ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ

ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΜΕΛΕΤΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κοζάνη 2012

ΤΙΤΛΟΣ ΔΙΠΛΩΜΑΤΙΚΗΣ:

ΜΕΛΕΤΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Φοιτήτρια: *Λέρα Μαρία*

Επιβλέπων: *Δρ. Αγγελίδης Παντελής*

Εξεταστική Επιτροπή : *Δρ. Αγγελίδης Π.*

Δρ. Λούτα Μ.

Κοζάνη, Ιούνιος 2012

Ευχαριστίες

Καταρχάς θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή της διπλωματικής μου εργασίας κ. Αγγελίδη Παντελή για την καθοδήγηση του, και την κυρία Καρανάσιου από την εταιρεία Vidavo για την συνεργασία της. Επίσης θέλω να εκφράσω την ευγνωμοσύνη μου στους γονείς μου για την διαρκή τους υποστήριξη, κατά την διάρκεια ολοκλήρωσης των σπουδών μου. Τέλος, να ευχαριστήσω τους φίλους και συνάδελφους μου για τα όμορφα φοιτητικά χρόνια.

Λέρα Μαρία,
Ιούνιος 2012

ΠΕΡΙΛΗΨΗ

Η χρήση των Πληροφοριακών Συστημάτων συνεχώς αυξάνεται. Πλέον οι περισσότεροι οργανισμοί βασίζονται στην λειτουργία τους. Αχίλλειος πτέρνα αυτών είναι η ασφάλεια τους. Στη παρούσα μελέτη παρουσιάζονται τα βασικά θέματα που αφορούν τις Πολιτικές Ασφάλειας των Πληροφοριακών Συστημάτων αναλύοντας την πολιτική ασφαλείας μιας εταιρείας που ειδικεύεται στη τηλεϊατρική. Σε πρώτη φάση εντάσσονται η έννοια της Πολιτικής Ασφάλειας στον ευρύτερο τομέα της Διαχείρισης της Ασφάλειας των Πληροφοριακών Συστημάτων, η σκοπιμότητα εφαρμογής και ανάπτυξης μιας πολιτικής ασφαλείας καθώς περιγράφονται και τα βασικά χαρακτηριστικά της. Στη συνέχεια δίνεται η μεθοδολογία υλοποίησης της μελέτης και το πεδίο ορισμού αυτής. Ακολουθεί περιγραφή της υφιστάμενης κατάστασης στην εταιρεία και η αποτύπωση των διαδικτυακών υπηρεσιών και εφαρμογών της. Στην επόμενη ενότητα προσδιορίζονται οι βασικές αρχές για την ανάπτυξη Πολιτικών Ασφάλειας των Πληροφοριακών Συστημάτων, διευκρινίζοντας το νομικό πλαίσιο προστασίας ιατρικών δεδομένων και το απόρρητο τους. Η επόμενη ενότητα αφορά την εφαρμογή των Πολιτικών Ασφάλειας στο πλαίσιο της εταιρείας και καταγράφει τα απαραίτητα μέτρα για την επιτυχή και αποτελεσματική εφαρμογή τους. Τέλος, παρουσιάζεται η αναγκαιότητα ενός σχεδίου έκτακτης ανάγκης και ανάκαμψης του συστήματος σε περιπτώσεις καταστροφών και η υλοποίηση ενός πλάνου διαχείρισης κινδύνων.

Λέξεις κλειδιά: Πληροφοριακά Συστήματα, Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών, Πολιτική Ασφάλειας, Σχέδιο Έκτακτης Ανάγκης και Ανάκαμψης, Πλάνο Διαχείρισης των Κινδύνων.

Abstract

The use of information systems is increasing, most organizations now rely for their operation. Achilles heel of these is safety. This study presents the main issues concerning the Security of Information Systems, and estimated as an example of a security company specializing in telemedicine. In the first phase included the concept of security policy in the wider field of Information Security Management Systems, the feasibility of developing and implementing a security policy as described and the basic characteristics. The implementation methodology of the study is given as also the definition scope of it. Also is described and given the current situation in the company and the mapping of web services and applications. Next are identifying the basic principles for the development of Security Policy of Information Systems, is clarifying the legal framework for the protection of medical data and their privacy. The next section concerns the application of security policies into the company and records the necessary steps for successful and effective implementation. Finally, describe the Contingency plan and Recovery system for disasters and implement a Risk management plan.

Key words: Information Systems, Information Security Management Systems, Security Policy, Contingency and Recovery plan, Risk management plan.

Ι. ΠΡΟΛΟΓΟΣ

Σκοπός της παρούσης διπλωματικής εργασίας είναι η μελέτη ασφαλείας της πληροφορίας και των Πληροφοριακών Συστημάτων (Π.Σ), καθώς επίσης και η ανάλυση και η πρόταση ενός σχεδίου ασφαλείας, μιας εταιρείας που ειδικεύεται στην τηλεϊατρική.

Η παρακάτω μελέτη περιλαμβάνει πιο αναλυτικά τα εξής στοιχεία:

Στο 1^{ο} κεφάλαιο γίνεται μια συνολική αναφορά στα βασικά χαρακτηριστικά της μελέτης.

Στο 2^{ο} κεφάλαιο αναλύεται η μεθοδολογία υλοποίησης της. Περιγράφοντας τις φάσεις από τις οποίες αποτελείται.

Στο 3^{ο} κεφάλαιο παρουσιάζεται το πεδίο εφαρμογής της μελέτης.

Σο 4^{ο} κεφάλαιο αποτυπώνεται το Δίκτυο και τα Πληροφοριακά Συστήματα της εταιρείας. Πιο συγκεκριμένα περιγράφονται οι δικτυακές υποδομές, οι υπηρεσίες και οι εφαρμογές της καθώς και τα λογισμικά πακέτα της εταιρείας, ενώ κατηγοριοποιούνται και οι χρήστες των Π.Σ της.

Στο 5^{ο} κεφάλαιο αναλύεται η πολιτική προστασίας και οι μηχανισμοί ασφάλειας.

Στο 6^{ο} κεφάλαιο παρουσιάζεται περιληπτικά η ανάγκη διασφάλισης του ιατρικού απορρήτου και οι τρόποι αντιμετώπισης της απαραίτητης αυτής προϋπόθεσης όταν πρόκειται για ιατρικά δεδομένα.

Στο 7ο κεφάλαιο παρουσιάζεται το πλαίσιο ορισμού του σχεδίου ασφάλειας .

Στο 8^{ο} κεφάλαιο περιγράφονται οι κανόνες και τα μέτρα υλοποίησης της πολιτικής ασφάλειας, περιγράφοντας την πολιτική ασφαλείας της εταιρείας και τους βασικούς άξονες ανάπτυξης της καθώς και τα μέτρα υλοποίησης της.

Στο 9^{ο} κεφάλαιο παρουσιάζεται το σχέδιο έκτακτης ανάγκης.

Στο 10^{ο} κεφάλαιο παρατίθεται το πλάνο διαχείρισης και αντιμετώπισης κινδύνων.

Τέλος στο 11^{ο} κεφάλαιο δίνονται οι πηγές και οι αναφορές της μελέτης.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΙΙ. ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

III. ΠΙΝΑΚΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

CERT	Computer Emergency Response Team
CRAMM	CCTA Risk Analysis and Management Method
DAC	Discretionary Access Control
DBIR	Data Breach Investigation Report
DMZ	DeMilitirised Zone
DOS	Disk Operating System
DPR	Συστήματα Επεξεργασίας Δεδομένων
DSS	Συστήματα Στήριξης Αποφάσεων
EIS	Πληροφοριακά Συστήματα Ανώτερης διεύθυνσης
EMR	Electronic Medical Records
EPROM	Erasable Programmable Read Only Memory
ERM	Enterprise risk management
ERP	Συστήματα Διαχείρισης Επιχειρηματικών Πόρων
ES, KBS	Έμπειρα Συστήματα
FTP	File Transfer Protocol
FVC	Forced Vital Capacity
GPS	Global Positioning System
GSM	Global System for Mobile communications
HER	Electronic Health Records
HLS	Health Level Seven
HTTP	Secure Hypertext Transfer Protocol
ISMS	Information Security Management System
ISO	International Organisation of Standardization
ITSEC	Information Technology Security Evaluation Criteria
MAC	Mandatory Access Control
MIS	Πληροφοριακά Συστήματα Διοίκησης
PDA	Personal Digital Assistant
RAC	Role-based Access Control.
RFID	Radio-frequency identification
RPC	Remote Procedure Call
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCP/IP	Transmission Control Program/Internet Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security
UPS	Uninterrupted Power Supply
URL	Universal Resource Locator
Η/Υ	Ηλεκτρονικός Υπολογιστής
ΗΙΦ	Ηλεκτρονικός Ιατρικός Φάκελος
Λ.Σ.	Λειτουργικό Σύστημα
Π.Σ.	Πληροφορικό Σύστημα

IV. ΕΙΣΑΓΩΓΗ

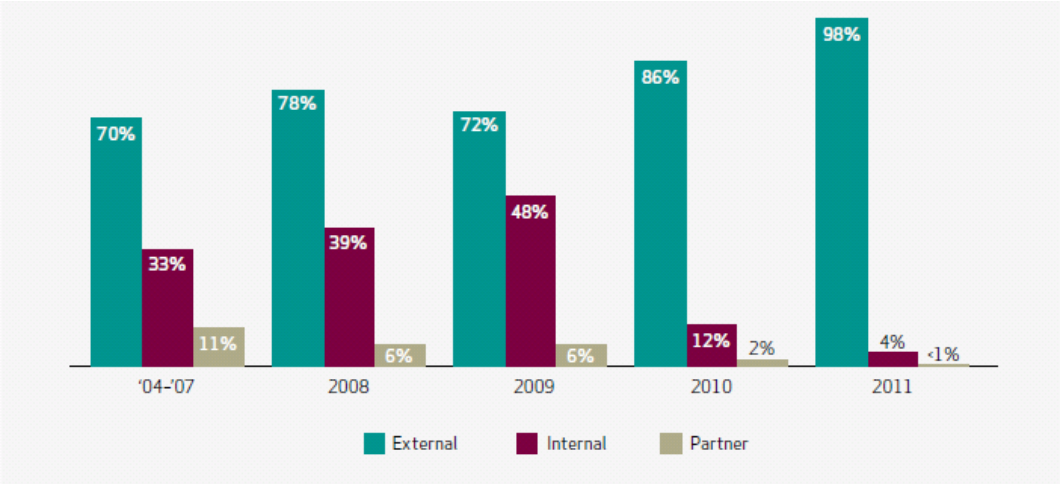
Η ελεύθερη ροή πληροφοριών, οι ευκολίες που παρέχει το Internet καθώς και το ηλεκτρονικό εμπόριο έχουν ωθήσει μέχρι και τις μικρότερες επιχειρήσεις να επενδύσουν στην χρήση πληροφοριακών συστημάτων και διαδικτυακών εφαρμογών. Η λειτουργικότητα των οργανισμών αυτών στηρίζεται στην λειτουργία των πληροφοριακών συστημάτων και η ορθή και ασφαλή λειτουργία τους κρίνεται απολύτως απαραίτητη για την επίτευξη των στόχων τους. Η παραμικρή δυσλειτουργία, διακοπή ή παράνομη διείσδυση στα συστήματα αυτά μεταφράζεται σε κόστος. Σε συστήματα που περιέχουν ευαίσθητα δεδομένα οι επιπτώσεις δεν είναι μόνο οικονομικές αλλά ζωτικής σημασίας.

Ενώ η χρήση πληροφοριακών συστημάτων είναι δεδομένη για κάθε οργανισμό η ασφάλεια τους αντίστοιχα μοιάζει να απειλείται ακόμα περισσότερο. Έρευνες Παραβίασης Δεδομένων (Data Breach Investigations Report, DBIR) που ξεκίνησαν από το 2004, έδειξαν ότι στην πραγματικότητα, το 2011 μπορεί να υπερηφανεύεται για τα υψηλά ποσοστά απώλειας δεδομένων.

Το 2011 θα μείνει ως έτος της πολιτικής και πολιτισμικής εξέγερσης. Πολίτες επαναστάτησαν, κυβερνήσεις δοκιμάστηκαν και ανατράπηκαν. Τα γεγονότα του 2011 ωστόσο δεν περιορίστηκαν μόνο στον φυσικό κόσμο. Ο διαδικτυακός κόσμος ήταν γεμάτος με συγκρούσεις ιδεωδών που πήραν την μορφή διαμαρτυριών ακτιβισμού, αντίποινων, και φαρσών. Το μεγαλύτερο μέρος των δραστηριοτήτων αυτών ήταν παραβιάσεις δεδομένων των οποίων βασική τους τακτική ήταν η κλοπή εταιρικών και προσωπικών πληροφοριών.

Σύμφωνα με έρευνα της Verizon, την παγκοσμίως γνωστή εταιρεία τηλεπικοινωνιών, που βασίστηκε σε δεδομένα από διάφορες νομικές υπηρεσίες και από διάφορες πρόσθετες πηγές όπως και από ομάδες CERT (Computer Emergency Response Team), πάνω από το 90% των παραβιάσεων σε πληροφοριακά συστήματα είναι αποτέλεσμα εξωτερικών επιθέσεων και σχεδόν το 60% των οργανισμών τις ανακαλύπτει μετά από μήνες ή χρόνια.

Η μελέτη αυτή, που πραγματοποιήθηκε από την Ομάδα Ανάλυσης κινδύνου της Verizon σε συνεργασία με την Αυστραλιανή Ομοσπονδιακή Αστυνομία, την Ολλανδική Δίωξη Ηλεκτρονικού Εγκλήματος σε Εθνικό Επίπεδο, την Υπηρεσία Ασφαλείας Πληροφόρησης και Πληροφοριών της Ιρλανδίας, την διεθνή Μονάδα Δίωξης Ηλεκτρονικού Εγκλήματος και την Μυστική Υπηρεσία των ΗΠΑ, έδειξε ότι τα κρούσματα ηλεκτρονικού εγκλήματος εκτινάχτηκαν το 2011 στο 98% των συνολικών απωλειών πληροφορίας, ενώ οι παραβιάσεις που οφείλονταν σε εσωτερικούς παράγοντες, συγκριτικά με άλλες χρονιές, μειώθηκαν στο 4%.



Εικόνα 1. Στατιστικά Αποτελέσματα Παραβιάσεων ΠΣ απο 2004-2011

Αναλυτικότερα οι εξωτερικοί παράγοντας οφείλονται σε εξωτερικές απειλές που προέρχονται από πηγές εκτός του οργανισμού και του δικτύου των συνεργατών. Τα παραδείγματα περιλαμβάνουν πρώην εργαζόμενους, hackers, οργανωμένες εγκληματικές ομάδες και κυβερνητικοί φορείς. Σε αυτή την κατηγορία επίσης συγκαταλέγονται και οι περιβαλλοντικοί παράγοντες όπως πλημμύρες, σεισμοί, και διακοπές παροχής ρεύματος.

Οι εσωτερικοί παράγοντες οφείλονται σε εσωτερικές απειλές προερχόμενες από τον οργανισμό. Αυτό περιλαμβάνει στελέχη της εταιρείας, εργαζόμενους κλπ., καθώς και από τις εσωτερικές υποδομές.

Υπάρχει και μια τρίτη κατηγορία παραγόντων που αφορά τους συνεργάτες καθώς και οποιοδήποτε τρίτο μέρος που μοιράζονται μια επιχειρηματική σχέση με τον οργανισμό. Αυτό περιλαμβάνει τους προμηθευτές, πωλητές, παροχείς υπηρεσιών φιλοξενίας, η όποια ανατιθέμενη υπηρεσία υποστήριξης πληροφορικής, κλπ. Το ποσοστό των εξωτερικών παραγόντων ξεπερνά κατά πολύ όλους τους υπόλοιπους παράγοντες. Στους εξωτερικούς παράγοντες συγκαταλέγονται

(α) οι παραβιάσεις από την χρήση κακόβουλου λογισμικό (malware),

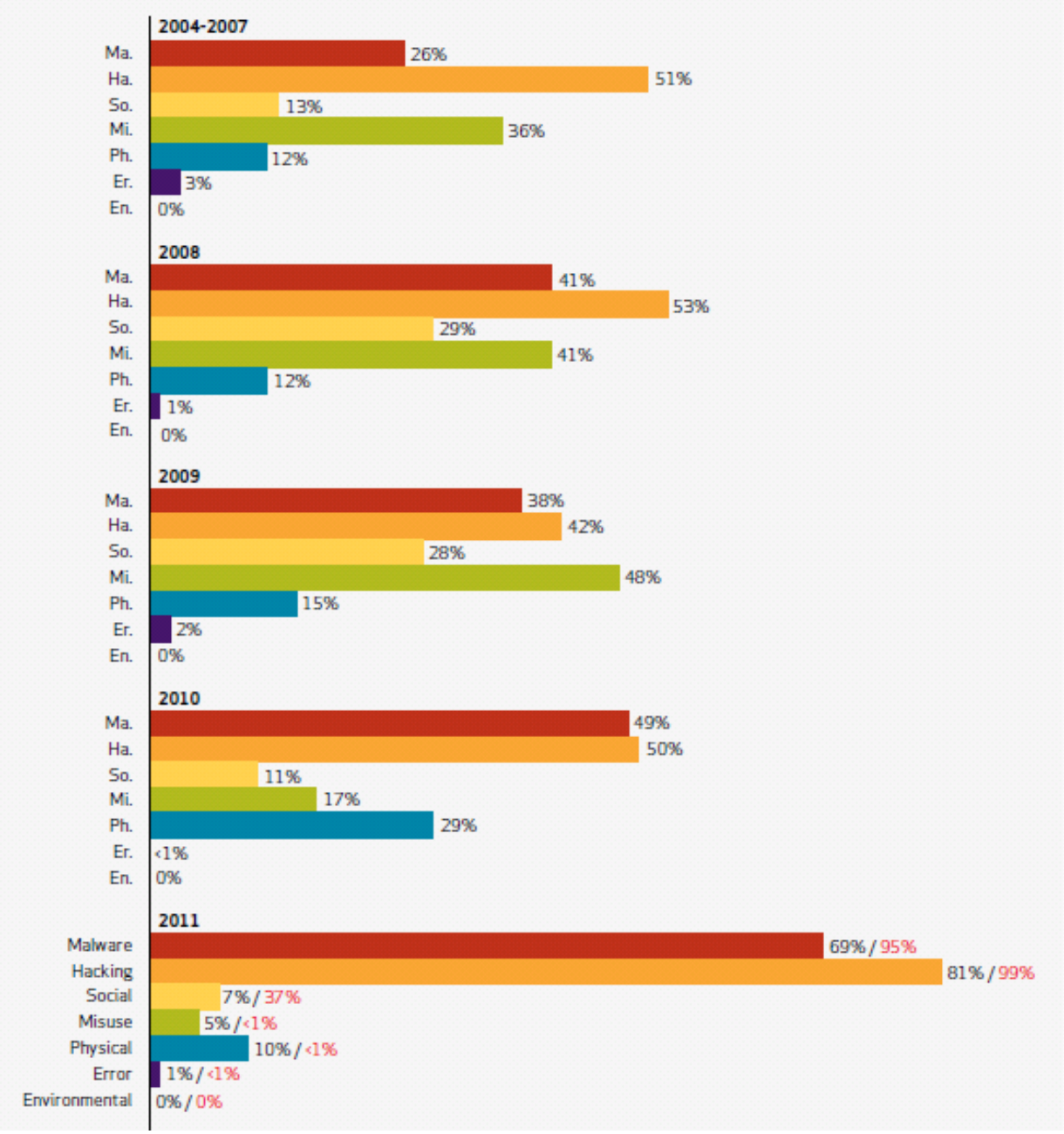
(β) οι επιθέσεις hacker και οι παραβιάσεις κοινωνικού περιεχομένου σκοπιμοτήτων(social),

(γ) η κακής χρήσης των πληροφοριακών συστημάτων (misuse)

(δ) οι φυσικές και περιβαλλοντικές απειλές (physical and environmental) και

(ε) η εμφάνιση διάφορων σφαλμάτων στα πληροφοριακά συστήματα (errors).

Στατιστικές μελέτες έδειξαν ότι την τελευταία δεκαετία το μεγαλύτερο μέρος παραβιάσεων εξωτερικών παραγόντων οφείλεται στις κακόβουλες επιθέσεις (hackers) και ένα μεγάλο ποσοστό στο κακόβουλο λογισμικό (malware).



Εικόνα 2. Αποτελέσματα έρευνας DBIR (Data Breaches Investigation Reports)

Βάσει της έρευνα της Verizon η πιο σημαντική αλλαγή που είδαμε το 2011 ήταν η άνοδος του 'hacktivism' σε όλο τον κόσμο φθάνοντας το ποσοστό 87% - 99% των συνολικών παραβιάσεων.

Το πλέγμα παρακάτω παρουσιάζει την ανάλυση των παραγόντων, τις δράσεις στα περιουσιακά στοιχεία και τα χαρακτηριστικά και την παρατήρηση και σύγκριση αυτών μαζί, για να δείξουν διασταυρώσεις μεταξύ τους. Δίνει μία μεγάλη εικόνα-λόγω των εκδηλώσεων που συνδέονται με την απειλή παραβιάσεων δεδομένων το 2011.

		Malware			Hacking			Social			Misuse			Physical			Error			Environmental		
		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
Servers	Confidentiality & Possession	381			518		1				9	8	1					2	1			
	Integrity & Authenticity	397			422		1				6	1	1									
	Availability & Utility	2			6						5											
Networks	Confidentiality & Possession										1											
	Integrity & Authenticity	1									1											
	Availability & Utility	1			1						1											
User Devices	Confidentiality & Possession	356			419						1			86								
	Integrity & Authenticity	355			355						1	1		86								
	Availability & Utility										1			3								
Offline Data	Confidentiality & Possession											23							1			
	Integrity & Authenticity																					
	Availability & Utility																					
People	Confidentiality & Possession							30	1													
	Integrity & Authenticity							59	2													
	Availability & Utility																					

Εικόνα 3. Πλέγμα Συχνότητας Απειλών 2004-2011.

Αποτέλεσμα των παραβιάσεων και των επιθέσεων αυτών, κατά των πληροφοριακών συστημάτων ενός οργανισμού οδηγούν στην ρήξη χαρακτηριστικών

όπως η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών που διαχειρίζεται και συνεπώς στην ρήξη της συνολικής ασφάλειας των συστημάτων αυτών. Αυτό αποτελεί σοβαρότατα πρόβλημα καθώς μπορεί που απειληθούν άμεσα ανθρώπινες ζωές αλλά και η ασφάλεια σε τοπικό, εθνικό αλλά και παγκόσμιο επίπεδο.

Σαφώς λοιπόν η ασφάλεια των πληροφοριακών συστημάτων αποτελεί ακρογωνιαίο λίθο για την σύγχρονη κοινωνία, για αυτό θα πρέπει να κατέχει πρωτεύοντα ρόλο κατά την σχεδίαση, συντήρηση και χρήση τους. Στην παρούσα μελέτη αναλύονται οι βασικές έννοιες της ασφάλειας των πληροφοριακών συστημάτων και πιο συγκεκριμένα το σχέδιο ασφαλείας του πληροφοριακού συστήματος μιας μικρομεσαίας εταιρείας, της Vidavo. Μια εταιρεία που ειδικεύεται στον τομέα της τηλεϊατρικής και διαχειρίζεται άμεσα ευαίσθητα προσωπικά και ιατρικά δεδομένα.

1. Βασικά χαρακτηριστικά μελέτης

1.1 Σκοπός

Η παρούσα μελέτη αφορά την ανάλυση των Βασικών εννοιών της ασφάλειας των πληροφοριακών συστημάτων και πιο συγκεκριμένα το σχέδιο ασφαλείας του πληροφοριακού συστήματος μιας μικρής εταιρείας που ειδικεύεται στον καινοτόμο τομέα της τηλεϊατρικής. Η εταιρεία Vidavo, έχει ως σκοπό την ανάπτυξη ολοκληρωμένων καινοτομικών τεχνολογικών λύσεων τηλεματικής στο χώρο της υγείας, τη συνεχή υποστήριξη των σχετικών εφαρμογών αλλά και την παροχή συμβουλευτικών υπηρεσιών για την αποτελεσματικότερη αξιοποίηση της ιατρικής πληροφορικής και της τηλεματικής στην υγεία. Επίσης διαθέτει προϊόντα υψηλής

τεχνολογίας και πρωτοποριακών υπηρεσιών τηλεματικής, που ενθαρρύνουν τους πολίτες να αναλάβουν ενεργό ρόλο στην παρακολούθηση της υγείας και της φυσικής τους κατάστασης, ενώ παράλληλα βελτιώνουν τη ζωή τους υποστηρίζοντας την αυτόνομη διαβίωση και την εξατομικευμένη φροντίδα καθώς και τη διαχείριση ιατρικών δεδομένων από απόσταση, γεφυρώνοντας τους πολίτες με τους φορείς παροχής υπηρεσιών υγείας και παρέχοντας εξελιγμένες υπηρεσίες υγείας στην περιφέρεια.

Η μελέτη περιλαμβάνει:

• Τον καθορισμό των κανόνων ασφαλείας που πρέπει να τηρούνται για την ορθή χρήση του πληροφοριακού συστήματος

• Τον προσδιορισμό των χρηστών και των ρόλων τους

• Την περιγραφή των δικαιωμάτων τους στο πληροφοριακό σύστημα

• Την ορθή χρήση των συστημάτων

• Τις περιπτώσεις παραβίασης

• Τα μέτρα αντιμετώπισης των παραβιάσεων

•Τα βήματα υλοποίησης μιας ολοκληρωμένης πολιτικής ασφαλείας.

•Την δημιουργία ενός ολοκληρωμένου σχεδίου ασφαλείας που θα περιλαμβάνει ένα σχέδιο έκτακτης ανάγκης και ανάκαμψης σε περίπτωση κάποιας καταστροφής καθώς και ένα πλάνο διαχείρισης και αντιμετώπισης των κινδύνων.

1.2 Θεμελιώδεις Έννοιες Ασφαλείας

Η ασφάλεια πληροφοριακών συστημάτων είναι κλάδος της επιστήμης της πληροφορικής που ασχολείται με την προστασία των υπολογιστών, των δικτύων που τους συνδέουν και των δεδομένων σε αυτά τα συστήματα, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους. Ανάμεσα στους συγγενικούς τομείς της ασφάλειας πληροφοριακών συστημάτων συμπεριλαμβάνονται η ψηφιακή εγκληματολογία και η εφαρμοσμένη κρυπτογραφία.

1.3 Προϋποθέσεις ασφάλειας Π.Σ.

Η ασφάλεια των πληροφοριακών συστημάτων είναι πολύ σημαντική καθώς στηρίζεται σε τρεις βασικές ιδέες οι οποίες είναι απαραίτητες για την ορθή λειτουργία ενός Π.Σ., και είναι οι εξής:

Ακεραιότητα (Integrity): Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή/και χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια. *Για παράδειγμα, μια εφημερίδα που δημοσιεύει τα άρθρα της και στο Διαδίκτυο θα ήθελε αυτά τα άρθρα να είναι ασφαλή από μετατροπές ενός χάκερ που επιθυμεί να εισάγει λανθασμένες πληροφορίες στα κείμενα.*

Διαθεσιμότητα (Availability): Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους. Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DOS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι, είτε προσωρινά είτε μόνιμα. Η άρνηση υπηρεσιών δεν προκαλείται αναγκαία από εχθρική επίθεση. *Για παράδειγμα: το φαινόμενο Slashdot, κατά το οποίο ένας σύνδεσμος προς μια ιστοσελίδα φιλοξενούμενη σε διακομιστή με σύνδεση χαμηλής χωρητικότητας δημοσιεύεται σε δημοφιλή ιστότοπο, με συνέπεια εκατοντάδες χιλιάδες αναγνώστες να υπερφορτώσουν τη σύνδεση της αναφερομένης ιστοσελίδας, προκαλεί το ίδιο αποτέλεσμα.*

Εμπιστευτικότητα (Confidentiality): Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα. Η διαρροή ευαίσθητων πληροφοριών μπορεί να γίνει με πιο παραδοσιακές μεθόδους από την ψηφιακή υποκλοπή. *Για παράδειγμα: με την κλοπή φορητών υπολογιστών από το κατάλληλο τμήμα μιας εταιρίας. Το 2006 μια μελέτη με τη συνεργασία 480 εταιριών έδειχνε ότι 80% των εταιριών είχε πρόβλημα με διαρροή πληροφοριών λόγο κλοπής φορητού.*

Εικόνα 4. Βασικές Αρχές Ασφάλειας.

1.4 Εμπλεκόμενοι στην Ανάπτυξη Πολιτικών Ασφάλειας

Η ανάπτυξη της πολιτικής ασφάλειας των πληροφοριακών συστημάτων ενός οργανισμού βασίζεται στην καταγραφή των απαιτήσεων ασφάλειας, με βάση τις οποίες διαμορφώνονται οι στόχοι της ασφάλειας, και στον προσδιορισμό των τρόπων για την επίτευξη των στόχων αυτών. Οι απαιτήσεις ασφάλειας μπορεί να προέρχονται από διαφορετικές πηγές, όπως:

Οι χρήστες των πληροφοριακών συστημάτων.

- Η διοίκηση του οργανισμού που επιθυμεί την απρόσκοπτη χρήση των πληροφοριακών συστημάτων στις λειτουργίες του οργανισμού.
- Οι πελάτες του οργανισμού, εφόσον δεδομένα που τους αφορούν αποτελούν συνιστώσα του πληροφοριακού συστήματος.
- Το νομικό και ρυθμιστικό πλαίσιο στο οποίο λειτουργεί ο οργανισμός.

Η πολιτική ασφάλειας θα πρέπει να ικανοποιεί όλες τις απαιτήσεις ασφάλειας που προκύπτουν για τα πληροφοριακά συστήματα, και μάλιστα με αναλογικό τρόπο, δηλαδή τα μέτρα και οι οδηγίες που περιλαμβάνει να εξασφαλίζουν το επιθυμητό επίπεδο ασφάλειας.

1.5 Ανάλυση Επικινδυνότητας

Η διαμόρφωση της πολιτικής ασφάλειας για τα πληροφοριακά συστήματα ενός οργανισμού έπεται της αξιολόγησης του επιπέδου ασφάλειας των συστημάτων αυτών. Η αξιολόγηση της ασφάλειας μπορεί να γίνει με διάφορους τρόπους, οι πιο συνηθισμένοι από αυτούς είναι η εκπόνηση μιας μελέτης ανάλυσης επικινδυνότητας (Risk Analysis) και η χρήση κάποιων από τα πρότυπα (standards) διαχείρισης της ασφάλειας.

Για καλύτερη κατανόηση αρχικά δίνονται οι βασικοί ορισμοί που χρησιμοποιούνται ευρέως στην ανάλυση κινδύνων:

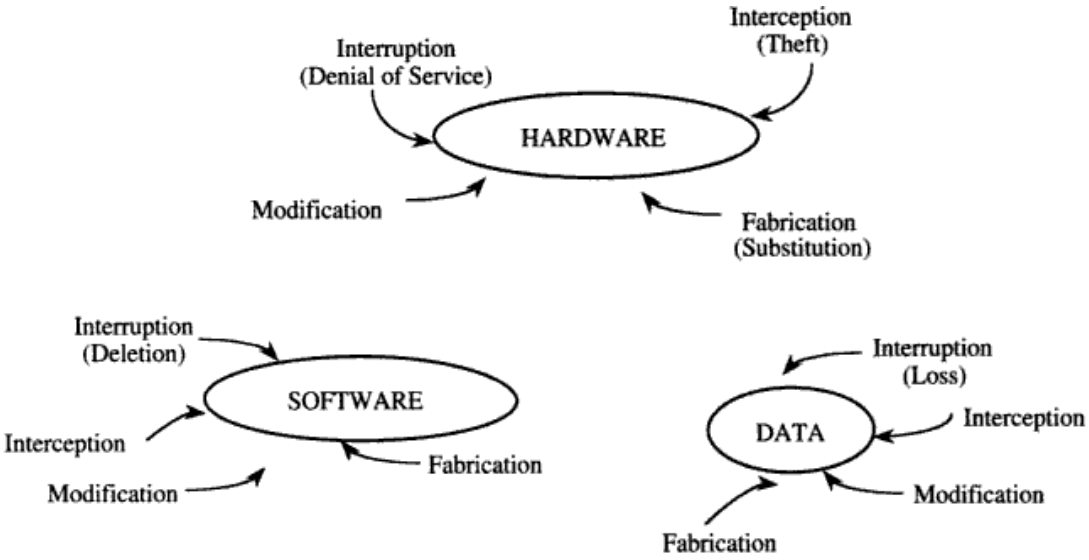
Απειλή: Ένα μη επιθυμητό γεγονός που μπορεί να προκαλέσει μη διαθεσιμότητα του συστήματος και των υπηρεσιών, τυχαία ή με πρόθεση μετατροπή των δεδομένων, καταστροφή των δεδομένων ή του συστήματος και τέλος μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών.

Ευπάθεια: Είναι η αδυναμία ή σχεδιαστική ατέλεια σε ένα σύστημα, στην εφαρμογή ή στην υποδομή που μπορεί να γίνει αιτία για την παραβίαση της ασφάλειας και της ακεραιότητας του συστήματος. Η ευπάθεια μπορεί να οριστεί και με την εξής συνάρτηση:

Ευπάθεια = Πιθανότητα να συμβεί μια απειλή x Πιθανότητα να είναι επιτυχής

Κίνδυνος: Η πιθανότητα μια συγκεκριμένη απειλή να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια. Ο κίνδυνος εκφράζει το ενδεχόμενο για απώλεια.

Αντίμετρο: Μέτρο που λαμβάνεται για την προστασία του πληροφοριακού συστήματος και την αντιμετώπιση των απειλών. Το μέτρο μπορεί να ενεργεί ανιχνεύοντας, προλαμβάνοντας ή μειώνοντας την απώλεια που σχετίζεται με την εμφάνιση μιας απειλής ή κατηγορίας απειλών.



Εικόνα 5. Ευπάθειες ενός Πληροφοριακού Συστήματος (ΠΣ)

1.5.1 Οφέλη Ανάλυσης Επικινδυνότητας

Με την διαδικασία της ανάλυσης των κινδύνων, προκύπτουν τα εξής οφέλη:

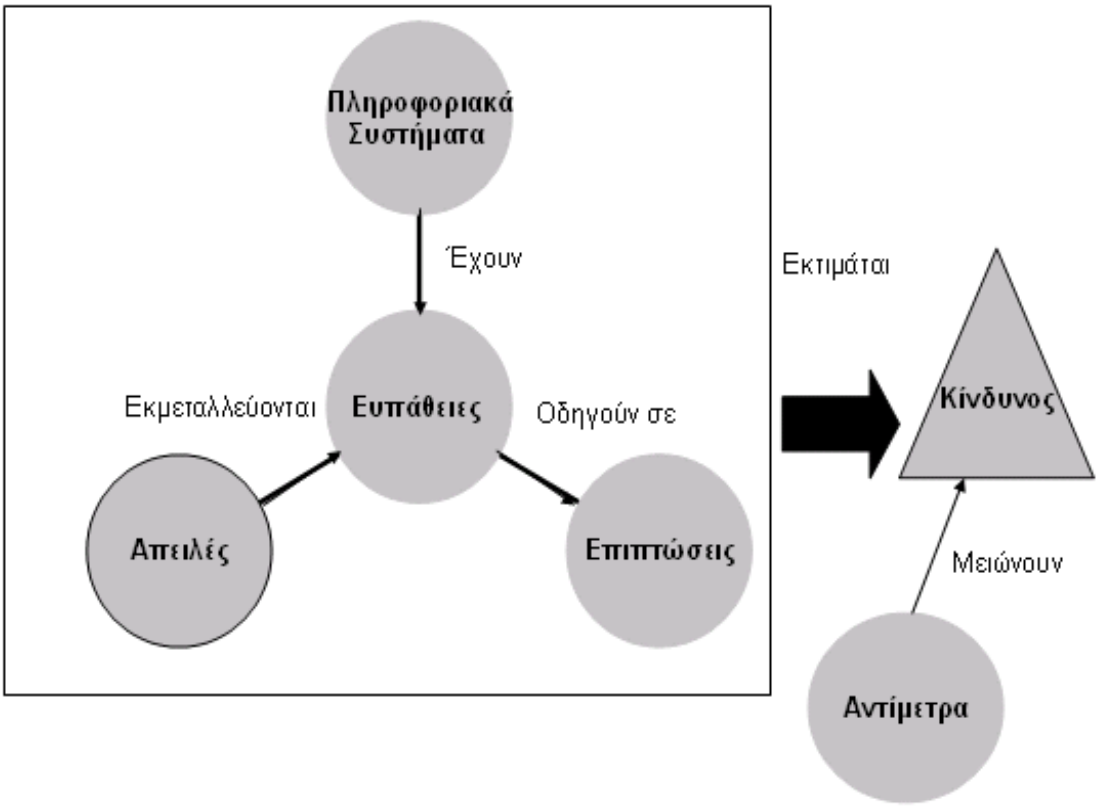
(α) Γενική βελτίωση της ασφάλειας του πληροφοριακού συστήματος

(β) Στόχευση της ασφάλειας

(γ) Βελτίωση της κατανόησης του συστήματος

(δ) Κατανόηση της αναγκαιότητας της ασφάλειας και

(ε) Δικαιολόγηση των δαπανών για την ασφάλεια



Εικόνα 6. Συσχέτιση των παραγόντων της ανάλυσης επικινδυνότητας.

1.5.2 Μέθοδοι ανάλυσης επικινδυνότητας

Για την αξιολόγηση, ή αλλιώς αποτίμηση, του επιπέδου ασφάλειας των πληροφοριακών συστημάτων μπορούν να εφαρμοστούν διάφορες τεχνικές α*νάλυσης επικινδυνότητας*. Οι πιο διαδεδομένες από τις οποίες αυτές οι SBA (Security By Analysis), η MARION και η CRAMM (CCTA Risk Analysis and Management Method). Σε αυτήν την περίπτωση, η διαμόρφωση της πολιτικής ασφάλειας γίνεται με βάση τα αποτελέσματα της ανάλυσης επικινδυνότητας.

Σημαντικά πλεονεκτήματα της πρακτικής αυτής είναι ότι η πολιτική ασφάλειας ανταποκρίνεται στις ιδιαίτερες ανάγκες του οργανισμού για τον οποίο έχει μελετηθεί η επικινδυνότητα, και ότι το επίπεδο της παρεχόμενης ασφάλειας με την κατάλληλη επιλογή των μέτρων προστασίας είναι αντίστοιχο των κινδύνων που τα πληροφοριακά συστήματα του οργανισμού αντιμετωπίζουν. Μειονέκτημα της προσέγγισης αυτής είναι το στοιχείο του υποκειμενισμού που εμπεριέχεται στις

μεθόδους ανάλυσης επικινδυνότητας, τα αποτελέσματα των οποίων εξαρτώνται σε μεγάλο βαθμό από την εμπειρία και τις γνώσεις του αναλυτή.

1.5.3 Τύπος BPL

Καρδιά της ανάλυσης κινδύνων αποτελεί ο τύπος: ***B > P * L***

Τα τρία στοιχεία του τύπου BPL είναι:

B = Το κόστος για την πρόληψη μιας απώλειας

P = Η πιθανότητα να συμβεί μια απώλεια

L = Το συνολικό κόστος μιας απώλειας

Ο τύπος αυτός αποτελεί την κεντρική ιδέα πίσω από κάθε ανάλυση κινδύνων, όχι μόνο για πληροφοριακά συστήματα. Την ιδέα του υπολογισμού της πιο συμφέρουσας λύσης. Ωστόσο αν και ο υπολογισμός του τύπου και η πρακτική του εφαρμογή βρίσκουν σημαντικές δυσκολίες, όλες οι μέθοδοι της ανάλυσης κινδύνων βασίζονται πάνω στην λογική του τύπου BPL.

Το νόημα του τύπου είναι ότι όταν το κόστος της πρόληψης μιας απώλειας είναι μεγαλύτερο από το γινόμενο του κόστους της απώλειας επί την πιθανότητα να συμβεί αυτή τότε η υλοποίηση του μέτρο πρόληψης κρίνεται ως υπερβολική. Στην αντίθετη περίπτωση το μέτρο πρόληψης συμφέρει να υλοποιηθεί. Συνήθως τα μεγέθη υπολογίζονται σε ετήσιες απώλειες και ετήσια πιθανότητα να συμβεί ένα γεγονός. Η αντιστοίχηση των απωλειών με οικονομικά νούμερα δεν είναι πάντα δυνατή διότι πολλές φορές στην ανάλυση κινδύνων αξιολογούνται απώλειες απροσδιόριστες όπως η εικόνα ενός οργανισμού και η εμπιστοσύνη που έχουν οι «πελάτες» του σε αυτόν.

