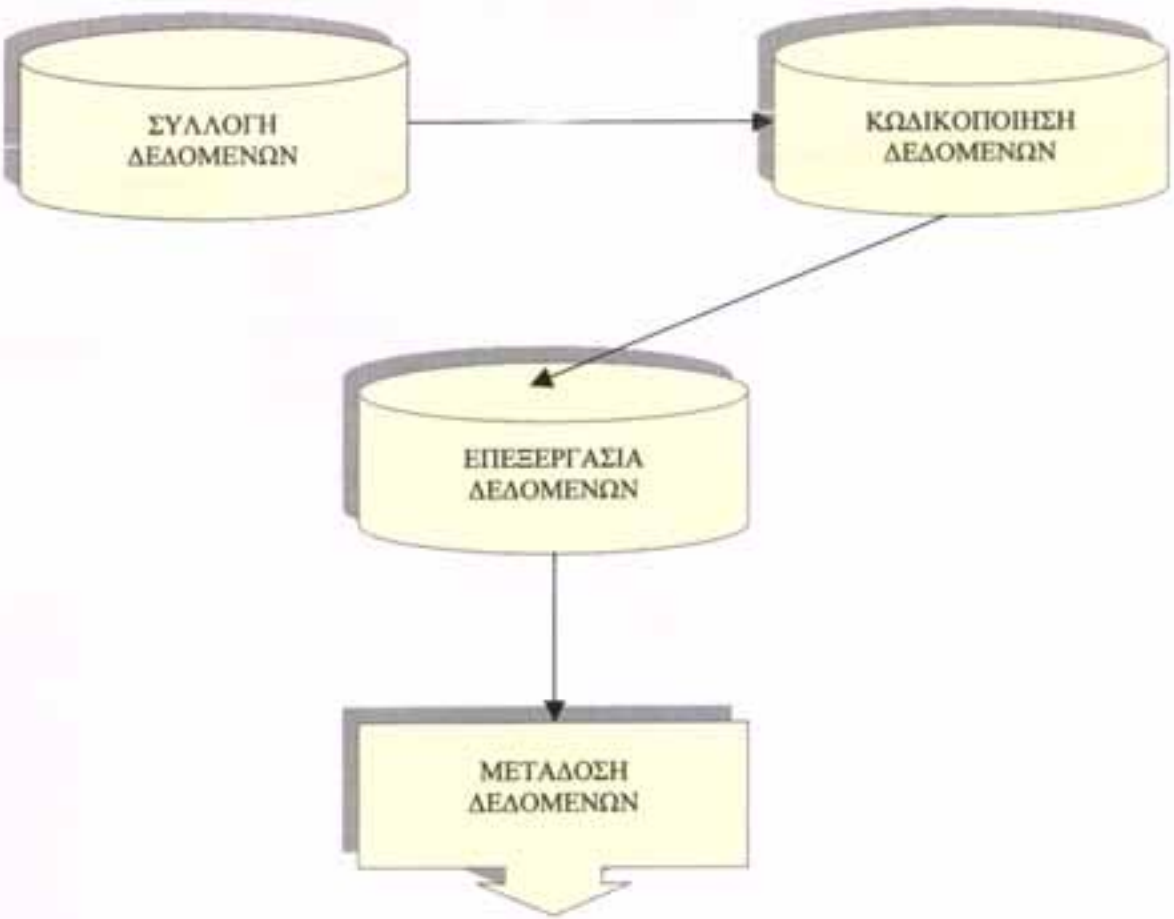
Για μεγάλο χρονικό διάστημα τόσο οι επιστήμονες όσο και οι επαγγελματίες του κλάδου της πληροφορικής και των Η/Υ έριχναν όλο το βάρος στην όσο το δυνατό καλύτερη επεξεργασία δεδομένων, για κάποιο εργασιακό περιβάλλον. Αργότερα όμως έγινε αντιληπτό ότι αυτά τα δεδομένα ήταν στην πραγματικότητα πληροφορίες που είχαν ξεχωριστή αξία και η κατοχή των οποίων σήμαινε πρόσβαση σε πηγές εξουσίας.

Η επεξεργασία δεδομένων άργησε πολύ να γίνει επεξεργασία πληροφοριών, γεγονός που οφείλεται στην μεταβολή της φιλοσοφίας αντιμετώπισης των υποκειμένων επεξεργασίας.

Έτσι παρατηρείται πιθανή ανασφάλεια ενός πληροφοριακού συστήματος κι έτσι οι επαγγελματίες του κλάδου πρέπει να υιοθετήσουν αποτελεσματικά μέτρα εξασφάλισης από κάθε ανεπιθύμητη ενέργεια.

2.5 Η έννοια των δεδομένων

Τα δεδομένα σε όποια μορφή κι αν βρίσκονται, είναι διάσπαρτα σε διάφορα σημεία είτε μέσα, είτε έξω από την επιχείρηση. Η αξιοποίησή τους απαιτεί το σχεδιασμό και την υλοποίηση μιας καλά οργανωμένης προσπάθειας που αποτελείται από τέσσερα στάδια: την συλλογή, την κωδικοποίηση, την επεξεργασία και τέλος την μετάδοσή τους.



Σχήμα: Τα τέσσερα βήματα για την αξιοποίηση των δεδομένων.

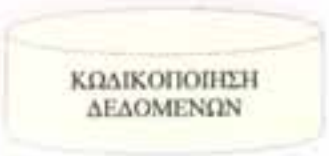
Η κατανόηση του τρόπου με τον οποίο λειτουργεί μια επιχείρηση είναι απαραίτητη προκειμένου να εντοπίσει κανείς τις πηγές που βρίσκονται τα δεδομένα, καθώς και τον τρόπο με τον οποίο αυτά μπορούν να «εξορυχτούν»

ΣΥΛΛΟΓΗ ΔΕΔΟΜΕΝΩΝ

Η κλασσική μέθοδος ***συλλογής*** των δεδομένων εμπεριέχει έξι βασικά στάδια:

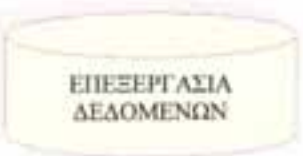
1) *Μελέτη βασικών στοιχείων της επιχείρησης*, η οποία μας δίνει μια γενική εικόνα για τη δραστηριότητά της και μας οδηγεί στον εντοπισμό των τμημάτων στα οποία θα πρέπει να υπάρχει η πληροφορία.
2) *Προσωπική παρατήρηση*, κατά την οποία μπαίνουν στο μικροσκόπιο τα παραπάνω στοιχεία ώστε να εντοπιστούν πιθανές αποκλίσεις.
3) *Διερεύνηση πραγματικής κατάστασης*. Εδώ ερχόμαστε σε επαφή με τα πρόσωπα – κλειδιά της επιχείρησης, τα οποία θα μπορούσαν να μας παρείχαν έγκυρη πληροφόρηση.
4) *Σχεδιασμός ειδικού εντύπου συλλογής των δεδομένων*, με το οποίο θα απευθυνθούμε σε αυτά τα πρόσωπα, ώστε να έχουμε αργότερα τη δυνατότητα να κωδικοποίησουμε τα δεδομένα και να λάβουν επεξεργάσιμη μορφή.
5) *Διανομή – συμπλήρωση – περισυλλογή του ειδικού εντύπου*, εργασίες που αναλαμβάνουν τα στελέχη της επιχείρησης και τέλος,

6) *Έλεγχος*, στο στάδιο του οποίου ο υπεύθυνος μηχανογράφησης ελέγχει τα παραπάνω έντυπα που του έχουν αποσταλλεί.



Προκειμένου τα δεδομένα να είναι επεξεργάσιμα με ηλεκτρονικό τρόπο, πρέπει να μετατραπούν σε μια αναγνωρίσιμη μορφή εκφραζόμενη σε μια ξεχωριστή γλώσσα με το δικό της αλφάβητο, συντακτικό και λεξιλόγιο.

Η διαδικασία της ***κωδικοποίησης*** περιλαμβάνει δύο φάσεις, την κωδικοποίηση *πριν* και *μετά* την εισαγωγή των δεδομένων. Στη μεν πρώτη υπάρχουν χαρακτήρες όπως γράμματα, ψηφία, σύμβολα, τα οποία στο σύνολό τους δημιουργούν λογικές εγγραφές, ενώ στη δεύτερη τα παραπάνω δεδομένα μετασχηματίζονται αυτόματα κατά την είσοδό τους στον Η/Υ, παίρνοντας δυαδική μορφή.



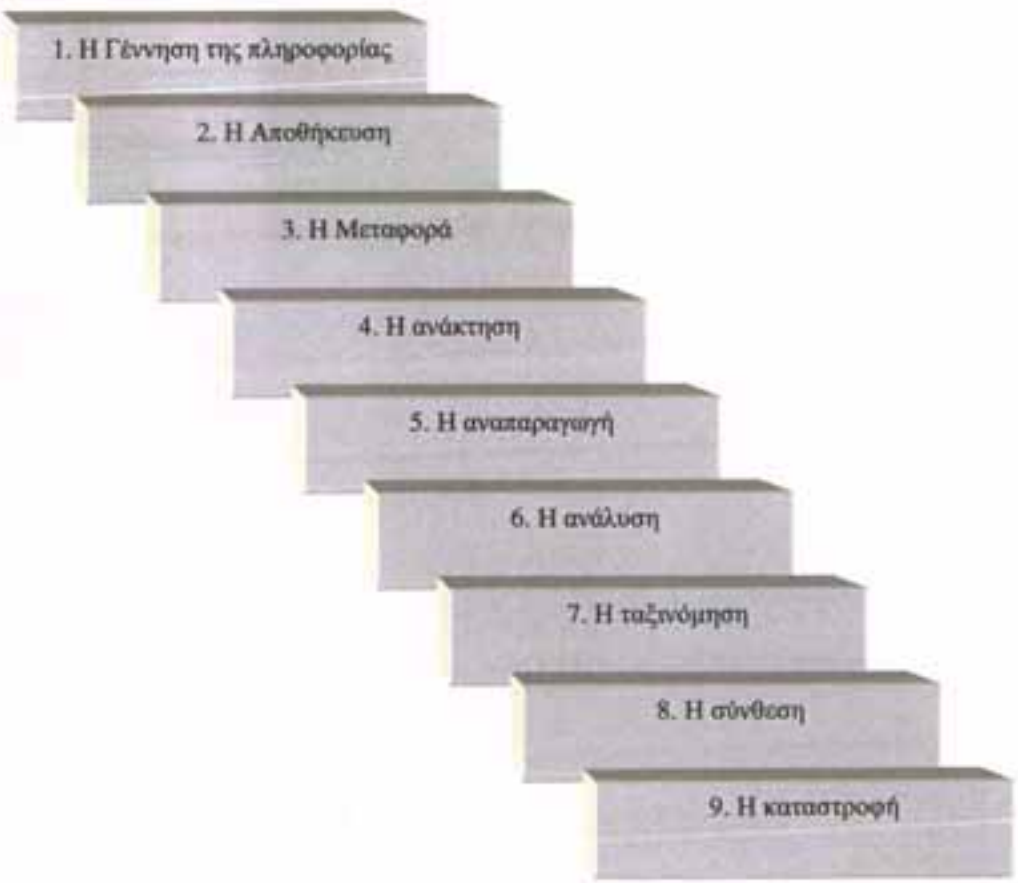
Στη συνέχεια ακολουθεί η ***επεξεργασία***, το τρίτο βήμα αξιοποίησης των δεδομένων, η οποία συμπεριλαμβάνει την κατηγοριοποίησή τους, τη διάταξη, τη σύνοψη και των υπολογισμό τους, καθώς και τους τρόπους αποθήκευσης και ανάκτησής τους. Μπορεί να γίνει είτε με τον παραδοσιακό χειρόγραφο τρόπο, είτε με τη βοήθεια του Η/Υ.

ΜΕΤΑΔΟΣΗ ΔΕΔΟΜΕΝΩΝ

Τα δεδομένα μετά την επεξεργασία τους πρέπει να μεταφερθούν με ηλεκτρονικό τρόπο στο τμήμα ή το συνεργάτη της επιχείρησης, ο οποίος τα χρειάζεται προκειμένου να εκτελέσει το έργο που του έχει ανατεθεί.

Η ***μετάδοση*** λοιπόν αυτών, γίνεται μέσω της μετατροπής τους σε ηλεκτρομαγνητικά σήματα ενέργειας.

Ο κύκλος της ζωής των πληροφοριών και των δεδομένων απεικονίζονται στο παρακάτω σχήμα:



Σχήμα: Ο κύκλος ζωής των πληροφοριών και των δεδομένων

ΚΕΦΑΛΑΙΟ 3ο
ΓΕΝΙΚΑ ΠΕΡΙ ΛΟΓΙΣΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

3.1 Η Έννοια του Λογιστικού Πληροφοριακού Συστήματος

Η λογιστική είναι από μόνη της ένα πληροφοριακό σύστημα και μια επικοινωνιακή διαδικασία που συλλέγει, αποθηκεύει, επεξεργάζεται και διανέμει πληροφορίες σε όσους τις χρειάζονται.

Για παράδειγμα, οι λογιστές στις εταιρίες συλλέγουν δεδομένα για την πορεία του οργανισμού, τα οποία τα επεξεργάζονται, τα παράγουν και τα διανέμουν ως οικονομικά στοιχεία. Δεν εμπλέκονται με την απευθείας παραγωγή των αγαθών και των υπηρεσιών, αντίθετα απασχολούνται σε υπαλληλικές θέσεις ενός οργανισμού με σκοπό την υποστήριξή του και την επίτευξη των στόχων του.

Ας θεωρήσουμε ένα πληροφοριακό σύστημα, το οποίο σαν υποσύστημα ενός οργανισμού, έχει σαν στόχο να παρέχει πληροφορίες στα στελέχη του Λογιστηρίου, επεξεργαζόμενο διάφορα δεδομένα, με σκοπό να υποστηρίζει λογιστικές

πράξεις και αποφάσεις για την αποτελεσματικότερη άσκηση των καθηκόντων τους.

Ένα τέτοιο σύστημα ονομάζεται **Λογιστικό Πληροφοριακό Σύστημα – Λ.Π.Σ. (αγγλικός όρος ACCOUNTING INFORMATION SYSTEM ή εν συντομία A.I.S.)** Οι εισροές σε ένα τέτοιο σύστημα ονομάζονται δεδομένα (DATA) και οι εκροές πληροφορίες (INFORMATION).

3.2 Ο ρόλος του λογιστή στην ανάπτυξη συστημάτων

Πολλές φορές ζητείται από τους λογιστές ή από τους ελεγκτές (Auditors) να συμμετέχουν σε δραστηριότητες και συγκεκριμένες διεργασίες που έχουν σχέση με την ανάπτυξη ή την επιβεβαίωση των Λογιστικών Πληροφοριακών Συστημάτων. Οι λογιστές συμμετέχουν στα πλαίσια εσωτερικών έργων της επιχείρησης που εργάζονται, ή σαν εξωτερικοί σύμβουλοι, ενώ οι ελεγκτές συνήθως αναμειγνύονται σε θέματα ανάπτυξης κατά τη διάρκεια της πιστοποίησης των ελέγχων που διενεργεί ένα πληροφοριακό σύστημα.

Γενικά, οι τρεις γενικές φάσεις που περιέχονται στην ανάπτυξη ενός συστήματος ειναι:

1) Η ανάλυση του συστήματος

2) Ο σχεδιασμός του και

3) Η υλοποίησή του.

