-

ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΝΟΣΗΛΕΥΤΙΚΗΣ

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ
ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΕΙΔΙΚΕΥΣΗ: ΠΛΗΡΟΦΟΡΙΚΗ ΤΗΣ ΥΓΕΙΑΣ

ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΣΥΝΤΑΓΟΓΡΑΦΗΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΥΓΕΙΑΣ: ΣΥΣΤΗΜΑΤΙΚΗ ΑΝΑΣΚΟΠΗΣΗ

ΑΠΟΣΤΟΛΟΥ Β. ΚΟΝΤΕ

ΙΑΤΡΟΥ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΘΗΝΑ 2018

ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΣΥΝΤΑΓΟΓΡΑΦΗΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΥΓΕΙΑΣ: ΣΥΣΤΗΜΑΤΙΚΗ ΑΝΑΣΚΟΠΗΣΗ

ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΝΟΣΗΛΕΥΤΙΚΗΣ

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ
ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ: 'ΟΡΓΑΝΩΣΗ ΚΑΙ ΔΙΟΙΚΗΣΗ ΥΠΗΡΕΣΙΩΝ ΥΓΕΙΑΣ - ΠΛΗΡΟΦΟΡΙΚΗ ΤΗΣ ΥΓΕΙΑΣ

ΕΙΔΙΚΕΥΣΗ: ΠΛΗΡΟΦΟΡΙΚΗ ΤΗΣ ΥΓΕΙΑΣ

ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΣΥΝΤΑΓΟΓΡΑΦΗΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΥΓΕΙΑΣ: ΣΥΣΤΗΜΑΤΙΚΗ ΑΝΑΣΚΟΠΗΣΗ

ΑΠΟΣΤΟΛΟΥ Β. ΚΟΝΤΕ

ΙΑΤΡΟΥ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΘΗΝΑ 2018

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ:

ΕΠΙΒΛΕΠΟΥΣΑ: ΑΝΑΠΛΗΡΩΤΡΙΑ ΚΑΘΗΓΗΤΡΙΑ Α.ΤΣΑΛΓΑΤΙΔΟΥ,

ΚΑΘΗΓΗΤΗΣ: Ι. ΜΑΝΤΑΣ,

ΕΠΙΚΟΥΡΟΣ ΚΑΘΗΓΗΤΗΣ: ΚΑΘΗΓΗΤΗΣ Α. ΠΙΚΡΑΚΗΣ

ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΝΟΣΗΛΕΥΤΙΚΗΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΣΥΝΤΑΓΟΓΡΑΦΗΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΥΓΕΙΑΣ: ΣΥΣΤΗΜΑΤΙΚΗ ΑΝΑΣΚΟΠΗΣΗ

ΑΠΟΣΤΟΛΟΥ ΚΟΝΤΕ

ΠΕΡΙΛΗΨΗ

Σήμερα παγκοσμίως αναγνωρίζεται η ανάγκη για προστασία της ιδιωτικότητας, των προσωπικών δεδομένων και της ασφάλειας των ΠΣ και επικοινωνιών. Ακόμα πιο μεγάλη είναι η ανάγκη αυτή στον χώρο της Υγείας, ένα κατεξοχήν πολύπλοκο και ευαίσθητο χώρο, που καθίσταται ακόμα πιο σύνθετος από την είσοδο των νεών ΤΠΕ σε όλο το φάσμα υπηρεσιών και λειτουργιών του. Σκοπός της εισόδου αυτής είναι να τον υποστηρίξουν, να τον εξελίξουν, αλλά και να τον ελέγξουν.

Προς αυτή την κατεύθυνση πρέπει και λαμβάνονται πλήθος μέτρων, τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο. Από την άλλη προβλέπεται ότι το κυβερνοέγκλημα θα αναπτύσσεται παγκοσμίως και το κόστος για τις επιχειρήσεις θα είναι τεράστιο. Αυτό σημαίνει ότι η ευρωπαϊκή και η παγκόσμια κοινότητα, θα πρέπει να δραστηριοποιηθεί και να επενδύσει σε θέματα ασφάλειας ΠΣ. Η ανάγκη για σχετική με τις παράνομες πράξεις νομοθεσία σε διεθνές επίπεδο είναι πάντα απαραίτητη, αλλά ακόμη πιο απαραίτητη είναι στην περίπτωση της ψηφιακής τεχνολογίας μιας και τα ψηφιακά σύνορα είναι πιο δύσκολο να ανιχνευθούν και να ελέγχθουν από τον μέσο άνθρωπο.

Πρωτόκολλα και νομοθετικές διατάξεις έχουν οπωσδήποτε θεσπιστεί από δεκαετίες παράλληλα με την εξέλιξη της ψηφιακής τεχνολογίας και συνεχώς

ανανεώνονται και αναθεωρούνται σε ένα κατεξοχήν δυναμικό και αναπτυσσόμενο περιβάλλον, όπως είναι η εισαγωγή ΤΠΕ σε όλες τις κοινωνικές δομές και στο χώρο της υγείας ειδικότερα.

Αντικείμενο της διπλωματικής, είναι να περιγράψει τις απειλές, το νομοθετικό πλαίσιο, τη διαχείριση κινδύνου, και τα τεχνικά μέτρα που πρέπει να λαμβάνονται υπ΄όψιν προκειμένου να τεθεί σε τάξη η ασφάλεια στην ψηφιακή υγεία, με σκοπό την προστασία της δημόσιας υγείας και των κοινωνικών αξιών γενικότερα. Αυτό θα αυξήσει το αίσθημα της εμπιστοσύνης των ανθρώπων στη χρήση και επέκταση των νέων ψηφιακών τεχνολογιών στην Υγεία, που είναι και το τελικό ζητούμενο.

Για το σκοπό της διπλωματικής μελέτης, χρησιμοποιήθηκαν μηχανές αναζήτησης, όπως η Google scholar η Pubmed και η IEEExplore και σχετικές με το θέμα λέξεις κλειδιά, όπως επίσης μελετήθηκαν εκτεταμένα και ιστότοποι σχετικών εθνικών, ευρωπαϊκών, διεθνών οργανισμών, και επιχειρήσεων.

Λέξεις κλειδιά: Κυβερνοασφάλεια, Ασφάλεια Πληροφοριακών συστημάτων Υγείας, Ασφάλεια και ηλεκτρονική συνταγογράφηση, Προστασία προσωπικών δεδομένων.

NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS FACULTY OF NURSING

INTERUNIVERSITY POSTGRADUATE PROGRAM IN HEALTH CARE MANAGEMENT AND HEALTH CARE INFORMATICS

DISSERTATION

PROTECTION OF PERSONAL DATA, AND SECURITY IN E-PRESCRIPTION AND HEALTH INFORMATION SYSTEMS: A SYSTEMATIC REVIEW

BY APOSTOLOS KONTES

SUMMARY

The need for the protection of privacy and personal information, and for the security of information systems is universally acknowledged in our time, as of extreme importance. This becomes more imperative in Healthcare as it is a profoundly complex and sensitive environment, which with the introduction of modern information and communication technologies in every aspect of its spectrum, becomes even more complex. The reason for the introduction of IT technologies in the Healthcare sector is to support, improve and also control the sector.

To this end multiple measures should be considered and addressed both in theoretical and practical level. Cybercrime is expected to rise in numbers world-wide, and the expected cost for businesses to be enormous. This means that both Europe and the global community will have to adjust and invest in IT security fields. The need for relevant legislation against illegal actions in an international level is always necessary, but even more so in the case of digital technologies, as the digital borders are even harder to be monitored and controlled from the average person.

For this purpose and for decades now in accordance with the evolution of IT, relative technical protocols, legislative acts are endorsed and are being continuously updated in a dynamic and constantly developing environment, as is the introduction of IT in all aspects of society and in Healthcare in particular.

This will be the object of this thesis, to outline the threats, the legal aspects, the risk-management, and the technical measures that must be considered in order to place digital health security under control, and thus protect both public health and society values. This in the end will increase trust in the use and development of new digital technologies in Healthcare, which is the main objective.

For this research, search engines like Google Scholar, PubMed, and IEEExplore were searched using relevant to the subject Keywords and also official business, national and international websites of important relevant organisations were visited.

Keywords: Cybersecurity, Health Information Systems Security, e-prescription Security, Personal Data Protection.

ΕΥΧΑΡΙΣΤΙΕΣ

Στον εκλιπόντα πατέρα μου Βασίλη και στη μητέρα μου Μαρία που με έβαλαν στη μάχη της μάθησης από τα πρώτα παιδικά μου χρόνια, και στο φίλο μου το Βίσβα για τις συστατικές επιστολές που μου έχει δώσει.

ΑΡΚΤΙΚΟΛΕΞΙΚΟ- ΣΥΝΤΜΗΣΕΩΝ

ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.
ΑΔΑΕ	Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών.
ΒΔ	Βάση Δεδομένων.
ΓΚΠΔ	Γενικός Κανονισμός για την Προστασία Δεδομένων.
ΔΠΧ	Δεδομένα Προσωπικού Χαρακτήρα.
ΕΔΕΤ	Εθνικό Δίκτυο Έρευνας & Τεχνολογίας.
ΕΣΔΑ	Ευρωπαϊκή σύμβαση των δικαιωμάτων του ανθρώπου.
ΕΕΤΤ	Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων.
ΗΔΙΚΑ Α.Ε.	«Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης ».
Η/Υ	Ηλεκτρονικός Υπολογιστής.
ΚτΠ	Κοινωνία της Πληροφορίας.
ΟΟΣΑ	Οργανισμός Οικονομικής Σταθερότητας και Ανάπτυξης.
ΟΤΕ	Οργανισμός Τηλεπικοινωνιών Ελλάδας.
ΠΔ	Προεδρικό Διάταγμα.
ΠΚ	Ποινικός Κώδικας
ΠΔΠΧ	Προστασία Δεδομένων Προσωπικού Χαρακτήρα.

ΠΣ	Πληροφοριακά Συστήματα.
ΠΣΝ	Πληροφοριακά Συστήματα Νοσοκομείων
ΠΣΥ	Πληροφοριακά Συστήματα Υγείας
ΣΔΑΠ	Σύστημα Διαχείρισης ασφάλειας πληροφοριών
ΣΗΣ	Σύστημα Ηλεκτρονικής Συνταγογράφησης.
ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών.
ΤΒΙΤ	Τμήμα βιοϊατρικής τεχνολογίας.
ΥΠΕΔΥΦΚΑ	Υπηρεσία Ελέγχου Δαπανών Υγείας Φορέων Κοινωνικής Ασφάλισης.
ΦΚΑ	Φορείς Κοινωνικής Ασφάλισης.
AP	Access Point.
ASCII	American Standard Code for Information Interchange.
AES	Advanced encryption standard.
ARC/NEMA	American College radiation / national, electrical, manufacturers association.
ARP	Address Resolution Protocol.
ANSI	American National Standards Institute.
APHII	Advisory panel of experts on health information infrastructure.
CALLIOPE	CALL for InterOPErability.
CEN ENV 12967-1	Committee European for Standardization (CEN).

(HISA),	
CLEMANTIS	Clinical Engineering Management Tool & Information System.
CD	Compact Disc.
CERT	Computer Emergency Response Teams.
CIA	Confidentiality, Integrity, Availability.
CSP	Customer service Provider.
CSIRT	Computer Security Incident Response Teams.
DIN	DIN (Deutsches Institut fur Normung), Γερμανικός Οργανισμός Τυποποίησης.
DPIA	Data Protection Impact Assessment.
EBDP	European Board of Data Protection.
ENISA	European Union Agency for Network and Information Security.
epSOS	European Patients Smart Open Services.
FDA	Food and Drug Administration.
GDPR	General Data Protection Rule.
HIPAA	Health Information, Privacy and accountability act.
HIPC	Health Information Privacy code.
HTTP	Hyper Text Transfer Protocol.
IANA	Internet Assigned Numbers Authority.
ICD	Διεθνής κατηγοριοποίηση ασθενειών.

IDS	Συστήματα ανίχνευσης παρείσφρυσης.
IEC	International Electrotechnical Commission.
IETF	Internet Engineering Task Force.
IP	Internet Protocol.
IPsec	Internet Protocol Security.
IPS	Intrusion Prevention Systems.
ISO	International Standards Organisation.
ISMS	Information System Management System.
(ISM) RF band	Industrial Scientific Medical Radiofrequency band.
LAN	Local Area Networks.
MAC	Media Access Control.
MMA's	Mobile Medical Applications.
NIH	Εθνικό Ινστιτουτο Υγείας – ΗΠΑ.
NIS (EC directive)	Security of network and information systems.
NIST	National Information Security Technology.
OSI	Open Systems interconnection.
PACS	Picture Archiving Computer Sytstem.
PIN	Personal Identification Number.
Proms	Patient reported outcomes.
Rdf	Resource Description Framework.
RFID	Radio Frequency Identification.

SNMP	Simple Network Management System.
SQL ή SEQUEL	Structured English Query Language.
SNOMED	Systematic Nomenclature - Medicine.
SSID	Service Set Identifier.
STD’s	Sexually Transmitted Diseases.
SSL	Secure Sockets Layer.
SSH	Secure Shell.
TCP	Transmission Control Protocol.
TLS	Transport Layer Security.
UDP	User Datagram Protocol.
URL	Uniform resource locator.
USB	Universal Serial Bus.
VPN	Virtual Private Networks.
WAP	Wireless Access Protocol.
WEP	Wired Equivalent Privacy.
WLAN	Wireless Local Area Network.
Owl	Web OntologyLanguage.
XML	Extended Markup Language.
HL7	Health Level Seven.

Πίνακας Περιεχομένων

Κεφάλαιο 1^{ο}: Εισαγωγή

1.1 Ιστορική Ανασκόπηση

Η σπουδαιότητα της μυστικότητας των μηνυμάτων ήταν γνωστή από τα αρχαία χρόνια.

Τα ιερογλυφικά χρησιμοποιούνταν από το 3000 π.Χ. εως το 1600 π.Χ. Από το 1850 εως το 1450 π.Χ. η γραμμική γραφή Α. Από το 1450 εως το 1200π.Χ. η γραμμική γραφή Β. Οσον αφορά τη γραμμική γραφή ο Sir Arthur Evans στην Κνωσσό το 1900μ.Χ. την ονόμασε γραμμική γραφή, γιατί θεώρησε ότι τα γράμματα έχουν μορφή γραμμών και όχι σφηνών όπως στη σφηνοειδή ή εικόνες όντων όπως αλλού. Τα γράμματα χαράσσονταν με αιχμηρό αντικείμενο πάνω σε πλάκες πήλινες, που στη συνέχεια αποξηραίνονταν στον ήλιο. Έχουν βρεθεί πάνω από 1500 επιγραφές που κατά κύριο λόγο θεωρούνται ότι ήταν λογιστικές εγγραφές για εμπορεύματα υπολογισμούς κερδών και οφειλών.

Από το 1700π.Χ. χρονολογείται και ο δίσκος της Φαιστού μια κυκλική πινακίδα με τη μορφή δύο σπειρών. Χαρακτηρίζεται από σύμβολα χαραγμένα με σφραγίδες. Οι Ρωμαίοι αργότερα όπως ο Ιούλιος Καίσαρας επιδίωκαν να μεταδίδουν με μυστικότητα τα μυνήματα που αντάλασσαν, μιας και εάν έπεφταν στα χέρια των εχθρών, ή των ανταγωνιστών τους, αυτό θα είχε δυσμενείς συνέπειες για τις επιδιώξεις τους ή ακόμα για την επιβίωση τους την ίδια.

Αργότερα στο μεσαίωνα οι λόγιοι χρησιμοποιούσαν λατινικά που και αυτά ήταν άγνωστα στους απλούς ανθρώπους της εποχής και για πολλούς αιώνες αφού ήταν ως επί το πλείστον αμόρφωτοι, και έτσι τα μηνύματα στις επιγραφές ήταν συχνά ακατάληπτα σε αυτούς, κάτι που εξασφάλιζε εν μέρει την ασφάλεια και το μυστήριο των αναγραφομένων.

Πολύ αργότερα στην πιο σύγχρονη εποχή αναπτύχθηκαν κωδικοί επικοινωνίας, όπως τα σήματα Mors και τεχνολογίες επικοινωνίας όπως ο τηλέγραφος, ενώ ενδιάμεσα υπήρξαν πολυάριθμες επινοήσεις προς τον

σκοπό αυτό. Αργότερα επινοήθηκαν διάφοροι τρόποι κρυπτογραφίας, κύριως για στρατιωτικούς αλλά και εμπορικούς σκοπούς (1).

Το 1900-1950 μ.Χ, ξεκινά η εποχή των κρυπτομηχανών όπως η Enigma των γερμανών, στον δεύτερο παγκόσμιο πόλεμο. Ο Marian Rejewski, από την Πολωνία αναφέρεται ως ο πρώτος που έσπασε τον κώδικα της περίφημης Enigma, χρησιμοποιώντας θεωρητικά μαθηματικά. Οι γερμανοί έκαναν συνεχείς τροποποιήσεις στον κώδικα, αλλά ο Alan Turing και οι συνεργάτες του στο Bletchley Park με μηχανές κρυπτανάλυσης των παραλλαγών αποκρυπτογραφούσαν τα μηνύματα τους με επιτυχία. Οι σύμμαχοι από την πλευρά τους, έιχαν και αυτοί ανάλογες κρυπτογραφικές μηχανές για να ανταλάσσουν μυνήματα με μυστικότητα. Οι βρεταννοί την Typex και οι αμερικανοί τη Sigaba.

Πιο πρόσφατα η εξέλιξη στην μυστικότητα των μυνημάτων, συνεχίστηκε με τον Claude Shannon, που θεωρείται ο πατέρας των μαθηματικών συστημάτων της κρυπτογραφίας, και εκείνος που καθιέρωσε την κρυπτογραφία και την κρυπτανάλυση (1).

Σε ότι αφορά τη μεταφορά τα κρυπτογραφημένα μυνήματα σε όλους αυτούς τους αιώνες, προκειμένου να μεταφερθούν χρειάζονταν επικοινωνιακά μέσα, και αυτά οπωσδήποτε προστατεύονταν και συντηρούνταν κατά το δυνατόν, προκειμένου να υφίστανται κατά το δυνατόν λιγότερες φθορές, διαταραχές και διακοπές από διάφορα αίτια, π.χ. φυσικές καταστροφές, επιθέσεις, υποκλοπές ενώ υπήρχαν και ομάδες αποκατάστασης και φροντίδας επικοινωνιών. Ήδη από την αρχαία εποχή, σχεδιάζονταν μέθοδοι και συστήματα που θα μπορούσαν να εξασφαλίσουν απρόσκοπτες επικοινωνίες μυνημάτων με αξιοπιστία, οικονομία και ασφάλεια σε μεγάλες αποστάσεις. Δρομείς όπως ο θρυλικός Φειδιππίδης, ιππείς, άμαξες, ταχυδρομικά περιστέρια, φρυκτωρίες ήταν τα μέσα που χρησιμοποιούνταν για αυτό τον σκοπό.

Το 1837 ο William Cooke και το 1844 ο Samuel Morse, δημιούργησαν τον τηλέγραφο, και χρησιμοποιώντας τον ηλεκτρισμό για την μεταφορά της πληροφορίας έστελναν ψηφιακές πληροφορίες μετατρέποντας τις λέξεις σε

μια σειρά από ηλεκτρικές παύλες και τελείες. Τα κρυπτογραφημένα μηνύματα της Enigma, μεταφέρονταν στην συνέχεια με σήματα Morse στους αποδέκτες τους αλλά οι σύμμαχοι παρόλο που τα λάμβαναν και αυτοί δεν μπορούσαν αρχικά να τα κατανοήσουν γιατί ήταν κρυπτογραφημένα.

Από την δεκαετία του 1870 με την εφεύρεση του τηλεφώνου από τον Graham Bell η επικοινωνία γινόταν αναλογικά (2). Στη συνέχεια δημιουργήθηκαν οι πρώτες σύγχρονες υπολογιστικές μηχανές με πρώτη τον Eniac, που συνεχώς εξελίσσονταν σε αποθηκευτικούς χώρους και ταχύτητα επεξεργασίας μετά την ανακάλυψη των τρανζίστορ τη δεκαετία του 1980.

Τα σύγχρονα κρυπτογραφικά συστήματα διεσφάλιζαν το περιεχόμενο των μυνημάτων, όμως το μήνυμα προκειμένου να μεταφερθεί από ένα σημείο Α-πομπό που εκπέμπει, σε ένα σημείο Β-δέκτη ή και περισσότερους δέκτες με ταχύτητα και προπαντώς ασφάλεια χρειάζονταν κατάλληλες επικοινωνιακές δομές και διαδρομές, δηλαδή την τεχνολογία των επικοινωνιών όπως σήμερα είναι γνωστή.

Στην εποχή του διαδικτύου, ως κρίσιμος παράγοντας που πρέπει οπωσδήποτε να λαμβάνεται υπόψιν σε θέματα ασφάλειας Π.Σ και ιδιωτικότητας, αναδεικνύεται το ίδιο το διαδίκτυο. Το διαδίκτυο στη σύγχρονη εποχή έχει εξελιχθεί σε ένα πολύπλοκο και παράλληλο με το φυσικό κόσμο, περιβάλλον. Η λειτουργία του διαδικτύου, στηρίζεται στις τηλεπικοινωνίες.

“Με τον γενικό όρο τηλεπικοινωνίες (telecommunications), χαρακτηρίζεται η κάθε μορφής ενσύρματη ή ασύρματη, ηλεκτρομαγνητική, ακουστική και οπτική μεταφορά πληροφορίας που πραγματοποιείται ανεξαρτήτως απόστασης, μεταξύ δυο ή περισσότερων στοιχείων” (2).

Ενσύρματα μέσα μετάδοσης δεδομένων είναι συνεστραμμένα ζεύγη (θωρακισμένα και αθωράκιστα), ομοαξονικά καλώδια (βασικής και ευρείας ζώνης), οπτικές ίνες (μονότροπες και πολύτροπες). Ασύρματα μέσα μετάδοσης είναι ραδιοκύματα, μικροκύματα, υπέρυθρες ακτινοβολίες. Καθένα από αυτά έχει τα πλεονεκτήματά του και τα μειονεκτήματά του.

Η μεταφορά της πληροφορίας, μέσω των τηλεπικοινωνιακών υποδομών, για να είναι σωστή, πρέπει να διακρίνεται από τα τρία Α :

Αποδοτικότητα, Αξιοπιστία, και Ασφάλεια.

Η αποδοτικότητα (efficiency), περιγράφει ότι ένα ΠΣ πρέπει να πετυχαίνει το μέγιστο επιθυμητό αποτέλεσμα σε σχέση με τους όποιους πόρους καταναλώνει για να το επιτύχει.

Η αξιοπιστία (Integrity), αναφέρεται στη μεταφορά του μυνήματος που βρίσκεται σε ψηφιακή μορφή bits, και που πρέπει να γίνεται χωρίς σφάλματα.

Η ασφάλεια (Security), αφορά την πληροφορία πρέπει να γίνεται γνωστή μόνο στα επιθυμητά σημεία που συμμετέχουν νόμιμα στην επικοινωνία.

Για τα δεδομένα θεωρείται απαραίτητο να τηρείται η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα (confidentiality, integrity,availability, ή αλλιώς γνωστές ως απαιτήσεις - CIA).

- Η εμπιστευτικότητα δηλώνει ότι η πληροφορία είναι προσβάσιμη μόνο σε όσους είναι εξουσιοδοτημένοι.

- Η ακεραιότητα αναφέρεται στην προστασία της ακρίβειας και της πληρότητας της πληροφορίας καθώς και στις μεθόδους πρόσβασης σε αυτή.

- Η διαθεσιμότητα υποδηλώνει την εξασφάλιση ότι οι εξουσιοδοτημένοι χρήστες θα έχουν πρόσβαση στην πληροφορία, και τους πληροφοριακούς πόρους όταν απαιτείται.

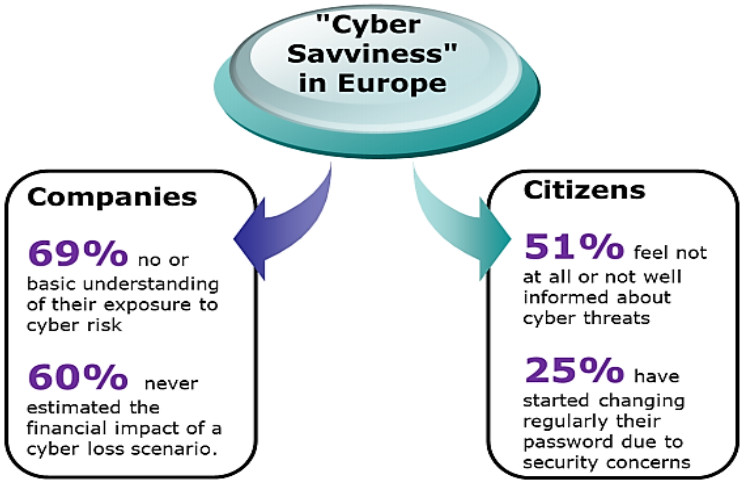
1.2 Αντικείμενο της διπλωματικής

Η ανάγκη για προστασία της ιδιωτικότητας, των προσωπικών δεδομένων, και της ασφάλειας των Πληροφορικών Συστημάτων (ΠΣ) και Επικοινωνιών, αναγνωρίζεται παγκοσμίως στις μέρες μας. Αυτή η ανάγκη γίνεται ακόμη πιο επιβεβλημένη στο χώρο της Υγείας, έναν κατεξοχήν πολύπλοκο και ευαίσθητο χώρο, που γίνεται ακόμα πιο σύνθετος με την είσοδο των νέων Τεχνολογιών

Πληροφορικής και Επικοινωνιών (ΤΠΕ) που σκοπό έχουν να τον υποστηρίξουν, να τον εξελίξουν, αλλά και να τον ελέγξουν.

Στόχος της διπλωματικής, είναι να μελετήσει τον έλεγχο της διαδικασίας εισαγωγής και εμπέδωσης των ΤΠΕ στο χώρο της υγείας, από τη σκοπιά της διαφύλαξης της ασφάλειας στα ΠΣΥ, και της προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας. Αυτό θα αυξήσει το αίσθημα της εμπιστοσύνης των ανθρώπων στην χρήση και επέκταση των νέων τεχνολογιών στα ΠΣΥ, που είναι και το τελικό ζητούμενο.

Πολλές μελέτες έχουν δείξει ότι επιχειρήσεις και οι πολίτες δεν είναι ικανοποιημένοι και έχουν ανησυχίες σχετικά με την κυβερνοασφάλεια των ΠΣ, όπως δείχνει και η σχετική μελέτη του ευρωβαρόμετρου, στην πιο κάτω εικόνα.



Sources: "Special Eurobarometer 464", 2017, Attitudes towards the impact of digitisation and automation on daily life" Eurobarometer 2017, Continental European Cyber Risk Survey 2016 Report

Εικόνα 1. Ευρωβαρόμετρο, πόσο ασφαλείς αισθάνονται πολίτες και οργανισμοί, με τον ψηφιακό κόσμο (3)

Προκειμένου να επιτευχθεί ο στόχος της διπλωματικής, ακολουθήθηκε η κάτωθι μεθοδολογία έρευνας:

Κατ΄αρχάς εντοπίσαμε ποιό είναι το πρόβλημα. Αυτό είναι ότι οι ανησυχίες για την ασφάλεια επηρεάζουν τις επιλογές των ευρωπαίων πολιτών, και τους θέτουν εμπόδια στο να εμπιστευτούν την ψηφιακή τεχνολογία, για σημαντικές

υπηρεσίες όπως υγεία, ενέργεια, μεταφορές κλπ, φοβούμενοι κάποιο σοβαρό ή/και δυσάρεστο επεισόδιο (3).

Στη συνέχεια θελήσαμε να δούμε τι είναι τα ΔΠΧ, ποια τα επιμέρους στοιχεία των ΠΣ και των Επικοινωνιών που θέλουμε να προστατέψουμε, και να εντοπίσουμε που πιθανώς υπάρχουν ευπάθειες και απειλές για αυτά αλλά και για τα ΔΠΧ, που διακινούνται ή βρίσκονται αποθηκευμένα σε αυτά.

Μετα εξετάσαμε ποιες νομοθετικές προβλέψεις υπάρχουν για να αντιμετωπίσουν το πρόβλημα, τόσο σε εθνικό, όσο και σε διεθνές επίπεδο, καθότι το διαδίκτυο είναι παγκόσμιο.

Μας απασχολούσε επίσης τι είναι ηλεκτρονικό έγκλημα, διαδικτυακό έγκλημα, και με ποια χαρακτηριστικά εμφανίζεται, επίσης ποιο είναι το προφίλ των δραστών, ποιες οι μέθοδοι τους, τα εργαλεία που χρησιμοποιούν, και οι σκοποί που θέλουν να εξυπηρετήσουν. Ποιο το κόστος των πράξεων τους για τα θύματα τους και τους οργανισμούς που προσβάλλουν.

Και τέλος πως μπορεί ένας οργανισμός, όπως π.χ. ένας μεγάλος υγιειονομικός σχηματισμός σαν αυτούς που απασχολούν εκατομμύρια εργαζόμενους και χρησιμοποιούν δισεκατομμύρια πολίτες να διαχειριστεί τον κίνδυνο.

Ποια τα πρότυπα, τα τεχνικά μέτρα, ποιες πολιτικές ασφάλειας, υπηρεσίες και ποιούς μηχανισμούς ασφάλειας θα πρέπει να χρησιμοποιήσει προκειμένου να μην υποστεί κυρώσεις από κάποια ενδεχόμενη αμέλεια ή εσκεμμένη πράξη ενάντια στην καλή λειτουργία του.

Για το πρόβλημα της ελαττωμένης εμπιστοσύνης των πολιτών ευθύνεται και το γεγονός ότι υπάρχουν πολλαπλές προσεγγίσεις και υποομάδες στα θέματα της κυβερνοασφάλειας, μέσα στην ίδια την ευρωπαϊκή κοινότητα, ακόμα και στα κράτη μέλη της. Ως αποτέλεσμα, οι ανησυχίες για την ασφάλεια επηρεάζουν τις επιλογές των Ευρωπαΐων πολιτών, και τους αποθαρρύνουν να εμπιστευτούν την ψηφιακή τεχνολογία, για σημαντικές υπηρεσίες όπως υγεία, ενέργεια, μεταφορές κλπ, φοβούμενοι κάποιο σοβαρό δυσάρεστο γεγονός (3).

Στην ανησυχία των πολιτών συντελεί επίσης και η εκρηκτική αύξηση των περιστατικών παραβίασης ΔΠΧ και κυβερνοεπιθέσεων στα ΠΣ, που παράλληλα δημιουργεί τεράστιο οικονομικό κόστος στις επιχειρήσεις και τους οργανισμούς.

Επομένως η ευρωπαϊκή και η παγκόσμια κοινότητα, θα πρέπει να δραστηριοποιηθεί και να επενδύσει σε θέματα ασφάλειας, τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο, καθώς και στη λήψη σχετικών μέτρων προς αυτή την κατεύθυνση, που να είναι κατανοητά στους πολίτες. Προς αυτή την κατεύθυνση στην Ευρώπη, μόλις ξεκίνησε να εφαρμόζεται ο Γενικός Κανονισμός για τα Προσωπικά Δεδομένα (ΓΚΠΔ), που στα Αγγλικά ονομάζεται General Data Protection Rule ή GDPR, όπως τείνει πλέον να γίνει και γνωστός. Στο παρελθόν υπήρχαν αντίστοιχοι νόμοι.

Για την συμμόρφωση σε αυτούς θα πρέπει ειδικοί επιστήμονες και τεχνικοί να εφαρμόζουν τεχνικά πρωτόκολλα, πρότυπα και πολιτικές αντιμετώπισης των προβλημάτων αυτών, συμμορφούμενοι προς αυτές τις νομοθετικές διατάξεις, και να παρακολουθούν συνεχώς την εφαρμογή και αποτελεσματικότητά των τεχνικών μέτρων. Πλήθος αναφορών υπάρχουν σχετικά, με τους κινδύνους που καλούνται να αντιμετωπίσουν και τα μέτρα προστασίας που πρέπει να εφαρμόσουν.

Στο κείμενο που ακολουθεί παρουσιάζονται τα αποτελέσματα της παραπάνω έρευνας που έχουν δομηθεί στα ακόλουθα κεφάλαια:

Στο πρώτο κεφάλαιο «Ιστορική ανασκόπηση» γίνεται μια σύντομη ανασκόπηση του τοπίου σχετικά με τη μυστικότητα των μυνημάτων και τις επικοινωνίες στο πέρασμα των αιώνων.

Το επόμενο κεφάλαιο που έχει τίτλο «Νομοθεσία και Διατάξεις» μελετά τα δικαιώματα, τα προβλήματα και τη νομοθεσία σχετικά με τα προσωπικά δεδομένα και την ασφάλεια των ΠΣ γενικότερα. Πιο συγκεκριμένα, εξετάζει κατα αρχήν το δικαίωμα προστασίας της ιδιωτικότητας και της νομοθετικής του κατοχύρωσης και εξασφάλισης. Επίσης τις αρμοδιότητες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), και τη χρήση βιομετρικών δεδομένων και τεχνολογιών για την ασφάλεια και προστασία

προσωπικών δεδομένων. Στη συνέχεια εξετάζει τις αρμοδιότητες της ανεξάρτητης εποπτικής αρχής «Ευρωπαίος Επόπτης Προστασίας Δεδομένων» καθώς και τον Γενικό Κανονισμό για την Προστασία Δεδομένων και τέλος το Νόμο 3418 του 2005 για το Ιατρικό Απόρρητο. Μια άλλη ενότητα του δεύτερου κεφαλαίου, εξετάζει την Ελληνική Νομοθεσία για την προστασία του απορρήτου από τον ποινικό κώδικα, και για την επεξεργασία ΔΠΧ. Στη συνέχεια εξετάζεται το πρόβλημα της δικαιοδοσίας στο Διαδίκτυο καθώς και της Νομικής ρύθμισης αυτού. Τέλος εξετάζεται η οδηγία 2016/1148 της Ευρωπαϊκής Ένωσης για την ασφάλεια δικτύων και Πληροφοριών καθώς και οι σχετικές συστάσεις του Οργανισμού Οικονομικής Σταθερότητας και Ανάπτυξης (ΟΟΣΑ).

Στο τρίτο κεφάλαιο «Πληροφοριακά Συστήματα» μελετώνται οι έννοιες των συστημάτων, της ασφάλειας αυτών από το σχεδιασμό, και της επιτυχούς διαλειτουργικότητας.

Στο τέταρτο κεφάλαιο «Το διαδίκτυο» αρχικά αναφέρομαστε στο πως φτάσαμε στην εποχή του διαδικτύου, τα πρωτόκολλα που διέπουν την ασφαλή λειτουργία του τόσο ενσύρματη όσο και ασύρματη, τα πρότυπα που πρέπει να εφαρμόζονται, το απλό διαχειριστικό πρωτόκολο δικτύου, τα προβλήματα και τα μέτρα προστασίας σχετικά με την ασφάλεια των ΠΣ που συνδέονται μέσω διαδικτύου, τις πολιτικές, υπηρεσίες και μηχανισμούς ασφάλειας σε επίπεδο δικτύου που πρέπει να εφαρμόζονται, την ανάγκη για μέτρα φυσικής προστασίας, επίσης στο ποια cookies είναι απαραίτητα για τη σύνδεση μας σε ένα δίκτυο και ποια από αυτά είναι κίνδυνος για τα ΔΠΧ του χρήστη. Τέλος σχετικές αναφορές γίνονται για την κινητή υγεία (m-health), την υπολογιστική νέφους και την πανταχού παρούσα υπολογιστική.

Στο πέμπτο κεφάλαιο «Διαχείριση ασφάλειας ΠΣΝ», αναλύονται τα προβλήματα σχετικά τη διαχείριση της ασφάλειας (security management), και του κινδύνου (risk management). Εξετάζουμε τους όρους ευπάθεια ΠΣ, απειλές, συνέπειες και τη συνάφεια τους. Αναφερόμαστε σε ISMS συστήματα, που συντελούν προς αυτό τον σκοπό, καθώς και στην σημασία της εσωτερικής απειλής και την υιοθέτηση μιας κουλτούρας ασφάλειας ΠΣ και ΔΠΧ, σε έναν οργανισμό. Τέλος σε μέτρα προστασίας όπως η ψηφιακή

υπογραφή, τα ψηφιακά πιστοποιητικά, οι έξυπνες κάρτες, η κρυπτογράφηση και ο κατακερματισμός μυνημάτων καθώς και στις χρήση αναχωμάτων πυροπροστασίας, αντιπυρική ζώνης, IDS κ.α.

Στο έκτο κεφάλαιο «Ηλεκτρονικό έγκλημα», ορίζονται οι έννοιες σχετικά με το ηλεκτρονικό έγκλημα, οι τύποι και τα χαρακτηριστικά των εγκλημάτων που σχετίζονται με το διαδίκτυο και τα ΠΣ, εξετάζονται τα προφίλ των εγκληματιών και οι μέθοδοι και οι κακόβουλες επιδιώξεις τους, καθώς και το αποτέλεσμα των πράξεων τους για τα θύματα.

Το έβδομο κεφάλαιο συγκεντρώνει τα συμπεράσματα αυτής της έρευνας, που εν συντομία είναι ότι με την εξασφάλιση της προστασίας των ΔΠΧ, και της ασφάλειας των ΠΣ, θα αυξηθεί η εμπιστοσύνη των πολιτών στην λειτουργία τους και θα διευρυνθεί η διείσδυση τους στον χώρο της υγείας.

Επίσης ότι αυτό θα επιτευχθεί με γνώση, ενημέρωση σε πολλούς επιστημονικούς και τεχνολογικούς τομείς, και όχι με την πολυδιάσπαση και συστηματική επιμεροποίηση τόσο καθηκόντων όσο και υπηρεσιών. Παράλληλα βέβαια θα πρέπει να υπάρχει καλή συνεργασία μεταξύ των διαφόρων ειδικών, και καλός συντονισμός των υπευθύνων τόσο σε επίπεδο οργανισμών, κράτους, όσο και διεθνώς.

Ένα άλλο συμπέρασμα είναι ότι οι επενδύσεις σε αυτό τον τομέα, θα οδηγήσουν στο να μειωθεί το οικονομικό κόστος για τους οργανισμούς υγείας που λαμβάνουν μέτρα μέσω της αποφυγή τυχόν ζημιών, αν γίνεται προηγούμενα σωστή διαχείριση κινδύνου.

Κεφάλαιο 2^{ο}: Νομοθεσία και Διατάξεις

2.1 Το δικαίωμα προστασίας της ιδιωτικότητας – τα ΔΠΧ

Για να υπάρχει κάποιο δικαίωμα, δεν αρκεί κάποιος να ισχυρίζεται ότι το έχει, πρέπει αυτό να κατοχυρώνεται και νομικά. Στην περίπτωση της ιδιωτικότητας και της προστασίας των ΔΠΧ, αυτό σίγουρα ισχύει και μάλιστα εκτεταμένα, και θα συζητηθεί στο παρών κεφάλαιο της εργασίας όπου θα εξεταστεί η σχετική νομοθεσία.

Η νομοθεσία σε ότι αφορά την προστασία της ιδιωτικότητας (privacy), καταρχάς στηρίχτηκε στην παγκόσμια διακήρυξη των δικαιωμάτων του ανθρώπου του ΟΗΕ, το 1948. Σύμφωνα με αυτή, για πρώτη φορά σε νομικό κείμενο στο άρθρο 12: κατοχυρώνεται το δικαίωμα προστασίας της ιδιωτικής ζωής του ατόμου, έναντι αυθαίρετων παρεμβάσεων από τρίτους και κυρίως του κράτους (4).

Οι πρώτες αναφορές που έμοιαζαν να αφορούν δικαιώματα υπήρξαν στην Αθηναϊκή Δημοκρατία το πολίτευμα της ισότητας (462 π.Χ. έως το 322 π.Χ.). Χρειάστηκε να περάσουν περισσότερο από δύο χιλιετίες για να ξαναπροβληθούν και πάλι αυτές οι έννοιες, στο σύνολο όλων των ανθρώπων αυτή τη φορά, από την Αμερικανική και τη Γαλλική Επανάσταση.

«Δεχόμαστε τις εξής αλήθειες ως αυταπόδεικτες, πως όλοι οι άνθρωποι δημιουργούνται ίσοι, και προικίζονται από τον Δημιουργό τους με συγκεκριμένα απαραβίαστα Δικαιώματα, μεταξύ των οποίων είναι το δικαίωμα στη Ζωή, το δικαίωμα στην Ελευθερία, και το δικαίωμα στην επιδίωξη της Ευτυχίας - Διακήρυξη της Ανεξαρτησίας των ΗΠΑ, 4 Ιουλίου 1776».

«Ο νόμος πρέπει να είναι ο ίδιος για όλους, ανεξάρτητα αν προστατεύει ή τιμωρεί. Εφόσον όλοι οι πολίτες είναι ίσοι απέναντι στο νόμο, μπορούν όλοι να μετέχουν το ίδιο και στα δημόσια αξιώματα, στις θέσεις και τις υπηρεσίες ανάλογα με τις ικανότητες τους, και χωρίς καμία άλλη διάκριση παρά αυτή που πηγάζει από την αρετή τους και το ταλέντο τους - Διακήρυξη των Δικαιωμάτων του Ανθρώπου και του Πολίτη, 26 Αυγούστου 1789».

Νωρίτερα στη Βρετανία το 1689 υπήρξε η αγγλική Διακήρυξη των Δικαιωμάτων (Bill of Rights), και η Αξίωση Δικαιωμάτων της Σκωτίας που κατέστησαν παράνομες πολλές καταπιεστικές κυβερνητικές ενέργειες (5) .

Τα ΔΠΧ προστατεύονται σύμφωνα με το πρόσθετο πρωτόκολλο στη σύμβαση 108 για τις εποπτικές αρχές και τη διασυνοριακή κίνηση δεδομένων. Με τη σύμβαση 108 ήδη από το 1981 (Strasbourg, 28.1.1981), το Συμβούλιο της Ευρώπης έχει καλέσει τα κράτη μέλη του, να παίρνουν μέτρα ώστε να προστατεύουν τους πολίτες από **αυτόματη επεξεργασία των προσωπικών τους δεδομένων** (που σύμφωνα με το άρθρο 2 αφορά: την ολική ή εν μέρει αποθήκευση, αριθμητική ή λογική εξεργασία, μεταβολή, διαγραφή, επανάκληση ή διάχυση αυτών) (6).

Η ιδιωτικότητα χαρακτηρίζεται σαν ένα θεμελιώδες δικαίωμα του ανθρώπου, σύμφωνα με το άρθρο 8 της Ευρωπαϊκής Συνθήκης για τα ανθρώπινα δικαιώματα. Σε αυτό αναφέρει ότι η ιδιωτικότητα και η οικογενειακή ζωή, το σπίτι και η αλληλογραφία κάποιου πρέπει να γίνονται σεβαστά (7).

Σε ευρύτερο πλαίσιο στο άρθρο 12 της Διακήρυξης των ανθρωπίνων δικαιωμάτων στο Παρίσι στις 10 Δεκεμβρίου το 1948, αναφέρεται ότι ο καθένας πρέπει να προστατεύεται από ανάμιξη στην ιδιωτικότητα του, την οικογένεια, τον οίκο και την αλληλογραφία του, καθώς και από επιθέσεις ενάντια στην υπόληψη και την φήμη του, και ότι η προστασία της ιδιωτικότητας θα πρέπει να θεωρείται απαραίτητο στοιχείο των δημοκρατικών κοινωνιών, και όχι απλά και μόνο ατομική αξία (8).

Παρομοίως ο χάρτης των θεμελιωδών δικαιωμάτων της Ευρωπαϊκής Ένωσης, με το άρθρο 7 ορίζει τον σεβασμό στην ιδιωτική και οικογενειακή ζωή της κατοικίας και της αλληλογραφίας του ανθρώπου, και προσθέτει ένα εξειδικευμένο άρθρο το 8 για την προστασία των προσωπικών δεδομένων. Οι δημόσιες αρχές δεν επιτρέπεται να παρεμβαίνουν σε αυτό το δικαίωμα, εκτός εαν επιβάλλεται από το νόμο και αποτελεί αναγκαιότητα στα πλαίσια μιας δημοκρατικής κοινωνίας, για την εθνική, την δημόσια ασφάλεια, την προάσπιση της τάξης, την οικονομική ευμάρεια της χώρας και την πρόληψη

ποινικών παραβάσεων ή την προστασία της υγείας και των δικαιωμάτων άλλων (9).

Η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ), στο άρθρο 8 αναφέρεται στο δικαίωμα να γίνεται σεβαστή η ιδιωτική και οικογενειακή ζωή, το σπίτι και η αλληλογραφία. Στο άρθρο 13 αναφέρεται στο **δικαίωμα πραγματικής προσφυγής**. Εάν τα δικαιώματα καταπατούνται, μπορεί κάποιος να προσφύγει γι' αυτό επισήμως στα δικαστήρια ή σε άλλα δημόσια σώματα.

Στο **άρθρο 34 αναφέρεται στις ατομικές προσφυγές για τα δικαιώματα.** Εάν τα δικαιώματα που περιλαμβάνονται στη Σύμβαση έχουν καταπατηθεί σε κάποιο κράτος, θα πρέπει πρώτα να γίνει προσφυγή σε όλες τις αρμόδιες εθνικές Αρχές. Εάν αυτό δεν αποδώσει, τότε θα πρέπει να γίνει προσφυγή απ' ευθείας στο Ευρωπαϊκό Δικαστήριο των Ανθρωπίνων Δικαιωμάτων στο Στρασβούργο (10).

Σύμφωνα με τη **Συνθήκη για τη λειτουργία της ευρωπαϊκής ένωσης (Σ.Λ.Ε.Ε),** και το άρθρο 16 παρ.1. κάθε πρόσωπο έχει δικαίωμα προστασίας των ΔΠΧ που το αφορούν. Επίσης με την παρ.2. το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, θεσπίζουν τους κανόνες σχετικά. Η τήρηση των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητων αρχών (11).

Στην Ελλάδα υπάρχουν σχετικές ανεξάρτητες αρχές, που ρυθμίστηκαν με τον **ν.3051/2002** (12), είναι η ΑΠΔΠΧ με το ν.2472/1997, ο συνήγορος του Πολίτη (ΣτΠ) που είναι συνταγματικά κατοχυρωμένος με το νόμο 2477/97, η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) που συστάθηκε με το Ν.3115/2003 (13). Η Εθνική Επιτροπή Τηλεπικοινωνιών Ταχυδρομείων (ΕΕΤΤ) είναι σχετική ανεξάρτητη αρχή όμως είναι νομοθετικά μόνο κατοχυρωμένη, και όχι συνταγματικά.

Επίσης τα ΔΠΧ προστατεύονταν εξειδικευμένα με την **οδηγία 95/46/ΕΚ** της 24/10/1995, και επίσης από την **2002/58/ΕΚ** της 12/7/2002 (σχετική με την επεξεργασία των ΔΠΧ και τη προστασία της ιδιωτικης ζωής στον τομέα των ηλεκτρονικών επικοινωνιών) που συγκεκριμενοποιούσε και συμπληρώνε την

95/46/ΕΚ σε πολλά σημαντικά ζητήματα όπως η μυστικότητα πληροφοριών, η αποστολή ηλεκτρονικών μηνυμάτων, η αποστολή σπαμ και η χρήση cookies.

Προβλέψεις σχετικές με τις διαδικασίες και τις τεχνικές και οργανωτικές εγγυήσεις για το πως μπορεί να γίνει η άρση του απορρήτου των επικοινωνιών, όταν απαιτείται σε θέματα εθνικής ασφάλειας, ή για την διακρίβωση εγκλημάτων, γίνονται με το **ΠΔ 47 του 2005** (14).

Η **οδηγία 2002/58/ΕΚ (ePrivacy),** ασχολείται με την επεξέργασια των προσωπικών δεδομένων, και την προστασία τους στην ψηφιακή εποχή. Ασχολείται με τα cookies και τις συσκευές παρακολούθησης, και θέτει κανόνες για το πως οι πάροχοι ηλεκτρονικών επικοινωνιών, θα πρέπει να παρέχουν τις υπηρεσίες τους και να διαχειρίζονται τα δεδομένα των συνδρομητών τους (15).

Στο άρθρο 4 ασχολείται με την ασφάλεια πληροφοριών, ενώ στο άρθρο 5 με **το απόρρητο των επικοινωνιών που διενεργούνται μέσω δημόσιου δικτύου επικοινωνιών** και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και με τα συναφή δεδομένων κίνησης.

Στο άρθρο 6 σχετικά με **τα Δεδομένα κίνησης** των συνδρομητών - χρηστών τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τον πάροχο δημόσιου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών, αναφέρει ότι **πρέπει να απαλείφονται**, **ή να καθίστανται ανώνυμα** όταν δεν είναι πλέον απαραίτητα για το σκοπό της μετάδοσης μιας επικοινωνίας,

Με το άρθρο 17 ζητήθηκε από τα κράτη μέλη την ενσωμάτωση της οδηγίας στο εθνικό δίκαιο και επίσης να θέσουν σε ισχύ τις αναγκαίες διατάξεις πριν από τις 31 Οκτωβρίου 2003.

Σχετικά με τα cookies γίνεται αναφορά και στο κεφάλαιο 4.7. της παρούσας εργασίας που αφορά το διαδίκτυο

Ο **ΝΟΜΟΣ 3471/2006** (ΦΕΚ 133/Α'/28.6.2006) – είναι ενσωμάτωση της Οδηγίας 2002/58/ΕΚ της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των

ΔΠΧ και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (16).

Στο άρθρο 4 αναφέρεται στο απόρρητο των ηλεκτρονικών επικοινωνιών και εξηγεί ότι επιτρέπει την καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης, όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής, με την προϋπόθεση ότι και τα δύο μέρη μετά από προηγούμενη ενημέρωση σχετικά με το σκοπό της καταγραφής, συγκατίθενται, όπως καθορίζει η ΑΠΔΠΧ. Ο τρόπος και ο χρόνος διατήρησης των καταγεγραμμένων συνδιαλέξεων και των συναφών δεδομένων κίνησης καθορίζεται επίσης από την ΑΠΔΠΧ.

Στο άρθρο 15 αναφέρεται στις ποινικές κυρώσεις όποιου παράνομα επεξεργάζεται ΔΠΧ ή τα θέτει σε διάθεση τρίτων, καθώς και εκείνες που αφορούν τους υπεύθυνους επεξεργασίας ή εκπροσώπους τους που δεν συμμορφώνονται με τις οδηγίες της ΑΠΔΠΧ, και αυτές συνίστανται σε κάθειρξη και χρηματική αποζημίωση.

Ο ν. 2472/1997 ενσωματώνει στο εθνικό δίκαιο την Οδηγία 95/46/ΕΚ, για την "Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα".

Σύμφωνα με τον αυτόν νοούνται ως:

α) ΔΠΧ, κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Όχι όμως τα στατιστικά συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.

β) "Ευαίσθητα δεδομένα" αναφέρει εκείνα που αφορούν τη φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, την υγεία, την κοινωνική πρόνοια και την ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων (17).

Με το άρθρο 15 του ν.2472/97, συνιστάται Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), για την εποπτεία της εφαρμογής του παρόντος νόμου και άλλων σχετικών ρυθμίσεων. Με την ΥΑ 130406/21.10.1997 (ΦΕΚ Β 967) ορίσανε σαν χρόνο έναρξης λειτουργίας της Αρχής την 10.11.1997.

Σύμφωνα με **το άρθρο 6** του ίδιου νόμου ένας υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει εγγράφως στην Αρχή ΔΠΧ, **ότι συστήνει και λειτουργεί αρχείο ή την έναρξη της επεξεργασίας καθώς και να απαντήσει σε μια λίστα ερωτημάτων** που μεταξύ άλλων περιλαμβάνουν και ποια μέτρα ασφαλείας και προστασίας λαμβάνει. Τα στοιχεία αυτά καταχωρούνται στο Μητρώο Αρχείων και Επεξεργασιών που τηρεί η Αρχή, που πρέπει να ενημερώνεται άμεσα από τον υπεύθυνο για κάθε μεταβολή αυτών.

Σύμφωνα με **το άρθρο 7**, απαγορεύεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων, εκτός εάν έχει δοθεί άδεια από την Αρχή και αυτό κάτω από κάποιες προϋποθέσεις, π.χ. το υποκείμενο των δεδομένων να έχει δώσει τη συγκατάθεση του, ή να είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή προβλεπόμενου από το νόμο συμφέροντος τρίτου, ή να αφορά θέματα υγείας και να εκτελείται από πρόσωπο που ασχολείται επαγγελματικά με την παροχή υπηρεσιών υγείας επιφορτισμένο με καθήκον εχεμύθειας ή συναφείς κώδικες δεοντολογίας (εφόσον όμως η επεξεργασία είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή τη διαχείριση υπηρεσιών υγείας), ή να εκτελείται από Δημόσια Αρχή και να είναι αναγκαία για λόγους εθνικής ασφάλειας ή για την εξυπηρέτηση των αναγκών εγκληματολογικής ή σωφρονιστικής πολιτικής ή για λόγους προστασίας της δημόσιας υγείας ή για την άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών. Αντίγραφο της σχετικής άδειας εάν τελικά δοθεί, καταχωρείται στο Μητρώο Αδειών που διατηρεί η Αρχή (17).

Με το **άρθρο 7 Α**, το άρθρο 7 εξειδικεύεται ακόμα περισσότερο για κάποιες περιπτώσεις που δεν χρειάζεται καν σχετική άδεια, όπως εαν αφορά

δεδομένα υγείας και γίνεται από ιατρούς ή άλλα πρόσωπα που παρέχουν υπηρεσίες υγείας και δεσμεύονται από επαγγελματικό απόρρητο.

Προκειμένου για **διασύνδεση αρχείων** γίνεται σχετική πρόβλεψη με το άρθρο 8, και αντίγραφα των αδειών διασύνδεσης καταχωρούνται στο **Μητρώο Διασυνδέσεων** που τηρεί η Αρχή.

Με το άρθρο 11, ο ν.2472/97 αναφέρεται στο **Δικαίωμα ενημέρωσης**. Το υποκείμενο των δεδομένων πρέπει να ενημερώνεται τουλάχιστον για: α. την ταυτότητα του υπεύθυνου επεξεργασίας β. το σκοπό της επεξεργασίας. γ. τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων. δ. ότι έχει το δικαιώμα πρόσβασης στα δεδομένα του.

Με το άρθρο 12 αναφέρεται στο **Δικαίωμα πρόσβασης**. Με το άρθρο 13 στο **Δικαίωμα αντίρρησης**. Οι αντιρρήσεις απευθύνονται εγγράφως στον υπεύθυνο επεξεργασίας και πρέπει να περιέχουν αίτημα για συγκεκριμένη ενέργεια, όπως «διόρθωση, προσωρινή μη χρησιμοποίηση, δέσμευση, μη διαβίβαση ή διαγραφή» (17). Στην παρ.3. αναφέρει ότι καθένας έχει δικαίωμα να δηλώσει στην Αρχή ότι δεδομένα που τον αφορούν δεν θέλει να είναι αντικείμενο επεξεργασίας από οποιονδήποτε για λόγους προώθησης, και πώλησης αγαθών ή παροχής υπηρεσιών εξ αποστάσεως. Η Αρχή τηρεί μητρώο με τα στοιχεία ταυτότητας αυτών των ανθρώπων.

Στο άρθρο 22 αναφέρεται στις ποινικές κυρώσεις αν παραβιαστούν κάποιοι από τους κανόνες (17).

2.1.1 **Η Αρχή Προστασίας Δεδομένων Προσωπικού χαρακτήρα (ΑΠΔΠΧ)**

Η ΑΠΔΠΧ συστάθηκε με το ν.2472/1997, με σκοπό την ΠΔΠΧ. Στη συνέχεια του κειμένου θα γίνει αναφορά στο αντικείμενο της. Η Αρχή συμμετέχει με εκπρόσωπό της στο **Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ).** Το ΕΣΠΔ είναι ένας ανεξάρτητος ευρωπαϊκός οργανισμός, ο οποίος συμβάλλει στη συνεκτική εφαρμογή των κανόνων προστασίας δεδομένων σε ολόκληρη την Ευρωπαϊκή Ένωση και προάγει τη συνεργασία μεταξύ των αρχών προστασίας δεδομένων της ΕΕ. Συστάθηκε με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ) και έχει την έδρα του στις Βρυξέλλες, ενώ αποτελεί τον διάδοχο της Ομάδας του άρθρου 29.

Σχετικός με το αντικείμενο της ΑΠΔΠΧ εκτός από το ν.2472, είναι και **ο νόμος 3917/2011** που αφορά τη διατήρηση δεδομένων σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, αλλά και τη χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και οι συναφείς διατάξεις (18).

Στην εφημερίδα της κυβερνήσεως δημοσιεύθηκε η κοινή Πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) ως προς τις υποχρεώσεις των παρόχων για την προστασία και ασφάλεια των δεδομένων σύμφωνα με τις διατάξεις του άρθρου 7 του ν. 3917/2011 (19).

Η Αρχή έχει τη δυνατότητα να επιβάλλει διοικητικές κυρώσεις, και με την απόφαση 60/2011 επέβαλε διοικητική κύρωση (προειδοποίηση) στο Ινστιτούτο Υγείας του Παιδιού επειδή τα μέτρα ασφαλείας του ήταν οργανωτικά και τεχνικά ελλιπή και διέρευσαν δεδομένα υγείας των νεογνών και παιδιών μετά από κλοπή Η/Υ του Ινστιτούτου (20).

2.2 Βιομετρικά δεδομένα

Βιομετρικά σύμφωνα με την ΑΠΔΠΧ, είναι τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται από βιομετρικά συστήματα. Έχουν ιδιαίτερη σημασία αφού αφορούν τα φυσικά χαρακτηριστικά ενός ανθρώπου (όπως δακτυλικά αποτυπώματα, γεωμετρία της παλάμης, ανάλυση της κόρης του ματιού, των χαρακτηριστικών του προσώπου, του DNA), και τα στοιχεία της συμπεριφοράς του (όπως υπογραφή, φωνή, τρόπο πληκτρολόγησης, τρόπο βαδίσματος), τα οποία τον προσδιορίζουν μοναδικά.

Οσον αφορά τις **βιομετρικές τεχνολογίες** και την διευρυνόμενη εφαρμογή τους σε διάφορους τομείς, αυτό δημιουργεί αρκετούς προβληματισμούς για την προστασία των δεδομένων που απασχολούν την ΑΠΔΠΧ. Η σημασία τους επίσης έγκειται στο ότι μπορούν να χρησιμοποιηθούν για τη πρόσβαση και τη διαβάθμηση φυσικών προσώπων σε ΠΣ, ως τεχνικές πιστοποίησης της ταυτότητας των ατόμων μέσω της ανάλυσης σταθερών χαρακτηριστικών τους για εφαρμογές που σχετίζονται με:

- Έλεγχο πρόσβασης σε φυσικούς χώρους.
- Ταυτοποίηση χρηστών εφαρμογών.
- Συνοριακό έλεγχο όπως συμβαίνει με τα βιομετρικά διαβατήρια.
- Παρακολούθηση χρόνου εργασίας προσωπικού εταιριών.
- Μηχανές αναζήτησης που αναγνωρίζουν αντικείμενα από φωτογραφίες.
- Εγκληματολογία για τον εντοπισμό δραστών.
- Εφαρμογές διαδικτύου (ηλεκτρονικό εμπόριο, ηλεκτρονική τραπεζική, κ.ά.).

Η συλλογή των βιομετρικών δεδομένων (π.χ. εικόνα του δακτυλικού αποτυπώματος, εικόνα της οφθαλμικής ίριδας, καταγραφή φωνής) γίνεται με την εγγραφή του ατόμου στο βιομετρικό σύστημα, από ένα ειδικό ηλεκτρονικό αισθητήρα (συνήθως μια κάμερα ή ένας σαρωτής) που μετατρέπει το

συγκεκριμένο βιομετρικό χαρακτηριστικό σε ηλεκτρονικό κώδικα τον οποίο αποθηκεύει («πρότυπο») αντιστοιχίζοντάς το με το συγκεκριμένο φυσικό πρόσωπο (21). Σε περίπτωση που το φυσικό πρόσωπο, προσπαθήσει αργότερα να αποκτήσει πρόσβαση κάπου χρησιμοποιώντας το βιομετρικό σύστημα, γίνεται έλεγχος της ταυτότητας του μέσω της επανάληψης της σάρωσης, τον εκ νέου υπολογισμό του ηλεκτρονικού κώδικα και τη σύγκρισή του με το αποθηκευμένο πρότυπο.

Ένα βιομετρικό πρότυπο μπορεί συνδυαζόμενο με άλλα μέτρα ελέγχου πρόσβασης όπως ένας κωδικός πρόσβασης (PIN), να παρέχει ακόμα μεγαλύτερη ασφάλεια. Σε αρκετές περιπτώσεις χρησιμοποιούνται και μικτά βιομετρικά συστήματα (multi-biometrics) που συνδυάζουν δυο ή περισσότερες βιομετρικές μεθόδους, για την επίτευξη ακόμα μεγαλύτερης πιστότητας και αξιοπιστίας.

Τα βιομετρικά συστήματα που αφήνουν ίχνη αποθηκεύοντας τα δεδομένα σε ένα μέσο, όταν είναι πάντα στην κατοχή του χρήστη (και όχι στη βιομετρική συσκευή ή σε μια κεντρική βάση δεδομένων) δημιουργούν λιγότερους κινδύνους για την παραβίαση των δικαιωμάτων του ατόμου.

Σύμφωνα με τις γενικές αρχές προστασίας των προσωπικών δεδομένων, είναι σημαντικός **ο τόπος αποθήκευσης των «προτύπων»**. Η αποθήκευση εξαρτάται κυρίως από το σκοπό εφαρμογής του βιομετρικού συστήματος καθώς και από το μέγεθος των προτύπων. Τα πρότυπα μπορούν να αποθηκευτούν:

- Στη μνήμη της βιομετρικής συσκευής.
- Σε κεντρική βάση δεδομένων.
- Σε πλαστικές ή έξυπνες κάρτες. Αυτός ο τρόπος επιτρέπει στους χρήστες να έχουν μαζί τους τα βιομετρικά τους στοιχεία.

Βιομετρικά συστήματα που επιτρέπουν την αποθήκευση των προτύπων σε μέσα που είναι υπό τον πλήρη έλεγχο του υποκειμένου, θεωρούνται πιο αποτελεσματικά για την προστασία των προσωπικών δεδομένων (22).

Η ΑΠΔΠΧ ασχολείται επίσης με ότι αφορά τις κάμερες για την προστασία προσώπων και αγαθών και στην περίπτωση νοσοκομείων, κλινικών, ιατρείων, διαγνωστικών κέντρων και λοιπών χώρων όπου παρέχονται υπηρεσίες υγείας, αναφέρει ότι επιτρέπεται να τοποθετούνται μόνο στα σημεία που ρητώς περιγράφονται στο άρθρο 20 παρ. 1 της **οδηγίας 1/2011/ΑΠΔΠΧ**, (επισημαίνεται ότι δεν επιτρέπεται με αυτές ο έλεγχος κίνησης σε χώρους αναμονής, διαδρόμους, θαλάμους ασθενών, θαλάμους εξέτασης) (23).