1.6 Μέτρα Ασφαλείας

Η πολιτική ασφαλείας συμπληρώνεται από τα Μέτρα Ασφαλείας / Μέτρα Προστασίας (controls) ή Αντίμετρα (countermeasures)}, που αφορούν όλες τις διαδικασίες, τις τεχνικές, τις ενέργειες και τις συσκευές που περιορίζουν τις ευπάθειες και τις απειλές του πληροφοριακού συστήματος, καθώς και από το Πλάνο Υλοποίησης τους.

Τα αντίμετρα χωρίζονται σε 4 μεγάλες κατηγορίες:

(α) *Πρόληψη*: τα αντίμετρα αυτά προσπαθούν να μειώσουν τον κίνδυνο

(β) *Διασφάλιση*: εργαλεία, έλεγχοι και στρατηγικές που διασφαλίζουν την συνεχή αποτελεσματικότητα των παρόντων αντιμέτρων

(γ) *Ανίχνευση*: προγράμματα και τεχνικές για την έγκαιρη ανίχνευση, αναχαίτιση και αντιμετώπιση περιστατικών

(δ) *Επαναφορά:* διαδικασίες που στοχεύουν στην γρήγορη επαναφορά σε ένα ασφαλές περιβάλλον έπειτα από ρήξη ασφαλείας και στην έρευνα της αιτίας που την προκάλεσε.

Για την επιτυχή εφαρμογή της πολιτικής ασφαλείας, το σχέδιο ασφαλείας πρέπει να περιλαμβάνει και συγκεκριμένες διαδικασίες συνεχούς ενημέρωσης με επισκοπήσεις - επιθεωρήσεις της εφαρμογής του, ώστε με τις κατάλληλες αναθεωρήσεις να είναι πάντα up-to-date σε σχέση με τις τεχνολογικές εξελίξεις και τις αλλαγές στην εταιρεία.

Ολοκληρώνοντας το σχέδιο ασφαλείας της εταιρείας, θα καταρτισθεί αναλυτικό σχέδιο έκτακτης ανάγκης, το οποίο θα περιλαμβάνει σχέδιο ανάκαμψης από καταστροφή (disaster recovery plan), καθώς και σχέδιο αποκατάστασης λειτουργίας (contingency action plan). Η εισαγωγή (προσθήκη μηχανισμών) ασφαλείας σε ένα πληροφοριακό σύστημα είναι ένα δύσκολο και περίπλοκο έργο. Για την ελληνική πραγματικότητα ίσως η πλέον σημαντική δυσκολία οφείλεται στο σημαντικό κόστος της ασφάλειας.

2 Μεθοδολογία Υλοποίησης

Η διαμόρφωση μιας ολοκληρωμένης πολιτικής ασφαλείας και η υλοποίηση ενός ολοκληρωμένου συστήματος ασφάλειας πληροφοριών απαιτεί την εκτέλεση ορισμένων βημάτων, για την ακρίβεια πέντε φάσεων.

2.1 Φάση 1η «Καταγραφή υφιστάμενης κατάστασης»

Στη φάση αυτή θα καταγραφεί η υπολογιστική και επικοινωνιακή υποδομή της επιχείρησης, δηλαδή όλων των περιουσιακών στοιχείων (assets) της εταιρείας. Τα περιουσιακά στοιχεία μιας εταιρείας μπορεί να χωριστούν στις παρακάτω κατηγορίες:

*Δεδομένα (Data assets):*Στην κατηγορία αυτή ανήκουν κάθε είδους δεδομένα, από δεδομένα προσωπικού χαρακτήρα σε μια βάση δεδομένων μέχρι και οι καταχωρήσεις σε έναν DNS server.

*Υπηρεσίες (End User Services):*Στην κατηγορία αυτή ανήκουν οι υπηρεσίες που επιτρέπουν στον τελικό χρήστη πρόσβαση στα δεδομένα. Για παράδειγμα η υπηρεσία πρόσβασης σε μια βάση δεδομένων που επιτρέπει στους χρήστες να προσπελάσουν τα δεδομένα που αυτή περιέχει.

Υλικά Στοιχεία: Η κατηγορία αυτή περιλαμβάνει τα υλικά στοιχεία που αποτελούν το υπολογιστικό σύστημα, δηλαδή τους υπολογιστές, το δίκτυο, μέσα αποθήκευσης κτλ.

Τοποθεσίες: Στην κατηγορία αυτή περιλαμβάνονται τα δωμάτια, κτίρια ή ακόμα και οικόπεδα τα οποία ανήκουν στον οργανισμό και περιέχουν μέρη των υπολογιστικών συστημάτων

Λογισμικό (software): Η κατηγορία αυτή μπορεί να χρησιμοποιηθεί σε οργανισμούς που παράγουν λογισμικό και επομένως είναι υψίστης σημασίας η προστασία του κώδικα.

Εφόσον γίνει η καταγραφή της υφιστάμενης κατάστασης, έπειτα αναλύονται οι πληροφοριακές διαδικασίες στη λειτουργία της εταιρείας και προσδιορίζεται ο ρόλος όλων των χρηστών, κατατάσσοντας τους σε κατηγορίες. Καταγράφονται επίσης όλες οι διαδικασίες της εταιρείας που σχετίζονται με την ασφάλεια του πληροφοριακού συστήματος και στη συνέχεια γίνεται η αξιολόγηση όλων των στοιχείων καθώς και η αξιολόγηση των υφιστάμενων μέτρων ασφαλείας τους. Τέλος, αναλύονται οι

ιδιαιτερότητες του πληροφοριακού συστήματος, όσον αφορά τα ευαίσθητα προσωπικά δεδομένα που τηρούνται από την εταιρεία.

2.2 Φάση 2η «Ανάλυση επικινδυνότητας»

Στη φάση αυτή και εφόσον έχει γίνει η ακριβής εκτίμηση και καθορισμός των περιουσιακών στοιχείων (assets) της εταιρείας και έχει εκτιμηθεί η αξία τους προς την εταιρεία, θα πρέπει να γίνει ανάλυση της επικινδυνότητας. Ένα πολύ σημαντικό βήμα για την χάραξη της πολιτικής που θα ακολουθήσει η εταιρεία για την υλοποίηση της ασφαλείας του Πληροφοριακού της Συστήματος (Π.Σ.). Για την ακρίβεια, εδώ γίνεται μελέτη των εκθέσεων σε κινδύνους (exposures) του συστήματος, προσδιορίζοντας τις ευπάθειες (vulnerabilities) και τις απειλές (threats) του συστήματος με βάση τον υφιστάμενο έλεγχο (control).

Η μέθοδος που θα ακολουθηθεί για την διενέργεια της ανάλυσης κινδύνων θα βασίζεται στον τύπο BPL που θα συγκρίνει το κόστος για την πρόληψη μιας απώλειας ή ζημιάς με το κόστος που προκαλεί αυτή η απώλεια, σε συνδυασμό με την πιθανότητα να συμβεί αυτή η απώλεια. Η μελέτη της υφιστάμενης κατάστασης θα βοηθήσει στην επιλογή του κατάλληλου μοντέλου (π.χ. εμπιστευτικότητας – BLP, ακεραιότητας – Biba, ροής πληροφοριών ή άλλου) που θα υιοθετηθεί στην εκπόνηση της πολιτικής και την κατάρτιση του σχεδίου ασφαλείας.

Αναλυτικότερα η ανάλυση επικινδυνότητας (Risk Analysis) του πληροφοριακού συστήματος αποτελείται από τα εξής βήματα:

Βήμα 1ο:. Η αναγνώριση των απειλών (threats) κατά του πληροφοριακού συστήματος Για κάθε κατηγορία περιουσιακών στοιχείων υπάρχουν και μια σειρά από απειλές. Στο βήμα αυτό αναγνωρίζονται οι απειλές για κάθε στοιχείο και οι επιπτώσεις που αυτές επιφέρουν.

Βήμα 2ο.: Η αναγνώριση των επιμέρους ευπαθειών (vulnerabilities). Ένα περιουσιακό στοιχείο μπορεί να είναι λιγότερο ευπαθής προς μια απειλή και περισσότερο προς μια άλλη. Διευκρινίζεται η ευπάθεια του κάθε περιουσιακού στοιχείου προς κάθε απειλή ξεχωριστά.

Βήμα 3ο. Η αναγνώριση των πιθανών κατηγοριών απωλειών (losses). Η κατηγοριοποίηση γίνεται βάσει του βαθμού κινδύνου που υπολογίζεται ξεχωριστά για κάθε απειλή και είναι συνάρτηση όλων των παραπάνω, δηλαδή των επιπτώσεων μιας

απειλής, που έχουν σχέση με την αξία του περιουσιακού στοιχείου, και της ευπάθειας του περιουσιακού στοιχείου ως προς την απειλή.

Βήμα 4^{ο}. Η εκτίμηση της πιθανότητας να συμβεί μια απώλεια. Αφού τελειώσει το στάδιο της αντιστοίχησης των απειλών τότε πρέπει να γίνει η αξιολόγηση της πιθανότητας να συμβεί μια απειλή σε κάθε περιουσιακό στοιχείο, καθώς και η ευπάθεια του προς την απειλή αυτή.

Βήμα 5^{ο}. Προσδιορισμό των απαραίτητων προφυλάξεων / αντίμετρων (countermeasures) για την αντιμετώπιση των κινδύνων. Υπάρχουν 3 τρόποι αντιμετώπισης του κινδύνου η αποφυγή του κινδύνου με πλήρη απόσυρση από μια συγκεκριμένη δραστηριότητα, η αποδοχή του κινδύνου και η μείωση του κινδύνου με χρήση αντιμέτρων (μέτρων ασφαλείας). Κατά το βήμα αυτό αναγνωρίζονται τα πιθανά αντίμετρα που μπορούν να εφαρμοστούν και επιλέγονται αυτά που συμφέρουν περισσότερο στην εταιρεία.

Βήμα 6^{ο}. Η διαμόρφωση και υλοποίηση του πλέον αποτελεσματικού και ενδεδειγμένου από άποψη κόστους (cost effective) συστήματος ασφαλείας.

Ωστόσο μια συνεχής παρακολούθηση των κινδύνων επιβάλλεται καθώς τα δεδομένα σε ένα πληροφοριακό σύστημα αλλάζουν συνεχώς, εισάγονται νέες απειλές, νέες ευπάθειες, νέες επιπτώσεις κτλ. Τα αντίμετρα που έχουν επιλεχθεί θα πρέπει να ελέγχονται συνεχώς για την αποτελεσματικότητα τους καθώς πολλά από αυτά με τον καιρό σταματούν να συμφέρουν και πρέπει να καταργηθούν ή να αντικατασταθούν από νέα αντίμετρα.

Για να είναι πλήρης η ανάλυση της επικινδυνότητας (Risk analysis) ενός ΠΣ, θα πρέπει να ληφθούν υπόψιν όλες οι απειλές είτε είναι ως προς την ασφάλεια του υπολογιστικού συστήματος(computer security) , είτε προς τις δικτυακές υποδομές, (network security), είτε ως προς την Φυσική Ασφάλεια (physical security) του συστήματος. Οι απειλές, μπορούν να κατηγοριοποιηθούν με βάση το περιεχόμενο τους σε κατηγορίες απειλών Λογικής Διείσδυσης (logical infiltration), Επικοινωνιακής Διείσδυσης (communications infiltration), Αποτυχίας Εξοπλισμού (failures of equipment) και Φυσικών Απειλών (physical threats) πχ. από φωτιά, πλημμύρα κτλ.

Σημαντική κατηγορία απειλών είναι αυτή της Λογικής Διείσδυσης (logical infiltration) στην Ασφάλεια Υπολογιστικού συστήματος. Η ασφάλεια του υπολογιστικού συστήματος αναφέρεται στην προστασία των πληροφοριών του συστήματος που διαχειρίζεται το λειτουργικό σύστημα (εφαρμογές, αρχεία δεδομένων, κ.ά.). Καθώς και στην Ασφάλεια βάσεων δεδομένων (database security) που σχετίζεται με την προστασία των περιεχομένων μιας βάσης δεδομένων.

Άλλη μια κατηγορία απειλών που δεν θα πρέπει να παραληφτεί είναι αυτή της Επικοινωνιακής Διείσδυσης (communications infiltration), που αφορά την ασφάλεια των δικτύων επικοινωνιών και αναφέρεται στις απειλές στην προστασία των πληροφοριών.

Τέλος, θα πρέπει να αναγνωριστούν και οι απειλές ως προς την Φυσική ασφάλεια ενός οργανισμού που περιλαμβάνει τη προστασία ολόκληρου του σχετικού εξοπλισμού του από φυσικές καταστροφές. Στόχος της είναι η πρόληψη απώλειας, ζημιών, έκθεσης των πόρων του οργανισμού και διακοπής των επιχειρησιακών δραστηριοτήτων του οργανισμού. Ο εξοπλισμός θα πρέπει να προστατεύεται φυσικά από κινδύνους ασφάλειας και περιβαλλοντολογικές απειλές. Συνεπώς, η προστασία του εξοπλισμού είναι απαραίτητη προκειμένου να ελαχιστοποιηθεί ο κίνδυνος μη εξουσιοδοτημένης προσπέλασης των δεδομένων, όπως και η προστασία απέναντι στο ενδεχόμενο απώλειας ή καταστροφής.

2.3 Φάση 3η «Πολιτική ασφαλείας»

Σκοπός της πολιτικής ασφάλειας πληροφοριών είναι η παροχή κατευθύνσεων και υποστήριξης για ζητήματα ασφάλειας πληροφοριών. Η πολιτική ασφάλειας καθορίζεται από την διοίκηση του οργανισμού και θα πρέπει να υποστηρίζεται έμπρακτα από την ίδια. Η πολιτική αυτή θα πρέπει να ρυθμίζει ζητήματα ασφάλειας σε όλα τα επίπεδα του οργανισμού.

Επιγραμματικά η φάση αυτή περιλαμβάνει την καταγραφή και εκπόνηση του συνόλου των νόμων, κανόνων και πρακτικών που ρυθμίζουν πως τα στοιχεία διαχειρίζονται, προστατεύονται και κατανέμονται μέσα σε έναν οργανισμό χρηστών. Η εκπόνηση θα γίνει με βάση τη διάκριση των υποκειμένων (ενεργά στοιχεία του συστήματος όπως χρήστες, διεργασίες και προγράμματα) και αντικειμένων (αρχεία, κατάλογοι, συσκευές, υποδοχές – sockets κ.α.), στηριγμένη στο σύστημα των ρόλων και αρμοδιοτήτων (roles and responsibilities). Κατά την χάραξη της πολιτικής ασφαλείας θα υιοθετηθούν διεθνή πρότυπα (standards), όπως τα TCSEC και ITSEC.

Το κείμενο της πολιτικής ασφάλειας θα πρέπει να γίνει αποδεκτό από τη διοίκηση του οργανισμού. Στη συνέχεια θα πρέπει να δημοσιοποιηθεί σε όλους τους χρήστες του οργανισμού. Θα πρέπει να αναφέρει τη δέσμευση της διοίκησης και τον τρόπο προσέγγισης του οργανισμού σε θέματα ασφάλειας. Σε γενικές γραμμές η πολιτική ασφαλείας θα περιλαμβάνει τα παρακάτω στοιχεία:

- *Αγαθά (Assets):* Καθορισμός των αγαθών του οργανισμού, αφηρημένων και μη.

• *Ρόλους και αρμοδιότητες (Roles and Responsibilities*): Τον ορισμό γενικών και ειδικών καθηκόντων για τη διαχείριση της ασφάλειας και την αναφορά συμβάντων.

• *Στόχους (Security policy objectives):* Τους στόχους της ασφαλείας και τον καθορισμό περιορισμών.

• *Πεδίο εφαρμογής της πολιτικής ασφαλείας (Scope of Security Policy):* Τον ορισμό της ασφάλειας των πληροφοριών, το σκοπό της και τη σπουδαιότητά της ως μηχανισμού που επιτρέπει την ανταλλαγή πληροφοριών. Γενικά, τον καθορισμό την εμβέλειας της πολιτικής ασφαλείας.

• *Οδηγίες, κατευθυντήριες γραμμές (Guidelines):* Την επεξήγηση της πολιτικής ασφάλειας, των αρχών, των προτύπων και των απαιτήσεων που πρέπει να ικανοποιεί ο οργανισμός, όπως σχετική νομοθεσία, προστασία από ιούς, επιπτώσεις μη συμμόρφωσης με την πολιτική ασφάλειας, διαχείριση επιχειρηματικής συνέχειας κλπ.

• *Κουλτούρα, άλλες πολιτικές, νομοθεσία (Culture, legislation, other policies):* Το σύνολο πεποιθήσεων, αξιών, αρχών πολιτικών, κωδίκων δεοντολογίας και νόμων που συνθέτουν την κουλτούρα του οργανισμού.

• Υλοποίηση και εφαρμογή - Ενημέρωση και συμμόρφωση (Implementation and application of the security policy – Awareness, enforcement, breach): Πρόκειται για το οργανωτικό πλαίσιο για την υλοποίηση και την εφαρμογής της πολιτικής ασφαλείας καθώς και ενημέρωση του προσωπικού και συμμόρφωση με τις ενέργειες που λαμβάνονται σε περίπτωση παραβίασης της πολιτικής ασφαλείας.

• *Επισκόπηση και αναθεώρηση της πολιτικής (Review and audit):* Πρόκειται για την επισκόπηση και αναθεώρηση της πολιτικής, ανά τακτικά χρονικά διαστήματα ανάλογα και με τις συνθήκες, έτσι ώστε να καλύπτει τις ανάγκες του οργανισμού.

Οι κανόνες (rules) που θα εκφράσουν την πολιτική ασφαλείας θα εκφράζουν γενικότερες αρχές της εταιρείας, θα ικανοποιούν τα χαρακτηριστικά απλότητας(χωρίς περιττούς τεχνικούς όρους και εξειδικευμένες αναφορές), της σαφήνειας, της εφαρμοσιμότητας, θα είναι γενικεύσιμοι και επεκτάσιμοι και θα απαιτούν συμμόρφωση από όλο το προσωπικό της εταιρείας, στο οποίο θα είναι διαθέσιμοι.

Σε δεύτερο επίπεδο, στη φάση αυτή θα ολοκληρωθεί η εκπόνηση των απαιτήσεων ασφαλείας του πληροφοριακού συστήματος, σύμφωνα με την ανάλυση επικινδυνότητας και την πολιτική ασφαλείας που έχει εκπονηθεί. Στη φάση αυτή θα επιλεγούν και τα κατάλληλα μοντέλα ασφαλείας του πληροφοριακού συστήματος(των επάλληλων στρωμάτων, του κιβωτισμού κλπ.) που θα χρησιμοποιηθούν ως βάση για την δημιουργία των μηχανισμών και των μέτρων προστασίας.

2.4 Φάση 4η «Καθορισμός Μέτρων Ασφαλείας»

Η φάση αυτή αφορά την βασική υλοποίηση του Σχεδίου Ασφαλείας με τον σχεδιασμό των μέτρων που θα ικανοποιήσουν τις απαιτήσεις ασφαλείας του συστήματος.

Τα μέτρα που σχεδιάζονται θα καλύπτουν τις παρακάτω βασικές κατηγορίες:

- Οργάνωση και διαχείριση της ασφάλειας του πληροφοριακού συστήματος
- Ασφάλεια ανάπτυξης και συντήρησης του πληροφοριακού συστήματος
- Φυσική ασφάλεια
- Ασφάλεια δεδομένων
- Ασφάλεια της υπολογιστικής και τηλεπικοινωνιακής υποδομής

Τα μέτρα που αφορούν την οργάνωση και τη διαχείριση του Π.Σ. πιο συγκεκριμένα αφορούν τον σχεδιασμό της ασφάλειας του Π.Σ., τον κώδικα δεοντολογίας του οργανισμού, μέτρα ως προς τον έλεγχο και την εποπτεία της ασφάλειας του Π.Σ. αλλά και ως προς τους ρόλους και τις αρμοδιότητες για την διαχείριση της ασφάλειας. Επίσης, περιλαμβάνει και μέτρα για τη εκπαίδευση και ενημέρωση των χρηστών για τις διαδικασίες και γενικότερα για τις λειτουργίες σχετικά με την ασφάλεια του Π.Σ.

Τα μέτρα που αφορούν την ασφάλεια ανάπτυξης και την συντήρηση του Π.Σ. περιλαμβάνουν μέτρα ανάπτυξης και συντήρησης εφαρμογών (Application development and maintenance), μέτρα για την διαχείρισης και υποστήριξη υλικού και λογισμικού από προμηθευτές (Vendor support-contracts reliability), καθώς και μέτρα για την απογραφή του υλικού και λογισμικού και διαχείριση των αλλαγών (hardware and software inventory).

Μέτρα για την φυσική ασφάλεια αποτελούν τα μέτρα για την ασφάλεια των κτιριακών εγκαταστάσεων, του εξοπλισμού πληροφορικής αλλά και της τηλεπικοινωνιακής υποδομής όπως και μέτρα ως προς τις φυσικές καταστροφές.

Άλλη μια σημαντική κατηγορία μέτρων είναι αυτή για την ασφάλεια των δεδομένων και περιλαμβάνει τους μηχανισμούς εξασφάλισης της ακεραιότητας και της εμπιστευτικότητας των δεδομένων και τα μέτρα για την κατηγοριοποίηση και ταξινόμηση των δεδομένων (Classification of data).

Και τέλος, όσον αφορά την ασφάλεια υπολογιστικής και τηλεπικοινωνιακής υποδομής εδώ συγκαταλέγονται τα εξής: οι διαδικασίες διαχείρισης εφεδρικών αντιγράφων ασφαλείας, οι διαδικασίες αντιμετώπισης ιών, οι διαδικασίες διαχείρισης συνθηματικών και έλεγχου προσπέλασης στα Π.Σ. καθώς και καταγραφής παραβιάσεων. Επίσης, και όλα τα μέτρα για την ασφάλεια των εφαρμογών, των βάσεων δεδομένων , των δικτύων καθώς της ασφάλειας κατά της σύνδεσης στο διαδίκτυο.

Η αποτελεσματικότητα των μέτρων προστασίας ή αντιμέτρων εξαρτάται από το πόσο σωστά χρησιμοποιούνται. Βασικοί παράγοντες που θα πρέπει να καλύπτονται στην κατεύθυνση αυτή είναι:

1. Επίγνωση του μεγέθους του προβλήματος από τους εμπλεκόμενους χρήστες.

2. Σχεδιασμός περιοδικών επισκοπήσεων και αναθεωρήσεων των μέτρων. Ο προσδιορισμός διαδικασιών τακτικής επιθεώρησης και ανασκόπησης των μέτρων ασφαλείας αποτελεί μια από τις σημαντικότερες συνιστώσες επιτυχίας ενός σχεδίου ασφαλείας.

3. Αλληλοεπικάλυψη των μέτρων. Ένας συνδυασμός μέτρων ελαχιστοποιεί τις απειλές και αυξάνει την αξιοπιστία του συστήματος προστασίας.

4. Αυξημένες πιθανότητες χρησιμοποίησης. Πρωταρχική προϋπόθεση για την απόδοση ενός μέτρου είναι να βρίσκεται σε εφαρμογή την κατάλληλη στιγμή, που απαιτεί να είναι επαρκές, κατάλληλο και εύκολο στη χρήση του.

Σε δεύτερο επίπεδο, στη φάση αυτή καταστρώνεται το πλάνο υλοποίησης που αφορά στον επιμερισμό ευθυνών και αρμοδιοτήτων για την εκτέλεση των επιμέρους εργασιών του έργου υλοποίησης των μέτρων ασφαλείας, καθώς και το σχετικό χρονοδιάγραμμα υλοποίησής τους. Η UniPlan παρέχει στο επίπεδο αυτό τις απαραίτητες συμβουλευτικές υπηρεσίες και υποστήριξη στην διαδικασία υλοποίησης των μέτρων ασφαλείας.

2.5 Φάση 5η «Σχέδιο έκτακτης ανάγκης»

Το Σχέδιο Έκτακτης Ανάγκης συμπληρώνει το σχέδιο ασφαλείας, καταγράφοντας τις διαδικασίες και υλοποιώντας μέτρα που εξασφαλίζουν την εταιρεία στην

αντιμετώπιση τέτοιας έκτασης καταστροφών που ουσιαστικά είναι αδύνατη η άμεση (ή έστω εντός λίγων ωρών ή/και ημερών) επαναλειτουργία του πληροφοριακού συστήματος. Αφορά δύο βασικές κατηγορίες: α) περιπτώσεις δυσλειτουργίας και β) περιπτώσεις ολικής καταστροφής.

Το σχέδιο έκτακτης ανάγκης θα πρέπει να περιλαμβάνει:

• Προσδιορισμός πιθανών κινδύνων και κριτηρίων για ενεργοποίηση του σχεδίου. Πρέπει να υπάρχουν σαφείς και γραπτές διαδικασίες που να θέτουν τον οργανισμό σε κατάσταση έκτακτης ανάγκης και να επιτρέπουν ανάκληση του σχεδίου.

• Προσδιορισμό των σημαντικών λειτουργιών και των αντίστοιχων συστημάτων (critical functions and systems) της εταιρείας,

• Καθορισμό της στρατηγικής προστασίας (protection strategy),

• Ιεράρχηση των δραστηριοτήτων και καθορισμός προτεραιοτήτων για την ενεργοποίησή τους στο εναλλακτικό σύστημα,

• Πλάνο Υλοποίησης με αρμοδιότητες προσωπικού και χρονοπρογραμματισμό ενεργειών αποκατάστασης. Το σχέδιο πρέπει να περιέχει μια κατάσταση με τα μέλη του προσωπικού που θα κληθούν στην περίπτωση καταστροφής καθώς και τα τηλέφωνα των προμηθευτών υλικού και λογισμικού, των σημαντικών συνεργατών ή πελατών, των ατόμων που βρίσκονται σε διαφορετικές εγκαταστάσεις που θα χρησιμοποιηθούν από την επιχείρηση για τη συνέχιση της λειτουργίας της.

Το σχέδιο έκτακτης ανάγκης θα πρέπει να πραγματεύεται, εκτός και την ανάκαμψη της λειτουργίας της υπολογιστικής και επικοινωνιακής υποδομής μετά από φυσικές καταστροφές (φωτιές, πλημμύρες, σεισμούς, κτλ.). Επιπλέον, εκτός από το λεπτομερειακό σχέδιο αποκατάστασης λειτουργίας της εταιρείας, δύναται να εκπονηθεί ένα σχέδιο ανάκαμψης από καταστροφή που θα προβλέπει και εφεδρική εγκατάσταση (disaster recovery facility), ενώ εξετάζεται και το θέμα της διάθεσης εναλλακτικής τοποθεσίας (alternate site).

3 Πεδίο εφαρμογής

Ορίζοντας το πεδίο εφαρμογής της μελέτης θα αναλυθεί αρχικά ο υπολογιστικός εξοπλισμός της εταιρείας, έπειτα η δικτυακή και τηλεπικοινωνιακή υποδομή της και τέλος οι χρήστες των συστημάτων της εταιρείας εκτός και εντός αυτής.

Πριν οριστεί ο υπολογιστικός εξοπλισμός της εταιρείας και η δικτυακή υποδομή της θα πρέπει να τονιστεί ότι τα περιουσιακά στοιχεία συσχετίζονται άμεσα μεταξύ τους. Τα δεδομένα μιας βάσης δεδομένων συσχετίζονται με την υπηρεσία πρόσβασης της βάσης δεδομένων, με τον υπολογιστή που περιέχει την βάση δεδομένων καθώς και με το δωμάτιο που βρίσκεται αυτός ο υπολογιστής. Το κάθε στοιχείο λοιπόν μεταφέρει ή προσθέτει απειλές και ευπάθειες στο άλλο και η ενδεχόμενη καταστροφή κάποιου από αυτά οδηγεί σε απώλεια ως προς την εταιρεία. Σε συνάντηση με υπεύθυνο της εταιρείας έγινε καταγραφή της υφιστάμενης κατάστασης του υπολογιστικού εξοπλισμού, αναγνώριση των βασικών υπηρεσιών της εταιρείας, όπως και των βάσεων δεδομένων που χρησιμοποιούν οι υπηρεσίες αυτές, όπως και των υπολοίπων διαδικτυακών εφαρμογών.

Συγκεκριμένα όσον αφορά τον υπολογιστικό εξοπλισμό της εταιρείας καταγράφηκαν τα εξής:

Οι servers της εταιρείας είναι εγκατεστημένοι σε ειδικό διαμορφωμένο χώρο μεγάλης ασφάλειας, ο οποίος λειτουργεί ως *Computer room* και είναι συνδεδεμένοι με το τοπικό δίκτυο της εταιρείας. Στο χώρο αυτό βρίσκονται συνολικά πέντε servers της εταιρείας καθώς επίσης εκεί φυλάσσονται και τα εφεδρικά αρχεία (backups) της. Το λειτουργικό σύστημα που διαθέτουν είναι Windows server 2000 και Red hat Enterprise Linux.

Οι servers του τοπικού δικτύου είναι εγκατεστημένοι σε ξεχωριστό χώρο εντός της εταιρείας, στο *Lab*, και δίνουν την δυνατότητα κεντρικής διαχείρισης και διαμοιρασμού αρχείων / εκτυπωτών. Στον χώρο αυτό υπάρχουν δυο servers που εξυπηρετούν υπηρεσίες της εταιρείας .

Μαζί με κάθε υπηρεσία της εταιρείας καταγράφθηκαν και οι βάσεις δεδομένων αυτών. Στην ουσία αναλύθηκαν μόνο αυτές που κρίθηκαν ότι είναι πολύ σημαντικές για την ασφάλεια των δεδομένων της εταιρείας, αλλά και για την εύρυθμη λειτουργία της, και είναι οι εξής:

Υπηρεσία Κεντρικού Backup: Σε τακτά χρονικά διαστήματα δημιουργούνται αντίγραφα ασφαλείας.

Υπηρεσία Vida 24: Πρωτοποριακό σύστημα τηλεμετρίας ιατρικών παραμέτρων που επιτρέπει την διαχείριση ιατρικών δεδομένων από απόσταση.

Υπηρεσία Vida track: Υπηρεσία διασφάλισης ευελιξίας και ασφάλειας ευαίσθητων και ευάλωτων ατόμων (ηλικιωμένοι, παιδία, άτομα με αναπηρία, χρόνια πάθηση)

Υπηρεσία Vida Ψ: Πρωτοποριακό σύστημα τηλεψυχιατρικής με παράλληλη μετάδοση δεδομένων ηλεκτρονικού ψυχιατρικού φακέλου, εικόνας και ήχου.

Καθώς και βάσεις δεδομένων για την υπηρεσία Vida Shop, Vidahome, pmp, Mobile applications (Vida 24 mobile, Vidahealth mob) και Pc Applications **(**εφαρμογές όπου η συσκευή συνδέεται μέσω Bluetooth, τα δεδομένα αποστέλλονται μέσω διαδικτύου από τον χρήστη στο server**)**

Χρήστες – Ομάδες

Οι χρήστες των συστημάτων της εταιρείας μπορούν να ομαδοποιηθούν σε εσωτερικούς χρήστες, που ανταποκρίνονται στις εσωτερικές δραστηριότητες και διεργασίες της εταιρείας. Αυτοί οι χρήστες ανήκουν στους παρακάτω τομείς:

- Διοικητικό συμβούλιο.
- Τομέας τεχνικών υπηρεσιών ανάπτυξης και υποστήριξης λογισμικού
- Τομέας επιχειρηματικής ανάπτυξης και καινοτομίας:
- Τομέας έρευνας και ανάπτυξης

Και τους εξωτερικούς χρήστες της εταιρείας, που μπορούν να έχουν πρόσβαση στις εφαρμογές και τις υπηρεσίες της και είναι οι εξής:

- Γενικός ιατρός
- Εξειδικευμένο προσωπικό
- Ασθενείς, Νοσηλευτές / συγγενικά πρόσωπα

4 Αποτύπωση Δικτύου και Πληροφοριακών Συστημάτων

4.1 Δικτυακές Υποδομές και Δίκτυα επικοινωνιών (περιγραφή computer room & lab)

Στα πληροφοριακά συστήματα της εταιρείας, για την σωστή και ασφαλή εκτέλεση των λειτουργιών της, υπάρχει συνεχή στήριξη και αναβάθμιση των πληροφοριακών συστημάτων από το προσωπικό που κατέχει την απαραίτητη γνώση.

Στο κτήριο της εταιρείας υπάρχει ένας μικρός αυτόνομος χώρος (computer room) όπου στεγάζονται οι τηλεπικοινωνιακές και υπολογιστικές υποδομές. Συγκεκριμένα, υπάρχει ένα κέντρο επικοινωνίας, αρκετοί κεντρικοί εξυπηρετητές (backup servers, database server, file server κ.α) στους οποίους υπάρχουν διάφορα εξειδικευμένα λειτουργικά συστήματα όπως Windows 2003 Server, Linux κ.α για την υποστήριξη των λειτουργιών της. Μερικές από τις κεντρικές εφαρμογές που υποστηρίζουν είναι Vida24, VidaΨ, Vidahome και Vidatrack.

Οι εξυπηρετητές εκτός των άλλων χρησιμοποιούνται από τους χρήστες σε μεγάλο βαθμό και ως file servers για την αποθήκευση και τη διαχείριση των προσωπικών τους αρχείων αλλά και για τη δημιουργία αντιγράφων ασφαλείας.

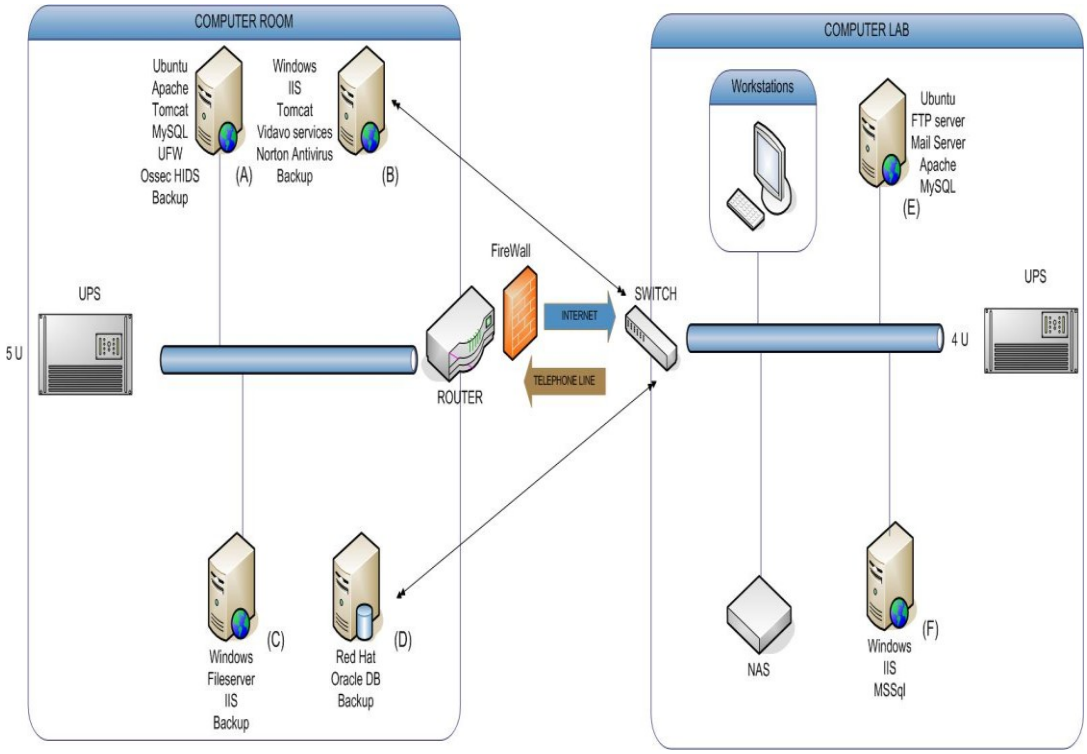
Η εταιρεία για να προστατέψει τους προσωπικούς της υπολογιστές από κακόβουλες επιθέσεις έχει εγκαταστήσει Eset Smart Security που περιέχει antivirus , firewall, antispyware και antispam. Επίσης, χρησιμοποιούν αυτόματο backup της Seagate και των Windows. Όσο για την προστασία των server της έχει εγκαταστήσει ασφάλεια Linux, Anticlam firewalls και σύστημα HID OSSEC, καθώς επίσης και Windows backups και την αντίστοιχη εφαρμογή για τον Linux server.

Όλες οι βάσεις δεδομένων που χρησιμοποιούν οι υπηρεσίες της Vidavo είναι κωδικοποιημένες, και δεν είναι δυνατή η προσπέλαση τους από οποιοδήποτε εκτός από το Διαχειριστή συστήματος μέσω της χρήσης πολλαπλών επιπέδων ασφαλείας (λειτουργικού συστήματος και βάσεως δεδομένων). Τα συστήματα ασφαλείας προστατεύουν από την μη εξουσιοδοτημένη πρόσβαση (hacking). Ένα από τα βασικά στοιχεία ασφαλείας είναι ότι δεν υπάρχει καμία δυνατότητα διαγραφής η παραμετροποίησης των δεδομένων εφόσον εισαχθούν στις βάσεις. Έτσι διασφαλίζεται η ακεραιότητα τους αλλά και το προσωπικό απόρρητο των χρηστών.

Οι εξυπηρετητές (servers) είναι εγκατεστημένοι σε ειδικό διαμορφωμένο χώρο υψηλής ασφάλειας, ο οποίος λειτουργεί ως data center και είναι συνδεδεμένοι με το τοπικό δίκτυο της εταιρείας. Το λειτουργικό σύστημα που διαθέτουν είναι Windows 2000 και Redhat Enterprise Linux.

Οι servers του τοπικού δικτύου, οι εκτυπωτές και το rack των συνδέσεων, είναι τοποθετημένα σε ξεχωριστό χώρο εντός της εταιρείας (lab) και δίνουν την δυνατότητα κεντρικής διαχείρισης, διαμοιρασμού αρχείων/ εκτυπωτών, προστασίας – antivirus.

Η Vidavo έχει κάνει σημαντική επένδυση στην ασφάλεια των δικτύων της, χρησιμοποιώντας antivirus σε κάθε προσωπικό υπολογιστή με αυξημένο δείκτη προστασίας ώστε να μειώσει τον κίνδυνο διείσδυσης από ανθρώπινο λάθος. Οι εξυπηρετητές της έχουν άμεση έκθεση στο διαδίκτυο μέσω firewall, antivirus αλλά και λογισμικά παρακολούθησης κίνησης δικτύου πραγματικού χρόνου, ώστε να αντιμετωπιστούν τυχόν εξωτερικές επιθέσεις καθιστώντας έτσι σταθερό το δίκτυο της.



Εικόνα 7. Αποτύπωση Δικτυακής Υποδομής

4.2 Υπηρεσίες – εφαρμογές

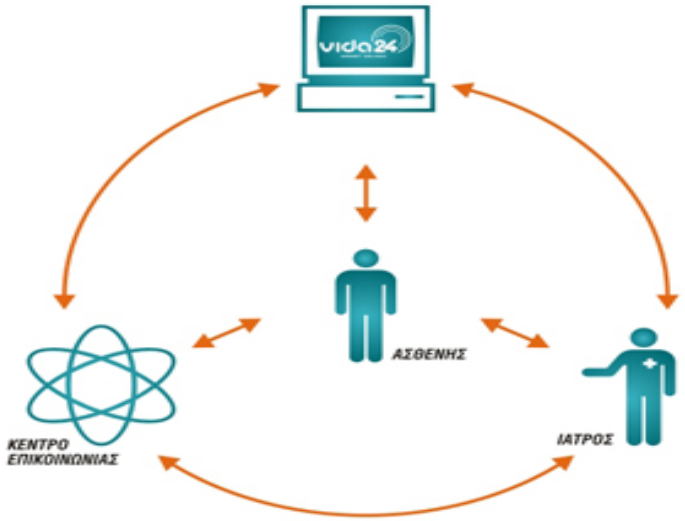
Στην φάση αυτή ακολουθεί περιγραφή των υπηρεσιών και των διαδικτυακών εφαρμογών της εταιρείας, παραθέτοντας τα βασικά χαρακτηριστικά της καθεμιάς χωριστά, τα σενάρια λειτουργίας τους καθώς και τους χρήστες τους.

