



**ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ  
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ  
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ  
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ  
ΚΑΤΕΥΘΥΝΣΗ**

**«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ,  
ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ  
ΠΡΟΣΟΜΟΙΩΣΗ»**

**ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ  
ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ – ΝΟΜΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗ**

**Γιοβανούλης Βασίλειος**

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

**Επιβλέπων Καθηγητής  
Αντωνής Κωνσταντίνος**

**Λαμία, Ιούνιος 2017**

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο «**Ασφάλεια προσωπικών δεδομένων στο διαδίκτυο και κυβερνοέγκλημα - Νομική αντιμετώπιση**» αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ

Γιοβανούλης Βασίλειος

6 Ιουνίου 2017

Υπογραφή

**ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ  
ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ – ΝΟΜΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗ**

### **Τριμελής Επιτροπή:**

Αντωνής Κωνσταντίνος, (επιβλέπων)

Σταμούλης Γεώργιος,

Λουκόπουλος Αθανάσιος.

### **ΕΥΧΑΡΙΣΤΙΕΣ**

Θα ήθελα να ευχαριστήσω πρωτίστως τον επιβλέποντα καθηγητή μου κ. Αντώνη Κωνσταντίνο για την αμέριστη συμπαράστασή του και την άρτια επιστημονική του συμβολή της παρούσας διατριβής.

Ιδιαίτερα ευχαριστώ τα παιδιά μου, που εκ όλων των άλλων, αποτελούν μια αέναη πηγή έμπνευσης για μένα.

Επίσης, ευχαριστώ τους καθηγητές μου αλλά και τους συναδέλφους συμφοιτητές μου για την υπέροχη διαδρομή από το ξεκίνημα των μεταπτυχιακών αυτών σπουδών μου μέχρι και την ολοκλήρωσή τους με τη μεταπτυχιακή τούτη διατριβή.

## **ΠΕΡΙΛΗΨΗ**

Η χρήση των Πληροφοριακών Συστημάτων συνεχώς αυξάνεται. Πλέον οι περισσότεροι οργανισμοί βασίζονται στην λειτουργία τους. Αχίλλειος πτέρνα αυτών είναι η ασφάλεια τους. Παράλληλα, η ραγδαία ανάπτυξη της τεχνολογίας της πληροφορικής και οι αυξημένες χάρη στην τεχνολογία δυνατότητες συλλογής, επεξεργασίας και ποικίλης χρήσης πληροφοριών που αφορούν το άτομο, συνεπάγονται κινδύνους για επεμβάσεις στην ιδιωτική ζωή του ατόμου. Μέθοδοι και

τεχνικές όπως τα cookies, δυναμιτίζουν την εφαρμοσιμότητα των κανόνων για διαφανή, θεμιτή και νόμιμη συλλογή προσωπικών δεδομένων. Στην παρούσα εργασία θα προσπαθήσουμε να αναπτύξουμε την έννοια των προσωπικών δεδομένων, τις προσβολές που αυτή δέχεται εντός του διαδικτύου και πως αυτή προστατεύεται από το ισχύον νομικό πλαίσιο. Στη συνέχεια, θα προσδιορίσουμε την έννοια του κυβερνοεγκλήματος και θα αναλύσουμε ορισμένες μορφές του όπως το spamming και την απάτη μέσω του internet banking. Επίσης, θα αναλύσουμε τα διάφορα είδη επιθέσεων σε πληροφοριακά συστήματα και τις τεχνικές με τις οποίες πραγματοποιούνται ενσύρματα και ασύρματα αλλά και τις δυνατότητες που διαθέτουμε για να τις αντιμετωπίσουμε σε τεχνικό επίπεδο. Τέλος, θα μελετήσουμε την πρόσφατη οδηγία της Ε.Ε 2016/1148 η οποία θέτει νέα δεδομένα για τη λήψη μέτρων σε διεθνές επίπεδο προκειμένου να θωρακιστεί η Ε.Ε από επιθέσεις στην ασφάλεια συστημάτων δικτύου και πληροφοριών.

## **ABSTRACT**

The applicability of information systems is rapidly increasing due to the need of the organizations and institutions to improve the effectiveness of their processes and operations. Even though the technology has reached a great level of automatization, human factor is still very important in creating information systems. For this reason, vulnerabilities of these systems might exist and as a result there is always the possibility that lack of safety issues arise. At the same time, the rapid development of

information technology (IT) with enhanced capabilities on data processing, handling and usage of personal information on individuals implies risk for interference in their private life. Methods and techniques such as “cookies” cancel the rules for transparent, fair and lawful collection of personal data. In this study, we present information relevant to personal data collection, different types of internet threats against sensitive personal information, as long as information on how people are protected by the current legal framework. Moreover, we define the concept of cybercrime and present certain types of it, such as spamming and fraud via internet banking. Also, we analyze the different types of wired and/or wireless attacks on information systems, and possible precautions against them at technical level. Finally, we review the recent EU Directive 2016/1148, which sets new standards for action at international level in order to protect the EU network security and information systems from potential cyber-attacks.

## **ΠΕΡΙΕΧΟΜΕΝΑ**

<b>ΕΥΧΑΡΙΣΤΙΕΣ.....</b>	<b>4</b>
<b>ΠΕΡΙΛΗΨΗ.....</b>	<b>5</b>
<b>ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ.....</b>	<b>7</b>

### **1. ΕΙΣΑΓΩΓΗ**

1.1 Ιστορική αναδρομή.....	11
1.2 Σκοπός.....	12
1.3 Βασικοί ορισμοί Ασφάλειας Προσωπικών Δεδομένων και Κυβερνοεγκλήματος.....	12

## 1. ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

1.1 Έννοια των προσωπικών δεδομένων και άλλες βασικές έννοιες του Ν.2472/1997.....	13
1.2 Γενικές Αρχές επεξεργασίας δεδομένων προσωπικού χαρακτήρα.....	19
1.3 Η συγκατάθεση του υποκειμένου των δεδομένων.....	24
1.4 Υποχρέωση γνωστοποίησης.....	27
1.5 Επεξεργασία των ευαίσθητων δεδομένων-λήψη άδειας.....	28
1.6 Απαλλαγή από τη υποχρέωση γνωστοποίησης ή λήψης άδειας.....	30
1.7 Απόρρητο των επικοινωνιών.....	31
1.8 Αρχεία cookies.....	32
1.9 Δεδομένα κίνησης και θέσης.....	34
1.10 Επιβολή κυρώσεων.....	36

## 2. ΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

2.1 Διακρίσεις - Συχνότερες μορφές.....	37
---	----

3.1.1			
Κυβερνοσφετερισμός.....	38		
3.1.2	Προστασία	Domain	
Names.....	38		
3.1.3	Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ν.2867/00).....		
38			
2.2	Διαφημίσεις μέσω του διαδικτύου, spamming.....	39	
2.3	Απάτη μέσω του διαδικτύου – Κίνδυνοι από τη χρήση του Internet Banking.....	40	
2.4	Εγκλήματα κατά της ηθικής και της αξιοπρέπειας - Προστασία ανηλίκων –Προστασία από παράνομο και βλαβερό περιεχόμενο.....	41	
3.	ΕΙΔΗ ΕΠΙΘΕΣΕΩΝ ΚΑΙ ΤΕΧΝΙΚΕΣ		
3.1	Επίθεση σε ιστοσελίδες.....	45	
3.2	Επίθεση στο ηλεκτρονικό ταχυδρομείο.....	45	
3.3	Επίθεση με εύρεση των κωδικών πρόσβασης.....	46	
3.4	Επίθεση με ωτακουστές (packet sniffers) .....	46	
3.5	Επίθεση με πλαστογράφηση της IPδιεύθυνσης (IP SPOOFING) .....	47	
3.6	Επίθεση με υπερχείλιση προσωρινής μνήμης.....	48	
3.7	Επίθεση μέσω άρνησης παροχής υπηρεσιών (DoS).....	48	
3.8	Επίθεση με «εχθρικό κώδικα».....	49	



#### 4. ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

4.1 Εισαγωγή.....	50
4.2 Χαρακτηριστικά των Ασύρματων δικτύων.....	50
4.3 Ευπάθειες και επιθέσεις κατά της ασφάλειας στα ασύρματα δίκτυα...	50
4.3.1 Επιθέσεις παράνομης χρήσης της ασύρματης επικοινωνίας.....	51
4.3.2 Επιθέσεις παρακολούθησης της κίνησης (Interception and Monitoring of Wireless Traffic) .....	52
4.3.3 Επιθέσεις παρεμβολής παρασίτων (jamming) .....	52
4.3.4 Επιθέσεις πελάτη προς πελάτη (client to client attacks).....	53
4.3.5 Επιθέσεις εναντίον των passwords στα Access Points (Brute Force Attacks Against Access Point Passwords) .....	53
4.3.6 Επιθέσεις εναντίον της κρυπτογράφησης (Attacks against Encryption).....	54
4.3.7 Έλλειψη κατάλληλων ρυθμίσεων (Misconfiguration).....	54
4.4 Μηχανισμοί ασφάλειας του προτύπου 802.11.....	54
4.5 Τεχνολογίες προστασίας ασυρμάτων δικτύων.....	55
4.5.1 Media Access Control (MAC) authentication.....	55
4.5.2 Ασφάλεια χρησιμοποιώντας το πρωτόκολλο EAP (Extensible Authentication Protocol) και το πρότυπο 802.1 X.....	55

4.5.3	RADIUS Authentication.....	57
4.5.4	Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network-VPN) .....	57
5.	METΡΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΕΠΙΘΕΣΕΩΝ	
5.1	Antivirus.....	60
5.2	Τείχη Προστασίας (Firewalls).....	61
5.2.1	Τύποι τειχών Προστασίας.....	63
5.2.1.1	Δρομολογητής Φιλτραρίσματος Πακέτων.....	64
5.2.1.2	Πύλες Επιπέδου Εφαρμογής.....	65
5.2.1.3	Πύλη Επιπέδου Κυκλώματος .....	66
5.3	Επάλξεις.....	66
5.4	Σύστημα Ανίχνευσης Επιθέσεων (IDS).....	68
5.5	Σύστημα Πρόληψης Επιθέσεων (IPS) .....	69
5.6	Μερικά σχετικά εργαλεία.....	70
5.7	Παραδείγματα χρήσης εφαρμογών.....	75
5.7.1	Tripewire.....	75
5.7.2	Nessus .....	77
6.	Η ΟΔΗΓΙΑ 2016/1148 ΤΗΣ Ε.Ε ΓΙΑ ΜΕΤΡΑ ΓΙΑ ΥΨΗΛΟ ΚΟΙΝΟ ΕΠΙΠΕΔΟ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΔΙΚΤΥΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ ΣΕ ΟΛΟΚΛΗΡΗ ΤΗΝ ΕΝΩΣΗ.	
6.1	Εισαγωγή.....	84
6.2	Αντικείμενο και πεδίο εφαρμογής.....	84
6.3	Εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών.....	85
6.4	Εθνικές αρμόδιες αρχές.....	86

6.5 Ομάδες συνεργασίας.....	87
6.6 Ασφάλεια συστημάτων δικτύου και πληροφοριών των φορέων εκμετάλλευσης βασικών υπηρεσιών.....	88
6.7 Ασφάλεια συστημάτων δικτύου και πληροφοριών των παρόχων ψηφιακών υπηρεσιών.....	90
6.8 Μεταφορά στο εθνικό δίκαιο.....	91
7. ΕΠΙΛΟΓΟΣ.....	91
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	93

## 1.ΕΙΣΑΓΩΓΗ

### 1.1 Ιστορική Αναδρομή

Το διαδίκτυο πριν από λίγα χρόνια είχε ένα πολύ μικρότερο εύρος συγκριτικά με σήμερα. Οι κόμβοι από τους οποίους απαρτιζόταν βρίσκονταν διασπαρμένοι σε κάποια ακαδημαϊκά ιδρύματα, σε ερευνητικά εργαστήρια και μεγάλες εταιρίες. Ως εκ τούτου, οι χρήστες του ήταν φοιτητές, ερευνητές και άνθρωποι που ασχολούνταν εξειδικευμένα με την επιστήμη και την τεχνολογία. Λόγω της περιορισμένης έκτασής του είχε σχεδιαστεί με τέτοιο τρόπο ώστε να εξυπηρετεί τις ανάγκες των χρηστών του χωρίς ιδιαίτερες ασφαλιστικές δικλίδες ή αποτρεπτικούς μηχανισμούς.

Όσο περνούν όμως τα χρόνια διαπιστώθηκε μια εκρηκτική ανάπτυξη του διαδικτύου που χαρακτηρίστηκε από την μετατροπή των καθημερινών κοινωνικών, πολιτιστικών και εμπορικών συναλλαγών του φυσικού κόσμου σε περιβάλλον ψηφιακό. Αυτό το φαινόμενο συμπεριέλαβε τόσο τις μεγάλες πολυεθνικές εταιρίες όσο και τους απλούς ιδιώτες – πολίτες.

Καθώς λοιπόν το μεγαλύτερο μέρος του αναπτυγμένου κόσμου χρησιμοποιεί πλέον σε καθημερινή βάση το διαδίκτυο για όλων των ειδών τις συναλλαγές του, η αξία της

πληροφορίας που συγκεντρώνεται αποκτά τεράστιες διαστάσεις. Σε κάποιες μάλιστα περιπτώσεις η πληροφορία αποθηκεύεται μόνο ψηφιακά, χωρίς να υπάρχει έντυπη ή αναλογική μορφή.

Κατά συνέπεια, δημιουργείται σταδιακά μια αυξημένη εξάρτηση του χρήστη (απλού ή εταιρικού – κρατικού) με τα υπολογιστικά συστήματα, γεγονός που υποβοηθείται από τη φιλικότητα που πλέον έχουν τα συστήματα αυτά. Η φιλικότητα καθώς και η πολυπλοκότητα των συστημάτων οδηγούν με τη σειρά τους σε πληθώρα αδυναμιών και προβλημάτων στην ασφάλειά τους. Οι χρήστες του διαδικτύου αν και έχουν ακουστά πολλές περιπτώσεις παραβίασης και κλοπής δεδομένων, δεν έχουν εκπαιδευτεί σε θέματα που αφορούν τη διαδικτυακή ασφάλεια, με αποτέλεσμα σε πολλές περιπτώσεις να έχουν την ψευδαίσθηση ότι τα δεδομένα τους είναι ασφαλή.

Σύμφωνα με την παγκόσμια Έρευνα Global Corporate IT Security Risks 2013, που πραγματοποιήθηκε από τη B2B International σε συνεργασία με την Kaspersky Lab, στην οποία έλαβαν μέρος και στελέχη του IT από την Ελλάδα, το 69% των Ελλήνων στελεχών που συμμετείχε, ανέφερε ότι οι εταιρείες τους δέχτηκαν επιθέσεις με διάφορα είδη κακόβουλων επιθέσεων (ο παγκόσμιος μέσος όρος ανέρχεται σε 66% για το 2013, έχοντας σημειώσει αύξηση σε σχέση με το 58% του 2012). Οι κακόβουλες επιθέσεις είναι στην πραγματικότητα ο Νο 1 λόγος πίσω από τις σοβαρές διαρροές εμπιστευτικών δεδομένων — το 22% των εταιρειών παγκοσμίως και το 21% των εταιρειών στην Ελλάδα ανέφεραν ότι έχουν υποστεί διαρροές δεδομένων έπειτα από τέτοιου είδους επιθέσεις. Τις περισσότερες φορές, αυτά τα περιστατικά σημειώνονται σε μικρού και μεσαίου μεγέθους επιχειρήσεις (23%), ενώ οι μεγάλες εταιρείες γίνονται στόχος των κακόβουλων επιθέσεων λιγότερο συχνά (17%).

## 1.2 Σκοπός

Στην παρούσα εργασία θα παρουσιάσουμε το βασικό νομικό πλαίσιο προστασίας των προσωπικών δεδομένων καθώς και αντίστοιχες οδηγίες της Ευρωπαϊκής Ένωσης σχετικά με την προστασία και επεξεργασία τους.

Επίσης, έχουμε σκοπό να προσδιορίσουμε την έννοια του κυβερνοεγκλήματος μέσα από τις διάφορες μορφές που αυτό εμφανίζεται καθώς και την αντιμετώπισή του από την ελληνική έννομη τάξη.

Στη συνέχεια, θα αναπτύξουμε διάφορα είδη επιθέσεων ενσύρματα και ασύρματα καθώς και τις δυνατότητες ασφάλειας και αντιμετώπισης τέτοιων επιθέσεων.

Τέλος, θα αναλύσουμε την πρόσφατη οδηγία της Ε.Ε για μέτρα επιδίωξης υψηλού κοινού επιπέδου ασφαλείας σε ολόκληρη την Ένωση.

### 1.3 Βασικοί ορισμοί Ασφάλειας Προσωπικών Δεδομένων και Κυβερνοεγκλήματος.

Προσωπικά δεδομένα είναι κάθε πληροφορία που αναφέρεται και περιγράφει ένα άτομο, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες. Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα ονομάζεται *υποκείμενο των δεδομένων*. Επεξεργασία των προσωπικών δεδομένων θεωρείται *κάθε εργασία που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα, όπως: συλλογή, καταχώριση, οργάνωση, διατήρηση ή αποθήκευση, τροποποίηση, εξαγωγή, χρήση, διαβίβαση, διάδοση, συσχέτιση ή συνδυασμός, διασύνδεση, δέσμευση, διαγραφή, καταστροφή*. Η επεξεργασία τους θεωρείται ασφαλής και σύννομη μόνο όταν το άτομο έχει δώσει την συγκατάθεσή του και κατ' εξαίρεση επιτρέπεται η επεξεργασία και χωρίς συγκατάθεση όταν συντρέχουν οι προϋποθέσεις που ορίζει ο Νόμος 2472/1997 στο άρθρο 5.

Ο όρος Ηλεκτρονικό έγκλημα<sup>1</sup> αποτελεί μια ευρεία έννοια στην οποία εμπίπτουν όλες εκείνες οι αξιόποινες πράξεις που τελούνται με τη χρήση ενός συστήματος ηλεκτρονικής επεξεργασίας δεδομένων. Ο όρος αυτός διακρίνεται σε στενή και σε ευρεία έννοια. Η εν στενή έννοια ηλεκτρονική εγκληματικότητα αναφέρεται στις αξιόποινες πράξεις όπως είναι η ηλεκτρονική απάτη, η χωρίς άδεια απόκτηση δεδομένων, η παραποίηση δεδομένων και η δολιοφθορά, δηλαδή εγκλήματα όπου ο ηλεκτρονικός υπολογιστής αποτελεί κύριο μέσο τέλεσης των εγκλημάτων. Αντίθετα, η εν ευρεία έννοια εγκληματικότητα μέσω Η/Υ περιλαμβάνει όλα εκείνα τα αδικήματα για την τέλεση των οποίων ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως βοηθητικό μέσο.

## 2. Ασφάλεια Προσωπικών Δεδομένων στο Διαδίκτυο

### 2.1 Έννοια των προσωπικών δεδομένων και άλλες βασικές έννοιες του Ν.2472/1997

<sup>1</sup> Χρίστος Μυλωνόπουλος, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο εκδόσεις Σάκκουλα, Αθήνα 2002

Ως δεδομένα προσωπικού χαρακτήρα<sup>2</sup> νοείται οποιαδήποτε πληροφορία αναφέρεται στο υποκείμενο των δεδομένων, σε ατομικά ορισμένο δηλαδή φυσικό πρόσωπο και του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα.

Προσωπικά δεδομένα είναι μεταξύ άλλων, προσωπικά στοιχεία όπως στοιχεία από το ληξιαρχείο, στοιχεία ταυτότητας, φυσικά χαρακτηριστικά, συνήθειες, ενδιαφέροντα, στοιχεία οικογενειακής κατάστασης, δεδομένα εκπαίδευσης και επαγγελματικής εξειδίκευσης, πάσης φύσεως οικονομικά δεδομένα, εργασιακά στοιχεία κ.λ.π.<sup>3</sup> Δε λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία που συλλέχθηκαν στο πλαίσιο στατιστικής έρευνας, από τα οποία δε μπορούν πλέον να προσδιοριστούν τα υποκείμενα των δεδομένων. Δηλαδή, δεδομένα προσωπικού χαρακτήρα, αν «ανωνυμοποιηθούν» και δεν εξατομικεύουν πλέον το φυσικό πρόσωπο στο οποίο αναφέρονται, δεν απασχολούν το νόμο. Σε κάθε περίπτωση δεδομένα προσωπικού χαρακτήρα αποτελούν στοιχεία καταγεγραμμένα και όχι προφορικά που αναφέρονται σε φυσικό πρόσωπο. Ξεχωριστή κατηγορία αποτελούν τα λεγόμενα ευαίσθητα δεδομένα, δηλαδή τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία (φυσική ή πνευματική κατάσταση), την κοινωνική πρόνοια και την ερωτική ζωή, τα σχετικά με ποινικές διώξεις ή καταδίκες. Τα ευαίσθητα δεδομένα αποτελούν το σκληρό πυρήνα της ιδιωτικής ζωής. Η αναφορά δεν είναι απαραίτητο να είναι ατομική, μπορεί να συμπεραίνεται απλώς ότι οι πληροφορίες αφορούν ένα συγκεκριμένο πρόσωπο.

Αρχείο δεδομένων προσωπικού χαρακτήρα, σύμφωνα με το άρθρο 2 στοιχ. ε'62 του ν. 2472/97, είναι «κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία είναι προσιτά με γνώμονα συγκεκριμένα κριτήρια». Το αρχείο στην υπολογιστική του μορφή (data file), προκάλεσε τη δημιουργία του δικαίου προστασίας των δεδομένων προσωπικού χαρακτήρα. Κάθε συλλογή, σε οποιοδήποτε μέσο, οπωσδήποτε περισσότερων από δύο δεδομένων προσωπικού χαρακτήρα αποτελεί αρχείο. «Υποκείμενο των δεδομένων», σύμφωνα με το νόμο (άρθρο 2 στοιχ. γ'), δε μπορεί να είναι μόνο φυσικό πρόσωπο, στο οποίο αναφέρονται τα δεδομένα, και μάλιστα ατομικά ορισμένο ή οριστό, δηλαδή η ταυτότητα του οποίου μπορεί να εξακριβωθεί άμεσα ή έμμεσα «ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από

<sup>2</sup> Βλ. Ευγενία Αλεξανδροπούλου – Αιγυπτιάδου «Προσωπικά Δεδομένα», εκδόσεις Σάκκουλα, Αθήνα 2007

<sup>3</sup> Βλ. <http://www.dpa.gr>, Ιστότοπος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

άποψη βιολογική, ψυχική, οικονομική, πολιτιστική ή κοινωνική». Με τον όρο επεξεργασία δεδομένων προσωπικού χαρακτήρα (άρθρο 2 στοιχ. δ), νοείται «κάθε εργασία ή σειρά εργασιών που πραγματοποιείται από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων που χρησιμοποιείται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώρηση, η οργάνωση, η διατήρηση ή η αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή και η καταστροφή». Η ανωτέρω απαρίθμηση είναι ενδεικτική καθώς μπορεί να περιλαμβάνει και άλλες εργασίες, όπως π.χ. τη δημοσιοποίηση ή την ανακοίνωση των δεδομένων στο internet. Οι παραπάνω εργασίες που συνιστούν την «επεξεργασία» κατά την έννοια του νόμου διακρίνονται σε τρία στάδια<sup>4</sup>. Το πρώτο στάδιο αφορά στη συλλογή ή καταχώριση ( τα δεδομένα στο στάδιο αυτό συλλέγονται ατομικά, ανεξαρτήτως της οργάνωσής τους σε αρχείο ή όχι) των δεδομένων προσωπικού χαρακτήρα, το δεύτερο στάδιο περιλαμβάνει τις εργασίες που αφορούν αυτή καθ' αυτή την επεξεργασία, όπως π.χ. η οργάνωση, η διατήρηση ή η αποθήκευση, η τροποποίηση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η διαγραφή και η καταστροφή των δεδομένων, ενώ το τρίτο στάδιο αφορά στη χρήση των αποτελεσμάτων του προηγούμενου σταδίου, όπως την εξαγωγή, τη διαβίβαση ή την κάθε άλλης μορφής διάθεση. Τα πρόσωπα στα οποία αναφέρονται οι ρυθμίσεις του νόμου είναι τα ακόλουθα :

- υπεύθυνος επεξεργασίας,
- ο εκτελών την επεξεργασία,
- ο τρίτος, και
- ο αποδέκτης.

«Υπεύθυνος επεξεργασίας» ( άρθρο 2 στοιχ. ζ εδ. α' ) είναι οποιοσδήποτε καθορίζει το σκοπό - το επιδιωκόμενο αποτέλεσμα ( ανεξαρτήτως της μεθόδου που θα χρησιμοποιηθεί) και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και είναι ο κύριος πρωταγωνιστής του δικαίου προστασίας δεδομένων προσωπικού χαρακτήρα. Όταν ο σκοπός και ο τρόπος επεξεργασίας καθορίζονται με διατάξεις νόμου ή κανονιστικές διατάξεις εθνικού ή κοινοτικού δικαίου, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια βάσει του οποίου γίνεται η επιλογή του, καθορίζονται αντίστοιχα από το εθνικό ή το κοινοτικό δίκαιο. Ο τρόπος της επεξεργασίας προϋποθέτει τεχνική γνώση, οπότε ο υπεύθυνος επεξεργασίας καλείται

<sup>4</sup> Βλ Ε. Παπακωνσταντίνου, Νομικά θέματα πληροφορικής, εκδόσεις Σάκκουλα, Αθήνα-Θεσ/νικη, 2006

να γνωρίζει τις ειδικότερες περιστάσεις της επεξεργασίας. Ως **«εκτελών την επεξεργασία»** ( άρθρο 2 στοιχ. η) ορίζεται αυτός που δεν επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για δικό του λογαριασμό, αλλά για λογαριασμό του υπευθύνου επεξεργασίας. Η διάκριση αυτή μεταξύ εκτελούντος και υπεύθυνου επεξεργασίας, συναντάται στις περιπτώσεις outsourcing, στις περιπτώσεις δηλ. που οργανισμοί αποφασίζουν να αναθέσουν σε τρίτους τη διενέργεια συγκεκριμένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που ήδη κατέχουν, επειδή δεν διαθέτουν οι ίδιοι την απαραίτητη τεχνογνωσία ή για λόγους μείωσης του κόστους. Είναι ένα απλό όργανο της επεξεργασίας χωρίς δική του κρίση ή δυνατότητα απόφασης. Πρέπει όμως να είναι πρόσωπο με αντίστοιχα επαγγελματικά προσόντα που παρέχει επαρκείς εγγυήσεις από πλευράς γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου. Η έννομη σχέση που μπορεί να συνδέει τον υπεύθυνο επεξεργασίας και τον εκτελούντα αυτήν μπορεί είναι η σύμβαση έργου, εντολής κλπ, πάντως ο εκτελών την επεξεργασία θα πρέπει να βρίσκεται υπό την άμεση εποπτεία του υπεύθυνου. **«Τρίτος»**, σύμφωνα με το νόμο ( άρθρο 2 στοιχ. θ) αλλά και το άρθρο 2 της Οδηγίας, είναι κάθε πρόσωπο φυσικό ή νομικό, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός το οποίο εμπλέκεται σε επεξεργασία δεδομένων προσωπικού χαρακτήρα από την πλευρά των διενεργούντων την επεξεργασία, χωρίς να είναι όμως ο ίδιος ούτε υπεύθυνος επεξεργασίας ούτε εκτελών την επεξεργασία. Ο τρίτος απαραίτητως τελεί υπό την άμεση εποπτεία ή ενεργεί για λογαριασμό του υπεύθυνου επεξεργασίας, δεν είναι όμως, όπως είπαμε και ο εκτελών την επεξεργασία. Ως **«αποδέκτης»** κατά την έννοια του νόμου, νοείται το φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός στον οποίο ανακοινώνονται ή μεταδίδονται τα δεδομένα, ανεξαρτήτως αν πρόκειται για τρίτο ή όχι. Αποδέκτης δηλαδή είναι ο λήπτης των αποτελεσμάτων της επεξεργασίας, αρκεί να έχει προηγηθεί στο πρόσωπό του η ανακοίνωση ή η μετάδοση των δεδομένων, χωρίς να είναι απαραίτητο να έχει προλάβει να τα αποθηκεύσει ή να τα καταγράψει.