Με την οδηγία **1/2011/ΑΠΔΠΧ**, ρυθμίζεται το ζήτημα των συστημάτων βιντεοεπιτήρησης για το σκοπό της προστασίας προσώπων και αγαθών, αλλά και για το σκοπό της παροχής υπηρεσιών υγείας, όπως όταν αφορά την παρακολούθηση ψυχικά ή νοητικά ασθενείς που εκτιμάται ότι μπορούν να προκαλέσουν βλάβη στην υγεία τους ή σε τρίτους και την παρακολούθηση ασθενών σε Μονάδες Εντατικής Θεραπείας. Ο σκοπός αυτός μπορεί να επιδιώκεται μόνο από νοσηλευτικά ιδρύματα, ψυχιατρικά ιδρύματα, ιδρύματα περίθαλψης ατόμων με αναπηρίες και παρόμοιους φορείς παροχής υπηρεσιών υγείας.

Η παρακολούθηση πρέπει να πραγματοποιείται από πρόσωπα που δεσμεύονται από το επαγγελματικό απόρρητο, και να τελεί υπό τις ειδικότερες προϋποθέσεις που ορίζονται **στο ειδικό μέρος** της παρούσας Οδηγίας. Αναφέρει στο άρθρο 20 για τα νοσοκομεία, κλινικές, ιατρεία, φυσικοθεραπευτήρια, διαγνωστικά κέντρα ότι η λειτουργία συστήματος βιντεοεπιτήρησης σε νοσοκομεία, κλινικές, ιατρεία και λοιπούς χώρους που παρέχονται υπηρεσίες υγείας πρέπει να περιορίζεται μόνο στα σημεία εισόδου και εξόδου, στους χώρους ταμείων ή χώρους κρίσιμων εγκαταστάσεων (π.χ. ηλεκτρομηχανολογικές εγκαταστάσεις, αποθήκες ιατροφαρμακευτικού υλικού κλπ) όπου, δεν μπορεί να έχει πρόσβαση ένας επισκέπτης ή ασθενής. Οι κάμερες δεν επιτρέπεται σε καμία περίπτωση να ελέγχουν την κίνηση στις αίθουσες αναμονής, τα κυλικεία και τους χώρους εστίασης, τους διαδρόμους του νοσοκομείου, τους θαλάμους ασθενών, τους θαλάμους εξέτασης ή ιατρικών επεμβάσεων, τις τουαλέτες και τα λουτρά, τα

γραφεία ιατρών και τους χώρους εργασίας του λοιπού ιατρικού και νοσηλευτικού προσωπικού (23).

Καταγραφή των δεδομένων επιτρέπεται το πολύ για σαράντα οκτώ ώρες με σκοπό τη διερεύνηση συμβάντων υγείας από το αρμόδιο ιατρικό προσωπικό. Σε περίπτωση που συγκεκριμένα δεδομένα που είχαν καταγραφεί για τον σκοπό παροχής υπηρεσιών υγείας απαιτείται αργότερα να χρησιμοποιηθούν περαιτέρω για σκοπούς επιστημονικής έρευνας, είναι δυνατή η αποθήκευση τους σε ξεχωριστό αρχείο αφού προηγουμένως ανωνυμοποιηθούν (π.χ. με θόλωση του προσώπου του ασθενούς), και αφου πρώτα δοθεί (α) έγκριση της αρμόδιας επιστημονικής επιτροπής του νοσοκομείου και (β) προηγούμενη συγκατάθεση του ασθενούς ή του νομίμου εκπροσώπου του.

Με την **οδηγία Αρ. 115/2001**, η ΑΠΔΠΧ επίσης ρυθμίζει και τα θέματα επεξεργασίας προσωπικών δεδομένων των εργαζόμενων. Γίνεται αναφορά και στο θέμα της εισαγωγής και χρήσης (κλειστών) κυκλωμάτων παρακολούθησης, ηχοσκόπησης, βιντεοσκόπησης και άλλων συναφών συστημάτων σε χώρους εργασίας (24).

Το 2011 η ΑΠΔΠΧ, εξέδωσε **άδεια (ΓΝ/ΕΞ/350/31.03.2011)** στη Γενική Γραμματεία Κοινωνικών Ασφαλίσεων, στην ΥΠΕΔΥΦΚΑ και στη Διεύθυνση Μηχανογραφικών Εφαρμογών για τη συλλογή και την περαιτέρω επεξεργασία ιατρικών συνταγών, παραπεμπτικών ιατρικών εξετάσεων, ιατρικών διαγνώσεων, στο πλαίσιο της εφαρμογής της ηλεκτρονικής συνταγογράφησης σύμφωνα με το **Ν.3892/2010** (25).

2.3 European Data Protection Supervisor (EDPS)

Στην Ευρώπη με τον **Κανονισμό (ΕΚ) 45/2001** θεσμοθετήθηκε μία ανεξάρτητη εποπτική αρχή, ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων (EDPS), επιφορτισμένη με τον έλεγχο της επεξεργασίας ΔΠΧ στα κοινοτικά όργανα και οργανισμούς.

Ο επίτροπος EDPS ήταν μέλος της Ομάδας του Άρθρου 29 (Working Part 29) που προέκυψε σύμφωνα με τα προβλεπόμενα στο άρθρο 29 του ν.95/46/ΕΚ και συνίστατο επίσης και από ένα αντιπρόσωπο της οριζόμενης αρμόδιας αρχής από κάθε κράτος- μέλος, εως ότου τελικά αυτή καταργήθηκε και μεταξύ άλλων συμβούλευε όλα τα κοινοτικά όργανα και οργανισμούς για κάθε ζήτημα σχετικό με την επεξεργασία προσωπικών δεδομένων. Αναφορικά με τα συστήματα βιντεοεπιτήρησης ο EDPS είχε εκδώσει κείμενο οδηγιών. Η ομάδα εργασίας για το άρθρο 29, τον Μαϊο του 2018 αντικαταστάθηκε από την Ευρωπαϊκή επιτροπή για την προστασία των δεδομένων - **European Board of Data Protection (EBDP)** (26).

2.4 Ο Γενικός Κανονισμός Προστασίας των Δεδομένων (ΓΚΠΔ ή GDPR-General Data Protection Rule)

Ο Γενικός Κανονισμός Προστασίας των Δεδομένων (ΓΚΠΔ) της 27ης Απριλίου 2016, αφορά την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των ΔΠΧ, την ελεύθερη κυκλοφορία των δεδομένων αυτών, και την κατάργηση της οδηγίας 95/46/ΕΕ.

Στον ΓΚΠΔ αναφέρεται μεταξύ άλλων τα ακόλουθα ότι η προστασία που παρέχει ο κανονισμός ισχύει για όλα τα φυσικά πρόσωπα ανεξαρτήτως της υπηκόοτητας ή του τόπου κατοικίας του φυσικού προσώπου, επίσης αναφέρει ότι η προστασία δεδομένων δεν αφορά τις ανώνυμες πληροφορίες, ή δεδομένα που έχουν καταστεί ανώνυμα. Η προστασία επίσης δεν αφορά προσωπικά δεδομένα θανόντων, αλλά σε αυτή την περίπτωση τα κράτη μέλη μπορούν να προβλέπουν σχετικούς κανόνες (27).

Με την **Αρχή του Σκοπού** ο ΓΚΠΔ προβλέπει επίσης ότι ο υπεύθυνος επεξεργασίας των δεδομένων, θα πρέπει να συλλέγει μόνο τα επαρκή και αναγκαία δεδομένα για τους σκοπούς της εργασίας του, καθώς επίσης θα πρέπει να τα συντηρεί για το ελάχιστο χρονικό διάστημα και να θέτει προθεσμίες για τη διαγραφή τους ή περιοδική τους επανεξέταση. Τα προσωπικά δεδομένα που δεν είναι ακριβή ή θα διορθώνονται ή θα διαγράφονται.

Ο κανονισμός GDPR στο άρθρο 4, δίνει τους ακόλουθους σχετικούς ορισμούς σχετικά με τα ΔΠΧ: Δεδομένα προσωπικού χαρακτήρα χαρακτηρίζει κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (ή αλλιώς υποκείμενο των δεδομένων). Ως ταυτοποιήσιμο θεωρεί εκείνον του οποίου η ταυτότητα μπορεί να διαπιστωθεί, άμεσα ή έμμεσα, μέσω αναφοράς σε κάποιο αναγνωριστικό χαρακτηριστικό, όπως όνομα, αριθμό ταυτότητας, δεδομένα θέσης, ή και έναν ή περισσότερους παράγοντες που αφορούν τη σωματική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου (27).

Στο ίδιο άρθρο χαρακτηρίζει ως «ψευδωνυμοποίηση» την επεξεργασία ΔΠΧ με τρόπο τέτοιο ώστε τα δεδομένα μετά να μην μπορεί να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς να γίνει και χρήση προστατευμένων συμπληρωματικών πληροφοριών, αφού αυτές οι συμπληρωματικές πληροφορίες θα διατηρούνται χωριστά και θα υπόκεινται σε τεχνικά και οργανωτικά μέτρα ώστε να διασφαλίζεται ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

Επίσης «τρίτο» θεωρεί οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέα, που δεν είναι το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας, ο εκτελών την επεξεργασία, και τα πρόσωπα που υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα (27).

Με το Άρθρο 25 ο GDPR ζητά η προστασία των δεδομένων να γίνεται ήδη από το σχεδιασμό και εξ ορισμού.

Το υποκείμενο των δεδομένων σύμφωνα με το **άρθρο 65** του κανονισμού, μπορεί να ζητά τη διόρθωση των δεδομένων του καθώς να έχει και το **Δικαίωμα στη Λήθη**. Το τελευταίο αυτό δικαίωμα επεκτείνεται στο επόμενο άρθρο 66, καθιστώντας υπόχρεο τον αρχικό υπεύθυνο της επεξεργασίας που δημοσιοποίησε τα δεδομένα να ενημερώσει τους υπεύθυνους που τα πήρανε από αυτόν να διαγράψουν πιθανούς συνδέσμους ή αντίγραφα των εν λόγω δεδομένων.

Με το **άρθρο 63** ασχολείται με το **μηχανισμό συνεκτικότητας μεταξύ των μελών της Ένωσης**, ώστε οι εποπτικές αρχές να συνεργάζονται μεταξύ τους και εφόσον απαιτείται με την Επιτροπή.

Με το άρθρο 68 αναφέρεται στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων («Συμβούλιο Προστασίας Δεδομένων») ότι συστήνεται ως όργανο της Ένωσης και διαθέτει νομική προσωπικότητα.

Στο άρθρο 70 αναφέρεται στα καθήκοντα του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων.

Με **το άρθρο 83**, ζητά από τον υπεύθυνο επεξεργασίας δεδομένων, ή τον εκτελώντα αυτήν να συμμορφώνεται με τον κανονισμό και να τα διατηρεί ασφαλή, αξιολογώντας τους κινδύνους και λαμβάνοντας μέτρα, όπως πχ. **Κρυπτογράφηση**. Κάτι αντίστοιχο αναφέρει και αργότερα στο άρθρο 90.

Στο **άρθρο 85 περιγράφει πιθανές συνέπειες** που μπορεί να προκληθούν στα φυσικά πρόσωπα λόγω απώλειας του ελέγχου από τον υπεύθυνο επεξεργασίας των ΔΠΧ, όπως: **υποκλοπή ταυτότητας, διακρίσεις, οικονομική απώλεια, βλάβη της φήμης ή άλλο κοινωνικό ή οικονομικό μειονέκτημα**. Για αυτό τον λόγο αμέσως μόλις ο υπεύθυνος επεξεργασίας αντιληφθεί κάποια παραβίαση, θα πρέπει χωρίς δεύτερη σκέψη και όσο το δυνατόν εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος, να γνωστοποιεί την παραβίαση των ΔΠΧ στην αρμόδια εποπτική αρχή.

Στο **άρθρο 82 αναφέρεται στο δικαίωμα που έχει για αποζημίωση** από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία για τη ζημία που ενδεχομένως υπέστη το υποκείμενο των δεδομένων (27).

Στο **άρθρο 83 ο ΓΚΠΔ** γίνεται πιο συγκεκριμένος, και αναφέρει γενικούς όρους **επιβολής διοικητικών προστίμων**. Μεταξύ άλλων αναφέρει ότι η μη συμμόρφωση προς εντολή της εποπτικής αρχής, όπως αναφέρεται στο άρθρο 58 παράγραφος 2 επισύρει διοικητικά πρόστιμα έως 20.000.000€, ή σε περίπτωση επιχειρήσεων έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα ποιο είναι μεγαλύτερο.

Το άρθρο 94 καταργεί την οδηγία 95/46/ΕΚ 1. Η οδηγία 95/46/ΕΚ καταργήθηκε από τις 25 Μαΐου 2018 (27).

Με το **άρθρο 100, συνιστά την θέσπιση μηχανισμών πιστοποίησης, σφραγίδων και σημάτων προστασίας των δεδομένων**, κάτι που θα δίνει τη δυνατότητα στα υποκείμενα να αξιολογούν γρήγορα το επίπεδο συμμόρφωσης, του εκάστοτε υπευθύνου επεξεργασίας.

Σχετικά με τις εποπτικές αρχές, στο άρθρο 118 ο ΓΚΠΔ αναφέρει ότι η ανεξαρτησία τους δεν πρέπει να σημαίνει ότι δεν μπορούν να υπόκεινται σε οικονομικό ή δικαστικό έλεγχο. Στο άρθρο 164 αναφέρει ότι όσον αφορά τις εξουσίες των εποπτικών αρχών να εξασφαλίζουν από τον υπεύθυνο επεξεργασίας πρόσβαση σε ΔΠΧ και στις εγκαταστάσεις του, τα κράτη μέλη θα μπορούν να νομοθετούν ειδικούς κανόνες ώστε να διαφυλάσσεται παράλληλα το επαγγελματικό απόρρητο, στον βαθμό που αυτό είναι αναγκαίο λαμβάνοντας συγχρόνως υπόψιν και το δικαιώμα ΠΔΠΧ και την υποχρέωση επαγγελματικού απορρήτου (27).

Με το **άρθρο 171 εξηγεί ότι η οδηγία 95/46/ΕΚ θα πρέπει να καταργηθεί** με τον παρόντα κανονισμό. Μια Οδηγία είναι μια νομοθετική Πράξη (act), που είναι αποτέλεσμα μιας ευρωπαϊκής συνθήκης. Είναι δεσμευτικές για τα κράτη μέλη. Ως επακόλουθο αυτής της οδηγίας τα κράτη μέλη, νομοθετούν και διατηρούν γραφεία που παρακολουθούν την εφαρμογή της σε εθνικό επίπεδο, όμως διατηρούν αρκετό ελεύθερο πεδίο στο αν και πως θα την εφαρμόσουν. Αντιθετα ένας Κανονισμός είναι υποχρεωτικός και απαιτεί ακριβή συμμόρφωση, και έχει μεγαλύτερη ισχύ, γεγονός που εξηγεί την αναβαθμισμένη σημασία του ΓΚΠΔ σε σχέση με προηγούμενες νομοθετικές ρυθμίσεις.

Με το άρθρο 97 αναφέρει ότι η Ευρωπαϊκή Επιτροπή θα πρέπει να κάνει εκθέσεις την πρώτη εως τις 25 Μαΐου 2020, και έπειτα κάθε τέσσερα έτη που να αφορούν την αξιολόγηση, και την αναθεώρηση του παρόντος κανονισμού στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο. Οι εκθέσεις θα δημοσιοποιούνται.

Σύμφωνα με το **άρθρο 33,** η Ευρωπαϊκή Επιτροπή, **υποχρεώνει τους διαφόρους οργανισμούς να διενεργούν «εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων» (data protection impact assessment - DPIA)**, όπου η επεξεργασία περικλείει κινδύνους για τα προσωπικά δεδομένα των ατόμων. Η DPIA πρέπει να θεωρείται ένα κομμάτι από μια ευρύτερη διαδικασία διαχείρισης κινδύνων (risk management) που οφείλει να εφαρμόζει ένας οργανισμός (27).

Με σκοπό να εφαρμοστεί η DPIA σε ένα νέο ΠΣ επεξεργασίας δεδομένων οι Σιασιάκος et.al (28), διατύπωσαν μια διαδικασία σε βήματα στην οποία συμπεριέλαβαν τις κατάλληλες δραστηριότητες, ώστε η εκτίμηση των επιπτώσεων σχετικά με τη προστασία των δεδομένων να εκτελείται με όσον το δυνατόν περισσότερη ευκολία και μεθοδικότητα.

Τα βήματα ήταν τα εξής: 1) καθορισμός της ανάγκης για την διενέργεια της DPIA, 2) Τι είδους προσωπικά δεδομένα επεξεργάζονται, 3) Ποιος είναι ο υπεύθυνος επεξεργασίας, 4) Να εξεταστεί αν θα υπάρξουν αρνητικές επιπτώσεις για τα φυσικά πρόσωπα, 5) Να εξεταστεί αν έχουν ληφθεί μέτρα προστασίας, 6) Να γίνει προσδιορισμός της ομάδας εκτέλεσης της DPIA, 7) Να γίνει αναγνώριση και περιγραφή της εφαρμογής/διαδικασίας (Περιγραφή του σχεδιασμού της εφαρμογής και των διεπαφών της με άλλα συστήματα και της διαδικασίας, της ροής των δεδομένων, των εμπλεκόμενων χρηστών και των επιμέρους υποσυστημάτων της εφαρμογής), 8) Να γίνει σύσκεψη με τους εμπλεκόμενους (άτομα από το εσωτερικό και εξωτερικό του οργανισμού που θα επισημάνουν τους κινδύνους που αφορούν το δικό τους πεδίο εξειδίκευσης), 9) Να γίνει αναγνώριση των σχετικών κινδύνων (Αναγνώριση των συνθηκών και των πιθανών κινδύνων που μπορεί να απειλήσουν τα προσωπικά δεδομένα των ατόμων και να επηρεάσουν την ιδιωτικότητα τους), 10) Να γίνει διαχείριση των κινδύνων (αξιολόγηση των ενδεχόμενων απειλών και των δυσμενών γεγονότων που μπορεί να έχουν αρνητικές επιπτώσεις για τα φυσικά πρόσωπα και λήψη μέτρων αντιμετώπισης και ασφάλειας), 11) Να γίνει έλεγχος νομοθετικής συμμόρφωσης, και 12) τεκμηρίωση και ολοκλήρωση της σχετικής έκθεσης, καθώς και 13) εξωτερικός έλεγχος και ανασκόπηση (28).

2.5 Άλλες σχετικές διεθνείς νομοθεσίες

Σχετικά με τη διαχείριση προσωπικών δεδομένων γίνεται αναφορά και στον **Διεθνή Υγειονομικό κανονισμό** για τον περιορισμό της διεθνούς εξάπλωσης νόσων του 2005. Ο συγκεκριμένος κυρώθηκε στην Ελλάδα το 2011 με το ν.3991 και στο άρθρο 45 αναφέρει ότι οι υγειονομικές πληροφορίες που λαμβάνονται απο ένα κράτος μέλος θα πρέπει να διατηρούνται εμπιστευτικές και να διεκπεραιώνονται ανώνυμα, να είναι συναφείς και όχι υπερβολικές σε σχέση με το σκοπό που συλλέγονται, να διορθώνονται όταν είναι ανακριβείς ή να διαγράφονται, και να παρέχονται στο άτομο που ανήκουν χωρίς αδικαιολόγητη καθυστέρηση ή δαπάνη.

Σκοπός όλων είναι οι κίνδυνοι για την ιδιωτικότητα και την ασφάλεια να εντοπίζονται, και να αντιμετωπίζονται. Επίσης όσον αφορά τα δεδομένα να μπορούν τα κράτη και οι οργανισμοί να εγγυηθούν την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα (29).

Σχετικά με τις βάσεις δεδομένων (ΒΔ), στην Ευρώπη εφαρμόζεται **η οδηγία 96/9/ΕΟΚ** του ευρωπαϊκού κοινοβουλίου και του συμβουλίου της 11/3/1996, που αφορά τη νομική προστασία της βάσης δεδομένων, είτε σε ηλεκτρονική είτε σε συμβατική μορφή. Σύμφωνα με το άρθρο 3 οι βάσεις δεδομένων που λόγω της επιλογής ή της διευθέτησης του περιεχομένου τους αποτελούν πνευματικά δημιουργήματα, προστατεύονται με βάση **το δικαιώμα του δημιουργού**. Δημιουργός της βάσης, θεωρείται η εταιρεία που αναλαμβάνει τη δημιουργία της. Αυτή έχει το δικαίωμα να εκτελεί ή να επιτρέπει τις ακόλουθες πράξεις: Αναπαραγωγή αυτής της ΒΔ, τμηματικής ή και ολόκληρης, μετάφραση, προσαρμογή και αλλαγή διάταξης των στοιχείων που την απαρτίζουν, διανομή, ανακοίνωση, παρουσίαση στο κοινό των αποτελεσμάτων. Έχει επίσης το δικαίωμα να διανείμει, ή να αντιγράψει τη ΒΔ του στο κοινό.

Στο άρθρο 10 σχετικά με τη διάρκεια της προστασίας αναφέρει ότι το δικαίωμα που προβλέπεται στο άρθρο 7 ισχύει από την περάτωση της κατασκευής της ΒΔ και λήγει 15 χρόνια μετά την 1η Ιανουαρίου του έτους που

έπεται της ημερομηνίας περάτωσης. Σημαντικό είναι και το γέγονος ότι επιτρέπεται η εκτέλεση οποιασδήποτε από τις πιο πάνω πράξεις από οποιοδήποτε νόμιμο χρήστη της βάσης, ανάλογα με τα κατάλληλα δικαιώματα και εξουσιοδότηση που έχει (οπωσδήποτε αν οι ΒΔ αφορούν προσωπικά δεδομένα τότε ρυθμίζονται από την ΑΔΠΧ).

Στο άρθρο 13 (Διατήρηση άλλων διατάξεων) αναφέρει ότι η παρούσα οδηγία δεν θίγει τις διατάξεις που διέπουν μεταξύ άλλων το εμπορικό απόρρητο, την ασφάλεια, την εμπιστευτικότητα, την προστασία των δεδομένων προσωπικού χαρακτήρα και το σεβασμό της ιδιωτικής ζωής, καθώς και την πρόσβαση σε δημόσια έγγραφα ή το ενοχικό δίκαιο (30).

Με την **οδηγία 2009/24/ΕΚ** που είναι συνέχεια της παλαιότερης οδηγίας 91/250/ΕΕC, **ρυθμίζεται η νομική προστασία των λογισμικών προγραμμάτων** που διαχειρίζονται ΒΔ.

Σύμφωνα με το άρθρο 1, τα κράτη μέλη προστατεύουν τα προγράμματα Η/Υ, με **δικαιώματα πνευματικής ιδιοκτησίας** σαν λογοτεχνικά έργα κατά την έννοια της σύμβασης της Βέρνης για την προστασία των λογοτεχνικών και καλλιτεχνικών έργων.

Άρθρο 2. Δημιουργός προγράμματος Η/Υ είναι το φυσικό πρόσωπο, ή μια ομάδα φυσικών προσώπων που έχει δημιουργήσει το πρόγραμμα ή εάν το επιτρέπει η νομοθεσία του κράτους μέλους, το νομικό πρόσωπο που ορίζεται ως δικαιούχος από τη νομοθεσία αυτή.

Άρθρο 7. Ειδικά μέτρα προστασίας πρέπει να λαμβάνουν τα κράτη μέλη, βάσει της εθνικής τους νομοθεσίας, κατά κάποιου που προβαίνει: α) σε κυκλοφορία αντίγραφου προγράμματος Η/Υ γνωρίζοντας, ή έχοντας λόγους να πιστεύει, ότι πρόκειται για κλεψίτυπο β) σε κατοχή για σκοπούς εμπορικούς ένος αντιγράφου προγράμματος Η/Υ γνωρίζοντας, ή έχοντας λόγους να πιστεύει, ότι πρόκειται πάλι για κλεψίτυπο· γ) σε κυκλοφορία ή κατοχή για εμπορικούς σκοπούς μέσων, με σκοπό να διευκολύνουν την χωρίς άδεια αφαίρεση ή εξουδετέρωση κάθε τεχνικού συστήματος που μπορεί να εφαρμόζεται για την προστασία ενός προγράμματος Η/Υ.

Με το άρθρο 8, αναφέρει ότι η οδηγία δεν θίγει τις άλλες νομικές διατάξεις για τα διπλώματα ευρεσιτεχνίας, τα σήματα, τον αθέμιτο ανταγωνισμό, το εμπορικό απόρρητο, την προστασία των προϊόντων ημιαγωγών ή το δίκαιο των συμβάσεων (31).

2.6 Νόμος 3418 του 2005 - Ιατρικό Απόρρητο

Ο Νόμος 3418 του 2005 ή κώδικας ιατρικής δεοντολογίας αναφέρει στο άρθρο 13 του ότι το ιατρικό απόρητο και η εχεμύθεια, είναι προϋπόθεση στο πλαίσιο της άσκησης των καθηκόντων των γιατρών, και σύμφωνα με αυτό ο κάθε γιατρός οφείλει να λαμβάνει συγκεκριμένα μέτρα για την αυστηρή και αποτελεσματική του τήρηση, εποπτεύοντας ακόμα και τους άλλους απασχολούμενους και τους βοηθούς του στη φροντίδα του ασθενή.

Μόνο κάτω από συγκεκριμένες προϋποθέσεις επιτρέπεται η άρση αυτού του απορρήτου, όπως όταν συντρέχει κάποιο συγκεκριμένο νομικό καθήκον π.χ. όταν κάποιος απεργάζεται την τέλεση κάποιου κακουργήματος, σε μια περίπτωση διαφύλαξης κάποιου ουσιώδους δημοσίου συμφέροντος ή συμφέροντος του γιατρού ή κάποιου τρίτου που δεν γίνεται να διαφυλαχθεί διαφορετικά, και σε κάποιες ακόμα συγκεκριμένες περιπτώσεις. Η τήρηση του απορρήτου δεν παύει να ισχύει με το θάνατο του ασθενή (32).

Παρόμοια υποχρέωση νομικά έχει και ο νοσηλευτής σύμφωνα με το **άρθρο 11, του Προεδρικού Διατάγματος 216/2001** - ΦΕΚ 167/Α/25-7-2001- Κώδικας Νοσηλευτικής Δεοντολογίας, που αναφέρει: «Ο Νοσηλευτής οφείλει απεριόριστο σεβασμό στην ιδιωτική ζωή του ασθενή και να απέχει από κάθε πράξη ή παράλειψη που είναι δυνατό να βλάψει τον απόρρητο χαρακτήρα των κάθε είδους πληροφοριών των οποίων λαμβάνει γνώση κατά την άσκηση των καθηκόντων του».

Γίνεται αντιληπτό λοιπόν ότι και οι επαγγελματίες υγείας και μάλιστα οι γιατροί, στην εποχή του διαδικτύου και της διαλειτουργικότητας, δεν μπορούν να αποδεχτούν σχεδίαση ΠΣΥ, στα οποία οι ίδιοι θα καταχωρούν και θα συντηρούν στοιχεία, και τα οποία δεν θα διασφαλίζουν το απόρρητο για το οποίο εγκαλούνται. Τους ενδιαφέρει ενδεχομένως ακόμα και περισσότερο από τους ίδιους τους ασθενείς να διασφαλίζεται το απόρρητο καθώς οι

τελευταίοι θα μπορούν ενδεχομένως να προσφύγουν και κατά των γιατρών, στους οποίους θα μπορούσαν να επιβληθούν διοικητικές και νομικές κυρώσεις.

Παράλληλα στο **άρθρο 14 του ίδιου νόμου 3418** «Κώδικας Ιατρικής Δεοντολογίας 2005», νομοθετείται η υποχρέωση του γιατρού να κρατάει αρχείο σε ηλεκτρονική ή μη μορφή, που θα περιέχει δεδομένα σχετικά με τον ασθενή και την κατάσταση της υγείας του. Το αρχείο αυτό θα πρέπει να τηρείται σύμφωνα με τις διατάξεις του νόμου 2472/1997 (ΦΕΚ 50 Α'). Πρόσβαση σε αυτό το αρχείο μπορεί να έχει μόνο ο αθενής και οι κληρονόμοι του μετά θάνατο. Δεν επιτρέπεται η πρόσβαση σε τρίτο με εξαίρεση τις εισαγγελικές αρχές, ή μετά από αίτηση τρίτου που επικαλείται έννομο συμφέρον, ή σε άλλα όργανα της ελληνικής πολιτείας που με βάση τις καταστατικές τους διατάξεις έχουν τέτοιο δικαίωμα και αρμοδιότητα (32).

Στο άρθρο 47 **ο νόμος 2071/92 «εκσυγχρονισμός και οργάνωση συστημάτων υγείας»,** ΦΕΚ 15 Ιουλίου 1992 αναφέρεται σχετικά με τα δικαιώματα του νοσοκομειακού ασθενούς, ότι **ο ασθενής έχει το δικαίωμα της παροχής φροντίδας σε αυτόν** με τον οφειλόμενο σεβασμό στην ανθρώπινη αξιοπρέπεια του, και αυτό αφορά όχι μόνο τις ιατρικές υπηρεσίες αλλά εκτός των άλλων και την διοικητική και τεχνική εξυπηρέτηση και σε άλλο σημείο αναφέρεται σχετικά ότι ο ασθενής έχει το δικαίωμα της προστασίας όπου και όσο αυτό είναι δυνατόν της ιδιωτικής του ζωής, καθώς και να διασφαλίζεται ο απόρρητος χαρακτήρας των πληροφοριών και του περιεχομένου των εγγράφων που τον αφορούν, του φακέλου, των ιατρικών σημειώσεων, και των ευρημάτων (33).

2.7 Ελληνική νομοθεσία

Η Ελληνική νομοθεσία για την προστασία του απορρήτου και της επεξεργασίας ΔΠΧ δεν διαφέρει από την αντίστοιχη Ευρωπαϊκή. Αποτελεί έναν συνδυασμό διεθνών συνθηκών, συνταγματικών διατάξεων, διατάξεων του κοινού ποινικού δικαίου και νόμων που έχουν εκδοθεί βάσει κοινοτικών οδηγιών.

2.8 Στο Σύνταγμα της Ελλάδος

Στο Σύνταγμα της Ελλάδας περιλαμβάνονται μια σειρά από διατάξεις για την προστασία της ιδιωτικής σφαίρας του ατόμου.

Η θεμελιώδης διάταξη του άρθρου 2 παρ. 1, αναφέρει ότι «ο σεβασμός και η προστασία της αξίας του ανθρώπου αποτελούν πρωταρχική υποχρέωση της πολιτείας».

Σημαντικές διατάξεις περιλαμβάνονται στα άρθρα 9 και 19. Στο άρθρο 9, αναφέρεται ότι «η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη» διάταξη που απαγορεύει τη δημοσιοποίηση της ζωής του ατόμου.

Στο άρθρο 9Α ότι καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, σύμφωνα με τους νόμους.

Το άρθρο 19 προστατεύει το απόρρητο των επιστολών και την ελεύθερη ανταπόκριση και επικοινωνία. Βασικό στοιχείο της επικοινωνίας θεωρεί την μυστικότητα του περιεχομένου της. Ο νόμος ορίζει πως η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Επίσης ορίζει τα σχετικά με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης αρχής που διασφαλίζει το απόρρητο.

Στο άρθρο 5Α το Σύνταγμα αναφέρει επίσης ότι καθένας έχει δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας (ΚτΠ). Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά, καθώς και της παραγωγής, ανταλλαγής και διάδοσης τους αποτελεί υποχρέωση του Κράτους, τηρουμένων πάντοτε των άρθρων 9, 9Α και 19 (34).

2.8.1 **Στον Ποινικό Κώδικα**

Η προστασία του απορρήτου προβλέπεται από τα άρθρα 370, 370Α, 370Β και 370Γ του ποινικού κώδικα (ΠΚ).

Ο **νόμος 1805/1988** αφορά εγκλήματα που διαπράττονται γενικά με Η/Υ.. Πιο συγκεκριμένα με το άρθρο 3 του νόμου αυτού προστέθηκαν τρία νέα άρθρα στον ΠΚ τα 370Β, 370Γ και 386Α.

Η πιο ουσιαστική διάταξη όσον αφορά το χώρο του Διαδικτύου, περιλαμβάνεται στο άρθρο 370Γ, που τιμωρεί την χωρίς άδεια πρόσβαση σε δεδομένα αποθηκευμένα σε Η/Υ (35).

Ο **Νόμος υπ΄αριθμ 4411/3.8.2016** ψηφίστηκε για την κύρωση της σύμβασης για το έγκλημα στον Κυβερνοχώρο και μεταφέρει στο Ελληνικό δίκαιο την **οδηγία 2013/40/ΕΕ** για τις επιθέσεις κατά συστημάτων πληροφοριών (36).

Ο νόμος 4411 συνοδευόταν και από τροποποιήσεις στον Ποινικό Κώδικα (ΠΚ). Στο άρθρο 13 του ΠΚ «προστέθηκαν με το ν.4411, οι περιπτώσεις η΄ και θ΄ ως εξής: «η') **Πληροφοριακό σύστημα** είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών. **Ψηφιακά δεδομένα** είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία».

Στο άρθρο 292Β του ΠΚ για την **Παρακώλυση λειτουργίας ΠΣ,** προσθέτει ότι αν κάποιος χωρίς δικαίωμα παρεμποδίζει σοβαρά ή διακόπτει τη λειτουργία ΠΣ με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση

ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα αυτά, τιμωρείται με φυλάκιση μέχρι τριών (3) ετών.

Τά άρθρα 370 και 370Α του ΠΚ, αναφέρονται στην προστασία των επιστολών και την παραβίαση του απορρήτου των τηλεφωνημάτων και της προσωπικής συνομιλίας, αντίστοιχα.

Στο προστιθέμενο άρθρο 292Γ, ο ΠΚ αναφέρει ότι τιμωρείται με φυλάκιση μέχρι δύο (2) ετών κάποιος που χωρίς δικαίωμα και με σκοπό να διαπράξει τα εγκλήματα του άρθρου 292Β παράγει, πουλάει, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με κάποιο άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα Η/Υ, β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα τέτοια που μπορεί να χρησιμοποιηθούν για να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός ΠΣ.

Το άρθρο 370Β του ΠΚ παρέχει ικανοποιητική προστασία μόνο όμως για κρατικά, επιστημονικά και επαγγελματικά απόρρητα, αποκλείοντας τα ιδιωτικά απόρρητα.

Στο 2ο άρθρο του ν.4411/2016, στην παρ.1 αναφέρει ότι όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα Η/Υ, τιμωρείται με κάθειρξη μέχρι 6 μήνες και πρόστιμο από 290 εως 5.900 ευρώ. Στην παρ.2, ότι αν κάποιος παραβιάσει μέτρα ασφαλείας ή απαγορεύσεις και αποκτήσει πρόσβαση σε ένα ΠΣ ή σε στοιχεία που μεταδίδονται με τηλεπικοινωνιακά συστήματα τιμωρείται με φυλάκιση.

Στην παρ.3 αναφέρει ότι αν ο δράστης είναι υπάλληλος του νομίμου κατόχου τότε η προηγούμενη πράξη τιμωρείται μόνο εάν απαγορεύεται ρητά από τον εσωτερικό κανονισμό. Οι παραπάνω πράξεις διώκονται ύστερα από έγκληση.

Προστέθηκε και άρθρο 370Δ στον ΠΚ, το οποίο αφορά κάποιον που αθέμιτα παρακολουθεί αποτυπώνει μη δημόσιες διαβιβάσεις δεδομένων ή ηλεκτρομαγνητικές εκπομπές ενός ΠΣ με σκοπό αυτός ή άλλος να μάθει το περιεχόμενο τους, πράξη που τιμωρείται με φυλάκιση εως 10 έτη. Με την ίδια ποινή τιμωρείται όποιος κάνει χρήση της πληροφορίας ή του υλικού που έχει αποκτηθεί κατ΄αυτόν τον τρόπο.

Προστέθηκε επίσης το άρθρο 370 Ε, όπου με κάθειρξη εως 2 έτη τιμωρείται όποιος με σκοπό τη διάπραξη των εγκλημάτων που περιγράφονται στα άρθρα 370, παράγει πωλεί, προμηθεύεται, εισάγει, κατέχει, διακινεί α) συσκευές ή προγράμματα Η/Υ ή β) συνθηματικά ή παρεμφερή δεδομένα για την παράνομη πρόσβαση σε ένα ΠΣ.

Το Άρθρο 381Α του ΠΚ, αφορά τη φθορά ηλεκτρονικών δεδομένων, που τιμωρείται με φυλάκιση εως 3 έτη. Με το 381 Β, εως 2 έτη τιμωρείται όποιος εμπορεύεται, διακινεί συσκευές, προγράμματα, ή συνθηματικά που θα χρησιμοποιηθούν για τον σκοπό της φθοράς που περιγράφεται στο 381 Α.

Το άρθρο 386 Α, πραγματεύεται την απάτη με Η/Υ. Με αυτό το απόρρητο προστατεύεται υπό μία ευρεία έννοια. Δεν περιλαμβάνει μόνο δεδομένα τα οποία χαρακτηρίζονται από τη φύση τους απόρρητα, αλλά προστατεύεται και το δικαίωμα του νομίμου κατόχου των δεδομένων να αποκλείει σε άλλους την πρόσβαση σε όλα τα δεδομένα, που είναι αποθηκευμένα στον υπολογιστή του.

Αδικήματα όπως η διασπορά κακόβουλου λογισμικού και οι επιθέσεις άρνησης εξυπηρέτησης δεν μπορούν να τιμωρηθούν με βάση την ισχύουσα στην Ελλάδα νομοθεσία. Αυτό το κενό, αντιμετωπίζεται επί του παρόντος με την υπάρχουσα νομοθεσία για τα συμβατικά εγκλήματα, εαν ο εικονικός κόσμος του διαδικτύου θεωρηθεί απλά ως ένα ακόμα μέσο για τη διάπραξη εγκλημάτων (36).

Η Σύμβαση για το έγκλημα στον κυβερνοχώρο, με αντικείμενο την καταπολέμηση της εγκληματικής δραστηριότητας στους κόλπους του διαδικτύου, καταρτίστηκε στις **23/11/2001 στη Βουδαπέστη**. Έχει υπογραφεί από τα περισσότερα μέλη του Ευρωπαϊκού Συμβουλίου, τις ΗΠΑ, τον Καναδά, την Ιαπωνία και τη Ν.Αφρική. Κύρια στόχευση είναι η εναρμόνιση των νομοθεσιών των μελών στον τομέα της διαδικτυακής εγκληματικότητας, που στρέφεται κατά του απορρήτου, της ακεραιότητας και της διαθεσιμότητας των συστημάτων, Η/Υ, δικτύων και των ηλεκτρονικών δεδομένων, με σκοπό την πονικοποίηση αυτής και την υιοθέτηση μέτρων καταπολέμησης της τόσο σε τοπικό όσο και διεθνές επίπεδο (36).

Παλαιότερα εκτενείς αναφορές είχαν γίνει σχετικά με την παρακολούθηση, ακόμα και επικοινωνιών πολιτικών προσώπων. Ο **Ν.2225/1994 για την «προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας»** σχετίζεται με κάποιες πτυχές του ηλεκτρονικού εγκλήματος. Με αυτό φαίνεται η σημασία που αποδίδει η σύγχρονη πολιτική ηγεσία στα θέματα των πληροφοριακών συστημάτων συστήνωντας ειδική επιτροπή (37).

Με το άρθρο 1 του ν.2225/94 ιδρύεται "**Εθνική Επιτροπή Προστασίας του Απορρήτου των Επικοινωνιών**". Αποστολή της Επιτροπής είναι: α) η προστασία του απορρήτου των επιστολών και της τηλεφωνικής και κάθε άλλης μορφής τηλεπικοινωνιακής ανταπόκρισης ή επικοινωνίας κατά το άρθρο 19 του Συντάγματος και β) ο έλεγχος της τήρησης των όρων άρσης του απορρήτου που έθεσε η δικαστική αρχή.

Η Επιτροπή αυτή συγκροτείται:

α) από έναν αντιπρόεδρο της Βουλής ως πρόεδρο της, που ορίζεται από τον Πρόεδρο της Βουλής.

β) από ένα βουλευτή-εκπρόσωπο κάθε κόμματος που διαθέτει κοινοβουλευτική ομάδα κατά τον Κανονισμό της Βουλής. Ο εκπρόσωπος ορίζεται από τον αρχηγό του κάθε κόμματος με έγγραφη δήλωση που διαβιβάζεται στον Πρόεδρο της Βουλής και τον πρόεδρο της Επιτροπής,

γ) από ένα πρόσωπο εγνωσμένου κύρους και με ειδικές γνώσεις σε θέματα επικοινωνιών, ο οποίος ορίζεται από τον Πρόεδρο της Βουλής.

Η τελική συζήτηση της Επιτροπής για τη διαμόρφωση και για τη λήψη των αποφάσεων διεξάγεται χωρίς την παρουσία τεχνικών συμβούλων. Οι τεχνικοί σύμβουλοι, δεν έχουν αρμοδιότητα εκπροσώπησης, ούτε μπορούν να προβαίνουν ατομικά σε οποιαδήποτε προβλεπόμενη από το νόμο ενέργεια επικαλούμενοι γενική ή ειδική εντολή του αντίστοιχου μέλους της Επιτροπής.

Για κάθε έλεγχο που πραγματοποιεί και ειδικά για κάθε παραβίαση του άρθρου 19 του Συντάγματος την οποία διαπιστώνει, η Επιτροπή συντάσσει σχετική έκθεση. Επίσης στο τέλος κάθε χρόνου υποβάλλει στη Βουλή έκθεση

πεπραγμένων, στην οποία περιγράφει και αξιολογεί το έργο της, διατυπώνει γενικότερες παρατηρήσεις, επισημαίνει παραλείψεις και προτείνει τη λήψη μέτρων για την προστασία του απορρήτου (37).

Στο άρθρο 3 αναφέρει σχετικά με την άρση του απορρήτου για λόγους εθνικής ασφάλειας.

1. Αίτηση για άρση του απορρήτου μπορεί να υποβάλλει μόνο δικαστική ή άλλη πολιτική, στρατιωτική ή αστυνομική δημόσια αρχή στην αρμοδιότητα της οποίας υπάγεται το θέμα εθνικής ασφάλειας που επιβάλλει την άρση.

2. Η αίτηση υποβάλλεται προς τον Εισαγγελέα Εφετών του τόπου της αιτούσας αρχής ή του τόπου, όπου πρόκειται να επιβληθεί η άρση. Ο Εισαγγελέας Εφετών αποφασίζει μέσα σε είκοσι τέσσερις ώρες για την άρση ή όχι του απορρήτου με διάταξη του

Με το άρθρο 4 σχετικά με την άρση του απορρήτου για διακρίβωση εγκλημάτων αναφέρει ότι: η χρονική διάρκεια της άρσης του απορρήτου δεν μπορεί να υπερβαίνει τους δύο μήνες. Και ότι το περιεχόμενο της ανταπόκρισης ή επικοινωνίας, το οποίο έγινε γνωστό λόγω της άρσης του απορρήτου, καθώς και κάθε άλλο σχετικό με αυτή στοιχείο απαγορεύεται με ποινή ακυρότητας, να χρησιμοποιηθεί και να ληφθεί υπόψη ως άμεση ή έμμεση απόδειξη σε άλλη ποινική, πολιτική, διοικητική και πειθαρχική δίκη και διοικητική διαδικασία για σκοπό διαφορετικό από εκείνον που είχε καθορισθεί με τη διάταξη (37).

2.9 Το πρόβλημα της δικαιοδοσίας στο διαδίκτυο

Το πρόβλημα της δικαιοδοσίας στα εγκλήματα που τελούνται στο διαδίκτυο είναι πολύπλοκο, εξαιτίας της παγκοσμιότητας του.

Δικαιοδοσία: είναι η αρμοδιότητα ενός δικαστηρίου να δικάσει μια συγκεκριμένη υπόθεση αλλά συγχρόνως και η αντίστοιχη αρμοδιότητα των διωκτικών αρχών να διερευνήσουν μια εγκληματική συμπεριφορά. Η ανεύρεση της αρμοδιότητας του δικαστηρίου είναι συνυφασμένη με τον καθορισμό του τόπου τέλεσης του αδικήματος.

Θεωρίες καθορισμού τόπου τέλεσης διαδικτυακού εγκλήματος.

Για τον καθορισμό του τόπου τελέσης του αδικήματος υποστηρίζονται τέσσερις θεωρίες:

1. Η θεωρία του τόπου του αποτελέσματος. Τόπος τέλεσης του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.

2. Η θεωρία του τόπου ενέργειας. Ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου έχει τελεστεί η ενέργεια που προκάλεσε το άδικο αποτέλεσμα. Εφόσον η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, ο τόπος ενέργειας είναι αυτός όπου ολοκληρώθηκε η ενέργεια.

3. Η μικτή θεωρία. Τόπος τέλεσης του αδικήματος θεωρείται τόσο ο τόπος ενέργειας, όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.

4. Η θεωρία του βαρύνοντος τόπου. Σύμφωνα με την αυτήν την θεωρία ο τόπος του αδικήματος θεωρείται το κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Όμως υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας καθώς είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας. Η κρατούσα θεωρία στην Ελλάδα και στην Ευρώπη είναι η θεωρία του βαρύνοντος τόπου (38).

2.10 Νομική προσέγγιση του διαδικτύου

Κυρίαρχο νομικό ζήτημα για την αντιμετώπιση του ηλεκτρονικού εγκλήματος, αποτελεί η νομική ρύθμιση του Διαδικτύου. Έως σήμερα δεν υπάρχουν συγκεκριμένες διατάξεις που να ρυθμίζουν συνολικά τις προσφερόμενες μέσω του Διαδικτύου, υπηρεσίες. Επιπλέον οποιαδήποτε προσπάθεια ρύθμισης συναντά εμπόδια, που οφείλονται στο ότι στο χώρο του διαδικτύου υπάρχουν δύο διαφορετικές απόψεις. Υπάρχουν αυτοί που είναι υπέρ και αυτοί που είναι κατά της οποιασδήποτε προσπάθειας ρύθμισης του Διαδικτύου.

1) Τα επιχειρήματα υπέρ της ρύθμισης του Διαδικτύου είναι τα εξής:

• Απαιτείται η ρύθμιση του για τον έλεγχο του παράνομου περιεχομένου του.

• Δεν αποτελεί διαφορετικό μέσο επικοινωνίας σε σχέση με το ραδιόφωνο και την τηλεόραση, που υπόκεινται σε νομοθετικές ρυθμίσεις.

• Υπάρχει πολύ επιβλαβές υλικό σε αυτό, όπως και αυξανόμενη εγκληματική δραστηριότητα, που γεννά υποχρέωση στην πολιτεία για έλεγχο και αντιμετώπισή της.

• Οι περισσότεροι δικαιούχοι (stakeholders) ενός ΠΣ, απαιτούν κάποια μορφή ρύθμισης για την προστασία των δεδομένων και των περιουσιακών δικαιωμάτων τους απέναντι σε επιθέσεις κακόβουλων χρηστών.

2) Τα επιχειρήματα εναντίον οποιασδήποτε μορφής ρύθμισης είναι:

• Η ελευθερία του λόγου που προσφέρει είναι απόλυτο δικαίωμα κάθε πολίτη, προστατευμένο από συνταγματικές διατάξεις.

• Διαφέρει από τα άλλα μέσα επικοινωνίας, διαθέτοντας ιδιαίτερα χαρακτηριστικά όπως η ελευθερία, η ειλικρίνεια και ο πειραματισμός και η ανοικτότητα.

• Το Διαδίκτυο δεν μπορεί να ρυθμιστεί, διότι είναι τεράστιο και παγκόσμιο και οποιαδήποτε προσπάθεια, θα έρχεται πάντοτε αντιμέτωπη με το ζήτημα της λογοκρισίας (38).

Καθένας εξετάζοντας αυτά τα επιχειρήματα μπορεί να βγάλει τα συμπεράσματα του, όμως όπως παρουσιάζεται το θέμα στην παρούσα εργασία ρύθμιση χρειάζεται.

2.11 Οδηγία (ΕΕ) 2016/1148 για την ασφάλεια δικτύων και ΠΣ (NIS)

Σύμφωνα με την **Οδηγία (ΕΕ) 2016/1148 για την ασφάλεια δικτύων και πληροφοριών** (σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση), ως Ασφάλεια Συστημάτων Δικτύου και Πληροφοριών**,** ορίζεται η ικανότητα

συστημάτων δικτύου και πληροφοριών να αντιμετωπίζουν αξιόπιστα ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που βρίσκονται αποθηκευμένα, μεταδίδονται ή υποβάλλονται σε επεξεργασία, ή ενέργειες που πλήττουν συναφείς υπηρεσίες που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών (39).

Με το άρθρο 7 ζητά από κάθε κράτος μέλος να θεσπίσει εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών. Επίσης ζητάει από τα κράτη να κοινοποιούν την εθνική στρατηγική τους για την ασφάλεια συστημάτων δικτύου και πληροφοριών στην Επιτροπή (Κομισιόν), με τη δυνατότητα όμως να εξαιρούν από την κοινοποίηση αυτή στοιχεία της στρατηγικής που συνδέονται με την εθνική ασφάλεια.

Με το άρθρο 9 ζητά να δημιουργηθούν ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT).

Με το άρθρο 11 ζητά να δημιουργηθεί ομάδα συνεργασίας με σκοπό την υποστήριξη και τη διευκόλυνση της στρατηγικής συνεργασίας και την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών, την ανάπτυξη της αξιοπιστίας και της εμπιστοσύνης, και την επίτευξη ενός κοινού υψηλού επιπέδου ασφάλειας συστημάτων δικτύου και πληροφοριών στην Ένωση. Η ομάδα συνεργασίας θα πρέπει να απαρτίζεται από αντιπροσώπους των κρατών μελών, την Επιτροπή, και τον ENISA.

Με το άρθρο 12 ζητά να δημιουργηθεί δίκτυο εθνικών CSIRT. Το ευρωπαϊκό δίκτυο CSIRT να απαρτίζεται από αντιπροσώπους των CSIRT των κρατών μελών και την CERT-EU. Η Επιτροπή θα συμμετέχει στο δίκτυο CSIRT σαν παρατηρητής. Ο ENISA θα παρέχει τη γραμματειακή υποστήριξη και την ενεργή υποστήριξη της συνεργασίας αυτής μεταξύ των CSIRT.

Με το άρθρο 14, αναφέρεται στις απαιτήσεις ασφάλειας και στην κοινοποίηση συμβάντων. Ζητά οι φορείς εκμετάλλευσης βασικών υπηρεσιών υπό την επίβλεψη των αντίστοιχων κρατών-μελών να παίρνουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων, σε

ότι αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών που διατηρούν.

Ειδικότερα ως **φορέα εκμετάλλευσης βασικών υπηρεσιών**, θεωρεί κάθε δημόσια ή ιδιωτική οντότητα που εκπληρώνει τα κριτήρια που ορίζονται στο άρθρο 5 παράγραφος 2 ως εξής: α) παρέχει υπηρεσία ουσιώδη για τη διατήρηση κρίσιμων κοινωνικών και/ή οικονομικών δραστηριοτήτων· β) η παροχή της υπηρεσίας της στηρίζεται σε συστήματα δικτύου και πληροφοριών· και γ) τυχόν συμβάν θα προκαλούσε σοβαρή διατάραξη της παροχής της εν λόγω υπηρεσίας. **Ως τέτοια οντότητα για το χώρο της Υγείας περιλαμβάνει μεταξύ άλλων νοσοκομεία και ιδιωτικές κλινικές** (39).

Με το άρθρο 18 αναφέρεται στο **θέμα της δικαιοδοσίας και εδαφικότητας**. Σύμφωνα με το άρθρο ένας πάροχος ψηφιακών υπηρεσιών θεωρείται ότι υπόκειται στη δικαιοδοσία του κράτους μέλους στο οποίο έχει την κύρια εγκατάσταση του. Θεωρείται ότι έχει την κύρια εγκατάστασή του στο κράτος μέλος που έχει την έδρα του. Επίσης ένας πάροχος ψηφιακών υπηρεσιών μη εγκατεστημένος στην Ένωση αλλά που προσφέρει υπηρεσίες εντός της Ένωσης θα πρέπει να ορίζει αντιπρόσωπο στην Ένωση. Ο πάροχος ψηφιακών υπηρεσιών θεωρείται ότι υπόκειται στη δικαιοδοσία του κράτους μέλους στο οποίο είναι εγκατεστημένος ο αντιπρόσωπος.

Με το άρθρο 23, αναφέρει ότι θα γίνει επανεξέταση της διαδικασίας. Έως τις 9 Μαΐου 2019, η Επιτροπή θα υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο, στην οποία αξιολογεί τη συνοχή των προσεγγίσεων των κρατών μελών.

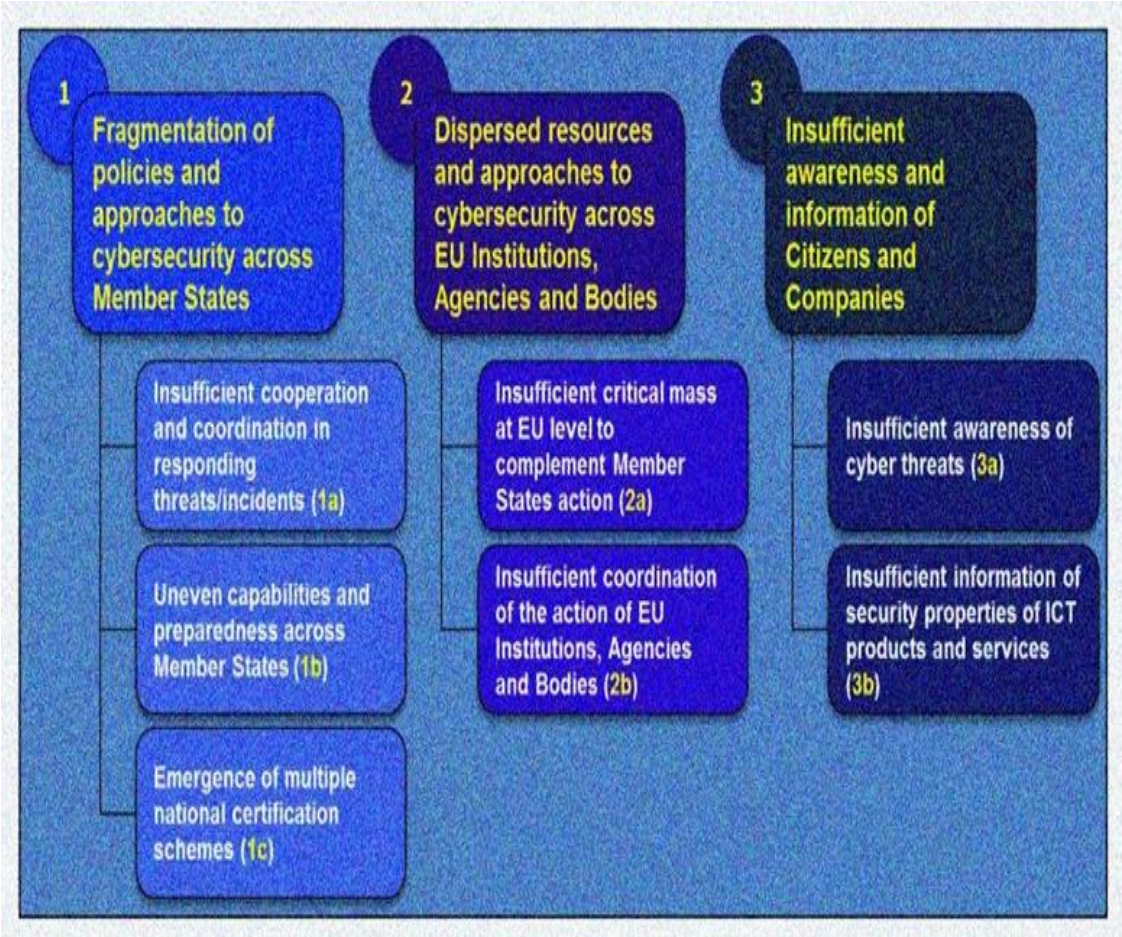
Με το άρθρο 25, καταστά σαφή την υποχρέωση μεταφοράς της οδηγίας στο εθνικό δίκαιο. Τα κράτη μέλη θα πρέπει να θεσπίσουν και δημοσιεύσουν έως τις 9 Μαΐου 2018 τις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις προκειμένου να συμμορφωθούν με την παρούσα οδηγία. Θα πρέπει να ανακοινώνουν αμέσως στην Επιτροπή τις εν λόγω διατάξεις, και να έχουν θέση τα μέτρα αυτά σε εφαρμογή ήδη από τις 10 Μαΐου 2018 (39).

Σύμφωνα με το ευρωπαϊκό κέντρο πολιτικής στρατηγικής: Η ομάδα αντιμετώπισης εκτάκτων αναγκών της ΕΕ (CERT-EU/Computer Emergency Response Teams) διαθέτει περιορισμένους πόρους (30 άτομα) και εξαιτίας αυτού μπορεί να παρέχει τις υπηρεσίες της μόνο στα θεσμικά όργανα της ΕΕ. Σε εθνικό επίπεδο οι δομές αυτών των ομάδων διαφέρουν σημαντικά τόσο ως προς τη μορφή όσο και ως προς τη λειτουργία τους. Έτσι παρόλο που υπάρχει κάποιος βαθμός τεχνικής συνεργασίας μεταξύ των ευρωπαϊκών ομάδων CERT, μόνο 10 κράτη μέλη εκπροσωπούνται σήμερα σε έναν περιορισμένο κύκλο, παράλληλα με την CERT-ΕΕ και τις αντιπροσωπείες της Νορβηγίας και της Ελβετίας. Τα νέα μέλη γίνονται δεκτά μόνο κατόπιν αιτήσεως και εφόσον θεωρούνται ότι έχουν επαρκώς ανεπτυγμένες δυνατότητες.

Εκτός από αυτές τις επιχειρησιακές ομάδες, η ΕΕ έχει συστήσει έναν Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), ο οποίος λειτουργεί ως το σχετικό **κέντρο εμπειρογνωμοσύνης** εντός της Ένωσης. Με προσωπικό 65 ατόμων, ο κύριος στόχος του Οργανισμού είναι να ευαισθητοποιήσει τα κράτη μέλη σχετικά με τα θέματα ασφάλειας στον κυβερνοχώρο, να υποστηρίξει την ανάπτυξη ευρωπαϊκών και εθνικών στρατηγικών για την ασφάλεια στον κυβερνοχώρο και να διευκολύνει την ανάπτυξη ικανοτήτων και τη συνεργασία (40).

Η ENISA καλείται να συμβάλλει στην επίλυση των ακόλουθων τριών σοβαρών προβλημάτων: πρώτο **την πολυδιάσπαση πολιτικών και προσεγγίσεων στην κυβερνοασφάλεια των Ευρωπαϊκών κρατών**, δεύτερο **τις πολυσχιδείς και ασυντόνιστες προσεγγίσεις** από ιδρύματα, αρμόδιους φορείς κλπ, και τρίτο την **ανεπαρκή πληροφόρηση των πολιτών και των εταιρειών στην κοινότητα.**

Καταναλώνονται πολλοί πόροι στην κοινότητα που είναι ενγένει ασυντόνιστοι, υπάρχει μια δαιδαλώδης γραφειοκρατία που δεν μπορεί να συγκροτηθεί σε ένα εύκολα διακριτό πλαίσιο



Εικόνα 2. Τα τρία προβλήματα της ENISA **(3)**

Από την άποψη της αστυνόμευσης υπάρχει το Ευρωπαϊκό Κέντρο για την καταπολέμηση του εγκλήματος του κυβερνοχώρου (EC3) **της Europol** με προσωπικό 52 άτομα, που παρέχουν σημαντική επιχειρησιακή υποστήριξη στις εθνικές αρχές των κρατών μελών για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Επίσης το κέντρο αυτό έχει καταστεί βασικός κόμβος εμπειρογνωμοσύνης σε επιχειρήσεις ενάντια στην εγκληματικότητα στον κυβερνοχώρο, π.χ. **παρέχοντας υπηρεσίες πληροφορικής, δικανική ανάλυση, νομική βοήθεια και εξειδικευμένη υποστήριξη** (3).

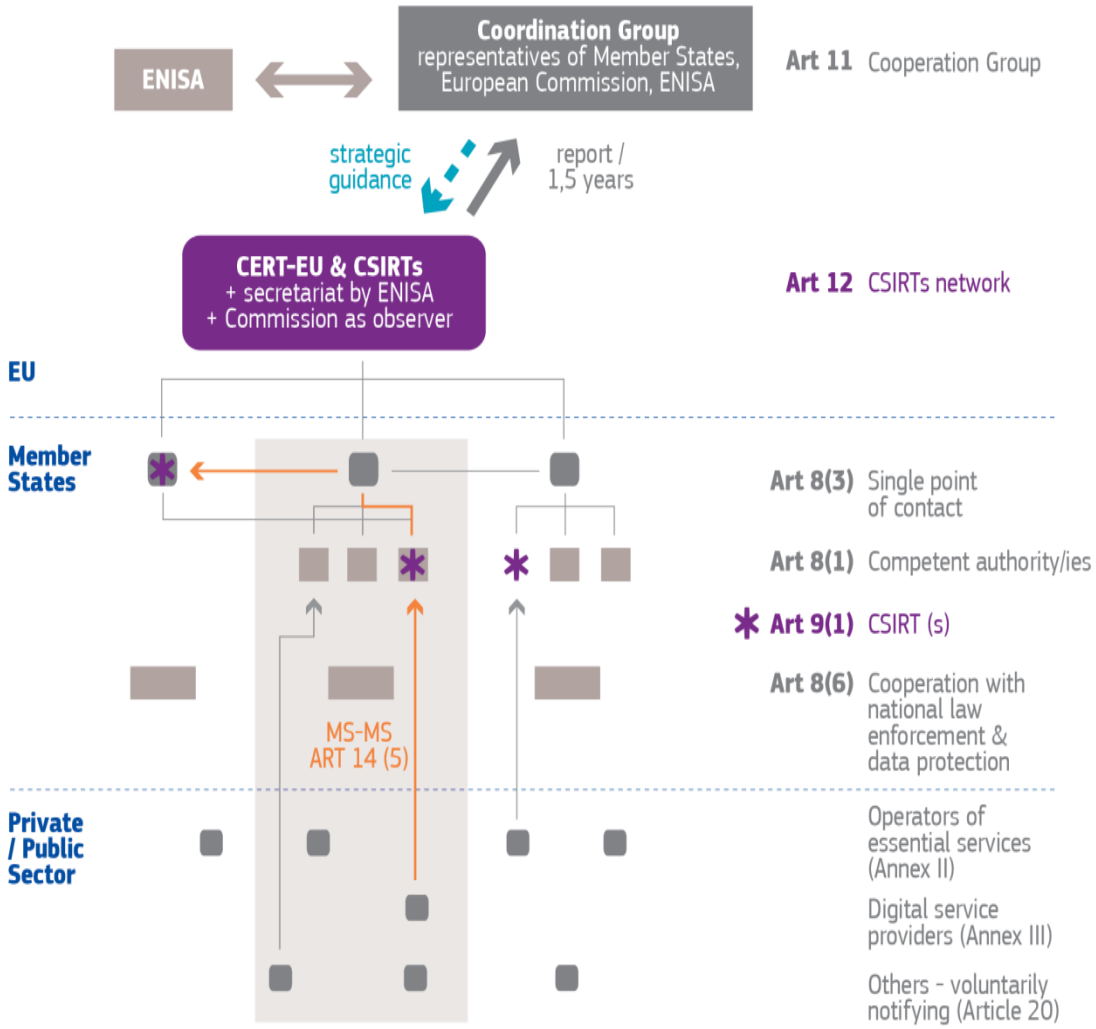
Στα τέσσερα χρόνια από τη δημιουργία του το 2013, το Ευρωπαϊκό Κέντρο για την καταπολέμηση του κυβερνοχώρου της Europol, βοήθησε να εξαλειφθούν πολλές επιχειρήσεις εγκληματικότητας στον κυβερνοχώρο, από

οικονομικούς απατεώνες έως δίκτυα σεξουαλικής εκμετάλλευσης παιδιών. Εντούτοις, λόγω της σημασίας και της αναγνώρισης που έχει αποκτήσει, θα χρειαστεί να ενισχυθούν σημαντικά οι πόροι του.

