Τ.Ε.Ι. ΠΕΛΟΠΟΝΝΗΣΟΥ

Τμήμα Μηχανικών Πληροφορικής Τ.Ε.
Σχολή Τεχνολογικών Εφαρμογών

Πτυχιακή εργασία

Ανάλυση Κινδύνων και Συστήματα Διαχείρισης Ασφαλείας Πληροφοριακών Συστημάτων σε Μεγάλους Οργανισμούς

Επιβλέπων καθηγητής: Σαλτάρη Γεωργία

Φοιτητής: Προκόπος Γεώργιος
ΑΜ:

Σπάρτη, Νοέμβριος 2014

Περίληψη

Τα τελευταία χρόνια διαπιστώνεται ραγδαία εξέλιξη στην ανάπτυξη των συστημάτων πληροφορικής. Πολλοί από τους οργανισμούς του Δημοσίου και του Ιδιωτικού τομέα, βασίζονται στην ύπαρξη των πληροφοριακών συστημάτων. Αξιοποιώντας τα συστήματα αυτά σε καθημερινή βάση ανταλλάζουν πληροφορίες, προσφέρουν και αναπτύσσουν υπηρεσίες μεταφέροντας μεγάλο όγκο δεδομένων. Η ασφάλεια των Π.Σ είναι κρίσιμος παράγοντας για τη λειτουργία αλλά και τη βιωσιμότητα ενός οργανισμού. Η παραμικρή δυσλειτουργία, η διακοπή και η παράνομη διείσδυση στα πληροφοριακά συστήματα έχουν ως αντίκτυπο να υπάρχουν οικονομικές απώλειες ακόμα και αδυναμία του οργανισμού να λειτουργήσει ομαλά. Ακόμα τα σοβαρότερα προβλήματα ασφαλείας των Π.Σ επικεντρώνονται περισσότερο στο κομμάτι των συστημάτων εκείνων, όπου υπάρχουν καταγεγραμμένα ευαίσθητα δεδομένα, πληροφορίες και σημαντικές λειτουργίες. Για να επιτευχθεί η ασφάλεια χρειάζεται να εφαρμοστούν κατάλληλα μέτρα απέναντι στις διάφορες απειλές που μπορεί να δεχθούν.

Η παρούσα πτυχιακή εργασία πραγματεύεται τα προβλήματα ασφαλείας που μπορεί να προκύψουν τόσο από το εσωτερικό όσο και από το εξωτερικό περιβάλλον, την ανάλυση κινδύνων των Πληροφοριακών Συστημάτων, και τις λύσεις που παρέχονται στη σύγχρονη αγορά (μέθοδοι, πακέτα λογισμικών κ.α.)

Λέξεις Κλειδιά: « Συστημάτων Πληροφορικής ,Όγκο Δεδομένων, Ασφάλεια , Απειλές, Ανάλυση Κινδύνων , Πακέτα Λογισμικών ».

Abstract

In the past few year is realised rapid development in the growth of systems of information technology. Many from the organisms of State and Private sector, as well as enterprises is based on the existence of informative systems. Developing this systems in daily base exchange information, offers and develops services exchanging big volume of data. The safety of informative systems is critical factor for the operation but also the viability of organism. The least dysfunction, the interruption and the illegal infiltration in the informative systems have as impact exist economic losses and also weakness of organism to function smoothly. Still the more serious problems of safety of informative systems are focused more in the piece of that systems, where exist recorded sensitive given, information and important operations. In order to is achieved the safety it needs are applied suitable metres opposite the various threats that it can accept.

The present final work deals the problems of safety that can result so much from the interior what from abroad environment, the analysis of dangers of informative systems, and the solutions that are provided in the modern market (methods, parcels of softwares e.t.c.).

Keywords: « Systems of Information Technology, Data Volume, Security, Threats, Risk Analysis, Software Packages ».

Ευχαριστίες

Ξεκινώντας αυτή την Πτυχιακή Εργασία θα ήθελα να ευχαριστήσω ιδιαίτερα την υπεύθυνη καθηγήτρια της Εργασίας μου κυρία Γεωργία Σαλτάρη για την πολύτιμη βοήθεια της τόσο σε συμβουλευτικό επίπεδο όσο και για την πληθώρα πληροφοριών που μου παρείχε προκειμένου να καταφέρω να αποπερατώσω την εργασία μου.

Επίσης να ευχαριστήσω όλους τους καθηγητές του τμήματος Μηχανικών Πληροφορικής Τ.Ε. του Τ.Ε.Ι. Πελοποννήσου, τόσο για τις γενικές γνώσεις που μου παρείχαν όσο και για τις χρήσιμες πληροφορίες που μου παρείχαν όταν τις ζήτησα.

Τέλος να ευχαριστήσω όσους συναδέρφους – συμφοιτητές με βοήθησαν στην διαδικτιακή αναζήτηση των πληροφοριών με σκοπό την αποπεράτωση αυτής της εργασίας.

Πίνακας Περιεχομένων

Εικόνες

Πίνακες

Συντομογραφίες

Π.Σ	Πληροφοριακό Σύστημα
CSI	Computer Security Institute
DBIR	Data Breach Investigations Report
DAC	Discretionary Access Control
MAC	Mandatory Access Control
RBAC	Role Based Access Control
ISO	International Organization for Standardization
PKIX	Internet PKI based on X.509
SPKI	Simple Puplic Key Infrastructure
PGP	Pretty Good Privacy
ΥΔΚ	Υποδομής Δημόσιου Κλειδιού
ΕΤΟ	Έμπιστη Τρίτη Οντότητα
SIM	Subscriber Identity Module
PIN	Personal identification number
DES	Data Encryption Standard
MIT	Massachusetts Institute of Technology
DES	Data Encryption Standard
IDEA	International Data Encryption Algorithm
SAFER	Secure And Fast Encryption Routine
TCP/IP	Transmission Control Protocol/Internet Protocol
OSI	Open Systems Interconnection
IP	Internet Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
CPU	Central Processing Unit
RAM	Random Access Memory
FTP	File Transfer Protocol
POP3	Post Office Protocol
HTTPS	Hypertext Transfer Protocol Secure
SSH	Secure Shell
VPN	Virtual Private Network
ESP	Encapsulating Security Payload
IKE	Internet Key Exchange
SSL	Secure Sockets Layer

Εισαγωγή

Έκθεση του Προβλήματος

Στην εποχή μας η ραγδαία τεχνολογική ανάπτυξη των πληροφοριακών συστημάτων και οι υπηρεσίες που μας παρέχουν καθημερινά είναι γεγονός. Πολλοί οργανισμοί βασίζονται στα πληροφοριακά συστήματα τα οποία αποτελούν καθοριστικό παράγοντα για τη λειτουργία και την ανάπτυξή τους. Ταυτόχρονα η συλλογή, η επεξεργασία, η αποθήκευση και η διάθεση δεδομένων αποτελούν σημαντικό αγαθό για τον κάθε οργανισμό. Τα τελευταία χρόνια και λόγω της αυξημένης χρήσης τους, τα πληροφοριακά συστήματα είναι ευάλωτα σε διαφόρων ειδών απειλών, είτε από το εσωτερικό, είτε από το εξωτερικό τους περιβάλλον. Οι απειλές αυτές μπορεί να έχουν ως συνέπεια να προκύψουν ανυπολόγιστα προβλήματα που πολλές φορές μεταφράζονται σε οικονομικές απώλειες ή με την παρεμπόδιση της σωστής λειτουργίας τους.

Πέρα όμως από τις οικονομικές επιπτώσεις τα προβλήματα ασφαλείας γίνονται πιο κρίσιμα σε συστήματα όπου υπάρχουν ευαίσθητα δεδομένα και σε συστήματα όπου πραγματοποιούνται και επεξεργάζονται σημαντικές λειτουργίες (π.χ συστήματα στρατού). Λόγω όμως της ιδιαιτερότητας των συστημάτων και της γρήγορης ανάπτυξής τους σε ένα σύνθετο περιβάλλον μεταβλητών και παραγόντων δημιουργείται μεγαλύτερη πολυπλοκότητα ως προς την ασφάλειά τους.

Επομένως η ανάγκη για ασφάλεια στα πληροφοριακά συστήματα αποτελεί σημαντική προτεραιότητα για όσους τα σχεδιάζουν και τα υλοποιούν καθώς και γι' αυτούς που τα χρησιμοποιούν και τα διαχειρίζονται.

Σκοπός της Εργασίας

Με την παρούσα εργασία θα επικεντρωθούμε στο ζήτημα της ασφάλειας των πληροφοριακών συστημάτων. Συγκεκριμένα θα επικεντρωθούμε στην ανάλυση αλλά και στην καταγραφή των κινδύνων που μπορούν να προκύψουν σε ένα πληροφοριακό σύστημα, τα προβλήματα ασφάλειας από απειλές τόσο από το εσωτερικό όσο και από το εξωτερικό περιβάλλον, που μπορεί να δεχθεί, καθώς και λύσεις που παρέχονται στη σύγχρονη αγορά, όπως μέθοδοι αντιμετώπισης και πακέτα λογισμικών.

Δομή Κεφαλαίων Εργασίας

Η παρούσα εργασία δομείται ως εξής:

Στην **Εισαγωγή** σχολιάζεται το θέμα της ασφάλειας πληροφοριακών συστημάτων.

Στο **1ο Κεφάλαιο** αναλύεται η έννοια των πληροφοριακών συστημάτων. Πιο συγκεκριμένα δίνονται τα χαρακτηριστικά τους , η δομή τους, οι στόχοι τους καθώς και οι λόγοι αποτυχίας στην ασφάλειά τους.

Στο **2ο Κεφάλαιο** αναφέρεται η διαχείριση των κινδύνων των πληροφοριακών συστημάτων. Παρουσιάζονται τα είδη των κινδύνων, η δομή τους, οι κατηγορίες τους, η διαδικασία διαχείρισής τους καθώς και οι υπεύθυνοι αντιμετώπισής τους.

Στο **3ο Κεφάλαιο** παρουσιάζεται ο εντοπισμός των κινδύνων. Γενικότερα αναφέρεται στις πληροφορίες που μπορούν να εξαχθούν από το περιβάλλον του οργανισμού έτσι ώστε να αντιμετωπιστούν οι κίνδυνοι καθώς και ο τρόπος της διαδικασίας που θα συλλεχθούν οι πληροφορίες αυτές.

Το **4ο Κεφάλαιο** αναφέρεται στην ανάλυση των κινδύνων. Προβάλλεται η διαδικασία της ποιοτικής και της ποσοτικής εκτίμησης των κινδύνων καθώς και τα αντίστοιχα πλεονεκτήματά – μειονεκτήματα τους. Τέλος παρουσιάζεται η σύσταση ελέγχου και η σύνταξη αναφοράς, οι οποίες βοηθάνε στη μετρίαση της πιθανής εμφάνισης των απειλών καθώς και την αντιμετώπισή τους.

Στο **5ο Κεφάλαιο** γίνεται αναφορά στην ασφάλεια των πληροφοριακών συστημάτων. Προσδιορίζονται οι πολιτικές ασφαλείας, οι διαδικασίες ταυτοποίησης και αυθεντικοποίησης, τα συστήματα αυθεντικοποίησης και βιομετρίας. Τέλος παρουσιάζονται οι τεχνικές κρυπτογραφίας, οι οποίες χρησιμεύουν για την εμπιστευτικότητα, ακεραιότητα και τη διαθεσιμότητα των δεδομένων.

Στο **6ο Κεφάλαιο** παρουσιάζεται η ασφάλεια των δικτύων. Γίνεται αναφορά στις τεχνολογίες ανίχνευσης και αντιμετώπισης των εισβολών, τις τεχνολογίες για την αντιμετώπιση των ιών (Antivirus), το πρωτόκολλο ασφαλείας του Internet IPsec, τα αναχώματα ασφαλείας (Firewalls), τα αντίγραφα ασφαλείας (BackUp) καθώς και σε περαιτέρω τεχνολογίες ασφάλειας Internet.

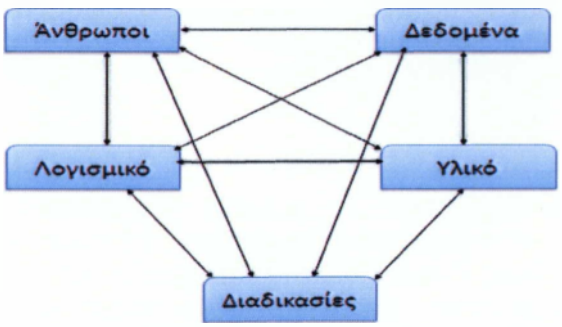
Στον **Επίλογο** εξάγονται τα συμπεράσματα της εργασίας αυτής καθώς και οι μελλοντικές προεκτάσεις.

Κεφάλαιο 1-Εισαγωγικές Έννοιες

Ορισμός Πληροφοριακού Συστήματος

Μέχρι και σήμερα αναφέρονται στη διεθνή βιβλιογραφία παραπάνω από ένας ορισμοί για την έννοια του πληροφοριακού συστήματος που διαφοροποιούνται μεταξύ τους. Πολλοί συγγραφείς δίνουν έμφαση μόνο στην τεχνική πλευρά του πληροφοριακού συστήματος, δηλαδή στην επεξεργασία δεδομένων και των πληροφοριών. Για παράδειγμα ο Aktas(1987) και ο Neuman(1990) ορίζουν το πληροφοριακό σύστημα ως «ένα σύστημα το οποίο δέχεται πληροφορίες, τις αποθηκεύει, ανακτά, μετασχηματίζει, επεξεργάζεται και τις διανέμει στους διάφορους χρήστες του οργανισμού, χρησιμοποιώντας υπολογιστές ή άλλα μέσα ». Για έναν οργανισμό ένα πληροφοριακό σύστημα αποτελεί οικονομική αξία και αποτελεί σημαντικό παράγοντα για την λειτουργία και την ανάπτυξη της. Ο πλησιέστερος ορισμός του Πληροφοριακού Συστήματος για την παρούσα εργασία είναι αυτός, στηριζόμενος με υπολογιστές, σύμφωνα με τον οποίο:

«Πληροφοριακό Σύστημα είναι ένα σύνολο από πέντε στοιχεία (άνθρωποι, λογισμικό, υλικό, διαδικασίες και δεδομένα), τα οποία αλληλεπιδρούν μεταξύ τους και με το περιβάλλον, με σκοπό την παραγωγή και διαχείρισης πληροφορίας, για την υποστήριξη των ανθρώπινων δραστηριοτήτων, στα πλαίσια του οργανισμού»[1]. Επομένως η χρήση του όρου αυτού σημαίνει ότι το πληροφοριακό σύστημα αποτελείται από επιμέρους στοιχεία που αλληλεπιδρούν, χαρακτηρίζεται από οργάνωση και εξετάζεται ως μια ενιαία ολότητα.[1]



Εικόνα 1 - Τα στοιχεία ενός Πληροφοριακού Συστήματος [1].

Χαρακτηριστικά Πληροφοριακών Συστημάτων

Τα Πληροφορικά Συστήματα είναι πολύπλοκα τεχνουργήματα και λόγω της ιδιαιτερότητας που έχουν πρέπει να σχεδιάζονται και αναπτύσσονται με τέτοιον τρόπο έτσι ώστε να στοχεύουν και να υποστηρίζουν την ομαδική και την οργανωτική λήψη αποφάσεων.

Επομένως για όσους τα σχεδιάζουν και τα υλοποιούν, τα συστήματα αυτά πρέπει να βασίζονται στα επιμέρους χαρακτηριστικά:

- ✓ Πρέπει να έχουν δυνατότητα ως προς την υποστήριξη μιας μεγάλης ποικιλίας από γνώσεις, στυλ και δεξιότητες.
- ✓ Πρέπει να είναι ευπροσάρμοστα και να παρέχουν επιλογές ως προς την αξιολόγηση πληροφοριών και χειρισμό δεδομένων.
- ✓ Πρέπει να είναι ισχυρά, να περιλαμβάνουν πολλά διαισθητικά και αναλυτικά μοντέλα αξιολόγησης δεδομένων καθώς και τη δυνατότητα παρατήρησης-αξιολόγησης εναλλακτικών ενεργειών και των επιπτώσεών τους.
- ✓ Πρέπει να είναι ευπροσάρμοστα και ευαίσθητα ως προς τις πολιτικές-γραφειοκρατικές απαιτήσεις του συστήματος.

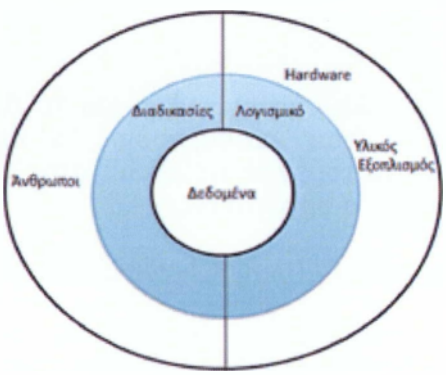
Τα Συστατικά Μέρη Ενός Πληροφοριακού Συστήματος

Ένα Πληροφοριακό Σύστημα, από τεχνικής άποψης, αποτελείται από 6 συστατικά μέρη, τα οποία αλληλεπιδρούν μεταξύ τους αλλά και με το περιβάλλον με στόχο την παραγωγή και τη διαχείριση της πληροφορίας για την υποστήριξη των λειτουργιών του οργανισμού:

1. **Οι Άνθρωποι (People)**: Το σύνολο των ατόμων που ασχολούνται με το πληροφοριακό σύστημα και διακρίνονται σε 3 βασικές κατηγορίες:
   - ✓ **Οι Χρήστες (users)**: Στην κατηγορία αυτή ανήκουν οι κυρίως χρήστες (τελικοί χρήστες – end users) και οι προϊστάμενοί τους (users managers).
   - ✓ **Οι Χειριστές του συστήματος (Operators)**: Στην κατηγορία αυτή βρίσκονται οι χειριστές συντηρητές υλικού και λογισμικού, όσοι εισάγουν στοιχεία (data entry).
   - ✓ **Οι Δημιουργοί του συστήματος (Developers)**: Στην κατηγορία αυτή ανήκουν τα άτομα που ασχολούνται και έχουν την ευθύνη για τη δημιουργία, ανάπτυξη, συντήρηση του πληροφορικού συστήματος. Αυτή η κατηγορία περιλαμβάνει:
     - Τον **Εκπαιδευτή,** που αναλαμβάνει την εκπαίδευση καθώς και την ενημέρωσή του προσωπικού, όπου χρειάζεται.
     - Τον **Προγραμματιστή,** που ασχολείται με το λογισμικό του πληροφοριακού συστήματος.
     - Τον **Αναλυτή,** που αναλύει ,αξιολογεί, καθορίζει τις προδιαγραφές του λογισμικού.
     - Τον **Σχεδιαστή της βάσης δεδομένων**, σε περίπτωση και μόνο αν το πληροφοριακό σύστημα χρησιμοποιεί κάποια βάση δεδομένων.
     - Τον **Ειδικό σε Θέματα Δικτύου**, σε περίπτωση που υπάρχει δίκτυο υπολογιστών στο σύστημα.

- Τον **Υπεύθυνο της Διαχείρισης του έργου,** που αναθέτει εργασίες, σχεδιάζει δραστηριότητες, ο συντονιστής και διευθύνων της ανάπτυξης του συστήματος.
- Ο **Σχεδιαστής Λογισμικού-Υλικού,** που καταγράφει την δημιουργία του λογισμικού-υλικού.
- Ο **Υπεύθυνος Ασφαλείας,** ο οποίος έχει την ευθύνη τόσο για τα δεδομένα όσο και για τα μηχανήματα του συστήματος.

2. **Οι Διαδικασίες (Procedures):** Οι διαδικασίες είναι το σύνολο των οδηγιών για τη χρήση και τη λειτουργία του συστήματος, τις οποίες πρέπει να ακολουθούν οι άνθρωποι. Μερικές οδηγίες είναι το πώς θα εξασφαλίσουν αντίγραφα ασφαλείας ή το πως θα αξιοποιήσουν το υλικό-λογισμικό.
3. **Τα Δεδομένα (Data):** Τα δεδομένα είναι εκείνα τα στοιχεία τα οποία επεξεργάζεται ένα πληροφοριακό σύστημα και εξαρτώνται από τους χρήστες και από τη φύση του συστήματος.
4. **Το Λογισμικό (Software):** Είναι ένα σύνολο προγραμμάτων το οποίο είναι απαραίτητο για τη λειτουργία του συστήματος και της επεξεργασίας των δεδομένων, της παραγωγικότητας (επεξεργαστές κειμένου, εργαλεία βάσης δεδομένων), των εφαρμογών (ελέγχου αποθήκης, λογιστικής).
5. **Ο Υλικός Εξοπλισμός (Hardware):** Είναι ένα σύνολο μηχανικών εξαρτημάτων (επεξεργαστές, οθόνες, πληκτρολόγια ,εκτυπωτές) που δέχονται πληροφορίες και εφόσον τις επεξεργαστούν τις εμφανίζουν.
6. **Το Δίκτυο Επικοινωνιών (Network of Communications):** Είναι το σύστημα σύνδεσης το οποίο είναι αναγκαίο για τη μεταφορά πόρων (πληροφοριών) σε υπολογιστές (Η/Υ).

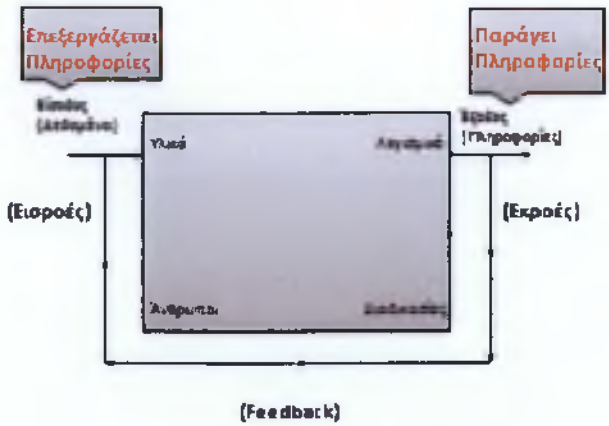


Εικόνα 2 - Η Αναπαράσταση της Δομής ενός Πληροφοριακού Συστήματος

Τα πληροφοριακά συστήματα έχουν εισροές οι οποίες μετατρέπονται ή επεξεργάζονται μέσω κάποιας λειτουργίας που αναπτύσσει το σύστημα και γίνονται εκροές. Έτσι λειτουργούν τα πληροφοριακά συστήματα σε ένα περιβάλλον, ενώ υπάρχει και το κομμάτι της ανατροφοδότησής τους. Τα μέρη από τα οποία αποτελούνται τα πληροφοριακά συστήματα είναι:

- **Οι Εισροές (Inflow)**: Οι εισροές είναι η συλλογή και απόκτηση των δεδομένων που είναι ανεπεξέργαστα, που μπορεί να προέρχονται είτε από το εσωτερικό ή από το εξωτερικό περιβάλλον του οργανισμού.
- **Η Διαδικασία Επεξεργασίας (Processing Procedure)**: Η επεξεργασία και η μετατροπή των ανεπεξέργαστων δεδομένων. Αυτή η διαδικασία επεξεργασίας συνιστάται σε ένα σύνολο δραστηριοτήτων που συνθέτουν τη λειτουργία όλου του συστήματος.

- **Οι Εκροές (Outflow)**: Οι εκροές είναι το αποτέλεσμα της λειτουργίας του συστήματος, δηλαδή οι μεταποιημένες ή επεξεργασμένες πληροφορίες ως προς τις δραστηριότητες και τα άτομα που θα χρησιμοποιηθούν.
- **Ο Μηχανισμός ανατροφοδότησης (Feedback)**: Είναι η εκροή του συστήματος που μετά από έλεγχο επιστρέφει στην επιχείρηση και για να βοηθήσει στην αξιολόγηση αλλά και στη διόρθωση των εισροών.[2]



Εικόνα 3 - Η Σχηματική Απεικόνιση του Πληροφοριακού Συστήματος

Στόχος των Πληροφοριακών Συστημάτων

Όπως και κάθε άλλο σύστημα, έτσι και τα Πληροφοριακά Συστήματα έχουν ένα σκοπό στο περιβάλλον που λειτουργούν. Το περιβάλλον αυτό συνήθως είναι ο οργανισμός, οι βασικές λειτουργίες τις οποίες στηρίζει το πληροφοριακό σύστημα καθώς και τους στόχους που έχει ο οργανισμός.

Οι σημαντικότεροι σκοποί των Πληροφοριακών Συστημάτων είναι οι εξής:

- Η συλλογή, επεξεργασία, αποθήκευση των δεδομένων για την εξαγωγή καθοριστικών πληροφοριών για τον οργανισμό.
- Η ενημέρωση και η χορήγηση λειτουργικής πληροφόρησης ως προς τους εργαζόμενους για να εκτελούν κατά το δυνατόν τρόπο τις δραστηριότητες σε καθημερινή βάση όπως συναλλαγές, προγραμματισμός και έλεγχος.
- Η χορήγηση στρατηγικής πληροφόρησης ως προς τα ανώτατα στελέχη, για την καλύτερη λήψη αποφάσεων για τη μελλοντική πορεία του οργανισμού.
- Η ανάπτυξη και η εξέλιξη των οργανισμών για την εδραίωσή τους στο χώρο των οργανισμών μέσω της σύνδεσης του πληροφοριακού συστήματος με εκείνα των προμηθευτών και πελατών για τη δημιουργία οφέλους από περισσότερη πληροφόρηση.

Παράγοντες Αποτυχίας ενός Πληροφοριακού Συστήματος

Τα Πληροφοριακά Συστήματα είναι συστήματα τα οποία στηρίζουν ανθρώπινες δραστηριότητες εστιάζοντας στις απαιτήσεις που αναφέρονται στις σχέσεις του ανθρώπου αλλά και του συστήματος. Επομένως οι σχεδιαστές θα πρέπει να σχεδιάζουν και να υλοποιούν τα πληροφοριακά συστήματα έχοντας υπόψη τους την ομαλή και σωστή λειτουργία του οργανισμού. Άρα ένας παράγοντας αποτυχίας των πληροφοριακών συστημάτων είναι ότι δίνεται ιδιαίτερη έμφαση ως προς την τεχνική πλευρά του συστήματος και όχι την κοινωνική. Επίσης ένα πληροφοριακό σύστημα μπορεί να έχει πλήρη επιτυχία από τεχνικής άποψης αλλά παράλληλα αποτυχημένο οργανωτικά.

Μερικοί σχεδιαστές δεν αναγνωρίζουν το πόσο σημαντικός παράγοντας είναι ο άνθρωπος, χωρίς να το λάβουν υπόψη κατά τη δημιουργία του πληροφοριακού συστήματος. Ακόμα ένας παράγοντας που οδηγεί στην αποτυχία των πληροφοριακών συστημάτων είναι ότι υπάρχει έλλειψη στο κομμάτι της εκπαίδευσης και της διαχείρισής τους. Επομένως στη διαδικασία της ανάπτυξης των πληροφορικών συστημάτων είναι σημαντικό κομμάτι ο προσδιορισμός των ανθρωπίνων αναγκών, η οποία προϋποθέτει ικανότητες που δεν υπάρχουν στους προγραμματιστές και αναλυτές. Αυτό γίνεται διότι οι αναλυτές και οι προγραμματιστές έχουν και βασίζονται μόνο στις τεχνικές γνώσεις και δε γνωρίζουν αλλά ούτε δίνουν ιδιαίτερη έμφαση ως προς το κομμάτι της ανθρώπινης ψυχολογίας και συμπεριφοράς.

Επομένως όποιος ασχολείται με τον τομέα των πληροφοριακών συστημάτων πρέπει να δίνει έμφαση και σε άλλους παράγοντες ώστε τα πληροφοριακά συστήματα να μπορούν να πετύχουν το σκοπό τους.[9]

Κεφάλαιο 2- Διαχείριση Κινδύνων στα Πληροφοριακά Συστήματα

Εισαγωγή

Κάθε οργανισμός επιλέγει να εισάγει στο περιβάλλον του ένα πληροφοριακό σύστημα βασιζόμενος στη λειτουργία, ανάπτυξη, επίτευξη κερδών καθώς και τη δημιουργία ανταγωνιστικού κλίματος και πλεονεκτήματος. Ωστόσο η ενοποίηση του οργανισμού με ένα πληροφοριακό σύστημα δεν είναι μια απλή αλλά μια περίπλοκη διαδικασία, κι αυτό γιατί το περιβάλλον που λειτουργεί και εξελίσσεται ο οργανισμός είναι πολύ ευμετάβλητο και περίπλοκο.

Οι κίνδυνοι των πληροφοριακών συστημάτων μπορούν να προέρχονται από πολλές πηγές. Σε περίπτωση που αγνοηθούν μπορούν να αποβούν μοιραίοι. Τα κύρια σημεία που πρέπει να δώσουν ιδιαίτερη προσοχή, λόγω των κινδύνων, τα διοικητικά στελέχη είναι η πρόσβαση στο δίκτυο του οργανισμού, η ακεραιότητα των πληροφοριών και δεδομένων του και η απόκτηση και ανάπτυξη των λογισμικών.

Επομένως για να αντιμετωπιστούν ενδεχόμενοι κίνδυνοι, που μπορεί να προκύψουν, πρέπει να εφαρμοστεί και να εκτελεστεί μια σειρά από ενέργειες οι οποίες αναφέρονται και αναλύονται παρακάτω. Η ενότητα αυτή εστιάζεται στη διευκρίνηση και ανάλυση των κινδύνων καθώς και του σχεδίου το οποίο πρέπει να κατέχει ένας οργανισμός ώστε αρχικά να εντοπίσει και ύστερα να αντιμετωπίσει τους κινδύνους, έτσι ώστε να αποφύγει κάθε αποτυχία ή απόκλιση των στόχων του.

Ορισμός Κινδύνου

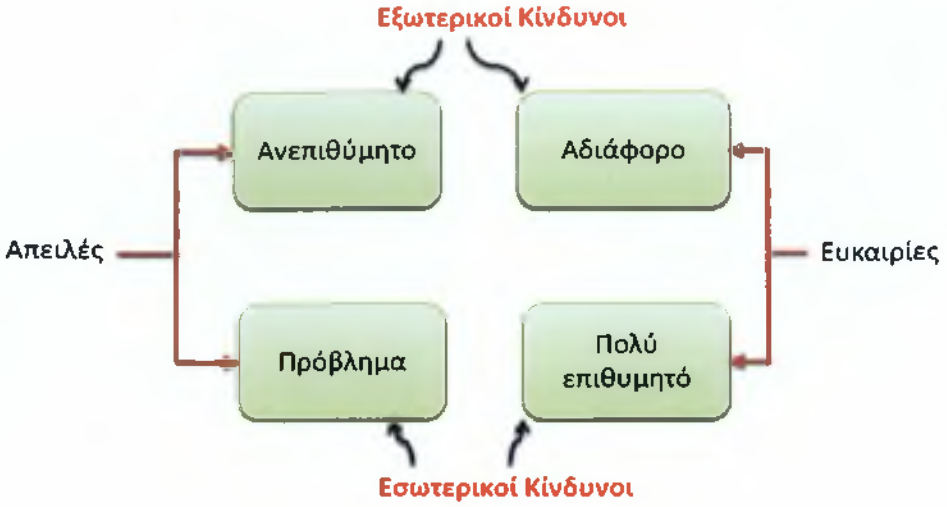
Η έννοια του κινδύνου μπορεί να οριστεί και σχετιστεί με οτιδήποτε μπορεί να προκαλέσει ζημιά σε έναν οργανισμό. Ο κίνδυνος είναι ένα γεγονός το οποίο δεν μπορούμε να συμπεράνουμε αν γίνει ή όχι. Το μόνο που μπορεί να προσδιοριστεί είναι πόσο πιθανό είναι να συμβεί ή όχι. Ακόμα ο κίνδυνος μπορεί να παρουσιαστεί έχοντας αρνητική ή θετική συνέπεια. Το κατά πόσο μπορεί να θεωρηθεί αρνητικός ή θετικός δεν είναι και πολύ σαφές. Οι κίνδυνοι χωρίζονται σε Ευκαιρίες **(Opportunities)** ή Απειλές **(Threats)** ανάλογα με το πώς επηρεάζουν ένα έργο θετικά η αρνητικά.[10]

Τα Είδη των Κινδύνων

Οι κίνδυνοι μπορούν να διαχωριστούν ανάλογα με την προέλευσή τους και τη φύση τους.

Ως προς την προέλευσή τους οι κίνδυνοι μπορεί να διαχωριστούν σε εσωτερικούς ή εξωτερικούς. Για να ξεχωρίσουμε έναν εσωτερικό ή εξωτερικό κίνδυνο θα πρέπει κάποιος να αναρωτηθεί αν ο οργανισμός που εκτελεί το έργο είναι σε θέση μέσω από κάποιες ενέργειες να υπολογίση την πιθανότητα εμφάνισης του κινδύνου.Το χαρακτηριστικό στοιχείο που έχουν οι εξωτερικοί κίνδυνοι είναι ότι είναι αδύνατον να αλλάξει η πιθανότητα εμφάνισής τους μέσω κάποια ενέργειας του οργανισμού.

Ως προς τη φύση τους μπορούν να προσδιοριστούν ως ευκαιρίες ή απειλές και σε ενδεχόμενο παρουσίασή τους να επηρεάσουν θετικά ή αρνητικά τους στόχους του οργανισμού.



Εικόνα 4 - Διάκριση των Κινδύνων ως προς την Φύση και την Προέλευση τους

Η Δομή των Κινδύνων

Ο κάθε κίνδυνος, ανεξαρτήτως από το είδος της φύσης του, της προέλευσής του και της περιοχής όπου επιδρά, έχει μια συγκεκριμένη δομή. Ο κίνδυνος παράγεται επειδή υπάρχουν κάποιες αιτίες, και με τον ερχομό του θα προξενήσει κάποιες συνέπειες στους στόχους του έργου που έχει ορίσει κάθε οργανισμός. Κάθε ένα στοιχείο της δομής του κινδύνου περιέχει και ορισμένα χαρακτηριστικά.

Ειδικότερα κάθε αιτία μπορεί να περιέχει είναι ένα συμβάν το οποίο θα οδηγήσει στην εμφάνιση ενός κινδύνου. Για την εμφάνιση ενός κινδύνου μπορεί να υπάρχουν πολλές αιτίες καθώς και μια αιτία μπορεί να αφορά περισσότερους κινδύνους. Επομένως ο κίνδυνος ή αλλιώς το πόσο σπουδαίος είναι έχει να κάνει με το ενδεχόμενο εμφάνισής του καθώς και με τη συνέπειά του. Το τελευταίο στοιχείο της δομής του κινδύνου είναι η συνέπεια η οποία δείχνει το πόσο σπουδαία είναι η συνέπεια του κινδύνου σε περίπτωση εμφάνισής του, ως προς τον στόχο του έργου. Επομένως ένας κίνδυνος μπορεί να έχει πολλές συνέπειες και μια συνέπεια μπορεί να δημιουργείται από πολλούς κινδύνους.[11]

Εικόνα 5 - Η Δομή του Κινδύνου

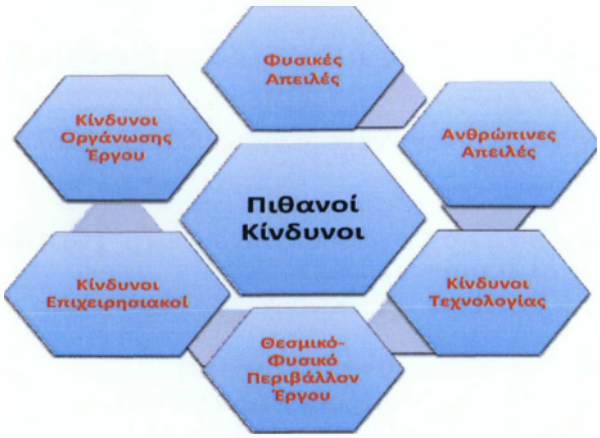
Οι Κατηγορίες των Κινδύνων

Οι κίνδυνοι οι οποίοι μπορούν να παρουσιαστούν κατά την περίοδο λειτουργίας ενός πληροφοριακού συστήματος καθώς και την περίοδο της ολοκλήρωσής του, μπορούν να ανιχνευτούν από εξειδικευμένο προσωπικό που κατέχει όχι μόνο γνώσεις και εμπειρίες αλλά και αντιληπτικότητα ώστε να αντιλαμβάνοται τους κινδύνους.