4.2.1 Υπηρεσία Vida 24

4.2.1.1 Χαρακτηριστικά συστήματος

Το σύστημα τηλεμετρίας ιατρικών παραμέτρων της VIDAVO αποτελεί μία διαδικτυακή εφαρμογή για την καταγραφή και παρακολούθηση από απόσταση των βιολογικών σημάτων χρόνιων ασθενών και πολιτών που επιθυμούν να διατηρούν τη φυσική τους κατάσταση προς την ευεξία. Το σύστημα βασίζεται στις τεχνολογίες κινητών επικοινωνιών και νέας γενιάς τηλεϊατρικών συσκευών αυτόματης μέτρησης και ασύρματης μετάδοσης των βιολογικών σημάτων, αξιοποιώντας παράλληλα τεχνολογία έξυπνων καρτών για την ταυτοποίηση των χρηστών και δημιουργεί προοπτικές ανάπτυξης μιας νέας αγοράς για την παροχή προηγμένων συνδρομητικών υπηρεσιών υγείας. Η υπηρεσία vida24 διατίθεται σε άτομα με χρόνιες παθήσεις μέσω των ιατρών που τους παρακολουθούν, αλλά και σε πολίτες που επιθυμούν την παρακολούθηση της φυσικής τους κατάστασης, καθώς και σε διαγνωστικά κέντρα, ιδιωτικές κλινικές, ασφαλιστικές εταιρίες και νοσοκομεία.

Η συνολική λειτουργία του συστήματος και η ροή της πληροφορίας, αποτυπώνεται παρακάτω:



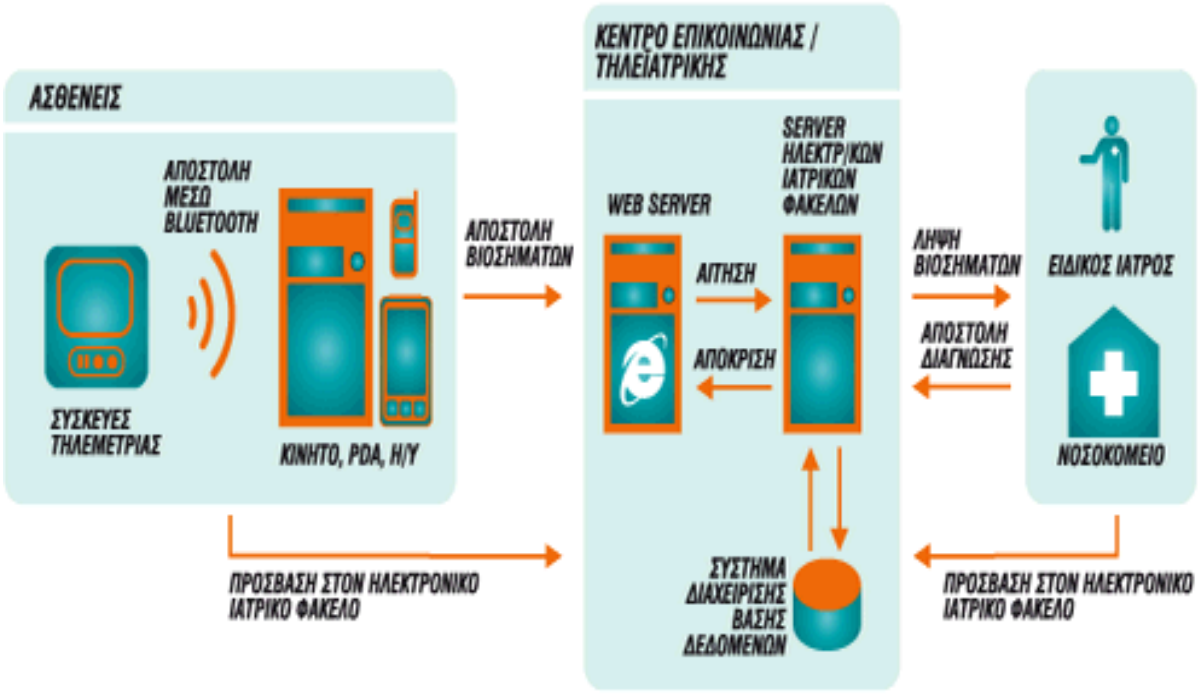
Εικόνα 8. Ροή Πληροφορίας Π.Σ. Vidavo

4.2.1.2 Σενάριο λειτουργίας φορητής βιολογικής τηλεμετρίας

Για τη λειτουργία της υπηρεσίας, ο χρήστης εφοδιάζεται με την κατάλληλη συσκευή καταγραφής βιολογικών σημάτων *(Καρδιογράφο, Σπιρόμετρο, Οξύμετρο, Πιεσόμετρο, Γλυκοζόμετρο, Καρδιοτοκογράφο*) και λογισμικό λήψης & διαχείρισης ιατρικού σήματος.

Οι καταγεγραμμένες μετρήσεις μεταφέρονται μέσω Bluetooth σε συσκευή ασύρματης πρόσβασης (κινητό τηλέφωνο, Smartphone, H/Y) και προωθούνται σε ένα κέντρο επικοινωνίας, όπου είναι διαθέσιμες συνεχώς (24 ώρες) για διάγνωση από το εξειδικευμένο ιατρικό προσωπικό.

Η υπηρεσία διασφαλίζει (όταν αυτό χρειάζεται) τη μέτρηση των φυσιολογικών παραμέτρων του ασθενούς τη στιγμή της κρίσης ή σε στιγμές που ο ασθενής αισθάνεται πόνο ή ενοχλήσεις και δεν μπορεί να επισκεφτεί ιατρό και επίσης, την αποστολή των μετρήσεων στο νοσοκομείο, όπου και θα αξιολογηθούν από εξειδικευμένους ιατρούς.



Εικόνα 9. Σενάριο λειτουργίας ΥπηρεσίαςVida24

4.2.1.3 Σενάριο λειτουργίας σταθερής βιολογικής τηλεμετρίας

Ο χρήστης εξοπλίζεται με μία συσκευή ακουστικής μετάδοσης όπως καρδιογράφο, ή σπιρόμετρο ανάλογα με τα βιολογικά σήματα που κρίνεται αναγκαίο να παρακολουθήσει.

Ο κάτοχος μιας εκ των δύο συσκευών, έχει την δυνατότητα να πραγματοποιήσει την μέτρηση από το σπίτι η από όπου αλλού βρίσκεται αρκεί να υπάρχει σύνδεση με το σταθερό τηλεφωνικό δίκτυο ή με την βοήθεια της ομάδας επέμβασης κατά τη διάρκεια κατ' οίκον επισκέψεων (π.χ. Βοήθεια στο σπίτι). Ο ασθενής τοποθετεί την συσκευή στα σημεία που του υποδεικνύονται και η μέτρηση καταγράφεται.

Ο χρήστης καλεί τον αριθμό του τηλεφωνικού κέντρου της εταιρείας και όταν του απαντήσουν, τοποθετεί τη συσκευή του στο ακουστικό του τηλεφώνου και με το πάτημα ενός κουμπιού αποστέλλει τα καταγεγραμμένα βιολογικά σήματα σε ένα κέντρο επικοινωνίας. Μέσω του ειδικού modem λήψης βιολογικών σημάτων η μέτρηση λαμβάνεται και καταχωρείται στην εφαρμογή λήψης & διαχείρισης ιατρικού σήματος που είναι εγκατεστημένη στον εξυπηρετητή της εταιρείας.

Με την είσοδο του στην εφαρμογή το εξειδικευμένο προσωπικό μπορεί να διαχειριστεί στοιχεία που χωρίζονται σε 2 υποενότητες την περιγραφή των προσωπικών στοιχείων και ιατρικών δεδομένων του πολίτη την περιγραφή των δημογραφικών στοιχείων του ιατρικού προσωπικού.

Χρησιμοποιώντας αυτή την εφαρμογή ο χρήστης, ελέγχει τις μετρήσεις και αν κρίνετε πρέπει να αποσταλούν σε ειδικό ιατρό τότε έχει την δυνατότητα: να στείλει τη μέτρηση χρησιμοποιώντας email στον ειδικό γιατρό να αποστείλει με fax την μέτρηση στο ειδικό γιατρό επικοινωνήσει τηλεφωνικά στο γιατρό και εκείνος με την σειρά του να συνδεθεί σε αντιστοιχισμένο σημείο στον υπολογιστή του κατευθείαν με την βάση δεδομένων.

4.2.1.4 Χρήστες και οφέλη

Την υπηρεσία μπορούν να παρέχουν ιδιωτικοί και δημόσιοι φορείς παροχής υπηρεσιών υγείας (πχ Νοσοκομεία, Κλινικές, Διαγνωστικά & Ιατρικά Κέντρα), Ασφαλιστικές εταιρίες, οι οποίες ενσωματώνουν στις υπηρεσίες τους και υπηρεσίες υγείας αλλά και ενώσεις επαγγελματιών υγείας που επιθυμούν τη δικτύωση με εξειδικευμένους συναδέλφους τους. Τελικοί χρήστες της υπηρεσίας είναι ασθενείς με χρόνιες παθήσεις, άτομα που αναρρώνουν μετεγχειρητικά εκτός του νοσοκομειακού περιβάλλοντος, ηλικιωμένοι που πρέπει να παρακολουθούν την κατάσταση της

υγείας τους, άτομα με ειδικές ανάγκες, εγκυμονούσες, αθλητές και αθλητικές ομάδες, για την παρακολούθηση της κατάστασης της υγείας τους και την τήρηση αρχείων σχετικά με τα ζωτικής σημασίας στοιχεία τους, πριν και μετά την άσκηση στο χώρο του αθλητισμού, αλλά και όλοι οι πολίτες που επιθυμούν να παρακολουθούν την κατάσταση της υγείας τους (προληπτική ιατρική)

Τα βασικά οφέλη της υπηρεσίας είναι:

• Εξυπηρέτηση μεγαλύτερου αριθμού ατόμων λόγω εξοικονόμησης χρόνου.

• Δυνατότητα μετρήσεων από το χώρο του πολίτη, επομένως προστιθέμενη αξία στην υπηρεσία του ιατρού.

• Δημιουργία αισθήματος ασφάλειας, επομένως αυξημένη εμπιστοσύνη των πολιτών προς τον ιατρό και δημιουργία ισχυρών δεσμών μαζί του.

• Επικοινωνία με τον πολίτη χωρίς γεωγραφικούς περιορισμούς.

• Προσφορά προηγμένων υπηρεσιών υγείας.

• Εξαγωγή και αξιοποίηση μετρήσιμων ανώνυμων στοιχείων για στατιστικούς και ερευνητικούς σκοπούς.

• Κοινωνική προσφορά σε όλους τους πολίτες ανεξαιρέτως.

• Διευκόλυνση του κλινικού προσωπικού και αποτελεσματικότερη διαχείριση πόρων.

• Διάχυση εξειδικευμένης γνώσης.

• Τήρηση ηλεκτρονικού αρχείου.

• Ασφαλής ενσωμάτωση των τεχνολογιών πληροφορικής στην υγεία και εντοπισμός βέλτιστων λύσεων για την κάλυψη των αναγκών του φορέα, μέσω ολοκληρωμένων τεχνοοικονομικών μελετών.

• Αποτελεσματικότερη αξιοποίηση των επενδυτικών κονδυλίων του φορέα με αποτελεσματική παρακολούθηση των επιμέρους διαδικασιών, από την επιλογή των προμηθευτών, μέχρι την παραγγελία και παραλαβή των ολοκληρωμένων έργων.

• Ανάπτυξη καινοτόμων προϊόντων και υπηρεσιών και χρηματοδότησή τους με την από κοινού συμμετοχή σε ερευνητικά έργα (εθνικά και διεθνή) με παροχή

εξειδικευμένης γνώσης στον τομέα της ιατρικής πληροφορικής και στη διαχείρισή τους

Τα κυριότερα οφέλη ως προς τους τελικού αποδέκτες είναι η βελτίωση της ποιότητας ζωής τους, λόγω καλύτερης διαχείρισης της πάθησης και ενεργής συμμετοχής στην φροντίδα της υγείας, η άμεση επικοινωνία με τον ιατρό ανεξάρτητα από τη γεωγραφική απόσταση, η δυνατότητα προληπτικής ιατρικής και παρακολούθησης περιορίζοντας τις άσκοπες μετακινήσεις. Επίσης μέσω της υπηρεσίας δίνεται η δυνατότητα στον χρήστη να συμμετέχει σε καθημερινές δραστηριότητες ενώ παράλληλα ο ιατρός παρακολουθεί την κατάσταση της υγείας τους. Με την παρακολούθηση της φυσικής κατάστασης, ενισχύεται η αυτοπεποίθηση ου ασθενή και η ευεξία του να φτάνει σε υψηλά επίπεδα αλλά και εξίσου σημαντικό διατηρείται το ιατρικό ιστορικό του.

4.2.2 Υπηρεσία Vidatrack

4.2.2.1 Χαρακτηριστικά συστήματος

Αυτή είναι άλλη μια εξελιγμένη τεχνολογικά υπηρεσία της VIDAVO για την διασφάλιση ευελιξίας και ασφάλειας ευαίσθητων και ευάλωτων ατόμων (ηλικιωμένοι, παιδιά, άτομα με αναπηρία, άτομα με χρόνια πάθηση) και παρέχεται ανεξάρτητα ή σε συνδυασμό με την υπηρεσία τηλεμετρίας vida24..

Η vidatrack δίνει τη δυνατότητα εκπομπής σήματος έκτακτης ανάγκης ηλικιωμένων και ατόμων με χρόνια προβλήματα υγείας αλλά και εντοπισμού θέσης ατόμων με Alzheimer (ή άλλες νοητικές ασθένειες) και παιδιών.

4.2.2.2 Σενάριο λειτουργίας

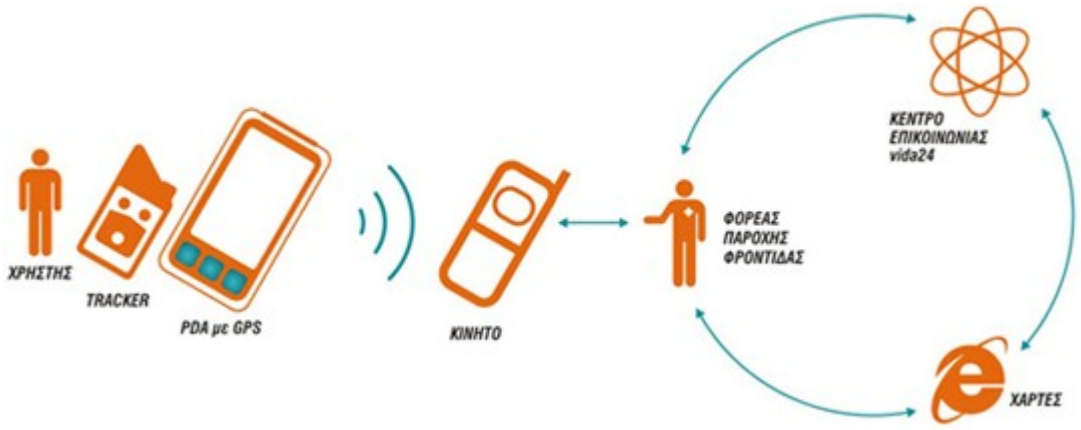
Για τη λειτουργία της υπηρεσίας, ο χρήστης (ηλικιωμένος, ασθενής, ΑΜΕΑ, άτομα μοναχικά, άτομα με άνοια) εφοδιάζεται με μια συσκευή εντοπισμού, η οποία συνδυάζει GPS και GSM και λειτουργεί σαν ένα απλοποιημένο κινητό τηλέφωνο, το οποίο αποστέλλει και συντεταγμένες θέσης. Η συσκευή διαθέτει και διεπαφή panic button για εκπομπή σήματος έκτακτης ανάγκης. Παρέχοντας έτσι τη δυνατότητα παρακολούθησης θέσης του ασθενή αλλά και ειδοποίησης / ενεργοποίησης ενδιαφερόμενων για επέμβαση.

Σενάριο 1 (alert button)

Σε περίπτωση που ο χρήστης αισθανθεί πόνο ή δυσφορία, μπορεί με μια απλή ενέργεια (πατώντας το πλήκτρο SOS) να ειδοποιήσει τους οικείους του, ή σε περίπτωση παροχής της υπηρεσίας από οργανωμένο κέντρο, να ειδοποιήσει ομάδα επέμβασης (με ασθενοφόρο ή άλλο τρόπο). Ο ειδοποιούμενος έχει τη δυνατότητα να εισέλθει στο σύστημα από οπουδήποτε έχει πρόσβαση σε διαδικτυακή συσκευή (H/Y, Smartphone) και να εντοπίσει την τοποθεσία που βρίσκεται ο χρήστης βλέποντας την καταγραφή της θέσης και της κίνησης του στο χάρτη ή να λάβει στο κινητό του SMS με τη διεύθυνση.

Σενάριο 2 (location tracking)

Άτομα με Alzheimer(και νόσους με συναφή χαρακτηριστικά) ή παιδιά εφοδιάζονται με συσκευή GPS Tracker (εντοπισμού θέσης), που μπορεί να είναι στην τσέπη ή ακόμα και ενσωματωμένη (ραμμένη) στο ρούχο του χρήστη. Σε περίπτωση ανησυχητικής και αδικαιολόγητης απουσίας του ασθενή, οι οικείοι του ή ομάδα επέμβασης έχουν πρόσβαση στην εφαρμογή εντοπισμού θέσης, όπου βλέπουν σε χάρτη το στίγμα του και μπορούν να επεμβαίνουν ανάλογα.



Εικόνα 10. Σενάριο Λειτουργίας Υπηρεσίας Vidatrack.

4.2.2.3 Χρήστες και οφέλη

Την υπηρεσία Vidatrack μπορούν να παρέχουν φροντιστές των ατόμων μεγάλης ηλικίας ή / και των ατόμων με Αλτσχάιμερ ή παρόμοιες ασθένειες, τα κέντρα ημερήσιας φροντίδας για τους ηλικιωμένους, ενώσεις για άτομα με Alzheimer αλλά

και άλλοι οργανισμοί / παροχής υπηρεσιών υγείας και κοινωνικής φροντίδας. Τα κυριότερα οφέλη είναι η βελτίωση της παρακολούθησης των ασθενών / ικανότητα αντίδρασης σε καταστάσεις έκτακτης ανάγκης. η καλύτερη διαχείριση των πόρων, η βελτίωση της αποτελεσματικότητας των οργανισμών.

Τελικοί Χρήστες της υπηρεσίας είναι άτομα με Alzheimer (ή παρόμοιες ασθένειες), ηλικιωμένοι, οι οποίοι μένουν μόνοι τους, άτομα με χρόνιες παθήσεις - at risk patients, άτομα με ειδικές ανάγκες και παιδιά, εγκυμονούσες. Τα οφέλη των τελικών αποδεκτών είναι ότι ενισχύεται το αίσθημα ασφάλειας και αυξάνεται η ποιότητα ζωής για τους χρήστες και τους φροντιστές τους. Παρέχεται ανεξαρτησία στους ασθενείςνα συμμετέχουν σε καθημερινές δραστηριότητες της ζωής.

4.2.3 Υπηρεσία VidaΨ

4.2.3.1 Χαρακτηριστικά συστήματος

Η υπηρεσία Vidaψ είναι ένα *πρωτοποριακό σύστημα τηλεψυχιατρικής* με παράλληλη μετάδοση δεδομένων, εικόνας και ήχου. Για κάθε ασθενή τηρείται ένας διαδικτυακός (web-based) ψυχιατρικός φάκελος, που ενδεικτικά περιλαμβάνει δημογραφικά στοιχεία, ατομικό και οικογενειακό ιστορικό, διάγνωση τρέχουσας νόσου βάσει κωδικοποίησης DSM- IV-TR παρούσα ψυχική κατάσταση, φαρμακευτική αγωγή σύμφωνα με τον Ε.Ο.Φ κ.α.

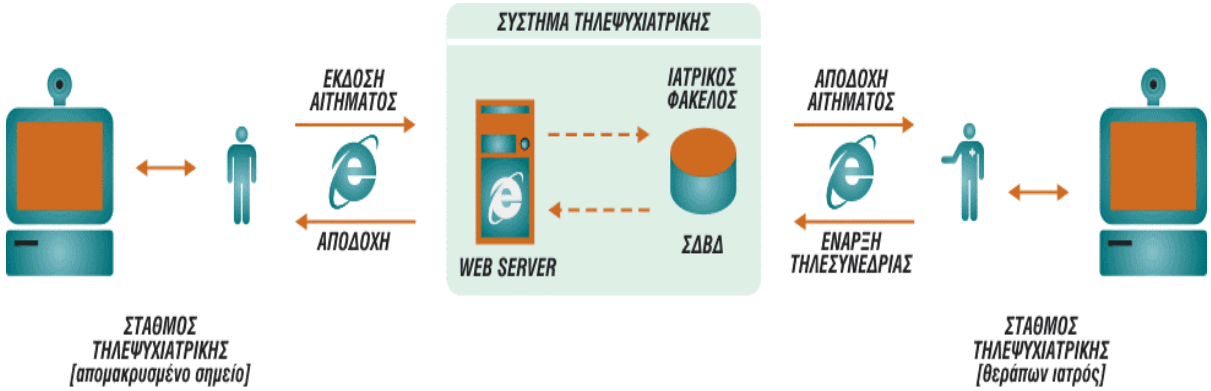
Οι υπηρεσίες που προσφέρει το σύστημα τηλεψυχιατρικής μπορούν να χωριστούν σε τρεις μεγάλες κατηγορίες:

(α) Ψυχιατρικός φάκελος

(β) Διεξαγωγή Τήλε-συνεδριών

(γ) Τηλεσυνεδρίες μέσω αιτημάτων

Η συνολική λειτουργία του συστήματος αποτυπώνεται παρακάτω:



Εικόνα 11. Συνολική Λειτουργία Υπηρεσίας Vida Ψ.

Η εφαρμογή παρέχει τη δυνατότητα σύνδεσης με άλλες συναφείς υπάρχουσες εφαρμογές όπως Πληροφορικά Συστήματα Νοσοκομείων, Ηλεκτρονικός Φάκελος Ασθενούς, Έξυπνη Κάρτα Υγείας.

Προτείνονται δύο τρόποι χρήσης του συστήματος:

- Ο Ηλεκτρονικός Ιατρικός Φάκελος Τηλεσυνεδριών (σε συνδυασμό με Ψυχιατρικό Φάκελο), απευθύνεται κυρίως σε ειδικούς Ψυχικής Υγείας (Ψυχίατρος / Ψυχολόγος / Κοινωνικός λειτουργός, Ψυχοθεραπευτής / Σύμβουλος) και τους πελάτες τους
- Ολοκληρωμένος Ψυχιατρικός Ηλεκτρονικός Φάκελος βάση αιτημάτων - ραντεβού, που απευθύνεται κυρίως σε Φορείς.

4.2.3.2 Σενάριο λειτουργίας

Σενάριο 1

Ηλεκτρονικός Ιατρικός Φάκελος Τηλεσυνεδριών (σε συνδυασμό με Ψυχιατρικό Φάκελο), που απευθύνεται κυρίως σε ειδικούς Ψυχικής Υγείας (Ψυχίατρος / Ψυχολόγος / Κοινωνικός λειτουργός, Ψυχοθεραπευτής / Σύμβουλος) και πελάτες.

Ο ειδικός Ψυχικής Υγείας εισέρχεται στο σύστημα vidaψ οποιαδήποτε στιγμή από οποιαδήποτε σημείο με στόχο τη διεξαγωγή Τηλεσυνεδριών με τους Πελάτες του.

Μέσω του συστήματος παρέχεται η δυνατότητα στον ιατρό να καταγράφει συνοπτικό ιστορικό, να διαχειρίζεται το χρόνο του και να τον κατανέμει αναλόγως στους πελάτες του. Επίσης, έχει δυνατότητα να καταγράφει όλες τις συνεδρίες μέσω οπτικής επαφής είτε μέσω Ίντερνετ είτε στο γραφείο του. Το σύστημα παρέχει σε εξουσιοδοτημένους χρήστες παράλληλη μετάδοση ήχου και εικόνας καθώς και καταγραφή της κάθε τηλεσυνεδρίας, όποτε είναι επιθυμητό. Ο ειδικός είναι υπεύθυνος για την εκκίνηση της και ο κάθε επιλεγμένος πελάτης έχει τη δυνατότητα να εισέλθει στη συγκεκριμένη συνεδρία. Επιπλέον, μπορεί να συνδυάσει και την καταγραφή στοιχείων σε ολοκληρωμένο ψυχιατρικό φάκελο, ο οποίος περιλαμβάνει, ατομικό, οικογενειακό, ψυχοπαθολογικό ιστορικό, εισαγωγή αυτοματοποιημένης διάγνωσης, παραπομπής ενός περιστατικού καθώς και εισαγωγή φαρμακευτικής αγωγής.

Σενάριο 2

Ολοκληρωμένος Ψυχιατρικός Ηλεκτρονικός Φάκελος βάση αιτημάτων – ραντεβού, που απευθύνεται κυρίως σε Φορείς.

Το προσωπικό (ιατρικό, παραϊατρικό, κοινωνικοί λειτουργοί κλπ) στο απομακρυσμένο σημείο εισάγει και διαχειρίζεται μέσω εξουσιοδοτημένης πρόσβασης στο σύστημα τα στοιχεία των ασθενών, εκδίδοντας και αιτήματα τηλεσυνεδριών. Ο ειδικός ιατρός αποδέχεται ή απορρίπτει το αίτημα για τη διεξαγωγή τηλεσυνεδρίας. Κατά τη διεξαγωγή της τηλεσυνεδρίας, και πάλι μέσω εξουσιοδοτημένης πρόσβασης, ο ιατρός συμπληρώνει/τροποποιεί τα στοιχεία του ιστορικού του ασθενούς, προσθέτοντας διάγνωση και φαρμακευτική αγωγή, αν είναι απαραίτητο.

Η εφαρμογή παρέχει τη δυνατότητα σύνδεσης με άλλες συναφείς υπάρχουσες εφαρμογές οι οποίες μπορούν να δρουν συμπληρωματικά, όπως Πληροφορικά Συστήματα Νοσοκομείων, Ηλεκτρονικός Φάκελος Ασθενούς, Έξυπνη Κάρτα Υγείας.

4.2.3.3 Χρήστες και οφέλη

Την υπηρεσία VidaΨ μπορούν να παρέχουν ψυχολόγοι και ψυχίατροι, ενώσεις επαγγελματιών στον τομέα της υγειονομικής περίθαλψης που επιθυμούν να απολαύσουν τα οφέλη της δικτύωσης αλλά και μονάδες υγείας ή/και υγειονομικές αρχές που επιθυμούν να παρέχουν εξειδικευμένες υπηρεσίες σε απομακρυσμένες περιοχές.

Οφέλη της υπηρεσίας είναι η βελτίωση της διαχείρισης δεδομένων του ασθενούς, η έγκαιρη πρόσβαση σε πληροφορίες, η καλύτερη διαχείριση των πόρων και βελτίωση της αποτελεσματικότητας των οργανισμών υγειονομικής περίθαλψηςμε ταυτόχρονη μείωση του κόστους προσωπικού και του κόστους των ασθενών, πρόσβαση σε υπηρεσίες υγειονομικής περίθαλψης αλλά και υποστήριξη των επαγγελματιών υγείας μικρών μονάδων από εξειδικευμένο επιστημονικό προσωπικό πολλαπλών ειδικοτήτων των Ψυχιατρικών Νοσοκομείων

Οι τελικοί Χρήστες της υπηρεσίας είναι ασθενείς με ψυχικές παθήσεις, αλλά και όλοι οι πολίτες που αντιμετωπίζουν στρες, εθισμούς κλπ ή απλά επιθυμούν να λάβουν επαγγελματικές συμβουλές και υποστήριξη. Η υπηρεσία αυτή προσφέρει συνεχή επικοινωνία με τους επαγγελματίες υγείας, ενίσχυση του αισθήματος ασφάλειας, βελτίωση ποιότητα ζωής για τους ασθενείς και τους φροντιστές, συμμετοχή σε καθημερινές δραστηριότητες της ζωής, ισότιμη πρόσβαση σε ποιοτικές υπηρεσίες ψυχικής υγείας - άρση της γεωγραφικής απομόνωσης και τέλος βοηθά στην αποασυλοποίησης.

4.2.4 Υπηρεσία Vidahome

4.2.4.1 Χαρακτηριστικά συστήματος

Η υπηρεσία vidahome είναι μια εξελιγμένη υπηρεσία για άτομα τα οποία χρειάζονται περίθαλψη και τη λαμβάνουν είτε στο σπίτι είτε σε κάποιο ίδρυμα που διαμένουν. Μέσω της υπηρεσίας vidahome υποστηρίζεται η ανεξάρτητη διαβίωση των ατόμων που χρήζουν εξατομικευμένη φροντίδα.

4.2.4.2 Σενάριο λειτουργίας

Για τη λειτουργία της υπηρεσίας, ο χρήστης εξοπλίζεται με μια ή περισσότερες ασύρματες συσκευές αποστολής σημάτων (πομπούς) και έναν πίνακα ελέγχου. Στην περίπτωση των ιδρυμάτων ο πίνακας ελέγχου παρακολουθεί πολλούς χρήστες ταυτόχρονα και ελέγχεται από ειδικευμένο προσωπικό. Ο πομπός μπορεί να ενεργοποιηθεί είτε χειροκίνητα από το χρήστη, με το πάτημα ενός πλήκτρου συναγερμού, έτσι ώστε να σταλεί σήμα στο πίνακα ελέγχου, είτε αυτόματα όταν πληρούνται ορισμένες προϋποθέσεις.

Ανάλογα με τις ανάγκες του κάθε ατόμου, μπορούν να χρησιμοποιηθούν διάφοροι είδη πομπών. Οι πιο συνηθισμένα πομποί είναι φορετές συσκευές και χρησιμοποιούνται σε περίπτωση έκτακτης ανάγκης, αλλά υπάρχουν επίσης αισθητήρες που ανιχνεύουν περιβαλλοντικές αλλαγές στο σπίτι ενός ατόμου ή σε ένα ίδρυμα.

Στο σχεδιάγραμμα επιδεικνύεται η λειτουργία εκπομπής σήματος κινδύνου με το πάτημα ενός πλήκτρου ή με ανίχνευση πτώσης:

Εικόνα 12. Λειτουργία Εκπομπής Σήματος κινδύνου.

4.2.4.3 Χρήστες και οφέλη

Την υπηρεσία Vida home μπορούν να παρέχουν οι φροντιστές των ηλικιωμένων ή των ατόμων που χρειάζονται περίθαλψη , τα ιδιωτικά και δημόσια κέντρα φροντίδας και οι φορείς που παρέχουν κοινωνικές υπηρεσίες.

Η υπηρεσία δίνει την δυνατότητα αντίδρασης σε καταστάσεις έκτακτης ανάγκης και καλύτερης διαχείρισης πόρων με αύξηση της αποτελεσματικότητας των οργανώσεων. Τελικοί Χρήστες της υπηρεσίας είναι άτομα μεγάλης ηλικίας, που ζουν μόνα τους ή διαμένουν μόνα τους κατά το μεγαλύτερο μέρος της ημέρας, άτομα που χρειάζονται περίθαλψη και τη λαμβάνουν είτε στο σπίτι είτε σε κάποιο ίδρυμα. Έτσι ενισχύεται η αίσθηση ασφάλειας και η ποιότητα ζωής των χρηστών και εξασφαλίζεται η ανεξαρτησία τους.

4.3 Λογισμικά Πακέτα

Για την χρήση των υπηρεσιών της, η εταιρεία διαθέτει τα ειδικά λογισμικά πακέτα. Ένα τέτοιο πακέτο είναι ο Ηλεκτρονικός Ιατρικό Φάκελο (ΗΙΦ), που αποτελεί μια web based εφαρμογή, η οποία εγκαθίσταται στον κεντρικό εξυπηρετητή ώστε να έχουν πρόσβαση οι χρήστες. Άλλο ένα είναι το λογισμικό αποστολής/λήψης του ιατρικού σήματος, το οποίο εγκαθίστανται στο μέσο διαδικτυακής πρόσβασης (κινητό/ PDA/ laptop/ netbook/ PC) του τελικού χρήστη, ώστε να μπορεί να στέλνει τις εξετάσεις και να δέχεται άμεσα τις γνωμοδοτήσεις του ειδικού και το λογισμικό ταυτοποίησης χρηστών το οποίο επιτρέπει την εξουσιοδοτημένη πρόσβαση σε πληροφορίες ηλεκτρονικού ιατρικού φακέλου.

Το ***λογισμικό του ΗΙΦ*** είναι μια εφαρμογή ηλεκτρονικού ιατρικού φακέλου ασθενούς/ιατρού, βασισμένη σε διεθνή αναγνωρισμένα πρότυπα ιατρικής επικοινωνίας (HL7, ECG-SCP) με τα εξής χαρακτηριστικά:

- Online ασφαλής διαχείριση ιατρικών δεδομένων
- Δημιουργία αναφορών
- Καταγραφή φυσιολογικών παραμέτρων
- Επεξεργασία δεδομένων
- Απομακρυσμένη πρόσβαση / διαχείριση ιατρικών δεδομένων
- Εξουσιοδοτημένη πρόσβαση στα δεδομένα ανά ομάδα χρήστη
- Αρχειοθέτηση
- Προβολή γραφικών παραστάσεων
- Αναλυτικές εκτυπώσεις
- Συνοπτική έκθεση ιατρικού φακέλου
- Φόρμες εκτύπωσης για συμπλήρωση δεδομένων ατομικού ιστορικού και επισκέψεων

• Ένδειξη εάν η λήψη της μέτρησης είναι πριν ή μετά τη χορήγηση φαρμάκου

Το ***λογισμικό αποστολής / λήψης***, όταν εγκαθίσταται σε PDA/laptop/netbook /PC αποτελεί μια εφαρμογή ενός συμπτυγμένου ιατρικού φακέλου στον οποίο όμως έχει πρόσβαση μόνο ο χρήστης που χρησιμοποιεί την συσκευή. Αποτελεί τον διακομιστή ανάμεσα στον τελικό χρήστη και τον ειδικό ιατρό. Το λογισμικό αποστολής/λήψης, όταν εγκαθίσταται σε κινητό τηλέφωνο αποτελεί τον διακομιστή της πληροφορίας ανάμεσα στον τελικό χρήστη και τον ειδικό ιατρό.

Το ***λογισμικό ταυτοποίησης***, επιτρέπει την αναγνώριση του χρήστη (ιατρού ή νοσηλευτή) για την εξουσιοδοτημένη πρόσβαση στο σύστημα και παράλληλα την αναγνώριση των χρηστών- ασθενών και άμεση ανάκτηση του ηλεκτρικού ιατρικού τους φακέλου.

4.4 Ομάδες χρηστών των πληροφοριακών συστημάτων

4.4.1 Ασθενείς

Ο ασθενής χειρίζεται τη συσκευή διαδικτυακής πρόσβασης και κάνει τις εξετάσεις μόνος του. Αποστέλλει τα αποτελέσματα μέσω της διαδικτυακής συσκευής που χρησιμοποιεί στο κέντρο και αυτά προστίθενται στον διαδικτυακό ιατρικό του φάκελο. Επίσης μπορεί να έχει πρόσβαση στον ιατρικό του φάκελο καθώς επίσης έχει και την δυνατότητα να χρησιμοποίει συσκευές φορητής βιολογικής τηλεμετρίας όπως ο καρδιογράφος, το πιεσόμετρο, το γλυκοζόμετρο κτλ και να δίνει τα αποτελέσματα της μέτρησης μέσω τηλεφώνου π.χ. σε κέντρο Τήλε-πρόνοιας και από εκεί μέσω του διαδικτύου στον ειδικό ιατρό. Άλλη μια δυνατότητα του είναι η εκπομπής σήματος έκτακτης ανάγκης σε περίπτωση δυσφορίας μέσω πομπού ως προς τους οικείους του ή τους φροντιστές του.

4.4.2 Εξειδικευμένο προσωπικό

Το εξειδικευμένο προσωπικό είναι το παραϊατρικό προσωπικό με περιφερειακές συσκευές φορητής βιολογικής τηλεμετρίας. Οι χρήστες που ανήκουν σε αυτή την κατηγορία έχουν εξουσιοδοτημένη πρόσβαση στο κέντρο επικοινωνίας καθώς επίσης και στον πίνακα ελέγχου και παρακολούθησης των ασθενών και είναι υπεύθυνοι για τον εντοπισμό την ενημέρωση των οικείων ή νοσηλευτών των ασθενών σε περίπτωση

κάποιας έκτακτης ανάγκης. Επίσης, διαθέτουν και χειρίζονται συσκευές διαδικτυακής πρόσβασης για να κάνουν εξετάσεις στους ασθενείς κατά τη διάρκεια κατ' οίκον επισκέψεων, στέλνοντας τα αποτελέσματα στους ειδικούς και λαμβάνοντας απαντήσεις.

4.4.3 Γενικός ιατρός

Οι Γενικοί Ιατροί μπορούν να έχουν πρόσβαση οποιαδήποτε στιγμή στο κέντρο επικοινωνίας καθώς και στους διαδικτυακούς ιατρικούς φακέλους των ασθενών τους. Με την τεχνολογία έξυπνων καρτών γίνεται η ταυτοποίηση τους. Επίσης, ο ειδικός ιατρός που εισέρχεται στο σύστημα Vidaψ οποιαδήποτε στιγμή από οποιαδήποτε σημείο έχει την δυνατότητα να διεξαγάγει Τηλεσυνεδρίες με τους Πελάτες του. Επιπλέον, μπορεί να συνδυάσει και την καταγραφή στοιχείων στον διαδικτυακό ιατρικό φάκελο εισάγοντας αυτοματοποιημένη διάγνωση, παραπομπή ενός περιστατικού καθώς και εισαγωγή φαρμακευτικής αγωγής αλλά δεν έχει την δυνατότητα να τα διαγράψει ή να τροποποιήσει τα ήδη υπάρχοντα στοιχεία.4.4.4 Νοσηλευτές / Συγγενικά πρόσωπα

Οι νοσηλευτές ή τα συγγενικά έχουν την δυνατότητα αίτησης ενημέρωσης συντεταγμένων του ασθενούς, αλλά και την δυνατότητα άμεσης ενημέρωσης σε περίπτωση χρήσης του panic button μέσω μηνύματος που τους αποστέλλεται.

4.4.5 Διαχειριστής

Ο Διαχειριστής ανήκει στον τομέα τεχνικών υπηρεσιών ανάπτυξης και υποστήριξης του λογισμικού. Είναι υπεύθυνος για το σχεδιασμό και την εφαρμογή των δραστηριοτήτων ανάπτυξης και υποστήριξης λογισμικού για εφαρμογές ιατρικής πληροφορικής. Επιπλέον, είναι υπεύθυνος για την οργάνωση, εγκατάσταση, αναβάθμιση, διαχείριση και επίλυση προβλημάτων υλικού και λογισμικού, και είναι ο μόνος που έχει πρόσβαση στις βάσεις δεδομένων της εταιρείας.

4.4.6 Υπεύθυνοι ασφαλείας

Στις αρμοδιότητες των υπεύθυνων ασφάλειας τους οποίους έχει καθορίσει η εταιρεία, ανήκει η τακτική ενημέρωση του σχεδίου ασφάλειας, η επανεξέταση όλων των ελέγχων, καθώς και των λειτουργιών. Ο ρόλος τους είναι πολύ σημαντικός για την εταιρεία καθώς αποτελεί σημαντικό βήμα προς τη θωράκιση των πληροφοριακών της συστημάτων, και την ενίσχυση των αμυντικών μηχανισμών τους. Άλλωστε, η

τεχνολογία εξελίσσεται με τόσο γρήγορο ρυθμό, που ακόμα και η παραμικρή αλλαγή θα πρέπει να αντικατοπτρίζεται άμεσα στα μέτρα ασφάλειας που τελικά υιοθετούνται.

5 Πολιτική προστασίας – μηχανισμοί ασφαλείας

5.1 Γενική αρχή κανόνων ασφαλείας

Γενική αρχή κανόνων ασφαλείας αποτελεί η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) που έχει ως στόχο της την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από τον νόμο.