Στο άρθρο 2 του νόμου 3471/2006, δίνονται οι ορισμοί κάποιων βασικών εννοιών, οι ακόλουθοι: Στο άρθρο 2 παρ. 1 ορίζεται ως **συνδρομητής** , κάθε φυσικό ή νομικό πρόσωπο που έχει συνάψει σύμβαση με φορέα παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, για την παροχή των υπηρεσιών αυτών. Ως **χρήστης** αναφέρεται το φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας ( άρθρο 2 παρ 2). Στο



νόμο 3471/2006 οι όροι συνδρομητής ή χρήστης χρησιμοποιούνται με τον ίδιο τρόπο που ο ν. 2472/97 χρησιμοποιεί τον όρο **υποκείμενο. Πάροχος**<sup>5</sup>, λέγεται για λόγους συντομίας ο φορέας παροχής δημοσίου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Ο υπεύθυνος επεξεργασίας μπορεί να είναι πρόσωπο διαφορετικό από τον πάροχο. **Δεδομένα κίνησης** ορίζονται τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή χρέωσής της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων και μεταξύ άλλων το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία ( άρθρο 2 παρ.3). **Δεδομένα θέσης** είναι τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών ( άρθρο 2 παρ.4). Στην έννοια των δεδομένων προσωπικού χαρακτήρα εδώ εντάσσονται τόσο τα δεδομένα κίνησης όσο και τα δεδομένα θέσης. Ως **επικοινωνία**, νοείται κάθε πληροφορία που ανταλλάσσεται ή διαβιβάζεται μεταξύ ενός πεπερασμένου αριθμού μερών, μέσω μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών (άρθρο 2 παρ.5). **Ηλεκτρονικό ταχυδρομείο**, σύμφωνα με το άρθρο 2 παρ.8, αποτελεί κάθε μήνυμα με κείμενο, φωνή, ήχο ή εικόνα που αποστέλλεται μέσω δημοσίου δικτύου επικοινωνιών, το οποίο μπορεί να αποθηκεύεται στο δίκτυο ή στον τερματικό εξοπλισμό του παραλήπτη, έως ότου ληφθεί από τον παραλήπτη.

Οι ρυθμίσεις του ν. 2472/97, σύμφωνα με το άρθρο 3 παρ. 1 του νόμου, βρίσκουν εφαρμογή σε κάθε είδους επεξεργασία δεδομένων, τόσο σε αυτοματοποιημένη όσο και σε μη, δηλαδή επεξεργασία με συμβατικές μεθόδους, στον ιδιωτικό και στο δημόσιο τομέα. Επομένως, πρέπει να τονιστεί ότι η γενική νομοθεσία για την προστασία των προσωπικών δεδομένων, δηλαδή ο ν. 2472/1997, ισχύει και εφαρμόζεται και στη συλλογή και επεξεργασία προσωπικών δεδομένων στο περιβάλλον του διαδικτύου, καθώς οι σχετικές διατάξεις εφαρμόζονται για κάθε επεξεργασία εν γένει- με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων.

Αυτοματοποιημένη<sup>6</sup> είναι η επεξεργασία που πραγματοποιείται σε υπολογιστικό

<sup>5</sup> Α.Φραγκούλη, Προστασία Δεδομένων στο Διαδίκτυο, εις συλλογικόν έργον Εφαρμογές Εμπορικού Δικαίου, Επιμέλεια Γ Τριανταφυλλάκη, Νομική Βιβλιοθήκη 2007

<sup>6</sup> Ιωάννης Δ. Ιγγλεζάκης, Εισαγωγή στο δίκαιο της Πληροφορικής, εκδόσεις Σάκκουλα Αθήνα-Θεσσαλονίκη, 2006

περιβάλλον. Ο νομοθέτης, ωστόσο, επέλεξε να διευρύνει το πεδίο εφαρμογής του νόμου και ως αυτοματοποιημένη επεξεργασία θεωρείται και οποιαδήποτε άλλη επεξεργασία τελείται με ηλεκτρονικά - αυτόματης λειτουργίας μέσα, όπως π.χ. η προβολή τηλεοπτικής εκπομπής, η αναπαραγωγή ηχογραφημάτων ή ψηφιακών φωτογραφιών κλπ. Μη αυτοματοποιημένη επεξεργασία είναι η επεξεργασία που πραγματοποιείται «δια χειρός» και με οποιονδήποτε άλλο τρόπο που δεν την καθιστά αυτοματοποιημένη. Ο νόμος, στις περιπτώσεις μη αυτοματοποιημένης επεξεργασίας, απαιτεί την οργάνωση των δεδομένων σε αρχείο, με την έννοια που αναφέρθηκε παραπάνω. Αντίθετα, στην αυτοματοποιημένη επεξεργασία δεδομένων, ο νόμος εφαρμόζεται τόσο σε ένα μοναδικό προσωπικό δεδομένο (π.χ. ένα έγγραφο word ή μια φωτογραφία) όσο και σε εκατομμύρια αυτών, οργανωμένα σε βάσεις δεδομένων. Γίνεται δεκτό ότι η επεξεργασία δεδομένων στο διαδίκτυο αποτελεί κατά κανόνα αυτοματοποιημένη επεξεργασία δεδομένων και άρα παρέλκει η εξέταση αν υπάρχει αρχείο.

Εξαίρεση από το πεδίο εφαρμογής του νόμου αποτελεί η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία πραγματοποιείται από φυσικό πρόσωπο για την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών ή οικιακών ( άρθρο 3 παρ. 2 ν. 2472/97). Προσωπικές ή οικιακές δραστηριότητες είναι εκείνες στις οποίες απουσιάζει το στοιχείο της εξωτερίκευσης και η χρήση τους γίνεται από το άτομο για σκοπούς μη εμπορικούς, όπως π.χ. η τήρηση οικιακών λογαριασμών, άλμπουμ φωτογραφιών, τήρηση τηλεφωνικού καταλόγου, όχι όμως και η ανάρτηση των παραπάνω στοιχείων στην προσωπική ιστοσελίδα του κατόχου τους. Στην περίπτωση αυτή δεν εφαρμόζεται καθόλου ο νόμος. Οι ρυθμίσεις αυτές του νόμου αφορούν μόνο τα φυσικά πρόσωπα, με συνέπεια να εξαιρούνται τα νομικά πρόσωπα από το πεδίο εφαρμογής του ( άρθρο 1 και 2 περ.γ'). Όσον αφορά στο εφαρμοστέο δίκαιο, σύμφωνα με το άρθρο 3 παρ.3 ν.2472/1997, ο νόμος εφαρμόζεται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα όταν αυτή εκτελείται είτε: α) από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, εγκατεστημένο στην Ελληνική Επικράτεια ή σε τόπο, όπου εφαρμόζεται σύμφωνα με το δημόσιο διεθνές δίκαιο το ελληνικό δίκαιο, β) είτε από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην επικράτεια κράτους - μέλους της Ευρωπαϊκής Ένωσης ή κράτους του Ευρωπαϊκού Οικονομικού χώρου, αλλά τρίτης χώρας, και για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προσφεύγει σε μέσα, αυτοματοποιημένα ή όχι, εκτός αν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη

διέλευση από την Ελλάδα. Δηλαδή, στην τελευταία αυτή περίπτωση, αν ο υπεύθυνος επεξεργασίας εκτός ΕΕ, επεξεργάζεται δεδομένα προσωπικού χαρακτήρα με μέσα που βρίσκονται στην Ελλάδα, ανεξαρτήτως αν τα δεδομένα αυτά αφορούν σε

κατοίκους της χώρας ή αν ο ίδιος ο εκτελών την επεξεργασία είναι εγκατεστημένος στην Ελλάδα, τότε και πάλι εφαρμόζεται το ελληνικό δίκαιο. Στην τελευταία αυτή περίπτωση ο υπεύθυνος επεξεργασίας οφείλει να υποδείξει με γραπτή δήλωσή του προς την αρχή, εκπρόσωπο εγκατεστημένο στην Ελληνική Επικράτεια, ο οποίος υποκαθίσταται στα δικαιώματα και τις υποχρεώσεις του υπεύθυνου, χωρίς ο τελευταίος αυτός να απαλλάσσεται από τυχόν ιδιαίτερη ευθύνη του. Το ίδιο ισχύει όταν ο υπεύθυνος επεξεργασίας καλύπτεται από ετεροδικία, ασυλία ή άλλο λόγο που κωλύει την ποινική δίωξη. Η παραπάνω ρύθμιση αναφέρεται κυρίως στον τόπο εγκατάστασης του υπεύθυνου επεξεργασίας, δηλαδή στον τόπο πραγματικής άσκησης δραστηριότητας μέσω μόνιμου καταστήματος και επομένως δεν ενδιαφέρει η έδρα του νομικού προσώπου της επιχείρησης που επεξεργάζεται προσωπικά δεδομένα.

Ο Ν. 3471/2006, όπως προαναφέραμε, αποτελεί πράξη προσαρμογής της ελληνικής νομοθεσίας στην κοινοτική Οδηγία 2002/58/EK, η οποία μάλιστα έχει εν μέρει τροποποιηθεί από την πρόσφατη Οδηγία 2006/24/EK για τη διατήρηση των δεδομένων που υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών. Ο Ν. 3471/2006, λοιπόν, βρίσκει εφαρμογή κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών, στο πλαίσιο της παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών ( άρθρο 3 παρ. 1 εδαφ β). Εδώ υπάγεται ένα σύνολο υπηρεσιών, μεταξύ των οποίων και οι υπηρεσίες που παρέχονται μέσω διαδικτύου, όσες παρέχονται μέσω κινητών ψηφιακών δικτύων κλπ.

Σε αντίθεση με το Ν.2472/97, ο Ν. 3471/2006 εφαρμόζεται και όταν ακόμη συνδρομητές είναι νομικά πρόσωπα. Αξίζει να αναφερθεί ότι οι διατάξεις που αφορούν την προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα δεν παρουσιάζουν αυτοτέλεια, αλλά εντάσσονται στο γενικότερο πλαίσιο των ρυθμίσεων του ν 2472/97. Συνεπώς, κύριο κορμό της προστασίας προσωπικών δεδομένων και στο περιβάλλον του διαδικτύου αποτελεί η γενική νομοθεσία για την προστασία των προσωπικών δεδομένων ,δηλαδή ο Ν. 2472/97, ενώ ο Ν.3471/2006 ισχύει παράλληλα και εφαρμόζεται εισάγοντας και ειδικότερες ρυθμίσεις. Οι

διατάξεις του Ν. 2472/1997 εφαρμόζονται σε κάθε ζήτημα που δε ρυθμίζεται ειδικότερα από το νόμο 3471/2006, σύμφωνα με το άρθρο 3 παρ2 του ν. 3471/2006.

## **2.2 Γενικές Αρχές επεξεργασίας δεδομένων προσωπικού χαρακτήρα**

Στο άρθρο 4 του ν. 2472/97 περιέχονται οι γενικές αρχές που αποτελούν βασική προϋπόθεση για την διαφύλαξη της νομιμότητας της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, ενώ στο σύνολό τους σχεδόν, όπως θα παρουσιαστεί και παρακάτω, οι αρχές αυτές αναφέρονται αποκλειστικά στο υπολογιστικό περιβάλλον, με εξαίρεση τις αρχές της νόμιμης και θεμιτής συλλογής και επεξεργασίας που πράγματι προστατεύουν και την ιδιωτική ζωή. Οι αρχές αυτές ισχύουν και για την επεξεργασία στο περιβάλλον του διαδικτύου, ενώ ορισμένες από αυτές επαναλαμβάνονται και εξειδικεύονται περαιτέρω και από το Ν. 3471/2006.

- Η αρχή της συλλογής με νόμιμο και θεμιτό τρόπο : Θεμελιώδης αρχή κατά το στάδιο της συλλογής των δεδομένων προσωπικού χαρακτήρα αποτελεί η προϋπόθεση του νόμου (άρθρο 4 παρ. 1 εδαφ. α' ν.2472/97) να συλλέγονται κατά τρόπο νόμιμο και θεμιτό. Νόμιμος είναι ο τρόπος συλλογής που γίνεται σύμφωνα με τις διατάξεις του ίδιου του νόμου περί προστασίας προσωπικών δεδομένων, αλλά και όταν η συλλογή δεν προσκρούει σε άλλη διάταξη νόμου της κείμενης νομοθεσίας (π.χ. δε συνιστά αδικοπραξία). Η συλλογή και η οποιαδήποτε επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι θεμιτές μόνο εφόσον πραγματοποιούνται για ένα συγκεκριμένο νόμιμο σκοπό, τον οποίο γνωρίζει και αποδέχεται το υποκείμενο των δεδομένων, ο οποίος καθορίζει το είδος της νόμιμης επεξεργασίας και τη χρονική διάρκεια της θεμιτής δυνατότητας επεξεργασίας. Αθέμιτη είναι η συλλογή όταν, να μεν δεν παραβιάζεται καμία διάταξη νόμου, ωστόσο γίνεται με ενέργειες ιδιαίτερης κοινωνικής απαξίας. Έχει κριθεί παράνομη η συλλογή ηλεκτρονικών διευθύνσεων και κωδικών πρόσβασης συνδρομητών της otenet χωρίς τη συγκατάθεσή τους, καθώς παραβιάζει τα άρθρα 4 και 5 του Ν.2472/9785 ή η συλλογή δεδομένων από μητέρες που μόλις γέννησαν σε χώρους μαιευτηρίων.
- Η αρχή της δεσμευτικότητας του σκοπού : Σύμφωνα με το άρθρο 4 παρ. 1 περ. α' ν.2472/97, προκειμένου τα δεδομένα προσωπικού χαρακτήρα να τύχουν νόμιμης επεξεργασίας πρέπει να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς. Η αρχή αυτή είναι επίσης θεμελιώδους σημασίας στο δίκαιο προστασίας δεδομένων προσωπικού χαρακτήρα, καθώς σύμφωνα με αυτήν οι επιδιωκόμενοι με την επεξεργασία στόχοι, πρέπει να

καθορίζονται ήδη κατά τη συλλογή των προσωπικών δεδομένων, προκειμένου να παρασχεθεί στη συνέχεια η δυνατότητα στον ενδιαφερόμενο να παρέχει τη συγκατάθεσή του. Καθορισμένοι είναι οι σκοποί οι οποίοι δηλώνονται στα πρόσωπα κατά το στάδιο συλλογής των δεδομένων προσωπικού χαρακτήρα που τα αφορούν, χρειάζεται δηλαδή η εξωτερίκευσή τους στο άτομο κατά το στάδιο της συλλογής. Σαφείς είναι οι σκοποί που δε δημιουργούν αμφιβολίες στο άτομο ως προς το περιεχόμενό τους. Την αρχή του σκοπού, εξειδικεύει περαιτέρω και ο Ν. 3471/2006 στο άρθρο 5 παρ. 1, σύμφωνα με το οποίο η επεξεργασία δεδομένων προσωπικού χαρακτήρα, περιλαμβανομένων και των δεδομένων κίνησης και θέσης, πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των σκοπών της, ενώ στο άρθρο 5 παρ. 4 ορίζεται ότι ο πάροχος δεν επιτρέπεται να χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα και τα δεδομένα κίνησης και θέσης ή να τα διαβιβάζει σε τρίτους για άλλους σκοπούς, εκτός αν ο συνδρομητής ή ο χρήστης έχει ρητά και ειδικά δώσει τη συγκατάθεσή του. Απαγορεύεται δηλαδή από το νόμο η τυχαία συλλογή δεδομένων προσωπικού χαρακτήρα για την περίπτωση που «χρειαστούν» στο μέλλον, για τυχόν δηλαδή μελλοντική χρήση. Η αρχή της δεσμευτικότητας του σκοπού αφαιρεί από το σύγχρονο marketing την πρόσβαση σε απεριόριστο αριθμό δεδομένων προσωπικού χαρακτήρα, ώστε να προβαίνει σε όποιες επεξεργασίες επιθυμεί για την επίτευξη καλύτερων πωλήσεων. Συγκεντρωτικές ενέργειες συλλογής δεδομένων, χωρίς εξαρχής καθορισμένο σκοπό, παρά μόνο για να υπάρχουν αποθηκευμένα στο σύστημα δεν επιτρέπεται. Αποκλείονται επομένως οι τεχνικές τύπου data mining (εξόρυξης δεδομένων) για δεδομένα προσωπικού χαρακτήρα, αφού η ίδια η φύση τους (εξόρυξη δεδομένων από διαφορετικές βάσεις δεδομένων) δε συμφωνεί με την αρχή της δεσμευτικότητας του σκοπού. Συνεπώς τα δεδομένα που συλλέγονται από την εκτέλεση μιας σύμβασης on-line δεν επιτρέπεται να χρησιμοποιηθούν για άλλους σκοπούς, όπως π.χ για τις ανάγκες ενός διαφημιστικού marketing (αποστολή διαφημιστικών μηνυμάτων ή διαφημιστικών φυλλαδίων), χωρίς την ύπαρξη συγκατάθεσης του υποκειμένου των δεδομένων.

- Η αρχή της επεξεργασίας με νόμιμο και θεμιτό τρόπο :Η επεξεργασία, όπως και η συλλογή των δεδομένων προσωπικού χαρακτήρα, θα πρέπει να είναι νόμιμη και θεμιτή (άρθρο 4 παρ. 1 περ. α' ν.2472/97). Νόμιμη είναι η επεξεργασία όταν ακολουθούνται κατά την οργάνωση και την εκτέλεσή της οι

διατάξεις του δικαίου για την προστασία δεδομένων προσωπικού χαρακτήρα, ενώ η σχετική κρίση είναι αναπόφευκτα τεχνική, εξετάζεται δηλαδή ο αλγόριθμος ή η οργάνωση των ερωτημάτων ή των επεξεργασιών σε μια βάση δεδομένων προκειμένου να διαπιστωθεί η τήρηση των προϋποθέσεων του νόμου. Αθέμιτη είναι η επεξεργασία που συνίσταται σε ενέργειες με ιδιαίτερη κοινωνική απαξία.

- Η αρχή της συνάφειας των δεδομένων : Σύμφωνα με την αρχή αυτή τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει να είναι πρόσφορα και όχι περισσότερα από όσα κάθε φορά απαιτείται ενόψει των σκοπών της επεξεργασίας (άρθρο 4 παρ. 1 περ. β' ν.2472/97). Η αρχή της δεσμευτικότητας του σκοπού και η αρχή της συνάφειας, όπως είναι φανερό είναι αλληλένδετες. Ο δηλωμένος σκοπός της επεξεργασίας επηρεάζει και την «ποσότητα» των δεδομένων προσωπικού χαρακτήρα που θα τύχουν επεξεργασίας. «Συναφή» είναι τα δεδομένα τα οποία ανταποκρίνονται στο περιεχόμενο των σκοπών μιας επεξεργασίας ( για παράδειγμα σε μια επεξεργασία με σκοπό την αποστολή διαφημιστικών φυλλαδίων απορρυπαντικών δεν τυγχάνουν επεξεργασίας και δεδομένα σχετικά με την οικογενειακή κατάσταση). «Πρόσφορα» θα είναι τα δεδομένα προσωπικού χαρακτήρα όταν το είδος τους είναι κατάλληλο για την πραγματοποίηση των σκοπών μιας επεξεργασίας, ενώ η σχετική κρίση είναι τεχνικού χαρακτήρα. Κρίνεται δηλαδή ποια ακριβώς δεδομένα είναι τα κατάλληλα που θα πρέπει να τύχουν επεξεργασίας, προκειμένου να επιτευχθεί ο συγκεκριμένος κάθε φορά σκοπός.
- Η αρχή της ποιότητας των δεδομένων : Σύμφωνα με την αρχή αυτή (βλ. άρθρο 4 παρ 1 στοιχ. γ του Ν. 2472/97), τα δεδομένα προσωπικού χαρακτήρα προκειμένου να τύχουν νόμιμης επεξεργασίας θα πρέπει να είναι ακριβή και να υποβάλλονται σε ενημέρωση. Η υποχρέωση ενημέρωσης είναι αυτονόητη, εφόσον αφορά σε δεδομένα προσωπικού χαρακτήρα, όπως ονόματα, τηλέφωνα, δεδομένα υγείας, διευθύνσεις κλπ. Η υποχρέωση αυτή του υπεύθυνου επεξεργασίας εμφανίζεται και ως η μόνη αρχή η οποία φαίνεται να προστατεύει και τα δικά του συμφέροντα, αφού κανείς δεν θα επιθυμούσε να κατέχει και να χρησιμοποιεί παρωχημένα δεδομένα προσωπικού χαρακτήρα, καθώς όχι μόνο δε βοηθούν τους σκοπούς του, αλλά μπορεί να αποβούν και επιζήμια για τον ίδιο (π.χ. αποστολή διαφημιστικών φυλλαδίων σε λάθος

διευθύνσεις ή σε πρόσωπα που δε βρίσκονται πια στη ζωή ή πρόσωπα που εμφανίζουν συνωνυμία).

- Η αρχή της πεπερασμένης διατήρησης των δεδομένων : Σύμφωνα με την αρχή αυτή (άρθρο 4 παρ 1 στοιχ. δ του Ν. 2472/97), «τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής, για την πραγματοποίηση των σκοπών της συλλογής και της επεξεργασίας τους». Παρά τη σχετικά προβληματική διατύπωση της αρχής στο νόμο, η αρχή αυτή επιβάλλει τα δεδομένα προσωπικού χαρακτήρα να διατηρούνται στο σύστημα του υπεύθυνου επεξεργασίας μόνο για όσο χρόνο απαιτείται για την πραγματοποίηση των σκοπών της επεξεργασίας. Μετά την παρέλευση του διαστήματος αυτού τα δεδομένα πρέπει να διαγράφονται από το σύστημα, εκτός αν η Αρχή εκδώσει αιτιολογημένη απόφαση με την οποία να επιτρέπει τη διατήρησή τους για λόγους ιστορικούς, στατιστικούς ή επιστημονικούς και εφόσον δε θίγονται τα δικαιώματα των υποκειμένων ή τρίτων. Επιπλέον, η διάταξη του άρθρου 6 παρ 1 του Ν. 3471/2006 ορίζει ότι τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τον φορέα παροχής δημοσίου δικτύου ή και διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών υπηρεσιών, πρέπει να απαλείφονται ή να καθίστανται ανώνυμα κατά τη λήξη της επικοινωνίας με κατάλληλη κωδικοποίηση.
- Η αρχή του απορρήτου της επεξεργασίας : Σύμφωνα με το άρθρο 10 παρ. 1 του Ν. 2472/97, «η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη. Διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνο κατ' εντολή του». Η αρχή αυτή αποτελεί ρητή εντολή, επισήμανση προς τα πρόσωπα που αναλαμβάνουν την επεξεργασία, να προσέξουν ώστε τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζονται να μην πέσουν σε χέρια μη εξουσιοδοτημένων τρίτων. Απόρρητη είναι η επεξεργασία όταν δεν ανακοινώνεται σε τρίτα πρόσωπα, μη συμμετέχοντα στη διαδικασία της. Στο άρθρο 4 του νόμου 3471/2006 ρυθμίζεται αναλυτικά το απόρρητο των επικοινωνιών, όπως θα εξετάσουμε διεξοδικότερα και παρακάτω.
- Η Αρχή της ασφάλειας των δεδομένων : Σύμφωνα με την αρχή αυτή ο υπεύθυνος επεξεργασίας υποχρεούται( άρθρο 10 παρ 3, εδ α' Ν. 2472/97): «

να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας». Σε περίπτωση λοιπόν παράνομης επεξεργασίας σε αρχείο δεδομένων προσωπικού χαρακτήρα, ευθύνες δε φέρει μόνο αυτός που τη διενεργεί, αλλά πιθανότατα και ο υπεύθυνος επεξεργασίας, από τον έλεγχο του οποίου διέφυγαν τα δεδομένα προσωπικού χαρακτήρα. Βέβαια κάθε υπεύθυνος επεξεργασίας δεν είναι υποχρεωμένος να λειτουργεί το καλύτερο σύστημα ασφάλειας για τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζεται. Αυτό που επιβάλλει ο νόμος είναι η τήρηση αναλογικότητας μεταξύ των μέτρων ασφαλείας και του περιεχομένου των δεδομένων που αυτά αφορούν. Ο Ν. 3471/2006 στο σημείο αυτό εξειδικεύει περισσότερο την υποχρέωση ασφάλειας του παρόχου, στο άρθρο 12, το οποίο θα εξετασθεί αναλυτικότερα παρακάτω.

### **2.3 Η συγκατάθεση του υποκειμένου των δεδομένων**

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για να είναι νόμιμη απαιτεί και την ύπαρξη της συγκατάθεσης του προσώπου στο οποίο αναφέρονται τα δεδομένα. Η συγκατάθεση του υποκειμένου των δεδομένων, μαζί με την αρχή της δεσμευτικότητας του σκοπού, αποτελεί τον ακρογωνιαίο λίθο του δικαίου προστασίας των δεδομένων προσωπικού χαρακτήρα, καθώς αποτελεί αυτοτελή όρο νομιμότητας της επεξεργασίας που προτάσσεται όλων των άλλων και ορίζεται ως εξής : «συγκατάθεση» του υποκειμένου των δεδομένων αποτελεί κάθε ελεύθερη, ρητή και ειδική δήλωση βούλησης, που εκφράζεται με τρόπο σαφή και εν πλήρη επίγνωση και με την οποία το υποκείμενο των δεδομένων, αφού προηγουμένως έχει ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Η συγκατάθεση απαιτείται να είναι ελεύθερη, δηλαδή θα πρέπει να μη γίνεται υπό καθεστώς οποιασδήποτε μορφής βίας ή απειλής. Για παράδειγμα δεν είναι πάντα ελεύθερη η συγκατάθεση που δίνει ένας εργαζόμενος στον εργοδότη του να επεξεργαστεί προσωπικά του δεδομένα ή ένας δανειολήπτης, όταν όλες οι Τράπεζες απαιτούν τη συγκατάθεσή του προκειμένου να του χορηγήσουν κάποιο δάνειο. Το υποκείμενο θα πρέπει να τελεί εν πλήρη επίγνωση του σκοπού και των λοιπών προϋποθέσεων της επεξεργασίας προκειμένου να είναι νόμιμη η συγκατάθεσή του. Επίσης, η δήλωση συγκατάθεσης θα πρέπει να είναι ρητή, έγγραφη ή προφορική. Σύμφωνα με την απόφαση της Αρχής 50/200099, ρητή



δεν είναι η δήλωση που εννοείται από τη μεταγενέστερη μη αντίδραση του ατόμου σε ήδη διενεργηθείσα επεξεργασία την οποία πληροφορήθηκε. Τέλος, η δήλωση συγκατάθεσης θα πρέπει να είναι ειδική, θα πρέπει δηλαδή να αναφέρεται σε συγκεκριμένη επεξεργασία και σε συγκεκριμένο υπεύθυνο επεξεργασίας και δεν αρκεί μια γενική δήλωση ότι αποδέχεται οποιαδήποτε επεξεργασία και αν αναλάβει ένας υπεύθυνος επεξεργασίας. Η προηγούμενη ενημέρωση, ως προϋπόθεση για τη νομιμότητα της συγκατάθεσης, περιλαμβάνει πληροφόρηση τουλάχιστον για το σκοπό της επεξεργασίας, τα δεδομένα ή τις κατηγορίες των δεδομένων που αφορά η επεξεργασία, τους αποδέκτες ή τις κατηγορίες των αποδεκτών, καθώς και το όνομα, την επωνυμία και τη διεύθυνση του υπεύθυνου επεξεργασίας και του τυχόν εκπροσώπου του. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς αναδρομικό αποτέλεσμα και απαιτείται να είναι έγγραφη μόνο όταν αφορά επεξεργασία ευαίσθητων δεδομένων, ενώ όταν αφορά απλά δεδομένα αρκεί να είναι προφορική, πάντως όμως ρητή. Η συγκατάθεση ορίζεται ως θεμελιώδης προϋπόθεση για τη νομιμότητα της επεξεργασίας και από το Ν. 3471/2006. Ειδικότερα σύμφωνα με τη διάταξη του άρθρου 5 παρ2 περ. α', η επεξεργασία επιτρέπεται μόνο αν ο συνδρομητής ή ο χρήστης έχει δώσει τη συγκατάθεσή του μετά από ενημέρωσή του για το είδος των δεδομένων, τον σκοπό και την έκταση της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών και στο άρθρο 5 παρ. 3, ορίζεται ότι ο υπεύθυνος επεξεργασίας θα πρέπει να εξασφαλίζει ότι ο συνδρομητής ή ο χρήστης έχει δώσει τη συγκατάθεσή του έχοντας πλήρη επίγνωση των συνεπειών που έχει η δήλωσή του και η οποία καταγράφεται με ασφαλή τρόπο, είναι ανά πάσα στιγμή προσβάσιμη στο χρήστη και μπορεί οποτεδήποτε να ανακληθεί. Σε σχέση με τη συγκατάθεση του ατόμου, σημαντικό είναι το ζήτημα των optin και opt-out επιλογών, δηλαδή των επιλογών «αποδέχομαι» και «δεν αποδέχομαι» στο τέλος των ιστοσελίδων. Η Αρχή στην απόφασή της 38/2002, έχει ήδη αποφανθεί ότι απαιτείται να υφίστανται και οι δύο επιλογές (δύο tick boxes- σε εμφανές σημείο), και ότι η συγκατάθεση δεν πρέπει να διατυπώνεται με τρόπο αρνητικό (π.χ. «αν δε συναινείτε σημειώστε στο ακόλουθο κουτί»), ωστόσο οι μέθοδοι άμεσης διαφήμισης που χρησιμοποιούν πολλές επιχειρήσεις παρουσιάζουν ιδιαίτερη ευρηματικότητα προκειμένου να αποσπάσουν τη συγκατάθεση των καταναλωτών. Τέλος, όσον αφορά στον τύπο της συγκατάθεσης για την επεξεργασία των απλών δεδομένων, ο νόμος δεν απαιτεί την τήρηση κάποιου ιδιαίτερου τύπου, σε αντίθεση με τη συγκατάθεση που απαιτείται για την επεξεργασία των ευαίσθητων δεδομένων, όπως θα εκτεθεί ακολούθως, και επομένως είναι δυνατή η παροχή της με ηλεκτρονικά μέσα, δηλ. σε

απευθείας σύνδεση online ή μέσω ηλεκτρονικού ταχυδρομείου, χωρίς να απαιτείται υποχρεωτικά έγγραφος τύπος για την παροχή της συγκατάθεσης.