Περαιτέρω σχετικές υπηρεσίες παρακολούθησης ασφάλειας λειτουργούν κυρίως σε εθνικό επίπεδο αν και υπάρχει συνεργασία σε ευρωπαϊκό επίπεδο. Το κύριο σημείο σύνδεσης με τα ευρωπαϊκά θεσμικά όργανα είναι το Κέντρο Πληροφοριών (Intelligence Centre - 3 άτομα), το οποίο βρίσκεται στην **Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης** (ΕΥΕΔ)- eEuropean External Action Service.

Τέλος ρόλο έχουν και **διπλωματικές υπηρεσίες,** και εκείνες που σχετίζονται με την άμυνα. Αποτελούνται από μια ομάδα 3 ατόμων στην Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης, που επικεντρώνεται στις διπλωματικές απαντήσεις σε κυβερνοεπιθέσεις και στην βελτίωση των ικανοτήτων αντιμετώπισης περιστατικών σε τρίτες χώρες, καθώς και από άλλα 3 άτομα στην Ευρωπαϊκό Οργανισμό Άμυνας - **European Defence Agency (EDA).** Επίσης υπάρχει το Στρατιωτικό Επιτελείο της ΕΕ (3 άτομα), για τον στρατιωτικό στρατηγικό σχεδιασμό των επιχειρήσεων και των αποστολών της **Κοινής Πολιτικής Ασφάλειας και Άμυνας (ΚΠΑΑ).**

Η ύπαρξη διαφορετικών ρυθμίσεων και προσεγγίσεων όσον αφορά την ασφάλεια του κυβερνοχώρου, και η ανομοιογένεια των επιπέδων ωριμότητας της στα κράτη μέλη, προβάλλουν περαιτέρω εμπόδια στην αποτελεσματική συνεργασία, κάτι που φαίνεται για παράδειγμα από τον περιορισμένο αριθμό κρατών μελών που συμμετέχουν στην Ομάδα ευρωπαϊκών κυβερνήσεων CERT (3).



***Εικόνα 3. Δομή και συνεργασίες φορέων στην Ε.Ε, για την κυβερνοασφάλεια* (3)**

Σχετικά με τη νομοθεσία για τα δίκτυα σύμφωνα με την κα Λιανού (38):

Στην Ελλάδα έως το 1990, οι υπηρεσίες που στηρίζονταν στην πληροφορική παρέχονταν μονοπωλιακά από τον ΟΤΕ. Το ίδιο συνέβαινε και σε άλλες ευρωπαϊκές χώρες. Το τοπίο διαφοροποιήθηκε με πρωτοβουλία της Ευρωπαϊκής Κοινότητας, η οποία με δύο **Οδηγίες την 90/38794** και την **90/38895** κατάργησε το μονοπώλιο των εθνικών τηλεπικοινωνιακών οργανισμών, δίνοντας τη δυνατότητα σε οποιονδήποτε φορέα να προσφέρει τηλεπικοινωνιακές υπηρεσίες.

Η προσαρμογή της ελληνικής νομοθεσίας προς τις παραπάνω οδηγίες της Ευρωπαϊκής Κοινότητας προήλθε, κατ' αρχήν, με τον **ν. 2075/92**. Ο νόμος αυτός πολύ σύντομα καταργήθηκε με τον νέο ν.2246/94 και στη συνέχεια με τον **ν.2867/2000** που ισχύει και σήμερα.

Με τον νόμο αυτό ιδρύθηκε ρυθμιστική αρχή, η «Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων», με σκοπό τη διασφάλιση των συμφερόντων των χρηστών του Διαδικτύου. Η αρχή αυτή έχει τη δυνατότητα να ελέγχει τους πάροχους τηλεπικοινωνιακών υπηρεσιών και να επιβάλλει κυρώσεις σε περίπτωση παραβίασης συγκεκριμένων δικαιωμάτων των χρηστών, όπως η διατήρηση του απόρρητου χαρακτήρα των επικοινωνιών τους (36).

Σύμφωνα με τον **νόμο 4070**, το Υπουργείο Υποδομών, Μεταφορών και Δικτύων αποτελεί την Αρχή Τηλεπικοινωνιών (Administration) όπως αυτή καθορίζεται στον Καταστατικό Χάρτη της **Διεθνούς Ένωσης Τηλεπικοινωνιών (International Telecommunication Union - ITU)**, και σχετική «Εθνική Ρυθμιστική Αρχή» είναι η **Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.).**

Η Ε.Ε.Τ.Τ. συγκροτείται από εννέα μέλη, εκ των οποίων ένας είναι Πρόεδρος και δύο Αντιπρόεδροι. **Από τους δύο Αντιπροέδρους, ο ένας είναι αρμόδιος για τον τομέα των ηλεκτρονικών επικοινωνιών**, και ο άλλος για τον τομέα παροχής ταχυδρομικών υπηρεσιών. Τα μέλη της Ε.Ε.Τ.Τ. είναι ανώτατοι κρατικοί λειτουργοί και κατά την άσκηση των καθηκόντων τους, απολαμβάνουν πλήρη προσωπική και λειτουργική ανεξαρτησία. Για τη στελέχωση της Ε.Ε.Τ.Τ. δημιουργούνται ακόμα συνολικά 247 θέσεις προσωπικού.

Στο άρθρο 12 αναφέρεται σε αρμοδιότητες της Ε.Ε.Τ.Τ., όπως ότι εκδίδει Κανονισμό για να ρυθμίσει κάθε θέμα που αφορά **στην εκχώρηση των ονομάτων χώρου στο Διαδίκτυο με κατάληξη «.gr»**, τους όρους χρήσης αυτών, τους λόγους διαγραφής, τους όρους μεταβίβασης, το μητρώο εκχωρούμενων ονομάτων χώρου, τα τέλη για την παροχή των σχετικών υπηρεσιών, την άσκηση εποπτείας για τη χρήση αυτών καθώς και

οποιουδήποτε άλλου χώρου ή υποχώρου χορηγηθεί στην Ελλάδα. Αναφέρει ότι τα ανωτέρω ονόματα χώρου αποτελούν πόρους του Ελληνικού Κράτους, και εκχωρούνται αποκλειστικά από την Ε.Ε.Τ.Τ., μόνο για χρήση. **Η Ε.Ε.Τ.Τ. ρυθμίζει επίσης με αποφάσεις της τα θέματα της ηλεκτρονικής υπογραφής, και εποπτεύει τους εμπλεκόμενους σχετκά φορείς** σύμφωνα με την κείμενη νομοθεσία (41).

Στο άρθρο 37 αναφέρεται στην ασφάλεια και ακεραιότητα δικτύων και υπηρεσιών, και υποχρεώνει τις επιχειρήσεις που παρέχουν πρόσβαση σε δημόσια δίκτυα επικοινωνιών ή σε υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό να κοινοποιούν στην Ε.Ε.Τ.Τ. κάθε παραβίαση της ασφάλειας ή κάθε απώλεια της ακεραιότητας που είχε σημαντικό αντίκτυπο στη λειτουργία δικτύων ή υπηρεσιών και εκείνη με τη σειρά της κοινοποιεί κάθε παραβίαση της ασφάλειας ή απώλεια της ακεραιότητας στην Α.Δ.Α.Ε.

Κατά περίπτωση, η Α.Δ.Α.Ε. ενημερώνει τις αρμόδιες εθνικές αρχές στα άλλα κράτη, καθώς και τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA). Η Ε.Ε.Τ.Τ. μπορεί να ενημερώσει το κοινό, ή να απαιτήσει η ενημέρωση αυτή να γίνει από τις επιχειρήσεις, εφόσον κρίνει ότι η αποκάλυψη της παραβίασης είναι προς το δημόσιο συμφέρον. Η Ε.Ε.Τ.Τ. υποβάλλει καθε χρόνο στην Ευρωπαϊκή Επιτροπή και στον ENISA συνοπτική έκθεση σχετικά με τις κοινοποιήσεις που έχει παραλάβει και τη δράση που έχει αναλάβει (41).

2.12 Εκθέσεις του ΟΟΣΑ

Η νομοθεσία ευρωπαϊκή και διεθνής ως προς τα προσωπικά δεδομένα σήμερα, στηρίζεται εν πολλοίς στις συστάσεις του Οργανισμού Οικονομικής Σταθερότητας και Ανάπτυξης - ΟΟΣΑ.

Σύμφωνα με τον ΟΟΣΑ οι επιδόσεις στον τομέα της υγείας, μπορούν να βελτιωθούν εάν τα δεδομένα υγείας συλλέγονται από εθνικές κυβερνήσεις και έπειτα διασυνδεθούν και διαμοιραστούν.

Η συλλογή των δεδομένων επιτρέπει την αποκάλυψη ιατρικών λαθών, ανεπιθύμητες φαρμακευτικές ενέργειες, απάτη, αλλά και τη συμμόρφωση με

τα κλινικά πρότυπα, αποτελεσματικές θεραπείες και την βέλτιστη ανταπόκριση στην αγωγή.

Οι μηχανισμοί και τα πλαίσια που προτείνει ο ΟΟΣΑ για τη συλλογή δεδομένων, στηρίζονται σε προϋπάρχουσες προσπάθειες όπως το oecd privacy framework 2013, και η ευρωπαϊκή οδηγία 95/46/EC, και θα πρέπει να βοηθήσουν τα κράτη να δημιουργήσουν κυβερνητικά πλαίσια και νομοθετήματα, περιλαμβανομένων όσων απαιτεί ο GDPR - General Data Protection Regulation.

Τελικό στόχο πρέπει να έχουν να αναπτύξουν υψηλής αξίας ΠΣΥ, αλλά και να προστατεύσουν την ιδιωτικότητα. Βοήθεια τους παρείχαν οι ειδικοί του APHII - Advisory panel of experts on health information infrastructure (42).

Ο ΟΟΣΑ θεωρεί τις πιο κάτω αναφερόμενες πρακτικές πολύ σημαντικές για την αποταυτοποίηση των δεδομένων και μέσω αυτής της προστασίας τους:

1. Να καταγράφονται οι μέθοδοι που χρησιμοποιούνται.

2. Να συμμετέχει και ένας ειδικός στην προστασία δεδομένων, στην ανάπτυξη και μελέτη των μεθόδων.

3. Να εντοπιστούν οι άμεσοι ή έμμεσοι ταυτοποιητές των δεδομένων.

4. Να διαγραφούν οι άμεσοι ή όπου χρειάζεται να ψευδωνυμοποιούνται.

5. Να αντικαθίστανται τα ψευδώνυμα με ασυνάρτητους αριθμούς, όταν τα δεδομένα παραχωρούνται σε τρίτους.

6. Να αποθηκεύεται η σχέση μεταξύ των ταυτοποιητών, των ψευδονύμων και των ασύντακτων αριθμών, για μελλοντική χρήση, π.χ. για επικύρωση ή επέκταση μιας μελέτης.

7. Να τίθονται γενικοί κανόνες για την αντιμετώπιση έμμεσων ταυτοποιητών, όπως με τεχνικές μασκαρέματος δεδομένων.

8. Να λαμβάνεται υπ΄όψιν η επίπτωση της προηγούμενης σύστασης στην μελέτη αλλά και άλλα μέτρα για την ελαχιστοποίηση των κινδύνων για τα δεδομένα.

9. Να περιλαμβάνονται οδηγίες.

10. Να γίνεται στο τέλος μελέτη της αποταυτοποίησης, για επιβεβαίωση ότι όλα τα βήματα ακολουθήθηκαν (42).

2.12.1 **8 αρχές του ΟΟΣΑ για τα δεδομένα**

Σύμφωνα με τον ίδιο τον ΟΟΣΑ τα νομοθετήματα κι οι πολιτικές ιδιωτικότητας, διεθνώς έχουν επηρρεαστεί από την έκδοση το 1980 των κατευθυντήριων οδηγιών του οργανισμού. Σύμφωνα με αυτές θα πρέπει να ακολουθούνται 8 αρχές, που αναθεωρήθηκαν από τον ΟΑΣΑ, το 2013 και επακολούθως περιελήφθησαν στην οδηγία 95/46/EC που ρυθμίζει την διεργασία των προσωπικών πληροφοριών.

Οι 8 αρχές του ΟΟΣΑ που πρέπει να τηρούνται σχετικά με τα δεδομένα είναι:

1. Αρχή της περιορισμένης συλλογής, δηλαδή να συλλέγονται όσο το δυνατόν λιγότερα.

2. Αρχή της ποιότητας. Θα πρέπει να είναι σχετικά με τον σκοπό που θα εξυπηρετήσουν και να είναι ακριβή, πλήρη και να ενημερώνονται τακτικά.

3. Της περιγραφής του σκοπού. Την στιγμή μάλιστα της συλλογής.

4. Του περιορισμού της χρήσης. Δεν θα πρέπει να αποκαλύπτονται ή να χρησιμοποιούνται για άλλους σκοπούς, εκτός αν υπάρχει σχετική συγκατάθεση του υποκειμένου ή τ επιτάσσεται απο το νόμο.

5. Των μέτρων προστασίας ενάντια στην απώλεια, στην πρόσβαση χωρίς εξουσιοδότηση, στην καταστροφή, χρήση, τροποποίηση, αποκάλυψη δεδομένων.

6. Της ανοικτότητας και διαφάνειας των πρακτικών καθώς και των στοιχείων του ελεγκτή.

7. Της συμμετοχικότητας των ατόμων που θα πρέπει να έχουν το δικαίωμα: α) να τους ενημερώνει ο ελεγκτής ή κάποιος άλλος αν έχει δεδομένα σχετικά με αυτούς, β) να τους μεταφέρονται μέσα σε σύντομο σχετικά χρόνο με κάποια χρέωση όχι ιδιαίτερα μεγάλη και με τρόπο κατανοητό από αυτούς, γ) να τους δοθούν εξηγήσεις αν κάποια τέτοια αίτηση τους απορριφθεί, και να μπορούν να προσβάλλουν μια τέτοια απόρριψη, δ) να αμφισβητήσουν δεδομένα που κρατούνται γι αυτούς και να μπορούν να τα διαγράψουν, διορθώσουν, συμπληρώσουν ή επανορθώσουν.

8. Της υπευθυνότητας. Να υπάρχει δηλαδή ένας ελεγκτής δεδομένων που να πρέπει να λογοδοτεί για το αν συμμορφώνεται με τις παραπάνω αρχές (42).

2.12.2 **Σχετική νομοθεσία σε άλλες χώρες**

Ο ΟΟΣΑ σχετικά με τις νομοθεσίες σε άλλες χώρες σημειώνει μεταξύ άλλων τα ακόλουθα: Ότι τα περισσότερα κράτη εξέφρασαν προβληματισμούς σε σχέση με την ποιότητα των δεδομένων που συγκεντρώνουν, μιας και δεν προβλέπεται και κανένα κίνητρο για τους υγειονομικούς που επιφορτίζονται με την επίπονη καταχώρησή τους πέραν των υπαρχόντων ήδη καθηκόντων τους, ούτως ώστε να δίνουν προσοχή στην επομελή καταχώρηση των δεδομένων, προκειμένου αυτά τελικά να είναι αξιόπιστα. Κάτι τέτοιο θα ήταν απαραίτητο προφανώς, και προκειμένου να προκύπτουν χρήσιμα και ασφαλή συμπεράσματα από την ανάλυση μεγάλων δεδομένων όπως αυτά του χώρου της υγείας.

Στον ΟΟΣΑ εξέτασαν επίσης αν αναγνωρίσιμα εθνικά προσωπικά δεδομένα υγείας διαμοιράστηκαν σε κατόχους ή κυβερνητικές οργανώσεις, και εάν μετά από αποταυτοποίηση μπορεί τα κράτη-μέλη να εγκρίνουν την πρόσβαση σε αιτούντες κοινωνικούς ή ξένους φορείς.

Σε ότι αφορά τις κρατικές νομοθεσίες για την υγεία αναφέρει σχετικά τα ακόλουθα.

Στη Νέα Ζηλανδία, έχουν το εθνικό Privacy Act και το Health Information Privacy code (HIPC), που καθορίζει ως ελάχιστη περίοδο διατήρησης των δεδομένων από παρόχους τα 10 χρόνια, χωρίς να καθορίζουν μέγιστη

περίοδο. Το HIPC δεν αφορά τις ιδιωτικές εταιρείες. Το Privacy Act, που υπάρχει όμως περιλαμβάνει τους πάντες.

Σε Νέα Ζηλανδία, Ισπανία και Τσεχία η νομοθεσία προστατεύει και την ιδιωτικότητα των παρόχων υγείας, και αυτό έχει σαν αποτέλεσμα να μη δίνεται η δυνατότητα να γίνονται στατιστικές σε επίπεδο παρόχου, χωρίς τη δική τους συγκατάθεση.

Ο Καναδάς σε εθνικό επίπεδο έχει τη νομοθετική πράξη της ιδιωτικότητας και της προστασίας των προσωπικών πληροφοριών και ηλεκτρονικών κειμένων (PIPEDA).

Στη Βρεττανία σύμφωνα με την πράξη - Health and social care act (01/04/2013), το κέντρο πληροφοριών της υγείας και της κοινωνικής ασφάλειας - **Health and social care Information Centre (HSCIC)** έγινε **ανεξάρτητη αρχή** από το υπουργείο υγείας, και διαχειρίζεται τα σχετικά δεδομένα και την πρόσβαση σε αυτά.

Αυτή η οδηγία συμπληρώθηκε και ενισχύθηκε με την Care Act (May 2014), που θεσμοθέτησε και την συμβουλευτική ομάδα εμπιστευτικότητας - Confidentiality Advisory Group. Αυτός ο νόμος κατέστησε επίσης σαφές ότι μπορεί κάποιος να αρνηθεί να έχει τα δεδομένα του καταχωρημένα σε δεδομένα φροντίδας.

Οι ΗΠΑ έχουν ως κύριο σχετικό εθνικό νόμο το HIPAA. Υπάρχουν ομοσπονδιακοί νόμοι που μπορεί να τον υπερβαίνουν, μόνο όμως σε περίπτωση που πλεονεκτούν στο επίπεδο προστασίας που προβλέπουν.

Ο HIPAA δεν έχει εφαρμογή στο Εθνικό Ινστιτούτο Υγείας - NIH, αλλά εκεί βρίσκει εφαρμογή η ομοσπονδιακή πράξη της ιδιωτικότητας του 1974, ούτε και σε εμπορικές δραστηριότητες του τύπου γυμναστήρια, διατροφικά κέντρα, κ.α. που ενδεχομένως αποθηκεύουν σχετικά με την υγεία δεδομένα (αυτά ελέγχονται από την αντίστοιχη εμπορική νομοθεσία).

Ο HIPAA, όπως και η ευρωπαϊκή νομοθεσία, χαρακτηρίζει κάποιες κατηγορίες προσωπικών δεδομένων ως ιδιαίτερα ευαίσθητες, και θεωρεί ότι αν αυτές

διαρρεύσουν μπορεί να προκαλέσουν στίγμα στο υποκείμενο των δεδομένων. Τέτοιες θεωρεί ότι είναι όσες αφορούν δεδομένα ψυχιατρικά, ή αφορούν σεξουαλικώς μεταδιδόμενα νοσήματα (STD΄s), κατάχρηση ουσιών, εκτρώσεις, φόνους, κλπ.

Στις ΗΠΑ σύμφωνα με τον HIPAA, επιτρέπεται η στατιστική ανάλυση δεδομένων χωρίς συγκατάθεση, εάν έχει προηγουμένως αυτή εγκριθεί από αρμόδια επιτροπή ηθικής. Εάν τα δεδομένα των ασθενών γίνουν ανώνυμα τότε δεν υπάρχει κανένα πρόβλημα για τη μεταφορά τους σε ένα τρίτο οργανισμό ή άτομο, για επιστημονικούς σκοπούς όπως η ιατρική έρευνα.

Ο HIPAA, θεσπίστηκε από το Αμερικανικό κογκρέσσο το 1996. Σύμφωνα με αυτόν μπορούν να χρησιμοποιηθούν τεχνικές όπως είναι το checksum (πρόσθεση των κωδικών ASCII κάθε χαρακτήρα του μυνήματος και διαίρεση του αθροίσματος με το 255), digital signage, token systems, double-triple handshaking, συστήματα κωδικού πρόσβασης, ως μέτρα προστασίας ΠΣ και αυθεντικοποίησης. Ορίζει επίσης ότι θα πρέπει να πραγματοποιείται risk–analysis.

Στις ΗΠΑ επίσης υπάρχει η πράξη για τους Αμερικανούς με αναπηρίες, και η πράξη ενάντια στις διακρίσεις λόγω γενετικών πληροφοριών που ελέγχει τους εργοδότες.

Στο Ισραήλ υπάρχει ο νόμος γενετικών πληροφοριών, καθώς και νόμοι για εκτρώσεις, θεραπείες υπογονιμότητας, και ψυχιατρικές υπηρεσίες.

Στη Δανία κάποια δεδομένα που αφορούν τους καταχραστές ουσιών και τους χρήστες ναρκωτικών, διατηρούνται χωριστά σε άλλες ΒΔ στο Statens Serum Institute (SSI), χωρίς τους αριθμούς μητρώων ασθενών. Σε ότι αφορά την στατιστική ανάλυση των δεδομένων, αυτή μπορεί να γίνει με τη συγκατάθεση των ατόμων ή εάν η ανάλυση έχει νομικά εγκριθεί.

Στη Σιγκαπούρη υπάρχει πράξη personal data protection act (PDPA) (42).

2.12.3 **HIPAA**

Ο Health Insurance Portability and Accountability Act (ασφαλιστική, μεταφοράς και καταλογισμού οδηγία για την υγεία) ψηφίστηκε από το Κονγκρέσσο των ΗΠΑ το 1996. Νομοθετήθηκε στο Αμερικανικό Κονγκρέσσο και υπογράφηκε από τον τότε πρόεδρο President Bill Clinton το 1996. Είναι γνωστή σαν Kennedy–Kassebaum Act ή Kassebaum–Kennedy Act. Είναι ο κύριος νόμος που αφορά τα δεδομένα υγείας στις ΗΠΑ. Νομοθετήθηκε για να διασαφηνίσει πολιτικές ασφάλειας και το δικαίωμα της ιδιωτικότητας σε όλο το φάσμα των υπηρεσιών υγείας (43).

Το δεύτερο κεφάλαιο του HIPAA για την αντιμετώπιση της απάτης στο χώρο της υγείας έχει πέντε κανόνες, τρείς από τους οποίους είναι: της ιδιωτικότητας, της ασφάλειας και της επιβολής κυρώσεων. Αυτός της ιδιωτικότητας υπάρχει πρόβλεψη να μην ισχύει αυστηρά ως έχει σε καταστάσεις φυσικών καταστροφών, όπως συνέβει στην περίπτωση του τυφώνα Harvey το 2017 και αυτό γιατί σε προηγούμενες καταστροφές δυσκολεύονταν οι συγγενείς να ενημερωθούν για την τύχη αγαπημένων τους προσώπων και να τους προστρέξουν. Αφορά όλες τις προστατευμένες πληροφορίες υγείας τόσο σε χαρτί, όσο και σε ηλεκτρονική μορφή. Ο κανόνας της Ασφάλειας συμπληρώνει εκείνον της Ιδιωτικότητας, και εξειδικεύεται στην ηλεκτονική υγεία με σκοπό την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα.

Ο HIPAA έχει προβλέψεις για ιατρικές εφαρμογές σε κινητά, όπως ότι πρέπει να γίνεται κρυπτογράφηση των δεδομένων που αποθηκεύουν, συχνή αναβάθμιση, είσοδος με ταυτοποιήσεις χρηστών, να υπάρχει σύστημα αξιολόγησης των δεδομένων, σύστημα ελέγχου αν έχουν τροποποιηθεί τα δεδομένα, και τέλος ότι πρέπει να υπάρχει δυνατότητα εφαρμογής της καταστροφής των δεδομένων από τις κινητές συσκευές εάν αυτές χαθούν ή κλαπούν.

Ο HIPAA, συμπληρώθηκε σε κάποια σημεία με την νομοθετική πράξη HITECH του 2010. Ο Health Information Technology for Economic and Clinical Health Act του 2010 απαιτεί από τις εταιρείες που χειρίζονται

προσωπικά δεδομένα υγείας να κοινοποιούν τις παραβιάσεις που μπορεί να συμβούν σε αυτά.

Το FDA εξέδωσε την οδηγία “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices”, που παρέχει λίστα με σχετικά πρότυπα για ΠΣΥ (44), (45).

Οι ΗΠΑ σε γενικότερο πλαίσιο πέραν του χώρου της υγείας δεν έχουν κεντρική νομοθεσία σχετικά με την προστασία ΔΠΧ, και η κάθε πολιτεία έχει τη δικιά της. Έτσι προκειμένου να οριστούν κάποια πράγματα απαιτείται κανείς να κοιτάξει σε μεγάλο αριθμό νόμων και κανονισμών.

Σύμφωνα με τον HIPAA privacy rule, τα δεδομένα μπορεί να θεωρούνται αποταυτοποιημένα όταν πιστεύεται ότι δεν ταυτοποιούν τα άτομα που αφορούν, είτε άμεσα είτε έμμεσα. Η πιθανότητα όμως αυτό να συμβεί, θεωρεί ότι δεν μπορεί να είναι και μηδενική. Ο HIPAA Privacy rule περιγράφει τις μεθόδους, με τις οποίες πρέπει να γίνεται η αποταυτοποίηση των δεδομένων.

- Σημαντικό στοιχείο είναι να υπάρχει η έννοια του «ασφαλή λιμένα» - ‘safe harbor’. Σύμφωνα με αυτή για την αποταυτοποίηση πρέπει δεκαοκτώ μεταβλητές όπως είναι τα ονόματα, τηλέφωνα κλπ, να μην είναι εμφανή. Επίσης πρέπει να αφαιρούνται φωτογραφίες και βιομετρικά, ενώ στα άτομα άνω των ογδονταεννέα ετών πρέπει να μην αναφέρονται τα μονά έτη ηλικίας.

- Επίσης ένας ειδικός πρέπει να αποφασίζει πόσο μεγάλος είναι ο κίνδυνος και ανάλογα με την απόφαση η διαδικασία μπορεί να είναι περισσότερο ή λιγότερο αυστηρή.

- Μια τεχνική αποταυτοποίησης που συνιστάται είναι το «μασκάρεμα των δεδομένων», όπου μεταβάλλοντας κάποιες μεταβλητές αυτών, μειώνεται η πιθανότητα να επαναταυτοποιηθούν (42).

Σύμφωνα με τον ΟΟΣΑ ρωτήθηκαν διάφορες χώρες αν αποταυτοποιούν τα δεδομένα τους προτού τα χρησιμοποιήσουν σε αναλύσεις. Επτά μόνο χώρες αποκρίθηκαν ότι το έκαναν πάντα (Τσεχία, Ιταλία, Κορέα, Ολλανδία,

Νορβηγία, Σιγκαπούρη, και ΗΠΑ). Άλλες χώρες απάντησαν ότι δεν το κάνουν ποτέ (Ισλανδία, Τουρκία, Ισραήλ).

• Οσον αφορά την ψευδονυμοποίηση, γίνεται μετατροπή των μεταβλητών σε ασυνάρτητα σχέδια με συστηματικό τρόπο. Εφαρμόζεται σε όλες τις σημαντικές μεταβλητές του τομέα υγείας στην Σκωτία, Ουαλία, Κορέα, Νεα Ζηλανδία, Σιγκαπούρη, Τσεχία, και στις περισσότερες στην Ιαπωνία, Φινλανδία, Ολλανδία, Νορβηγία, Δανία, Ισλανδία, Σουηδία και Αγγλία.

• Σύμφωνα με τον ΟΟΣΑ, κρυπτογράφηση δεδομένων πρίν την αντιγραφή τους σε μορφή CD ή USB, γίνεται στη Φινλανδία, Κορέα και Ηνωμένο Βασίλειο. Κάποιες άλλες χώρες καταγράφουν ότι τα δεδομένα μεταφέρθηκαν μεν σε CD ή USB, αλλά δεν αναφέρουν αν προηγήθηκε ή όχι κρυπτογράφηση. Κάποιες άλλες δεν επιτρέπουν καθόλου τέτοιες μεταφορές.

• Μόνο δυο χώρες μοιράστηκαν εμπειρίες τους διαρροής προσωπικών δεδομένων υγείας.

• Σε ένα άλλο σημείο της μελέτης του ΟΟΣΑ, αναφέρει ότι ένα νοσοκομείο σε κάποια χώρα επέδειξε αμέλεια αφού πριν διαθέσει κάποιους Η/Υ του δεν είχε προβεί σε κρυπτογράφηση των δεδομένων που περιείχοντο στους σκληρούς δίσκους και ούτε και είχε λάβει μέτρα να καθαρίσει τους σκληρούς δίσκους. Αποτέλεσμα ήταν να επεβληθεί βαρύ οικονομικό πρόστιμο (42).

Συμπερασματικά με το παρόν κεφάλαιο εξετάστηκε διεξοδικά η νομοθεσία στην Ελλάδα και διεθνώς σε ότι αφορά τα ΔΠΧ, την ιδιωτικότητα, την ασφάλεια των ΠΣ και των επικοινωνιών, κάτι που οπωσδήποτε πρέπει να γνωρίζει όποιος θέλει να προστατέψει τα ΔΠΧ, και ασχολείται με τα ΠΣ στο χώρο της υγείας.

Κεφάλαιο 3^{ο}: Πληροφοριακά Συστήματα

Η προστασία των προσωπικών δεδομένων είναι και μερικός και ευρύτερος όρος της ασφάλειας των πληροφοριακών συστημάτων.

Μερικός γιατί τα ΠΣ, μπορεί να έχουν προβλήματα ασφάλειας και πέραν της ενδεχομένως ανεπαρκούς προστασίας των προσωπικών δεδομένων. Για παράδειγμα μπορεί να υπάρχουν προβλήματα στα λειτουργικά συστήματα ή στην εξασφάλιση αδιάλειπτης επικοινωνίας και παροχής υπηρεσιών. Ευρύτερος γιατί προσωπικά δεδομένα, βρίσκονται και συντηρούνται και εκτός των βάσεων δεδομένων ενός ΠΣ, π.χ. σε βιβλία, ταινίες, δίσκους βινυλίου κλπ. Βέβαια αυτό δεν αφορά τόσο την πληροφορική.

Εντούτοις καθώς τα ΠΣ εισβάλλουν ολοένα και περισσότερο στην ανθρώπινη δραστηριότητα και αυξάνεται ολοένα η αλληλοεξάρτηση μεταξύ τους, φαίνεται πως η ασφάλεια ΠΣ και η ΠΔΠΧ, θα πρέπει να εξετάζονται και να αντιμετωπίζονται με ενιαίο τρόπο. Για την αντιμετώπιση των προβλημάτων δεν αρκεί να λειτουργούν σωστά τα ΠΣ από τεχνική άποψη κατασκευής και συντήρησης, αλλά να υπάρχουν και εξειδικευμένες δομές παρακολούθησης και αντιμετώπισης σύγχρονων κακόβουλων εσκεμμένων ή μη ενεργειών, που μπορεί να προκαλέσουν βλάβη.

Όποιος θέλει να προστατέψει τα ΔΠΧ, την ιδιωτικότητα, αλλά και να παρέχει ασφάλεια στα ΠΣΥ πέρα από τη νομοθεσία, πρέπει να γνωρίζει από τι συνίστανται και πως λειτουργούν τα ίδια τα ΠΣ. Άνθρωποι και διαδικασίες, λογισμικό και υλικά, εμπλέκονται στα ΠΣ, όπως και στο υποσύστημα αυτών εκείνο της κυβερνοασφάλειας που θέλει να τα προστατέψει.

Κάθε σύστημα γενικά έχει εσωτερικό περιβάλλον και εξωτερικό περιβάλλον. Τα συστατικά στοιχεία του συστήματος (άνθρωποι – μηχανές – διαδικασίες) καθορίζουν το εσωτερικό περιβάλλον του. Ότι βρίσκεται εκτός του εσωτερικού περιβάλλοντος ονομάζεται εξωτερικό περιβάλλον. Τα δύο περιβάλλοντα βρίσκονται σε συνεχή επικοινωνία ανταλλάσοντας δεδομένα, έχουν εισόδους

και εξόδους για αυτή την επικοινωνία (46). Τα ΠΣ είναι εκείνα τα συστήματα που παίρνουν σαν είσοδο δεδομένα, τα επεξεργάζονται και τα αποδίδουν στην έξοδο σαν πληροφορίες. Τα ΠΣ για την επίτευξη του σκοπού τους χρησιμοποιούν τις τηλεπικοινωνιακές υποδομές (1).

Τα συστήματα διακρίνονται σε ανοικτά ή κλειστά, ανάλογα με το αν επιτρέπουν ή όχι αλληλεπιδράσεις με το περιβάλλον τους, και με το εαν προσαρμόζονται άμεσα σε νέα δεδομένα και απαιτήσεις, ή όχι (47).

Σύμφωνα με τον κ. Μαντά, “Σύστημα είναι ένα σύνολο συστατικών στοιχείων (π.χ. άνθρωποι – μηχανές – διαδικασίες) που διέπονται από συγκεκριμένους τρόπους λειτουργίας και τα οποία αλληλεπιδρούν μεταξύ τους για τη διεκπεραίωση κάποιου έργου.” Όπως υπάρχουν διάφοροι ρόλοι και διαδικασίες σε ένα οποιοδήποτε σύστημα, έτσι και στα ΠΣ υπάρχουν οι άνθρωποι, τα πρότυπα, οι διαδικασίες, το λογισμικό, οι βάσεις δεδομένων και ο εξοπλισμός (46).

Όλα αυτά μαζί λειτουργούν για να παράγουν το επιδιωκόμενο αποτέλεσμα που είναι οι πληροφορίες και κατ΄επέκταση η προαγωγή της σύγχρονης κοινωνίας της Πληροφορίας (ΚτΠ), και αποτελούν πληροφοριακούς πόρους. Πληροφοριακός πόρος ή αγαθό (asset) είναι κάθε αντικείμενο ή πόρος που ανήκει ή υποστηρίζει ένα ΠΣ, και το οποίο αξίζει να προστατευθεί. Τα αγαθά διακρίνονται σε φυσικά αγαθά (χρήστες, υπολογιστικά συστήματα, δικτυακή υποδομή, Λοιπός εξοπλισμός), αγαθά δεδομένων (αρχεία-δεδομένα-διαδικασίες), αγαθά λογισμικού.

Ειδικότερα:

- Οι ρόλοι των ανθρώπων διακρίνονται σε ρόλους χρηστών, χειριστών, προϊσταμένων, διαχειριστών, ιδιοκτητών, κλπ.

- Το λογισμικό software, διακρίνεται σε λειτουργικό σύστημα, εφαρμογές, εργαλεία κλπ, όπου αποθηκεύονται και επεξεργάζονται δεδομένα, και παράγονται πληροφορίες και υπηρεσίες. Ιδιαίτερη σημασία έχουν οι ΒΔ, όπου φυλάσσονται και τα ΔΠΧ, και μπορεί να αποτελέσουν σημαντικό στόχο της παραβίασης ενός ΠΣ.

• Το υλικό είναι: α) ο εξοπλισμός hardware, της εταιρίας ή του οργανισμού ή του παρόχου ή του χρήστη υπηρεσιών υγείας, και περιλαμβάνει φυσικά μέρη όπως laptops, desktops, κινητά, καλώδια, usb, αποθηκευτικά ψηφιακά μέσα (cd, dvd), περιφερειακές συσκευές (π.χ. εκτυπωτές, κάμερες, ψηφιακά εξεταστικά μηχανήματα), άλλες ενσύρματες και ασύρματες συσκεύες και β) ο δικτυακός εξοπλισμός middleware που περιλαμβάνει καλώδια, κάρτες, ραδιοκύματα, οπτικές ίνες, δορυφόρους για τον οποίο εξοπλισμό και τη σωστή συντήρηση και αξιοποίηση του, είναι υπεύθυνες οι χώρες, οι τηλεπικοινωνιακοί οργανισμοί και οι υπενοικιαστές αυτών.

Για να λειτουργήσουν σωστά και αρμονικά όλα αυτά, πρέπει να υπάρχει σωστός σχεδιασμός και πολιτικές λειτουργίας βασιζόμενες σε πρότυπα και νομοθεσίες.

Δικαιούχοι (stakeholders) ενός ΠΣ μπορούν να είναι όσοι νόμιμα και στα πλαίσια που τους αφορούν συμμετέχουν στο ΠΣ, όπως:

- Η διοίκηση του οργανισμού - Οι ιδιοκτήτες και διαχειριστές των δεδομένων και διεργασιών - Οι χειριστές - Οι υπεύθυνοι ανάπτυξης του συστήματος - Οι υπεύθυνοι λειτουργίας του - Οι καταναλωτές των τελικών προϊόντων και υπηρεσιών - Η πολιτεία.

Πιο εξειδικευμένα στο χώρο της υγείας ένα ΠΣΝ – Health Information System (HIS), είναι το υπολογιστικό σύστημα που φροντίζει για τη συνύπαρξη της εσωτερικής με την εξωτερική ροή της πληροφορίας, την σωστή επικοινωνία με το εξωτερικό περιβάλλον και τον κοινό τρόπο λειτουργίας του λογισμικού και των υπολογιστικών πόρων που λειτουργούν μέσα σε ένα νοσοκομείο (47).

Ένα ΠΣΝ χαρακτηρίζεται πάντα από κάποιο ιεραρχικό σχεδιασμό και αποτελείται από περισσότερα υποσυστήματα που αντιστοιχούν στα επιμέρους τμήματά του. Τέτοια είναι το εργαστηριακό, το κλινικό, το χειρουργικό, το φαρμακείο, το διοικητικό και το οικονομικό τμήμα, κ.α.. Αυτά πρέπει να είναι κατάλληλα διασυνδεδεμένα ώστε να επιτρέπουν ανταλλαγή πληροφοριών μεταξύ τους και με αντίστοιχα ΠΣ άλλων υγειονομικών μονάδων μέσω διαλειτουργικότητας, και συγχρόνως να κάνουν έλεγχο της ταυτοποίησης των χρηστών και του επίπεδου πρόσβασής τους στο σύστημα,

προστατεύοντας τόσο την ασφάλεια των ΠΣΝ όσο και τα ΔΠΧ. Όλα μαζί διασυνδεδεμένα έτσι, συναποτελούν ένα ολοκληρωμένο πληροφοριακό σύστημα υγείας (ΟΠΣΥ).

Υποσύστημα ενός ΟΠΣΥ πρέπει απαραίτητα να είναι ένα σύστημα ασφάλειας ΠΣ και προστασίας ΔΠΧ, που σε μεγάλους οργανισμούς θα στελεχώνεται από εξειδικευμένο προσωπικό.

Μόλις υπάρξει πρόσβαση στις πληροφορίες ενός ΠΣ, κάτι που προϋποθέτει η διαλειτουργικότητα, αμέσως εγείρεται το θέμα ενδεχόμενης παραβίασης της ιδιωτικότητας. Θα πρέπει να υπάρχει πρόσβαση μόνο για εξουσιοδοτημένους χρήστες, μέσω μηχανισμών αυθεντικοποίησης, π.χ. με συνθηματικά, βιομετρικά χαρακτηριστικά κλπ.

Πιο εξειδικευμένα υποσυστήματα που απαντώνται στο περιβάλλον ενός ΠΣΝ επίσης είναι τα συστήματα τηλεϊατρικής, τηλε-εκπαίδευσης αλλά και τα έμπειρα συστήματα - εκείνα δηλαδή που διαθέτουν αποθηκευμένη εμπειρία, π.χ. σύνολο κανόνων σε μια βάση γνώσης, ένα περιβάλλον διεπαφής και μια συμπερασματική μηχανή. Στα έμπειρα ή συστήματα λήψης αποφάσεων (Σ.Υ.Λ.Α.), εντάσσονται και τα **Συστήματα Ιατρικής Υποστήριξης** (Medical support systems), που κάνουν ερωτήσεις στο χρήστη για να πάρουν τις πληροφορίες που χρειάζονται. Μετά η συμπερασματική μηχανή χρησιμοποιεί τη βάση της γνώσης και επιστρέφει μια συμβουλή. Μπορούν να δουλεύουν με «αβεβαιότητα», στοχαστικά δηλαδή με ποσοστά, οπότε το σύστημα δίνει στους χρήστες αρκετές απαντήσεις που τις κατατάσσει ταυτόχρονα, και εκείνος επιλέγει.

Ένας «Μηχανικός Γνώσεων», εισάγει γνώση στο έμπειρο σύστημα, συνεργαζόμενος με τον «ειδικό του τομέα». Συμβάλλει επίσης και ο «μηχανικός του συστήματος», που είναι για τον σχεδιασμό της πλατφόρμας διεπαφής με τον χρήστη, και τη λειτουργία της συμπερασματικής μηχανής (λογισμικό).

Άλλα συστήματα λήψης αποφάσεων όπως τα CLE-MANTIS (clinical engineering management tool & information system), είναι εργαλεία

παρακολούθησης των τμημάτων βιοϊατρικής τεχνολογίας (ΤΒΙΤ) και είναι εγκατεστημένα σε αρκετά νοσοκομεία στην Ελλάδα (47).

Στην Ελλάδα το ευρύτερα χρησιμοποιούμενο ΠΣ, είναι το σύστημα ηλεκτρονικής συνταγογράφησης. Οι κύριοι κίνδυνοι σε αυτό είναι τα σφάλματα καταχώρησης δεδομένων, όπως π.χ. η λάθος επιλογή κάποιου φαρμάκου και η αποκάλυψη απόρρητων πληροφοριών για την υγεία του ασθενή στο διαδίκτυο λόγω ανεπαρκών πρακτικών ασφαλείας. Γι αυτό πρέπει να έχει υψηλά επίπεδα κρυπτογράφησης και να γίνεται κωδικοποίηση δεδομένων, χρήση έξυπνων καρτών καθώς και ηλεκτρονικών κρυπτογραφημένων υπογραφών (48).

Ο **νόμος 3892/2010** στο άρθρο 1, αναφέρει ότι «**Ηλεκτρονική συνταγογράφηση** είναι η παραγωγή, διακίνηση και έλεγχος των ιατρικών συνταγών και παραπεμπτικών ιατρικών πράξεων, με τη χρήση τεχνολογίας Ηλεκτρονικών Υπολογιστών και Τηλεπικοινωνιών, με τρόπο που διασφαλίζει την εγκυρότητα, την ασφάλεια και τη διαφάνεια των διακινούμενων πληροφοριών». Επίσης ορίζει ότι Σύστημα Ηλεκτρονικής Συνταγογράφησης (ΣΗΣ), είναι ένα ολοκληρωμένο σύστημα που περιλαμβάνει εξοπλισμό, λογισμικό, εφαρμογές και διαδικασίες που αφορούν την ηλεκτρονική συνταγογράφηση (49).

Σύμφωνα με τα **άρθρα του 3 και 4** αντίστοιχα, οι ιατροί και οι φαρμακοποιοί που είναι εγγεγραμμένοι ως χρήστες του ΣΗΣ **ταυτοποιούνται κατά την είσοδο** τους στο σύστημα, με τη χρήση στοιχείων ταυτοποίησης. Κάθε συνταγή ή παραπεμπτικό που καταχωρείται ηλεκτρονικά έχει ένα μοναδικό κωδικό αριθμό, ο οποίος εμφανίζεται και με την μορφή γραμμωτού κώδικα (barcode).

Οι φαρμακοποιοί, αφού προβούν στην ταυτοποίηση του ασθενούς για τον οποίο έχει καταχωρηθεί η ηλεκτρονική συνταγή, εισάγουν τα προς πώληση φάρμακα στην εφαρμογή, σκανάροντας τους δύο γραμμωτούς κώδικες που υπάρχουν στην ταινία γνησιότητας κάθε φαρμακευτικού προϊόντος.

Με το άρθρο 6, ζητάει τη σύσταση ΒΔ του συστήματος ηλεκτρονικής συνταγογράφησης (ΣΗΣ). Η Γενική Γραμματεία Κοινωνικών Ασφαλίσεων

(ΓΓΚΑ) είναι αυτή που δημιουργεί και λειτουργεί τη βάση. Η βάση λειτουργεί υπό την εποπτεία της Υπηρεσίας Ελέγχου Δαπανών Υγείας των Φορέων Κοινωνικής Ασφάλισης (ΥΠΕΔΥΦΚΑ) και της Διεύθυνσης Μηχανογραφικών Εφαρμογών. Στη βάση καταχωρείται κάθε συνταγή και παραπεμπτικό, και ταξινομούνται σύμφωνα με τον αντίστοιχο φορέα κοινωνικής ασφάλισης – ΦΚΑ. Επίσης στη ΒΔ καταχωρούνται και οι λοιπές πληροφορίες που απαιτούνται για την λειτουργία του ΣΗΣ, όπως οι τιμές των φαρμάκων και της παροχής υπηρεσιών, τα στοιχεία των χρηστών στους οποίους επιτρέπεται η πρόσβαση στο ΣΗΣ, τα στοιχεία των Φ.Κ.Α., των μονάδων παροχής υπηρεσιών υγείας ή άλλων μονάδων που παρέχουν υπηρεσίες ή παροχές σε ασφαλισμένους, των προμηθευτών των φαρμάκων και υλικών, καθώς και τα άλλα δεδομένα που διαχειρίζεται το ΣΗΣ (49).

Η ηλεκτρονική διακυβέρνηση της κοινωνικής ασφάλισης (ΗΔΙΚΑ, Α.Ε.), διαχειρίζεται και συντηρεί τη βάση. **Η ΓΓΚΑ και η ΗΔΙΚΑ Α.Ε. οφείλουν να παίρνουν όλα τα κατάλληλα και ανάλογα προς τους εκάστοτε κινδύνους, τεχνικά και οργανωτικά μέτρα για την ασφάλεια** των υποδομών, των ΠΣ και των δεδομένων, και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, από απώλεια, αλλοίωση, απαγορευμένη διάδοση και όποια άλλη μορφή αθέμιτης επεξεργασίας ή μη νόμιμης και εξουσιοδοτημένης πρόσβασης και χρήσης.

Σε ανάλογα μέτρα υποχρεώνονται και οι επιμέρους ΦΚΑ που έχουν πρόσβαση στα δεδομένα (άρθρο 7.παρ.2). Η πρόσβαση τους περιορίζεται στα στοιχεία της βάσης που αφορά τον κάθε ένα από τους φορείς. Η πρόσβαση στη βάση γίνεται από πρόσωπα που ασχολούνται κατ' επάγγελμα με την παροχή υπηρεσιών υγείας και δεσμεύονται από ιατρικό απόρρητο ή άλλο απόρρητο που προβλέπει νόμος ή κώδικας δεοντολογίας ή που είναι ειδικά για αυτό εξουσιοδοτημένα και υπόκεινται σε καθήκον εχεμύθειας (49).

Η συνταγογράφηση είναι πολύ σημαντική υπηρεσία για τους πολίτες, είναι η πιο συνήθης ιατρική πράξη, και το δεύτερο πιο ισχυρό θεραπευτικό εργαλείο στα χέρια των ιατρών μετά από τις επεμβάσεις. Θα πρέπει οι ασθενείς να παίρνουν τα κατάλληλα φάρμακα στις κατάλληλες δόσεις όπως έχουν συνταγογραφηθεί από τους θεράποντες ιατρούς, και να μην υπάρχει

δυνατότητα μεταβολής αυτών των στοιχείων από τρίτους. Για αυτό θα πρέπει να προστατεύεται αλλά επίσης και για λόγους εχεμύθειας.

3.1 Privacy by Design

Ο σχεδιασμός ένος ΟΠΣΥ γενικά λαμβάνει υπ΄όψιν του τις συνήθεις και τις ειδικότερες ανάγκες, τις διαδικασίες και τις υπηρεσίες ενός υγιειονομικού σχηματισμού και προσπαθεί να τις καλύψει.

Στην ιδιωτικότητα από τον σχεδιασμό δίνει εξέχουσα σημασία και ο **Ευρωπαϊκός Οργανισμός για την Ασφάλεια των Πληροφοριών και των Δικτύων ή αλλιώς - European Union Agency for Network and Information Security (Enisa),** με έδρα το Ηράκλειο της Κρήτης. Σύμφωνα με αυτόν σημαντικό πρώτο βήμα και μέθοδος προς την κατεύθυνση ασφάλειας, είναι η ιδιωτικότητα από το σχεδιασμό και η προστασία δεδομένων από τον σχεδιασμό. Αυτό είναι κάτι που προβλέπεται και από τον ΓΚΠΔ. Η έννοια της ιδιωτικότητας από το σχεδιασμό, είναι βασική πλέον στις ΤΠΕ. **Οι βασικές αρχές που πρέπει να χαρακτηρίζουν την "Privacy by Design" για να επιτύχει τους στόχους της είναι:**

1. Πρόληψη και όχι αντίδραση.

2. Προστασία της Ιδιωτικότητας ως προεπιλεγμένη ρύθμιση.

3. Ενσωμάτωση προστασίας της Ιδιωτικότητας στον σχεδιασμό.

4. Πλήρης λειτουργικότητα, που σκοπό θα πρέπει να έχει το θετικό και όχι το μηδενικό αποτέλεσμα (Positive-Sum vs Zero-Sum). Δηλαδή το γεγονός ότι οφείλουν να προστατεύονται δεν σημαίνει ότι θα υπολειτουργούν ή δεν θα λειτουργούν.

5. Καθολική ασφάλεια (End to End security) και πλήρης προστασία κατά τη διάρκεια ζωής του ΠΣ. Από τη δημιουργία μέχρι την καταστροφή του ΠΣ, ολόκληρου ή μερικώς.

6. Ορατότητα και διαφάνεια.

7. Σεβασμός στην ιδιωτική ζωή του χρήστη (50).

Καλό είναι ιδιωτικότητα, η ασφάλεια δεδομένων και η ελαχιστοποίηση των κινδύνων να είναι η συνήθης πρακτική στο σχεδιασμό εφαρμογών και ΠΣ.

Η Privacy-preserving data mining (PPDM) είναι μια μέθοδος εξόρυξης δεδομένων που έχει γίνει δημοφιλής γιατί επιτρέπει τον διαμοιρασμό ευαίσθητων δεδομένων για ανάλυση. Χρησιμοποιεί στατιστικές τεχνικές τροποποίησης των αρχικών δεδομένων ώστε να παραμένουν ιδιωτικά ακόμα και μετά την διαδικασία εξόρυξης. Καλό είναι να λαμβάνονται υπ΄όψιν παρόμοιες τεχνικές από τον σχεδιασμό.

3.2 Διαλειτουργικότητα ΠΣ

Σε ένα διεθνοποιημένο περιβάλλον, όπου άνθρωποι, ασθενείς και αγαθά κινούνται από τόπο σε τόπο, από χώρα σε χώρα και από ήπειρο σε ήπειρο, θα πρέπει να λαμβάνεται επίσης υπόψιν εκτός από την λειτουργικότητα και την ιδιωτικότητα και η διαλειτουργικότητα.

Ο σκοπός της διαλειτουργικότητας είναι η επικοινωνία μεταξύ των υποσυστημάτων ενός ΠΣ ή μεταξύ διαφορετικών ΠΣ, ελαχιστοποιώντας ταυτόχρονα τη διαταραχή στη ροή των δεδομένων από τις πηγές προς τους χρήστες των δεδομένων, καθώς και τον κίνδυνο διακοπής αυτής. Για να επιτευχθεί όπως όλα στην πληροφορική χρειάζεται προτυποποίηση, και κοινές τεχνικές προδιαγραφές. Αυτό μπορεί να επιτευχθεί με τον καθορισμό επιπέδων διαλειτουργικότητας, μέσω του σημασιολογικού ιστού, και με τεχνολογικές γλώσσες όπως η Rdf, η XML, η HL7, χρησιμοποιώντας πρότυπες βιβλιοθήκες κοινά αποδεκτές, και δημιουργώντας όπου χρειάζεται κατάλληλες βιβλιοθήκες και πρότυπα.

Η ευρωπαϊκή ένωση έχει στόχο τη διασυνοριακή υγειονομική περίθαλψη, και για αυτό δημιουργεί και στηρίζει σχετικές πρωτοβουλίες.

Μια τέτοια πρωτοβουλία αφορά τη διαλειτουργικότητα των συστημάτων ηλεκτρονικών ιατρικών φακέλλων, και το άλλο τις ευφυείς ανοικτές υπηρεσίες

(smart Open Services/EPSOS). Αυτές οι πρωτοβουλίες έχουν 22 εκατομμύρια ευρώ χρηματοδότηση ανα τριετία, από τα οποία τα 11 καλύπτονται από το πρόγραμμα ανταγωνιστικότητας και καινοτομίας της ευρωπαϊκής επιτροπής (CIP, competiveness-inovation programm).

Σύμφωνα με την CALLIOPE ή αλλιώς κάλεσμα για διαλειτουργικότητα, όλες οι χώρες που λαμβάνουν μέρος πρέπει να ακολουθούν 6 βασικές αρχές: Της **διαφάνειας, συμμετοχής, διασφάλισης ποιότητας, αναλογικότητας, συνοχής,** και **ηθικής.** Και το δίκτυο Καλλιόπη και το έργο epSOS (European Patients Smart Open Services) σχετίζονται με το ιατρικό απόρρητο, τη διαλειτουργικότητα, την ακεραιότητα και ασφάλεια των δεδομένων και τη συμβατότητα και ομοιογένεια τους σε διευρωπαϊκό επίπεδο (47).

Οι μεταφορές πληροφοριών από ένα σύστημα σε κάποιο άλλο γίνεται με χρήση ενός συνόλου πρωτοκόλλων, που αποτελούν τα πρότυπα επικοινωνίας. Σημαντικό είναι αυτό να γίνεται με εξασφάλιση κατά το δυνατόν της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας αυτών κατά την μεταφορά (CIA). Ο νέος κλάδος της ηλεκτρονικής υγείας με τον οποίο σχετίζονται όλες αυτές οι πρωτοβουλίες είναι ο τρίτος μεγαλύτερος τομέας της υγείας, με κύκλο εργασιών 11δις ευρώ. Μπορεί να είναι και σημαντικό ποσοστό του συνολικού προϋπολογισμού για την υγεία (6% το 2015) (47).

3.2.1 **Ευρωπαϊκό πλαίσιο διαλειτουργικότητας- Στρατηγική εφαρμογής**

Σύμφωνα με το ευρωπαϊκό πλαίσιο διαλειτουργικότητας (ΕΠΔ), ως διαλειτουργικότητα “**νοείται η ικανότητα των φορέων, οργανισμών, μονάδων δημόσιας διοίκησης, να αλληλεπιδρούν προς την κατεύθυνση της επίτευξης αμοιβαία ωφέλιμων στόχων,** οι οποίοι αφορούν την ανταλλαγή πληροφοριών και γνώσεων μεταξύ των εν λόγω οργανισμών διά μέσου των επιχειρησιακών διαδικασιών που υποστηρίζουν, μέσω της ανταλλαγής δεδομένων μεταξύ των οικείων συστημάτων ΤΠΕ.” Ανάμεσα στις βασικές αρχές του ΕΠΔ είναι και η ιδιωτικότητα και ασφάλεια. Το ΕΠΔ προβλέπει επίσης 4 επίπεδα, που απεικονίζονται στον ακόλουθο πίνακα (51).

***Πίνακας 1. Επίπεδα διαλειτουργικότητας* (51)**

Σύμφωνα με το ευρωπαϊκό πλαίσιο διαλειτουργικότητας, τα επίπεδα διαλειτουργικότητας είναι τα ακόλουθα:

- Επίπεδο νομικό, δηλαδή η ύπαρξη συμβατών νομοθεσιών διευρωπαϊκά.

- Επίπεδο επιχειρησιακό των διαδικασιών, δηλαδή συμβατές διαδικασίες ανάμεσα σε διαφορετικές δομές εντός ή εκτός ενος οργανισμού, ώστε να μπορούν να συνεργαστούν και να ανταλλάξουν πληροφορίες αποτελεσματικά.

- Επίπεδο σημασιολογικό. Ότι δηλαδή η πληροφορία που ανταλάσσεται έχει την ίδια σημασία για όλα τα μέρη. Απαραίτητη είναι η επεξεργασία των δεδομένων από πλευράς ολοκλήρωσης, λειτουργικότητας και παρουσίασης.

- Επίπεδο τεχνικό. Δηλαδή όλα τα τεχνικά θέματα να είναι συμβατά.

Η νομική διαλειτουργικότητα είναι απαραίτητη προκειμένου να υπάρχει συνεργασία μεταξύ οργανισμών ή κρατών που λειτουργούν σύμφωνα με διαφορετικά νομικά πλαίσια, πολιτικές και στρατηγικές. Προϋποθέτει να γίνουν έλεγχοι διαλειτουργικότητας που να εξετάσουν την ισχύουσα νομοθεσία, και

να εντοπίσουν εάν υπάρχουν νομικοί φραγμοί, περιορισμοί ή εμπόδια τομεακά, εθνικά ή άλλα (51).

Το επιχειρησιακό επίπεδο σε ένα κατανεμημένο ΠΣΝ ειδικότερα, περιλαμβάνει τόσο τις λειτουργίες των εργαστηρίων, του φαρμακείου, των κλινικών, όσο και των διοικητικών, οικονομικών τμημάτων του νοσοκομείου, βιβλιοθήκης, της ιατρικής εκπαίδευσης της βασισμένης σε Η/Υ, την τηλειατρική κλπ (43).

Το CEN ENV 12967-1 (σύμφωνα με την HISA - Health Informatics Service Architecture, ή αλλιώς αρχιτεκτονική υπηρεσιών πληροφορικής υγείας) είναι ένα πρότυπο που προωθείται από την ευρωπαϊκή επιτροπή, και αναφέρεται σε τρία επίπεδα. Από αυτά το ενδιάμεσο επίιπεδο, που χρειάζεται για **την διαλειτουργικότητα μεταξύ των διαφορετικών υποσυστημάτων επιτυγχάνεται μέσω της γλώσσας HL7 (middleware) ενός ΟΠΣΥ.** Αυτό κρίνεται απαραίτητο, προκειμένου να διασυνδεθούν τα ετερογενή υποσυστήματα ενός νοσοκομειακού οργανισμού, που όμως διατηρούν και διαχειρίζονται ένα κοινό σύνολο δεδομένων και υπηρεσιών. **Τα άλλα δυο επίπεδα σύμφωνα με τη HISA, είναι: εκείνο των εφαρμογών** (για τα επιμέρους τμήματα του νοσοκομείου), **και το bitways** (τεχνολογικό επίπεδο, για τη φυσική δικτυακή σύνδεση ετερογενών πληροφοριακών υποσυστημάτων σε ένα ΟΠΣΥ) (47).

Το πρότυπο της HISA **υλοποιήθηκε από την τεχνική επιτροπή του CEN** του ευρωπαϊκού οργανισμού τυποποίησης, **την technical comitee (TC) 251 για την Πληροφορική Υγείας.** Η επιτροπή αποτελείτο από 4 ομάδες εργασίας που ασχολούνταν με τα εξής θέματα: ΠΣΥ, συστήματα ορολογίας και εννοιών, ασφάλεια, και τεχνολογίες διαλειτουργικότητας.

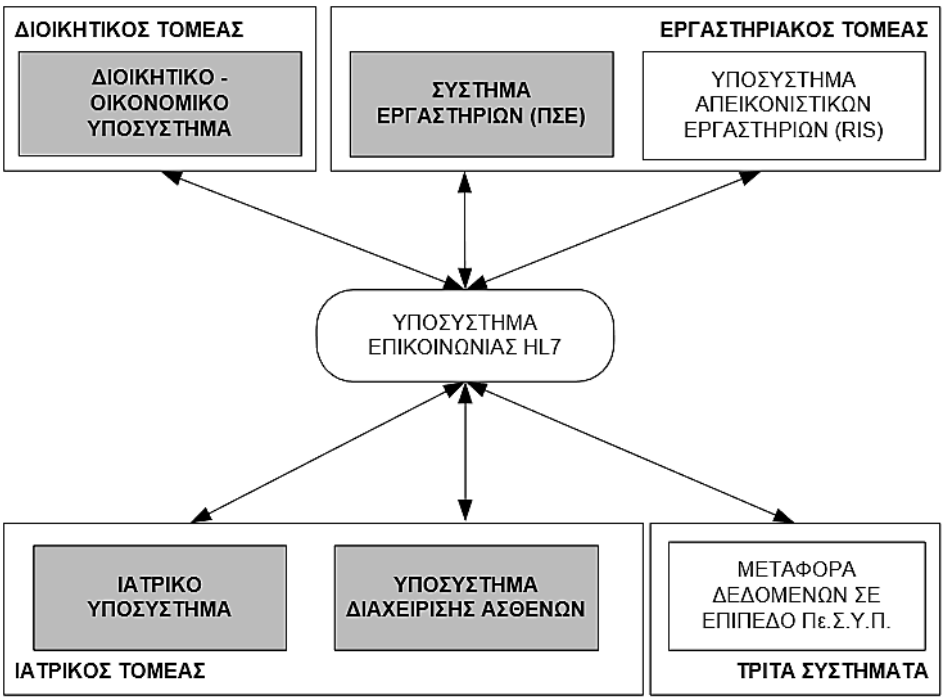
Σχετικός με τη διαλειτουργικότητα είναι ο οργανισμός **ISO/TC215,** έχει και αυτός τεχνική επιτροπή με έξι ομάδες εργασίας - working groups WG1-6, εκ των οποίων το WG 4, ασχολείται με την ασφάλεια (47).

Ο οργανισμός HL7 συστάθηκε το 1987 στις ΗΠΑ, αλλά πλέον βρίσκεται σε όλες τις ηπείρους, και σε κάθε χώρα της Ευρώπης. Παρέχει το πρότυπο

ανταλλαγής πληροφοριών μέσω μηνυμάτων ανάμεσα στα διάφορα υποσυστήματα ενός ΟΠΣΥ.

Από το 2003 λειτουργεί στην Ελλάδα το ελληνικό τμήμα του HL7, που αποσκοπεί να εξασφαλίσει την επικοινωνία όλων αυτών των διαφορετικών υποσυστημάτων και την τεχνική προσαρμογή των προτύπων HL7, στις απαιτήσεις του ελλληνικού χώρου.

Παρέχει ένα κοινό πρωτόκολλο για τις διεπαφές ανταλλαγής των ΠΣ, και για να κατανοήσουν τα στοιχεία που ανταλλάσουν. Επιπλέον καθορίζει τα trigger events και τα error messaging που προκύπτουν όταν η ανταλλαγή δεδομένων δεν είναι επιτυχής (52).



***Εικόνα 4. Ανταλλαγή μηνυμάτων HL-7 - διαλειτουργικότητα* (52)**

Σχεδόν όλα τα ευφυή διαγνωστικά μηχανήματα μπορούν να μιλήσουν HL7, και έχει ήδη αναγνωριστεί από πολλά εθνικά ιδρύματα προτυποποίησης όπως ο ANSI (ΗΠΑ) και ο DIN (Γερμανία). Είναι ανεξάρτητη από τις πλατφόρμες και τις τεχνολογίες, και λειτουργεί στο 7ο επίπεδο του μοντέλου OSI δηλαδή στο επίπεδο των εφαρμογών.

Προκειμένου να επιτευχθεί η διαλειτουργικότητα, χρειάζονται να χρησιμοποιούνται πρότυπα δηλαδή διατάξεις από κάποιον επίσημο φορέα ευρέως αποδεκτό όπως ο ISO. Οι σχεδιαστές και οι κατασκευαστές ΠΣΥ πρέπει πλέον να τα χρησιμοποιούν, ώστε τα συστήματά τους να είναι συμβατά με άλλα και να λειτουργούν με κοινά αποδεκτό τρόπο (52).