Παρακάτω αναφέρονται έξι σημαντικές κατηγορίες κινδύνων που μπορούν να παρουσιαστούν σε ένα πληροφοριακό σύστημα:

- **Οι Φυσικές Απειλές (Natural Threats)**: Οι φυσικές απειλές όπως οι πλημμύρες και οι σεισμοί δεν επικεντρώνονται μόνο στα πληροφοριακά συστήματα αλλά έχουν άμεση σχέση με τις κτηριακές υποδομές του οργανισμού αλλά και έμμεση με τα πληροφοριακά συστήματα που στεγάζονται εκεί. Αυτό έχει ως συνέπεια τέτοιες καταστροφές να δημιουργήσουν προβλήματα που θα ενισχύσουν το κόστος και το χρόνο πραγματοποίησης του έργου.
- **Οι Ανθρώπινες Απειλές (Human Threats)**: Στις ανθρώπινες απειλές βρίσκονται τα άτομα τα οποία προκαλούν βλάβες στο λογισμικό του πληροφοριακού συστήματος αποτελούν είτε ανταγωνιστές που αποσκοπούν να βλάψουν την αξιοπιστία, ακεραιότητα και την εμπιστευτικότητα του οργανισμού και του έργου του, καθώς και άτομα που αποτελούν το ίδιο το προσωπικό του οργανισμού επιχείρησης που τα προκαλούν για προσωπικούς λόγους.
- **Οι Κίνδυνοι Τεχνολογίας (Dangers of Technology)**: Οι κίνδυνοι της τεχνολογίας αποτελούν τους κινδύνους που μπορεί να προκληθούν από την εισαγωγή νέων συστημάτων σε έναν οργανισμό εξαιτίας την μη δυνατότητας να λειτουργήσουν σύμφωνα με τις απαιτήσεις τους.Ακόμα ο μη κατάλληλος εξοπλισμός της νέας τεχνολογίας μπορεί να δημιουργήσει διάφορα προβλήματα όπως το να βγει εκτός προγράμματος στους στόχους που έχει θέσει.
- **Το Θεσμικό-Φυσικό Περιβάλλον Έργου (Institutional-Natural Environment Project)**: Με τον όρο «θεσμικό» περιβάλλον του έργου αναφερόμαστε σε εκείνους τους θεσμούς τους οποίους πρέπει να εφαρμόσει και αναπτύξει το πληροφοριακό σύστημα του οργανισμού έτσι ώστε να πειθαρχεί με αυτούς για να αποφύγει ενδεχόμενες κυρώσεις για θεσμική ανυπακοή αποτέλεσμα που θα προκαλέσει μεγάλες οικονομικές ζημίες αλλά και χάσιμο πολύτιμου χρόνου.

  Με τον όρο «φυσικό» περιβάλλον έργου αναφερόμαστε στις εγκαταστάσεις του οργανισμού που στεγάζονται τα πληροφοριακά συστήματα. Σε περίπτωση που στεγάζονται σε παλαιές εγκαταστάσεις προκύπτει το ενδεχόμενο να υπάρχει πρόβλημα σε θέματα όπως η παροχή ηλεκτρισμού το οποίο μπορεί να καταστεί δυνατό να επιφέρει τη διακοπή λειτουργίας αλλά και την καταστροφή του εξοπλισμού (λογισμικού, απώλεια δεδομένων).
- **Οι Επιχειρησιακοί Κίνδυνοι (Dangers Operational)**: Οι κίνδυνοι αυτοί αναφέρονται στην αδυναμία της προσάρτησης νέας τεχνολογίας σε κάθε οργανισμό που έχει σαν αποτέλεσμα την εμπόδιση της λειτουργίας του πληροφοριακού συστήματος. Αυτός ο κίνδυνος προκαλείται από τις τυχόν καθυστερήσεις της υλοποίησης του έργου αλλά και της μη κατάλληλης εκπαίδευσης του προσωπικού του οργανισμού.
- **Οι Κίνδυνοι Οργάνωσης Έργου (Dangers of Organisation of Work)**: Ο κίνδυνος αυτός αναφέρεται στην οργάνωση και τη δομή του έργου. Έχει σχέση άμεσα με τα άτομα τα οποία έχουν την ευθύνη για την υλοποίηση και το σχεδιασμό του. Σε περίπτωση που υπάρχει έλλειψη εκπαίδευσης των ειδικών, ανεπάρκεια τεχνογνωσιών και μη λήψη αποφάσεων μπορεί να προκαλέσει οικονομικά και χρονικά ζητήματα στον οργανισμό.[10]

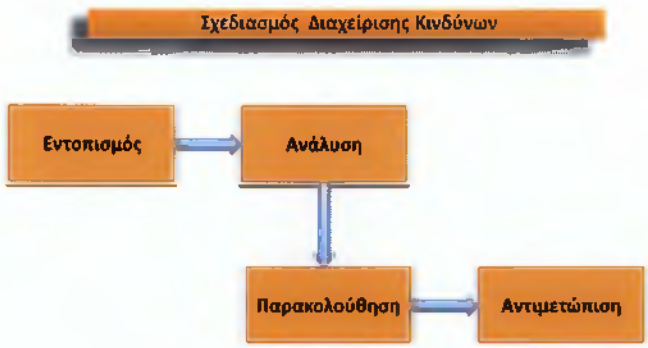


Εικόνα 6 - Κατηγορίες Κινδύνων Πληροφοριακών Συστημάτων.

Η Διαχείριση των Κινδύνων

Η διαχείριση κινδύνων είναι η διεξαγωγή εντοπισμού, παρακολούθησης, ανάλυσης και αντιμετώπισης των κινδύνων που προκύπτουν και σχετίζεται με την ελαχιστοποίηση των κινδύνων. Ως επί των πλείστων αυξάνει το ποσοστό και τις συνέπειες εμφάνισης θετικών γεγονότων και μειώνει τον ποσοστό και τις συνέπειες αρνητικών γεγονότων με στόχο την εκτέλεση του έργου.

Συγκεκριμένα η διαχείριση κινδύνων είναι η διαδικασία που στοχεύει στη βοήθεια των ατόμων της ομάδας διαχείρισης κινδύνων να μην παρεκκλίνουν από τον στόχο του οργανισμού και να λαμβάνουν μέτρα ασφαλείας καθώς και την επίλυση προβλημάτων πριν καν εμφανιστούν στα πληροφοριακά συστήματα. Με το έργο διαχείρισης κινδύνου (Project Risk Management) στο οποίο περιλαμβάνεται ο τρόπος που θα εκτελεστεί η διαδικασία και ο ρυθμός συναντήσεων μπορεί να καταγραφεί πριν την έναρξη της διαδικασίας. Ο στόχος του έργου διαχείρισης κινδύνου είναι να προστατέψει δίνοντας ασφάλεια σε διάφορες πληροφορίες και δεδομένα σε όποιον προσπαθήσει να τα αφαιρέσει από οποιοδήποτε πληροφοριακό σύστημα.



Εικόνα 7 - Εξέλιξη Διαχείρισης Κινδύνων.

Η Εκτέλεση της Διαδικασίας Διαχείρισης Κινδύνων

Η εκτέλεση της διαδικασίας διαχείρισης κινδύνων ακολουθεί 6 βήματα τα οποία είναι τα εξής:

- Ανάπτυξη σχεδίου διαχείρισης Κινδύνων **(Growth of drawing of management of Dangers).**
- Ανίχνευση και εντοπισμός Κινδύνων **(Detection and localisation of Dangers).**
- Ανάλυση Κινδύνων **(Analysis of Dangers).**
- Αντιμετώπιση Κινδύνων **(Dangers Prevention).**
- Παρακολούθηση Κινδύνων **(Oobservation of Dangers).**
- Αναφορά και Αξιολόγηση Κινδύνων **(Report and Dangers Assessment).**

Το αρχικό στάδιο της διαδικασίας διαχείρισης κινδύνων περιέχει την ανάπτυξη σχεδίου διαχείρισης κινδύνων (Growth of drawing of management of Dangers) το οποίο είναι βασικό στοιχείο που υλοποιεί τη διαδικασία διαχείρισης κινδύνων. Ο σχεδιασμός του και η πληρότητα είναι σημαντικός παράγοντας για την επιτυχία και αποτυχία του. Το σχέδιο αυτό παρουσιάζει τον τρόπο με τον οποίο υλοποιούνται τα στάδια της διαδικασίας της διαχείρισης κινδύνων. Το μέγεθος του σχεδίου είναι ισοδύναμο με το μέγεθος του έργου και είναι αναγκαίο όσο μικρό και αν είναι το έργο. Τα περιεχόμενα του σχεδίου ανάλυσης κινδύνων κατηγοριοποιούνται ως εξής:

- **Η Τεχνική (Technique)**: Η τεχνική περιέχει μεθόδους καταγραφής ώστε να οριστεί ο τρόπος προσέγγισης της διαχείρισης των κινδύνων και τα εργαλεία καθώς και οι πηγές για την αναζήτηση στοιχείων. Για παράδειγμα σε μια τεχνική θα πρέπει να καθοριστεί αν ο εντοπισμός των κινδύνων θα γίνει από τον ίδιο οργανισμό που είναι αρμόδιος για την υλοποίηση του έργου.
- **Οι Ρόλοι και Αρμοδιότητες (Roles and Responsibilities):** Έχοντας επιλέξει την τεχνική μπορεί αμέσως να συγκροτηθεί η ομάδα της διαχείρισης του κινδύνου και να γίνει η μοιρασιά των αρμοδιοτήτων. Μετά εγκρίνεται ο αρμόδιος της διαδικασίας και αποφασίζεται αν η ομάδα είναι εσωτερική ή εξωτερική. Ως προς την εσωτερική ομάδα δεν προκύπτει πρόβλημα στην εξουσία διότι τα στελέχη έχουν τις κατάλληλες γνώσεις για τα δεδομένα του οργανισμού. Αντιθέτως στην εξωτερική ομάδα πρέπει να υλοποιείται πλήρως το πρόγραμμα του έργου και να υπάρχει καλή συνεννόηση της ομάδας και της διοίκησης για το καλύτερο αποτέλεσμα.
- **Ο Οικονομικός Προϋπολογισμός (Financial Budget):** Για να οριστεί ο οικονομικός προϋπολογισμός της διαχείρισης των κινδύνων υπάρχουν πολλοί τρόποι. Ένας από αυτούς είναι να καθοριστεί ένα ποσό του κόστους του έργου για την αντιμετώπιση του κινδύνου. Το μειονέκτημα είναι ότι δεν μπορούν να καθοριστούν από πριν οι κίνδυνοι άρα το ποσό μπορεί να ξεπεράσει το υπάρχον με συνέπεια να προκαλέσει λάθος αποτέλεσμα. Ένας δεύτερος τρόπος είναι η ανάλυση των κινδύνων και η εκτίμηση μιας συνολικής έκθεσης. Το μειονέκτημα και σε αυτήν την περίπτωση είναι ότι ο προϋπολογισμός θα υπολογιστεί σε ανάλογο χρόνο έτσι ώστε να προσδιοριστούν καλύτερα ο εντοπισμός και η ανάλυση τω κινδύνων.Μια παραλλαγή και τρόπων αυτών είναι η επιλογή και των δύο. Από τη μια θα είναι γνωστό το κόστος της διαχείρισης των κινδύνων και από την άλλη το κόστος θα πρέπει να συνυπολογίζεται στο συνολικό κόστος για τη διαχείριση των κινδύνων του έργου.
- **Ο Χρονισμός (Timing):** Θα πρέπει να διεξάγονται περιοδικές συναντήσεις για τη συζήτηση των αναφορών σχετικά με την εξέλιξη, εντοπισμό και την αντιμετώπιση των νέων κινδύνων.
- **Η Εκπαίδευση (Education):** Θα πρέπει να διεξάγονται προγράμματα εκπαίδευσης για τα στελέχη της διαχείρισης έργων είτε από εσωτερικούς ή από

εξωτερικούς συμβούλους προβάλλοντας τεχνικές και εργαλεία αντιμετώπισης για τους κινδύνους.

- **Η Επικοινωνία (Communication):** Είναι ο τρόπος που διέπει την καταγραφή, ανάλυση και την κοινοποίηση των αποτελεσμάτων της διαχείρισης των κινδύνων στους ενδιαφερόμενους του έργου.
- **Η Τεχνική Μέτρησης και Κλίμακες (Technique of measurement and scales):** Εδώ προσδιορίζονται οι τεχνικές μέτρησης (ποσοτικές, ποιοτικές) που θα χρησιμοποιηθούν καθώς και οι κλίμακες (συνέπεια, πιθανότητα) που προσδιορίζουν τα χαρακτηριστικά των κινδύνων.
- **Τα Όρια (Limits):** Πρέπει να προσδιορίζονται τα όρια για τους κινδύνους. Υπάρχουν τρείς κατηγορίες κινδύνων οι ασήμαντοι, οι μέσοι και οι σημαντικοί. Τα όρια αυτά είναι διαφορετικά για κάθε οργανισμό και προσδιορίζουν την κατηγορία στην οποία βρίσκεται ο κίνδυνος. Είναι σημαντικό να προσδιορίζονται τα όρια πριν την εκτέλεση του έργου.[10]

Ο Υπεύθυνος Αντιμετώπισης Κινδύνων

Οι διάφορες κατηγορίες των κινδύνων που υπάρχουν πρέπει να έχουν και τον ανάλογο «Αρμόδιο».Ο διαχειριστής του έργου (Project Manager) σε συνεργασία με το Project Board δίνουν τα κριτήρια αυτά σε ορισμένα άτομα που πρέπει να λαμβάνουν υπόψη τους τα εξής:

- Το υπόβαθρο του συνολικού κινδύνου.
- Η επιθυμία της ομάδας να αντιμετωπίσει τον κίνδυνο, καθώς και της εφαρμογής πολιτικής.
- Τον άμεσο εντοπισμό και αναγνώριση των κινδύνων (είδος απειλής),αντίδραση και γνωστοποίηση στον επικεφαλή της ομάδας (Team Manager).
- Τη διενέργεια καταμετρήσεων ως προς τη συμπεριφορά του κινδύνου.
- Κίνδυνοι που εξαρτώνται και αφορούν την οργάνωση καθώς και τις διαδικασίες του οργανισμού.

Ο εκτελεστής (Executive) είναι αρμόδιος να κατέχει ένα αρχείο καταγραφής κινδύνων (Risk Log) όπου θα έχει καταγράψει όλες τις δραστηριότητες και αρμοδιότητες των ατόμων που εμπλέκονται που προσδιορίζουν τις διαδικασίες για την καταπολέμηση των κινδύνων σε επίσημη μορφή καθώς και τις ευθύνες που έχουν για την καταπολέμηση αυτών. Ο υπεύθυνος του έργου (Project Manager) πρέπει να πληροφορεί για τη συνολική κατάσταση των κινδύνων καθώς και τις ενέργειες που πραγματοποιήθηκαν μετά την κατάσταση αυτή. Σε επίπεδο ομάδας (Group Level) οι κίνδυνοι πρέπει να γνωστοποιούνται στην έκθεση ελέγχου (Checkpoint Report) και σε περίπτωση που ο υπεύθυνος έργου το θεωρήσει κρίσιμο να γνωστοποιήσει κάποιες αναφορές στην κυριότερη έκθεση (Highlight Report). Όμως στο τελικό στάδιο της έκθεσης (End Stage Report) αναφέρεται η τωρινή κατάσταση κινδύνου (Situation of Danger).Οποιαδήποτε αλλαγή που μπορεί να διεξαχθεί στους κινδύνους αναφέρονται στο έλεγχο αλλαγής (Change Control).[11]

Κεφάλαιο 3-Εντοπισμός Κινδύνων

Εισαγωγή

Ο εντοπισμός των κινδύνων αποτελεί το δεύτερο στάδιο διαχείρισης κινδύνων μετά την ανάπτυξη σχεδίου διαχείρισης κινδύνων. Οι οργανισμοί εφαρμόζουν τον εντοπισμό των κινδύνων σε ένα πληροφοριακό σύστημα για την εμφάνιση πιθανών κινδύνων και απειλών σε αυτό κατά τη περίοδο εγκατάστασής του. Η διαδικασία αυτή διασαφηνίζει τους κατάλληλους ελέγχους για τη μείωση ή την εξαφάνιση των κινδύνων.

Πληροφορίες σχετικά με το περιβάλλον του οργανισμού

Το αρχικό στάδιο της διαχείρισης κινδύνων περιλαμβάνει τη συλλογή πληροφοριών του οργανισμού στον οποίο θα λειτουργήσει το πληροφοριακό σύστημα, τις ανάγκες που πρέπει να καλύψει και πληροφορίες για την πραγματοποίηση σχετικών έργων κατά το παρελθόν. Αυτός ο τρόπος συλλογής πληροφοριών θα βοηθήσει στη διερεύνηση κινδύνων που μπορεί να προκύψουν για το έργο καθώς και στην εξεύρεση μεθόδων για τη μείωσή τους ή και την εξάλειψη αυτών και των συνεπειών τους.

Επομένως πρέπει να συλλεχθούν πληροφορίες για το περιβάλλον του πληροφοριακού συστήματος. Η κατηγοριοποίηση των πληροφοριών γίνεται σύμφωνα με τα παρακάτω:

- **Το Υλικό (Hardware)**: Η συλλογή πληροφοριών στον παρόντα εξοπλισμό αλλά και τον εξοπλισμό που θα χρησιμοποιηθεί από το νέο πληροφοριακό σύστημα.
- **Το Λογισμικό (Software)**: Η συλλογή πληροφοριών για νέο και παλιό λογισμικό.
- **Οι Διεπαφές Συστημάτων**: Ο προσδιορισμός για τις εξωτερικές και εσωτερικές συνδέσεις του συστήματος.
- **Οι Βάσεις Δεδομένων (Bases of data)**: Η αξία, ο όγκος και το είδος δεδομένων και πληροφοριών που θα αναλάβει το νέο λογισμικό.
- **Η Υποστήριξη και η Μεταχείριση του Συστήματος από τα Στελέχη**: Τα στελέχη πρέπει να κατέχουν τις κατάλληλες γνώσεις, ώστε να κατανοούν την αξία, τη χρησιμότητα του νέου συστήματος καθώς και το χειρισμό του λογισμικού.
- **Ο Προορισμός του Νέου Συστήματος**: Οι λειτουργίες που πρέπει να υλοποιήσει το πληροφοριακό σύστημα.
- **Η Αξία του Νέου Συστήματος**: Η σημαντικότητα της εγκατάστασης του νέου πληροφοριακού συστήματος για τη λειτουργία του οργανισμού.
- **Η Ευαισθησία του Συστήματος**: Το επίπεδο προστασίας που πρέπει να υπάρχει για τη διασφάλιση της ακεραιότητας, εμπιστευτικότητας, διαθεσιμότητας των πληροφοριών και συστημάτων.

Επιπρόσθετες πληροφορίες που έχουν σχέση με το λειτουργικό περιβάλλον του συστήματος και είναι το ίδιο σημαντικές για τη διαδικασία της διαχείρισης κινδύνων, είναι οι παρακάτω:

- **Οι Λειτουργικές Απαιτήσεις του Συστήματος.**
- **Οι Πολιτικές Ασφαλείας των Συστημάτων**: Οι πολιτικές που εφαρμόζει ο οργανισμός.
- **Η Τωρινή Δικτυακή Τοπολογία**: Το δίκτυο στο οποίο στηρίζεται το σύστημα.
- **Η Προστασία των Αποθηκευμένων Πληροφοριών.**
- **Η Ροή Πληροφοριών Σχετικές με το Σύστημα**: Οι διασυνδέσεις του συστήματος, πληροφορίες που εισέρχονται και εξέρχονται από το σύστημα.

- **Οι Τεχνικοί Έλεγχοι που Εφαρμόζονται για το Πληροφοριακό Έργο**: Εδώ αναφέρονται οι διακριτοί ή αυστηροί έλεγχοι πρόσβασης, η προστασία πληροφοριών και τεχνικές κρυπτογράφησης.
- **Οι Διοικητικοί Έλεγχοι για την Προστασία του Συστήματος.**
- **Οι Λειτουργικοί Έλεγχοι**: Εδώ αναφέρονται ο έλεγχος πρόσβασης χρηστών (ιδιαίτερα σε αυτούς που έχουν πρόσβαση σε λειτουργίες και αρχεία πέρα από των υπαρχουσών), περιπτώσεις της αποκατάστασης και συντήρησης των συστημάτων, περιπτώσεις προσθήκης και διαγραφής δεδομένων.
- **Η Ασφάλεια των Εγκαταστάσεων του Οργανισμού**: Η ασφάλεια τόσο σε εσωτερικό όσο και εξωτερικό επίπεδο.
- **Η Ασφάλεια σε Σχέση με το Φυσικό Περιβάλλον του Έργου**: Εδώ τονίζονται οι έλεγχοι για τη διαχείριση ενέργειας, την έκθεση σε φυσικές καταστροφές.[10,12]

Η Διαδικασία Συλλογής Πληροφοριών

Για τα πληροφοριακά συστήματα τα οποία είναι στο στάδιο της έναρξης ή στο στάδιο του σχεδιασμού οι πληροφορίες προέρχονται είτε από την κατάσταση με τις απαιτήσεις του έργου είτε από το ίδιο το σχέδιο. Όταν το έργο αναπτύσσεται μπορεί να προέρχονται χρήσιμες πληροφορίες από τον προσδιορισμό των σημαντικών κανόνων και των στοιχείων ασφάλειας που προκαθορίζονται για το σύστημα. Για οποιαδήποτε έργο λογισμικού, οι πληροφορίες που προέρχονται από το περιβάλλον δημιουργίας του έργου, συμπεριλαμβάνουν τα στοιχεία που αφορούν την διαμόρφωση συστημάτων, την διασύνδεσή τους, και τις πρακτικές. Έτσι λοιπόν η περιγραφή των συστημάτων μπορεί να στηριχτεί στην ασφάλεια που δίνεται από την υπάρχουσα υποδομή ή τα σχέδια χρήσης για ασφάλεια στο μέλλον. Όμως αυτή η συγκέντρωση πληροφοριών δεν αποτελεί μια εύκολη διαδικασία και η εκτέλεση της πρέπει να είναι προσεκτική, να καθορίζεται σε επιστημονικό επίπεδο και να απαιτείται αυστηρή ενασχόληση από τα άτομα που θα συγκεντρώσουν αυτές τις πληροφορίες, έτσι ώστε τα αποτελέσματα να είναι αξιόπιστα για να μπορούν να βοηθήσουν στην διαδικασία της διαχείρισης των κινδύνων και όχι να οδηγήσουν σε λάθος συμπεράσματα. Μερικές μέθοδοι για τον εντοπισμό και τη διαχείριση των κινδύνων είναι οι εξής:

- **Τα Ερωτηματολόγια**: Η ομάδα της διαχείρισης κινδύνων για να συγκεντρώσει πληροφορίες θα πρέπει να δημιουργήσει κάποια ερωτηματολόγια που θα επικεντρώνονται στους λειτουργικούς ελέγχους αλλά και στη διαχείριση που κανονίζονται για το νέο πληροφοριακό σύστημα ή των υπαρχόντων συστημάτων. Τα ερωτηματολόγια θα πρέπει να διανεμηθούν στο προσωπικό που θα ασχοληθεί με τη σχεδίαση και την υποστήριξη του πληροφοριακού συστήματος.
- **Οι Συνεντεύξεις**: Οι συνεντεύξεις που θα διενεργούνται τόσο στο προσωπικό υποστήριξης και σχεδίασης του συστήματος όσο και το προσωπικό της διοικήσεως του οργανισμού, μπορούν να παρέχουν στα άτομα τα οποία διεξάγουν την αξιολόγηση των κινδύνων σημαντικές πληροφορίες για την πολυτιμότητα και τον προορισμό του συστήματος καθώς και τις διαφωνίες των στελεχών για την εισαγωγή νέας τεχνολογίας. Ακόμα οι συνεντεύξεις βοηθάνε στην κατανόηση όσον αφορά τα λειτουργικά χαρακτηριστικά του οργανισμού και στην αποτίμηση του περιβάλλοντος που θα εγκατασταθεί το πληροφοριακό σύστημα.
- **Το Πόρισμα Ειδικών**: Εδώ αναφερόμαστε στη συγκέντρωση των πληροφοριών όσον αφορά το φυσικό και λειτουργικό περιβάλλον του έργου από την ομάδα της αξιολόγησης κινδύνων. Η αξία αυτού του πορίσματος είναι σημαντική διότι δεν συμπεριλαμβάνει τις προσωπικές απόψεις των στελεχών του οργανισμού, που υπάρχει περίπτωση να είναι απόλυτα αντικειμενικές, αλλά μόνο την παρακολούθηση και καταγραφή των γεγονότων με βασικό παράγοντα τη διορατικότητα και την ουδετερότητα των ειδικών.
- **Η Αναθεώρηση Εγγράφων**: Με την αναθεώρηση των εγγράφων εννοούμε τα έγγραφα που έχουν πολιτικό περιεχόμενο (νομοθεσίες, κρατικές οδηγίες), τα έγγραφα που αναφέρονται στο σύστημα (σχέδια τους συστήματος, οδηγοί χρήσεων, διοικητικά εγχειρίδια συστημάτων) και έγγραφα που αναφέρονται στην

ασφάλεια (διαδικασίες και σχεδιασμός συστημάτων, έκθεση λογιστικού και ελέγχου και αξιολόγηση κινδύνου) που παρέχουν πολλές και σημαντικές πληροφορίες που μπορούν να διαμορφώσουν μια άψογη εικόνα του οργανισμού και της ποιότητας της λειτουργικότητας του νέου έργου.

- **Η Συγκέντρωση Πληροφοριών από Παρόμοια έργα Πληροφορικής που έχουν ήδη Υλοποιηθεί**: Οι πληροφορίες αυτές είναι πολύτιμες διότι μέσα από αυτές εξάγονται εμπειρίες από παρόμοια έργα και έτσι μπορούν να αποφθεχθούν κάποια λάθη και παραλήψεις από το παρελθόν δημιουργώντας έτσι μια πιο πρακτική εικόνα των τρόπων αντιμετώπισης των συνεπειών.
- **Η Χρήση Αυτοματοποιημένου Ανιχνευτικού Εξοπλισμού**: Μπορούν να αξιοποιηθούν δυναμικές μέθοδοι για τη συλλογή πληροφοριών.[11]

Εικόνα 8 - Μέθοδος Συλλογής Πληροφοριών

Κεφάλαιο 4-Ανάλυση Κινδύνων

Εισαγωγή

Στο κεφάλαιο αυτό θα προβληθεί η διαδικασία ποιοτικής εκτίμησης του επιπέδου έκθεσης των κινδύνων που πρόκειται να εμφανιστούν καθώς και του συνολικού επιπέδου έκθεσης του έργου.Ακόμα θα προβληθεί η διαδικασία της ποσοτικής εκτίμησης των κινδύνων αλλά και η προβολή της αναφοράς που περιέχει τα αποτελέσματα των συνολικών βημάτων της διαδικασίας εκτίμησης των κινδύνων. Η αξιολόγηση των κινδύνων που είναι είτε ποιοτική είτε ποσοτική ακολουθεί και αυτή με τη σειρά της τη διαδοχή των βημάτων της διαδικασίας εκτίμησης των κινδύνων. Ουσιαστικά πρώτα διενεργείται η εκτίμηση της πιθανότητας παρουσίασης νέου κινδύνου και στη συνέχεια η αξιολόγηση των συνεπειών και στο τέλος πραγματοποιείται μια εκτίμηση των παραπάνω σταδίων για την εξαγωγή συμπερασμάτων για τη σοβαρότητα των κινδύνων. Αυτό αναφέρεται κυρίως για την ποιοτική αξιολόγηση που εκθέτεται παρακάτω.

Η Ποιοτική Αξιολόγηση

Η ποιοτική αξιολόγηση κινδύνων στηρίζεται στην πιθανότητα εμφάνισης κινδύνων και των επιπτώσεων που έχουν αυτοί στο έργο, όμως δεν προσδιορίζονται σε απόλυτα μεγέθη. Για τη διατύπωση της πιθανότητας εμφάνισης κινδύνων εφαρμόζονται κάποιες συγκεκριμένες διαβαθμίσεις που δημιουργούν συγκεκριμένες κλίμακες (π. χ λίγο, ελάχιστο, πολύ, πάρα πολύ).Το πρώτο σημαντικό και αξιόλογο εργαλείο της ποιοτικής ανάλυσης είναι οι κλίμακες.

Έχοντας σημειωθεί οι ενδεχόμενοι κίνδυνοι και έχοντας προσδιοριστεί οι έλεγχοι ασφαλείας που προστατεύουν και απειλούν το πληροφοριακό σύστημα, το επόμενο στάδιο είναι η πιθανότητα εμφάνισης κινδύνου.

Κατά τη διεξαγωγή της διαδικασίας εκτίμησης 3 στοιχεία πρέπει να λαμβάνονται υπόψην:

- Οι δυνατότητες και τα κίνητρα της κάθε πηγής των κινδύνων.
- Η φύση των ευπαθειών.
- Η αποτελεσματικότητα και η παρουσία των ελέγχων που υφίστανται.

Η διαδικασία της εκτίμησης των κινδύνων δεν είναι και τόσο απλή. Τα άτομα τα οποία θα διεξάγουν αυτήν την εκτίμηση θα πρέπει να κατέχουν την κατάλληλη κατάρτιση, ενημέρωση και γνώση για να μπορέσουν να εκτιμήσουν σωστά τη πιθανότητα κάθε εμφάνισης κινδύνου ή ανεπιθύμητου γεγονότος. Επομένως οι λανθασμένες εκτιμήσεις μπορεί να έχουν και τις ανάλογες επιπτώσεις (π.χ αξιοπιστία όλης της διαδικασίας διαχείρισης κινδύνων).

Από την άλλη μεριά υπάρχουν οι αισιόδοξες και απαισιόδοξες εκτιμήσεις.Όσον αφορά τις απαισιόδοξες εκτιμήσεις θα έχουν ως συνέπεια τη χρήση πολλών κονδυλίων και την αύξηση της βραδύτητας και πολυπλοκότητας λειτουργίας των συστημάτων για κάποιους κινδύνους που δεν αποτελούν ιδιαίτερη απειλή.

Ο κίνδυνος ως προς την πιθανότητα εμφάνισής του μπορεί να παρουσιαστεί σε 5 κατηγορίες (Πολύ Χαμηλή, Χαμηλή, Μέτρια, Υψηλή, Πολύ Υψηλή):

Πιθανότητα εμφάνισης κινδύνου/ Επίπεδο	Περιγραφή
Πολύ Υψηλή (Very High)	Ο κίνδυνος είναι σχεδόν βέβαιο ότι θα εμφανιστεί και οι διαδικασίες ελέγχου είναι απαραίτητες.
Υψηλή (High)	Ο κίνδυνος υπάρχει μεγάλη πιθανότητα να εμφανιστεί και οι διαδικασίες ελέγχου παρουσιάζουν ελλείψεις και αδυναμίες.
Μέτρια (Moderate)	Ο κίνδυνος δεν έχει μεγάλη πιθανότητα να εμφανιστεί, και οι διαδικασίες ελέγχου τον αντιμετωπίζουν αποτελεσματικά.
Χαμηλή (Low)	Ο κίνδυνος έχει μικρή πιθανότητα να εμφανιστεί αλλά οι διαδικασίες ελέγχου τον αντιμετωπίζουν εύκολα.
Πολύ Χαμηλή (Very Low)	Ο κίνδυνος είναι αδύνατον να εμφανιστεί και οι διαδικασίες ελέγχου αδιαπέραστες.

Πίνακας 1 - Πίνακας Πιθανότητας Εμφάνισης Κινδύνων.

Η κλίμακα που προσδιορίζει τον κίνδυνο εμφάνισης του κινδύνου εντοπίζεται ανάμεσα στο 0,0 (όπου δεν υπάρχει καμία πιθανότητα) και στο 1, 2 (όπου υπάρχει βεβαιότητα). Για να γίνει επακριβής υπολογισμός εμφάνισης κινδύνου αποτελεί μια διαδικασία πολύ δύσκολη και διαρκή καθώς και τα αποτελέσματα που θα παραχθούν είναι δύσκολο να αξιολογηθούν ως προ την ορθότητά τους. Έτσι χρησιμοποιείται συχνά μια έτοιμη γενική κλίμακα που καθορίζει τις πιθανότητες εμφάνισης ενός κινδύνου, οι τιμές που το καθορίζουν είναι: 0,1 . 1,3 . 0,5 . 0,7 . 0,9. Όπως καταγράψαμε και είδαμε παραπάνω τους κινδύνους μπορούμε να τους κατατάξουμε ανάλογα ως προς την πιθανότητα εμφάνισής τους. Σε αυτήν την περίπτωση είναι δύσκολο να προσδιορίσουμε την εμφάνιση της κάθε απειλής. Σε αυτό το σημείο θα είναι χρήσιμες οι πληροφορίες οι οποίες συγκεντρώθηκαν για τον οργανισμό και τους στόχους που θα υλοποιήσει το καινούργιο πληροφοριακό έργο καθώς και τα μέτρα ασφαλείας που υφίστανται. Όπως για παράδειγμα η χρησιμοποίηση των νέων τεχνολογιών παρουσιάζουν μεγάλο ποσοστό επικινδυνότητας και μπορεί να εμφανίσουν κάποια προβλήματα στη χρήση τους και στο τέλος να μην μπορούν να αντεπεξέλθουν στις απαιτήσεις του οργανισμού.Από την άλλη όμως μεριά η χρήση συστημάτων που έχουν ξαναδοκιμαστεί δεν προβληματίζουν ως προς τη χρησιμοποίηση της λειτουργικότητά τους. Αντιθέτως αντιμετωπίζουν τον κίνδυνο να γίνουν παλαιές σε σύντομο χρονικό διάστημα από την ημέρα της λειτουργίας τους, κάτι που έχει λιγότερες πιθανότητες να συμβεί στα συστήματα της νέας τεχνολογίας.

Οι επιπτώσεις που θα προέλθουν κατά την υλοποίηση ενός έργου πρέπει να προσδιορίζονται από τους υπεύθυνους πραγματοποίησή τους και από το διοικητικό τομέα του οργανισμού$, για να έχουν μια ολοκληρωμένη αντίληψη για τις επιπτώσεις καθώς και να διασφαλίσουν σημαντικές αρχές ασφαλείας του συστήματος. Οι σημαντικές απώλειες που μπορεί να εμφανιστούν:

- **Η Απώλεια Ακεραιότητας (Loss of Integrity)**: Η ακεραιότητα στα συστήματα και στις πληροφορίες έχει ως στόχο να προστατεύονται αυτά από κάποιες τροποποιήσεις και καταστροφές καθώς και την άμεση επιδιόρθωση της λειτουργίας σε περίπτωση προβλήματος. Η απώλεια ακεραιότητας μπορεί να γίνει είτε στο λογισμικό είτε στη βάση δεδομένων του συστήματος. Αυτό συνεπάγεται με τη μη σωστή λειτουργία και την προστασία των πληροφοριών του συστήματος, το μη γρήγορο εντοπισμό σφαλμάτων που μπορεί να έχει ως συνέπεια τις λανθασμένες αποφάσεις της διοίκησης. Ακόμα η απώλεια της ακεραιότητας μπορεί να οδηγήσει, στο πρώτο στάδιο, σε μια επιτυχημένη επίθεση κατά της εμπιστευτικότητας και ακεραιότητας των συστημάτων.
- **Η Απώλεια Διαθεσιμότητας (Loss of Availability)**: Σε περίπτωση μη διαθεσιμότητας όλου ή κάποιου τμήματος του συστήματος λόγω κάποιας βλάβης

που παρουσιάστηκε κατά τη διάρκεια της λειτουργίας του,μπορεί να οδηγήσει το έργο εκτός λειτουργίας μέχρι να γίνει επιδιόρθωση. Η απώλεια της διαθεσιμότητας μπορεί να αποτελεί επακόλουθο της απώλειας ακεραιότητας του συστήματος. Επομένως, όπως είναι γνωστό, μπορεί να φέρει μια σειρά από αρνητικά αποτελέσματα όπως τη μείωση της αξιοπιστίας και κύρους του οργανισμού ακόμα και την αποδιοργάνωση των διαδικασιών αυτών.

- **Η Απώλεια Εμπιστευτικότητας (Loss of Confidentiality)**: Η απώλεια εμπιστευτικότητας μπορεί να πραγματοποιηθεί με την παράνομη κοινοποίηση δεδομένων ή πληροφοριών του οργανισμού. Οι επιπτώσεις σε τέτοια περίπτωση μπορεί να είναι η διαρροή μελλοντικών σχεδίων του οργανισμού, προσωπικά δεδομένα στελεχών ή άλλα στοιχεία που υπάρχουν στη βάση δεδομένων του συστήματος. Εκτός αυτών η παράνομη κοινοποίηση τέτοιων πληροφοριών θα μπορούσε να έχει αντίκτυπο της απώλειας της δημόσιας εμπιστοσύνης ακόμα και τη νομική δράση εναντίον του οργανισμού για την κοινοποίηση αυτή.[1,11]

Πίνακας Έκθεσης Κινδύνων

Ο παρακάτω πίνακας προσδιορίζει τον υπολογισμό της έκθεσης των κινδύνων. Η έκθεση υπολογίζεται από το γινόμενο: Πιθανότητα Εμφάνισης * Συνέπεια Εμφάνισης.