Από πρακτική άποψη, η ασφάλεια μπορεί να έγκειται στην επαρκή προστασία ανθρώπων και αγαθών, για την οποία μπορεί να λαμβάνονται διάφορα μέτρα προστασίας από πιθανούς κινδύνους. Για παράδειγμα, η φυσική ασφάλεια ενός κτηρίου έγκειται στην αποτροπή εισόδου κακόβουλων ατόμων και στην αποτροπή ζημιών από φυσικές καταστροφές. Αντίστοιχα, η ασφάλεια μίας ηλεκτρονικής βάσης δεδομένων έγκειται στην προστασία των δεδομένων από καταστροφή, διαγραφή, αλλοίωση ή αποκάλυψη σε μη εξουσιοδοτημένους χρήστες.

Θα πρέπει να ορίζονται, να τεκμηριώνονται, να εφαρμόζονται και να αναθεωρούνται συγκεκριμένες διαδικασίες ασφάλειας. Οι διαδικασίες ασφάλειας καθορίζονται από την ΑΔΑΕ και ορίζουν συγκεκριμένες ενέργειες των εργαζομένων και των συνεργατών τους, των χρηστών και των συνδρομητών, του προσώπου που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, την αλληλουχία των ενεργειών, τους υπεύθυνους για την εκτέλεσή τους και τον τρόπο και τα μέσα τεκμηρίωσής τους

5.2 Γενική αρχή ασφαλούς μεταφοράς δεδομένων μέσω διαδίκτυο

1. Για την ασφάλεια και την διασφάλιση του απορρήτου των εφαρμογών διαδικτύου έχουν αναπτυχθεί διάφορα πρωτόκολλα και εφαρμογές που βασίζονται

στις γενικές αρχές κρυπτογράφησης. Ανάλογα και με τον τύπο της εφαρμογής έχουν προτυποποιηθει και συγκεκριμένα πρωτόκολλα .

2. Οι πάροχοι διαδικτυακών υπηρεσιών οφείλουν να κάνουν χρήση του ευρέως αποδεκτών τεχνικών και πρωτοκόλλων ασφαλείας των εφαρμογών διαδικτύου. Ενδεικτικά αναφέρονται για εφαρμογές παγκοσμίου ιστού (www) το πρωτόκολλο SSL (Secure Sockets Layer) , για εφαρμογές ηλεκτρονικού ταχυδρομείου το S/MIME, το PEM (Privacy Enhanced Mail) και το PGP (Pretty Good Privacy)και για ηλεκτρονικές πληρωμές μέσω πιστωτικών καρτών το πρωτόκολλο SET (Secure Electronic Transaction).

3. Δεδομένου ότι τα νέα πρωτόκολλα και τεχνολογίες θα ανακύπτουν με την πρόοδο της επιστήμης των υπολογιστών, η ΑΔΑΕ θα εκδίδει τεχνικές οδηγίες και συστάσεις προς τους παρόχους διαδικτύου σχετικά με τα νέα πρωτόκολλα και τις τεχνολογίες. Οι πάροχοι διαδικτύου είναι υποχρεωμένοι να ακολουθούν τα εκάστοτε ευρέως χρησιμοποιούμενα πρωτοκόλλα και τεχνολογίες, είτε αυτόβουλα είτε έπειτα από έλεγχο και αντίστοιχη οδηγία από την ΑΔΑΕ.

5.3 Γενική αρχή των υποχρεώσεων των παροχέων διαδικτυακών υπηρεσιών

Πρωταρχικό στοιχείο για την διασφάλιση του απορρήτου των επικοινωνιών στο διαδίκτυο αποτελεί η ύπαρξη πολιτικής ασφάλειας στους παρόχους, η οποία αφορά τους χρήστες, τους χρήστες του παρόχου και στα συστήματα που εμπλέκονται στην επικοινωνία από και προς το Διαδίκτυο. Η γενική αρχή που θα πρέπει να ακολουθήσει ο πάροχος πρέπει να ανταποκρίνεται στις ειδικές απαιτήσεις της ασφάλειας του, να καθορίζει την πολιτική πρόσβασης σε συστήματα και πληροφορίες, την πολιτική αποδέκτης χρήσης , τι ενέργειες που ακολουθούνται για την διατήρηση τις ασφάλειας και τα μέτρα που εφαρμόζονται σε περιπτώσεις παραβίασης ή έκτακτης ανάγκης. Μέσω της γενικής αρχής των παροχέων διαδικτύου προστατεύονται και διασφαλίζονται τα δεδομένα επικοινωνίας των χρηστών και των χρηστών του παρόχου, το απόρρητο των επικοινωνιών, η προστασία των υπολογιστικών συστημάτων και των δικτυακών υποδομών και η προστασία των διαδικτυακών υπηρεσιών και εφαρμογών.

Η πολίτικη ασφάλειας που ακολουθεί ο πάροχος θα πρέπει να συμφωνεί με την γενική αρχή της ΑΔΑΕ, γι αυτό και θα υπόκειται σε έλεγχο από αυτήν τόσο ως προς την αποτελεσματικότητα της αλλά και ως προς τον βαθμό εφαρμογής της. Η φύση των επενδύσεων που γίνονται από τους παρόχους για την διατήρηση της ασφάλειας και της ακεραιότητας του δικτύου πρέπει να ακολουθεί την αρχή της αναλογικότητας, η οποία λαμβάνει υπόψη της το μέγεθος του παρόχου και των αριθμό των χρηστών παρόχου.

Σύμφωνα λοιπόν με την ΑΔΑΕ ο πάροχος υποχρεούται να τηρεί τα παρακάτω:

1. Να διαθέτει και να τηρεί πολιτική πρόσβασης για τα συστήματα τα οποία αναφέρονται σε εξωτερικές συνδέσεις, επικοινωνίες δεδομένων, τηλεπικοινωνιακές συσκευές και λογισμικά προγράμματα.

2. Καθώς και να λαμβάνει όλα τα απαραίτητα και πρόσφορα μέτρα για τη φυσική προστασία των εγκαταστάσεών του, για τον έλεγχο της φυσικής πρόσβασης, ώστε αυτή να επιτρέπεται μόνο σε εξουσιοδοτημένα πρόσωπα.

3. Να ενημερώνουν τους χρήστες σχετικά με τα μέτρα προστασίας που μπορούν να λαμβάνουν για την διασφάλιση του απορρήτου των επικοινωνιών και των δεδομένων τους π.χ. την χρήση συγκεκριμένου λογισμικού ή τεχνολογιών κρυπτογράφησης.

4. Να ενημερώνουν τους χρήστες για δεδομένα επικοινωνίας τα οποία πιθανόν να αποθηκεύονται σε αντίγραφα ασφαλείας αλλά και να του κοινοποιούν το μέγιστο χρονικό διάστημα για το οποίο τα δεδομένα θα είναι αποθηκευμένα.

5. Να λαμβάνουν υπόψη και να εφαρμόζουν στο τμήμα της πολιτικής τους τις διατάξεις της νομοθεσίας για την επεξεργασία των δεδομένων επικοινωνίας.

6. Να χρησιμοποιούν συστήματα ανίχνευσης επισυνδέσεων για την ενίσχυση προστασίας του δικτύου, 24 ώρες το 24ωρο. Η διακοπή των συστημάτων αυτών επιτρέπεται μόνο σε περιπτώσεις συντήρησης ή κάποιας βλάβης του συστήματος.

7. Να διαθέτει απαραίτητο λογισμικό για την προστασία από Ιούς όλων των υπηρεσιών και εφαρμογών που προσφέρει στους χρήστες.

8. Να αναπτύξει και να συντηρεί ένα σχέδιο εκτάκτου ανάγκης του συστήματος μετά από κακόβουλες επιθέσεις περιλαμβάνοντας την εκτέλεση αντίγραφων ασφαλείας, την παροχή διαδικασιών για συνέχιση της λειτουργίας σε περίπτωση ανάγκης και την ανάκτηση από μια επίθεση. Επιπλέον, να παραδίδει την πιο πρόσφατη πολιτική Αντιγράφων Ασφάλειας κάθε φορά που επιτελείται κάποια σημαντική αλλαγή σε αυτήν.

9. Να διαθέτει σαφή Διαδικασία Χειρισμού Περιστατικών Ασφαλείας (ΔΧΠΑ) τα οποία απειλούν την ασφάλεια των επικοινωνιακών υποδομών αλλά και την διασφάλιση του απορρήτου των επικοινωνιών που διεξάγονται μέσω του παρόχου. Επιπλέον οφείλει να την ανανεώνει και να ελέγχει σε τακτικά διαστήματα την ετοιμότητα ενεργοποίησης όλων των μηχανισμών και προσώπων της ΔΠΧΑ καθώς επίσης και να την παραδίδει στην ΑΔΑΕ κάθε φορά για έλεγχο.

10. Να διαθέτει ομάδα ελέγχου ασφάλειας του δικτύου του και κατά τους ελέγχους, να επιτρέπει την πρόσβαση στο δίκτυο ως το επίπεδο που κρίνεται αναγκαίο για την εκτέλεση τους καθώς και ομάδα αντιμετώπισης Ιών που θα μπορεί να παραπέμψει και ένα χρήστη που χρήζει βοήθειας, στην αρμόδια εταιρεία όταν της ζητηθεί.

11. Να συγκροτεί ομάδα αποτίμησης κίνδυνου, που θα περιλαμβάνει τόσο τεχνικό προσωπικό (προγραμματιστές, τεχνικούς ασφάλειας κτλ) όσο και ανώτερα στελέχη, ώστε η αποτίμηση να είναι όσο το δυνατόν πιο ολοκληρωμένη.

5.4 Γενική αρχή δικαιωμάτων των χρηστών διαδικτυακών υπηρεσιών

Η γενική αρχή των δικαιωμάτων των χρηστών προσδιορίζει τις ειδικές απαιτήσεις σχετικά με τους συνδρομητές ή χρήστες των παρεχομένων διαδικτυακών υπηρεσιών με βάση τα δικαιώματα αυτών.

Πιο συγκεκριμένα προσδιορίζει τις απαιτήσεις των χρηστών από τον πάροχο διαδικτυακών υπηρεσιών, που είναι οι εξής:

Το πρόσωπο που ασχολείται με την παροχή διαδικτυακών υπηρεσιών ή και ηλεκτρονικών επικοινωνιών οφείλει να διατηρεί αρχείο που αναφέρει αναλυτικά τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης που χρησιμοποιούνται για την πρόσβαση των συνδρομητών ή χρηστών του στις υπηρεσίες ή/και τα δίκτυα που παρέχει.

Το πρόσωπο που ασχολείται με την παροχή διαδικτυακών υπηρεσιών ή και ηλεκτρονικών επικοινωνιών οφείλει να διαμορφώσει και να ακολουθεί συγκεκριμένη διαδικασία διαχείρισης των λογαριασμών πρόσβασης των συνδρομητών ή χρηστών στις υπηρεσίες ή/και τα δίκτυα που παρέχει , στην οποία θα περιγράφεται με σαφήνεια ο τρόπος προσθήκης και κατάργησης λογαριασμών πρόσβασης, καθώς και η απόδοση του ονόματος χρήστη και του κωδικού πρόσβασης στους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών, στην περίπτωση που αυτά καθορίζονται αρχικά από αυτό. Στην περίπτωση αυτή, το πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να δημιουργεί τους αρχικούς κωδικούς πρόσβασης με τρόπο που να αποτρέπει τον εύκολο προσδιορισμό τους. Επιπρόσθετα, οφείλει να ενημερώνει με κάθε πρόσφορο μέσο τους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών σχετικά με την αναγκαιότητα αλλαγής του αρχικού κωδικού πρόσβασης, καθώς και σχετικά με ενδεδειγμένους κανόνες δημιουργίας ισχυρών κωδικών πρόσβασης.

Το πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να διαθέτει διαδικασία σύμφωνα με την οποία διενεργείται περιοδικός έλεγχος σχετικά με την αλλαγή του αρχικού κωδικού πρόσβασης από τους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών και εξασφαλίζει την εκ νέου ενημέρωσή τους σχετικά με την αναγκαιότητα αλλαγής των κωδικών πρόσβασης σε περίπτωση που δεν έχουν προβεί στην σχετική αλλαγή, σύμφωνα με την Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών.

Σε περίπτωση που το πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών προσφέρει τη δυνατότητα στους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών να αποκτήσουν πρόσβαση σε δεδομένα επικοινωνίας τους (ενδεικτικά, εξερχόμενες κλήσεις, ηλεκτρονικό ταχυδρομείο) μέσω συγκεκριμένης ιστοθέσης (web account), οφείλει να χρησιμοποιεί τους ευρέως αποδεκτούς μηχανισμούς ασφαλούς αυθεντικοποίησης και κρυπτογράφησης και να περιγράφει αυτούς σε σχετικό αρχείο το οποίο οφείλει να διατηρεί.

Το πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να ενημερώνει τους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών σχετικά με τους κανόνες ενδεδειγμένης συμπεριφοράς αναφορικά με την προστασία των κωδικών πρόσβασης που κατέχουν, με έντυπη ή ηλεκτρονική ενημέρωση, τουλάχιστον κατά την σύναψη της μεταξύ τους σύμβασης, καθώς και σε εύκολα προσβάσιμο σημείο του ισοτόπου του. Οι κανόνες αυτοί θα πρέπει να ακολουθούν τις ευρέως αποδεκτές και διεθνείς πρακτικές.

5.5 Πλαίσιο χρήσης μηχανισμών ασφαλείας στο διαδίκτυο

Μια ολοκληρωμένη υλοποίηση Διαδικτυακής επικοινωνίας θα πρέπει να περιλαμβάνει επαρκείς μεθόδους κρυπτογράφησης (encryption), χρησιμοποίηση επαλήθευσης ή προσδιορισμού ταυτότητας (authentication) από τους χρήστες, και ένα σχέδιο διαχείρισης που θα ενσωματώνει αποδοτικές μεθόδους κλειδιών και κωδικών πρόσβασης. Υπάρχουν περιπτώσεις που οι κωδικοί πρόσβασης δεν αρκούν και χρειάζεται ένα είδος δυναμικής πιστοποίησης των δεδομένων. Αυτό επιτυγχάνεται με μια σειρά από διαφορετικές τεχνολογίες όπως οι γεννήτριες δυναμικών κωδικών, τεχνικές βασισμένες στην κρυπτογραφία, καθώς και ψηφιακές υπογραφές και πιστοποιητικά.

Επίσης, ο πάροχος διαδικτύου θα πρέπει να προστατεύει τους διακομιστές του δικτυού του και να παρέχει την δυνατότητα ανάκτησης των αρχείων του σε περίπτωση απώλειας αυτών. Οι διαχειριστές δικτύου θα πρέπει να παρέχουν μεθόδους εφεδρικών αντιγράφων όπως η πλήρη, η αυξητική και η διαφορική αντιγραφή αρχείων. Άλλη μια μέθοδος είναι η Δικτυακή αντιγραφή αρχείων στην οποία κρυπτογραφημένα δεδομένα με αυτόματο και ασφαλή τρόπο αντιγράφονται και αποθηκεύονται σε μια περιοχή εκτός του εσωτερικού δικτυού του παρόχου του διαδικτύου. Επιπλέον, απαραίτητη είναι η χρήση λογισμικού κατά των κακόβουλων επιθέσεων, αυτό γίνεται κυρίως με την χρήσης αναχωμάτων ασφάλειας (firewalls), για την προστασία από ιούς.

Επιπλέον, οι εξυπηρετητές (servers) των εφαρμογών ηλεκτρονικού ταχυδρομείου μπορεί να είναι αρχικοποιημένοι ώστε κάθε μήνυμα να υπογράφεται χρησιμοποιώντας την ψηφιακή υπογραφή του αποστολέα, να απαγορεύουν την αποστολή μηνυμάτων σε μη κατάλληλους προορισμούς και να ανιχνεύουν τα κατάλληλα προγράμματα για αποστολή / λήψη μηνυμάτων. Οι χρήστες θα πρέπει να συμμορφώνονται με τους κανόνες ασφαλείας που ορίζει ο πάροχος διαδικτύου είτε ενυπόγραφα είτε ηλεκτρονικά, καθώς επίσης δεν θα πρέπει να δημοσιοποιούν υλικό σε ακατάλληλους ή παράνομους ηλεκτρονικούς τόπους.

	Threats	Consequences	Countermeasures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerability to all other threats	Cryptographic checksums
Confidentiality	• Eavesdropping on the Net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	Encryption, Web proxies
Denial of Service	• Killing of user threads • Flooding machine with bogus threats • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	Difficult to prevent
Authentication	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic techniques

Εικόνα 13. Πίνακας Σύγκρισης Απειλών Διαδικτύου.

Παρακάτω περιγράφονται εκτενέστερα οι μέθοδοι της κρυπτογράφησης, της αυθεντικοποίησης και οι μηχανισμοί προστασίας από ιούς.

Κρυπτογράφηση

Η κρυπτογραφία είναι μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Η κρυπτογράφηση στο διαδίκτυο έχει σκοπό την διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της μη αποποίησης ευθύνης στις συναλλαγές προστατεύοντας έτσι την ιδιωτικότητα του χρήστη. Για αυτό και οι πάροχοι οφείλουν να εφαρμόζουν αλγορίθμους και τεχνικές κρυπτογράφησης τόσο στα συστήματα και τις εφαρμογές τους όσο και στην μετάδοση των δεδομένων, ακολουθώντας διεθνή πρότυπα, καθώς υποχρεούνται να ενημερώνουν για τις τεχνικές τους την ΑΔΑΕ. Η ΑΔΑΕ από την μεριάς της οφείλει να εκδίδει τεχνικές οδηγίες και συστάσεις που θα καθορίζουν το μήκος του κλειδιού ανά πεδίο κρυπτογράφησης. Το επίπεδο της κρυπτογράφησης πρέπει να είναι τέτοιο ώστε η παραβίαση να μην είναι δυνατή σε λογικό χρόνο και με λογικούς υπολογιστικούς πόρους.

Ενδεικτικοί αλγόριθμοι είναι οι εξής: RSA, Diffie Helman και El Gamal για ασύμμετρη κρυπτογραφία, 3DES(Data Encryption Standard), AES (Advanced Encryption Algorithm), Blowfish, CAST για συμμετρική κρυπτογραφία.

Αναγνώριση και ταυτοποίηση

Όλοι οι χρήστες του συστήματος (τεχνικό προσωπικό, διαχειριστές, προγραμματιστές, κοινοί χρήστες κλπ.), θα πρέπει να έχουν ένα μοναδικό αναγνωριστικό (user ID), για καθαρά προσωπική τους χρήση στο σύστημα. Με αυτόν τον τρόπο είναι δυνατός ο εντοπισμός του υπεύθυνου ατόμου για όλες τις δραστηριότητες που γίνονται στο πληροφοριακό σύστημα του οργανισμού. Επιπλέον, τα user IDs δεν πρέπει να φανερώνουν τα δικαιώματα του χρήστη στο σύστημα. Μια ομάδα μπορεί να μοιράζεται το ίδιο user ID για την εκτέλεση συγκεκριμένων εργασιών στο σύστημα, μόνο σε εξαιρετικές περιπτώσεις, και εφόσον κάτι τέτοιο είναι απαραίτητο για τον οργανισμό. Σε μια τέτοια περίπτωση θα πρέπει να υπάρχει ειδική έγκριση από τη διοίκηση του οργανισμού, όπως επίσης και να χρησιμοποιηθεί κάποιος μηχανισμός που θα καθορίζει τις ευθύνες των μελών της ομάδας.

Υπάρχουν διάφορες διαδικασίες αυθεντικοποίησης που μπορούν να χρησιμοποιηθούν για την επιβεβαίωση της ταυτότητας ενός χρήστη. Τα συνθηματικά

είναι ο πλέον συνηθισμένος τρόπος, ο οποίος βασίζεται στη χρήση ενός μυστικού, γνωστού μόνο στο χρήστη. Άλλοι μηχανισμοί αυθεντικοποίησης περιλαμβάνουν συνδυασμούς κρυπτογραφίας και πρωτοκόλλων εξακρίβωσης της ταυτότητας του χρήστη.

Διάφορα αντικείμενα, όπως έξυπνες κάρτες, τα οποία έχει στην κατοχή του ο χρήστης, μπορούν επίσης να χρησιμοποιηθούν για αυθεντικοποίηση στο σύστημα. Ένας άλλος τρόπος εξακρίβωσης της ταυτότητας, περιλαμβάνει την εξέταση διάφορων βιομετρικών χαρακτηριστικών του χρήστη, όπως είναι τα δακτυλικά αποτυπώματα. Ο συνδυασμός πολλαπλών τεχνολογιών εξακρίβωσης της ταυτότητας, έχει ως αποτέλεσμα ισχυρότερη αυθεντικοποίηση.

Προστασία από ιούς

Ο πάροχος θα πρέπει να διαθέτει κατάλληλο λογισμικό για την προστασία από ιούς για όλες τις υπηρεσίες και εφαρμογές που προσφέρει στους χρήστες . Για παράδειγμα υπηρεσία e-mail απαιτεί χρήση e-mail scanner.

Θα πρέπει επίσης να εγκαθιστά μονίμως μνήμη (memory resident) των υπολογιστικών συστημάτων λογισμικό προστασίας από ιούς το οποίο θα εξετάζει αυτομάτως όλα τα εισερχόμενα μηνύματα. Επίσης, και οι χρήστες από την άλλη θα πρέπει να προστατεύονται ομοιοτρόπως και θα πρέπει να ελέγχονται αλλά και να ενημερώνονται από τον πάροχο σχετικά με το πως μπορούν να προστατευθούν επιπλέον.

Θα πρέπει να υλοποιηθούν οι κατάλληλοι μηχανισμοί για την αποτροπή και τον εντοπισμό κακόβουλου λογισμικού. Η προστασία απέναντι στο κακόβουλο λογισμικό θα πρέπει να βασίζεται στην ενημέρωση του προσωπικού για την ασφάλεια του οργανισμού, τα κατάλληλα δικαιώματα προσπέλασης και τους μηχανισμούς διαχείρισης αλλαγών στο σύστημα.

Οι παρακάτω μηχανισμοί ελέγχου έχουν ιδιαίτερη σημασία για την προστασία αρχείων που εξυπηρετούν μεγάλο αριθμό σταθμών εργασίας.

• Μια επίσημη πολιτική που να επιβάλει την ύπαρξη των κατάλληλων αδειών χρήσης λογισμικού και να απαγορεύει τη χρήση μη εξουσιοδοτημένου λογισμικού

• Μια επίσημη πολιτική που να προστατεύει το πληροφοριακό σύστημα από λογισμικό και αρχεία που μπορούν να εισέλθουν στο σύστημα από κάποιο εξωτερικό δίκτυο ή μέσο αποθήκευσης.

• Εγκατάσταση και τακτική ενημέρωση προγραμμάτων antivirus για τον έλεγχο προσωπικών υπολογιστών και αποθηκευτικών μέσων.

• Τακτικός έλεγχος του χρησιμοποιούμενου λογισμικού και των αρχείων του συστήματος. Οποιαδήποτε αλλαγή θα πρέπει να ερευνάται.

• Ο έλεγχος αρχείων και αποθηκευτικών μέσων για ιούς πριν από τη χρήση τους.

• Ο έλεγχος των εισερχόμενων ηλεκτρονικών μηνυμάτων για ιούς. Ο συγκεκριμένος έλεγχος μπορεί να γίνει σε διάφορα σημεία του συστήματος, όπως τους εξυπηρετητές ηλεκτρονικού ταχυδρομείου, τους προσωπικούς υπολογιστές κλπ.

• Την εκπαίδευση των χρηστών και ύπαρξη διαδικασιών για την αντιμετώπιση ιών.

•Την ύπαρξη σχεδίου επιχειρησιακής συνέχειας στην περίπτωση εκτεταμένων ζημιών στο σύστημα από ιούς.

• Την ύπαρξη διαδικασιών για τον έλεγχο της ακρίβειας της πληροφόρησης για ιούς.

6 Πολιτική ασφαλείας ιατρικών δεδομένων στο διαδίκτυο

6.1 Θεσμικό Πλαίσιο Προστασίας Ιατρικών Δεδομένων στην Τηλεϊατρική.

Η VIDAVO έχει κατοχυρώσει την ασφάλεια των δεδομένων της και τηρεί πλήρως όλα όσα η νομοθεσία επιβάλλει για την προστασία των προσωπικών δεδομένων. Τα δεδομένα που αφορούν την υγεία του ατόμου αποτελούν μέρος της προσωπικότητας του και είναι απαραίτητη η συγκατάθεση του ασθενή για κάθε ανάκτηση, καταγραφή, επεξεργασία ή μεταφορά τους. Η πρόσβαση και η επεξεργασία των δεδομένων πρέπει να συμφωνεί με τις σχετικές διατάξεις για την προστασία των προσωπικών δεδομένων, ν. 2472/97 και ν. 2774/99 και το ιατρικό απόρρητο . Όσον αφορά το

νομικό πλαίσιο τα ευαίσθητα δεδομένα προστατεύονται και από την Αρχή Προστασίας Προσωπικών Δεδομένων.

Οι ασθενείς έχουν δικαιώματα για την προστασία των προσωπικών δεδομένων τους και την εμπιστευτικότητα της μεταφοράς δεδομένων που σχετίζονται με τη διαχείριση της περίθαλψής τους. Κάθε είδους εξ' αποστάσεως παροχή περίθαλψης σε ασθενείς πρέπει να γίνεται σε κατάλληλο περιβάλλον που εγγυάται την απουσία ατόμων που δεν σχετίζονται με αυτή. Οι ασθενείς πρέπει να γνωρίζουν την παρουσία άλλων στην άλλη άκρη του συστήματος τηλεδιάσκεψης, ακόμα και αν δεν φαίνονται στην κάμερα.

Οι ασθενείς, ή μέλη των οικογενειών τους, θα πρέπει επίσης να ενημερώνονται για τυχόν αποθήκευση σε ηλεκτρονικό ή μαγνητικό μέσο των τηλεσυνεδριών και να την εγκρίνουν προφορικά ή κατά προτίμηση γραπτά. Όπως και σε κάθε άλλη διαδικασία, ο ασθενής πρέπει να γνωρίζει τους πιθανούς κινδύνους αλλά και τα πλεονεκτήματα της τηλεσυνεδρίας, και βέβαια πρέπει να του παρέχεται η επιλογή να μην συμμετέχει.

Η ελληνική νομοθεσία, σε συνέχεια της οδηγίας 95/46/ΕΚ, μέσω των προβλέψεων του Ν. 2472/97 και των τροποποιήσεων αυτού, περιγράφει το γενικό νομικό πλαίσιο που διέπει τη χρήση ευαίσθητων προσωπικών δεδομένων. Στα πλαίσια της παρούσας επιδεικτικής εφαρμογής θα ληφθεί ιδιαίτερη πρόνοια για την πιστή τήρηση του νομικού αυτού πλαισίου, αναγνωρίζοντας ότι, ειδικά τα ψυχιατρικά δεδομένα, είναι άκρως ευαίσθητα.

Οι συγκεκριμένες προβλέψεις της νομοθεσίας για την προστασία των ευαίσθητων προσωπικών δεδομένων των ασθενών περιγράφονται συνοπτικά παρακάτω :

1. Η επεξεργασία των ιατρικών δεδομένων επιτρέπεται μόνο όταν συντρέχει μία από τις επόμενες περιπτώσεις:

(α) Ο ασθενής έχει δώσει ρητά τη συγκατάθεσή του, ή

(β) η επεξεργασία είναι απαραίτητη για τη διασφάλιση ζωτικού συμφέροντος του ασθενούς ενώ ο ίδιος τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του, ή

(γ) η επεξεργασία είναι αναγκαία για την ιατρική πρόληψη ή διάγνωση, την παροχή ιατροφαρμακευτικής αγωγής ή τη διαχείριση των ιατροφαρμακευτικών υπηρεσιών, η δε επεξεργασία εκτελείται από κατ' επάγγελμα θεράποντα της υγείας που δεσμεύεται από το ιατρικό απόρρητο ή από άλλο πρόσωπο το οποίο υπέχει ανάλογη υποχρέωση.

2. Οι βασικές αρχές της νόμιμης και θεμιτής επεξεργασίας που πρέπει απαραίτητα να τηρούνται, σε συνδυασμό με τα παραπάνω είναι:

(α) Ο σκοπός και η διάρκεια της επεξεργασίας πρέπει να ορίζεται με σαφήνεια εκ των προτέρων και δεν επιτρέπεται να τροποποιείται αργότερα. Τα δεδομένα πρέπει να είναι απαραίτητα και να μην υπερβαίνουν το σκοπό της επεξεργασίας. Η λεγόμενη αρχή του σκοπού σημαίνει ότι πρέπει να συλλέγονται όσο το δυνατόν λιγότερα προσωπικά δεδομένα για το σκοπό της επεξεργασίας και όπου είναι δυνατό να χρησιμοποιούνται ανώνυμα δεδομένα ή ψευδώνυμα. Τα δεδομένα πρέπει επίσης να είναι ακριβή και εφόσον χρειάζεται να ενημερώνεται η ακρίβειά τους.

(β) Ο υπεύθυνος επεξεργασίας πρέπει να λαμβάνει όλα τα απαραίτητα τεχνικά και οργανωτικά μέτρα προστασίας των δεδομένων από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση, ιδίως εάν η επεξεργασία συμπεριλαμβάνει και διαβίβαση των δεδομένων μέσω δικτύου. Ο βαθμός ασφάλειας κρίνεται από τις εξής συνιστώσες: τη φύση των δεδομένων, την επικινδυνότητα της επεξεργασίας, την τεχνολογική εξέλιξη και το κόστος εφαρμογής των μέτρων ασφάλειας. Έτσι η διακίνηση ευαίσθητων δεδομένων μέσω δικτύου απαιτεί αυστηρά μέτρα ενώ το κόστος αποκτά δευτερεύουσα σημασία όσο αυξάνει η επικινδυνότητα της επεξεργασίας.

(γ) Επίσης, ο υπεύθυνος της επεξεργασίας πρέπει να γνωστοποιήσει την επεξεργασία στην αρμόδια Αρχή Προστασίας. Σημειώνουμε ότι σε ειδικές κατηγορίες επεξεργασίας που ενέχουν ιδιαίτερους κινδύνους η αρμόδια Αρχή μπορεί να προβεί σε προληπτικό έλεγχο της επεξεργασίας.

(δ) Ο υπεύθυνος επεξεργασίας πρέπει να σέβεται και να εξασφαλίσει την άσκηση των δικαιωμάτων του υποκειμένου της επεξεργασίας (ασθενούς).

3. Τηρούνται τα νόμιμα δικαιώματα του ασθενούς:

(α) Ο υπεύθυνος επεξεργασίας πρέπει να ενημερώσει τον ασθενή για το σκοπό της επεξεργασίας, τα δεδομένα που είναι απαραίτητα για το σκοπό αυτό και τους αποδέκτες της επεξεργασίας, το κατά πόσο η επεξεργασία είναι υποχρεωτική, και για την ύπαρξη δικαιώματος πρόσβασης στα δεδομένα του.

(β) Ο ασθενής έχει το δικαίωμα ανά πάσα στιγμή να ζητήσει να πληροφορηθεί ποια προσωπικά του δεδομένα και για ποιο σκοπό έχουν γίνει αντικείμενο επεξεργασίας.

(γ) Ο ασθενής έχει το δικαίωμα της διόρθωσης και διαγραφής των δεδομένων εάν αυτά δεν είναι ακριβή ή η επεξεργασία δεν είναι νόμιμη.

(δ) Ο ασθενής έχει το δικαίωμα ν' αντιταχθεί στην επεξεργασία.

6.2 Ιατρικό Απόρρητο

Το ιατρικό απόρρητο κατοχυρώνεται στο άρθρο 371 του Ποινικού Κώδικα σύμφωνα με το οποίο κάθε παραβίαση του απορρήτου από τον ιατρό ή τους βοηθούς του, δηλαδή εάν φανερώσει πληροφορίες σε σχέση με τον ασθενή, αποτελεί αδίκημα. Δεν αποτελεί αδίκημα η πράξη εάν ο ιατρός φανερώσει πληροφορίες στο πλαίσιο της εκπλήρωσης καθήκοντος ή της διαφύλαξης έννομου ή για άλλο λόγο δικαιολογημένου, ουσιώδους συμφέροντος του ίδιου ή κάποιου άλλου, το οποίο δεν μπορούσε να διαφυλαχθεί διαφορετικά. Το ιατρικό απόρρητο ως υποχρέωση του ιατρού που παρέχει τις υπηρεσίες του ιδιωτικά ή μέσω οργανισμών δημοσίου ή ιδιωτικού δικαίου κατοχυρώνεται επίσης στον Κανονισμός Ιατρικής Δεοντολογίας (Β.Δ. της 25/5/1955). Η προστασία της ιδιωτικής ζωής του ασθενούς και ο απόρρητος χαρακτήρας του ιατρικού φακέλου κατοχυρώνονται επίσης στο άρθρο 47 (6) του Ν. 2071/92

Συνεπώς, σε εφαρμογές ιατρικής πληροφορικής και τηλεϊατρικής οι διατάξεις για το ιατρικό απόρρητο και την προστασία των προσωπικών δεδομένων εφαρμόζονται σωρευτικά.

6.3 Ασφάλεια των ιατρικών δεδομένων

Η χρήση Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) στον τομέα της υγείας πρέπει να εξασφαλίζει την:

• *Πιστοποίηση* (authentication): έλεγχος της αυθεντικότητας της ταυτότητας των μερών μιας ανταλλαγής δεδομένων.

• *Εξουσιοδότηση* (Authorisation): η πρόσβαση του χρήστη πρέπει να είναι εξουσιοδοτημένη.

• *Εμπιστευτικότητα* (confidentiality): η τήρηση του απορρήτου των δεδομένων.

• *Ακεραιότητα* (integrity): τα δεδομένα θα πρέπει να παραμείνουν ακέραια, δηλαδή να μην υποστούν αλλοίωση.

• *Μη δυνατότητα άρνησης συμμετοχής* (non-repudiation): ο χρήστης δεν πρέπει να μπορεί να αρνηθεί τη συμμετοχή του στην ανταλλαγή των δεδομένων.

• *Δυνατότητα ελέγχου* (revision / audit): κάθε τροποποίηση ή επεξεργασία των δεδομένων πρέπει να μπορεί να ελεγχθεί, δηλαδή από ποιόν έγινε και πότε.

• *Ευθύνη* (accountability): πρέπει να προκύπτει ποιος είναι υπεύθυνος για την εισαγωγή, πρόσβαση ή τροποποίηση κάθε δεδομένου.

• *Διαφάνεια* (transparency): πρέπει να γίνεται τεκμηρίωση των διαδικασιών της επεξεργασίας ώστε να μπορούν να ελεγχθούν.

• *Διαθεσιμότητα* (availability): τα δεδομένα πρέπει να είναι διαθέσιμα όταν χρειάζεται.

7 Πλαίσιο Ορισμού σχεδίου Ασφαλείας

7.1 Απαιτήσεις Ασφαλείας

Οι θεμελιώδης αρχές χρήσης και λειτουργίας των πληροφοριακών συστημάτων θα πρέπει να ικανοποιούν τις ακόλουθες απαιτήσεις ασφάλειας:

1. Οι πληροφορίες που συσχετίζονται με προσωπικά δεδομένα θα πρέπει να διαχειρίζονται από το συνολικό σύστημα με σκοπό τη βελτίωση των παρεχομένων υπηρεσιών προς τους πολίτες.

2. Η διαχείριση των πληροφοριών θα πρέπει να γίνεται αποκλειστικά από κατάλληλο εξουσιοδοτημένο προσωπικό .

3. Τα δικαιώματα πρόσβασης στο σύστημα θα πρέπει να έχουν προσδιοριστεί με διαδικασίες ανεξάρτητες της φάσης υλοποίησης του πληροφοριακού συστήματος. Ο καθορισμός των διαδικασιών αυτών γίνεται σε επίπεδο νομοθετικό (νόμοι, διατάγματα), οργανωτικό (κανόνες λειτουργίας οργανισμού, καθηκοντολόγιο) και δομικό (κατάλληλη στελέχωση, υπεύθυνη επιτροπή ασφάλειας).

4. Η παροχή εμπιστευτικών πληροφοριών προς τρίτους θα επιτρέπεται κατόπιν έγγραφης άδειας του άμεσα ενδιαφερόμενου.

5. Οι μηχανισμοί ασφάλειας, δε θα πρέπει να μειώνουν τη συνολική αποτελεσματικότητα του συστήματος. Στη περίπτωση που δεν είναι δυνατή η εφαρμογή του προηγούμενου αξιώματος, θα πρέπει να υπάρχει ικανοποιητική ισορροπία μεταξύ απόδοσης και ασφάλειας του συστήματος.

6. Η σωστή ανάπτυξη και η αποδοτική λειτουργία πληροφοριακών συστημάτων είναι μια διαδικασία, που εμπεριέχει αναπόσπαστα τη ταυτόχρονη δόμηση ενός πλαισίου ασφάλειας, το οποίο να εξασφαλίζει τις απαιτήσεις ορθότητας, διαθεσιμότητας και μυστικότητας των περιεχομένων πληροφοριών.

7.2 Απειλές Ασφάλειας - Μέθοδοι Ασφάλειας

Στην ασφάλεια, μια αποκάλυψη αποτελεί απειλή καθώς είναι ένας τρόπος για πιθανή απώλεια ή βλάβη του Πληροφοριακού Συστήματος. Παραδείγματα αποκαλύψεων είναι η μη εξουσιοδοτημένη αποκάλυψη των δεδομένων, τροποποίηση των δεδομένων ή άρνηση του νόμιμου δικαιώματος πρόσβασης στο σύστημα. Η ευπάθεια είναι η αχίλλειος πτέρνα στο σύστημα ασφάλειας που μπορεί να εκμεταλλευτεί από τρίτους για την πρόκληση απωλειών ή ζημίας.

Ένα πρόσωπο που εκμεταλλεύεται την ευπάθεια του συστήματος διαπράττει μια επίθεση στο σύστημα. Ο συνεχής έλεγχος είναι ένα προστατευτικό μέτρο, που μπορεί να είναι είτε μια ενέργεια ή μια συσκευή ή ακόμα και μια διαδικασία ή τεχνική μέθοδος, και που μειώνει την ευπάθεια του συστήματος.

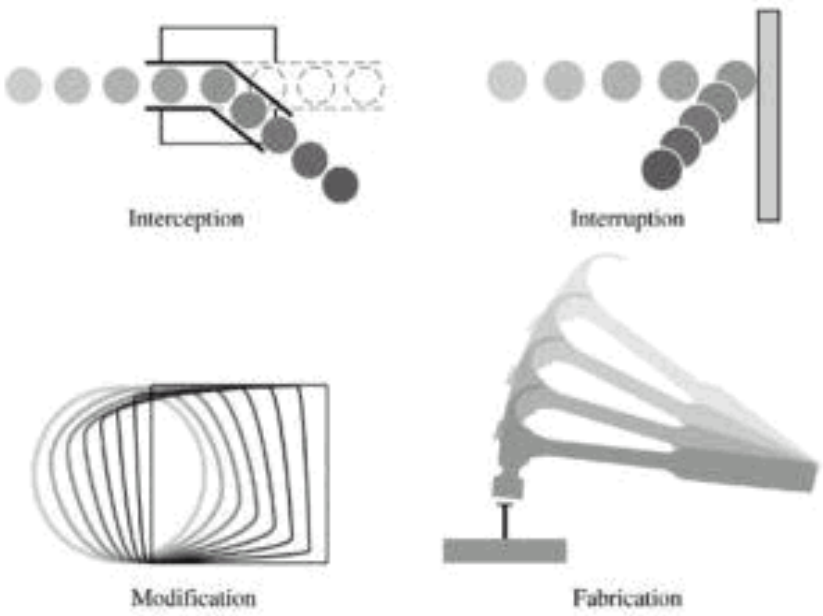
Τα μεγαλύτερα αντικείμενα του Πληροφοριακού Συστήματος είναι το υλικό, το λογισμικό και τα δεδομένα. Υπάρχουν τέσσερα είδη απειλής στην ασφάλεια του Π.Σ. που είναι:

• **Διακοπή (interruption).** Τα αντικείμενα του συστήματος χάνονται, δεν είναι διαθέσιμα ή είναι μη χρησιμοποιήσιμα. Παραδείγματα είναι η ηθελημένη καταστροφή μιας συσκευής, το σβήσιμο ενός προγράμματος ή ενός αρχείου δεδομένων, ή η δυσλειτουργία του διαχειριστή αρχείων του λειτουργικού συστήματος, έτσι ώστε να μην μπορεί να βρεθεί ένα συγκεκριμένο αρχείο στο δίσκο.