Παρά το γενικό κανόνα ότι η επεξεργασία επιτρέπεται μόνο εφόσον το υποκείμενο δώσει τη συγκατάθεσή του, προβλέπονται ορισμένες εξαιρέσεις, στις οποίες η επεξεργασία των δεδομένων είναι νόμιμη ακόμη και όταν το άτομο δεν έχει συγκατατεθεί σχετικά. Πρόκειται για τις περιοριστικά αναφερόμενες περιπτώσεις οι οποίες παρατίθενται στο άρθρο 5 παρ. 2 του νόμου 2472/1997<sup>101</sup>.

Οι εξαιρέσεις που προβλέπονται στο άρθρο 5 παρ 2 του Ν. 2472/1997 και αφορούν γενικά στη νόμιμη επεξεργασία δεδομένων χωρίς τη συγκατάθεση του υποκειμένου είναι οι εξής:

- Όταν η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης στην οποία συμβαλλόμενο μέρος είναι υποκείμενο δεδομένων ή για τη λήψη μέτρων κατόπιν αιτήσεως του υποκειμένου κατά το προσυμβατικό στάδιο. Πρόκειται για περιπτώσεις τραπεζικών δανείων, ασφαλιστηρίων συμβολαίων, εργασιακών σχέσεων, ιατρού εργασίας κλπ.
- Όταν η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρέωσης του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο (π.χ. διαβίβαση φορολογικών στοιχείων που περιέχουν προσωπικά δεδομένα στο Υπουργείο Οικονομικών)
- Όταν η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει της συγκατάθεσή του
- Όταν η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημοσίου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια αρχή ή έχει ανατεθεί από αυτή είτε στον υπεύθυνο επεξεργασίας είτε σε τρίτο στον οποίο γνωστοποιούνται τα δεδομένα. Η Αρχή στην απόφασή της 11/2001 ως έργο δημοσίου συμφέροντος έκρινε τη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα εκλογέων από υποψήφιους βουλευτές για τις επικοινωνιακές ανάγκες και μόνο από δημόσια προσβάσιμες πηγές και μόνο για το σκοπό αυτό.
- Όταν η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του εννόμου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος ή τρίτοι στους οποίους ανακοινώνονται τα δεδομένα υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και των συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα και επιπρόσθετα ότι δε θίγονται οι θεμελιώδεις ελευθερίες αυτών.

Απαιτείται δηλαδή στάθμιση συμφερόντων μεταξύ του υποκειμένου και του υπεύθυνου επεξεργασίας σε εξαιρετικές περιπτώσεις.

Ωστόσο, ειδικά για τη επεξεργασία των δεδομένων στο διαδίκτυο, ο Ν. 3471/2006 στο άρθρο 5 παρ.2 περ. β' περιλαμβάνει ειδικότερη ρύθμιση σε σχέση με το Ν 2472/1997 και οι προϋποθέσεις που τάσσει είναι αυστηρότερες σε σχέση με τις προϋποθέσεις νομιμότητας που θέτει ο Ν. 2472/1997 στο άρθρο 5 παρ.2. Συγκεκριμένα, η επεξεργασία δεδομένων στο διαδίκτυο καθίσταται νόμιμη όταν δε δίνεται συγκατάθεση, μόνο στις ακόλουθες δύο περιπτώσεις :

- στην περίπτωση που η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης στην οποία συμβαλλόμενο μέρος είναι ο συνδρομητής ή ο χρήστης και
- για τη λήψη μέτρων κατά το προσυμβατικό στάδιο μετά από αίτηση του συνδρομητή (άρθρο 5 παρ 2 περ. β').

## **2.4 Υποχρέωση γνωστοποίησης**

Η υποχρέωση γνωστοποίησης αποτελεί θεμελιώδη υποχρέωση κάθε υπεύθυνου επεξεργασίας, προκειμένου να επεξεργαστεί νομίμως τα δεδομένα του. Ο ν. 2472/1997 προβλέπει σύστημα γνωστοποίησης κάθε επεξεργασίας ή αρχείου προσωπικών δεδομένων. Καθιερώνεται λοιπόν η υποχρέωση γνωστοποίησης για τον υπεύθυνο επεξεργασίας, η οποία μαζί με το δικαίωμα ενημέρωσης του υποκειμένου, εκπληρώνουν την επιταγή του άρθρου 21 της οδηγίας 95/46/EK για διαφάνεια των επεξεργασιών. Έτσι, σύμφωνα με το άρθρο 6 παρ.1, δεν απαιτείται η χορήγηση άδειας για τη σύσταση ενός αρχείου, αλλά ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει εγγράφως στην Αρχή τη σύσταση και τη λειτουργία αρχείου ή την έναρξη της επεξεργασίας. Άδεια απαιτείται μόνο για τις ειδικές κατηγορίες επεξεργασίας του άρθρου 7 παρ. 2, όπως θα δούμε ακολούθως. Σύμφωνα με την κρατούσα μάλλον άποψη, η υποχρέωση γνωστοποίησης δεν επιτελεί προληπτικό αλλά κατασταλτικό ρόλο, δεν αποτελεί δηλαδή προϋπόθεση έναρξης της επεξεργασίας ή τη σύστασης ενός αρχείου. Η Αρχή, δηλαδή, δεν δίνει άδεια με βάση τα στοιχεία της γνωστοποίησης, αλλά αντίθετα ο υπεύθυνος επεξεργασίας μπορεί να ξεκινήσει τη συλλογή και την επεξεργασία των δεδομένων, εφόσον δεν είναι ευαίσθητα, και παράλληλα να προβεί σε γνωστοποίηση στην Αρχή. Στόχος της γνωστοποίησης είναι η δημιουργία ενός κεντρικού μητρώου αρχείων και επεξεργασίας το οποίο τηρείται από την Αρχή και είναι προσιτό σε όποιον

ενδιαφέρεται να ασκήσει τα δικαιώματά του έναντι των εκάστοτε υπευθύνων επεξεργασίας (άρθρο 6 παρ.3, άρθρο 19 παρ 5 Ν. 2472/97).

## **2.5 Επεξεργασία των ευαίσθητων δεδομένων - λήψη άδειας από την Αρχή**

Όσο αναφορά την επεξεργασία των ευαίσθητων δεδομένων, δεν αρκεί η απλή γνωστοποίηση στην Αρχή, αλλά απαιτείται η λήψη άδειας από αυτήν, κατόπιν υποβολής αιτήσεως από τον υπεύθυνο επεξεργασίας. Σύμφωνα με το άρθρο 7 παρ. 1, κατ' αρχήν απαγορεύεται η συλλογή και επεξεργασία ευαίσθητων δεδομένων, ωστόσο επιτρέπεται κατ' εξαίρεση στις παρακάτω περιπτώσεις (άρθρο 7 παρ 2) και εφόσον παρέχεται άδεια από την Αρχή:

- Αν το υποκείμενο έδωσε τη γραπτή συγκατάθεσή του, εκτός αν η συγκατάθεσή του έχει αποσπασθεί με τρόπο που αντίκειται στο νόμο ή στα χρηστά ήθη ή αν ο νόμος ορίζει ότι η συγκατάθεση δεν αίρει την απαγόρευση. Επομένως, για την επεξεργασία των ευαίσθητων δεδομένων, δεδομένου ότι ο Ν. 3471/2006 δεν περιλαμβάνει ειδικότερη διάταξη, απαιτείται υποχρεωτικά έγγραφος τύπος για την παροχή της συγκατάθεσης και συνεπώς δεν είναι δυνατή η παροχή της με ηλεκτρονικά μέσα, δηλ. σε απευθείας σύνδεση on-line ή μέσω ηλεκτρονικού ταχυδρομείου, ενώ απαιτείται και άδεια της Αρχής, σύμφωνα με τις προϋποθέσεις του άρθρου 7 Ν 2472/1997. Ωστόσο, επιτρέπεται η συλλογή και επεξεργασία ευαίσθητων δεδομένων χωρίς τη συγκατάθεση του υποκειμένου και στις παρακάτω περιπτώσεις:
- Αν η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος (π.χ. κυοφορούμενου), ή προβλεπόμενου από το νόμο συμφέροντος τρίτου, εάν το υποκείμενο τελεί σε φυσική αδυναμία (σοβαρή νόσος/ απουσία) ή νομική αδυναμία να δώσει τη συγκατάθεσή του.
- Αν η επεξεργασία αφορά δεδομένα που δημοσιοποιεί το ίδιο το υποκείμενο, καθώς σ' αυτή την περίπτωση η δημοσιοποίηση ισοδυναμεί με συγκατάθεση εν ευρεία έννοια ή είναι αναγκαία για την άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου ή πειθαρχικού οργάνου.
- Αν η επεξεργασία αφορά θέματα υγείας και εκτελείται από πρόσωπο που ασχολείται κατ' επάγγελμα με την παροχή υπηρεσιών και υπόκειται σε καθήκον εχεμύθειας ή σε συναφείς κώδικες δεοντολογίας υπό τον όρο ότι η επεξεργασία είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη.

- Αν η επεξεργασία τελείται από Δημόσια Αρχή και είναι αναγκαία είτε α) για λόγους εθνικής ασφάλειας είτε β) για την εξυπηρέτηση των αναγκών εγκληματολογικής ή σωφρονιστικής πολιτικής και αφορά τη διακρίβωση εγκλημάτων, ποινικές καταδίκες ή μέτρα ασφάλειας είτε γ) για λόγους προστασίας της δημόσιας υγείας είτε δ) για την άσκηση δημοσίου φορολογικού ελέγχου ή δημοσίου ελέγχου κοινωνικών παροχών.
- Αν η επεξεργασία πραγματοποιείται για ερευνητικούς και επιστημονικούς αποκλειστικά σκοπούς και υπό τον όρο ότι τηρείται η ανωνυμία και λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται.
- Αν η επεξεργασία αφορά δεδομένα δημοσίων προσώπων, εφόσον αυτά συνδέονται με την άσκηση δημοσίου λειτουργήματος ή τη διαχείριση συμφερόντων τρίτων και πραγματοποιείται αποκλειστικά για την άσκηση του δημοσιογραφικού επαγγέλματος. Η άδεια της αρχής χορηγείται μόνο εφόσον η επεξεργασία είναι απολύτως αναγκαία για τη διασφάλιση του δικαιώματος πληροφόρησης επί θεμάτων δημοσίου ενδιαφέροντος καθώς και στο πλαίσιο καλλιτεχνικής έκφρασης, εφόσον δεν παραβιάζεται καθ' οιονδήποτε τρόπο το δικαίωμα προστασίας της ιδιωτικής και οικογενειακής ζωής. Σε κάθε περίπτωση επεξεργασίας ευαίσθητων δεδομένων απαιτείται η προηγούμενη άδεια της Αρχής.

Αν συντρέχει κάποια από τις παραπάνω προϋποθέσεις, η Αρχή οφείλει κατά δέσμια αρμοδιότητα να χορηγήσει άδεια επεξεργασίας ευαίσθητων δεδομένων. Η άδεια εκδίδεται ύστερα από αίτηση, την οποία υποβάλλει ο υπεύθυνος επεξεργασίας στην Αρχή, αλλά και στην περίπτωση που η Αρχή διαπιστώσει ότι πραγματοποιείται επεξεργασία ευαίσθητων δεδομένων, μετά από γνωστοποίηση αρχείου. Η γνωστοποίηση αρχείου τότε επέχει θέση αιτήσεως για τη χορήγηση άδειας (Βλ. άρθρο 7 παρ. 3). Η Αρχή, πριν χορηγήσει την άδεια καλεί σε ακρόαση τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία και μπορεί να επιβάλλει όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία του δικαιώματος ιδιωτικής ζωής του υποκειμένου ή τρίτων.

## **2.6 Απαλλαγή από υποχρέωση γνωστοποίησης ή λήψης άδειας.**

Στο άρθρο 7 Α προβλέπεται απαλλαγή από την υποχρέωση γνωστοποίησης του άρθρου 6 και λήψης άδειας του άρθρου 7, σε ορισμένες περιοριστικά αναφερόμενες περιπτώσεις και συγκεκριμένα:

- Όταν η επεξεργασία πραγματοποιείται αποκλειστικά για σκοπούς που συνδέονται άμεσα με σχέση εργασίας ή έργου ή με παροχή υπηρεσιών στο δημόσιο τομέα, εφόσον τα δεδομένα δεν διαβιβάζονται σε τρίτους. Έτσι για παράδειγμα, η Αρχή προέβη σε προειδοποίηση σε κάποια εταιρεία να μην προβαίνει στην καταγραφή των ιστοσελίδων που επισκέπτονται οι εργαζόμενοι και να μην προβαίνει σε συλλογή και επεξεργασία δεδομένων που αφορούν κλήσεις στο χώρο εργασίας, παρά μόνο εφόσον είναι αναγκαίο για την οργάνωση και τον έλεγχο του κύκλου εργασιών και ιδίως τον έλεγχο των δαπανών (και την καταβολή της μισθοδοσίας).
- Όταν η επεξεργασία αφορά πελάτες ή προμηθευτές, εφόσον τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους. Δεν απαλλάσσονται από την υποχρέωση γνωστοποίησης οι ασφαλιστικές εταιρίες, οι φαρμακευτικές εταιρίες, οι εταιρίες εμπορίας πληροφοριών και τα χρηματοπιστωτικά ιδρύματα – όπως οι Τράπεζες και οι εταιρίες έκδοσης πιστωτικών καρτών.
- Όταν η επεξεργασία γίνεται από σωματεία, εταιρίες, ενώσεις προσώπων και πολιτικά κόμματα και αφορά δεδομένα των μελών ή εταιριών τους.
- Όταν η επεξεργασία αφορά δεδομένα υγείας και γίνεται από γιατρούς ή άλλα πρόσωπα που παρέχουν υπηρεσίες υγείας και εφόσον δεν κοινοποιούνται σε τρίτους. Όταν τα δεδομένα κοινοποιούνται σε δικαστήρια ή δημόσιες αρχές απαλλάσσεται ο υπεύθυνος επεξεργασίας από την υποχρέωση γνωστοποίησης ή λήψης άδειας, εφόσον τη διαβίβαση ή κοινοποίηση επιβάλλει νόμος ή δικαστική απόφαση. Δεν ισχύει όμως η απαλλαγή για ιατρικές υπηρεσίες που παρέχονται μέσω δικτύου ή όταν η επεξεργασία διεξάγεται στο πλαίσιο προγραμμάτων τηλεϊατρικής.
- Όταν η επεξεργασία γίνεται από δικηγόρους, συμβολαιογράφους, άμισθους υποθηκοφύλακες και δικαστικούς επιμελητές ή εταιρίες των προσώπων αυτών και αφορά στην παροχή νομικών υπηρεσιών προς πελάτες τους, εφόσον ο υπεύθυνος επεξεργασίας δεσμεύεται από υποχρέωση απορρήτου που προβλέπει νόμος και τα δεδομένα δε διαβιβάζονται ούτε κοινοποιούνται σε τρίτους, εκτός από τις περιπτώσεις που αυτό είναι αναγκαίο και συνδέεται άμεσα με την εκπλήρωση εντολής του πελάτη.
- Όταν η επεξεργασία γίνεται από δικαστικές αρχές ή υπηρεσίες στο πλαίσιο απονομής της δικαιοσύνης ή την εξυπηρέτηση των αναγκών της λειτουργίας τους.

## 2.7 Απόρρητο των επικοινωνιών<sup>7</sup>

Στο άρθρο 4 του νόμου 3471/2006, ορίζεται ότι οποιαδήποτε χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών που παρέχονται μέσω δημοσίου δικτύου επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης και θέσης, προστατεύεται από το απόρρητο των επικοινωνιών, ενώ η άρση αυτού επιτρέπεται μόνο υπό τους όρους και τις διαδικασίες που προβλέπονται από το άρθρο 19. Οι ανωτέρω διατάξεις του νόμου αυτού συμβάλλουν αποφασιστικά στην επαύξηση της προστασίας του απορρήτου των επικοινωνιών, και ενδεικτικό είναι ότι η προστασία αυτή επεκτείνεται πέρα από το περιεχόμενο της επικοινωνίας, και στα δεδομένα κίνησης και θέσης. Επιπλέον, στο άρθρο 4 παρ. 2 του Ν. 3471/2006, ορίζεται ειδικότερα ότι απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης, εκτός αν προβλέπεται αλλιώς από το νόμο. Καθίσταται επομένως σαφές ότι θα απαγορεύεται αφενός η χρήση λογισμικού υποκλοπής των δεδομένων που διαβιβάζονται μέσω του Διαδικτύου (packet sniffing) και αφετέρου, η αποθήκευση των δεδομένων κίνησης με σκοπό τη δημιουργία πορτραίτων προσωπικότητας των χρηστών, δίχως τη συγκατάθεσή τους. Επιτρέπεται όμως η τεχνική αποθήκευση η οποία είναι αναγκαία για τη διαβίβαση επικοινωνίας με την επιφύλαξη της αρχής του απορρήτου (άρθρο 4 παρ. 4). Επιτρέπεται δηλαδή, η αυτόματη, ενδιάμεση ή παροδική αποθήκευση των πληροφοριών, εφόσον γίνεται με μοναδικό σκοπό την πραγματοποίηση της μετάδοσης στο ηλεκτρονικό δίκτυο επικοινωνιών ( από τον Internet Service Provider) και υπό την προϋπόθεση ότι οι πληροφορίες δεν φυλάσσονται για χρονικό διάστημα μεγαλύτερο απ' όσο απαιτείται για τη μετάδοση και σκοπούς διαχείρισης της κίνησης, ενώ κατά τη διάρκεια περιόδου αποθήκευσης διατηρούνται οι εγγυήσεις του απορρήτου.

## 2.8 Αρχεία cookies<sup>8</sup>

Στο νόμο ρυθμίζεται ακόμη, η χρήση των λεγόμενων κατασκοπευτικών λογισμικών (sniffing software) τα οποία αποτελούν σαφή απειλή για την ιδιωτική σφαίρα του χρήστη του διαδικτύου. Συγκεκριμένα, προβλέπεται ότι απαγορεύεται η χρήση των

<sup>7</sup> Ιωάννης Δ. Ιγγλεζάκης, Εισαγωγή στο δίκαιο της Πληροφορικής, εκδόσεις Σάκκουλα Αθήνα-Θεσσαλονίκη, 2006

<sup>8</sup> Γεώργιος Νούσκαλης, Ψηφιακή Τεχνολογία και Δίκαιο, εκδόσεις Αντ.Ν. Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2004

δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή για την απόκτηση πρόσβασης σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη, ιδίως δε με την εγκατάσταση κατασκοπευτικών λογισμικών, κρυφών αναγνωριστικών στοιχείων και άλλων παρόμοιων διατάξεων (άρθρο 4 παρ. 5). Κατ' εξαίρεση επιτρέπεται η οποιασδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια ή διευκόλυνση της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή η οποία είναι αναγκαία μόνο για την παροχή υπηρεσίας στην κοινωνία της πληροφορίας, την οποία έχει ρητά ζητήσει ο χρήστης ή ο συνδρομητής. Στην τελευταία αυτή περίπτωση η χρησιμοποίηση τέτοιων διατάξεων επιτρέπεται μόνο εάν παρέχονται στο συγκεκριμένο συνδρομητή ή χρήστη σαφείς και εκτεταμένες πληροφορίες σύμφωνα με το άρθρο 11 του Ν 2472/1997, και ο υπεύθυνος ελέγχου των δεδομένων παρέχει στο συνδρομητή ή χρήστη το δικαίωμα να αρνείται την επεξεργασία αυτή. Υιοθετείται επομένως ένα σύστημα «opt-out», όσον αφορά τα αρχεία «cookies», σύμφωνα με το οποίο ο συνδρομητής ή χρήστης δύναται να δηλώσει τη συγκατάθεσή του, αλλά μόνο εκ των υστέρων. Όταν επισκεπτόμαστε ένα δικτυακό τόπο, ο υπολογιστής μας αυτομάτως δέχεται ένα cookie. Τα cookies είναι ένα σύνολο δεδομένων ,μικρά αρχεία κειμένου, τα οποία πιστοποιούν την ταυτότητα του υπολογιστή μας στον διακομιστή αρχείων. Συγκεκριμένα, τα cookies υπάρχουν σε ιστοσελίδες και τα στέλνει ο server για να αποθηκευτούν στον σκληρό δίσκο του ηλεκτρονικού υπολογιστή του χρήστη κατά τη διάρκεια της επίσκεψης στην ιστοσελίδα, προκειμένου να δημιουργηθεί ένα αρχείο στον υπολογιστή του χρήστη, για να χρησιμοποιηθεί στην επόμενη επίσκεψή του στον ίδιο web server. Συνήθως περιγράφουν στοιχεία όπως το όνομα του χρήστη (user name) και συνθηματικό πρόσβασης (password), με σκοπό κατά την επίσκεψή μας στον ίδιο ιστότοπο αργότερα, να μας θυμάται κατά κάποιον τρόπο, να μας αναγνωρίζει και να κάνει login χωρίς να χρειάζεται να γράψουμε εμείς τίποτα άλλο. Πρόσβαση στα cookies αυτά έχει μόνο ο ιδιοκτήτης της σελίδας την οποία επισκέφτηκε ο χρήστης. Τα cookies δεν δίνουν στοιχεία για την ταυτότητα του χρήστη, παρά μόνο πληροφορίες που αφορούν τη χρήση των σελίδων που έκανε ο χρήστης. Καταγράφουν ποιες περιοχές του δικτυακού τόπου επισκέφθηκε ένας υπολογιστής και για πόση ώρα. Οι χρήστες έχουν τη δυνατότητα να ρυθμίσουν τους υπολογιστές τους ώστε να δέχονται όλα τα cookies, να τους ειδοποιούν κάθε φορά που δημιουργείται ένα cookie, ή να μην δέχονται κανένα cookie. Στην περίπτωση όμως που δε δέχονται κανένα cookie καθίσταται πολλές φορές αδύνατη η πρόσβαση σε ιστοσελίδες. Στο σημείο αυτό



τίθεται το ζήτημα της «αθόρυβης» συλλογής προσωπικών δεδομένων στο χώρο του Διαδικτύου, για το οποίο έγινε λόγος αναλυτικά και παραπάνω, μέσω της τεχνολογίας των cookies. Συγκεκριμένα, μέσω της συνδυαστικής χρήσης των διαφόρων cookies, επιτρέπεται η εξαγωγή συμπερασμάτων ακόμα και η δημιουργία ενός ακριβούς ψυχολογικού profil του χρήστη, το οποίο ενδέχεται στη συνέχεια να χρησιμοποιηθεί στο πλαίσιο του λεγόμενου e-marketing, μέσω της αποστολής ηλεκτρονικών μηνυμάτων (πρακτική των spams), με απευθείας προτάσεις για την αγορά συγκεκριμένων προϊόντων σύμφωνα με τις προσωπικές προτιμήσεις του κάθε χρήστη. Παραδείγματος χάριν, μια ιστοσελίδα πώλησης προϊόντων μέσω Internet, εισάγει ένα cookie κάθε φορά που κάποιος χρήστης επιλέγει ένα προϊόν, έτσι ώστε όταν ο πελάτης φθάσει στη σελίδα που περιέχει το έντυπο για την ολοκλήρωση της πώλησης να εμφανίζεται ένας κατάλογος με όλα τα προϊόντα που επέλεξε. Τα cookies μπορούν να χρησιμοποιηθούν με πολλούς τρόπους καθώς περιέχουν τεχνικές πληροφορίες για το ιστορικό της πλοήγησης του χρήστη στο Διαδίκτυο ή άλλα χαρακτηριστικά του υπολογιστή του χρήστη, όπως τις διευθύνσεις από τις προηγούμενες ιστοσελίδες, τις οποίες επισκέφθηκε ο χρήστης ή τα είδη του λογισμικού που χρησιμοποιεί. Επίσης μια μηχανή αναζήτησης τοποθετεί cookies ανάλογα με τις ιστοσελίδες που επισκέφθηκε ο χρήστης (π.χ. μουσική, κινηματογράφος, αθλητικά) με σκοπό να εισάγει αργότερα διαφημιστικές επιγραφές που να ανταποκρίνονται στις προτιμήσεις του χρήστη και πιθανόν να αποφέρουν το επιθυμητό αποτέλεσμα της προώθησης των σχετικών προϊόντων.

## 2.9 Δεδομένα κίνησης και θέσης<sup>9</sup>

Ως δεδομένα κίνησης ορίζονται τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας στο Διαδίκτυο ή της χρέωσής της (άρθρο 2 παρ. 3 του Ν. 3471/2006). Τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τον παροχέα, πρέπει να καταστρέφονται ή να καθίστανται ανώνυμα με κατάλληλη κωδικοποίηση με τη λήξη της επικοινωνίας, σύμφωνα με το άρθρο 6 παρ. 1 του ν. 3471/2006.

<sup>9</sup> Α.Φραγκούλη, Προστασία Δεδομένων στο Διαδίκτυο, εις συλλογικόν έργον Εφαρμογές Εμπορικού Δικαίου, Επιμέλειας Γ Τριανταφυλλάκη, Νομική Βιβλιοθήκη 2007

Στα δεδομένα κίνησης σύμφωνα με το άρθρο 2 παρ. 3 μπορεί να περιλαμβάνονται ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων και μεταξύ άλλων, το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία. Με βάση τις πληροφορίες αυτές είναι δυνατή η δημιουργία πορτραίτων των χρηστών των δικτύων ηλεκτρονικής επικοινωνίας, αλλά και γενικότερα η παρακολούθηση της σχετικής δραστηριότητας των συνδρομητών και χρηστών, από την οποία μπορούν να εξαχθούν ποικίλα συμπεράσματα για τους σκοπούς της άμεσης προώθησης προϊόντων, αλλά και για τους σκοπούς της αντιεγκληματικής πολιτικής. Ο κανόνας είναι η απαγόρευση της επεξεργασίας των δεδομένων αυτών, εκτός αν ο χρήστης παρέχει τη συγκατάθεσή του. Εδώ επομένως, σε αντίθεση με τη ρύθμιση των αυτοεγκαθιστώμενων αρχείων cookies, υιοθετείται ένα σύστημα «opt-in». Σύμφωνα λοιπόν με το άρθρο 5 παρ 4 εδ. α' ν. 3471/2006, «ο πάροχος δεν επιτρέπεται να χρησιμοποιεί τα δεδομένα κίνησης και θέσης (όπως και όλα τα δεδομένα προσωπικού χαρακτήρα) ή να τα διαβιβάζει σε τρίτους για άλλους σκοπούς, εκτός αν ο συνδρομητής ή ο χρήστης έχει δώσει ρητά τη συγκατάθεσή του». Όπως προβλέπεται στο άρθρο 5 παρ.4 ν. 3471/2006: «εξαίρεση αποτελούν οι σκοποί που συνδέονται με την παροχή ηλεκτρονικών επικοινωνιών και την παροχή υπηρεσιών προστιθέμενης αξίας που έχει ζητήσει ο συνδρομητής ή ο χρήστης, όπως η διαφήμιση ή η εμπορική έρευνα αγοράς και υπηρεσιών. Σε περίπτωση που απαιτείται η συγκατάθεση του υποκειμένου για να υποβληθούν τα δεδομένα κίνησης σε επεξεργασία, ο πάροχος οφείλει να ενημερώσει τον συνδρομητή ή χρήστη σχετικά με τον τύπο των δεδομένων που υποβάλλονται σε επεξεργασία κατά τη διάρκεια της επεξεργασίας αυτής ( άρθρο 5 παρ 4 εδ. α' ν.3471/2006). Προκειμένου τα δεδομένα κίνησης να διαβιβασθούν από τον πάροχο σε τρίτους η συγκατάθεση πρέπει να είναι έγγραφη. Η συγκατάθεση αυτή μπορεί να ανακληθεί οποτεδήποτε, όπως ορίζεται στο άρθρο 5 παρ 4 εδ. β' ν.3471/2006. Τα δεδομένα κίνησης επιτρέπεται να υποβάλλονται από τον πάροχο σε επεξεργασία, μόνο όταν η επεξεργασία γίνεται με σκοπό τη χρέωση των συνδρομητών και την πληρωμή των διασυνδέσεων, εφόσον κάτι τέτοιο είναι αναγκαίο. Η επεξεργασία αυτή είναι επιτρεπτή μόνο ως το τέλος της περιόδου, εντός της οποίας μπορεί να αμφισβητηθεί νομίμως ο λογαριασμός ή να επιδιωχθεί η πληρωμή του. Σε κάθε περίπτωση όμως ο φορέας πρέπει να ενημερώνει το συνδρομητή για τον τύπο των δεδομένων κίνησης που υποβάλλονται σε επεξεργασία καθώς και για τον τύπο της επεξεργασίας. Ο πάροχος μπορεί να υποβάλλει σε

επεξεργασία δεδομένα κίνησης που αφορούν συνδρομητές ή χρήστες, όταν απαιτείται προκειμένου να αντιμετωπίζει τεχνικές βλάβες ή σφάλματα κατά τη διαβίβαση επικοινωνιών (βλ. υπ' αριθμ. 29 αιτιολογική σκέψη Οδηγίας 2002/58/EK).