Έκθεση του κινδύνου σε Έργο (Ποσοστά)					
Πιθανότητα					
0,9 Πολύ Υψηλή (Very High)	0,05	0,09	0,18	0,36	0,72
0,7 Υψηλή (High)	0,04	0,07	0,14	0,28	0,56
0,5 Μέτρια (Moderate)	0,03	0,05	0,10	0,20	0,40
0,3 Χαμηλή (Low)	0,02	0,03	0,06	0,12	0,24
0,1 Πολύ Χαμηλή (Very Low)	0,01	0,01	0,02	0,04	0,08
	0,05 Πολύ Χαμηλή (Very Low)	0,10 Χαμηλή (Low)	0,20 Μέτρια (Moderate)	0,40 Υψηλή (High)	0,80 Πολύ Υψηλή (Very High)
Συνέπεια					
Κίνδυνος Αποδεκτός	Κίνδυνος Μη Επιθυμητός		Κίνδυνος Μη Αποδεκτός		

Πίνακας 2 - Πίνακας Έκθεσης Κινδύνων

Με βάση τον παραπάνω πίνακα το επίπεδο έκθεσης σε κίνδυνο μπορεί να αξιολογηθεί ως Πολύ Υψηλή **(Very High)**, Υψηλή **(High)**, Μέτρια **(Moderate)**, Χαμηλή **(Low)**, Πολύ Χαμηλή **(Very Low)**. Με την αξιολόγηση σε Υψηλό Επίπεδο υπάρχει άμεση ανάγκη για λήψη μέτρων ώστε να αποφευχθεί η ακύρωση της υλοποίησης του έργου. Όσα μέτρα είναι κρίσιμα και απαραίτητα πρέπει να εφαρμόζονται και να υλοποιούνται από τα πρώτα στάδια.

Η Ποσοτική Αξιολόγηση

Η ποσοτική αξιολόγηση των κινδύνων είναι περισσότερο επιστημονική μέθοδος σε αντίθεση με την ποιοτική αξιολόγηση η οποία αφορά τους κινδύνους που βρίσκονται στο υψηλό επίπεδο. Έχει ως στόχο τη μαθηματική παρουσίαση της πιθανότητας να εμφανιστεί κίνδυνος καθώς και των επιπτώσεων του κατά τη διάρκεια της υλοποίησης του έργου. Για να πραγματοποιηθεί μια ποσοτική αξιολόγηση υπάρχουν πολλές τεχνικές που πρέπει να εφαρμοστούν:

- **Τα Δένδρα Σφαλμάτων (Fault Tree)**: Τα δένδρα σφαλμάτων αποτελούν γραφική αναπαράσταση των ανεπιθύμητων γεγονότων που μπορεί να προκύψουν στο σύστημα. Οι υποχρεωτικές ενέργειες που πρέπει να γίνουν είναι ο προσδιορισμός του κινδύνου, η αξιολόγηση των βλαβών που προκλήθηκαν, η εικονική έκθεση του συστήματος και η ποσοτική ανάλυση. Ο σημαντικότερος λόγος για την κατασκευή των δένδρων σφαλμάτων δεν είναι μόνο να καθοριστούν οι αιτίες που οδηγούν σε κάποιο κίνδυνο, αλλά ο καθορισμός της πιθανότητας εμφάνισης του κινδύνου σύμφωνα με τις πιθανότητες των αιτιών του. Το σημαντικότερο πλεόνασμα στην τεχνική αυτή είναι η καταγραφή όλων των μικρών κινδύνων ώστε να υπάρχει η καλύτερη αντιμετώπιση συνολικής απειλής.
- **Τα Δένδρα Γεγονότων (Tree Events)**: Τα δένδρα γεγονότων εκθέτουν τα επιθυμητά αποτελέσματα ή μη ενός αρχικού συμβάντος. Ο στόχος τους είναι να προσδιορίσουν την αιτία καθώς και τα αλλεπάλληλα αποτελέσματα που μπορεί να φέρει. Εξαιτίας όμως των διαστάσεων που μπορεί να έχει ένα δένδρο γεγονότων, απαιτείται ανάλογο λογισμικό για την ανάπτυξή του. Κάποια άλλη μορφή των δένδρων γεγονότων είναι τα δένδρα αποφάσεων τα οποία είναι διαγράμματα που εκθέτουν και αυτά ένα τρόπο λήψης αποφάσεων έχοντας όλες τι διαθέσιμες επιλογές υπόψη.
- **Η Ανάλυση Ευαισθησίας (Sensitivity Analysis)**: Η τεχνική αυτή καθορίζει ποιοι κίνδυνοι έχουν τις πιο αρνητικές επιπτώσεις στη λειτουργία του έργου και κατά πόσο είναι επικίνδυνες αυτές, έτσι ώστε ο οργανισμός να δίνει περισσότερο βάση στους κινδύνους που μπορεί να προκαλέσουν σοβαρές και περισσότερες απώλειες στον οργανισμό. Τα διαγράμματα ευαισθησίας που μπορούν να χρησιμοποιηθούν είναι δύο, της αράχνης και το Tornado. Και τα δύο αυτά διαγράμματα ενισχύουν τη διαδικασία και τη διαχείριση της ανάλυσης κινδύνων και εκθέτουν εκείνες τις μεταβλητές που είναι σημαντικές έτσι ώστε να βοηθήσουν τα στελέχη του οργανισμού σε πιθανή επίπτωση μιας λάθος εκτίμησης.
- **Η Προσομοίωση Monte Carlo (Monte Carlo Simulation)**: Περιλαμβάνει κυρίως στοχαστικές διαδικασίες, εκείνες δηλαδή που βασίζονται στη χρήση των τυχαίων αριθμών και της στατιστικής για τη λύση προβλημάτων. Η τεχνική αυτή παίρνει τις τιμές της μέσα από μια κλίμακα όπου ο κάθε αριθμός της έχει ίση πιθανότητα να εμφανιστεί. Για να μπορεί να φέρει αξιόπιστα αποτελέσματα θα πρέπει να ξαναγίνει πολλές φορές. Όσες περισσότερες επαναλήψεις έχουμε τόσο περισσότερες πιθανές λύσεις θα προκύψουν.
- **Η Τεχνική Pert (Technical Pert)**: Η τεχνική Pert είναι μια τεχνική ελέγχου προγράμματος και αξιολόγησης βασισμένη στη θεωρία των πιθανοτήτων για μια πρακτική αξιολόγηση μεγάλης διάρκειας έργων. Για την πραγματοποίησή της επιβάλλεται η δημιουργία διαγραμμάτων με κατανομή Βήτα ή Τριγωνική που θα πρέπει να είναι ίδια για όλες τις δραστηριότητες. Επομένως βασισμένα σε αυτά υπολογίζεται η αισιόδοξη, η πιθανή, η διχοτόμος, η μέση και η απαισιόδοξη τιμή για τη διάρκεια του έργου, για να βρεθεί το κρίσιμο μονοπάτι, η διαδρομή που θα πρέπει να ακολουθήσει κάθε οργανισμός για να διαφύγει τυχόν καθυστερήσεις στην υλοποίηση των δραστηριοτήτων της.

- **Η Αναμενόμενη Τιμή (Expected Value)**: Η αναμενόμενη τιμή είναι συνδεδεμένη με την πρόγνωση αποτελεσμάτων επειδή δείχνει τα γεγονότα που μπορούν να γίνουν σε ένα έργο επηρεάζοντάς το λίγο ή και περισσότερο στην ανάπτυξή του. Ο όρος αυτός για να έχει την απαιτούμενη βαρύτητα είναι υποχρεωτικό να έχουμε μια συνολική έκθεση των κινδύνων ενός έργου. Άρα προκύπτει:

$$E\sigma = \sum_{j=1}^{n} (\Pi j * \Sigma j)$$

Όπου το Εσ προσδιορίζει το σύνολο των κινδύνων.

Το Πj προσδιορίζει το σύνολο της πιθανότητας εμφάνισης j κινδύνων.

Το Σj προσδιορίζει τις οικονομικές απώλειες που θα έχει η εμφάνιση j κινδύνων.

Εδώ χρειάζεται να τονιστεί ότι οι οικονομικές συνέπειες προσθέτονται στο συνολικό άθροισμα όταν κάνουμε λόγο για απειλές, ενώ αφαιρούνται όταν μιλάμε για ευκαιρίες εφόσον πρόκειται για κέρδος. Η τεχνική αυτή εφαρμόζεται ανάλογα με τους στόχους του κάθε οργανισμού.

Τα Πλεονεκτήματα και Μειονεκτήματα Ποσοτικής και Ποιοτικής Αξιολόγησης

Στη διάρκεια της εκτίμησης των κινδύνων πρέπει να λαμβάνουμε υπόψη τα μειονεκτήματα και τα πλεονεκτήματα της ποσοτικής αξιολόγησης ως προς την ποιοτική αξιολόγηση. Το μειονέκτημα της ποιοτικής ανάλυσης είναι ότι δεν υπάρχουν κάποια ορισμένα μεγέθη υπολογίσιμα για να εκτιμηθεί το μέγεθος των επιπτώσεων, με συνέπεια η ανάλυση κέρδους-κόστους για προτεινόμενες δράσεις είναι πολύ δύσκολη. Το σημαντικότερο πλεονέκτημα όμως της ποιοτικής αξιολόγησης είναι ότι βάζει προτεραιότητες μεταξύ των κινδύνων καθώς και να εντοπίζει τα τμήματα του έργου που χρειάζονται γρήγορη βελτίωση, προσδιορίζοντας τις ευαίσθητες περιοχές αυτού.

Σε αντίθεση στην ποσοτική ανάλυση το μειονέκτημα είναι ότι τα αριθμητικά αποτελέσματα υπάρχει περίπτωση να μην καταλήγουν σε λογικά και ξεκάθαρα συμπεράσματα και έτσι να απαιτείται επιπλέον ποιοτική ανάλυση των αποτελεσμάτων αυτών. Το πλεονέκτημα της ποσοτικής ανάλυσης είναι ότι προσφέρει τέτοιες πληροφορίες, διευκολύνοντας τις αναλύσεις κέρδους-κόστους παρέχοντας συγκεκριμένες τιμές για την δράση μας. Στο σημείο αυτό πρέπει να τονιστεί ότι στην ποσοτική αξιολόγηση το επίπεδο της πολυπλοκότητας και του κόστους είναι υψηλότερα από αυτά της ποιοτικής αξιολόγησης.

Ανακεφαλαιώνοντας, η ποιοτική ανάλυση στηρίζεται στην εμπειρία και τη λογική καθώς και στις δυνατότητες των ατόμων που τις παρουσιάζουν, ενώ η ποσοτική ανάλυση στηρίζεται στα αριθμητικά αποτελέσματα καθώς και στην αξιοπιστία των τεχνικών και μοντέλων που χρησιμοποιούνται. Όταν παρουσιάζεται θέμα κόστους χρησιμοποιείται η ποσοτική αξιολόγηση για να βγουν συμπεράσματα, αλλά όταν το κόστος δεν θεωρείται σημαντικός παράγοντας παρουσιάζονται και οι δύο τρόποι για να βγουν πιο ορθότερα και ασφαλέστερα συμπεράσματα.

Επομένως για την πλήρη αξιολόγηση των κινδύνων είτε μιλάμε για ποσοτική είτε για ποιοτική, είναι απαραίτητο να ληφθεί υπόψη και ο παράγοντας της συνεχής εμφάνισης ενός κινδύνου στα πλαίσια μια συγκριμένης χρονικής περιόδου έχοντας υπόψη και τις επιπτώσεις που έχει σε κάθε εμφάνισή του.[11]

Οι Συστάσεις Ελέγχου

Στη διάρκεια αυτού του βήματος χορηγούνται στοιχεία ελέγχου που έχουν τη δυνατότητα να μετριάσουν ή να απαλείψουν όλους τους κινδυνους που εμφανίζονται. Ο σκοπός των ελέγχων αυτών είναι να μειωθεί το επίπεδο των κινδύνων σε ένα πληροφοριακό σύστημα σε αποδεκτό επίπεδο. Οι παρακάτω παράγοντες πρέπει να λαμβάνονται υπόψη για τη μείωση ή την απαλοιφή των εντοπισμένων κινδύνων:

- Οι Κανονιστικές και οι Νομοθετικές Διατάξεις.
- Η Πολιτική Οργάνωσης.
- Η Αποτελεσματικότητα των Επιλογών που Προτάθηκαν.
- Οι Επιχειρησιακές Επιπτώσεις.
- Η Ασφάλεια και η Αξιοπιστία.

Οι συστάσεις ελέγχων προέρχονται από τη διαδικασία της αξιολόγησης των κινδύνων και εδώ πρέπει να σημειωθεί ότι όλοι οι πιθανοί έλεγχοι μπορούν να βοηθήσουν στην μείωση των απειλών του συστήματος. Για να αξιολογηθεί μια τεχνική πρέπει πρώτα να διεξαχθεί μια ανάλυση οφέλους – κόστους έτσι ώστε να καταδείξει ότι το κόστος της εφαρμογής μπορεί να δικαιολογείσει τη μείωση του επιπέδου του κινδύνου. Τέλος είναι απαραίτητο να αξιολογούνται οι συνέπειες που θα προκύψουν από τον έλεγχο στον οργανισμό.

Η Σύνταξη Αναφοράς

Το τελευταίο στάδιο της διαδικασίας της εκτίμησης των κινδύνων είναι η διατύπωση της τελικής αναφοράς των αποτελεσμάτων της. Η συγγραφή της αναφοράς αυτής πρέπει να γίνει με προσεκτικότητα καθώς αποτελεί βασικό εργαλείο για την προστασία των απειλών που υφίσταται κάθε πληροφοριακό έργο. Στην αναφορά αυτή προσδιορίζονται όλοι οι πιθανότεροι κίνδυνοι που απειλούν το έργο, η πιθανότητα εμφάνισης καθώς και οι συνέπειες από αυτούς.

Για να είναι μια αναφορά πλήρης πρέπει εκτός από τα παραπάνω να συμπεριλαμβάνει και τα εξής:

- Οι πηγές από τις οποίες προήρθαν οι πληροφορίες.
- Τα άτομα που συμμετείχαν στη διαδικασία αυτή.
- Τις τεχνικές που χρησιμοποιήθηκαν για τη διεξαγωγή αποτελεσμάτων.
- Οι παρατηρήσεις και τα σχόλια που διατυπώθηκαν σε κάθε βήμα της διαδικασίας από τους ειδικούς.
- Η τεκμηρίωση των τεχνικών συμπερασμάτων και των πηγών που χρησιμοποιήθηκαν.

Πρέπει να διασαφηνιστεί ότι τα παραπάνω βήματα της διαδικασίας των κινδύνων πρέπει να πραγματοποιούνται και να επαναλαμβάνονται σε όλη τη διάρκεια της υλοποίησης του έργου, για να υπολογίζονται οι αλλαγές των συνθηκών έτσι ώστε να υπολογίζονται πάλι οι εντοπισμένοι και αναγνωρισμένοι κίνδυνοι και να προσθέτονται και νέοι κίνδυνοι αν αυτό είναι και εκτιμηθεί αναγκαίο.

Κεφάλαιο 5-Ασφάλεια Πληροφοριακών Συστημάτων

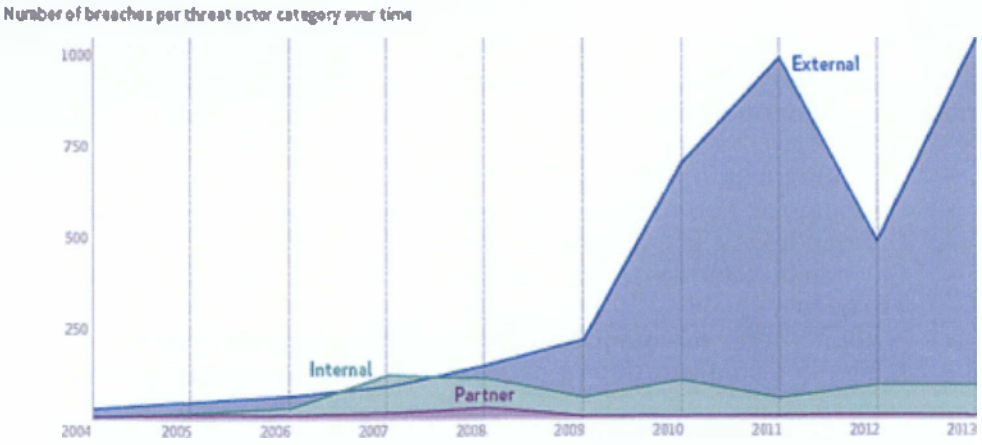
Εισαγωγή

Στην εποχή μας, οι ανέσεις που διαθέτει το Internet, η μεγάλη ροή πληροφοριών και δεδομένων, καθώς και το ηλεκτρονικό εμπόριο, έχουν οδηγήσει μεγάλους ή μικρούς οργανισμούς να επενδύσουν στη χρήση των πληροφοριακών συστημάτων και των διαδικτυακών εφαρμογών αυτών. Όπως είπαμε και στην αρχή η λειτουργικότητα και η αξιοπιστία των οργανισμών βασίζεται στη λειτουργία των πληροφοριακών συστημάτων και η ασφαλής και σωστή λειτουργία τους αποτελεί σημαντικό παράγοντα για την επίτευξη των στόχων τους. Σε περίπτωση δυσλειτουργίας, διακοπής ακόμα και της παράνομης εισχώρησης στα πληροφοριακά συστήματα ισοδυναμεί σε κόστος. Όμως η παραβίαση σε πληροφοριακά συστήματα που περιέχουν ευαίσθητα προσωπικά στοιχεία οι συνέπειες δεν είναι μόνο οικονομικές αλλά παίζουν καθοριστικό ρόλο και για τη λειτουργία του οργανισμού.

Καθώς η χρήση των πληροφοριακών συστημάτων είναι σίγουρη για κάθε οργανισμό, η ασφάλειά τους φαίνεται να απειλείται όλο και περισσότερο. Σύμφωνα με τις έρευνες Παραβίασης Δεδομένων (2014,DBIR.Data Breach Investigations Report)[1],η οποία περιλαμβάνει τις παραβιάσεις από το 2004-2012, και τα 1.361 γεγονότα τα οποία ο συμβιβασμός των στοιχείων επιβεβαιώθηκε το 2013.

Το έτος του 2013 σύμφωνα με την Verizon, της γνωστής παγκόσμιας εταιρίας τηλεπικοινωνιών, μπορεί να θεωρηθεί ως «έτος της παραβίασης λιανοπωλητών,» αλλά μια γενική αξιολόγηση προτείνει ότι ήταν ένα έτος μετάβασης από τις γεωπολιτικές επιθέσεις στης μεγάλης κλίμακας επιθέσεις στα συστήματα καρτών πληρωμής.[2]

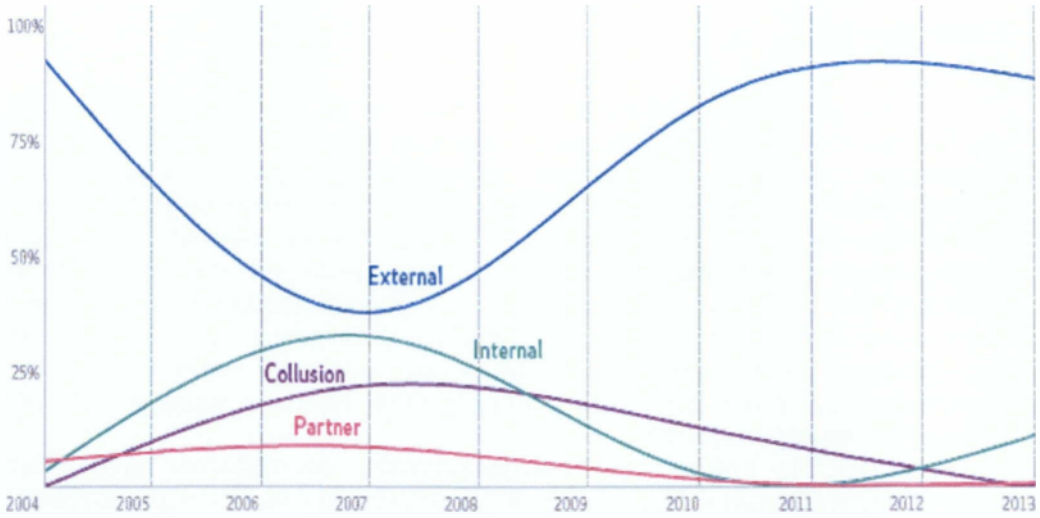
Σύμφωνα με την έρευνα: **Η παρακάτω εικόνα** μας προσδιορίζει την αριθμητική καταμέτρηση των παραβιάσεων των Π. Σ σε εσωτερικούς, εξωτερικούς παράγοντες καθώς και τους συνεργάτες του φορέα.



Εικόνα 9 - Παραβίασης Πληροφοριακών Συστημάτων από 2004-2013

[1,2] Στοιχεία Έρευνας (2014,DBIR) Data Breach Investigations Report - Verizon, http://www.verizonenterprise.com/DBIR/

Η **εικόνα 10** μας προσδιορίζει το ποσοστό του συνόλου των παραβιάσεων. Χρησιμοποιεί μια γραμμή του τρίτου βαθμού πολυώνυμο τάσης για να είναι ωραία και ομαλή, έτσι μπορεί να φανεί η βασική συμπεριφορά με την πάροδο του χρόνου.

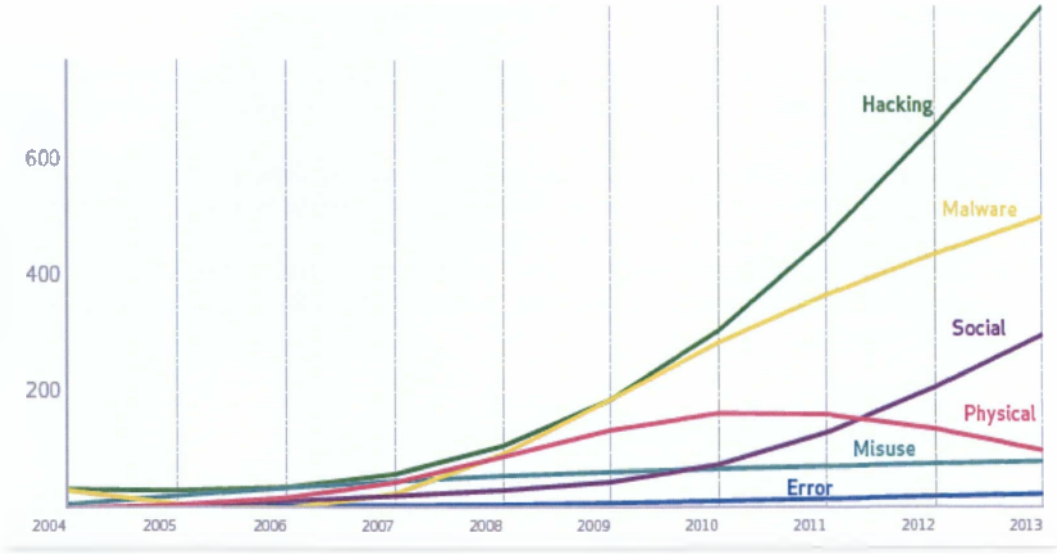


Εικόνα 10 - Ποσοστό Παραβίασης Πληροφοριακών Συστημάτων από 2004-2013

Όσον αφορά τους εσωτερικούς παράγοντες αυτοί προέρχονται από εσωτερικές απειλές (Internal Threats) του οργανισμού. Αυτό συμπεριλαμβάνει όλους τους εργαζόμενους, τα στελέχη και τις εσωτερικές υποδομές επίσης. Οι εξωτερικοί παράγοντες προέρχονται από τις εξωτερικές απειλές όπως από τις πηγές εκτός του οργανισμού και από το δίκτυο των συνεργατών. Για παράδειγμα τα άτομα τα οποία μπορεί να είναι Hackers, πρώην εργαζόμενοι των φορέων ή και ακόμα εγκληματικές ομάδες. Εκτός αυτών υπάρχει και μια άλλη κατηγορία παραγόντων που έχει σχέση με τους συνεργάτες καθώς και τρίτα πρόσωπα που έχουν και μοιράζονται κάποια επιχειρησιακή σχέση με τον οργανισμό. Τα τρίτα πρόσωπα μπορεί να είναι πωλητές, προμηθευτές, υπηρεσίες υποστήριξης πληροφορικής κ.τ.λ. Εκτός των άλλων παραγόντων το ποσοστό των εξωτερικών παραγόντων υπερέχει κατά πολύ. Στους εξωτερικούς παράγοντες μπορούν τοποθετούνται οι παρακάτω απειλές:

- Οι επιθέσεις από Hackers **(Hacking).**
- Παραβιάσεις που προέρχονται από τη χρήση κακόβουλων λογισμικών **(Malware).**
- Οι παραβιάσεις κοινωνικού περιεχομένου **(Social).**
- Οι περιβαλλοντικές και φυσικές απειλές **(Environmental and Physical Threats).**
- Η κακή χρήση των πληροφοριακών συστημάτων **(Misuse).**
- Διάφορα σφάλματα που προκύπτουν στα πληροφορικά συστήματα **(Error).**

Στατιστικές μελέτες έδειξαν ότι την τελευταία δεκαετία 2004-2013 το μεγαλύτερο ποσοστό παραβιάσεων οφείλεται σε εξωτερικούς παράγοντες που προέρχονται από επιθέσεις κακόβουλες **(Hackers)** και από μεγάλο ποσοστό στη χρήση κακόβουλων λογισμικών **(Malware).**



Εικόνα 11 - Αποτελέσματα Έρευνας (2014,DBIR.Data Breach Investigations Report).

Επομένως οι κάθε είδους παραβιάσεις και επιθέσεις κατά των πληροφοριακών συστημάτων των οργανισμών οδηγούν στην απώλεια εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας των πληροφοριών και των δεδομένων που διαχειρίζονται καθώς και την παράβαση ολόκληρων των συστημάτων αυτών. Αυτό μπορεί να είναι και το σοβαρότερο πρόβλημα καθώς μπορεί να απειληθούν ζωές ανθρώπων αλλά και η ασφάλεια τόσο σε τοπικό, εθνικό και παγκόσμιο επίπεδο. Έτσι η ασφάλεια στα πληροφοριακά συστήματα αποτελεί σημαντικό παράγοντα στη σύγχρονη κοινωνία, που στηρίζεται σε αυτά, γι' αυτό και θα πρέπει να λαμβάνεται υπόψη από τα άτομα που ασχολούνται με τη σχεδίαση, υλοποίηση και τη χρήση τους.

Ορισμός Ασφάλειας Πληροφοριακού Συστήματος

Όπως είναι γνωστό τα 5 συστατικά στοιχεία από τα οποία αποτελείται το πληροφοριακό σύστημα είναι οι άνθρωποι, οι διαδικασίες, τα δεδομένα, το υλικό, και το λογισμικό. Με τον όρο ασφάλεια πληροφοριακών συστημάτων **(Information Systems Security)** δίνεται έμφαση στην προστασία αυτών των στοιχείων ενός πληροφοριακού συστήματος και στο σύνολό του. Ως προς τον ορισμό είναι γεγονός ότι στη διεθνή επιστημονική βιβλιογραφία δεν υπάρχει ένας ορισμός της ασφάλειας των πληροφοριακών συστημάτων που να συμφωνούν όλοι. Ένας ορισμός που προσδιορίζει την έννοια της ασφάλειας είναι ο παρακάτω:

«**Ασφάλεια Πληροφοριακού Συστήματος είναι** το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του Πληροφοριακού Συστήματος, αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή»[3].

Ο παραπάνω ορισμός μας δίνει το πλεονέκτημα για την άμεση αναφορά στα παρακάτω βασικά στοιχεία:

- Επισήμανση όχι μόνο στο Πληροφοριακό Σύστημα ως σύνολο αλλά και στα επιμέρους στοιχεία του.
- Η προστασία σχετίζεται με κάθε είδους απειλής (τυχαία ή σκόπιμη).
- Η ασφάλεια του Πληροφοριακού Συστήματος σχετίζεται άμεσα με τις τεχνικές, διαδικασίες, τα διοικητικά μέτρα όσο και με τις αντιλήψεις, αρχές και παραδοχές.
- Το πλαίσιο αυτό χαρακτηρίζεται από οργάνωση.

[3] Ευάγγελος Κιουντούζης: Μεθοδολογίες Ανάλυσης & Σχεδιασμού Πληροφοριακών Συστημάτων, Εκδόσεις Ε. Μπένου, Γ΄ Έκδοση (2009).

Η ασφάλεια Πληροφοριακών Συστημάτων σχετίζεται με:

- **Πρόληψη (Prevention)**: Τη λήψη μέτρων για την αποτροπή πραγματικής ή πιθανής απειλής που μπορεί να προκαλέσει φθορές στα συστατικά μέρη ενός πληροφοριακού συστήματος.
- **Ανίχνευση (Detection)**:Η ανίχνευση είναι η λήψη μέτρων για την εμφάνιση ενός περιστατικού ή μιας παραβίασης που προκάλεσε φθορές σε κάποιο συστατικό μέρος του πληροφοριακού συστήματος.
- **Αντίδραση (Reaction)**: Την υιοθέτηση κατάλληλων ενεργειών για την αποκατάσταση ή την ανάκτηση των συστατικών μερών ενός πληροφοριακού συστήματος.

Η Ασφάλεια ως Απαίτηση των Δικαιούχων

Στα Πληροφοριακά Συστήματα η ύπαρξη μέτρων εκτιμάται από πολλούς ότι έχουν άμεσο συμφέρον μόνο οι σχεδιαστές και οι ιδιοκτήτες. Όμως με το πέρασμα των χρόνων τα πληροφοριακά συστήματα παίζουν σημαντικό ρόλο μέσα στον οργανισμό καθώς και το δικαίωμα της απαίτησης στην ασφάλεια του Πληροφοριακού Συστήματος. Επομένως αυτοί που έχουν το δικαίωμα της απαίτησης να υπάρχουν μέτρα ασφαλείας και μηχανισμοί είναι οι εξής:

- **Η Διοίκηση του Οργανισμού**: Λόγω του ρόλου του πληροφοριακού συστήματος και της σπουδαιότητας των πληροφοριακών πόρων, σε σχέση με τις οικονομικές δαπάνες που πραγματοποιούντε για την απρόσκοπτη λειτουργία του συστήματος είναι λογικό η διοίκηση να ενδιαφέρεται για το επίπεδο ασφάλειάς του.
- **Οι Ιδιοκτήτες και οι Διαχειριστές Δεδομένων και Διεργασιών**: Σε περίπτωση μειωμένων μέτρων ασφαλείας κάνουν το σύστημα ευπαθές και ευπρόσβλητο σε κάθε είδους φύσεως απειλές από τρίτους.
- **Οι Υπεύθυνοι της Λειτουργίας και της Ανάπτυξης του Πληροφοριακού Συστήματος**: Στην κατηγορία αυτή ανήκουν τα άτομα που ασχολούνται με την ορθή λειτουργία του τεχνολογικού και υπολογιστικού εξοπλισμού.
- **Οι Καταναλωτές των Τελικών Προϊόντων και Υπηρεσιών**: Στην κατηγορία αυτή ανήκουν οι πολίτες ή τα απλά άτομα που χρησιμοποιούν το πληροφοριακό σύστημα για την πραγματοποίηση μιας ενέργειας του ή την λήψη μιας υπηρεσίας.
- **Η Πολιτεία**: Η πολιτεία έχει τον πρωταρχικό ρόλο για τη διαμόρφωση των μέτρων ασφαλείας με το να θεσπίζει κανόνες και πλαίσια για να τηρούνται οι κανόνες που πρέπει. Επομένως η σοβαρότητα των πιθανών αδικημάτων που μπορεί να διαπραχθούν από τη συλλογή, χρήση, μετάδοση καθώς και την επεξεργασία των πληροφοριών σε σχέση με τον κάθε απλό πολίτη να αντιμετωπίσει την πολυπλοκότητα της νέας τεχνολογίας, οδηγεί την πολιτεία να διορίσει Ανεξάρτητες Διοικητικές Αρχές (π.χ Επιτροπή Τηλεπικοινωνιών, Αρχή Προστασίας Δεδομένων),με σκοπό τον έλεγχο των πληροφοριακών συστημάτων.

Σε περίπτωση αποτυχίας της αντιμετώπισης μιας επίθεσης σε έναν οργανισμό, πέρα από την απώλεια ευαίσθητων ιδιωτικών ή δημόσιων δεδομένων και πληροφοριών από τα αρχεία του, θα έχει επιπτώσεις τόσο στη δημόσια εικόνα του καθώς και στην αξιοπιστία του.
Είναι εμφανές ότι σε όλο το ζήτημα εμπλέκονται πολλοί παράγοντες καθώς και πολλοί ενδιαφερόμενοι. Όπως είπαμε και παραπάνω η διοίκηση είναι φυσικό να δίνει μεγάλη σημασία στις οικονομικές δαπάνες και στην περίπτωση του πιθανού αυτοσχεδιασμού δραστηριοτήτων που συνεπάγεται η εφαρμογή των μέτρων ασφαλείας. Από την άλλη μεριά η πολιτεία και οι τελικοί χρήστες δίνουν σημασία στην τελειότητα της ικανοποίησης των απαιτήσεων της ασφάλειας, χωρίς να τους ενδιαφέρει το κόστος. Οι υπεύθυνοι της λειτουργίας και οι διαχειριστές των διεργασιών ενδιαφέρονται, για τα μέτρα τα οποία προτείνονται, να ανταποκρίνονται στα χαρακτηριστικά της οργάνωσης και της ιδεολογίας του οργανισμού, έτσι ώστε να μην χρειάζονται πολλές αλλαγές στον τρόπο λειτουργίας και δομής του. Τέλος οι ειδικοί ασφαλείας και οι υπεύθυνοι της ανάπτυξης του πληροφοριακού συστήματος δίνουν σημασία σε μια σειρά από παράγοντες όπως ο ρόλος

του αναλυτή, ο ρόλος του χρήστη, το οντολογικό και επιστημονικό πλαίσιο της κάθε οντολογικής προσέγγισης κ.α.

Οι Επίβουλοι του Συστήματος

Οι επιθέσεις κατά του συστήματος, αν κατηγοριοποιηθούν με βάση το σκοπό τους, δίνουν τις παρακάτω 5 κατηγορίες:

- Εισαγωγή ή μετατροπή δεδομένων χωρίς εξουσιοδότηση ή καταστροφή των δεδομένων και των προγραμμάτων ενός πληροφοριακού συστήματος.
- Αλλοίωση ή μείωση της αξιοπιστίας των δεδομένων ενός πληροφοριακού συστήματος.
- Παρεμπόδιση της ομαλής λειτουργίας του.
- Χωρίς άδεια εισβολή και αφαίρεση στοιχείων του.
- Παραβίαση των αποκλειστικών δικαιωμάτων του δημιουργού, του κατόχου, των δεδομένων, των προγραμμάτων και γενικά του πληροφοριακού υλικού.