ΑΝΑΛΥΣΗ ΣΥΣΤΗΜΑΤΟΣ

Κατ'αρχήν η *ανάλυση* του συστήματος έχει να κάνει κυρίως με την τυποποίηση και αξιολόγηση των λύσεων στα προβλήματα που αντιμετωπίζει ο εκάστοτε χρήστης. Η ανάλυση αναφέρεται σε ολόκληρο το σύστημα και μεταξύ των άλλων προσδιορίζει τα χαρακτηριστικά και τις λειτουργίες που αυτό θα προσφέρει. Οι βασικοί σκοποί της ανάλυσης είναι:

- Να βελτιώσει την ποιότητα της πληροφορίας προς δύο κατευθύνσεις, α) την πληροφορία που έχει ήδη ληφθεί από τους χρήστες για το πως θέλουν να οργανωθεί το υπό ανάπτυξη σύστημα και β) την πληροφορία που θα δίνει το ίδιο το σύστημα όταν αναπτυχθεί, δηλ. τις υπηρεσίες και τις λειτουργίες που θα προσφέρει.

- Να βελτιώσει τον εσωτερικό έλεγχο

- Να ελαχιστοποιήσει τα κόστη, όπου αυτό είναι δυνατό.

ΣΧΕΔΙΑΣΜΟΣ ΣΥΣΤΗΜΑΤΟΣ

Εν συνεχεία, ο *σχεδιασμός* του συστήματος σκοπό έχει να προσδιορίσει τις λεπτομέρειες των λύσεων που έχουν προταθεί από τη φάση της ανάλυσης και τέλος,

ΥΛΟΠΟΙΗΣΗ ΣΥΣΤΗΜΑΤΟΣ

Κατά την *υλοποίηση* του συστήματος γίνεται η τελική διαδικασία κατά την οποία θα μετατραπεί το πλήρως σχεδιασμένο σύστημα σε ένα σύστημα έτοιμο προς λειτουργία. Για παράδειγμα, αν αναφερόμαστε σε ένα νέο πρόγραμμα για υπολογιστές τότε η υλοποίηση μεταξύ των άλλων περιλαμβάνει τη συγγραφή του τελικού κώδικα σε κάποια γλώσσα προγραμματισμού.

Κατά τη συνολική διαδικασία ανάπτυξης ενός πληροφοριακού συστήματος προκύπτουν ποικίλα προβλήματα. Τέτοια μπορούν να είναι τεχνικά καθώς και οργανωτικά ή διαχειριστικά. Όλη η διαδικασία της ανάπτυξης όμως, πρέπει να αντιμετωπιστεί ως ένα έργο που στελεχώνεται από εκπροσώπους της διοίκησης, των χρηστών και το προσωπικό ανάπτυξης.

Μάλιστα, το γεγονός της ανάπτυξης ιδιαίτερα των χρηστών, αποτελεί πολύ σημαντική στρατηγική που εξασφαλίζει το χαμηλότερο κόστος λειτουργίας του συστήματος, καθώς και μακροβιότητα. Επιπροσθέτως, ένα νέο πληροφοριακό σύστημα κατά κανόνα αλλάζει τις εργασιακές σχέσεις του προσωπικού, αφού αλλάζει το περιεχόμενο της εργασίας και ίσως την τυπική οργανωτική δομή της επιχείρησης.

Έτσι, η συνεργασία των χρηστών είναι πολύ σημαντική γιατί στην ουσία οι χρήστες είναι αυτοί που θα δώσουν τις αρχικές πληροφορίες για την ανάπτυξη του συστήματος και αυτοί είναι που θα το δοκιμάσουν μετά την ολοκλήρωσή του. («Λογιστικά Πληροφοριακά Συστήματα – Σύγχρονες Υπηρεσίες», Β.Ταμπακάς - Γ.Ορφανός, σημειώσεις ομώνυμου μαθήματος)

3.3 Τεχνικές Τεκμηρίωσης των ΛΠΣ

Για την ανάλυση, τον σχεδιασμό και την τεκμηρίωση των συστημάτων και των υποσυστημάτων ενός Λογιστικού Πληροφοριακού Συστήματος χρησιμοποιούνται συγκεκριμένες μέθοδοι που είναι γνωστές ως Τεχνικές Τεκμηρίωσης Συστημάτων. Αυτές οι τεχνικές χρησιμοποιούν κυρίως διαγράμματα και γι' αυτό χαρακτηρίζονται ως γραφικές τεχνικές.

Η χρήση των διαγραμμάτων δίνει σημαντικά πλεονεκτήματα γιατί προσφέρει τον απαραίτητο βαθμό εποπτείας για την αναπαράσταση, τον έλεγχο και την ανάλυση ενός συστήματος.

Οι γραφικές μέθοδοι ανάλυσης και τεκμηρίωσης θεωρούνται ένα απαραίτητο βήμα κατά τη δημιουργία οποιουδήποτε ΛΠΣ. Χρησιμοποιούνται κατ' αρχάς από το προσωπικό που ασχολείται με την ανάλυση και το σχεδιασμό του συστήματος, είτε είναι εξειδικευμένο σε θέματα πληροφορικής, είτε είναι λογιστές που λαμβάνουν μέρος στο σχεδιασμό του λογιστικού συστήματος. Γενικά τα διαγράμματα τεκμηρίωσης που έχουν αναπτυχθεί για ένα σύστημα αποτελούν ένα σημαντικό μέρος του και το συνοδεύουν σε όλο τον κύκλο της ζωής του. Σε αυτά προστρέχει κατά κύριο λόγο οποιοσδήποτε θέλει να κατανοήσει ή να βελτιώσει, και τελικά να ελέγξει ένα Λογιστικό Πληροφοριακό Σύστημα.

3.3.1 Χρησιμοποίηση των Τεχνικών Τεκμηρίωσης στο σχεδιασμό και ανάπτυξη των Συστημάτων

Για το σχεδιασμό και ανάπτυξη ενός ΛΠΣ συνεργάζονται αρκετοί άνθρωποι διαφόρων ειδικοτήτων. Κατά κύριο λόγο λαμβάνουν μέρος οι Λογιστές,

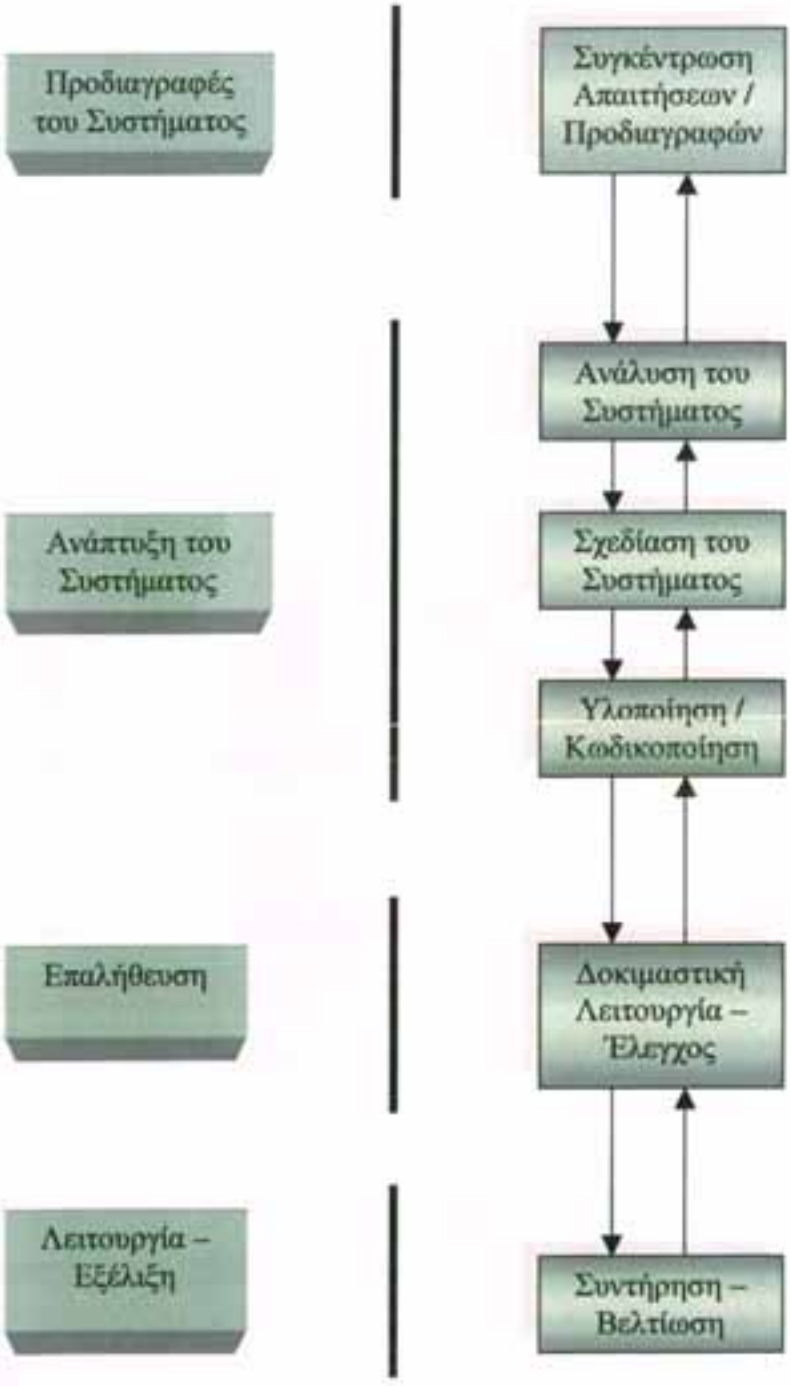
που συνεισφέρουν στη συγκέντρωση των απαιτήσεων που πρέπει να ικανοποιεί το σύστημα, στο σχεδιασμό και στον έλεγχο λειτουργίας του συστήματος.

Επίσης λαμβάνουν μέρος ειδικοί της πληροφορικής που έχουν ευθύνη του σχεδιασμού, της υλοποίησης του συστήματος αλλά και της βελτίωσής του, όταν αυτό είναι απαραίτητο. Οι έννοιες αυτές επεξηγούνται στη συνέχεια μέσω των *μοντέλων κύκλου ζωής* των πληροφοριακών συστημάτων.

3.3.2 Μοντέλα κύκλου ζωής και το μοντέλο του Καταρράκτη

Ένα μοντέλο κύκλου ζωής περιγράφει τις εργασίες που πρέπει να γίνουν και την ομαδοποίησή τους σε φάσεις, από την αρχή δημιουργίας ενός πληροφοριακού συστήματος μέχρι και την απόσυρσή του.

Για το λόγο αυτό έχουν δημιουργηθεί και χρησιμοποιούνται αρκετά μοντέλα κύκλου ζωής. Το Μοντέλο του Καταρράκτη (Waterfall Model) είναι από τα πιο παλιά και περιγράφεται στο επόμενο σχήμα:



Σχήμα: Το Μοντέλο του Καταρράκτη

Παρατηρούμε πως το μοντέλο του Καταρράκτη υποστηρίζει 4 βασικές φάσεις:

1) Προδιαγραφές του Συστήματος

- Στη φάση των **προδιαγραφών** συγκεντρώνονται και καθορίζονται οι απαιτήσεις από το νέο πληροφοριακό σύστημα. Χρησιμοποιούνται τεχνικές συνέντευξης, ερωτηματολόγια προς τους εργαζόμενους, παρακολουθήσεις και παρατηρήσεις των λειτουργιών / διαδικασιών της επιχείρησης.

  Γενικά ο σκοπός της φάσης αυτής είναι η συγκέντρωση (κυρίως σε μορφή κειμένου) της περιγραφής των ιδιοτήτων του συστήματος με τη μορφή των απαιτήσεων όπως αυτές εκφράζονται από το εργασιακό περιβάλλον που θα εγκατασταθεί το σύστημα.

2) Ανάπτυξη του Συστήματος

I. Κατά την **ανάλυση** πραγματοποιείται η συστηματική κι επιστημονική οργάνωση και αναπαράσταση των προδιαγραφών που συγκεντρώθηκαν στην προηγούμενη φάση.

Σκοπός της ανάλυσης είναι να παρουσιαστούν με ένα σαφή και τεκμηριωμένο τρόπο οι λειτουργίες του πληροφοριακού συστήματος και των υποσυστημάτων του, η ροή των πληροφοριών που αυτό θα υποστηρίζει, μια αρχική οργάνωση των δεδομένων / αρχείων και των βάσεων δεδομένων που θα χρησιμοποιεί και μια συστηματική καταγραφή των εννοιών και όρων που θα χρησιμοποιούνται γενικά στην ανάπτυξη. Οι τεχνικές τεκμηρίωσης συστημάτων βοηθούν σημαντικά τους αναλυτές στις παραπάνω εργασίες.

Για παράδειγμα, χρησιμοποιούνται τα *Διαγράμματα Ροής Δεδομένων (Data Flow Diagrams)* για την αναπαράσταση των λειτουργιών των διαφόρων υποσυστημάτων και της ροής των πληροφοριών μεταξύ των διαδικασιών τους. Επίσης χρησιμοποιούνται τα *Διαγράμματα Ροής(Flowcharts)* και τα *Αναλυτικά Διαγράμματα Ροής* τα οποία περιγράφουν με μεγαλύτερη λεπτομέρεια τι ακριβώς κάνει κάθε υποσύστημα και κάθε διαδικασία. Τέλος, για τις βάσεις δεδομένων δημιουργούνται τα γνωστά *Διαγράμματα Οντοτήτων Συσχετίσεων (ΔΟΣ).*

II. Κατά τη **σχεδίαση** θα πρέπει το σύστημα να διαμορφωθεί στα τελικά χαρακτηριστικά του, τα οποία πρέπει να περιγράφουν λεπτομερώς.

Σκοπός της σχεδίασης είναι να προσδιοριστούν επακριβώς τα διάφορα υποσυστήματα και οι διαδικασίες που τα αποτελούν, δηλαδή να προσδιοριστεί η λεπτομερής αρχιτεκτονική του πληροφοριακού συστήματος. Επίσης θα πρέπει να προσδιοριστεί με λεπτομέρεια η λειτουργικότητα της κάθε διαδικασίας (δηλ. τι κάνει η κάθε διαδικασία και με ποιο τρόπο το κάνει), ο τρόπος που συνδέονται και συνεργάζονται μεταξύ τους οι διαδικασίες, τα δεδομένα που χρησιμοποιούνται και ο τρόπος που ανταλλάσσονται. Και εδώ χρησιμοποιούνται οι τεχνικές τεκμηρίωσης συστημάτων.

Για παράδειγμα, χρησιμοποιούνται τα *Διαγράμματα Ροής Προγράμματος (Program Flowcharts)* για τη λεπτομερή περιγραφή των προγραμμάτων. Επίσης τα *IPO HIPO διαγράμματα, ο ψευτοκώδικας* κλπ. Στις βάσεις δεδομένων δημιουργείται η τελική μορφή και ο τύπος του κάθε πεδίου. Αν το πληροφοριακό σύστημα περιλαμβάνει και διαχείριση εγγράφων σχεδιάζονται ηλεκτρονικές φόρμες διαχείρισης και ο τρόπος δρομολόγησης των εγγράφων. Αν η σχεδίαση είναι επιτυχής τότε η υλοποίηση είναι μια απλή υπόθεση.