Τα δεδομένα θέσης σύμφωνα με το άρθρο 2 παρ. 4156 είναι τα δεδομένα που υποβάλλονται σε επεξεργασία στο Διαδίκτυο και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Στην περίπτωση αυτή η επεξεργασία νομιμοποιείται μόνον εφόσον καθίστανται ανώνυμα με την κατάλληλη κωδικοποίηση ή εφόσον παρέχεται συγκατάθεση, στην απαιτούμενη έκταση και για την απαιτούμενη διάρκεια για την παροχή μιας υπηρεσίας προστιθέμενης αξίας. Πριν δώσει ο συνδρομητής ή ο χρήστης τη συγκατάθεσή του, ο πάροχος είναι υποχρεωμένος να τον ενημερώνει σχετικά με τον τύπο των δεδομένων θέσης που υποβάλλονται σε επεξεργασία, τους σκοπούς και τη διάρκεια της επεξεργασίας αυτής, αλλά και το ενδεχόμενο μετάδοσής τους σε τρίτους για το σκοπό παροχής της υπηρεσίας προστιθέμενης αξίας. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, ενώ μπορεί να παρέχεται στον συνδρομητή ή χρήστη η δυνατότητα να αρνείται την προσωρινή επεξεργασία των εν λόγω δεδομένων με απλά μέσα και ατελώς. Δεν απαιτείται η συγκατάθεση του χρήστη ή συνδρομητή για την επεξεργασία δεδομένων θέσης από τον φορέα, όταν η επεξεργασία πραγματοποιείται για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης με την παροχή πληροφοριών στις αρμόδιες αρχές (π.χ. διωκτικές αρχές, υπηρεσίες πρώτων βοηθειών κλπ) για τον εντοπισμό του καλούντος και μόνο γι' αυτό το σκοπό. Οι διαδικασίες, ο τρόπος και κάθε τεχνική λεπτομέρεια για την ως άνω ενέργεια καθορίζονται με πράξη της Αρχής Διασφάλισης του απορρήτου των επικοινωνιών.

## **2.10 Επιβολή κυρώσεων<sup>10</sup>**

Μια πραγματιστική προσέγγιση για την αντιμετώπιση του πληροφορικού εγκλήματος παρουσιάζεται ως η πλέον αποτελεσματική λύση, καθώς αποτελεί το συνδυασμό τόσο της εντατικοποίησης της διωκτικής προσπάθειας σε ποινική- κατασταλτική βάση, όσο και της ωφελιμιστικής προσέγγισης. Προτείνεται δηλαδή, σύμφωνα με το πραγματιστικό μοντέλο η ποινή να σχεδιάζεται με τέτοιο τρόπο, ώστε να ανταποκρίνεται στο έγκλημα αλλά και στις ιδιαιτερότητες του δράστη. Η επιβολή οικονομικού προστίμου μπορεί να αποδειχθεί ιδιαίτερα αποδοτική σε ορισμένα είδη εγκλημάτων και δραστών αλλά όχι σε όλα. Για παράδειγμα, η επιβολή μιας ποινής υψηλού χρηματικού προστίμου για μια χωρίς εξουσιοδότηση πρόσβαση σε

<sup>10</sup> Γρηγόρης Λάζος, Πληροφορική και έγκλημα, εκδόσεις Νομική Βιβλιοθήκη, Αθήνα 2001

υπολογιστή τρίτου (hacking) μάλλον θα άφηνε αδιάφορο έναν νεαρό φοιτητή με περιορισμένα εισοδήματα, ενώ θα μπορούσε να είναι αποτελεσματική για έναν επαγγελματία στο χώρο της πληροφορικής. Σε κάποιες άλλες περιπτώσεις μέτρα που σχετίζονται με την ψυχική τιμωρία του δράστη θα μπορούσαν να είναι περισσότερο αποτελεσματικά. Πολλοί εγκληματίες είναι ψυχολογικά και οικονομικά εξαρτώμενοι από τους υπολογιστές τους, οπότε ποινές όπως η κατάσχεση του υπολογιστή με το οποίο διαπράχθηκε το έγκλημα ή η επιβολή περιορισμού στη χρήση του υπολογιστή θα μπορούσαν να οδηγήσουν στην αποτροπή τέλεσης των εγκλημάτων.

Πέραν της απόψεως αυτής την οποία ο νομοθέτης θα έπρεπε να λάβει σοβαρά υπόψη στο μέλλον για τη δημιουργία ενός αποτελεσματικού νομικού πλαισίου προστασίας απέναντι στο πληροφορικό έγκλημα, η ισχύουσα νομοθεσία προβλέπει συγκεκριμένες κυρώσεις. Σε περίπτωση παράβασης της νομοθεσίας προστασίας προσωπικών δεδομένων προβλέπονται διοικητικές, ποινικές και αστικές κυρώσεις. Οι διοικητικές κυρώσεις επιβάλλονται από την Αρχή Προστασίας Προσωπικών Δεδομένων, ενώ οι ποινικές και οι αστικές από τα αρμόδια δικαστήρια.

### **3. Το Κυβερνοέγκλημα<sup>11</sup>**

#### **3.1 Διακρίσεις – Συχνότερες μορφές**

Σύμφωνα με τα αποτελέσματα έρευνας που διεξήγαγε η McConnell International σε 52 χώρες, με τίτλο «Cyber Crime and Punishment» κατατάσσει τα αδικήματα που διαπράττονται στον Κυβερνοχώρο στις παρακάτω κατηγορίες:

- Παρεμπόδιση (κυβερνο)κυκλοφορίας
- Τροποποίηση και Κλοπή δεδομένων
- Εισβολή και Σαμποτάζ σε δίκτυο με μη εξουσιοδοτημένη πρόσβαση
- Διασπορά ιών
- Υπόθαλψη αδικημάτων
- Πλαστογραφία και Απάτη.

Κύριες μορφές Κυβερνοεγκλημάτων που εξιχνιάσθηκαν στην Ελλάδα από το Τμήμα Ηλεκτρονικού Εγκλήματος/ΔΑΑ:

- Απάτες μέσω Διαδικτύου

<sup>11</sup> Χρίστος Μυλωνόπουλος, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, εκδόσεις Σάκκουλα, Αθήνα 2002

- Παιδική πορνογραφία
- Cracking και hacking
- Διακίνηση-πειρατεία λογισμικού
- Πιστωτικές κάρτες
- Διακίνηση ναρκωτικών
- Έγκλημα στα chat rooms.

Με κριτήριο το προσβαλλόμενο έννομο αγαθό, τα εγκλήματα που διαπράττονται στο διαδίκτυο μπορούν να διακριθούν:

- σε εγκλήματα κατά των προσωπικών δικαιωμάτων του πολίτη
- σε εγκλήματα εναντίον του κοινωνικού συνόλου και
- σε εγκλήματα εναντίον περιουσιακών αγαθών .

Οι διάφορες μορφές του ηλεκτρονικού εγκλήματος ρυθμίζονται και τιμωρούνται ξεχωριστά και από άλλα ειδικότερα νομοθετήματα στην Ελλάδα και στην Ευρωπαϊκή Ένωση. Ειδικότερα αναλύονται οι εξής μορφές:

### 3.1.2 Κυβερνοσφετερισμός

Κυβερνοσφετερισμός (cybersquatting) είναι το ηλεκτρονικό αδίκημα κατά το οποίο κάποιος χρήστης του Διαδικτύου για εμπορικούς σκοπούς κατοχυρώνει και χρησιμοποιεί ηλεκτρονική διεύθυνση (domain name) που περιέχει είτε την επωνυμία γνωστών επιχειρήσεων είτε σήματα φήμης με αποτέλεσμα να προκαλείται βλάβη στη φήμη των νόμιμων δικαιούχων αλλά και αποκλεισμός τους από τη χρήση του διαδικτύου με την επωνυμία τους.

### 3.1.3 Προστασία Domain Names<sup>12</sup>

Η προστασία των domain name παρέχεται ανάλογα με το περιεχόμενο του δεύτερου μέρους τους. Αν τη διαδικτυακή διεύθυνση αποτελεί ένα όνομα, τότε παρέχεται η προστασία των άρθρων 57 και 58 ΑΚ. Αν πρόκειται για εμπορική επωνυμία, δηλαδή ένα όνομα με το οποίο ο έμπορος διεξάγει τις συναλλαγές του ή για διακριτικό τίτλο τότε μαζί με την προστασία του άρθρου 58 ΑΚ παρέχεται και η προστασία του άρθρου 13 του νόμου 146/1914. Το άρθρο 13 του νόμου 1146/1914 εφαρμόζεται και όταν ένα domain name αποτελεί εικονικό κατάστημα που είναι γνωστό και επικρατεί στις ηλεκτρονικές συναλλαγές. Αν η ηλεκτρονική διεύθυνση ταυτίζεται με το σήμα

<sup>12</sup> Καρακώστας Ιωάννης, Δίκαιο και Internet – Νομικά Ζητήματα του Διαδικτύου, Εκδόσεις Δίκαιο και Οικονομία Π.Ν. Σάκκουλας, Αθήνα, 2003

και υπάρχει κίνδυνος σύγχυσης στις συναλλαγές παρέχεται η προστασία των άρθρων 4, 18 και 26 του νόμου 2239/1994 περί σημάτων.

### **3.1.4 Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ν.2867/00)**

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ) αποτελεί σημαντική Αρχή στον χώρο του διαδικτύου . Σύμφωνα με το άρθρο 3 Ν. 2867/2000 αποτελεί την Εθνική ρυθμιστική Αρχή σε θέματα τηλεπικοινωνιών. Είναι ανεξάρτητη διοικητική Αρχή με έδρα την Αθήνα και απολαμβάνει διοικητικής και οικονομικής αυτοτέλειας. Τα μέλη της Ε.Ε.Τ.Τ. κατά την άσκηση των καθηκόντων τους απολαύουν πλήρους προσωπικής και λειτουργικής ανεξαρτησίας. Ο Πρόεδρος, οι Αντιπρόεδροι και τα υπόλοιπα μέλη της διορίζονται με απόφαση του Υπουργού Μεταφορών και Επικοινωνιών μετά από προηγούμενη επιλογή τους από τη Διάσκεψη των Προέδρων της Βουλής με την αυξημένη πλειοψηφία των τεσσάρων πέμπτων των μελών της: Ως μέλη της Ε.Ε.Τ.Τ. επιλέγονται πρόσωπα εγνωσμένου κύρους, που απολαύουν ευρείας κοινωνικής αποδοχής και διακρίνονται για την επιστημονική τους κατάρτιση και την επαγγελματική τους ικανότητα στον τεχνικό, οικονομικό ή νομικό τομέα. Κατά την εκτέλεση των καθηκόντων τους, τα μέλη της Ε.Ε.Τ.Τ. δεσμεύονται από το νόμο, έχουν δε υποχρέωση τηρήσεως, των αρχών της αντικειμενικότητας και αμεροληψίας. Ο Πρόεδρος, οι Αντιπρόεδροι και τα μέλη της Ε.Ε.Τ.Τ. υποχρεούνται στην τήρηση εμπιστευτικότητας εμπορικών πληροφοριών για τέσσερα (4) έτη μετά την εκούσια ή ακούσια αποχώρηση τους από την Ε.Ε.Τ.Τ..

### **3.2 Διαφημίσεις μέσω του διαδικτύου - Spamming<sup>13</sup>**

Ως προς το ισχύον γενικό ρυθμιστικό πλαίσιο για τη διαφήμιση, πρέπει να αναφέρουμε την Οδηγία 2005/29/EK «για τις αθέμιτες εμπορικές πρακτικές». Σε συμμόρφωση με την παραπάνω, με το Ν. 3587/2007 τροποποιήθηκε το άρθρο 9 του Ν. 2251/1994, με την προσθήκη των άρθρων 9α έως 9θ, τα οποία μεταξύ άλλων απαγορεύουν την αθέμιτη και παραπλανητική διαφήμιση. Η διαφήμιση συμπεριλαμβάνεται ρητά στην ευρύτερη έννοια της «εμπορικής πρακτικής» (άρθρο 9α περ. δ' Ν. 2251/1994) και ρυθμίζεται πλέον από τις παραπάνω διατάξεις για τις «αθέμιτες εμπορικές πρακτικές». Λόγω, δε, του γενικού χαρακτήρα των διατάξεων αυτών, εφαρμόζονται και σε διαφημίσεις που γίνονται μέσω του Διαδικτύου. Κατά την έννοια του άρθρου 9 παρ. 1 Ν. 2251/1994, διαφήμιση είναι κάθε ανακοίνωση που γίνεται με κάθε μέσο στο πλαίσιο εμπορικής, βιομηχανικής, βιοτεχνικής ή

<sup>13</sup> Λάζος Γρ. , Πληροφορική και Έγκλημα, Νομική Βιβλιοθήκη, Αθήνα 2001

επαγγελματικής δραστηριότητας, με στόχο την προώθηση της διάθεσης αγαθών ή υπηρεσιών συμπεριλαμβανομένων των ακινήτων και των συναφών δικαιωμάτων και υποχρεώσεων. Σύμφωνα, λοιπόν, με το άρθρο 9δ παρ. 1 Ν. 3587/2007, απαγορεύεται κάθε διαφήμιση που περιλαμβάνει εσφαλμένες πληροφορίες και είναι, συνεπώς, αναληθής, ή που, με οποιονδήποτε τρόπο, συμπεριλαμβανομένης της συνολικής παρουσίας της, παραπλανά ή ενδέχεται να παραπλανήσει το μέσο καταναλωτή, ακόμα και αν οι πληροφορίες είναι αντικειμενικά ορθές, όσον αφορά ένα ή περισσότερα από μια σειρά στοιχείων που αναλυτικά ορίζει

ο νόμος (π.χ. φύση προϊόντος, τιμή, διαθεσιμότητα κ.ά.) και, ούτως ή άλλως, τον οδηγεί ή ενδέχεται να τον οδηγήσει να λάβει απόφαση συναλλαγής, την οποία διαφορετικά δεν θα ελάμβανε.

Το κυριότερο πρόβλημα της διαδικτυακής διαφήμισης είναι το λεγόμενο spamming, η αποστολή δηλαδή πολυάριθμων e-mail, με διαφημιστικό περιεχόμενο σε χιλιάδες καταναλωτές-χρήστες του internet. Η τακτική αυτή απαγορεύεται από τα εθνικά δίκαια, είτε βάσει της νομοθεσίας για τον αθέμιτο ανταγωνισμό (στην Ελλάδα ισχύει ο Ν. 146/1914 «περί αθέμιτου ανταγωνισμού»), είτε βάσει του κώδικα δεοντολογίας στο Διαδίκτυο. Με το άρθρο 9 παρ. 5 του Ν. 2251/1994, επιδιώκεται η προστασία της προσωπικότητας του καταναλωτή-χρήστη του διαδικτύου, αφενός έναντι παρενοχλήσεων που πραγματοποιούνται με την απευθείας μετάδοση του διαφημιστικού μηνύματος, μέσω του e-mail, και αφετέρου έναντι της χρησιμοποίησης δεδομένων ή πληροφοριών που αφορούν στο πρόσωπό τους, στην απευθείας μετάδοση του διαφημιστικού μηνύματος. Κάθε, λοιπόν, καταναλωτής-χρήστης του διαδικτύου νομιμοποιείται να στραφεί, ατομικά ή μέσω κάποιας ένωσης καταναλωτών, κατά εκείνου του προμηθευτή, που πραγματοποιεί αθέμιτες εμπορικές πρακτικές και να ζητήσει αποζημίωση για τη ζημία που υπέστη, εξαιτίας των πρακτικών αυτών. Μπορεί, δε, να ζητήσει δικαστικά και παύση της εν λόγω πρακτικής, καθώς και παράλειψή της στο μέλλον (άρθρο 9θ παρ. 1 Ν. 3587/2007). Η τακτική αυτή επίσης απαγορεύεται από την Οδηγία 2002.58 όπου στο άρθρο 13 αναφέρεται ότι « η χρησιμοποίηση αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση (συσκευές αυτόματων κλήσεων), τηλεομοιοτυπικών συσκευών (φαξ) ή ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνον στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους».

### **3.3 Απάτη μέσω του διαδικτύου – Κίνδυνοι από τη χρήση Internet Banking**

Από τη σκοπιά του ποινικού δικαίου κατά τη χρήση του Διαδικτύου είναι δυνατό να τελεστούν απάτες μέσω υπολογιστή όπου ο υπολογιστής είναι απλώς το μέσο τέλεσης της κοινής απάτης ( ΠΚ 386) αλλά και απάτες με υπολογιστή όπου το οικονομικό όφελος ή ζημιά προκύπτει με απευθείας παρέμβαση στον υπολογιστή στο πρόγραμμα και στα δεδομένα του (ΠΚ 386Α). Στην Ευρωπαϊκή ένωση ισχύει η Απόφαση-πλαίσιο του Συμβουλίου με αριθμό 2001/413/ΔΕΥ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών. Οι νέες διαδικτυακές υποδομές και η συνεχής ανάπτυξη της τεχνολογίας δημιουργούν ολόένα και περισσότερες απειλές στις ηλεκτρονικές συναλλαγές και κατ' επέκταση στην ηλεκτρονική τραπεζική. Επειδή, δε, οι περισσότερες τράπεζες προσφέρουν σήμερα on-line υπηρεσίες, παρατηρείται αύξηση στην συχνότητα των ηλεκτρονικών επιθέσεων τα τελευταία χρόνια, παρά τις καταβαλλόμενες προσπάθειες από πλευράς τραπεζών για χρήση εξελιγμένων μεθόδων, ώστε να διασφαλίζονται οι τραπεζικές συναλλαγές. Το φαινόμενο της απειλούμενης ασφάλειας των ηλεκτρονικών συναλλαγών, όπως και στο

προηγούμενο κεφάλαιο αναφέραμε, δικαιολογεί την εν μέρει επιφυλακτική στάση των πελατών των τραπεζών απέναντι στην ηλεκτρονική τραπεζική, καθόσον στην σχέση πελάτη – τράπεζας εμφιλοχωρεί το στοιχείο της άκρας εμπιστοσύνης, ειδικά δε ως προς τα προσωπικά και οικονομικά τους στοιχεία.

Η πραγματικότητα, ωστόσο, αποδεικνύει ότι παρά τις όποιες υπάρχουσες αδυναμίες στα συστήματα e-banking των τραπεζών, η μεγαλύτερη απειλή προέρχεται από κακόβουλες ενέργειες τρίτων, επίδοξων δηλαδή εισβολέων. Τα άτομα αυτά, εκμεταλλεζόμενα κυρίως αδυναμίες τόσο στα συστήματα όσο και στην ανυποψίαστη διαχείριση αυτών από τους πελάτες, κατορθώνουν να παραπλανήσουν τους τελευταίους και, τελικά, να αποσπάσουν πληροφορίες για τα ευαίσθητα προσωπικά τους στοιχεία, με σκοπό να αποκομίσουν παρανόμως προσωπικό οικονομικό όφελος. Οι εισβολείς μπορούν να εισχωρήσουν σε τράπεζες, οι οποίες ήδη εφαρμόζουν σύστημα ηλεκτρονικής τραπεζικής, με τέτοιες μεθόδους απάτης, ώστε να είναι σε θέση είτε να εκμαιεύουν τις απαραίτητες πληροφορίες απευθείας από τους χρήστες του ηλεκτρονικού τραπεζικού συστήματος, είτε να τις υφαρπάζουν με τεχνικές παρακολούθησης κατά την εισαγωγή τους.

Οι κυριότερες αυτές μέθοδοι είναι το phishing (αποστολή πλαστών e-mail), το pharming (επιλογή link από πελάτη στο e-mail του), τα spam (δημιουργία πλαστών δικτυακών τόπων τραπεζών) και keyloggers και οι δούρειοι ίπποι ή αλλιώς trojan horses (εγκατάσταση κακόβουλου λογισμικού).



### **3.4 Εγκλήματα κατά της ηθικής και της αξιοπρέπειας-Προστασία ανηλίκων.**

#### **Προστασία από παράνομο και βλαβερό περιεχόμενο**

Παράνομο και βλαβερό περιεχόμενο που θίγει την προσωπικότητα και την ηθική των ατόμων αποτελούν η δυσφήμιση μέσω του διαδικτύου και η διάδοση πορνογραφικού υλικού. Ο προσβληθείς στην προσωπικότητα του από κάποιο μήνυμα που διακινείται στο διαδίκτυο προστατεύεται από τις διατάξεις 361, 362, 366 και 367 του Π.Κ. Δυσχερέστερο είναι το ζήτημα της διάδοσης πορνογραφικού υλικού στο διαδίκτυο ιδιαίτερα σε σχέση με τους ανηλίκους και την προστασία τους από την έκθεση σε αυτό.

Στην Ευρωπαϊκή Ένωση έχουν ληφθεί και ισχύουν αρκετά μέτρα για την αντιμετώπιση αυτού του είδους εγκληματικότητας.

- Η Απόφαση του Συμβουλίου με αριθμό 2000/C 8/06 που περιέχει προτροπές του Συμβουλίου προς τα κράτη μέλη και την Επιτροπή ώστε να ληφθούν μέτρα για την προστασία των ανηλίκων στα οπτικοακουστικά μέσα και στο Ίντερνετ,
- Η Σύσταση με αριθμό 98/560/EK όπου αναφέρονται οι συστάσεις του Συμβουλίου στα κράτη μέλη για την προστασία των ανηλίκων και της ανθρώπινης αξιοπρέπειας στις οπτικοακουστικές υπηρεσίες και τις υπηρεσίες πληροφόρησης,
- Η Απόφαση του Συμβουλίου με αριθμό 2000/375/ΔΕΥ όπου γίνεται λόγος για τα μέτρα που λαμβάνουν τα κράτη μέλη της Ευρωπαϊκής Ένωσης ώστε οι χρήστες του διαδικτύου να βοηθήσουν στην ποινική δίωξη της παραγωγής, επεξεργασίας, διανομής και κατοχής πορνογραφικού υλικού με θέμα παιδιά,
- Η Απόφαση του Συμβουλίου με αριθμό 2001/C 213/0301 όπου υπάρχουν οι προτροπές του Συμβουλίου της Ευρωπαϊκής Ένωσης προς τα κράτη μέλη για την προστασία των ανηλίκων σε όλα τα οπτικοακουστικά μέσα και για την προστασία των ανηλίκων στο ψηφιακό περιβάλλον και με την συμμετοχή των γονέων.
- Η Απόφαση του Συμβουλίου με αριθμό 1999/C 362/06 όπου αναφέρεται ότι τα κράτη μεταξύ τους πρέπει να συνεργάζονται ώστε να διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη ποινικών αδικημάτων που αφορούν την παιδική πορνογραφία στο Ίντερνετ,
- Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 65/02 για την αξιολόγηση του περιεχομένου των βιντεοπαιχνιδιών και των ηλεκτρονικών παιχνιδιών,

- Η Απόφαση 276/1999/ΕΚ για την έγκριση, την διάρκεια, τη χρηματοδότηση και τους στόχους προγράμματος για την προώθηση της ασφαλέστερης χρήσης του Ίντερνετ,
- Η Απόφαση 1151/2003/ΕΚ που τροποποιεί την απόφαση αριθ. 276/1999/ΕΚ και
- Η Ανακοίνωση της Επιτροπής COM/2002/0152 για τα επακόλουθα μέτρα παρακολούθησης του πολυετούς κοινοτικού προγράμματος δράσης για την προώθηση της ασφαλέστερης χρήσης του Διαδίκτυου (Ίντερνετ) μέσω της καταπολέμησης του παράνομου και βλαβερού περιεχομένου στα παγκόσμια δίκτυα.

Ένα ακόμα ζήτημα που τίθεται σχετικά με την χρήση του διαδικτύου από τους ανήλικους είναι η πραγματοποίηση συναλλαγών με ηλεκτρονικά μέσα. Είναι γνωστό ότι οποιαδήποτε συναλλαγή με ανήλικο είναι άκυρη και μπορεί να επισύρει ποινή για τον αντισυμβαλλόμενο εφόσον το περιεχόμενό της δεν απευθύνεται σε παιδιά και εφήβους. Στην περίπτωση όμως των ηλεκτρονικών συναλλαγών δεν είναι πάντα δυνατή η εξακρίβωση των στοιχείων του καταναλωτή. Για την προστασία των προμηθευτών που δραστηριοποιούνται μέσω κάποιας ιστοσελίδας είναι απαραίτητη η αναγραφή στους όρους χρήσης του site ότι δεν επιτρέπονται οι συναλλαγές με ανήλικους και ότι η ιστοσελίδα δεν φέρει καμία ευθύνη.

Τα sites με σελίδες του διαδικτύου ήταν πάντα ο αγαπημένος στόχος των επιτιθέμενων και αυτό γιατί δεν προσφέρουν ικανοποιητική ασφάλεια ενώ τις επισκέπτονται πολλοί άνθρωποι κάθε μέρα. Η αλλαγή της κεντρικής σελίδας αυτών των sites γίνεται συνήθως για να διαβαστούν από πολλούς πολιτικά ή αντικυβερνητικά μηνύματα. Δεν είναι λίγες οι περιπτώσεις που οργανισμοί και εταιρείες έχουν δει τη φήμη τους να πληγώνεται από τέτοιες επιθέσεις. Μεγάλες εταιρείες, κυβερνητικοί οργανισμοί και στρατιωτικά προγράμματα είναι οι κύριοι στόχοι. Ένας άλλος τρόπος για να τροποποιηθούν οι ιστοσελίδες ενός site που βλέπουν οι χρήστες είναι να αλλάξει η IP διεύθυνση που υποτίθεται πως έχει από την υπηρεσία ονοματολογίας (Domain Name Service) ο κόμβος αυτός. Για παράδειγμα αν η IP διεύθυνση του κόμβου [www.ece.upatras.gr](http://www.ece.upatras.gr) ήταν 150.140.130.1, θα μπορούσε να αλλάξουν τα στοιχεία της βάσης δεδομένων του DNS και να δείχνει σε ένα άλλο site με μη έγκυρες πληροφορίες με σκοπό την παραπληροφόρηση του ενδιαφερόμενου επισκέπτη.

#### 4. ΕΙΔΗ ΕΠΙΘΕΣΕΩΝ ΚΑΙ ΤΕΧΝΙΚΕΣ<sup>14</sup>

Μια εισβολή στο σύστημα αποτελεί απειλή που προκαλείται σκόπιμα και πραγματοποιείται από οντότητες που έχουν σκοπό την παραβίαση της ασφάλειας. Οι εισβολές συνήθως έχουν σαν στόχο την καταστροφή, την υποκλοπή ή την τροποποίηση πληροφοριών. Με αυτό τον τρόπο αποκαλύπτονται πληροφορίες οπότε έχουμε απώλεια εμπιστευτικότητας ή τροποποιούνται άρα έχουμε παραβίαση της ακεραιότητας των πληροφοριών.