• **Παρεμπόδιση (interception).** Σημαίνει πως μια μη εξουσιοδοτημένη ομάδα έχει κερδίσει το δικαίωμα πρόσβασης σε ένα αντικείμενο. Αυτή η εξωτερική ομάδα μπορεί να είναι είτε πρόσωπα, είτε προγράμματα ή ακόμα και παρέμβαση ενός άλλου πληροφοριακού συστήματος. Παραδείγματα αυτού του είδους της αποτυχίας είναι η παράνομη αντιγραφή των προγραμμάτων ή των αρχείων δεδομένων ή οι υποκλοπές των τηλεφωνημάτων για την απόκτηση δεδομένων από το δίκτυο. Παρόλο που μια απώλεια μπορεί να αποκαλυφθεί σχετικά γρήγορα, ο υποκλοπέας μπορεί να μην αφήσει καθόλου ίχνη για την ανίχνευση της ύπαρξης του.

• **Τροποποίηση (modification).** Εάν μια μη εξουσιοδοτημένη ομάδα όχι μόνο προσπελάσει τα δεδομένα, αλλά ανακατευτεί και με κάποια αντικείμενα, τότε μιλάμε για τροποποίηση. Για παράδειγμα κάποιος μπορεί να αλλάξει τις τιμές σε μια βάση δεδομένων ή να μετατρέψει ένα πρόγραμμα έτσι ώστε να εκτελεί επιπλέον υπολογισμούς ή να τροποποιεί τα δεδομένα που μεταφέρονται ηλεκτρονικά. Είναι ακόμα δυνατό να τροποποιηθεί και το υλικό μέρος του συστήματος.

• **Πλαστοποίηση (fabricate).** Τέλος μια μη εξουσιοδοτημένη ομάδα μπορεί να κατασκευάσει πλαστά αντικείμενα σε ένα Π.Σ. Ο εισβολέας μπορεί να προσθέσει εγγραφές σε μια υπάρχουσα βάση δεδομένων. Μερικές φορές αυτές οι προσθέσεις ανιχνεύονται σαν πλαστές, αλλά εάν έχουν γίνει περίτεχνα τότε είναι αδιαχώριστες από τα πραγματικά αντικείμενα.



Εικόνα 14. Απειλές Ασφαλείας.

Κατά καιρούς έχουν προταθεί διάφοροι τρόποι ασφάλειας ενός πληροφοριακού συστήματος. Οι τρόποι αυτοί χρησιμοποιούνται στην συνέχεια ως βάση για την δημιουργία των μηχανισμών και των μέτρων προστασίας, των οποίων ο συνδυασμός θα μας δώσει το μοντέλο ασφαλείας.

Τα πιο γνωστά από αυτά είναι :

• Το *μοντέλο του κιβωτισμού* (Μια σειρά από ομόκεντρους εμφανίζονται να προστατεύουν τα δεδομένα. Αντιστοιχούν, εξεταζόμενοι από μέσα προς τα έξω, στα δεδομένα, στον Η/Υ, το υπολογιστικό κέντρο, την επιχείρηση και το υπάρχον νομικο-κοινωνικό πλαίσιο).

• Το *μοντέλο του καταλόγου* (Λίστα παραγόντων και θέματα που είναι σημαντικά. Τι πρέπει να γίνει για να θεωρηθεί ασφαλές το σύστημα και τι το απειλεί).

• Το *μοντέλο του πίνακα* (Ένας τρισδιάστατος πίνακας που απεικονίζει διαφορετικά θέματα, όπως τα βασικά χαρακτηριστικά, τα μέτρα προφύλαξης και της καταστάσεις που βρίσκεται η πληροφορία)

• Το *μοντέλο του φίλτρου* (Ένας συνδυασμός των μοντέλων καταλόγου και πίνακα) .

• Το *μοντέλο των επαλλήλων στρωμάτων* (Τα θέματα ασφάλειας αντιμετωπίζονται σε διαφορετικά επάλληλα επίπεδα, όπου το καθένα ορίζει τους στόχους του και τους προορισμούς του). [14]

7.3 Απώλειες σε ένα Πληροφοριακό Σύστημα

Οι απώλειες που μπορούν να συμβούν σε ένα Π.Σ. μπορεί να είναι είτε ηθελημένες, δηλαδή ο μη εξουσιοδοτημένος χρήστης γνωρίζει τα αποτελέσματα των ενεργειών του, είτε αθέλητες όταν δεν τα γνωρίζει, και μπορούν να ταξινομηθούν σε τρεις κατηγορίες. Απώλειες από:

(α) Αδυναμία Χρήσης του Η/Υ. Όταν ο Η/Υ είναι εκτός ενέργειας, οι υπηρεσίες που παρέχει διακόπτονται, αυτό μπορεί να οφείλεται:

• *Προσωρινή Διακοπή εξαιτίας πτώσης του ηλεκτρικού ρεύματος.* Η αντιμετώπιση γίνεται με γεννήτριες παροχής ηλεκτρικού ρεύματος, οι οποίες συνδέονται αυτόματα στο δίκτυο αν και όταν παραστεί ανάγκη (UPS, Uninterrupted Power Supply) .

• *Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ* εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου. Το πρόβλημα αυτό είναι ιδιαίτερα σοβαρό σε αποκεντρωμένα Π.Σ. που λειτουργούν όμως με συγκεντρωτική μέθοδο επεξεργασίας (π.χ. δίκτυα Τραπεζών) .

• *Πρόβλημα Υλικού*, εξαιτίας ανθρώπινου λάθους ή πλημμελούς συντήρησης.

• *Πρόβλημα Λογισμικού*, εξαιτίας ανθρώπινου λάθους ή επαγγελματικής ανεπάρκειας. Σε ό,τι αφορά την προμήθεια τυποποιημένων εφαρμογών, η πιο καλή αντιμετώπιση είναι η εγγύηση διαρκούς καλής λειτουργίας και ο μακρύς χρόνος παράλληλης λειτουργίας της νέας εφαρμογής με το χειρόγραφο ή αυτοματοποιημένο σύστημα που αντικατέστησε.

(β) Απώλεια Χρημάτων. Αν το Π.Σ. καταστραφεί ή η λειτουργία του υποβαθμισθεί, τότε υπάρχει απώλεια χρημάτων και μπορεί να εμφανισθεί σε δυο μορφές είτε μέσω της χρή*σης του Η/Υ*., για έργο διαφορετικό από αυτό που τους ανατέθηκε είτε με κλ*οπή του Η/Υ* που συνήθως πρόκειται για μεσαία και μεγάλα συστήματα.

(γ) Απώλεια Αποκλειστικής Χρήσης. Αν ένας μη εξουσιοδοτημένος χρήστης μπορέσει να χρησιμοποιήσει το Π.Σ., τότε ο κάτοχος του παύει να έχει την αποκλειστική του χρήση.

7.4 Πολιτική Αντιγράφων Ασφαλείας

Η δημιουργία αντιγράφων ασφαλείας των αρχείων στοχεύει στην προστασία τους από τη μόνιμη απώλεια ή αλλαγή τους σε περίπτωση ακούσιας διαγραφής, επίθεσης από ιό ή σε περίπτωση αστοχίας του λογισμικού ή του υλικού. Εάν συμβεί κάτι από τα παραπάνω η εταιρεία έχοντας αντίγραφα ασφαλείας, θα είναι σε θέση να κάνει επαναφορά των δεδομένων της. Τα αντίγραφα εξυπηρετούν σε πολύ μεγάλο βαθμό την ασφάλεια των δεδομένων και των συστημάτων της εταιρείας, καθώς πολλά από τα δεδομένα αυτά είναι ιδιαίτερα ευαίσθητα και είναι πολύ σημαντική η προστασία του απορρήτου τους.

Η πολιτική αντιγράφων ασφαλείας περιλαμβάνει τις διαδικασίες και τους ελέγχους που εξασφαλίζουν ότι ο τηλεπικοινωνιακός εξοπλισμός μπορείς να ανακτήσει τη λειτουργία εντός μια λογικής χρονικής περιόδου μετά από οποιαδήποτε ζημιά από κακόβουλες επιθέσεις. Στόχος της πολιτικης αυτής είναι να καθορίζει τους κανόνες και τις διαδικασίες αντιγράφων ασφαλείας και ανάκτησης δεδομένων.

Πιο συγκεκριμένα η πολιτική αντιγραφών ασφαλείας καθορίζει και περιλαμβάνει τα εξής:

• Μια διαδικασία ανάλυσης της ευαισθησίας, των ευπαθειών και της ασφάλειας των προγραμμάτων και των πληροφοριών που λαμβάνουν, χειρίζονται, αποθηκεύουν ή μεταδίδουν, ώστε να προσδιοριστεί ο λόγος για τον οποίον θα πρέπει να αποθηκεύονται τα δεδομένα.

• Ένα σχέδιο ανάκτησης δεδομένων που θα ενημερώνεται σε τακτά χρονικά διαστήματα για να δημιουργήσει και να διατηρήσει, για καθορισμένη χρονική περίοδο ακριβή αντίγραφα των πληροφοριών.

• Ένα σχέδιο αποκατάστασης έτσι ώστε να επιτρέπει τον πάροχο να την επαναφορά των στοιχείων που ζημιώθηκαν σε κάποια περίπτωση κακόβουλης επίθεσης ή κάποιας διακοπής της λειτουργίας του συστήματος.

• Ένα σχέδιο λειτουργίας τρόπου έκτακτης ανάγκης το οποίο θα επιτρέπει την άμεση λειτουργία σε περίπτωση αποτυχίας του συστήματος.

• Διαδικασίες αναθεώρησης και δοκιμών των ων σχεδίων έκτακτης ανάγκης με στόχο την κάλυψη αδυναμιών.

• Διαδικασία ελέγχου των εφεδρικών αντιγράφων καθώς και διαδικασία προσδιορισμού του τρόπου δημιουργίας τους.

• Τα αντίγραφα θα πρέπει να έχουν ίδιο επίπεδο ασφαλείας με τα αρχικά στοιχειά και θα πρέπει να διατηρούνται σε διαφορετικό χώρο/φυσική τοποθεσία από τα αρχικά δεδομένα.

7.5 Πολιτική διαχείρισης και εγκατάστασης Τηλεπικοινωνιακής Υποδομής – Κίνδυνοι Δικτύου

Με στόχο την ελαχιστοποίηση των κινδύνων προσβολής του κατανεμημένου συστήματος, μέσω της δικτυακής υποδομής θα πρέπει να εφαρμοστεί μία συνεπής πολιτική ασφάλειας. Το πλαίσιο της πολιτικής αυτής διαφοροποιείται ανάλογα με την έκταση και τη λειτουργία του συστήματος. Σε περιπτώσεις εκτεταμένων συστημάτων (π.χ. δημόσια δίκτυα), όπου οι χρήστες καλύπτουν ιδιωτικές - προσωπικές ανάγκες είναι υπό αμφισβήτηση η έκταση και η φύση του διαχειριστικού ελέγχου.

Προκύπτει δηλαδή το ερώτημα, αν είναι θεμιτή η παρακολούθηση των εργασιών ενός χρήστη από το διαχειριστή του δικτύου ή αν το γεγονός αυτό θεωρείται παραβίαση της ιδιωτικής του δραστηριότητας. Για να αποφύγουμε πιθανά παρόμοια προβλήματα περιορίζουμε την έκταση των συστημάτων, που εξετάζουμε, σε αυτά που καλύπτουν τις πληροφοριακές ανάγκες μίας μεγάλης επιχείρησης- οργανισμού.

Οι χρήστες των συστημάτων αυτών δεσμεύονται με κάποια σύμβαση, στην οποία θα πρέπει να καταγράφονται οι πληροφοριακές απαιτήσεις και το επιτρεπτό επίπεδο πρόσβασης για την εκτέλεση της καθημερινής εργασίας τους.

Τα συστήματα αυτά υποστηρίζονται επικοινωνιακά από τοπικά, μητροπολιτικά και δημόσια δίκτυα περιορισμένης όμως πρόσβασης.

Η πολιτική ασφάλειας, που θα πρέπει να εφαρμόζεται στις περιπτώσεις αυτές θα πρέπει να περιέχει τις ακόλουθες βασικές οδηγίες :

• Η πρόσβαση στις επικοινωνιακές υπηρεσίες περιορίζεται σε συγκεκριμένες οντότητες (χρήστες, διαδικασίες, διεργασίες) και για καθορισμένο χρονικό διάστημα. Κάθε λειτουργία, που έχει τη δυνατότητα να εκτελεστεί τοπικά, δε θα επιτρέπεται να χρησιμοποιεί απομακρυσμένους πόρους.

• Οι διαθέσιμες διαδικασίες ταυτοποίησης και εξακρίβωσης γνησιότητας θα πρέπει να ελέγχουν όλες τις οντότητες, που χρησιμοποιούν την επικοινωνιακή υποδομή. Για την εξακρίβωση της ορθότητας των μηνυμάτων είναι χρήσιμη η μέθοδος των ψηφιακών υπογραφών. Ειδικά κατά τη διάρκεια πρόσβασης σε κρίσιμους πόρους του συστήματος (π.χ. εξυπηρετητές), θα πρέπει οι διαδικασίες ταυτοποίησης και εξακρίβωσης γνησιότητας να είναι διπλές.

• Κάθε πρόσβαση στο δίκτυο θα πρέπει να καταγράφεται (ημερομηνία, ώρα, κόμβος, χρήστης, εφαρμογή, διάρκεια, αρχεία και συσκευές πρόσβασης). Η λειτουργία κατάλληλων εφαρμογών παρακολούθησης και καταγραφής των επικοινωνιακών δραστηριοτήτων και του προκαλούμενου φόρτου είναι αναγκαία, καθώς και η επισήμανση καταστάσεων συναγερμού σε πραγματικό χρόνο.

• Τα συνθηματικά των χρηστών των επικοινωνιακών υπηρεσιών θα πρέπει να αλλάζουν σε τακτικά χρονικά διαστήματα.

• Βελτιστοποιημένες μέθοδοι κρυπτογράφησης θα πρέπει να χρησιμοποιούνται για την αποφυγή διαρροής πληροφοριών. Θα πρέπει να τονιστεί ότι στην περίπτωση που δεν εφαρμόζονται κρυπτογραφικές μέθοδοι σε όλα τα μηνύματα, θα πρέπει να εφαρμόζονται τουλάχιστο στα μηνύματα, που μεταφέρουν ταυτότητες και συνθηματικά. Είναι γνωστό ότι η πλειοψηφία των εφαρμογών υπηρεσιών δικτύου (rlogin, ftp, κλπ) μεταφέρουν αυτούσια τις ταυτότητες - συνθηματικά μέσω δικτύου σε μορφή κειμένου. Το ίδιο ισχύει και στις εφαρμογές πρόσβασης βάσεων δεδομένων, που λειτουργούν σύμφωνα με το μοντέλο πελάτη-εξυπηρετητή, καθώς και στις κατανεμημένες βάσεις δεδομένων.

Κάθε χρήστης, συνεπώς, που έχει δυνατότητα πρόσβασης στις εφαρμογές παρακολούθησης του δικτύου ή έχει γνώσεις προγραμματισμού κατανεμημένων εφαρμογών (RPC), είναι δυνατό να υποκλέψει σταδιακά τα μεταφερόμενα συνθηματικά.

• Στις περιπτώσεις συνεχών αποτυχημένων προσπαθειών πρόσβασης θα πρέπει να απενεργοποιείται η μέθοδος πρόσβασης (πχ getty-login στο Unix) και να ειδοποιείται ο διαχειριστής του συστήματος, κρατώντας παράλληλα την ταυτότητα με την οποία επιχειρήθηκε η πρόσβαση. Σαν εναλλακτική τακτική προτείνεται η εισαγωγή του εισβολέα σε φαινομενικό περιβάλλον-κέλυφος (μετά από συνεχή εισαγωγή λανθασμένων συνθηματικών) με παράλληλη ενεργοποίηση διαδικασιών

συναγερμού του διαχειριστή. Με τη μέθοδο αυτή είναι δυνατός ο φυσικός εντοπισμός του εισβολέα.

• Παράλληλα με τα μέτρα ασφάλειας του συστήματος από τους χρήστες, θα πρέπει να διασφαλίζονται και οι χρήστες έναντι του συστήματος. Συγκεκριμένα, όπως ο χρήστες ταυτοποιούνται στο σύστημα, με τον ίδιο τρόπο το σύστημα θα πρέπει να ταυτοποιείται στον χρήστη. Συνηθισμένη πρακτική των εισβολέων είναι η δημιουργία προγραμμάτων ταυτοποίησης παρόμοια με αυτά των λειτουργικών-δικτυακών συστημάτων με στόχο την υφαρπαγή των συνθηματικών, κατά τη διαδικασία καταχώρησης τους από τους τελικούς χρήστες.

• Θα πρέπει να μελετηθεί στατιστικά οι κυκλοφορία, που εισάγει στο δίκτυο κάθε χρήστης. Με τον τρόπο αυτό θα είναι δυνατός ο εντοπισμός του υπερβολικού κυκλοφοριακού φόρτου, τον οποίο προκαλούν οι εισβολείς, με τελικό σκοπό τη δημιουργία καθυστερήσεων και την πιθανή πλήρη κατάρρευση του δικτύου.

• Θα πρέπει να υπάρχουν διπλές διαδικασίες επιβεβαίωσης (από δύο τουλάχιστον διαχειριστές), για κάθε ζωτική αλλαγή της σύνθεσης (νέος κόμβος, νέοι χρήστες, διαδικασίες συντήρησης), καθώς και για τις διαδικασίες παρακολούθησης (monitoring) του συστήματος. Σε κάθε εγκατάσταση νέου κόμβου, νέου λογισμικού θα πρέπει να αλλάζουν τα συνθηματικά που δίδονται από τις κατασκευάστριες εταιρίες, τα οποία συνήθως καλύπτουν βασικές λειτουργίες των συστατικών αυτών του κατανεμημένου συστήματος (εγκατάσταση, συντήρηση).

• Σταθμοί εργασίας χωρίς δισκέτες ή σκληρούς δίσκους θα πρέπει να χρησιμοποιούνται όπου είναι δυνατόν. Με τη μέθοδο αυτή θα αποφεύγεται η εισαγωγή προγραμμάτων ιών και η ανεπιθύμητη αντιγραφή μηνυμάτων-πληροφοριών. Οι διαδικασίες εκκίνησης των συστημάτων (boot) αυτών θα ενεργοποιούνται από μνήμες EPROM ή από απομακρυσμένους κόμβους (remote boot).

• Ολα τα ενεργά συστατικά του δικτύου (κόμβοι, εξυπηρετητές, συσκευές διαδικτύωσης, συγκεντρωτές, επαναλήπτες), θα πρέπει να είναι φυσικά προστατευμένα. Σε εκτεταμένες εγκαταστάσεις είναι αναγκαία η προστασία των συσκευών, οι οποίες δεν ελέγχονται από απομακρυσμένους κόμβους.

Τέτοιες συσκευές είναι οι παθητικοί επαναλήπτες χωρίς υποστήριξη SNMP πρωτοκόλλου, καθώς και οι εξυπηρετητές 'κουτών' τερματικών (terminal servers). Οι καλωδιώσεις πρέπει να διασχίζουν χώρους μη προσβάσιμους από το κοινό και να ευρίσκονται σε μεταλλικές σωληνώσεις. Τα κιβώτια διακλαδώσεων θα πρέπει να προστατεύονται από κλειδαριές. Η χρήση οπτικών ινών συστήνεται λόγω δυσκολίας στη διακλάδωσή τους, καθώς επίσης και η ύπαρξη εναλλακτικών καλωδιώσεων - διαδρομών με αυτόματη ενεργοποίηση των εφεδρικών φυσικών διαδρομών. Επίσης,

συνίσταται να αποφεύγεται η χρήση δημοσίων δικτύων. Αν αυτό δεν είναι δυνατόν θα πρέπει να χρησιμοποιούνται αποκλειστικές γραμμές και να δεσμεύεται ο τηλεπικοινωνιακός οργανισμός, με κατάλληλη σύμβαση, σχετικά με πιθανή εισβολή με δική του υπαιτιότητα. Οι οδηγίες, που αναφέραμε, αφορούν την προστασία της δικτυακής υποδομής από πιθανές εισβολές. Για την πλήρη διαθεσιμότητα και σωστή λειτουργία του συστήματος θα πρέπει να ληφθούν επιπρόσθετα μέτρα.

Οι κίνδυνοι των δικτυακών υποδομών απέναντι σε μη εξουσιοδοτημένες προσπάθειες πρόσβασης είναι αρκετοί. Βασικός λόγος είναι η επιθυμία πρόσβασης σε αποθηκευμένα αντικείμενα ενός κατανεμημένου συστήματος και η χρήση των παρεχομένων υπηρεσιών του. Σημαντικότατος λόγος επίσης είναι η αυξανόμενη ποσότητα και αξία των πληροφοριών που διακινούνται μεταξύ των διασυνδεδεμένων υπολογιστικών συστημάτων (εξυπηρετητές, σταθμοί εργασίας), και σε συνδυασμό με την ανάπτυξη και επέκταση σε έκταση επικοινωνιακών υποδομών (διαδίκτυο), αυξάνουν την δυνατότητα πρόσβασης από μη έξουσιοδοτημένα άτομα και καθιστούν την ασφάλεια των δικτύων ευάλωτη.

Ένας εισβολέας μπορεί να περιλαμβάνεται, στο σύνολο των εξουσιοδοτημένων χρηστών (και να επιθυμεί πρόσβαση υψηλότερου του επιτρεπτού επιπέδου), αλλά είναι δυνατό να προέρχεται και εκτός του οργανισμού, που εξυπηρετείται από το σύστημα. Σκοπός μίας μη εξουσιοδοτημένης εισβολής μπορεί να είναι η γνωστοποίηση πληροφοριών, η μεταβολή και η καταστροφή πληροφοριών, η μερική ή συνολική χρήση-καταστροφή των πόρων του συστήματος καθώς επίσης και η εισαγωγή προγραμμάτων καταστροφέων (ιών).

Οι πιο γνωστές εσκεμμένες απειλές που μπορούν να διαταράξουν την ασφάλεια ενός δικτύου είναι οι ακόλουθες:

- Μη-εξουσιοδοτημένη χρήση ή μεταμφίεση κατά την οποία επιχειρείται προσπέλαση στα δεδομένα ή στις προαναφερόμενες υπηρεσίες του δικτύου από μη εξουσιοδοτημένους χρήστες.

- Μη-ενεργός παρακολούθηση κατά την οποία απειλείται η εμπιστευτικότητα των ανταλασσομένων μηνυμάτων στο δίκτυο από μη-ενεργούς παρεμβολείς.

- Ενεργός παρακολούθηση κατά την οποία επιχειρείται τροποποίηση ή εξαγωγή των ανταλασσομένων δεδομένων στο δίκτυο. Ο ενεργός παρεμβολέας μπορεί μεν να εντοπισθεί πιο εύκολα, αλλά μπορεί δε να προκαλέσει μεγαλύτερη ζημία στο δίκτυο.

• Καταλογισμός ευθύνης, όπου ένας εξουσιοδοτημένος χρήστης μπορεί να απαρνηθεί την ευθύνη αποστολής ή παραλαβής ενός συγκεκριμένου μηνύματος ή ακόμη να κατασκευάσει ένα μη έγκυρο μήνυμα.

• Άρνηση εξυπηρέτησης κατά την οποία το δίκτυο δεν ανταποκρίνεται στο απαιτούμενο επίπεδο εξυπηρέτησης ή και λειτουργικότητας.

• Επανάληψη, όπου ένας εξουσιοδοτημένος χρήστης προβαίνει στην επανάληψη ενός μηνύματος με στόχο να θεωρηθεί από τον αποδέκτη του ως πρωτότυπο.

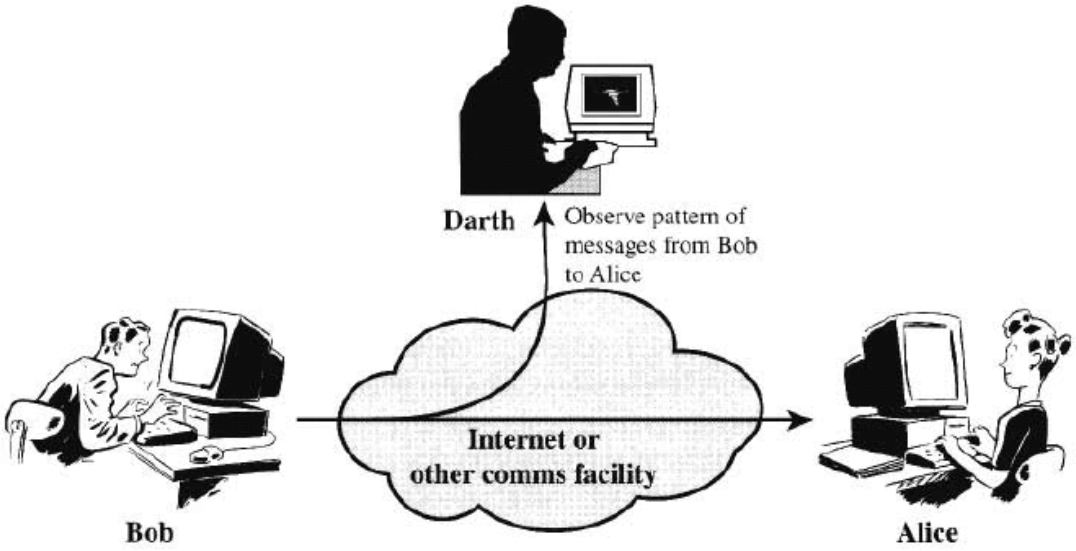
• Ανάλυση επικοινωνίας κατά την οποία παρακολουθείται η μετάδοση των μηνυμάτων στο δίκτυο για τον εντοπισμό κυρίως της προέλευσή τους ή και της αποστολής τους.

• Ιοί, σημαντικό πρόβλημα των υπολογιστικών συστημάτων. εν είναι τίποτα άλλο παρά λογισμικό που σχεδιάζεται για να προκαλέσει προβλήματα στην ομαλή λειτουργία του συστήματος. Ο τρόπος λειτουργίας τους είναι η επαναλαμβανόμενη αντιγραφή τους σε σημεία που ήδη βρίσκονται καταχωρημένα άλλα δεδομένα.

Οι προσπάθειες εισόδου στη δικτυακή δομή ανάλογα με τον στόχο τους μπορούν να διακριθούν σε δύο κατηγορίες εισβολών, τις *παθητικές* και τις *ενεργητικές*. Στις παθητικές εισβολές, ο εισβολέας παρατηρεί τα μηνύματα, που διέρχονται στο φυσικό μέσον, χωρίς να παρεμβαίνει στη φύση και τη ροή τους. Αυτού του είδους εισβολές διακρίνονται σε δυο υποκατηγορίες παθητικής εισβολής.

• *Παρατήρηση του περιεχομένου των μηνυμάτων*, κατά την οποία ο εισβολέας υποκλέπτει μέρος ή τον σύνολο των διακινουμένων πληροφοριών.

• *Ανάλυση της κυκλοφορίας*, κατά την οποία ο εισβολέας καταγράφει και αναλύει τα διερχόμενα μηνύματα με σκοπό τη συγκέντρωση άμεσων ή επαγωγικών πληροφοριών. Οι πληροφορίες αυτές αφορούν τη δομή του συστήματος, τα χρησιμοποιούμενα πρωτόκολλα, την ονοματολογία, τους ενεργούς χρήστες, τους ενεργούς κόμβους, τις εκτελούμενες εφαρμογές και τις υπηρεσίες του συστήματος.



Εικόνα 15. Παθητικές Εισβολές

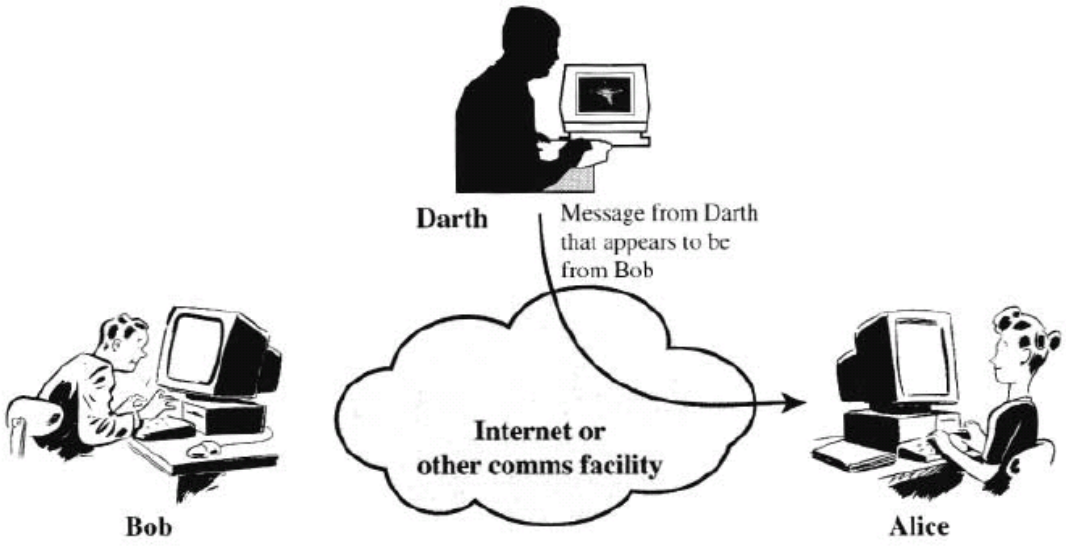
Στις ενεργητικές εισβολές ο εισβολέας επεξεργάζεται τα διερχόμενα μηνύματα και πιθανά εισάγει νέα. Αυτού του είδους εισβολές διακρίνονται σε τέσσερις υποκατηγορίες :

(α) Τη μεταβολή των μηνυμάτων. Κατά την παραβίαση αυτή μεταβάλλεται το περιεχόμενο των μηνυμάτων (δεδομένα, διευθύνσεις, τμήματα ελέγχου), εισάγονται νέα μηνύματα ή μεταβάλλεται η σειρά των αποστελλόμενων μηνυμάτων.

(β) Τη διαγραφή μηνυμάτων. Κατά την οποία καταστρέφεται μέρος ή το σύνολο των μηνυμάτων, που ανταλλάσσονται κατά τη διάρκεια των συνόδων.

(γ) Την καθυστέρηση επικοινωνίας. Ο εισβολέας άμεσα με την κατακράτηση και επαναποστολή μηνυμάτων ή έμμεσα με την εισαγωγή υψηλού φόρτου στο δίκτυο προκαλεί καθυστέρηση της επικοινωνιακής κυκλοφορίας.

(δ) Μεταμφίεση του εισβολέα. Στην περίπτωση αυτή ο εισβολέας δημιουργεί μία, ή περισσότερες συνόδους με ψευδή ταυτότητα. Αυτό επιτυγχάνεται με την υφαρπαγή των στοιχείων ταυτότητας ενός 'νόμιμου' χρήστη, καθώς και με την επανάληψη μηνυμάτων που έχουν αντιγραφεί από μία προηγούμενη 'νόμιμη' σύνοδο.



Εικόνα 16. Ενεργητικές Εισβολές.

7.6 Διαδικασία χειρισμού περιστατικών ασφαλείας

Με στόχο την άμεση αντιμετώπιση των κινδύνων μιας προσβολής του συστήματος, θα πρέπει να εφαρμοστεί μία πολιτική διαχείρισης έκτακτων περιστατικών ασφαλείας. Σύμφωνα με την Πολιτική Διαχείρισης Περιστατικών Ασφάλειας, ορίζεται μια διαδικασία χειρισμού περιστατικών ασφαλείας που έχει ως στόχο της:

(α) να καταγραφούν οι λεπτομέρειες κάθε περιστατικού ασφάλειας,

(β) να διερευνηθούν τα αίτια και να προσδιοριστούν οι τεχνικές ή/και οργανωτικές αδυναμίες στις οποίες οφείλεται το περιστατικό ασφάλειας,

(γ) να καθοριστούν και να υλοποιηθούν οι ενέργειες αποκατάστασης καθώς και να σχεδιαστεί κατάλληλο χρονοδιάγραμμα και

(δ) να ενημερωθούν ο υπεύθυνος Διασφάλισης του Απορρήτου των Επικοινωνιών και τα αρμόδια στελέχη του προσώπου που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, οι αρμόδιες Αρχές καθώς και οι θιγόμενοι χρήστες των παρεχόμενων δικτύων ή υπηρεσιών.

Η Διαδικασία Διαχείρισης έκτακτων περιστατικών προϋποθέτει τα εξής:

Κάθε πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να καταρτίζει και να εφαρμόζει Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας, η οποία θα ενεργοποιείται σε κάθε περίπτωση παραβίασης ή ιδιαίτερου κινδύνου παραβίασης του απορρήτου των επικοινωνιών ή όταν διαπιστώνεται ότι δεν εφαρμόζεται ή υφίσταται ιδιαίτερος κίνδυνος μη εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών.

Στη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας προβλέπεται η καταγραφή όλων των παραπάνω στοιχείων, που αποτελούν τα στάδια για τη διαχείριση των περιστατικών ασφάλειας, καθώς και η σύνταξη και διατήρηση σε αρχείο όλων των σχετικών με τα περιστατικά ασφάλειας εγγράφων, από τα οποία θα τεκμηριώνεται και η τέλεση των προαναφερόμενων βημάτων.

Στη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας ορίζονται τα αρμόδια στελέχη του προσώπου που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών στα οποία θα πρέπει να αναφέρονται άμεσα τα περιστατικά ασφάλειας από τους εργαζόμενους και τους συνεργάτες του, καθώς και τα σχετικά στοιχεία επικοινωνίας αυτών (τηλέφωνα, fax, email ή άλλο μέσο που κρίνεται πρόσφορο).

Το πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να παρέχει στους συνδρομητές ή χρήστες των δικτύων ή υπηρεσιών του τη δυνατότητα να καταγγέλλουν με απλά μέσα (π.χ. μέσω της ιστοθέσης του) την ενδεχόμενη παραβίαση του απορρήτου των επικοινωνιών τους.

7.7 Τεχνικές διασφάλισης εμπιστευτικότητας

Οι βασικές τεχνικές διασφάλισης εμπιστευτικότητας στα πληροφοριακά συστήματα είναι δύο. Μια τεχνική είναι ο *έλεγχος ταυτότητας*, μέσω του οποίου εξασφαλίζεται ότι η οντότητα που παρουσιάζεται με κάποια ταυτότητα είναι όντως αυτή που ισχυρίζεται, η τεχνικής αυτή στηρίζεται στην χρήση κωδικών για την επαλήθευση της ταυτότητας.

Υπάρχουν τρεις βασικοί τρόποι για την διακρίβωση της ταυτότητας οι οποίοι μπορούν να χρησιμοποιηθούν μεμονωμένα ή συνδυαστικά:

(α) *να ζητείται κάτι που ο χρήστης γνωρίζει* (ένα μυστικό, π.χ. ένα συνθηματικό, ένας προσωπικός αριθμός αναγνώρισης ή ένα κρυπτογραφικό κλειδί)

(β) *να ζητείται κάτι που βρίσκεται υπό την κατοχή του χρήστη*, όπως μία έξυπνη κάρτα, μία κάρτα αυτόματων ταμειακών συναλλαγών κ.λπ.

(γ) *να εξετάζεται κάποιο βιομετρικό χαρακτηριστικό του χρήστη*, όπως π.χ. δακτυλικά αποτυπώματα, σχήμα ίριδας, τρόπος γραφής κ.τ.λ.

Η δεύτερη τεχνική είναι ο *έλεγχος προσπέλασης* που χρησιμοποιείται για να επιτρέψει σε κάποια διακριβωμένη πια οντότητα να προσπελάσει μόνο τα αντικείμενα και τις υπηρεσίες για τα οποία είναι εξουσιοδοτημένη.

7.8 Πολιτική Χρήσης Κωδικών Ασφαλείας

Το βασικό δομικό στοιχείο της ασφάλειας συστημάτων, αποτελεί η διακρίβωση ταυτότητας καθώς είναι τη βάση για τους περισσότερους τύπους ελέγχου πρόσβασης και καταλογισμού ευθυνών. Το σύστημα θα πρέπει να έχει τη δυνατότητα να ταυτοποιεί τους χρήστες και να μπορεί να τους ξεχωρίζει. Για παράδειγμα, ο έλεγχος πρόσβασης συχνά βασίζεται στην αρχή των ελάχιστων προνομίων, δίνοντας στους χρήστες μόνο τα δικαιώματα που τους είναι απολύτως απαραίτητα για την επιτέλεση των εργασιών τους.

Με τον όρο καταλογισμό ευθυνών εννοούμε τη σύνδεση των δραστηριοτήτων σε ένα υπολογιστικό σύστημα με συγκεκριμένα άτομα, έτσι ώστε το σύστημα να μπορεί να γνωρίζει την ταυτότητα των χρηστών. Κατά τη διακρίβωση ταυτότητας, η οντότητα αρχικά παρουσιάζει στο σύστημα έναν ισχυρισμό περί της ταυτότητας της και ακολούθως το σύστημα εξετάζει αν αυτός ο ισχυρισμός είναι αληθής.

Στη διαδικασία αυτή υπάρχουν τα εξής βήματα: η συλλογή των πληροφοριών που δίνει ο χρήστης, η ασφαλής μετάδοσή τους και ο προσδιορισμός του αν ο χρήστης που αρχικά διακριβώθηκε εξακολουθεί να είναι ο ίδιος που τώρα χρησιμοποιεί το σύστημα. Για παράδειγμα, αν ένας χρήστης συνδεθεί σε κάποιο τερματικό και στη συνέχεια το εγκαταλείψει προσωρινά, είναι δυνατόν κάποιος άλλος χρήστης να το χρησιμοποιήσει υπό την ταυτότητα του πρώτου.

Μολονότι φαίνεται ότι οποιοδήποτε από αυτά τα μέσα μπορεί να παρέχει ισχυρή διακρίβωση ταυτότητας, υπάρχουν και κάποια προβλήματα: τα συνθηματικά μπορεί να διαρρεύσουν ή να μαντευθούν, οι έξυπνες κάρτες μπορεί να κλαπούν ή να κατασκευαστούν πλαστές ακόμη και τα βιομετρικά συστήματα μπορούν να ξεγελασθούν.

Κάθε μέθοδος έχει πλεονεκτήματα αλλά και κάποια μειονεκτήματα για τους διαχειριστές και τους νόμιμους χρήστες, για παράδειγμα οι χρήστες ξεχνάνε τα συνθηματικά ή χάνουν τις έξυπνες κάρτες, και η διαχειριστική επιβάρυνση για την αντιμετώπιση αυτών των ζητημάτων μπορεί να είναι σημαντική. Επίσης, τα βιομετρικά συστήματα συναντούν προβλήματα αποδοχής από πλευράς χρηστών, έχουν υψηλό κόστος και τεχνικές δυσκολίες. Οι τεχνικές αυτές αλλά και οι δυσκολίες τους αναλύονται παρακάτω.

(α)Τεχνικές όπου ζητείται κάτι που ο χρήστης γνωρίζει. Η πιο συνηθισμένη τεχνική διακρίβωσης ταυτότητας συσχετίζει κάθε ταυτότητα χρήστη με ένα συνθηματικό. Η τεχνική αυτή βασίζεται αποκλειστικά σε κάτι που ο χρήστης γνωρίζει. Υπάρχουν και άλλες τεχνικές που ζητούν κάτι που γνωρίζει ο χρήστης, όπως π.χ. ένα κρυπτογραφικό κλειδί.

• *Συνθηματικά*: Εδώ απαιτείται από τον χρήστη να εισάγει την ταυτότητά του μαζί με ένα συνθηματικό. Το σύστημα συγκρίνει το συνθηματικό με αυτό που είναι αποθηκευμένο στο αρχείο συνθηματικών για τον συγκεκριμένο χρήστη. Αν είναι ίδια, η ταυτότητα έχει διακριβωθεί επιτυχώς. Η χρήση συνθηματικών έχει παράσχει ασφάλεια σε υπολογιστικά συστήματα για μεγάλο χρονικό διάστημα. Οι σχετικοί μηχανισμοί είναι ενσωματωμένοι στα λειτουργικά συστήματα και οι χρήστες, αλλά και οι διαχειριστές συστημάτων είναι εξοικειωμένοι με αυτά. Με κατάλληλη διαχείριση σε ένα ελεγχόμενο περιβάλλον μπορούν να αποτελέσουν αποτελεσματικό μηχανισμό διακρίβωσης ταυτότητας.