III. Η **υλοποίηση** περιλαμβάνει την κωδικοποίηση, τη συνένωση και τον έλεγχο των προγραμμάτων για τους υπολογιστές, την εκπαίδευση του προσωπικού, την εγκατάσταση νέου εξοπλισμού για υπολογιστές και τη συγγραφή της υπόλοιπης τεκμηρίωσης (documentation) του συστήματος. Μέρος της τεκμηρίωσης είναι τα διάφορα διαγράμματα που έχουν δημιουργηθεί κατά την ανάλυση και τη σχεδίαση του συστήματος. Κατά την υλοποίηση, κατά κύριο λόγο δημιουργούνται τα διάφορα εγχειρίδια χρήσης και συντήρησης του συστήματος.

3) Επαλήθευση

- Στη φάση της **επαλήθευσης** το νέο πληροφοριακό σύστημα μαζί με το νέο εξοπλισμό και το υπόλοιπο υλικό εγκαθίσταται στο εργασιακό περιβάλλον. Ακολουθεί μια δοκιμαστική χρήση από τους ίδιους τους εργαζόμενους με χρήση πραγματικών δεδομένων, η οποία αποδεικνύει αν είναι απαλλαγμένο από λάθη και αν ικανοποιεί τις αρχικές απαιτήσεις που είχαν διατυπωθεί. Αν ναι, τότε ακολουθεί η τελευταία φάση της κανονικής λειτουργίας.

4) Λειτουργία – Εξέλιξη

- Εδώ γίνονται εργασίες συντήρησης και βελτίωσης / μετατροπής του συστήματος, όταν αυτό κριθεί απαραίτητο. Και για τα δύο, σημαντικότερο ρόλο παίζει το υλικό τεκμηρίωσης που έχει δημιουργηθεί κατά τη φάση ανάπτυξης.

Χαρακτηριστικό του Μοντέλου του Καταρράκτη είναι η ακολουθιακή φύση του, δηλαδή θα πρέπει να ολοκληρωθεί συνολικά μια φάση ή υπο – φάση για να περάσουμε στην επόμενη. Αυτό με απλά λόγια σημαίνει πως πρέπει να δημιουργήσουμε τις προδιαγραφές για όλο το σύστημα, μετά να κάνουμε την ανάλυση για όλο το σύστημα, ύστερα να σχεδιάσουμε όλο το σύστημα κοκ. Στο τέλος κάθε φάσης ή υπο – φάσης γίνεται έλεγχος για να διαπιστωθεί αν όλα πήγαν κατ' ευχήν. Αν χρειαστεί μπορεί να γίνει οπισθοδρόμηση στην προηγούμενη φάση ή υπο – φάση όπου θα γίνουν οι απαραίτητες μετατροπές.

Το σύστημα εμφανίζει τα τελικά χαρακτηριστικά του μετά την υλοποίηση, όπου γίνεται και η συνένωση των διαφόρων μονάδων που το αποτελούν. Όπως αναφέρθηκε και στην αρχή, πρόκειται για ένα παλιό μοντέλο που χρησιμοποιείται αρκετά και στις μέρες μας.

Επίσης χρησιμοποιούνται και νέα, πιο αποδοτικά μοντέλα, τα οποία χρησιμοποιούν κατά βάση τις ίδιες εργασίες (φάσεις ή υπο – φάσεις) με διαφορετική όμως διάταξη και κατά κύριο λόγο ανατρέπουν την ακολουθιακή φύση του Μοντέλου του Καταρράκτη.

3.4 Λογιστικό Πληροφοριακό Σύστημα και Οικονομικές Επιστήμες

Μεταξύ των οικονομικών επιστημών, ο τομέας της Λογιστικής χαρακτηρίζεται από δυο περιοχές ενδιαφέροντος σε σχέση με τα ΛΠΣ: Το καθαρά *λογιστικό μέρος* ασχολείται με την καταχώρηση εσόδων – εξόδων για συγκεκριμένες χρονικές περιόδους, όπως κάθε μήνα ή έτος ή την έκδοση του ισολογισμού στο τέλος μιας περιόδου. Οι απολογισμοί τέτοιων περιόδων απευθύνονται προς πιθανούς επενδυτές και δημόσιους φορείς και κατά συνέπεια το καθαρά λογιστικό μέρος έχει περιορισμένη χρησιμότητα όσον αφορά τη λήψη διοικητικών αποφάσεων.

Το *διαχειριστικό* όμως μέρος ενδιαφέρει για τον προσδιορισμό συναφών δαπανών και την εκτέλεση αναλύσεων που χρησιμεύουν στον διαχειριστικό έλεγχο και τη λήψη αποφάσεων σε επίπεδο διοίκησης. Εστιάζει στην προετοιμασία προϋπολογισμών και την ανάλυση της απόδοσης σύμφωνα με τον προϋπολογισμό.

ΚΕΦΑΛΑΙΟ 4°
ΑΣΦΑΛΕΙΑ ΣΤΑ ΛΟΓΙΣΤΙΚΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Στο κεφάλαιο αυτό παρουσιάζονται τα προβλήματα Ασφάλειας των ΛΠΣ καθώς και τα μέτρα που μπορούν να ληφθούν για την προστασία τους.

Σκοπός του κεφαλαίου είναι η ευαισθητοποίηση για τα προβλήματα αυτά και για τους τρόπους αντιμετώπισης, καθώς και η ανάδειξη της σημασίας ύπαρξης σχεδίου και μηχανισμού ασφάλειας ενός Πληροφοριακού Συστήματος.

4.1 Γενικά περί Ασφάλειας ΛΠΣ

Η έννοια της ασφάλειας θα πρέπει από νωρίς να απασχολήσει έναν οργανισμό, ο οποίος επιπλέον θα πρέπει να καθορίσει και το επίπεδο ασφάλειας (ανάλογα με το κόστος). Τίποτα όμως δε μπορεί να εγγυηθεί ένα τέλειο σύστημα ασφάλειας, γι' αυτό και οι υπεύθυνοι είναι υποχρεωμένοι να μάθουν να ζουν με τη πιθανότητα ότι κάτι μπορεί να συμβεί αναλαμβάνοντας το ρίσκο της αποτυχίας του συστήματος ασφαλείας. Ακόμα, πρέπει να υπάρχει υψηλός δείκτης ετοιμότητας για επαναφορά του συστήματος.

Είναι αναγκαίο οι υπεύθυνοι να δίνουν μεγάλη σημασία στην ασφάλεια των συστημάτων που επιβλέπουν και να την επιβεβαιώνουν μετά τη προμήθεια του κατάλληλου προϊόντος (υλικού ή λογισμικού). Οι χρήστες από την άλλη μεριά, θα πρέπει να καταλάβουν τη σπουδαιότητα της προστασίας και της ασφάλειας των δεδομένων τους.

4.2 Ασφάλεια Εξοπλισμού και Πρόσβασης σε Δεδομένα

Στις μονάδες εισόδου και εξόδου του υπολογιστή πρέπει να έχουν το δικαίωμα πρόσβασης μόνον εξουσιοδοτημένα άτομα. Οι μονάδες αυτές καθώς και ο ίδιος ο υπολογιστής (όταν πρόκειται για κεντρικό σύστημα), μπορεί να βρίσκονται σε δωμάτια ελεγχόμενης πρόσβασης, που απαιτούν κάποιο ειδικό κλειδί ή μαγνητική κάρτα ή και το συνδυασμό τους.

Επιπλέον, ένας χρήστης δε μπορεί να έχει πρόσβαση σε οποιοδήποτε αρχείο δεδομένων, αλλά μόνο σε εκείνα που αφορούν τη δουλειά του. Αυτό επιτυγχάνεται με τη χρήση κωδικών από τη πλευρά του χρήστη που για λόγους αποτελεσματικότητας πρέπει να αλλάζουν περιοδικά. Αυτοί οι κωδικοί είναι τα γνωστά *passwords*. Επίσης, η πρόσβαση του εκάστοτε χρήστη πρέπει να ελέγχεται, έτσι ώστε ο καθένας να έχει περιορισμένο ορίζοντα του συστήματος, τόσο σε επίπεδο εφαρμογών, όσο και σε επίπεδο λειτουργίας.

4.2.1 Βασικές Αρχές Ασφάλειας

ΑΠΟΚΕΝΤΡΩΣΗ (DISPERSION)

Για την ολοκληρωτική καταστροφή ενός αποκεντρωμένου πληροφοριακού συστήματος απαιτούνται πολλαπλές επεμβάσεις, και γι' αυτό ο σχεδιασμός αποκεντρωμένων συστημάτων ελαχιστοποιεί τις απώλειες σε κάθε περίπτωση προσβολής. Τα τελευταία μοντέλα υπολογιστών είναι σχεδιασμένα πάνω σε αυτή την αρχή.

ΥΠΑΡΞΗ ΑΝΤΙΚΑΤΑΣΤΑΤΗ (DUBLICATION)

Αυτή η αρχή βασίζεται στην ανάγκη συνεχούς λειτουργίας ενός πληροφοριακού συστήματος, έστω κι αν πάψει κάποιο υποσύστημα να λειτουργεί. Αυτή μέθοδος είναι εξαιρετικά αποτελεσματική για την ανίχνευση λαθών στην επεξεργασία των πληροφοριών.

ΑΜΥΝΑ ΣΕ ΒΑΘΟΣ (DEFENSE IN DEPTH)

Η τρίτη αρχή στηρίζεται στο γεγονός που απαιτεί την ύπαρξη πολλαπλών ελέγχων προτού ο μη εξουσιοδοτημένος χρήστης αποκτήσει πρόσβαση στο Πληροφοριακό Σύστημα.

4.3 Διαχείριση Δικαιωμάτων και Εξουσιοδοτήσεων

Η ασφάλεια, η ακεραιότητα των δεδομένων, καθώς επίσης οι πολιτικές διάθεσης και πρόσβασης σ' αυτά, καθορίζονται με τη βοήθεια εργαλείων που συμπεριλαμβάνονται σε ένα Σύστημα Διαχείρισης Βάσεων Δεδομένων. Συνηθέστερο απ' αυτά είναι το Security Management, με το οποίο δημιουργούνται και καθορίζονται οι ρόλοι και το προφίλ των χρηστών.

Ειδικότερα:

➢ *Διαχείριση Πρόσβασης Χρηστών*

Σχεδιάζεται και επιβάλλεται για τον περιορισμό πρόσβασης στα δεδομένα και περιλαμβάνει:

- Τον καθορισμό κάθε χρήστη στη βάση δεδομένων,
- Την εκχώρηση password σε κάθε χρήστη,
- Τον καθορισμό ομάδας χρηστών,
- Την εκχώρηση δικαιωμάτων και δυνατοτήτων σε ειδικούς χρήστες και ομάδες χρηστών.

➢ *Καθορισμός θέασης δεδομένων*

Καθορίζεται η δυνατότητα της θέασης των δεδομένων σε χρήστες ή ομάδες χρηστών

➢ *Προφύλαξη δολιοφθορών*

Απαιτούνται ενέργειες για την αποφυγή σκόπιμων παρεμβάσεων από hackers ή από ανεπιθύμητες καταστροφές που προέρχονται από ιούς.

4.4 Αντίγραφα Ασφαλείας (Back – Up)

Η ύπαρξη αντιγράφων ασφαλείας αναφέρεται στη διαθέσιμη υποστήριξη μιας εγκατάστασης και χρησιμοποιούνται όταν ένα ή περισσότερα τμήματα του εξοπλισμού , που απαιτούνται για τη φυσιολογική λειτουργία του συστήματος, αχρηστεύονται ή δυσλειτουργούν για κάποιο σημαντικό διάστημα του χρόνου.

Η σπουδαιότητα της ύπαρξης των αντιγράφων ασφαλείας δε μπορεί να τεκμηριωθεί με ιδιαίτερη έμφαση. Όσο όμως και αξιόπιστο να είναι ένα σύστημα, είναι καταδικασμένο κάποτε να αποτύχει και μολονότι η μέση συχνότητα τέτοιων σφαλμάτων μπορεί να προβλεφθεί, δε μπορεί να προβλεφθεί μια διακεκριμένη εμφάνιση λάθους.

4.4.1 Αντίγραφα Ασφαλείας Υλικού

Η περίπτωση αντιγράφων ασφαλείας υλικού μπορεί να εφαρμοστεί πολύ καλά χρησιμοποιώντας μια εγκατάσταση μαγνητικής ταινίας. Είναι συχνά καλό, να κρατείται μια ταινία παραπάνω από αυτές που

απαιτούνται για τη λειτουργία του συστήματος. Κατά την εμφάνιση ενός λάθους, η επαναφορά του συστήματος είναι εύκολη υπόθεση και γίνεται με τη χρήση εφεδρικών ταινιών. Όταν ένα κρίσιμο κομμάτι του υλικού δυσλειτουργεί, όπως ένας δίσκος ή ένας κεντρικός επεξεργαστής, ο αναλυτής του συστήματος και ο χρήστης πρέπει να αναπτύξουν μια διαδικασία για να αντιμετωπίσουν το σφάλμα. Αυτή η διαδικασία μπορεί να διαπραγματεύεται την απόφαση αν το σύστημα θα λειτουργήσει σε μια άλλη μηχανή που εκτελεί τις ίδιες δραστηριότητες ή αν θα αναπτυχθούν οι δραστηριότητες αυτές για δεύτερη φορά στην ίδια θέση. Όσο απλή κι αν είναι η διαδικασία αυτή, πρέπει να αναπτυχθεί πριν την εμφάνιση του λάθους.

4.4.2 Αντίγραφα Ασφαλείας Δεδομένων

Αυτά παρέχουν την εγγύηση και τη βεβαιότητα απέναντι στην απώλεια των δεδομένων, που μπορεί να γίνει από δυσλειτουργία του υλικού, την αποτυχία του προγράμματος ή κάποιο άλλο ατύχημα. Ο τύπος των αντιγράφων ασφαλείας των δεδομένων εξαρτάται κατά πολύ από το μέγεθος των πρωτότυπων αρχείων.

4.4.3 Αντίγραφα Συστήματος

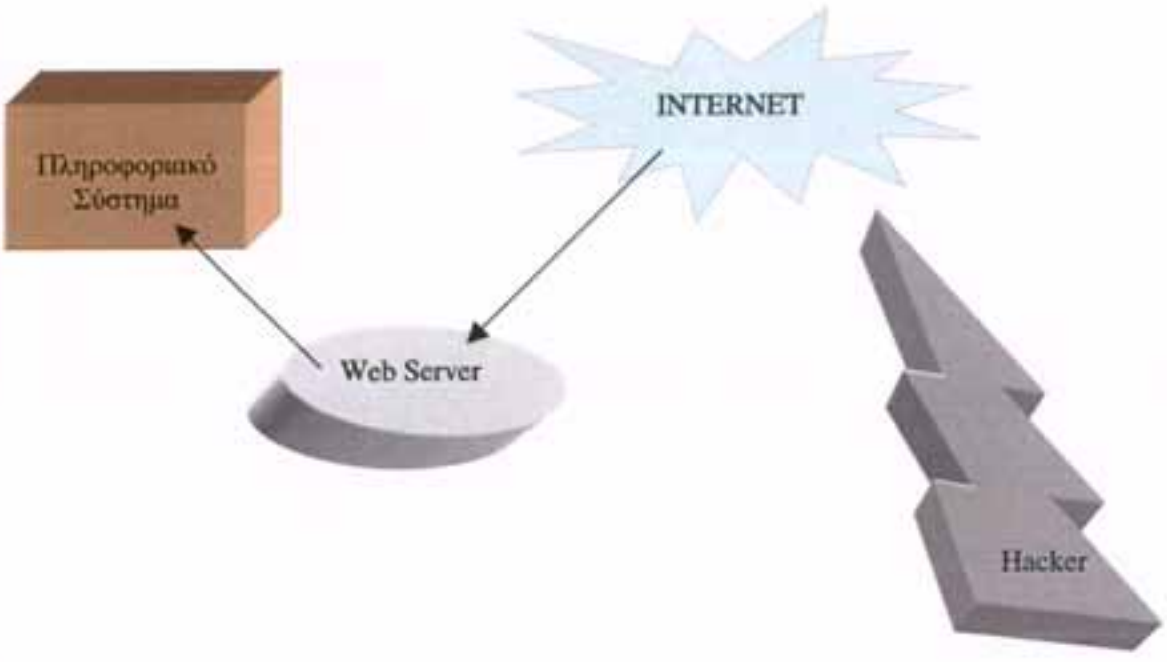
Η συντήρηση ενός μεγάλου αρχείου σε έναν δίσκο, μπορεί να απαιτεί την εξακολούθηση της λειτουργίας του συστήματος, ακόμα κι όταν ο δίσκος δε λειτουργεί σωστά. Τότε θα πρέπει να σχεδιαστεί ένα εναλλακτικό σχήμα επεξεργασίας, το οποίο θα επιτρέπει τη συνέχιση της λειτουργίας. Στη χειρότερη περίπτωση, το σύστημα μπορεί να απαιτήσει διαδικασίες ανάκτησης για τη συνέχιση της λειτουργίας του, κατά την εμφάνιση ενός παρατεινόμενου μηχανικού λάθους. («Διοικητικά Πληροφοριακά Συστήματα», Δ.Γιαννακόπουλος, Ι.Παπουτσής).