Οποιαδήποτε προσπάθεια η οποία καταστρατηγεί τους κανόνες ασφάλειας, όπως αυτοί έχουν καθοριστεί μέσω της πολιτικής ασφάλειας η οποία με τη σειρά της προσδιορίζει τους επιτρεπτούς τρόπους πρόσβασης στα αντικείμενα του συστήματος, θεωρείται ως παραβίαση των κανόνων ασφάλειας.

Οι εισβολές μπορούν να διακριθούν σε άμεσες και έμμεσες.

- Άμεσες εισβολές (direct attacks)

Θεωρούνται αυτές που στοχεύουν απευθείας στο αντικείμενο στόχο. Βέβαια κατά τη διαδικασία εισβολής μπορεί να υπάρξουν ενδιάμεσες επιθέσεις σε τμήματα του συστήματος πριν οδηγηθεί ο εισβολέας στο αντικείμενο στόχο. Στην περίπτωση αυτή και οι ενδιάμεσες επιθέσεις θεωρούνται άμεσες εισβολές.

- Έμμεσες εισβολές (indirect attacks)

Θεωρούνται αυτές που έχουν σαν στόχο τη συλλογή πληροφοριών για ένα αντικείμενο χωρίς να στοχεύουν απευθείας στο αντικείμενο αυτό. Για παράδειγμα η αναζήτηση έμμεσων πληροφοριών σε μια βάση δεδομένων η οποία μπορεί να οδηγήσει σε συλλογή πληροφοριών εμπιστευτικών για ένα αντικείμενο.

Διακρίνονται δύο είδη επιθέσεων οι παθητικές και οι ενεργητικές.

- Παθητικές (passive)

Θεωρούνται αυτές που έχουν σαν στόχο την παρακολούθηση ενός συστήματος και τη συλλογή πληροφοριών για τον τρόπο λειτουργίας του. Γενικά είναι δύσκολο να εντοπισθεί μια παθητική εισβολή διότι συνήθως δεν απαιτεί αλληλεπίδραση με το σύστημα και δεν διαταράσσει την ομαλή λειτουργία του. Ως παράδειγμα μπορεί να θεωρηθεί η παρακολούθηση κυκλοφορίας σε ένα δίκτυο δεδομένων. Η κρυπτογράφηση μπορεί να λύσει μερικώς το πρόβλημα διότι η ύπαρξη και μόνο κίνησης σε ένα δίκτυο μπορεί να προκαλέσει αποκάλυψη πληροφοριών αναλύοντας

<sup>14</sup> Κωνσταντίνος Αντωνής, Ασφάλεια Υπολογιστικών Συστημάτων, Λαμία 2003

για παράδειγμα χρόνους και συχνότητες μετάδοσης ή μήκος πληροφορίας ανεξάρτητα από περιεχόμενο.

- Ενεργητικές (active)

Θεωρούνται αυτές που προκαλούν αλλαγές στη συμπεριφορά ενός συστήματος. Για παράδειγμα η παρεμβολή μηνυμάτων σε ένα δίκτυο, η πρόκληση καθυστέρησης, η αναδιάταξη τους, η αναπαραγωγή ή και η διαγραφή υπαρχόντων μηνυμάτων, η σκόπιμη εκμετάλλευση του λογισμικού του συστήματος για την πρόκληση ζημιάς κλπ. Μια απλή ενέργεια όπως αυτή της τροποποίησης μια αρνητικής αναγνώρισης (NACK) από ένα εξυπηρετητή δεδομένων (database server) σε θετική(ACK) μπορεί να προκαλέσει μεγάλη σύγχυση ή και ζημιά. Οι ενεργητικές επιθέσεις σε αντίθεση με τις παθητικές μπορούν να εντοπιστούν ευκολότερα αν έχουν ληφθεί τα κατάλληλα μέτρα.

#### **4.1 Επίθεση σε ιστοσελίδες**

Τα sites με σελίδες του διαδικτύου ήταν πάντα ο αγαπημένος στόχος των επιτιθέμενων και αυτό γιατί δεν προσφέρουν ικανοποιητική ασφάλεια ενώ τις επισκέπτονται πολλοί άνθρωποι κάθε μέρα. Η αλλαγή της κεντρικής σελίδας αυτών των sites γίνεται συνήθως για να διαβαστούν από πολλούς πολιτικά ή αντικυβερνητικά μηνύματα. Δεν είναι λίγες οι περιπτώσεις που οργανισμοί και εταιρείες έχουν δει τη φήμη τους να πληγώνεται από τέτοιες επιθέσεις. Μεγάλες εταιρείες, κυβερνητικοί οργανισμοί και στρατιωτικά προγράμματα είναι οι κύριοι στόχοι. Ένας άλλος τρόπος για να τροποποιηθούν οι ιστοσελίδες ενός site που βλέπουν οι χρήστες είναι να αλλάξει η IP διεύθυνση που υποτίθεται πως έχει από την υπηρεσία ονοματολογίας (Domain Name Service) ο κόμβος αυτός. Για παράδειγμα αν η IP διεύθυνση του κόμβου [www.ece.upatras.gr](http://www.ece.upatras.gr) ήταν 150.140.130.1, θα μπορούσε να αλλάξουν τα στοιχεία της βάσης δεδομένων του DNS και να δείχνει σε ένα άλλο site με μη έγκυρες πληροφορίες με σκοπό την παραπληροφόρηση του ενδιαφερόμενου επισκέπτη.

#### **4.2 Επίθεση στο ηλεκτρονικό ταχυδρομείο**

Το πρωτόκολλο SMTP (Simple Mail Transfer Protocol) αποτελεί το TCP/IP πρωτόκολλο επικοινωνίας των MTA (Mail Transfer Agents) της υπηρεσίας του ηλεκτρονικού ταχυδρομείου. Το κυριότερο πρόγραμμα που χρησιμοποιείται και αποτελεί πηγή του προβλήματος είναι το sendmail (σε Berkeley UNIX συστήματα). Πιο πρόσφατα προγράμματα με μεγαλύτερη ασφάλεια έχουν δημιουργηθεί τόσο για

UNIX όσο και για Windows λειτουργικά συστήματα. Στη κατηγορία αυτή περιέχονται προβλήματα που προκύπτουν από τη προβληματική χρήση του SMTP. Τέτοια προβλήματα είναι το mail spoofing (απόκρυψη αποστολέα ή αλλαγή διεύθυνσης του), mail bombs (μεγάλος όγκος μηνυμάτων σε συγκεκριμένο παραλήπτη), binmail, mailtrace, mail abuse. Ένα ακόμα πρόβλημα το οποίο αναπτύσσεται όλο και περισσότερο σήμερα και μπορεί να κατηγοριοποιηθεί κάτω από τον ευρύτερο όρο mail, είναι το spamming, που είναι η παράνομη χρήση mail relays για την αποστολή μηνυμάτων ακατάλληλου ή αδιάφορου περιεχομένου σε ένα μεγάλο αριθμό χρηστών.

#### **4.3 Επίθεση με εύρεση των κωδικών πρόσβασης**

Οι επιθέσεις που έχουν γίνει εδώ συνδέονται με τη λάθος διαμόρφωση συστημάτων και κυρίως αυτή που αφορά το δίκτυο. Σε αυτή τη περίπτωση παραμένουν τα αρχικά συνθηματικά που δημιουργούνται κατά την εγκατάσταση ενός λογισμικού ή συστήματος και ο διαχειριστής δεν τα αλλάζει. Επίσης μπορεί να παραμείνουν τα αρχικά δικαιώματα προσπέλασης που δεν είναι κατά ανάγκη ασφαλή. Η τρωτότητα των κωδικών πρόσβασης είναι και η πιο συχνή μορφή παραβίασης της πρόσβασης. Η εύρεση του κωδικού πρόσβασης ενός χρήστη μπορεί να γίνει με αρκετούς τρόπους:

- αντιγραφή του αρχείου κωδικών και μετέπειτα επεξεργασία του,
- «σπάσιμο» κωδικών πρόσβασης με χρήση προγραμμάτων που προσπαθούν να μαντέψουν passwords κωδικοποιώντας συνήθεις λέξεις,
- «αδύνατοι κωδικοί» που μπορεί εύκολα να βρει κάποιος αν γνωρίζει το πρόσωπο στο οποίο ανήκει ο λογαριασμός.

Επίσης, μπορεί να πραγματοποιηθεί επίθεση με «σπαστήρια» κωδικών. Πρόκειται για προγράμματα (password cracks) τα οποία με είσοδο ένα αρχείο κωδικών πρόσβασης και με χρήση ενός λεξικού συνηθισμένων λέξεων που χρησιμοποιούνται για κωδικοί, προσπαθούν να ανακαλύψουν όσο το δυνατό περισσότερους κωδικούς για πρόσβαση σε κάποιο σύστημα. Τα προγράμματα αυτά τα χρησιμοποιούν και οι διαχειριστές συστημάτων για να προλάβουν παρόμοιες ενέργειες από εισβολείς.

#### **4.4 Επίθεση με «ωτακουστές» (packet sniffers)**

Οι «ωτακουστές» πακέτων (packet sniffers) είναι προγράμματα που μπορούν να παρακολουθούν την κίνηση του δικτύου σε επίπεδο IP πακέτων. Με κατάλληλες τεχνικές, έχουν τη δυνατότητα να ανακατασκευάσουν τα μηνύματα και να κάνουν

αναγνώριση των πρωτοκόλλων που περνούν πάνω από το δίκτυο. Τα προγράμματα αυτά τρέχουν συνήθως σε τοπικά δίκτυα (Ethernet) και «κλέβουν» κωδικούς πρόσβασης ή παρακολουθούν τις ηλεκτρολογήσεις από συγκεκριμένους σταθμούς εργασίας. Με κατάλληλους μηχανισμούς ανασυνθέτουν τα πακέτα που μπορεί να έχουν χρήσιμες πληροφορίες χωρίς όμως να επηρεάζουν το περιεχόμενό τους. Ο τρόπος επίθεσης με αυτούς δείχνει μία κλιμάκωση στον τρόπο δράσης: ξεκινά από απλή ανίχνευση του στόχου και αφού εντοπίσει παραλείψεις στην ασφάλεια, εισβάλλει, σβήνει τα ίχνη, αποδυναμώνει την άμυνα του συστήματος και εγκαθιστά Trojans για την εξάπλωσή του. Η χρήση ενός sniffer απαιτεί προνόμια διαχειριστή, αλλά σήμερα ο καθένας είναι «διαχειριστής» του προσωπικού του συστήματος και μάλιστα με σύνδεση στο διαδίκτυο.

#### **4.5 Επίθεση με πλαστογράφηση της IP διεύθυνσης (ip spoofing)**

Η τεχνική αυτή βασίζεται στη δυνατότητα την οποία μπορεί να έχει ένας κόμβος να ισχυρίζεται πως έχει την IP διεύθυνση ενός άλλου. Από την στιγμή που πολλά συστήματα ορίζουν ποια πακέτα επιτρέπονται και ποια όχι να εισέλθουν σε ένα δίκτυο ανάλογα με την IP διεύθυνση του αποστολέα, αυτή είναι μία χρήσιμη τεχνική σε έναν εισβολέα. Με τον τρόπο αυτό είναι δυνατό να διασφαλίσει την προσπέλαση σε υπηρεσίες που επιτρέπονται σε κόμβους με συγκεκριμένες IP διευθύνσεις. Επίσης, μπορεί να σταλεί από ένα εξωτερικό δίκτυο ένα πακέτο δεδομένων που να φαίνεται πως έχει σταλεί από εσωτερικό κόμβο ενός προφυλαγμένου δικτύου, δίνοντας έτσι τη δυνατότητα να εκτελεστούν εντολές που επιτρέπονται να εκτελεστούν μόνο από εσωτερικούς κόμβους. Η πλαστογράφηση της IP διεύθυνσης (ip spoofing) είναι μία νέα τεχνική επίθεσης σε δικτυωμένους υπολογιστές που συνεχώς όμως κερδίζει έδαφος, ενώ είναι όλο και περισσότεροι αυτοί που τη χρησιμοποιούν. Γενικά είναι δύσκολο να εντοπιστούν τέτοιες επιθέσεις αφού η πρώτη εντύπωση είναι ότι η επίθεση έχει προέλθει από τη πλαστή διεύθυνση. Η επαλήθευση συνήθως αργεί επιτρέποντας έτσι στον επιτιθέμενο να δρα ανενόχλητος για κάποιο διάστημα.

- Επίθεση με «πειρατεία» IP διεύθυνσης

Πρόκειται για μία σχετικά σύνθετη επίθεση. Με αυτή, ένας εισβολέας μπορεί να καταλάβει την σύνδεση ενός χρήστη με έναν εξυπηρετητή και να εκτελεί εντολές που έχει δικαίωμα ο χρήστης. Επιπλέον, μπορεί να βλέπει τι γράφει ο χρήστης.

- Επίθεση με παραποίηση IP διεύθυνσης

Αποτελεί ένα είδος επίθεσης που εμφανίστηκε το 1998. Βασίζεται στο IP spoofing ενώ εκμεταλλεύεται και αδυναμίες της υλοποίησης των IP και ICMP (Internet Control Message Protocol) πρωτοκόλλων σε δικτυακές συσκευές.

#### **4.6 Επίθεση με υπερχείλιση προσωρινής μνήμης**

Οι επιτιθέμενοι μπορούν να εισβάλουν σε ένα σύστημα χωρίς να χρειάζεται να κάνουν login σε αυτό. Αντίθετα χρησιμοποιούν ένα πρόγραμμα που ήδη τρέχει/υπάρχει στον υπολογιστή και του δίνουν να εκτελέσει ένα κομμάτι εντολών. Για να το πετύχουν αυτό φτιάχνουν ένα μεγάλο τμήμα από χαρακτήρες που περιέχει τις εντολές που θέλουν να εκτελεστούν και το εισάγουν σαν παράμετρο εισόδου στο πρόγραμμα. Κανονικά το πρόγραμμα δεν εκτελεί τον κώδικα που περνά σαν παράμετρος. Αν όμως το μήκος του κειμένου της παραμέτρου είναι μεγαλύτερο από το μήκος που έχει δοθεί σαν χώρος για το πέρασμα της παραμέτρου, τότε μέρος του περνά στον χώρο του εκτελέσιμου προγράμματος και εκτελείται. Ο κώδικας εκτελείται με ότι προνόμια έχει το πρόγραμμα που εκτελείται. Αν λοιπόν μία διεργασία του συστήματος τρέχει με προνόμια διαχειριστή και καταφέρει ο επιτιθέμενος να περάσει με παράμετρο τον κώδικά του, τότε θα μπορέσει να εκτελέσει εντολές που θα του δώσουν διάφορα προνόμια (root access).

#### **4.7 Επίθεση μέσω άρνησης παροχής υπηρεσιών (DoS)**

Μια denial-of-service (DoS) επίθεση είναι μια κακόβουλη προσπάθεια από ένα μεμονωμένο πρόσωπο ή μια ομάδα ανθρώπων να αναγκάσει το site ή τον κόμβο του θύματος να αρνηθεί υπηρεσία στους πελάτες του. Όταν αυτή η προσπάθεια προέρχεται από ένα συγκεκριμένο host του δικτύου, συνιστά μια DoS επίθεση. Από την άλλη πλευρά, είναι επίσης δυνατό πολλοί κακόβουλοι hosts να συντονίζονται για να πλημμυρίσουν το θύμα με μια αφθονία πακέτων επίθεσης έτσι ώστε η επίθεση να πραγματοποιείται ταυτόχρονα από πολλά σημεία. Σε αυτήν την περίπτωση πρόκειται για μια κατανεμημένη επίθεση άρνησης υπηρεσίας (DDoS-Distributed Denial of Service Attack). Η μεθοδολογία της επίθεσης αυτής είναι απλή: αν σταλούν σε έναν εξυπηρετητή περισσότερες αιτήσεις από αυτές που μπορεί να εξυπηρετήσει τότε οι λειτουργίες που επιβάλλουν οι αιτήσεις αυτές δεσμεύουν πόρους του συστήματος με αποτέλεσμα μετά από κάποιο σύντομο χρονικό διάστημα, το σύστημα να μην είναι σε θέση να εξυπηρετήσει τους χρήστες και να μην μπορεί να παρέχει αρκετούς πόρους

για την εκτέλεση διεργασιών. Παράδειγμα αποτελεί το mail spam, που είναι η επαναλαμβανόμενη αποστολή μηνυμάτων προκειμένου να φτάσει το σύστημα στα όρια της χωρητικότητας του. Τα εργαλεία που χρησιμοποιούνται είναι εξειδικευμένα και έχουν αποδείξει πως τα συστήματα ανίχνευσης εισβολών δεν τα καταφέρνουν καλά σε αυτές τις επιθέσεις.

#### **4.8 Επίθεση με «εχθρικό κώδικα».**

Πρόκειται για κώδικα ο οποίος δείχνει να ξεκινά διαδικασίες χρηστών αλλά στην πραγματικότητα προσπαθεί να μαζέψει ή να εκμεταλλευτεί ευαίσθητα δεδομένα.

- Επίθεση με Δούρειους Ίππους

Όπως αναφέραμε και σε προηγούμενο κεφάλαιο, οι δούρειοι ίπποι είναι προγράμματα που προσποιούνται ότι έχουν άλλες λειτουργίες από αυτές που πραγματικά υλοποιούν. Συνήθως κρύβονται σε άλλα προγράμματα αλλά μπορούν να βρίσκονται και μεμονωμένα.

- Επίθεση με «σκουλήκια» (Worms)

Είναι προγράμματα που δρουν αυτόνομα και μεταφέρονται από site σε site εκμεταλλευόμενα διάφορες τρύπες του συστήματος. Σε κάθε site το σκουλήκι δρα αυτόνομα και ανεξάρτητα από τα υπόλοιπα sites που προσπαθεί να μεταφερθεί.

- Επίθεση με Ιούς (Viruses)

Πρόκειται για τα πιο γνωστά προγράμματα που προσπαθούν να εγκατασταθούν σε κάποιους υπολογιστές και να προσβάλουν την ακεραιότητα του συστήματος με διάφορους τρόπους (από τους πιο ανώδυνους, αφήνοντας μια υπογραφή-ίχνος της παρουσίας τους ή πιο επώδυνους, με απώλεια δεδομένων, καταστροφή της διαμόρφωσης του συστήματος). Από τα παραπάνω λοιπόν φαίνεται η σχέση που υπάρχει ανάμεσα σε αυτό που ονομάζουμε εχθρικό κώδικα (και περιλαμβάνει τους ιούς, τα σκουλήκια, τους δούρειους ίππους, τις πίσω πόρτες) και τους hackers, και πως αυτοί το χρησιμοποιούν προκειμένου να εισβάλουν σε ένα σύστημα και να αποκτήσουν τον έλεγχό του ή να εκτελέσουν διάφορες διεργασίες, όπως το να καταστρέψουν αρχεία και δεδομένα.

### **5. ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ<sup>15</sup>**

#### **5.1 Εισαγωγή**

<sup>15</sup> Χρήστος Α. Ηλιούδης, Κων/νος Ράντος, Θέματα ασφάλειας των εφαρμογών κινητών τηλεφώνων, Λαμία



Τα ασύρματα δίκτυα (wireless LAN – WLAN) αποτελούν μία ευέλικτη λύση, ως επέκταση των ενσύρματων δικτύων ή ακόμα ως εναλλακτική λύση για υλοποίηση ολοκληρωμένων δικτυακών λύσεων.

Τα πρώτα ασύρματα δίκτυα που εμφανίστηκαν ήταν τα ραδιοδίκτυα δεδομένων (Data) τεχνολογίας TCP/IP. Η τεχνολογία των ασυρμάτων δικτύων μετάδοσης πακέτων άρχισε να αναπτύσσεται στην δεκαετία 1970-1980, αν και η μεγάλη ανάπτυξή της συμπίπτει με την διάδοση των μικροϋπολογιστών στην δεκαετία 1980-1990. Λόγω των

ιδιαίτερων χαρακτηριστικών του μέσου μεταδόσεως τα ασύρματα δίκτυα χρησιμοποιούν εξειδικευμένα πρωτόκολλα για το υποεπίπεδο πρόσβασης μέσου (Medium Access Control) και το επίπεδο σύνδεσης δεδομένων (Data Link Layer) και συχνά και για ανώτερα επίπεδα (π.χ. δρομολόγηση πακέτων).

Σήμερα είναι διαθέσιμος ένας πολύ μεγάλος αριθμός από προϊόντα ασύρματης επικοινωνίας που βασίζονται σε νέες τεχνολογίες και νέα πρότυπα. Τα τελευταία χρόνια οι κινητοί υπολογιστές (notebook, laptop, palmtop, smartphones) είναι διαθέσιμοι και προσιτοί για το ευρύ κοινό, αφού έχουν πλέον χαμηλό κόστος, υπολογιστική ισχύ και ποιότητα υπηρεσιών ίδια με τους σταθερούς υπολογιστές. Όλα αυτά έχουν σαν αποτέλεσμα την έρευνα ανάπτυξης προτύπων για την υποστήριξη των ασύρματων επικοινωνιών.

## **5.2 Χαρακτηριστικά των Ασύρματων δικτύων**

Ένα WLAN είναι ένα δίκτυο τοπικής περιοχής χωρίς καλώδια. Τα ασύρματα δίκτυα χρησιμοποιούν τα ραδιοκύματα σε αντίθεση με τα ενσύρματα δίκτυα στα οποία οι τερματικοί σταθμοί (ή οι πελάτες) στέλνουν και ανακτούν τα δεδομένα χρησιμοποιώντας τα καλώδια.

Η οικογένεια προτύπων 802.11 έχουν καθιερωθεί στα ασύρματα δίκτυα, τα οποία χρησιμοποιούν το πρωτόκολλο CSMA (carrier sense multiple access), όπως και το MAC (medium access control) με αποφυγή σύγκρουσης CA (collision avoidance).

## **5.3 Ευπάθειες και επιθέσεις κατά της ασφάλειας στα ασύρματα δίκτυα**

Οι επιθέσεις ενάντια στο 802.11b και στις άλλες ασύρματες τεχνολογίες θα αυξάνονται σε αριθμό και ποιότητα ανάλογα με την εξάπλωση της τεχνολογίας και διακρίνονται στις παρακάτω κατηγορίες:

- ✓ Επιθέσεις παράνομης χρήσης της ασύρματης επικοινωνίας

- ✓ Επιθέσεις υποκλοπής και μη εξουσιοδοτημένης παρακολούθησης της κίνησης (Interception and unauthorized monitoring of wireless traffic)
- ✓ Επιθέσεις παρεμβολής παρασίτων (Jamming)
- ✓ Επιθέσεις πελάτη-προς-πελάτη (Client-to-Client attacks)
- ✓ Επιθέσεις εναντίων των passwords των σημείων πρόσβασης (Brute force attacks against access point passwords)
- ✓ Επιθέσεις κατά της κρυπτογράφησης (Encryption attacks)
- ✓ Έλλειψη κατάλληλων ρυθμίσεων (Misconfigurations)

### 5.3.1 Επιθέσεις παράνομης χρήσης της ασύρματης επικοινωνίας

Οι επιθέσεις παράνομης χρήσης είναι βασισμένες στην εγκατάσταση παράνομων συσκευών ή τη δημιουργία νέων ασύρματων δικτύων. Διακρίνονται στις παρακάτω κατηγορίες επιθέσεων:

- *Μη εξουσιοδοτημένοι Πελάτες ( Unauthorized Clients)*

Ένας επιτιθέμενος προσπαθεί να συνδέσει έναν ασύρματο πελάτη, π.χ. έναν laptop ή ένα PDA, με ένα σημείο πρόσβασης χωρίς να έχει έγκριση. Τα σημεία πρόσβασης μπορούν να διαμορφωθούν κατάλληλα για να απαιτήσουν έναν κωδικό πρόσβασης για την πρόσβαση των πελατών. Εάν δεν υπάρχει κανένας κωδικός πρόσβασης, ένας εισβολέας μπορεί να συνδεθεί με το εσωτερικό δίκτυο απλά με τη ενεργοποίηση της επικοινωνίας του πρόσβασης με το σημείο πρόσβασης μέσω μιας ασύρματης κάρτας. Επιπλέον μερικά σημεία πρόσβασης, έχοντας κακή πολιτική ασφάλειας, χρησιμοποιούν τον ίδιο κωδικό πρόσβασης για όλες τις ασύρματες συνδέσεις.

- *Μη εξουσιοδοτημένα σημεία πρόσβασης (Unauthorized or Rogue Access Points)*

Ένας οργανισμός που διαθέτει ασύρματο δίκτυο μπορεί να μην γνωρίζει την εγκατάσταση (παράνομης) επιπλέον access points στο υπάρχον δίκτυο. Αυτή η έλλειψη γνώσης θα μπορούσε να οδηγήσει στην προηγούμενη επίθεση, με τους παράνομους χρήστες να αποκτούν πρόσβαση στους εταιρικούς πόρους μέσω ενός σημείου πρόσβασης που δεν ακολουθεί ή δεν είναι πιστοποιημένο από την διαχείριση δικτύου του οργανισμού. Επιβάλλεται λοιπόν από τους οργανισμούς να εφαρμόσουν μια πολιτική ασφάλειας για να εξασφαλίσουν καταρχήν την ασφαλή ρύθμιση των σημείων πρόσβασης και επιπλέον το δίκτυο να ανιχνεύεται για την παρουσία μη εξουσιοδοτημένων συσκευών.

### 5.3.2 Επιθέσεις παρακολούθησης της κίνησης (Interception and Monitoring of Wireless Traffic)

Στο ασύρματο δίκτυο, όπως και στο ενσύρματο είναι δυνατό να καταγραφεί και να ελεγχθεί η κυκλοφορία των δεδομένων, αρκεί ο επιτιθέμενος να είναι μέσα στην ακτίνα κάλυψης του σημείου πρόσβασης. Η καταγραφή της κυκλοφορίας του ασύρματου δικτύου γίνεται πιο εύκολα από ότι στο ενσύρματο μια και δεν απαιτείται ενεργητική παρακολούθηση του δικτύου, αρκεί μόνο ένα λογισμικό καταγραφής της κίνησης το οποίο δεν γίνεται αντιληπτό αφού δεν δημιουργεί «ανωμαλίες» στην κυκλοφορία.

- *Ανάλυση ασύρματων πακέτων δεδομένων(Wireless Packet Analysis)*

Ένας έμπειρος επιτιθέμενος συλλαμβάνει την ασύρματη κυκλοφορία χρησιμοποιώντας τεχνικές παρόμοιες με εκείνες που χρησιμοποιούνται στα ενσύρματα δίκτυα. Πολλά από τα εργαλεία ανίχνευσης καταγράφουν δεδομένα όπως όνομα του χρήστη και κωδικός πρόσβασης. Ένας εισβολέας μπορεί στη συνέχεια να μεταμφιεστεί ως νόμιμος χρήστης κάνοντας χρήση αυτών των πληροφοριών .

- *Παρακολούθηση εκπομπής (Broadcast Monitoring)*

Εάν ένα σημείο πρόσβασης συνδέεται με ένα hub και όχι με ένα switch, τα δεδομένα μεταδίδονται σε όλες τις άλλες συνδεδεμένες συσκευές. Έτσι ένας επιτιθέμενος μπορεί να ελέγξει τα ευαίσθητα δεδομένα που μεταδίδονται στο ασύρματο δίκτυο.

- *Κλώνοι σημείων πρόσβασης (Access Point Clone)*

Ένας επιτιθέμενος εγκαθιστά ένα σημείο πρόσβασης με ισχυρότερο σήμα σε σχέση με τα νόμιμα σημεία πρόσβασης. Οι χρήστες προσπαθούν να συνδεθούν με το νόμιμο Access Point αλλά στην ουσία επιχειρούν, χωρίς να το γνωρίζουν, την εγκατάσταση μιας επικοινωνίας με τον κλώνο και αποκαλύπτουν έτσι τους κωδικούς πρόσβασής τους.

### 5.3.3 Επιθέσεις παρεμβολής παρασίτων( jamming)

Οι επιθέσεις παρεμβολής παράσιτων οδηγούν στην άρνηση υπηρεσιών, και εφαρμόζονται εύκολα στα ασύρματα δίκτυα, όπου σε τέτοιες περιπτώσεις η νόμιμη κυκλοφορία δεν μπορεί να φθάσει στους πελάτες ή στο σημείο πρόσβασης εξαιτίας της παράνομης κυκλοφορίας που καταναλώνει τις συχνότητες. Ένας επιτιθέμενος με τον κατάλληλο εξοπλισμό και τα εργαλεία μπορεί εύκολα να πλημμυρίσει τη συχνότητα των 2,4 GHz, αλλοιώνοντας το σήμα έως ότου πάψει να λειτουργεί το

ασύρματο δίκτυο. Επιπλέον, τα ασύρματα τηλέφωνα και άλλες συσκευές που λειτουργούν στη ζώνη των 2,4 GHz μπορούν να προσβάλουν ένα ασύρματο δίκτυο χρησιμοποιώντας αυτήν την συχνότητα.