Στις προαναφερθείσες κατηγορίες πρέπει να σημειωθεί και η επίθεση από κακόβουλο λογισμικό. Ποιοι είναι αυτοί όμως που απειλούν ένα πληροφοριακό σύστημα; Σε μία πρόσφατη έρευνα που διεξάχθηκε στις ΗΠΑ το 2003 εξακριβώθηκε ότι το 55%των παραβιάσεων έγινε από τους ίδιους τους υπαλλήλους του οργανισμού, το 38% επιθέσεις από Hackers, και το 8% από τους ανταγωνιστές. Σύμφωνα με τις ετήσιες εκθέσεις των τελευταίων χρόνων του Computer Security Institute, CSI/FBI (Computer Crime and Security Survey,2003), δείχνουν ότι η κυριότερη απειλή προέρχεται μέσα από τον οργανισμό. Συνεταίροι, σύμβουλοι και δυσαρεστημένοι υπάλληλοι που θέλουν να διεκδικήσουν την διοίκηση για τις αποφάσεις της καθώς και χρήστες που έχουν λανθασμένη αντίληψη για τα προνόμια και τα δικαιώματά τους, είναι μερικές αιτίες που οδηγούν και προκαλούν αυτού του είδους τις ενέργειες.[4][1]

Οι Ιδιότητες της Ασφάλειας

Για να υλοποιηθεί ο στόχος της ασφάλειας πρέπει να υιοθετηθούν και να εφαρμοστούν τα αντίστοιχα μέτρα ασφαλείας (Safeguards). Χωρίς αυτά τα πληροφοριακά συστήματα είναι ευάλωτα απέναντι σε απειλές.
Η πρόσβαση σε πληροφορίες από μη εξουσιοδοτημένα άτομα καταργεί την εμπιστευτικότητα **(Confidentiality)** των πληροφοριών. Η τροποποίηση των πληροφοριών από μη εξουσιοδοτημένα άτομα έχει ως συνέπεια την καταστροφή της ακεραιότητας **(Integrity)** και τέλος η διαγραφή πληροφοριών και δεδομένων ή κατάργηση άλλων λειτουργιών του πληροφοριακού συστήματος από μη εξουσιοδοτημένα άτομα κάνουν αδύνατη τη διαθεσιμότητα **(Availability)** των πληροφοριών. Οι 3 αυτές έννοιες Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα αποτελούν τις πιο σημαντικές ιδιότητες της πληροφορίας ως αγαθό, όπου η διασφάλισή τους και η προστασία τους αποτελούν πρωταρχικό στόχο για την ασφάλεια των πληροφοριακών συστημάτων. Παρακάτω αναφέρονται οι 3 βασικές ιδιότητες ασφάλειας πιο αναλυτικά:

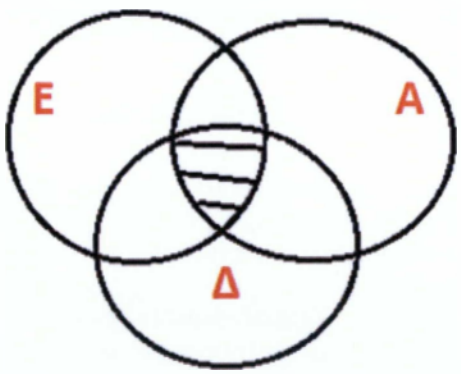
- **Η Εμπιστευτικότητα (Confidentiality)**: Προφυλάσσει την αποκάλυψη ευαίσθητων πληροφοριών από μη εξουσιοδοτημένα άτομα. Τα ευάλωτα στοιχεία των πληροφοριακών συστημάτων (πληροφορίες, υπολογιστικοί πόροι) πρέπει να εμφανίζονται μόνο σε εξουσιοδοτημένα άτομα. Οι μηχανισμοί προστασίας που υπάρχουν πραγματοποιούν τους αναγκαίους ελέγχους, για να ελαττώσουν την πρόσβαση στα στοιχεία αυτά. Η εμπιστευτικότητα επιτυγχάνεται με την κρυπτογράφηση των δεδομένων η οποία κάνει τα δεδομένα μη αναγνώσιμα καθώς

[4] Ευάγγελος Κιουντούζης: Μεθοδολογίες Ανάλυσης & Σχεδιασμού Πληροφοριακών Συστημάτων, Εκδόσεις Ε. Μπένου, Γ΄ Έκδοση (2009).

και με έλεγχο πρόσβασης στα δεδομένα. Άλλες μορφές της εμπιστευτικότητας είναι οι εξής:

- ✓ Η μυστικότητα **(Secrecy)**: Είναι η προστασία των δεδομένων που έχουν μορφή προσωπικού χαρακτήρα (αφορούν συγκεκριμένα άτομα).
- ✓ Η ιδιωτικότητα **(Privacy)**: Είναι η προστασία των δεδομένων σε ένα οργανισμό

- **Η Ακεραιότητα (Integrity)**: Είναι η διασφάλιση της ακρίβειας, της πληρότητας καθώς και των μεθόδων επεξεργασίας του πληροφοριακού συστήματος. Στόχος της ακεραιότητας είναι η κάθε αλλαγή και τροποποίηση στο πληροφοριακό σύστημα (π.χ τιμές πληροφοριών) να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας ενώ σε περίπτωση μη εξουσιοδοτημένης αλλαγής να μη γίνεται επιτρεπτή. Η ακεραιότητα επιτυγχάνεται με τις ψηφιακές υπογραφές, με τη χρήση των μηχανισμών αυθεντικοποίησης καθώς και με τον έλεγχο πρόσβασης.
- **Η Διαθεσιμότητα (Availability)**: Είναι η ιδιότητα που κάνει αδιάλειπτη και απρόσκοπτη την πρόσβαση των εξουσιοδοτημένων χρηστών όταν τη χρειάζονται έτσι ώστε να μην υπάρχουν προβλήματα αδικαιολόγητης καθυστέρησης ή να μην είναι προσπελάσιμες οι υπηρεσίες ενός πληροφοριακού συστήματος. Στόχος της διαθεσιμότητας είναι:
  - ✓ Η έγκαιρη ανταπόκριση της διάθεσης των δεδομένων.
  - ✓ Η δίκαιη κατανομή τω πόρων.
  - ✓ Η δυνατότητα χρησιμοποίησης των πόρων και των δεδομένων όπως σχεδιάστηκαν.
  - ✓ Ο κατάλληλος χρόνος διάθεσης πόρων.
  - ✓ Η ικανότητα χειρισμού των απαραίτητων πόρων.



Εικόνα 12 - Σχέση μεταξύ Εμπιστευτικότητας, Ακεραιότητας, Διαθεσιμότητας

Σε πολλές ερευνητικές εργασίες έχει διαπιστωθεί πως οι παραπάνω 3 ιδιότητες δεν είναι αρκετές για να προσδιοριστεί η έννοια της ασφάλεια των πληροφοριών. Επιπρόσθετες ιδιότητες που συναντώνται είναι οι εξής:

- **Η Ταυτοποίηση (Identification)**: Είναι η διαδικασία κατά την οποία μία οντότητα (π.χ άνθρωπος , υπολογιστής) αναγνωρίζει μια άλλη οντότητα.
- **Η Αυθεντικοποίηση ή Πιστοποίηση ταυτότητας(Authentication)**: Είναι η διαδικασία κατά την οποία μια οντότητα επιβεβαιώνει την ταυτότητα μιας άλλης οντότητας. Η διαδικασία αυτή χωρίζεται σε αυθεντικοποίηση μηνύματος και αυθεντικοποίηση της οντότητας.
- **Η Εξουσιοδότηση (Authorization)**: Η παροχή σε ένα υποκείμενο το δικαίωμα πρόσβασης σε ένα αντικείμενο. Η παροχή αυτή γίνεται και τυπικά μετά την ταυτοποίηση και αυθεντικοποίηση του υποκειμένου.
- **Η Απονομή ευθυνών (Accountability)**: Αποδεικνύει ότι μια οντότητα πρέπει να έχει αναγνωριστή και να είναι υπεύθυνη των πράξεων της.

- **Η Μη αποποίηση (Non-repudiation)**: Είναι η διαθεσιμότητα των αδιάψευστων αποδείξεων που μπορούν να χρησιμοποιηθούν σε μια διαφωνία.

Οι διαφορετικές απόψεις που υπάρχουν για τις ιδιότητες της ασφάλειας δεν πρέπει να θεωρηθούν παράδοξες επειδή στον ευρύ τομέα της πληροφορικής η ασφάλεια αποτελεί μια αφηρημένη έννοια, οι οποία δέχεται διάφορες ερμηνείες. Επομένως η έννοια της ασφάλειας προσδιορίζεται σε ποικίλες ιδιότητες της πληροφορίας, με βάση το πώς το βλέπει ο ερευνητής και ως προς το πληροφοριακό σύστημα που αναφέρεται. Οι προαναφερθείσες ιδιότητες ασφαλείας των πληροφοριών δεν μπορούν μετρηθούν σε απόλυτα μεγέθη. Παρά το γεγονός ότι οι ορισμοί για τις 3 βασικές κατηγορίες που παρέχονται με απλότητα και σαφήνεια, δεν είναι πάντα εύκολο να προσδιορίσουμε ποιες από αυτές έχουν παραβιαστεί. Για παράδειγμα σε περίπτωση παραβίασης διαθεσιμότητας με τη μη διάθεση της πληροφορίας μπορεί να αξιολογηθεί με ποικίλους τρόπους σε διαφορετικές περιπτώσεις, διότι ο χρόνος αναμονής διαφέρει από εφαρμογή σε εφαρμογή. Επομένως μια καθυστέρηση μιας συγκεκριμένης χρονικής περιόδου 5 λεπτών για την εξαγωγή μια σημαντικής ιατρικής πληροφορίας μπορεί να θεωρηθεί έλλειψη διαθεσιμότητας αλλά ο ίδιος χρόνος για την αναζήτηση κάποιων στοιχείων για ένα φορολογούμενο σε μια δημόσια υπηρεσία μπορεί να θεωρηθεί αποδεκτός.

Η Πολιτική Ασφαλείας

Η πολιτική ασφαλείας σε έναν οργανισμό, ως προς τη λειτουργία των πληροφοριακών συστημάτων, περιλαμβάνει τους κανόνες, τις οδηγίες, τις διαδικασίες, τις αρμοδιότητες και γενικά με ότι έχει σχέση με την ασφάλεια και αφορά την προστασία των πληροφοριακών συστημάτων. Η πολιτική ασφαλείας παρουσιάζεται σε ένα έγγραφο το οποίο υποχρεούνται οι χρήστες των πληροφοριακών συστημάτων να το ξέρουν και να το εφαρμόζουν.

Ένας ρόλος έχει μια δομή και είναι η βάση της πολιτικής ελέγχου προσπέλασης. Ο ρόλος μπορεί να περιλαμβάνει εξουσιοδοτήσεις από αρμοδιότητες και ενέργειες που έχουν σχέση με τη λειτουργία του συστήματος, και παραχωρείται σε χρήστες, δίνοντας τους έτσι την δυνατότητα να εκτελέσουν τις ενέργειες για να λειτουργήσουν στα πλαίσια των αρμοδιοτήτων. Για παράδειγμα στο μοντέλο ελέγχου προσπέλασης RBAC, οι διαχειριστές των συστημάτων αναπτύσσουν ρόλους με βάση τα καθήκοντα και τις θέσεις εργασίας που υπάρχουν σε ένα οργανισμό.

Η πολιτική ασφαλείας εφαρμόζεται για να κατανοήσουμε τα παρακάτω ερωτήματα:

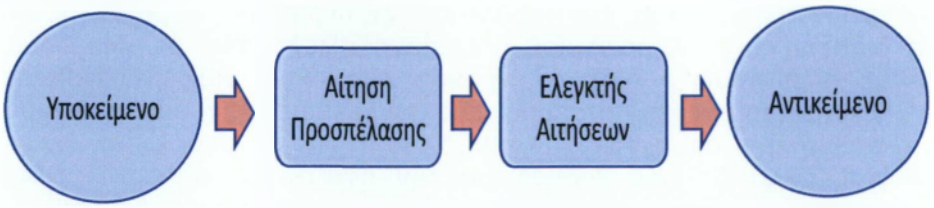
- Ποιος είναι οι στόχοι και ο σκοπός της πολιτικής;
- Ποια είναι τα αγαθά του συστήματος που χρειάζονται προστασία;
- Για την προστασία των αγαθών ποιοι είναι υπεύθυνοι και ποιες αρμοδιότητες έχουν;

Ο Έλεγχος Προσπέλασης

Το πρώτο στάδιο της άμυνας ενός πληροφοριακού συστήματος είναι η αναγνώριση και η επαλήθευση της ταυτότητας των χρηστών. Αυτές οι 2 ενέργειες είναι απαραίτητες και σημαντικές γιατί η ταυτότητα του χρήστη αποτελεί βασικό παράγοντα στις αποφάσεις του ελέγχου προσπέλασης. Το γεγονός όμως ότι κάποιος χρήστης έχει την εξουσιοδότηση να συνδεθεί με ένα πληροφοριακό σύστημα δεν συνεπάγεται ότι έχει και εξουσιοδότηση να κάνει ό,τι θέλει σε αυτό. Από την άλλη μεριά οι μη εξουσιοδοτημένες προσβάσεις χρηστών σε εγκαταστάσεις πληροφοριακού συστήματος επιφέρουν την καταστροφή των αγαθών. Επομένως, είναι σημαντικό να υπάρχει ένας μηχανισμός που να επιβλέπει τη δυνατότητα των χρηστών να κάνουν χρήση των πληροφοριών ή των υπολογιστικών πόρων κάποιου πληροφοριακού συστήματος. Ο μηχανισμός αυτός είναι γνωστός ως μηχανισμός προσπέλασης.

Ο έλεγχος προσπέλασης είναι ένα κοινό μέτρο ασφαλείας ενός πληροφοριακού συστήματος και περιλαμβάνει τα παρακάτω:

- Το μηχανισμό αυθεντικοποίησης του χρήστη.
- Το μηχανισμό της διαχείρισης δικαιωμάτων των χρηστών.
- Το μηχανισμό του ελέγχου και της καταγραφής των ενεργειών.
- Το μηχανισμό λήψης απόφασης της εξουσιοδότησης .
- Το μηχανισμό της επιβολής του ελέγχου εξουσιοδότησης.



Εικόνα 13 - Έλεγχος Προσπέλασης

Οι Πολιτικές Ελέγχου Προσπέλασης

Ο έλεγχος προσπέλασης σύμφωνα με τον OSI **(International Organization for Standardization)** αποτελείται από δύο τμήματα:

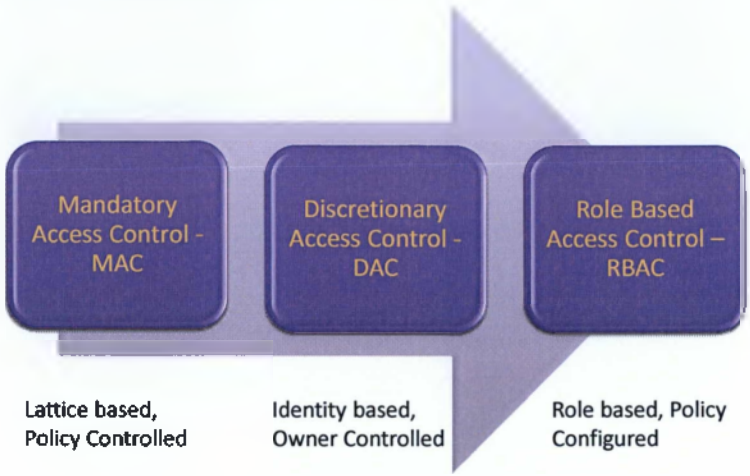
- ✓ ένας μηχανισμός ο οποίος αποφασίζει αν θα δοθεί ή όχι άδεια προσπέλασης υποκειμένων σε αντικείμενα **(Access Control Decision Facility)** με βάση προσδιορισμένους κανόνες
- ✓ και ένας μηχανισμός που ορίζει την απόφαση **(Access Control Enforcement Facility).**

Υπάρχουν διάφορες πολιτικές ελέγχου προσπέλασης που έχουν δημιουργηθεί για να καλύψουν τις απαιτήσεις των διαφορετικών χώρων λειτουργίας των πληροφοριακών συστημάτων. Οι πολιτικές ελέγχου προσπέλασης διακρίνονται σύμφωνα με το βαθμό εμπιστοσύνης και το βαθμό ευαισθησίας της πληροφορίας (Αδιαβάθμητη **(Infinitely)**, Εμπιστευτική **(Confidential)**, Απόρρητη **(Secret)**, Άκρως Απόρρητη **(Top Secret)**.

Εικόνα 14 - Βαθμοί Ευαισθησίας της Πληροφορίας

Οι πιο γνωστές πολιτικές ελέγχου προσπέλασης στο ευρύ κοινό είναι ο Διακριτικός Έλεγχος Προσπέλασης (Discretionary Access Control-DAC), ο Υποχρεωτικός Έλεγχος Προσπέλασης (Mandatory Access Control-MAC), και ο Ρολο-Κεντρικός Έλεγχος Προσπέλασης (Role Based Access Control-RBAC). Είναι σημαντικό να τονιστεί ότι ο υποχρεωτικός έλεγχος προσπέλασης όσο και ο έλεγχος προσπέλασης στηριζόμενος σε

ρόλους θεωρούνται μη διακριτές πολιτικές ελέγχου προσπέλασης, πολιτικές όπου οι κανόνες για την πρόσβαση σε κάποιο αντικείμενο δεν εξαρτώνται από την πρόθεση και τις ενέργειες τους ιδιοκτήτη του αντικειμένου, αλλά προσδιορίζονται από την ολότητα της πολιτικής ασφάλειας του πληροφοριακού συστήματος.[1]



Εικόνα 15 - Πολιτικές Ελέγχου Προσπέλασης

Υποχρεωτικός Έλεγχος Προσπέλασης MAC

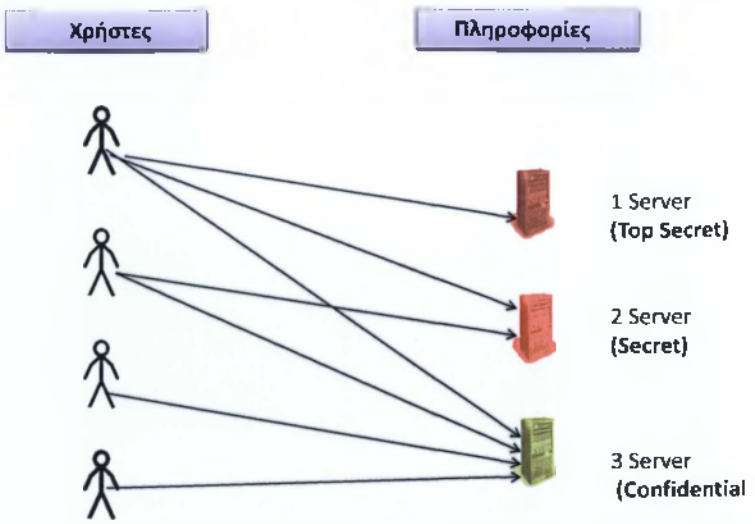
Η Πολιτική Ελέγχου Προσπέλασης–MAC για την ασφάλεια των πληροφοριακών συστημάτων είναι μια συνηθισμένη πολιτική ελέγχου προσπέλασης, μολονότι αναφέρεται περισσότερο σε περιβάλλοντα στρατιωτικά και σε εκείνα που προϋποθέτουν απαιτήσεις υψηλής ασφάλειας.

Η πολιτική ελέγχου MAC υπάγεται στην κατηγορία του ελέγχου πρόσβασης εκείνων των συστημάτων των οποίων υπάρχει μια αυστηρά καθορισμένη ροή των πληροφοριών. Στα συστήματα αυτά η ροή των πληροφοριών διέπεται από μαθηματικά μοντέλα. Με αυτήν την εφαρμογή της τεχνικής αυτής μπορούν να αποφθεχθούν παραβιάσεις που περιέχονται από επιθέσεις του τύπου «Δούρειου Ίππου (Trojan ή Trojan Horse)[5]». Οι τύποι των επιθέσεων αυτών δεν προσπαθούν μόνοι τους την πρόσβασή τους σε άλλα αρχεία, όπως κάνουν άλλοι ιοί σε υπολογιστές. Κατά κανόνα οι Trojans εκτός το ότι παρέχουν στον επιτιθέμενο μη εξουσιοδοτημένη πρόσβαση, έχουν τη δυνατότητα να κάνουν αντίγραφα του εαυτού τους, να βλάψουν τα πληροφοριακά συστήματα, να μολύνουν, ακόμα και να κλέψουν πληροφορίες.

Στην πολιτική ελέγχου MAC, τα δικαιώματα του χρήστη δεν περιστρέφονται γύρω από την έννοια της ιδιοκτησίας. Εδώ η έννοια της ιδιοκτησίας δεν υπάρχει διότι η πολιτική αυτή στηρίζεται στην ευαισθησία της πληροφορίας. Επομένως στην περίπτωση αυτή για να αποκτήσει πρόσβαση ένα υποκείμενο σε ένα αντικείμενο πρέπει να κατέχει και την αντίστοιχη διαβάθμιση ασφαλείας που επιβάλλεται από το αντικείμενο (η ετικέτα του αντικειμένου προσδιορίζει το επίπεδο ασφάλειας).

Στην προηγούμενη ενότητα αναφέραμε ότι οι βαθμοί ευαισθησίας της πληροφορίας είναι η Αδιαβάθμητη Εμπιστευτική, η Απόρρητη και η Άκρως Απόρρητη. Κάθε υποκείμενο και αντικείμενο εντάσσεται σε ένα επίπεδο ευαισθησίας (Sensitivity Level).[1]

[5] Ο δούρειος ίππος **(Trojan ή Trojan Horse)** είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα.



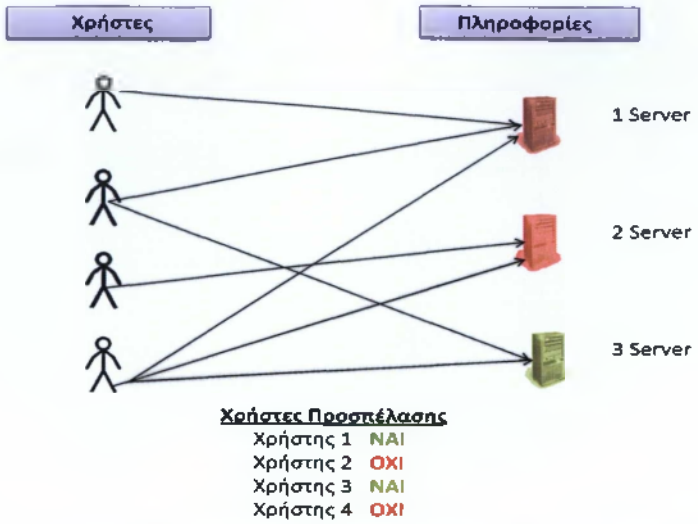
Εικόνα 16 - Υποκειμένου και Αντικειμένου σε ένα Επίπεδο Ευαισθησίας

Διακριτικός Έλεγχος Προσπέλασης DAC

Η πολιτική διακριτού ελέγχου προσπέλασης DAC, αντίθετα με τη MAC, είναι ένα μέσο περιορισμού πρόσβασης σε αντικείμενα, το οποίο βασίζεται ή στην ταυτότητα των χρηστών ή της ομάδας στην οποία ανήκουν αυτοί, ή και των δύο.Οι μηχανισμοί της πολιτικής DAC εντάσσουν συνήθως τη σημασία της ιδιοκτησίας του αντικειμένου, όπου ο ιδιοκτήτης του αντικειμένου έχει τη δυνατότητα και την άδεια να εγκρίνει την πρόσβαση στο αντικείμενο και σε άλλα υποκείμενα. Αυτός ο ορισμός υπάγεται σε ένα βιβλίο γνωστό στο ευρύ κοινό και ως «πορτοκαλί βιβλίο» με τίτλο Κριτήρια Αξιολόγησης Έμπιστων Υπολογιστικών Συστημάτων **(Trusted Computer Systems Evaluation Criteria - TSEC)**.[6] Ο πιο γενικός μηχανισμός για την εφαρμογή της πολιτικής DAC είναι της χρήσης των bits r-w-x (read-write-execute) και των λιστών του ελέγχου προσπέλασης **(Access Control Lists – ACL)**[7].

[6] United States Department of Defense, Trusted Computer System Evaluation Criteria,United States Department of Defense, 1983. http://csrc.nist.gov/publications/history/dod85.pdf

[7] Η Λίστα Ελέγχου Πρόσβασης καθορίζει ποιος μπορεί να εκτελέσει κάποια εργασία πάνω σε ένα αντικείμενο και τι είδους εργασία θα είναι αυτή.



Εικόνα 17 - Περιορισμός Προσπέλασης στα Αντικείμενα με Βάση τη Ταυτότητα του Χρήστη.

Ανακεφαλαιώνοντας, η πολιτική DAC είναι εύκολη στην υλοποίηση και προσφέρει ευελιξία σε μεγάλο βαθμό καθώς και οι χρήστες της έχουν τη δυνατότητα να ελέγξουν οι ίδιοι την πρόσβαση στους πληροφοριακούς πόρους που έχουν την ευθύνη. Όμως υπάρχει και μια αδυναμία, γνωστή ως και το πρόβλημα της αντιγραφής. Οι πληροφορίες μπορεί να αντιγραφούν από το ένα αντικείμενο στο άλλο, έτσι ώστε να είναι δυνατή η πρόσβαση στο αντίγραφο ακόμη και αν ο ιδιοκτήτης του πρωτότυπου αντίγραφου δε δίνει το δικαίωμα προσπέλασης στο πρωτότυπο. Αυτά τα αντίγραφα μπορούν να αυξηθούν από κακόβουλα λογισμικά όπως ο Δούρειος Ίππος (Trojan Horse), δίχως να είναι υποχρεωτική η συνεργασία των χρηστών που κατέχουν νόμιμες εξουσιοδοτήσεις για τα πρωτότυπα αντίγραφα.

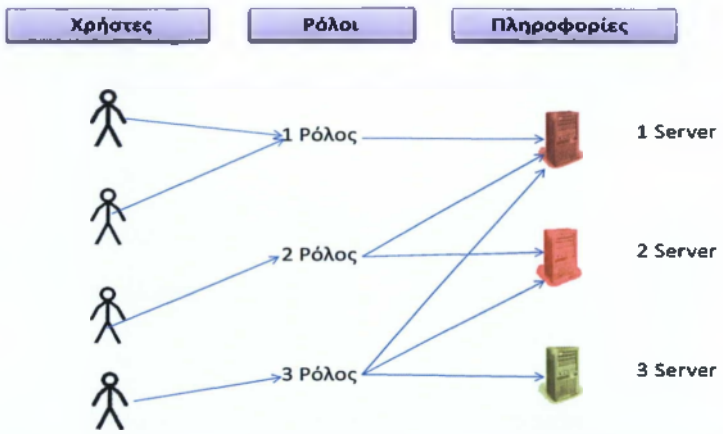
Επομένως ο Διακριτικός Έλεγχος Προσπέλασης DAC δεν παρέχει τρόπους διαφύλαξης της ροής των πληροφοριών, επειδή ορίζει τους χρήστες υπεύθυνους για τη θέσπιση της πολιτικής ασφαλείας κάτι που αποτελεί σημαντικό ρήγμα ασφαλείας. Άρα σε περίπλοκα συστήματα όπου συνηθίζεται μια κεντρική διαχείριση της ασφάλειας ή απαιτείται η ανάγκη για πολλαπλά επίπεδα ασφαλείας, η πολιτική DAC αμφισβητείται.

Ρολο-Κεντρικός Έλεγχος Προσπέλασης RBAC

Ο έλεγχος πρόσβασης των χρηστών με βάση ρόλων RBAC είναι η πιο γνωστή πολιτική εξουσιοδότησης. Χρησιμοποιεί μια κατάταξη ρόλων και πλήθος περιορισμών πρόσβασης έτσι μέσα από αυτούς να σημειωθεί ένα πλήθος πολιτικών ασφαλείας. Η χρήση των ρόλων για την οργάνωση των δικαιωμάτων κάνει πιο εύκολο τον τρόπο διαχείρισης ασφάλειας στην πρόσβαση σε λειτουργίες και δεδομένα. Η διάκριση των καθηκόντων είναι ζήτημα σχετικό με την ανάληψη των ρόλων για τον έλεγχο πρόσβασης των χρηστών. Η έννοια της διάκρισης των καθηκόντων βρίσκεται στη μείωση της απάτης, χωρίς να επιτρέπει στον καθένα να έχει πρόσβαση στο σύστημα έτσι ώστε να τελέσει την απάτη. Τέτοιου είδους πρόσβασης μπορούν με ευκολία να διατυπωθούν με τη χρήση της λογικής της διάκρισης των καθηκόντων στο μοντέλο των ρόλων, στις διανομές ρόλων σε χρήστες και στις διανομές των δικαιωμάτων πρόσβασης στους ρόλους.

Αυτός ο έλεγχος πρόσβασης με βάση τους ρόλους παρέχει πολλά πλεονεκτήματα σε αντίθεση με κλασικές τεχνικές πρόσβασης στα πληροφοριακά συστήματα άμεσα από τους χρήστες. Σε αυτά τα πλεονεκτήματα συμπεριλαμβάνονται η απλούστευση της διαχείρισης και των δικαιωμάτων πρόσβασης των χρηστών καθώς και η δυνατότητα της αποτελεσματικότητας του ελέγχου και των εξουσιοδοτήσεων των χρηστών. Η χρήση τέτοιας πολιτικής ελέγχου της πρόσβασης με βάση τους ρόλους έχει ως αποτέλεσμα τα δικαιώματα πρόσβασης να δίνονται στους ρόλους και όχι στους χρήστες. Επομένως όποια αλλαγή και τροποποίηση γίνεται στα δικαιώματα πρόσβασης των ρόλων, αυτόματα τροποποιούνται τα δικαιώματα των χρηστών που τα έχουν λάβει.

Εν κατακλείδι, η κεντρική ιδέα της πολιτικής RBAC είναι ότι οι αποφάσεις για εξουσιοδοτήσεις δεν γίνονται με βάση την ταυτότητα του χρήστη αλλά με βάση του ρόλου που έχει ο χρήστης στα πλαίσια του πληροφοριακού συστήματος.



Εικόνα 18 - Τα Δικαιώματα Πρόσβασης που Δίνονται στους Ρόλους

Διαδικασία Ταυτοποίησης και Αυθεντικοποίησης

Σε ένα πληροφοριακό σύστημα υπάρχουν ποικίλες τεχνικές και διαδικασίες για την ταυτοποίηση και αυθεντικοποίηση των διάφορων χρηστών. Η καλύτερη δυνατή επιλογή ανάμεσα σε πολλές τεχνικές παίζει σημαντικό ρόλο και αποτελεί βασικό στοιχείο για την ασφάλεια των επικοινωνιακών όσο και των υπολογιστικών συστημάτων.

- ✓ Ως προς τη διαδικασία της ταυτοποίησης **(Identification)** ενός λογικού υποκείμενου είναι εκείνη η διαδικασία στην οποία το υποκείμενο παρέχει σε ένα πληροφοριακό σύστημα τις πληροφορίες που χρειάζεται για να συσχετιστεί με ένα από τα αντικείμενα που δικαιούται προσπέλασης στους πόρους του.[8]
- ✓ Ως προς τη διαδικασία της αυθεντικοποίησης **(Authentication)** ενός λογικού υποκειμένου είναι εκείνη η διαδικασία στην οποία το υποκείμενο παρέχει σε ένα πληροφοριακό σύστημα τις πληροφορίες που χρειάζεται ώστε να ελεγχθεί η βασιμότητα της συσχέτισης που επιτεύχθηκε κατά τη διαδικασία της ταυτοποίησης.[9]

Δεδομένα Αυθεντικοποίησης

Συνθηματικά (Passwords)

Τα Συνθηματικά είναι ο πιο συνηθισμένο μέσο της αυθεντικοποίησης. Τα συνθηματικά αναφέρονται σε εκείνους τους μηχανισμούς αυθεντικοποίησης που στηρίζονται σε κάτι που οι χρήστες γνωρίζουν.
Επομένως συνθηματικό **(Password)** είναι η πληροφορία η οποία σχετίζεται με ένα λογικό υποκείμενο (δηλαδή χρήστες) και η οποία επιβεβαιώνει την ταυτότητα του λογικού υποκειμένου.[10]

Εικόνα 19 - Μηχανισμός Αυθεντικοποίησης Password

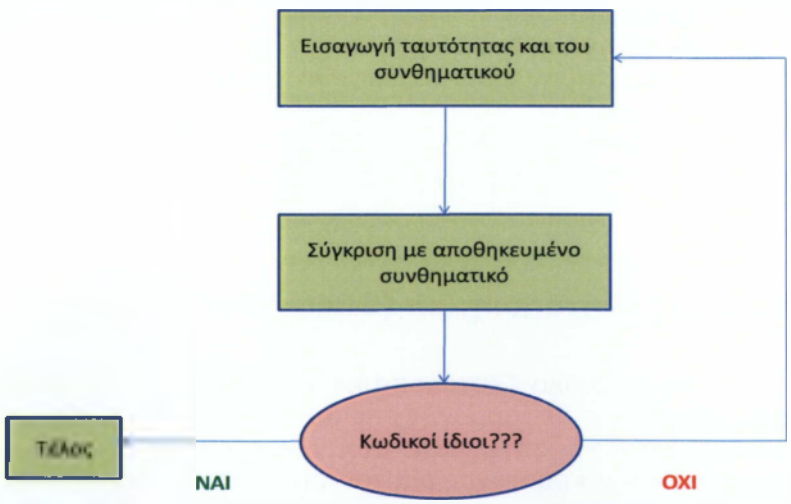
Η διάδοση της χρήσης των συνθηματικών στηρίζεται στα παρακάτω εξής πλεονεκτήματα:

- Έχουν απλή λειτουργία καθώς και απλούστερη σχεδιαστική πολυπλοκότητα.
- Έχουν χαμηλό κόστος.
- Έχουν παροχή σε ικανοποιητικό βαθμό προστασίας.

Όμως τα συνθηματικά ως μηχανισμός αυθεντικοποίησης έχουν και κάποια μειονεκτήματα:

- Υπάρχει πιθανότητα αποκάλυψης του συνθηματικού.
- Υπάρχει πιθανότητα αποκάλυψης με συστηματικό τρόπο του συνθηματικού.
- Υπάρχει πιθανότητα αποκάλυψης του συνθηματικού κατά τη διάρκεια της μετάδοσής του.

Η χρήση των συνθηματικών (Passwords) συνδυάζεται σύμφωνα με τα μοναδικά χαρακτηριστικά που προσδιορίζουν τους χρήστες ξεχωριστά. Έτσι για την αυθεντικοποίηση ο χρήστης αναγράφει το αναγνωριστικό του και στη συνέχεια το συνθηματικό στο σύστημα. Μετά την εισαγωγή τους, το σύστημα κάνει επαλήθευση των στοιχείων που ανεγράφησαν με αυτά που έχουν από την αρχή καταχωρηθεί στο σύστημα, στο φάκελο των αρχείων (Password File). Επομένως η πρόσβαση στο σύστημα επιτυγχάνεται με την εγκυρότητα του αναγνωριστικού και του συνθηματικού. Σε οποιαδήποτε περίπτωση αν κάποιο από τα προαναφερθέντα στοιχεία είναι λανθασμένο τότε η προσπάθεια πρόσβασης είναι μη επιτυχής.



Εικόνα 20 - Διαδικασία Αυθεντικοποίησης Password

Για λόγους ασφαλείας κάποια συστήματα χρησιμοποιούν έναν μετρητή ο οποίος καταγράφει τις αποτυχημένες προσπάθειες πρόσβασης από τους χρήστες και σε περίπτωση που κάποιος ξεπεράσει το όριο των αποτυχημένων προσπαθειών, το οποίο έχει ορίσει σύστημα, τότε ο λογαριασμός αυτόματα μπλοκάρεται (δηλαδή κλειδώνεται).

Σε κάποιες άλλες περιπτώσεις για να αποτραπεί η πρόσβαση και η χρήση του συστήματος από κάθε μη εξουσιοδοτημένο άτομο μπορεί να εφαρμοστεί ο μηχανισμός της

επαναλαμβανόμενης αυθεντικοποίησης. Δηλαδή η αυθεντικοποίηση εφαρμόζεται όχι μόνο τη στιγμή της προσβάσεως του συστήματος αλλά και κατά τη διάρκεια της χρήσης του συστήματος, σε τακτές χρονικές περιόδους.

Επομένως η επιλογή των συνθηματικών αποτελεί κρίσιμο παράγοντα για την ασφάλεια στα υπολογιστικά συστήματα. Η κάθε προσπάθεια πρόσβασης από κάποιον μη εξουσιοδοτημένο χρήστη είναι να μαντέψει ή να μάθει με διάφορες τεχνικές το συνθηματικό. Η υποκλοπή των συνθηματικών είναι και η πιο συνηθισμένη μορφή προσπάθειας παραβίασης.

Υπάρχουν δύο τεχνικές για την υποκλοπή των συνθηματικών οι οποίοι είναι οι εξής:

- **Το Συστηματικό ψάξιμο**: Εδώ έχουμε τη δοκιμή όλων των πιθανών συνδυασμών για τους αλφαριθμητικούς χαρακτήρες συγκεκριμένου μεγέθους. Εδώ οι κωδικοί σπάνε εύκολα (abcd, cdmt, 1990ba) και σε σύντομο χρονικό διάστημα.
- **Το Έξυπνο ψάξιμο**: Εδώ έχουμε τη δοκιμή των συνδυασμών που προέρχονται από πληροφορίες που έχουν σχέση με το χρήστη (αυτό μπορεί να αφορά το όνομά ή την ημερομηνία γέννησης του). Στην κατηγορία αυτή ανήκουν και οι δοκιμές συνθηματικών που χρησιμοποιούνται συχνά από τους χρήστες. Στην περίπτωση αυτή ανήκουν και οι επιθέσεις που γίνονται με την χρήση του λεξικού [εδώ δοκιμάζονται οι λέξεις που υπάρχουν σε ένα λεξικό π.χ το αγγλικό λεξικό. Ένας τέτοιος κωδικός (μια αγγλική λέξη όπως η λέξη probability) μπορεί να σπάσει σε σύντομο χρονικό διάστημα].