4.5 Ασφάλεια δεδομένων στα Λογιστικά Πληροφοριακά Συστήματα

Η ασφάλεια δεδομένων είναι κρίσιμος και καθοριστικός παράγοντας καθώς και κύρια απαίτηση τόσο κατά την φάση σχεδιασμού όσο και κατά την λειτουργία (επεξεργασία συναλλαγών) ενός Λογιστικού Πληροφοριακού Συστήματος. Περιλαμβάνει και λειτουργεί με μηχανισμούς που αποτρέπουν την μη εξουσιοδοτημένη πρόσβαση , αλλοίωση, και απώλεια κρίσιμων δεδομένων κατά την αποθήκευση και μεταφορά τους.

Ιδιαίτερα η ασφάλεια συναλλαγών στο Διαδίκτυο (internet) βρίσκει εφαρμογή σε σύγχρονες υπηρεσίες που σχετίζονται με εμπορικές και επιχειρηματικές δραστηριότητες, όπως είναι το ηλεκτρονικό εμπόριο και οι ηλεκτρονικές επιχειρήσεις.
(«Λογιστικά Πληροφοριακά Συστήματα – Σύγχρονες Υπηρεσίες», Γ.Ορφανός, σημειώσεις ομώνυμου μαθήματος)

Διαδικτυακές συναλλαγές που δεν γίνονται κάτω από ένα πλέγμα ασφάλειας, βάλονται από ανεπιθύμητους χρήστες και ο αντίκτυπος φθάνει και καταστρέφει το πληροφοριακό σύστημα, όπως φαίνεται στο παρακάτω σχήμα:



Σχήμα: Ανασφαλείς και απροστάτευτες διαδικτυακές συναλλαγές.

4.6 Προβλήματα ασφάλειας στα Λογιστικά Πληροφοριακά Συστήματα.

Στο σημείο αυτό γίνεται μια αναφορά στο πρόβλημα των απειλών της ασφάλειας των δεδομένων ενός Λογιστικού Πληροφοριακού Συστήματος. Οι απειλές αυτές έχουν να κάνουν με τη μη-εξουσιοδοτημένη πρόσβαση σε δεδομένα η οποία ενδέχεται να οδηγήσει σε παραβιάσεις του απόρρητου ή αλλοίωση των δεδομένων και απώλεια.

Οι επιχειρήσεις αναζητώντας την επίλυση των προβλημάτων αυτών πρώτα ορίζουν τους κινδύνους ασφάλειας και κατόπιν καθορίζουν το επίπεδο ευπάθειας για κάθε ταξινόμηση δεδομένων. Στη συνέχεια, μπορούν να εφαρμοστούν έλεγχοι λογικής πρόσβασης (logical access controls), όπου είναι απαραίτητο, για να αποδειχθεί η γνησιότητα του χρήστη.

Ένα σύστημα που υποστηρίζει έλεγχο λογικής πρόσβασης έχει τα παρακάτω συστατικά:

- Ο κωδικός πρόσβασης (συνθηματικό- password) ή το PIN περιορίζουν την πρόσβαση σε ένα σύστημα. Ωστόσο , ο διαχειριστής (administrator) του συστήματος έχει την ευθύνη για την εξασφάλιση της απορρήτου και της ακεραιότητας των δεδομένων, η γενικότερα της αποτελεσματικής λειτουργίας του συστήματος.

- Από την στιγμή που ένας χρήστης τελικά αποκτήσει πρόσβαση στο σύστημα, υπάρχουν περαιτέρω έλεγχοι για τον περιορισμό της πρόσβασής του σε αρχεία ,συναλλαγές ή λειτουργίες. Αυτό επιτρέπει την δημιουργία επιπέδων εξουσιοδότησης στο σύστημα και ως αποτέλεσμα , ο κάθε χρήστης έχει το κατάλληλο προφίλ πρόσβασης σύμφωνα με την ιδιότητα και την φύση της εργασίας του μέσα στην επιχείρηση.

- Μέτρα επίσης θα πρέπει να ληφθούν έτσι ώστε να αποφευχθεί η περίπτωση όπου κάποιος θα μπορέσει να εξάγει συμπεράσματα από την υποκλοπή (κρυφάκουσμα) μιας συναλλαγής δεδομένων ή από την πρόσβαση σε αποθηκευμένα δεδομένα. Η κύρια τεχνική προστασίας σε αυτό το πρόβλημα είναι η *κρυπτογράφηση*. Μόνο ο χρήστης με το σωστό κλειδί μπορεί να ανακτήσει και να διαβάσει τα δεδομένα.

- Επειδή τα συστήματα είναι διασυνδεδεμένα με το Διαδίκτυο είναι επιρρεπή σε εξωτερικές επιθέσεις λογισμικού (τα συστήματα firewall αμβλύνουν ή περιορίζουν στο ελάχιστο το πρόβλημα αυτό).

- Άλλοι κίνδυνοι προέρχονται από τους ιούς υπολογιστών (computer viruses) . Ο διαχειριστής του συστήματος εγκαθιστά και αναβαθμίζει τακτικά κατάλληλο λογισμικό για την ανίχνευση ιών και την εκκαθάριση προσβεβλημένων αρχείων.

- Ο διαχειριστής του συστήματος τακτικά (σύμφωνα με την πολιτική ασφαλείας της επιχείρησης) δημιουργεί αντίγραφα ασφάλειας των κρίσιμων δεδομένων για περιπτώσεις φυσικής καταστροφής των πόρων αποθήκευσης του συστήματος.

ΑΠΩΛΕΙΕΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΑΦΟΥ ΠΑΡΑΒΙΑΣΤΟΥΝ ΟΙ ΔΙΑΔΙΚΑΣΙΕΣ ΕΞΑΣΦΑΛΙΣΗΣ ΤΟΥ :

➢ Αδυναμία χρήσης του Η/Υ:

Όταν ο Η/Υ είναι εκτός λειτουργίας, διακόπτονται οι παρεχόμενες υπηρεσίες του. Η αδυναμία χρήσης ενός Η/Υ και κατά συνέπεια του συστήματος το οποίο υλοποιεί, μπορεί να οφείλεται στους εξής παράγοντες:

I. Προσωρινή διακοπή λόγω πτώσης της τάσης του ηλεκτρικού ρεύματος. Η αντιμετώπιση τέτοιων περιπτώσεων γίνεται συνήθως με γεννήτριες παροχής ηλεκτρικού ρεύματος και οι οποίες συνδέονται στο δίκτυο αυτόματα, όταν υπάρχει ανάγκη.

II. Αδυναμία σύνδεσης με τον κεντρικό Η/Υ. λόγω υπερφόρτωσης των δικτύων τηλεπικοινωνίας. Το πρόβλημα αυτό βρίσκεται σε αποκεντρωμένα Π.Σ. που λειτουργούν όμως με συγκεντρωτική μέθοδο επεξεργασίας, π.χ. δίκτυα τραπεζών.

III. Πρόβλημα υλικού εξαιτίας της μη καλής συντήρησης ή ανθρώπινου λάθους.

IV. Πρόβλημα λογισμικού εξαιτίας επαγγελματικής ανεπάρκειας ή ανθρώπινου λάθους.

➢ **Απώλεια Χρημάτων:**

Όταν καταστραφεί το Πληροφοριακό Σύστημα ή υποβαθμισθεί η λειτουργία του, τότε υπάρχει απώλεια χρημάτων η οποία μπορεί να εμφανιστεί με δυο μορφές.

Η πρώτη μορφή απώλειας χρημάτων είναι αυτή της χρήσης του Η/Υ. Είναι ένα σύνηθες φαινόμενο αφού πολλά στελέχη ενός κέντρου πληροφορικής συχνά ξεφεύγουν απ' αυτό που τους ανατέθηκε να κάνουν και χρησιμοποιούν τις δυνατότητες που έχουν για δικό τους σκοπό, ενώ η δεύτερη μορφή απώλειας είναι της σπάνιας μεν, εφικτής δε, κλοπής του Η/Υ.

➢ **Απώλεια αποκλειστικής χρήσης:**

Αν κάποιος χρησιμοποιήσει το Πληροφοριακό Σύστημα χωρίς όμως να είναι εξουσιοδοτημένος, τότε ο κάτοχός του παύει να έχει την αποκλειστική του χρήση.

➢ **Παραβίαση δικαιωμάτων:**

Η παραβίαση των ανθρωπίνων δικαιωμάτων μπορεί να οφείλεται σε προγράμματα που γράφτηκαν έχοντας σαν σκοπό τη διάκριση μεταξύ των πολιτών με βάση τις πολιτικές τους πεποιθήσεις κλπ. («Διοικητικά Πληροφοριακά Συστήματα», Δ.Γιαννακόπουλος, Ι.Παπουτσής)

4.7 Ασφάλεια συναλλαγών στο Διαδίκτυο

Η ασφάλεια των διαδικτυακών συναλλαγών περιλαμβάνει:

ΕΛΕΓΧΟ ΑΥΘΕΝΤΙΚΟΤΗΤΑΣ (AUTHENTICATION)

Η δυνατότητα να πιστοποιηθεί ένας χρήστης ή ένα σύστημα ότι πραγματικά είναι αυτός ή αυτό που ισχυρίζεται ότι είναι δηλαδή εξακρίβωση ταυτότητας. Η απαίτηση αυτή θέλει τους χρήστες να παρουσιάζουν

επιβεβαιώσιμα διαπιστευτήρια ταυτότητας έτσι ώστε τα συστήματα υπολογιστών να είναι σε θέση να επιβεβαιώσουν ότι ο συμμετέχων σε μία συναλλαγή είναι πραγματικά αυτός που ισχυρίζεται ότι είναι.

ΕΞΟΥΣΙΟΔΟΤΗΣΗ (AUTHORIZATION)

Από την στιγμή που ένας χρήστης έχει πιστοποιηθεί, το σύστημα πρέπει να ελέγξει το δικαίωμα(-τα) του χρήστη για την πραγματοποίηση διαφόρων ενεργειών. Ένα τυπικό σύστημα διαχείρισης δικαιωμάτων και ελέγχου που βασίζεται στους ρόλους των χρηστών παρέχει την δυνατότητα του να επιτρέπει / αποτρέπει την πρόσβαση των χρηστών στα δεδομένα ή στις υπηρεσίες του συστήματος με βάση τα συγκεκριμένα δικαιώματα.

ΑΚΕΡΑΙΟΤΗΤΑ ΔΕΔΟΜΕΝΩΝ (DATA INTEGRITY)

Κατά τις φάσεις μεταφοράς ή αποθήκευσης των δεδομένων, αυτά θα πρέπει να προστατεύονται από εξωτερικές επιθέσεις ,οι οποίες έχουν ως στόχο την αλλοίωση των δεδομένων. Κατάλληλα πρότυπα και τεχνικές πρέπει να εφαρμοστούν για να εμποδίσουν την αλλοίωση των δεδομένων κατά την διάρκεια μιας συναλλαγής. Επιπρόσθετα μέσα, όπως ιδιωτικές συνδέσεις, μπορούν να αυξήσουν την εμπιστοσύνη όσον αφορά στην ακεραιότητα των δεδομένων.

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ (CONFIDENTIALITY)

Τα δεδομένα πρέπει να προστατεύονται από την μη-εξουσιοδοτημένη έκθεσή τους σε τρίτους. Μέσω κατάλληλων προτύπων και τεχνικών (αυτών που αναφέρθηκαν και προηγούμενα) είναι δυνατόν να εξασφαλιστεί ότι μόνο πιστοποιημένοι και εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση σε εμπιστευτικά δεδομένα.

ΚΑΤΑΓΡΑΦΗ ΣΥΝΑΛΛΑΓΩΝ (AUDITING)

Οι ενέργειες σε ένα σύστημα πρέπει να καταγράφονται έτσι ώστε οι λεπτομέρειες της κάθε συναλλαγής να είναι διαθέσιμες για έλεγχο οποτεδήποτε. Αυτή η καταγραφή βοηθά στο να ανακαλεστεί το ιστορικό των συμμετεχόντων και οι λεπτομέρειες της κάθε συναλλαγής.

ΜΗ ΑΠΟΠΟΙΗΣΗ ΕΥΘΥΝΗΣ (NON-REPUDIATION)

Η δυνατότητα να αποδειχτεί ότι ο συμμετέχων πήρε πραγματικά μέρος σε μια συναλλαγή. Μέσω της χρήσης των τεχνικών που αναφέρθηκαν προηγούμενα (έλεγχος αυθεντικότητας, εξουσιοδότηση, ακεραιότητα δεδομένων και καταγραφή συναλλαγών), είναι εφικτό να αποδειχτεί ότι οι συγκεκριμένοι χρήστες πήραν μέρος σε κάποια συναλλαγή και προσπέλασαν τα σχετικά δεδομένα.

ΚΕΦΑΛΑΙΟ 5°
ΓΕΝΙΚΑ ΠΕΡΙ ΙΩΝ

5.1 Οι ιοί στους Η/Υ

Πρόσφατα, στον κόσμο των Υπολογιστών έχουν εισβάλλει οι ιοί. Η ιστορία τους ξεκινά το 1988, όταν ένας σπουδαστής του Πανεπιστημίου Cornell δημιούργησε έναν ιό και τον διοχέτευσε σε περισσότερους από 6000 Η/Υ του δικτύου ARPANET (ένα ειδικό δίκτυο για εργασία πάνω σε αμυντικά σχέδια των ΗΠΑ). Αυτό το γεγονός απέδειξε ότι οι ιοί δεν είναι μόνο ενοχλητικοί για τους χρήστες, αλλά μπορεί να γίνουν και καταστροφικοί για τα προγράμματα.

Από τότε μέχρι και σήμερα έχουν γίνει πολλά στον κόσμο των ιών. Δημιουργήθηκαν και ανιχνεύτηκαν χιλιάδες και φυσικά δεν σταμάτησαν τον καταστρεπτικό τους ρόλο, όχι μόνο σε μεμονωμένους χρήστες Η/Υ, ή μικρούς οργανισμούς, αλλά ακόμα και στη NASA.