Χρήσιμα πρότυπα διαλειτουργικότητας σε σημασιολογικό επίπεδο, στον τομέα της Υγείας είναι:

- Η διεθνής κατηγοριοποίηση ασθενειών ICD (International Classification of Diseases) της παγκόσμιας οργάνωσης υγείας (ΠΟΥ), που είναι αποδεκτή παγκοσμίως.

- Το SNOMED, που συντηρείται από το College of American Pathologists (CAP), και βοηθά στην συνταξινόμηση των ιατρικών όρων που περιγράφουν το ίδιο πράγμα. Για αυτό είναι εξαιρετικά χρήσιμο πρότυπο στην καταχώρηση στοιχείων ασθενών με ελεγχόμενο λεξιλόγιο, και στη δημιουργία και συντήρηση ηλεκτρονικών ιατρικών φακέλλων (EHR) – σύμφωνα με το Ευρωπαϊκό ινστιτούτο Φακέλλου του ασθενή (European institute for health records - **EuroRec**), που είναι ο ευρωπαϊκός οργανισμός πιστοποίησης και προτυποποίησης για τους ηλεκτρονικούς ιατρικούς φακέλλους. Χρησιμοποιείται επίσης από αντίστοιχους οργανισμούς που υπάρχουν και στα επιμέρους ευρωπαϊκά κράτη. **Στην Ελλάδα αυτός είναι το ΙΤΕ** - το ινστιτούτο τεχνολογίας και έρευνας, ενώ σε παγκόσμιο επίπεδο, ο αντίστοιχος οργανισμός είναι το **Medical record institute (MRI)** (47).

- Το DRG (Diagnosis-related group), είναι πρότυπο για οικονομικές αναλύσεις.

- Το PACS, (Picture Archiving & Communications System-Σύστημα Αρχειοθέτησης και μετάδοσης εικόνας), είναι online-σύστημα που επιτρέπει τη συλλογή, επεξεργασία και ανταλλαγή ψηφιακών εικόνων μεταξύ ΠΣΝ.

- Με το ARC/NEMA ομογενοποιήθηκαν οι συσκευές ιατρικής απεικόνησης ώστε να μπορούν να συνδέονται και να ανταλλάσουν σχετικές εικόνες και δεδομένα.

- Το Dicom (Digital Imaging and communications in Medicine) - είναι ένα σύστημα που επιτρέπει σε διαγνωστικές και θεραπευτικές συσκευές αλλά και Η/Υ από διάφορους κατασκευαστές, να μεταφέρουν ψηφιακές εικόνες (π.χ. αξονικές τομογραφίες), και χρησιμοποιεί το πρωτόκολλο TCP/IP.

Ως **πρότυπα ανάγνωσης** που χαρακτηρίζουν τον ασθενή λειτουργούν αριθμοί, όπως της κοινωνικής ασφάλισης (ΑΜΚΑ - τα Social security number ή SSN). Ανάλογοι κωδικοί υπάρχουν για γιατρούς και προμηθευτές.

Σε νομοθετικό επίπεδο τα πρότυπα εξασφάλισης του απορρήτου των δεδομένων αναφέρονται σε νομοθετικές πράξεις όπως π.χ. στη Βρεττανία η Data Protection act και η Computer Misuse Act.

Σε επίπεδο τεχνολογικό τα διάφορα ΠΣ, θα πρέπει να χρησιμοποιούν συμβατές τεχνολογίες που να μην δημιουργούν προβλήματα στην διαλειτουργικότητα.

Η ηλεκτρονική ανταλλαγή αρχείων απαιτεί τη χρήση τυποποιημένων μηνυμάτων μεταξύ ετερογενών ΠΣΥ, τη χρήση αποτελεσματικών μέτρων προστασίας δεδομένων και ασφάλειας των ΠΣ.

Συμπερασματικά σε αυτό το κεφάλαιο εξετάσαμε την δομή των ΠΣ στον χώρο της υγείας, τα θέματα της προστασίας τους και των δεδομένων, την ανάγκη για ιδιωτικότητα από τον σχεδιασμό, αλλά και τις προκλήσεις που δημιουργεί η εφαρμογή των ευρωπαϊκών πρωτοβουλιών διαλειτουργικότητας στους τομείς ενδιαφέροντος της εργασίας.

Κεφάλαιο 4ο: Το διαδίκτυο

4.1 Ανασκόπηση και σημασία

Παλαιότερα οι υπολογιστές ήταν μεμονωμένοι ή σε μικρά τοπικά δίκτυα καλά ελεγχόμενα, οπότε και οι κίνδυνοι ήταν λιγότεροι και πιο εύκολο να αντιμετωπιστούν, σήμερα είναι πιο πολλοί λόγω και του διαδικτύου – internet. Αυτός ο παράγοντας πρέπει επίσης να λαμβάνεται καλά υπ΄όψιν από κάποιον που θέλει να προστατέψει τα ΔΠΧ, και τα ΠΣΥ, και αυτό θα εξεταστεί στο παρόν κεφάλαιο.

Το διαδίκτυο αναπτύχθηκε αρχικά τη δεκαετία του 1950 με την λειτουργία του αρπανετ, που επινοήθηκε σαν μέσο προστασίας από διαταραχές στις επικοινωνίες κρίσιμων υποδομών και από επιθέσεις εναντίον τους δολιοφθοράς ή καταστροφής. Αργότερα διασυνδέθηκαν μεταξύ τους κάποια ΠΣ αμερικανικών πανεπιστημίων. Χάρη στον Tim Berners Lee τον θεωρούμενο ως πατέρα του διαδικτύου που το εισήγαγε στο ευρύ κοινό, αποτελεί σήμερα θεμελιακό κομμάτι της ΚτΠ, και ο σύγχρονος κόσμος το χρησιμοποιεί για να επικοινωνεί, εργάζεται, ψυχαγωγείται, εκπαιδεύεται και το κάνει για πολλές ώρες στη διάρκεια μιας ημέρας.

Περιγράφεται σαν **ένα τεράστιο πλέγμα ψηφιακών γραμμών**, που διασυνδέει συσκευές και ανθρώπους, ταχύτερα από ποτέ με ένα κλικ ποντικιού ή με το πάτημα ενός κουμπιού στο πληκτρολόγιο. Ένα γράμμα που χρειαζόταν πολλές μέρες για να ταξιδέψει από μια ήπειρο σε μια άλλη, τώρα φτάνει στον προορισμό του σε δευτερόλεπτα με τη μορφή ηλεκτρονικού ταχυδρομείου. Έχει κάνει εξαιρετικά εύκολη τη ζωή από πολλές απόψεις, και έχει καταστήσει την πληροφορία στην σύγχρονη εποχή κυρίαρχη.

Βασικό του χαρακτηριστικό είναι το ότι η πληροφορία **δεν κινείται μέσω μιας συγκεκριμένης πορείας.** Έτσι παρέχει ασφάλεια στην επικοινωνία, αφού αν ένα τμήμα του δικτύου καταστραφεί τυχαία ή εσκεμμένα τότε οι πληροφορίες ακολουθούν άλλη δίοδο που παρακάμπτει το κατεστραμμένο τμήμα, και έτσι

συνεχίζεται η απρόσκοπτη ροή των πακέτων όπως ονομάζεται η κατάσταση στην οποία μεταφέρονται τα δεδομένα.

Το διαδίκτυο αποτελεί μία από τις βάσεις της σημερινής κοινωνίας. Στα σπουδαιότερα πλεονεκτήματα του έχουν περιληφθεί, η ταχύτητα και η άνεση. Στο διαδίκτυο ο γεωγραφικός τόπος δεν έχει σημασία. Ειδικότερα όλοι οι συνδεδεμένοι με το διαδίκτυο Η/Υ, συνεργάζονται για να μεταφέρουν πληροφορίες προς διάφορες κατευθύνσεις σε όλο τον κόσμο.

Με την αποστολή μιας ηλεκτρονικής πληροφορίας αυτή χωρίζεται από το TCP (Transmission Control Protocol) και το IP (Internet Protocol) σε μικρότερα κομμάτια που ονομάζονται πακέτα (packets). Το κάθε πακέτο αποκτά τη δική του ταυτότητα και ακολουθεί διαφορετικό δρόμο για να φτάσει στον προορισμό του.

Όταν η ηλεκτρονική πληροφορία φτάσει στον προορισμό της, τότε όλα τα διασπασμένα κομμάτια (πακέτα) της πληροφορίας ενώνονται ξανά, και υπεύθυνο για την ασφαλή και ορθή επανένωση τους είναι πάλι το TCP (Transmission Control Protocol), και το IP (Internet Protocol).

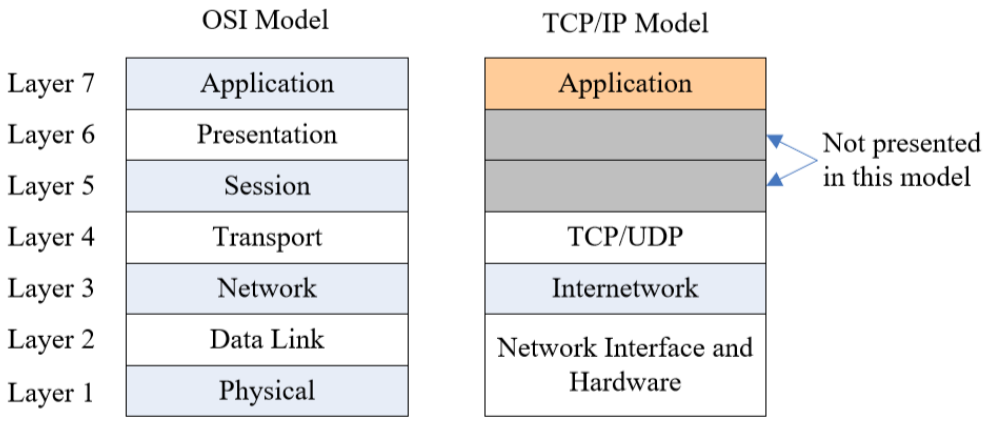
Την κυκλοφορία μέσω του διαδικτύου διευθύνει ένας ειδικός υπολογιστής που ονομάζεται δρομολογητής (Router). Ένα πακέτο μπορεί να περάσει από πολλούς Routers ως τον τελικό προορισμό του. Ρούτερ σύμφωνα με το RFC 4949 (request for comments) είναι μια πύλη ανάμεσα σε δυο δίκτυα στο επίπεδο 3 του OSI (δικτύου), και προωθεί ή κατευθύνει τα πακέτα δεδομένων μεσα στο διαδίκτυο.

4.2 Πρωτόκολλα διαδικτυακής επικοινωνίας

Δύο είναι οι σημαντικότεροι διεθνείς οργανισμοί τυποποίησης στον χώρο των τηλεπικοινωνιών και είναι υπεύθυνοι για πολλά πρότυπα και πρωτόκολλα επικοινωνίας: Η ITU- International Telecommunication Union διεθνής ένωση Τηλεπικοινωνιών (με 193 κράτη μέλη) είναι πιο εξειδικευμένη για τις τηλεπικοινωνίες, και ο ISO – International Standardisation Organisation που είναι μη κυβερνητική οργάνωση-ΜΚΟ (non governmental organization-NGO), με 163 κράτη μέλη και έδρα την Ελβετία (2).

Ο ISO το 1980 παρουσίασε το **μοντέλο Ανοικτής Διασύνδεσης Συστημάτων** με 7 στρώματα το γνωστό OSI - Open Systems interconnection, που είναι και το επικρατούν πλέον μοντέλο στις τηλεπικοινωνίες και τα δίκτυα. Σε αυτό επικρατεί μια ιεραρχική σχεδίαση, στην οποία κάθε επίπεδο εσωκλείει τα δεδομένα σε ένα φάκελλο με header και trailer, πριν το περάσει στο επόμενο επίπεδο (2).

Ανάλογο του OSI αλλά πιο πρακτικό, είναι το πρωτόκολλο TCP/IP (Transmission Control Protocol/ Internet Protocol), μέσω του οποίου κινούνται τα πακέτα στο διαδίκτυο. Είναι γνωστό και ως μοντέλο του Υπουργείου Άμυνας (Department of Defence - DoD), επειδή η ανάπτυξη της μεθόδου δικτύωσης χρηματοδοτήθηκε από το Υπουργείο Άμυνας των ΗΠΑ, μέσω της DARPA (Defense Advanced Research Projects Agency). Το UDP(User Datagram Protocol), που είναι πιο απλό και λιγότερο ασφαλές και είναι κατάλληλο για μικρά δίκτυα.



***Εικόνα 5. Τα μοντέλα OSI and TCP/IP* (53)**

Για την μελέτη των πρωτοκόλλων των τηλεπικοινωνιών χρησιμοποιείται η έννοια της στοίβας πρωτοκόλλων TCP/IP, **όπου κάθε επίπεδο επιτελεί διαφορετικές λειτουργίες, και υλοποιεί διαφορετικά πρωτόκολλα.** Σύμφωνα με την στοίβα TCP/IP υφίστανται πέντε επίπεδα, που μοιάζουν με τη διαστρωμάτωση OSI, μόνο που εδώ το επίπεδο εφαρμογής ενοποιεί τα επιμέρους επίπεδα συνόδου, παρουσίασης και εφαρμογής. Αυτό είναι **γνωστό και ως υβριδικό μοντέλο**, ενώ το γνήσιο απεικονίζεται με τέσσερα

μόνο επίπεδα όπως στην πιο πάνω εικόνα, όπου έχουν συγχωνευτεί επιπλέον και το επίπεδο Data link με το Physical (2).

Η επικοινωνία σε **επίπεδο εφαρμογής** γίνεται μέσω του πρωτοκόλλου HTTP - Hyper Text Transfer Protocol, και υφίστανται δυο εκδοχές: αυτή του πελάτη-εξυπηρετητή (client-server) που χρησιμοποιούν όλοι στα σπίτια, και η άλλη που είναι το μοντέλο των ισότιμων οντοτήτων (peer to peer ή P2P). Το δεύτερο (P2P), είναι πιο σύγχρονο από το πρώτο, ταχύτερο, και επιτρέπει την μεταφορά μεγάλου όγκου δεδομένων σε πιο πολλούς χρήστες. Σε αυτό κάθε χρήστης είναι ταυτόχρονα και πελάτης και εξυπηρετητής, ενώ πλεονεκτεί και στο ότι δεν υπερφορτώνεται ο εξυπηρετητής.

Το πρωτόκολο HTTPS (hypertext transfer protocol secure), αλλιώς ονομάζεται HTTP πάνω από ασφαλές επίπεδο μεταφοράς (Transport Layer Security-TLS), ή HTTP πάνω από SSL, ή ασφαλές HTTP. Είναι ένα πρωτόκολλο για ασφαλείς επικοινωνίες μέσω δικτύου, και είναι ευρέως διαδεδομένο στο διαδίκτυο.

Το HTTPS συνίσταται σε επικοινωνία μέσω πρωτοκόλλου μεταφοράς υπερκειμένου HTTP, εν τω μέσω κρυπτογραφημένης σύνδεσης με Transport Layer Security ή τον πρόγονο αυτής το Secure Sockets Layer.

Συντελεί στην ταυτοποίηση του επισκεπτόμενου ιστοτόπου και του εξυπηρετητή, και την προστασία της ιδιωτικότητας και της ακεραιότητας των ανταλασσόμενων πακέτων. Με αυτόν τον τρόπο προστατεύει από επιθέσεις man-in-the-middle. **Παρέχει επίσης αμφίδρομη κρυπτογράφηση των επικοινωνιών** ανάμεσα στον πελάτη και τον εξυπηρετητή, προστατεύοντας έτσι από eavesdropping, και παραποίηση ή διασάλευση του περιεχομένου των πακέτων που ανταλάσσονται από κάποιο τρίτο πρόσωπο (2).

Ιστορικά το HTTPS χρησίμεψε αρχικά για ηλεκτρονικές πληρωμές, και άλλες ευαίσθητες συναλλαγές σε εταιρικά ΠΣ-Corporate Information Systems (CIS). Σταδιακά η χρήση του έγινε εκτεταμένη, παρέχοντας προστασία των επικοινωνιών, της ιδιωτικότητας αλλά και αυθεντικοποίηση των ιστοτόπων.

Η επικοινωνία μεταξύ του επιπέδου εφαρμογής και μεταφοράς γίνεται μέσα από ειδικές δομές που **υλοποιούνται στο λειτουργικό** σύστημα, και καλούνται **θύρες - ports**. Προκειμένου να μεταφερθούν τα πακέτα του μηνύματος, από τη θύρα στην κατάλληλη υποδοχή - socket της εφαρμογής, άρα και στην κατάλληλη εφαρμογή, χρησιμοποιούνται ειδικά αναγνωριστικά των θυρών από τα σόκετ του λειτουργικού. Αυτά μαζί με τις IP διευθύνσεις, μπορούν να παράσχουν συσχετισμό μεταξύ μηνυμάτων και των sockets (2)**.** Ο αριθμός θυρών του αποστολέα και του παραλήπτη μεταφέρονται μαζί με τα δεδομένα, και οι δημοφιλείς εφαρμογές, όπως το www το email κλπ. έχουν γνωστούς αριθμούς ports.

Η IANA (Internet Assigned Numbers Authority), είναι υπεύθυνη για το συντονισμό των υπηρεσιών ονομάτων – τομέων (domain - name), τη διευθυνσιοδότηση και άλλες υπηρεσίες σχετικές με τα πρωτόκολλα διαδικτύου, όπως η καταχώρηση αριθμών συνήθων θυρών (για γνωστές υπηρεσίες διαδικτύου). Οι αριθμοί θυρών κατανέμονται σε τρείς κατηγορίες. Τις πολύ γνωστές από 0 εως 1023, τις καταχωρημένες στην IANA από 1024 εως 49151, και τις δυναμικές ή ιδιωτικές 49152 εως 65535- ephemeral ports.

Παραδείγματα της πρώτης κατηγορίας είναι :

- 21: File Transfer Protocol (FTP)
- 22: Secure Shell (SSH)
- 23: Telnet remote login service
- 25: Simple Mail Transfer Protocol (SMTP)
- 53: Domain Name System (DNS) service
- 80: Hypertext Transfer Protocol (HTTP) used in the World Wide Web
- 110: Post Office Protocol (POP3)
- 119: Network News Transfer Protocol (NNTP)
- 123: Network Time Protocol (NTP)

- 143: Internet Message Access Protocol (IMAP)
- 161: Simple Network Management Protocol (SNMP)
- 194: Internet Relay Chat (IRC)
- 443: HTTP Secure (HTTPS)

Ο όρος θύρες σε Η/Υ χρησιμοποιείται για υποδοχείς, **στο λογισμικό όμως περιγράφουν μια λογική σύνδεση, μια εξειδικευμένη διαδικασία επικοινωνιακής φύσης.** Πάντα σχετίζονται με τη διεύθυνση IP μιας συσκευής και τον τύπο πρωτοκόλου επικοινωνίας. Αφού επιτευχθεί η αρχική επικοινωνία με τις ευρέως γνωστές θύρες, αυτές στη συνέχεια απελευθερώνονται μεταφέροντας την επικοινωνία σε άλλη θύρα ούτως ώστε και άλλοι πελάτες να μπορούν να εξυπηρετηθούν.

Οι θύρες χρησιμοποιούνται κατεξοχήν από πρωτόκολλα μεταφοράς όπως το Transmission Control Protocol (TCP), και το User Datagram Protocol (UDP). Οι ανοικτές θύρες λειτουργούν και ως πύλες στην ασφαλή περίμετρο, που πίσω από αυτές περιμένουν socket των εφαρμογών για συνδέσεις με πακέτα από το διαδίκτυο. Για την ασφάλεια δικτύου χρειάζεται ένα τείχος πυροπροστασίας που να ελέγχει ποιες θύρες είναι ανοικτές, και ποιες κλειστές σε ένα εξυπηρετητή που συνδέεεται στο διαδίκτυο.

Κανονικά οι θύρες δεν πρέπει να είναι όλες ανοικτές αλλά μόνο όσες χρειάζονται με βάση τις ανάγκες των εφαρμογών-socket, όπως π.χ. η πόρτα 80 για το διαδίκτυο ή άλλες αν χρειάζονται για απομακρυσμένη διαχείριση του συστήματος όπως η πόρτα 22**. Η ρύθμιση των ανοικτών ή μη θυρών των εξυπηρετητών γίνεται με το firewall** (2)**.**

Πιο απλό από το TCP/IP πρωτόκολο σε επίπεδο μεταφοράς είναι το UDP, που παρέχει μόνο πολυπλεξία (χρησιμοποιώντας πάλι αναγνωριστικά ports για να οδηγηθούν τα δεδομένα από τον πελάτη στις εφαρμογές του εξυπηρετητή), και ανίχνευση, αλλά δεν παρέχει διόρθωση σφαλμάτων. Το UDP αναφέρει το σφάλμα, όμως παραδίδει το πακέτο και συνεπώς δεν εγγυάται την άνευ σφαλμάτων παράδοση, γι αυτό προτιμάται μόνο σε

συγκεκριμένες εφαρμογές πραγματικού χρόνου που δεν είναι τόσο απαιτητικές, και μπορεί να υπάρχει ανοχή για σφάλματα μεταφοράς όπως π.χ. σε IP τηλεφωνία ή IP τηλεόραση.

Στο **επίπεδο μεταφοράς** επιτελούνται οι λειτουργίες της πολυπλεξίας (δηλαδή της μεταφοράς πολλαπλών σημάτων ταυτόχρονα στον ίδιο δίαυλο), της εγγυημένης παράδοσης, του ελέγχου ροής και του ελέγχου συμφόρησης. Το TCP εκτελείται στα άκρα του δικτύου και δεν έχει εικόνα για μια κατάσταση συμφόρησης αλλά μπορεί να την αντιληφθεί όταν υπάρχει απώλεια πακέτων που την υποδηλώνουν. Σε αυτή την περίπτωση, το TCP μειώνει το ρυθμό μετάδοσης του στο μισό, και σταδιακά τον αυξάνει πάλι μέχρι να συμβεί η επόμενη απώλεια. Αυτοί λοιπόν **είναι οι μηχανισμοί προστασίας σε επίπεδο μεταφοράς** (2)**.**

Στο επίπεδο δικτύου η βασική λειτουργία του είναι η δρομολόγηση, δηλαδή να επιλέξει τα επιμέρους δίκτυα και τις τηλεπικοινωνιακές ζεύξεις (που οδηγούν στους επόμενους δρομολογητές) μέσω των οποίων θα διέλθει το κάθε πακέτο προκειμένου να μεταφερθεί στο επίπεδο μεταφοράς του παραλήπτη. Βασίζεται στην ύπαρξη ενός πίνακα δρομολόγησης που υπάρχει σε κάθε δρομολογητή και που αντιστοιχίζει συνοπτικά τις διευθύνσεις παραλήπτη και τη θύρα εξόδου στον δρομολογητή. Αυτή η διαδικασία καλείται **αυτοδύναμη προώθηση πακέτων**, γιατί κάθε πακέτο προωθείται ξεχωριστά, και είναι αυτή που ακολουθείται σε δίκτυα τύπου TCP/IP (2)**.** Αυτό είναι χρήσιμο και από πλευράς ασφάλειας, αφού ένας κακόβουλος θα πρέπει να συλλέξει το σύνολο των πακέτων και με τη σωστή σειρά εάν θέλει να υποκλέψει ένα μήνυμα.

Βασικό ρόλο στο επίπεδο δικτύου παίζουν οι IP διευθύνσεις, οι οποίες αποτελούνται από 4 bytes, καθένα από τα οποία έχει 8 bits (octets) ή αλλιώς ψηφία (εξού και ψηφιακή επικοινωνία). Έτσι είναι σχεδιασμένο το σύστημα διευθυνσιοδότησης IPv4, ενώ υπάρχει ήδη το IPv6 που προσφέρει θεωρητικά απεριόριστες διευθύνσεις.

Θεωρητικά εάν θέλει ο διαχειριστής του τοπικού δικτύου μπορεί να ορίσει στατικές διαδρομές μεταξύ δρομολογητών, κάτι που μπορεί να γίνει σε

μεγάλους οργανισμούς όπως τα συστήματα υγείας, τα νοσοκομεία, και κέντρα υγείας, ενώ στα οικιακά μοντέλα επικρατούν οι δυναμικές IP λόγω του περιορισμένου αριθμού διευθύνσεων, **μέσω του πρωτοκόλου DHCP (Dynamic Host Configuration Protocol)**, και οι IP διευθύνσεις ανατίθενται σε κάποιον χρήστη κάθε φορά για ένα συγκεκριμένο χρονικό διάστημα π.χ. μιας ημέρας και μετά αλλάζει η IP του, ούτως ώστε να εξυπηρετηθούν όσο το δυνατόν περισσότεροι χρήστες με την επαναχρησιμοποίηση των ίδιων επικοινωνιακών πόρων.

Η δυναμική IP ανατίθεται σε κάποιον άλλον κάθε φορά που κάποιος αποσυνδέεται. Έτσι το IP που είχε κάποιος αρχικά μπορεί να το έχει κάποια άλλη συσκευή στη συνέχεια, όμως **όλες αυτές οι αλλαγές καταχωρούνται σε ειδικούς πίνακες τους ARP** (address resolution protocol), ώστε να κατευθύνονται τα πακέτα πάντα στο σωστό παραλήπτη από τον σωστό αποστολέα, και να υπάρχει ασφάλεια των επικοινωνιών (2)**.**

Ακολουθεί **το επίπεδο ζεύξης δεδομένων (Data Link)**, που ασχολείται με την πλαισίωση, τον έλεγχο και τη διόρθωση σφαλμάτων, τον έλεγχο της ροής και την πολλαπλή πρόσβαση. Σε αυτό το επίπεδο απαιτούνται διευθύνσεις – **αναγνωριστικά Media Access Control (MAC)**, για να διαχωρίζονται οι μεταδόσεις μεταξύ κόμβων και εφόσον κάποιος κόμβος λάβει ένα πλαίσιο που δεν προορίζεται για αυτόν οφείλει να το απορρίψει, ώστε να φτάσει μόνο στον σωστό παραλήπτη (2)**.**

4.3 Ασύρματα Δίκτυα

Η διασύνδεση με Ethernet (IEEE 802.3 - Bob Metcalfe), είναι η πιο διαδεδομένη, αποτελεσματική και οικονομική μέθοδος σύνδεσης στο διαδίκτυο. Διαδεδομένη όμως είναι και η ασύρματη σύνδεση μέσω Wi-Fi (προτύπου IEEE 802.11). Στις ασύρματες συνδέσεις συσκευών σε δίκτυα υπάρχουν ακόμα περισσότερα θέματα ασφάλειας. Υπάρχει η ασφάλεια ALOHA: σύμφωνα με αυτή η μόνη δικλείδα ασφάλειας που έχει ένα ασύρματο δίκτυο, είναι το στάδιο χειραψίας ενός χρήστη με το δίκτυο και τους άλλους χρήστες που επιβεβαιώνει ποιος είναι ποιος, και αρχίζει η επικοινωνία.

Αυτό επινοήθηκε στο πανεπιστήμιο της Χαβάης, προκειμένου να συνδέσει τους κεντρικούς Η/Υ της Χονολουλού με χρήστες στα υπόλοιπα νησιά χωρίς υποθαλάσσια καλώδια, και προκειμένου να αποφευχθούν τα προβλήματα που δημιουργούν οι συγκρούσεις πακέτων (collisions) από χρήστες που χρησιμοποιούν το ίδιο κανάλι (54).

Το **πρωτόκολλο Secure Socket Layer - SSL,** περιλαμβάνει μια φάση χειραψίας που αρχικά επιτρέπει στον πελάτη και τον εξυπηρετητή να ταυτοποιήσουν ο ένας τον άλλο με κρυπτογραφικές τεχνικές δημοσίου κλειδιού, όπως ο RSA. Στη συνέχεια της συνόδου τους επιτρέπει να δημιουργήσουν και να **ανταλλάξουν συμμετρικά κλειδιά που βοηθούν την γρήγορη** κρυπτογράφηση και αποκρυπτογράφηση μεγάλου όγκου δεδομένων, που μεταφέρονται στη διάρκεια μιας συνόδου (2).

Περαιτέρω η κινητικότητα που συχνά έχουν οι ασύρματες συσκευές αποτελεί επιπλέον κίνδυνο να κλαπούν ή να χαθούν και να πέσουν σε λάθος χέρια. Επίσης έχουν προβλήματα εξάντλησης της ενέργειας τους (π.χ. αν λειτουργούν με μπαταρίες).

Στα ασύρματα δίκτυα όπως και στα ενσύρματα πρέπει να χρησιμοποιούνται **πρωτόκολλα ασφάλειας στο επίπεδο δικτύου ή διευθύνσεων IP** όπως **το IP layer (IPsec)**, καθώς και στο επίπεδο μεταφοράς TCP layer (TLS/SSL). Αυτά τα πρωτόκολλα δικτύου μπορούν εύκολα να παραβιαστούν.

Πολλά από αυτά τα πρωτόκολλα αφορούν μόνο την ασφαλή δικτυακή πρόσβαση τοποθεσίας – **παρέχουν ασφαλή σύνδεση ανάμεσα σε μια ασύρματη συσκευή και το σημείο πρόσβασης**, το σταθμό βάσης ή την πύλη εισόδου (55). Πολλές μελέτες δείχνουν ότι η ασφάλεια των ασύρματων επικοινωνιών είναι ανεπαρκής και μπορούν να παραβιαστούν από χάκερς.

Για την ασφάλεια της πρόσβασης μπορούν να χρησιμοποιηθούν απλές τεχνικές όπως: κώδικες ή εισαγωγή pin, αλλά και πιο εξελιγμένες μέθοδοι όπως η βιομετρική ταυτοποίηση. Αν κλαπούν οι συσκευές τότε αυτές οι τεχνικές προσφέρουν ένα βασικό επιπεδο προστασίας και ταυτοποίησης.

Προκειμένου για ασύρματες συσκεύες, η πρόσβαση τους στο internet γίνεται μέσω **802.11 προτύπων ή αλλιώς WAP - Wireless Access Protocol**. Υπάρχουν τα 802.11b, a, n και άλλα πιο σύγχρονα. Για τις ασύρματες συσκευές υπάρχει ακόμα μεγαλύτερος κίνδυνος υποκλοπής στοιχείων και επικοινωνίας (π.χ. μπορεί πιο εύκολα να κλαπούν), και ως εκ τούτου χρειάζεται ακόμα μεγαλύτερη ασφάλεια.

Η πύλη του ασύρματου πρωτοκόλλου πρόσβασης - WAP μεταφράζει κυκλοφορία πακέτων πρωτοκόλλου WAP, από και προς την ασύρματη συσκευή πελάτη με κατεύθυνση προς τους συνήθεις εξυπηρετητές που λειτουργούν με συμβατικά πρωτόκολλα διαδικτύου (HTTP/TCP/IP) διευκολύνοντας την συνεργασία.

Το πρωτόκολλο WAP 1.X, είναι κατάλληλο για μικρές συσκευές με μικρή διάρκεια μπαταρίας που θέλουν να έχουν ισχυρή πρόσβαση στο internet. – όπως τα κινητά. Αυτό αποτελείται από πέντε επίπεδα.

- WIRELESS APPLICATION ENVIRONMENT (WAE) - Περιβάλλον ασύρματης εφαρμογής.
- WIRELESS SESSION PROTOCOL (WSP) - Πρωτόκολλο ασύρματης σύνδεσης.
- WIRELESS TRANSACTION PROTOCOL (WTP) - Πρωτόκολλο ασύρματων συναλλαγών.
- WIRELESS TRANSPORT LAYER SECURITY (WTLS) - Ασφάλεια Επιπέδου Μεταφοράς - Ασύρματης Επικοινωνίας.
- WIRELESS DATAGRAM PROTOCOL (WDP) - Πρωτόκολλο ασύρματης τεχνολογίας ροής δεδομένων.

Η ασφάλεια WTLS λειτουργεί στο επίπεδο μεταφοράς παρόμοια με το SSL (ή με το νεότερο TLS), παρέχοντας τόσο στον server όσο και στον client ταυτοποίηση **μέσω X.509 πιστοποιητικών**. Λειτουργεί ως προαιρετικό στρώμα παρέχοντας έναν μηχανισμό ασφαλείας βασισμένο στη κρυπτογράφηση δημόσιου κλειδιού όπως το TLS (56), (57).

Το ασύρματο πρωτόκολλο κρυπτογράφησης WEP είναι ενσωματωμένο στο WiFi, προκειμένου να κρυπτογραφεί τα δεδομένα επικοινωνίας μεταξύ μιας συσκευής-πελάτη και ενός σημείου ασύρματης πρόσβασης (AP). Το πρότυπο WEP έχει πλέον ξεπερασθεί και έχει δώσει τη θέση στα περισσότερο δυνατά και ασφαλή πρότυπα WPA και WPA2. Βοηθούσε στην αποδοτικότητα του συστήματος αφού απάλλασσε τους χρήστες από την αγορά εξειδικευμένου λογισμικού, ή την αγορά και συντήρηση ακριβών και δύσκολων στην παραμετροποίηση εξυπηρετητών. Τους προσέφερε αποθήκευση δεδομένων χωρίς τη χρήση δικού τους υλικού ή λογισμικού, δίνοντάς τους ευελιξία στην αποθήκευση δεδομένων. Με αυτούς τους τρόπους οι χρήστες επίσης εκτελούσαν τις εργασίες τους πιο αποτελεσματικά και πιο αξιόπιστα (58).

4.3.1 **Wireless Security**

Στην εργασία του ο Boncella.R. (57) παρουσιάζει μια επισκόπηση του τρόπου που επιτυγχάνεται ένα ασφαλές κανάλι επικοινωνίας, σε ασύρματο περιβάλλον που χρησιμοποιεί τα 802.11 πρότυπα, ή WAP.

Το ασύρματο περιβάλλον πλεονεκτεί από πλευράς ελευθερίας και ικανότητας επικοινωνίας από οπουδήποτε και οποτεδήποτε και για αυτό οι χρήστες φαίνεται να το προτιμούν, όμως παρουσιάζει προβλήματα ασφάλειας (αυθεντικοποίησης, ακεραιότητας και εμπιστευτικότητας). Η εργασία του Boncella εστιάζει στο να παρουσιάσει τις τεχνικές ασφαλείας που υπάρχουν για Wireless Local Area Network (WLAN), και για ασύρματες συσκευές που χρησιμοποιούνται για πρόσβαση στο internet (57).

Τα WLAN είναι πιο κατάλληλα για οικιακούς χρήστες ή για μικρά δίκτυα με χαμηλές απαιτήσεις σε ασφάλεια. Η φυσική πρόσβαση σε ένα WLAN είναι διαφορετική από ότι σε ένα ενσύρματο LAN που απαιτεί συγκεκριμένα σημεία φυσικής πρόσβασης στο κτίριο, δυσκολεύοντας το να συνδεθεί ο οποιοσδήποτε μέσω κλειδιών ή καρτών.

Ένα **ασύρματο σημείο πρόσβασης AP (Access Point)**, μπορεί να γίνει προσβάσιμο και εκτός του κτιρίου ή των υποδομών εάν το σήμα είναι ανιχνεύσιμο, γι αυτό απαιτείται να απομονώνουμε το AP από το εσωτερικό

δίκτυο εως ότου γίνει ταυτοποίηση μιας συσκευής και αφου γίνει αυτό το βήμα, μετά ταυτοποιείται και ο χρήστης αυτής και μπορεί να ζητήσει ένα ασφαλές κανάλι επικοινωνίας. Όλα αυτά γίνονται μέσω του **προτύπου 802.11**.

Το ασύρματο σήμα που μεταφέρει τα δεδομένα, χρησιμοποιεί είτε ηλεκτρομαγνητικά κύματα είτε ραδιοσυχνότητα, είτε υπέρυθρη συχνότητα, που είναι τμήματα του ηλεκτρομαγνητικού φάσματος. Η ραδιοσυχνότητα πλεονεκτεί έναντι της υπέρυθρης επικοινωνίας και έχει τρείς ζώνες την βιομηχανική, την επιστημονική και την ιατρική (ISM-RF band). Συνήθως τα δίκτυα χρησιμοποιούν την RF 2,4GHz (57).

Ο Boncella (57) περιγράφει επίσης την **αρχιτεκτονική ενός WLAN.** Ένα WLAN έχει σταθμούς και ένα σημείο πρόσβασης AP. Η βασική του δομή καλείται **BSS, basic service set**. Το AP χρησιμεύει ως ενδιάμεσος σταθμός με δύο hops για επικοινωνία μεταξύ δύο σταθμών, και χρησιμεύει για τη κατασκευή ενός BSS που έχει κάποια λειτουργία ελέγχου πρόσβασης. Αν συνδυαστούν διάφορα BSS έχουμε την κατασκευή ESS – extended service set που επιτρέπει στο χρήστη να μετακινείται από σημείο σε σημείο, χωρίς να χάνει τη σύνδεση του (57).

Τα πιο συχνά Exploits που μπορεί να συμβούν σε ένα WLAN είναι:

•Insertion Attacks - Παρείσφρυση, δηλαδή ένας μη εξουσιοδοτημένος χρήστης εισχωρεί στο σύστημα μέσω ενός BSS για να προσεγγίσσει τις διανομές σε ένα ESS - extended service set με το οποίο αυτό είναι συνδεδεμένο, και με σκοπό να χρησιμοποιεί τις δομές internet χωρίς να πληρώνει.

•Interception - Υποκλοπή, μελών του BSS όπου με παθητική στάση κρυφακούει τι κάνουν τα άλλα μέλη στο BSS, και μπορεί να κάνει ανάλυση πακέτων αν αυτά δεν είναι κρυπτογραφημένα ή αλλιώς ανάλυση κυκλοφορίας. Μπορεί επίσης να κλωνοποίησει το κανονικό AP, με αποτέλεσμα να καταλάβει το BSS και να κάνει επιθέσεις κρυπτογράφησης των πακέτων που μεταδίδονται μέσω WEP πρωτοκόλλου που έχει υπονομευθεί.

•Mac spoofing - Επιθέσεις παραποίησης όπου κάποιος εκτός λίστας του σημείου πρόσβασης (APL), μπορεί να αλλάξει την MAC - διεύθυνση με την οποία εμφανίζεται στο διαδίκτυο ώστε να χρησιμοποιήσει μια που είναι αποδεκτή στο Σημείο Πρόσβασης (AP). Αυτό μπορεί να το πετύχει χρησιμοποιώντας ένα «ανιχνευτικό» λογισμικό (packet sniffer), που πολλές φορές το βρίσκει δωρεάν στο διαδίκτυο, και βρίσκοντας ποιες διευθύνσεις είναι κάθε φορά αποδεκτές από το AP να προσποιηθεί μια από αυτές προκειμένου να συνδεθεί.

•Denial of Service (DoS) – Επιθέσεις άρνησης εξυπηρέτησης μέσω μπλοκαρίσματος του σήματος που είναι broadcast, από οποιαδήποτε συσκευή μεταδίδει στις συχνότητες ISM.

•Brute Force attacks ενάντια στους κωδικούς των AP.

•Man in the Middle Attacs όπου γίνεται επίθεση στο Address Resolution Protocol (ARP) μέσω των πινάκων cache του διαχειριστή - controller και των τερματικών, προκειμένου να αποκτηθεί παράνομη πρόσβαση στο ΠΣ, και να παρεμβληθούν μεταξύ δύο νόμιμων χρηστών που δεν αντιλαμβάνονται ότι τα δεδομένα που ανταλάσσουν παίρνουν άλλη πορεία διαμέσω της MAC Address του επιτιθέμενου (57).

4.3.2 **Προστασία WLAN**

Για προστασία από αυτές τις επιθέσεις ο Boncella (57) αναφέρει τρεις βασικές μεθόδους προκειμένου να ασφαλίσει κάποιος τα κανάλια ασύρματης επικοινωνίας.

Αυτές οι μέθοδοι προστασίας είναι:

- Service Set Identifier (SSID),
- Media Access Control (MAC),
- Wired Equivalent Privacy (WEP).

Μπορεί να εφαρμοστούν και ξεχωριστά όμως πιο αποτελεσματικό είναι να χρησιμοποιούνται όλες (57).

Το SSID χωρίζει ένα ασύρματο δίκτυο σε περισσότερα, με δικό τους το καθένα σημείο AP. Το κάθε AP έχει δικό του SSID, και προκειμένου να έχει πρόσβαση ένας Η/Υ σε αυτό το AP που αντιπροσωπεύει ένα τμήμα δικτύου, θα πρέπει να έχει διαμορφωθεί κατάλληλα αλλιώς δεν έχει πρόσβαση, λειτουργεί δηλαδή κάπως σαν συνθηματικό. Αν χρειάζεται ο Η/Υ μπορεί να είναι ρυθμισμένος και για άλλα SSID.

Το MAC Address filtering, με το οποίο αναγνωρίζεται η συσκευή μέσω της **802.11 κάρτας δικτύου** της που φέρει τη μοναδική διεύθυνση MAC. Κάθε AP έχει μια λίστα διευθύνσεων MAC, και αν εκείνη κάποιας συσκευής δεν περιλαμβάνεται σε αυτήν, τότε δεν επιτρέπει την πρόσβαση στο AP, ακόμα και εάν το SSID ταιριάζει.

Το WEP πρωτόκολο μέσω του προτύπου 802.11 παρέχει κρυπτογραφημένα μηνύματα, ανάμεσα στους πελάτες και το AP. Χρησιμοποιεί ένα συμμετρικό κλειδί κρυπτογράφησης RSA. **Όλοι οι hosts και το AP θα χρησιμοποιούν το ίδιο κλειδί** για να κρυπτογραφούν και να αποκρυπτογραφούν δεδομένα. Συνήθως πρόκειται για κλειδί μεγέθους 40 bit, αν και μπορεί να είναι και 104. Αυτό είναι συνδυασμένο με ένα άξονα αρχικοποίησης μήκους 24 bit και συνεπώς το τελικό μέγεθος θα είναι αντίστοιχα ή 64 ή 128 bits. Το διαμοιρασμένο κλειδί μπορεί να χρησιμοποιηθεί για την ταυτοποίηση του Η/Υ του χρήστη, με μιας διαδικασία αναγνώρισης τεσσάρων βημάτων. Οι χρήστες θα πρέπει να αλλάζουν τα κλειδιά τους σε συχνή βάση προκειμένου να ελαχιστοποιηθούν οι όποιοι κίνδυνοι.

Το AES-advanced encryption standard, θεωρείται πιθανός αντικαταστάτης του WEP που είναι ευαίσθητο σε επιθέσεις (57).

Επίσης θα χρειαστούν και περιβάλλοντα sandboxes όπου να δοκιμάζονται μη ελεγμένοι κώδικες σε συνδυασμό με ψηφιακά πιστοποιητικά για να πιστοποιούν την ποιότητα ατόμων και προγραμμάτων μέσα στο διαδίκτυο που ενδεχομένως να θέλουμε να εγκαταστήσουμε, έτσι ώστε να προστατεύεται το ΠΣ από επιθέσεις εκμετάλλευσης και από ενέσεις κακόβουλου κώδικα (55). Η χρήση «sandbox» (περιβάλλοντος δοκιμασίας-εκτέλεσης προγραμμάτων), με την απόδοση ψηφιακών πιστοποιητικών στη

συνέχεια για τα πιστοποιημένα - ασφαλή εκτελέσιμα προγράμματα, μπορούν να ελαχιστοποιήσουν την πιθανότητα κάποιου malware να παρεισφρύσει στην ασύρματη συσκευή.

Τα πρωτόκολλα κρυπτογράφησης μπορούν επίσης να προσαρμοστούν για ασύρματες συσκευές τροποποιώντας τις σχετικές πολιτικές τους, χρησιμοποιώντας, π.χ. πιο απλούς αλγόριθμους που μπορεί να υποστηριχτούν από αυτές. Η πλατφόρμα MOSES προάγει την επιτάχυνση προτοκόλλων ασφαλείας όπως το SSL, IPsec, WTLS κλπ και χρησιμοποιεί για ασφαλείς συναλλαγές συσκευών- χειρός την τροποποίηση OpenSSL του SSL (55).

4.3.3 **VPN**

Τέλος για εγγυημένη ασφάλεια από άκρο σε άκρο μιας ασύρματης σύνδεσης, μπορεί να χρησιμοποιηθεί ένα **VPN-virtual private network**, εναλλακτικά στο SSID/ MAC ADDRESS FILTERING/ WEP PROTOCOL, ιδιαίτερα όταν υπάρχουν υψηλές απαιτήσεις ασφάλειας και πολλοί πελάτες. Για να λειτουργήσει, χρειάζεται να εγκατασταθεί στο δίκτυο που θέλει να προσεγγίσει ο πελάτης ένας VPN-εξυπηρετητής, και ο πελάτης να έχει εγκατεστημένο VPN-λογισμικό πελάτη. Το εικονικό ιδιωτικό δίκτύο είναι μια αποτελεσματική μέθοδος κρυπτογράφησης δεδομένων, λειτουργεί σαν επικάλυψη μιας φανερής δομής, και βοηθάει στην πρόσβαση από ένα μη έμπιστο δίκτυο στο ελεγχόμενο δίκτυο (57).

4.4 Το πρωτοκολλό SNMP

Η παρακολούθηση, ο έλεγχος, η ρύθμιση και η συντήρηση της καλής λειτουργίας του συστήματος δικτύου και των επιμέρους τμημάτων του, γίνεται από τη **διαδικασία της Διαχείρισης Δικτύων**.

Αυτή είναι μια σύνθετη διαδικασία, και σε ένα πολύπλοκο δίκτυο δεν μπορεί να πραγματοποιηθεί στηριζόμενη στην ανθρώπινη προσπάθεια μόνο, αλλά χρειάζονται και αυτοματοποιημένα εργαλεία.

Το **απλό πρωτόκολο διαχείρισης δικτύου** το Simple Network Management System (SNMP), είναι αυτό που διαχειρίζεται και παρακολουθεί τους πόρους του δικτύου (59). Ένα απλό πρωτόκολλο διαχείρισης καθορίζει κοινές μορφές δεδομένων και παραμέτρων και κάνει εύκολη την ανάκτηση πληροφοριών. Το σύνθετο πρωτόκολλο προσθέτει επιπλέον δυνατότητες αλλαγής και δυνατότητες ασφάλειας. Το Απλό Πρωτόκολλο Διαχείρισης Δικτύου είναι το πιο σύνηθες, χρησιμεύει ως πλαίσιο που παρέχει διευκολύνσεις για τη διαχείριση και παρακολούθηση των πόρων του δικτύου.

Είναι εργαλείο για τη διαλειτουργική διαχείριση του δικτύου και χρησιμοποιείται για ένα ευρύ φάσμα προϊόντων, όπως τελικά/τερματικά συστήματα, switches, routers, γέφυρες, και άλλο τηλεπικοινωνιακό εξοπλισμό. **Καθορίζει ένα σύνολο από πρότυπα** με τα οποία καθίσταται δυνατή η διαχείριση του δικτύου με: ένα πρωτόκολλο, μια προδιαγραφή δομής βάσης δεδομένων, και ένα σύνολο αντικειμένων δεδομένων (59). Βασίζεται στο πρωτόκολλο TCP/IP για τις επικοινωνίες.

Συστατικά του πλαισίου SNMP είναι :

- Τα πρωτόκολλα SNMP.

- Οι πράκτορες SNMP.

- Οι διαχειριστές SNMP.

- Οι βάσεις Διαχείρισης Πληροφοριών (Management Information Bases – MIB). Τα αντικείμενα στη Βάση Πληροφοριών Διαχείρισης είναι χωρισμένα σε τάξεις (classes) με δεντρική δομή. Το κάθε αντικείμενο αντιστοιχεί σε συγκεκριμένο αναγνωριστικό.

΄Ενας πράκτορας SNMP είναι μια λειτουργική μονάδα (λογισμικό), που βρίσκεται σε κάθε μια διαχειριζόμενη συσκευή (Η/Υ, δρομολογητής, εκτυπωτής, κλπ), και παρέχει τις πληροφορίες διαχείρισης σε μια Βάση Δεδομένων. Επίσης οι πράκτορες αποδέχονται οδηγίες για να ρυθμιστεί η συσκευή. Οι πληροφορίες από τη βάση δεδομένων Β.Δ., βρίσκονται στις βάσεις διαχείρισης πληροφοριών (Management Information Bases- MIB).

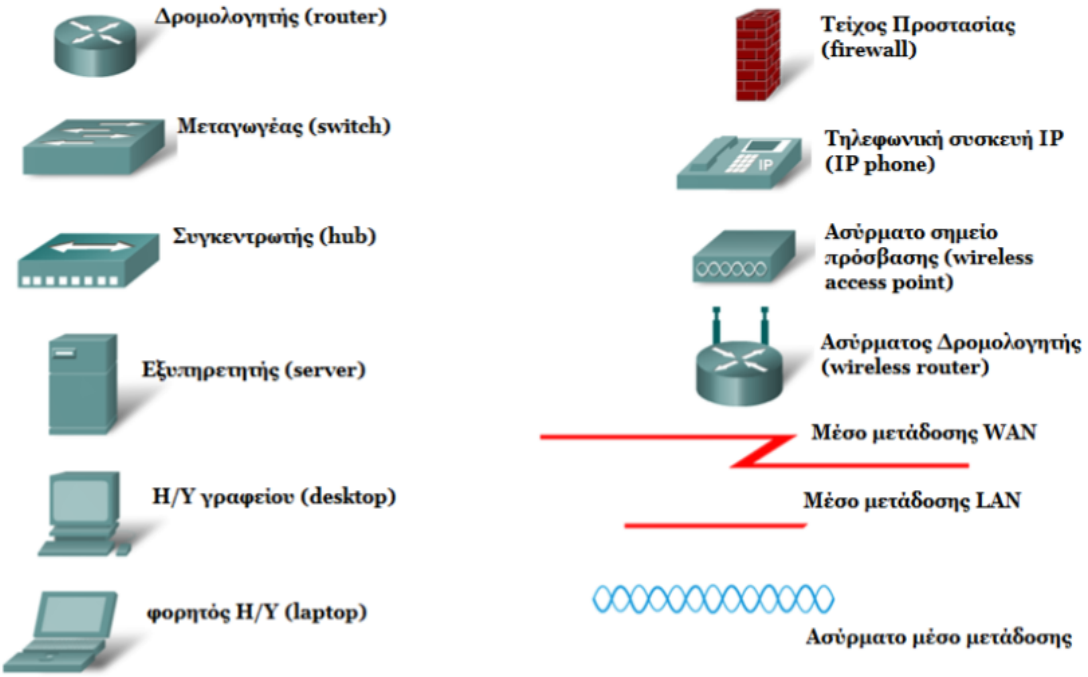
Ο διαχειριστής SNMP είναι ένα πρωτόκολλο επιπέδου εφαρμογής. Παρέχει πληροφορίες διαχείρισης σχετικά με τη διαχείριση συσκευής στον υπεύθυνο. Αποδέχεται τις οδηγίες για να ρυθμιστεί η συσκευή (59).

Για να την καλύτερη οργάνωσή του, το διαδίκτυο χωρίζεται σε περιοχές ή αλλιώς αυτόνομα συστήματα (Autonomous Systems-AS), όπου κάθε AS βρίσκεται κάτω από την ίδια διαχειριστική αρχή (π.χ. ελέγχονται από τον ίδιο πάροχο ή ανήκουν στο ίδιο εταιρικό δίκτυο). Αυτόνομα συστήματα είναι μεγάλου μεγέθους δίκτυα που προκύπτουν από την ομαδοποίηση κοντινών IP.

Για την επικοινωνία και την δρομολόγηση των πακέτων στο διαδίκτυο, χρειάζονται πρωτόκολλα δρομολόγησης, που διακρίνονται ανάλογα:

- με τον τρόπο λειτουργίας (στατικό ή δυναμικό),
- τον σκοπό (πρωτόκολλα εσωτερικής πύλης για επικοινωνία μεταξύ συσκευών στο ίδιο AS, ή εξωτερικής πύλης για επικοινωνία μεταξύ συσκευών διαφορετικών AS),
- και τη συμπεριφορά (classfull ή classless) πρωτόκολλα δρομολόγησης (59).

Στην εικόνα που ακολουθεί παρουσιάζονται οι γνωστοί συμβολισμοί που χρησιμοποιούνται στις διάφορες απεικονίσεις αρχιτεκτονικής διαχείρισης δικτύου.



***Εικόνα 6. Γνωστοί συμβολισμοί απεικόνισης αρχιτεκτονικής δικτύου* (59)**

4.4.1 **Λογισμικό Διαχείρισης Δικτύου**

Πολλοί μεγάλοι οργανισμοί για τη σωστή λειτουργία τους πρέπει να χρησιμοποιούν λογισμικό διαχείρισης δικτύου. Αυτό χρησιμεύει για την παρακολούθηση και τον έλεγχο των δικτύων τους, από ένα Σύστημα Διαχείρισης Δικτύων (NMS) - network management system.

Σύμφωνα με τον ISO, η Διαχείριση Δικτύου αφορά 5 κατηγορίες: τη ρύθμιση, τα σφάλματα, την επίδοση, την ασφάλεια και τη λογιστική. Ειδικότερα για τη **διαχείριση της ασφάλειας αυτή θα αφορά στην παραγωγή, διανομή και αποθήκευση των κλειδιών κρυπτογράφησης.** Ασχολείται επίσης με τους κωδικούς πρόσβασης και με άλλες πληροφορίες εξουσιοδότησης ή ελέγχου πρόσβασης, καθώς και με την παρακολούθηση της πρόσβασης Η/Υ σε δίκτυα και επίσης με τα αρχεία καταγραφής.

Η **διαχείριση των σφαλμάτων** ανιχνεύει και δίνει λύσεις σε σφάλματα στο δίκτυο. Σφάλμα θεωρείται μια ανώμαλη κατάσταση που απαιτεί ανάληψη δράσης για την επισκευή του (π.χ. σε περίπτωση καταστροφής κάποιας

γραμμής). Η **διαχείριση της ρύθμισης** αφορά τη ρύθμιση διάφορων παραμέτρων συνδεσιμότητας των στοιχείων του δικτύου ανάλογα με τις εκάστοτε ανάγκες των χρηστών (59).

4.5 Ασφάλεια σε όλα τα επίπεδα του δικτύου

Από τα παραπάνω καταλαβαίνουμε πόσο σημαντική είναι η ασφάλεια σε όλα τα επίπεδα του δικτύου. Στο επίπεδο του διαδικτύου υπάρχει το πρωτόκολλο ασφάλειας του διαδικτύου ή **Internet Protocol Security (IPsec)**, που προσφέρει ένα ασφαλές κανάλι επικοινωνίας μεταξύ δυο συσκευών κρυπτογραφώντας τα περιεχόμενα κάθε πακέτου. Έχει πρότυπα στο επίπεδο δικτύου για δύο τρόπους μεταφοράς:

- Μοντέλο μεταφοράς, που κρυπτογραφεί μόνο τα δεδομένα χωρίς να επεμβαίνει στην Επικεφαλίδα (Header) και

- Μοντέλο τούνελ, που βάζει μια καινούργια επικεφαλίδα ενω κρυπτογραφεί και την αρχική επικεφαλίδα, σε κάθε πακέτο και είναι πιο ασφαλές. Στον αποδέκτη της πληροφορίας μια συσκευή συμβατή με IPsec αποκρυπτογραφεί στη συνέχεια το κάθε πακέτο (59).

Στην IETF (Internet Engineering Task Force) που αναπτύσσει και προωθεί τα εθελοντικά πρότυπα του Διαδικτύου έκαναν τροποποιήσεις στην τρίτη έκδοση του πρωτοκόλλου **Secure Sockets Layer-SSL3.0,** στο επίπεδο μεταφοράς και **δημιούργησαν ένα νέο πρωτόκολλο το Transport Layer Security (TLS)**. Συχνά οι δυο όροι περιγράφουν την ίδια έννοια.

Το Secure Shell (SSH). Αυτό είναι μια διεπαφή εντολών και ένα πρωτόκολλο, που επιτρέπει να επιτυγχάνεται ασφαλή πρόσβαση σε απομακρυσμένο Η/Υ, **και χρησιμοποιείται ευρέως από τους διαχειριστές** για να ελέγχουν εξυπηρετητές δικτύων και άλλους εξυπηρετητές από απόσταση. Η έκδοση SSH2, είναι μια ομάδα προτύπων από την IETF. Χρησιμεύει σαν μια ασφαλή εναλλακτική λύση αντί των αντίστοιχων εφαρμογών Telnet (που δεν χαρακτηρίζονται από ασφάλεια).

Τα VPN που χρησιμοποιούνται συχνά για να παρέχουν ασφαλή επικοινωνία ανάμεσα σε ένα μη έμπιστο δίκτυο (όπως π.χ. το διαδίκτυο) και σε ένα εσωτερικό έμπιστο δίκτυο. Οι συσκευές VPN που θα χρησιμοποιηθούν για να προστατέψουν τα συστήματα ελέγχου, θα πρέπει να τεστάρονται ενδελεχώς για συμβατότητα της τεχνολογίας τους με τις εφαρμογές και ότι δεν θα δημιουργήσουν προβλήματα στη ροή των πακέτων στο δίκτυο (59).

4.6 Πολιτικές και Μηχανισμοί ασφαλείας για δίκτυα ISO, IEC, ITU

Το **πρότυπο ISO/IEC 7498-1** αναφέρει **ότι κάθε επίπεδο πρωτοκόλου**, θα πρέπει να αφορά **τρία επιμέρους λειτουργικά επίπεδα**. Εκείνα των χρηστών, της σηματοδοσίας και ελέγχου, και της διαχείρισης.

Το ISO 27005, είναι ένα πρότυπο για τη διαχείριση του πληροφοριακού κινδύνου (1). Το ISO 27001 είναι πρότυπο για τον καθορισμό απαιτήσεων ασφάλειας ΠΣ και το ISO 27002 είναι πρότυπο για την εφαρμογή ΣΔΑΠ με βάση τις απαιτήσεις ασφάλειας του 27001.

Το πρότυπο ISO/IEC 7498-2 που είναι πρότυπο ασφάλισης δικτύου, αλλά και η αρχιτεκτονική ασφαλείας **ITU –T X.800** (60), βασίζονται στο 7498-1, και το επεκτείνουν για να καλύψουν τις πτυχές ασφάλειας δικτύων. Με βάση τα δυο αυτά πρότυπα, οι στόχοι ασφάλειας επιτυγχάνονται μέσω **πολιτικών και υπηρεσιών ασφαλείας** ενός οργανισμού.

4.6.1 Πρότυπο ISO 7498-2 – Υπηρεσίες ασφάλειας δικτύου

Ο κ.Παταρίδης αναφέρεται στο πρότυπο ISO 7498-2 (61). Σύμφωνα με αυτό, θα πρέπει **ένα δίκτυο να παρέχει τις ακόλουθες υπηρεσίες ασφάλειας:**

1. **Υπηρεσίες ταυτοποίησης**, που παρέχουν την εγγύηση για την ταυτότητα μιας οντότητας, ενός χρήστη (user authentication), ή της προέλευσης κάποιων δεδομένων (data origin authentication), και άρα εμπιστευτικότητα.
2. **Υπηρεσίες ακεραιότητας** (integrity), που να διασφαλίζουν ότι ένα μήνυμα δεν έχει παραποιηθεί. Δηλαδή όταν ένας χρήστης Α στέλνει

ένα μήνυμα σε ένα χρήστη Β, το περιεχόμενο θα πρέπει να είναι αναλλοίωτο. Θεωρεί ότι από μόνη της η ακεραιότητα των δεδομένων δεν έχει νόημα αλλά πρέπει και ταυτόχρονα να συνδυάζεται με την εξακρίβωση της πηγής προέλευσης των δεδομένων, να είναι αυθεντική.

3. **Υπηρεσίες μη αποποίησης ευθύνης** (non-repudiation). Προστατεύει από την άρνηση της συμμετοχής κάποιου σε μια σύνοδο επικοινωνίας, όπως επίσης όταν λαμβάνει ένα μήνυμα να μην μπορεί να αρνηθεί ότι το έλαβε. Αυτή η υπηρεσία σύμφωνα με το συγγραφέα επιτυγχάνεται με τη χρήση ψηφιακών υπογραφών.
4. **Υπηρεσίες εμπιστευτικότητας**, δηλαδή να προστατεύουν τα δεδομένα που διακινούνται στο διαδίκτυο από την αποκάλυψη τους σε μη εξουσιοδοτημένες οντότητες. Για κάθε τρίτο εκτός από τον Α και τον Β χρήστη, η πληροφορία θα πρέπει να παραμένει σε ακατανόητη μορφή.
5. **Υπηρεσίες ελέγχου πρόσβασης**, προστατεύουν τους πόρους, τις εφαρμογές του δικτύου, τα αρχεία και τα δεδομένα από μη εξουσιοδοτημένη προσπέλαση (61).

Οι **υπηρεσίες ασφαλείας** σύμφωνα με αυτά τα πρότυπα, υποστηρίζεται ότι επιτυγχάνονται με **τεχνικά μέσα**, ή αλλιώς **μηχανισμούς ασφαλείας**, όπως:

- μηχανισμούς κρυπτογράφησης (encipherment), με αλγόριθμους: RSA, ElGamal, DSA.
- ψηφιακές υπογραφές- Digital signatures,
- μηχανισμούς ελέγχου πρόσβασης - Access Control Mechanisms,
- μηχανισμούς ακεραιότητας δεδομένων-Integrity Mechanisms, όπου προσθέτοντας στα δεδομένα κάποια αθροίσματα ελέγχου μνήμης (checksums), μπορεί να αποδειχθεί πιθανή τροποποίηση των δεδομένων. Επίσης οι κώδικες αυθεντικοποίησης μυνήματος (Message Authentication Codes- MACs)
- μηχανισμούς ταυτοποίησης - Authentication Mechanisms, με χρήση κωδικών πρόσβασης (pin), κρυπτογραφικές τεχνικές ή βιομετρικά χαρακτηριστικά.

- μηχανισμούς προστασίας κίνησης (Traffic-Pading), παρέχουν προστασία από επιθέσεις ανάλυσης κίνησης,
- μηχανισμούς ελέγχου-δρομολόγησης Routing Control (επιτρέπουν την επιλογή μιας συγκεκριμένης διαδρομής για τα δεδομένα είτε στατικά είτε μέσω προσχεδιασμένων διαδρομών - μπορούν επίσης να τους προσθέτουν ετικέτες ασφαλείας),
- μηχανισμοί συμβουλαιογράφου - Notarization (μπορεί να παρέχονται από μια Τρίτη έμπιστη οντότητα) όπως κωδικοί, διπλά συνθηματικά, κάρτες, βιομετρικά κλπ (47)**.**

Σε ότι αφορά την **ευθύνη μιας ηλεκτρονικής ενέργειας** κανένας από τους συναλλασσόμενους, δεν πρέπει να έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή. Πρέπει να υπάρχει καταλογισμός της ευθύνης για την προέλευση, αποστολή, μετάδοση ή παραλαβή δεδομένων, π.χ. στο ηλεκτρονικό ταχυδρομείο, ο αποστολέας ή ο παραλήπτης ενός μηνύματος να μην μπορεί να αρνηθεί τη ευθύνη αποστολής/ παραλαβής του συγκεκριμένου μηνύματος. Στον χώρο της υγείας, η άσκηση της ιατρικής/ νοσηλευτικής πράξης φέρει απαιτήσεις υπευθυνότητας, συνεπώς ένα ΠΣΥ πρέπει να υποστηρίζει την **καταγραφή των συναλλαγών που λαμβάνουν χώρα (Log Files).** Ένας μηχανισμός για τη μη αποποίηση ευθύνης είναι η χρήση ψηφιακής υπογραφής σε συνδυασμό με την ύπαρξη μιας Έμπιστης Τρίτης Οντότητας – ΕΤΟ (Trusted Third Party – TTP).