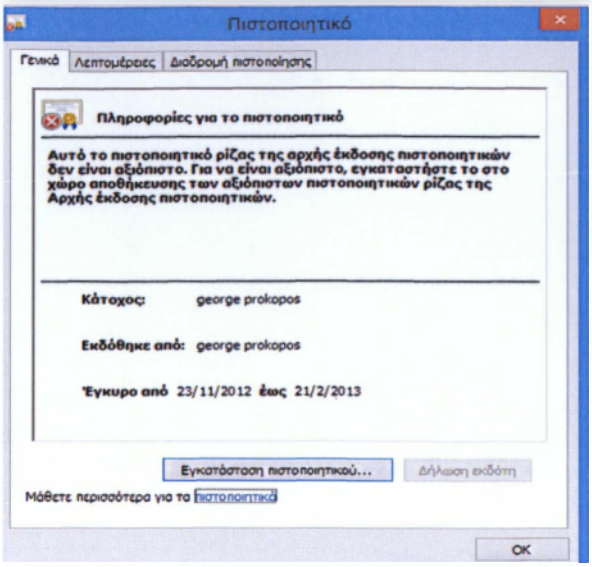
Επομένως η επιλογή των συνθηματικών πρέπει να στηρίζεται σε ορισμένα κριτήρια. Η επιλογή τους μπορεί να διεξαχθεί είτε από την έμπιστη οντότητα που βρίσκεται στο πληροφοριακό σύστημα (διαχειριστής του συστήματος), είτε έχει επιλογή από τον ίδιο τον χρήστη (εφόσον έχουν οριστεί προηγουμένως κάποια περιορισμοί). Η δεύτερη κατηγορία είναι η πιο συνηθισμένη αλλά και η πιο προτιμότερη έναντι της πρώτης. Κάποια κριτήρια για τη χρήση και την επιλογή των συνθηματικών σε κάποιο σύστημα είναι τα εξής:

- **Το Μήκος του Συνθηματικού**: Εδώ ορίζεται το ελάχιστο και το μέγιστο μήκος για τα συνθηματικά.
- **Το Μορφότυπο του Συνθηματικού**: Εδώ υπάρχει ο συνδυασμός των γραμμάτων, αριθμών και ειδικών χαρακτήρων.
- **Η Αποφυγή Έυκολων Συνθηματικών**: Εδώ απαιτείται η εκπαίδευση των χρηστών.
- **Οι Οδηγίες Φύλαξης**: Τα συνθηματικά πρέπει να φυλάσσονται σε ασφαλές μέρος ώστε να μην είναι σε εμφανή σημείο καθώς και να μην ανακοινώνονται σε τρίτα άτομα).
- **Η Αλλαγή Συνθηματικών**: Εδώ πρέπει να εφαρμόζεται ένας αυτόματος έλεγχος σε κάθε αλλαγή των συνθηματικών από τους χρήστες.

Ψηφιακά Πιστοποιητικά (Digital Certificate)

Τα Ψηφιακά Πιστοποιητικά **(Digitals Certificates)** αποτελούν μια διαδεδομένη μιας τεχνολογίας εφαρμογής της αυθεντικοποίησης που στηρίζεται σε κάτι που έχει στην κατοχή του ο χρήστης. Αυτά έχουν την μορφή δυαδικών αρχείων και η λειτουργία τους βασίζεται στην κρυπτογραφία του δημόσιου κλειδιού. Έτσι μπορούν να χρησιμοποιηθούν για τον περιορισμό ως προς τον την αποκάλυψη της ταυτότητας του χρήστη ενσωματώνοντας ψευδώνυμα αντί της πραγματικής ταυτότητάς του. Ένα ψηφιακό πιστοποιητικό περιλαμβάνει το δημόσιο κλειδί ενός χρήστη, το όνομα του κατόχου, τους αλγόριθμους που χρησιμοποιούνται και διάφορες άλλες πληροφορίες σχετικά με τον κάτοχο του κλειδιού. Για να είναι έγκυρο ένα ψηφιακό πιστοποιητικό, πρέπει να είναι

υπογεγραμμένο από κάποια Αρχή Πιστοποίησης[10] και περιλαμβάνει μια ημερομηνία λήξης (Περίοδο ισχύος).



Εικόνα 21 - Ψηφιακό Πιστοποιητικό (Digital Certificate).

Κάποια πρότυπα ψηφιακών πιστοποιητικών είναι τα εξής:

- ✓ Internet PKI based on X.509 **(PKIX)**: Το PKIX είναι μια σειρά από προσχέδια για το διαδίκτυο που προσδιορίζουν διάφορα θέματα σχετικά ως προς την ανάπτυξη μιας ιεραρχικής Υποδομής Δημόσιου Κλειδιού (ΥΔΚ). Αυτά τα προσχέδια PKIX αναπτύχτηκαν εξαιτίας του συμβάντος ότι το X.509 είναι ένα γενικό πρότυπο, το οποίο αφήνει πολλά κενά που έχουν σχέση με την πραγματική λειτουργία και διαχείρισης μια Έμπιστης Τρίτης Οντότητας (ΕΤΟ).[11]
- ✓ Simple Puplic Key Infrastructure **(SPKI)**: Σε αντίθεση με το Internet PKI based on X.509 **(PKIX)** που αντιστοιχίζει δημόσια κλειδιά με βάση τα ονόματα, το SPKI χρησιμοποιεί πιστοποιητικά που ο κώδικας αναφοράς στηρίζεται στο δημόσιο κλειδί αντί στα ονόματα, που αντιστοιχούν σε ρόλους και όχι στα πρόσωπα.
- ✓ Pretty Good Privacy **(PGP)**: Είναι μια κρυπτογράφηση των δεδομένων και το πρόγραμμα του υπολογιστή αποκρυπτογράφησης που παρέχει κρυπτογραφική προστασία της ιδιωτικής ζωής και της ταυτότητας για την επικοινωνία των δεδομένων. Το Pretty Good Privacy χρησιμοποιείται συχνά για την υπογραφή, κρυπτογράφηση, αποκρυπτογράφηση κειμένων, τα e-mails, αρχεία, καταλόγους, καθώς και ολόκληρο τμήματα του δίσκου και να αυξήσουν την ασφάλεια του ηλεκτρονικού ταχυδρομείου.[13]

[10] Η Αρχή Πιστοποίησης είναι μία οντότητα η οποία έχει το δικαίωμα να εκδίδει και να ανακαλεί ψηφιακά πιστοποιητικά.

[11] Η Έμπιστη Τρίτη Οντότητα (ΕΤΟ) αποτελεί την απαραίτητη υποδομή προκειμένου να διασφαλιστεί η αυθεντικότητα, ακεραιότητα και εμπιστευτικότητα των ηλεκτρονικών συναλλαγών που πραγματοποιούνται καθώς και οποιονδήποτε πληροφοριών διακινούνται μεταξύ των οντοτήτων που έχουν πιστοποιηθεί από την ΕΤΟ).

Τύπος πιστοποιητικού	Χαρακτηριστικά εμπιστοσύνης και πιστοποίησης	Πεδίο αναγνώρισης πιστοποιητικού
PKIX (X.509)	1) Ιεραρχική εμπιστοσύνη 2) Ονοματοδοσία οικουμενικής εμβέλειας 3) Δια-πιστοποίηση 4) Πολιτικές και δηλώσεις πρακτικών	*Οικουμενικά μοναδικό (X.500):* Διακριτικό όνομα επιλεγμένο από τον πάροχο
SPKI	1) Αυτόνομη αρχή πιστοποίησης 2) Ονόματα τοπικής εμβέλειας 3) Δεν απαιτούνται δηλώσεις πρακτικών	*Τοπικό και αυθαίρετο:* Δημόσιο κλειδί
PGP	1) Πλέγμα εμπιστοσύνης 2) Πολλαπλές εναλλακτικές διαδρομές πιστοποίησης 3) Υπογραφή πιστοποιητικού από οποιονδήποτε 4) Δεν επιβάλλεται πολιτική	*Οικουμενικά μοναδικό αλλά μη σταθερό:* Διεύθυνση e-mail

Εικόνα 22 - Τα Πρότυπα των Πιστοποιητικών.

Έξυπνες Κάρτες (Smart Cards)

Με δεδομένη την ανάπτυξη της τεχνολογίας άλλο ένα μέσο αυθεντικοποίησης που στηρίζεται σε αυτό που κατέχει ο χρήστης είναι οι Έξυπνες Κάρτες (Smart Cards). Οι έξυπνες κάρτες είναι ουσιαστικά μικροσκοπικοί υπολογιστές, οι οποίες έχουν το μέγεθος και τη φόρμα μιας πιστωτικής κάρτας, στην οποία πάνω υπάρχει ενσωματωμένο ένα ολοκληρωμένο κύκλωμα (Chip)[12], στην μπροστινή αριστερή πλευρά. Η συγκεκριμένη τεχνολογία έχει υιοθετηθεί σε εφαρμογές όπως: Τα κινητά τηλέφωνα, τον έλεγχο φυσικής πρόσβασης σε εγκαταστάσεις, τον έλεγχο λογικής πρόσβασης σε δίκτυα κ τ λ.

Εικόνα 23 - Έξυπνες Κάρτες (Smart Cards).

Οι έξυπνες κάρτες (Smart Cards) έχουν ένα ολοκληρωμένο κύκλωμα (Chip) που περιλαμβάνει τις επαφές εισόδου – εξόδου και μπορεί να περιέχει μόνο μνήμη ή και μικροεπεξεργαστή. Στον μικροεπεξεργαστή, διαμέσου του οποίου εξασφαλίζεται ένα υψηλό επίπεδο ασφαλείας για τα δεδομένα που αποθηκεύουν και τα επεξεργάζονται, ενώ συγχρόνως στηρίζει την ασφαλή ενημέρωση ή την εγγραφή των δεδομένων στην κάρτα

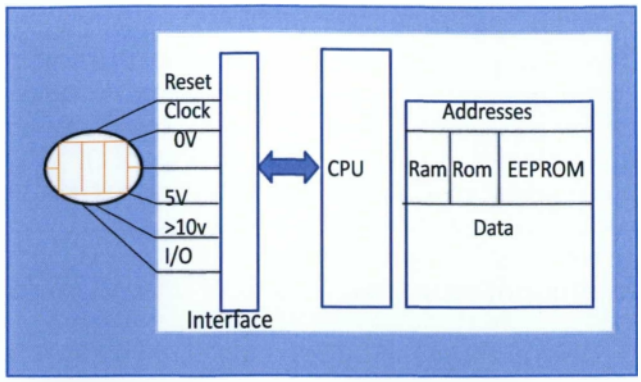
[12] Ολοκληρωμένο κύκλωμα ένα κύκλωμα συνδεδεμένων λογικών πυλών, δημιουργημένο πάνω σε ένα φύλλο. Η πλειονότητα των ολοκληρωμένων κυκλωμάτων δημιουργούνται πάνω σε φύλλα ημιαγωγών, κατά κύριο λόγο πυριτίου. Το φύλλο (ημιαγωγού) ονομάζεται στα αγγλικά τσιπ (chip), από το οποίο προκύπτει μια εναλλακτική ονομασία του ολοκληρωμένου κυκλώματος.

οποιαδήποτε χρονική περίοδο μετά την έκδοσή της. Επομένως το ολοκληρωμένο κύκλωμα παρέχει μια ασφαλή δομή πολλαπλών επιπέδων καθώς και το να επιτρέπει μια ιεραρχημένη πρόσβαση, κάνοντας δύσκολη την πρόσβαση στα στοιχεία που υπάρχουν αλλά και στην παραποίηση αυτών, καθώς και να κάνει άμεσα αντιληπτή τις προσπάθειες πρόσβασης οι οποίες δεν είναι έγκυρες (όπως συνήθως γίνεται με τις κάρτες SIM σε περίπτωση λανθασμένου PIN, πάνω από 3 φορές).
Τέλος, προκειμένου τα Chip να χρησιμοποιηθούν και σε τερματικά τα οποία δεν έχουν το ίδιο μέγεθος για την εισαγωγή της ολόκληρης κάρτας τους, καθίστανται δυνατή η δημιουργία καρτών με εγκοπές γύρω από το Chip, ώστε να αφαιρείται και στην συνέχεια να τοποθετείται στη τερματική συσκευή (δηλαδή όπως οι κάρτες SIM).

Τα κύρια τμήματα που περιλαμβάνει μια έξυπνη κάρτα είναι τα εξής:

- **Η Μνήμη Εργασίας** (Working Memory – Random Access Memory): Εδώ διατηρούνται τα περιεχόμενά της μόνο στη διάρκεια που η έξυπνη κάρτα τροφοδοτείται με ρεύμα και στην περίπτωση αυτή χρησιμοποιείται μόνο από τον μικροεπεξεργαστή για την προσωρινή αποθήκευση των δεδομένων.
- **Η Μη Διαγράψιμη Μνήμη ROM** (Read Only Memory): Εδώ δεν χρειάζεται να τροφοδοτείται συνεχώς ρεύμα για τη διατήρηση των δεδομένων που έχουν αποθηκευτεί. Η μνήμη αυτή αξιοποιείται για την αποθήκευση του λειτουργικού συστήματος της κάρτας στο οποίο στηρίζονται οι μηχανισμοί ασφαλείας και οι λειτουργικές προδιαγραφές.
- **Η Μνήμη Εφαρμογών** (EEPROM): Η μνήμη εφαρμογών είναι διαχωρισμένη σε ανεξάρτητα τμήματα, και αποθηκεύει συγκεριμένες κατηγορίες δεδομένων. Ανάλογα με το είδος της έξυπνης κάρτας, ο προσδιορισμός της μνήμης μπορεί να γίνει προσδιορίζοντας συγκεκριμένες περιοχές της μνήμης.Τα ανεξάρτητα τμήματα της μνήμης αυτής είναι τα παρακάτω:

    - ✓ Μυστική Περιοχή **(Secret Area)**: Η περιοχή αυτή έχει τη δυνατότητα να εγγραφεί μόνο μια φορά, ενώ απαγορεύεται οποιαδήποτε άλλη προσπάθεια προσπέλασης για την ανάγνωση των δεδομένων. Τα δεδομένα αυτά αποθηκεύονται στην περιοχή αυτή και συμπεριλαμβάνουν ποικίλα μυστικά κλειδιά και κωδικούς τα οποία χρησιμοποιούνται εσωτερικά από την κάρτα για τους μηχανισμούς ασφαλείας.
    - ✓ Περιοχή Ιστορικού Πρόσβασης **(Access Area)**: Στην περιοχή αυτή υπάρχει η δυνατότητα καταγραφής όλων των προσπαθειών που έχουν γίνει για την πρόσβαση σε κάποια προστατευόμενη πληροφορία χωρίς να χαρακτηριστεί ως επιτυχείς ή όχι. Σε περίπτωση συνεχόμενων προσπαθειών με λανθασμένο κωδικό τότε η κάρτα κλειδώνεται αυτομάτως.
    - ✓ Περιοχή Ελεύθερης Πρόσβασης **(Public Area)**: Στην περιοχή αυτή δεν απαιτείται η χρήση κωδικών ή μυστικών κλειδιών για προσπέλαση. Αξιοποιείται ως προς την αποθήκευση των μη εμπιστευτικών δεδομένων.
    - ✓ Περιοχή Εργασίας **(Work Area)**: Η περιοχή αυτή χρησιμοποιείται για την αποθήκευση των δεδομένων από τις εφαρμογές. Αναλόγως με τα χαρακτηριστικά της εφαρμογής τα δεδομένα μπορούν να προστατεύουν σε ως προς την ανάγνωση, την εγγραφή ή και τη διαγραφή τους μέσω κάποιων μυστικών κλειδιών.



Εικόνα 24 - Αρχιτεκτονική Άποψη Έξυπνης Κάρτας

Η ταυτοποίηση (Identification) του κατόχου και χρήστη των έξυπνων καρτών πραγματοποιείται με τον προσωπικό μυστικό κωδικό (PIN) που έχει. Στη συνέχεια ο συγκεκριμένος κωδικός PIN συγκρίνεται με τον αντίστοιχο κωδικό ο οποίος είναι αποθηκευμένος στη μυστική περιοχή της μνήμης που έχει η έξυπνη κάρτα. Τέλος η διαδικασία σύγκρισης πραγματοποιείται εσωτερικά μέσα στην έξυπνη κάρτα. Επομένως το γεγονός αυτό εξαλείφει όποιες απειλές υπάρξουν διότι το τερματικό των έξυπνων καρτών δεν απαιτείται να εκτελέσει κάποιον αλγόριθμο αποκρυπτογράφησης ή να αποθηκεύσει κάποιον κωδικό. Συγκρίνοντας με άλλες τεχνολογίες οι έξυπνες κάρτες παρέχουν ένα μεγάλο αποθηκευτικό χώρο, επιτρέποντας να πραγματοποιηθεί ένας μηχανισμός ταυτοποίησης με βιομετρικά χαρακτηριστικά (σε αυτό το σημείο θα αναφερθούμε και παρακάτω). Έχοντας αυτήν τη μέθοδο της ταυτοποίησης και χωρίς να χρειάζεται να δώσουμε κάποιο κωδικό PIN, μπορούμε να παρέχουμε εξαιρετική υψηλή ασφάλεια.

Με την αυθεντικοποίηση (Authentication) των έξυπνων καρτών στόχος είναι να διασφαλιστεί η γνησιότητα της έξυπνης κάρτας. Επομένως αυθεντικοποίηση μπορούμε να κάνουμε με τα εξής:

- ✓ Με τη χρήση ψηφιακών πιστοποιητικών και των ασύμμετρων κρυπτογραφικών αλγορίθμων[13].
- ✓ Αξιοποιώντας τους συμμετρικούς αλγορίθμους κρυπτογράφησης (για παράδειγμα ο DES).[17]

Συστήματα Αυθεντικοποίησης

Τα συστήματα αυθεντικοποίησης και διανομής κλειδιών που υπάρχουν χρησιμοποιούνται για τα δίκτυα και τα κατανεμημένα συστήματα, ώστε να παρέχουν υπηρεσίες ασφαλείας σε επίπεδο εφαρμογής. Σήμερα υπάρχουν ποικίλα τέτοια συστήματα όπως τα Kerberos και το SESAME.

Σύστημα KERBEROS

Το Kerberos είναι ένα σύστημα το οποίο αναπτύχθηκε από το Massachusetts Institute of Technology (MIT) με στόχο να προστατέψει τις διαδικτυακές υπηρεσίες οι οποίες παρέχονταν στα πλαίσια του προγράμματος Athena και στηρίζεται στο μοντέλο

[15, 16] Υπάρχουν δύο μεγάλες οικογένειες αλγόριθμων κρυπτογράφησης, οι συμμετρικοί αλγόριθμοι (ή αλγόριθμοι μυστικού κλειδιού) και οι ασύμμετροι (ή αλγόριθμοι δημόσιου κλειδιού). Στην συμμετρικοί κρυπτογραφία το ίδιο το κλειδί χρησιμοποιείται και για την κρυπτογράφιση και την αποκρυπτογράφιση των δεδομένων. Ενώ στην ασσύμετρη κρυπτογραφία γίνεται χρήση δύο κλειδιών, ενός δημόσιου και ενός ιδιωτικού τα οποία σχετίζονται μεταξύ τους με κάποιες μονόδρομες συναρτήσεις (one-way functions).

διανομής κλειδιών. Υπάρχουν οι εκδόσεις 1-3 οι οποίες χρησιμοποιήθηκαν μόνο εσωτερικά στο MIT. Η 4η έκδοση διατέθηκε δημόσια και χρησιμοποιήθηκε σε μεγάλο βαθμό. Ωστόσο λόγω των πολλών απαιτήσεων που υπήρχαν, τις οποίες δεν μπορούσε να καλύψει 4η έκδοση, υιοθετήθηκαν νέα χαρακτηριστικά και αναπτύχθηκε ο Kerberos 5η έκδοση η οποία μπορούσε να αναφερθεί σε περισσότερες περιπτώσεις.

Το Kerberos είναι ένα σύστημα πιστοποίησης ταυτότητας το οποίο δημιουργήθηκε και αναπτύχθηκε με στόχο την αντικατάσταση του συστήματος που καλείται πιστοποίηση βάσει ισχυρισμού (Authentication By Assertion). Η πιστοποίηση αυτή βασίζεται στα εξής: όταν ένας χρήστης τρέχει ένα πρόγραμμα που απαιτεί πρόσβαση σε κάποια δικτυακή υπηρεσία (Network Services), επομένως το πρόγραμμα ανακοινώνει στον server ότι λειτουργεί με βάση του συγκεκριμένου χρήστη. Έτσι ο server πιστεύει τα στοιχεία που του παρέχει το πρόγραμμα και εξυπηρετεί το χρήστη χωρίς να ζητά άλλες αποδείξεις. Άρα, όπως είναι κατανοητό, η συγκεκριμένη ασφάλεια που παρέχεται είναι πολύ χαμηλού επιπέδου (Low Level) έως και ελλιπής.

Κάποιο άλλο σύστημα που χρησιμοποιείται πάρα πολύ, είναι η συνοδεία του ονόματος του χρήστη από κάποιο μυστικό κωδικό. Με αυτόν τον τρόπο υπάρχουν δύο διαφορετικά μειονεκτήματα. Το πρώτο έχει ως αποτέλεσμα το χάσιμο χρόνου για το χρήστη. Το δεύτερο και το σπουδαίο είναι ευάλωτο σε επιθέσεις λόγω ότι ο κωδικός που περνάει το δίκτυο δεν είναι κρυπτογραφημένος. Άρα το σύστημα Kerberos βασίζεται στο να καλύπτει ένα σημαντικό κενό των συστημάτων της πιστοποίησης της ταυτότητας.

Επομένως το σύστημα Kerberos:

- Στηρίζεται σε πρωτόκολλα διανομής κλειδιών.
- Μετέπειτα τροποποιήθηκαν και για να περιβάλλουν και χρονοσφραγίδες.
  - ✓ Το σύστημα είναι οργανωμένο σε «πεδία ».
  - ✓ Κάθε «πεδίο» έχει έναν Authentication Server (AS)- (Εξυπηρετητής Αυθεντικοποίησης).
  - ✓ Ένα μυστικό κλειδί για κάθε P-AS.
  - ✓ Εισιτήρια Αυθεντικοποίησης & session keys.
  - ✓ Ticket Granting Tickets (TGT).
  - ✓ Ticket Granting Server (TGS).
  - ✓ TC,S={U,C,S,K,tstart,texpire}Ks.
  - ✓ Ac,tgs={C,t}K.

Σύμφωνα με τα παραπάνω το σύστημα Kerberos λειτουργεί ως εξής:

Το σύστημα είναι οργανωμένο σε πεδία. Σε κάθε πεδίο υπάρχει ένας ασφαλής και κεντρικός εξυπηρετητής αυθεντικοποίησης, το οποίο έχει έναν κοινό συμμετέχοντα P ένα μυστικό κλειδί Kp. Εάν ο P είναι ο χρήστης, τότε το Kp παράγεται από το συνθηματικό του, χρησιμοποιώντας μια μονόδρομη συνάρτησης σύνοψης.[14]

Έτσι το σύστημα λειτουργεί, με το να παρέχει στους συμμετέχοντες εισιτήρια με τα οποία μπορεί να αποδείξουν την ταυτότητά τους καθώς και να κάνουν πιο ασφαλείς τις επικοινωνίες μεταξύ τους. Έτσι ο Authentication Server (AS) αυθεντικοποιεί τους χρήστες κατά τη σύνδεσή τους και τους παρέχει ένα εισιτήριο έκδοσης εισιτηρίων Ticket Granting Tickets (TGT). Το εισιτήριο αυτό μπορεί να χρησιμοποιηθεί για την έκδοση εισιτηρίων από κάποιον εξυπηρετητή έκδοσης εισιτηρίων Ticket Granting Server (TGS), και στη συνέχεια μπορούν να χρησιμεύσουν ως διαπιστευτήρια ως προς την επαφή για άλλους εξυπηρετητές.

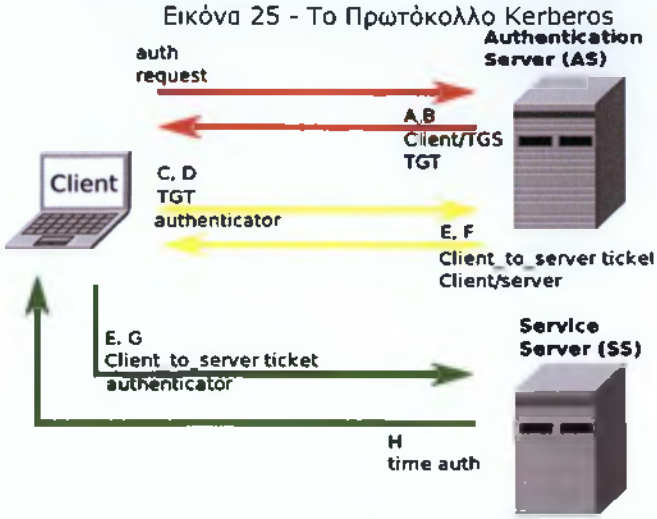
Η έκφραση TC,S={U,C,S,K,tstart,texpire}Ks υποδηλώνει κάποιο εισιτήριο με το οποίο ο πελάτης C μπορεί να το χρησιμοποιήσει για να επικοινωνήσει με τον εξυπηρετητή S για το χρήστη U. Το εισιτήριο αυτό περιλαμβάνει τα ονόματα των συμμετεχόντων U και S, τη διεύθυνση του δικτύου C, ένα κλειδί συνόλου K, ένα χρόνο έναρξης (tstart) και ένα χρόνο λήξης (texpire) αντίστοιχα. Το εισιτήριο αυτό είναι κρυπτογραφημένο με το

[14] Οι μονόδρομες συναρτήσεις σύνοψης **(One - Way Hash Functions)** αποτελούν θεμελιώδη στοιχεία για την ανάπτυξη των περισσότερων πρωτοκόλλων κρυπτογράφησης.

Ks, το μυστικό κλειδί του S, ώστε να το C να μην μπορεί να το διαβάσει ή και να το τροποποιήσει. Επιπλέον για να το προστατεύσει από επιθέσεις επανάληψης, ο C αναπτύσσει και στέλνει επιπλέον έναν αυθεντικοποιητή AC,S = {C,t}K, που περιέχει την διεύθυνση του δικτύου C και μια χρονοσφραγίδα (Timestamping) t. Ο αυθεντικοποιητής αυτός είναι και κρυπτογραφημένος με το κλειδί συνόδου.[18]

1: C	→	AS	: U,TGS
2: AS	→	C	: Tc,tgs, {TGS, K, tstart, texpire}Ku
3: C	→	TGS	: S, Tc,tgs, Ac,tgs
4: TGS	→	C	: Tc,s, {S, K', t'start, t'expire}K
5: C	→	S	: Tc,s, Ac,s
6: S	→	C	: {t'}K'

Εικόνα 25 - Το Πρωτόκολλο Kerberos



Εικόνα 26 - Η Διαδικασία του Πρωτόκολλου Kerberos στο Σύστημα.

Σύστημα SESAME

Το σύστημα SESAME είναι το Ευρωπαϊκό Σύστημα Ασφαλείας και χρησιμοποιείται για εφαρμογές σε ανομοιογενή υπολογιστικά περιβάλλοντα και δεν αποτελεί εμπορικό προϊόν. Αυτό παρέχει τις σημαντικές λειτουργίες ασφαλείας, με τις οποίες οι κατασκευαστές που υλοποιούν τα τελικά προϊόντα πληροφορικής. Το σύστημα SESAME έχει πολλές ομοιότητες με το σύστημα Kerberos. Ακόμα χρησιμοποιεί τις δομές δεδομένων καθώς και είναι προσβάσιμο από το πρωτόκολλο του Kerberos.

Το σύστημα SESAME αναπαράχθηκε με απώτερο σκοπό να αναπτύξει τεχνολογία αυθεντικοποίησης των χρηστών με έλεγχο κατανεμημένης πρόσβασης. Η τωρινή έκδοση του SESAME είναι η 4η έκδοση και η σημαντική αλλαγή της είναι από την προηγουμένη έκδοση είναι ότι ολόκληρος κώδικας του Kerberos 5 αντικαταστάθηκε με τον κώδικα του SESAME. Έτσι αυτό είχε ως αποτέλεσμα να αφαιρέσει τους ελέγχους εξόδου και να κάνει απλούστερη τη διαδικασία της εγκατάστασης του συστήματος.

Επομένως η αρχιτεκτονική δομή του SESAME απαρτίζεται από 3 εξυπηρετητές οι οποίοι είναι οι εξής:

- Ο Εξυπηρετητής Αυθεντικοποίησης **(Server Authentication – AS)**: Ο εξυπηρετητής αυθεντικοποίησης αποτελεί το κεντρικό σημείο της

αυθεντικοποίησης του χρήστη. Στην αρχή για να προχωρήσει ο εκκινητής της διαδικασίας πρέπει να συνδεθεί με τον εξυπηρετητή αυθεντικοποίησης.

- Ο Εξυπηρετητής Εκχώρησης των Δικαιωμάτων **(Privilige Attribute Server – PAC)**: Ο εξυπηρετητής εκχώρησης δικαιωμάτων επαληθεύει του εκκινητή τα δικαιώματα πρόσβασης και συγχρόνως του παράγει ένα πιστοποιητικό προνομίων.
- Ο Εξυπηρετητής Διανομής Κλειδιών **(Key Distribution Server – KDS)**: Τέλος αφού ο εκκινητής επιλέξει την εφαρμογή με την οποία θέλει να συνδεθεί στη συνέχεια του παρέχονται οι πληροφορίες για τα κλειδιά. Σε περίπτωση που αυτή η εφαρμογή χρησιμοποιεί μια ασύμμετρη κρυπτογράφηση, παρέχεται από τον εξυπηρετητή της διανομής των κλειδιών.

Τέλος η υποδομή χρειάζεται για να υλοποιηθεί η προαναφερθείσα αρχιτεκτονική περιλαμβάνεται από τα εξής:

- Τους εξυπηρετητές που παρέχουν τις προαναφερθείσες υπηρεσίες.
- Τους εξυπηρετητές που παρέχουν τις κατάλληλές λειτουργίες, για να διαχειρίζονται τα υπογεγραμμένα πιστοποιητικά καταλόγων που είναι βασικά για τις υπηρεσίες της ασύμμετρης κρυπτογράφησης:
  - ✓ Τοπική Αρχή Εγγραφής **(Local Registration Authority)**.
  - ✓ Αντιπρόσωπο Αρχής Πιστοποίησης **(Certification Authority Agent)**.
  - ✓ Αρχή Πιστοποίησης **(Certification Authority)**.[19]

Βιομετρικά Συστήματα

Εισαγωγή

Μια άλλη ασφαλής τεχνική ταυτοποίησης είναι η εφαρμογή της τεχνολογίας των βιομετρικών συστημάτων, η οποία στηρίζεται στα φυσικά χαρακτηριστικά του ανθρώπινου σώματος. Τα κύρια στοιχεία της διαδικασίας της αυθεντικοποίησης είναι η ίριδα του ματιού, τα δακτυλικά αποτυπώματα, η χροιά φωνής και το DNA.

Η βιομετρική τεχνολογία αναπτύχθηκε με στόχο την εφαρμογή ελέγχου ταυτοποίησης και αυθεντικοποίησης, αρχικά από κυβερνητικούς οργανισμούς σε εφαρμογές που αφορούν ελέγχους προσβάσεις σε εγκαταστάσεις που είναι ιδιαίτερα κρίσιμες για την εθνική ασφάλεια. Αρχικά εμφανίστηκαν πολλά προβλήματα, αλλά με την εξέλιξη και την πάροδο του χρόνου βελτιώθηκαν αρκετά.

Τα βιομετρικά συστήματα εφαρμόζουν τεχνικές για τη μέτρηση των φυσικών χαρακτηριστικών του προσώπου ή κάποιας ανθρώπινης συμπεριφοράς. Επομένως κατά τη διάρκεια της καταγραφής ενός ανθρώπινου χαρακτηριστικού σε ένα βιομετρικό σύστημα, το οποίο αμέσως αποθηκεύεται μέσω κάποιων εξειδικευμένων μετρήσεων. Οι τεχνικές αυτές προσδιορίζονται ως έχων:

- ✓ Στις τεχνικές των ανθρώπινων χαρακτηριστικών (φυσικό): Εδώ έχουμε την ανάλυσης της ίριδας του ματιού, τα δακτυλικά αποτυπώματα, το DNA και τη γεωμετρία χεριού.
- ✓ Στις τεχνικές που αφορά τη μέτρηση της συμπεριφοράς: Εδώ έχουμε την ανάλυση της φωνής και την αναγνώριση της υπογραφής.

Η τεχνολογία της μέτρησης των χαρακτηριστικών στα βιομετρικά συστήματα είναι απαρτίζεται από δύο βασικές έννοιες: την ανοχή σε σφάλματα και η τεχνική αποθήκευσης των προτύπων ανάλυσης.

Σε αυτά τα συστήματα η ρύθμιση του βαθμού σφάλματος αποτελεί κρίσιμο παράγοντα για το ρυθμό και την απόδοση του συστήματος. Επομένως το επίπεδο της ανοχής πρέπει να είναι χαμηλό (μέσα στα όρια) και προσδιορίζεται από τον ίδιο τον κατασκευαστή του συστήματος.

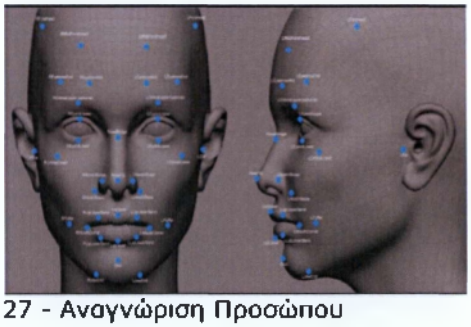
Η αποθήκευση των προτύπων (βιομετρικής μέτρησης του γνωρίσματος) μπορεί να γίνεται σε διάφορα μέσα, ανάλογα με την τεχνολογία η οποία χρησιμοποιείται και απαιτήσεις ασφαλείας της συγκριμένης εφαρμογής (στα πρότυπα υπάρχει η δυνατότητα αποθήκευσης ή στη ίδια συσκευή μέτρησης ή σε κάποια βάση δεδομένων.

Κάποια από τα βασικά χαρακτηριστικά των βιομετρικών συστημάτων είναι η ακρίβεια **(Accuracy)**, η αξιοπιστία **(Reliability)**, η ταχύτητα **(Speed)**, η μοναδικότητα **(Uniqueness)**, η αποδοχή του χρήστη **(User Acceptance)**, η παραποίηση στοιχείων **(Falsifying Data)**, η αποθήκευση δεδομένων **(Data Storage)** και απαιτήσεις επεξεργασίας **(Processing Requirements)** καθώς και η διαδικασία καταχώρησης **(Registration Procedure).**

Αναγνώριση Προσώπου

Η αναγνώριση της ταυτότητας ενός ανθρώπου από την ανάλυση των χαρακτηριστικών του προσώπου είναι μια διαδικασία που κάθε άλλο θα μπορούσε να χαρακτηριστεί απλή. Αρχικά υπάρχει μια κάμερα που συλλαμβάνει την εικόνα του προσώπου του χρήστη και στη συνέχεια το σύστημα προσπαθεί να εντοπίσει τα βασικά σημεία πάνω σε αυτήν (σχήμα ματιών, μέγεθος μύτης, τα βλέφαρα, το στόμα). Εφόσον γίνει αυτό οι αποστάσεις που θα υπάρξουν των βασικών σημείων, μετριούνται και τα αποτελέσματα αποθηκεύονται για να αποτελέσουν με τη σειρά τους το βιομετρικό πρότυπο (Biometric Template) του χρήστη. Τα πιο εξελιγμένα συστήματα προσφέρουν περισσότερη ακρίβεια αλλά και τρισδιάστατα μοντέλα προσώπου.

Άλλη μια παρόμοια τεχνική είναι και η θερμογραφία του προσώπου η οποία χρησιμοποιεί μια υπέρυθρη κάμερα για να χαρτογραφήσει τη ροή του αίματος κάτω από την επιφάνεια του δέρματος. Οι σχηματισμοί που προκύπτουν από τα αιμοφόρα αγγεία είναι αρκετοί, για την επιβεβαίωση της ταυτότητας κάποιου, εφόσον είναι μοναδικά για κάθε άτομο. Το μειονέκτημα είναι ότι δεν μπορεί να λειτουργήσει σε ικανοποιητικό βαθμό σε κάποιο σημείο το οποίο δεν είναι φωτισμένο καλά και από την άλλη ο εξοπλισμός είναι αρκετά ακριβός.



Εικόνα 27 - Αναγνώριση Προσώπου

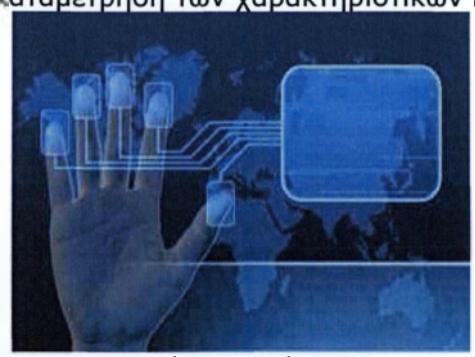
Το ιδιαίτερο πρόβλημα που μπορεί να διαπιστωθεί στην αναγνώριση του προσώπου είναι ότι τα χαρακτηριστικά του προσώπου μπορούν να αλλάξουν εύκολα με την πάροδο του χρόνου (το ίδιο συμβαίνει και σε περίπτωση που ο χρήστης φοράει γυαλιά ή και κάποια παραπάνω κιλά που μπορεί να αποκτήσει μπορεί να επιφέρουν στο σύστημα κάποια προβλήματα). Επομένως για να αντιμετωπιστούν και να ξεπεραστούν τα προβλήματα που εμφανίζονται τα συστήματα χρησιμοποιούν εξελιγμένες τεχνικές νοημοσύνης και εκμάθησης. Άρα μπορούν να προσαρμοστούν σε αλλαγές.