#### **5.3.4 Επιθέσεις πελάτη-προς-πελάτη (Client-to-Client Attacks)**

Δύο ασύρματοι πελάτες μπορούν να επικοινωνήσουν ασύρματα άμεσα ο ένας στον άλλο, παρακάμπτοντας το σημείο πρόσβασης. Οι χρήστες επομένως πρέπει να αμύνονται όχι μόνο ενάντια σε μια εξωτερική απειλή αλλά και ο ένας ενάντια στον άλλο.

- *Διαμοίραση δεδομένων και επιθέσεις υπηρεσιών TCP/IP (File Sharing and Other TCP/IP Service Attacks)*

Οι ασύρματοι πελάτες που τρέχουν διάφορες TCP/IP υπηρεσίες όπως ένας WEB server ή peer-to-peer προγράμματα (π.χ. KAZAA) είναι εκτεθειμένοι στους ίδιους κινδύνους και στις ίδιες δυσλειτουργίες όπως αντίστοιχα είναι και οι ενσύρματοι χρήστες τους.

- *Επιθέσεις άρνησης υπηρεσιών DOS (Denial of Service)*

Μία ασύρματη συσκευή «πλημμυρίζει» κάποιον ασύρματο πελάτη με άχρηστα πακέτα, προκαλώντας κατάσταση άρνησης εξυπηρέτησης. Επιπλέον, συγκρούσεις με κοινές διευθύνσεις είτε IP είτε MAC, (σκόπιμες ή τυχαίες) μπορούν να προκαλέσουν αδυναμία εξυπηρέτησης.

#### **5.3.5 Επιθέσεις εναντίων των Passwords στα Access Points (Brute Force Attacks Against Access Point Passwords)**

Τα περισσότερα σημεία πρόσβασης χρησιμοποιούν ένα ενιαίο κλειδί ή ένα κωδικό πρόσβασης που μοιράζονται με όλους τους συνδεδεμένους ασύρματους πελάτες τους. Οι επιθέσεις brute force προσπαθούν να ανακαλύψουν αυτό το κλειδί μεθοδικά εξετάζοντας κάθε πιθανό κωδικό πρόσβασης. Ο εισβολέας αποκτά πρόσβαση στο σημείο πρόσβασης μόλις ο κωδικός πρόσβασης αποκαλυφθεί.

Επιπλέον, οι κωδικοί πρόσβασης μπορούν να αποκαλυφθούν μέσω λιγότερο επιθετικών μεθόδων. Ένας πελάτης μπορεί να εκθέσει το σημείο πρόσβασης. Η μη αλλαγή των κλειδιών σε συχνή βάση ή όταν ορισμένοι υπάλληλοι απολύονται αποτελούν περιπτώσεις όπου δημιουργείται το κατάλληλο έδαφος για επιθέσεις. Η διαχείριση ενός μεγάλου αριθμού σημείων πρόσβασης και πελατών περιπλέκει το ζήτημα αυτό, κάτι που ενθαρρύνει τις χαλαρές πρακτικές ασφάλειας.

### **5.3.6 Επιθέσεις εναντίον της κρυπτογράφησης (Attacks against Encryption)**

Το 802.11b χρησιμοποιεί το σύστημα κρυπτογράφησης WEP (wired equivalent privacy). Το WEP έχει γνωστές αδυναμίες οι οποίες δεν αναμένονταν να αντιμετωπιστούν άμεσα. Αν και στο παρελθόν δεν υπήρχαν πολλά εργαλεία για την εκμετάλλευση αυτών των αδυναμιών του WEP οι έμπειροι επιτιθέμενοι μπορούν να εκμεταλλευτούν τις ευπάθειές του.

### **5.3.7 Έλλειψη κατάλληλων ρυθμίσεων (Misconfiguration)**

Σοβαρό πρόβλημα αποτελούν οι περιπτώσεις όπου η πώληση των AP γίνεται με τα εργαλεία ασφάλειας να μην είναι ενεργοποιημένα εξ' ορισμού. Τα μη σωστά ρυθμισμένα APs έθεταν σε σοβαρό κίνδυνο το δίκτυο εκτός αν οι διαχειριστές αντιλαμβάνονταν τους κινδύνους ασφάλειας και διαμόρφωναν κατάλληλα κάθε μονάδα πριν από την εγκατάσταση.

## **5.4 Μηχανισμοί ασφάλειας του προτύπου 802.11**

Όπως και με τα άλλα δίκτυα, η ασφάλεια των WLAN εστιάζεται στον έλεγχο της πρόσβασης και την ιδιωτικότητα. Ο ισχυρός έλεγχος πρόσβασης αποτρέπει τους μη νόμιμους χρήστες να χρησιμοποιούν την υποδομή του ασύρματου δικτύου. Η ιδιωτικότητα εξασφαλίζει ότι μόνο οι χρήστες για τους οποίους προορίζονται τα δεδομένα τα αντιλαμβάνονται. Η μυστικότητα των δεδομένων προστατεύεται με τη χρήση τεχνολογιών κρυπτογράφησης.

Η ασφάλεια του 802.11 περιλαμβάνει τη χρήση μεταξύ άλλων:

- Service Set Identifiers (SSIDs)
- την ανοικτή αυθεντικοποίηση ή με διαμοιραζόμενο κλειδί
- τα στατικά κλειδιά WEP και
- την προαιρετική Media Access Control (MAC) αυθεντικοποίηση.

## **5.5 Τεχνολογίες προστασίας ασύρματων δικτύων**

Γνωρίζοντας ότι η κρυπτογράφηση WEP δεν ήταν αρκετή, διάφοροι προμηθευτές εισήγαγαν μεγαλύτερα κλειδιά, 128-bit ή το 152-bit ακόμη και 256-bit κλειδιά. Εντούτοις αυτές οι παραλλαγές του βασικού WEP κλειδιού ήταν ιδιόκτητες και συχνά μη διαλειτουργικές. Αποδείχθηκε ότι, λόγω των τεχνικών προβλημάτων του WEP, τα μεγαλύτερα κλειδιά δεν πρόσθεταν καμία σημαντική προστασία. Έγινε κατανοητό ότι πρόσθετες αποδεκτές τεχνολογίες ασφάλειας έπρεπε να προστεθούν για να επιτύχουν

τα αποδεκτά επίπεδα ασφάλειας, τεχνολογίες όπως οι : Virtual Private Networks (VPNs) and Remote Access Dial-In User Service (RADIUS) authentication servers

### **5.5.1 Media Access Control (MAC) authentication.**

Μερικοί προμηθευτές WLAN υποστηρίζουν την αυθεντικοποίηση **βασισμένη στη φυσική διεύθυνση, ή τη διεύθυνση MAC**, της κάρτας διεπαφών (NIC). Κάθε AP μπορεί να διαμορφωθεί με έναν κατάλογο διευθύνσεων MAC που συνδέονται με τους υπολογιστές των πελατών στους οποίους επιτρέπεται η πρόσβαση στο AP. Ένα σημείο

πρόσβασης θα επιτρέψει την σύνδεση με έναν πελάτη μόνο εάν η διεύθυνση της MAC

εκείνου του πελάτη ταιριάζει με μια διεύθυνση σε έναν πίνακα αυθεντικοποίησης που χρησιμοποιείται από εκείνο το σημείο πρόσβασης.

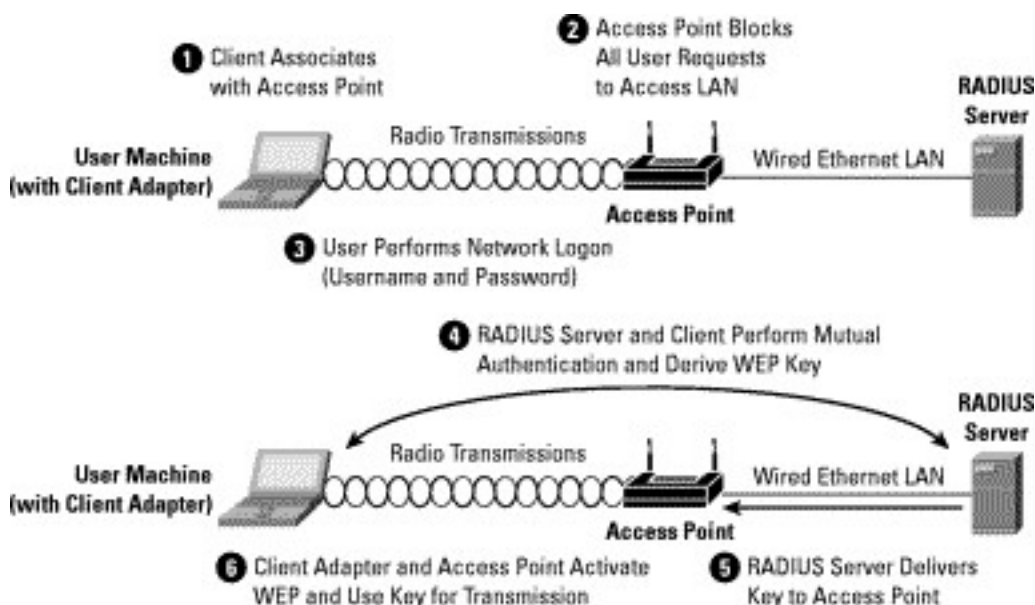
Παρόλα αυτά **η αυθεντικοποίηση με βάση τη MAC** είναι ένα ανεπαρκές μέτρο ασφάλειας, επειδή οι διευθύνσεις της MAC μπορούν να αλλάξουν κατά βούληση, ή ένα NIC μπορεί να χαθεί ή να κλαπεί. Η μέθοδος αυτή παρέχει καλή ασφάλεια αλλά ταιριάζει μόνο σε μικρά δίκτυα.

### **5.5.2 Ασφάλεια χρησιμοποιώντας το πρωτόκολλο EAP (Extensible Authentication Protocol) και το πρότυπο 802.1X**

Μια εναλλακτική λύση ασφάλειας στα ασύρματα δίκτυα εστιάζεται στην ανάπτυξη ενός πλαισίου το οποίο να προσφέρει κεντρική αυθεντικοποίηση και δυναμική διανομή κλειδιού. Μια πρόταση υποβλήθηκε αρχικά από στον οργανισμό προτυποποίησης IEEE από την Cisco Systems, την Microsoft, και από άλλους οργανισμούς, εισήγαγε ένα end-to-end πλαίσιο χρησιμοποιώντας το πρότυπο 802.1X και το **Πρωτόκολλο Επαυξημένης Αυθεντικοποίησης (Extensible Authentication Protocol - EAP)** για να παρέχει αυτήν την ενισχυμένη λειτουργία. Δύο είναι τα κύρια χαρακτηριστικά της πρότασης αυτής:

- Το EAP επιτρέπει ασύρματους clients οι οποίοι μπορεί να υποστηρίζουν διαφορετικούς τύπους αυθεντικοποίησης, και να επικοινωνούν με διαφορετικούς back-end εξυπηρετητές (servers) όπως οι Remote Access Dial-In User Service (RADIUS)
- Το πρότυπο IEEE 802.1X, είναι βασισμένο στον έλεγχο πρόσβασης στο δίκτυο

επάνω στις θύρες (port). Το πρότυπο 802.1X χρησιμοποιεί την επιτυχία των RADIUS (Remote Authentication Dial-In User Service) servers για να παρέχει ένα πιο υψηλό επίπεδο ασφάλειας για τους χρήστες των WLAN. Γνωστό και ως port-based έλεγχος πρόσβασης δικτύου, το 802.1X πρότυπο χρησιμοποιεί το Πρωτόκολλο Έκτατης Αυθεντικοποίησης (EAP) and RADIUS για την αυθεντικοποίηση των clients καθώς



και για την διανομή των κλειδιών.

Το πρωτόκολλο EAP παρέχει μια υποδομή που επιτρέπει στους χρήστες να αυθεντικοποιούνται σε έναν κεντρικό server αυθεντικοποίησης. Όταν ο server δέχεται την απόδειξη της ταυτότητας του πελάτη, το κλειδί στέλνεται στον πελάτη καθώς και στα σημεία πρόσβασης (APs) με τα οποία server έχει καθιερώσει ήδη μια «έμπιστη σχέση.» Αυτή η σχέση αλλά και η χρήση “αμοιβαίας αυθεντικοποίησης”, στην οποία πελάτες και server αποδεικνύουν τις ταυτότητές τους ο ένας στον άλλο, εξασφαλίζει ότι τα σημεία πρόσβασης είναι μοναδικά και πιστοποιημένα. Το πρότυπο 802.1X και το πρωτόκολλο EAP επίσης εξασφαλίζει ότι τα νέα κλειδιά κρυπτογράφησης παράγονται και διανέμονται συχνά. Αυτή η συχνή διανομή είναι γνωστή και ως διανομή “δυναμικού κλειδιού”, και αποτελεί ένα απαραίτητο στοιχείο σε μια καλή λύση ασφάλειας. Με την ελαχιστοποίηση του χρονικού διαστήματος στο οποίο οποιοδήποτε κλειδί κρυπτογράφησης χρησιμοποιείται, το πρότυπο 802.1X και το EAP μειώνουν σημαντικά την πιθανότητα αποκάλυψης του κλειδιού.

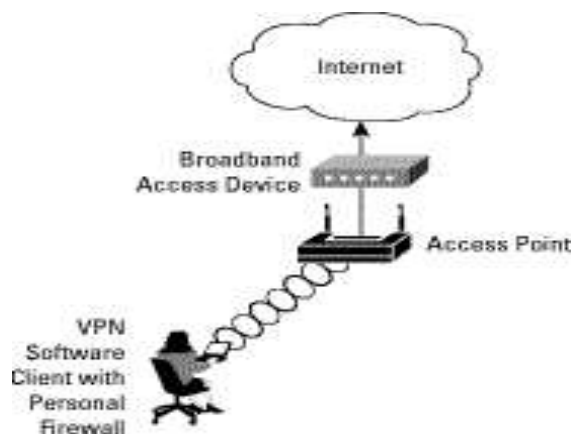
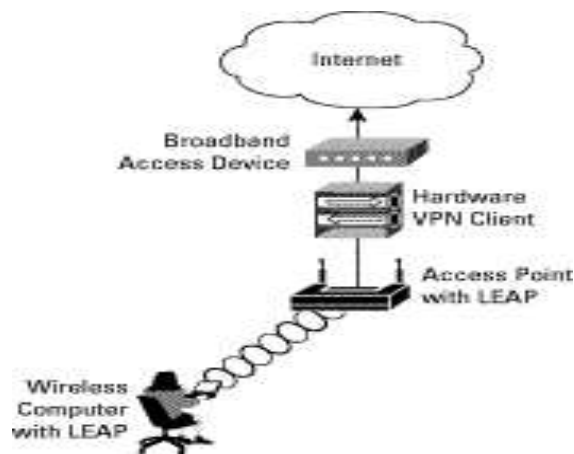
### 5.5.3 RADIUS Authentication

Το πρωτόκολλο *Remote Address Dial-In User Service (RADIUS)* αναπτύχθηκε από την Livingston Enterprises, Inc., σαν ένα πρωτόκολλο αυθεντικοποίησης πρόσβασης σε εξυπηρετητές . Η τεχνολογία RADIUS είναι άλλη μια τυποποιημένη τεχνολογία για την προστασία πρόσβασης στα ασύρματα δίκτυα. Το RADIUS είναι ένα σχέδιο ονόματος και κωδικού πρόσβασης χρηστών που επιτρέπει μόνο στους εγκεκριμένους χρήστες να έχουν πρόσβαση στο δίκτυο. Δεν κρυπτογραφεί και δεν επηρεάζει τα δεδομένα. Την πρώτη φορά που ένας χρήστης ζητήσει πρόσβαση στο δίκτυο, πρέπει να εισαγάγει το όνομα και τον κωδικό πρόσβασής του/της και να τον υποβάλει στον RADIUS εξυπηρετητή. Ο RADIUS εξυπηρετητής είναι αρμόδιος για τη λήψη του αιτήματος σύνδεσης, αυθεντικοποίησης του, δηλαδή ότι υπάρχει κάποιος λογαριασμός του συγκεκριμένου χρήστη, και αν αυτό ισχύει εξασφαλίζει ότι ο χρήστης χρησιμοποιεί τον σωστό κωδικό πρόσβασης πριν τον αφήσει να εισέλθει στο δίκτυο. Τέλος ο RADIUS εξυπηρετητής μπορεί να δράσει και σαν proxy client σε κάποιον άλλο RADIUS εξυπηρετητή ή σε άλλης μορφής αυθεντικοποίησης εξυπηρετητές .

#### **5.5.4 Εικονικό Ιδιωτικό δίκτυο (Virtual Private Network -VPN)**

Η τεχνολογία Εικονικού Ιδιωτικού δικτύου (VPN) χρησιμοποιείται για την προστασία των επικοινωνιών μεταξύ απομακρυσμένων σταθμών μέσω του Διαδικτύου από την δεκαετία του 90'. Αποτελεί μια γνωστή και ήδη ευρέως χρησιμοποιημένη τεχνολογία στον χώρο των επιχειρήσεων, όμως μπορεί εύκολα να επεκταθεί και στους τομείς των ασύρματων μερών ενός ενσύρματου δικτύου. Αν και τα VPNs αναπτύχθηκαν αρχικά για να παρέχουν την από σημείο σε σημείο (point-to-point) κρυπτογράφηση για τις συνδέσεις με το Διαδίκτυο μεταξύ απομακρυσμένων χρηστών και των εταιρικών δικτύων τους, έχουν επεκταθεί πρόσφατα και στα ασύρματα τοπικά δίκτυα (WLANs).





Λειτουργεί με τη δημιουργία ενός ασφαλούς εικονικού «καναλιού» από τον υπολογιστή του χρήστη μέσω του σημείου ή της πύλης πρόσβασης του τελικού χρήστη, μέσω του Διαδικτύου, μέχρι τους κεντρικούς υπολογιστές και τα συστήματα της εταιρίας. Όταν ένας πελάτης ασύρματου δικτύου WLAN χρησιμοποιεί το VPN, τα δεδομένα της επικοινωνίας παραμένουν κρυπτογραφημένα έως ότου φθάσουν στην πύλη VPN, η οποία είναι πίσω από το ασύρματο σημείο (AP). Ένα Εικονικό Ιδιωτικό δίκτυο δουλεύει μέσω ενός VPN server στην έδρα της επιχείρησης, δημιουργώντας ένα πλαίσιο κρυπτογράφησης για τα δεδομένα που μεταφέρονται στους υπολογιστές έξω από τα εταιρικά γραφεία. Το ειδικό VPN λογισμικό που χρησιμοποιείται στον απομακρυσμένο υπολογιστή ή το lap-top χρησιμοποιεί το ίδιο πλαίσιο κρυπτογράφησης, διευκολύνοντας τα δεδομένα να μεταφέρονται ακίνδυνα και προς τις δυο κατευθύνσεις χωρίς την πιθανότητα παρεμπόδισης ή αλλοίωσης τους. Αφού το VPN κρυπτογραφεί ολόκληρη τη σύνδεση από τον υπολογιστή (PC) έως την πύλη του Εικονικού Ιδιωτικού δικτύου στην καρδιά

του εταιρικού δικτύου, το ασύρματο τμήμα δικτύου μεταξύ του υπολογιστή και του σημείου πρόσβασης Access Point είναι επίσης κρυπτογραφημένο. Κατά συνέπεια, οι εισβολείς εμποδίζονται αποτελεσματικά στο να παρεμποδίζουν τις επικοινωνίες του δικτύου.

## 6. ΜΕΤΡΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΕΠΙΘΕΣΕΩΝ<sup>16</sup>

Τα μέτρα προστασίας (ή αντίμετρα) είναι όλες εκείνες οι διαδικασίες, τεχνικές, ενέργειες και συσκευές που περιορίζουν τις ευπάθειες ενός συστήματος. Οι διαφορετικοί τύποι αντίμετρων έχουν ως αποτέλεσμα την ανάλυση του προβλήματος της ασφάλειας στις ακόλουθες συνιστώσες:

- Φυσική ασφάλεια συστήματος

Αναφέρεται στην προστασία του σχετικού εξοπλισμού του υπολογιστή από φυσικές καταστροφές όπως πλημμύρες, σεισμοί, φωτιά, κλπ.

- Ασφάλεια υπολογιστικού συστήματος

Αναφέρεται στην προστασία εκείνων των πληροφοριών του υπολογιστή που διαχειρίζεται άμεσα το λειτουργικό σύστημα (προγράμματα εφαρμογών, αρχεία δεδομένων, κλπ.).

- Ασφάλεια βάσεων δεδομένων

Αναφέρεται στην ικανότητα του συστήματος να εφαρμόσει μια προκαθορισμένη πολιτική προστασίας των περιεχομένων μιας βάσης δεδομένων, στην οποία διευκρινίζεται ποιοι εξουσιοδοτούνται να δουν ή και να τροποποιήσουν τα προστατευόμενα δεδομένα.

- Ασφάλεια επικοινωνιών

Αναφέρεται στην προστασία των πληροφοριών κατά τη μετάδοσή τους μέσω των διαφόρων δικτύων.

Τα συστήματα ανακάλυψης ιών, οι προστασία δικτύων με firewalls, και τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems – IDS) φαίνεται να είναι από τις δημοφιλείς τεχνολογίες στην ασφάλεια υπολογιστικών συστημάτων. Ιδιαίτερα ο στόχος της τεχνολογίας IDS, που είναι να αναγνωρίζει την απαγορευμένη χρήση των πόρων, θεωρείται ένα γενικά δύσκολο πρόβλημα στην αντιμετώπιση και υλοποίηση του, αφού χρειάζεται να παράγονται γρήγορα αποτελέσματα που να είναι αξιόπιστα και χρήσιμα.

<sup>16</sup> Κωνσταντίνος Αντωνής, Ασφάλεια Υπολογιστικών Συστημάτων, Λαμία 2003

## 6.1 Antivirus

Τα antivirus προγράμματα είναι προγράμματα τα οποία τρέχουν σε ένα σύστημα και ελέγχουν κάθε διεργασία που εκτελείται για να δουν αν πρόκειται για μια διεργασία η οποία δεν κάνει κάτι μη επιτρεπτό, ή για μια διεργασία που έχει χαρακτηριστεί ως ιός, σκουλήκι ή δούρειος ίππος και η οποία είναι κακόβουλη. Σήμερα υπάρχουν αρκετά τέτοια προγράμματα, εμπορικά ή μη, τα οποία έχουν διάφορους τρόπους λειτουργίας. Ο συνηθέστερος είναι με την χρήση Signatures. Όσα λειτουργούν με τον τρόπο αυτό ελέγχουν για διεργασίες που εκτελούν συγκεκριμένη ακολουθία ενεργειών, η οποία έχει αναγνωριστεί και χαρακτηριστεί ως κακόβουλη. Μόλις μια τέτοια ακολουθία ενεργειών εκτελεστεί στο σύστημα, τότε αυτομάτως το πρόγραμμα που την εκτέλεσε θεωρείται ιός και η εκτέλεσή του εμποδίζεται από το antivirus. Η χρήση antivirus προγραμμάτων θεωρείται βασικό συστατικό ενός πλάνου ασφαλείας και δεν πρέπει να λείπει σχεδόν ποτέ από κανένα σύστημα. Επειδή μάλιστα είναι και από τις πρώτες τεχνολογίες που εμφανίστηκαν για την προστασία των συστημάτων, μπορεί να θεωρηθεί ότι βρίσκεται σε αρκετά ώριμο στάδιο, σε ενός συστήματος από κακόβουλες διεργασίες. Ωστόσο τα antivirus προγράμματα, αν και θεωρείται ότι αυξάνουν σε μεγάλο βαθμό το επίπεδο ασφαλείας των συστημάτων, έχουν αρκετά μειονεκτήματα. Το μεγαλύτερο από τα οποία εντοπίζεται στο ότι υπάρχει άμεση εξάρτηση από τον κατασκευαστή του προγράμματος. Επειδή ιοί και άλλα κακόβουλα προγράμματα αναπτύσσονται συνεχώς, πρέπει να βγαίνουν συνεχώς signatures για αυτά ώστε να μπορεί το antivirus να το αναγνωρίσει.

Το πόσο γρήγορα θα προσφέρει την ενημέρωση αυτή η εταιρεία κατασκευής του κάθε antivirus είναι πολύ κρίσιμο για την προστασία του συστήματος. Όσο πιο γρήγορα ανακοινωθούν τα νέα signatures, τόσο πιο γρήγορα θα προστατευτεί ο υπολογιστής. Το μεσοδιάστημα μέχρι την ενημέρωση των signatures είναι κρίσιμος παράγοντας. Σημαντικό είναι επίσης και ο τρόπος με τον οποίο γίνεται ο έλεγχος της κάθε διεργασίας. Διαφορετικά antivirus προγράμματα πιθανά να έχουν διαφορετικά αποτελέσματα σε ότι αφορά την ανίχνευση μιας απειλής. Ανάλογα με τον μηχανισμό ελέγχου θα ανιχνεύουν περισσότερες ή λιγότερες απειλές από κάποια άλλα. Απάντηση στην ερώτηση «Ποιό είναι το καλύτερο antivirus πρόγραμμα;» δεν υπάρχει. Κάθε τέτοιο πρόγραμμα έχει κάποια θετικά στοιχεία, ενώ μειονεκτεί σε κάποια άλλα. Βασικός ωστόσο παράγοντας που πιθανά μας επηρεάσει στην επιλογή ενός antivirus είναι η εταιρεία ανάπτυξής του. Έχει επίσης παρατηρηθεί πως το βασικότερο πρόβλημα των antivirus προγραμμάτων δεν έχει να κάνει με τον τρόπο

λειτουργίας τους, αλλά με τους χρήστες τους. Για να γίνει αντιληπτός ο λόγος, ας θεωρήσουμε την ιδανική περίπτωση κατά την οποία έχουμε το καλύτερο antivirus πρόγραμμα, για το οποίο βγαίνουν ενημερώσεις αμέσως μόλις κυκλοφορήσει ένας νέος ιός. Αν ο χρήστης δεν ενημερώσει το πρόγραμμά του, τότε αυτομάτως αφήνει τον υπολογιστή του εκτεθειμένο σε κίνδυνο από τον οποίο θα μπορούσε να έχει προστατευτεί. Οι περισσότεροι χρήστες δεν ενημερώνουν συχνά το antivirus που χρησιμοποιούν, με αποτέλεσμα αυτό να αγνοεί την ύπαρξη των νέων απειλών. Επομένως η προστασία που τους παρέχει είναι υποδεέστερη από αυτή που θα έπρεπε ή θα μπορούσε, απλά και μόνο επειδή ο χρήστης αμελεί να εκτελέσει μια απλή διαδικασία. Τέτοιες περιπτώσεις είναι πολύ συχνές και για το λόγο αυτό είναι περισσότερο από θεμιτή η ύπαρξη ενός μηχανισμού αυτόματης ενημέρωσης του προγράμματος. Αν μάλιστα υπάρχει η δυνατότητα ύπαρξης ενός εξυπηρετητή στο δίκτυο, ο οποίος θα αναλαμβάνει να ενημερώνει τους πελάτες του, τότε έχουμε ακόμη καλύτερη κατάσταση, αφού εννοείται πως ο εξυπηρετητής αυτός θα βρίσκεται υπό την επίβλεψη του διαχειριστή ασφαλείας, δηλαδή στα χέρια ενός έμπειρου και ενημερωμένου χρήστη.

## **6.2 Τείχη Προστασίας (Firewalls)**

Πριν προχωρήσουμε με τις λεπτομέρειες των τύπων και των διαμορφώσεων των τειχών προστασίας, καλό είναι να αναφέρουμε περιληπτικά τι μπορεί κανένας να περιμένει από ένα τείχος. Θα ξεκινήσουμε τη συζήτηση στην παράγραφο αυτή εξετάζοντας πρώτα ποιοι είναι οι στόχοι σχεδίασης ενός αναχώματος.

Ο πρώτος μας στόχος είναι να εξασφαλίσουμε ότι όλη η κίνηση, από το εσωτερικό δίκτυο προς τα έξω και αντίστροφα, πρέπει να διέρχεται από το τείχος. Ο στόχος αυτός επιτυγχάνεται απαγορεύοντας κάθε φυσική πρόσβαση στο εσωτερικό δίκτυο, εκτός αν αυτή διέρχεται από το τείχος. Όπως θα δούμε αργότερα, είναι δυνατές διάφορες διαμορφώσεις αναχωμάτων που επιτυγχάνουν το στόχο αυτό. Ο δεύτερος στόχος μας είναι ότι μόνο εξουσιοδοτημένη κίνηση, όπως αυτή ορίζεται από την τοπική πολιτική ασφάλειας, πρέπει να επιτρέπεται να διέλθει από το τείχος. Όπως θα δούμε αργότερα, υπάρχουν διάφοροι τύποι τειχών προστασίας, που επιτρέπουν την υλοποίηση διάφορων πολιτικών. Τέλος, το τείχος το ίδιο πρέπει να είναι απρόσβλητο από παρεισφρήσεις. Αυτό σημαίνει ότι ως τείχος προστασίας πρέπει να χρησιμοποιηθεί ένα έμπιστο σύστημα με ένα έμπιστο λειτουργικό σύστημα.