• *Κρυπτογραφικά κλειδιά*: Σε αυτή την προσέγγιση θα λέγαμε ότι πραγματεύεται η διακρίβωση ταυτότητας βάσει αντικειμένων που έχει στην κατοχή του ο χρήστης. Αν και η δυνατότητα διακρίβωσης της ταυτότητας μέσω κρυπτογραφικού κλειδιού βασίζεται σε κάτι που γνωρίζει ο χρήστης, αυτός πρέπει συνήθως να έχει στη διάθεσή του κάποια συσκευή (π.χ. έξυπνη κάρτα ή PC), η οποία θα εκτελέσει τους κρυπτογραφικούς υπολογισμούς.

Μειονεκτήματα της τεχνικής αυτής είναι αρκετά. Η λειτουργία αυτής της τεχνικής βασίζεται στο ότι δεν θα διαρρεύσουν τα συνθηματικά. Δυστυχώς, υπάρχουν πολλοί τρόποι με τους οποίους είναι δυνατόν να αποκαλυφθούν όπως το μάντεμα του συνθηματικού, ο διαμοιρασμός του συνθηματικού , η ηλεκτρονική παρακολούθηση ή ακόμα και η πρόσβαση στο αρχείο των συνθηματικών.

Όσον αφόρα την ηλεκτρονική παρακολούθηση ούτε η κρυπτογράφηση λύνει το πρόβλημα, καθώς η επανακρυπτογράφηση του ίδιου συνθηματικού θα δώσει το ίδιο κρυπτογραφημένο κείμενο. Συνεπώς, σε ό,τι αφορά το σύστημα που λαμβάνει το συνθηματικό, αν του σταλεί ξανά το κρυπτογραφημένο κείμενο που υπεκλάπη θα το θεωρήσει ως σωστό συνθηματικό.

Όσον αφόρα την πρόσβαση στο αρχείο συνθηματικών τα περισσότερα αρχεία συνθηματικών συνήθως προστατεύονται με μονόδρομη κρυπτογράφηση. Πάραυτα με εξαντλητική αναζήτηση και την αυξημένη υπολογιστική ισχύ των σύγχρονων υπολογιστών, εξακολουθεί να είναι δυνατή η εύρεση των συνθηματικών.

(β) Τεχνικές όπου ζητάται κάτι που ο χρήστης κατέχει. Αν και αρκετές τεχνικές βασίζονται αποκλειστικά σε κάτι που ο χρήστης κατέχει, συνήθως ζητάται παράλληλα και κάτι που ο χρήστης γνωρίζει. Ο συνδυασμός αυτός συνήθως αποφέρει υψηλότερα επίπεδα ασφάλειας. Τα αντικείμενα που κατέχει ο χρήστης για σκοπούς διακρίβωσης ταυτότητας καλούνται *διακριτικά* (tokens). Τα Διακριτικά διαχωρίζονται σε *διακριτικά* μνήμης και σε έξυπνα διακριτικά.

• *Διακριτικά μνήμης:* Τα διακριτικά μνήμης αποθηκεύουν αλλά δεν επεξεργάζονται πληροφορίες. Η εγγραφή και η ανάγνωση δεδομένων σε/από αυτά διενεργείται μέσω ειδικών συσκευών. Ο πιο διαδεδομένος τύπος διακριτικών μνήμης είναι οι κάρτες που είναι εφοδιασμένες με μία μαγνητική ταινία, οι οποίες διαβάζονται από ειδικούς αναγνώστες όπως οι κάρτες τραπεζών για ανάληψη μετρητών από αυτόματες ταμειακές μηχανές – ATM. Οι χρήστες απαιτείται, πέρα από το ίδιο το διακριτικό, να εισάγουν και έναν προσωπικό αριθμό αναγνώρισης. Σε μερικά συστήματα η διακρίβωση ταυτότητας γίνεται αποκλειστικά μέσω ενός διακριτικού, χωρίς να ζητάται κάτι που ο χρήστης γνωρίζει. Τα συστήματα αυτά είναι σχετικά λίγα και κυρίως αφορούν τον έλεγχο φυσικής πρόσβασης σε χώρους.

• *Έξυπνα διακριτικά:* Ένα έξυπνο διακριτικό επεκτείνει τη λειτουργικότητα ενός διακριτικού μνήμης, ενσωματώνοντας ένα ή περισσότερα ολοκληρωμένα κυκλώματα. Όταν χρησιμοποιείται για διακρίβωση ταυτότητας, ένα έξυπνο διακριτικό εμπίπτει στην κατηγορία τεχνικών όπου ζητάται κάτι που ο χρήστης κατέχει, ενώ είναι δυνατόν παράλληλα να ζητάται κάτι που ο χρήστης γνωρίζει όπως π.χ. ένας προσωπικός αριθμός αναγνώρισης. Υπάρχουν πολλά διαφορετικά είδη έξυπνων διακριτικών.

Πλεονεκτήματα των διακριτικών μνήμης είναι ότι αν συνδυαστούν με προσωπικούς αριθμούς αναγνώρισης είναι πολύ πιο ασφαλή από τα συνθηματικά. Επισης, είναι ιδιαίτερα φθηνά, ενώ για να καταφέρει ένας μη εξουσιοδοτημένος χρήστης να αποκτήσει πρόσβαση πρέπει και να έχει στην κατοχή του και το διακριτικό και να γνωρίζει τον αριθμό. Ο συνδυασμός αυτός είναι πιο δύσκολο να αποκτηθεί απ’ ό,τι ένα ζεύγος (ταυτότητα χρήστη, συνθηματικό), ειδικότερα αν λάβουμε υπόψη ότι οι ταυτότητες χρήστη δεν είναι μυστικές. Ένα ακόμα

πλεονέκτημα των διακριτικών είναι ότι μπορούν να χρησιμοποιηθούν για παραγωγή αρχείων καταγραφής, χωρίς να είναι απαραίτητο να εισάγει ο χρήστης την ταυτότητά του για κάθε δοσοληψία ή συμβάν που πρέπει να καταγραφεί, καθώς το σύστημα αντλεί τη σχετική πληροφορία από το διακριτικό. Αν το διακριτικό χρησιμοποιείται, εκτός από την διακρίβωση ταυτότητας στον υπολογιστή, και για είσοδο και έξοδο από τον φυσικό χώρο, τότε οι χρήστες αναγκαστικά το αφαιρούν από τον υπολογιστή όταν απομακρύνονται από τον χώρο. Με τον τρόπο αυτό μηδενίζεται η πιθανότητα να χρησιμοποιήσει κανείς κάποιο τερματικό που άφησε ανεπιτήρητο ένας χρήστης.

Η χρήση διακριτικών μνήμης όμως έχει και κάποια μειονεκτήματα. Αν και είναι τελικά δυνατή η πραγματοποίηση πολύ καλά προετοιμασμένων επιθέσεων ενάντια σε συστήματα που χρησιμοποιούν αυτή τη μέθοδο, τα περισσότερα προβλήματα ανάγονται στο κόστος, τη διαχείριση, την απώλεια των διακριτικών, τη δυσαρέσκεια των χρηστών και τη διαρροή των προσωπικών αριθμών αναγνώρισης. Όσον αφόρα το κόστος τα διακριτικά μνήμης απαιτούν εξιδικευμένες συσκευές ανάγνωσης του προσωπικού αριθμού του χρήστη καθώς και την χρήση κρυπτογραφίας για την μετάδοση των δεδομένων. Από την άλλη αν ένας χρήστης χάσει το διακριτικό του, δεν θα μπορεί να συνδεθεί στο σύστημα μέχρι να αντικατασταθεί το διακριτικό. Με τον τρόπο αυτό αυξάνεται το διαχειριστικό κόστος και η επιβάρυνση.

Το απολεσθέν διακριτικό μπορεί να έχει κλαπεί ή μπορεί να βρεθεί από κάποιον και ο νέος κάτοχός του μπορεί να επιχειρήσει να εισέλθει στο σύστημα. Επίσης, έχουμε και την δυσαρέσκεια των χρηστών, οι οποίοι επιθυμούν υπολογιστές εύκολους στη χρήση. Πολλοί από αυτούς το βρίσκουν άβολο να κουβαλάνε και να χρησιμοποιούν ένα διακριτικό. Οι αντιδράσεις ωστόσο περιορίζονται αν είναι προφανής η αναγκαιότητα για αυξημένη ασφάλεια.

Όσον αφορά τα έξυπνα διακριτικά μπορούν να καταταχθούν σε κατηγορίες βάσει των φυσικών χαρακτηριστικών τους, της διεπαφής τους και των πρωτοκόλλων που χρησιμοποιούν. Οι κατηγοριοποιήσεις αυτές δεν είναι αμοιβαία αποκλειόμενες.

Φυσικά χαρακτηριστικά: Τα έξυπνα διακριτικά μπορεί να είναι «έξυπνες κάρτες», οι οποίες μοιάζουν με πιστωτικές κάρτες αλλά περιλαμβάνουν επίσης και κάποιον μικροεπεξεργαστή. Οι έξυπνες κάρτες περιγράφονται από ένα πρότυπο του διεθνούς οργανισμού προτύπων (ISO). Τα έξυπνα διακριτικά που δεν είναι «έξυπνες κάρτες» μοιάζουν συνήθως με μικρές αριθμομηχανές.

Διεπαφή: Τα έξυπνα διακριτικά έχουν μία διεπαφή που μπορεί να τους επιτρέπει να επικοινωνούν είτε με ανθρώπους είτε με ηλεκτρονικά συστήματα. Τα

διακριτικά που έχουν διεπαφή για επικοινωνία με ανθρώπους ενσωματώνουν οθόνες ή/και πληκτρολόγια για να επιτρέπουν την εισαγωγή και την προβολή στοιχείων. Τα διακριτικά με διεπαφές για επικοινωνία με ηλεκτρονικά συστήματα ανταλλάσσουν δεδομένα με ειδικές διατάξεις ανάγνωσης/εγγραφής. Τα διακριτικά που έχουν τη μορφή αριθμομηχανών συνήθως διαθέτουν διεπαφή για επικοινωνία με ανθρώπους.

Πρωτόκολλο: Ένα έξυπνο διακριτικό μπορεί να χρησιμοποιήσει διάφορα πρωτόκολλα για την διακρίβωση ταυτότητας.

Τα έξυπνα διακριτικά που χρησιμοποιούν πρωτόκολλα ανάλογα με το είδος πρωτοκόλλου που χρησιμοποιούν μπορούν να διακριθούν σε τρεις κατηγορίες:

(α) *Στατική ανταλλαγή συνθηματικών*. Βάσει του πρωτοκόλλου αυτού οι χρήστες εισάγουν το συνθηματικό τους στο έξυπνο διακριτικό, το οποίο κατόπιν συνεργάζεται με τον υπολογιστή για τη διακρίβωση της ταυτότητας του χρήστη.

(β) *Δυναμική γέννηση συνθηματικών*. Βάσει του πρωτοκόλλου αυτού, το έξυπνο διακριτικό δημιουργεί μία μοναδική τιμή, π.χ. έναν οκταψήφιο αριθμό, ο οποίος αλλάζει περιοδικά. Αν το διακριτικό έχει διεπαφή προσανατολισμένη σε επικοινωνία με ανθρώπους, ο χρήστης απλά διαβάζει τον αριθμό από την οθόνη του διακριτικού και το εισάγει στον υπολογιστή για διακρίβωση της ταυτότητάς του. Αν το διακριτικό έχει διεπαφή προσανατολισμένη σε επικοινωνία με ηλεκτρονικές διατάξεις, ο αριθμός αποστέλλεται αυτομάτως. Αν η εισαχθείσα τιμή είναι σωστή (δηλαδή είναι ανάμεσα στις παραδεκτές τιμές που ο υπολογιστής γνωρίζει ότι μπορεί να παράγει το συγκεκριμένο διακριτικό για τη δεδομένη χρονική περίοδο), θεωρείται ότι η ταυτότητα του χρήστη έχει διακριβωθεί.

(γ) Πρωτόκολλα ερωταποκρίσεων. Βάσει του πρωτοκόλλου αυτού ο υπολογιστής δημιουργεί μία ερώτηση π.χ. μία τυχαία ακολουθία από αριθμούς. Το έξυπνο διακριτικό παράγει μία απάντηση, ως συνάρτηση της ερώτησης, η οποία αποστέλλεται στον υπολογιστή, και ο υπολογιστής διακριβώνει την ταυτότητα του χρήστη βάσει της απάντησης. Οι αλγόριθμοι υπολογισμού της απάντησης από την ερώτηση στηρίζονται σε κρυπτογραφικές μεθόδους. Τα πρωτόκολλα ερωταποκρίσεων μπορούν να χρησιμοποιηθούν είτε με διεπαφές προσανατολισμένες σε επικοινωνία με ανθρώπους είτε με διεπαφές για επικοινωνία με ηλεκτρονικές διατάξεις.

Τα έξυπνα διακριτικά παρέχουν μεγάλη ευελιξία και μπορούν να λύσουν πολλά προβλήματα διακρίβωσης ταυτότητας. Τα πλεονεκτήματα που αποκομίζουμε από τη

χρήση τους ποικίλλουν, ανάλογα με το είδος των διακριτικών που χρησιμοποιούνται, στη γενική περίπτωση πάντως προσφέρουν μεγαλύτερη ασφάλεια από τα διακριτικά μνήμης. Τα έξυπνα διακριτικά μπορούν να λύσουν και το πρόβλημα της υποκλοπής των συνθηματικών κατά τη δικτυακή επικοινωνία, ακόμη και αν αυτή πραγματοποιείται μέσα από ανοικτά δημόσια δίκτυα, καθώς μπορούν να εφαρμόσουν τεχνικές συνθηματικών μίας χρήσης (π.χ. στην περίπτωση του πρωτοκόλλου ερωταποκρίσεων).

(γ) να εξετάζεται κάποιο βιομετρικό χαρακτηριστικό του χρήστη, όπως π.χ. δακτυλικά αποτυπώματα, σχήμα ίριδας, τρόπος γραφής κ.τ.λ.

8 Κανόνες και μέτρα υλοποίησης της πολιτικής ασφαλείας

8.1 Κανόνες Πολιτικής Ασφαλείας

Γενικά, στο πλαίσιο της λειτουργίας ενός οργανισμού, μια *πολιτική* αποτελεί το σύνολο των οδηγιών της διοίκησης για τον τρόπο με τον οποίο πρέπει να λειτουργεί ο οργανισμός. Περιλαμβάνει δηλαδή γενικές προτάσεις (high-level statements) που έχουν στόχο να καθοδηγήσουν τη λήψη αποφάσεων σχετικά με τα τρέχοντα και μελλοντικά ζητήματα που αντιμετωπίζουν τα μέλη του οργανισμού. Πολλές φορές στον όρο ‘πολιτική’ αποδίδεται η έννοια των γενικευμένων απαιτήσεων, στις οποίες θα πρέπει να ανταποκρίνεται η δράση και οι επιλογές των ανθρώπων τους οποίους αφορά η πολιτική.

Για τη σχεδίαση της πολιτικής ασφαλείας απαιτείται η ικανοποίηση των παρακάτω προϋποθέσεων :

- Πολιτική εξασφάλισης (security policy): Πρέπει να υπάρχει μια σαφής δέσμη βασικών αρχών, η οποία περιλαμβάνει τους στόχους των σχεδιαστών του Λ.Σ.

• Ταυτοποίηση (identification): Κάθε αντικείμενο του συστήματος πρέπει να μπορεί να αναγνωρισθεί θετικά.

• Σήμανση (marking): Κάθε αντικείμενο του συστήματος πρέπει να συνοδεύεται από μια ένδειξη του βαθμού εμπιστευτικότητας του.

• Ελεγκτικότητα (accountability): Το σύστημα πρέπει να καταγράφει όλες τις ενέργειες που αφορούν ή μπορούν να επηρεάσουν την ασφάλεια του.

• Διαβεβαίωση (assurance): Το σύστημα πρέπει να παρέχει τεχνικές ρυθμίσεις για την υλοποίηση της πολιτικής εξασφάλισής του, οι οποίες να μπορούν να εκτιμηθούν ως προς την αποτελεσματικότητά τους.

• Συνεχής προστασία (continuous protection): Οι τεχνικές εξασφάλισης του Λ.Σ. πρέπει να προστατεύονται από κάθε ανεπιθύμητη μετατροπή.

Επίσης, θα πρέπει να πληροί τις παρακάτω ιδιότητες:

• Ευχρηστία (Usability). Το σύστημα πρέπει να είναι σχεδιασμένο με στόχο την διευκόλυνση του χρήστη.

• Γενικότητα (Generality). Το σύστημα πρέπει να μπορεί να εκτελέσει ποικίλες διαδικασίες, σύμφωνα με τις ανάγκες του χρήστη.

• Αποδοτικότητα (Effeciency). Το σύστημα πρέπει να λειτουργεί γρήγορα και ορθά, χρησιμοποιώντας κατά βέλτιστο τρόπο τους διατιθέμενους πόρους.

• Ευελιξία (Flexibility). Το σύστημα πρέπει να μπορεί να προσαρμόζεται σε διαρκώς μεταβαλλόμενες καταστάσεις

• Αδιαφάνεια (Opacity). Ο χρήστης πρέπει να γνωρίζει μόνο ότι είναι απαραίτητο για να διεκπεραιώσει την εργασία του .

• Ασφάλεια (Security). Το σύστημα πρέπει να διαφυλάσσει τα δεδομένα ενός χρήστη από μη εξουσιοδοτημένη χρήση τους από άλλους.

• Ακεραιότητα (Integrity). Οι χρήστες και τα δεδομένα τους πρέπει να διαφυλάσσονται από απρόβλεπτες μετατροπές από μη εξουσιοδοτημένους χρήστες.

• Ευκινησία (Capacity). Οι χρήστες δεν πρέπει να υφίστανται άσκοπους περιορισμούς στις ενέργειές τους.

• Αξιοπιστία (Reliability). Τα συστήματα πρέπει να λειτουργούν σωστά, για όσο το δυνατόν μεγαλύτερο χρονικό διάστημα.

• Συντηρησιμότητα (Serviceability). Πιθανά προβλήματα στη λειτουργία του συστήματος πρέπει να μπορούν να ξεπεραστούν εύκολα και γρήγορα.

• Επεκτασιμότητα (Extentability). Το σύστημα πρέπει να μπορεί να αναβαθμισθεί εύκολα, με επέκταση των δυνατοτήτων που διαθέτει.

• Διαθεσιμότητα (Availability). Το σύστημα πρέπει να εξυπηρετεί τους χρήστες όσο το δυνατόν πληρέστερα.

8.2 Πολιτική Ασφάλειας της Εταιρείας Vidavo

Για τον ορθό σχεδιασμό της πολιτικης ασφαλείας που θα ακολουθήσει η εταιρεία θα πρέπει να τηρούνται όλοι οι παραπάνω κανόνες, έτσι ώστε να προσφέρεται μέγιστη ασφάλεια στα συστήματα της και στα δεδομένα που αυτή χειρίζεται. Οι κυριότεροι άξονες για την ανάπτυξη της πολιτικης ασφαλείας και των αντίστοιχων αντίμετρων είναι οι εξής:

• Ζητήματα Προσωπικού (Personnel Security).

• Φυσική Ασφάλεια.

• Ελεγχος πρόσβασης.

• Διαχείριση Υλικού Λογισμικού. Οδηγίες σχετικά με την προμήθεια και συντήρηση υλικού και την ανάπτυξη και συντήρηση του λογισμικού.

• Συμμόρφωση με νομικές υποχρεώσεις.

• Διαδικασίες διαχείρισης Πολιτικης ασφάλειας

• Οργανωτική δομή

• Σχέδιο Έκτακτης ανάγκης.

Ακολουθεί ανάλυση των αξόνων ανάπτυξης της πολιτικής ασφαλείας των συστημάτων της εταιρείας καθώς και εκτενέστερη περιγραφή των μέτρων υλοποίησης της πολιτικης που αυτή ακολουθεί.

Η Εταιρεία Τηλεματικής Vidavo λόγω του ότι διαχειρίζεται ευαίσθητα δεδομένα δίνει υψηλή προτεραιότητα στην Ασφάλεια του Πληροφοριακού της Συστήματος. Τα δεδομένα του πληροφοριακού συστήματος, ανεξάρτητα από τον τρόπο δημιουργίας, μετάδοσης ή αποθήκευσής τους, και ανεξάρτητα από τη μορφή στην οποία βρίσκονται, καθώς και το σύνολο του υλικού εξοπλισμού και του λογισμικού που χρησιμοποιείται για την επεξεργασία τους, αποτελούν αναγκαίους πόρους για τη λειτουργία της Εταιρείας. Η παραβίαση της ασφάλειας του ΠΣ της Εταιρείας μπορεί να έχει πολλές επιπτώσεις, όπως η μείωση του μεριδίου αγοράς και η απώλεια της καλής της φήμης.

Η παρούσα Πολιτική Ασφάλειας αφορά στο σύνολο των πληροφοριών που συλλέγονται και τυγχάνουν επεξεργασίας στο πλαίσιο του πληροφοριακού συστήματος της Εταιρείας Vidavo, καθώς και στον υλικό εξοπλισμό, στο λογισμικό και στις διαδικασίες που χρησιμοποιούνται για την επεξεργασία αυτών των πληροφοριών.

Η Πολιτική Ασφάλειας έχει καθολική εφαρμογή από όλα τα μέλη της εταιρείας Vidavo, που επεξεργάζονται τέτοιες πληροφορίες. Όλοι οι υπάλληλοι της Εταιρείας είναι υπεύθυνοι για την ασφάλεια των ΠΣ, δηλαδή την προστασία των πληροφοριών από πιθανή απώλεια της ακεραιότητας, της διαθεσιμότητας ή της εμπιστευτικότητας τους.

Για την υλοποίηση της Πολιτικής Ασφάλειας αναπτύσσεται και διατηρείται επίκαιρο ένα Σχέδιο Ασφάλειας, το οποίο περιλαμβάνει τα μέτρα και τις διαδικασίες προστασίας που πρέπει να λαμβάνονται για τη διασφάλιση του πληροφοριακού συστήματος.

1. Ζητήματα προσωπικού

Η Εταιρεία Vidavo παρέχει επαρκή και κατάλληλη εκπαίδευση σε θέματα ασφάλειας, στο προσωπικό που αξιοποιεί ή διαχειρίζεται το πληροφοριακό σύστημα, ανάλογα με το ρόλο που κάθε υπάλληλος διαδραματίζει στη λειτουργία του συστήματος.

Οι υπάλληλοι της Εταιρείας υποχρεούνται να μην εκθέτουν, με τις ενέργειες ή τις παραλείψεις τους, σε κινδύνους το πληροφοριακό σύστημα και να συμβάλλουν στην αντιμετώπιση των σχετικών κινδύνων. Υποχρεούνται επίσης να προστατεύουν τα συνθηματικά τους και να μην τα αποκαλύπτουν σε κανέναν, να μη χρησιμοποιούν αναξιόπιστο λογισμικό που λαμβάνουν με το ηλεκτρονικό ταχυδρομείο ή που αποκτούν από το διαδίκτυο, και να μην χρησιμοποιούν πειρατικό ή άλλο παράνομο λογισμικό.

Κάθε μέλος του προσωπικού της Εταιρείας, καθώς και κάθε άλλος εμπλεκόμενος στη λειτουργία του πληροφοριακού συστήματος, οφείλει να αναφέρει οποιαδήποτε περίπτωση παραβίασης της Πολιτικής Ασφάλειας υποπίπτει στην αντίληψη του, καθώς και κάθε άλλο γεγονός που κρίνει ότι θέτει σε κίνδυνο την ασφάλεια του πληροφοριακού συστήματος.

Η Εταιρεία επιλέγει, σε θέσεις που είναι σημαντικές για την ασφαλή λειτουργία του πληροφοριακού της συστήματος, προσωπικό με κατάλληλα τυπικά και ουσιαστικά προσόντα.

2. Φυσική Ασφάλεια

Η εταιρεία Vidavo λαμβάνει μέτρα για την ασφάλεια των εγκαταστάσεων στις οποίες στεγάζονται λειτουργίες του πληροφοριακού συστήματος, ώστε να είναι κατάλληλα οργανωμένες για το σκοπό αυτό.

3. Έλεγχος Πρόσβασης στο Πληροφοριακό Σύστημα

Οι υπάλληλοι της Εταιρείας έχουν πρόσβαση σε εκείνες τις πληροφορίες και υπηρεσίες του ΠΣ, οι οποίες κρίνονται απαραίτητες για την εκτέλεση των εργασιών και αρμοδιοτήτων που τους έχουν ανατεθεί.

4. Διαχείριση Υλικού και Λογισμικού

Κάθε σύστημα, υποσύστημα ή εφαρμογή που αναπτύσσεται από ή για λογαριασμό της εταιρείας και εντάσσεται στο πληροφοριακό της σύστημα ή επικοινωνεί άμεσα με αυτό, πρέπει να εγγυάται ένα επαρκές επίπεδο ασφάλειας.

Κατά την ανάθεση εργασιών συντήρησης ή ανάπτυξης συστημάτων, υποσυστημάτων ή εφαρμογών, που εντάσσονται στο πληροφοριακό σύστημα της εταιρείας Vidavo ή επικοινωνούν άμεσα με αυτό, σε αναδόχους λαμβάνεται μέριμνα τήρησης της παρούσας Πολιτικής Ασφάλειας και των κανόνων που απορρέουν από αυτήν.

5. Συμμόρφωση με νομικές υποχρεώσεις

Η Εταιρεία Vidavo προβαίνει σε όλες τις ενέργειες που απαιτούνται για να γίνεται σεβαστή η νομοθεσία που αφορά τα πνευματικά δικαιώματα, την προστασία

προσωπικών δεδομένων, το ηλεκτρονικό έγκλημα και γενικά τη νομοθεσία που αφορά τη χρήση υπολογιστικών και επικοινωνιακών συστημάτων.

6. Διαδικασίες Διαχείρισης της Πολιτικής Ασφάλειας

Η Πολιτική Ασφάλειας πρέπει να τηρείται κατά το δυνατόν επίκαιρη. Ο ορισμός του κατάλληλου προσώπου που είναι αρμόδιο για την εξασφάλιση της επικαιρότητάς της και τη διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη της Διοίκησης της Εταιρείας Vidavo.

Η εφαρμογή της Πολιτικής Ασφάλειας και των κανόνων που απορρέουν από αυτήν είναι υποχρεωτική για όλους τους εμπλεκόμενους στη λειτουργία του πληροφοριακού συστήματος. Είναι ευθύνη της Εταιρείας να εξασφαλίσει ότι κάθε εργαζόμενος που εμπλέκεται, κατά την εκτέλεση της εργασίας του, στη λειτουργία του πληροφοριακού συστήματος, είναι ενήμερος τόσο για την Πολιτική Ασφάλειας, όσο και για τη χρησιμότητα και τον τρόπο εφαρμογής της.

Περιοδικές επιθεωρήσεις από εσωτερικούς ελεγκτές θα λαμβάνουν χώρα με σκοπό την διασφάλιση της συμμόρφωσης με την Πολιτική Ασφάλειας. Η Εταιρεία διατηρεί το δικαίωμα να επιβάλλει κυρώσεις σε περιπτώσεις παραβίασής της.

7. Οργανωτική Δομή

Η Διοίκηση της εταιρείας ορίζει τους ρόλους που είναι απαραίτητοι για τη διαχείριση της ασφάλειας του πληροφοριακού συστήματος, τις αρμοδιότητες που αντιστοιχούν σε κάθε ρόλο και αναθέτει τους ρόλους αυτούς σε συγκεκριμένα πρόσωπα.

8. Σχέδιο Συνέχισης Λειτουργίας

Για την εξασφάλιση της συνέχειας της λειτουργίας του πληροφοριακού συστήματος, έπειτα από ενδεχόμενη καταστροφή, εφαρμόζεται Σχέδιο Συνέχισης Λειτουργίας, το οποίο περιγράφεται αναλυτικά στο αντίστοιχο έγγραφο.

8.2 Μέτρα Υλοποίησης Πολιτικής Ασφαλείας

Τα μέτρα υλοποίησης της Πολιτικής Ασφαλείας των ΠΣ μπορούν να κατηγοριοποιηθούν ανάλογα με τον στόχο προστασίας τους σε μέτρα για την

- Προστασία Χώρων και υποδομών
- Προστασία Πληροφοριακών Συστημάτων
- Προστασία Δεδομένων
- Προστασία Δικτύων

8.2.1 Προστασία Χώρων και Υποδομών

Η προστασία των χώρων και των υποδομών αναφέρεται στα μέτρα που υποστηρίζουν τη φυσική ασφάλεια και έχουν ως κύριο στόχο την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στους χώρους όπου είναι εγκατεστημένα τα πληροφοριακά συστήματα και της καταστροφής των αγαθών τους. Αφορά κυρίως τον Έλεγχο φυσικής πρόσβασης σε κρίσιμους χώρους όπως το Computer Room και στην Προστασία της υγείας των χρηστών των πληροφοριακών συστημάτων (safety).

Όσον αφόρα τους κρίσιμους χώρους της εταιρείας, η πρόσβαση εξαρτάται από τους ρόλους και τις δραστηριότητες του προσωπικού της εταιρείας. Με στόχο την αποφυγή και την προφύλαξη των συστημάτων και των δεδομένων της εταιρείας από κλοπή έχει εγκατασταθεί αντικλεπτικό σύστημα συναγερμού.

Η αντιμετώπιση φυσικών απειλών όπως οι πυρκαγιές, οι πλημμύρες, οι σεισμοί κ.α., που είναι σημαντικές απειλές και για τους ίδιους τους χρήστες των συστημάτων, εξαρτάται και από τον σχεδιασμό του κτιρίου ή του χώρου όπου είναι εγκατεστημένα τα συστήματα. Επίσης, η φυσική ασφάλεια των συστημάτων σχετίζεται άμεσα και με την κατάλληλη εκπαίδευση του προσωπικού και των κατάλληλων μηχανισμών προστασίας, όπως συσκευών πυρόσβεσης.

Απαραίτητη επίσης είναι η συστηματική συντήρηση των ηλεκτρικών εγκαταστάσεων καθώς χρήσιμη είναι η ύπαρξη μιας γεννήτριας παροχής ηλεκτρικής ενέργειας ή συστήματος αδιάλειπτης παροχής τάσεως (UPS), για να αποφεύγονται πιθανές απώλειες του λογισμικού και να υποστηρίζεται η καλή λειτουργία του

μηχανολογικού εξοπλισμού κατά την πτώση της τάσης του ρεύματος ή διακοπής της παροχής του ηλεκτρικού ρεύματος.

8.2.2 Προστασία Πληροφοριακών Συστημάτων

8.2.2.1 Έλεγχος Πρόσβασης

Βασική προϋπόθεση στην ασφάλεια των συστημάτων της εταιρείας είναι ο έλεγχος πρόσβασης στα συστήματα της τόσο από φυσική άποψη στο υλικό κομμάτι, φυλάσσοντας και προστατεύοντας τους servers της και τα υπόλοιπα υπολογιστικά συστήματα σε ασφαλείς χώρους, εξασφαλίζοντας περιορισμένη και ελεγχόμενη πρόσβαση σε αυτά, όσο και ο έλεγχος πρόσβασης των απομακρυσμένων χρηστών της στις υπηρεσίες της και της εφαρμογές της. Η πρόσβαση θα πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες καθότι απειλές μπορει να δεχτούν τα συστήματα και από εσωτερικούς χρήστες, όχι μόνο από εξωτερικούς. Οι απειλές εκ των έσω μπορεί να είναι η διαρροή ευαίσθητων πληροφοριών, κρούσματα ιών, απάτες από κακόβουλους χρήστε κ.α τα οποία χρήζουν αντίστοιχης αντιμετώπισης. Για αυτό απαραίτητη προϋπόθεση για ολοκληρωμένη ασφάλεια είναι και η προστασία από εσωτερικές απειλές.

Η πρόσβαση θα επιτρέπεται μόνο μέσω διαδικασιών αυθεντικοποίησης και ταυτοποίησης. Η έξυπνη κάρτα (smart card) είναι μια κάρτα. που ενσωματώνει ένα μικροεπεξεργαστή, ο οποίος βρίσκεται κάτω από μια επαφή από χρυσό, προσαρμοσμένο στη μια πλευρά της. Τα δεδομένα στην έξυπνη κάρτα δεν είναι εύκολο να παραλλαχθούν ή και να διαγραφούν, γιατί ο μικροεπεξεργαστής της δεν περιέχει δεδομένα για το χρήστη. Ο μικροεπεξεργαστής της κάρτας και ο υπολογιστής, με τον οποίο συνδέεται, επικοινωνούν πριν ο μικροεπεξεργαστής επιτρέψει την πρόσβαση στα δεδομένα που περιέχονται στη μνήμη της κάρτας. Με τον τρόπο αυτό αποτρέπεται η παραχάραξη των δεδομένων κι έτσι ο χρήστης διασφαλίζεται, αν η κάρτα του βρεθεί σε διαφορετικά από τα δικά του χέρια.

Η τροφοδοσία της κάρτας με ενέργεια εξασφαλίζεται από τον αναγνώστη έξυπνης κάρτας (smart card reader), στον οποίο εισάγεται η κάρτα προκειμένου να χρησιμοποιηθεί. Αυτός μπορεί να επικοινωνήσει με κάποιο κεντρικό υπολογιστή, όπου υπάρχουν τα στοιχεία του χρήστη, προκειμένου να εξασφαλιστεί η πρόσβαση σε δεδομένα.

8.2.2.2 Έλεγχος Προσπέλασης

Απαραίτητη προϋπόθεση ασφαλής λειτουργίας των πληροφοριακών συστημάτων είναι ο έλεγχος. Από τη στιγμή που έχει διακριβωθεί η ταυτότητα ενός χρήστη μέσω του έλεγχου πρόσβασης, το σύστημα θα πρέπει να φροντίζει έτσι ώστε ο χρήστης αυτός να μπορεί να ενεργήσει μόνο στα πλαίσια των κανόνων που καθορίζονται από την πολιτική ασφάλειας. Αυτό επιτυγχάνεται εφαρμόζοντας ελέγχους προσπέλασης. Σχετικά με τους ελέγχους προσπέλασης ισχύουν οι ακόλουθες έννοιες:

- *Υποκείμενα.* Πρόκειται για τις ενεργές οντότητες στο σύστημα (χρήστες, διεργασίες, υπηρεσίες)

- *Αντικείμενα.* Με τον όρο αυτό περιγράφονται οι πόροι ή οι παθητικές οντότητες στο σύστημα (αρχεία, συσκευές, προγράμματα)

- *Τρόπος προσπέλασης.* Ο όρος αυτός αναφέρεται στην ενέργεια που πραγματοποιεί ένα υποκείμενο σε ένα αντικείμενο π.χ. ανάγνωση, εγγραφή, εκτέλεση, αναφορά ιδιοχαρακτηριστικών.

Ο έλεγχος προσπέλασης συνίσταται στην εξέταση αν το υποκείμενο έχει δικαίωμα για τον συγκεκριμένο τρόπο προσπέλασης στο αντικείμενο, και στην απαγόρευση της ενέργειας, αν τελικά δεν υπάρχει το σχετικό δικαίωμα. Η επιλογή της πολίτικης έλεγχου προσπέλασης εξαρτάται από τα επιμέρους χαρακτηριστικά του περιβάλλοντος που πρόκειται να προστατευτεί

Οι τρεις βασικές προσεγγίσεις ελέγχου προσπέλασης είναι οι εξής:

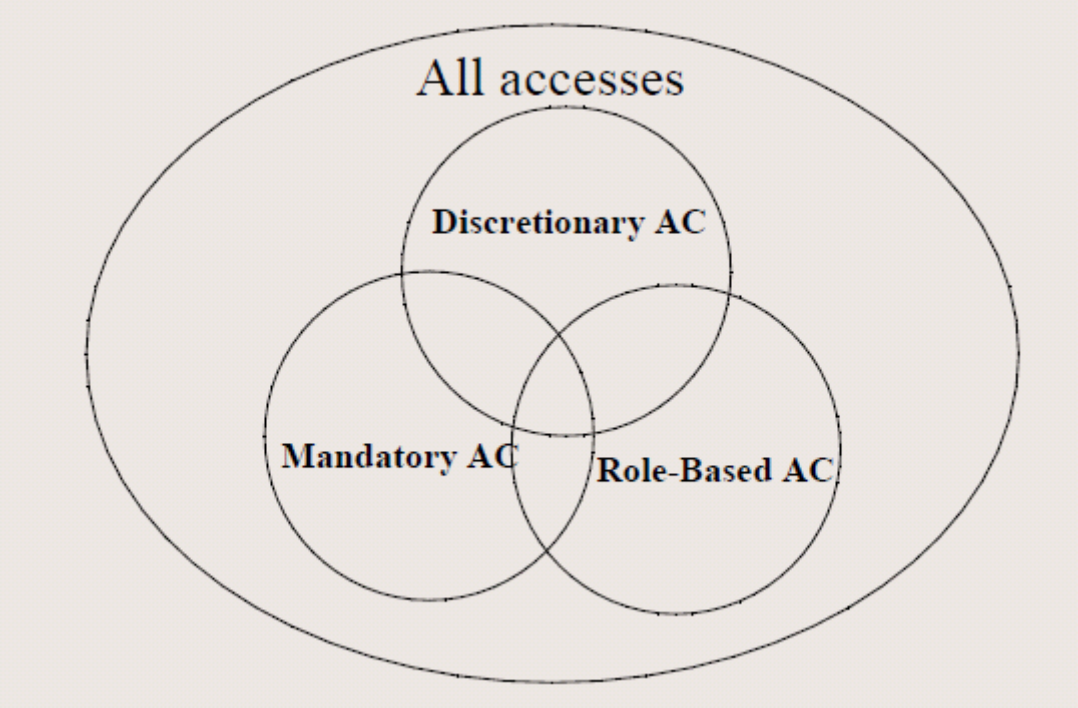
• *Η κατά-διάκριση (Discretionary Access Control - DAC)*. Μια αρκετά διαδεδομένη προσέγγιση κυρίως σε στρατιωτικούς οργανισμούς, από όπου και προέρχεται, είναι η υποχρεωτική (mandatory) προσέγγιση. Σύμφωνα με αυτή την προσέγγιση, επιτρεπτές είναι μόνο οι ενέργειες που προβλέπονται και προδιαγράφονται στην πολιτική ασφάλειας. Οτιδήποτε δεν περιλαμβάνεται στην πολιτική ασφάλειας απαγορεύεται, ανεξάρτητα από τις συνθήκες ή τις συνέπειες που η απαγόρευση αυτή μπορεί να επιφέρει. Η προσέγγιση αυτή είναι αρκετά δημοφιλής στην ανάπτυξη πολιτικών ασφάλειας πληροφοριακών συστημάτων, παρόλο που οι πολιτικές ασφάλειας που την ακολουθούν συχνά αποδεικνύονται άκαμπτες και αναποτελεσματικές. Είναι προφανές ότι οι προδιαγραφές και οδηγίες ασφάλειας δε μπορούν να είναι τόσο λεπτομερείς, ούτε τέτοιες που να μπορούν να καλύψουν το σύνολο των δυνατών περιπτώσεων που απαιτείται κάποια ενέργεια από τους χρήστες του πληροφοριακού συστήματος. Ειδικά σε δυναμικά περιβάλλοντα με συχνές

αλλαγές, η προσέγγιση αυτή είναι λιγότερο αποτελεσματική από τις άλλες προσεγγίσεις [24].

• *Η κατά-απαίτηση (Mandatory Access Control - MAC).* Για τις πολιτικές ασφάλειας που διαμορφώνονται με βάση την προσέγγιση διακριτού (discretionary) ελέγχου, όλες οι ενέργειες που δεν περιλαμβάνονται στις απαγορευμένες θεωρούνται επιτρεπτές και σύμφωνες με την πολιτική. Έτσι, στην περίπτωση που απαιτείται κάποια ενέργεια η οποία δεν περιλαμβάνεται στην πολιτική ασφάλειας, θεωρείται ότι ο χρήστης θα δράσει με τρόπο που συμβαδίζει με τους στόχους της πολιτικής ασφάλειας. Η προσέγγιση αυτή, είναι ευκολότερα να γίνει αποδεκτή από τους χρήστες των πληροφοριακών συστημάτων που καλούνται να εφαρμόσουν την πολιτική ασφάλειας, διότι είναι αντίστοιχη με τον τρόπο που ισχύει η νομοθεσία ενός κράτους: οι πολίτες γνωρίζουν ότι οι ενέργειες τους θεωρούνται νόμιμες, εκτός αν ανήκουν σε αυτές που απαγορεύονται. Το προτέρημα της προσέγγισης αυτής έναντι των υπολοίπων είναι η μεγαλύτερη αποδοχή των πολιτικών ασφάλειας από τους χρήστες των πληροφοριακών συστημάτων. Από την άλλη πλευρά, η μεγάλη ευελιξία των πολιτικών αυτών μπορεί να οδηγήσει σε μείωση του επιπέδου ασφάλειας, αυξάνοντας την επικινδυνότητα.