Τέλος η μέθοδος αυτή είναι πολύ απλή και δεν κουράζει το χρήστη γιατί το μόνο που πρέπει να κάνει είναι να σταθεί για κάποια δευτερόλεπτα όρθιος.

Δακτυλικά Αποτυπώματα

Ο κάθε άνθρωπος έχει διαφορετικό τύπο και γεωμετρία δακτυλικών αποτυπωμάτων. Η εφαρμογή των δακτυλικών αποτυπωμάτων γίνεται σε 2 στάδια:

- Στο 1° στάδιο έχουμε την οπτική ανίχνευση των δακτυλικών αποτυπωμάτων. Γίνεται από ειδικές κάμερες που υπάρχουν, οι οποίες είναι σχετικά μεγάλες. Άρα έχουμε αρχικά τη μέτρηση των χαρακτηριστικών καθώς και την αποθήκευσή τους:
  - ✓ Στο server που κάνει την συγκεκριμένη αναγνώριση.
  - ✓ Σε κάποια έξυπνη κάρτα (Smart Card) που έχει ο χρήστης στην κατοχή του.
- Στο 2° στάδιο έχουμε την επιβεβαίωση:
  - ✓ Ο χρήστης δίνει το login name.
  - ✓ Επομένως γίνεται η καταμέτρηση των χαρακτηριστικών και η επιβεβαίωση.



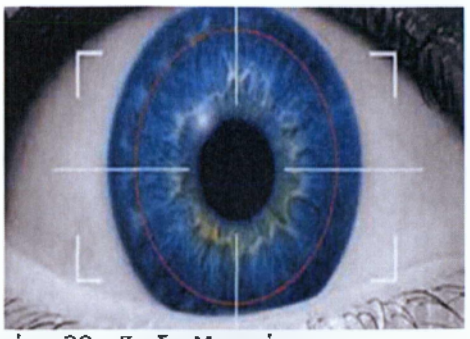
Εικόνα 28 - Δακτυλικά αποτυπώματα

Στην περίπτωση τέτοιων βιομετρικών συστημάτων υπάρχουν και κάποια μειονεκτήματα. Ένα από αυτά είναι ότι δεν μπορεί να γίνει διάκριση του πραγματικού δακτύλου αποτυπώματος από ένα αντίγραφο. Από την άλλη κάποιες αλλαγές στο δακτυλικό αποτύπωμα (τραυματισμός, κατάσταση χεριού) μπορεί να οδηγήσει στη μη σωστή επίδοση του συστήματος. Τέλος υπάρχει αντίδραση από ένα μέρος της κοινωνίας για αυτήν την τεχνική διότι συνδυάζεται η χρήση τους από τις αστυνομικές αρχές.

Ίριδα Ματιού

Η διαδικασία της εξέτασης της ίριδας του ματιού είναι απλή: Κάποια κάμερα συλλαμβάνει την εικόνα της ίριδας και στη συνέχεια τη μετατρέπει σε ένα είδος του μαθηματικού κώδικα. Σημαντική προϋπόθεση για τη σωστή λειτουργία του συστήματος είναι η εγκατάσταση σε περιβάλλον που θα έχει καλό φωτισμό ώστε η εικόνα της ίριδας να είναι καλύτερη.
Στην περίπτωση αυτή υπάρχουν δύο τεχνικές για την εξέταση της ίριδας του ματιού, η ενεργητική και η παθητική.

- Στην ενεργητική τεχνική χρειάζεται η συμμετοχή του χρήστη, ο οποίος πρέπει να εστιάσει στην κάμερα του συστήματος την ίριδα του ματιού με το να μετακινεί το κεφάλι του στην κατάλληλη θέση. Η διαδικασία αυτή μπορεί να αποσταθεροποιείσει την λειτουργία και την ευελιξία της τεχνική αυτής.
- Στην παθητική τεχνική εξέτασης της ίριδας αντί της μίας κάμερας υπάρχουν πολλές οι οποίες εστιάζουν αρχικά στο πρόσωπο, μετά στο μάτι και τέλος στην ίριδα του χρήστη, χωρίς να χρειάζεται ιδιαίτερη συμμετοχή από αυτόν.



Εικόνα 29 - Ίριδα Ματιού

Κρυπτογραφία (Cryptography)

Τόσο σε κοινωνικό όσο και σε νομικό επίπεδο, γίνεται ζήτημα προστασίας του απορρήτου σε όλες τις δικτυακές συναλλαγές (τραπεζικό απόρρητο, στρατιωτικό απόρρητο, εμπορικές συναλλαγές, e-mail) και πιο συγκεκριμένα ζήτημα προστασίας προσωπικών δεδομένων του κάθε χρήστη του Internet.

Έτσι η κρυπτογράφηση έρχεται να εξασφαλίσει το απόρρητο των προσωπικών δεδομένων και πληροφοριών. Είναι η επιστήμη που στηρίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Ο πρωτεύον στόχος της είναι να παρέχει μηχανισμούς ώστε 2 ή περισσότερα άκρα επικοινωνίας (όπως προγράμματα υπολογιστών, άνθρωποι) να ανταλλάξουν μηνύματα, χωρίς να μπορεί κανένα τρίτο άτομο να είναι ικανό να διαβάζει την πληροφορία που παρέχεται εκτός από τα δύο άκρα.

Οι τεχνικές της κρυπτογράφησης κάνουν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο σε αυτούς που έχουν το δικαίωμα της εξουσιοδότησης. Έτσι εξασφαλίζουν το απόρρητο στις ψηφιακές επικοινωνίες και στην αποθήκευση των ευαίσθητων πληροφοριών.

Οι περισσότερες μονόδρομες συναρτήσεις **(One-Way Hash Functions)** αποτελούν σημαντικά στοιχεία για την ανάπτυξη των συστημάτων κρυπτογραφίας. Οι συναρτήσεις αυτές είναι συναρτήσεις οι οποίες δέχονται ως είσοδο μια ακολουθία από κάποιους χαρακτήρες μεταβλητού μήκους και παρέχουν ένα μήνυμα σταθερού μεγέθους (μικρότερο) που ονομάζεται ως τιμή σύνοψης (Hash Value). Οι συναρτήσεις αυτές λειτουργούν μόνο σε μία κατεύθυνση: η τιμή σύνοψης μπορεί να υπολογιστεί εύκολα για κάποιο δεδομένο μήνυμα, από την άλλη είναι δύσκολο να υπολογιστεί το μήνυμα στο οποίο αντιστοιχείται μια καθορισμένη τιμή σύνοψης. Μια μονόδρομη συνάρτηση σύνοψης που είναι καλά σχεδιασμένη είναι επίσης ελεύθερη από συγκρούσεις (Collision-Free), με έννοια ότι είναι δύσκολο να εντοπιστούν δύο μηνύματα με το ίδια τιμή σύνοψης. Έτσι οι μονόδρομες συναρτήσεις χρησιμοποιούνται κυρίως για εφαρμογές επαλήθευσης. Η τιμή σύνοψης αντιπροσωπεύει το αρχικό μήνυμα. Η αλλαγή σε κάποιο τουλάχιστον bit στο αρχικό μήνυμα μπορεί να αλλάξει κατά μέσο όρο τα μισά bits της τιμής σύνοψης.

Παραδείγματα μονόδρομων συναρτήσεων σύνοψης είναι οι **MD4, MD5** και **SHA.**

Οι κώδικες πιστοποίησης μηνυμάτων **(Message Authentication Codes, MAC)** είναι μονόδρομες συναρτήσεις σύνοψης οι οποίες στηρίζονται σε μυστικό κλειδί ώστε μόνο ένας να γνωρίζει το κλειδί, το οποίο είναι το μόνο που μπορεί να επιβεβαιώσει την τιμή σύνοψης. Είναι πολύ χρήσιμη ώστε να παρέχεται η αυθεντικότητα. Μπορεί μια συνάρτηση σύνοψης να μετατραπεί σε κώδικα πιστοποίησης σε περίπτωση που η τιμή σύνοψης κρυπτογραφηθεί με ένα συμμετρικό αλγόριθμο.

Όσων αφορά τη διαχείριση του κλειδιού η οποία είναι η διαδικασία της παραγωγής, της διανομής, της επαλήθευσης, της χρησιμοποίησης, της ενημέρωσης, της αποθήκευσης και της καταστροφής των κλειδιών σε κάποιο σύστημα κρυπτογράφησης. Η ασφαλής τεχνική για τη διαχείριση των κλειδιών είναι πολύ σημαντική. Στην πραγματικότητα οι επιθέσεις σε συστήματα ασφαλείας έχουν ως στόχο τις διαδικασίες διαχείρισης των κλειδιών και όχι τους αλγόριθμους.

Οι αλγόριθμοι του δημόσιου κλειδιού κάνουν τη διαχείριση πολύ πιο εύκολη. Το ιδιωτικό κλειδί δε χρειάζεται να μεταδοθεί ποτέ. Υπάρχει ένα πρόβλημα όμως, πρέπει ο κάθε χρήστης να δ98ιαθέτει ένα δικό του ζεύγος κλειδιών. Τα συστήματα που κάνουν χρήση της ασύμμετρης κρυπτογραφίας χρειάζονται τεχνικές διανομής και επαλήθευσης κλειδιών.

Στη σύγχρονη ανάπτυξη των κρυπτοσυστημάτων ο κρυπτυναλητής θεωρείται γνωστό ότι πρέπει να γνωρίζει όλες τις λεπτομέρειες πάνω στους αλγόριθμους κρυπτογράφησης και ότι έχει απεριόριστη πρόσβαση στα κρυπτογραφικά δεδομένα.

Επιθέσεις που μπορεί να δεχθεί ένα κρυπτοσύστημα μπορεί να διαχωριστεί σε 3 είδη, ανάλογα με την πληροφορία που προσπαθεί να εκμεταλλευτεί ο κρυπταναλυτής.

- Επίθεση στο κρυπτογραφημένο κείμενο **(Attack Ciphertext)**: Στην περίπτωση αυτή ο κρυπταναλυτής ξέρει τον αλγόριθμο της κρυπτογράφησης, κάποιο μέρος του κρυπτογραφημένου κειμένου, και τη δομή του αρχικού κειμένου.
- Επίθεση στο γνωστό αρχικό κείμενο **(Attack Known Plaintext)**: Στην περίπτωση αυτή ο κρυπταναλυτής ξέρει τον αλγόριθμο κρυπτογράφησης, κατέχει το αρχικό κείμενο μαζί με το αντίστοιχο κρυπτογραφημένο κείμενο.
- Επίθεση στο επιλεγμένο αρχικό κείμενο **(Attack Choses Plaintext)**: Στην περίπτωση αυτή κρυπταναλυτής ξέρει το αλγόριθμο της κρυπτογράφησης, και έχει τη δυνατότητα να διαλέξει κάποιο αρχικό κείμενο και στη συνέχεια να δημιουργήσει το κρυπτογραφημένο κείμενο.

Οι βασικές λειτουργίες της κρυπτογραφίας είναι οι εξής:

- Εμπιστευτικότητα **(Confidentiality)**: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα άτομα που έχουν εξουσιοδότηση. Η πληροφορία θα είναι ακατανόητη σε κάποιον τρίτο άτομο.
- Ακεραιότητα **(Integrity)**: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη, όμως το μήνυμα δεν μπορεί να αλλοιωθεί από άτομο που δεν έχει εξουσιοδότηση.
- Μη απάρνηση **(Non-Repudiation)**: Όποια ενέργεια κι αν κάνει κάποιος (όπως η πιστοποίηση της ταυτότητας) είτε ο αποστολέας είτε ο παραλήπτης της πληροφορίας, δεν μπορεί αργότερα να την αρνηθεί.
- Πιστοποίηση **(Certification)**: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους, αλλά και την πηγή και τον προορισμό της πληροφορίας, με το να διαβεβαιώνουν ότι οι ταυτότητές τους δεν είναι πλαστές.

Βασικές Έννοιες στην Κρυπτογραφία

Κρυπτογράφηση **(Encryption)** ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου ώστε έτσι να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.

Ο Αλγόριθμος Κρυπτογράφησης **(Cipher)** είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Έτσι όσο αυξάνεται ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο ελαχιστοποιείται η πιθανότητα να τον προσπελάσει κάποιος. Επομένως ο αλγόριθμος της κρυπτογράφησης λειτουργεί με ένα κλειδί **(Key)**, για την κρυπτογράφηση του απλού κειμένου. Όταν όμως χρησιμοποιούνται 2 διαφορετικά κλειδιά το απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα.

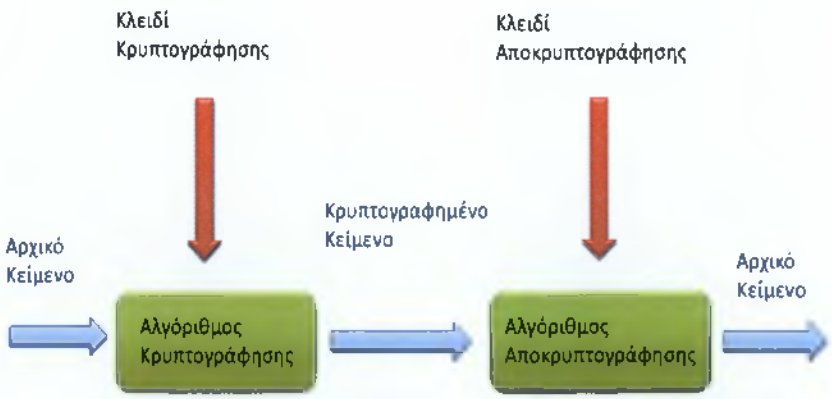
Αρχικό Κείμενο ονομάζεται **(Plaintext)** είναι το μήνυμα που το οποίο αποτελεί την είσοδο σε κάποια διεργασία κρυπτογράφησης.

Το Κλειδί **(Key)** είναι κάποιος αριθμός αρκετών bit ο οποίος χρησιμεύει ως είσοδο στη συνάρτηση κρυπτογράφησης.

Το Κρυπτογραφημένο Κείμενο **(Ciphertext)** είναι το μήνυμα που προκύπτει μετά την κρυπτογράφηση του απλού κειμένου.

Η Αποκρυπτογράφηση **(Decrypt)** είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου.

Η Κρυπτανάλυση **(Cryptanalysis)** είναι η επιστήμη που ασχολείται με το σπάσιμο μιας κρυπτογραφικής μεθόδου, χωρίς όμως να είναι γνωστό το κλειδί κρυπτογράφησης.[22]



Εικόνα 30 - Τυπικό Σύστημα Κρυπτογράφησης – Αποκρυπτογράφησης

Συμμετρική Κρυπτογραφία (*Symmetric Cryptography*)

Στη Συμμετρική Κρυπτογραφία **(Symmetric Cryptography)** χρησιμοποιείται κατά την διαδικασία της κρυπτογράφησης – αποκρυπτογράφησης ένα κοινό κλειδί. Στις περισσότερες περιπτώσεις τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι τα ίδια. Στη συμμετρική κρυπτογραφία απαιτείται η ανταλλαγή του κλειδιού μέσα από ένα κανάλι επικοινωνίας ή μέσα από τη φυσική παρουσία των προσώπων. Αυτοί οι αλγόριθμοι χρειάζονται τη συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί, για να μπορέσουν να επικοινωνήσουν με ασφάλεια. Άρα η ασφάλεια των αλγορίθμων βασίζεται στη μυστικότητα του κλειδιού. Σε κάθε περίπτωση που επιθυμούμε η επικοινωνία να παραμείνει μυστική, πρέπει και το κλειδί να παραμείνει μυστικό.

Οι συμμετρικοί αλγόριθμοι μπορούν να χωριστούν σε δύο υποκατηγορίες:

- ✓ Οι Αλγόριθμοι Ροής **(Stream Ciphers)** οι οποίοι κρυπτογραφούν μια ροή μηνύματος χωρίς να τη διαχωρίζουν σε τμήματα (οι αλγόριθμοι ροής λειτουργούν bit προς bit).
- ✓ Οι Αλγόριθμοι Δέσμης **(Block Ciphers)** οι οποίοι λειτουργούν πάνω σε κομμάτια δεδομένων και κρυπτογραφούν κάθε κομμάτι ξεχωριστά (συνήθως των 64 bit).

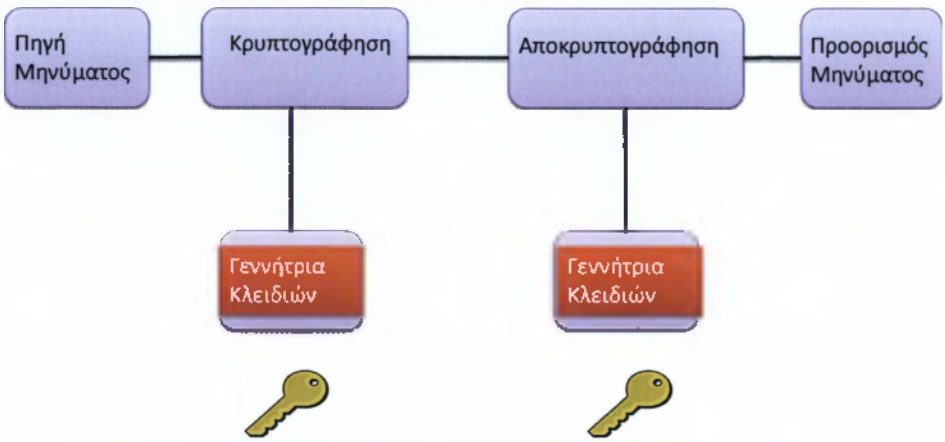
Παραδείγματα Συμμετρικών Αλγορίθμων είναι οι: **DES, IDEA, RC5** και **SAFER.**

Η συμμετρική κρυπτογραφία παρέχει πολύ γρήγορο ρυθμό ως προς την εκτέλεση των αλγορίθμων. Επομένως είναι σε θέση να εγγυηθεί για την εμπιστευτικότητα των επικοινωνιών, χωρίς να προκαλεί με επιβάρυνση τη διαθεσιμότητα του συστήματος. Αυτά είναι και τα πλεονεκτήματά της. Από την άλλη όμως μεριά έχει και κάποια μειονεκτήματα:

- Το σημαντικότερο πρόβλημα είναι η διαχείριση και διανομή των απαιτούμενων κλειδιών. Σε μια επικοινωνία δύο μερών με συναλλασσόμενα μέρη, πρέπει να χρησιμοποιήσουν ένα ασφαλές κανάλι για τον προσδιορισμό του κλειδιού πριν αρχίσουν οι διαδικασίες αποστολής και λήψης των μηνυμάτων.
- Σε μεγάλα κυρίως δίκτυα, όπου διαπιστώνεται ότι ο αριθμός των κλειδιών που διακινούνται αυξάνονται λόγων το αριθμό των χρηστών, αλλά και επειδή τα κλειδιά αλλάζουν συχνά για να παραμείνει ο υψηλός βαθμός της ασφάλειας. Αυτό έχει ως συνέπεια τα κλειδιά να έχουν ισχύ μόνο για μια επικοινωνία. Τα συστήματα ασφαλούς τρόπους ανταλλαγής κλειδιών όπως το σύστημα Kerberos που

αναφερθήκαμε παραπάνω, δεν είναι σε θέση να επεκταθούν για την εξυπηρέτηση του μεγάλου όγκου χρηστών και έχει ως αποτέλεσμα να χρειάζονται επιπλέον διαδικασίες ασφάλειας.

- Εκτός από την εμπιστευτικότητα των μηνυμάτων, υπάρχουν και επιπλέον απαιτήσεις ασφαλείας κυρίως στα μεγάλα δίκτυα, όπως το Internet, για τις οποίες η συμμετρική κρυπτογραφία δεν προσφέρει κάποιες λύσεις. Όπως αναφερθήκαμε και παραπάνω στις βασικές λειτουργίες της κρυπτογραφίας η Εμπιστευτικότητα **(Confidentiality)**, η Ακεραιότητα **(Integrity)** και η Μη απάρνηση **(Non-Repudiation)** η πρόσφατη κρυπτογραφία δημόσιου κλειδιού μπορεί να προσφέρει κάποιες ικανοποιητικές διεξόδους.



Εικόνα 31 - Μοντέλο Συμμετρικής Κρυπτογραφίας

Ασύμμετρη Κρυπτογραφία (*Asymmetric Cryptography*)

Η Ασύμμετρη Κρυπτογραφία **(Asymmetrical Cryptography)** ή κρυπτογραφία δημόσιου κλειδιού αναπτύχθηκε για να καλύψει την αδυναμία της μεταφοράς των κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Το βασικό χαρακτηριστικό είναι ότι χρησιμοποιούνται 2 ζεύγη κλειδιών 1 Δημόσιο **(Public)** και 1 Ιδιωτικό **(Private)**. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό **(Secret)**. Το βασικό στοιχείο είναι ότι κρυπτογραφεί το ένα και αποκρυπτογραφεί μόνο με το άλλο. Ο καθένας μπορεί να κρυπτογραφήσει ένα μήνυμα με το δημόσιο κλειδί αλλά μόνο αυτός που κατέχει το αντίστοιχο ιδιωτικό κλειδί μπορεί να το αποκρυπτογραφήσει. Οι δυνατότητες στην ασύμμετρη κρυπτογραφία οδήγησαν στην δημιουργία των Ψηφιακών Υπογραφών **(Digital Signatures)** και συνέχεια στην ανάπτυξη της Υποδομής του Δημόσιου Κλειδιού **(Public Key Infrastructure)** και τέλος στα Ψηφιακά Πιστοποιητικά **(Digital Certificates)**.

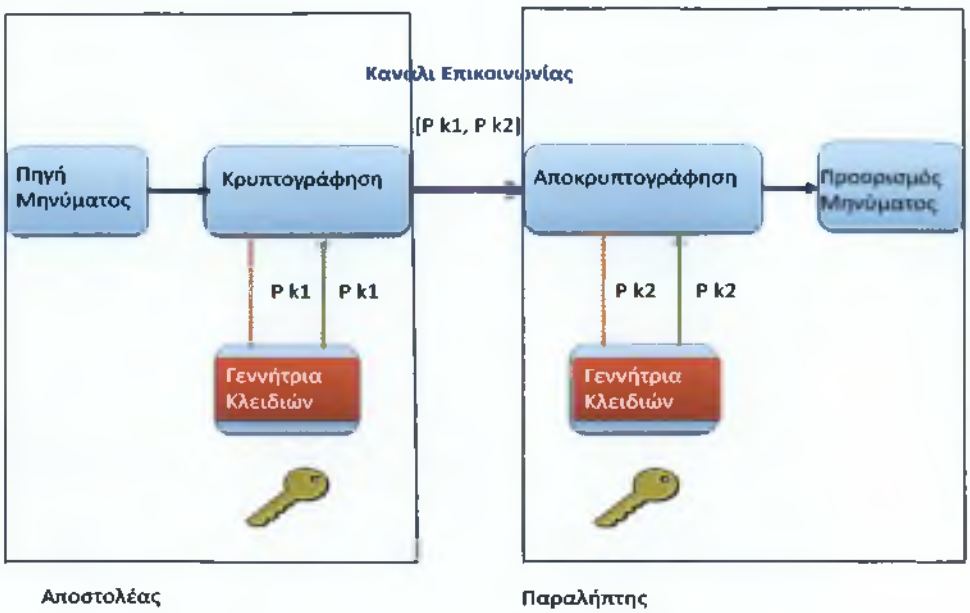
Παραδείγματα Ασύμμετρων Αλγορίθμων είναι οι: **RSA, ElGamal** και **DSA**.

Η ασύμμετρη κρυπτογραφία αποτελεί τεχνολογικά το βασικό στοιχείο σε μηχανισμούς και ασφαλείας στο Internet όπως:

- ✓ Οι Υποδομές Πιστοποίησης **(Infrastructure Certification)** οι οποίες διαχειρίζονται σε ψηφιακά πιστοποιητικά από έμπιστους τρίτους φορείς, με στόχο την αναγνώριση και την πιστοποίηση της ταυτότητας των χρηστών καθώς και τον έλεγχο των εξουσιοδοτήσεών τους.
- ✓ Η Ασφαλής Παρουσίαση **(Secure Presentation)** των ιστοσελίδων καθώς και των αγορών μέσω διαδικτύου, με βάσει το πρωτόκολλο SSL **(Secure Sockets Layer)** καθώς και του πρωτόκολλου TLS **(Transport Layer Security)**.[15]

[15] Το πρωτόκολλο SSL **(Secure Sockets Layer)** αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε την βάση για

- ✓ Οι Ασφαλείς Συναλλαγές **(Secure Transactions)** μέσω των πιστωτικών καρτών με βάση του πρωτοκόλλου SET **(Secure Electronic Transactions)** για τις πιστωτικές κάρτες Visa και Mastercard.[16]
- ✓ Η Ασφαλής Ηλεκτρονική Αλληλογραφία **(Secure Electronic Mail)** με βάση του πρωτοκόλλου S/MIME **(Secure/Multipurpose Internet Mail Extensions).**[17]



Εικόνα 32 - Μοντέλο Ασύμμετρης Κρυπτογραφίας

Ψηφιακές Υπογραφές (*Digital Signatures*)

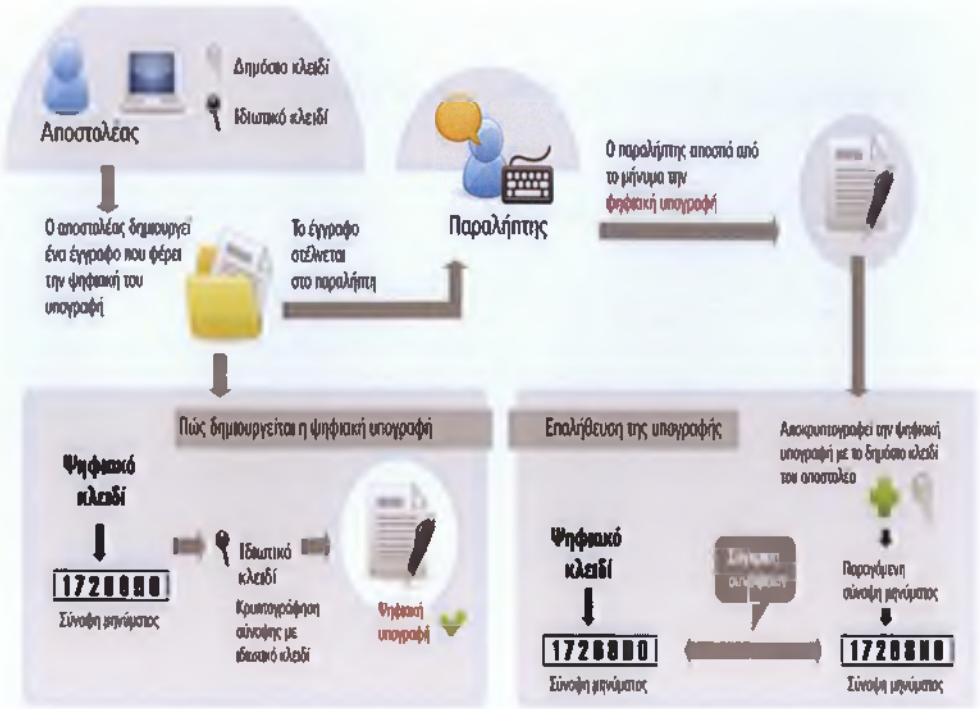
Η Ψηφιακή Υπογραφή **(Digital Signatures)** είναι ένα μαθηματικό σύστημα που χρησιμοποιείται ως απόδειξη τη γνησιότητα ενός ψηφιακού μηνύματος ή εγγράφου. Με την έγκυρη ψηφιακή υπογραφή παρέχεται στον παραλήπτη η πιστοποίηση ότι το μήνυμα είναι αυθεντικό το οποίο δημιούργησε ο αποστολέας και το υπέγραψε ψηφιακά καθώς και ότι δεν αλλοιώθηκε κατά την μεταφορά του. Για τη δημιουργία και την επαλήθευση των ψηφιακών υπογραφών χρησιμοποιείται η κρυπτογράφηση του δημόσιου κλειδιού. Το ιδιωτικό κλειδί χρησιμοποιείται για την δημιουργία και το δημόσιο κλειδί για την επαλήθευση της υπογραφής.

Επομένως οι ψηφιακές υπογραφές χρησιμοποιούνται για τους μηχανισμούς γνησιότητας ή της αυθεντικοποίησης αυτών που επικοινωνούν (Entity Authentication) μεταξύ τους, για την επαλήθευση της ταυτότητας προέλευσης των δεδομένων (Data Origin Authentication), την ακεραιότητα των δεδομένων (Data Integrity), καθώς και σε υπηρεσίες μη αμφισβήτησης (Non – Repudiation) για την αποστολή και λήψη των μηνυμάτων, καθώς και την δημιουργία ή την τροποποίησή τους.[21,22]

την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security), το οποίο πλέον τείνει να αντικαταστήσει το SSL.

[16] Το πρωτόκολλο SET **(Secure Electronic Transactions)** είναι ένα πρωτόκολλο επικοινωνιών για να
εξασφαλίσει με ασφαλή τρόπο τις συναλλαγές πιστωτικών καρτών μέσω δικτύων.

[17] Το πρωτόκολλο S/MIME **(Secure/Multipurpose Internet Mail Extensions)** είναι ένα πρότυπο δημόσιου κλειδιού κρυπτογράφησης και υπογραφή δεδομένων για την ασφαλή ηλεκτρονική αλληλογραφία.

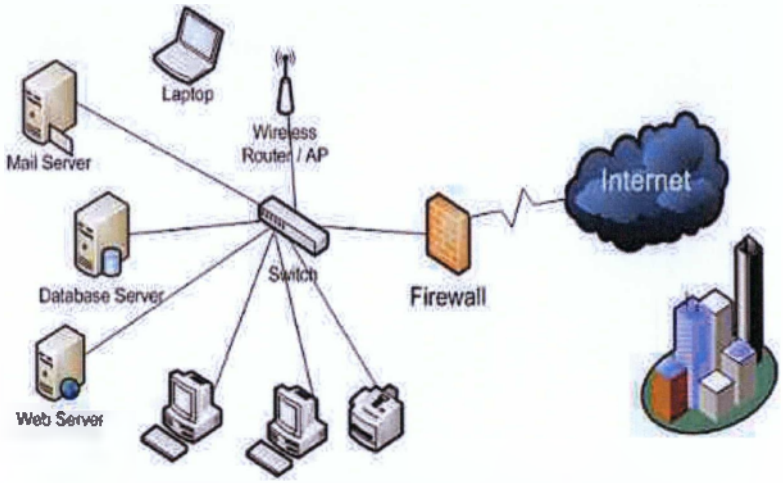


Εικόνα 33 - Απεικόνιση Ψηφιακής Υπογραφής

Κεφάλαιο 6-Ασφάλεια Δικτύου

Έννοια Ασφάλειας Δικτύου

Η έννοια της Ασφάλειας Δικτύου **(Network Security)** έχει σχέση με την ικανότητα ενός οργανισμού να προστατεύει τις πληροφορίες του από πιθανές αλλοιώσεις και καταστροφές, καθώς και τη χρήση των πόρων του από μη εξουσιοδοτημένα άτομα. Ακόμα θεωρείται ως η δυνατότητα του δικτύου ή του συστήματος των πληροφοριών να αντισταθεί, να βρίσκεται σε επίπεδο αξιοπιστίας (Level Of Reliability), σε κάποια τυχαία συμβάντα (Random Events) ή από κάποιες κακόβουλες ενέργειες (Malicious Actions) που καθιστούν σε κίνδυνο τη διάθεση, την ακεραιότητα (Integrity), την επαλήθευση της ταυτότητας (Authentication), καθώς και την τήρηση του απορρήτου των δεδομένων (Confidentiality Of Data), τα οποία έχουν αποθηκευτεί ή μεταδοθεί και τις αντίστοιχες υπηρεσίες που παρέχονται ή είναι προσβάσιμες διαμέσου των δικτύων και συστημάτων αυτών.



Εικόνα 34 - Απεικόνιση Ασφάλειας Δικτύου

Στην εποχή μας και κυρίως λόγω της ανάπτυξης και της εξάπλωσης των τεχνολογιών και υπηρεσιών Web, οι πληροφοριακοί κίνδυνοι κατά της ασφάλειας Η/Υ και των δικτύων αυξάνονται συνεχώς. Άρα την ασφάλεια τη χρειαζόμαστε για τους παρακάτω λόγους:

- Το Κακόβουλο Λογισμικό **(Malicious Software)**, όπως οι Ιοί (Viruses), τα Σκουλήκια (Worms)[18], οι Δούρειοι Ίπποι (Trojan Horses),[19] Spyware[20], Adware[21], με στόχο τη μη εξουσιοδοτημένη πρόσβαση στους πόρους ενός Η/Υ.

---

[18] Ένα σκουλήκι υπολογιστή **(Computer Worm)** είναι ένα αυτοαναπαραγόμενο και κακόβουλο πρόγραμμα υπολογιστή, το οποίο χρησιμοποιεί δίκτυο υπολογιστών για να στείλει αντίγραφα του εαυτού του σε άλλους κόμβους (υπολογιστές του δικτύου) και μπορεί να το πράξει χωρίς την παρέμβαση του χρήστη.

[19] Στην ο δούρειος ίππος **(Trojan Horse ή απλά Trojan)** είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα

[20] Με τον όρο Spyware **(Λογισμικό Κατασκοπίας)** αναφερόμαστε σε ένα είδος κακόβουλου λογισμικό το οποίο φορτώνεται κρυφά σε έναν υπολογιστή χωρίς να το ξέρει ο χρήστης και εκτελείται στο παρασκήνιο κάνοντας διάφορα πράγματα πίσω από την πλάτη του χρήστη.

[21] **Adware** ή διαφήμιση που υποστηρίζεται από το λογισμικό είναι οποιοδήποτε πακέτο λογισμικού που καθιστά αυτόματα τις διαφημίσεις. Ο όρος μερικές φορές χρησιμοποιείται για να αναφέρεται σε λογισμικό που εμφανίζει ανεπιθύμητες διαφημίσεις.

- Οι Επιθέσεις Άρνησης Εξυπηρέτησης **(Denial Of Service)**. Η διακοπή ή και η υποβάθμιση των παρεχομένων υπηρεσιών ενός συστήματος.
- Η Μη Εξουσιοδοτημένη Εισβολή **(Authorized Invasion)** σε υπολογιστικά και πληροφοριακά συστήματα (Hacking). Χρήση κακόβουλου λογισμικού με στόχο την εκμετάλλευση των αδυναμιών και την πρόσβαση στους πόρους του συστήματος.
- Η Παραβίαση Δικαιωμάτων Πνευματικής Ιδιοκτησίας **(Violation of Rights of Intellectual Property)**. Η Αντιγραφή, η αναπαραγωγή, παραποίηση καθώς και η αναδιανομή των δεδομένων και πληροφοριών που προστατεύονται από τους νόμους ως προς την πνευματική τους ιδιοκτησίας, χωρίς τη συναίνεση του δημιουργού τους.
- Οι Υποκλοπές των Επικοινωνιών **(Intercepting Communications)** και η Αλλοίωση των Δεδομένων **(Alteration of Data)**. Οι επιθέσεις στην εμπιστευτικότητα (Confidentiality) και την ακεραιότητα (Integrity) των δεδομένων και των πληροφοριών τα οποία είναι αποθηκευμένα ή ανταλλάσσονται μεταξύ δύο ηλεκτρονικών διατάξεων.
- Οι Επιθέσεις Πλαστοπροσωπίας **(Spoofing / Masquerading).** Χρήση «πλαστής» ταυτότητας με στόχο τη μη ανίχνευση του επιτιθέμενου, καθώς και την παράκαμψη των τεχνικών ελέγχου πρόσβασης του συστήματος.
- Η Μη Ζητηθείσα Επικοινωνία **(Spam)**. Τα μηνύματα ηλεκτρονικής αλληλογραφίας που αποστέλλονται χωρίς τη συναίνεση του παραλήπτη, ενώ συχνά η ταυτότητα είναι πλαστογραφημένη του αποστολέα ή απλά είναι αδύνατον να εντοπιστεί.