Υπάρχουν τέσσερις γενικές τεχνικές που χρησιμοποιούν τα τείχη για να ελέγχουν την πρόσβαση και για να επιβάλλουν την πολιτική ασφάλειας του δικτύου που προστατεύουν:

- Έλεγχος υπηρεσιών:

Καθορίζει τους τύπους των υπηρεσιών του διαδικτύου που μπορούν να προσπελαστούν προς τα μέσα ή προς τα έξω. Το τείχος μπορεί να φιλτράρει την κίνηση με βάση τη διεύθυνση IP και τον αριθμό θύρας TCP. Μπορεί επίσης να έχει λογισμικό πληρεξουσίου που δέχεται και ερμηνεύει κάθε αίτηση παροχής υπηρεσίας πριν την μεταβιβάσει. Μπορεί επίσης να φιλοξενεί το ίδιο το λογισμικό του εξυπηρετητή, π.χ. μια υπηρεσία ταχυδρομείου ή WWW.

- Έλεγχος κατεύθυνσης:

Καθορίζει την κατεύθυνση προς την οποία επιτρέπεται η υποβολή αιτήσεων για παροχή συγκεκριμένων υπηρεσιών μέσω του τείχους.

- Έλεγχος χρηστών:

Ελέγχει την πρόσβαση σε μια υπηρεσία, ανάλογα με το ποιος χρήστης προσπαθεί να την προσπελάσει. Το χαρακτηριστικό αυτό συνήθως εφαρμόζεται σε χρήστες συστημάτων που βρίσκονται μέσα στην περίμετρο που προστατεύει το τείχος (τοπικούς χρήστες). Μπορεί όμως να εφαρμοστεί και σε εισερχόμενη κίνηση από εξωτερικούς χρήστες. Η εφαρμογή αυτή απαιτεί κάποια μορφή τεχνολογίας ασφαλούς αυθεντικοποίησης, όπως αυτή που παρέχεται από το IPSec.

- Έλεγχος συμπεριφοράς:

Ελέγχει πώς χρησιμοποιούνται συγκεκριμένες υπηρεσίες. Για παράδειγμα, το τείχος μπορεί να φιλτράρει το ηλεκτρονικό ταχυδρομείο ή μπορεί να επιτρέπει την εξωτερική πρόσβαση μόνο σε ένα τμήμα της πληροφορίας που περιέχει ένας εξυπηρετητής WWW.

Μπορούμε τώρα να έρθουμε και στα χαρακτηριστικά των τειχών προστασίας.

Πρώτα –πρώτα, το τείχος αποτελεί ένα μοναδικό σημείο φραγής που κρατάει τους μη εξουσιοδοτημένους χρήστες έξω από το προστατευόμενο δίκτυο, απαγορεύει σε δυνητικά ευπαθείς υπηρεσίες να εισέλθουν ή να εξέλθουν από το δίκτυο και παρέχει προστασία από διάφορες επιθέσεις δρομολόγησης και παραποίησης διευθύνσεων IP. Βέβαια, η χρήση ενός μοναδικού σημείου φραγής απλοποιεί τη διαχείριση της ασφάλειας, αφού όλες οι λειτουργίες ασφάλειας είναι συγκεντρωμένες σε ένα σύστημα ή σε ένα σύνολο συστημάτων.

Επιπλέον, το τείχος αποτελεί ένα μοναδικό σημείο αναφοράς γεγονότων που σχετίζονται με την ασφάλεια. Επομένως, μπορούμε εκεί να υλοποιήσουμε όλους τους ελέγχους και τους συναγερμούς.

Ακόμη, το τείχος αποτελεί μια βολική πλατφόρμα για την εκτέλεση διάφορων λειτουργιών του διαδικτύου που δε σχετίζονται με την ασφάλεια. Αυτές περιλαμβάνουν ένα μεταφραστή διευθύνσεων δικτύου, που αντιστοιχεί τις τοπικές διευθύνσεις σε διευθύνσεις διαδικτύου, και μια λειτουργία διαχείρισης δικτύου, που ελέγχει ή καταγράφει τη χρήση του διαδικτύου.

Τέλος, το τείχος μπορεί να χρησιμοποιηθεί ως πλατφόρμα για το IPSec. Επιπλέον, μπορεί να χρησιμοποιηθεί για τη δημιουργία εικονικών ιδιωτικών δικτύων (Virtual Private Networks – VPN). Δυστυχώς, παρά τις παραπάνω, σημαντικές, δυνατότητές τους, τα τείχη έχουν και περιορισμούς, όπως άλλωστε και κάθε τεχνική. Έτσι, κανένα τείχος δεν μπορεί να παρέχει προστασία απέναντι σε επιθέσεις που το παρακάμπτουν. Παράκαμψη του τείχους μπορεί να γίνει από συστήματα του εσωτερικού δικτύου που μέσω ίντερνετ μπορούν να συνδεθούν με κάποιον παροχέα διαδικτύου. Επίσης, σ' ένα εσωτερικό τοπικό δίκτυο μπορούν να υπάρχουν modems, που παρέχουν τη δυνατότητα σύνδεσης σε υπαλλήλους που μετακινούνται. Ακόμη, κανένα τείχος δεν παρέχει προστασία εναντίον εσωτερικών απειλών. Παραδείγματα τέτοιων απειλών είναι ένας δυσαρεστημένος υπάλληλος ή ένας υπάλληλος που αθέλητα συνεργάζεται με έναν εξωτερικό επιτιθέμενο. Τέλος, κανένα τείχος δεν μπορεί να παρέχει προστασία εναντίον της μεταφοράς προγραμμάτων ή αρχείων μολυσμένων με ιούς. Λόγω της ποικιλίας των λειτουργικών συστημάτων και των εφαρμογών που υποστηρίζονται μέσα στην περίμετρο, δεν θα ήταν πρακτικό και –ίσως– ούτε καν δυνατό για το τείχος να σαρώνει όλα τα εισερχόμενα αρχεία, ηλεκτρονικό ταχυδρομείο και μηνύματα για ιούς.

### **6.2.1 Τύποι τειχών προστασίας**

Υπάρχουν τρεις κύριοι τύποι τειχών:

- δρομολογητές φιλτραρίσματος πακέτων
- πύλες επιπέδου εφαρμογής και
- πύλες επιπέδου κυκλώματος.

Θα εξετάσουμε αυτούς τους τρεις τύπους ξεχωριστά.

#### **6.2.1.1 Δρομολογητής φιλτραρίσματος πακέτων**

Ο δρομολογητής φιλτραρίσματος πακέτων (Packet Filtering Router) εφαρμόζει ένα σύνολο κανόνων σε κάθε εισερχόμενο πακέτο IP και στη συνέχεια προωθεί ή απορρίπτει το πακέτο. Ο δρομολογητής συνήθως είναι διαμορφωμένος για να φιλτράρει πακέτα που πηγαίνουν και προς τις δύο διευθύνσεις (από και προς το εσωτερικό δίκτυο). Οι κανόνες φιλτραρίσματος βασίζονται σε πεδία της επικεφαλίδας IP και της επικεφαλίδας μεταφοράς (TCP ή UDP, ανάλογα), που περιλαμβάνουν τις διευθύνσεις πηγής και προορισμού IP, το πεδίο πρωτοκόλλου IP (που ορίζει το πρωτόκολλο μεταφοράς) και τον αριθμό θύρας TCP ή UDP (που ορίζει την εφαρμογή, π.χ. SNMP ή TELNET). Αν τα περιεχόμενα κάποιας επικεφαλίδας αντιστοιχιστούν μ' αυτά κάποιου κανόνα, ο κανόνας ενεργοποιείται για να καθορίσει αν το πακέτο πρέπει να προωθηθεί ή να απορριφθεί. Αν δεν βρεθεί κανόνας με κατάλληλα περιεχόμενα, εκτελείται μια προκαθορισμένη ενέργεια. Οι προκαθορισμένες πολιτικές είναι δύο:

- ✓ Ότι δεν επιτρέπεται ρητά, απαγορεύεται.
- ✓ Ότι δεν απαγορεύεται ρητά, επιτρέπεται.

Η πρώτη πολιτική είναι, βέβαια, η πιο συντηρητική. Αρχικά, τα πάντα είναι απαγορευμένα και οι επιτρεπόμενες υπηρεσίες πρέπει να προσθέτονται μία μία, ανά περίπτωση. Η πολιτική αυτή είναι περισσότερο αντιληπτή από τους χρήστες, που ενδέχεται και να δουν το τείχος ως εμπόδιο στην καθημερινή τους δουλειά. Αντίθετα, η δεύτερη πολιτική αυξάνει την ευκολία χρήσης, αλλά έχει μειωμένη ασφάλεια. Ο διαχειριστής ασφάλειας πρέπει, βασικά, να αντιδρά σε κάθε νέα απειλή, καθώς αυτή γίνεται γνωστή. Πλεονεκτήματα αυτού του τύπου τείχους είναι η απλότητά τους, η διαφάνεια που παρέχουν στους χρήστες και η μεγάλη τους ταχύτητα. Τα μειονεκτήματα περιλαμβάνουν τη δυσκολία της κατασκευής σωστών κανόνων φιλτραρίσματος πακέτων και την έλλειψη αυθεντικοποίησης. Επιθέσεις που μπορούν να εκδηλωθούν εναντίον τέτοιων τειχών προστασίας και τα αντίστοιχα αντίμετρα είναι οι εξής:

- ✓ Παραποίηση διεύθυνσης IP:

Ο επιτιθέμενος μεταδίδει πακέτα από το εξωτερικό της περιμέτρου με πεδίο διεύθυνσης IP που περιέχει τη διεύθυνση ενός εσωτερικού συστήματος, με την ελπίδα ότι η χρήση της παραποιημένης διεύθυνσης θα επιτρέψει την παραβίαση συστημάτων που χρησιμοποιούν απλά μέτρα ασφάλειας ως προς τη διεύθυνση προέλευσης, δηλαδή στα συστήματα εκείνα στα οποία πακέτα προερχόμενα από κάποια έμπιστα συστήματα γίνονται αποδεκτά. Το αντίμετρο είναι να απορρίπτουμε τα πακέτα που έχουν εσωτερική διεύθυνση αποστολέα αλλά φτάνουν σε εξωτερική διεπαφή.

✓ Επιθέσεις δρομολόγησης αποστολέα:

Ο σταθμός αποστολής καθορίζει το δρομολόγιο που το κάθε πακέτο θα πάρει στη διαδρομή του μέσα στο διαδίκτυο, ελπίζοντας ότι η πρακτική αυτή θα παρακάμψει μέτρα ασφάλειας που δεν αναλύουν την πληροφορία δρομολόγησης από τον αποστολέα. Το αντίμετρο είναι να απορρίπτονται όλα τα πακέτα που χρησιμοποιούν την επιλογή αυτή.

✓ Επιθέσεις απειροελάχιστων τμημάτων:

Ο επιτιθέμενος χρησιμοποιεί την επιλογή τμηματοποίησης IP για να δημιουργήσει τμήματα εξαιρετικά μικρά σε μέγεθος και να επιβάλει έτσι την τοποθέτηση της πληροφορίας που περιέχει η επικεφαλίδα TCP σε ξεχωριστό τμήμα πακέτου. Η επίθεση αυτή στοχεύει στην παράκαμψη κανόνων φιλτραρίσματος που βασίζονται στην πληροφορία αυτή. Ο επιτιθέμενος ελπίζει ότι ο δρομολογητής φιλτραρίσματος εξετάζει μόνο το πρώτο τμήμα και ότι τα υπόλοιπα περνούν χωρίς έλεγχο. Η επίθεση αποκρούεται απορρίπτοντας όλα τα πακέτα με τύπο πρωτοκόλλου TCP και IP Fragments Offset ίσο με 1.

### 6.2.1.2 Πύλες επιπέδου εφαρμογής

Οι πύλες επιπέδου εφαρμογής (Application Level Gateways), που ονομάζονται επίσης και πληρεξούσιοι εξυπηρετητές (proxy servers), λειτουργούν ως αναμεταδότες κίνησης στο επίπεδο εφαρμογής. Ο χρήστης επικοινωνεί με την πύλη μέσω μιας εφαρμογής TCP/IP (π.χ. Telnet, FTP) και η πύλη του ζητάει το όνομα του απομακρυσμένου συστήματος που πρέπει να προσπελαστεί. Όταν απαντήσει ο χρήστης και δώσει τις απαραίτητες και έγκυρες πληροφορίες αυθεντικοποίησης που τον αφορούν, η πύλη επικοινωνεί με την εφαρμογή στο απομακρυσμένο σύστημα και αναμεταδίδει όλα τα τμήματα TCP που περιέχουν τα δεδομένα της εφαρμογής μεταξύ των δύο άκρων. Αν η πύλη δεν υποστηρίζει τον κώδικα πληρεξουσίου για μια συγκεκριμένη εφαρμογή, η υπηρεσία δεν παρέχεται και δεν μπορεί να διακινηθεί δια μέσου του αναχώματος. Επιπλέον, η πύλη μπορεί να διαμορφωθεί έτσι ώστε να υποστηρίζει μόνο συγκεκριμένα χαρακτηριστικά μιας εφαρμογής, τα οποία ο διαχειριστής δικτύου κρίνει απαραίτητα, απορρίπτοντας όλα τα υπόλοιπα. Τα τείχη αυτά είναι περισσότερο ασφαλή από τους δρομολογητές φιλτραρίσματος πακέτων. Αντί να προσπαθούν να χειριστούν τους απειράριθμους πιθανούς συνδυασμούς που πρέπει να επιτρέπονται ή να απαγορεύονται στα επίπεδα TCP και IP, η πύλη επιπέδου εφαρμογής χρειάζεται μόνο να εξετάζει εξονυχιστικά ένα μικρό αριθμό επιτρεπόμενων εφαρμογών. Επιπλέον, είναι εύκολο να καταγράφεται και να ελέγχεται



όλη η εισερχόμενη κίνηση στο επίπεδο εφαρμογής. Ένα βασικό μειονέκτημα των τειχών αυτού του τύπου είναι η επιπλέον επιβάρυνση της επεξεργασίας σε κάθε σύνδεση. Στην πραγματικότητα υπάρχουν δύο τμήματα σύνδεσης μεταξύ των τελικών χρηστών, με την πύλη στο σημείο τομής τους, και η πύλη πρέπει να εξετάζει και να διακινεί όλη τη κίνηση και προς τις δυο κατευθύνσεις.

#### **6.2.1.3 Πύλη επιπέδου κυκλώματος**

Μια πύλη επιπέδου κυκλώματος (Circuit Level Gateway) μπορεί να είναι ένα αυτόνομο σύστημα ή μπορεί να είναι μια ειδική λειτουργία που εκτελείται από μια πύλη επιπέδου εφαρμογής για συγκεκριμένες εφαρμογές. Μια τέτοια πύλη δεν επιτρέπει συνδέσεις TCP απ' άκρη σ' άκρη. Αντίθετα, εγκαθιστά δύο συνδέσεις TCP, μία μεταξύ της ίδιας και ενός χρήστη TCP σε κάποιο εσωτερικό σύστημα και μια άλλη μεταξύ της ίδιας και ενός χρήστη TCP σε κάποιο εξωτερικό σύστημα. Από τη στιγμή που θα εγκατασταθούν και οι δύο συνδέσεις, η πύλη συνήθως αναμεταδίδει τμήματα TCP από τη μια σύνδεση στην άλλη χωρίς να εξετάζει τα περιεχόμενά τους. Η λειτουργία ασφάλειας συνίσταται στον καθορισμό του ποιες συνδέσεις επιτρέπονται. Τυπική χρήση τέτοιων τειχών είναι μια κατάσταση στην οποία ο διαχειριστής συστήματος εμπιστεύεται τους εσωτερικούς χρήστες. Η πύλη μπορεί να διαμορφωθεί έτσι ώστε να λειτουργεί ως πύλη επιπέδου εφαρμογής ή ως πληρεξούσιος εξυπηρετητής για τις εισερχόμενες συνδέσεις και ως πύλη επιπέδου κυκλώματος για τις εξερχόμενες συνδέσεις. Στη διαμόρφωση αυτή, η πύλη επιβαρύνεται με την εξέταση της εισερχόμενης πληροφορίας αλλά όχι με αυτήν της εξερχόμενης. Παράδειγμα τέτοιου τείχους αποτελεί το πακέτο SOCKS.

### **6.3 Επάλξεις**

Οι επάλξεις (Bastion hosts) είναι μηχανές που έχουν αναγνωρισθεί από τον υπεύθυνο ασφάλειας του δικτύου ως ισχυρά και κρίσιμα σημεία για την ασφάλεια του δικτύου. Τυπικά, η επάλξη χρησιμοποιείται ως πλατφόρμα για μια πύλη επιπέδου εφαρμογής ή μια πύλη επιπέδου κυκλώματος. Τα κυριότερα χαρακτηριστικά των επάλξεων είναι τα εξής:

- ✓ Στην πλατφόρμα υλικού τους τρέχει ασφαλής έκδοση του λειτουργικού συστήματος
- ✓ Μόνο οι υπηρεσίες που ο διαχειριστής συστήματος θεωρεί βασικές είναι εγκατεστημένες στην επάλξη. Αυτές περιλαμβάνουν πληρεξούσιες εφαρμογές, όπως Telnet, DNS, FTP, SMTP και αυθεντικοποίηση χρήστη.

- ✓ Η έπαλξη μπορεί να απαιτεί επιπρόσθετη αυθεντικοποίηση πριν επιτρέψει πρόσβαση ενός χρήστη στις πληρεξούσιες υπηρεσίες. Επιπλέον, κάθε πληρεξούσια υπηρεσία μπορεί να απαιτεί τη δική της αυθεντικοποίηση πριν επιτρέψει την πρόσβαση σε κάποιο χρήστη.
- ✓ Κάθε πληρεξούσια υπηρεσία είναι διαμορφωμένη έτσι ώστε να υποστηρίζει μόνο ένα υποσύνολο του κανονικού συνόλου εντολών της εφαρμογής.
- ✓ Κάθε πληρεξούσια υπηρεσία είναι διαμορφωμένη έτσι ώστε να επιτρέπει πρόσβαση μόνο σε συγκεκριμένα συστήματα. Αυτό σημαίνει ότι το περιορισμένο σύνολο χαρακτηριστικών/εντολών μπορεί να εφαρμοστεί σε περιορισμένο μόνο υποσύνολο συστημάτων του προστατευόμενου δικτύου.
- ✓ Κάθε πληρεξούσια υπηρεσία διατηρεί λεπτομερείς πληροφορίες ελέγχου καταγράφοντας όλη την κίνηση, κάθε σύνδεση και τη διάρκειά της. Το ίχνος ελέγχου είναι ένα βασικό εργαλείο για τον καθορισμό και τερματισμό επιθέσεων.
- ✓ Κάθε σπόνδυλος υπηρεσίας πληρεξουσίου είναι ένα πολύ μικρό πακέτο λογισμικού ειδικά σχεδιασμένο για να παρέχει ασφάλεια δικτύου. Λόγω της σχετικής τους απλότητας, είναι ευκολότερο να ελέγξουμε τέτοιους σπονδύλους για ελαττώματα σχετικά με την ασφάλεια. Για παράδειγμα, μια τυπική εφαρμογή ταχυδρομείου στο Unix μπορεί κάλλιστα να περιέχει 20.000 γραμμές κώδικα, ενώ μια αντίστοιχη υπηρεσία πληρεξουσίου λιγότερες από 1.000.
- ✓ Κάθε πληρεξούσια υπηρεσία είναι ανεξάρτητη από τις άλλες που βρίσκονται στην ίδια έπαλξη. Αν υπάρξει κάποιο πρόβλημα με τη λειτουργία μιας υπηρεσίας ή αν ανακαλυφθεί μια ευπάθεια, η υπηρεσία μπορεί να απεγκατασταθεί χωρίς να επηρεαστεί η λειτουργία των υπολοίπων. Επίσης, αν οι χρήστες απαιτούν την υποστήριξη μιας νέας υπηρεσίας, ο διαχειριστής δικτύου μπορεί εύκολα να εγκαταστήσει τη νέα πληρεξούσια υπηρεσία στην έπαλξη.
- ✓ Κάθε πληρεξούσια υπηρεσία προσπελάζει το δίσκο μόνο για να διαβάσει το αρχείο αρχικής της διαμόρφωσης. Έτσι, είναι δύσκολο στον επιτιθέμενο να εγκαταστήσει Δούρειους Ίππους ή άλλα επικίνδυνα αρχεία στην έπαλξη.
- ✓ Κάθε πληρεξούσια υπηρεσία εξυπηρετεί τους μη προνομιούχους χρήστες χρησιμοποιώντας ένα ιδιωτικό και ασφαλή κατάλογο στην έπαλξη.

## 6.4 Σύστημα Ανίχνευσης Επιθέσεων (IDS)

Ένα τείχος προστασίας (firewall) που έχει ρυθμιστεί σωστά αποτελεί την πρώτη γραμμή άμυνας του δικτύου και ελέγχει την δικτυακή κίνηση προς τους υπολογιστές που προστατεύει. Παρόλα αυτά υπάρχει περίπτωση παρά την ορθή λειτουργία του firewall κάποιος από αυτούς να κυριευτεί από κάποια απειλή επειδή ήταν ευάλωτος σε μια ασυνήθιστη αίτηση. Εκτός από firewall πιθανά να υπάρχουν και άλλα στοιχεία που να χρησιμοποιούνται ως πρώτη γραμμή άμυνας, όπως οι Λίστες Ελέγχου Πρόσβασης (Access Control Lists – ACLs).

Αν και όλα αυτά συμβάλλουν στην βελτίωση του επιπέδου ασφάλειας, ωστόσο δεν μπορούμε ποτέ να είμαστε σίγουροι ότι ακολουθήθηκαν οι βέλτιστες λύσεις που θα προσφέρουν την καλύτερη δυνατή προστασία. Για τον λόγο αυτό θεωρείται καλή ιδέα η ύπαρξη μιας δεύτερης γραμμής άμυνας. Η τακτική αυτή, δηλαδή η χρήση πολλών επιπέδων άμυνας στο δίκτυο, είναι γνωστή με τον όρο «Defense in Depth» (Άμυνα σε Βάθος). Ενισχύουμε όσο μπορούμε την πρώτη γραμμή άμυνας ώστε να μην επιτρέπεται η παράνομη πρόσβαση στο εσωτερικό μας δίκτυο, αλλά αν αυτό αποτύχει, τότε έχουμε και εναλλακτικό σχέδιο. Ένας ανιχνευτικός μηχανισμός είναι πολύ καλή λύση για το δεύτερο επίπεδο προστασίας. Ένα σύστημα ανίχνευσης επιθέσεων (IDS) αποτελεί στα χέρια του διαχειριστή ασφαλείας ένα κατάλληλο εργαλείο που του επιτρέπει να ανιχνεύει άμεσα και να αντιδρά γρήγορα σε μια επίθεση που δέχεται το δίκτυό του. Το IDS είναι ένα σύστημα λογισμικού ή ένας συνδυασμός υλικού και λογισμικού, το οποίο πραγματοποιεί την ανίχνευση περιέργης δικτυακής κίνησης σε έναν υπολογιστή ή στο δίκτυο. Εξ' ορισμού ένα IDS απλά ανιχνεύει επιθέσεις και τις παρουσιάζει στο διαχειριστή ασφαλείας του δικτύου. Δεν αναλαμβάνει δράση, υπό την έννοια ότι δεν κάνει κάτι για να περιορίσει την εξάπλωση της επίθεσης. Τα περισσότερα συστήματα ανίχνευσης επιθέσεων λειτουργούν με την χρήση Signatures, δηλαδή ανιχνεύουν παράνομες ακολουθίες ενεργειών, όπως κάνουν και τα περισσότερα antivirus προγράμματα που περιγράψαμε παραπάνω. Εκτός από την χρήση των Signatures τα IDS συστήματα ανιχνεύουν και αναλύουν περίεργη δικτυακή κίνηση και αποφασίζουν αν πρόκειται για κάποιου είδους επίθεση ή όχι.

## 6.5 Σύστημα Πρόληψης Επιθέσεων (IPS)

Τα συστήματα πρόληψης επιθέσεων είναι το λογικό επόμενο βήμα των συστημάτων ανίχνευσης επιθέσεων. Από τη στιγμή που ανιχνεύεται μια επίθεση είναι θεμιτό να αντιμετωπιστεί και αυτόματα. Μάλιστα η αντιμετώπιση αυτή είναι καλό να γίνει

χωρίς την ανθρώπινη παρέμβαση για να ελαχιστοποιηθεί ο χρόνος αντίδρασης στην επίθεση. Συχνά ένα IPS (Intrusion Prevention System) αποτελεί μέρος ενός IDS και δεν αποτελούν ξεχωριστές οντότητες. Αυτό συμβαίνει επειδή το IDS είναι αυτό που ανιχνεύει μια επίθεση, οπότε αυτό πρέπει να πάρει και την πρωτοβουλία για να την σταματήσει. Στην ουσία ένα IPS, συνδυάζει τα χαρακτηριστικά ενός Firewall και ενός IDS, καθώς μπορεί και μπλοκάρει την ανεπιθύμητη κίνηση έχοντας την βοήθεια ανίχνευσης των κακόβουλων πακέτων που προσφέρει ένα IDS. Η διαφορά του από το firewall είναι ότι έχει καλύτερη και πιο ολοκληρωμένη πληροφορία. Αυτό οφείλεται στην ύπαρξη του IDS, το οποίο και παρακολουθεί όλη την δικτυακή κίνηση. Τα συστήματα αποτροπής επιθέσεων συναντώνται στους παρακάτω τύπους:

✓ Host-Based (HIPSs),

Βρίσκονται σε ένα συγκεκριμένο μηχάνημα και παρακολουθούν την κίνηση και κάποια άλλα στοιχεία προκειμένου να αποτρέψουν επιθέσεις.

✓ Network-based (NIPSs),

Όπου η εφαρμογή IPS ή το υλικό που παίζει το ρόλο του IPS βρίσκεται στο δίκτυο και έχει IP αυτού του δικτύου. Τα συστήματα αυτά αναλύουν, βρίσκουν, και αναφέρουν συμβάντα που έχουν να κάνουν με ζητήματα ασφάλειας. Είναι σχεδιασμένα ώστε να ελέγχουν τη δικτυακή κίνηση.

✓ Content-based (CBIPSs),

Είναι τα συστήματα εκείνα που παρακολουθούν το περιεχόμενο των πακέτων για μοναδικές ακολουθίες, τις οποίες ονομάζουμε υπογραφές, με σκοπό να αναγνωρίσουν και να αποτρέψουν γνωστούς τύπους επιθέσεων.

✓ Rate-based (RBIPSs),

Είναι τα συστήματα εκείνα που στόχο έχουν να αποτρέψουν επιθέσεις τύπου άρνησης εξυπηρέτησης. Η λειτουργία τους βασίζεται στο γεγονός ότι παρακολουθούν και μαθαίνουν φυσιολογικές δικτυακές συμπεριφορές. Με βάση λοιπόν την πραγματικού χρόνου παρακολούθηση του δικτύου και κάποια στατιστικά στοιχεία μπορούν να αναγνωρίσουν κάποια μη αποδεκτά όρια για συγκεκριμένους τύπους κίνησης, π.χ. TCP, UDP. Οι επιθέσεις αναγνωρίζονται όταν ξεπεραστούν κάποια φράγματα.

Τα φράγματα αυτά προσαρμόζονται δυναμικά ανάλογα με την ημέρα, την ώρα, τη βδομάδα κ.α. Όταν η επίθεση αναγνωριστεί, τότε εφαρμόζονται διάφοροι μηχανισμοί αποτροπής όπως είναι για παράδειγμα το port/protocol filtering (black-listing, white-listing). Οι βασικές περιοχές έρευνας σε αυτό το τομέα είναι παρόμοιες με αυτές των IDS.