Στην πιο κατω εικόνα από τον καθηγητή κ. Μαντά (62) παρουσιάζονται συγκεντρωτικά οι απαιτήσεις που υπάρχουν από ένα ΠΣ, οι απειλές ενάντια στην ικανοποιησή τους, οι συνέπειες που μπορεί να υπάρξουν για το ΠΣ αν οι απειλές δεν αντιμετωπιστούν, και τα αντίμετρα που θα πρέπει να λάβει ο διαχειριστής ενός ΠΣ εάν θέλει να το προφυλάξει.

***Πίνακας 2. Απαιτήσεις: ασφάλειας, απειλές, συνέπειες, αντίμετρα* (62)**

Απαίτηση	Απειλές	Συνέπειες	Αντίμετρα
Ακεραιότητα	· Τροποποίηση των δεδομένων · Trojan Horse · Τροποποίηση της μνήμης · Τροποποίηση της κίνησης των μηνυμάτων κατά τη μεταφορά	· Απώλεια πληροφορίας · Ευπάθεια σε όλες τις άλλες απειλές	· Ψηφιακές Υπογραφές
Εμπιστευτικότητα	· Υποκλοπή κατά τη μεταφορά · Κλοπή πληροφορίας από τους διακομιστές/ πελάτες · Πληροφορίες σχετικές με τη διαμόρφωση του Δικτύου	· Απώλεια πληροφορίας · Απώλεια μυστικότητας · Έκπτωση κύρους για τον οργανισμό · Οικονομικές Απώλειες	· Κρυπτογράφηση · Εικονικά Ιδιωτικά Δίκτυα · Ψηφιακά Πιστοποιητικά σε συνδυασμό με Ε.Τ.Ο.
Διαθεσιμότητα (Άρνηση Υπηρεσίας)	· Πλημμύρισμα υπολογιστικής μηχανής με 'σκουπίδια' · Περιορισμένοι Πόροι	· Οικονομικές απώλειες · Μη διαθεσιμότητα των υπηρεσιών · Έκπτωση κύρους για τον οργανισμό	· Firewall · Πόροι των συστημάτων ανάλογοι των απαιτήσεων
Αυθεντικοποίηση (Εξακρίβωση Γνησιότητας)	· Προσποίηση οντοτήτων	· Συνέπειες σε όλες τις παραμέτρους της ασφάλειας	· Τεχνικές αναγνώρισης της ταυτότητας των οντοτήτων

Η ασφάλεια πληροφοριών υγείας θα πρέπει να αφορά τέσσερις διακριτές περιοχές : 1) Την φυσική ασφάλεια (physical security) του εξοπλισμού και του κέντρου ελέγχου του ΠΣ. 2) Την ασφάλεια του υπολογιστικού συστήματος (computer security) - μέσω ελέγχου του ποιος έχει πρόσβαση στο ΠΣ και σε ποιους πόρους. 3) Την ασφάλεια των Βάσεων Δεδομένων (database security) – από πρόσβαση στη ΒΔ και επεξεργασία, και τέλος 4) την ασφάλεια δικτύων επικοινωνιών (network security) (62). Συμπερασματικά για όλους τους παραπάνω τομείς, θα πρέπει να υπάρχουν και να λειτουργούν συγκεκριμένες **πολιτικές ασφαλείας,** σύμφωνα με τις οποίες θα εφαρμόζονται αντίστοιχοι μηχανισμοί ασφαλείας, που θα ικανοποιούν μια σειρά από υπηρεσίες ασφάλειας.

4.6.2 **Φυσική ασφάλεια - Καταστροφές**

Σε περιπτώσεις φυσικών καταστροφών (τυφώνες, πλημμύρες, σεισμοί, πυρκαγιές), τρομοκρατικών επιθέσεων (βόμβες, όπλα, βιοχημικά όπλα, κλπ), και εγκληματικών ενεργειών (εμπρησμοί, κλοπές, κλπ), σημαντικές είναι δυο παράμετροι για ένα ΠΣ, η επαναλειτουργία συστήματος (εδώ ενδιαφέρει και ο χρόνος επαναλειτουργίας RTO - recovery time objective), και η επανάκτηση δεδομένων (63). Σε ότι αφορά τα δεδομένα θα πρέπει να είναι αποθηκευμένα και σε άλλη θέση από όπου μπορεί να ανακτηθούν με ασφάλεια και αξιοπιστία σε κάθε περίπτωση απώλειας συσκευής, ή φυσικής καταστροφής της βάσης δεδομένων.

4.7 Ασφάλεια στο επίπεδο Συνόδου (Cookies)

Σύμφωνα με την ομάδα εργασίας για το άρθρο 29 (WP 29), το **αρθρό 5.3 της οδηγίας 2002/58/EC,** μετά την ανθεώρησή του με την οδηγία 2009/136/EC ενισχύει την προστασία χρηστών δικτύων και υπηρεσιών απαιτώντας συγκατάθεση προτού κάποια πληροφορία αποθηκευτεί η προσπελαστεί στην συσκευή του χρήστη.

Το ίδιο άρθρο της οδηγίας 2002/58, επιτρέπει κάποια cookies να εξαιρούνται από τη συγκατάθεση του χρήστη, αν όμως πρώτα ικανοποιούν δυο απαιτήσεις (64).

Πρώτη απαίτηση, να χρησιμεύουν αποκλειστικά και μόνο για την επίτευξη μετάφορας πληροφοριών, και επικοινωνίας μέσω ενός δικτύου. Δεύτερη απαίτηση ο πάροχος μιας ομάδας υπηρεσιών πληροφοριών να μην μπορεί να παράσχει αυτές ή κάποιες από αυτές στον συνδρομητή εάν προηγουμένως οι υπηρεσίες αυτές ή κάποιες από αυτές δεν ζητήθηκαν ρητά από τον συνδρομητή. Ο πελάτης πρέπει να μπορεί να διαλέξει τι θέλει και τι δεν θέλει από το σύνολο των υπηρεσιών του παρόχου και όχι να είναι υποχρεωμένως να παίρνει σε πακέτο και άλλες που δεν θέλει (64). Αναλύεται επίσης

ενδελεχώς, ποιες μπορεί να είναι οι εξαιρέσεις από αυτόν τον κανόνα οσον αφορά τα cookies και την σχετική τεχνολογία.

Κάποια cookies θεωρούνται απαραίτητα για την επικοινωνία δυο συσκευών μεσω δικτύου (πρώτο κριτήριο) όπως είναι εκείνα που:

1) δρομολογούν την πληροφορία στο διαδίκτυο ταυτοποιώντας τα τελικά άκρα αυτής.

2) συμβάλλουν στην ανταλλαγή πακέτων δεδομένων με την σωστή σειρά, αριθμώντας τα.

3) ανιχνεύουν σφάλματα μετάδοσης ή απώλειες δεδομένων.

Αν ικανοποιούν έστω ένα από τα τρία παραπάνω στοιχεία τότε θεωρείται ότι ικανοποιούν και το πρώτο κριτήριο.

Σχετικά με το **δεύτερο κριτήριο θα πρέπει ταυτόχρονα:**

1) να έχει κάνει ο χρήστης κάποια επιβεβαιωτική ενέργεια που να δείχνει ότι θέλει την συγκεκριμένη υπηρεσία με σαφώς περιγεγραμμένο εύρος, και

2) τα cookies να είναι αυστηρά απαραίτητα για αυτή την υπηρεσία, έτσι που χωρίς αυτά η υπηρεσία δεν θα λειτουργούσε.

Τα cookies, διακρίνονται σε:

- συνόδου ή μόνιμα
- τρίτης οντότητας ή όχι

Τα συνόδου διαγράφονται αυτόματα όταν ο χρήστης κλείσει τον φυλλομετρητή του (λήξει η σύνοδος), ενώ αντίθετα τα μόνιμα cookies αποθηκεύονται στην συσκευή μέχρι να λήξει η διάρκεια ζωής τους (κάτι μπορεί να γίνει μετά από λεπτά, μέρες ή και χρόνια) (64).

Για τα τρίτης οντότητας cookies εξηγεί ότι σύμφωνα με την οδηγία 95/46/EC, παρότι **σαν τρίτο μέρος ορίζεται στις ΤΠΕ** κάθε φυσικό ή νομικό πρόσωπο, δημόσιος οργανισμός, εταιρεία ή ότι άλλο - εκτός από το υποκείμενο των δεδομένων, τον ελέγκτη τον επεξεργαστή, και τα άτομα που

υπόκεινται σε αυτούς και τα έχουν εξουσιοδότησει να επεξεργάζονται τα δεδομένα, **προκειμένου για browsers-φυλλομετρητές, η Τρίτη οντότητα ορίζεται αυστηρά κοιτώντας το URL (United resource location),** και το εαν τα cookies της ιστοσελίδας τοποθετούνται από ιστοσελίδες άλλες από εκείνη που επισκέπτεται ο χρήστης**, ακόμα και αν τα έχει βάλει ένας ελεγκτής δεδομένων ή όχι.**

Παρόλα αυτά τα cookies δεν λήγουν σε όλες τις περιπτώσεις τη στιγμή που σταματά η σύνοδος του φυλλομετρητή. Για παράδειγμα ο χρήστης μπορεί να έχει ζητήσει ρητά να θυμάται η υπηρεσία κάποιες πληροφορίες ενώ σε κάποιες περιπτώσεις όπως στο καλάθι αγορών, ο πωλητής μπορεί να ρυθμίσει τα cookies να καθυστερούν λίγο να λήξουν για την περίπτωση κάποιου τυχαίου σφάλματος του φυλλομετρητή. Αυτό έχει κάποια χρησιμότητα ενδεχομένως. Αντίθετα κάποιες νέες τεχνολογίες πάλι σύμφωνα με την ομάδα 29, επιτρέπουν στα cookies να παραμένουν επ' άπειρον στην συσκευή του χρήστη, παρά τις επίμονες προσπάθειες του να τα αφαιρέσει. Αυτά λέγονται "Ever-cookies" or "Zombie-cookies". Αυτά απαρέγκλειτα απαγορεύονται.

Τα cookies για πολυμεσικές συνόδους χρησιμεύουν για την κατάλληλη αποθήκευση τεχνικών δεδομένων, και για αναπαραγωγή βίντεο ή ήχου. Είναι γνωστά σαν **flash-cookies,** αφού η Adobe Flash είναι η επικρατούσα τεχνολογία στα διαδικτυακά βίντεο. Αυτά θα έπρεπε να λήγουν με το που λήγει η σύνοδος, όμως σύμφωνα με την οδηγία της WP29 θα μπορούσαν ίσως να παραμείνουν, εαν περιορίζονταν στα απολύτως απαραίτητα για την λειτουργία τους, και απέφευγαν οποιαδήποτε περιττή καταγραφή πληροφορίας (64).

Τα cookies ρύθμισης προτιμήσεων διεπαφής μπορεί να είναι συνόδου ή μόνιμα, ανάλογα τον σκοπό. Τυπικά τέτοια cookies προτιμήσεων είναι:

Τα γλωσσικής προτίμησης όπως αυτά σε μια ιστοσελίδα που ο χρήστης επιλέγει για παράδειγμα κάνοντας κλικ σε μια σημαία.

Τα σχετικά με σελίδες προτίμησης, ανάλογα με τον αριθμό των επιλογών του χρήστη. Αυτές οι υπηρεσίες πληροφοριών ρητώς πρέπει όμως να ενεργοποιήθηκαν από τον χρήστη.

Τα cookies κοινωνικής δικτύωσης. Τα μέσα κοινωνικής δικτύωσης προτείνουν στους διαχειριστές ιστοσελίδων “social plug-in modules”, που μπορεί να τα ενσωματώσουν στην πλατφόρμα τους, ώστε οι χρήστες να μπορούν να μοιράζονται περιεχόμενο με τους «φίλους» τους στα κοινωνικά δίκτυα. Αυτά πρέπει να αφορούν συνδεδεμένους χρήστες, και να υπάρχει ρητή αίτηση του χρήστη για να χρησιμοποιηθούν. Εϊναι μόνο για τη συγκεκριμένη σύνοδο, και θα πρέπει να λήγουν με το που ο χρήστης αποσυνδεθεί από το κοινωνικό του δίκτυο ή κλείσει ο φυλλομετρητής (64).

4.7.1 **Μη εξαιρούμενα cookies**

Οπωσδήποτε τα cookies παρακολούθησης που είναι εγκατεστημένα σε plug-ins π.χ. κοινωνικών δικτύων, πρέπει να μην εξαιρούνται. Αυτά παρακολουθούν τους χρήστες με cookies-τρίτης οντότητας για σκοπούς όπως να αποκτήσουν πληροφορίες πλοήγησης χρηστών σε διάφορες ιστοσελίδες, για συμπεριφορική διαφήμιση, αναλύσεις ή έρευνας αγοράς, και αποτελούν κατ΄εξοχήν απειλή για την ιδιωτικότητα.

Μελλοντικές εξαιρέσεις. Η ομάδα εργασίας WP29 επίσης προτείνε σε μια επόμενη αναθεώρηση να περιληφθούν στις εξαιρέσεις κάποια cookies μετά όμως από συγκατάθεση του χρήστη των υπηρεσιών, και υπό συγκεκριμένες προϋποθέσεις κάποια να παραμένουν για λίγες ώρες σε κάποιες περιπτώσεις. Όπως τα cookies ταυτοποίησης, τα cookies ανίχνευσης καταστρατήγησης υπηρεσιών ταυτοποιησής, τα flash- cookies, κλπ (64).

4.8 Ασφάλεια από τους παρόχους υπηρεσιών διαδικτύου

Η ΕΕΤΤ αναφέρει ότι απέστειλε ειδικά ερωτηματολόγια στις 6 μεγαλύτερες εταιρείες υπηρεσιών πρόσβασης στο διαδίκτυο (Cosmote, Cyta, Forthnet (Nova), OTE, Vodafone, Wind), που καλύπτουν μερίδιο συνδρομητών σχεδόν 100% (σύμφωνα με τα στοιχεία της ΕΕΤΤ για το Α’ εξάμηνο 2017). Σύμφωνα με την ΕΕΤΤ οι πάροχοι υπηρεσιών διαδικτύου στην Ελλάδα απαγορεύουν

την πρόσβαση σε παράνομους παρόχους τυχερών παιγνίων μέσω του διαδικτύου, όπως αυτοί αναφέρονται στον οικείο **κατάλογο (black list)** που τηρεί η Επιτροπή Εποπτείας και Ελέγχου Παιγνίων (ΕΕΕΠ). Η υποχρέωση προκύπτει από το Ν. 4002/2011 (άρθρο 51, παρ. 5). **Η λίστα με τις παράνομες ιστοσελίδες**, που αριθμεί περίπου 2000 ιστοσελίδες (Ιούνιος 2018), βρίσκεται στο https://www.gamingcommission.gov.gr/images/epopteia-kai-elegxos/blacklist/blacklist.xlsx (65). Τρείς από τους έξι παρόχους ανέφεραν ότι εφαρμόζουν απαγόρευση πρόσβασης σε ιστοσελίδες που περιέχουν περιεχόμενο με δικαιώματα πνευματικής ιδιοκτησίας, μετά από σχετική δικαστική απόφαση.

Η συχνότερη πρακτική ασφαλείας που εφαρμόζουν οι πάροχοι αφορά σε μέτρα πρόληψης και αντιμετώπισης κατανεμημένων επιθέσεων άρνησης υπηρεσίας (Distributed Denial-of-Service attack, DDoS attack), για τις οποίες εφαρμόζονται μέτρα όπως: **φραγή θυρών TCP/UDP**, φραγή **ευάλωτων πρωτοκόλλων** που χρησιμοποιούνται για τέτοιες επιθέσεις (π.χ. OSPF, NTP, Netbios), και **φραγή IP διευθύνσεων**. Αν δεν αντιμετωπιστούν τέτοιες επιθέσεις αυτό θα έχει ως αποτέλεσμα τη μη διαθεσιμότητα, ή την περιορισμένη διαθεσιμότητα υπηρεσιών πρόσβασης στο διαδίκτυο, **λόγω συμφόρησης στο δικτυακό εξοπλισμό** (65).

Για την προστασία από κακόβουλο λογισμικό και την προστασία από πιθανή απάτη γίνεται αποκλεισμός ονομάτων τομέων (DNS blocking), ενώ για την προστασία από επιθέσεις spam/phishing γίνεται αποκλεισμός εισερχομένων/εξερχομένων θυρών TCP (π.χ. SMTP θύρες). Από τις 10 εφαρμοζόμενες πρακτικές, οι 7 έχουν προσωρινό χαρακτήρα, ενώ οι 3 εφαρμόζονται πάντα. Η φραγή τομέων για προστασία από απάτη, ή ιστοσελίδων που βρίσκονται σε λίστες αποκλεισμού είναι μόνιμη, ωστόσο αλλάζει δυναμικά όταν ενημερώνονται οι λίστες ή παύει να υπάρχει λόγος αποκλεισμού. Τα αναφερόμενα μέτρα για την προστασία από spam/phishing αφορούν συγκεκριμένους συνδρομητές από τους οποίους πηγάζουν τέτοια μηνύματα και αίρονται όταν οι συνδρομητές αποκαταστήσουν το πρόβλημα.

Σε σχέση με την περίοδο 2016-2017, η ΕΕΤΤ αναφέρει ότι σημειώθηκε σημαντική **αύξηση του αριθμού παραπόνων** (186 έναντι 106, δηλ. αύξηση

75.47%). Η μεγάλη πλειοψηφία των παραπόνων συνεχίζει να αφορά στη γενική ποιότητα υπηρεσίας που λαμβάνουν οι συνδρομητές (65). Επιπλέον, αναφέρει ότι το επόμενο διάστημα θα γίνει αναβάθμιση της υποδομής του ΥΠΕΡΙΩΝ, με νέους εξυπηρετητές και σύνδεση στα 10 Gbps. Αναφορικά με την παρακολούθηση της απόδοσης στα κινητά δίκτυα, η ΕΕΤΤ εντός του 2018 θα θέσει σε λειτουργία πιλοτικά αρχικά, σύστημα μέτρησης των δεικτών ποιότητας δικτύων κινητών επικοινωνιών.

4.9 Mobile Health

Οι ιατρικές εφαρμογές για κινητά είναι εφαρμογές σχεδιασμένες να συγκεντρώνουν, να μετρούν και να μεταδίδουν ευαίσθητα προσωπικά δεδομένα υγείας που σύμφωνα με την ισχύουσα νομοθεσία οφείλουν να διατηρούνται ασφαλή.

Οι Ceara και McCaffery (66) στηρίζουν την μελέτη τους στην ασφάλεια ΔΠΧ το σχετικό πρότυπο IEC/TR 80001-2-2:2012, που αναφέρουν ότι είναι το μόνο σχετικό δημοσιευμένο. Διακρίνουν στην κινητή υγεία (mHealth) δυο ειδών λογισμικές εφαρμογές: τις κινητές εφαρμογές για υγεία/ευεξία του εμπορίου, και ιατρικές εφαρμογές που επιβλέπονται και χρησιμοποιούνται από γιατρούς και υγιεινομικές υπηρεσίες (66).

MHA’s - Mobile Health/wellbeing εφαρμογές (apps) και MMA’s - Mobile Medical apps αντίστοιχα, που δεν θα πρέπει να συγχέονται, παρά την κατ’ αρχάς συντακτική τους ομοιότητα. Οι δεύτερες εφαρμογές μπορούν ακόμα και να γίνουν αποδεκτές σαν οποιαδήποτε άλλη αναγνωρισμένη ιατρική συσκευή από το FDA. Οι εφαρμογές κινητών της ευζωΐας είναι εμπορικές, και στις ΗΠΑ μπορεί να εμπίπτουν στις νομοθετικές προβλέψεις της Federal Trade Commission Act (1914, FTC) όμως δεν ρυθμίζονται από τον HIPAA, όπως αντίστοιχα ρυθμίζονται οι επαγγελματικές ιατρικές εφαρμογές. Η FTC δεν έχει το ίδιο αυστηρές προβλέψεις όπως ο HIPAA και η πράξη HITECH act και μπορεί να εναπόκειται στον εμπορικό αντιπρόσωπο της εφαρμογής όσον αφορά το τι καλύπτει σε αποζημιώσεις παραβίασης ασφάλειας και ΔΠΧ, και για τι ποσό. Αντίθετα αν η εφαρμογή κινητής υγείας είναι πιστοποιημένη σαν ιατρική συσκευή, τότε μπορεί να ρυθμίζεται επίσης εκτός από τον HIPAA και

από το FDA (Food and Drug Association), το οποίο δεν δίνει τόσο βαρύτητα στην ιδιωτικότητα αλλά δίνει πολύ σημασία στην ασφάλεια κατά τη χρήση ιατρικών συσκευών (45).

Το 78% των καταναλωτών της έρευνας υγείας της 2015 PwC, ανησυχούν για την ασφάλεια ιατρικών δεδομένων, ενώ το 68% για την ασφάλεια των δεδομένων στις εφαρμογές κινητών. Επισημαίνουν επίσης, ότι μια παραβίαση ιατρικών δεδομένων από κακόβουλους που μπορεί να οδηγήσει σε τροποποίηση διάγνωσης και θεραπείας κάποιου ατόμου μπορεί να του προκαλέσει ανήκεστο βλάβη στην υγεία του και στην φυσική του κατάσταση. Τα στοιχεία της ευρωπαϊκής επιτροπής για τις εφαρμογές mhealth όπως καταγράφονται στο «Green paper on mhealth», αναφέρουν ότι η συγκεκριμένη αγορά κυριαρχείται από μικρές εταιρείες κατα 34,3%, ή ανεξάρτητους επαγγελματίες 30%, κάτι που μπορεί να υποδηλώνει έλλειψη εμπειρίας, τεχνικής γνώσης και οικονομικών δυνατοτήτων σε θέματα ασφάλειας (66).

Οι ιατρικές εφαρμογές για κινητά τρέχουν συνήθως από κινητές συσκευές, που **συνδέονται με ασύρματα δίκτυα και ασύρματες τεχνολογίες**. Η πρόθεση να χρησιμοποιηθούν wireless body area networks, προϋποθέτει ενδελεχή μέτρα ασφάλειας. Αυτό μπορεί να επιτευχθεί με επικοινωνία μεσω ραδιοκυμάτων συντονισμένων στο ίδιο μήκος κύματος (66).

4.9.1 **Προβλήματα ασφάλειας δεδομένων στην m-Health**

Σημαντικό πρόβλημα με τα MMA’s είναι ότι βρίσκονται εγκατεστημένα σε συσκευές κινητές που εύκολα μπορεί να κλαπούν ή να χαθούν, βάζοντας σε κίνδυνο τα δεδομένα. Γι αυτό θα πρέπει να έχουν σχεδιαστεί εξ΄ορισμού, έτσι ώστε στην ανάγκη από απόσταση να κλειδώνει η συσκευή, να απαγορεύεται η πρόσβαση σε υπηρεσίες, να διαγράφονται πλήρως τα δεδομένα από τη συσκευή, και να εμποδίζεται η πρόσβαση και επικοινωνία με άλλες αλληλοϋποστηριζόμενες συσκεύες (66).

Εδώ υπάρχει και το πρόβλημα, όπου χρήστες δεν ακολουθούν πιστά τις πολιτικές ασφαλείας των οργανισμών υγείας που εργάζονται σχετικά με την απαγόρευση του BYOD (bring your own device) και χρησιμοποιούν συχνά τις

δικές τους συσκευές στο εσωτερικό δίκτυο μιας εταιρείας ή οργανισμού, συσκευές που ενπολλοίς μπορεί να παρουσιάζουν προβλήματα ασφάλειας. Οι χρήστες επίσης δεν εγκαθιστούν στα κινητά τους λογισμικό προστασίας όπως firewall, αντιϊκό κλπ, ενώ η προσβασιμότητα που τα διακρίνει σε μέσα κοινωνικής δικτύωσης και ηλεκτρονικό ταχυδρομείο, κάνει εύκολο το διαμοιρασμό δεδομένων, παραβιάζοντας τους κανονισμούς HIPAA. Επίσης δεν υπάρχουν διεπαφές διαχείρισης στα κινητά που να ελέγχουν τα πιστοποιητικά συμμόρφωσης κάθε εφαρμογής (66).

Άλλοι πάλι χρήστες τέτοιων εφαρμογών, ούτε καν κλειδώνουν τα κινητά τους με μηχανισμούς ταυτοποίησης, όπως συνθηματικά κατά 50% σύμφωνα με μια έρευνα (45).

Άλλο πρόβλημα είναι ότι ένας εισβολέας μπορεί να χρησιμοποιήσει καμουφλαρισμένες επιθέσεις - Masque Attacks, για να προσπεράσει τη συνήθη άμυνα, και μετά να πάρει ακόμα και δικαιώματα διαχειριστή στην εφαρμογή. **Οι κλωνοποιημένες εφαρμογές** για κινητά, αποτελούν επίσης πρόβλημα, καθώς το 50% από αυτές είναι κακόβουλες. Αυτές φαίνεται να έχουν την ίδια διεπαφή με μια κανονική εφαρμογή και μπορούν να πάρουν και τα δεδομένα της αυθεντικής εφαρμογής εαν εκείνη δεν έχει στο μεταξύ απεγκατασταθεί (66).

Κρυπτογράφηση δεν χρησιμοποιείται συνήθως στα κινητά. Έτσι τα δεδομένα δεν προστατεύονται στο επίπεδο μεταφοράς. Επίσης πολλές εφαρμογές στέλνουν τα δεδομένά τους μέσω HTTPS χωρίς όμως προηγουμένως να έχουν ελέγξει αν τα πιστοποιητικά του πρωτοκόλου που χρησιμοποιούν, έχουν επικαιροποιηθεί πρόσφατα ή κάποτε.

Άλλες εφαρμογές στα κινητά πάλι αποθηκεύουν συνθηματικά και ονόματα χρηστών, χωρίς να τα κρυπτογραφούν. Στις εφαρμογές για κινητά, μόνο το γεγονός της κυκλοφορίας αναβαθμισμένου κώδικα (patch), δεν σημαίνει κιόλας ότι οι χρήστες τους τα έχουν εγκαταστήσει στις συσκευές τους.

Σχετικά με τους προγραμματιστές εφαρμογών αναφέρουν ότι προκειμένου να υπάρχει αποτελεσματικότερη προστασία θα πρέπει να γνωρίζουν καλά την πλατφόρμα κινητών που χρησιμοποιούν, και τις ανάγκες και ιδιότητες

ασφάλειας που έχει. Όλα τα παραπάνω είναι σημαντικές ευπάθειες, που οι χάκερ τα έχουν υπόψιν τους και θα στοχοποιήσουν τις εφαρμογές m-health στην προσπάθεια τους να αποκτήσουν παράνομα πρόσβαση ΔΠΧ ή σε ένα ΠΣΥ (66).

4.10 Η πανταχού παρούσα πληροφορική- Τηλεϊατρική

Ανάγκη για ασφάλεια υπάρχει και για την **πανταχού παρούσα υπολογιστική (ubiquitous computing)** που είναι μια εξελιγμένη έννοια στη χρήση των Η/Υ, με βάση την οποία οι υπολογιστικές δυνατότητες είναι διάσπαρτες παντού και πάντα κατά τη χρήση οποιασδήποτε συσκευής. Αυτή η νέα προσέγγιση ονομάζεται και **περιβάλλουσα νοημοσύνη** (pervasive computing) ή everyware (από τη λέξη everywhere, που σημαίνει «παντού»). Σε αυτή σχεδόν κάθε σχετικό αντικείμενο έχει επεξεργαστική ισχύ, με ασύρματη ή ενσύρματη σύνδεση σε ένα ευρύτερο δίκτυο. Με τεχνολογία Radio Frequency IDentification (RFID), καθημερινά αντικείμενα μπορεί να είναι μέρος ενός δικτύου. Μια RFID-ετικέττα μοιάζει με αυτοκόλλητο μεγέθους γραμματοσήμου, που μπορεί να τοποθετηθεί σε οποιοδήποτε αντικείμενο, ώστε να εντοπίζεται. Στην παθητική τους μορφή δεν χρειάζονται καν μπαταρία αφού την ενέργεια που χρειάζονται για να λειτουργήσουν την παίρνουν από τους RFID-αναγνώστες, με τη μορφή ραδιοκυμάτων. Μπορούν να έχουν υπολογιστική δύναμη και να χρησιμοποιηθούν για τη σύσταση Sensor Networks, και να παρακολουθούν εκφάνσεις του φυσικού κόσμου, και μπορούν να βρούν θέση μεταξύ άλλων και στο χώρο της υγείας (54).

Ο χρήστης δεν χρειάζεται να σκέφτεται πώς θα χρησιμοποιήσει την επεξεργαστική ισχύ κάποιου αντικειμένου, αλλά **η επεξεργαστική ισχύς βοηθά αυτόματα το χρήστη να εκτελέσει μια εργασία** (invisible computing) (58). Στον τομέα της υγείας παρουσιάζει ενδιαφέρον μεταξύ άλλων για τη φροντίδα ηλικιωμένων (Elderly-care) με διαδικασίες αυτόματης και συνεχούς παρακολούθησης ηλικιωμένων ή ατόμων που έχουν προβλήματα υγείας, και σκοπό την ευφυή φροντίδα τους. Θέματα ασφάλειας ΠΣ και ΠΔΠΧ υπάρχουν με την τηλεϊατρική και τις συσκευές παρακολούθησης ασθενών και ηλικιωμένων από απόσταση. Για παράδειγμα δεδομένα από μια τέτοια συσκευή, όπως μια αντλία έγχυσης ινσουλίνης μπορούν να παραβιαστούν και

να τροποποιηθούν όταν στέλνονται μέσω διαδικτύου. Επίσης μπορεί οι συσκευές παρακολούθησης να στέλνουν παράλληλα ευαίσθητες πληροφορίες από το σπίτι π.χ. του παρακολουθούμενου ηλικιωμένου, ακόμα και πληροφορίες του τύπου πότε είναι άδειο το σπίτι. Γίνεται αντιληπτό ότι και στη περίπτωση αυτής της τεχνολογίας θα πρέπει να λαμβάνονται μέτρα για την ασφάλεια των ΠΣ (κρυπτογράφηση) και για την προστασία των δεδομένων των ασθενών, όπως άλλωστε και σε όλες τις ΤΠΕ που χρησιμοποιούνται στον χώρο της υγείας των ασθενών (45).

Τον Σεπτέμβριο του 2015 το FBI εξέδωσε προειδοποίηση κυβερνοασφάλειας, ενημερώνοντας πως οι Internet of Things (IoT) συσκευές, μπορεί να αποτελέσουν στόχο κυβερνοεγκληματιών, και να βάλουν σε κίνδυνο τους χρήστες τους (66). Στο μέλλον δε είναι πιθανό να προκληθούν και τα μεγαλύτερα προβλήματα ασφάλειας από παρόμοιες τεχνολογίες, καθώς θα εναπόκειται στις μηχανές με την **τεχνητή νοημοσύνη** να αποφασίζουν για την καλή υγεία (ή μη) των ανθρώπων χρηστών τους.

Προβλήματα ασφάλειας που μπορεί να δημιουργηθούν σήμερα στις τεχνολογίες–τεχνητής νοημοσύνης έχουν σχέση με το ψηφιακό σήμα, και είναι π.χ., αν το σήμα υποστεί υποβαθμίσεις (impairments) και εξ΄αυτού προκύψουν προβλήματα επικοινωνίας και διαλειτουργικότητας. Για αυτό χρήσιμο είναι να γίνεται **ανίχνευση σφαλμάτων μετάδοσης μέσω ειδικών αλγορίθμων ομαδοποίησης των bits.** Επίσης απασχολεί το πόσο επηρρεάζονται τα δεδομένα από την καθυστέρηση στην μετάδοση (2). Οι εφαρμογές πραγματικού χρόνου (Real time applications) μπορεί να επηρρεαστούν από την διασπορά καθυστέρησης (delay jitter) και να μην είναι αξιοποιήσιμες πλέον από το δέκτη. Για ασφάλεια συνήθως μπορεί να χρησιμοποιηθεί **προσωρινός ενταμιευτής (buffer) στο δέκτη** οπότε αρκετά δεδομένα εικόνας και ήχου που πρόκειται να μεταφερθούν είναι ήδη αποθηκευμένα, και έτσι να αντιμετωπιστεί μιας περιορισμένης έκτασης καθυστέρηση. Σε κάποιες περιπτώσεις, η ανοχή της μετάδοσης σε σφάλματα στους τηλεπικοινωνιακούς διαύλους δεν έχει τόση σημασία, αφού για κάποιες εφαρμογές δεν είναι δυνατή ή επιθυμητή η διόρθωση τους, και εντέλει δεν προβληματίζει τον τελικό χρήστη (π.χ. σε μια φιλική επικοινωνία μεσω skype).

Για άλλες όμως όπως πρέπει να ισχύει και για τα δεδομένα στο χώρο της υγείας δεν πρέπει να υπάρχει τέτοια ανοχή, πρέπει να απαιτείται ορθή λήψη του συνόλου των δεδομένων και ο προορισμός θα πρέπει να εμποδίζεται να ανασυνθέσει τα αρχικά δεδομένα εαν έστω και ένα μόνο αρχικό bit είναι λάθος. Οι μεταφορές αρχείων και δεδομένων μη πραγματικού χρόνου, δεν παρουσιάζουν κάποια χρονική ευαισθησία (2).

4.11 Υπολογιστική Νέφους - Cloud Computing

Σύμφωνα με την εθνική υπηρεσία ασφάλειας τεχνολογιών των ΗΠΑ-NIST, **η υπολογιστική νέφους** είναι ένα μοντέλο με το οποίο επιτυγχάνεται καλή και έγκαιρη προσβασή σε ένα διαμοιραζόμενο τόπο πληροφοριακών πόρων (δίκτυα, εξυπηρετητές, αποθηκευτικοί χώροι και υπηρεσίες), με ελάχιστη ανάμειξη του παρόχου εξυπηρέτησης πελατών (CSP). Οι υπηρεσίες της υπολογιστικής νέφους, μπορούν να προσφερθούν είτε μέσω διαδικτύου είτε μέσω ιδιωτικών δικτύων. Οι πελάτες τραβούν πόρους μέσα από την αντίστοιχη δεξαμενή πόρων, η οποία βρίσκεται σε απομακρυσμένα κέντρα δεδομένων (67).

4.11.1 **Τα κύρια μοντέλα υπηρεσιών υπολογιστικής νέφους**

• Το **Infrastructure as a Service (IaaS),** κατά το οποίο παρέχονται μόνο το υλικό και το δίκτυο. Ο πελάτης εγκαθιστά ή αναπτύσσει τα δικά του λειτουργικά συστήματα, λογισμικό εφαρμογών.

• Το **Platform as a Service (PaaS),** κατά το οποίο παρέχονται το υλικό, το δίκτυο, το λειτουργικό σύστημα, ενώ ο πελάτης εγκαθιστά ή αναπτύσσει το δικό του λογισμικό εφαρμογών.

• Το **Software as a Service (SaaS),** κατά το οποίο παρέχεται μια προκατασκευασμένη εφαρμογή, το υλικό, το δίκτυο, μαζί με το απαιτούμενο λειτουργικό σύστημα και λογισμικό εφαρμογών (58).

Ο **Υπολογισμός Σύννεφου** (Cloud Computing) είναι μια τεχνολογία που χρησιμοποιεί το διαδίκτυο και κεντρικούς απομακρυσμένους επεξεργαστές (servers) όπου διατηρείται μεγάλος όγκων δεδομένων. Επιτρέπει στους καταναλωτές και στις επιχειρήσεις να χρησιμοποιούν διάφορες εφαρμογές,

χωρίς να χρειάζονται να τις εγκαταστήσουν, ούτε και κάποιον σκληρό δίσκο ή άλλα αποθηκευτικά μέσα. Επίσης τους παρέχει πρόσβαση σε όλα τους τα αρχεία οποιαδήποτε στιγμή και σε οποιοδήποτε μέρος με οποιαδήποτε συσκευή, που μπορεί να έχει σύνδεση στο διαδίκτυο. Προσφέρει την πληροφορική τεχνολογία σαν υπηρεσία (as a service).

Έχει τρία τμήματα: την εφαρμογή, την αποθήκευση και την συνδεσιμότητα. Στον χώρο της υγείας βοηθάει τους επαγγελματίες υγείας να αρχειοθετούν όλα τα στοιχεία των ασθενών τους, ενώ και οι ασθενείς μπορούν να παρακολουθήσουν την πορεία της κατάστασης τους. Συγχρόνως συντελεί στη μείωση του λειτουργικού κόστους (αποδοτικότητα) για τους οργανισμούς και τις κοινωνίες, αφού τα πάντα παρέχονται σαν υπηρεσία.

Η υπολογιστική νέφους **παρέχει επίσης Disaster Recovery**, γιατί πλημμύρες, σεισμοί, πόλεμοι, και άλλες φυσικές καταστροφές μπορεί να προκαλέσουν στέρηση της πρόσβασης σε συγκεκριμένες περιόδους του έτους ή της ημέρας. Αυτό το επιτυγχάνει μέσω της διατήρησης πιστών αντιγράφων ασφάλειας (back-ups) σε πολλά και διαφορετικά κέντρα (68).

Οι υπάρχοντες πάροχοι νέφους διαθέτουν έλεγχο πρόσβασης μέσω SSO - single sign on, που επιτρέπει στους χρήστες να μην είναι υποχρεωμένοι να απομνημονεύουν πολλά συνθηματικά, ούτε να τα κολλάνε σε μικρά χαρτάκια π.χ. στο συρτάρι του γραφείου τους. Τα συνθηματικά προστατεύονται με κρυπτογράφηση (68).

Στην σημερινή εποχή ολοένα και περισσότερες υπηρεσίες και οργανισμοί φαίνεται να προτιμούν την υπολογιστική νέφους και για θέματα ασφάλειας ΠΣ και ΔΠΧ, καθώς μεταφέρουν την σχετική ευθύνη και το κόστος στον πάροχο της πληροφορικής τεχνολογίας σαν υπηρεσία. Βέβαια αυτό έχει και μειονεκτήματα, όπως περιγράφονται πιο κάτω.

4.11.2 **Μειονεκτήματα του cloud**

Η υπολογιστική νέφους δεν παρέχει στον πελάτη καμμία δυνατότητα να βρεί ποια δεδομένα του έχουν πειραχθεί από τον «επιτιθέμενο». Αν έχουν πειραχτεί ευαίσθητα δεδομένα τότε δεν είναι εμφανές ποια έχουν πειραχτεί και

ποια όχι. Επίσης κάποια δεδομένα μπορεί να έχουν τροποποιηθεί ή να έχουν διαγραφεί από τον επιτιθέμενο ή ενδεχομένως και από τον εξυπηρετητή νέφους-CSP π.χ. για λόγους αποθήκευσης, σε αυτή την περίπτωση θα μπορούσαν να βοηθήσουν εαν υπάρχουν καλά metadata (μηχανισμοί προέλευσης). Σε αυτή την περίπτωση θα βοηθούσε επίσης να υπήρχε κάποια εφαρμογή – API (Application Programe Interface), που θα δίνει στους πελάτες πληροφορίες για σφάλματα και γεγονότα σύνδεσης.

Επίσης χρήσιμο θα ήταν ο πάροχος νέφους να εγκαταστήσει κρυπτογραφικό σύστημα Proofs of Retrievability (POR), και αν ο εξυπηρετητής διατηρεί κάποιο σχετικό φάκελλο να μπορεί να τον επαναφέρει απείρακτο. Άλλες χρήσιμες τεχνικές στην υπολογιστική νέφους, είναι η Provable Data Possession (PDP) για να διαπιστωθεί αν ένας ακατάλληλος, μη έμπιστος εξυπηρετητής έχει αποκτήσει βασικά δεδομένα.

Μειονέκτημα του cloud επίσης είναι το **«κλείδωμα προμηθευτή»,** δηλαδή αν χρειαστεί να γίνει αλλαγή παρόχου CSP είναι εξαιρετικά δύσκολο να πραγματοποιηθεί, σε οτι αφορά τη μεταφορά δεδομένων από τον ένα πάροχο στον άλλο. Άλλο μειονέκτημα είναι ότι επειδή την κατεύθυνση, κίνησης των πακέτων μεσα στο διαδίκτυο, την ορίζουν τα router θα χρειαστεί τα πακέτα να περάσουν μέσα από πολλά router εως ότου φτάσουν στον προορισμό τους, κάτι που αυξάνει την ευπάθεια του συστήματος (68).

Στην Ελλάδα το εθνικό δίκτυο έρευνας και τεχνολογίας, η ΕΔΕΤ Α.Ε. (ΕΔΕΤ – GRNET) όπως αναφέρει στην σελίδα της στο διαδίκτυο είναι ο εθνικός πάροχος υποδομών και υπηρεσιών δικτύου (networking), υπολογιστικού νέφους (cloud computing) και πληροφορικής (IT). Εξυπηρετεί σε καθημερινή βάση εκατοντάδες χιλιάδες χρήστες στους στρατηγικούς τομείς της έρευνας, της εκπαίδευσης, της υγείας και του πολιτισμού, τη διασύνδεση των οποίων τομέων έχει σαν αντικείμενό της.

Διαθέτει **κέντρο δεδομένων για την υγεία στην Κρήτη,** και **διασυνδέει τα νοσοκομεία με οπτικές ίνες και ασύρματο wi-fi.** Επίσης παρέχει υπηρεσίες όπως: «• **Διάδοσις**: για τον διαδανεισμό ιατρικών άρθρων • **Harmoni**: για την εφεδρική αποθήκευση και απομακρυσμένη πρόσβαση σε

απεικονιστικά δεδομένα, • Κατάλογο χρηστών για το προσωπικό κάθε νοσοκομείου, και ενσωμάτωση των καταλόγων στην **ομοσπονδία Ταυτοποίησης & Εξουσιοδότησης ΕΔΕΤ • eduroam**: Περιαγωγή (roaming) ασύρματης πρόσβασης στο διαδίκτυο • **ViMa: Εικονικές Μηχανές**, φιλοξενία υπηρεσιών, πειραμάτων και εφαρμογών • **Μέτρηση Η/Μ ακτινοβολίας εντός του χώρου του νοσοκομείου • ΕΜΑ**: Κεντρικές Ηλεκτρονικές Υπηρεσίες Διαχείρισης Εθνικού Μητρώου Εθελοντών Αιμοδοτών» (69).

Γενικά τα ΠΣΥ στην Ελλάδα υπενοικιάζουν υπηρεσίες και είναι διασυνδεδεμένα όπως και άλλες υπηρεσίες του δημοσίου μέσω του προγράμματος Σύζευξης 2 που τους παρέχει περαιτέρω ασφάλεια και αποδοτικότητα, ενώ οι χρήστες πριν να εισέλθουν σε αυτά ταυτοποιούνται.

Ο απλός χρήστης υπηρεσιών υγείας ή ένας ιδιώτης επαγγελματίας της υγείας εάν θέλει να εξετάσει την κατάσταση του δικτύου του, μπορεί να χρησιμοποιήσει τον Υπερίωνα. Στον τομέα της παρακολούθησης ποιότητας δικτύων, η ΕΕΤΤ αναβάθμισε τη **μετρητική πλατφόρμας ΥΠΕΡΙΩΝ**, επικαιροποιώντας τη δομή των δεδομένων και καθιστώντας τα δεδομένα μετρήσεων ανοιχτά σε κάθε ενδιαφερόμενο. Μέσω της πλατφόρμας, οι χρήστες μπορούν να κάνουν **μετρήσεις της ποιότητας σύνδεσης στο διαδίκτυο**, χρησιμοποιώντας το εργαλείο NDT (Network Diagnostic Tool) του M-Lab. Υπάρχουν περίπου 14,000 εγγεγραμμένοι χρήστες του Υπερίωνος (65).

4.12 Ασφάλεια σε πλατφόρμα διαχείρισης big-data, Hadoop

Τα ΠΣΝ επεξεργάζονται «μεγάλα δεδομένα», δηλαδή δεδομένα επεξεργασμένα ή όχι, που αφορούν προσωπικά, αισθητηριακά, επιχειρηματικά, ή ιατρικά στοιχεία (ανθρώπων, ομάδων ή οργανισμών).

Όσον αφορά τα μεγάλα δεδομένα στον υπολογισμό σύννεφου υπάρχουν εξειδικευμένες πλατφόρμες όπως είναι η Hadoop (Highly Archived Distributed Object Orientated Programming) που τα διαχειρίζονται. Χρησιμεύει στην αποθήκευση, διαχείριση και διαμοιρασμό των μεγάλων δεδομένων, κατά μήκος πολλών κόμβων εξυπηρέτησης. Είναι ανοικτή τεχνολογία βασισμένη σε Java. Τα δεδομένα που διαχειρίζεται μπορεί να είναι αισθητηριακά, ιατρικά,

εμπορικά (70). Δημιουργήθηκε από τους Goug Cutting και Mike Cafarella το 2005, και έχει δυο τμήματα: το διανεμητικό αρχειακό σύστημα - Hadoop Distributed File System (HDFS) που ασχολείται αποκλειστικά με την αποθήκευση, και το Map Reduce που παρέχει ανάλυση δεδομένων σε περιβάλλον ομαδοποίησης. Η ασφάλεια του αρχειακού συστήματος αυτής στηρίζεται σε τρείς προσεγγίσεις Κέρβερος, Κόμβο Αλγορίθμου, και Κόμβο ονόματος (70).

Κεφάλαιο 5ο: Διαχείριση Ασφάλειας του ΠΣΝ

Σε αυτό το κεφάλαιο θα γίνει αναφορά στο διαχειριστικό μέρος του όλου εγχειρήματος της προστασίας των ΠΣ και της συμμόρφωσης στις νομοθετικές διατάξεις, πως δηλαδή θα αναγνωριστούν οι κίνδυνοι που απειλούν τα δεδομένα και τους πληροφορικούς πόρους του συστήματος και τι θα πρέπει να κάνει ένας υγιειονομικός σχηματισμός για να τους αντιμετωπίσει.

Η ασφάλεια του ΠΣΝ θα πρέπει να αφορά τόσο τις υποδομές hardware, middleware, software, όσο και τα δεδομένα και τις πληροφορίες που τυχόν να εξαχθούν από αυτά. Θα πρέπει να διασφαλιστεί το σύστημα δηλαδή να μην το βγάλουν κάποιοι εκτός λειτουργίας, να προστατευτεί η σωστή και απρόσκοπτη λειτουργία του, και να αποτραπεί η καταστροφή ή κλοπή των πόρων του συστήματος. Μετά θα πρέπει να διασφαλιστούν τα δεδομένα, θα πρέπει να εφαρμοστούν καταρχάς οι αρχές της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας (η αποφυγή παρακράτησης μιας πληροφορίας). Επίσης σημαντική αρχή που πρέπει να διασφαλιστεί είναι και η αρχή της μη-αποποίησης μιας ενέργειας ή μιας ενημέρωσης του ΠΣ.

Η απόλυτη ασφάλεια είναι αδύνατη, και πρέπει να ακολουθηθεί μια risk-based approach, δηλαδή μια προσέγγιση μείωσης των κινδύνων – κάτι που θα πρέπει να βασίζεται στον εντοπισμό των κινδύνων στην πρόληψη, καθώς και στην ανίχνευση και αποκατάσταση των ευπαθειών. Θα πρέπει να λαμβάνονται μέτρα ασφάλειας. Τα μέτρα προστασίας για την ασφάλεια ενός ΠΣ μπορεί να είναι **διοικητικά (**διαδικασίες**, πολιτικές,** οδηγίες**,** πρακτικές, **οργανωτικές δομές),** τεχνικά, ή νομικά.

Προκειμένου να αντιμετωπιστεί ο κίνδυνος θα πρέπει να γίνεται τακτικά Διαχείριση Ασφάλειας που περιλαμβάνει:

- διαχείριση κινδύνου και ανάλυση κινδύνου
- σύνταξη πολιτικής ασφάλειας

- σύνταξη σχεδίου επαγγελματικής συνέχειας λειτουργιών.
- σύνταξη σχεδίου ανάκαμψης συστημάτων και πληροφοριών (1).

Στα διοικητικά μέτρα ασφαλειας υπεισέρχεται η **Διαχείριση κινδύνου** που λαμβάνει υπόψιν της όρους όπως το κόστος (αγορά, εγκατάσταση, χρήση, συντήρηση) του όποιου μέτρου ασφάλειας, και προϋποθέτει να έχει προηγούμενα γίνει **risk-analysis**. **Η διαχείριση επικινδυνότητας** (**risk-management**), αναφέρεται στον έλεγχο της επικινδυνότητας ώστε να παραμένει σε αποδεκτά επίπεδα. Η επικινδυνότητα μπορεί να μειωθεί με την εφαρμογή αντιμέτρων, να μεταβιβαστεί, π.χ. με ασφάλιση, ή να αναληφθεί, δηλαδή να γίνει αποδεκτή και να είναι κάποιος διατεθειμένος να υποστεί τις επιπτώσεις αν συμβεί ένα επεισόδιο (1). Είναι απαραίτητο στην αρχή να γίνει **αποτίμηση της επικινδυνότητας** κάποιας ευπάθειας του ΠΣ, γιατί π.χ. δεν έχει καμμία απολύτως λογική να ξοδεύονται μεγάλα χρηματικά ποσά για να προστατευτεί κάποιο αγαθό πολύ μικρής αξίας και σημασίας. Θα πρέπει να ξοδεύονται τόσοι οικονομικοί πόροι όσοι προκύπτουν ότι χρειάζονται μέσω της διαχείρισης κινδύνου.

Διαχείριση επικινδυνότητας = Αποτίμηση επικινδυνότητας (risk assessment) + Αντιμετώπιση της επικινδυνότητας (risk treatment).

Αποτίμηση επικινδυνότητας (risk assessment) είναι η διαδικασία που περιλαμβάνει την αναγνώριση επικινδυνότητας (risk identification), την ανάλυση επικινδυνότητας (risk analysis) και την αξιολόγηση της επικινδυνότητας (risk evaluation). **Ακολουθεί η επιβεβαίωση ασφάλειας**. Δηλαδή ότι όλα βαίνουν καλώς, και όπως έχουν σχεδιασθεί. Αυτό μπορεί να γίνει με εσωτερικούς ελέγχους από ειδικές υπηρεσίες μέσα στον οργανισμό ή και εξωτερικούς ελέγχους από τρίτους ανεξάρτητους οργανισμούς. Οι έλεγχοι αυτοί μπορεί να γίνονται με εργαλεία όπως είναι τα ερωτηματολόγια, penetration τεστ, κ.α., και στη συνέχεια ανάλογα με τα αποτελέσματα των ελέγχων να γίνεται κάποια αναθεώρηση των σχεδιασμών και των πολιτικών ασφαλείας. Γίνεται δηλαδή ένας κύκλος PDCA- plan, do, check, act.

Απομένουσα επικινδυνότητα (residual risk) είναι εκείνη που απομένει μετά τη λήψη των μέτρων προστασίας (1).

5.1.1 **ΣΔΑΠ-Σύστημα Διαχείρισης ασφάλειας πληροφοριών- ISO 27001**

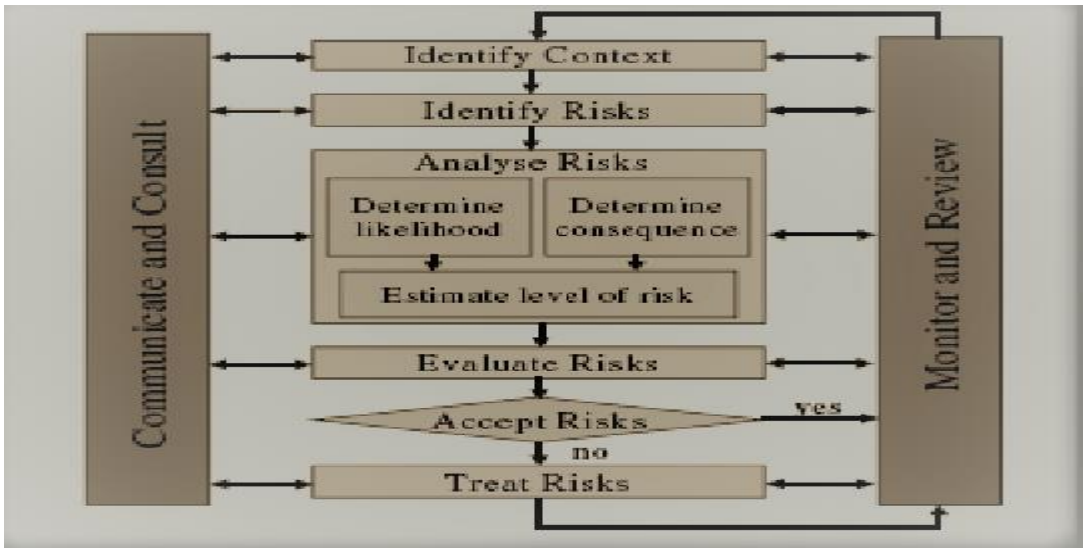
Κεντρικός πυλώνας της όλης διαδικασίας διαχείρισης κινδύνου και ασφάλειας είναι το ΣΔΑΠ - Σύστημα Διαχείρισης ασφάλειας πληροφοριών **(ISMS)**, που έχει ως βασικό πρότυπο το **ISO 27001 (πρώην ISO 17799)**. Αυτό ακολουθεί ένα κύκλο ζωής το μοντέλο PDCA.

Η διαμόρφωση πολιτικών ασφάλειας σε ένα ΣΔΑΠ, **διακρίνονται σε 3 είδη** σύμφωνα με τον κ. Δουληγέρη (1): Την υποχρεωτική εφαρμογή, την κατά περίπτωση εφαρμογή, και την εφαρμογή του διακριτού ελέγχου όπου όλα όσα δεν περιγράφονται από την πολιτική είναι επιτρεπτά. Το ISO 27001 παρέχει τις απαιτήσεις για τη εγκαθίδρυση και συντήρηση και βελτίωση ενός ISMS ενώ το 27002 δίνει μια λίστα ενδυνάμει ελέγχων ασφάλειας. Αυτά τα δύο ISO, παρέχουν σε έναν μεγάλο οργανισμό το πλαίσιο για να αξιολογήσει (audit checklists), πόσο καλά λειτουργεί στο θέμα της διαχείρισης ασφάλειας ΠΣ (1)

«Η Πολιτική Ασφάλειας των Πληροφοριακών Συστημάτων περιλαμβάνει το σκοπό και τους στόχους της ασφάλειας, οδηγίες, διαδικασίες, κανόνες, ρόλους και υπευθυνότητες, που αφορούν την προστασία των ΠΣ του οργανισμού» (1). **Πρέπει να βρίσκεται διατυπωμένη σε έγγραφο, και θα πρέπει να τη γνωρίζουν και να την εφαρμόζουν όλοι οι χρήστες του εκάστοτε ΠΣ.** Οι οδηγίες και τα μέτρα προστασίας που καθορίζει η πολιτική ασφάλειας ενός ΠΣ θα πρέπει να λαμβάνουν υπ΄όψιν τους θέματα: προσωπικού, φυσικής ασφάλειας, ελέγχου πρόσβασης στο ΠΣ, υλικού και λογισμικού, νομικές υποχρεώσεις, διαχείρισης κινδύνου, σύγχρονης τεχνολογίας, οργανωτικής δομής, αναγκών του οργανισμού και των χρηστών, σχεδίου συνέχισης λειτουργίας (1).

Το πρότυπο ISO27002, παρέχει **όλες τις βέλτιστες πρακτικές για την υλοποίηση των απαιτήσεων που περιγράφονται στο πρότυπο 270001**, για καθορισμό, εφαρμογή, διατήρηση και συνεχή βελτίωση ενός συστήματος διαχείρισης πληροφοριών με σκοπό την προστασία της πληροφορίας ενός οργανισμού, δηλαδή την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα (CIA) (71).

Το σύστημα ISMS θα πρέπει να είναι ένα πλαίσιο διαχείρισης και οργάνωσης της ασφάλειας που θα πρέπει να παρακολουθείται συνεχώς και να επανεξετάζεται περιοδικά. Η διοίκηση χρειάζεται να ενημερώνεται ενεργά από την πρώτη μέρα για το ΣΔΑΠ. Αυτό μπορεί να επιτευχθεί με την οργάνωση ειδικών συναντήσεων της διοίκησης μαζί με τον project manager ασφάλειας της εταιρείας, που θα εξηγήσει στη διοίκηση τους στόχους του έργου, την ζητούμενη υποστήριξη και την περιγραφή των θετικών αποτελεσμάτων για την επιχείρηση, εαν αυτή υλοποιήσει και πιστοποιήσει το ISMS.



***Εικόνα 7. Risk Assessment overview according to The Australian/New Zealand standard AS/NZS* (72)**

Όπως και κάθε πρότυπο ISO, έτσι και το ISO 27001 ακολουθεί τον plan-do-check-act (PDCA) κύκλο, που θα πρέπει να εκτελείται τακτικά.

5.1.2 **Παράγοντες που εξετάζει ένα ΣΔΑΠ**

Στα πλαίσια ενός ISMS θα πρέπει να γίνεται μια **ανάλυση επικινδυνότητας**. Αυτή **αντιστρέφει το μοντέλο της αξιολόγησης επενδύσεων** όπου μια επένδυση θεωρείται συμφέρουσα εαν το κόστος της (σε σταθερές τιμές) υπολείπεται του γινομένου του αναμενόμενου κέρδους επί την πιθανότητα επίτευξης του κέρδους. Στην περίπτωση της επένδυσης στην ασφάλεια ΠΣ, δεν επιδιώκεται η αποκόμιση κέρδους, αλλά η αποφυγή ζημιάς (71).

Ως Επικινδυνότητα (Ε) ορίζεται ως το γινόμενο της Πιθανότητας (Π) πραγματοποίησης ενός επεισοδίου ασφάλειας επί το (οικονομικό ή άλλο) Κόστος (Κ) που θα επιφέρει, δηλαδή Ε = Π x Κ.

Ανάλυση κινδύνου. Για προληπτικούς λόγους εκτός από τα μέτρα προστασίας που πρέπει να λαμβάνονται θα πρέπει να γίνεται και ανάλυση κινδύνου (risk-analysis). Υπάρχουν **εργαλεία υπολογισμού-ανάλυσης του κινδύνου (π.χ. το Cramm)** (71). Στο χώρο της υγείας και μια ελάχιστη απώλεια ή τροποποίηση πληροφοριακών πόρων ενός ΠΣΝ μπορεί να οδηγήσει κάποιον στο θάνατο ή σε βαριά σωματική αναπηρία. Θα πρέπει να είναι σαφής ποιος είναι ο σκοπός και **ποιοι οι στόχοι της πολιτικής.** Τι θέλουμε να προστατέψουμε, ποιοι είναι οι χρήστες, οι διαχειριστές, ποιοι οι υπευθυνοι ασφαλείας, ποιος ο ρόλος τους, ποια η διάρκεια της ισχύος της πολιτικής.

Ρίσκο = περιουσιακό στοιχείο* απειλή * ευπάθεια.

Γενικά υπάρχουν δυο κατηγορίες τέτοιας ανάλυσης.

Η Ποσοτική ανάλυση κινδύνου. Σε αντικειμενικές αριθμητικές τιμές, π.χ. ποιά θα είναι τα ποσά για κάθε συνιστώσα ανάλυσης κινδύνου. Είναι πιο ουσιαστική, αλλά πιο δύσκολα υλοποιήσιμη.

Η Ποιοτική ανάλυση αρκείται να χαρακτηρίζει με εκφράσεις π.χ. μικρό, μεγάλο, μέτριο, πιο υποκειμενική μέθοδος. Η ανάλυση κόστους/οφέλους δεν βασίζεται σε μαθηματική απόδειξη.

Η Βασική Μεθοδολογία ανάλυσης Κινδύνου είναι η BPL.

Αν B<P*L, τότε αξίζει να υλοποιηθεί η πρόληψη, αλλιώς είναι υπερβολικό.

Β είναι το κόστος που θα στοιχήσει η πρόληψη μιας απώλειας. Ρ είναι η πιθανότητα να συμβεί αυτή η απώλεια και L είναι το συνολικό κόστος μιας απώλειας αν τελικά συμβεί (43).

Η έρευνα έχει δείξει ότι μέσω μεθόδων ανάλυσης του μοντέλου των απειλών - Threat Modeling Analysis (TMA) προάγεται η κατανόηση και η εκτίμηση των

κινδύνων για την ασφάλεια. Θεωρούνται έγκυρες μέθοδοι και προτείνονται από τα πρότυπα της National Institute of Standards and Technology (NIST) για την εκτίμηση κινδύνων, που σχετίζονται με τα δίκτυα και τις εφαρμογές για κινητά (OWASP- Open Web Application Security Project). Απαιτεί κατανόηση των απειλών και το πως αυτές εκμεταλλευόνται τις ευπάθειες για να προσβάλλουν ένα δίκτυο ή μια ιατρική εφαρμογή π.χ. κινητού (66).

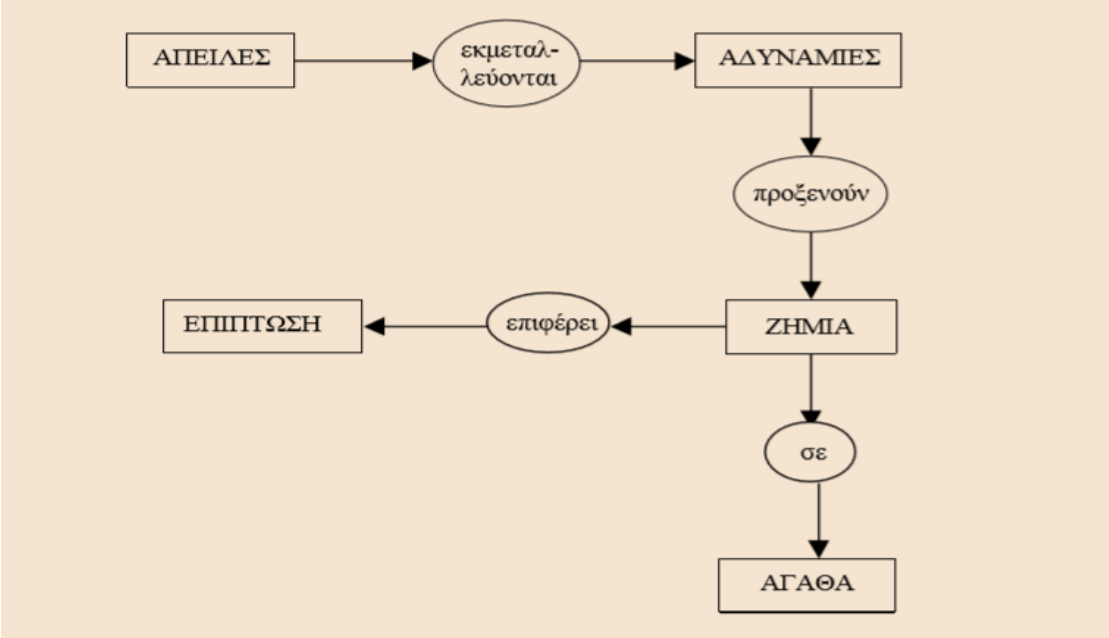
5.1.3 **Το τρίγωνο της Ευπάθειας - Απειλής - Συνέπειας**

Βασική για την έννοια της **πολιτική ασφάλειας** είναι η έννοια της **συνέπειας**, δηλαδή ποιος θα ζημιωθεί από την παραβίαση της ασφάλειας, πόσο θα ζημιωθεί, ποια θα είναι άμεση (π.χ. κόστος επαναγοράς, κόστος διαμόρφωσης, επανεισαγωγής δεδομένων), και ποια η μεταγενέστερη ή μακροχρόνια ή έμμεση συνέπεια. Είδη συνεπειών είναι π.χ. κοινωνικές συνέπειες (Δυσφήμηση), νομικές συνέπειες, λειτουργικές συνέπειες (απώλειες από διακοπή ή παρεμπόδιση λειτουργιών).