Τεχνολογίες Ανίχνευσης και Αντιμετώπισης Εισβολών Συστημάτων (*Technologies Intrusion Detection and Prevention Systems* - IDPS)

Εισαγωγή

Οι Τεχνολογίες Ανίχνευσης και Αντιμετώπισης Εισβολής Συστημάτων **(Technologies Intrusion Detection and Prevention Systems - IDPS)** είναι η διαδικασία παρακολούθησης των γεγονότων που προκύπτουν σε ένα σύστημα ηλεκτρονικού υπολογιστή ή ενός δικτύου καθώς και της ανάλυσή τους για τα σημάδια των πιθανών περιστατικών, που είναι παραβιάσεις των πολιτικών ασφαλείας των υπολογιστών, τις πολιτικές αποδεκτής χρήσης ή τις τυποποιημένες πρακτικές ασφαλείας. Κάποια περαστικά είναι το κακόβουλο λογισμικό (όπως worms, spyware), κάποιοι εισβολείς που προσπαθούν να αποκτήσουν πρόσβαση μη εξουσιοδοτημένη σε κάποια συστήματα μέσω του διαδικτύου καθώς και εξουσιοδοτημένοι χρήστες που κάνουν κατάχρηση των προνομιών ή προσπαθούν να αποκτήσουν περισσότερα προνόμια για τους οποίους δεν επιτρέπετε. Εκτός από κάποια περαστικά που έχουν τη μορφή κακόβουλου χαρακτήρα υπάρχουν και κάποια άτομα τα οποία μπορούν να εισάγουν λανθασμένα κάποια διεύθυνση του υπολογιστή και στη συνέχεια αυτό να συνδεθεί σε κάποιο διαφορετικό σύστημα χωρίς να υπάρχει η επιτρεπτή άδεια.

Επομένως ένα Σύστημα Ανίχνευσης Εισβολής **(Intrusion Detection System – IDS)** είναι είδος λογισμικού που αυτοματοποιεί τις διαδικασίες ανίχνευσης εισβολών. Ένα Σύστημα Αποτροπής Εισβολών – IPS) είναι λογισμικό που έχει όλες τις δυνατότητες ενός συστήματος ανίχνευσης εισβολών καθώς μπορεί να σταματήσει τα ενδεχόμενα συμβάντα που θα προκύψουν.

Εικόνα 35 - Απεικόνιση Συστήματος IDPS

Χρήση των Συστημάτων Ανίχνευσης και Πρόληψης (IDPS)

Τα συστήματα **IDPSs** στοχεύουν κυρίως στον εντοπισμό των πιθανών συμβάντων. Για παράδειγμα ένα IDPS θα μπορούσε να ανιχνεύσει έναν επιτιθέμενο ο οποίος έχει εισβάλει επιτυχώς στο σύστημα με την εκμετάλλευση μιας ευπάθειας του συστήματος. Το IDPS θα μπορούσε απευθείας να παρουσιάσει το συμβάν στους διοικητές ασφάλειας του οργανισμού, οι οποίοι με τη σειρά τους θα μπορούσαν γρήγορα να αρχίσουν τις σχετικές ενέργειες και να ελαχιστοποιήσουν την ζημιά που προκλήθηκε από το συμβάν. Επιπλέον το IDPS θα μπορούσε να καταγράψει τις πληροφορίες που χρησιμοποιούνται από τους συναφείς χειριστές. Πολλά IDPSs μπορούν να διαμορφωθούν έτσι ώστε να αναγνωρίζουν τις παραβιάσεις των πολιτικών ασφαλείας.

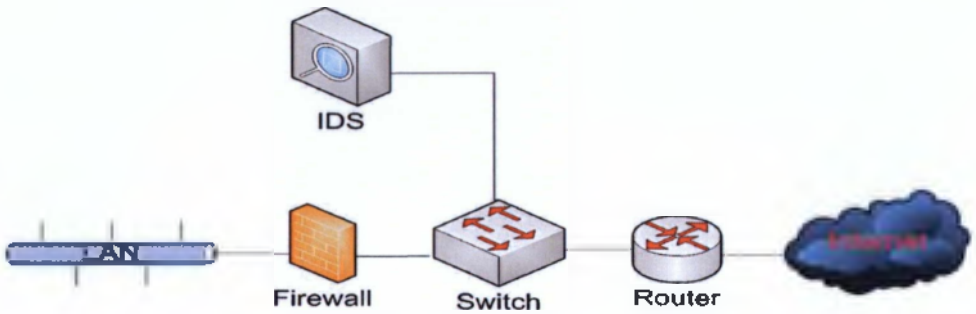
Για παράδειγμα ένα IDPS μπορεί να κάνει τον έλεγχο της μεταφοράς των αρχείων και να εντοπίσει αυτούς που έχουν ύποπτη κίνηση, όπως με την αντιγραφή μεγάλης βάσης δεδομένων στον υπολογιστή ενός χρήστη.

Επίσης το IDPS μπορεί να προσδιορίσει τη δραστηριότητα της αναγνώρισης, η οποία μπορεί να δείξει ποια επίθεση είναι αναμενόμενη.Ένα IDPS βρίσκεται σε θέση να παρεμποδίσει την αναγνώριση και να ειδοποιήσει τους διοικητές ασφαλείας, οι οποίοι στη συνέχεια μπορούν να λάβουν μέτρα εάν είναι απαραίτητο και να αλλάξουν την ασφάλεια ελέγχου για να αποτρέψουν τα συμβάντα. Τα IDPSs εκτός από τη χρήση τους για τον καθορισμό των γεγονότων και την υποστήριξη των σχετικών προσπαθειών αντιμετώπισης των συμβάντων, οι οργανισμοί έχουν εντοπίσει και άλλες χρήσεις για τα IDPSs, τα οποία συμπεριλαμβάνουν τα παρακάτω:

- Ο Προσδιορισμός των Πολιτικών Προβλημάτων Ασφάλειας **(Identifying Security Policy Problems)**: Ένα IDPS έχει τη δυνατότητα να παρέχει κάποιο βαθμό ποιοτικού ελέγχου για την πολιτική εφαρμογή της ασφάλειας, όπως η αναπαραγωγή των αναχωμάτων ασφαλείας (Firewalls) ενός συνόλου κανόνων και να προειδοποιεί όταν βλέπει κίνηση δικτύου που θα έπρεπε να έχει αποκλειστεί από τα αναχώματα ασφαλείας (Firewalls).
- Η Τεκμηρίωση της Υπάρχουσας Απειλής σε έναν Οργανισμό **(Documenting the Existing Threat to an Organization)**: Τα IDPSs κάνουν καταγραφή των πληροφοριών σχετικά με τις απειλές που ανιχνεύουν. Γνωρίζοντας τη συχνότητα και τα χαρακτηριστικά των επιθέσεων κατά των υπολογιστικών πόρων που κάποιος οργανισμός χρησιμεύει για τον εντοπισμό των κατάλληλων μέτρων ασφαλείας για την προστασία των πόρων. Επιπλέον οι πληροφορίες μπορεί να χρησιμοποιηθούν για την εκπαίδευση τη διαχείρισης των απειλών από τα πρόσωπα του οργανισμού.
- Η Αποτροπή των Ατόμων από την Παραβίαση των Πολιτικών Ασφάλειας (**Deterring Individuals from Violating Security Policies)**: Αν τα άτομα έχουν την επίγνωση ότι οι δικές τους ενέργειες παρακολουθούνται εσωτερικά από τεχνολογίες για τις παραβιάσεις των πολιτικών ασφαλείας, είναι πιθανόν να προσπαθήσουν να διαπράξουν τέτοιου είδους παραβιάσεις.
- Έτσι λόγω της αύξησης της εξάρτησης από τα συστήματα πληροφοριών και τις πιθανές επιπτώσεις των πιθανών εισβολών έναντι των συστημάτων αυτών, τα IDPSs είναι απαραίτητα για την υποδομή ασφαλείας σε κάθε οργανισμό.

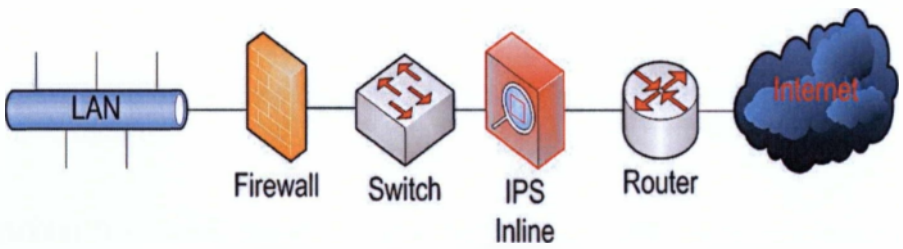
Αρχιτεκτονικές IPS και IDS

Τα **NIDS** έχουν τουλάχιστον 1 κάρτα δικτύου η οποία συνδέεται σε ένα switch και «ακούει» (υποκλέπτει μέσω ενός sniffer)[22] την κίνηση στο υπόλοιπο δίκτυο προσπαθώντας να εντοπίσει τις πιθανές επιθέσεις.



Εικόνα 36 - Αρχιτεκτονική Απεικόνιση IDS

Τα **IPS** τοποθετούνται ανάμεσα σε δύο δίκτυα (Inline). Η διαφορά είναι ότι αν εντοπίσει κάποιο κακόβουλο πακέτο έχει τη δυνατότητα να αποτρέψει την είσοδό του.



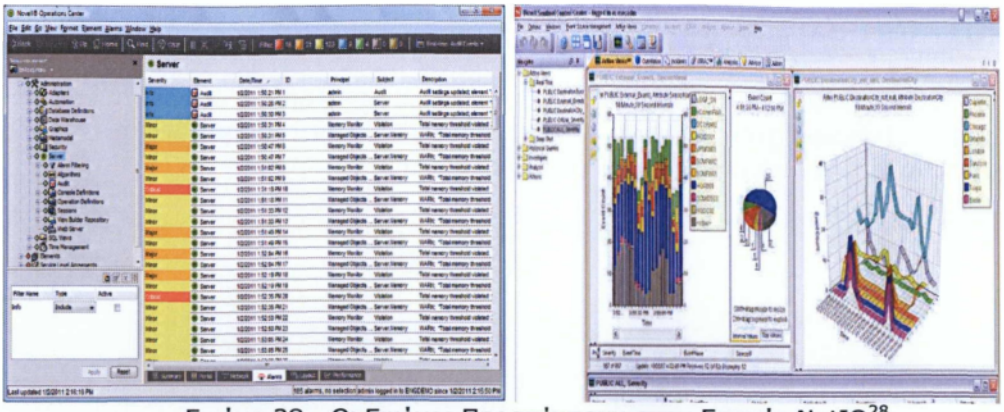
Εικόνα 37 - Αρχιτεκτονική Απεικόνιση IPS

Παρακολούθηση και Διαχείριση Συστημάτων IDPSs

- ✓ Η παρακολούθηση και η διαχείριση μπορεί να γίνει με διάφορες τεχνικές (WEB GUI[23], Special Software).
- ✓ Επιπλέον συνήθως απαιτείται εξειδικευμένο σύστημα συγκέντρωσης και ανάλυσης των γεγονότων που ανιχνεύονται (σημαντικές απαιτήσεις σε Storage (αποθήκευση), CPU, RAM).

[22] Το Sniffer ή και αποκαλούμενο **Network Monitor** ή **Network Analyzer**, είναι λογισμικό με δυνατότητα παρακολούθησης των πακέτων ενός δικτύου. Όταν γίνει αντιληπτό κάποιο πακέτο το οποίο ικανοποιεί συγκεκριμένα κριτήρια, καταγράφεται σε ένα αρχείο.

[23] Το **Web GUI** είναι ένα ανοικτό σύστημα (Open Source) διαχείρισης περιεχομένου πηγής που γράφεται σε Perl (γλώσσα προγραμματισμού) και που εκδίδεται με άδεια ευρέος κοινού GNU (General Public License).



Εικόνα 38 - Οι Εικόνες Παραπέμπουν στην Εταιρία NetIQ[28]

Στα Συστήματα Ανίχνευσης και Πρόληψης (IDPS) μπορεί να προκύψουν και κάποια προβλήματα:

- Πιθανόν να προκύψουν πολλοί ψεύτικοι συναγερμοί **(False Alarms)**.
- Πρέπει να ρυθμιστεί σωστά από την αρχή έτσι ώστε να παρουσιάζει μια σωστή λειτουργία.
- Οπωσδήποτε πρέπει κάποιος να ασχολείται μαζί του, σε περίπτωση πιθανής εισβολής να αντιλαμβάνεται το συναγερμό.
- Σε περίπτωση που υπάρχουν ψεύτικοι συναγερμοί (για ακόμα μια φορά), αν είναι πολλοί τότε:
  - ✓ Εάν είναι Σύστημα Αποτροπής Εισβολών – IPS ή αν έχει ρυθμιστεί ώστε να αντιδρά σε επιθέσεις τότε:
    - ➢ Μπορεί κατά λάθος (ψεύτικου συναγερμού) να σταματήσει τη νόμιμη κυκλοφορία.
  - ✓ Εάν είναι επί γραμμής (Inline) σε ενδεχόμενο κάποιας αστοχίας του υλικού διακόπτει το δίκτυο.

Τεχνολογίες για Προστασία κατά των Ιών (Antivirus)

Εισαγωγή

Τα Αντιικά Συστήματα **(Antivirus)**, είναι λογισμικά υπολογιστών που χρησιμεύουν για την πρόληψη (Prevention), τον εντοπισμό (Localisation) και την αφαίρεση κακόβουλων ιών (Remove Malicious Viruses) των υπολογιστών. Το μεγαλύτερο ποσοστό των προγραμμάτων αυτών των λογισμικών, λειτουργεί ενάντια σε άλλους τύπους malware, όπως για παράδειγμα το κακόβουλα αντικείμενα βοήθειας του προγράμματος περιήγησης (BHOs)[24],Πίσω Πόρτες (Backdoors), Δούρειοι Ίπποι (Trojan Horses), τα Σκουλήκια (Worms), Adware και Spyware. Επομένως η ασφάλεια του υπολογιστή, συμπεριλαμβάνοντας και την προστασία από τις κοινωνικές μηχανές, συνήθως προσφέρονται σε υπηρεσίες και προϊόντα μέσω των εταιριών λογισμικού προστασίας από ιούς.

Κάποια λογισμικά κατά των ιών (Antivirus) είναι τα παρακάτω:

[24] Πρόγραμμα περιήγησης ή **BHOs** , είναι εφαρμογές που μπορούν να προσθέσουν ειδικά χαρακτηριστικά για web browsers . Αυτή η κατηγορία περιλαμβάνει το λογισμικό εργαλείων και spyware blockers , αλλά μπορεί επίσης να παραπέμπει σε ανεπιθύμητα προγράμματα που μπορούν να στραφούν τα αποτελέσματα της αναζήτησης σας , να κλέψουν πληροφορίες ή σας παρενοχλεί ανεπιθύμητες διαφημίσεις.

- Avast Antivirus
- AVG
- McAfee
- Panta Antivirus
- Norton Antivirus
- Kaspersky
- Eset Antivirus
- Avira Antivirus

Η Χρήση των Λογισμικών κατά των Ιών (Antivirus)

Ένα λογισμικό κατά των ιών **(Antivirus)** ελέγχει το σύστημα αν περιέχει μολυσμένα αρχεία, κάποιο άλλο καθαρίζει τον ιό από τον σκληρό δίσκο. Μερικές φορές τα προγράμματα έχουν την δυνατότητα να καθαρίσουν τον ιό χωρίς να χρειαστεί να διαγράψουν τα μολυσμένα αρχεία δεδομένων ή τα μολυσμένα προγράμματα, ενώ κάποιες άλλες φορές τα μολυσμένα αρχεία πρέπει να διαγραφούν. Ακόμα υπάρχει και μια άλλη κατηγορία προγραμμάτων που δεν επιτρέπουν την εκτέλεση ενός μολυσμένου προγράμματος αποτρέποντας τη μόλυνση του συστήματός σας. Επιπλέον μεγαλύτερες εταιρίες καταπολέμησης ιών παρέχουν πακέτα προγραμμάτων της μορφής όλα σε ένα και δεν είναι απαραίτητο να γίνεται ξεχωριστή προμήθεια και εγκατάσταση για το κάθε πρόγραμμα.

Επομένως η λειτουργίας τους καθορίζεται ως εξής:

- Στους Σταθμούς Εργασίας **(Host Antivirus)** – Επιπλέων εξιδανικευμένες εκδόσεις και για Server (Mail, Web).
- Ανιχνεύουν και σταματούν τους ιούς και κάθε άλλο κακόβουλο λογισμικό (πίσω πόρτες (Backdoors), Δούρειοι Ίπποι (Trojan Horses), τα Σκουλήκια (Worms), Adware και Spyware).

- Με τρόπους ανίχνευσης:

  - ✓ Με τις υπογραφές **(Virus Signature Definitions)**.
  - ✓ Με τη συμπεριφορά **(Behavor)**.

- Κάποια πιθανά προβλήματα:

  ✓Πολλές φορές απενεργοποιείται από τους χρήστες, λόγω της επιβράδυνσης του υπολογιστή

  ✓Δεν ενημερώνεται από τους χρήστες πολλές φορές με αποτέλεσμα να μην παρέχει την απαιτούμενη προστασία.

  ✓Επιπλέον δεν εντοπίζουν πάντα άγνωστους ιούς (εδώ αναφέρονται νέοι ιοί που δεν έχουν οριστεί ακόμα).

- Στο επίπεδο του δικτύου:

  ✓ Τοποθετούνται μεταξύ των δικτύων (έτσι γίνεται με τα αναχώματα ασφαλείας – Firewalls) και τις περισσότερες φορές μεταξύ του Internet και του εσωτερικού δικτύου.

  ✓ Επιπλέον επιθεωρούν συγκεκριμένα πρωτόκολλα μεταφοράς αρχείων (HTTPS[25], POP3[26], FTP[27]).

---

[25] Το HTTPS **(Hypertext Transfer Protocol Secure)** χρησιμοποιείται στην πληροφορική για να δηλώσει μία ασφαλή δικτυακή σύνδεση http.

[26] Το POP **(Post Office Protocol)** επίσης γνωστό και ως **POP3** είναι ένα πρωτόκολλο που χρησιμοποιείται για την παραλαβή των ηλεκτρονικών μηνυμάτων (email) από έναν απομακρυσμένο εξυπηρετητή (server) χρησιμοποιώντας σύνδεση TCP/IP.

- Ανιχνεύουν και σταματούν τους ιούς και κάθε άλλο κακόβουλο λογισμικό όπως και στους σταθμούς εργασίας (Host Antivirus),{(Πίσω Πόρτες (Backdoors), Δούρειοι Ίπποι (Trojan Horses), τα Σκουλήκια (Worms), Adware και Spyware)}.

- Κάποια πιθανά προβλήματα:
  - ✓ Δεν ανιχνεύουν το κακόβουλο λογισμικό στα κρυπτογραφημένα κανάλια (SSH).[28]
  - ✓ Δεν μπορούν να ανιχνεύσουν κακόβουλο λογισμικό σε άγνωστα σε αυτά πρωτόκολλα (P2P).[29]
  - ✓ Έχουν την δυνατότητα να προστατεύουν περιμετρικά. Σε περίπτωση που κάποιος χρήστης πάρει το laptop στον σπίτι του και κολλήσει κάποιον ιό μπορεί να τον φέρει στο γραφείο χωρίς να ελεχθεί αυτό.

Τεχνολογίες Ελέγχου Περιεχομένου (*Content Control Technologies)*

Το Λογισμικό Ελέγχου του Περιεχομένου (**Content-control software)**, το Λογισμικό Φιλτραρίσματος Περιεχομένου **(Content Filtering Software)**, οι Ασφαλείς Πύλες στο Διαδίκτυο (Secure Web Gateways), η Ασφάλεια Περιεχομένου και Ελέγχου (Content Security and Control), το Λογισμικό Φιλτραρίσματος Web (Web Filtering Software), το Περιεχόμενο Λογοκρισία Λογισμικού (Content-Censoring Software), και το Λογισμικό Περιεχομένου Αποκλεισμού (Content-Blocking Software) είναι όροι που προσδιορίζουν το λογισμικό που έχει σχεδιαστεί να περιορίσει ή να ελέγξει το περιεχόμενο που ένας αναγνώστης εξουσιοδοτείται για να έχει πρόσβαση, όταν ειδικότερα χρησιμοποιείται για να περιορίσει το υλικό που παρέχεται μέσω του διαδικτύου μέσω Web, E-mail κτλ. Το Λογισμικό Ελέγχου του Περιεχομένου (Content-control software) προσδιορίζει ποιο περιεχόμενο θα είναι διαθέσιμο ή πόσο συχνά αυτό θα πρέπει να αποκλειστεί.

Η χρήση του Λογισμικού Ελέγχου του Περιεχομένου (**Content-control software)** προσδιορίζεται ως εξής:

- Είναι εξειδικευμένες εφαρμογές που ελέγχουν το περιεχόμενο της πληροφορίας που διακινείται:
  - ✓ Η Περιήγηση στο Διαδίκτυο **(Web)**.
  - ✓ Το Ηλεκτρονικό Ταχυδρομείο **(E-mail).**

- Οι λειτουργίες τους:
  - ✓ Γίνεται ο έλεγχος του περιεχόμενου των sites σε κάθε επίσκεψη.
  - ✓ Ακολουθούν τη δυναμικότητα στο Διαδίκτυο (URL- List Classified Updated).[30]
  - ✓ Αυξάνουν την αποδοτικότητα της εργασίας.
  - ✓ Μείωση της νομικής ευθύνης.
  - ✓ Σώζουν το Bandwidth.[31]

---

[27] Το FTP **(File Transfer Protocol)** είναι ένα ευρέως χρησιμοποιούμενο πρωτόκολλο σε δίκτυα τα οποία υποστηρίζουν το πρωτόκολλο TCP/IP (δίκτυα όπως internet ή intranet). Ο υπολογιστής που τρέχει εφαρμογή FTP client μόλις συνδεθεί με τον server μπορεί να εκτελέσει ένα πλήθος διεργασιών όπως ανέβασμα αρχείων στον server, κατέβασμα αρχείων από τον server κτλ.

[28] Το SSH **(Secure Shell)** είναι ένα ασφαλές δικτυακό πρωτόκολλο το οποίο επιτρέπει τη μεταφορά δεδομένων μεταξύ δύο υπολογιστών.

[29] Το πρωτόκολλο Peer-to-peer **(P2P)** δίκτυα συνδέουν πολλές τελικούς ξενιστές με τρόπο ad-hoc. Τα δίκτυα P2P συνήθως χρησιμοποιούνται για την κοινή χρήση αρχείων και εφαρμογές, οι οποίες επιτρέπουν να τον μοιρασμό ψηφιακού περιεχομένου, όπως έγγραφα, ήχο και βίντεο.

[30] Ο όρος **Uniform Resource Locator (URL)** δηλώνει μια διεύθυνση ενός πόρου του Παγκόσμιου Ιστού. Είναι παρόμοιο με το όνομα ενός αρχείου, αλλά κρατάει και επιπλέον πληροφορία σχετικά με το όνομα του εξυπηρετητή, καθώς και το είδος του πρωτοκόλλου που αυτός χρησιμοποιεί.

✓ Δυνατότητα μείωσης της πιθανότητας να μεταδώσουν πληροφορίες σε τρίτα άτομα.
✓ Δυνατότητα παγίδευσης E-mails με συγκεκριμένο περιεχόμενο.

- Συχνά πρόκειται για εξειδικευμένες συσκευές του δικτύου (συσκευές περιμέτρου) ή κάποιο εξειδικευμένο λογισμικό ως πρόσθετο σε servers (όπως στον proxy).[32]

Η χρήση του Λογισμικού Ελέγχου του Περιεχομένου (**Content-control software)** στο Διαδίκτυο **(Web).**

- Κανόνες πρόσβασης στο Internet:
  - ✓ Ανά ομάδα χρηστών.
  - ✓ Ανά κατηγορία σελίδας.
  - ✓ Ανά ώρα ημέρας.
- Κάποιες κατηγορίες που δεν επιτρέπεται η πρόσβαση:
  - ✓ Η διακίνηση πειρατικών λογισμικών και δεδομένων.
  - ✓ Σε πορνογραφικό περιεχόμενο.
  - ✓ Σε εξτρεμιστικό περιεχόμενο.
- Κάποιες κατηγορίες που επιτρέπεται η πρόσβαση υπό κάποιες συνθήκες:
  - ✓ Των Ανακοινώσεων (όπως κάποια Sites και Forum).
  - ✓ Των Χόμπι (όπως φωτογραφίες, μηχανάκια).
  - ✓ Τα Νέα και οι Ειδήσεις (News).
- Πιθανά προβλήματα:
  - ✓ Δεν τα εντοπίζουν όλα.
  - ✓ Η λάθος κατηγοριοποίηση των σελίδων.

Η χρήση του Λογισμικού Ελέγχου του Περιεχομένου (**Content-control software)** στο Ηλεκτρονικό Ταχυδρομείο **(E-Mail).**

- Η επιβολή κανόνων που αφορούν τα E-mail:
  - ✓ Το μέγιστο μέγεθος ανά E-mail κάθε χρήστη.
  - ✓ Κάποιοι τύποι από Attachments (η αποτροπή επισύναψης και αποστολή λήψης με μορφές *.mp3, *.exe, κτλ).
- Ο έλεγχος για την ανεπιθύμητη αλληλογραφία (SPAM):
  - ✓ Το RBIs[33] εντοπίζει τα SPAM τα οποία αποστέλλονται από διάφορους Spammers[34].

---

[31] Το **Bandwidth** στα Δίκτυα υπολογιστών και πληροφορικής είναι το εύρος ζώνης του δικτύου εύρος ζώνης δεδομένων ή το ψηφιακό εύρος ζώνης και είναι μια μέτρηση της ταχύτητας των πόρων επικοινωνίας δεδομένων διαθέσιμη ή καταναλώνεται εκφράζεται σε bit ανά δευτερόλεπτο ή πολλαπλάσια του.

[32] Ο **Proxy** είναι ο Διακομιστής μεσολάβησης, είναι ένας διακομιστής που έχει στόχο να βελτιώσει την ταχύτητα πλοήγησης στο διαδίκτυο και παράλληλα να μειώσει την κίνηση του δικτύου προς το διαδίκτυο.

[33] Το **RBIs** γνωστό και ως κατάλογος σε πραγματικό χρόνο **(Blackhole List)** είναι ένας τρόπος με τον οποίο ένας χώρος διαδικτύου μπορεί να δημοσιεύσει έναν κατάλογο διευθύνσεων IP με μια μορφή που μπορεί να ρωτηθεί εύκολα από τους κεντρικούς υπολογιστές ταχυδρομείου στο διαδίκτυο. Αυτές οι διευθύνσεις είναι εκείνες των γνωστών spammers. Εάν ένα E-mail προέρχεται από μια από αυτές τις διευθύνσεις, μπορεί να απορριφθεί ως Spam.

- ✓ Τα SURLs, στο κείμενο του E-mail διαπιστώνονται παραπομπές σε URLs (Web Sites) από γνωστούς Spammers.
- ✓ Οι λέξεις κλειδιά. Υπάρχει πληθώρα γνωστών λέξεων που αν εντοπίζεται σε ένα E-mail δηλώνονται ως SPAM (όπως sex, drugs κτλ).

- Κάποια πιθανά προβλήματα:

  - ✓ Κάποιοι πιθανοί λάθος χαρακτηρισμοί (μερικές φορές χαρακτηρίζονται ως Spam, E-mail που δεν είναι και το αντίστοιχο).
  - ✓ Το σύστημα απαιτεί την αντίστοιχη εκπαίδευση για να λειτουργήσει αποδοτικά.

Το Πρωτόκολλο Ασφάλειας του Internet (Internet Protocol Security-IPsec)

Εισαγωγή

Το πρωτόκολλο του Internet **(Internet Protocol Security -IPsec)** συμπεριλαμβάνεται σε μια οικογένεια πρωτοκόλλων για την εξασφάλιση στις επικοινωνίες με πρωτόκολλο Internet **(IP)** τον έλεγχο ταυτότητας καθώς και για την κρυπτογράφηση του κάθε πακέτου IP μιας συνόδου επικοινωνίας. Το IPsec συμπεριλαμβάνει τα πρωτόκολλα τα οποία μπορούν να αναπτύσσουν αμοιβαίο έλεγχο ταυτότητας μεταξύ των πρακτόρων στην αρχή της περιόδου επικοινωνίας και της διαπραγμάτευσης των κρυπτογραφικών πλήκτρων που χρησιμοποιούντα κατά την διάρκεια της χρονικής περιόδου της επικοινωνίας.

Το IPsec μπορεί να χρησιμοποιηθεί και στην προστασία των ροών στοιχείων μεταξύ ενός ζεύγους από hosts (Host το Host), μεταξύ ενός ζεύγους των πυλών (Gateways) ασφαλείας (Network to Network) ή μεταξύ μιας πύλης ασφαλείας και υποδοχής (Network to Host).Το IPsec χρησιμοποιεί υπηρεσίες ασφαλείας για την προστασία των επικοινωνιών μέσω του πρωτοκόλλου Internet IP. Επίσης το IPsec υποστηρίζει τον έλεγχο της ταυτότητας σε επίπεδο δικτύου, τα στοιχεία της ταυτότητας της προέλευσης, την ακεραιότητα των δεδομένων, την εμπιστευτικότητα των δεδομένων (κρυπτογράφηση) και η προστασία της αναπαραγωγής.

Το IPsec είναι ένα σύστημα ασφαλείας που λειτουργεί στο στρώμα του διαδικτύου (Internet Layer), της ακολουθίας του πρωτοκόλλου του διαδικτύου (Internet Protocol Suite) ενώ μερικά άλλα συστήματα ασφάλειας διαδικτύου σε διαδεδομένη χρήση όπως η ασφάλεια στρώματος μεταφορών (Transport Layer Security – TLS) και η ασφαλής Shell (SSH), λειτουργούν στα ανώτερα στρώματα του μοντέλου TCP/IP. Έτσι το IPsec προστατεύει οποιαδήποτε κυκλοφορία εφαρμογής μέσω ενός δικτύου IP.[23]

Η Αρχιτεκτονική Ασφαλείας IPsec

- Το IPsec υλοποιείται με μια σειρά από πρωτόκολλα:

  - ✓ Για την ασφαλή ροή **(Secure Flow)**.
  - ✓ Για την αμοιβαία αυθεντικοποίηση **(Mutual Authentication)**.
  - ✓ Και τον προσδιορισμό των κρυπτογραφικών παραμέτρων **(Identification of Cryptographic Parameters)**.

- Κάνει χρήση της έννοιας «Συσχετισμού Ασφάλειας».
  - ✓ Εφόσον αποτελείται μια συλλογή από αλγόριθμους και παραμέτρους που λειτουργούν μεταξύ τους για να υπάρχει ασφαλής διακίνηση των πακέτων.
- Λειτουργεί με 2 τρόπους **(Mode of Operation)**:

---

[34] Οι **Spammers** είναι αυτοί που συνήθως στέλνουν κακόβουλο υλικό είτε βρίσκεται μέσω ιστοσελίδων είτε μέσω του ηλεκτρονικού ταχυδρομείου.

- Το **Transport** Mode:
  - ✓ Μόνο το ωφέλιμο φορτίο (Payload) ενός πακέτου κρυπτογραφείται ή αυθεντικοποιείται (τα πραγματικά δεδομένα και όχι οι επικεφαλίδες όπως ο αποστολέας και ο παραλήπτης).
- Το **Tunnel** Mode:
  - ✓ Το πακέτο κρυπτογραφείται (μαζί και οι επικεφαλίδες). Η χρήση αυτή είναι συνηθισμένη στα VPN.[35]
- Στο πρωτόκολλο IPv6 το IPsec είναι υποχρεωτικό ενώ στο IPv4 είναι προαιρετικό.

Τεχνικές Λεπτομέρειες του IPsec

- Η Αυθεντικοποίηση της Επικεφαλίδας (Authentication Header):
  - ✓ Εξασφαλίζεται η αυθεντικότητα και η ακεραιότητα του πακέτου IP.
  - ✓ Προστατεύει από τις επιθέσεις επανάληψης (Replay).
  - ✓ Προστατεύει ολόκληρο το πακέτο (επικεφαλίδες και ωφέλιμο φορτίο – headers και payload).
- Ενθυλάκωσης Ωφέλιμου Φορτίου Ασφάλειας (Encapsulating Security Payload - ESP):
  - ✓ Η Εξασφαλίζει την ακεραιότητα – την αυθεντικότητα, την εμπιστευτικότητα του πακέτου IP αλλά μόνο του Ωφέλιμου Φορτίου (Payload) των δεδομένων και όχι των επικεφαλίδων.
- Μπορεί να προσφέρει μόνο ακεραιότητα ή τη αυθεντικότητα.
  - ➢ Δεν ενθαρρύνεται η χρήση μόνο παροχής της εμπιστευτικότητας (γιατί αυτό είναι μόνο ανασφαλές).
- Διάφοροι αλγόριθμοι μπορούν να χρησιμοποιηθούν:
  - ✓ Για την αυθεντικότητα ακεραιότητας md5, sha, RSA.
  - ✓ Για την εμπιστευτικότητα 3DES, AES.[23]

Η Ανταλλαγή Κλειδιών στο IPsec

- Για να επικοινωνήσουν δύο οντότητες αρχικά πρέπει να συμφωνήσουν και να ανταλλάξουν κάποια κλειδιά με ασφάλεια.
- Για να επιτευχθεί ένας «Συσχετισμός Ασφάλειας» πρέπει να χρησιμοποιείται το Internet Key Exchange - IKE (RFC 4306).[36]
- Το IKE χρησιμοποιεί Diffie-Helman[37] key exchange για να ορίσει ένα «κοινό μυστικό», από όπου προκύπτουν τα κλειδιά κρυπτογραφίας που θα χρησιμοποιηθούν.
- Για την ταυτοποίηση των δύο μερών χρησιμοποιούνται μέθοδοι δημόσιου κλειδιού.
- Κάποια προβλήματα με το IKE:

---

[35] Ένα **εικονικό ιδιωτικό δίκτυο (Virtual Private Network - VPN)** είναι ένα δίκτυο που χρησιμοποιεί κατά κύριο λόγο δημόσια τηλεπικοινωνιακή υποδομή, όπως το Διαδίκτυο, και δίνει τη δυνατότητα σε απομακρυσμένα γραφεία ή σε χρήστες που ταξιδεύουν να έχουν πρόσβαση σε ένα κεντρικό οργανωτικό δίκτυο.

[36] Στην επιστήμη των υπολογιστών, **Internet Key Exchange (IKE)** είναι το πρωτόκολλο που χρησιμοποιείται για να δημιουργήσει μιας σύνδεσης ασφαλείας (SA) στη σουίτα του πρωτοκόλλου IPsec.

[37] Το **Diffie-Hellman** είναι μια ειδική μέθοδος της ανταλλαγής κρυπτογραφικών κλειδιών. Είναι ένα από τα πρώτα πρακτικά παραδείγματα των βασικών ισοτιμιών που εφαρμόζονται στον τομέα της κρυπτογραφίας.

- ✓ Κατά την διάρκεια των υλοποιήσεων υπάρχουν ασυμβατότητες ενώ πρέπει οι παράμετροι μεταξύ τους να εφαρμόζονται με ακρίβεια.
- ✓ Απαιτείται το ίδιο λογισμικό (IPsec, VPN client).
- ✓ Η πολυπλοκότητα οδηγεί σε αύξηση SSL, VPN.[23]

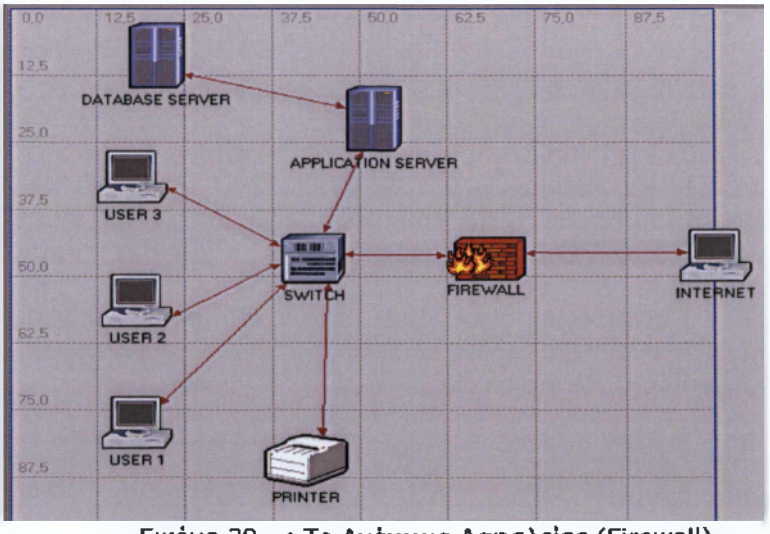
Αναχώματα Ασφαλείας (Firewalls)

Ορισμός Αναχωμάτων Ασφαλείας (Firewalls)

Η απαίτηση σύνδεσης του δικτύου του οργανισμού με το διαδικτύου (Internet) ανοίγει ταυτόχρονα ένα κανάλι αμφίδρομης επικοινωνίας: οι χρήστες (Insiders) από το εσωτερικό περιβάλλον του δικτύου αποκτούν επικοινωνία με τον έξω κόσμο, αλλά ταυτόχρονα οι χρήστες (Outsiders) από το εξωτερικό περιβάλλον αποκτούν δυνατότητα πρόσβασης ως προς το δίκτυο αυτό. Επομένως η αύξηση του μεγέθους του διαδικτύου εγκυμονεί την αύξηση των κινδύνων που προέρχονται από τα ιδιωτικά δίκτυα (Private Networks) που κάνουν σύνδεση μαζί του. Άρα για την προστασία τους από πιθανές παρακολουθήσεις, εισβολές και άλλες διαδικτυακές απειλές συνίστανται τα αναχώματα ασφαλείας. Ο ορισμός που ορίζει τα αναχώματα ασφαλείας είναι ο εξής:

> «Τα Αναχώματα Ασφαλείας Διαδικτύου **(Internet Firewalls)** είναι η συλλογή από κατάλληλα συστήματα, εγκαταστημένα στην περιοχή σύνδεσης της υπό προστασίας διαδικτυακής περιοχής με τα υπόλοιπα δίκτυα, που ορίζει συγκεκριμένη πολιτική προστασίας.»