• Η βασισμένη-*σε-ρόλους (Role-Based Access Control).* Σύμφωνα με την προσέγγιση αυτή, οι οδηγίες ασφάλειας που προδιαγράφονται στην πολιτική εφαρμόζονται, μπορούν και να παρακαμφθούν όμως όταν υπάρχουν αντικρουόμενες απαιτήσεις. Επίσης οι πολιτικές αυτές μπορεί να παρακαμφθούν και στην περίπτωση που τα προσδοκώμενα οφέλη από τη μη τήρηση των οδηγιών αυτών (εξαιρουμένου του προσωπικού-ατομικού οφέλους) υπερτερούν των οφελών που θα προκύψουν από την εφαρμογή των οδηγιών της πολιτικής ασφάλειας, σε όρους επιχειρηματικών στόχων και στόχων ασφάλειας. Τα πλεονεκτήματα αυτής της προσέγγισης γίνονται περισσότερο φανερά σε ειδικές περιπτώσεις που δε θα μπορούσαν να έχουν προβλεφθεί και συμπεριληφθεί στις οδηγίες μιας πολιτικής ασφάλειας. Στις περιπτώσεις αυτές, η δράση των χρηστών είναι πιο ευέλικτη, σε σχέση με τις άλλες προσεγγίσεις. Το μειονέκτημα της 'κατά περίπτωση' πολιτικής ασφάλειας συνδέεται με τη δυνατότητα παράκαμψης της πολιτικής κατά την κρίση των χρηστών του πληροφοριακού συστήματος. Η δυνατότητα επιλογής για τη συμμόρφωση ή μη με την πολιτική ασφάλειας σε σχέση με τα αναμενόμενα οφέλη από την εφαρμογή της πολιτικής εισάγει το στοιχείο της υποκειμενικότητας, καθώς εναπόκειται στους χρήστες του πληροφοριακού συστήματος να αξιολογήσουν και να κρίνουν τις πιθανές συνέπειες και τα πιθανά οφέλη από την εφαρμογή των οδηγιών ασφάλειας [24].

Οι δυο πρώτες κατηγορίες χαρακτηρίζονται ως κλασσικές, καθώς έχουν αναγνωρίσει και εφαρμοστεί από τους ερευνητές και επαγγελματίες ασφάλειας για πολύ καιρό. Τα τελευταία χρόνια κατά γενική ομολογία υπάρχουν μοντέλα έλεγχου προσπέλασης που έχουν τα χαρακτηριστικά και των δυο προσεγγίσεων όπως τα βασισμένα σε ρόλους μοντέλα., τα οποία έχουν μονοπωλήσει τα τελευταία χρόνια το ενδιαφέρον των ερευνητών.



Εικόνα 17. Έλεγχοι Προσπέλασης.

8.2.3 Προστασία Βάσεων Δεδομένων

Όσον αφορά την ασφάλεια βάσεων δεδομένων, θα πρέπει να λαμβάνεται υπ' όψιν ότι η βάση δεδομένων είναι ένα σύστημα που εκτελείται σε έναν υπολογιστή, πάνω από ένα λειτουργικό σύστημα, και έτσι επηρεάζεται άμεσα από τους μηχανισμούς ασφάλειας που παρέχει ο συνδυασμός αυτός υλικού/λογισμικού. Αν για παράδειγμα το λειτουργικό σύστημα δεν παρέχει επαρκείς μηχανισμούς διακρίβωσης ταυτότητας, η βάση δεδομένων θα πρέπει να υλοποιήσει δικούς της. Επίσης, αν η βάση δεδομένων αποθηκεύεται σε αρχεία που δεν προστατεύονται επαρκώς από το λειτουργικό σύστημα, οι μηχανισμοί ελέγχου πρόσβασης που υλοποιούνται από τη βάση δεδομένων μπορούν να παρακαμφθούν, απλά διαβάζοντας ή τροποποιώντας τα αρχεία σε επίπεδο λειτουργικού συστήματος.

Βασικοί κανόνες για την προστασία των βάσεων είναι ότι τόσο κατά τη φάση της επεξεργασίας των πληροφοριών όσο και κατά τη φάση της μετάδοσης πρέπει αφενός να εκτελεστούν στο σύνολο τους όλες οι δοσοληψίες και αφετέρου ότι να εφαρμόζονται όλοι οι κανόνες ακεραιότητας που έχουν ορισθεί για τη βάση δεδομένων.

Σε γενικές γραμμές μία βάση δεδομένων θα πρέπει να διαφυλάσσει την εμπιστευτικότητα των πληροφοριών την παρέχοντα πρόσβαση σε εξουσιοδοτημένους χρήστες, την ακεραιότητα των πληροφοριών της καθώς και την διαθεσιμότητα τους.

Η εμπιστευτικότητα των πληροφοριών επιτυγχάνεται με τον έλεγχο πρόσβασης στις ΒΔ, ώστε να διαπιστώνεται αν ένας χρήστης έχει το δικαίωμα να χρησιμοποιήσει το σύστημα βάσεων δεδομένων ή όχι. Για διακρίβωση της ταυτότητας των χρηστών διατίθενται οι παρακάτω τεχνικές:

(α) Διακρίβωση ταυτότητας με όνομα χρήστη-συνθηματικό.

Η βάση δεδομένων διαθέτει κατάλογο με τις έγκυρες αντιστοιχίες ονομάτων χρηστών και συνθηματικών ώστε να αποφασίζει για το αν τα παρουσιασθέντα διαπιστευτήρια είναι έγκυρα. Η τεχνική αυτή είναι χρήσιμη όταν το λειτουργικό σύστημα δεν παρέχει αξιόπιστους μηχανισμούς διακρίβωσης ταυτότητας των χρηστών ή όταν πραγματοποιούνται συνδέσεις μέσω δικτύου στη βάση δεδομένων, οπότε η ταυτότητα του χρήστη στο λειτουργικό σύστημα δεν είναι διαθέσιμη ή αξιόπιστη.

(β) Διακρίβωση ταυτότητας από το λειτουργικό σύστημα.

Σ’ αυτή την περίπτωση η πρόσβαση στην ΒΔ στηρίζεται στους μηχανισμούς του λειτουργικού συστήματος για την διακρίβωση ταυτότητας. Από τη στιγμή που ένας χρήστης έχει αναγνωριστεί από το λειτουργικό σύστημα και ο χρήστης λειτουργικού συστήματος είναι εξουσιοδοτημένος να χρησιμοποιεί τη βάση δεδομένων, δεν ζητάται κανένα πρόσθετο στοιχείο για την προσπέλαση του χρήστη στη βάση δεδομένων. Η τεχνική αυτή δεν μπορεί να χρησιμοποιείται ως αποκλειστικός μηχανισμός διακρίβωσης ταυτότητας σε συστήματα όπου επιτρέπεται δικτυακή πρόσβαση στη βάση δεδομένων, καθώς χρειάζεται κάθε χρήστης να έχει λογαριασμό στο λειτουργικό σύστημα. Επίσης, πρέπει να χρησιμοποιείται μόνον όταν το λειτουργικό σύστημα έχει επαρκώς αξιόπιστους μηχανισμούς διακρίβωσης ταυτότητας.

(γ) Διακρίβωση ταυτότητας μέσω καθολικών υπηρεσιών καταλόγου.

Ο χρήστης εισάγει ένα όνομα και ένα συνθηματικό και για διακρίβωση του το σύστημα διασυνδέεται με καθολικές υπηρεσίες καταλόγου. Η προσέγγιση αυτή έχει το πλεονέκτημα ότι προωθεί τη χρήση κεντρικού σημείου φύλαξης των διαπιστευτηρίων σύνδεσης. Έχοντας ένα κεντρικό σημείο φύλαξης, είναι δυνατόν όλες οι ενότητες λογισμικού που απαιτούν πιστοποίηση (λειτουργικό σύστημα, βάση δεδομένων κ.λπ.) να συνδιαλέγονται με το σημείο αυτό, ούτως ώστε κάθε χρησιμοποιεί ένα μόνο ζεύγος διαπιστευτηρίων για προσπέλαση σε όλους τους πόρους.

Η ακεραιότητα των δεδομένων στα συστήματα βάσεων δεδομένων αποτελεί βασική προϋπόθεση για αυτό και τα δεδομένα πρέπει να διασώζονται σε περιπτώσεις βλαβών υλικού και δυσλειτουργιών του λογισμικού, οι τροποποιήσεις πρέπει να γίνονται μόνο από εξουσιοδοτημένους χρήστες και κάθε φορά να επιστρέφονται τα δεδομένα που έχουν αποθηκευτεί. Σε περίπτωση παραβίασης της ακεραιότητας, οι ενδιαφερόμενοι χρήστες πρέπει τουλάχιστον να ειδοποιούνται.

Η φυσική ακεραιότητα της βάσης δεδομένων συσχετίζεται με τη φθορά που μπορούν να υποστούν τα μαγνητικά μέσα αποθήκευσης από διακοπές ρεύματος, βλάβες κυκλωμάτων ή φυσιολογική φθορά. Το σύστημα θα πρέπει να παρέχει μηχανισμούς ανάκαμψης από το σφάλμα και ανάκτησης των δεδομένων. Ένα τρόπος διαφύλαξης της φυσικής ακεραιότητας είναι η τήρηση εφεδρικών αντιγράφων. Για τα εφεδρικά αντίγραφα είναι σημαντικό να μπορούν να λαμβάνονται ενόσω η βάση δεδομένων βρίσκεται εν λειτουργία.

Υπάρχουν δύο είδη εφεδρικών αντιγράφων βάσεων δεδομένων:

• Τα φυσικά αντίγραφα αποτυπώνουν τα περιεχόμενα των δίσκων, όπως ακριβώς τα αποθηκεύει η βάση δεδομένων, χωρίς να ενδιαφέρονται για τη λογική τους δομή, λαμβάνονται σε μικρότερο χρόνο και αποκαθίστανται ταχύτερα. Συνήθως όμως απαιτούν να διακόπτεται η λειτουργία της βάσης δεδομένων κατά τη λήψη τους και είναι πιθανόν να λειτουργούν μόνο σε σύστημα «όμοιο» με αυτό από το οποίο ελήφθησαν.

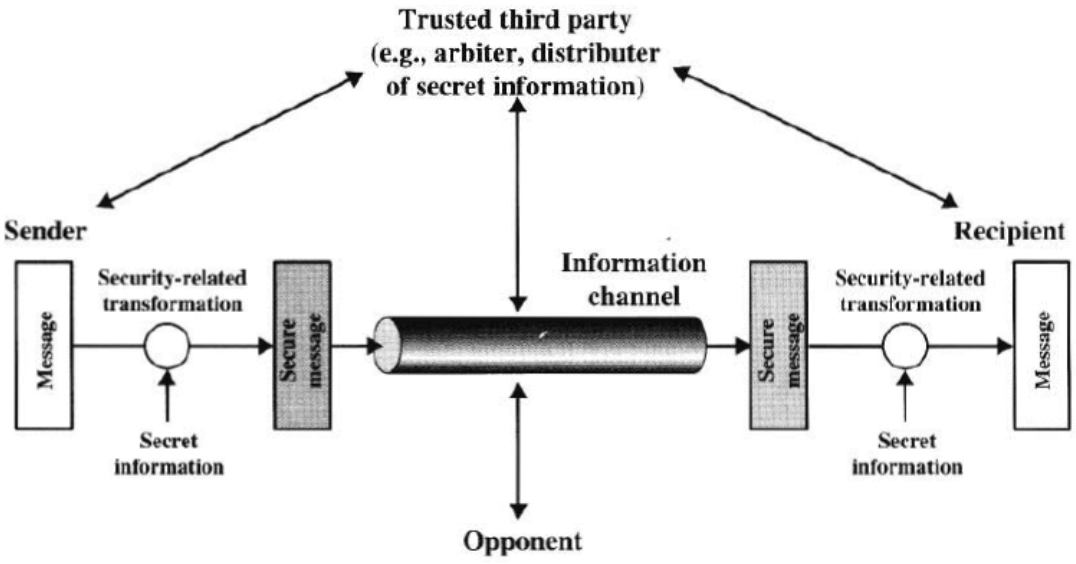
• Τα λογικά αντίγραφα αποτυπώνουν τα δεδομένα της βάσης σε μορφή που αντικατοπτρίζει τη λογική τους δομή, χωρίς να αποτυπώνουν τον επακριβή τρόπο αποθήκευσης των δεδομένων στους δίσκους, απαιτούν περισσότερο χρόνο για να ληφθούν και η αποκατάστασή τους διαρκεί περισσότερο. Μπορούν να λαμβάνονται

κατά την διάρκεια λειτουργίας της βάσης δεδομένων και μπορούν να λειτουργήσουν και σε συστήματα «ανόμοια» προς αυτό από το οποίο ελήφθησαν.

Τέλος, η διαθεσιμότητα των πληροφοριών επίσης μία σημαντική διάσταση που ορίζει ότι τα δεδομένα πρέπει να είναι πάντα διαθέσιμα στους εξουσιοδοτημένους χρήστες. Για το λόγο αυτό σε τακτά χρονικά σημεία, πρέπει να διενεργούνται στη βάση δεδομένων έλεγχοι ορθότητας (audits) για εντοπισμό πιθανών προβλημάτων. Οι έλεγχοι αυτοί πρέπει να είναι κατά το δυνατόν λεπτομερείς και διεξοδικοί χωρίς να επηρεάζεται την απόδοση του συστήματος.

8.2.4 Προστασία Δικτύων Υπολογιστικών Συστημάτων

Βασική προϋπόθεση για ορθή υλοποίηση της πολιτικής ασφαλείας μιας εταιρείας είναι ότι θα πρέπει να διασφαλίζει την ασφάλεια των δικτύων των υπολογιστικών συστημάτων της εταιρείας. Τα δίκτυα της εταιρείας συνίσταται από τη διασύνδεση δυο ή περισσοτέρων υπολογιστικών συστημάτων κατά τρόπο ώστε να παρέχεται η δυνατότητα στους χρήστες να επωφελούνται από ολόκληρο το υπολογιστικό δυναμικό. Αυτό πραγματοποιείται μέσω της ανταλλαγής πληροφοριών μεταξύ των χρηστών και της κοινής χρήσης των διαθέσιμων υπολογιστικών πόρων. Για αυτό το λόγο η εταιρεία πρέπει να προνοεί και για την προστασία από απειλές των δικτύων της.



Εικόνα 18. Μοντέλο Ασφάλειας Δικτύου.

Η διασύνδεση ενός εταιρικού δικτύου με το Διαδίκτυο ή άλλα εξωτερικά μη έμπιστα δίκτυα, καθιστά ολόκληρη την εταιρική πληροφορική υποδομή ευάλωτη σε μια σειρά από απειλές που δύναται να προσβάλλουν την ασφάλεια της επιχείρησης. Για αυτό τον λόγο συνίσταται η χρήση πρωτόκολλων για ασφαλή επικοινωνία όπως το HTTPS και SSL.

Η χωρίς προστασία παροχή υπηρεσιών επιτρέπει την εκμετάλλευση πιθανών υπαρκτών αδυναμιών από τρίτους, με σκοπό την παραβίαση της ασφάλειας. Για το λόγο αυτό, κρίνεται απαραίτητη η υλοποίηση εξειδικευμένων μηχανισμών ασφάλειας όπως Firewall, Web Access Systems, Mail Security Systems, Network IPS/IDS.

Η εταιρεία εξασφαλίζει την προστασία των δικτύων της μέσω ενός ολοκληρωμένου πακέτου ασφαλείας το End Point Security System, το οποίο στοχεύει στην υλοποίηση υπηρεσιών ασφάλειας στην πύλη του δικτύου (Gateway Security) από και προς το διαδίκτυο.

Οι βασικές υπηρεσίες είναι:

- Firewall
- Antivirus
- Antisyare
- Antispam
- URL Filtering
- DMZ (De Military Zone)
- Intrusion Detection / Prevention Systems

8.2.4.1 Παραδείγματα Πρωτόκολλων Ασφαλής Επικοινωνίας

Απαραίτητο μέτρο για ασφαλή σύνδεση και ανταλλαγή πληροφοριών ιδίως μέσω διαδικτύου είναι η χρήση και εφαρμογή πρωτόκολλων για ασφαλή επικοινωνία. Τα πρωτόκολλα αυτά παρέχουν επιπλέον ασφάλεια στην διακίνηση πληροφοριών μέσω δικτύων και στηρίζονται κυρίως στη μέθοδο της κρυπτογράφησης.

Πρωτόκολλο HTTPS (Secure HTTP)

Το σύστημα αυτό σχεδιάστηκε αρχικά από την εταιρία Netscape Communications Corporation για να χρησιμοποιηθεί σε sites όπου απαιτείται αυθεντικοποίηση χρηστών και κρυπτογραφημένη επικοινωνία. Σήμερα χρησιμοποιείται ευρέως στο διαδίκτυο όπου χρειάζεται αυξημένη ασφάλεια διότι διακινούνται ευαίσθητες πληροφορίες. Το HTTPS δεν είναι ξεχωριστό πρωτόκολλο όπως μερικοί νομίζουν, αλλά αποτελεί συνδυασμό του απλού HTTP πρωτοκόλλου και των δυνατοτήτων κρυπτογράφησης που παρέχει το πρωτόκολλο Secure Sockets Layer (SSL). Η κρυπτογράφηση που χρησιμοποιείται διασφαλίζει ότι τα κρυπτογραφημένα δεδομένα δεν θα μπορούν να υποκλαπούν από άλλους κακόβουλους χρήστες ή από επιθέσεις man-in-the-middle.

Για να χρησιμοποιηθεί το HTTPS σε έναν εξυπηρετητή (server), θα πρέπει ο διαχειριστής του να εκδώσει ένα πιστοποιητικό δημοσίου κλειδιού. Στην συνέχεια το πιστοποιητικό αυτό θα πρέπει να υπογραφεί από μία αρχή πιστοποίησης (certificate authority), η οποία πιστοποιεί ότι ο εκδότης του πιστοποιητικού είναι νομότυπος και ότι το πιστοποιητικό είναι έγκυρο. Με τον τρόπο αυτό οι χρήστες μπορούν να δουν την υπογραφή της αρχής πιστοποίησης και να βεβαιωθούν ότι το πιστοποιητικό είναι έγκυρο και ότι κανένας κακόβουλος χρήστης δεν το έχει πλαστογραφήσει.

Όπως αναφέρθηκε προηγουμένως, το HTTPS χρησιμοποιείται κυρίως όταν απαιτείται μεταφορά ευαίσθητων προσωπικών δεδομένων. Το επίπεδο προστασίας των δεδομένων εξαρτάται από το πόσο σωστά έχει εφαρμοστεί η διαδικασία ασφάλειας και από το πόσο ισχυροί είναι οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται.

Όσον αφορά την χρήση και τις συναλλαγές μέσω πιστωτικών καρτών, πολλοί χρήστες θεωρούν ότι το HTTPS προστατεύει ολοκληρωτικά τον αριθμό της πιστωτικής τους κάρτας από κατάχρηση, αυτό όμως δεν ισχύει. Το HTTPS χρησιμοποιεί την κρυπτογράφηση για να μεταδώσει τον αριθμό από τον υπολογιστή του πελάτη προς τον εξυπηρετητή. Η μετάδοση είναι ασφαλής και τα δεδομένα φτάνουν στον εξυπηρετητή χωρίς κανείς να μπορέσει να τα υποκλέψει. Παρόλα αυτά υπάρχει το ενδεχόμενο διάφοροι χάκερ να έχουν επιτεθεί στον εξυπηρετητή και από εκεί να έχουν υποκλέψει τα ευαίσθητα προσωπικά δεδομένα.

Πρωτόκολλο SSL (Secure Sockets Layer)

Το πρωτόκολλο SSL 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 την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security), το οποίο πλέον τείνει να αντικαταστήσει το SSL. Τα δύο αυτά πρωτόκολλα

χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου.

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το telnet κοκ.

Το SSL προσφέρει συνοπτικά τις ακόλουθες υπηρεσίες:

(α) Πιστοποίηση του server από τον client.

(β) Πιστοποίηση του client από τον server

(γ) Εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.

Ένα μειονέκτημα της χρήσης του πρωτοκόλλου SSL είναι ότι αυξάνει τα διακινούμενα πακέτα μεταξύ των δύο μηχανών και συνεπώς καθυστερεί την μετάδοση των πληροφοριών επειδή χρησιμοποιεί μεθόδους κρυπτογράφησης και αποκρυπτογράφησης. Ειδικότερα οι διάφορες καθυστερήσεις εντοπίζονται στα εξής σημεία:

Στην αρχική διαδικασία χειραψίας όπου κανονίζονται οι λεπτομέρειες της σύνδεσης και ανταλλάσσονται τα κλειδιά της συνόδου.

Στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης που γίνεται στους δύο υπολογιστές με αποτέλεσμα να δαπανώνται υπολογιστικοί πόροι και χρόνος.

Στην καθυστέρηση μετάδοσης των κρυπτογραφημένων δεδομένων αφού αυτά αποτελούνται από περισσότερα bytes σε σχέση με την αρχική μη κρυπτογραφημένη πληροφορία.

Λόγω αυτών των επιβαρύνσεων που εισάγει το πρωτόκολλο SSL, χρησιμοποιείται πλέον μονάχα σε περιπτώσεις όπου πραγματικά χρειάζεται ασφαλής σύνδεση (πχ μετάδοση κωδικών χρήστη ή αριθμών πιστωτικών καρτών μέσω του διαδικτύου) και όχι σε περιπτώσεις απλής επίσκεψης σε μία ιστοσελίδα.

8.2.4.2 End point Security Systems

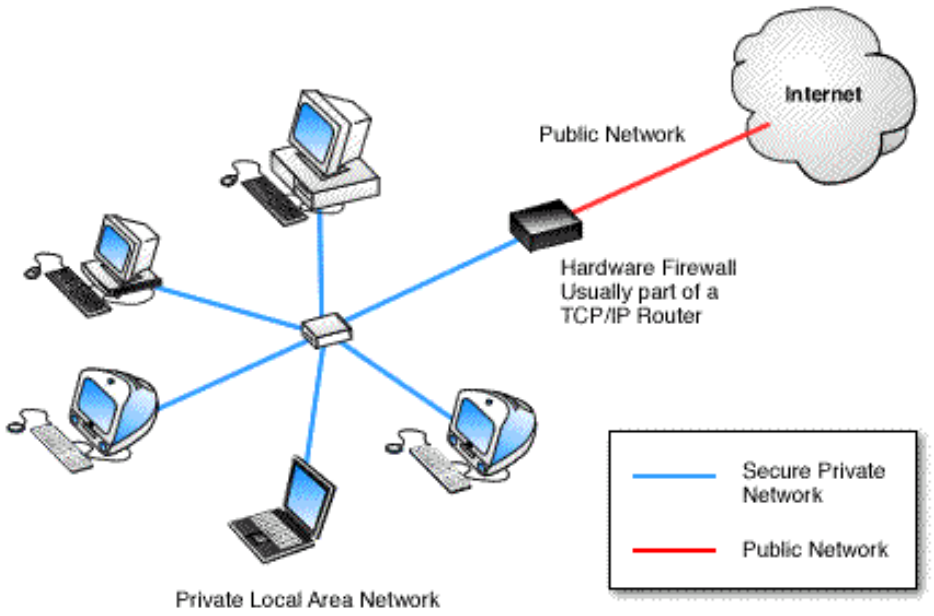
Αποτελεί πολύ βασικό μέτρο για την ασφάλεια των συστημάτων της εταιρείας. Στόχος του πακέτου αυτού είναι να προστατεύει όλους τους υπολογιστές και τα δεδομένα της εταιρείας, να ελέγχει τις εξωτερικές συσκευές και τις εφαρμογές καθώς και την πρόσβαση στο δίκτυο, παρέχοντας στην εταιρεία ασφάλεια και συμβατότητα με τις κανονιστικές ρυθμίσεις και εσωτερικές πολιτικές.

Επίσης ασφαλίζει τους υπολογιστές και τα ευαίσθητα δεδομένα με τεχνολογίες anti-virus, anti-spyware και firewall. Ελαχιστοποιεί τις επιπτώσεις στους υπολογιστές προσφέροντας προστασία δεδομένων και προστασία από ιούς και malware. Ελέγχει αυτόματα τόσο τους υπολογιστές υπό διαχείριση, όσο και τους "άγνωστους" υπολογιστές επισκεπτών για τυχόν μη ενημερωμένα προγράμματα ασφάλειας, πριν αποκτήσουν πρόσβαση στο δίκτυο. Σταματά τους hackers με το ενσωματωμένο client firewall που υποστηρίζει κεντρική διαχείριση και είναι ενσωματωμένο στον anti-virus agent. Και γενικότερα βοηθά στην αύξηση της παραγωγικότητας των συστημάτων χωρίς να τα επιβραδύνει, ή να καταλύει πόρους του συστήματος. Η εταιρεία για την ακρίβεια χρησιμοποιεί το Synematic Endpoint Protection 11.

8.2.4.3 Firewall

Το firewall είναι απαραίτητο μέτρο προστασίας των δικτύων και των συστημάτων ης εταιρείας. Τα firewalls μπορεί να ενσωματώνουν όλες τις υπηρεσίες Antivirus, URL Filtering, Antispam κλπ. καθότι μπορούν να περιλαμβάνουν πλήθος των χαρακτηριστικών ασφάλειας τους σε ένα σύνολο που ονομάζεται UTM (Unified Threat Management)

Το firewall μπορεί να είναι εκτός από software και hardware, μια συσκευή δηλαδή που τοποθετείται στην σύνδεση του ηλεκτρονικού υπολογιστή με το διαδίκτυο. Επίσης μέσω αυτών μπορεί να καθορίσει ποίοι υπολογιστές και με ποιόν τρόπο θα ανταλλάσσουν πληροφορίες. Αυτό επιτυγχάνεται με την χρήση διάφορων φίλτρων τα οποία αναλύουν τα εισερχόμενα πακέτα και ανάλογα με τις οδηγίες που υπάρχουν τα αφήνουν να περάσουν ή όχι. Η μεγάλη σημασία του firewall έγκειται στο ότι συγκεντρώνει τον πλήρη έλεγχο των πακέτων που εισέρχονται στον υπολογιστή αποτελώντας ουσιαστικά έναν πύργο ελέγχου της πληροφορίας.



Εικόνα 19. Χρήση Firewall σε τοπικό επίπεδο.

Επίσης, με το firewall η εταιρεία μπορεί να προλαμβάνει πιθανές εισβολές στο δίκτυό της όπως από:

Απομακρυσμένη Είσοδος (Remote login): Με απομακρυσμένο έλεγχο μπορεί κάποιος να εισβάλει σε κάποιον υπολογιστή και να τον ελέγχει με οποιαδήποτε μορφή. Αυτό μπορεί να ποικίλει ανάλογα με το πόσο εύκολη είναι η πρόσβαση στα δεδομένα του υπολογιστή και σε ποια δεδομένα μπορεί να έχει πρόσβαση.

Εφαρμογές backdoors (Application backdoors): Κάποια προγράμματα έχουν τη δυνατότητα απομακρυσμένου ελέγχου και πρόσβασης ή μπορεί να έχουν κάποιες «τρύπες» στο λογισμικό τους τις οποίες να εκμεταλλεύονται κακόβουλα κάποιοι για να εισβάλουν παράνομα στον υπολογιστή που θέλουν.

Βομβαρδισμοί με e-mail (E-mail bombs): Πρόκειται για προσωπική-ατομική επίθεση κατά την οποία αποστέλλονται στον ίδιο παραλήπτη(mail server ή e-mail) εκατοντάδες ηλεκτρονικά μηνύματα με αποτέλεσμα το σύστημα να μη μπορεί να δεχτεί άλλα και έτσι να υπολειτουργεί ή να καταρρέει κάνοντας έτσι πιο εύκολη τη πρόσβαση στον υπολογιστή ή στο δίκτυο.

Μακροεντολές (Macros): Κάποια προγράμματα για να απλοποιηθούν ορισμένες λειτουργίες τους επιτρέπουν τη σύνταξη μακροεντολών. Οι χάκερς εκμεταλλεύονται αυτή την ιδιότητα των προγραμμάτων και δημιουργούν τις δικιές τους μακροεντολές κάνοντας έτσι τη πρόσβασή τους στο σύστημα εύκολη υπόθεση.

Ιοί (Viruses): Ίσως η πιο γνωστή απειλή των υπολογιστών στις μέρες μας. Οι ιοί είναι μικρές συνήθως εφαρμογές οι οποίες έχουν την ικανότητα να δημιουργούν κλώνους και με αυτό τον τρόπο να εξαπλώνονται γρήγορα από υπολογιστή σε υπολογιστή. Έχουν την ικανότητα να «κρύβονται» μέσα σε άλλα προγράμματα ή να εγκαθίστανται σε αυτά. Οι ιοί μπορούν να προκαλέσουν μια μικρή ζημιά μέχρι και την ολική απώλεια των δεδομένων του συστήματος.

Spam: Είναι τα ενοχλητικά e-mail, όπως τα διαφημιστικά, τα οποία από μόνα τους συνήθως δεν αποτελούν απειλή. Συνήθως περιέχουν υπερσυνδέσεις από άλλες σελίδες οι οποίες όμως μπορεί να σου μεταφέρουν ιούς.

8.2.4.4 Λογισμικό Antivirus

Στόχος του Antivirus είναι να ανιχνεύονται όλα τα αρχεία ή η μνήμη του υπολογιστή για αρχεία που μπορεί να έχουν κάποιον ιό. Τα αρχεία που ψάχνει είναι βασισμένα στις υπογραφές, ή τους ορισμούς, των γνωστών ιών. Ένας από τους τρόπους κατηγοριοποίησης των μηχανισμών Antivirus είναι ο ακόλουθος:

1. Λογισμικό που εγκαθίσταται στους Servers ή στους Η/Υ και αφενός δεν επιτρέπει τη μόλυνση από κακόβουλο κώδικα, αφενός καθαρίζει τυχόν ήδη μολυσμένους Η/Υ

2. Λογισμικό που εγκαθίσταται στη είσοδο ενός δικτύου (mail servers, proxy servers κλπ.) και ελέγχει την κίνηση που διέρχεται μέσω αυτών από και προς τους Η/Υ

3. Συσκευές που διαθέτουν φίλτρα ελέγχου και λειτουργούν ως Gateways του δικτύου.

Συνήθως, αναλόγως του μεγέθους του δικτύου υλοποιείται ένας συνδυασμός των ανωτέρω λύσεων και γενικότερα συνίσταται η ενσωμάτωση μηχανισμών ελέγχου σε όλα τα σημεία πιθανής εισόδου ιών.

8.2.4.5 Λογισμικό Antispyware

Είναι ένας μηχανισμός που αποτρέπει τη μόλυνση του Η/Υ με προγράμματα που ελέγχουν και καταγράφουν τον τρόπο χρήσης του. Επίσης τα προγράμματα Spyware καταναλώνουν το εύρος (bandwidth) της σύνδεσης με το διαδίκτυο.

Υπάρχουν δύο τρόποι υλοποίησης που μπορούν να λειτουργούν παράλληλα.

• Ο ένας, είναι η υλοποίηση του μηχανισμού Antispyware στη πύλη δικτύου (Gateway) συνήθως με την εγκατάσταση κατάλληλης συσκευής που λειτουργεί ως διακομηστής μεσολάβησης (proxy).

• Ο άλλος τρόπος, είναι η υπηρεσία να υπάρχει στον κάθε ένα Η/Υ του δικτύου.

Καθώς η συντριπτική πλειοψηφία των περιπτώσεων μόλυνσης με Spyware γίνεται από επίσκεψη σε ακατάλληλα sites, οι υπηρεσία Antispyware τείνει να ταυτιστεί με την υπηρεσία URL Filtering και ενίοτε να προσφέρεται από τον ίδιο μηχανισμό.

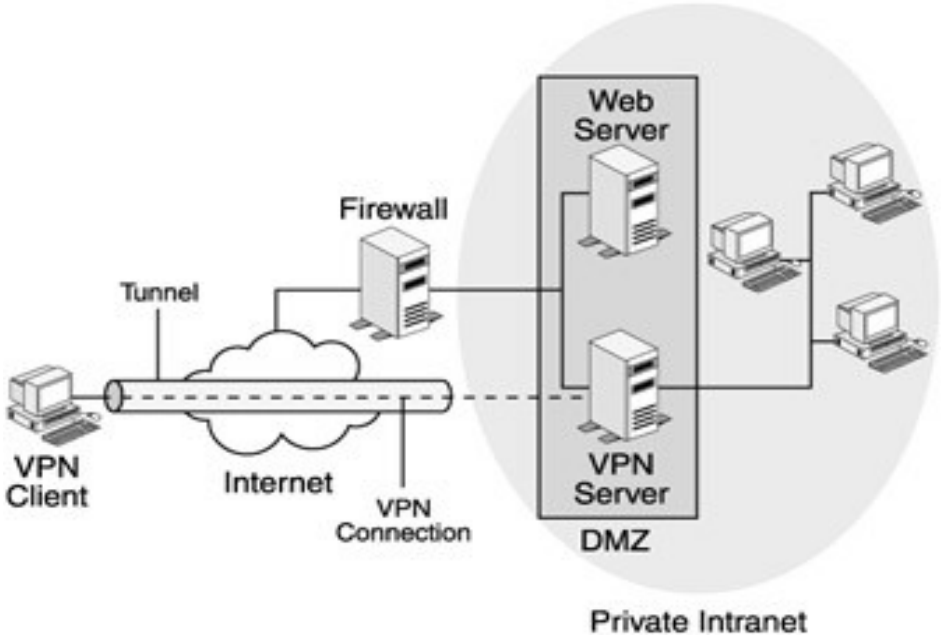
8.2.4.6 Λογισμικό Antispam

Το Antispam είναι πλέον απαραίτητο για την ασφαλή και παραγωγική χρήση των emails, ενώ όπως όλα δείχνουν το πρόβλημα του spam θα συνεχίσει να εντείνεται. Για αυτό το λόγο διατίθενται πολλοί μηχανισμοί και τεχνολογίες για την αντιμετώπισή του. Ο ποιο οικονομικός, αλλά και αποτελεσματικός τρόπος είναι η παροχή υπηρεσίας Antispam μέσω των μηχανισμών firewall.

Βασικό μειονέκτημα αυτών των λύσεων είναι ότι δεν έχουν πληρότητα παραμετροποίησης ώστε η λειτουργία του Antispam να προσαρμοστεί στις ανάγκες του δικτύου. Αντίστοιχης αποτελεσματικότητας και κόστους λύσεις είναι και αυτές που υλοποιούν ελέγχους Antispam στα mails πριν φτάσουν στο εταιρικό δίκτυο. Και πάλι δεν προσφέρονται πλήρεις δυνατότητες παραμετροποίησης της υπηρεσίας.

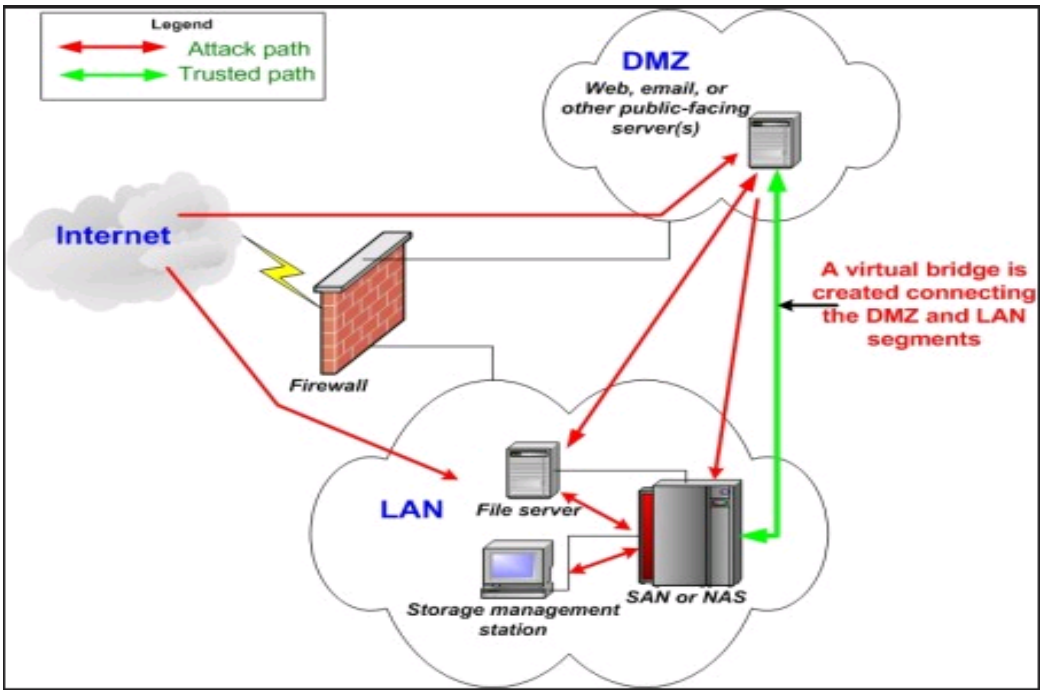
8.1.4.7 DMZ (De Militirized Zone)

Το DMZ σημαίνει DeMilitirised Zone και είναι χαρακτηριστικό ενός hardware firewall. Σε ένα hardware firewall υπάρχουν τρείς κάρτες δικτύου (interfaces). Στη μία συνδέεται το εσωτερικό δίκτυο της εταιρίας και εκεί υπάρχουν όλοι οι χρήστες. Στη δεύτερη συνδέεται το Ίντερνετ. Το firewall ελέγχει τι εισέρχεται και τι εξέρχεται μεταξύ των δύο αυτών θέσεων, δηλαδή μεταξύ του Internet και του εσωτερικού δικτύου. Χρειάζεται όμως και μία τρίτη θέση για παράδειγμα για να μπορούν οι χρήστες από το internet να έχουν πρόσβαση σε κάποια δεδομένα της εταιρείας, μέσα από το site της, χωρίς όμως να έχουν οποαδήποτε σχέση με τη εσωτερικό δίκτυό της.



Εικόνα 20. Χρήση DMZ

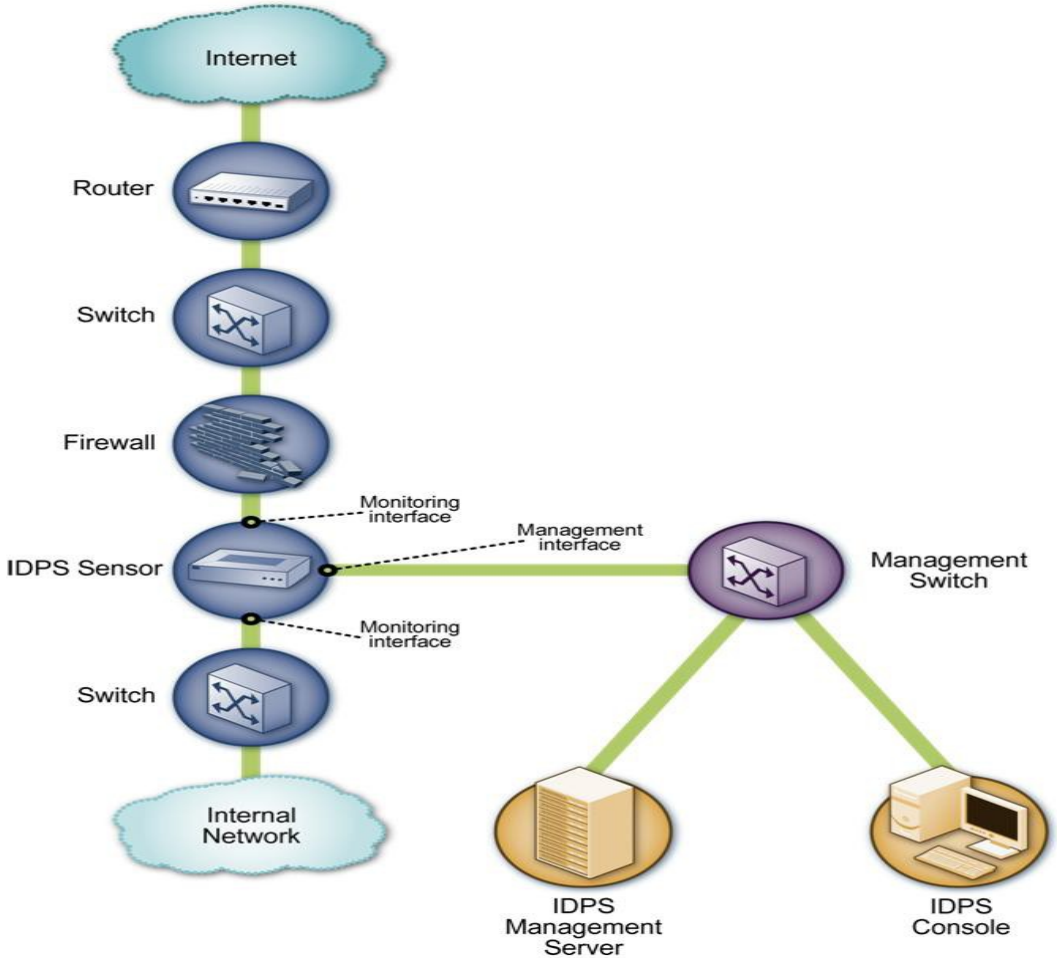
Γενικά το DMZ χρησιμοποιείται για να εφαρμόστεί μια πολιτική ασφαλείας όσον αφορά τα δίκτυα της εταιρείας. Στην ουσία το DMZ λειτουργεί ως απομονωτής μεταξύ των ασφαλών τοπικών δικτύων της εταιρείας και του Διαδικτύου.