Απειλή είναι οτιδήποτε μπορεί να προκαλέσει συνέπεια σε κάποιο αγαθό. Μπορεί να είναι κάποια φυσική καταστροφή, ή κάποια ανθρώπινη εσκεμμένη ή τυχαία ενέργεια.

Αδυναμία – Ευπάθεια είναι οποιαδήποτε κατάσταση μπορεί να οδηγήσει σε έκφραση απειλής, ή να μεγιστοποιήσει μια συνέπεια.

Από το γινόμενο της αδυναμίας, της απειλής και της επακόλουθης συνέπειας, προκύπτει **η έννοια της επικινδυνότητας (risk)** (1).



***Εικόνα 8. Ανάλυση, Αποτίμηση Επικινδυνότητας ΠΣ* (73)**

5.1.4 **Μεθοδολογίες ανάλυσης κινδύνου**

Υπάρχουν διάφορες μεθοδολογίες ανάλυσης κινδύνου, όπως είναι η υψηλού κύρους βρεττανική **CRAMM - Central Computer and Telecommunications Agency** του 1987, την οποία χρησιμοποιούν πάνω από 500 οργανισμοί ανάμεσα τους και το ΝΑΤΟ και ΠΣΥ (43). Η **CCTA Risk Analysis and Management Method** αναπτύχθηκε το 1987 στη Μεγάλη Βρετανία από την Κεντρική Υπηρεσία Υπολογιστών και Επικοινωνιών (CCTA) και έχει χρησιμοποιηθεί σε εκατοντάδες μελέτες διεθνώς. Παρέχει κατάλογο απειλών και αντιμέτρων (1). Το πρόγραμμα CRAMM, βοηθάει τους οργανισμούς να συμμορφώνονται με το διεθνές πρότυπο ISO 17799/BS7799. Έχει μια βάση αντιμέτρων με 3000 αντίμετρα, ανανεώνεται διαρκώς, οδηγούς για τη δημιουργία πολιτικών ασφαλείας, κ.α.

Μια μέθοδος της είναι εκείνη των ερωτηματολογίων, όπου για κάθε περιουσιακό στοιχείο παράγει ένα πλήθος ερωτημάτων MCQ's, για το δίδυμο απειλή-πληροφοριακός πόρος. Το πρόγραμμα υπολογίζει τον κίνδυνο, ανάλογα με τις απαντήσεις των ειδικών. Η κλίμακα κυμαίνεται από το 1 (πολύ μικρός κίνδυνος) εως το 7 (πολύ μεγάλος). Η μέτρηση της επικινδυνότητας (σε κλίμακα 1:7) γίνεται: - Με αποτίμηση περιουσιακών στοιχείων (κλίμακα

1:10), βάσει των επιπτώσεων στον οργανισμό - Με αξιολόγηση απειλών (κλίμακα 1:5) - Με αξιολόγηση ευπαθειών (κλίμακα 1:3) (43).

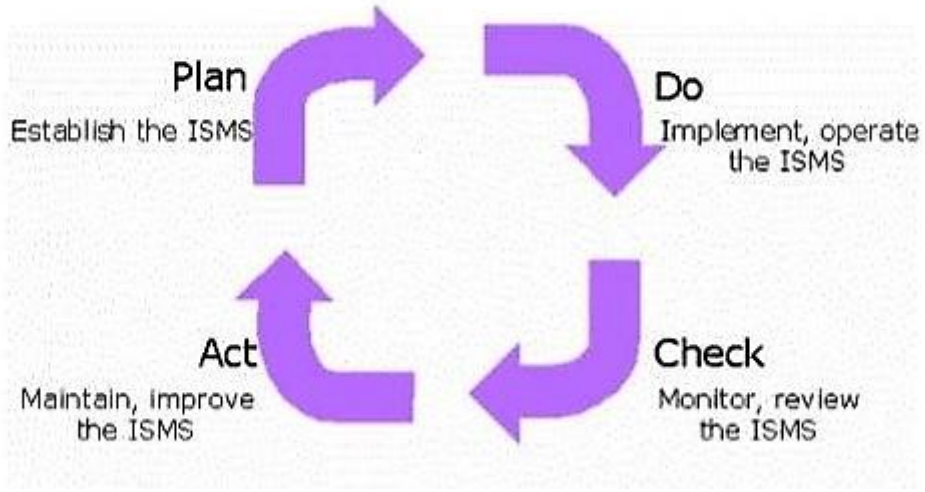
Η μέθοδος συνοδεύεται και από λογισμικό υποστήριξης που υποστηρίζει όλα τα βήματα της μεθόδου και μέσω αυτού παρακολουθείται η ορθή, βήμα προς-βήμα εφαρμογή της μεθοδολογίας, αποθηκεύονται όλα τα στοιχεία που συλλέγονται κατά την εφαρμογή της, υποστηρίζει όλους τους σύνθετους υπολογισμούς που απαιτούνται για τον προσδιορισμό της επικινδυνότητας, εμπεριέχει μία βιβλιοθήκη αντιμέτρων, και τους μηχανισμούς συμπερασματολογίας που επιλέγουν τα αντίμετρα. Τέλος, παρέχει αναφορές (reports) για όλα τα στάδια της μεθόδου. Για την επιτυχία της μεθόδου CRAMM απαιτείται η συμμετοχή της διοίκησης του οργανισμού στο υψηλότερο δυνατό επίπεδο και η συνεργασία των αρμόδιων στελεχών του οργανισμού κυρίως για τις αξιολογήσεις των αγαθών και την εκτίμηση απειλών και αδυναμιών.

Μια άλλη μέθοδος ανάλυσης κινδύνου είναι η **SBA (Security By Analysis)** που είναι η πιο δημοφιλής και ευρέως εφαρμοζόμενη μέθοδο ανάλυσης επικινδυνότητας στη Σουηδία. Έχει ως σημείο αναφοράς το πρότυπο ISO/IEC 17799 και ακολουθεί το κλασικό μοντέλο του καταλόγου (checklist model), υποστηρίζεται επίσης από ειδικό λογισμικό (73). Άλλη πιο πρόσφατη μεθολογία ανεπτυγμένη ειδικά για το χώρο της υγείας **η ODESSA,** παρέχει επίσης στο διαχειριστή του συστήματος τη δυνατότητα να επιλέξει τα κατάλληλα αντίμετρα**. Η μεθοδολογία OCTAVE–Operationally Critical Threat, Asset and Vulnerability Evaluation**, μπορεί να χρησιμεύσει σε σχετικά μικρούς και απροετοίμαστους οργανισμούς. Κάθε σημαντική ανάλυση κινδύνου προϋποθέτει μια ομάδα ατόμων με ευρέως φάσματος γνώσεις, δεξιότητες και εμπειρίες. Απαιτεί επένδυση από τον κάθε οργανισμό σε ανθρώπους, εκπαίδευση και χρήματα (43).

Οι Susanto Herru και συνεργάτες (74) μελέτησαν κάποια συγκεκριμένα ISMS. Τα ISO 27001, BS 7799, PCIDSS, ITIL, COBIT. Πρόκειται για συστήματα ISMS που αποτελούνται από πολιτικές ασφάλειας που υπαγορεύουν πως πρέπει να χρησιμοποιούνται και να προστατεύονται οι υπολογιστικοί πόροι σε έναν οργανισμό. Αυτοί μελέτησαν ποιό από τα 5 πλεονεκτεί, ανάλογα με το προφίλ τους και την μεθοδολογία που ακολουθούν (74).

Το ISO 27001, χρησιμοποιεί ένα κυκλικό μοντέλο «Plan-Do-Check-Act» (PDCA), που έχει σκοπό να εγκαθιδρύσει, υποστηρίξει, παρακολουθήσει και βελτιώσει την αποτελεσματικότητα ενός ISMS.

Το BS7799, εκδόθηκε από τον Βρεττανικό οργανισμό προτυποποίησης (BSI) το 1995 και αποτελείτο από 7 τμήματα. Το πρώτο τμήμα υιοθετήθηκε το 1999 από το ISO ως ISO17799. Το 1999 το δεύτερο τμήμα στην έκδοση του 2002 εισήγαγε την έννοια του PDCA.



***Εικόνα 9. Κύκλος PDCA ενός ΣΔΑΠ* (74)**

Το 2005 το δεύτερο τμήμα του BS7799 έγινε το ISO 27001 με το οποίο συνεπώς παρουσιάζουν αρκετές ομοιότητες.

Το Πρότυπο Προστασίας Δεδομένων των Πιστωτικών Καρτών - Payment Card Industry Data Security Standard (PCIDSS) βοηθάει στην διεξαγωγή

πληρωμών μέσω πιστωτικών καρτών και στην καταπολέμηση της απάτης με πιστωτικές κάρτες (74).

Ένα άλλο ISMS είναι το Information Technology Infrastructure Library (ITIL), και τέλος το COBIT - Control Objectives for Information and related Technology. Τα δυο τελευταία εστιάζουν περισσότερο στην σχέση της ασφάλειας πληροφοριών και την διοίκηση. Αφού τα μελέτησαν κατέληξαν ότι το ISO 27001 είναι η παγκόσμια γλώσσα των στάνταρντς, αναγνωρισμένη παγκοσμίως όπως αντίστοιχα τα αγγλικά στις ομιλούμενες γλώσσες. Έχει ποσοστό χρήσης και εμπιστοσύνης πάνω από 80% του συνολικού. Πολύ περισσότερες χώρες το χρησιμοποιούν παγκοσμίως και είναι πιο εύκολα εφαρμόσιμο (74).

Αναφέρουν ότι ο ISO27001 προκειμένου να επιτύχει την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριακών περιουσιακών στοιχείων, χρειάζεται την υιοθέτηση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών ISMS, που πρέπει να χαρακτηρίζεται από:

1. Μια πολιτική ασφάλειας πληροφοριών, γνωστή σε όλους στον οργανισμό.

2. Την ανάθεση αρμοδιοτήτων ασφάλειας πληροφοριών, μέσω διαδικασιών, ελέγχων και συγκεκριμένων υπευθύνων.

3. Μια καλά οργανωμένη υπηρεσία που ασχολείται με την προμήθεια, ανάπτυξη και τέλος με τη συντήρηση των υπολογιστικών πόρων ενός οργανισμού.

4. Μια εξειδικευμένη υπηρεσία που να ασχολείται με την ασφάλεια πληροφοριών σε δυο κατευθύνσεις εσωτερικά και εξωτερικά του οργανισμού.

5. Την αποτίμηση των αγαθών και τον έλεγχο αυτών.

6. Τον έλεγχο-ασφάλειας του προσωπικού, τον διαμοιρασμό αρμοδιοτήτων και την εκπαίδευση.

7. Την φυσική και περιβαλλοντική ασφάλεια.

8. Την ασφάλεια επικοινωνιών και επιχειρησιακών συστημάτων.

9. Τον έλεγχο προσβάσεων τόσο στη φυσική τοποθεσία όσο και στα ΠΣ από συγκεκριμένη υπηρεσία.

10. Συμμόρφωση που να αφορά δυο τομείς. Ο πρώτος την συμμόρφωση με τους πολυπληθείς νόμους και διατάξεις ή συμβατικές απαιτήσεις, και ο δεύτερος την συμμόρφωση προς τις πολιτικές ασφαλείας, τα τεχνικά πρότυπα και τις διαδικασίες. Πάνω σε αυτές τις αρχές τα αξιολόγησαν και έβγαλαν τα συμπεράσματα που σημείωσαν στον πιο κάτω πίνακα 3 (74).

5.1.1 **Αρχεία καταγραφής (Log- Files)**

Στα αρχεία καταγραφής ενός ΠΣ είναι αποθηκευμένες πληροφορίες σχετικές με τη λειτουργία του συστήματος. Για να έχουν σημασία πρέπει να έχουν ενεργοποιηθεί προηγούμενα συγκεκριμένες πολιτικές (group policies). Για κάθε ομάδα χρηστών ορίζεται μια συγκεκριμένη **πολιτική ασφάλειας**, και τα security logs (sys-logs) δεν παραμένουν κενά (38).

Υπεύθυνος για τον **καθορισμό πολιτικών ασφαλείας** είναι ο διαχειριστής του συστήματος. Αν κάποιος ερευνά ένα ηλεκτρονικό έγκλημα μπορεί με τη βοήθεια των αρχείων καταγραφής να εξακριβώσει εάν κάποια συγκεκριμένη εφαρμογή χρησιμοποιήθηκε από χρήστη και αν ο χρήστης αυτός είχε ή όχι εξουσιοδοτημένη πρόσβαση στο σύστημα. Σε τεχνικό επίπεδο **ένα ανάχωμα ασφάλειας** επιτρέπει καταγραφή της δραστηριότητας στο δίκτυο (network activity logging) **και έχει δυνατότητα ενεργοποίησης συναγερμών,** κατά τον εντοπισμό μιας ύποπτης δραστηριότητας τη στιγμή που αυτή πραγματοποιείται (1).

Πίνακας 3. Σύγκριση 5 διαφορετικών μοντέλων ISMS (74)

		ISO 27001	BS 7799	PCIDSS V2.0	ITIL V4.0	COBIT V4.1
1.	*Information Security Policy*	√	√	√	√	√
2.	*Communications and Operations Management*	√	√	√	●	√
3.	*Access Control*	√	√	√	√	√
4.	*Information Systems Acquisition, Development and Maintenance*	√	√	√	●	√
5.	*Organization of Information Security*	√	√	√	√	√
6.	*Asset Management*	√	√	√	√	√
7.	*Information Security Incident Management*	√	●	√	√	√
8.	*Business Continuity Management*	√	√	√	√	√
9.	*Human Resources Security*	√	√	√	●	√
10.	*Physical and Environmental Security*	√	√	√	●	√
11.	*Compliance*	√	√	√	√	√

5.1.2 **Σκοποί ενός ISMS**

Σύμφωνα με την εργασία της κ. Λερατάκη (71) το ISMS σκοπό έχει:

- Να αναγνωρίσει το μέγεθος της ζημιάς σε περίπτωση απώλειας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας για κάθε αγαθό.

- Να επιλέξει τα controls (μέτρα) που θα υλοποιήσει με βάση το πρότυπο, και τέλος

- Να ετοιμάσει την Αναφορά Προσαρμοστικότητας (Statement of Applicability) - με βάση την εκτίμηση κινδύνου, καταγράφοντας τα επιλεγμένα controls, και δικαιολογώντας τυχόν επιλογές και εξαιρέσεις στα πλαίσια του ISMS.

- Την προβολή όλων των καταχωρημένων αξιολογήσεων, και την επεξεργασία τους. Να δίνει τη δυνατότητα στον διαχειριστή πρόσβασης σε όλες τις καταχωρήσεις τις οποίες να μπορεί να επεξεργαστεί/διορθώσει.

- Την διαγραφή καταχωρήσεων: Ο διαχειριστής μπορεί ακόμα και να διαγράψει τις καταχωρήσεις αν κριθεί απαραίτητο.

- Την εξαγωγή καταχωρήσεων σε “csv” μορφή: Ο administrator θα μπορεί να εξάγει τις καταχωρήσεις και τα αποτελέσματα σε csv μορφή για περαιτέρω επεξεργασία ή για αποστολή των αποτελεσμάτων σε τρίτους.

Θα πρέπει να εξασφαλιστεί ότι ένα ΠΣ, είναι όσο το δυνατόν ασφαλές. Για το σκοπό αυτό στην εργασία της κ. Λερατάκη (71) πραγματοποίησαν δοκιμές penetration testing στην εφαρμογή του ISMS. Εντόπισαν και κατέγραψαν για παράδειγμα τα ακόλουθα προβλήματα:

- Εντοπίσαν πρώην εργαζόμενους οι οποίοι ενω είχαν αποχωρήσει από την εταιρεία ο εταιρικός τους λογαριασμός δεν είχε απενεργοποιηθεί στο active directory και ούτε στις εφαρμογές που τους είχε χορηγηθεί πρόσβαση. Η καθυστέρηση στην ανάκληση των δικαιωμάτων πρόσβασης χρηστών μπορεί να αυξήσει τον κίνδυνο οι πρώην εργαζόμενοι και /ή άλλοι εξωτερικοί συνεργάτες, να αποκτήσουν μη εξουσιοδοτημένη πλέον πρόσβαση σε συστήματα και εφαρμογές της εταιρείας. Οι περιττοί λογαριασμοί χρηστών μπορεί ακόμα να χρησιμοποιηθούν καταχρηστικά από τους υπάρχοντες εργαζόμενους της εταιρείας για την εκτέλεση μη εξουσιοδοτημένων συναλλαγών.

- Παρατηρήθηκε ότι παρόλο που είχε εγκατασταθεί μηχανισμός για έλεγχο της φυσικής πρόσβασης στο ISMS εντός του ανελκυστήρα, αυτός δεν είχε ενεργοποιηθεί και επομένως δεν εφαρμοζόταν. Ως εκ τουτου οποιοσδήποτε με πρόσβαση στο κτήριο μπορεί να εισέλθει και σε όλες τις εγκαταστάσεις της εταιρείας και στο data και computer room. Ο μηχανισμός αυτός θα πρέπει να ενεργοποιηθεί και μόνο εξουσιοδοτημένα άτομα να έχουν πρόσβαση (71).

5.2 Έλεγχος μιας νέας δικτυακής εφαρμογής στο ΠΣ

Σχετικά με νέες τεχνολογίες όπως μία web εφαρμογή, μια εφαρμογή κινητών κλπ, πριν χρησιμοποιηθούν στο ΠΣ είναι σημαντικό να εξασφαλιστεί ότι είναι ασφαλής. Πραγματοποιώντας ένα penetration test σε μία νέα εφαρμογή μπορεί ένας οργανισμός πολλές φορές να γλυτώσει χρόνο, χρήμα και μπελάδες. Επιπλέον πρέπει κατά τη διάρκεια ζωής μιας εφαρμογής, να ελέγχεται περιοδικά ώστε να εξασφαλίζεται ότι το σύστημα παραμένει ασφαλές από αυτή. Η προσέγγιση γι΄αυτό πρέπει να συνδυάζει αυτόματες αλλά και επιθυμητές τεχνικές για την διεξαγωγή white box - security τέστ της εφαρμογής και της υποδομής (έγινε δηλαδή ανάλυση και εντοπισμός ευπαθειών του ΠΣ, με βάση το ISO27K, αλλά δεν διεξήχθησαν και «επιθέσεις» εναντίον αυτών των ευπαθειών). Έχοντας πλήρη γνώση των λειτουργιών της εφαρμογής και της υποστηρικτικής της υποδομής, χρησιμοποίησαν διάφορα εργαλεία και manual τεχνικές για να αναγνωρίσουν συνήθεις ευπάθειες και προβλήματα ασφάλειας (71).

Αρχικά στην εργασία της κ. Λερατάκη (71) κάνουν μια χαρτογράφηση της εφαρμογής χρησιμοποιώντας εργαλεία κυρίως το Burp Suite Pro και το Nikto. Αναφέρει ότι μπορούσαν να χρησιμοποιήσουν άλλα εργαλεία όπως το Dirbuster και το SSLScan όμως δεν το έκαναν καθώς ακολουθήθηκε white-box προσέγγιση. Κάθε εύρημα επιβεβαιώθηκε με χειροκίνητους ελέγχους. Στο τέλος του ελέγχου εκτιμήθηκε η εκμετάλλευση αδυναμιών.

Η μετρική κινδύνου που χρησιμοποιήσαν για την αξιολόγηση κινδύνου, βασιζόταν στην επίπτωση, στην ευκολία εκμετάλλευσης και σε κάποιες περιπτώσεις την αυθεντικοποίηση και την δικτυακή τοποθεσία. Για κάθε

ευπάθεια που βρέθηκε, μετρήθηκε ο κίνδυνος με τα παραπάνω κριτήρια χρησιμοποιώντας την παρακάτω συνάρτηση:

Risk = Impact * Exploitability * (Authentication + Location)

- Η εφαρμογή που εξέτασαν, επέστρεφε μήνυμα λάθους κατά την φάση της ταυτοποίησης, αποκαλύπτωντας εαν ο χρήστης υπάρχει ή όχι στο σύστημα. Αυτό είναι ευπάθεια, που μπορεί να εκμεταλλευτεί ένας χάκερ ώστε να αναγνωρίσει τα έγκυρα ονόματα χρηστών. Μπορεί να χρησιμοποιηθεί αργότερα για επιθέσεις όπως brute force και στα συνθηματικά σε περίπτωση που δεν έχει υλοποιηθεί lock out μηχανισμός κλειδώματος, συντελώντας εντέλει σε κακόβουλη πρόσβαση στο ΠΣ. Την ίδια ευπάθεια αν εκμεταλλευτεί ένας επιτιθέμενος μπορεί ακόμα να προκαλέσει Denial of Service (DoS), κλειδώνοντας τους λογαριασμούς αυτούς.

- Παρατήρησαν επίσης ότι η εφαρμογή δεν κλειδώνει έναν χρήστη μετά από επανειλημμένες προσπάθειες σύνδεσης με λάθος συνθηματικό. Σε περίπτωση brute force επιθέσεων, αυτό μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση στην εφαρμογή.

- Ταυτόχρονες συνδέσεις: Ήταν δυνατό να δημιουργηθούν δυο ταυτοποιημένες συνδέσεις στην εφαρμογή με τον ίδιο χρήστη συγχρόνως. Αυτό ελέγχθηκε κάνοντας login στην εφαρμογή από δύο διαφορετικούς browsers την ίδια χρονική στιγμή, κάτι τέτοιο όμως επιτρέπει το διαμοιρασμό των ίδιων στοιχείων εισόδου μεταξύ των χρηστών, και μειώνει το επίπεδο καταλογισμού.

- Η κίνηση των δεδομένων από και προς την ISO27001:2013 web εφαρμογή εστέλνετο μη κρυπτογραφημένη. Αυτό σημαίνει ότι δεδομένα, όπως τα στοιχεία σύνδεσης είναι ευάλωτα σε Man-in-The-Middle επιθέσεις. Ένας επιτιθέμενος μπορεί να παρεισφρήσει στην επικοινωνία παραποιώντας τα δεδομένα (spoofing).

- Επιπλέον σημειώθηκε ότι proxy servers μεταξύ του χρήστη και του server μπορούσαν να διατηρούν logs και ευαίσθητη πληροφορία σε clear text μορφή. Προτείνεται να χρησιμοποιείται το HTTPS πρωτόκολλο για τη

μεταφορά τέτοιας πληροφορίας. Κάθε request στο HTTP κανάλι θα πρέπει να δρομολογείται στο HTTPS και το HTTP κανάλι συστήνεται να απενεργοποιηθεί τελείως (71) .

- Η έλλειψη τερματισμού της συνόδου από τη πλευρά του server, επιτρέπει το ενδεχόμενο επανεισόδου κάποιου, σε περίπτωση που πάρει τη συσκευή ένας επιτιθέμενος (session hijacking). Επιπλέον αν ο Η/Υ χρησιμοποιείται από περισσότερους από έναν χρήστη η αδυναμία αυτή μπορεί να προκαλέσει πειρατεία συνόδου - και επιθέσεις επανάληψης- replay attacks, όπου επαναλαμβάνεται κάποιο μήνυμα για κακόβουλους σκοπούς.

- Η εφαρμογή βρέθηκε ευάλωτη σε επιθέσεις Clickjacking. Με την επίθεση αυτή ένας επιτιθέμενος μπορεί να δημιουργήσει μία κακόβουλη σελίδα η οποία φορτώνει μέσω του iframe το έμπιστο site. Το θύμα πιστεύοντας ότι είναι στο έμπιστο site περιπλανείται και εκτελεί ενέργειες χωρίς τη θέληση του. Αξίζει να σημειωθεί ότι η επίθεση αυτή προσπερνάει αντίμετρα για CSRF επιθέσεις (Cross Site Request Forgery). Για να προστατευτεί μία εφαρμογή από επιθέσεις Clickjacking, προτείνει να τεθεί ο X-Frame-Options HTTP header στην τιμή SAMEORIGIN ή DENY (71).

5.3 Κουλτούρα ασφάλειας ΠΣ σε έναν οργανισμό

Η υιοθέτηση ενός πλαισίου κουλτούρας ασφάλειας ΠΣ σύμφωνα με τους A. Da Veiga, J.H.P. Eloff (75), θα ελαχιστοποιεί τους κινδύνους από την ανθρώπινη συμπεριφορά και θα βοηθάει να επιτυγχάνονται οι στόχοι κάθε οργανισμού (75). Σύμφωνα με την εργασία της κ.Θεοχαρίδου, et al (76), το ISO υιοθέτησε το **Βρεττανικό Πρότυπο BS7799** («Πρακτικής για Διαχείριση ασφάλειας των πληροφοριών») και το εξέδωσε στη συνέχεια σαν **Διεθνές Πρότυπο ISO17799**. Αυτό παρέχει οδηγίες που καλύπτουν την προστασία τις πληροφορίας, σαν περιουσιακό στοιχείο, αλλά καλύπτει και τις πλευρές των φυσικών στοιχείων, του προσωπικού, κλπ. Βασίζεται στη Διαχείριση Κινδύνου, δηλαδή στην διαδικασία αναγνώρισης, περιορισμού, και ελαχιστοποίησης των κινδύνων ασφάλειας των ΠΣ, για ένα αποδεκτό κόστος,

όμως ενώ ασχολείται ικανοποιητικά με τις εξωτερικές απειλές δεν ασχολείται επαρκώς με τις εσωτερικές απειλές (76).

Η κ Θεοχαρίδου et al (76) , στην εργασία τις για την εσωτερική απειλή στα ΠΣ, την εξέτασε υπό **το πρίσμα διάφορων προτύπων εγκληματολογικών θεωριών.** Το πρότυπο πρόληψης του ευκαιριακού εγκλήματος π.χ. εξετάζει την απειλή όχι μόνο σε σχέση με το κίνητρο που τυχόν έχει ο υποψήφιος παραβάτης, αλλά και τις ευκαιρίες που μπορεί να του παρουσιάζονται. Βασίζεται με τη σειρά του στη θεωρία τις πρόληψης εγκληματικότητας βάσει ευκαιριών του 1980 (Clarke situational crime prevention). Σύμφωνα με αυτή πρέπει να λαμβάνονται μέτρα που να ελαχιστοποιούν τις εγκληματικές ευκαιρίες.

- Κάνοντας το έγκλημα πιο δύσκολο (έλεγχος πρόσβασης)
- Πιο επικίνδυνο (παρακολούθηση, επαναξιολόγηση audit)
- Ελαττώνοντας το προσδωκόμενο από αυτό κέρδος
- Αποδομώντας τις τυχόν δικαιολογίες που μπορεί να επικαλεστεί κάποιος, για να δικαιολογήσει τις πράξεις του. Σε αυτό μπορεί να συντελέσει η ύπαρξη πολιτικής ασφαλείας και προγραμμάτων ενημέρωσης.

Με την περίπτωση τις εσωτερικής απειλής ασχολείται και η **γενική θεωρία τις αποτροπής** GDT-General Deterrence Theory, σύμφωνα με την οποία οι άνθρωποι παίρνουν λογικές αποφάσεις βασιζόμενοι στη μεγιστοποίηση του οφέλους και στην ελαχιστοποίηση του κόστους (Beccaria, 1963). Η αποτροπή μιας πράξης, βασίζεται στη βεβαιότητα τις ποινής και στη βαρύτητά της (Straub & Welke 1998), ιδιαίτερα όταν το κίνητρο είναι μικρό (76).

Σύμφωνα με τον κ. Μαγκλάρα (77), μια εσωτερική απειλή θα πρέπει να ταξινομείται σε τρείς βασικές διαστάσεις και πρέπει να αξιολογείται με κέντρο τους ανθρώπους. **Τον ρόλο των απασχολουμένων στο ΠΣ** (χρήστες, εργαζόμενοι στους σέρβερ, στις τηλεπικοινωνίες), **τον λόγο που προβαίνουν στην κατάχρηση, και τις συνέπειες για το ΠΣ** από τη δράση τους (77). Ο «παράγοντας άνθρωπος» ως προς την ασφάλεια πληροφοριών

πρέπει να εξετάζεται σε δύο διαστάσεις τη Γνώση και την Συμπεριφορά, που είναι αλληλοσχετιζόμενες

1) Ανάλογα με το ρόλο τους και το επίπεδο και τον τύπο γνώσης που έχουν για το σύστημα, οι χρήστες κατηγοριοποιούνται:

- σε αυτούς που έχουν πλήρη διαχειριστικά δικαιώματα, τους διαχειριστές δηλαδή του συστήματος - αυτοί είναι σοβαρή πιθανή απειλή σε έναν οργανισμό,

- στους προχωρημένους χρήστες, όπως π.χ. προγραμματιστές, διαχειριστές ΒΔ, ή παλιούς διαχειριστές του συστήματος. Οι τελευταίοι αν και δεν έχουν πλέον πρόσβαση σε όλους τους πόρους εντουτοις είναι γνώστες πιθανών ευπαθειών και μπορεί να επιχειρήσουν να τις εκμεταλλευτούν. Παράλληλα συχνά έχουν και το μεγαλύτερο κίνητρο για να κάνουν κατι τέτοιο ιδιαίτερα αν θεωρούν ότι έχουν τύχει μιας άδικης συμπεριφοράς και απόλυσης από τον οργανισμό ή έχουν πάει να εργαστούν σε έναν ανταγωνιστικό οργανισμό.

- στους απλούς χρήστες εφαρμογών. Εδώ περιλαμβάνονται οι υπόλοιποι νόμιμοι χρήστες που χρησιμοποιούν τους πόρους των ΠΣΝ σαν περιηγητές, π.χ. χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο ή κάποιες άλλες εφαρμογές (77).

2) Ανάλογα με τον λόγος της «κακής χρήσης», οι πράξεις τους μπορεί να αξιολογούνται ως εσκεμμένες ή τυχαίες. Οι εσκεμμένες ενέργειες θα μπορούσε να αποσκοπούν στο κέρδος, στην εκδίκηση ενάντια σε κάποιον ή σε ολόκληρο τον οργανισμό (προσωπικές διαφορές) ή στην επίτευξη προσωπικών στόχων να καταλάβουν π.χ. μια υψηλότερη θέση σε έναν ανταγωνιστικό οργανισμό πραγματοποιώντας κυβερνοεπίθεση στο πληροφοριακό σύστημα και στα δεδομένα που είχαν πρόσβαση λόγω της προηγούμενης θέσης τους στον οργανισμό υγείας που δούλευαν προηγούμενα.

Το τυχαίο ανθρώπινο λάθος, μπορεί να υποκατηγοριοποιηθεί σε ελιπή γνώση του συστήματος λόγω κακής κατάρτισης και σε παράγοντες που

μπορεί να επηρρεάζουν δυσμενώς την εργασιακή τους απόδοση π.χ. υπερκόπωση, ή συναισθηματικά προβλήματα. Επίσης μπορεί να τυχαίνει κάποιος χρήστης να μην είναι γνώστης ενός συγκεκριμένου κανονισμού ασφαλείας (77).

Οι **συνέπειες στο σύστημα από την «κακή χρήση»,** αποτελούν το αντικείμενο του **εργαλείου «Insider Threat Prediction Tool–ITPT»** που βάζει τα θεμέλια των κριτηρίων ελέγχου που πρέπει να εφαρμόζονται. Αυτό μοιάζει στη δομή με ένα IDS.

Όπως ένα IDS, μπορεί να αφορά το δίκτυο, το λογισμικό ή τον εξοπλισμό του ΠΣ. Εξετάζοντας το σύστημα αρχείων, το εργαλείο μπορεί να εντοπίσει προσπάθειες τροποποίησης της δομής του συστήματος αρχείων, της διαγραφής, αλλαγής ή εκτέλεσης ενός συγκεκριμένου αρχείου, καθώς επίσης και την αποθήκευση μη εξουσιοδοτημένου λογισμικού (όπως άσχετα εργαλεία, πορνογραφικό υλικό, παιχνίδια, και δούρειοι ίπποι). Το πόρισμα του αναλυτή του ITPT εργαλείου, είναι μια ομαδοποίηση των «προφίλ απειλής» όλων των χρηστών του ΠΣ.

Προκειμένου για μια **πιθανή εσκεμμένη απειλή**, το εργαλείο ITPT βρίσκει αποδείξεις ότι κάποιος χρήστης πιθανώς θα επιχειρήσει «κακή χρήση» του συστήματος. Πιθανή εσκεμμένη απειλή υπάρχει: όταν δίνει ενδείξεις ότι κάποιος συγκεκριμένος χρήστης, είναι πολύ πιθανό να εκδηλώσει κάποια συγκεκριμένη κακόβουλη ενέργεια.

Παρόμοια και για μια **πιθανή τυχαία απειλή** από κάποιον χρήστη που είναι απρόσεκτος. Επίσης ανιχνεύει ακόμα και υποψία για απειλές χωρίς σαφείς πιθανότητες να είναι όντως, και τέλος επιβεβαιώνει και ποιοι είναι καλοί από τους χρήστες (επιβεβαίωση ασφάλειας) (77).

Άλλα προφίλ χρηστών που μπορούν να υποδείχθουν από το ITPT εργαλείο είναι: **Εν δυνάμει ακούσια απειλή**: όταν παρέχει ενδείξεις, πως ένας χρήστης πρόκειται να κάνει μια συγκεκριμένη επιβλαβή χρήση κατά λάθος. **Ύποπτη Χρήση**: όταν ανιχνεύει ύποπτες δραστηριότητες κάποιου χρήστη αλλά δεν είναι σαφές ότι αυτές οι δράσεις θα οδηγήσουν σε βλάβη. **Ακίνδυνη**

Χρήση: όταν δεν υπάρχει καμμία ένδειξη ότι ο συγκεκριμένος χρήστης θα προκαλέσει κάποια ανεπιθύμητη βλάβη (77).

Ένας μεγάλος οργανισμός θα πρέπει οπωσδήποτε να έχει μια στρατηγική ασφαλείας απέναντι στην εσωτερική απειλή. Θα μπορούσε κανείς να σκεφτεί ότι τα οικονομικά έξοδα για την ασφάλεια ΠΣ, βρίσκοναι ως ένα σημείο σε αντιδιαστολή με τους συνήθεις στόχους μιας επιχείρησης, που είναι να μεγιστοποιήσει την παραγωγικότητα - ελαχιστοποιώντας παράλληλα το κόστος. Αυτό γιατί χρειάζονται να καταναλωθούν εργατοώρες του προσωπικού και να γίνουν μεγάλα έξοδα προμήθειας εξοπλισμού που δεν έχουν στόχο το κέρδος του οργανισμού, αλλά την αποφυγή ζημιάς. Τα μέτρα ασφάλειας δεν είναι μέτρα που αυξάνουν τα οικονομικά οφέλη στην επιχείρηση ή στον οργανισμό. Οπωσδήποτε τα μέτρα ασφαλείας ενός ΠΣΥ κοστίζουν πολύ, ίσως όμως όχι τόσο όσο μια ενδεχόμενη παραβίαση και αυτό είναι κάτι που μια ανάλυση κινδύνου θα πρέπει να το αποτυπώνει ώστε να λαμβάνονται τα απαραίτητα μέτρα (78).

Η όποια στρατηγική ασφαλείας ενός οργανισμού θα πρέπει να λαμβάνει υπόψιν της τον **«παράγοντα-άνθρωπο»**. Αν προωθηθεί μια **κουλτούρα ασφάλειας πληροφοριών,** οι εργαζόμενοι στο ΠΣ θα μεταβληθούν σε πλεονέκτημα αντί για κίνδυνο. Η στρατηγική αυτή θα πρέπει να δημιουργεί ένα πλαίσιο που θα ενσωματώνει και την διαχειριστική και την οικονομική επιστήμη προκειμένου να είναι πιο κατανοητή από τη διοίκηση του οργανισμού. Εκστρατείες ενημέρωσης στον οργανισμό, όπως προτείνονται από τον ISO 27002, βοηθούν στο πρόβλημα έλλειψης σχετικής γνώσης στην καθημερινή εργασία του κάθε υπαλλήλου.

Στην εργασία του Eric Albrechtsen (79) μελετήθηκε η διάθεση των υπαλλήλων στο να εφαρμόσουν πολιτική ασφάλειας σε σχέση με τις απαιτήσεις της διοίκησης και πως θα αξιολογηθεί το επίπεδο κουλτούρας ασφάλειας του οργανισμού. Η εργασία απέδωσε το ότι οι χρήστες δεν είναι ενήμεροι σχετικά με τις απαιτήσεις ασφαλείας ενός ΠΣ:

- στην έλλειψη χρόνου για να τις διαβάσουν,

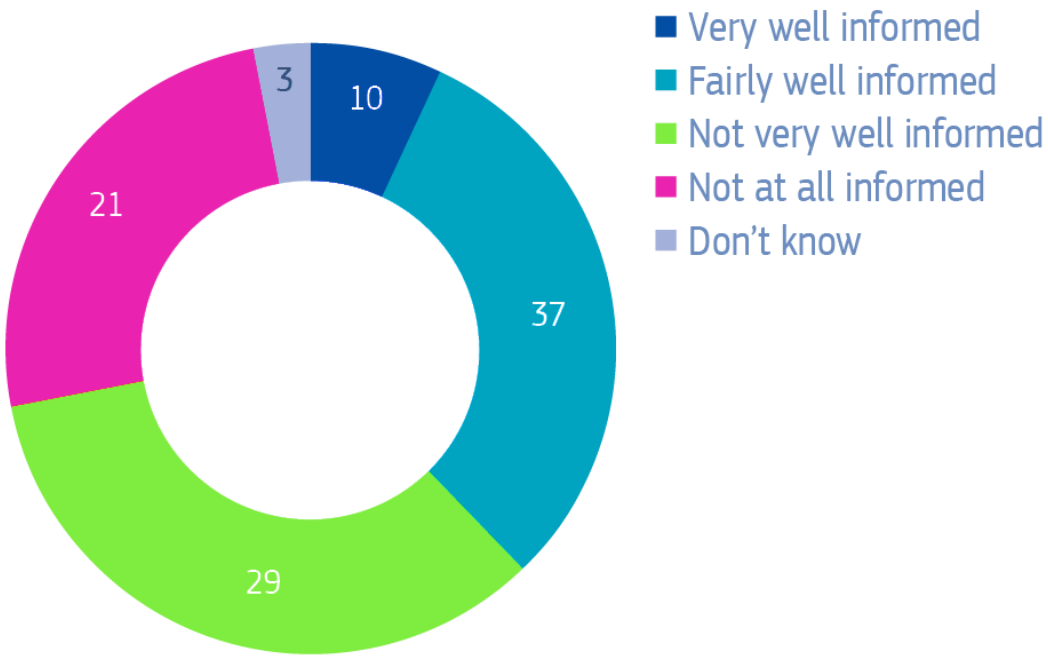
- στην έλλειψη ενημέρωσης για το που μπορεί να βρούν τις οδηγίες χρήσης,
- στην έλλειψη κινήτρων για να τις διαβάσουν,
- στην έλλειψη γνώσης για να τις κατανοήσουν.

Τα αποτελέσματα της μελέτης, βασίστηκαν σε συνεντεύξεις χρηστών στο κέντρο εξυπηρέτησης μια εταιρείας πληροφορικής και σε μια τράπεζα αλλά ενδεχομένως παρόμοια θα ήταν και τα αποτελέσματα σε αντίστοιχα τμήματα ενός άλλου οργανισμού όπως ενός νοσοκομείο ή ένα κέντρο υγείας. Η μελέτη επικεντρώθηκε σε χρήστες χωρίς μεγάλη ευθύνη στον οργανισμό και με χαμηλό βαθμό αντίληψης και γνώσης σχετικά με τα ΠΣ (79)

Στα αποτελέσματα προκύπτει ότι οι χρήστες φαίνεται να αντιλαμβάνονται την σπουδαιότητα του ρόλου τους στην ασφάλεια πληροφοριών. Όμως προέκυπτε χάσμα μεταξύ των προθέσεων και της συμπεριφοράς τους και επίσης ότι δεν είναι εξοικειωμένοι με το τι πρέπει να κάνουν στην πράξη από πλευράς ασφάλειας ΠΣ και προστασίας δεδομένων. Επίσης φαίνεται να πιστεύουν ότι περαιτέρω απασχόληση τους με το θέμα της ασφάλειας ΠΣ θα είχε δυσμενή επίδραση στην αποδοτικότητά και αποτελεσματικότητά τους, στα άλλα τους καθήκοντα. Όσον αφορά τους χρήστες αυτοί παραδόξως προτιμούν να ενημερωθούν μέσω σεμιναρίων αν και διαμαρτύρονται ότι δεν έχουν χρόνο, παρά με ενημερωτικές καμπάνιες ή με μελέτη πρωτοκόλλων και οδηγιών χρήσης που δεν κοστίζουν τόσο πολύ από πλευράς χρόνου (79).

Προέκυπτε δηλαδή ότι δεν είναι κάτι απλό από πλευράς εφαρμογής η εκτεταμένη απαίτηση από τους χρήστες του ΠΣ ενός οργανισμού να απασχολούνται και να ενημερώνονται για θέματα ασφάλειας των ΠΣ. Πόσο μάλλον αντίστοιχα σύνθετο θα ήταν σε ένα χώρο νοσοκομείου όπου οι εργαζόμενοι δεν έχουν την πολυτέλεια να αφήνουν από την προσοχή τους τους ασθενείς και να ασχολούνται με τα ΠΣ και τις ανάγκες αυτών για ασφάλεια. Εν τούτοις κάποια προσπάθεια, θα πρέπει να γίνεται συνεχώς αφού τα ΠΣ έχουν καλώς ή κακώς ενσωματωθεί στην καθημερινή λειτουργία των νοσοκομείων. Μπορεί να γίνεται μέσα από καμπάνιες - ενημέρωσης από τα ΜΜΕ, ή με εκτυπωμένες οδηγίες προς το προσωπικό, και σεμινάρια.

Στην παρακάτω εικόνα, καταγράφονται οι απαντήσεις των ευρωπαΐων πολιτών στην ερώτηση ‘ Πόσο καλά ενημερωμένος αισθάνεστε σχετικά με τον κίνδυνο από κυβερνοεγκλήματος ;’



***Εικόνα 10. EPSC- Πόσο ενημερωμένοι αισθάνονται οι ευρωπαΐοι για το κυβερνοέγκλημα* (40)**

Οι εργαζόμενοι της μελέτης (79) , δεν έβρισκαν σημαντικές τις καμπάνιες ευαισθητοποίησης. αφού μια που έγινε με φυλλάδιο για την προσεκτική χρήση του ηλεκτρονικού ταχυδρομείου και συνοδευόταν με κάποια σοκολατάκια, φάνηκε ότι δεν την βρήκαν αποτελεσματική είτε γιατί δεν υπήρχε αρκετός χρόνος, είτε γιατί τα σοκολατάκια τους φάνηκαν πιο ενδιαφέροντα, είτε γιατί ξέχναγαν αμέσως το μήνυμα, είτε το μήνυμα δεν ήταν κάτι το καινούργιο. Σε άλλο σημείο αναφέρεται στην αντίθεση μεταξύ του ατομικού συμφέροντος και της λειτουργικότητας ενός ΠΣ, όταν οι συνεντευξιαζόμενοι ανέφεραν π.χ. ότι γράφανε τα συνθηματικά τους σε ποστ-ιτ χαρτάκια, αφού δεν μπορούσαν να τα θυμούνται αλλιώς ώστε να μπορούν δουλέψουν. Αυτό βέβαια από πλευράς

ασφάλειας είναι μεγάλο σφάλμα (79), αφού μπορεί εύκολα κάποιος να τα κλέψει.

5.4 Ασφάλεια στο επίπεδο εφαρμογής

5.4.1 **Ασφάλεια Λειτουργικών συστημάτων**

Για τον καθημερινό χρήστη η ασφάλεια οφείλει να ξεκινάει από το λειτουργικό σύστημα που χρησιμοποιεί. Αν και τα Linux θεωρούνται γενικά πιο ασφαλή, τα Windows είναι πιο διαδεδομένα σε μεγάλους οργανισμούς όπως τα νοσοκομεία, λόγω και της εξοικείωσης του μέσου χρήστη.

Τα Windows, διαθέτουν μια πληθώρα από μηχανισμούς ασφαλείας όπως :

1. Τους κωδικούς πρόσβασης.

2. Τον διαχειριστή του συστήματος που είναι ο χρήστης εγκατάστασης, και έχει πλήρη δικαιώματα. Μπορεί επίσης να δημιουργήσει λογαριασμούς χρηστών, ή και ομάδας αυτών, και μετά να τους δώσει συγκεκριμένα δικαιώματα.

3. Τα τείχη Προστασίας στα windows που είναι προγράμματα και όχι συσκευές.

4. Τα αντίγραφα ασφαλείας. Έτσι προστατεύονται αρχεία από εκούσια ή ακούσια καταστροφή τους.

5. Με βάση τα Windows μπορεί να στηθεί επίσης ένα έμπιστο δίκτυο VPN από Η/Υ, οι οποιοί μπορούν να ανταλάσσουν δεδομένα μεταξύ τους με ασφάλεια. Με τις τεχνολογίες IP/VPN, μπορεί να κατασκευασθεί ένα δίκτυο που θα συνδέσει έναν Η/Υ που βρίσκεται εκτός του ασφαλούς δικτύου με το έμπιστο δίκτυο, περνώντας τα IP πακέτα του κρυπτογραφημένα μέσω TCP/IP. Το VPN είναι μια κρυπτογραφημένη σύνδεση από το ένα σημείο στο άλλο, και ενεργεί σαν να είναι ιδιωτικό δίκτυο. Μπορεί να χρησιμοποιεί τεχνολογία “tunneling”, που σημαίνει ότι τα ιδιωτικά δεδομένα είναι κρυπτογραφημένα και ενθυλακώνονται σε IP πακέτα δεδομένων για μεταφορά στο διαδίκτυο, όπως επίσης και τα άλλα δεδομένα κίνησης.

6. Τις προειδοποιήσεις ασφαλείας που εμφανίζονται αν κάποιος χρήστης από αμέλεια θέσει σε κίνδυνο το λειτουργικό σύστημα.

5.4.2 **Ψηφιακή Υπογραφή**

Αφού η ψηφιακή τεχνολογία μπαίνει ολοένα και περισσότερο στην καθημερινότητα ενός ευαίσθητου χώρου όπως η υγεία και τα ηλεκτρονικά έγγραφα αντικαθιστούν τους παλαιούς χάρτινους ιατρικούς φακέλλους, γεννάται το θέμα πως θα υπογράφονται από τους δημιουργούς τους όλα αυτά τα ηλεκτρονικά έγγραφα που συντάσσονται. Επίσης το ίδιο προκύπτει και για όλα τα άλλα έγγραφα (διοικητικά, οικονομικά κλπ), ενός ΟΠΣΥ πως θα πρέπει να υπάρχει δυνατότητα αυθεντικοποίησης των δεδομένων, και της ταυτότητας του συντάκτη τους. Υπάρχει δηλαδή η ανάγκη μην υπάρχει αμφιβολία για το ποιος καταχώρησε τα δεδομένα και εκείνος να μην έχει τη δυνατότητα να αποποιηθεί τη συμμετοχή του στην ηλεκτρονική συναλλαγή.

Σχετικές με την ψηφιακή υπογραφή νομοθετικές οδηγίες είναι:

Το **ΠΔ 150/2001** (ΦΕΚ Α΄/125 25-6-2001) που αναφέρει ότι με τον όρο ψηφιακή υπογραφή περιγράφονται **δεδομένα σε ηλεκτρονική μορφή που είναι συνημμένα σε άλλα δεδομένα, ή σχετίζονται λογικά με αυτά,** και χρησιμεύουν για την βεβαίωση της γνησιότητας τους (47). Ο λόγος που τα έγγραφα υπογράφονται είναι για να ταυτοποιήσουν τον δημιουργό τους ή μια συναίνεση. **Με την χειρόγραφη υπογραφή πιστοποιείται** : 1.Η ταυτότητα του υπογράφοντα, 2. Η πρόθεση του να υπογράψει ένα έγγραφο, 3. Το ότι εγκρίνει και υοθετεί το περιεχόμενο ενος εγγράφου. **΄Έγγραφο θεωρείται** κάθε γραπτό που προορίζεται ή είναι πρόσφορο να αποδείξει γεγονός που έχει έννομη σημασία όπως και κάθε σημείο που προορίζεται να αποδείξει ένα τέτοιο γεγονός (47).

Στις ΗΠΑ στις 30/6/2000 ο Μπιλ Κλίντον υπέγραψε την πράξη για τις ηλεκτρονικές υπογραφές: Electronic signatures in global and national commerce Act ή αλλιώς Esign.

Αντίστοιχη οδηγία στην Ευρώπη ήταν η 1999/93/ΕΚ (13/12/99) που δεν παρείχε όμως ένα ολοκληρωμένο διασυνοριακό και διατομεακό πλαίσιο, και

γι΄αυτό αντικαταστάθηκε από την eIDAS Regulation (80). Σύμφωνα με αυτές τις οδηγίες οι ηλεκτρονικές υπογραφές γίνονται αποδεκτές πλέον στα συμβόλαια και σε άλλα δεδομένα που παλαιότερα απαιτούσαν απαραίτητα την ιδιόχειρη υπογραφή (81). Εντούτοις υπάρχει ακόμα διάκριση για απλές υπογραφές (όπως π.χ. με την τοποθέτηση απλά του ονόματος κάποιου κάτω από ένα κείμενο του ηλεκτρονικού ταχυδρομείου) και προηγμένες ηλεκτρονικές υπογραφές.

Ο ν.3979/2011 για την ηλεκτρονική διακυβέρνηση ορίζει ως ηλεκτρονική υπογραφή: «δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας» (82). Στο άρθρο 7 αναφέρει ότι κατά το σχεδιασμό, διαμόρφωση και προμήθεια ΠΣ και υπηρεσιών ηλεκτρονικής διακυβέρνησης γίνεται αξιολόγηση των επιπτώσεων τους στην ιδιωτικότητα και στην ΠΔΠΧ.

Στο άρθρο 34 ορίζει ότι: σε κάθε Υπουργείο συνιστάται Γενική Διεύθυνση ή Διεύθυνση Ηλεκτρονικής Διακυβέρνησης, στο δε Υπουργείο Οικονομικών οι αρμοδιότητες, όπως ορίζονται στην παράγραφο 1, ασκούνται από τη Γενική Γραμματεία Πληροφοριακών Συστημάτων (Γ.Γ.Π.Σ.). Στο άρθρο 35 αναφέρει ότι με απόφαση του Υπουργού Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης συγκροτείται Διυπουργική Επιτροπή Ηλεκτρονικής Διακυβέρνησης (82).

Στο άρθρο 36 αναφέρει ότι σε κάθε φορέα του δημόσιου τομέα συγκροτείται Ο.Δ.Ε. (Ομάδα Διοίκησης Έργου) με αντικείμενο τη διαδικαστική, οργανωτική και τεχνική υποστήριξη της εφαρμογής του παρόντος νόμου. **Η Ο.Δ.Ε. ορίζει ένα από τα μέλη της ως εσωτερικό υπεύθυνο ΠΔΠΧ**. Ο εσωτερικός υπεύθυνος ΠΔΠΧ **φροντίζει για τη λήψη όλων των αναγκαίων τεχνικών και οργανωτικών μέτρων** για την τήρηση των αρχών και των υποχρεώσεων που περιγράφονται στον ίδιο νόμο και στο ν. 2472/1997, όπως: η υιοθέτηση και εφαρμογή πολιτικών ασφάλειας και ΠΔΠΧ, η περιοδική κατάρτιση και η ευαισθητοποίηση των εργαζόμενων του φορέα ως προς την προστασία ΔΠΧ, η πρόταση για λήψη εσωτερικών διαδικασιών ελέγχου και επαλήθευσης της

αποτελεσματικής εφαρμογής των μέτρων κατά τη λειτουργία των συστημάτων και υπηρεσιών ηλεκτρονικής διακυβέρνησης

Με το άρθρο 37 αναφέρει ότι το **Τεχνικό Γνωμοδοτικό Συμβούλιο** γνωμοδοτεί: α) για τη διαμόρφωση και επικαιροποίηση των προτύπων διαλειτουργικότητας των ΠΣ και των επικοινωνιακών συστημάτων και εν γένει των ΤΠΕ που παράγουν, προμηθεύονται ή χρησιμοποιούν οι φορείς του δημόσιου τομέα και β) για τη δημιουργία και προμήθεια υποδομών και ΤΠΕ για την ανάπτυξη και παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης από τους φορείς του δημόσιου τομέα (82).

Με το άρθρο 39 αναφέρει ότι **το Δίκτυο Δημόσιου Τομέα**, έχει σκοπό τη συγκέντρωση της ζήτησης υπηρεσιών ηλεκτρονικών επικοινωνιών και την κάλυψη του συνόλου των αναγκών και αιτημάτων για την παροχή και προμήθεια των σχετικών υπηρεσιών και συστημάτων των φορέων της Γενικής Κυβέρνησης, υπό την εποπτεία του Υπουργείου Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης. Με την έναρξη λειτουργίας του Δικτύου Δημόσιου Τομέα εντάσσονται αυτόματα σε αυτό οι φορείς που εξυπηρετούνται από το Δίκτυο ΣΥΖΕΥΞΙΣ. Σε διάστημα τριών (3) μηνών από τη λειτουργία του εντάσσονται και οι λοιποί φορείς (82).

Σύμφωνα επίσης με τον **ν.3979/2011** για την ηλεκτρονική διακυβέρνηση και λοιπές διατάξεις, «**ηλεκτρονικό έγγραφο** είναι κάθε μέσο το οποίο χρησιμοποιείται από Η/Υ ή περιφερειακή μνήμη Η/Υ με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, **για εγγραφή**, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο **υλικό στο οποίο εγγράφεται** οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, **εφ' όσον τα μέσα και τα υλικά αυτά προορίζονται** ή είναι πρόσφορα **να αποδείξουν γεγονότα που έχουν έννομη σημασία**» (82).

Για την δημιουργία τεχνικά της ψηφιακής υπογραφής χρησιμοποιείται και πάλι η τεχνική της κρυπτογράφησης. Στην κρυπτογραφία Δημοσίου Κλειδιού (public key infrastructure-PkI), το δημόσιο κλειδί είναι αυτό που μπορεί να γνωστοποιηθεί από το χρήστη σε τρίτους, το ιδιωτικό κλειδί είναι αυτό που

αποθηκεύεται με ασφάλεια και μόνο ο συγκεκριμένος χρήστης το γνωρίζει και το έχει στην κατοχή του (43) . Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη (που το έχει αποστείλει στον αποστολέα από άλλο δρόμο), και έτσι ο παραλήπτης είναι ο μόνος που μπορεί να το αποκρυπτογραφήσει αφού είναι και ο μόνος κάτοχος του ιδιωτικού του κλειδιού (δηλαδή χρησιμοποιούνται τα κλειδιά του παραλήπτη). Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφορά με την κρυπτογράφηση είναι ότι στην τελευταία ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για την δημιουργία της κρυπτογράφησης, ενώ ο παραλήπτης το δημόσιο κλειδί του αποστολέα για την επαλήθευση (δηλαδή χρησιμοποιούνται τα κλειδιά του αποστολέα) (43).

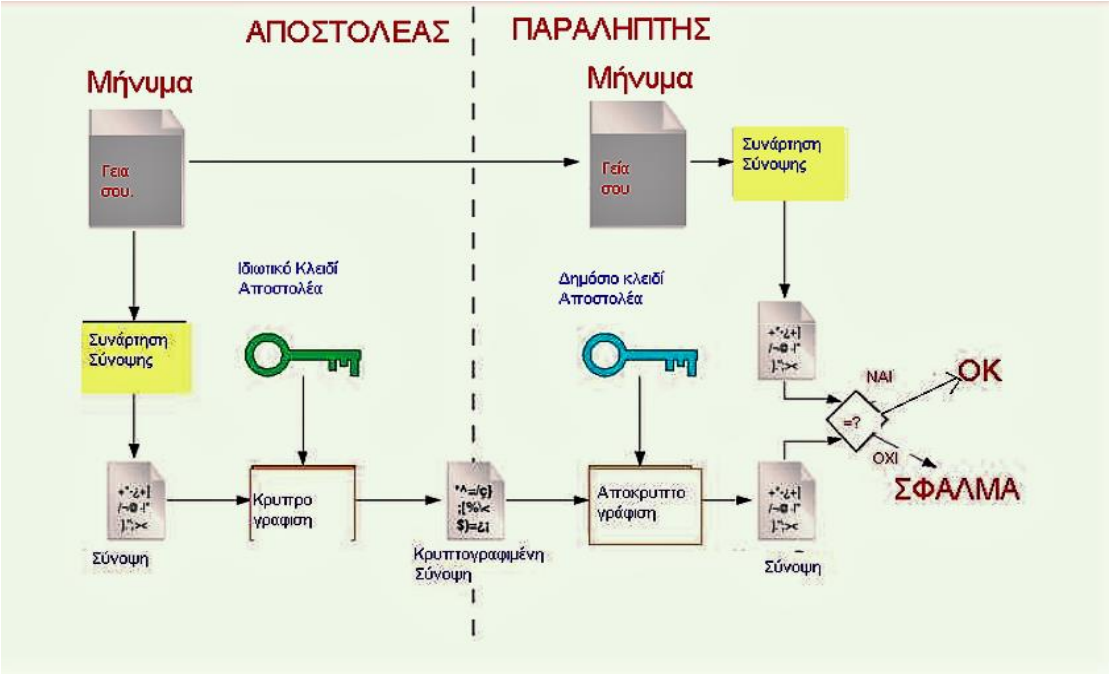
Χρειάζεται επίσης μια Αρχή, μια Έγκυρη Τρίτη Οντότητα (ΕΤΟ) - Certification Authority ή Trusted third party (TTP), που να πιστοποιεί την εγκυρότητα των ψηφιακών υπογραφών και να παρέχει πιστοποίηση. Αυτό γιατί για παράδειγμα ένας κακόβουλος επιτιθέμενος στο ΠΣ, που θέλει να υποκλέψει την επικοινωνία μεταξύ δυο άλλων χρηστών θα μπορούσε να διαθέσει το δικό του κλειδί υποκρινόμενος ότι είναι ένας εκ των δύο. Έτσι ο παραλήπτης ανυποψίαστος θα υπέγραφε με το δημόσιο κλειδί του κακόβουλου και μετα εκείνος θα χρησιμοποιούσε το ιδιωτικό του για να διαβάσει το μήνυμα και μετά να υπογράψει με το δημόσιο κλειδί του άλλου νόμιμου συνομιλητή υποκρινόμενος ότι είναι ο πρώτος και να του το προωθήσει. Έτσι στην ουσία θα υποκλέψει τα μηνύματα τους, χωρίς να γίνει αντιληπτός από εκείνους. Αν οι δυο πλευρές, χρησιμοποιούν πιστοποιητικά της ίδιας αρχής πιστοποίησης τα πράγματα είναι πιο απλά, αλλιώς πιο περίπλοκα. **Οι διαφορετικές αρχές σχετίζονται μεταξύ τους με κάποια δομή δέντρου με κλαδιά** (61) **.**

Τέλος σημαντική είναι **η Συνάρτηση Κατακερματισμού - Hush Function**, που χρησιμεύει για τη δημιουργία και επαλήθευση της ψηφιακής υπογραφής. Έτσι διασφαλίζεται η ταυτότητα του αποστολέα αλλά και η υπογραφή του, ακόμα και αν έχει κλαπεί η συσκευή του.

Μια απλή ηλεκτρονική υπογραφή όπως π.χ. η ψηφιακή εικόνα μιας χειρόγραφης υπογραφής θα είχε χαμηλή αξιοπιστία. Αντίθετα αν παράγεται με τη βοήθεια κρυπτογραφίας είναι αξιόπιστη, όμως μπορεί να υπάρξει

πλαστογραφία στην περίπτωση που ο κάτοχος του ιδιωτικού κλειδιού δεν το έχει πια υπό την κατοχή του (π.χ. μπορεί να έχει χάσει το μέσο στο οποίο αυτό έχει αποθηκευτεί π.χ. ένα κομπιούτερ, ή laptop) (47).

Στην περίπτωση της ψηφιακής υπογραφής διακρίνουμε δυο διαδικασίες**: την δημιουργία και την επαλήθευση.** Κατά τη δημιουργία ο αποστολέας χρησιμοποιεί κάποιον αλγόριθμο κατακερματισμού (one way hash), και με αυτόν δημιουργεί τη **σύνοψη του μυνήματος ή αλλιώς message digest,** που θέλει να στείλει.



Εικόνα 11. Δημιουργία- Επαλήθευση, Ψηφιακής Υπογραφής **(83)**

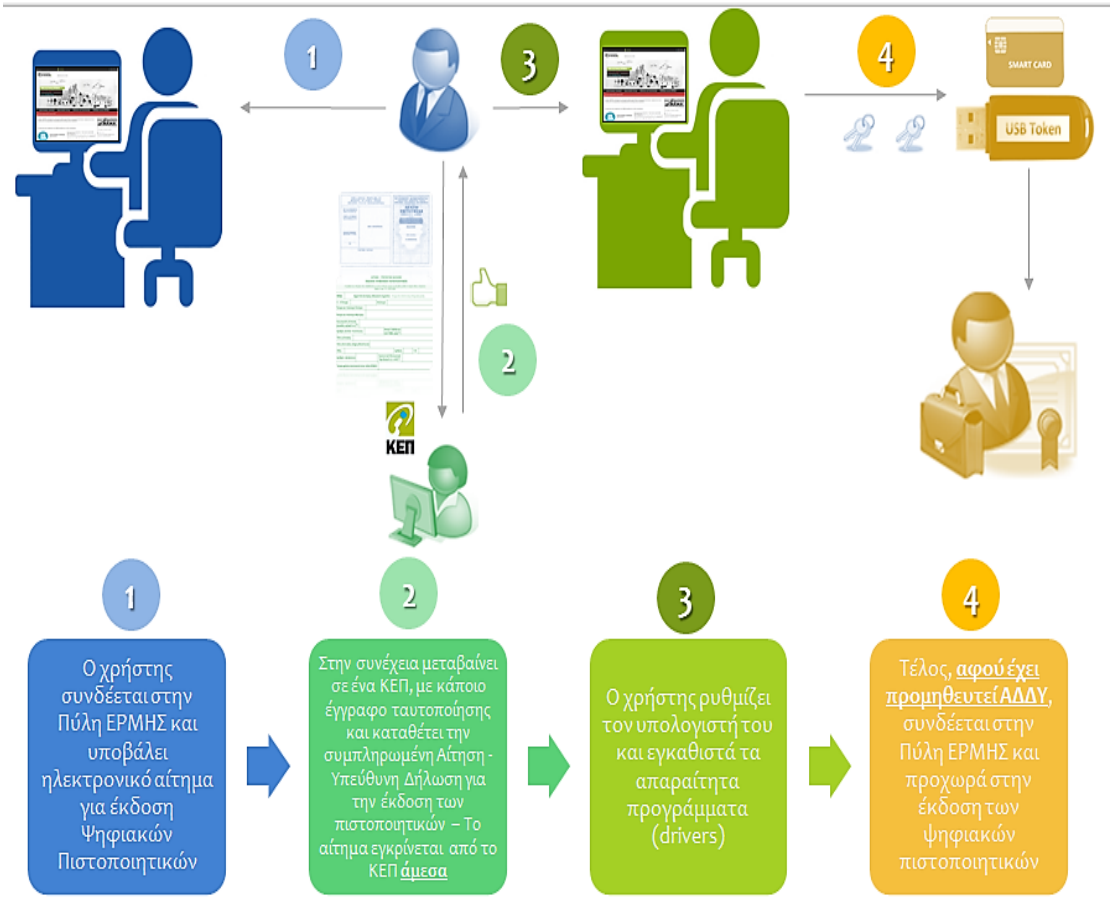
Με το ιδιωτικό του κλειδί κάνει την κρυπτογράφηση της σύνοψης και παράγει εν τέλει την ψηφιακή υπογραφή. Αυτή η κρυπτογραφημένη σύνοψη προσαρτάται στο κείμενο και τα δυο τους μεταδίδονται μέσω του δικτύου. Αν το επιθυμούσε ο αποστολέας θα μπορούσε να κρυπτογραφήσει τη σύνοψη του και το μήνυμα του κατ΄επέκταση με το δημόσιο κλειδί (που μοιράζεται με τον παραλήπτη). Ο παραλήπτης εφαρμόζει στο μήνυμα που έλαβε τον ίδιο one way hash για να εντοπίσει τη σύνοψη του μυνήματος και μετά αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα.