Ένας ιός είναι ένα πρόγραμμα του οποίου την παρουσία δεν μπορεί να επισημάνει –τουλάχιστον στην αρχή- ο χρήστης και το οποίο έχει σκοπό να αλλοιώσει ή αλλιώς να «μολύνει» ένα σύστημα.

Ο ιός έχει την ιδιότητα να αναπαράγει τον εαυτό του με απρόβλεπτο ρυθμό και να προκαλεί μια συγκεκριμένη ενέργεια, κάτω από κάποιες προκαθορισμένες συνθήκες.

Ακόμη, ένα μοναδικό χαρακτηριστικό των ιών είναι ότι μπορούν να παραμείνουν ανενεργοί σε έναν υπολογιστή, χωρίς να προκαλέσουν κάποια ζημιά και μέχρι να συμπληρωθεί κάποιος χρόνος ή να συγκεντρωθούν κάποια προκαθορισμένα αρχεία.

Σε ένα δίκτυο οι ιοί μεταδίδονται στους χρήστες από μολυσμένες δισκέτες ή άλλο μέσο αποθήκευσης που χρησιμοποιούν για την αποθήκευση των προγραμμάτων και των δεδομένων τους. Με τη σημερινή τεχνολογία ένας ιός μπορεί να δημιουργηθεί ακόμη και σε έναν προσωπικό υπολογιστή, ενώ οι καταστροφές που επιφέρει μπορούν να είναι και καταστροφικές π.χ. κατάρρευση συστήματος.

Οι ιοί είναι οι πιο ευρέως γνωστή απειλή για τους υπολογιστές και τα δεδομένα. Συγκαταλέγονται όμως και στα προβλήματα που μπορούμε να προλάβουμε ευκολότερα. Ο κύριος κίνδυνος από τους ιούς προέρχεται από την πεποίθηση του καθενός μας ότι αυτό μπορεί να συμβεί μόνο σε άλλους.

Αυτό είναι και ο λόγος για τον οποίο όσοι έπεσαν κάποτε θύμα ενός ιού παίρνουν πάντα τα κατάλληλα μέτρα προφύλαξης. Παρόλα αυτά ,οι περισσότεροι χρήστες που δεν χρειάστηκε ποτέ να αντιμετωπίσουν τις συνέπειες ενός ιού δεν παίρνουν στην πράξη κανενός είδους προφύλαξη. Ορισμένοι

μάλιστα, φτάνουν στο σημείο ακόμα να αμφιβάλλουν ακόμα και για την ύπαρξη των ιών.

Η προστασία του υπολογιστή από τους ιούς είναι εύκολη και δεν απαιτεί ειδικό λογισμικό. Το μόνο που πρέπει να κάνουμε είναι να αποφεύγουμε κάποιες ενέργειες που είναι πιθανό να εκθέσουν το σύστημά μας στους ιούς. Ωστόσο επειδή κανείς δε μπορεί να μας εγγυηθεί ότι δε θα πάθουμε κάποιο ατύχημα, καλό είναι να κάνουμε χρήση καλού κακού κάποιου προγράμμαυος προστασίας από τους ιούς .

5.2 Τι είναι οι Ιοί ?

Ιός (virus) είναι ένα πρόγραμμα που έχει γραφεί από κάποιον προγραμματιστή. Μπορεί ο ιός να είναι μια ξένη και καταστροφική οντότητα της οποίας ο τρόπος αναπαραγωγής μοιάζει με αυτόν ενός ανθρώπινου ιού, αλλά οι ομοιότητες σταματούν εκεί.

Όταν βρεθεί ένας ιός στο σκληρό σας δίσκο, ο υπολογιστής δεν «αρρωσταίνει». Συνεχίζει να δουλεύει απολύτως φυσιολογικά. Απλώς εκτελεί ένα πρόγραμμα πού έχει γράψει κάποιος ο οποίος, τις περισσότερες φορές, θέλει να τρομάξει ή να καταστρέψει τούς άλλους πειράζοντας τα δεδομένα τους. Μερικές φορές στόχος κάποιου είναι να προκαλέσει όσο το δυνατόν μεγαλύτερη καταστροφή. Αν και δεν είναι τόσο συχνό κάποιοι άλλοι δημιουργοί ιών δρουν τρομοκρατικά και απαιτούν λύτρα για να εξαφανίσουν τα αποτελέσματα του ιού.

Τις περισσότερες φορές , οι ιοί είναι έργα ασυνείδητων προγραμματιστών που θέλουν απλώς να αποδείξουν πόσο έξυπνοι είναι. Κάποιες φορές, οι ιοί είναι προγράμματα που γράφτηκαν για καλό σκοπό αλλά εξαιτίας προγραμματιστικών λαθών , κατέληξαν να αποτελούν αιτία αναρίθμητων κακών. Για παράδειγμα, κάποιοι προγραμματιστές έχουν γράψει προγράμματα «κυνηγούς ιών» που χρησιμοποιούν τις ίδιες τεχνικές με τους εχθρούς τους για να πολλαπλασιάσουν τους εαυτούς τους. Δυστυχώς έχει αποδειχτεί ότι αυτά τα προγράμματα κάνουν περισσότερο κακό παρά καλό.

Κάθε ιός αποτελείται από δύο προγράμματα που δρουν ανεξάρτητα. Στόχος του πρώτου προγράμματος είναι να αναπαράγει τον ιό-δημιουργώντας όσα περισσότερα αντίγραφα του μπορεί. Το δεύτερο πρόγραμμα ενός ιού εκτελεί κάποια ενέργεια η οποία, είτε καταστρέφει τα δεδομένα , είτε κάνει αισθητή την παρουσία του ιού για να τρομοκρατήσει τον χρήστη. Κατά τη διάρκεια της φάσης αναπαραγωγής (της επώασης της νόσου),ο ιός είναι πολύ διακριτικός. Το μόνο που εκτελείται είναι το πρώτο πρόγραμμα, αυτό της αναπαραγωγής του ιού. Σε κάποια δεδομένη στιγμή (ίσως μια συγκεκριμένη ημερομηνία, ίσως όταν έχουν δημιουργηθεί αρκετά αντίγραφα του ιού, ή όταν ο χρήστης εκτελέσει μια συγκεκριμένη ενέργεια),εκτελείται το δεύτερο πρόγραμμα.

Αυτό το πρόγραμμα μπορεί για παράδειγμα , να φορμάρει το σκληρό δίσκο (με συνέπεια την απώλεια όλων των δεδομένων), να καταστρέψει τον οδηγό (προγραμματίζοντας τον ελεγκτή να τοποθετήσει την κεφαλή ανάγνωσης σε μία τροχεία που δεν υπάρχει), να εμφανίσει ένα πολιτικό ή χιουμοριστικό μήνυμα, ή απλώς να ανακατέψει τα περιεχόμενα της οθόνης έτσι ώστε να κάνει την ανάγνωση τους αδύνατη. («Πώς δουλεύουν οι ιοί», Εκδόσεις Κλειδάριθμος.)

5.3 Μέτρα κατά των Ιών

- Έλεγχος των μαγνητικών μέσων που χρησιμοποιούνται.
- Απαγόρευση της ανεξέλεγκτης χρήσης του λογισμικού.
- Περιοδικός έλεγχος για απρόσμενες αλλαγές στο μέγεθος των προγραμμάτων ή για άλλες ενδείξεις ιών.
- Λήψη αντιγράφων ασφαλείας.
- Χρήση «Αντιβιοτικών».

5.4 Κίνητρα Παραβίασης των Α.Π.Σ.

Ένας μεγάλος αριθμός προσβολών αποβλέπει στο είτε άμεσο, είτε έμμεσο οικονομικό όφελος. Δεν χρησιμοποιείται συνήθως βία, αφού οι γνώσεις αυτών που προσβάλλουν το Πληροφοριακό Σύστημα είναι μεγάλες, και το ποσόν που υπεξαιρείται είναι τις περισσότερες φορές σημαντικό.

Τα κίνητρα που ωθούν στην παραβίαση των Λογιστικών Πληροφοριακών Συστημάτων είναι το οικονομικό όφελος, η δύναμη και η εξουσία αφού η Πληροφορική δεν είναι μόνο πηγή, αλλά και ισχυρό όργανο κοινωνικού ελέγχου.

5.4.1 Αμυντικά Συστήματα Εξασφάλισης των Λ.Π.Σ.

1) ΥΠΟΣΥΣΤΗΜΑ ΣΥΝΑΓΕΡΜΟΥ (ALARM SYSTEM):

Ο ρόλος αυτού του συστήματος είναι να ειδοποιεί τον εξουσιοδοτημένο χρήστη για πιθανή απόπειρα προσπέλασης χωρίς εξουσιοδότηση και κατά συνέπεια να αποθαρρύνει τους μη εξουσιοδοτημένους χρήστες.

2) ΥΠΟΣΥΣΤΗΜΑ ΑΝΤΙΔΡΑΣΗΣ (RESPONSE SYSTEM):

Ο ρόλος του είναι να οργανώνει την αντίδραση των εξουσιοδοτημένων χρηστών και να ελαχιστοποιεί τις συνέπειες προσβολής.

3) ΥΠΟΣΥΣΤΗΜΑ ΕΠΑΝΟΡΘΩΣΗΣ (RECOVERY SYSTEM):

Ο ρόλος του είναι να οργανώνει την αποκατάσταση της λειτουργίας των Λ.Π.Σ., τα οποία έχουν προσβληθεί, και να προετοιμάζει την επαναλειτουργία τους.

5.4.2 Δακτύλιοι Άμυνας (Defense Rings)

1) ΥΛΙΚΟ (HARDWARE):

Είναι ο εσωτερικός Δακτύλιος άμυνας και περιλαμβάνει εγγενείς μηχανισμούς εξασφάλισης.

2) ΣΥΣΤΗΜΑ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ:

Περιλαμβάνει τις διαδικασίες αναγνώρισης και επαλήθευσης (Identification – Authentication) των ταυτοτήτων των χρηστών που έρχονται σε επικοινωνία, καθώς και διαδικασίες που έχουν σχέση με την κρυπτογραφία.

3) ΠΡΟΓΡΑΜΜΑΤΑ ΕΦΑΡΜΟΓΩΝ:

Αυτά πρέπει να είναι βασισμένα σε πλήρεις λειτουργικές προδιαγραφές για να κάνουν σωστά αυτά για τα οποία σχεδιάστηκαν.

4) ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ:

Αναφέρεται κυρίως στην αντιμετώπιση φυσικών απειλών όπως ο σεισμός, η πυρκαγιά κλπ.

5) ΔΙΑΔΙΚΑΣΙΕΣ ΧΕΙΡΙΣΜΟΥ:

Καλούνται να εξασφαλίζουν την μη δυνατότητα προσπέλασης σε μη εξουσιοδοτημένους χρήστες.

6) ΣΧΕΔΙΑΣΜΟΣ ΣΥΣΤΗΜΑΤΟΣ:

Καθορίζει τα όρια μέσα στα οποία μπορεί να λειτουργήσουν οι διαδικασίες εξασφάλισης.

7) ΔΙΑΔΙΚΑΣΙΕΣ ΑΝΑΠΤΥΞΗΣ:

Πρέπει να έχουν τη δυνατότητα να εγγυηθούν ότι μόνο ελεγμένα και αξιόπιστα προγράμματα προστίθενται στο χρησιμοποιούμενο λογισμικό.

8) ΕΛΕΓΧΟΣ:

Όταν οι αμυντικοί δακτύλιοι λειτουργούν σωστά, ο έλεγχος είναι ένας από τους αποφασιστικότερους παράγοντες που καθορίζουν την εξασφάλιση ενός Λ.Π.Σ. Καμιά διαδικασία δε μπορεί να είναι αποτελεσματική αν δε διασφαλίζεται η πλήρης λειτουργία της. («Διοικητικά Πληροφοριακά Συστήματα», Δ.Γιαννακόπουλος, Ι.Παπουτσής)

5.5 Προβλήματα Καθορισμού Δικαιωμάτων Πρόσβασης

Κατά τη διάρκεια λειτουργίας ενός Λογιστικού Πληροφοριακού Συστήματος εμφανίζεται ένα απ' τα βασικότερα προβλήματα, που είναι ο καθορισμός των δικαιωμάτων πρόσβασης κάθε χρήστη σε κάθε υποσύνολο δεδομένων, αρχείων ή εφαρμογών του Λ.Π.Σ.

Μια πρώτη προσέγγιση σ' αυτό το πρόβλημα απαιτεί τον ορισμό και την περιγραφή του περιβάλλοντος ενός Λ.Π.Σ. Υπάρχουν δύο φιλοσοφίες προσέγγισης: Η πρώτη χρησιμοποιεί την κατεύθυνση του καθορισμού διαβάθμισης, ανά χρήστη και αρχείο / εφαρμογή. Η δεύτερη χρησιμοποιεί γλώσσες ερωτο-ανταποκρίσεων, για να καθορίσει τις «εικόνες» στις οποίες έχει πρόσβαση ο χρήστης του Λ.Π.Σ.

I. Η πρώτη προσέγγιση είναι γνωστή σαν Πολύ – επίπεδη Προσέγγιση Ασφαλείας και βασίζεται στις έννοιες: Χρήστες, Μονάδες δεδομένων και Πίνακες επιπέδων ασφαλείας. Ο κάθε χρήστης έχει ένα επίπεδο προσπέλασης και κάθε μονάδα δεδομένων έχει μια διαβάθμιση.
II. Η δεύτερη προσέγγιση που έχει εφαρμογή σε Π.Σ. τα οποία χρησιμοποιούν Βάσεις Δεδομένων (όπως τα Λ.Π.Σ.), απαιτεί βαθιά γνώση του συστήματος διαχείρισης της βάσης δεδομένων και του συγκεκριμένου μοντέλου δόμησης της βάσης δεδομένων.

5.6 Αναγνώριση – Επαλήθευση Ταυτότητας

Κάθε Λογιστικό Πληροφοριακό Σύστημα πλαισιώνεται από ένα σύνολο ανθρώπων οι οποίοι είτε αναπτύσσουν τις δυνατότητες του διατιθέμενου υλικού και λογισμικού, είτε το συντηρούν, είτε χρησιμοποιούν τις υπηρεσίες που τους παρέχει.

Για να ολοκληρωθεί η σύνδεση με τον υπολογιστή γίνονται τα εξής:

- Ταυτοποίηση (Identification):

  Ο χρήστης αναγγέλλει στον Η/Υ την ταυτότητά του. Πρόκειται για το στάδιο της αναγνώρισης.

- Αυθεντικοποίηση (Authentication):

  Ο χρήστης βεβαιώνει τον Η/Υ ότι είναι αυτός που ισχυρίζεται. Πρόκειται για το στάδιο της επαλήθευσης της ταυτότητας του χρήστη.

- Εξουσιοδότηση (Authorization):

  Ο χρήστης αξιοποιεί τις δυνατότητες που του παρέχει το Λ.Π.Σ.

Για την πραγματοποίηση της αυθεντικοποίησης υπάρχουν τρεις κατευθύνσεις, και σε καθεμιά απ' αυτές ο χρήστης χρησιμοποιεί κάτι:

1) Που γνωρίζει (π.χ. συνθηματικό)
2) Που κατέχει (π.χ. μαγνητική κάρτα)
3) Που τον χαρακτηρίζει (π.χ. συσκευή ανίχνευσης δακτυλικών αποτυπωμάτων, φωνής κλπ).