Εικόνα 21. Εικονική γέφυρα σύνδεσης DMZ με τοπικό Δίκτυο.

8.1.4.8 IDS/IPS (Introdusion Detective/Prevention System)

Για επιπλέον ασφάλεια στο δίκτυο συνίσταται η χρήση IDS/IPS συστημάτων, είναι μηχανισμός προστασίας που αποτρέπει δικτυακές επιθέσεις και επιθέσεις σε επίπεδο εφαρμογής όπως worms, Trojans, spyware, keyloggers κλπ. Η λειτουργία τους βασίζεται σε ενσωματωμένα φίλτρα ελέγχου (zero day protection) και σε σύγκριση της ενδεχόμενης απειλής με ήδη γνωστές απειλές (signature & pattern matching). Για την ακρίβεια το σύστημα αυτό εντοπίζει πιθανές διεισδύσεις, στόχος του είναι η ανίχνευση επιθέσεων κατά του υπολογιστή ή την κακή χρήση του υπολογιστή και ειδοποίηση των αρμόδιων ατόμων όταν ανιχνευτεί κάτι περίεργο. Η εγκατάσταση ενός IDS σε ένα δίκτυο παρέχει το ίδιο αποτέλεσμα με την εγκατάσταση ενός συναγερμού σε ένα σπίτι. Με διάφορες μεθόδους και τα δύο ανιχνεύουν την παρουσία ενός εισβολέα/διαρρήκτη και τα δύο στη συνέχεια εκδίδουν κάποιο είδος προειδοποίησης και συναγερμού.



Εικόνα 22. Παράδειγμα Αρχιτεκτονικής Αισθητήρων IDPS

Η διαφορά τους από τις τεχνολογίες των Firewall είναι ότι τα IPS συστήματα ελέγχουν την πρόσβαση σε επίπεδο εφαρμογής, πέρα από τη διεύθυνση IP ή τις πόρτες. Πολλαπλές μελέτες έχουν δείξει ότι παραδοσιακοί μηχανισμοί ασφάλειας (π.χ. Firewalls) μπορούν να παρακαμφθούν λόγω ύπαρξης / παρουσίασης αδυναμιών. Ένα σφάλμα, ελάττωμα, σφάλμα προγραμματισμού ή ακόμη μια λανθασμένη παραμετροποίηση μπορεί να γίνει αντικείμενο εκμετάλλευσης από χάκερς ή από κάποιο κακόβουλο πρόγραμμα, και παράνομα να αποκτηθεί πρόσβαση σε δίκτυα ηλεκτρονικών υπολογιστών.

Προτείνεται λοιπόν, ένα σύστημα ανίχνευσης και αποτροπής εισβολέων το οποίο παρακολουθεί την εξωτερική και εσωτερική κίνηση ενός δικτύου, με σκοπό την έγκαιρη ανίχνευση πιθανών επιθέσεων και την αποτροπή τους πριν την είσοδο τους στο εσωτερικό δίκτυο και τα συστήματα της εταιρείας.

Η εταιρεία χρησιμοποιεί σύστημα HID OSSEC (Host-based Introdusion Detective System). Το εργαλείο αυτό αποτελεί αναπόσπαστο μέρος της λεπτομερούς και πλήρης ασφάλειας του συστήματος. Δεν εγγυάται πλήρως την ασφάλεια αλλά όταν συνδυαστεί με την πολιτική ασφαλείας τρωτών σημείων, την κρυπτογράφηση δεδομένων, την ταυτοποίηση του χρήστη, τον έλεγχο πρόσβασης και τα τείχη προστασίας, μπορεί να ενισχύσει σημαντικά την ασφάλεια του δικτύου.

9 Σχέδιο Έκτακτης Ανάγκης

Το σχέδιο έκτακτης ανάγκης (Disaster recovery plan and contingency plan) είναι το έγγραφο που αναφέρεται στα μέτρα, τα οποία εφαρμόζονται σε περιπτώσεις έκτακτης ανάγκης. Το σχέδιο αυτό έρχεται για να συμπληρώσει το σχέδιο ασφάλειας που προέκυψε από την ανάλυση επικινδυνότητας (risk analysis review) της υπολογιστικής και επικοινωνιακής υποδομής της εταιρείας.

Η εταιρεία για να μπορέσει να έχει ένα ολοκληρωμένο σύστημα ασφαλείας που περιορίζει όσο των δυνατόν περισσότερο τις πιθανότητες εμφάνισης κινδύνων αλλά και ευπαθειών των υπολογιστικών της συστημάτων, θα πρέπει να διαθέτει και ένα σχέδιο έκτακτης ανάγκης.

Στόχοι του σχεδίου έκτακτης ανάγκης είναι:

- Η Ελαχιστοποίηση διακοπών της κανονικής λειτουργίας

• Περιορισμός της έκτασης των ζημιών και καταστροφών, και αποφυγή πιθανής κλιμάκωσης αυτών

• Δυνατότητα ομαλής υποβάθμισης

• Εγκατάσταση εναλλακτικών μέσων λειτουργίας εκ των προτέρων

• Εκπαίδευση, εξάσκηση και εξοικείωση του ανθρώπινου δυναμικού με διαδικασίες έκτακτης ανάγκης

• Δυνατότητα ταχείας και ομαλής αποκατάστασης της λειτουργίας

• Ελαχιστοποίηση των οικονομικών επιπτώσεων

Η εταιρεία ειδικεύεται σε θέματα τηλεϊατρικής, χειρίζεται ευαίσθητα προσωπικά δεδομένα και κάθε είδους ζημία ή απώλεια αυτών έχει σοβαρό αντίκτυπο τόσο στην εύρυθμη λειτουργία της εταιρεία όσο και στην φήμη της ως προς τους πελάτες της. Για αυτό το λόγο το σχέδιο έκτακτης ανάγκης και ανάκαμψης από τέτοιου είδους περιστατικά, είναι απαραίτητο.

Αναλυτικότερα στο σχέδιο έκτακτης ανάγκης πρέπει σε πρώτη φάση να περιλαμβάνει σαφή προσδιορισμό των συνθηκών υπό των οποίων η κατάσταση θα θεωρείται έκτακτη, ώστε να πρέπει να εφαρμοστεί το σχέδιο. Η εταιρεία πραγματοποιεί σε τακτά χρονικά διαστήματα ελέγχους τόσο στο υλικό όσο και στο λογικό μέρος των συστημάτων της. Το σχέδιο έκτακτης ανάγκης πρέπει να περιλαμβάνει και προσδιορισμό των σημαντικών λειτουργιών και των αντίστοιχων συστημάτων της εταιρείας. Αν κατά την διάρκεια των ελέγχων αυτών διαπιστωθεί ότι υπάρχουν κενά ή δυσλειτουργίες στο σύστημα, που ακυρώνουν βασικές και απαραίτητες προϋποθέσεις και απατήσεις για την ασφάλεια, τότε η κατάσταση θεωρείται έκτακτη. Όπως επίσης κρίσιμη μπορεί να θεωρηθεί η κατάσταση και σε περιπτώσεις φυσικών απειλών όπως φωτιά, πλημμύρα κτλ.

Σε δεύτερη φάση το σχέδιο έκτακτης ανάγκης περιλαμβάνει στρατηγική προστασίας των λειτουργιών και των συστημάτων της εταιρείας καθώς και τον προσδιορισμό προτεραιότητας των δραστηριοτήτων του οργανισμού που θα τεθούν σε εφαρμογή στο εναλλακτικό σύστημα. Βασικό μέρος του σχεδίου είναι η καταγραφή μιας κατάστασης με τα μέλη του προσωπικού που θα κληθούν στην περίπτωση καταστροφής καθώς και τα τηλέφωνα των προμηθευτών υλικού και λογισμικού, των σημαντικών συνεργατών ή πελατών, των ατόμων που βρίσκονται σε διαφορετικές εγκαταστάσεις που θα χρησιμοποιηθούν από την επιχείρηση για τη συνέχιση της λειτουργίας της. Απαραίτητη επίσης είναι η ύπαρξη μιας κατάστασης ανάθεσης καθηκόντων στα μέλη αυτά, για την αποκατάσταση της λειτουργίας.

Σε τρίτη φάση το σχέδιο θα πρέπει να περιέχει διαδικασίες για τον υπολογισμό της ζημιάς από την καταστροφή που συντελέστηκε.

9.1 Έλεγχος προστασίας

Κατά τους ελέγχους προστασίας στο λογισμικό τηλεμετρίας ιατρικών παραμέτρων, που διαθέτει η εταιρία, θα πρέπει να καλύπτονται οι εξής απαραίτητες απαιτήσεις ασφάλειας :

• Ασφάλεια: διασφαλίζεται η ιδιωτικότητα, ενώ πραγματοποιείται πιστή καταγραφή των κλινικών ενεργειών και των ενεργειών του χρήστη, ταυτοποίηση του χρήστη και έλεγχος πρόσβασης.

• Διασυνδεσιμότητα: διασφαλίζεται η δυνατότητα διανομής και ανταλλαγής δεδομένων. Αυτό επιτρέπει όχι μόνο την αναγνωσιμότητα των δεδομένων από ανθρώπους αλλά και την αυτοματοποιημένη επεξεργασία των δεδομένων από άλλα συστήματα EHR.

• Ευρύτητα-περιεκτικότητα: υπάρχει η δυνατότητα υποστήριξης μιας ευρείας γκάμας πρακτικών στο χώρο της ιατρικής φροντίδας, υποστήριξης πολλών τύπων δεδομένων, υποστήριξης εισαγωγής δεδομένων σε δομημένη μορφή καθώς και σε μορφή ελευθέρου κειμένου.

• Μεταφερσιμότητα: το σύστημα διασφαλίζει «φορητότητα» και δυνατότητα διασύνδεσης μεταξύ ιδρυμάτων, ανεξάρτητα από το υλικό, το λογισμικό και την εθνική γλώσσα που χρησιμοποιεί ο καθένας.

• Εξέλιξη: υπάρχει η δυνατότητα υποστήριξης ιατρικού φακέλου για μακρά χρονικά διαστήματα, μέσω της συμβατότητας επεξεργασίας του ιατρικού φακέλου από προηγούμενες και επόμενες εκδόσεις συστημάτων λογισμικού EHR.

• Επεκτασιμότητα: υπάρχει η δυνατότητα παραμετροποίησης και διεύρυνσης της υφιστάμενης λειτουργικότητας, σύμφωνα με τις ιδιαίτερες ανάγκες του τελικού χρήστη.

• Διαθεσιμότητα: διασφαλίζεται η αδιάλειπτη παροχή της υπηρεσίας

• Ευρεία χρήση προτύπων: χρησιμοποιούνται διεθνή πρότυπα ανταλλαγής ιατρικής Πληροφορίας.

Η μη κάλυψη όλων των παραπάνω αποτελεί δυσλειτουργία για την εταιρεία και τις εφαρμογές της και θα πρέπει σε σύντομο χρονικό διάστημα να διορθωθεί.

9.2 Στρατηγική Προστασίας

Το σχέδιο έκτακτης ανάγκης πραγματεύεται, εκτός των άλλων, την ανάκαμψη της λειτουργίας της υπολογιστικής και επικοινωνιακής υποδομής μετά από φυσικές καταστροφές (φωτιές, πλημμύρες, σεισμούς, κτλ.). Για την ταχύτερη δυνατή αντιμετώπιση των έκτακτων περιστάσεων, προτείνεται η τοποθέτηση συναγερμών, οι οποίοι χρησιμοποιούνται τόσο για την ανίχνευση επικείμενης ζημιάς λόγω των φαινομένων αυτών, αλλά και για την ανίχνευση εισβολών στα συστήματα.

Αναφορικά με την αντιμετώπιση των έκτακτων καταστάσεων, μπορούν να χρησιμοποιηθούν ειδικές συσκευές φιλτραρίσματος, όπως είναι τα φίλτρα αέρος, που περιορίζουν τις ζημιές από τον καπνό και από άλλα βλαβερά αέρια και τα φίλτρα θορύβου, που ελαττώνουν το άκουσμα εξωτερικών θορύβων. Επίσης, για τους περιβαλλοντικούς ελέγχους υπάρχουν συσκευές ή μέθοδοι που ελέγχουν τη θερμοκρασία, την πίεση, την υγρασία και άλλους περιβαλλοντικούς παράγοντες. Παραδείγματα είναι τα κλιματιστικά, οι ελεγκτές υγρασίας και οι ιονιστές της ατμόσφαιρας.

Για την αντιμετώπιση περιστατικών πυρκαγιάς, μπορεί να τοποθετηθεί ειδικός εξοπλισμός σε ενδεικνυόμενα μέρη. Παραδείγματα αποτελούν οι πυροσβεστήρες, οι ειδικοί αφροί, ειδικά χρηματοκιβώτια για την αποθήκευση σπουδαίων εγγράφων και άλλων σημαντικών αντικειμένων, και οι εγκαταστάσεις αποθήκευσης νερού, οι οποίες έχουν και δυνατότητες άντλησης. Αυτό το τελευταίο είναι πολύ σημαντικό και για την αντιμετώπιση διαρροών νερού.

Όσον αφορά τις εισβολές, για την ανίχνευση και αντιμετώπισή τους μπορούν να χρησιμοποιηθούν ειδικά συστήματα λογισμικού, τα επονομαζόμενα συστήματα ανίχνευσης εισβολών, τα οποία κάνουν χρήση διαφόρων αισθητήρων και δίνουν τακτικές αναφορές στα κέντρα ελέγχου.

Πρέπει να επισημανθεί, ωστόσο, ότι οι κίνδυνοι αυτού του είδους ελαχιστοποιούνται, αν έχει προηγουμένως καταστρωθεί ένα προσεγμένο σχέδιο ασφάλειας. Το σχέδιο έκτακτης ανάγκης, άλλωστε, έρχεται να καλύψει τα κενά που πιθανόν να έχει αφήσει το σχέδιο ασφάλειας.

Ακόμα, στο σχέδιο έκτακτης ανάγκης προβλέπεται τρόπος αντιμετώπισης των διακοπών στην παροχή ηλεκτρικού ρεύματος. Για το λόγο αυτό συνιστάται η χρήση ειδικών γεννητριών, οι οποίες παρέχουν συνεχώς ενέργεια σε ζωτικά τμήματα του εξοπλισμού. Στο σχέδιο έκτακτης ανάγκης περιλαμβάνονται και τα μέτρα για τον έλεγχο της φυσικής πρόσβασης κατά τη διάρκεια της αντιμετώπισης έκτακτων περιστάσεων.

Το σχέδιο έκτακτης ανάγκης αντιμετωπίζει τις περιπτώσεις απώλειας δεδομένων, λογισμικού και υλικού με τη δημιουργία αντιγράφων, τα οποία φυλάσσονται σε άλλους προστατευόμενους χώρους (κτίρια).

Αναφορικά για την αντιμετώπισης της έλλειψης διαθεσιμότητας της υποδομής, διακρίνονται κυρίως δύο τρόποι εναλλακτικής τοποθεσίας:

• Τα cold sites ή shells. Εγκαταστάσεις όπου υπάρχει παροχή ηλεκτρικής ενέργειας και κλιματισμός. Στις εγκαταστάσεις αυτές θα μπορεί να εγκαθίσταται ένα υπολογιστικό σύστημα, όμοιο ακριβώς με αυτό που λειτουργεί στα κυρίως κτίρια, το οποίο θα μπορεί να τίθεται άμεσα σε λειτουργία, κάθε φορά που κάτι τέτοιο θα κρίνεται απαραίτητο

• Τα hot sites. Εγκαταστάσεις, στις οποίες υπάρχει ήδη εγκατεστημένο ένα υπολογιστικό σύστημα, το οποίο είναι και ανά πάσα στιγμή έτοιμο για λειτουργία και χρήση. Το σύστημα αυτό διαθέτει περιφερειακά, τηλεπικοινωνιακές γραμμές, γεννήτριες, και, ακόμα και προσωπικό για να το χειριστεί άμεσα, σε περίπτωση έκτακτης ανάγκης. Για την ενεργοποίηση ενός hot site, αρκεί να φορτωθούν τα δεδομένα και τα αντίγραφα του γενικού λογισμικού και των εφαρμογών, αντίγραφα των οποίων φυλάσσονται αποθηκευμένα, κατά κανόνα, σε διαφορετικά κτίρια από αυτά που βρίσκονται τα συστήματα κανονικής λειτουργίας του οργανισμού.

10 ΠΛΑΝΟ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΚΙΝΔΥΝΩΝ

Η υλοποίηση ενός πλάνου διαχείρισης και αντιμετώπισης κινδύνων είναι μια σημαντική διαδικασία για κάθε επιχείρηση. Σκοπός του πλάνου είναι η αποφυγή προβλέψιμων κινδύνων, η προστασία από λάθος επενδυτικές αποφάσεις και η ελαχιστοποίηση των απωλειών και ζημιών από απρόβλεπτα γεγονότα.

Η επιχειρησιακή διαχείριση κινδύνων (Enterprise risk management, ERM) είναι η διαδικασία σχεδιασμού, οργάνωσης, καθώς και ελέγχου των δραστηριοτήτων μίας επιχείρησης, προκειμένου να ελαχιστοποιηθούν οι επιπτώσεις του κινδύνου. Δεν περιλαμβάνει μόνο κινδύνους που σχετίζονται με τυχαίες ζημιές, αλλά και οικονομικά, στρατηγικά, λειτουργικά και άλλα συναφή είδη κινδύνων.

Η λειτουργική διαδικασία του πλάνου διαχείρισης και αντιμετώπισης κινδύνων παρέχει στην ουσία ένα χάρτη πορείας, εργαλεία και πόρους για την επίτευξη της

ασφάλειας των συστημάτων της εταιρείας. Η τυποποίησή τους γίνεται απαραίτητη για την ασφαλή λειτουργία της εταιρεία γιατί παρέχει επιπλέον σταθερότητα στην επιχείρηση.

Πιο συγκεκριμένα το πλάνο διαχείρισης και αντιμετώπισης κινδύνων των πληροφοριακών συστημάτων της εταιρείας προϋποθέτει όλα τα παρακάτω:

1. Την εκτίμηση και τον ακριβή καθορισμό των κρίσιμων περιουσιακών στοιχείων της εταιρείας

2. Την αναγνώριση των απειλών κατά των πληροφοριακών συστημάτων της εταιρείας

3. Την αναγνώριση των επιμέρους ευπαθειών

4. Την αναγνώριση των πιθανών κατηγοριών απωλειών.

5. Την εκτίμηση της πιθανότητας να συμβεί μια απώλεια

6. Τον προσδιορισμό των απαραίτητων προφυλάξεων / αντίμετρων για την αντιμετώπιση των κινδύνων και τέλος

7. Την διαμόρφωση και υλοποίηση του πλέον αποτελεσματικού και ενδεδειγμένου από άποψη κόστους συστήματος ασφαλείας.

Έχοντας καταγράψει λοιπόν την υφιστάμενη κατάσταση της εταιρείας και αναλύοντας στην συνέχεια τους κινδύνους ως προς τα αγαθά της, αναγνωρίστηκαν όλες οι απειλές και οι ευπάθειες αυτών, τόσο σε φυσικό όσο και σε λογικό επίπεδο, καθώς και η πιθανότητα εμφάνισης τους. Ακόμα έγινε καταγραφή όλων των πιθανών απωλειών που αυτά μπορεί να επιφέρουν, και έπειτα προσδιορίστηκαν και οι απαραίτητες προφυλάξεις που πρέπει να ληφθούν από την εταιρεία. Το επόμενο βήμα είναι η διαμόρφωση ενός αποδοτικού συστήματος ασφαλείας που θα εξασφαλίζει και θα εγγυάται την ακεραιότητα, την εμπιστευτικότητα αλλά και την διαθεσιμότητα των δεδομένων της εταιρείας, χωρίς να επιβαρύνει ιδιαιτέρα την εταιρεία.

Λαμβάνοντας υπ΄όψιν ότι η εταιρεία διαχειρίζεται ευαίσθητα προσωπικά δεδομένα για την διασφάλιση της προστασίας αυτών, συνιστάται η εφαρμογή του προτύπου ISO 27001 που ορίζει τις απαιτήσεις για την εφαρμογή ενός Συστήματος Διαχείρισης Ασφάλειας της Πληροφορίας (Information Security Management

System, ISMS) με τα υψηλότερο ως τώρα επίπεδο ασφάλειας. Οι απαιτήσεις αυτές εφαρμόζονται σε όλες τις λειτουργικές διεργασίες που σχετίζονται με την ασφάλεια της πληροφορίας, τόσο σε τεχνικό, όσο και σε λογικό επίπεδο. Το προτύπου ISO 27001 παρέχει μια κοινή βάση ανάπτυξης των προτύπων και των πρακτικών ασφάλειας που θα εφαρμόσει η εταιρεία και παρέχει εμπιστοσύνη κατά τις ενδο-εταιρικές συναλλαγές. Το Σύστημα Διαχείρισης Ασφαλείας Πληροφοριών είναι μέρος του συνολικού συστήματος διοίκησης του Οργανισμού ISO, συμβατό με άλλα διαχειριστικά συστήματα (ISO 9001, ISO 14001 κλπ.) και αποτελείται από διαδικασίες και ελέγχους.

Το Σύστημα Διαχείρισης της Ασφάλειας της Πληροφορίας πιστοποιείται σύμφωνα με το πρότυπο ISO 27001, από Ανεξάρτητους Φορείς Πιστοποίησης διαχειριστικών συστημάτων και αποτελεί ένα αποτελεσματικό μέσο διαχείρισης των ευαίσθητων πληροφοριών. Στόχος του είναι η προστασία των πληροφοριακών συστημάτων της εταιρείας, των διεργασιών αλλά και του προσωπικού της. Οι εταιρείες που πιστοποιούνται σύμφωνα με το Πρότυπο ISO 27001 καταδεικνύουν ότι η ασφάλεια των διεργασιών της διαχείρισης των πληροφοριών τους είναι σε αρκετά υψηλό επίπεδο.

Το Σύστημα Διαχείρισης της Ασφάλειας της Πληροφορίας προτείνει μια σειρά από μέτρα ασφάλειας τα οποία καλύπτουν ένα ευρύ σύνολο κινδύνων. Μεταξύ αυτών περιλαμβάνονται τόσο αυτόματοι μηχανισμοί όσο και διαδικασίες που πρέπει να ακολουθούνται από τα στελέχη της εταιρείας. Οι κατηγορίες που καλύπτονται είναι:

- Πολιτική Ασφαλείας
- Οργάνωση Ασφάλειας Πληροφοριών
- Διαχείριση Περιουσιακών Στοιχείων
- Διαχείριση Ανθρώπινων Πόρων
- Φυσική και Περιβαλλοντική Ασφάλεια
- Διαχείριση Επικοινωνιών και Λειτουργιών
- Έλεγχος Πρόσβασης
- Προμήθεια, Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων
- Διαχείριση Συμβάντων Ασφάλειας Πληροφοριών
- Διαχείριση Επιχειρησιακής Συνέχειας
- Συμμόρφωση

Όσον αφορά την ασφάλεια των πληροφοριών υποστηρίζει ένα λειτουργικό και ενημερωμένο σύστημα Antivirus και πλήρες σύστημα Backup, καθώς και την χρήση Firewall τόσο ως Hardware όσο και ως Software. Αναπόσπαστο κομμάτι του συστήματος είναι οι έλεγχοι πρόσβασης στα δικαιώματα των χρηστών ως προς τα αγαθά της εταιρείας, οι έλεγχοι σε έγγραφα (Document Control) όπως ιστορικό αλλαγών ή αναθεωρήσεων, καταστροφή απαρχαιωμένου υλικού κ.α. και το σπουδαιότερο παρέχει Πολιτική Αποκατάστασης (Disaster Recovery Policy) μετά από καταστροφή-φυσική ή μη.

Το πλάνο διαχείρισης ενός τέτοιου συστήματος εφαρμόζεται σε τέσσερις φάσεις, σε γενικές γραμμές οι φάσεις αυτές είναι οι εξής:

• *Σχεδιασμός (Plan):* Σε αυτήν την φάση σχεδιάζεται το όλο σύστημα, καταγράφονται όλα τα αγαθά και περιουσιακά στοιχειά, αναλύεται η επικινδυνότητα αυτών και επιλέγονται οι απαραίτητοι έλεγχοι.

• *Εκτέλεση (Do):* Εδώ συντελείται η εφαρμογή του συστήματος και των ελέγχων λειτουργίας

• *Έλεγχος (Check):* Φάση στην οποία έχουμε την αντικειμενική αξιολόγηση του ISMS αλλά και η αξιολόγηση των επιδόσεων αυτού (αποδοτικότητα και αποτελεσματικότητα)

• *Ενεργοποίηση (Act):* Σε αυτήν την φάση γίνονται αλλαγές όπου χρειάζονται, ώστε να βελτιστοποιηθεί το σύστημα.

Τα οφέλη που αποκομίζει η εταιρεία με την εφαρμογή ενός συστήματος ISM είναι ότι εκτός του ότι θα κερδίζει την εμπιστοσύνη του πελάτη, θα μειώσει τα συμβάντα σχετικά με την ασφάλεια της και επομένως θα αυξήσει και την αξιοπιστία της, εξασφαλίζοντας τα αγαθά και τα περιουσιακά στοιχεία της από υποβάθμιση, απώλεια, ζημιά ή και κλοπή. Συμμορφώνεται επίσης με την σχετική νομοθεσία αποκτώντας ανταγωνιστικό πλεονέκτημα καθότι θα έχει πρόσβαση σε αγορές και πελάτες που απαιτούν υψηλά επίπεδα ασφάλειας από τους συνεργάτες τους. Και το σημαντικότερο όφελος θα είναι ότι θα έχει εξασφαλίσει την άμεση επαναφορά και λειτουργία των συστημάτων της σε περίπτωση καταστροφής μεγάλης κλίμακας.

11 ΕΠΙΛΟΓΟΣ - ΠΡΟΤΑΣΕΙΣ

Αν η ασφάλεια παρομοιαστεί με μια πυραμίδα τότε σίγουρα την βάση αυτής αποτελεί η σχεδίαση και εφαρμογή μιας ολοκληρωμένης πολιτικής ασφαλείας. Η πολιτική ασφάλειας είναι το πρώτο βήμα που πρέπει να κάνει κάποιος αν θέλει να έχει ένα ασφαλές δίκτυο. Απαραίτητες διαδικασίες για την υλοποίηση της είναι η ανάλυση ρίσκου και η αποτίμηση κινδύνων, που πλέον διευκολύνονται σημαντικά από την ύπαρξη των σχετικών λογισμικών, που δίνουν σημαντικές υποδείξεις και κατευθύνσεις για ένα σημαντικό επίπεδο ασφάλειας. Στις μέρες μας δεν νοείται λειτουργία ενός οργανισμού χωρίς Internet και γενικότερα χωρίς δικτύωση μεταξύ των εργαζομένων. Η οικονομία και η στρατηγική μιας εταιρίας είναι πλέον ταυτισμένη με το δίκτυό της. Μείζον ζήτημα της εποχής μας λοιπόν αποτελεί η ασφάλεια των πληροφοριακών συστημάτων και των δικτύων τους. Η πολιτική ασφάλειας καλείται να προβλέψει πιθανά συμβάντα και καταστάσεις, απειλητικές για την ασφάλεια αυτών, και να προτείνει μια σειρά μέτρων αντιμετώπισης τους. Εμπειρικά έχει αποδειχθεί ότι οι μηχανισμοί και οι τεχνικές από μόνα τους δεν συνιστούν μέτρα ασφαλείας. Αυτά πρέπει να λειτουργούν κάτω από ένα μοντέλο ασφάλειας. Ωστόσο η πρόβλεψη κινδύνων σε οποιαδήποτε ενέργεια μας είναι αδύνατη, από την άποψη ότι οι πιθανοί συνδυασμοί ενεργειών που δύνανται να προκαλέσουν πρόβλημα είναι άπειροι ο δυσκολότερος παράγοντας είναι η ανθρώπινη φύση που κρύβει εκπλήξεις, άλλοτε ευχάριστες άλλοτε δυσάρεστες.

Μελλοντικές επεκτάσεις

Η παρούσα μελέτη είχε ως στόχο να καλύψει σε έναν σημαντικό βαθμό το ζήτημα της εκτίμησης κινδύνων στα ΠΣ καλύπτοντας τα πιο σημαντικά και κρίσιμα ζητήματα ασφάλειας που καλείται να αντιμετωπίσει ένας οργανισμός για να προστατέψει το πληροφοριακό της σύστημα.

Το κυριότερο ωστόσο για ένα ασφαλές Π.Σ. είναι η διαχείριση. Ένα γενικότερο πλαίσιο σωστής διαχείρισης ξεκινά από ένα καλά δομημένο, χωρίς προβλήματα και απώλειες, δίκτυο. Μία μελλοντική επέκταση λοιπόν θα μπορούσε να σταθεί πολύ περισσότερο στο κομμάτι της διαχείρισης δικτύου. Η καταγραφή επιπλέον χαρακτηριστικών του δικτύου όπως ο αριθμός των υπολογιστών που το αποτελούν και των ασύρματων και ενσύρματων συνδέσεων, η ταχύτητα μεταφοράς των δεδομένων, το είδος του hardware που χρησιμοποιείται καθώς και άλλα σχόλια, ώστε να υπάρξει μια καλύτερη εικόνα για το πώς είναι δομημένο το δίκτυο και πως μπορεί να το βελτιωθεί.

Επίσης μια πολύ καλή πρόταση θα ήταν να δοθεί περισσότερη έκταση στην διαδικασία ανάλυσης της επικινδυνότητας των συστημάτων, αναλύοντας τα εργαλεία λογισμικού που υπάρχουν και να εκτιμηθεί η επικινδυνότητα μέσω ενός τέτοιου λογισμικού, όπως το CRAMM. Όπως και να έχει το ανθρώπινο μυαλό δεν μπορεί να προβλέψει τα πάντα, με το κατάλληλο λογισμικό όμως η διαδικασία αυτή γίνεται ευκολότερη και δεν υπάρχει πιθανότητα παράλειψης.

12 ΒΙΒΛΙΟΓΡΑΦΙΑ – ΑΝΑΦΟΡΕΣ

[1] ISO/IEC, 17799 Code of Practice for Information Security Management, Geneva, Switzerland, 2000.

[2] ISO/IEC/JTC1, TR 13335 Information Technology - Security Techniques - Guidelines for the management of IT Security (GMITS), Geneva, Switzerland, 1996.

[3] Νόμος 2472/97, Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, 10-4-97/ΦΕΚ 50/Τεύχος Α', 1997.

[4] Νόμος 2474/1999, Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.

[5] Νόμος 3418/2005, Κώδικας Ιατρικής Δεοντολογίας.

[6] Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

[7] Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα.

[8] Σύσταση Αρ. R (99) 5 της επιτροπής υπουργών των κρατών μελών για την προστασία της ιδιωτικότητας στο Διαδίκτυο.

[9] 'Data Breach Investigation report 2011', Verizon.

[10] Andrew S. Tanenbaum, 'Computer Networks', 4th Edition, Pearson Education Inc, 2003.

[11] Πανέτσος Σ., 'Επικοινωνίες & Δίκτυα Υπολογιστών', εκδόσεις Τζιόλα, Θεσσαλονίκη 2007.

[12] Μάττας Α., 'Ασφάλεια Πληροφοριακών Συστημάτων σε συνεργατικά περιβάλλοντα εφαρμογών με βάση το διαδίκτυο', Θεσσαλονίκη 2007.

[13] Καρύδα Μαρία, 'Διοίκηση ασφάλειας πληροφοριακών συστημάτων', Αθήνα 2005.

[14] Μπόζιος Ε., 'Σημειώσεις Εφαρμοσμένης Ασφάλειας Πληροφοριακών Συστημάτων', Θεσσαλονίκη, 2007.

[15] Πάγκαλος Γ., Μαυρίδης Ι., 'Ασφάλεια πληροφοριακών συστημάτων και δικτύων' Θεσσαλονίκη, 2002.

[16] Λαζακίδου Α., 'Πληροφοριακά Συστήματα Νοσοκομείων & Ηλεκτρονικές Υπηρεσίες Υγείας', Εκδόσεις Κλειδάριθμος, Αθήνα 2005.

[17] Κομνηνός , Θόδωρος Π. Σπυράκης , Παύλος Γ. , 'Ασφάλεια δικτύων & υπολογιστικών συστημάτων : αναχαιτίστε τους εισβολείς', 2002.

[18] Κιουντούζης Ε, 'Μεθοδολογίες ανάλυσης και σχεδιασμού πληροφοριακών συστημάτων', Β' Εκδόσεις Μπένου, Αθήνα 2002.

[19] Σ. Κάτσικας, "Ασφάλεια Δικτύων", ΕΑΠ, Πάτρα, 2001

[20]Γκριτζάλης Δημήτρης Α. , Κάτσικας Σωκράτης Κ., 'Ασφάλεια δικτύων υπολογιστών: τεχνολογίες και υπηρεσίες σε περιβάλλοντα ηλεκτρονικού επιχειρείν και ηλεκτρονικής διακυβέρνησης', 2003.

[21]Κλαδάκης Ν., Λεκάτης Γ., 'Ασφάλεια δικτύων και συστημάτων' , Αθήνα , 2001.

[22]Β. Ζορκάδης, "Κρυπτογραφία", ΕΑΠ, Πάτρα, 2002

[23]W. Stallings, "Network Security Essentials: Applications and Standards", 2nd edition, Prentice Hall, USA, 2003

[24]K. Scasfone, P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)", National Institute of Standards and Technology,2007

[25] Pfleeger, 'Security in Computing', Prentice-Hall Inc, 1997.

[26] Simson Garfinkel, Gene Spafford, 'Practical UNIX & Internet Security', 2nd Edition, O' Reilly & Associates Inc, 1996.

[27]S. Powell, J.P. Shim, "Wireless Technology Application, Management and Security", Springer, 2009

[28] G. Pangalos, 'Security in Medical Database Systems', EEC, SEISMED Project Report, 1992.

[29]Siponen M., 'Policies for Construction of Information Systems Security Guidelines', Kluwer Academic Publishers, 2000.

[30]Hossein Bidgoli, 'Handbook of Information Security', John Wiley & Sons, California 2006.

[31]Rash, Michael et al, Intrusion Prevention and Active Response: Deployment Network and Host IPS, Syngress, 2005.

[32]Joseph Boyce, 'Information Assurance: Managing Organizational It Security Risks', ΗΠΑ, 2002.

[33] Δικτυακός τόπος 'Αρχής Προστασίας Προσωπικών Δεδομένων', www.dpa.gr , Μάρτιος 2012.

[34]Δικτυακός τόπος 'Inventory of Risk Management /Risk Assessment methods and tools', http://rm-inv.enisa.europa.eu, Μάρτιος 2012.

[35] Δικτυακός τόπος 'Information Security Policies and Standards', http://www.information-security-policies-and-standards.com/, Ιούνιος 2012.

[36] Δικτυακός τόπος 'Risk World', http://www.riskworld.net/, Ιούνιος 2012.

[37]Δικτυακός τόπος 'Specialist services and solutions for IT governance, risk management, compliance and information security'. http://www.itgovernance.co.uk/, Ιούνιος 2012.

Αντιστοίχηση Ελληνικών - Αγγλικών Όρων

Αναγνώστης έξυπνης κάρτας	Smart card reader
Εμπιστευτικότητα	Confidentiality
Εναλλακτική τοποθεσία	Alternate site
Ευπάθειες	Vulnerabilities
Αγαθά Πληροφοριακού Συστήματος	Information System Assets
Αδιαφάνεια	Opacity
Ακεραιότητα	Integrity
Αναθεώρηση	Review
Ανάλυση Επικινδυνότητας	Risk Analysis
Αντίμετρα	Countermeasures
Απειλές	Threats
Αποδοτικότητα	Effeciency
Αποτυχίας Εξοπλισμού	Failures of equipment
Απώλειες	Losses
Ασφάλεια βάσεων δεδομένων	Database security
Βασισμένη-σε-ρόλους Έλεγχος πρόσβασης	Role-Based Access Control
Γενικές Προτάσεις	High-level statements
Γενικότητα	Generality
Διαβεβαίωση	Assurance
Διαδικασίες	Procedures
Διαθεσιμότητα	Availability
Διακοπή	Interruption

Διαχείριση Ασφάλειας	Security Management
Διεθνή πρότυπα	Standards
Ελεγκτικότητα	Accountability
Έλεγχοι εγγράφων	Document Controls
Έλεγχος	Audit
Έλεγχος πρόσβασης	Access control
Εμπιστευτηκότητα	Confidentiality
Εμπλεκόμενοι	Stakeholders
Ενημέρωση και συμμόρφωση	Awareness and enforcement
Εξυπηρετητές	Servers
Επεκτασιμότητα	Extentability
Επικινδυνότητα	Risk
Επικοινωνιακής Διείσδυσης	Communications Infiltration
Επισκόπηση και αναθεώρηση	Review and audit
Επιχειρησιακή διαχείριση κινδύνων	Enterprise risk management
Ευελιξία	Flexibility
Ευκινησία	Capacity
Ευχρηστία	Usability
Εφεδρική εγκατάσταση	Disaster recovery facility
Ιοί	Viruses
Κανόνες	Rules
Κατά -Απαίτηση Έλεγχος πρόσβασης	Mandatory Access Control
Κατά-Διάκριση Έλεγχος πρόσβασης	Discretionary Access Control

Κατηγοριοποίηση δεδομένων	Classification of data
Κουλτούρα ασφάλειας	Security culture
Λογική Διείσδυση	Logical infiltration
Μακροεντολές	Macros
Μέτρα ασφάλειας	Security measures
Οδηγίες	Guidelines
Οργανωσιακή πολιτική	Organisational policy
Παραβίαση ασφάλειας	Security breach
Παρεμπόδιση	Interception
Πεδίο εφαρμογής της πολιτικής ασφ.	Scope of Security Policy
Περιστατικό ασφάλειας	Security incident
Πιστοποίηση	Certification
Πλαστοποίηση	Fabrication
Πολιτική Αποκατάστασης	Disaster Recovery Policy
Πολιτική Ασφάλειας	Security Policy
Πρότυπα	Standards
Πύλη δικτύου	Gateway
Ρόλοι και αρμοδιότητες	Roles and responsibilities
Σήμανση	Marking
Σημαντικές λειτουργίες και συστήματα	Critical functions and systems
Στόχοι	Security policy objective
Στρατηγική Προστασίας	Protection Strategy
Συμμόρφωση	Compliance

Συντηρησιμότητα	Serviceability
Σχέδιο Ανάκαμψης	Recovery Plan
Σχέδιο Ασφάλειας	Security Plan
Ταυτοποίηση	Identification
Τροποποίηση	Modification
Υλοποίηση και εφαρμογή	Implementation and application
Υπεύθυνος Ασφάλειας	Security Officer
Υπευθυνότητα	Responsibility
Φυσική ασφάλεια	Physical security