Ένα ανάχωμα ασφαλείας «σηκώνει» ένα εξωτερικό τοίχο ασφαλείας, καθορίζοντας μια περίμετρο ασφαλείας. Αυτό έχει ως αποτέλεσμα να γίνει ένας διαχωρισμός ανάμεσα στο εσωτερικό προστατευόμενο δίκτυο (το οποίο είναι ασφαλές και έμπιστο) κάποιου οργανισμού με το εξωτερικό διαδίκτυο (τα οποίο είναι μη ασφαλές και μη έμπιστο). Ένα τυπικό σύστημα firewall μπορεί να επιτρέψει με κατά επιλογή την πρόσβαση των εξωτερικών χρηστών με βάση τα ονόματά ή και συνθηματικά των χρηστών, σε IP διευθύνσεις ακόμα και σε ονόματα επικρατειών (Domain Names). Αυτή είναι και η επιδίωξή του, να κρατήσει μακριά τις παράνομες και επικίνδυνες δραστηριότητες από το προστατευόμενο δίκτυο.



Εικόνα 39 - : Το Ανάχωμα Ασφαλείας (Firewall).

Ο κυριότερος λόγος ύπαρξης ενός συστήματος Firewall σε έναν οργανισμό είναι για να του δίνεται ένας μηχανισμός ελέγχου προσπέλασης (Access Control), πρώτου επιπέδου (Layer 1), για τον Web server. Ένα σύστημα Firewall μπορεί να κάνει τον έλεγχο και την καταγραφή της ροής της επικοινωνίας που υλοποιείται μέσω του διακομιστή Web. Επομένως βρίσκεται σε θέση να προστατεύσει τα δεδομένα που παρουσιάζονται από μη

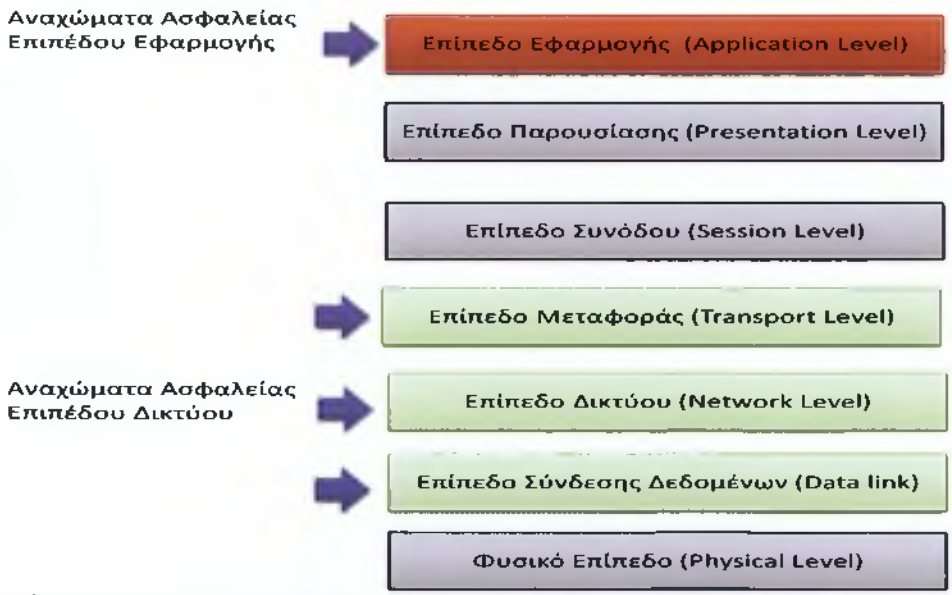
επιθυμητές αλλαγές καθώς και να κάνει τον έλεγχο πρόσβαση του Web απαγορεύοντας τους μη εξουσιοδοτημένους χρήστες από τα ευαίσθητα σημεία του δικτύου. Ένας ακόμα λόγος που ο οργανισμός χρησιμοποιεί ένα σύστημα Firewall είναι ότι θέλει να χωρίσει τις επικοινωνίες ανάμεσα στα επιμέρους τμήματά του.[1,23,24]

Διάφορα Είδη Αναχωμάτων Ασφαλείας (Firewalls)

Το κάθε είδος των Firewalls λειτουργεί σε διαφορετικά επίπεδα του μοντέλου OSI εφαρμόζοντας διαφορετικά κριτήρια για τον έλεγχο της κυκλοφορίας. Το πιο χαμηλό επίπεδο που μπορεί να λειτουργήσει ένα Firewall είναι το επίπεδο δικτύου στο μοντέλο OSI ή στο επίπεδο του Internet Protocol στο μοντέλο TCP/IP. Ένα Firewall στο επίπεδο αυτό μπορεί να προσδιορίσει μόνο εάν το πακέτο προέρχεται από έμπιστη πηγή αλλά δεν μπορεί να ξέρει τι περιέχει και με ποια άλλα πακέτα συνδέεται. Τα Firewalls τα οποία λειτουργούν στο επίπεδο μεταφοράς ξέρουν περισσότερες πληροφορίες για τα πακέτα το αν θα επιστρέψουν ή να αρνηθούν την πρόσβαση. Στο επίπεδο όμως εφαρμογής τα Firewalls ξέρουν πολλές πληροφορίες και μπορούν να γίνουν πιο αυστηρά στην παροχή πρόσβασης.

Συνήθως τα Firewalls που λειτουργούν σε υψηλότερα από το επίπεδο εφαρμογής θα πρέπει να υπερισχύουν των άλλων επιπέδων. Αυτό δεν είναι πάντα ορθό γιατί όσο παρεμποδίζεται ένα πακέτο σε ένα χαμηλό επίπεδο τόσο το Firewall είναι ασφαλές.

Σε περίπτωση που ο επιτιθέμενος εισέλθει και περάσει και το τρίτο επίπεδο δεν μπορεί να αποκτήσει τον έλεγχο του λειτουργικού συστήματος.



Εικόνα 40 - Τα επίπεδα OSI που Καλύπτει το κάθε Ανάχωμα Ασφαλείας (Firewall).

Τα Firewalls μπορούν χωριστούν στις εξής κατηγορίες:

- ✓ Φίλτρα Πακέτων **(Packet Filter)**.
- ✓ Πύλες Επιπέδου Κυκλώματος **(Circuit Level Gateways)**.
- ✓ Πύλες Επιπέδου Εφαρμογής, **(Application Level Gateways)**.
- ✓ Stateful Multilayer Inspection Firewalls.[24]

Πολιτική των Αναχωμάτων Ασφαλείας (Firewalls)

Οι πολιτικές για τα τείχη ασφαλείας **(Firewall Policies)** προσδιορίζουν τις διαδικασίες διαχείρισης της κυκλοφορίας στα δίκτυα υπολογιστών (Computer Networks)

για συγκεκριμένες IP διευθύνσεις (Internet Protocol), για τις εφαρμογές, για τα πρωτόκολλα και τα είδη των ενεργού περιεχομένου, με βάση τις πολιτικές ασφαλείας των πληροφοριών (Security Policies) κάθε οργανισμού. Η εξέταση των πιθανών κινδύνων και η δημιουργία ενός καταλόγου ο οποίος θα συμπεριλαμβάνει μια λίστα με τα δεδομένα που μεταδίδονται εντός του δικτύου, θα πρέπει αν έχει προτεραιότητα κάθε άλλης διαδικασίας. Η οργάνωση και η ταξινόμηση έχει ως αποτέλεσμα να διασφαλίζει εν μέρει την ακεραιότητα των δεδομένων τα οποία διέρχονται από τα αναχώματα ασφαλείας. Η πραγματοποίηση της διαδικασίας αυτής επιτρέπει στην υλοποίηση πολιτικών για τα αναχώματα ασφαλείας (Firewall Policies). Επομένως η ανάλυση των κινδύνων (Risk Analysis) θα πρέπει να στηρίζεται στην ανάλυση των πιθανών απειλών, των ευπρόσβλητων σημείων και των συνεπειών για τα υπολογιστικά δεδομένα και των συστημάτων σε περίπτωση κινδύνου. Έτσι κρίνεται αναγκαία η επιβεβαίωση των πολιτικών για τα αναχώματα ασφαλείας και η συνεχής ενημέρωση αυτών για νέα είδη επιθέσεων ή ευπρόσβλητα σημεία σε σχέση τις ανάγκες του οργανισμού.[24]

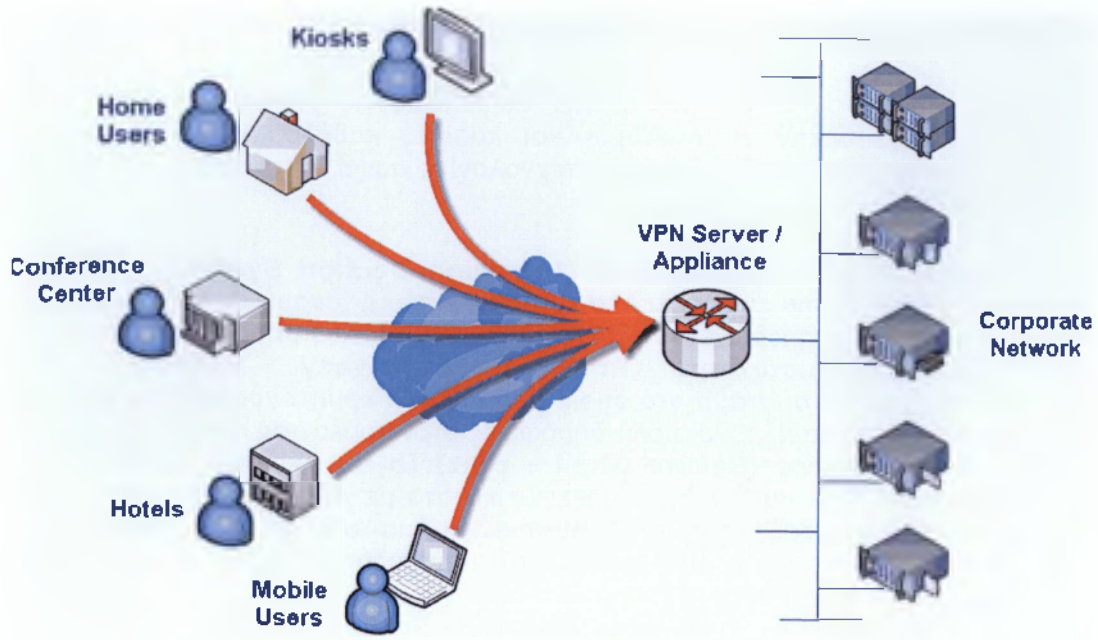
Χρήση Εικονικών Δικτύων (Virtual Private Network)

Ένα Εικονικό Ιδιωτικό Δίκτυο (**Virtual Private Network - VPN**) είναι ένα δίκτυο το οποίο χρησιμοποιεί κατά κύριο λόγο τη δημόσια τηλεπικοινωνιακή υποδομή όπως το Internet, και δίνει τη δυνατότητα σε απομακρυσμένα γραφεία ή και χρήστες οι οποίοι ταξιδεύουν να έχουν κάποια ουσιώδη πρόσβαση σε ένα κεντρικό οργανωτικό δίκτυο. Το VPN απαιτεί από τους χρήστες που είναι μακριά του δικτύου κάποια πιστοποίηση και συχνά ασφαλίζει τα δεδομένα με τις τεχνολογίες της κρυπτογραφίας για να παρεμποδίσει τη διάδοση των ιδιωτικών πληροφοριών από χρήστες που είναι μη εξουσιοδοτημένοι. Ένα VPN μπορεί να αναπτύσσεται για τη λειτουργικότητα κάποιου δικτύου που βρίσκεται σε οποιαδήποτε δίκτυο (όπως με την κοινή χρήση των δεδομένων καθώς και η πρόσβαση σε πόρους δικτύου, σε εκτυπωτές, βάσεις δεδομένων κλπ).

Ο χρήστης VPN αντιμετωπίζει συνήθως το κεντρικό δίκτυο με τρόπο όμοιο με αυτόν που συνδέεται άμεσα στο κεντρικό δίκτυο. Η τεχνολογία VPN μέσω του κοινόχρηστου Internet έχει αντικαταστήσει την ανάγκη για διατήρηση ακριβών μισθωμένων γραμμών τηλεπικοινωνιακών κυκλωμάτων περιοχές εγκαταστάσεων του δικτύου.

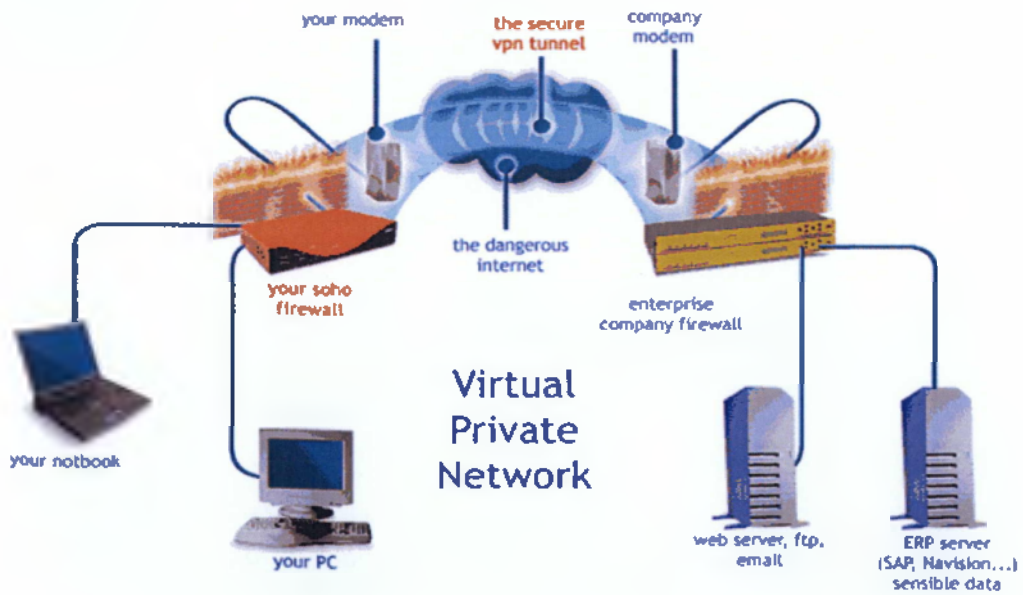
Τα συστήματα VPN **(Virtual Private Network**) μπορούν να ταξινομηθούν από:

- ✓ Τα πρωτόκολλα τα οποία χρησιμοποιούνται για τη σήραγγα της κυκλοφορίας.
- ✓ Το τερματικό σημείο της σήραγγας, δηλαδή, την άκρη του πελάτη ή την άκρη του δικτύου παροχής.
- ✓ Τα επίπεδα ασφαλείας τα οποία παρέχονται.
- ✓ Το στρώμα του OSI που παρουσιάζουν για τη σύνδεση του δικτύου, όπως τα κυκλώματα $2^{ου}$ επιπέδου ή $3^{ου}$ επιπέδου σύνδεσης με το δίκτυο.



Εικόνα 41 - Απεικόνιση Εικονικού Ιδιωτικού Δικτύου (Virtual Private Network).

Για να διατηρηθούν οι πληροφορίες κρυφές καθώς τα αυτοδύναμα πακέτα διέρχονται μέσω του Internet από τη μια τοποθεσία στην άλλη, το λογισμικό του εικονικού ιδιωτικού δικτύου (VPN) χρησιμοποιεί μια σήραγγα IP σε IP **(IP - IP tunnel)**. Το λογισμικό του VPN κρυπτογραφεί ολόκληρο το αυτοδύναμο πακέτο και στη συνέχεια τοποθετεί σε κάποιο άλλο αυτοδύναμο πακέτο για να το μεταδώσει. [24]



Εικόνα 42 - Απεικόνιση Σήραγγας Εικονικού Ιδιωτικού Δικτύου (Virtual Private Network).

Οι Βασικές Τεχνολογίες Ασφάλειας Internet

Έχουν αναπτυχθεί πολλές τεχνολογίες ασφάλειας για χρήση στο Internet (μερικές από αυτές αναφέρθηκαν εν συντομία και κάποιες καθόλου σε αυτό το κεφάλαιο, παρακάτω προσδιορίζουμε τις επιπλέον τεχνολογίες ασφαλείας και τις υπάρχουσες λίγο πιο αναλυτικά).

- Σύστημα Ανίχνευσης Εισβολής (**Intrusion Dection System – IDS)**: Το IDS είναι σύστημα που επιβλέπει όλα τα πακέτα που φτάνουν σε κάποια τοποθεσία και στη συνέχεια ενημερώνει τον διαχειριστή σε περίπτωση παραβίασης ασφαλείας. θ
- Πολύ Καλή Μυστικότητα **(Pretty Good Privacy - PGP)**: Το PGP είναι κρυπτογραφικό σύστημα στο οποίο μπορούν να κρυπτογραφηθούν δεδομένα πριν την αποστολή τους. Είναι πολύ δημοφιλές στον τομέα της πληροφορικής.
- Ασφαλές Κέλυφος **(Secure Shell - SSH)**:Το SSH είναι πρωτόκολλο επιπέδου εφαρμογής και εγγυάται την εμπιστευτικότητα με την κρυπτογράφηση δεδομένων πριν τη μεταφορά τους στο Internet. Η πιο σημαντική κρυπτογράφηση της μακρινής σύνδεσης, επειδή χωρίς αυτή οποιοσδήποτε υποκλοπέας μπορεί να δει τους κωδικούς πρόσβασης.
- Ασφαλές Επίπεδο Υποδοχών **(Secure Socket Layer - SSL)**: Το SSl χρησιμοποιείται για την κρυπτογράφηση για να παρέχει πιστοποίηση ταυτότητας και εμπιστευτικότητα. Το SSl εφαρμόζεται μεταξύ κάποιας εφαρμογής και του API[38] υποδοχών, καθώς κρυπτογραφεί τα δεδομένα πριν σταλθούν στο Internet. Το SSl χρησιμοποιείται στις συνδέσεις WEB και κυρίως στους χρήστες που τους επιτρέπουν να πραγματοποιήσουν οικονομικές συναλλαγές.

- IPsec **(IP Security- Ασφάλεια IP)**: Το IPsec είναι πρότυπο ασφαλείας που χρησιμοποιείται στα πακέτα IP. Το IPsec χρησιμοποιεί κρυπτογραφικές μεθόδους και επιτρέπει να διαλέξει κάθε χρήστης ή στην πιστοποίηση ταυτότητας ή της εμπιστευτικότητας.
- Υπηρεσία απομακρυσμένης ταυτότητα χρήστη που συνδέεται μέσω τηλεφώνου **(Remote Authentication Dial -In User Service - RADIUS)**: Το RADIUS είναι ένα πρωτόκολλο το οποίο χρησιμοποιούνται να παρέχει κεντρική πιστοποίηση ταυτότητας, λογιστική εξουσιοδότηση και λογική παρακολούθηση. Το RADIUS είναι γνωστό στους χρήστες που χρησιμοποιούν σύνδεση μέσω τηλεφώνου και σε συστήματα εικονικών δικτύων (VPN) που έχουν πρόσβαση σε μακρινούς χρήστες.
- **Wired Equivalent Privacy - WEP**: Το πρότυπο WEP αποτελεί μέρος τους πρότυπου Wi – Fi για ασύρματα τοπικά δίκτυα. Κάποιο ερευνητές έδειξαν ότι το WEP έχει αρκετές αδυναμίες. Έτσι αναπτύχθηκε ένα νέο πρότυπο WPA (Wi – Fi Protected Access) προστατευόμενη πρόσβαση Wi – Fi.

Αντίγραφα Ασφαλείας (BACK Up)

Εισαγωγή

Στον τομέα της τεχνολογίας των πληροφοριών, ένα Αντίγραφο Ασφαλείας **(BACK Up)** ή διαδικασία ως προς τη δημιουργία αντιγράφων ασφαλείας αναφέρεται στην αντιγραφή καθώς και την αρχειοθέτηση των δεδομένων στον υπολογιστή έτσι ώστε να

[38] Η Διεπαφή Προγραμματισμού Εφαρμογών **(Application Programming Interface - API)**, είναι η διεπαφή των προγραμματιστικών διαδικασιών που ένα λειτουργικό σύστημα, βιβλιοθήκη ή εφαρμογή παρέχει προκειμένου να επιτρέπει να γίνονται προς αυτό αιτήσεις από άλλα προγράμματα ή και ανταλλαγή δεδομένων.

μπορεί να χρησιμοποιηθεί για την επαναφορά στην αρχική κατάσταση μετά την απώλεια των δεδομένων.

Τα Αντίγραφα Ασφαλείας (BACK Up) έχουν δύο διαφορετικούς στόχους. Ο αρχικός στόχος είναι να ανακτήσουν τα δεδομένα μετά την απώλεια, είτε έχει να κάνει με την διαγραφή ή την καταστροφή των δεδομένων. Ο άλλος στόχος είναι να ανακτήσουν στοιχεία από μια προηγούμενη εποχή, σύμφωνα και με την πολιτική προστασίας των δεδομένων η οποία έχει καθοριστεί από το χρήστη.

Τα αντίγραφα ασφαλείας καθορίζουν γενικά μια απλή μορφή της αποκατάστασης μετά από κάποια καταστροφή και θα πρέπει να αποτελεί μέρος ενός σχεδίου της αποκατάστασης καταστροφών. Επομένως ένας λόγος για αυτό είναι ότι όλα τα εφεδρικά συστήματα ή οι εφαρμογές της δημιουργίας των αντιγράφων ασφαλείας είναι σε σημείο να ανασυστήσουν ένα σύστημα ηλεκτρονικού υπολογιστή ή κάποιων άλλων πιο πολύπλοκων διαμορφώσεων όπως ένα σύμπλεγμα υπολογιστή που έχει ενεργούς διακομιστές καταλόγου, ή έναν διακομιστή βάσεως δεδομένων, την αποκατάσταση μόνο των δεδομένων από ένα αντίγραφο ασφαλείας.

Εκτός του ότι ένα εφεδρικό σύστημα περιέχει τουλάχιστον 1 αντίγραφο ασφαλείας όλων των δεδομένων, οι απαιτήσεις της αποθήκευσης των δεδομένων μπορεί να είναι σημαντικές. Η οργάνωση της αποθήκευσης και της διαχείρισης της διαδικασίας για την δημιουργία των αντιγράφων ασφαλείας μπορεί να καταστεί μια πολύπλοκη επιχείρηση. Στην εποχή μας υπάρχουν πολλά είδη συσκευών αποθήκευσης των δεδομένων που χρησιμεύουν για τη δημιουργία αντιγράφων ασφαλείας. Επιπλέον υπάρχουν και πολλοί διαφορετικοί τρόποι με τους οποίους οι συγκεκριμένες συσκευές μπορούν να οργανωθούν και να παρέχουν την ασφάλεια των δεδομένων καθώς και τη φορητότητα. Υπάρχουν πολλές διαφορετικές τεχνικές που έχουν δημιουργηθεί για τη διαδικασία της δημιουργίας αντιγράφων ασφαλείας. Αυτές περιλαμβάνουν για τη συμπίεση, την κρυπτογράφηση, τις ζωντανές πηγές των δεδομένων. Κάθε εφεδρικό σύστημα πρέπει να περιλαμβάνει κάποιες διαδικασίες για να επικυρώνει την αξιοπιστία των δεδομένων που υποστηρίζονται. Είναι αξιοσημείωτο ότι πρέπει να αναγνωρίζονται οι περιορισμοί του ανθρώπινου παράγοντα που εμπλέκονται σε κάθε σύστημα αντιγράφων ασφαλείας.[27]

Πολιτικές Αντιγράφων Ασφαλείας (*Backup Policies)*

Οι εταιρίες και οι οργανισμοί που κατέχουν γραπτές πολιτικές για τα αντίγραφα ασφαλείας τους, αναλόγως με τις ανάγκες τους. Επομένως καθορίζονται ως εξής:

- ✓ Η συχνότητα για τα αντίγραφα ασφαλείας.
- ✓ Ο αριθμός των κρατούμενων αντιγράφων.
- ✓ Ο χρόνος κράτησής τους.
- ✓ Οι διαφορετικές τοποθεσίες που πρέπει να κρατούνται.
- ✓ Τα πρόσωπα που έχουν πρόσβαση σε αυτά.

Η Λειτουργία των Αντιγράφων Ασφαλείας (Operation of Backup)

- Τα ψηφιακά δεδομένα μπορούν να αποθηκευτούν σε ψηφιακά μέσα:
  - ✓ Σκληροί δίσκοι **(μαγνητικό μέσο)**.
  - ✓ CD/DVD **(οπτικό μέσο)**.
  - ✓ Δισκέτες **(μαγνητικό μέσο)**.
  - ✓ Flash Drives **(τύπος EPROM)**.[39]
  - ✓ Μνήμες RAM.

- Πιθανός κίνδυνος για την απώλεια των δεδομένων:
  - ✓ Κάποια αστοχία στα κυκλώματα ή τα μηχανικά μέρη της συσκευής (σκληρών δίσκων).
  - ✓ Ο απομαγνητισμός **(όπως οι δισκέτες)**.
  - ✓ Φυσική Απώλεια **(κυρίως τα USB - Memory)**.
  - ✓ Κάποια Ατυχήματα **(format – delete)**.
  - ✓ Ο χρόνος αστοχίας για μια συσκευή **(όλα κάποια στιγμή χαλάνε)**.

- Η λύση είναι:
  - ✓ Τα Αντίγραφα Ασφαλείας **(Back up)**.

Επομένως τα αντίγραφα ασφαλείας πρέπει να λαμβάνονται:

- Κεντρικά:
  - ✓ Από το File Server.
  - ✓ Από το E-mail Server.
  - ✓ Κάποιο υπεύθυνοι για την φύλαξη (κυρίως Administrators).
  - ✓ Δεν είναι πάντα εφικτό.

---

[39] Μια **EPROM** ή διαγραφόμενες προγραμματιζόμενες μνήμη μόνο για ανάγνωση, είναι ένα είδος τσιπ μνήμης που διατηρεί τα δεδομένα της όταν η τροφοδοσία του είναι απενεργοποιημένη.

- Τοπικά:

  - ✓ Στα έγγραφά μου όταν φυλάσσονται τοπικά.
  - ✓ Από το E-mail (από το Outlook).
  - ✓ Οι χρήστες είναι οι κύριοι υπεύθυνοι.[27]

Διαδικασία λήψης Αντιγράφων Ασφαλείας (Backup Process)

- Αναλόγως με τις απαιτούμενες ανάγκες που υπάρχουν:
  - ✓ Χρειάζεται ανάλυση για την έκδοση του προγράμματος.
- Πιθανόν πρόβλημα στην περίπτωση που δεν περιέχει αυτό που θέλεις το τελευταίο BackUp ή το συγκεκριμένο είναι καταστραμμένο.
- Επομένως υπάρχει ανάγκη για βάθος χρόνου:
  - ✓ Η ανάγκη για διαδικασία λήψης αντιγράφων ασφαλείας ανάλογα με το μέγεθος του οργανισμού και την κρισιμότητα των πληροφοριών που κατέχει και παρέχει (BackUp ανά 1 εβδομάδα, 1 μήνα, 3 μήνες, 6 μήνες, 1 χρόνο). Το BackUp μπορεί να γίνει για όλο το εύρος του οργανισμού από τον Administrator.[27]

Επίλογος

Συμπεράσματα

Η ραγδαία εξέλιξη στον τομέα της Τεχνολογίας Πληροφορικής και των Επικοινωνιών οφείλεται στην ανάπτυξη των υπηρεσιών που υποστηρίζουν την ανταλλαγή των δεδομένων από απόσταση καθώς και την επεξεργασία ων πληροφοριών. Έτσι είναι επιτακτική η ανάγκη για δημιουργία πληροφοριακών συστημάτων τα οποία θα εξασφαλίζουν με ασφάλεια τη διακίνηση των δεδομένων που οδηγούν σε πληροφορίες και να διαθέτουν τις ιδιότητες της εμπιστευτικότητας (Confidentiality) της ακεραιότητας (Integrity) και τις διαθεσιμότητας (Availability).

56Τα δεδομένα αποτελούν το αγαθό μεγάλης αξίας σε κάθε οργανισμό. Επομένως η ασφάλεια των δεδομένων και των κρίσιμων πληροφοριών αποτελούν σημαντική πρόκληση σε όλα τα επίπεδα. Τα θέματα ασφαλείας των πληροφοριακών συστημάτων και των δικτύων που στηρίζοντα σε αυτά είναι μεγάλης αξίας και εξελίσσονται καθημερινά.

Στην παρούσα πτυχιακή μελετήθηκαν οι πιθανοί κίνδυνοι που μπορεί να υπάρξουν σε ένα πληροφοριακό σύστημα και στο δίκτυο το οποίο στηρίζεται καθώς και τρόπους αντιμετώπισής τους με την παροχή της ασφαλείας (λογισμικά, τεχνικές).

Το συμπέρασμα είναι ότι αν και ακολουθούνται τα μέτρα ασφαλείας πάντα θα υπάρχει συνεχής σύγκρουση με τους κακόβουλους χρήστες (Hackers) οι οποίοι προκαλούν σοβαρά προβλήματα στους οργανισμούς είτε το κάνουν ως χόμπι είτε έχουν κάποια κίνητρα (οργανωμένο έγκλημα, ανταγωνιστές των οργανισμών) και στους αναλυτές των συστημάτων και τους προγραμματιστές που αντιμετωπίζουν τις ενέργειες και τις απειλές των Hackers.

Μελλοντικές επεκτάσεις

Η ασφάλεια των πληροφοριακών συστημάτων πάντα θα αποτελεί ένα μείζον θέμα. Στην ερώτηση αν υπάρχει ή αν θα υπάρξει πλήρης ασφάλεια στα πληροφοριακά συστήματα δεν είναι θετική. Αν και οι οργανισμοί που στηρίζονται σε αυτά για να λειτουργήσουν σωστά αλλά και να γίνουν και πιο ανταγωνιστικοί τους παρέχουν την ουσιώδη προστασία με διάφορες τεχνικές, τα λογισμικά καθώς και το κατάλληλο εκπαιδευμένο προσωπικό (αναλυτές συστημάτων, προγραμματιστές), πάντα θα έχουν το πρόβλημα της ασφάλειας.

Λόγω της ραγδαίας τεχνολογικής εξέλιξης πάντα θα υπάρχουν οι κακόβουλοι χρήστες που θα προσπαθούν μέσω νέων πιο εξελιγμένων τεχνικών να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση ή τον έλεγχο σε συστήματα για να προκαλέσουν ζημιά.

Επομένως για την ασφάλεια πρέπει να κινούνται όλοι οι εμπλεκόμενοι στο σωστό δρόμο ώστε να βελτιώνονται συνέχεια οι υποδομές τους, με τη χρήση των πιο σύγχρονων τεχνικών και λογισμικών που παρουσιάζονται στην αγορά ώστε να μπορούν να αντεπεξέλθουν στις πιθανές νέες απειλές. Επίσης οι εταιρίες θα πρέπει να εφαρμόζουν τις πολιτικές ασφαλείας και οι χρήστες να είναι ενήμεροι για τους υπάρχοντες κινδύνους καθώς και για τους πρωτοεμφανιζόμενους αλλά και να συμπεριφέρονται ανάλογα σε περίπτωση εμφάνισής τους.

Βιβλιογραφία

[1] Σωκρ. Κάτσικας - Δημ. Γκρίτζαλης - Στεφ. Γκρίτσαλης: Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών (2004).

[2] Ευάγγελος Κιουντούζης: Μεθοδολογίες Ανάλυσης & Σχεδιασμού Πληροφοριακών Συστημάτων, Εκδόσεις Ε. Μπένου, Γ΄ Έκδοση (2009).

[3] DOUGLAS E. COMER: Δίκτυα και Διαδίκτυα Υπολογιστών και Εφαρμογές τους στο Internet, Εκδόσεις Κλειδάριθμος, Δ΄ Αμερικανική Έκδοση.

[4] National Institute of Standards and Technology (NIST), Special Publication 800-94 Natl. Inst. Stand. Technol. Spec. Publ. 800-94, 127 pages (February 2007):
Guide to Intrusion Detection and Prevention Systems (IDPS).
http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[5] Copyright © 1990-1998 Network Associates, Inc. and its Affiliated Companies. All Rights Reserved: An Introduction to Cryptography.
ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf

[6] United States Department of Defense, Trusted Computer System Evaluation Criteria, United States Department of Defense, 1983.
http://csrc.nist.gov/publications/history/dod85.pdf

[7] Βικιεπιστήμιο, http://el.wikiversity.org.

[8] Βικιπαίδεια, «Information System».
http://en.wikipedia.org/wiki/Information_system

[9] Βικιπαίδεια, «Πληροφοριακά Συστήματα ».
http://el.wikipedia.org/wiki/%CE%A0%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CE%AC_%CF%83%CF%85%CF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1

[10] Βικιπαίδεια, «Διαχείριση Κινδύνου ».
http://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CF%87%CE%B5%CE%AF%CF%81%CE%B9%CF%83%CE%B7_%CE%9A%CE%B9%CE%BD%CE%B4%CF%8D%CE%BD%CE%BF%CF%85

[11] Βικιπαίδεια, «Ασφάλεια Πληροφοριακών Συστημάτων».
http://el.wikipedia.org/wiki/%CE%91%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CF%8E%CE%BD_%CF%83%CF%85%CF%83%CF%84%CE%B7%CE%BC%CE%AC%CF%84%CF%89%CE%BD

[12] «Η Ασφάλεια Πληροφοριακών Συστημάτων».
http://84.205.229.18/securityc/index.php

[13] Βικιπαίδεια, «Προσομοίωση Monte Carlo».
http://en.wikipedia.org/wiki/Monte_Carlo_methods_for_option_pricing

[14] Βικιπαίδεια, «Τεχνική Pert».
http://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%AC%CE%B3%CF%81%CE%B1%CE%BC%CE%BC%CE%B1_%CE%A0%CE%B5%CF%81%CF%84

[15] Στοιχεία Έρευνας (2014,DBIR) Data Breach Investigations Report - Verizon.
http://www.verizonenterprise.com/DBIR/

[16] Trusted Computer System Evaluation Criteria (TCSEC)
http://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria

[17] Βικιπαίδεια, «Έξυπνες Κάρτες (Smart Cards)».
http://en.wikipedia.org/wiki/Smart_card

[18] Βικιπαίδεια, «Σύστημα KERBEROS».
http://en.wikipedia.org/wiki/Kerberos_%28protocol%29

[19] «Σύστημα SESAME».
http://www.cs.nyu.edu/~wanghua/course/security/final/presentation.html

[20] Βικιπαίδεια, «Biometrics».
http://en.wikipedia.org/wiki/Biometrics

[21] Βικιπαίδεια, «Κρυπτογραφία».
http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

[22] Βικιπαίδεια, «Ψηφιακές Υπογραφές».
http://el.wikipedia.org/wiki/%CE%A8%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%AE_%CF%85%CF%80%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AE

[23] Βικιπαίδεια, «Το Πρωτόκολλο IPsec».
http://en.wikipedia.org/wiki/IPsec

[24] Βικιπαίδεια, «Αναχώματα Ασφαλείας (Firewalls)».
http://el.wikipedia.org/wiki/Firewall#.CE.A0.CE.BF.CE.BB.CE.B9.CF.84.CE.B9.CE.BA.CE.AD.CF.82_Firewall

[25] Βικιπαίδεια, «Antivirus Software (Λογισμικά κατά των Ιών)».
http://en.wikipedia.org/wiki/Antivirus_software

[26] Βικιπαίδεια, «Content - Control Software».
http://en.wikipedia.org/wiki/Content-control_software

[27] Βικιπαίδεια, «Backup».
http://en.wikipedia.org/wiki/Backup

[28] Βικιπαίδεια, «Virtual private Network».
http://en.wikipedia.org/wiki/Virtual_private_network