ΚΕΦΑΛΑΙΟ 6°
ΤΕΧΝΟΛΟΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

6.1 Εισαγωγή

Όχι πολλά χρόνια πριν, η κρυπτογραφία στην ισχυρή μορφή της (strong encryption) χρησιμοποιείτο μόνο για στρατιωτικές εφαρμογές. Σήμερα ωστόσο, στη λεγόμενη εποχή της πληροφορίας, αποτελέι ένα βασικό εργαλείο για την προστασία δεδομένων, καθώς και τη διασφάλιση του απορρήτου και της εγκυρότητας των δικτυακών συναλλαγών.

Για την πραγματοποίηση ηλεκτρονικών συναλλαγών και επικοινωνιών απαιτείται η προστασία του περιεχομένου των μηνυμάτων από κάθε παραποίηση κατά τη διαδρομή μεταξύ αποστολέα και παραλήπτη. Ο τρόπος κωδικοποίησης πρέπει να εξασφαλίζει ότι κανείς δε μπορεί να προσθέσει, να αφαιρέσει ή να αλλάξει οτιδήποτε στο περιεχόμενο του μηνύματος. Δεν πρέπει να είναι δυνατή η εξαπάτηση της μιας ή της άλλης πλευράς από κάποιον που μπόρεσε να παραποιήσει το μήνυμα σε έναν ενδιάμεσο κόμβο.

6.2 Κρυπτογράφηση δεδομένων

Ας υποθέσουμε ότι ένας αποστολέας θέλει να στείλει ένα μήνυμα σε έναν παραλήπτη. Επιπλέον ο αποστολέας θέλει να στείλει το μήνυμα με ασφάλεια, δηλαδή, θέλει να είναι σίγουρος ότι κάποιος τρίτος δε θα μπορέσει να κρυφακούσει (υποκλέψει) το μήνυμα. Σε αυτό το κεφάλαιο αναφερόμαστε στις κύριες τεχνολογίες ασφαλείας που είναι διαθέσιμες σήμερα.

Η ασφάλεια επικοινωνίας αναφέρεται στην πρόβλεψη παρενεργειών και ανεξέλεγκτων καταστάσεων που αφορούν τη γραμμή επικοινωνίας, όπως:

α) Διαρροή (άκουσμα) των πληροφοριών και των μηνυμάτων που στέλνονται μέσω της γραμμής επικοινωνίας.

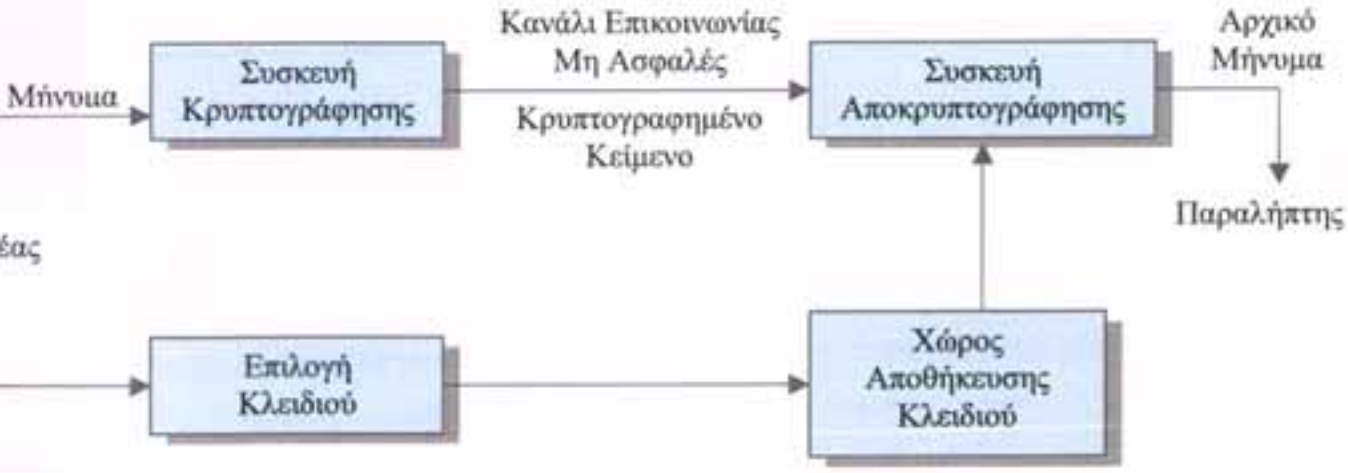
β) Καταγραφή της μετάδοσης με σκοπό την αλλοίωσή της.

Για την ασφάλεια των αποστελόμενων πληροφοριών χρησιμοποιούνται τεχνικές κωδικοποίησης που ονομάζονται και τεχνικές κρυπτογράφησης δεδομένων.

ΚΡΥΠΤΟΓΡΑΦΗΣΗ (ENCRYPTION):

Είναι η διαδικασία μετατροπής ενός πρωτότυπου μηνύματος (plaintext) σε κρυπτογράφημα (ciphertext). Στην κρυπτογράφηση δεδομένων ο κάθε χαρακτήρας του μηνύματος αντικαθίσταται από άλλους κωδικοποιημένους χαρακτήρες. Ο αποστολέας είναι εκείνος που καθορίζει τον τρόπο κωδικοποίησης (αλγόριθμο αντικατάστασης), σύμφωνα με ένα προεπιλεγμένο κλειδί. Αν κάποιος κλέψει το κρυπτογραφημένο μήνυμα, ακόμη κι αν γνωρίζει τον αλγόριθμο κρυπτογράφησης, είναι πολύ δύσκολο να αποκρυπτογραφήσει το μήνυμα, επειδή δε γνωρίζει το κλειδί.

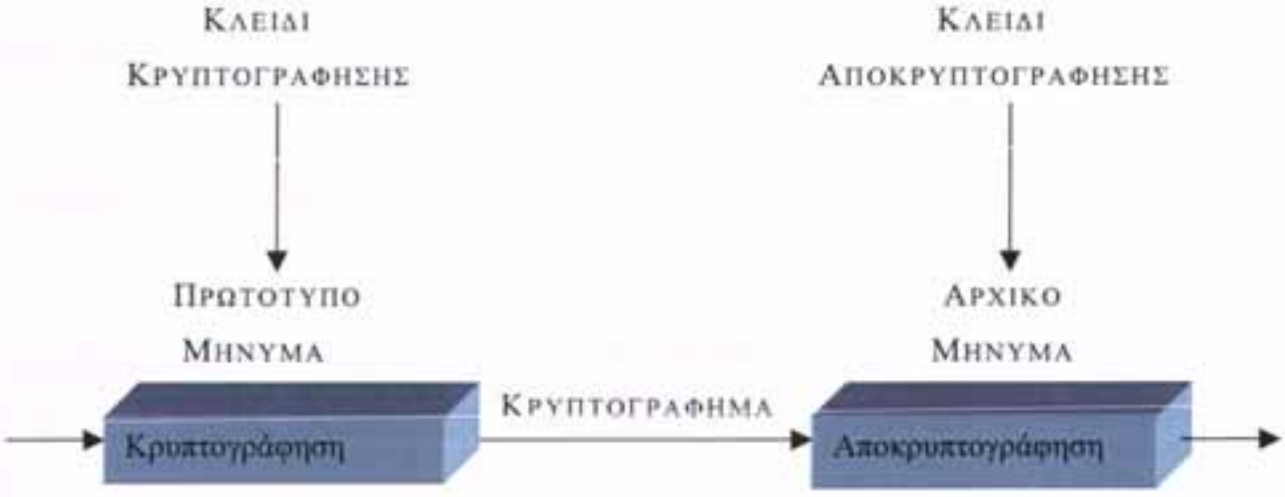
Σχετικό σχήμα παρουσιάζεται παρακάτω :



Σχήμα: Κρυπτογράφηση μηνύματος με τη χρήση κλειδιού.

ΚΡΥΠΤΟΑΝΑΛΥΣΗ (CRYPTOANALYSIS)

Καλείται η επιστήμη που ασχολείται με την ανάλυση (ή απλά μιλώντας: το ''σπάσιμο'') του κρυπτογραφήματος:



Σχήμα: Κρυπτογράφηση και αποκρυπτογράφηση

Η κρυπτογραφία είναι μια επιστήμη που βασίζεται στα Μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι.

Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες, αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Το αρχικό μήνυμα ονομάζεται *απλό κείμενο (plaintext)*, ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται *κρυπτογράφημα (cipher text)*.

ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ (DECRYPTION)

Η αντίστροφη διαδικασία δηλαδή η μετατροπή του κρυπτογραφήματος στο αρχικό μήνυμα, καλείται αποκρυπτογράφηση (decryption). Αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγόριθμου. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτή μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος.

Υπάρχουν δύο τύποι συστημάτων κρυπτογράφησης και είναι οι εξής:

1) Συστήματα τα οποία ο τρόπος κρυπτογράφησης είναι γνωστός μόνο στα δύο μέρη (υπολογιστές) που επικοινωνούν.
2) Συστήματα στα οποία ο τρόπος κρυπτογράφησης είναι γενικότερα γνωστός αλλά στηρίζεται σε ένα κλειδί (Key), το οποίο με την σειρά του είναι γνωστό μόνο στα δύο μέρη που επικοινωνούν.

Η επικοινωνία με τον δεύτερο τύπο είναι περισσότερο ασφαλής , διότι το γεγονός ότι ο τρόπος κρυπτογράφησης είναι ευρύτερα γνωστός οδηγεί στο ότι έχει κρυπτοαναλυθεί αρκετά και τα οποία προβλήματα έχουν επιλυθεί. Κάποιος εισβολέας λοιπόν, θα πρέπει να υποκλέψει ή να αναπαράγει το κλειδί προκειμένου να διασπάσει την ασφάλεια του συστήματος. Τα συστήματα αυτά χρησιμοποιούνται κυρίως στις συναλλαγές μέσω Διαδικτύου.

Για τον δεύτερο τύπο συστημάτων διακρίνουμε δύο κατηγορίες:

i. Συμμετρικά συστήματα:

Αυτή η κατηγορία χρησιμοποιεί το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση. Όσο το κλειδί παραμένει μυστικό , τόσο τα μηνύματα μεταφέρονται με ασφάλεια.

ii. Ασυμμετρικά συστήματα (ή συστήματα δημοσίου κλειδιού):

Η δεύτερη κατηγορία χρησιμοποιεί διαφορετικά κλειδιά για κρυπτογράφηση και αποκρυπτογράφηση. Τα συστήματα αυτά καλούνται και συστήματα δημοσίου κλειδιού (public key) διότι το κλειδί αποκρυπτογράφησης είναι γνωστό σε όλους. Ο καθένας λοιπόν μπορεί να χρησιμοποιήσει το δημόσιο κλειδί για να κρυπτογραφήσει ένα μήνυμα, άλλα μόνο ένας συγκεκριμένος χρήστης με το αντίστοιχο κλειδί αποκρυπτογράφησης μπορεί να αποκρυπτογραφήσει το μήνυμα.

Το κλειδί αποκρυπτογράφησης καλείται ιδιωτικό κλειδί (private key) . («Διοικητικά Πληροφοριακά Συστήματα», Δ.Γιαννακόπουλος, Ι.Παπουτσής)

6.3 Ψηφιακές Υπογραφές

Η ψηφιακή υπογραφή (digital signature) είναι μια ηλεκτρονική υπογραφή η οποία χρησιμοποιείται για να εξακριβωθεί η ταυτότητα του αποστολέα ενός μηνύματος ή του υπογράφοντος ένα έγγραφο, και πιθανώς για να διασφαλίσει ότι το αρχικό περιεχόμενο του μηνύματος ή εγγράφου που εστάλη δεν έχει υποστεί αλλαγές. Επιτυγχάνεται με τη χρήση δημόσιου και ιδιωτικού κλειδιού, δηλαδή ο αποστολέας είναι αυτός που υπογράφει χρησιμοποιώντας το ιδιωτικό του κλειδί, ενώ ο παραλήπτης κάνει χρήση του δημοσίου κλειδιού προκειμένου να αποκωδικοποιήσει την υπογραφή του αποστολέα.

Οι ψηφιακές υπογραφές μεταφέρονται εύκολα, δεν μιμούνται από κάποιον τρίτο, και μπορούν αυτόματα να ανανεώνονται με στιγμιότυπα χρόνου (timestamps) . Η χρήση της έχει ως στόχο την επαλήθευση του αποστολέα, αλλά και την ακεραιότητα του ίδιου του μηνύματος, ότι δηλαδή δεν αλλοιώθηκε κατά τη μεταφορά. Η επαλήθευση αυτή γίνεται με τη χρήση του δημοσίου κλειδιού, ενώ η μέθοδος αυτή χαρακτηρίζεται ως ασφαλής, εκτός της περίπτωσης εκείνης που κλαπεί το ιδιωτικό κλειδί.

Η δυνατότητα εξασφάλισης ότι το αρχικό υπογεγραμμένο μήνυμα έφθασε , σημαίνει ότι ο αποστολέας δεν μπορεί εύκολα να το αρνηθεί αυτό αργότερα. Τέλος , η ψηφιακή υπογραφή δεν θα πρέπει να συγχέεται με το ψηφιακό πιστοποιητικό .

Η ψηφιακή υπογραφή μπορεί να χρησιμοποιηθεί με οποιοδήποτε τύπο μηνύματος, είτε είναι κρυπτογραφημένο είτε όχι, έτσι ώστε ο παραλήπτης να μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα και για το ότι το μήνυμα έφθασε άθικτο. Ένα ψηφιακό πιστοποιητικό περιέχει την ψηφιακή υπογραφή της εκδούσας αρχής έτσι ώστε οποιοσδήποτε να μπορεί να επιβεβαιώσει ότι είναι γνήσιο.

ΠΑΡΑΔΕΙΓΜΑ: ΧΡΗΣΗΣ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ ΣΕ ΜΙΑ ΣΥΝΑΛΛΑΓΗ:

Ας υποθέσουμε ότι ένας χρήστης θέλει να στείλει την πρόχειρη έκδοση ενός συμβολαίου στον δικηγόρο του σε μια άλλη πόλη. Εκείνο πού θέλει ο χρήστης είναι να δώσει στον δικηγόρο του την επιβεβαίωση ότι αυτό που έφθασε είναι ακριβής εικόνα αυτού πού εστάλη και ότι ο χρήστης είναι αυτός που ισχυρίζεται ότι είναι.

Στην κρυπτογράφηση με δημόσιο κλειδί, τα κλειδιά (δημόσιο και ιδιωτικό) δημιουργούνται ταυτόχρονα από την αρχή της πιστοποίησης. Το ιδιωτικό κλειδί δίνεται μόνο στον αιτούντα χρήστη, ενώ το δημόσιο κλειδί είναι διαθέσιμο (ως μέρος του ψηφιακού πιστοποιητικού) σ'έναν κατάλογο όπου όλοι έχουν πρόσβαση. Το ιδιωτικό κλειδί δεν μοιράζεται με κάνεναν στο διαδίκτυο.

Πιο αναλυτικά, ο Α χρήστης χρησιμοποιεί το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει ένα μήνυμα το οποίο έχει αποκρυπτογραφηθεί από τον Β χρήστη (με δημόσιο κλειδί του χρήστη Α). Ο χρήστης Β βρίσκει το δημόσιο κλειδί του χρήστη Α από έναν κοινά διαθέσιμο κατάλογο. Επιπλέον , ο χρήστης Α μπορεί να πιστοποιήσει την ταυτότητα του στον χρήστη Β (έτσι ώστε ο χρήστης Β να είναι σίγουρος για το ποιος έστειλε το μήνυμα) χρησιμοποιώντας το ιδιωτικό του κλειδί για να κρυπτογραφήσει ένα ψηφιακό πιστοποιητικό. Εν συνεχεία ο χρήστης Β χρησιμοποιεί το δημόσιο κλειδί του Α για να το αποκρυπτογραφήσει.