Συγκρίνονται οι δύο συνόψεις και αν βρεθούν ίδιες τότε το μήνυμα έχει φτάσει στον παραλήπτη ακέραιο. Αλλοιώς θα διαφέρουν. Έτσι μπορεί να επιβεβαιωθεί η ακεραιότητα των μυνημάτων αλλά και η εμπιστευτικότητα και η μη αποποίηση, που είναι βασικοί παράγοντες της ασφάλειας πληροφοριών (47). Στην Ελλάδα, το νοσοκομείο Μετροπόλιταν αναφέρεται ως παράδειγμα στην εργασία της κας Μυλωνά (47), ότι έχει εφαρμόσει σύστημα ψηφιακής υπογραφής για τα αποτελέσματα των εργαστηριακών εξετάσεων. Αναφέρεται ότι χρησιμοποιεί ένα λογισμικό, με κουμπιά sign και verify. Ο χρήστης ενημερώνεται για το αποτέλεσμα ελέγχου επαλήθευσης αν η υπογραφή είναι έγκυρη ή όχι (47).

5.4.3 **Ψηφιακά Πιστοποιητικά**

Ψηφιακό πιστοποιητικό είναι: «μια ηλεκτρονική βεβαίωση, η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο και επιβεβαιώνει την ταυτότητα του» (82).

Στα ψηφιακά πιστοποιητικά, το πρότυπο που έχει επικρατήσει διεθνώς είναι **το X-509, της ITU** (ISO/IEC 9594-8-1998), αλλά υπάρχουν και άλλα. Το X509v1 (version) το έχουν υιοθετήσει και η VISA και η MASTERCARD, για το δικό τους ασφαλές πρότυπο ηλεκτρονικών συναλλαγών (Secure Electronics Transaction / SET). Ανάλογα με το ποια είναι η έκδοση καθορίζονται και οι πληροφορίες που θα συμπεριλαμβάνει ένα πιστοποιητικό. Υπάρχουν τρείς εκδόσεις (v1, v2, v3). Το πρότυπο X509, συνίσταται επίσης για τη δημιουργία πιστοποιητικών των επαγγελματιών υγείας. Πρέπει να γίνεται διαχείριση των πιστοποιητικών αυτών που να περιλαμβάνει επίσης την διανομή, την αποθήκευση και την ακύρωση αυτών (61).



***Εικόνα 12. Συνοπτικά η διαδικασία έκδοσης ψηφιακού πιστοποιητικού* (84)**

Στην Ελλάδα η έκδοσή των ψηφιακών πιστοποιητικών, γίνεται από την κεντρική Δικτυακή πύλη Ερμής. Τα ψηφιακά πιστοποιητικά που έχουν εκδοθεί από την ΑΠΕΔ (Αρχή Πιστοποίησης του Ελληνικού Δημοσίου) μέχρι τις 19 Ιουνίου 2018, έχουν διάρκεια ζωής πέντε (5) χρόνια. Από τις 20 Ιουνίου 2018, τα πιστοποιητικά που εκδίδονται έχουν πλέον διάρκεια ισχύος τα 3 έτη.

Η **ΑΔΔΥ** (**Α**σφαλής **Δ**ιάταξη **Δ**ημιουργίας **Υ**πογραφής), που απαιτείται δεν είναι ένα απλό αποθηκευτικό μέσο. Είναι είτε ειδική συσκευή (σε μορφή έξυπνης κάρτας ή usb token), είτε μια κεντρική διάταξη εξ΄αποστάσεως δημιουργίας ψηφιακής υπογραφής. Χρησιμοποιείται μόνο για την δημιουργία ψηφιακής υπογραφής, και πρέπει να έχει μεταξύ άλλων προδιαγραφών και συμβατότητα με Υποδομή Δημοσίου Κλειδιού ΕΡΜΗ (VSP Verisign) (84).

5.4.4 **Κρυπτογράφηση**

Οι βασικότεροι στόχοι που επιτυγχάνονται με την κρυπτογράφηση είναι:

- Η Αυθεντικοποίηση. Το μήνυμα δε θα διαρρεύσει σε χρήστη που δεν έχει δικαίωμα πρόσβασης.

-. Η Ακεραιότητα. Το μήνυμα θα φτάσει στον παραλήπτη του χωρίς να έχει υποστεί αλλοίωση ή μετατροπή.

- Η Μη Αποποίηση της Παραλαβής - Αποστολής. Ο αποστολέας ή ο παραλήπτης του μηνύματος δε θα αρνηθούν ότι έστειλαν το μήνυμα.

Η συνάρτηση, ή το σύνολο των κανόνων, στοιχείων, και βημάτων που καθορίζουν την κρυπτογράφηση και αποκρυπτογράφηση, ονομάζεται κρυπτογραφικός αλγόριθμος. Αυτός σε συνδυασμό με ένα μυστικό κλειδί, μετατρέπει το αρχικά κατανοητό κείμενο σε μυστική πληροφορία. Η υλοποίηση του κρυπτογραφικού αλγορίθμου γίνεται από ένα κρυπτογραφικό σύστημα.

Οι δύο πιο διαδεδομένοι τύποι κρυπτογράφησης είναι:

- **η συμμετρική** (χρησιμοποιείται ένα ίδιο κλειδί και στο πομπό και στον αποδέκτη του μυνήματος), υπάρχουν οι ακόλουθοι τύποι:

1) Ο **DES-data encryption standard του 1977** που μειονεκτεί καθώς μπορεί να σπάσει με εφαρμογή brute Force από τους ισχυρούς Η/Υ των hackers ιδιαίτερα εαν ελέγχουν κάποιο botnet με πολλούς zobbie Η/Υ, οι χρήστες των οποίων αγνοούν για ποιόν κακόβουλο σκοπό χρησιμοποιούνται.

2) Ο νεότερος **AES-Advanced encryption algorithm του 2001.** Αυτός περιλαμβάνει ένα ξεχωριστό μηχανισμό ασφαλούς μεταφοράς του κλειδιού από τον χρήστη στον παραλήπτη κάτι που δεν είναι πάντα εύκολο γεωγραφικά, ενώ επίσης για n αριθμό οντοτήτων απαιτούνται n* (n-1)/2 αριθμός κλειδιών, κάτι εξαιρετικά πολύπλοκο να υλοποιηθεί. Για παράδειγμα για επικοινωνία μεταξύ δυο οντοτήτων χρειάζεται ένα συμμετρικό κλειδί, για τρείς οντότητες- τρία κλειδιά, για τέσσερις οντότητες - έξι κλειδιά κ.ο.κ.. Οπότε

είναι πάρα πολύ δύσκολο να εξασφαλισθεί η κρυπτογραφημένη επικοινωνία σε ομάδες χιλίων και πλέον ατόμων (61)**.**

- και **η ασύμμετρη κρυπτογραφία ή δημόσιου κλειδιού**.

Στα μέσα της δεκαετίας του 1970, ο Whitfield Diffie και ο Martin Hellman πρότειναν την χρήση ενός ζεύγους κλειδιών (key pair). Αυτά αν και διαφορετικά σχετίζονται με ένα ορισμένο μαθηματικό τρόπο και συνεργάζονται. Η γνώση του ενός δεν επιτρέπει την παραγωγή ή τον υπολογισμό του άλλου, το ένα όμως μπορεί να αποκρυπτογραφήσει ότι κρυπτογράφησε το άλλο.

Ο κάτοχος του ζεύγους κλειδιών διανέμει το δημόσιο κλειδί ελεύθερα, ενώ είναι υποχρεωμένος να προστατεύει με αυστηρότητα το ιδιωτικό του κλειδί για να μην καταρρεύσει η ασφάλεια. Όλο αυτό **στηρίζεται στην έννοια των συναρτήσεων μονής κατεύθυνσης.** Δηλαδή **μπορούμε να υπολογίσουμε το f(x) από το χ αλλά όχι και το αντίστροφο, από το ένα κλειδί υπολογίζεται το άλλο.** Απαιτείται έτσι μικρότερος αριθμός κλειδιών όσος και ο αριθμός χρηστών. Η μέθοδος αυτή προσφέρεται και για τη δημιουργία ψηφιακών υπογραφών ενώ οι συμμετρικές κρυπτογραφικές μέθοδοι όχι. Υστερεί σε ταχύτητα, και επίσης **επειδή τα δημόσια κλειδιά δεν είναι μυστικά χρειάζονται να είναι αυθεντικά και άρα απαιτούνται πιστοποιητικά δημόσιων κλειδιών (public key certificates)** που να είναι διαθέσιμα μέσω μιας έμπιστης αρχής πιστοποίησης, που τα δημοσιοποιεί σε ένα κατάλογο (directory) (61)**.**

Ο RSA και ο Rabin, βασίζονται στη δυσκολία παραγοντοποίησης του γινομένου δύο μεγάλων αριθμών (Rivest-Shamir-Adelman), ενώ ο ElGamal στο πρόβλημα Διακριτού Λογαρίθμου DLP. Τα πιο ασφαλή σήμερα κλειδιά είναι των 2048 bits, ενώ τα μικρότερα των 512 bits θεωρούνται ανίσχυρα.

Μελλοντικά μπορεί να χρησιμεύσει η αρχική ιδέα της **κβαντικής κρυπτογραφίας** που διατυπώθηκε πριν από 25 χρόνια από τον Charles Benett της IBM και τον Ζύλ Μπρασάρ του παν/μίου του Μόντρεαλ. Βασίζεται στην κβαντική αρχή της απροσδιοριστείας του Heisenberg. Λειτουργεί στέλνοντας δέσμες σωματιδίων φωτονίων, οι οποίες διαταράσσονται αν

κάποιος επιχειρήσει να υποκλέψει το μήνυμα. Πλεονεκτεί στο ότι κανείς στο συγκεκριμένο κανάλι επικοινωνίας δεν μπορεί να κρυφακούσει χωρίς να αποκαλύψει το δικό του κλειδί. Υπάρχει και το σχετικό ευρωπαϊκό πρόγραμμα SECOQC με συντονιστή του τον Kristian Monik (61).

5.4.5 **Στεγανογραφία**

Μια άλλη τεχνική μέθοδος είναι η στεγανογραφία. Η στεγανογραφία και η κρυπτογραφία δεν είναι το ίδιο. Η κρυπτογραφία κρύβει το περιεχόμενο ενός μηνύματος από ένα κακόβουλο πρόσωπο, ενώ **η στεγανογραφία κρύβει την ύπαρξη του ίδιου του μηνύματος.** Επίσης υπάρχει διαφορά στο πότε θεωρείται ότι το σύστημα «έσπασε». Στην κρυπτογραφία το σύστημα σπάει όταν ο επιτιθέμενος καταφέρει να διαβάσει το μυστικό περιεχόμενο. Ένα στεγανογραφικό σύστημα από την άλλη για να σπάσει χρειάζεται απλά ο επιτιθέμενος να εντοπίσει την ύπαρξη του μυστικού μηνύματος και να μπορέσει μετά να το διαβάσει ή να το καταστρέψει. Η διαδικασία στεγανογράφησης, είναι απλή στην χρήση και ουσιαστικά απαιτεί από το χρήστη μόνο το ανέβασμα της εικόνας στην εφαρμογή, το κλειδί κωδικοποίησης καθώς και το μήνυμα που επιθυμεί να αποκρύψει. Επίσης και η διαδικασία της ανάκτησης του μηνύματος είναι εξίσου απλή. Αρκεί ο δέκτης του μηνύματος να ανεβάσει στην εφαρμογή τη στεγανογραφημένη εικόνα καθώς και το κλειδί με το οποίο έχει κωδικοποιηθεί το μήνυμα που επιθυμεί να διαβάσει (85).

5.4.6 **΄Εξυπνες Κάρτες – Πρότυπο ISO 7816**

Ο όρος έξυπνες κάρτες χρησιμοποιείται κυρίως για πλαστικές κάρτες με μικοεπεξεργαστή. Οι κάρτες χωρίς μικροεπεξεργαστή καλούνται κάρτες μνήμης και είναι περιορισμένων δυνατοτήτων. Πιο απλές ακόμα είναι οι κάρτες μαγνητικής ταινίας που είναι οι πιο διαδεδομένες και χρησιμοποιούνται για τις τραπεζικές συναλλαγές. Οι smart cards μπορούν να χρησιμοποιηθούν για την ταυτοποίηση του χρήστη τους, κατά την πρόσβαση του σε ΠΣΥ και σε υπηρεσίες με χρήση ψηφιακών πιστοποιητικών που βρίσκονται αποθηκευμένα στην κάρτα. Μπορεί επίσης να χρησιμοποιηθούν για

δημιουργία αξιόπιστων ψηφιακών υπογραφών (61), (47). Το μεγάλο τους πλεονέκτημα είναι ότι **έχουν τη δυνατότητα της κρυπτογράφησης/αποκρυπτογράφησης,** που τις καθιστά ικανές για χρήση σε διαδικασίες ασφαλών συναλλαγών και μπορούν να χρησιμοποιηθούν **για αποθήκευση και διακίνηση ιατρικών και μη πληροφοριών.**

Διακρίνονται σε:

1) έξυπνες κάρτες επαφής, που πρέπει να εισαχθούν σε έναν αναγνώστη έξυπνων καρτών ώστε να διαβαστούν στο σημείο που το μικρό χρυσό πιάτο εφάπτεται με ειδικούς ηλεκτρικούς συνδετήρες που μεταφέρουν δεδομένα από και προς το τσιπ. Πρότυπο τέτοιων έξυπνων καρτών με επαφές αποτελεί ο ISO-7816, ο οποίος ορίζει τις διαστάσεις, τα χαρακτηριστικά και τις λειτουργίες τους (47). Το κυριότερο μειονέκτημα της τεχνολογίας είναι ότι η πλειοψηφία των Η/Υ δεν έχουν ενσωματωμένο smartcard reader, από κατασκευής τους (61).

2) και σε κάρτες χωρίς επαφή, που χρειάζεται μόνο να περάσουν κοντά από μια κεραία για να πραγματοποιήσουν μια συναλλαγή. Αυτή επικοινωνεί με την κεραία μιας μονάδας σύζευξης χωρίς φυσική επαφή μεταξύ των δυο. Αυτές **είτε διαθέτουν αυτόνομη μπαταρία, είτε αντλούν την απαιτούμενη ενέργεια από τα ραδιοκύματα του αναγνώστη.** Χρησιμοποιούνται ευρέως για την είσοδο - έξοδο από χώρους, και στις αστικές συγκοινωνίες που απαιτείται γρήγορη πρόσβαση, όμως είναι λιγότερο ασφαλείς από εκείνες που χρειάζονται επαφή με τον reader για να λειτουργήσουν (47)**.**

Ένα σημαντικό πλεονέκτημα των έξυπνων καρτών είναι ότι μέσω αυτών, ο εξουσιοδοτημένος χρήστης μπορεί να έχει πρόσβαση στον ηλεκτρονικό ιατρικό φάκελλο του ασθενή οποιαδήποτε ώρα και από οπουδήποτε. Η έξυπνη κάρτα υγείας προστατεύει τα προσωπικά δεδομένα των ασθενών με τη χρήση προσωπικού κωδικού pin. Μόνο με την εισαγωγή αυτού, είναι δυνατή η ανάγνωση και η προσθήκη ιατρικών δεδομένων. Αντίστοιχη κάρτα με PIN μπορεί να έχει και ο γιατρός με το οποίο μπορεί να προσπελάσει ή και να μεταβάλλει τα ιατρικά δεδομένα του ασθενή. **Δεν έχουν προς το παρόν νομοθετική ρύθμιση σε εθνικό όσο και σε ευρωπαϊκό επίπεδο** (61).

5.5 Αρμοδιότητες ασφαλείας του διαχειριστή του τοπικού δικτύου ΠΣ

Για τον διαχειριστή του δικτύου υπάρχουν διάφορες αρμοδιότητες ασφάλειας, που πρέπει να λάβει υπόψιν του. Θα πρέπει να χρησιμοποιεί κατάλληλα εργαλεία για να προστατέψει το ΠΣ για το οποίο είναι υπεύθυνος. Τέτοια είναι τα ακόλουθα.

5.5.1 **Αντιπυρική Ζώνη**

• Η Αντιπυρική Ζώνη, λειτουργεί με βάση κάποια πρότυπα ασφάλειας και πρόκειται για δρομολογητές φιλτραρίσματος πακέτων, που μπορούν να δημιουργούν ένα δίκτυο περιορισμένης πρόσβασης αποκαλούμενο αποστρατικοποιημένη ζώνη (Demilitarized zone-DMZ) και το οποίο παρεμβάλλεται μεταξύ των δύο δικτύων, και φιλτράρουν την κυκλοφορία μεταξύ τους.

“Κάθε διεύθυνση στο Διαδίκτυο έχει και έναν αντίστοιχο αριθμό IP. Το Σύστημα Ονομάτων Χώρου (Domain Name System - DNS) μετατρέπει τα ονόματα των απλών διευθύνσεων που προτιμάνε οι χρήστες, σε αριθμούς (IP διευθύνσεις), έτσι ώστε να μπορεί να τις επεξεργαστεί το δίκτυο. Αυτό γίνεται γιατί οι χρήστες δεν μπορούν να θυμούνται μεγάλους αριθμούς. Ο επιτιθέμενος κατά την εκδήλωση μιας επίθεσης πλαστογραφεί τη διεύθυνση του με σκοπό να φαίνεται ότι είναι ένας νόμιμος χρήστης, δεν μπορεί όμως να πλαστογραφήσει την IP διεύθυνση (τον αριθμό). Συσκευές όπως τα firewalls καθώς και άλλα εργαλεία λογισμικού και on-line δικτυακοί τόποι έχουν τη δυνατότητα να ελέγχουν αν μια διεύθυνση είναι αληθινή ή όχι και ανάλογα να αποτρέπουν ή να απαγορεύουν την πρόσβαση του ενπολλοίς ανυποψίαστου χρήστη.

• **Βασικά εργαλεία του διαχειριστή του δικτύου,** είναι ο έλεγχος της κίνησης (**traffic monitoring**), και η καταγραφή των γεγονότων (**event logging**). Επιπλέον στην αποστρατικοποιημένη ζώνη μπορούν να τοποθετηθούν **συστήματα ανίχνευσης παρείσφρυσης (IDS)** στο δίκτυο.

• Οι δρομολογητές φιλτραρίσματος της αντιπυρικής ζώνης ακολουθούν κάποιους κανόνες από μια **Λίστα ελέγχου Πρόσβασης – Access Control**

List (ACL), και μέσω αυτών αποφασίζουν ποια πακέτα θα αφήσουν να διέλθουν, ενώ εμποδίζουν πακέτα που στην λίστα τους ενημερώνονται ότι δεν πρέπει να διέλθουν. Παρέχουν Ασφάλεια σε επίπεδο δικτύου και μεταφοράς.

- Σε επίπεδο εφαρμογών, π.χ. όπως το ηλεκτρονικό ταχυδρομείο χρειάζονται proxy services - υπηρεσίες πληρεξουσίων που εκτελούνται σε εξυπηρετητές έπαλξης (bastion hosts) αλλιώς γνωστούς σαν **πύλες επιπέδου εφαρμογής (gateways)**. Αυτές βρίσκονται επίσης και στην αποστρατικοποιημένη ζώνη και δεν επιτρέπουν την ελεύθερη πρόσβαση στον κεντρικό Η/Υ.

- Δεν μπορούν όμως να προστατέψουν σε επίπεδο δεδομένων από επιθέσεις π.χ. ιών. Εδώ χρειάζεται πιο συστηματική ανάλυση των μηνυμάτων, όπως γνώση του πως αυτά κατασκευάζονται π.χ. το πρότυπο MIME (Multipurpose Internet Mail Extension), το ZIP κλπ. Οι διαχειριστές δικτύου θα πρέπει να ενημερώνονται συνεχώς και να εφαρμόζουν τις συμβουλές ασφάλειας και τις καινούργιες υπογραφές ιών (virus signatures).

- **Το Firewall** το ίδιο μπορεί να παραβιαστεί γι αυτό πρέπει να υπάρχει **σχέδιο εντοπισμού παραβιάσεων ασφαλείας**. Σε αυτό συντελούν τα **Συστήματα Ανίχνευσης Παρείσφρυσης (Intrusion Detection Systems-IDS)** που τοποθετούνται μέσα στην DMZ. Αυτά μπορούν να χρησιμοποιούν **παγίδες (Honey-pots)** που μοιάζουν με πιθανούς στόχους στους οποίους οι εξουσιοδοτημένοι χρήστες δεν μπαίνουν κανονικά, και άρα αν κάποιος μπει αυτό είναι ένδειξη εισβολής. Ένα μειονέκτημα των Firewall είναι ότι μπορεί να γίνει σημείο συμφόρησης λόγω κατά πρώτον των ολοένα πιο αυξημένων ταχυτήτων των γραμμών επικοινωνίας και κατά δεύτερον των ολοένα πιο απαιτητικών πρωτοκόλλων που πρέπει να ακολουθούν οι κατασκευαστές τους, κάτι που μπορεί να μπλοκάρει τα πακέτα. Τα Firewalls, πρέπεί να έχουν **αυτοματοποιημένα αντίμετρα** για επιθέσεις παραποίησης (spoofing), όπως τα Συστήματα Πρόληψης Παρείσφρυσης (Intrusion Prevention Systems-IPS).

5.5.2 **Συστήματα Ανίχνευσης Παρείσφρυσης (IDS)**

Τα **συστήματα ανίχνευσης παρείσφρυσης Intrusion Detection Systems** (IDS), μέσω των οποίων ανιχνεύονται ακατάλληλες και εσφαλμένες δραστηριότητες διακρίνονται σε αυτά που βρίσκονται σε μια συσκευή του χρήστη, και αυτά που ελέγχουν εσωτερικά το δίκτυο. Επίσης η αντίδραση στην παρείσφρυση μπορεί να είναι ενεργητική ή παθητική. Στην παθητική απλά ανιχνεύουν και έπειτα ενημερώνουν ώστε ο διαχειριστής να προβεί σε κάποια ενέργεια διόρθωσης, ενώ στην ενεργητική μπορούν τα ίδια να εμποδίσουν την πρόσβαση του εισβολέα και την περαιτέρω δραστηριότητα του.

Τα IDS είναι προγράμματα που προσπαθούν να ανιχνεύσουν εισβολές, συγκρίνοντας την όποια παρατηρούμενη συμπεριφορά με αντίστοιχες ύποπτες, κατά προτίμηση σε πραγματικό χρόνο. **Με τον όρο εισβολή περιγράφεται η απόπειρα μη εξουσιοδοτημένης πρόσβασης σε ένα υπολογιστικό σύστημα και η πρόκληση ηθελημένης ή περιστασιακής βλάβης** (86).

Τον γενικό έλεγχο έχει ο διαχειριστής του ΠΣ, στον οποίο ένα καλό IDS, πρέπει να μεταφέρει επαρκή πληροφορία αλλά και να μην ταλαιπωρεί με ασήμαντες πληροφορίες. Συνεπώς χρειάζεται ένα αυτόματο σύστημα να παρεμβαίνει ενδιάμεσα εως τον κεντρικό έλεγχο.

Οι Ahmed Martuza et al. (86), αφού μελέτησαν κάποια IDS ανέφρραν ποιές **ιδιότητες είναι απαραίτητες για ένα ιδανικό IDS**. Αυτές είναι:

- Να είναι ικανό να αντιμετωπίζει πολλαπλές επιθέσεις.
- Να μην καταναλώνει πολύ χρόνο στην ανίχνευση, γιατί όσο πιο πολύ χρόνο καταναλώνει, τόσο περισσότερο χρόνο δίνει στον εισβολέα να πραγματοποιήσει το σκοπό του.
- Να συνδυάζονται καλά τα IDS του χρήστη με τα δικτυακά.
- Να έχει καλή ανάλυση συμπεριφοράς.

- Να μη χρειάζεται να διακόπτει δικτυακές συνδέσεις για να ανιχνεύσει ή εμποδίσει έναν εισβολέα.

- Καλό είναι να χρησιμοποιούνται και ενεργητικά και παθητικά IDS, συνδυαστικά.

- Η επεξεργασία των δεδομένων να μπορεί να γίνει και κεντρικά και κατανεμημένα.

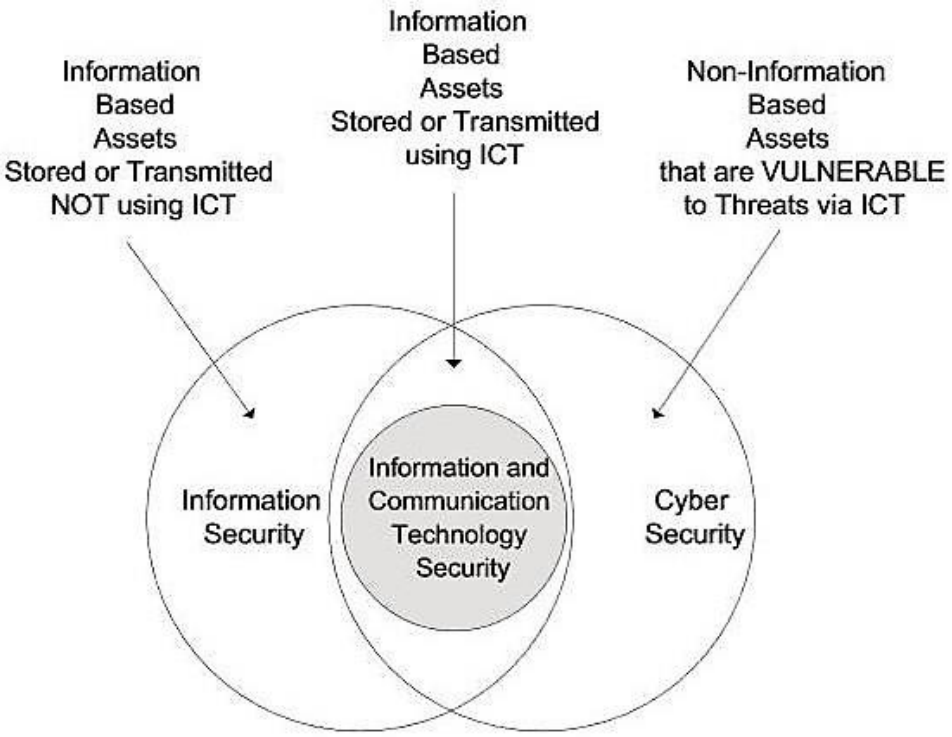
- Να μην σημαίνει άκυρο συναγερμό.

- Να μπορεί να λειτουργεί σε μη έμπιστο δίκτυο.

- Τα επιμέρους στοιχεία του να μην αλληλοεξαρτώνται, ουτως ώστε να μην καταρρέει το σύνολο, όταν ένα μέρος ανεπαρκεί. (86)

Κεφάλαιο 6ο: Ηλεκτρονικό έγκλημα - Κυβερνοασφάλεια

Συχνά συγχέεται η έννοια της κυβερνοασφάλειας με την ασφάλεια ενός ΠΣ. Είναι έννοιες που είναι σχετιζόμενες αλλά δεν είναι ταυτόσημες όπως παρουσιάζεται στο πιο κάτω διάγραμμα. Σύμφωνα με τους Solms και Niekerk υπάρχουν πληροφορίες που δεν αποθηκεύονται ούτε μεταφέρονται με τη χρήση ΤΠΕ, υπάρχουν πληροφορίες που αυτό γίνεται, και τέλος υπάρχουν αγαθά που δεν σχετίζονται με ΤΠΕ και παρόλα αυτά μπορούν να δεχθούν σοβαρή απειλή από τη χρήση ΤΠΕ. Έτσι διαγραμματικά σχηματίζονται δυο τεμνόμενα σύνολα που δεν είναι όμως ταυτόσημα (87).



***Εικόνα 13. Η σχέση μεταξύ κυβερνοασφάλειας, ασφάλειας πληροφοριών και επικοινωνιών, και ασφάλειας μόνο πληροφοριών* (87)**

Τα προβλήματα στην ασφάλεια των ΠΣ, συχνά έχουν το χαρακτήρα του ηλεκτρονικού εγκλήματος.

“Δογματικό ορισμό του εγκλήματος δίνει ο Ποινικός Κώδικας (ΠΚ), στην διάταξη του άρθρου 14, «έγκλημα είναι πράξη άδικος και καταλογιστή εις τον πράξαντα, τιμωρούμενη υπό του νόμου».

Το έγκλημα θίγει τις αξίες της κοινωνικής ζωής όπως αυτή εκλαμβάνεται στις γενικότερης αποδοχής πλευρές της, και η τέλεση του δείχνει έλλειψη σεβασμού του δράστη προς τις αξίες αυτές, καθιστώντας επιτακτική την ποινική καταστολή της πράξης που κρίνεται επιπρόσθετα κοινωνικά απόλυτα αναγκαία (36). Διαχρονικά υπήρχε, υπάρχει και θα υπάρχει έγκλημα, και διαχρονική είναι και η αντιμετώπισή του και η ποινή για την τέλεσή του Υπάρχει ένας αδιάσπαστος κύκλος κανόνες, παράβαση κανόνων, κυρώσεις σε κάθε εγκληματικό φαινόμενο.

Το ηλεκτρονικό έγκλημα είναι μια καινούργια μορφή του παραδοσιακού εγκλήματος. Ηλεκτρονικό έγκλημα σύμφωνα με τους Forester and Morrison (1994), είναι «Μια εγκληματική πράξη στην οποία ο Η/Υ χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της». Σύμφωνα με τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (1986), «Ηλεκτρονικό έγκλημα συνιστά κάθε παράνομη, ανήθικη ή χωρίς έγκριση συμπεριφορά που περιλαμβάνει την αυτόματη επεξεργασία δεδομένων ή/και τη μετάδοση δεδομένων» (38).

Απαραίτητο στοιχείο για την τέλεση του είναι να υπάρχει συσκευή όπως ένας Η/Υ, κινητό τηλέφωνο, τάμπλετ κλπ. Ο ρόλος που διαδραματίζει ο Η/Υ είναι σημαντικός, για τους εξής λόγους:

• Μπορεί να είναι το «θύμα» της επίθεσης.

• Μπορεί να είναι το μέσο για τη διάπραξη κάποιας επίθεσης

• Μπορεί να είναι και μόνο βοηθητικό μέσο για τη διάπραξη του εγκλήματος.

Στη συνέχεια βέβαια με την εμφάνιση του διαδικτύου τα πράγματα έγιναν ακόμα πιο περίπλοκα στο ηλεκτρονικό έγκλημα, και μεγαλύτερη έγινε και η ανάγκη για νομική του αντιμετώπιση. Το διαδικτυακό έγκλημα (cybercrime) αποτελεί μία ειδικότερη μορφή ηλεκτρονικού εγκλήματος, που σχετίζεται με την όποια μορφή κατάχρησης των δυνατοτήτων του διαδικτύου (38).

Η Εξεταστική Επιτροπή της Μεγάλης Βρετανίας, ένα ανεξάρτητο σώμα κατηγοριοποίησε το ηλεκτρονικό έγκλημα σε **επιμέρους κατηγορίες** ως εξής:

Την **απάτη,** όταν κάποιος για προσωπικό όφελος αλλοιώνει τα εισαγόμενα δεδομένα, κάνει καταστροφή / συμπίεση / ακαταλληλότητα εκροών, ή αλλοιώνει τα υπάρχοντα δεδομένα του Η/Υ, αλλοίωνει ή κάνει κακή χρήση των προγραμμάτων.

Την **κλοπή:** των δεδομένων, του λογισμικού, του εξοπλισμού

Την **χρήση παράνομων αντιγράφων λογισμικού.**

Την **μη εγκεκριμένη χρήση δυνατοτήτων των συστημάτων Η/Υ** ενός οργανισμού από κάποιον εργαζόμενο προκειμένου να αποκομίσει κάποιο ίδιον όφελος.

Το **χάκινγκ**: μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα Η/Υ συνήθως από απόσταση.

Το **σαμποτάζ** δηλαδή η εσκεμμένη πρόκληση ζημίας στον εξοπλισμό.

Την **εισαγωγή παράνομου υλικού στο ΠΣ**, πχ. πορνογραφικό

Την **μετάδοση ιών,** δηλαδή την εσκεμμένη έκθεση ενός προγράμματος σε ιούς με σκοπό την ματαίωση κάποιας εφαρμογής (88).

Τα συνηθέστερα κίνητρα για την διάπραξη ενός κυβερνοεγκλήματος-cybercrime είναι : α) η διασκέδαση β) το χρηματικό όφελος γ) ο θυμός, εκδίκηση και άλλου τύπου συναισθήματα, δ) τα πολιτικά κίνητρα, ε) τα σεξουαλικά κίνητρα, στ) οι σοβαρές ψυχικές ασθένειες. Πρόσφατη ήταν και η περίπτωση που πήρε δημοσιότητα υποκλοπής στοιχείων και εξετάσεων άλλων ασθενών που στη συνέχεια χρησιμοποιήθηκαν από έγκλειστο για να «αποδείξει ποσοστό αναπηρίας» στα δικαστήρια τέτοιου βαθμού ικανό ώστε να τον αποφυλακίσει.

Οι επιτιθέμενοι στο ΠΣ μπορεί να είναι: - Εσωτερικοί και εξωτερικοί συνεργάτες - Ανταγωνιστές - Εγκληματικές οργανώσεις - Δυσαρεστημένοι υπάλληλοι, πελάτες, πολιτικοί ακτιβιστές - Κρατικοί ή «παρακρατικοί» φορείς

– Άλλοι πάλι μπορεί να προκαλούν βλάβες και μέσα από τυχαία γεγονότα και ακούσιες ενέργειες (38).

Οι επιπτώσεις της παραβίασης ΔΠΧ, μπορεί να είναι ποικίλες από την κακή προστασία των προσωπικών στοιχείων υγείας και την διαρροή τους. Σύμφωνα με τον ΟΟΣΑ είναι :

- Οικονομικές μέσω διακρίσεων στην ασφάλεια υγείας ή στην αγορά εργασίας.

- Ψυχοκοινωνικές επιπτώσεις όπως ντροπή, στίγμα, δυσφήμιση που οδηγούν σε απομόνωση και στρές.

- Επίσης μπορεί να οδηγήσουν σε κλοπή ταυτότητας.

- Γενικότερα μπορεί να οδηγήσει σε απώλεια εμπιστοσύνης των πολιτών στην κυβέρνηση, και τους οργανισμούς της όπως το σύστημα υγείας (42).

7.1 Ιδιατερότητες των διαδικτυακών εγκλημάτων στον κυβερνοχώρο

Συνοπτικά **τα βασικότερα χαρακτηριστικά του, είναι:**

1. Το διαδικτυακό έγκλημα γίνεται σε χρόνο ελάχιστων δευτερολέπτων, τόσο γρήγορα που πολλές φορές δεν γίνεται αντιληπτό ούτε από το ίδιο το θύμα. Ο δράστης συνδέεται στο διαδίκτυο, επιτίθεται και μπορεί να προσβάλλει τα υπολογιστικά συστήματα μιας επιχείρησης ή ενός οργανισμού από οπουδήποτε στον πλανήτη. Δεν απαιτείται φυσική παρουσία του δράστη στον τόπο τέλεσης του εγκλήματος καθώς με το πάτημα μερικών κουμπιών στο πληκτρολόγιο ενός Η/Υ μπορεί να επιτελέσει έγκλημα ακόμα και από το σπίτι ή το αυτοκίνητο του.

2. Οι βλάβες, φθορές καθώς και αλλοιώσεις που προκαλούνται σε αντικείμενα όπως σκληρούς δίσκους, μνήμες κλπ, δεν είναι παρά δευτερεύουσες συνέπειες της κύριας βλάβης που αφορά τα δεδομένα και την πληροφορία που περιέχουν τα ηλεκτρονικά δεδομένα.

3. Μεσα στο ίδιο το διαδίκτυο διατίθονται ελεύθερα εφαρμογές λογισμικού με τις οποίες οι χάκερς μπορούν να εισβάλλουν σε δίκτυα και υπολογιστικά συστήματα και να πραγματοποιήσουν ηλεκτρονικές επιθέσεις.

4. Για τη διερεύνηση του ηλεκτρονικού εγκλήματος συχνά απαιτείται συνεργασία από δύο ή περισσότερα κράτη (του κράτους στο οποίο γίνεται αντιληπτή η διάπραξη του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία). Υπάρχει δηλαδή διασυνοριακός χαρακτήρας του ηλεκτρονικού εγκλήματος και διαφορετική συχνά αξιολόγηση της σημασίας του, αφού αυτό μπορεί να είναι νόμιμο στο κράτος που βρίσκεται ο δράστης ή όπου υπάρχουν αποθηκευμένα τα δεδομένα, και να είναι παράνομο στο κράτος που τα δεδομένα λαμβάνονται ή βρίσκεται ο αποδέκτης τους.

5. Για τη διερεύνηση του δεν επαρκούν οι παλαιότεροι τρόποι αντιμετώπισης εγκλημάτων, αλλά απαιτούνται εξειδικευμένες γνώσεις σε θέματα πληροφορικής τεχνολογίας και διαδικτύου, καθώς και συνεχή εκπαίδευση όποιων είναι αρμόδιοι για τη δίωξή του (αστυνομία και δικαστικές αρχές).

6. Είναι δύσκολο να προσδιοριστεί :

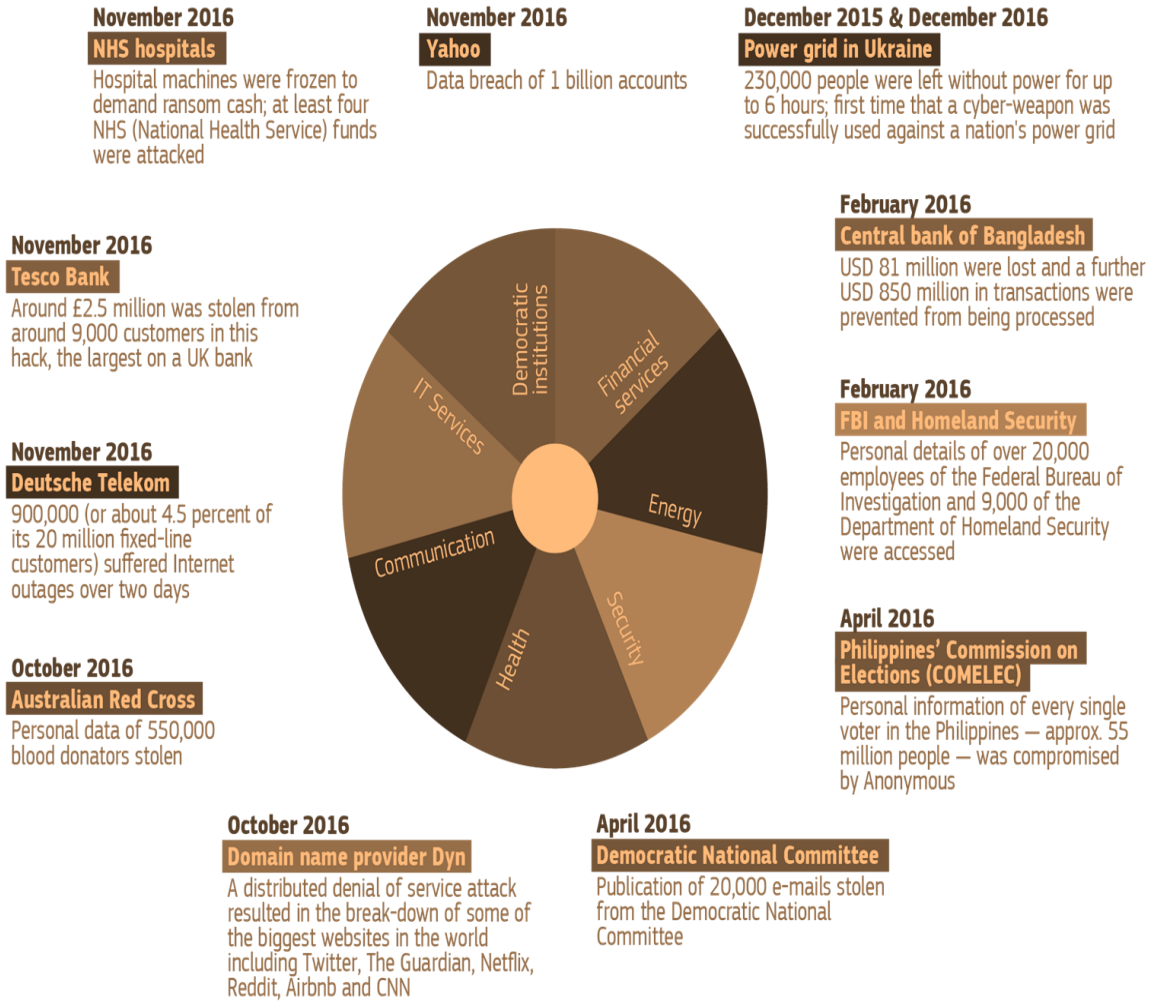
α) ο τόπος τέλεσης του εγκλήματος και αυτό γιατί με τη χρήση ενός μόνο δικτυωμένου Η/Υ ο εγκληματίας μπορεί να το διαπράξει από οποιοδήποτε σημείο του κόσμου και

β) ο ακριβής χρόνος τέλεσης του εγκλήματος και αυτό γιατί τα θύματα κατά κανόνα αντιλαμβάνονται την επίθεση και τη ζημιά που προκλήθηκε πολύ αργότερα από το χρόνο που πραγματοποιήθηκε η επίθεση.

7. Ως έναν από τους κύριους λόγους που είναι δύσκολο να εκτιμηθεί το κόστος των κυβερνοεπιθέσεων είναι ότι πολλές εταιρείες είναι διστακτικές στο να δώσουν πληροφορίες σχετικά με τα προβλήματα που έχουν αντιμετωπίσει και τις ζημιές που έχουν υποστεί, φοβούμενες να μη διαταραχτεί η φήμη τους, ιδιαίτερα εάν φημίζονται για την προστασία που παρέχουν σε ευαίσθητα δεδομένα. Σε αυτό θα επιφέρουν αλλαγές ο ΓΚΠΔ και το NIS που θα

ακολουθήσει και θα τις υποχρεώνουν να προβαίνουν σε σχετικές ενημερώσεις (38).

Το **EPSC-European Political Strategy Centre** στην πιο κάτω εικόνα παρουσιάζει μια μικρή επιλογή των επιθέσεων που έλαβαν χώρα το 2016.



***Εικόνα 14. Τύποι κυβερνοεπιθέσεων που έλαβαν χώρα το 2016* (40)**

7.1.1 **Διαδεδομένα Ηλεκτρονικά Εγκλήματα – Κίνητρα**

Τα κυριότερα και πιο διαδεδομένα εγκλήματα που περιλαμβάνονται σε αυτήν την κατηγορία είναι : • Κακόβουλες εισβολές σε δίκτυα (hacking, cracking) •SQL injections •Ανεπιθύμητη αλληλογραφία (spamming) • Ηλεκτρονικό «Ψάρεμα» (phishing - pharming) • Διασπορά κακόβουλου λογισμικού (ιοί - viruses, σκουλήκια - worms, δούρειοι ίπποι - Trojan horses) • Πειρατεία ονομάτων χώρου (domain names piracy) • Απάτη με τη Νιγηριανή

Επιστολή (Nigerian scam) • Επιθέσεις Άρνησης Εξυπηρέτησης (Do's, Denial of Service) (38).

7.1.2 **Κακόβουλες εισβολές σε δίκτυα**

Οι εισβολές γίνονται μετά από επιθέσεις. Χρησιμοποιούν τεχνικές για να προσβάλλουν εφαρμογές ΤΠΕ που μπορεί να παρουσιάζουν ευπάθειες. Οι επιτιθέμενοι επιδιώκουν να αποκτήσουν παράνομα πρόσβαση σε εξυπηρετητές και Βάσεις δεδομένων. Τις πιο συστηματικές επιθέσεις τις εξαπολύουν συνήθως οι λεγόμενοι χάκερς.

Σύμφωνα με τη Cisco στο χώρο της υγείας η εισβολή κάποιου κακόβουλου σε ένα ΠΣΥ, ή στους ηλεκτρονικούς ιατρικούς φακέλους ασθενών, μπορεί να έχει ανυπολόγιστες συνέπειες για την ίδια τους την ζωή ακόμα. Εάν για παράδειγμα αλλάξουν την ομάδα αίματος κάποιου ασθενή ή το ιστορικό αλλεργιών του, ή τις θεραπείες του, ή τα αποτελέσματα των εξετάσεων του. Οι απειλές αυτές είναι πολύ πιο σοβαρές από μια παρείσφρυση π.χ. σε δίκτυο τράπεζας, όπου αν κλαπούν π.χ. χρήματα μπορεί στη συνέχεια να αποζημιωθούν ή να ανευρεθούν. Εδώ το δυσμενές αποτέλεσμα δυστυχώς μπορεί να είναι ανεπανόρθωτο (89).

Όταν αποκτήσουν παρανόμα δεδομένα από ιατρικούς φακέλους, οι κυβερνο-εγκληματίες μπορούν να τα επιμεροποιήσουν, για να τα εμπορευτούν σε τμήματα στη συνέχεια με ακόμα μεγαλύτερο κέρδος. Μπορούν να πουλήσουν π.χ. τα στοιχεία ταυτότητας του θύματος σε άλλους κακόβουλους, την ασφαλιστική κάλυψη (πουλώντας την σε άτομα που δεν έχουν), τα στοιχεία των τραπεζικών λογαριασμών (και να τους αδειάσουν), άλλα στοιχεία πάλι να δοθούν για εκβιασμό ή παράνομη δημοσίευση. Άλλοι πάλι μπορεί να αποσκοπούν να αποκτήσουν πλαστό πιστοποιητικό αναπηρίας ή πρόβλημα υγείας, προκειμένου να τυγχάνουν οικονομικών ή άλλων προνομίων.

Με αυτόν τον παράνομο τρόπο μπορεί κάποιοι να επιδιώξουν να γίνουν πλούσιοι. Το κόστος της ζημιάς για τους παρόχους υγείας, προμηθευτές, χρήστες, την κοινωνία ακόμα γενικότερα μπορεί να είναι ανυπολόγιστο. Επίσης εξίσου σημαντικά θα είναι και τα πρόστιμα που θα επιβληθούν στους υπευθύνους των ΠΣΥ, στη συνέχεια από τις αρμόδιες επιτροπές τόσο μεγάλα

που μπορεί να βγάλουν παρόχους αλλά και ολόκληρους υγειονομικούς οργανισμούς εκτός λειτουργίας εάν δεν έχουν σπαταλήσει τεράστια ποσά σε σχετικές ασφαλιστικές εισφορές που να μπορούν να τους καλύψουν. Και μπορεί να υπάρχουν και γενικότερες συνέπειες για τα συστήματα υγείας ενός τόπου ή μιας χώρας με το κλείσιμο υπηρεσιών. Αρκεί να φανταστεί κανείς ότι μπορεί να χρειαστεί να ταξιδέψει 300 χιλιόμετρα σε μια έκτακτη ανάγκη π.χ. γιατί όλες οι πλησιέστερες υγειονομικές μονάδες έκλεισαν λόγω των συνεπειών της παραβίασης των δεδομένων και των ΠΣ τους (89).

Οι συνηθέστερες κακόβουλες εισβολές γίνονται με τους ακόλουθους τρόπους:

Το Cracking αποτελεί την παράνομη πρόσβαση σε ξένα υπολογιστικά συστήματα, η αλλαγή των σχετικών κωδικών πρόσβασης σε προγραμμάτα και η προσπάθεια να καταστήσουν δυνατή την παράνομη αντιγραφή αυτών. Βασικός σκοπός είναι η κλοπή πληροφοριών και η πρόκληση οικονομικής ή άλλου είδους ζημιάς (38)**.**

Το **Hacking,** είναι μη εξουσιοδοτημένη πρόσβαση, και η χωρίς δικαίωμα διείσδυση σε συστήματα Η/Υ, σκοπός της οποίας μπορεί να είναι η δολιοφθορά, η καταστροφή ή η αποκόμιση οικονομικού οφέλους, αλλά και άλλοι λόγοι όπως η ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας και η επιβεβαίωση της ικανότητας να εισβάλουν σε ένα υπολογιστικό σύστημα. Η έννοια του hacking μπορεί να αφορά από καλόπιστες ενέργειες μέχρι μια σειρά από παράνομες και εγκληματικές δράσεις που απαιτούν διάφορες τεχνολογικές ικανότητες.

Η εισβολή σε κάποιο δίκτυο απρόκλητα, ακόμα και αν δεν είναι κακόβουλη, ενέχει κακόβουλο χαρακτήρα. Αυτό γιατί ο επιτιθέμενος ή αλλιώς hacker, εισχωρώντας στο σύστημα αποκτά γνώσεις για την ασφάλεια του ΠΣ, εντοπίζει πιθανά αδύνατα σημεία του και έτσι αργότερα αν θέλει μπορεί να διαπράξει κακόβουλη επίθεση ή ακόμα και να διαθέσει τις πληροφορίες που έχει συγκεντρώσει σε κάποιον τρίτο που θα προχωρήσει στην επίθεση. Συνοπτικά ως χάκερ (hacker) μπορεί να ορισθεί το άτομο εκείνο το οποίο χωρίς δικαίωμα αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε Η/Υ, ή

σε περιφερειακή μνήμη Η/Υ, ή μεταδίδονται με συστήματα τηλεπικοινωνιών (38). Γενικότερα υπάρχουν **τρεις τύποι χάκερ.**

7.1.3 **Κατηγορίες hacker**

1. Οι White hat-hackers: Στόχος τους είναι να καταπολεμούν το ηλεκτρονικό έγκλημα και δρούν ενάντια στους black hat. Μπορεί να είναι κάποιοι ειδικοί ασφαλείας ή διαχειριστές συστημάτων. Η ηλικία τους κυμαίνεται από 25 έως και 40 έτη.

2. Οι Black hat- hackers: Είναι αυτοί που εμπλέκονται στο ηλεκτρονικό έγκλημα. Χρησιμοποιούν τις γνώσεις τους σε οργανωμένες ομάδες φτιάχνουν κακόβουλα προγράμματα, όπως ηλεκτρονικούς ιούς και κατασκοπευτικά προγράμματα. Διεισδύουν σε δίκτυα και τα κατασκοπεύουν, σπάνε κωδικούς από ιστοσελίδες και τις καταστρέφουν. Το κίνητρο τους είναι χρηματικό τις περισσοτέρες φορές και όχι ιδεολογικό.

3. Οι Grey hat-hackers που παραβιάζουν τον νόμο χωρίς κακόβουλους στόχους. Κίνητρο τους είναι η μάθηση και ο πειραματισμός με τα ηλεκτρονικά συστήματα. Είναι ως επί το πλείστο μικρής ηλικίας ξεκινούν στην εφηβεία συνήθως, και φτάνουν στο αποκορύφωμα των γνώσεων τους ως φοιτητές. Οι ίδιοι τον εαυτό τους δεν τον θεωρούν εγκληματία και ας παραβιάζουν νόμους γιατί θεωρούν ότι δεν καταστρέφουν ούτε δημιουργούν ζημία στα ΠΣ που εισβάλουν. Πιστεύουν ότι είναι ερευνητές της τεχνολογίας και σε κάποιες περιπτώσεις ενημέρωνουν ακόμα και το κοινό ή τους διαχειριστές συστημάτων για τυχόν προβλήματα ασφάλειας (38).

7.1.4 **Ανεπιθύμητη αλληλογραφία (spamming)**

Η ανεπιθύμητη αλληλογραφία ή spamming είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων ηλεκτρονικού ταχυδρομείου που απευθύνονται σε ένα σύνολο παραληπτών του διαδικτύου χωρίς όμως οι παραλήπτες να έχουν επιδιώξει συνειδητά την αλληλογραφία με τον αποστολέα. Συνήθως αναφέρεται περισσότερο στην αποστολή μεγάλων ποσοτήτων μηνυμάτων

διαφημιστικού ή ενημερωτικού περιεχομένου. Ο παραλήπτης για να προστατευτεί θα πρέπει να μη δίνει χωρίς σημαντικό λόγο τη διεύθυνση του email του, να μην απαντάει στα σπαμ, να τα διαγράφει χωρίς να τα ανοίγει και να αναφέρει τα σπαμ που δέχεται ως τέτοια προκειμένου να ενημερωθεί ο πάροχος.

7.1.5 **Ηλεκτρονικό «Ψάρεμα», και άλλες εγκληματικές διαδικτυακές συμπεριφορές**

Το **phishing**: προέρχεται από το συνδυασμό των λέξεων password και fishing και είναι η διαδικασία παραπλάνησης και εξαπάτησης ενός ατόμου (ή μιας ομάδας ατόμων), με σκοπό την απόσπαση προσωπικών στοιχείων. Συνήθως τα στοιχεία αυτά έχουν χαρακτήρα οικονομικό και αφορούν κωδικούς πρόσβασης, τραπεζικούς λογαριασμούς (e-banking), πιστωτικές κάρτες κτλ. Συχνά είναι τα φαινόμενα της παραβίασης προσωπικών δεδομένων και της εξαπάτησης κατά τη διενέργεια διαδικτυακών συναλλαγών. Μπορεί να οδηγήσει σε κλοπή ταυτότητας (identity theft), όπου επιτήδειοι κλέβουν προσωπικές πληροφορίες και τις χρησιμοποιούν παράνομα παριστάνοντας το άτομό που υποκλέψανε. Συχνά αυτή η διαδικασία γίνεται μέσω του phishing και του pharming.

Στο **Phishing** ο απατεώνας που στέλνει τα μηνυμάτα επιχειρεί να αποσπάσει από το θύμα του προσωπικά οικονομικά δεδομένα, όπως τα στοιχεία πιστωτικής κάρτας, τραπεζικού λογαριασμού. Το υποψήφιο θύμα π.χ. μπορεί να λάβει ένα email, αποστολέας του οποίου φαίνεται να είναι η «κανονική» του τράπεζα που του ζητάει να επιβεβαιώσει το username και το password του λογαριασμού του που διατηρεί μέσω web, με κάποια πρόφαση ότι υπάρχουν κάποια προβλήματα σε Η/Υ της τράπεζας ή σε υποψίες ότι ο συγκεκριμένος λογαριασμός έχει ήδη παραβιαστεί και αν δεν γίνει η «επιβεβαίωση» θα κλειδωθεί. Το email αυτό συνοδεύεται από σύνδεσμο προς τον δικτυακό τόπο της «τράπεζας», οποίος όμως δεν είναι πραγματικός και έτσι το θύμα στέλνει τα στοιχεία που του έχουν ζητηθεί στον απατεώνα. Το **Vishing** είναι παραλλαγή του ηλεκτρονικού ψαρέματος (phishing) σε αυτούς που χρησιμοποιούν το τηλέφωνο ή το VoIP (Voice over IP tools). Ο χρήστης λαμβάνει e-mail ή SMS με το οποίο του ζητείται να καλέσει έναν αριθμό χωρίς

χρέωση με στόχο να επιβεβαιώσει τα στοιχεία του. Μπορεί ακόμα να λάβει ένα τηλέφωνο με μαγνητοφωνημένο μήνυμα που να του ζητά να εισάγει τα προσωπικά του στοιχεία. Το **spear phishing** είναι στοχευμένα μηνύματα απατεώνων που μοιάζουν αυθεντικά και στα οποία ζητούνται προσωπικά δεδομένα, όπως όνομα χρήστη και κωδικοί πρόσβασης

Το **Pharming** αφορά την εκμετάλλευση μιας ευπάθειας στην υπηρεσία DNS (Domain Name System) που επιτρέπει σε έναν hacker να ανακατευθύνει την κυκλοφορία αυτού του δικτυακού τόπου σε άλλο δικτυακό τόπο. Εκτρέπουν τη ροή των επισκεπτών σε άλλο ιστότοπο όπου τα όποια στοιχεία συναλλαγών που καταχωρούνται, κατόπιν χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών. Το pharming είναι μια μορφή απάτης - ηλεκτρονικής διεύθυνσης, που έχει ως αποτέλεσμα να πιστεύουν οι χρήστες ότι βρίσκονται σε μια γνήσια ιστοσελίδα με το σωστό URL.

Η διαφορά με το phising είναι ότι δεν επιζητούν να πείσουν το θύμα, αλλά χρησιμοποιούν κακόβουλα προγράμματα που επαναδρομολογούν την κυκλοφορία των δεδομένων. Με παρεμβάσεις στο λογισμικό του υπολογιστή του θύματος ή και σε άλλους υπολογιστές, το θύμα που θέλει να επισκεφθεί μια ιστοσελίδα και να πραγματοποιήσει κάποια συναλλαγή κατευθύνεται σε άλλη σελίδα - αντίγραφο της γνήσιας με την οποία θέλει να συνδεθεί. Έτσι όταν μετά καταχωρεί τα στοιχεία του νομίζοντας ότι βρίσκεται στην γνήσια ιστοσελίδα στην πραγματικότητα τα «παραδίδει» στην ιστοσελίδα του δράστη. Σε άλλες περιπτώσεις, οι δράστες μπορεί να κάνουν το pharming αποστέλλοντας μέσω e-mail κρυμμένα προγράμματα, τα οποία μετά την εγκατάστασή τους στον Η/Υ του θύματος, συλλέγουν και αποστέλλουν τα στοιχεία (PIN, κωδικούς κ.λπ.) τα οποία τους ενδιαφέρουν στους απατεώνες. Κατόπιν οι τελευταίοι τα χρησιμοποιούν προκαλώντας περιουσιακή ζημιά στο θύμα (38).

Οι **SQL injections**: όπου χρησιμοποιώντας κατάλληλες εντολές sql αποκτά κάποιος παράνομα πρόσβαση σε μια βάση δεδομένων (ΒΔ) ενός ΠΣ, που δεν είναι κατάλληλα προστατευμένη από τέτοιου τύπου επιθέσεις (π.χ. κάνοντας όλα τα μυνήματα λάθους να είναι εσωτερικά), και αποκτά παράνομα τα δεδομένα όσων είναι καταχωρημένοι στη Β.Δ.

Το **Cyberbulling**: έχει σκοπό την παρενόχληση ή τον εκφοβισμό και την εκμετάλλευση του θύματος. Μπορεί να λάβουν χώρα με μυνήματα, me διάδοση φημών, μαγνητοσκοπήσεων και με ανάρτηση ή απειλή ανάρτησης σε μέσα κοινωνικής δικτύωσης, blogs, forums, ιστοσελίδες κλπ. Η ηλεκτρονική παρενόχληση (cyberbullying) είναι επιθετική συμπεριφορά από πρόθεση με τη χρήση ηλεκτρονικών μέσων. Περιστατικά παρενόχλησης μεταξύ παιδιών και εφήβων μπορούν να συμβούν με πολύ διαφορετικές μορφές. Όχι μόνο μέσω καυγάδων και επιθετικότητας, αλλά και μέσω διαφορετικών τύπων εκφοβισμού που αφήνουν το θύμα εκτεθειμένο.

Οι συμπεριφορές που μπορεί να παρατηρηθούν, περιλαμβάνουν αποστολή κειμένων, e-mail ή άμεσων μηνυμάτων με κακό περιεχόμενο, την ανάρτηση προσβλητικών/εξευτελιστικών φωτογραφιών, βίντεο και άλλου υλικού - σε ιστοσελίδες, blogs, ιστοσελίδες κοινωνικής δικτύωσης καθώς και τη χρήση του ονόματος άλλου χρήστη με σκοπό τη διάδοση φημών στο περιβάλλον του θύματος μέσω της χρήσης κινητού, ηλεκτρονικού ταχυδρομείου ή άλλου ηλεκτρονικού μέσου.

Οι μορφές του μπορεί να περιλαμβάνουν: την αποστολή υβριστικών μηνυμάτων (flaming), την παρενόχληση (harassment), τη δυσφήμηση (denigration), την αντιποίηση προσώπου (impersonation) όπου ο δράστης κάνει αναρτήσεις χρησιμοποιώντας τον κωδικό πρόσβασης του θύματος, την καταδίωξη στο διαδίκτυο (cyberstalking) όπου διεξάγεται επαναλαμβανόμενη παρενόχληση και απειλητική επικοινωνία, το χαρούμενο χαστούκισμα («happy slapping») όπου μαγνητοσκοπούν το θύμα και στη συνέχεια αναρτούν ένα σκοπίμως προκαλούμενο βίαιο και εξευτελιστικό γεγονός, καθώς και η έξοδος και απάτη (outing and trickery) όπου αφορά εξαπάτηση για να αποκαλυφθούν προσωπικές πληροφορίες του θύματος οι οποίες στη συνέχεια θα δημοσιευθούν από το δράστη σε τρίτα άτομα (90).

Το **Doxing,** που έχει σχέση με τα μέσα κοινωνικής δικτύωσης (social enginering), όπου οι επιτιθέμενοι παίρνουν επιλεκτικά στοιχεία από αυτά που αναρτούν τα άτομα-στόχοι τους, τα μορφοποιούν, έτσι ώστε να τους παρουσιάζουν με άσχημο τρόπο ώστε να μπορούν έπειτα να τα εκβιάσουν.

Απάτη με τη **Νιγηριανή Επιστολή.** Γίνεται με e-mail με ψευτικές ιστορίες μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν μεγάλα χρηματικά ποσά από ανυποψίαστους χρήστες, δελεάζοντας τους με τεράστια κέρδη. Ο απατεώνας μπορεί να συσταθεί ως ένα σημαντικό πρόσωπο του καθεστώτος της Νιγηρίας. Επικαλείται κυρίως λόγους πολιτικής φύσεως, και ζητάει τη βοήθεια του θύματος-παραλήπτη της επιστολής, προκειμένου να βγάλει εκτός χώρας (Νιγηρίας) κάποιο τεράστιο χρηματικό ποσό.

Το ανυποψίαστο θύμα καλείται να διευκολύνει το δράστη λειτουργώντας ως αποδέκτης του ποσού, έτσι ώστε να γίνει δεκτή από την κυβέρνηση η διοχέτευση των χρημάτων εκτός Νιγηρίας. Για τη βοήθεια που θα προσφέρει θα ανταμειφθεί με ένα σημαντικό χρηματικό ποσό. Όταν το σύνολο του ποσού θα έχει μεταφερθεί στον τραπεζικό λογαριασμό του υποψήφιου θύματος τότε υποτίθεται ότι έναντι μιας υψηλής προμήθειας θα πρέπει να το παραδώσει στον αποστολέα του e-mail. Αρχικά αυτό που ζητείται είναι η συγκατάθεση του παραλήπτη του e-mail και η παροχή πληροφοριών σχετικών με τους τραπεζικούς λογαριασμούς του, και άλλων στοιχείων που θα βοηθούσαν στην πραγματοποίηση της συναλλαγής. Έπειτα από τη στιγμή που κάποιος αποφασίζει να απαντήσει στην αρχική προσφορά και να την αποδεχτεί, ξεκινάει μια διαδικασία ανταλλαγής επιστολών και υπογραφή κάποιου συμφωνητικού μέσω fax ή ταχυδρομείου. Το θύμα έχει αρχίσει να πιστεύει ότι βρίσκεται πολύ κοντά στην απόκτηση του χρηματικού ποσού. Στην πορεία και μετά την αποστολή των χρημάτων από την πλευρά του θύματος, θα χαθεί η επικοινωνία με το δράστη. Υπάρχει επίσης και η περίπτωση που ο δράστης γνωρίζοντας τα στοιχεία της ταυτότητας του θύματος να χρεώνει τον τραπεζικό του λογαριασμό με υπέρογκα ποσά. Τα Νιγηριανά e-mail είναι γνωστά και ως «419», από το άρθρο του Νιγηριανού Ποινικού Κώδικα που παραβιάζουν (38) .