Στο παρακάτω σχήμα μπορούμε να δούμε συνοπτικά τις σχετικές λειτουργίες:

Ενέργεια	**Χρησιμοποίηση**
Αποστολή Κρυπτογραφημένου μηνύματος	Δημόσιου κλειδιού παραλήπτη
Αποστολή κρυπτογραφημένης υπογραφής	Ιδιωτικού κλειδιού αποστολέα
Αποκρυπτογράφηση κρυπτογραφημένου μηνύματος	Ιδιωτικού κλειδιού παραλήπτη
Αποκρυπτογράφηση κρυπτογραφημένης υπογραφής	Δημοσίου κλειδιού αποστολέα

Σχήμα: Κρυπτογράφηση μηνύματος και υπογραφής

6.3.1 Ψηφιακά Πιστοποιητικά

Ένα μεγάλο πρόβλημα στον κυβερνοχώρο έχει να κάνει με την πιστοποίηση του γνήσιου της ταυτότητας. Οποιοσδήποτε γνώστης μπορεί να 'μασκαρευτεί' καταλλήλως, παριστάνοντας ένα άλλο πρόσωπο, τράπεζα, οργανισμό ή δικτυακό κατάστημα. Γίνεται φανερή λοιπόν η ανάγκη ενός μηχανισμού πιστοποίησης της πραγματικής ταυτότητας κάποιου φυσικού ή νομικού προσώπου.

Ακόμα και στη περίπτωση κατά την οποία ο αποστολέας έχει υπογράψει ένα μήνυμα ο παραλήπτης αντιμετωπίζει ένα σημαντικό πρόβλημα. Πώς λοιπόν είναι σίγουρος ο παραλήπτης ότι αυτός που έστειλε το δημόσιο κλειδί είναι πραγματικά ο αποστολέας που ισχυρίζεται ότι είναι; Προκειμένου να διαφυλαχτεί ο παραλήπτης απέναντι σ'αυτή τη πιθανότητα, κοινώς αποδεκτές αρχές παρέχουν ψηφιακά πιστοποιητικά στους χρήστες. («Λογιστικά Πληροφοριακά Συστήματα – Σύγχρονες Υπηρεσίες», Β.Ταμπακάς - Γ.Ορφανός, σημειώσεις ομώνυμου μαθήματος)

Λύση στο πρόβλημα αποτελούν τα λεγόμενα ψηφιακά πιστοπιητικά (certificates). Πρόκειται για ειδικά μορφοποιημένα ψηφιακά έγγραφα που επιτρέπουν σε ένα πρόσωπο να δηλώνει την ταυτότητά του σε ένα

πρόγραμμα πλοήγησης (browser), σε ένα διαχειριστή e-mail, σε κάποιον ασφαλή διακομιστή κλπ.

Η γνωστή σε όλους μας αστυνομική ταυτότητα αποτελεί τη βεβαίωση κάποιας αρχής –της αστυνομίας- για την ύπαρξη ενός συγκεκριμένου προσώπου. Το ψηφιακό πιστοποιητικό παίζει ακριβώς αυτόν τον ρόλο, δηλαδή της πιστοποίησης της ταυτότητας του συναλλασσόμενου ενώπιον κάποιας αρχής (τράπεζας, οργανισμού κλπ.). (www.in.gr/Articles ηλεκτρονική διεύθυνση περιοδικού 'Ram'.)

Το ψηφιακό πιστοποιητικό (digital certificate) είναι μια ηλεκτρονική «ψηφιακή κάρτα» η οποία εγκαθιστά τα διαπιστευτήρια σε εμπορικές ή άλλες συναλλαγές μέσω του Διαδικτύου. Εκδίδεται από μια αρχή πιστοποίησης (certificate authority) . Η αρχή πιστοποίησης είναι μία αρχή στο Διαδίκτυο η οποία εκδίδει και διαχειρίζεται διαπιστευτήρια ασφαλείας και δημόσια κλειδιά για την κρυπτογράφηση μηνυμάτων. Περιλαμβάνει το όνομα του χρήστη, έναν σειριακό αριθμό, ημερομηνία λήξης , ένα αντίγραφο του δημόσιου κλειδιού του κατόχου του πιστοποιητικού (το κλειδί χρησιμοποιείται για την κρυπτογράφηση μηνυμάτων και ψηφιακών υπογραφών) και την ψηφιακή υπογραφή της αρχής της πιστοποίησης έτσι ώστε ένας παραλήπτης να μπορεί να επαληθεύσει ότι το πιστοποιητικό είναι γνήσιο.

Η αρχή της πιστοποίησης μεσολαβεί μεταξύ του πελάτη και της επιχείρησης και εγγυάται ότι η επιχείρηση είναι νόμιμη κι ότι διαθέτει μηχανισμό κρυπτογράφησης προκειμένου να διασφαλιστούν οι εμπορικές συναλλαγές. Με τη σειρά της η επιχείρηση μπορεί να παρέχει πιστοποιητικά τόσο στο προσωπικό της, όσο και στους πελάτες της (πχ.πελάτες τραπεζών). («Διοικητικά Πληροφοριακά Συστήματα», Δ.Γιαννακόπουλος, Ι.Παπουτσής).

6.4 Η τέχνη του σύγχρονου «κρύπτεσθαι» με απλά λόγια

Όλα τα προηγούμενα γίνονται πολύ περισσότερα κατανοητά, αν σκεφτούμε ένα κουτί με μια 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 μία 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 (ουσιαστικά της μεθόδου κρυπτογράφησης), το κλειδί δεν είναι τίποτε 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 δηλώνει και το μήκος των κλειδιών που αναφέρεται σε διάφορα συστήματα και εκφράζεται σε bit. (www.in.gr/Articles ηλεκτρονική διεύθυνση περιοδικού 'Ram')

6.5 Συστήματα Προστασίας Από Εισβολείς (Firewalls)

Σε πολλά δίκτυα η εισβολή είναι τυχαίο και σπάνιο φαινόμενο, ενώ σε άλλα είναι καθημερινό γεγονός. Ειδικά για τα δίκτυα υπάρχουν στην αγορά πολλά πακέτα, τα οποία ελέγχουν και προστατεύουν έναντι των επιθέσεων.

Συνήθως τα πακέτα αυτά χρησιμοποιούν ένα είδος προστατευτικού πλέγματος (firewall), ώστε να αποτρέψουν τις ανεπιθύμητες επισκέψεις. Το καλό είναι ότι μπορεί και ο απλός χρήστης να χρησιμοποιήσει firewall, προκειμένου να προστατέψει το σύστημά του.

Οι hackers του Internet μπορούν θεωρητικά να εισέλθουν στο δίκτυο και να προκαλέσουν ζημιά με διάφορους τρόπους:

- μπορούν να κλέψουν ή να καταστρέψουν σημαντικά δεδομένα, να προκαλέσουν ζημιά σε ανεξάρτητους υπολογιστές ή σε ολόκληρο δίκτυο, να χρησιμοποιήσουν τους πόρους των επιχειρησιακών υπολογιστών ή να
- χρησιμοποιήσουν το επιχειρηματικό δίκτυο και τους πόρους του και να φαίνεται ότι το κάνει κάποιος υπάλληλος της επιχείρησης.

Η λύση δεν είναι η αποκοπή του δικτύου από το Internet. Αντιθέτως, η εταιρία μπορεί να δημιουργήσει firewalls για να προστατέψει το δίκτυό της. Τα εν λόγω firewalls αφ' ενός επιτρέπουν στους υπαλλήλους της επιχείρησης να έχουν πρόσβαση στο Internet και αφ' ετέρου εμποδίζουν τους επίδοξους hackers και crackers να αποκτήσουν πρόσβαση στο εταιρικό δίκτυο και να προκαλέσουν ζημιές.

Τα firewalls αποτελούν συνδυασμούς hardware και software και συντίθενται χρησιμοποιώντας routers, servers, και μια ποικιλία λογισμικού, τοποθετούνται στο πιο ευπαθές σημείο μεταξύ του δικτύου και του Internet και μπορεί να είναι από απλά ως εξαιρετικά πολύπλοκα συστήματα. («Διοικητικά Πληροφοριακά Συστήματα», Δ.Γιαννακόπουλος – Ι.Παπουτσής.)

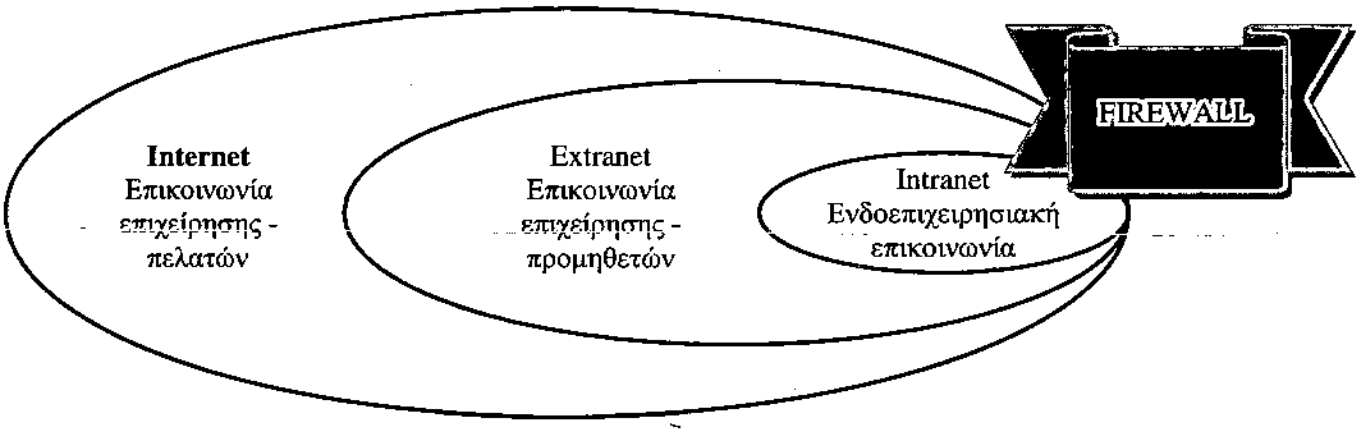
Το ζήτημα της ασφάλειας για τη νέα επιχείρηση επικεντρώνεται σε δύο τομείς:

ΙΙ) ΤΟ ΕΣΩΤΕΡΙΚΟ ΚΑΘΕΣΤΩΣ ΑΣΦΑΛΕΙΑΣ ΤΗΣ ΕΠΙΧΕΙΡΗΣΗΣ ΣΤΟ ΔΙΑΔΙΚΤΥΑΚΟ ΠΕΡΙΒΑΛΛΟΝ:

Η λειτουργία της επιχείρησης στο διαδίκτυο, ασφαλώς και αποτελεί το διαβατήριο εισόδου στη νέα αγορά του μέλλοντος, από την άλλη όμως την καθιστά ευάλωτη σε μια σειρά κινδύνους και απειλές.

Η είσοδος ενός μη εξουσιοδοτημένου προσώπου στο ενδοδίκτυο (intranet) της επιχείρησης, είτε υποκλέπτοντας ευαίσθητες πληροφορίες και διοχετεύοντάς τις σε ανταγωνιστές, είτε αλλοιώνοντας (διαγράφοντας στοιχεία και δεδομένα) μπορεί να αποβεί καταστροφική για την επιχείρηση.

Έτσι, οδηγείται στη χρήση των firewalls, δηλαδή όταν λειτουργεί σε διαδικτυακό περιβάλλον, το εσωτερικό της δίκτυο διασυνδέεται με το Internet και μέσω αυτού έρχεται σε επικοινωνία τόσο με τους πελάτες της, όσο και με τους προμηθευτές της.

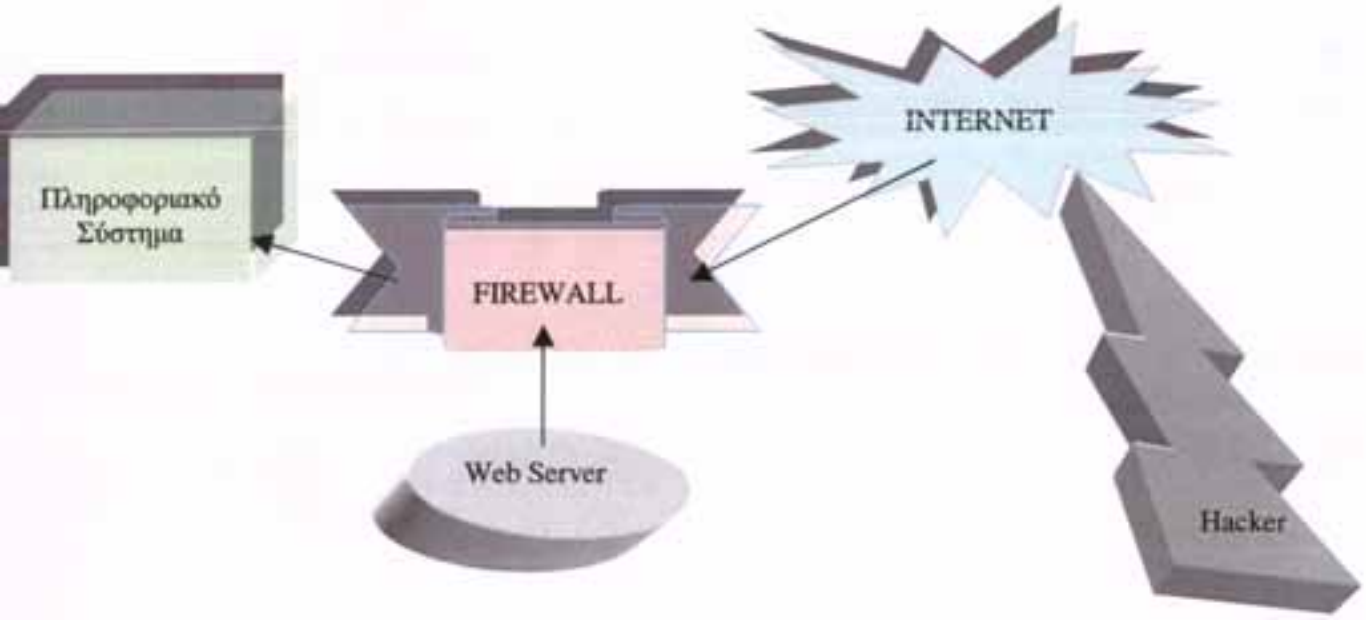


Σχήμα: Σχέση των τριών επιπέδων επικοινωνίας της επιχείρησης σε διαδικτυακό περιβάλλον και το σύστημα Firewall

Τα συστήματα firewalls ανάλογα με τον τρόπο που ελέγχουν τις επικοινωνίες διακρίνονται σε Screening routers, σε Circuit – level Proxies και Application level Proxies.

Η εξέλιξη της έννοιας του Firewall ακούει στο όνομα Secure Network Interface Points –SNIP, το οποίο βρίσκει εφαρμογή σε δίκτυα ευρείας περιοχής με στόχο τον περιορισμό της κακής μεταχείρισης μεγάλου όγκου διακινούμενης πληροφορίας στο Internet, και της ταυτόχρονης επιβολής πολιτικής ασφάλειας κρατών σε εθνικό επίπεδο.

**Virtual Private Networks:* η χρήση του IPSec πρωτοκόλλου προσφέρει υπηρεσίες κλιμακωτής κρυπτογράφησης ενώ τα VPN με Routers διαθέτουν ενσωματωμένες υπηρεσίες στις οποίες περιλαμβάνονται Firewalls, υπηρεσίες ψηφιακών πιστοποιητικών κλπ.



Σχήμα: Η λειτουργία ενός Internet Firewall

2) ΤΟ ΚΑΘΕΣΤΩΣ ΑΣΦΑΛΕΙΑΣ ΤΗΣ ΕΠΙΧΕΙΡΗΣΗΣ ΣΕ ΣΧΕΣΗ ΜΕ ΤΟΥΣ ΠΕΛΑΤΕΣ ΤΗΣ:

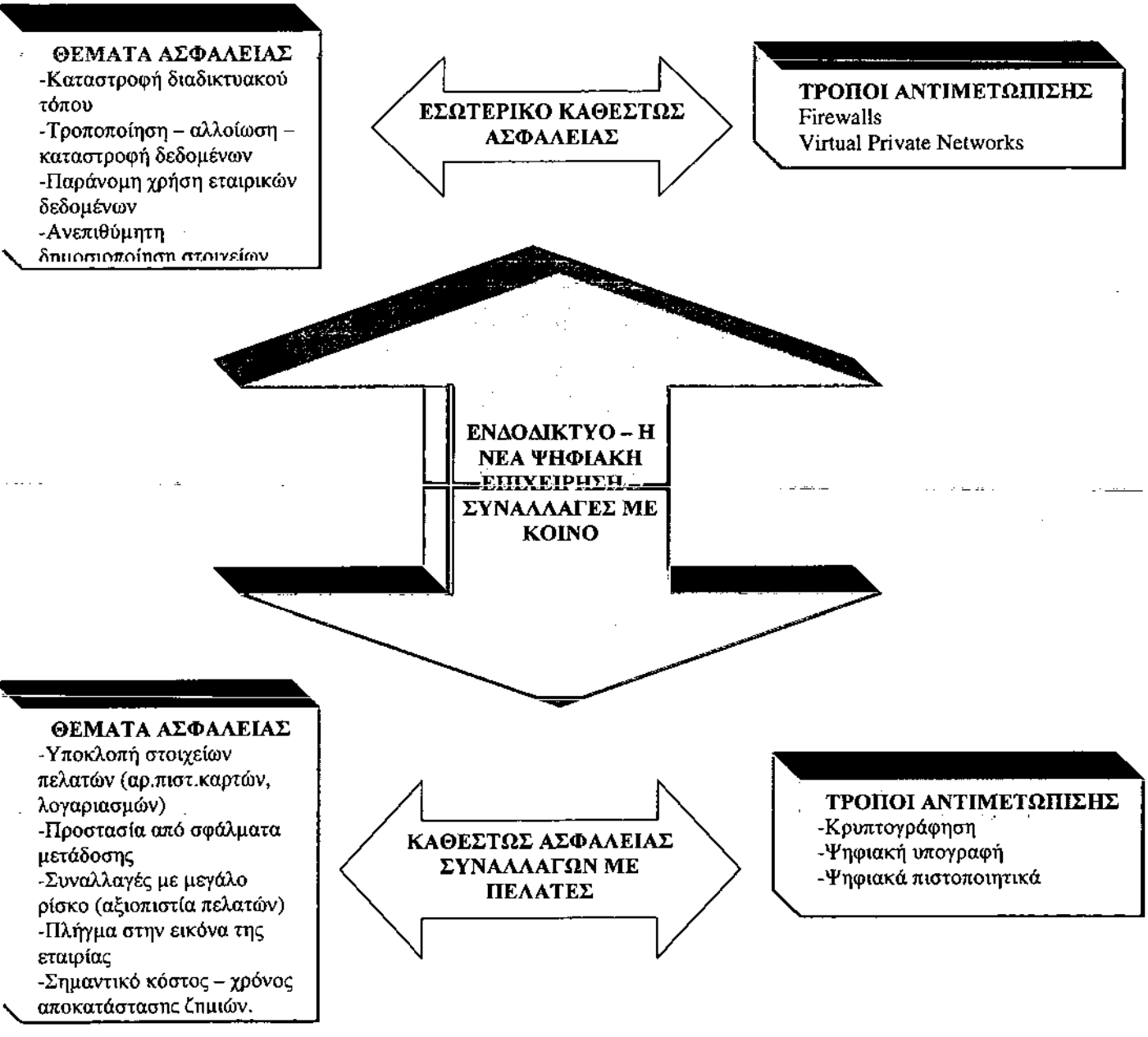
Ο δεύτερος τομέας αφορά το καθεστώς ασφάλειας που η επιχείρηση οφείλει να δομήσει προκειμένου να διασφαλίσει τις σχέσεις της με τους πελάτες. Η εφαρμογή του ηλεκτρονικού εμπορίου δίνει τη δυνατότητα στις επιχειρήσεις να απευθύνονται σε μια τεράστια εικονική αγορά.

Στους διαδικτυακούς τόπους και τα ηλεκτρονικά καταστήματα χιλιάδες καταναλωτές προκειμένου να εκτελέσουν τις εμπορικές τους συναλλαγές δίνουν αρκετά ευαίσθητα δεδομένα οικονομικού κυρίως χαρακτήρα. Η διείσδυση ενός μη εξουσιοδοτημένου χρήστη με την βοήθεια ειδικών προγραμμάτων λογισμικού μπορεί να αποβεί καταστροφική τόσο για την εταιρία, όσο και για τους καταναλωτές.

Η υποκλοπή στοιχείων συναλλαγής, όπως ο αριθμός πιστωτικής κάρτας, οι τραπεζικοί λογαριασμοί, αλλά και προσωπικών στοιχείων, όπως όνομα, διεύθυνση, επάγγελμα κλπ. δίνουν τη δυνατότητα στον υποκλοπέα να πάρει τη θέση του πραγματικού καταναλωτή και να διενεργεί για 'λογαριασμό' του εκτεταμένες συναλλαγές με ανύποπτες εταιρίες οι οποίες δραστηριοποιούνται στο διαδίκτυο.

Προκειμένου οι εταιρίες να διασφαλίσουν την παρουσία τους στο διαδίκτυο και ιδιαίτερα να προστατεύσουν την εκτέλεση των εμπορικών συναλλαγών από τους καταναλωτές, προσπαθούν να δημιουργήσουν ένα ενιαίο περιβάλλον που προστατεύει το απόρρητο και την ακεραιότητα των ανταλλασσόμενων πληροφοριών με τη βοήθεια της κρυπτογράφησης, της ψηφιακής υπογραφής και των ψηφιακών πιστοποιητικών που αναφέρθηκαν εκτενώς παραπάνω.(«Τα Πληροφοριακά Συστήματα Διοίκησης Στη Νέα Οικονομία», Παν.Σ.Αναστασιάδης.)

Το παρακάτω λεπτομερές σχήμα περιγράφει συνοπτικά όλη την ασφάλεια του Πληροφοριακού Συστήματος:



Σχήμα: Η ασφάλεια του πληροφοριακού συστήματος μίας νέας επιχείρησης και τρόποι αντιμετώπισης.

ΕΠΙΛΟΓΟΣ – ΣΥΜΠΕΡΑΣΜΑΤΑ

Με την πάροδο του χρόνου και με τη ραγδαία εξέλιξη της τεχνολογίας της Πληροφορικής, είναι αξιοσημείωτη η πρόοδος που έχει παρουσιάσει ο τομέας της Ασφάλειας των Πληροφοριακών Συστημάτων εν γένει, και των Λογιστικών ειδικότερα, γεγονός βέβαια που δε σημαίνει πως δεν υπάρχουν ακόμη πολλά περιθώρια βελτίωσης. Οι ανακατατάξεις που συντελούνται λόγω της εξέλιξης αυτής δεν επιτρέπουν κανένα περιθώριο στασιμότητας, αντίθετα, παρασύρουν τον τομέα της Ασφάλειας στη βελτίωση και στην ανάπτυξή του.

Η ραγδαία ανάπτυξη των πληροφοριακών συστημάτων συνέβαλλε στην απελευθέρωση της πληροφορίας από τα χρονικά και γεωγραφικά της δεσμά, καθιστώντας την από γραφειοκρατική αναγκαιότητα, το πολυτιμότερο ίσως περιουσιακό στοιχείο της επιχείρησης. Η ανάπτυξη ενιαίων πληροφοριακών περιβαλλόντων με δυνατότητα συνεργατικής διαχείρισης, ανέδειξε το πληροφοριακό σύστημα ως το κέντρο αυτοματοποίησης της επιχειρηματικής διαδικασίας και της υποστήριξης σύνθετων αποφάσεων σε όλα τα επίπεδα διοικητικής και λογιστικής διάρθρωσης.

Η πρόσβαση των υπαλλήλων και των μεσαίων στελεχών στο πολυτιμότερο περιουσιακό στοιχείο της επιχείρησης, μέσω της δυνατότητας ενημέρωσης, τροποποίησης και εισαγωγής νέων στοιχείων και δεδομένων, αποτελεί ένα σημαντικό ζήτημα που άπτεται της προστασίας των πληροφοριών από λάθος χειρισμούς ή κακόβουλες ενέργειες.

Μη ξεχνάμε βέβαια ότι οι Η/Υ είναι ευάλωτοι και όσο αυξάνονται οι δυνατότητες επικοινωνίας μεταξύ τους, γίνονται όλο και πιο ευπρόσβλητοι σε ιούς, οι οποίοι με τη σειρά τους βελτιώνονται με τον ίδιο ρυθμό, κι έτσι η επιταγή μεγαλύτερης Ασφάλειας στα Πληροφοριακά Συστήματα έρχεται και θα έρχεται πάντα στο προσκήνιο.

Η επέκταση της επιχειρηματικής δραστηριότητας στον κόσμο της εικονικής πραγματικότητας, αποτελεί απτή καθημερινότητα για χιλιάδες μικρές και μεγάλες επιχειρήσεις σε ολόκληρο τον κόσμο. Στις λεωφόρους των πληροφοριών, εκατομμύρια καταναλωτές συνωστίζονται στις ηλεκτρονικές βιτρίνες των καταστημάτων, αναζητώντας προϊόντα και υπηρεσίες προκειμένου να ικανοποιήσουν τις καταναλωτικές τους ανάγκες. Μια ιδιότυπη, χωρίς ιστορικό προηγούμενο αγορά, η οποία λειτουργεί 24 ώρες το 24ωρο, 365 μέρες το χρόνο, απαλλαγμένη από γεωγραφικούς και χρονικούς περιορισμούς, τείνει να αντικαταστήσει την παραδοσιακή αγορά, έτσι όπως την γνωρίζαμε αιώνες τώρα.

Αν μέχρι σήμερα το κύριο μέλημα των επιχειρήσεων ήταν η εξασφάλιση των περιουσιακών τους στοιχείων, των εγκαταστάσεων, των εμπορευμάτων και του εξοπλισμού τους έναντι φυσικών καταστροφών ή κακόβουλης βλάβης, η μετάβαση της επιχειρηματιής δραστηριότητας στην παγκόσμια εικονική αγορά μέσω του Internet δημιουργεί νέες ανάγκες και απαιτήσεις στον τομέα της ασφάλειας. Για τη νέα επιχείρηση το διαδίκτυο αποτελεί την πύλη εισόδου προκειμένου να δραστηριοποιηθεί στη νέα παγκόσμια ψηφιακή αγορά και να έρθει σε επαφή με εκατομμύρια καταναλωτές από ολόκληρο τον κόσμο.

Η νέα αυτή πρόκληση συνοδεύεται και από σημαντικούς κινδύνους καθώς το διαδικτυακό περιβάλλον από τη φύση του δεν φιλοξενεί μόνο αγαθούς σκοπούς και δραστηριότητες, αλλά συγκεντρώνει ικανό πλήθος επιβλαβών και παράνομων δραστηριοτήτων. Η δραστηριοποίηση της επιχείρησης στο χώρο της νέας οικονομίας και του διαδικτύου αλλάζει τα δεδομένα, καθώς δεν αποτελεί πλέον μια απομονωμένη πληροφοριακή νησίδα επιχειρηματικότητας, αλλά πλέον συμμετέχει σε ένα παγκόσμιο ιστό επικοινωνίας και διασύνδεσης με απλές αντίστοιχες επιχειρήσεις από ολόκληρο τον κόσμο.

Το γεγονός αυτό την καθιστά ευάλωτη σε οργανωμένες και συστηματικές επιθέσεις από τους πειρατές των ηλεκτρονικών λεωφόρων, των λεγόμενων 'hackers', αλλά και οποιουδήποτε άλλου, ο οποίος έχει λόγους να βλάψει την εταιρία αποκομίζοντας βέβαια τα σχετικά οφέλη.

Η είσοδος της επιχείρησης στο χώρο της νέας οικονομίας διευρύνει κατά πολύ την πιθανότητα παραβίασης της ασφάλειας των Πληροφοριακών Συστημάτων, καθώς πλέον κινδυνεύουν από οποιονδήποτε γνωρίζει τα μυστικά του μαγικού κόσμου του διαδικτύου. Παράλληλα, το εύρος των παραβιάσεων και των επιλογών που έχει στη διάθεσή του ο επίδοξος 'κυβερνοεισβολέας' , καθιστά οδυνηρότατες τις συνέπειες για την επιχείρηση αν τελικά επιτύχει το έργο του.

Έτσι, η ραγδαία εισαγωγή πληροφοριακών συστημάτων έχει δημιουργήσει πλήρη εξάρτηση των επιχειρησιακών λειτουργιών από την Πληροφορική. Αυτό έχει σαν αποτέλεσμα να αυξάνονται σημαντικά οι κίνδυνοι που προκύπτουν από τη χρήση της, όπως η επικινδυνότητα ως προς την πρόσβαση στις πληροφορίες, η ακεραιότητα των πληροφοριών, η εμπιστευτικότητα των μηνυμάτων και η αξιοπιστία των δικτυακών υποδομών. Προκειμένου λοιπόν να αντιμετωπιστούν οι κίνδυνοι αυτοί με επιτυχία, αναπτύχθηκαν μέθοδοι και προγράμματα Ασφάλειας Λογιστικών, και όχι μόνο, Πληροφοριακών Συστημάτων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Γιαννακόπουλος Διονύσης, Παπουτσής Ιωάννης (2003), «Διοικητικά Πληροφοριακά Συστήματα», Σύγχρονη Εκδοτική, Αθήνα.

[2] Αναστασιάδης Παναγιώτης, (2001), «Τα Πληροφοριακά Συστήματα Διοίκησης Στη Νέα Οικονομία – Η Νέα Ψηφιακή Μεταμηχανογραφημένη Επιχείρηση», Εκδόσεις Alfa Books – Scientific Editions, Αθήνα.

[3] «Πώς Δουλεύουν οι Η/Υ», Εκδόσεις Κλειδάριθμος, Βιβλιοθήκη ΤΕΙ Πατρών.

[4] «Λογιστικά Πληροφοριακά Συστήματα – Σύγχρονες Υπηρεσίες», σημειώσεις ομώνυμου μαθήματος των καθ. Β.Ταμπακά και Γ.Ορφανού, ΤΕΙ Πατρών.

[5] www.in.gr Ηλεκτρονική διεύθυνση περιοδικού 'Ram'.