7.1.6 **Πειρατεία ονομάτων χώρου (domain names piracy) και άλλες διαδικτυακές απάτες**

Domain names piracy. Βασική προϋπόθεση για επικοινωνία στο διαδίκτυο μέσω ΠΣ π.χ. για τον προγραμματισμό ενός ραντεβού αποτελεί η δημιουργία ενός τόπου στο διαδίκτυο όπου θα καθίσταται δυνατή η πρόσβαση πελατών και η κατάρτιση των συναλλαγών. Μέσο (εισιτήριο) για την είσοδο στο χώρο αποτελεί το «domain name» (όνομα τομέα ή όνομα χώρου), το οποίο κατ' ουσίαν επιτελεί ρόλο ηλεκτρονικής διευθύνσεως ή «κυβερνοδιευθύνσεως», επιτρέποντας την επικοινωνία του χρήστη του διαδικτύου με τον κάτοχο της ηλεκτρονικής διευθύνσεως. Το «domain name» αποτελείται από σειρά αλφαριθμητικών χαρακτήρων (τουλάχιστον τριών και όχι περισσότερων των είκοσι τεσσάρων), χωρίς ή με λογικό ειρμό, σε μια ή περισσότερες λέξεις που χωρίζονται από διάφορα σημεία, διαιρείται δε σε τρία μέρη. Το ένα δηλώνει το πρωτόκολλο επικοινωνίας π.χ. το HTTP, το δεύτερο το κατ'εξοχήν όνομα (π.χ. του φορέα υγείας), το τρίτο ή top-level domain δηλώνει την τοποθεσία, την δραστηριότητα (π.χ. δημόσιος οργανισμός- .gov, εκπαίδευση- .edu, την τοποθεσία- .gr) κλπ (38).

Ο επιτιθέμενος μπορεί να επιχειρήσει πάλι να ξεγελάσει τον χρήστη και να παρουσιάσει κάποια υπηρεσία ως γνήσια, εκείνη την οποία αναζητά ο χρήστης στο διαδίκτυο, ενώ στην πραγματικότητα θα πρόκειται για άλλη ίσως σχετική υπηρεσία.

Ξέπλυμα χρήματος.

Ο όρος **«ξέπλυμα χρήματος»** περιγράφει πως κέρδη κακοποιών (βρώμικο χρήμα) υπόκεινται σε μία σειρά διαδικασιών προκειμένου να καλύψουν τις παράνομες προελεύσεις τους και να τα κάνουν να εμφανίζονται σαν να προέρχονται από νόμιμες πηγές (καθαρό χρήμα). Γίνεται με τρία βασικά βήματα:

1. Τοποθέτηση : Ο δράστης τοποθετεί τα παράνομα χρήματα ως επένδυση στο γενικότερο οικονομικό σύστημα, όπως π.χ. σε τράπεζα με κατάθεση σε λογαριασμό, χρηματιστήριο με αγορά μετοχών εισηγμένων σε αυτό, ανταλλακτήριο συναλλάγματος, καζίνο κ.α.

2. Στρωματοποίηση: με μια σειρά συναλλαγών απομακρύνει τα ίχνη των κεφαλαίων από την αρχική τους προέλευση και έτσι μεταμφιέζει τις αληθινές πηγές κεφαλαίων, εμποδίζοντας τον εντοπισμό των παράνομων πηγών από τα ελεγκτικά όργανα.

3. Ενσωμάτωση: Ο δράστης στο τέλος επενδύει τα κεφάλαια σε κλάδους νόμιμης οικονομικής δραστηριότητας π.χ. σε αγορά ακινήτων, επιχειρηματικές και εμπορικές δραστηριότητες κλπ, έτσι ώστε να επανεμφανιστούν στο χρηματοοικονομικό σύστημα ως καθόλα νόμιμα κεφάλαια. Το διαδίκτυο έχει πλεονεκτήματα για τους δράστες καθώς δεν υπάρχει προσωπική επαφή μεταξύ των συναλλασσόμενων, κάτι που κάνει τους δράστες να νιώθουν μεγαλύτερη ασφάλεια και κρυμμένοι πίσω από την ανωνυμία τους να νομιμοποιούν έσοδα παράνομων δραστηριοτήτων.

Η πειρατεία λογισμικού (software) αναφέρεται στην αναπαραγωγή ή/και διάθεση προγραμμάτων Η/Υ που προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων χωρίς να υπάρχει σχετική γραπτή συναίνεση από τον δημιουργό τους. Οι κυριότερες μορφές της είναι οι εξής:

1. Η χρήση ενός προγράμματος από περισσότερους Η/Υ, από όσους προβλέπει η άδεια χρήσης: Είναι η πιο συνηθισμένη μορφή παράνομης χρήσης. Εκδηλώνεται ως εξής:

α. Με την αντιγραφή του προγράμματος χωρίς την απατούμενη άδεια χρήσης από ιδιώτες ή εταιρίες.

β. Με την δήλωση μικρότερου από τον πραγματικό αριθμό εγκαταστάσεων σε μια εταιρεία που διαθέτει μεν άδειες αλλά για έναν συγκεκριμένο πιο μικρό αριθμό χρηστών και Η/Υ.

γ. Με τον δανεισμό προϊόντων λογισμικού μεταξύ φίλων και συνεργατών.

δ. Με την διανομή αντιγράφων λογισμικού από τους πωλητές Η/Υ στους πελάτες τους. Οι τελευταίοι θέλουν να κάνουν την αγορά ενός Η/Υ πιο ελκυστική και προσφέρουν προγράμματα χωρίς τις άδειες χρήσης. Για αυτό χρειάζεται έλεγχος των αδειών από τους πελάτες κατά την αγορά Η/Υ που

διαθέτουν προεγκατεστημένα προγράμματα. Το λογισμικό αυτό συνήθως δεν συνοδεύεται από οδηγίες χρήσης ή βοηθητικές δισκέτες για τα προγράμματα (38).

7.1.7 **Διασπορά κακόβουλου λογισμικού (ιοί - viruses, σκουλήκια - worms, δούρειοι ίπποι - trojan horses)**

Εργαλεία των χάκερ είναι τα malware. Η λέξη «malware» είναι σύνθεση των λέξεων malicious και software. Περιγράφει προγράμματα που έχουν στόχο να παραβιάσουν την ασφάλεια των προσωπικών Η/Υ, και να προκαλέσουν ζημιά ή να υποκλέψουν προσωπικά στοιχεία. Τα πιο γνωστά είναι οι ηλεκτρονικοί ιοί (viruses), τα ηλεκτρονικά σκουλήκια (worms) και οι δούρειοι ίπποι (Trojan horses) . Ως κακόβουλο λογισμικό (malware) επίσης θεωρείται κάποιος προγραμματιστικός κώδικας που προστίθεται, αλλάζει ή αφαιρείται από κάποιο λογισμικό με την πρόθεση να προκληθεί ζημιά ή να μεταστρέψει την προβλεπόμενη λειτουργία ενός ΠΣ. Μπορεί να προκαλέσουν απώλεια πληροφορίας, χρημάτων, ακόμα και ζωής και αποτελούν τεράστια απειλή για την τεχνολογία και την εξέλιξή της. Η ταξινόμηση των διαφόρων malware γίνεται με βάση τα χαρακτηριστικά εκτέλεσης του κακόβουλου προγράμματος, την ισχύ τους, και τον τρόπο που εξαπλώνονται και προσβάλουν.

Πίνακας 4. Μερικά από τα πιο καταστρεπτικά malware της τελευταίας δεκαετίας (91)

Year	Malware Name	Details
2007	Storm	Infected about 10 million computers in 9 months
	Zeus	Suspected to have infected over 3.6 million computers in US alone by end of 2009. Was later used to distribute CryptoLocker ransomware and became the malware writing kit for malware seen in the later years like GameOver Zeus, Spyeye.
2008	Koobface	Targeted Myspace and Facebook users
	Conficker	Infected over 15 million Windows systems and Microsoft set a bounty of $250,000 on the malware writer.
2010	Stuxnet Worm	Mainly affected the Iranian nuclear plants and a uranium enrichment plant.
2013	Cryptolocker Trojan	One of the first ransomware seen where it used social engineering to trick users into infecting their systems.
2013	ZeroAccess Botnet	Infected over 1.9 million computers and used their resources for bitcoin mining.
2014	Sony Picture Hack	Sony's film division systems were brought down for two hours and then wiped of data while rebooting.
2016	Mirai	First malware to scan the Internet of things vulnerable devices and used them to perform DDoS attacks on various sites.
2017	WannaCrypt0r Ransomware	Globally targeted Windows systems and demanded payment in Bitcoin. Affected over 300,000 machines across 150 countries.

▪ Οι Ιοί (Viruses) είναι κακόβουλα πρόγραμματα που μολύνουν άλλα προγράμματα με αντίγραφά τους. Εξαπλώνονται με το να αυτοαναπαράγονται συνέχεια και μπορούν να μεταδοθούν από ένα ΠΣ σε ένα άλλο. Εξαπλώνονται παθητικά μέσω μεταφοράς από αρχείο σε αρχείο, ή μέσω διαδικτυακών αρχείων. Μπορούν να χρησιμοποιηθούν για να βλάψουν αρχεία, να υποκλέψουν πληροφορίες, να σχηματίσουν botnets, να βλάψουν δίκτυα, υπηρεσίες, να κλέψουν χρήματα κ.α. (91).

Σκοπό έχουν την δυσλειτουργία ή και την καταστροφή ολόκληρων ΠΣ, την διαγραφή αρχείων ή και ολόκληρων σκληρών δίσκων. Τα προγράμματα αυτά είναι ένας βλαβερός εκτελέσιμος κώδικας που επιζεί με το να περιέχεται μέσα σε ένα άλλο πρόγραμμα ή σε ένα αρχείο. Δεν μπορεί να υπάρξει αυτόνομα σαν ξεχωριστό πρόγραμμα. Συνήθως η μετάδοση των ιών γίνεται μεσω διανομής τους με ηλεκτρονικό ταχυδρομείο (e-mail), αλλά μπορεί να μεταφερθούν και με φυσική σύνδεση μιας συσκευής σε μια άλλη που έχει ιό (όπως πολύ συχνά συμβαίνει με usb sticks ή cd rom). Πρωτοεμφανίστηκαν σαν πνευματικά παιχνίδια των ερευνητών σε επιστημονικά εργαστήρια αμερικανικών πανεπιστημίων όπως του M.I.T. Διακρίνονται σε :

1. Ιούς που μολύνουν τον τομέα που περιέχει εντολές εκκίνησης του υπολογιστή (Boot Viruses).

2. Ιούς που προσκολλώνται σε διάφορα τμήματα του λογισμικού ή στο πρόγραμμα ελέγχου εφαρμογών και μολύνουν το σύστημα (System Cluster Viruses).

3. Ιούς που προσβάλλουν προγράμματα Η/Υ και κρύβονται μέσα σε εκτελέσιμα αρχεία (*.exe). Αυτοί αρχίζουν να τρέχουν μόλις ξεκινήσει ένα πρόγραμμα που έχουν μολύνει (Software Viruses).

4. Ιούς ικανούς να αναπαράγονται με πολλούς και διάφορους τρόπους (Polymorphous Viruses), που καθίστανται έτσι ιδιαίτερα ανθεκτικοί έναντι των διαφόρων προγραμμάτων Anti-Virus.

5. Ιούς που έχουν την ικανότητα να «καμουφλάρουν» τις αλλαγές που πραγματοποιούν στον τομέα εκκίνησης ενός συστήματος ή ενός αρχείου (Stealth Viruses).

6. Άλλους που αποσκοπούν στο να καταστρέψουν ή να σβήσουν εντελώς τα αντιϊκά προγράμματα (Retroviruses) και τέλος

7. Ιούς που προσβάλλουν τις μακροεντολές σύγχρονων προγραμμάτων εφαρμογών (Data Viruses) (38).

▪ **Τα Σκουλήκια (worms)** είναι και αυτά αυτοαναπαραγόμενα κακόβουλα προγράμματα, που εξαπλώνονται μέσω διαδικτύου εκμεταλλευόμενα ευπάθειες των ΠΣ, και ενεργητικά μεταφέρουν άλλα καταστρεπτικά προγράμματα όπως π.χ. έναν ιό.

Διαφέρουν από τους ιούς, γιατί μπορούν να ενεργοποιηθούν και να εξαπλωθούν αυτόνομα, χωρίς ανθρώπινη παρεμβολή. Επίσης προκαλούν την δυσλειτουργία σύνδεσης του προσβληθέντος ΠΣ στο διαδίκτυο, ακόμα και την κατάρρευση αυτής γιατί καταναλώνουν πολλούς πόρους και το εύρος φάσματος διασύνδεσης για τις λειτουργίες τους (91).

▪ **Άλλοι τύποι malware είναι οι Δούρειοι ίπποι (Trojan Horses).** Αυτοί είναι προγράμματα και έχουν δύο μέρη, το server και το client. Για να μολυνθεί ένας Η/Υ από ένα πρόγραμμα δούρειου ίππου θα πρέπει με κάποιον τρόπο να εγκατασταθεί και να εκτελεστεί σε αυτόν το μέρος server. Αργότερα και αφού εκτελεστεί το μέρος client στον Η/Υ του επιτιθέμενου και δοθεί η IP διεύθυνση του υπολογιστή που έχει προσβληθεί, ο έλεγχος του θα είναι πλέον εύκολος. Οι δούρειοι ίπποι μεταφέρονται στον Η/Υ μέσω προγραμμάτων που λέγονται **droppers**.

Οι δούρειοι ίπποι λειτουργούν μέσω διαφόρων θυρών (ports) του Η/Υ οι οποίες για αυτό θα έπρεπε να είναι απενεργοποιημένες με τη χρήση κάποιου τοίχους προστασίας (firewall). Λέγονται δούρειοι ίπποι γιατί ενώ φαινομενικά είναι προγράμματα που λειτουργούν κανονικά και για χρήσιμο σκοπό, παράλληλα εκτελούν και κάποιες εργασίες μη επιτρεπόμενες. ‘Ετσι αν και ένα τέτοιο κακόβουλο λογισμικό μπορεί να έχει συνήθως την μορφή ενός παιχνιδιού, αυτό που κάνει στην πραγματικότητα είναι να κλέβει τα ονόματα και τους κωδικούς των ανυποψίαστων χρηστών του Διαδικτύου.

Συνήθως ένας δούρειος ίππος δημιουργεί μια κερκόπορτα (trapdoor) στο σύστημα, την οποία μπορεί μετά να χρησιμοποιήσει ο επιτιθέμενος για να συνδεθεί σε αυτό. Επιτρέπει σε κάποιον που τη γνωρίζει να αποκτήσει δικαιώματα προσπέλασης στο σύστημα, παρακάμπτοντας τις συνήθεις διαδικασίες ελέγχου προσπέλασης. Οι δούρειοι ίπποι δεν μπορούν να

αυτοαναπαραχθούν και συνήθως οι νόμιμοι χρήστες είναι αυτοί που προκαλούν άθελα και εν αγνοία τους, την αναπαραγωγή τους.

▪ Οι **λογικές βόμβες** είναι μικρά προγράμματα που προστίθενται σε κάποιο υπάρχον πρόγραμμα ή τροποποιούν κάποιον υπάρχοντα κώδικα. Είναι προγραμματισμένες να «εκραγούν» ηλεκτρονικά κάτω από ορισμένες προϋποθέσεις. Η επεξεργασία αυτή γίνεται από κάποιον που έχει πρόσβαση στο ΠΣ και φυσικά την απαιτούμενη γνώση για την εγκατάσταση της. Είναι περισσότερο επικίνδυνες από τα σκουλήκια και τους δούρειους ίππους γιατί κατασκευάζονται ευκολότερα και προξενούν σοβαρές ζημιές ακόμα και καταστροφές σε αρχεία, αλλά και σε ολόκληρο το λογισμικό ενός Η/Υ (38).

7.1.8 **Άλλα είδη κακόβουλου λογισμικού.**

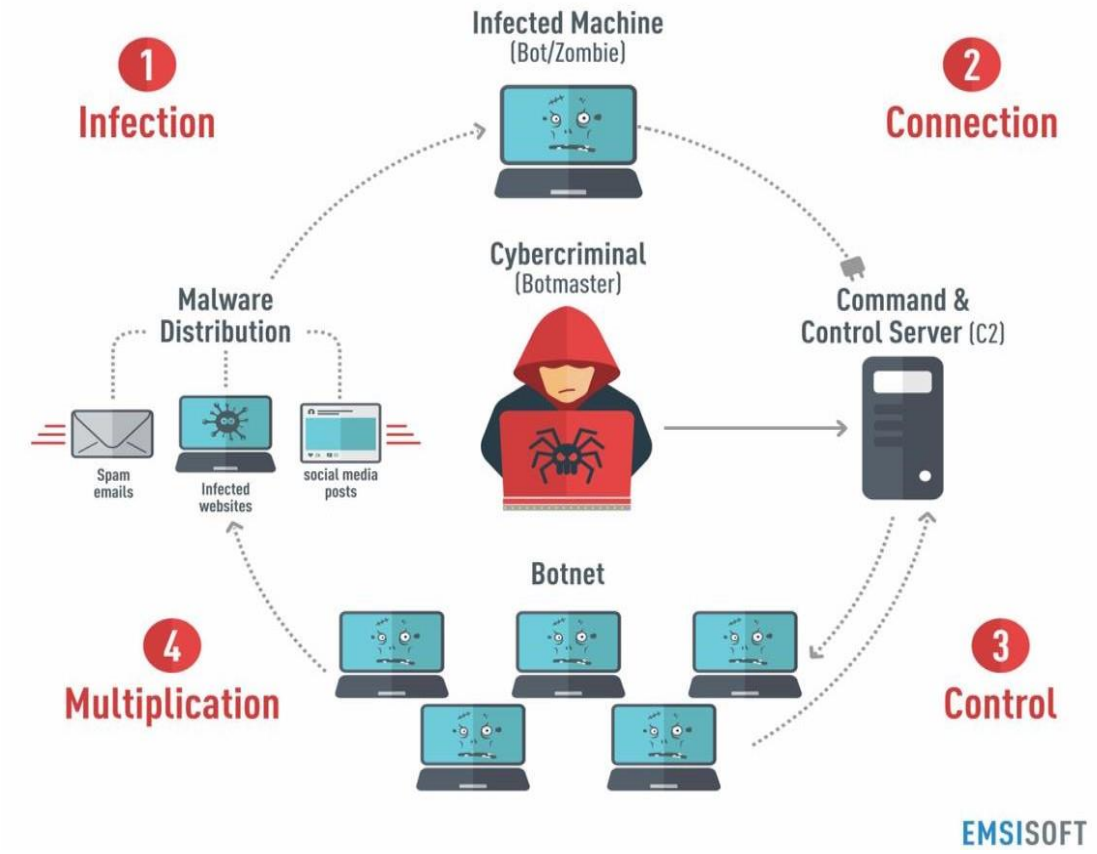
Οι Dialers είναι malware σχεδιασμένα με σκοπό να υποκλέπτουν σημαντικές πληροφορίες (κωδικοί πρόσβασης, στοιχεία λογαριασμών κλπ) του χρήστη, εν αγνοία του. Οι δημιουργοί προγραμμάτων spyware σκοπό έχουν τον προσπορισμό πολλών χρημάτων εύκολα και γρήγορα. Οι dialers επεμβαίνουν στις ρυθμίσεις ενός δικτύου μέσω τηλεφώνου (dial up networking) για να υποχρεώσουν το χρήστη να καλεί έναν συγκεκριμένο άγνωστο σε αυτόν αριθμό που είθισται να είναι διεθνής κλήση με υψηλό κόστος. Μετά διαγράφουν τον πάροχο υπηρεσιών διαδικτύου (ISP) που χρησιμοποιεί ο χρήστης και τον αντικαθιστούν με τον δικό τους πάροχο. Με αυτόν τον τρόπο κάθε φορά που ο χρήστης συνδέεται στο διαδίκτυο χρησιμοποιεί τον αριθμό του dialer και όχι τον αριθμό του δικού του παρόχου υπηρεσιών διαδικτύου (38).

▪ Τα **Rootkits εί**ναι προγράμματα που διαθέτουν εξελιγμένα και πολύπλοκα εργαλεία που τους επιτρέπουν να διαφεύγουν του εντοπισμού τους από το ΠΣ στο οποίο εισβάλλλουν, και δίνουν τη δυνατότητα στους χάκερς να διατηρήσουν την πρόσβαση τους στο ΠΣ που έχουν εισβάλει. Τα εργαλεία επίσης του rootkit θα του επιτρέψουν να βρεί ονόματα χρηστών και κωδικούς πρόσβασης, να εξαπολύσει επιθέσεις κατά συστημάτων από απόσταση και να αποκρύψει τις δράσεις του με την απόκρυψη αρχείων και την διαγραφή κάθε δραστηριότητας από τα αρχεία καταγραφής του συστήματος. Με τα

rootkit μπορεί ακόμα να αποκτήσουν και τον πλήρη έλεγχο ενός ΠΣ παραδείγματος χάριν, μπορεί να ελέγξει την κίνηση, την πληκτρολόγηση, να επιτίθεται σε άλλους υπολογιστές στο δίκτυο, ή να δημιουργήσει κερκόπορτες (trapdoors) στο ΠΣ, για την εξυπηρέτηση των εισβολέων (91), (38).

▪ Τα **Ransomware**, με αυτά οι κακόβουλοι από απόσταση κρυπτογραφούν δεδομένα του χρηστή και για να του τα αποκρυπτογραφήσουν έπειτα απαιτούν «λύτρα» από το χρήστη. Την Παρασκευή 12 Μαϊου 2017, μια μεγάλη κυβερνοεπίθεση εξαπολήθηκε εναντίον ΠΣ που χρησιμοποιούσαν Microsoft Windows στη Μεγάλη Βρεταννία. Προσέβαλε τους Η/Υ του Εθνικού Σύστημα Υγείας, τους μαγνητικούς τομογράφους, τα ψυγεία συντήρησης αίματος, και τον εξοπλισμό στα χειρουργεία. Η παροχή υγειονομικής φροντίδας εξαιτιάς της επίθεσης υπονομεύθηκε, για όσο η επίθεση ηταν στην κορύφωσή της. Η κατάσταση ήταν δυνατό να είχε αποφευχθεί αν είχε εφαρμοστεί μια σχετική αναβάθμιση της Microsoft που είχε τεθεί στην κυκλοφορία τον Μάρτιο του 2017 (92).

▪Τα **Bots – zombies**. Με ένα είδος κακόβουλου λογισμικού ο εισβολέας αποκτά παράνομα τον πλήρη έλεγχο πάνω σε έναν Η/Υ. Οι Η/Υ που έχουν μολυνθεί με bot καλούνται ζόμπι. Τα bots αρχικά πήρανε το όνομά τους από τα «robots» που είχανε δημιουργηθεί για τη διαχείρηση καναλιών του πρωτοκόλλου του Internet relay chat (IRC), και κάποια από αυτά χρησιμοποιούνται για νόμιμους σκοπούς. Χιλιάδες υπολογιστές στο διαδίκτυο έχουν μολυνθεί με κάποιο είδος κακόβουλου bot και δεν το αντιλαμβάνονται οι χρήστες τους, λειτουργώντας σαν Zombie Η/Υ, εν αγνοία τους. Ο εισβολέας ή αλλιώς botmaster μπορεί να χρησιμοποιήσει τους μολυσμένους Η/Υ για να προσβάλει ή να στείλει spam σε άλλους υπολογιστές χωρίς να το ξέρουν οι ιδιοκτήτες τους ή να εξαπολύσει επιθέσεις άρνησης εξυπηρέτησης σε ΠΣ. Τα CAPTCA τεστ χρησιμοποιούνται για την προστασία ιστοτόπων από bots πιστοποιώντας τους χρήστες ως ανθρώπους (38), (91).



Εικόνα 15. Περιγραφή ενός botnet **(93)**

▪ **Spyware**. Είναι κακόβουλα προγράμματα που δρούν στο λειτουργικό σύστημα με σκοπό να κατασκοπεύουν την δραστηριότητα των χρηστών. Εξαπλώνονται μέσω επικόλλησης τους σε νόμιμο λογισμικό, ή μέσω δούρειων ίππων και εκμετάλλευσης ευπαθειών. Μπορούν να καταγράφουν τη συμπεριφορά των χρηστών, την πληκτολόγηση τους (keyloggers) και στέλνουν αυτές τις πληροφορίες στον δημιουργό του κακόβουλου προγράμματος.

▪ **Adware**. Σύνθετη λέξη από το advertising supported software και σκοπό έχουν την αυτόματη διαφήμιση μέσω pop-up διαφημιστικών σε ιστοσελίδες. Συνήθως χρησιμεύουν σε διαφημιστές αλλά μπορεί να βρίσκονται και σε συνδυασμό με spyware και είναι ακόμα πιο επικίνδυνα (91).

▪ **Scareware**. Είναι προγράμματα εξαπάτησης - fraudware τα οποία συχνά εμφανίζουν pop-up παράθυρα με σκοπό να εκφοβίσουν τους χρήστες του διαδικτύου (π.χ. ότι Η/Υ τους έχει μολυνθεί με κακόβουλο λογισμικό) και να

τους πείσουν να προβούν στην αγορά ή/και εγκατάσταση συγκεκριμένου λογισμικού που δήθεν θα τους προστατέψει από επιθέσεις και απειλές, εξυπηρετώντας στην πραγματικότητα τους σκοπούς των δραστών.

▪ Τα **βακτήρια (bacteria)** είναι προγράμματα που αν και δεν καταστρέφουν αρχεία, εντούτοις είναι επιβλαβή μέσω του συνεχούς πολλαπλασιασμού τους μεσα στο ΠΣ (όπως κάνουν τα τυπικά βακτήρια στον ανθρώπινο οργανισμό). Ένα βακτήριο μπορεί να μην κάνει τίποτε περισσότερο από το να τρέχει ταυτόχρονα δύο αντίγραφά του σε ένα ΠΣ ή να δημιουργεί συνεχώς δύο νέα αρχεία καθένα απ' τα οποία είναι αντίγραφο του αρχικού αρχείου που περιέχει το βακτήριο. Και τα δύο αυτά προγράμματα μπορούν στη συνέχεια να αντιγράψουν τον εαυτό τους δύο φορές κ.ο.κ. Έτσι τελικά καταλαμβάνουν όλη τη χωρητικότητα του επεξεργαστή, της μνήμης ή του δίσκου, στερώντας τους πόρους αυτούς από τους χρήστες.

▪ **Τα exploit** είναι κακόβουλο κομμάτι κώδικα που εκτελούμενο μπορεί να εκμεταλλευτεί κάποιο bug ή κάποιο κενό ασφαλείας μιας εφαρμογής ή του λειτουργικού συστήματος και να παρέχει μη εξουσιοδοτημένη πρόσβαση ή και αύξηση δικαιωμάτων (από απλό χρήστη σε root) στον επιτιθέμενο που το εκτέλεσε (38). Τα exploits μπορεί να εκτελούνται σε ένα μηχάνημα στόχο, είτε απομακρυσμένα προσπαθώντας να εκμεταλλευτούν κάποια ευπάθεια μιας εφαρμογής λογισμικού που τρέχει εκεί, όπως για παράδειγμα ενός mail server ή client, ενός FTP server ή client, ενός browser κ.τ.λ (remote exploits), είτε τοπικά δηλαδή κατευθείαν επάνω στο ίδιο το μηχάνημα του στόχου οπότε μιλάμε για local exploits, που δίνουν πρόσβαση υπερχρήστη (root) στο μηχάνημα που εκτελείται ο κακόβουλος κώδικας.

Με τις **επιθέσεις άρνησης εξυπηρέτησης (DoS)** ένας εισβολέας εξαπολύει ηλεκτρονικές επιθέσεις, προσπαθώντας να διαταράξει ή να σταματήσει τη λειτουργία μιας διαδικτυακής υπηρεσίας για παράδειγμα ενός διακομιστή ιστοσελίδας (web server) ή ενος διακομιστή αρχείων (file server), π.χ. του ΠΣ ενός νοσοκομείου. Οι βασικότερος στόχος που επιτυγχάνεται με τις επιθέσεις άρνησης εξυπηρέτησης είναι η υποβάθμιση της ποιότητας των προσφερόμενων υπηρεσιών στους χρήστες .

Software bug: Ως bug χαρακτηρίζεται κάποιο ελάττωμα ή σφάλμα ενός προγράμματος το οποίο οδηγεί σε λανθασμένη εκτέλεση του.

Στο κεφάλαιο αυτό εξετάστηκαν τα εγκλήματα που εντοπίζονται στον κυβερνοχώρο που μπορεί να οφείλονται σε έλλειψη λήψης κατάλληλων μέτρων, και γι αυτό όποιος ασχολείται με το αντικείμενο θα πρέπει να τα γνωρίζει και να λαμβάνει μέτρα αντιμετωπισής τους.

Κεφάλαιο 7ο: Συμπεράσματα

Το πρόβλημα της ασφάλειας των ΠΣΥ και της προστασίας των προσωπικών δεδομένων υγείας που φυλάσσονται σε αυτά, οπωσδήποτε αποτελεί πρόκληση για τους ειδικούς αλλά και παράγοντα ανησυχίας για την κοινωνία ιδιαίτερα για τον μη ενημερωμένο πολίτη ή εργαζόμενο στο χώρο της υγείας.

Στην δυσκολία αντιμετώπισης των ποικίλλων θεμάτων ασφάλειας ΠΣ και προστασίας ΔΠΧ, στην ευρωπαϊκή κοινότητα συμβάλλει και η πολυδιάσπαση νομοθετημάτων, τεχνικών επιτροπών τόσο ανάμεσα στα διάφορα κράτη μέλη, όσο και μέσα στα ίδια κράτη μέλη. Για αυτό κρίνεται απαραίτητο (και η Ε.Ε. το δείχνει με πρωτοβουλίες της όπως ο ΓΚΠΔ, και η σύσταση της Enisa) να υπάρχει μεγαλύτερος συντονισμός τους, διαφάνεια στις διαδικασίες και ενημέρωση των πολιτών.

Ο κάθε υπεύθυνος για την προστασία ΔΠΧ και ασφάλειας ΠΣΥ, θα πρέπει να έχει γνώσεις σχετικά με τη νομοθεσία, τη λειτουργία των ΠΣ και του διαδικτύου, τα τεχνικά μέτρα προστασίας, τα ΣΔΑΠ, την εκπόνηση αξιολογήσεων κινδύνου, και τις απειλές και τα εγκλήματα στον κυβερνοχώρο.

Με οργάνωση, πολύ δουλειά και συνέπεια, μπορεί να πετύχει στο έργο του ενπολλοίς αν και όχι απόλυτα, σε συνεργασία με τις αρμόδιες υπηρεσίες και φορείς που δεν είναι και λίγες και πρέπει να συντονίζονται καλύτερα, αποτελεσματικότερα, και αποδοτικότερα. Επίσης θα επιτύχει αν διαθέτει γνώση, ενημέρωση σε πολλούς επιστημονικούς και τεχνολογικούς τομείς. Οι υπολογιστικές μηχανές έχουν τεράστια δύναμη ανάλυσης, αποθήκευσης και επεξεργασίας δεδομένων, είναι διαρκώς εξελισσόμενες, και ο σύγχρονος άνθρωπος πρέπει να συνδυάζει πολλές ικανότητες αν θέλει να τις κρατήσει υπό τον έλεγχο του προκειμένου να υποστηρίξει με αυτές την βελτίωση της ποιότητας της ζωής του.

Όσον αφορά τις διάφορες υπηρεσίες θα εξυπηρετούσε να είναι λιγότερες και με πιο συγκεκριμένα καθήκοντα, πρότυπα λειτουργίας και πλαίσια αναφοράς, τόσο σε εθνικό, ευρωπαϊκό όσο και διεθνές επίπεδο, υπό τον έλεγχο διεθνών

οργανισμών όπως τα Ηνωμένα Έθνη, η Ευρωπαϊκή Ένωση, η Enisa, ανεξάρτητων αρχών όπως η ΑΠΔΠΧ, ΑΔΑΕ κλπ, οι ομάδες CSIRT και με τη χρήση διεθνώς αναγνωρισμένων τεχνολογικών προτύπων όπως του ISO, της ITU, της IETF, της IEEE, της NIST κλπ.

Νομοθετικά, σημαντικό είναι ότι προβλέπεται στη νομοθεσία η περιοδική και συχνή σύνταξη εκθέσεων σχετικά με τη συμμόρφωση φυσικών προσώπων, επιχειρήσεων, οργανισμών, κρατικών φορέων και κρατών με τις προβλέψεις της. Θα συνέβαλλε ενδεχομένως σύμφωνα και με τις αρχές της διαλειτουργικότητας, να είναι ακόμα πιο καθορισμένα τα πρότυπα και οι μέθοδοι προστασίας, ώστε να υπάρχει ποιοτικότερος συντονισμός στην αντιμετώπιση των επιτιθεμένων και των απειλών.

Συχνά θα πρέπει να γίνονται μελέτες διαχείρισης ασφάλειας και κινδύνου μέσω κάποιου ΣΔΑΠ, όπως το ISO27K, και παρακολούθηση του με αξιολογήσεις και χρήση εργαλείων αξιολόγησης κινδύνου όπως το Cramm και μεθόδων όπως penetration testing. Σημαντικός είναι και ο ρόλος της κουλτούρας ασφάλειας μέσα στον οργανισμό και η χρήση εργαλείων ελέγχου της όπως το IPTT.

Στην ασφάλεια μπορεί και οφείλει να συμβάλλει σημαντικά ο κάθε εργαζόμενος στον χώρο της υγείας και ο κάθε χρήστης των ΠΣΥ, αλλά σίγουρα απαιτεί συνεργασία πολλών ειδικών: πληροφορικών, διοικητικών, ΜΜΕ, οικονομοτεχνικών, υγειονομικών, δικαστικών, πολιτικών, ανεξάρτητων αρχών, διεθνών οργανισμών, υπό την καθοδήγηση εξειδικευμένων στην κυβερνοασφάλεια ατόμων που ασχολούνται κατά προτεραιότητα με αυτό το αντικείμενο και με τελικό κύριο γνώμονα τον πρόσφατα εφαρμοσθέντα κανονισμό GDPR και τους αντίστοιχους που υπάρχουν και άλλους που θα ακολουθήσουν όπως η οδηγία NIS.

Ένα άλλο βασικό συμπέρασμα είναι ότι η ΠΔΠΧ και η επένδυση στην ασφάλεια των ΠΣ θα βοηθήσει εντέλει την καλή φήμη και την προστασία του ίδιου του υγειονομικού σχηματισμού, εφοσον προηγούμενα έχει γίνει σωστή διαχείριση και αποτίμηση κινδύνων και απειλών.

Το τελικό και ουσιαστικό αποτέλεσμα πλην όλων των άλλων θα είναι να αυξηθεί η εμπιστοσύνη των πολιτών, και η διάθεσή τους να χρησιμοποιούν τα ΠΣΥ κάτι που είναι προς την κατεύθυνση που επιτάσσουν οι ευρωπαϊκές και παγκόσμιες νομοθετικές πρωτοβουλίες για την ενσωμάτωση των νέων ψηφιακών τεχνολογιών στον χώρο της υγείας.

Η μελέτη αυτή προσπάθησε να ενημερώσει και να εξηγήσει τα λεπτά ζητήματα που κυριαρχούν στον τομέα της κυβερνοασφάλειας στην εποχή της εκπόνησής της, ζητήματα όπως τα ΔΠΧ, η ιδιωτικότητα, τα πρωτόκολλα επικοινωνιών και δικτύων, η νομοθεσία, οι τεχνικές προστασίας ΤΠΕ, η διαχείριση κινδύνου με τα ISMS, οι παράνομες πράξεις στον ψηφιακό κόσμο.

Για τον ίδιο σκοπό, θα ήταν χρήσιμο περιοδικά στο μέλλον να επαναλαμβάνονται μελέτες όπως αυτή που έγινε στην παρούσα εργασία. Θα ήταν επίσης ενδιαφέρον να γίνουν σχετικές έρευνες που θα αφορούν πως θα είναι η κατάσταση στο μέλλον της cybersecurity, της e-privacy και της data protection.

Βιβλιογραφία

1. Δουληγέρης Χ. Ασφάλεια Πληροφοριακών και Επικοινωνιακών συστημάτων. Ανάπτυξη και Διαχείρηση ασύρματων Ευρυζωνικών Δικτύων, Συστημάτων Διαχείρησης Πληροφοριών & Ελέγχου Αυτοματισμών στην Γεωργική Παραγωγή και Ηλεκτρονικό Επιχειρείν στην Περιφέρεια Πελλοποννήσου. Τρίπολη: Υπουργείο Παιδείας και Θρησκευμάτων, Εκπαίδευση και Δια βίου μάθηση; 2015.

2. Φιλλόπουλος Π, Γιαννόπουλος Κ. Εισαγωγή στις επικοινωνίες. Ανάπτυξη και Διαχείρηση ασύρματων Ευρυζωνικών Δικτύων, Συστημάτων Διαχείρησης Πληροφοριών & Ελέγχου Αυτοματισμών στην Γεωργική Παραγωγή και Ηλεκτρονικό Επιχειρείν στην Περιφέρεια Πελλοποννήσου. Τρίπολη: Υπουργείο Παιδείας και Θρησκευμάτων, Εκπαίδευση και Διαβίου μάθηση; Σεπτέμβριος 2015.

3. COMMISSION E. [IMPACT ASSESSMENT,Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA,the "EU Cybersecurity Agency",and repealing Regulation(EU)526/2013,and on Information and Communication Technology cybersecurity]. Brussels; 2017 [cited 2018 07 02]. Διαθέσιμο από: https://eur-lex.europa.eu/resource.html?uri=cellar:2413e286-985e-11e7-b92d-01aa75ed71a1.0001.02/DOC_2&format=PDF.

4. Έθνη Η. United Nations. [Online].; 1948 [cited 2018 07 02]. Διαθέσιμο από: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf.

5. wikipedia. [Ανθρώπινα Δικαιώματα]. [cited 2017 08 07]. Διαθέσιμο από: https://el.wikipedia.org/wiki/%CE%91%CE%BD%CE%B8%CF%81%CF%8E%CF%80%CE%B9%CE%BD%CE%B1_%CE%B4%CE%B9%CE%BA%CE%B1%CE%B9%CF%8E%CE%BC%CE%B1%CF%84%CE%B1.

6. Συμβασή 108, Council of Europe. [Online].; 1981 [cited 2018 07 02]. Διαθέσιμο από: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.

7. Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe. [Online].; 1950 [cited 2018 6 20]. Διαθέσιμο από: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680063765.

8. O.H.E.. Preamble., Universal Declaration of Human Rights. [Online].; 1948 [cited 2017 07 05]. Διαθέσιμο από: http://www.un.org/en/universal-declaration-human-rights/.

9. EurLex, Το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και η Επιτροπή. [Online].; 2012 [cited 2018 06 02]. Διαθέσιμο από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN.

10. ΕΣΔΑ. Απλοποιημένη μορφή επιλεγμένων άρθρων της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου. [Online]. Brussels; 2013 [cited 2017 05 05]. Διαθέσιμο από: https://www.echr.coe.int/Documents/Convention_ELL.pdf.

11. ΕΝΟΠΟΙΗΜΕΝΗ ΑΠΟΔΟΣΗ ΤΗΣ ΣΥΝΘΗΚΗΣ ΓΙΑ ΤΗ ΛΕΙΤΟΥΡΓΙΑ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ. [Online].; 2012 [cited 2018 06 05]. Διαθέσιμο από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:12012E/TXT&from=EL.

12. ΦΕΚ. e-nomothesia.gr, Νόμος 3051. Συνταγματικά κατοχυρωμένες ανεξάρτητες αρχές. [Online].; 2002 [cited 2018 05 02]. Διαθέσιμο από: https://www.e-nomothesia.gr/kat-demosia-dioikese/n-3051-2002.html.

13. ΑΔΑΕ. ΦΕΚ, Νόμος 3115, ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 3674, Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις. [Online].; 2003 [cited 2018 07 02]. Διαθέσιμο από: http://www.adae.gr/fileadmin/docs/nomoi/N.3115-2003.pdf.

14. ΦΕΚ. ΠΔ., 47/2005 [Π.Δ., 47/2005, Διαδικασίες και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών καθώς και για τη διασφάλισή του.].; 2005 [cited 2017 07 02]. Διαθέσιμο από: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/pd-47-2005.html.

15. EUR-Lex. Ευρωπαϊκό Συμβούλιο, ΟΔΗΓΙΑ 2002/58/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνι. [Online]. Βρυξέλλες; 2002 [cited 2018 7 2]. Διαθέσιμο από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32002L0058&qid=1532602414943&from=EL.

16. ΦΕΚ. Νόμος 3471/2006, Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής. [Online].; 2006 [cited 2017 05 02]. Διαθέσιμο από: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/PROSOPIKA%20DEDOMENA/FILES/%CE%9D3471_06.PDF.

17. ΦΕΚ. ΑΠΔΠΧ, ΝΟΜΟΣ 2472/1997, ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΤΟΜΟΥ ΑΠΟ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΜΕ ΕΝΣΩΜΑΤΩΜΕΝΕΣ ΤΙΣ ΤΡΟΠΟΠΟΙΗΣΕΙΣ. [Online].; 1997 [cited 2018 07 28]. Διαθέσιμο από: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/PROSOPIKA%20DEDOMENA/FILES/2472_97_JUNE2013.PDF.

18. ΦΕΚ. Αρχή Διασφάλισης Απορρήτου Επικοινωνιών. [Online].; 2011 [cited 2018 07 02]. Διαθέσιμο από: http://www.adae.gr/fileadmin/docs/nomoi/nomoi/Nomos__3917_2011_diatirisi_dedomenon.pdf.

19. ΦΕΚ. Κοινή Πράξη της ΑΠΔΠΧ και ΑΔΑΕ για τις υποχρεώσεις των παρόχων για προστασία και ασφάλεια δεδομένων, σύμφωνα με το άρθρο 7 του ν. 3917/2011. [Online].; 2013 [cited 2018 06 18]. Διαθέσιμο από: http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=254,89,110,102,22,103,89,84.

20. ΑΠΔΠΧ. πολλές σχετικές νομοθετικές διατάξεις. [Online].; 2011 [cited 2018 7 2]. Διαθέσιμο από: http://www.dpa.gr/portal/page?_pageid=33,123437&_dad=portal&_schema=PORTAL.

21. ΑΠΔΠΧ. βιομετρικά δεδομένα. [Online]. [cited 2018 07 02]. Διαθέσιμο από: http://www.dpa.gr/portal/page?_pageid=33,131221&_dad=portal&_schema=PORTAL.

22. ΑΠΔΠΧ. Βιομετρικά δεδομένα. [Online]. [cited 2018 07 02]. Διαθέσιμο από: http://www.dpa.gr/portal/page?_pageid=33,131221&_dad=portal&_schema=PORTAL.

23. ΑΠΔΠΧ. ΟΔΗΓΙΑ 1/2011 , Χρήση συστημάτων βιντεοεπιτήρησης για την προστασία προσώπων και αγαθών. [Online]. Αθήνα; 2011 [cited 2018 06 05]. Διαθέσιμο από: http://www.dpa.gr/portal/page?_pageid=33,124816&_dad=portal&_schema=PORTAL.

24. ΑΠΔΠΧ. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. [Online]. [cited 2018 07 02]. Διαθέσιμο από: http://www.dpa.gr/portal/page?_pageid=33,124876&_dad=portal&_schema=PORTAL.

25. ΑΠΔΠΧ. στην ΥΠΕΔΥΦΚΑ και στη Διεύθυνση Μηχανογραφικών Εφαρμογών για τη συλλογή και την περαιτέρω επεξεργασία ιατρικών συνταγών, παραπεμπτικών ιατρικών εξετάσεων, ιατρικών διαγνώσεων, στο πλαίσιο της εφαρμογής της ηλεκτρονικής συνταγογράφησης κατά τα προβλεπόμενα. [Online].; 2011 [cited 2018 06 22]. Διαθέσιμο από: http://www.dpa.gr/portal/page?_pageid=33,124684&_dad=portal&_schema=PORTAL.

26. ΑΠΔΠΧ. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ), European Data Protection Supervisor - EDPS). [Online]. Αθήνα [cited 2018 7 2]. Διαθέσιμο από: http://www.dpa.gr/portal/page?_pageid=33,124906&_dad=portal&_schema=PORTAL.

27. GDPR Γ. ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ. ; 2016.

28. Σιασιάκος , Αναστασίου Σ, Τούντας Κ. Εκτίμηση των Επιπτώσεων σχετικά με την Προστασία Δεδομένων σε έργα Ηλεκτρονικής Διακυβέρνησης. In Ελληνικό Ινστιτούτο Οικονομικών της Εκπαίδευσης, Δια Βίου Μάθησης, Έρευνας και Καινοτομίας; 2016; Αθήνα: Χαροκόπειο παν/μιο. p. 542-55.

29. ΦΕΚ. Keelpno, Νόμος υπ' αριθ. 3991, Διεθνή Υγειονομικό κανονισμό, Παγκόσμιος Οργανισμός Υγείας. [Online].; 2011 [cited 2018 07 03]. Διαθέσιμο από: http://www.keelpno.gr/Portals/0/%CE%91%CF%81%CF%87%CE%B5%CE%AF%CE%B1/

Highlights/DYK_2018/%CE%A6%CE%95%CE%9A_162_250711.pdf.

30. EUR- lex, Ευρωπαϊκό Κοινοβούλιο, Ευρωπαϊκό Συμβούλιο. [Online].; 1996 [cited 2018 07 20]. Διαθέσιμο από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31996L0009&from=EN.

31. EUR-lex, ΟΔΗΓΙΑ 2009/24/ΕΚ για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών. [Online].; 2009 [cited 2018 08 01]. Διαθέσιμο από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009L0024&from=EN.

32. ΑΠΔΠΧ. ΝΟΜΟΣ ΥΠ'ΑΡΙΘ. 3418, Κώδικας Ιατρικής Δεοντολογίας. [Online].; 2005 [cited 2018 06 22]. Διαθέσιμο από: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/THEMATIKES_ENOTITES/NOM%203418_2005.PDF.

33. ΦΕΚ. e-nomothesia.gr, Άρθρο 47 Νόμος 2071 « εκσυγχρονισμός και οργάνωση συστημάτων υγείας». [Online].; 1992 [cited 2018 07 02]. Διαθέσιμο από: Διαθέσιμο από : https://www.e-nomothesia.gr/inner.php/kat-ygeia/n-2071-1992.html?print=1.

34. Σύνταγμα. Βουλή των Ελλήνων. [Online].; 2008 [cited 2018 08 02]. Διαθέσιμο από: https://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma.

35. ΦΕΚ. e-nomothesia.gr, Νόμος 1805/1988 - ΦΕΚ 199/Α/31-8-1988, Εκσυγχρονισμός του θεσμού του ποινικού μητρώου, τροποποίηση ποινικών διατάξεων και ρύθμιση άλλων σχετικών θεμάτων. [Online].; 1988 [cited 2018 08 03]. Διαθέσιμο από: https://www.e-nomothesia.gr/kat-dikasteria-dikaiosune/n-1805-1988.html.

36. ΦΕΚ. ΑΔΑΕ, ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4411 - Κύρωση Σύμβασης για το έγκλημα στον Κυβερνοχώρο. [Online]. Αθήνα; 2016 [cited 2018 7 2]. Διαθέσιμο από: http://www.adae.gr/fileadmin/documents/4411_2016.pdf.

37. Αρχή διασφάλισης του απορρήτου των επικοινωνιών. [Online].; 1994 [cited 2018 07 02]. Διαθέσιμο από: http://www.adae.gr/fileadmin/docs/nomoi/nomoi/2225.1994.pdf.

38. Λιανού Κ. ΕΓΚΛΗΜΑ ΚΑΙ ΔΙΑΔΙΚΤΥΟ. ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ. Αθήνα: ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ, ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΤΟΜΕΑΣ ΑΝΘΡΩΠΙΣΤΙΚΩΝ & ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ & ΔΙΚΑΙΟΥ ; 2013 Φεβρουάριος.

39. EurLex, ΟΔΗΓΙΑ (ΕΕ) 2016/1148 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση. [Online].; 2016 [cited 2018 05 03]. Διαθέσιμο από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

40. European Political Strategy Centre E. Ευρωπαϊκή Επιτροπή, Building an Effective European Cyber Shield - Taking EU Cooperation to the Next Level. [Online].; 2017 [cited 2018 7 29]. Διαθέσιμο από: http://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en.

41. ΑΔΑΕ. ΦΕΚ, ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 4070,Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις. [Online].; 2012 [cited 2018 07 02]. Διαθέσιμο από: http://www.adae.gr/fileadmin/docs/nomoi/nomoi/N.4070.pdf.

42. Oecd. «Health data governance, privacy, monitoring and research.». [Online]. Paris: OECD Publishing; 2015 [cited 2017 06 08]. Διαθέσιμο από: http://www.oecd.org/publications/health-data-governance-9789264244566-en.htm.

43. Καρασταμάτη Ε. Ασφάλεια και ιδιωτικότητα στα πληροφοριακά συστήματα Υγείας. Μεταπτυχιακή Εργασία. Πειραιάς: Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων; 2012.

44. Wikipedia. HIPAA. [Online]. [cited 2018 7 2]. Διαθέσιμο από: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act.

45. Hall JL, McGraw D. For Telehealth To Succeed, Privacy And Security Risks Must Be Identified And Addressed. Health Affairs. 2014 February; 33(no.2 (2014):216-221).

46. Μαντάς Ι. Πληροφορική της Υγείας: Πληροφοριακά Συστήματα Νοσοκομείων Νοσηλευτικής Τ, editor. Αθήνα: Πανεπιστήμιο Αθηνών; 2016.

47. Βασιλείου Μυλωνά Δ. Πληροφοριακά Συστήματα Υγείας. Διπλωματική εργασία. Πειραιάς: Πανεπιστήμιο Πειραιά, Τμήμα Οργάνωσης και διοίκησης επιχειρήσεων; 2013.

48. Κασκαφέτου Σ. Μεταπτυχιακή εργασία: Μελέτη της ηλεκτρονικής συνταγογράφησης και η διερεύνηση της εφαρμογής της στην Ελλάδα ¨ΟΑΕΕ Πειφέρεια Πελοποννήσου. Πανεπιστήμιο Πειραιά, Διοϊκησή Υπηρεσιών Υγείας.

49. 189 Φ. ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 3892 Ηλεκτρονική καταχώριση και εκτέλεση ιατρικών συνταγών και παραπεμπτικών ιατρικών εξετάσεων. [Online].; 2010 [cited 2018 7 22]. Διαθέσιμο από: https://www.e-nomothesia.gr/kat-ygeia/n-3892-2010.html.

50. Domingo-Ferrer J, Hansen M, Hoep JH, Danezis G, Le Métayer , Tirtea , et al. ENISA, Privacy and Data Protection by Design – from policy to engineering. [Online].; 2014 [cited 2018 7 21]. Διαθέσιμο από: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

51. Επιτροπή Ε. Ευρωπαϊκό πλαίσιο διαλειτουργικότητας - Στρατηγική εφαρμογής , ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ

ΠΕΡΙΦΕΡΕΙΩΝ. [Online]. Βρυξέλλες; 2017 [cited 2018 08 11]. Διαθέσιμο από: https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0020.02/DOC_3&format=PDF.

52. Καραστόγιαννης Ε. Δίκτυο ηλεκτρονικής υγείας στη Δυτική Μακεδονία. Διπλωματική εργασία. Θεσσαλονίκη: Πανεπιστήμιο Μακεδονίας, Μεταπτυχιακό Πρόγραμμα"επιχειρηματική πληροφορική"; 2006.

53. Ren J, Li T. Chapter 12: Network Management. In Bidgoli, Ph.D H, editor. The Handbook of Technology Management, Volume III, Management Support Systems, Electronic Commerce, Legal and Security Considerations.: Wiley; 2010.

54. TANENBAUM A, WETHERALL J. COMPUTER NETWORKS. FIFTH EDITION ed. Hirsch , editor. Boston: Prentice Hall; 2011.

55. Srivaths R, Anand R, Nachiketh P. Securing Wireless Data : System Architecture Challenges. NL 08540: Computer & Communications Research Labs NEC USA, Princeton.

56. wikipedia. WAP PROTOCOL. [Online]. [cited 2018 07 02]. Διαθέσιμο από: https://en.wikipedia.org/wiki/Wireless_Application_Protocol.

57. Boncella RJ. Wireless Security : An Overview. Communications of the Association for Information Systems. Article 15. 2002 October; 9.

58. Δουληγέρης Χ, Χίμος Κ. ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΕΦΑΡΜΟΓΕΣ. Ανάπτυξη και Διαχείρηση ασύρματων Ευρυζωνικών Δικτύων, Συστημάτων Διαχείρησης Πληροφοριών & Ελέγχου Αυτοματισμών στην Γεωργική Παραγωγή και Ηλεκτρονικό Επιχειρείν στην Περιφέρεια Πελλοποννήσου. Τρίπολη: Υπουργείο Παιδείας και Θρησκευμάτων; 2015.

59. Δουληγέρης Χ, Βέργαδος ΔΔ, Σγώρα Α. Διαχείρηση δικτύων. Ανάπτυξη και Διαχείρηση ασύρματων Ευρυζωνικών Δικτύων, Συστημάτων Διαχείρησης Πληροφοριών & Ελέγχου Αυτοματισμών στην Γεωργική Παραγωγή και Ηλεκτρονικό Επιχειρείν στην Περιφέρεια Πελλοποννήσου. Τρίπολη: Υπουργείο Παιδείας και Θρησκευμάτων; 2015.

60. (10/96) RX81. International Telecommunication Union (ITU). [Online].; 1996 [cited 2018 08 06]. Διαθέσιμο από: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=3794&lang=en.

61. Παταρίδης Θ. Ασφάλεια και Εφαρμογές Κρυπτογραφικών εργαλείων στο χώρο της Υγείας. Διπλωματική εργασία. Θεσσαλονίκη: Πανεπιστήμιο Μακεδονία, Τμήμα Εφαρμοσμένης Πληροφορικής; 2010.

62. Μαντάς Ι. Πληροφορική της Υγείας: Θέματα ασφαλείας δεδομένων υγείας Αθήνα: Τμήμα Νοσηλευτικής, Πανεπιστήμιο Αθηνών; 2016.

63. Stouffer K, et al. Guide to Industrial Control,Systems (ICS) Security,Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS),and Other Control System Configurations such as Programmable Logic Controllers (PLC). 100 Bureau Dr., Stop 1070,Gaithersburg, MD 20899-1070.U.S.A.: National Institute of Standards and Technology (NIST), NIST Special Publication 800-82; 2015.

64. WP29. WORKING PARTY, ARTICLE 29 DATA PROTECTION , Opinion 04/2012 on Cookie Consent Exemption. Article 29 of Directive 95/46/EC. Brussels: Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013., independent European advisory body on data protection and privacy; 2012. Report No.: http://ec.europa.eu/justice/data-protection/index_en.htm.

65. ΕΕΤΤ. Ετήσια έκθεση της ΕΕΤΤ προς την Ευρωπαϊκή Επιτροπή και το Σώμα Ευρωπαίων Ρυθμιστών Ηλεκτρονικών Επικοινωνιών (BEREC) για την εφαρμογή του Κανονισμού (ΕΕ) 2015/2120 σχετικά με την πρόσβαση στο ανοικτό διαδίκτυο για το διάστημα από 1/5/2017 – 30/4/2018. Ανεξάρτητη Αρχή. Αθήνα:, ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΤΑΧΥΔΡΟΜΕΙΩΝ; 2018.

66. Ceara T, McCaffery F. Data Security Overview for Medical Mobile Apps, Assuring the confidentiality,Integrity,and Availability of data in transmission. International Journal on Advances in Security. 2016 January ; 9(1942-2636): p. 146-157.

67. Mell , P.; Grance, T. The NIST Definition of Cloud Computing, Version 15. [The NIST definition of Cloud Computing, Special Publication 800-145].; 2009 [cited 2018 05 03]. Διαθέσιμο από: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

68. Τότσικα Δ. Η εξέλιξη στον υπολογισμό συννέφου. 2015. Διοίκηση επιχειρήσεων, τ.ε.ι. Δυτικής Ελλάδας.

69. ΕΔΕΤ. Εθνικό Δίκτυο Έρευνας & Τεχνολογίας. [Online]. [cited 2018 07 02]. Διαθέσιμο από: https://grnet.gr/health/.

70. Saraladevia B, Pazhanirajaa N, Paula V, Bashab SMS, Dhavacheivanc P. Big Data and Hadoop- A Study in Security Perspective. In 2nd International Symposium on Big Data and Cloud Computing; 2015.

71. Λερατάκη Δ. Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών κατά ISO27001:2013 – Υλοποίηση web εφαρμογής για audits. Π.Μ.Σ. "Τεχνο-οικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων". Πειραιάς: Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων; Φεβρουάριος 2016.

72. image. [google images. Risk Assessment overview according to The Australian/New Zealand standard AS/NZS]. [cited 2018 08 03]. Διαθέσιμο από:

https://goo.gl/images/w49Qx7.

73. Κοκολάκης Σ. Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας ΠΣ. In Ασφάλεια Πληροφοριακών Συστημάτων. Σάμος: Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου; 2004.

74. Susanto H, Nabil Almunawar , Chee Tuan. Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 05. 2011 October; 11(5): p. 23-29.

75. Veiga D, Eloff JHP. (A framework and assessment instrument for information security culture).

76. Theoharidou M, Kokolakis S, Karyda M, Kiountouzis E. The insider threat to information systems and the effectiveness of ISO 17799. Computers & Security. 2005 May 10; (24): p. 472-484.

77. Magklaras GB, Furnell SM. Insider Threat Prediction Tool: Evaluating the probability of IT misuse. Network Research Group, Department of Communication and electrical Engineering.

78. Van Niekerk , Von Solms. Information security culture : A management perspective. South Africa: Nelson Mandela Metropolitan University, Institute for information and communication technology advancement.

79. Albrechtsen E. A qualitative study of users' view on information security. Department of Industrial Economics and Technology Management ,N-7491.

80. EurLex, ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) αριθ. 910/2014, eIDAS Regulation. [Online].; 2014 [cited 2018 07 02]. Διαθέσιμο από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32014R0910&qid=1532866772825&from=EN.

81. EurLex. ΟΔΗΓΙΑ 1999/93/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές. [Online].; 1999 [cited 2018 07 03]. Διαθέσιμο από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31999L0093&qid=1532867104743&from=EN.

82. ΦΕΚ. (ΥΔΜΗΔ), Υπουργείο Διοικητικής Μεταρρύθμισης & Ηλεκτρονικής Διακυβέρνησης, ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 3979, Για την ηλεκτρονική διακυβέρνηση. [Online].; 2011 [cited 2018 08 02]. Διαθέσιμο από: http://www.minadmin.gov.gr/wp-content/uploads/20110616_FekA138_3979_2011.pdf.

83. Γκανάτσιος Δ. [Ηλεκτρονική αρχειοθέτηση Ηλεκτρονική αρχειοθέτηση και διακίνηση εγγράφων και διακίνηση εγγράφων με ηλεκτρονικά μέσα]. [cited 2018 07 02]. Διαθέσιμο από: https://free.openeclass.org/modules/document/file.php/IT231/%CE%A0%CE%91%CE%

A1%CE%9F%CE%A5%CE%A3%CE%99%CE%91%CE%A3%CE%95%CE%99%CE%A3/%CE%A0%CE%91%CE%A1%CE%9F%CE%A5%CE%A3%CE%99%CE%91%CE%A3%CE%97%201%CE%B7%CF%82%20%CE%B7%CE%BC%CE%AD%CF%81%CE%B1%CF%82.pdf.

84. Διαδικτυακή πύλη "Ερμής" ΑΠΕδ. [Εικ. Ψηφιακές Υπογραφές].; 2017 [cited 2018 08 02]. Διαθέσιμο από: http://www.aped.gov.gr/more/obtainsignature/4-step1.html.

85. Μπαλκούρας. ΣΤΕΓΑΝΟΓΡΑΦΙΑ ΨΗΦΙΑΚΩΝ ΕΙΚΟΝΩΝ. Ειδική Επιστημονική Εργασία. Πάτρα: πανεπιστήμιο; 2013.

86. Martuza A, al e. A comparative study on the currently existing intrusion detection systems. Sylhet,Bangladesh: Shahjalal University of Science & Technology, Rima Pal , Dept. of Computer Science & Engineering.

87. Solms Rv, Niekerk vJ. From information security to cybersecurity. Computers & Security. 2013; School of ICT,Nelson Mandella Metropolitan University,Port Elizabeth 6031. South Africa(38): p. 97-102.

88. Furnell S. Κυβερνοέγκλημα , καταστρέφοντας την κοινωνία της πληροφορίας, μετάφραση Φωτεινή Μηλιώνη. In. Αθήνα: εκδόσεις Παπαζήση; 2006. p. 26,28.

89. Cisco. [White Paper, Combating Cybercrime in the Healthcare Industry].; 2015 [cited 2018 07 06]. Διαθέσιμο από: pubs.cyberthoughts.org/cisco_Healthcare_Pharma_whitepaper.pdf.

90. Παππά Λ. Αξιοποίηση Τεχνολογιών Κοινωνικής Δικτύωσης από Ευάλωτες Κοινωνικές Ομάδε, το Φαινόμενο και οι διαστάσεις της βίας.. Μεταπτυχιακή εργασία, στο πρόγραμμα"Επιστήμη και Τεχνολογία Υπολογιστών". Πάτρα: Πολυτεχνική σχολή, πανεπιστήμιο Πατρών., Τμήμα Μηχανικών Η/Τ & Πληροφορικής ; 2012.

91. Namanya AP, Awan I, Cullen AJ, Diss JP. The World of Malware:"An Overview". In IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud); 2018; Barcelona, Spain. p. 420-427.

92. Ehrenfeld J. WannaCry, Cybersecurity and Health Information Technology: ATime to Act. J Med Syst. (2017) May 24; 41(104).

93. emsisoft. Διαθέσιμο από: https://goo.gl/images/W5fdkD.

94. ENISA. Selection of significant cyber-attacks in 2016. [Online].; 2016 [cited 2017 07 06]. Διαθέσιμο από: https://eur-lex.europa.eu/resource.html?uri=cellar:2413e286-985e-11e7-b92d-01aa75ed71a1.0001.02/DOC_2&format=PDF.

95. EuroLex, ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) αριθ. 910/2014, eIDAS Regulation. [Online].; 2014 [cited 2018 07 02]. Διαθέσιμο από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32014R0910&qid=1532866772825&from=EN.

96. ΦΕΚ. ΑΔΑΕ. Νόμος 3917/2011, διατήρηση δεδομένων. [Online].; 2011 [cited 2018 07 02]. Διαθέσιμο από: http://www.adae.gr/fileadmin/docs/nomoi/nomoi/Nomos__3917_2011_diatirisi_dedomenon.pdf.

97. ΑΠΔΠΧ. Πολλές σχετικές νομοθετικές διατάξεις. [Online].; 2011 [cited 2018 7 2]. Διαθέσιμο από: Διαθέσιμο : http://www.dpa.gr/portal/page?_pageid=33,123437&_dad=portal&_schema=PORTAL.

Εικόνες

Πίνακες