## 6.6 Μερικά σχετικά εργαλεία

✓ Η εφαρμογή **SATAN** (Security Analysis Tool for Auditing Networks) είναι ένα από τα γνωστότερα εργαλεία για την ανίχνευση τρωτών σημείων στη διαμόρφωση ενός δικτύου. Επειδή χρησιμοποιείται από τους περισσότερους επίδοξους εισβολείς, είναι καλό να έχει εγκατασταθεί σε κάθε μεγάλο δίκτυο δεδομένων. Στο βασικό ρυθμό λειτουργίας το SATAN συλλέγει πληροφορίες σχετικά με την αρχιτεκτονική και τις διαθέσιμες υπηρεσίες ενός δικτύου, καθώς και για την ύπαρξη γνωστών τρωτών σημείων στη διαμόρφωση του συστήματος ή θεμελιωδών κανόνων ασφαλείας οι οποίοι δεν υλοποιούνται από τα υπάρχοντα μέτρα. Στον εξερευνητικό ρυθμό λειτουργίας το SATAN επιτρέπει την αξιολόγηση διαφόρων μέτρων για την ασφάλεια του δικτύου, βοηθώντας έτσι το διαχειριστή δικτύου να ορίσει ένα εύρωστο σύνολο από τεχνικούς ελέγχους για την υλοποίηση της πολιτικής ασφαλείας.

✓ Η εφαρμογή **ISS** (Internet Security Scanner) ελέγχει TCP/IP δίκτυα για γνωστά τρωτά σημεία. Το ISS δεν προσπαθεί να αποκτήσει πρόσβαση στο σύστημα που ελέγχει, αλλά ειδοποιεί το διαχειριστή του συστήματος για προβλήματα ασφαλείας στη διαμόρφωση του συστήματος. Μεταξύ άλλων, το ISS ελέγχει την ασφάλεια των κωδικών πρόσβασης σε συνηθισμένους λογαριασμούς, όπως guest, lp, κλπ., προβλήματα με το πρόγραμμα sendmail, προβλήματα στη διαμόρφωση του συστήματος NFS, κλπ.

✓ Το **Texas A&M Network Security Package** (tamu) κατασκευάστηκε μετά την επίθεση μιας ομάδας εισβολέων στο δίκτυο του Πανεπιστημίου Texas A&M. Αυτό το πακέτο ασφαλείας περιλαμβάνει την εφαρμογή drawbridge, που χρησιμοποιείται για φιλτράρισμα πακέτων, την εφαρμογή tiger, που ανιχνεύει τους κόμβους του δικτύου για γνωστά προβλήματα ασφαλείας, και την εφαρμογή netlog, που παρακολουθεί τη δραστηριότητα του δικτύου δεδομένων και ειδοποιεί στην περίπτωση εισβολής (intrusion detection tool).

✓ Η εφαρμογή **COPS** (Computer Oracle and Password System) εκτός από προβλήματα που σχετίζονται με την ασφάλεια των κωδικών πρόσβασης (βλ. κεφάλαιο για ταυτοποίηση και πιστοποίηση), μπορεί να χρησιμοποιηθεί για τη διαπίστωση άλλων γνωστών τρωτών σημείων στην ασφάλεια UNIX εξυπηρετητών. Μεταξύ άλλων, το COPS περιλαμβάνει ένα σύστημα-εμπειρογνώμονα (expert system) το οποίο ελέγχει αν ο λογαριασμός ενός

συγκεκριμένου χρήστη (συνήθως του διαχειριστή συστήματος) μπορεί να παραβιαστεί, εφόσον συντρέχουν συγκεκριμένες συνθήκες.

✓ Η εφαρμογή **Courtney** παρακολουθεί ένα δίκτυο δεδομένων και ειδοποιεί στην περίπτωση που το δίκτυο ελέγχεται για τρωτά σημεία από την εφαρμογή SATAN. Το Courtney ειδοποιεί στην περίπτωση που ένας επίδοξος εισβολέας προσπαθεί να συλλέξει πληροφορίες και να προετοιμάσει την επίθεσή του χρησιμοποιώντας την εφαρμογή SATAN.

✓ Η εφαρμογή **Swatch** παρέχει δυνατότητα προεπεξεργασίας των διαφόρων αρχείων δραστηριότητας συστήματος, και μπορεί να διαμορφωθεί να εντοπίζει συγκεκριμένη δραστηριότητα η οποία θεωρείται ύποπτη. Επιπλέον, ο εντοπισμός ύποπτων γεγονότων μπορεί να γίνει σε πραγματικό χρόνο (on-line). Σε περίπτωση εντοπισμού ενός ύποπτου γεγονότος, το swatch μπορεί να διαμορφωθεί να εκτελεί συγκεκριμένες ενέργειες (π.χ. ειδοποίηση του διαχειριστή συστήματος).

✓ Η εφαρμογή **logsurfer** παρακολουθεί και αναλύει το περιεχόμενο των αρχείων δραστηριότητας του συστήματος σε πραγματικό χρόνο. Το logsurfer λειτουργεί σε οποιοδήποτε αρχείο κειμένου, επιτρέπει στο διαχειριστή συστήματος να καθορίσει εξαιρέσεις με χρήση κανονικών εκφράσεων, μπορεί να παρακολουθεί και να εντοπίζει ομάδες γεγονότων αντί για μεμονωμένα γεγονότα, και μπορεί να εκτελέσει ομάδες εντολών για κάθε ύποπτο γεγονός που εντοπίζει.

✓ Η εφαρμογή **ALVA** (Audit Log Viewer and Analyzer) έχει σχεδιαστεί και υλοποιηθεί από την General Electric για λειτουργικό σύστημα Solaris. Το ALVA έχει σχεδιαστεί για λειτουργία σε περιβάλλοντα ασφάλειας κατηγορίας C2, και επιτρέπει την παρακολούθηση και ανάλυση των αρχείων δραστηριότητας σε πραγματικό χρόνο. Το ALVA διατηρεί άθροισμα ποινών για κάθε χρήστη, το οποίο ενημερώνεται ανάλογα με τις ενέργειές του. Όταν ο χρήστης ξεπεράσει ένα συγκεκριμένο όριο, τότε το ALVA ειδοποιεί για εισβολή /ύποπτη δραστηριότητα.

✓ Η εφαρμογή **Computer Watch** έχει αναπτυχθεί από τα AT&T Bell Laboratories και είναι ένα εξαιρετικό εργαλείο για την ανάλυση των αρχείων δραστηριότητας, ενώ παρέχει και περιορισμένες δυνατότητες ανίχνευσης εισβολής. Το Computer Watch έχει σχεδιαστεί να βοηθάει το διαχειριστή συστήματος στην παρακολούθηση της δραστηριότητας ελαττώνοντας σημαντικά τον όγκο της διαθέσιμης πληροφορίας, με την αφαίρεση εγγραφών που αντιστοιχούν σε κανονική δραστηριότητα.

✓ Η εφαρμογή **argus** χρησιμοποιείται για την παρακολούθηση δραστηριότητας δικτύων που χρησιμοποιούν το πρωτόκολλο IP. Παρέχει εργαλεία για την

ανάλυση διαφόρων ειδών δραστηριότητας δικτύου, και μπορεί να χρησιμοποιηθεί για να επιβεβαιώσει το βαθμό στον οποία τα υπάρχοντα μέτρα υλοποιούν τις πολιτικές αποφάσεις για την ασφάλεια του δικτύου. Επίσης, το argus παρέχει εργαλεία για ανάλυση της απόδοσης και διαχείριση του δικτύου.

✓ Η εφαρμογή **logdaemon** παρέχει εξελιγμένες εκδόσεις των προγραμμάτων rshd, rlogind, ftpd, rexecd, login, και telnetd, με δυνατότητα καταγραφής περισσότερων πληροφοριών από τις συνηθισμένες εκδόσεις τους. Με αυτό τον τρόπο, ο διαχειριστής συστήματος μπορεί να έχει πληρέστερη αντίληψη για τη χρήση των αντίστοιχων υπηρεσιών.

✓ Η εφαρμογή **scan detector** παρακολουθεί και εντοπίζει την εφαρμογή μιας αυτοματοποιημένης διαδικασίας ελέγχου (automated scan) των θυρών επικοινωνίας UDP και TCP. Η εφαρμογή μπορεί είτε να ειδοποιήσει το διαχειριστή συστήματος, είτε να καταγράψει το γεγονός μέσω της λειτουργίας syslog.

✓ Η εφαρμογή **Abacus Sentry** παρακολουθεί και εντοπίζει σε πραγματικό χρόνο τη λειτουργία ενός προγράμματος που ελέγχει τις θύρες επικοινωνίας (port scanner).

✓ Η εφαρμογή **Intelligent Auditing and Categorizing System** έχει σχεδιαστεί και υλοποιηθεί από το Research Institute for Advanced Computer Science. Αυτή η εφαρμογή παρακολουθεί και αναφέρει μεταβολές στο σύστημα αρχείων. Αυτή η δραστηριότητα προστατεύει από μη εξουσιοδοτημένη μεταβολή των αρχείων του λειτουργικού συστήματος, και των εκτελέσιμων εντολών, προγραμμάτων, και εφαρμογών.

✓ Η εφαρμογή **tripwire** παρακολουθεί και εντοπίζει μη εξουσιοδοτημένες μεταβολές στα αρχεία λειτουργικού συστήματος και στα εκτελέσιμα αρχεία ενός υπολογιστή.

✓ Η εφαρμογή **WebStalker Pro** διαχειρίζεται και ελέγχει την πρόσβαση στα αρχεία μιας WWW τοποθεσίας, παρέχοντας δυνατότητα μεταβολής των αρχείων μόνο σε εξουσιοδοτημένους χρήστες. Το WebStalker Pro εντοπίζει προσπάθειες μη εξουσιοδοτημένης μεταβολής, και ειδοποιεί σχετικά το διαχειριστή του συστήματος.

✓ Η εφαρμογή **TTY-watcher** μπορεί να χρησιμοποιηθεί για την παρακολούθηση του τερματικού/πληκτρολογίου ενός πολυχρηστικού υπολογιστικού συστήματος.

✓ Η εφαρμογή **AID** (Adaptive Intrusion Detection) χρησιμοποιεί μία αρχιτεκτονική πελάτη-εξυπηρετητή (client-server), για να ανιχνεύσει προσπάθειες

εισβολής σε ένα σύνολο υπολογιστικών συστημάτων, από έναν κεντρικό εξυπηρετητή. Ειδικές εφαρμογές πελάτη που λειτουργούν στα υπολογιστικά συστήματα επεξεργάζονται τα περιεχόμενα των αρχείων δραστηριότητας, και στέλνουν τα αποτελέσματα στον κεντρικό εξυπηρετητή. Ο κεντρικός εξυπηρετητής επεξεργάζεται περαιτέρω αυτά τα δεδομένα με χρήση ενός έμπειρου συστήματος (expert system). Παρέχει δυνατότητα δημιουργίας αναφορών ασφάλειας, μέσω ενός γραφικού περιβάλλοντος επικοινωνίας με το διαχειριστή συστήματος.

✓ Η εφαρμογή **CSM** (Cooperating Security Manager) είναι ένα σύστημα ανίχνευσης εισβολής για κατανεμημένα δικτυακά περιβάλλοντα. Η εφαρμογή CSM βασίζεται στο πακέτο ασφάλειας του Πανεπιστημίου A&M Texas. Η εφαρμογή CSM χρησιμοποιεί κατανεμημένους ανιχνευτές ύποπτης δραστηριότητας στο δίκτυο, οι οποίοι συνεργάζονται μεταξύ τους για να εντοπίσουν (σε πραγματικό χρόνο) προσπάθειες εισβολής.

✓ Η εφαρμογή **Cybercop** αναγνωρίζει περίπου 170 διαφορετικές ακολουθίες γεγονότων, οι οποίες συνιστούν τυπικές προσπάθειες εισβολής σε ένα δίκτυο δεδομένων. Επιτρέπει την ανίχνευση σε πραγματικό χρόνο ύποπτης δραστηριότητας και προσπαθειών εισβολής.

✓ Η εφαρμογή **DIDS** (Distributed Intrusion Detection System) συλλέγει αναφορές για τη δραστηριότητα των κόμβων του δικτύου σε ένα μοναδικό εξυπηρετητή. Στη συνέχεια χρησιμοποιεί ένα έμπειρο σύστημα για να εντοπίσει απόπειρες εισβολής. Στην περίπτωση εντοπισμού εισβολής, το DIDS έχει αυξημένη δυνατότητα παρακολούθησης και εντοπισμού του εισβολέα.

✓ Η εφαρμογή **Emerald** μπορεί να παρακολουθήσει και να ανιχνεύσει απόπειρες εισβολής σε μεγάλα κατανεμημένα συστήματα και δίκτυα ευρείας περιοχής αποτελούμενα από μεγάλο αριθμό κόμβων. Το Emerald μπορεί να ανιχνεύσει τόσο μεμονωμένες προσπάθειες εισβολής, όσο και συντονισμένες επιθέσεις κατά του δικτύου. Για την παρακολούθηση, το Emerald χρησιμοποιεί ένα κατανεμημένο σύστημα ελέγχου, το οποίο παρέχει στο διαχειριστή του συστήματος σημαντικές δυνατότητες διαμόρφωσης και προσαρμογής στις ιδιαιτερότητες κάθε δικτύου.

✓ Το **INTOUCH INSA Network Security Agent** είναι ένα πλήρες πακέτο ασφάλειας που βασίζεται σε ένα 64-bit RISC υπολογιστικό σύστημα, το οποίο παρακολουθεί για κάθε αξιοπερίεργη ή ύποπτη δραστηριότητα στο δίκτυο δεδομένων και στα υπολογιστικά συστήματα που είναι συνδεδεμένα σε αυτό.



Αυτή η εφαρμογή ελέγχει όλα τα πακέτα που διακινούνται στο δίκτυο, ανασυνθέτει τη δραστηριότητα των χρηστών, και ελέγχει για κάθε παραβίαση των κανόνων ασφαλείας του συστήματος

✓ Η εφαρμογή **NADIR** (Network Anomaly Detection and Intrusion Reporter) έχει αναπτυχθεί στα εργαστήρια του Los Alamos των Η.Π.Α., και χρησιμοποιεί ένα έμπειρο σύστημα για την άμεση ανίχνευση προσπαθειών εισβολής ή άλλης ύποπτης δραστηριότητας. Το NADIR μπορεί να επεξεργαστεί μεγάλο όγκο αρχείων δραστηριότητας, να συσχετίσει διαφορετικά είδη δραστηριότητας προερχόμενα από τον ίδιο ή διαφορετικούς χρήστες, ενώ έχει δυνατότητα αυτοματοποιημένης παραγωγής αναφορών ασφάλειας. Η αρχιτεκτονική του NADIR είναι πελάτη-εξυπηρετητή, με τον εξυπηρετητή να λειτουργεί σε ένα UNIX υπολογιστικό σύστημα και να χρησιμοποιεί το Sybase. Το NADIR έχει χρησιμοποιηθεί πρόσφατα για την ανίχνευση περιστατικών απάτης στο ηλεκτρονικό σύστημα επιστροφής φόρου των Η.Π.Α., και σε απάτες με κάρτες μετρητών / πιστωτικές κάρτες.

✓ Η εφαρμογή **NID** (Network Intrusion Detection) μπορεί να χρησιμοποιηθεί για την καταγραφή, την ανάλυση, και την ανίχνευση προσπαθειών εισβολής σε δικτυακά περιβάλλοντα που βασίζονται σε τεχνολογία Ethernet ή FDDI και χρησιμοποιούν πρωτόκολλο IP. Το NID συγκεντρώνει πληροφορίες γύρω από τη χρήση του δικτύου, και χρησιμοποιεί αναγνώριση attack signatures, ανίχνευση ύποπτης δραστηριότητας, και ανάλυση των τρωτών σημείων του δικτύου, ώστε να εντοπίσει προσπάθειες εισβολής ή παραβίασης της ασφάλειας του συστήματος.

✓ Η εφαρμογή **Stalker** αναλύει τα αρχεία δραστηριότητας και αναφέρει σε περίπτωση ύποπτου χρήστη ή ύποπτης δραστηριότητας. Επίσης, παρέχει δυνατότητα προεπεξεργασίας των δεδομένων των αρχείων δραστηριότητας και κρατά μόνο τις χρήσιμες πληροφορίες.

✓ Η εφαρμογή **WatchDog** αναλύει τα αρχεία δραστηριότητας και αναφέρει σε περίπτωση ύποπτου χρήστη ή ύποπτης δραστηριότητας. Επίσης, υποστηρίζει και τη δυνατότητα παρακολούθησης και ειδοποίησης σε πραγματικό χρόνο.

✓ Η εφαρμογή **IDES/NIDES** (Intrusion Detection Expert System/Next Generation IDES) παρέχει ειδοποίηση εισβολής σε πραγματικό χρόνο. Επιπλέον, μαθαίνει την κανονική συμπεριφορά χρηστών, ομάδων, κλπ. και όταν υπάρχει απόκλιση μεγάλη από την κανονική συμπεριφορά, τότε θεωρεί ότι υπάρχει κίνδυνος παραβίασης και ειδοποιεί το διαχειριστή του συστήματος.

## 6.7 Παραδείγματα χρήσης εφαρμογών<sup>17</sup>

### 6.7.1 Tripwire

Το πρόγραμμα Tripwire χρησιμοποιείται από τους διαχειριστές των συστημάτων unix σαν ένα εργαλείο για τη σύγκριση των ιδιοτήτων των αρχείων του συστήματος. Το Tripwire ελέγχει όλο τον δίσκο ή τους επιμέρους φακέλους που έχει ορίσει ο διαχειριστής και κατασκευάζει μια βάση δεδομένων με τις πληροφορίες του κάθε αρχείου. Καταγράφει πληροφορίες όπως το μέγεθος, η ημερομηνία δημιουργίας και τροποποίησης του αρχείου κ.λ.π.

Έπειτα από κάποια χρονική περίοδο ο διαχειριστής ξαναεκτελεί το tripwire το οποίο κατασκευάζει άλλη μια τέτοια λίστα και την συγκρίνει με την προηγούμενη. Έτσι το πρόγραμμα είναι σε θέση να γνωρίζει τι αλλαγές έγιναν στο σύστημα, ποια αρχεία δημιουργήθηκαν, διαγράφηκαν ή τροποποιήθηκαν.

Στο παρακάτω παράδειγμα θα δημιουργήσουμε μια βάση δεδομένων με πληροφορίες για τον φάκελο /etc και τον φάκελο /var. Ύστερα θα δημιουργήσουμε και θα τροποποιήσουμε ένα αρχείο μέσα σε αυτούς τους φακέλους και θα επανεκτελέσουμε το πρόγραμμα Tripwire. Με αυτό τον τρόπο θα δούμε πως το tripwire θα μας επισημάνει τι αλλαγές έγιναν στο σύστημα αρχείων και τι δημιουργήθηκε, διαγράφηκε ή τροποποιήθηκε.

Εκτελώντας `joe /etc/tripwire/tw.config` βλέπουμε τους κανόνες που έχουμε θέσει στο tripwire και ποια αρχεία θα ελέγξει.

Μεταβαίνουμε στο φάκελο `/etc/tripwire` και εκτελούμε την εντολή

```
#tripwire --init
```

Tripwire(tm) ASR (Academic Source Release) 1.3.1

File Integrity Assessment Software

(c) 1992, Purdue Research Foundation, (c) 1997, 1999 Tripwire

Security Systems, Inc. All Rights Reserved. Use Restricted to

<sup>17</sup> Κωνσταντίνος Αντωνής, Ασκήσεις Εργαστηρίου Ασφάλειας Υπολογιστικών Συστημάτων, Λαμία 2006

Authorized Licensees.

```
### Warning: creating ./databases directory!
```

```
###
```

```
### Phase 1: Reading configuration file
```

```
### Phase 2: Generating file list
```

```
### Phase 3: Creating file information database
```

Database file placed in ./databases/tw.db

Με αυτή την εντολή θέτουμε το tripwire σε κατάσταση δημιουργίας της βάσης δεδομένων.

Αφού περιμένουμε για λίγη ώρα το tripwire θα μας ενημερώσει ότι η βάση δεδομένων έχει κατασκευαστεί. Μεταβαίνουμε στο φάκελο /etc και τροποποιούμε το αρχείο motd

```
joe motd
```

Αποθηκεύουμε την τροποποίηση που κάναμε και πηγαίνουμε στο φάκελο /var. Εκεί δημιουργούμε έναν κρυφό φάκελο με το όνομα .test

(Η τελεία μπροστά από ένα αρχείο ορίζει ότι το αρχείο αυτό θα είναι κρυφό. Για να δούμε όλα τα αρχεία σε ένα φάκελο κάνουμε ls -al και όχι απλό ls)

Επίσης διαγράφουμε με την εντολή rm -r το φάκελο empty.

```
rm -r empty
```

Εκτελώντας τώρα το tripwire θα δούμε ότι με την σύγκριση των βάσεων δεδομένων θα ανακαλύψει με 100% επιτυχία τις αλλαγές που κάναμε στο filesystem.

```
#tripwire
```

Tripwire(tm) ASR (Academic Source Release) 1.3.1

(c) 1992, Purdue Research Foundation, (c) 1997, 1999 Tripwire  
Security Systems, Inc. All Rights Reserved. Use Restricted to  
Authorized Licensees.

### Phase 1: Reading configuration file

### Phase 2: Generating file list

### Phase 3: Creating file information database

### Total files scanned: 1091

### Files added: 1

### Files deleted: 1

### Files changed: 0

###

### Total file violations: 2

###

changed: -rw-r--r-- root 117 Mar 17 21:18:56 2003 /etc/motd

deleted: -rw-r--r-- root 117 Mar 17 21:18:56 2003 /var/empty

### **6.7.2 Nessus**

Θα χρησιμοποιήσουμε το πρόγραμμα Nessus Client, για να ανιχνεύσουμε ανοιχτές  
θύρες και ευπάθειες σε έναν υπολογιστή που βρίσκεται στο τοπικό δίκτυο.

### **Εκκίνηση Server**

Θα τρέξουμε το Server του Nessus με την εντολή:

```
#nessusd -D
```

Για να δημιουργήσουμε πιστοποιητικά για το server εκτελούμε την εντολή:

#nessus-mkcert

Για να δημιουργήσουμε κάποιο νέο user:

#nessus-adduser

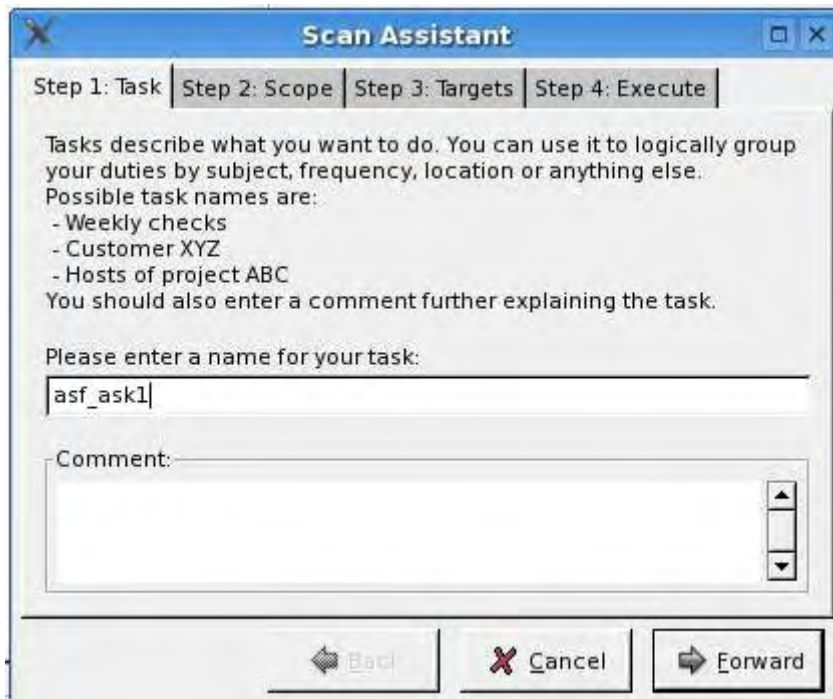
## Χρήση του Nessus Client

Για την εκκίνηση του Client εκτελούμε την εντολή:

#NessusClient

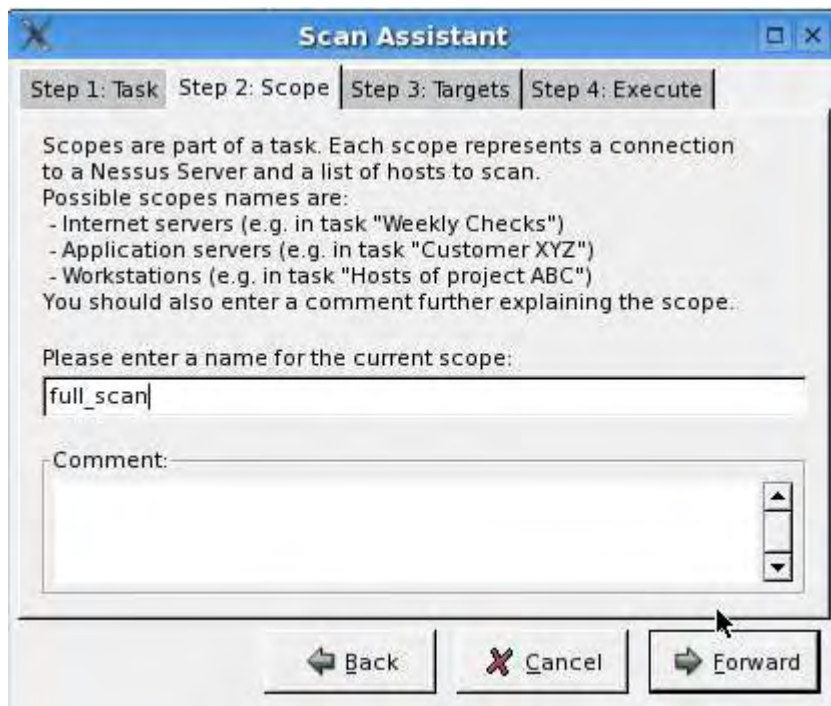
Μετά την εκκίνηση του Client επιλέγουμε File -> Scan Assistant

Εμφανίζεται ο οδηγός ελέγχου του Nessus Client



The screenshot shows the 'Scan Assistant' window with the 'Step 1: Task' tab selected. The window has a title bar with a close button. Below the title bar are four tabs: 'Step 1: Task', 'Step 2: Scope', 'Step 3: Targets', and 'Step 4: Execute'. The main area contains the following text: 'Tasks describe what you want to do. You can use it to logically group your duties by subject, frequency, location or anything else. Possible task names are: - Weekly checks - Customer XYZ - Hosts of project ABC. You should also enter a comment further explaining the task.' Below this is a text input field with the value 'asf\_ask1' and a label 'Please enter a name for your task:'. Underneath is a larger text area with the label 'Comment:'. At the bottom are three buttons: 'Back', 'Cancel', and 'Forward'.

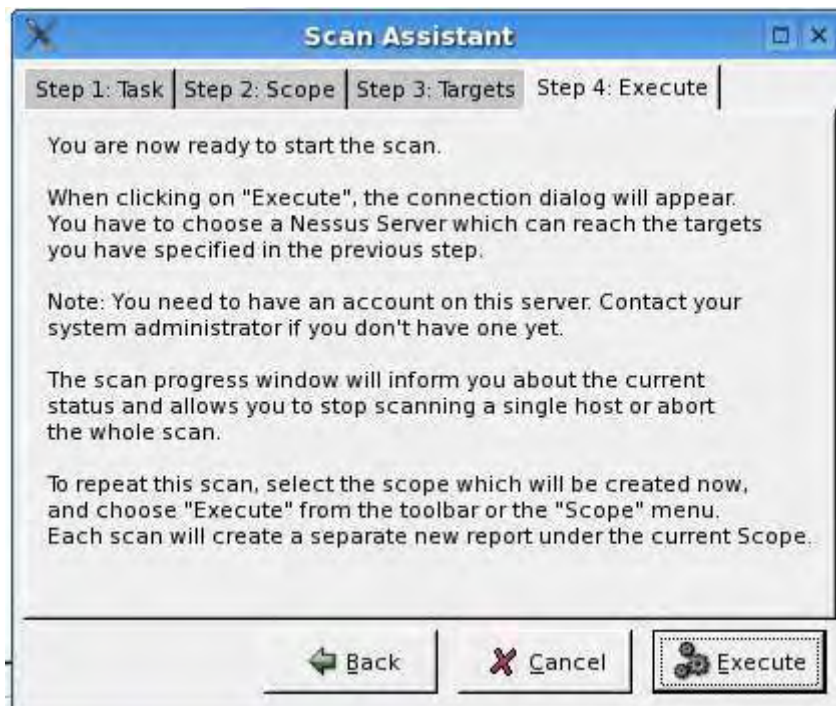
Δίνουμε ως όνομα άσκησης το *asf\_ask1* και πατάμε Forward.



Δίνουμε ως όνομα το *full\_scan* και πατάμε Forward.



Δίνουμε την IP διεύθυνση του υπολογιστή που θέλουμε να ελέγξουμε και πατάμε Forward.



Τέλος για να ξεκινήσει η διαδικασία εισόδου στον Nessus Server και έναρξης του ελέγχου πατάμε **Execute**

Μετά την ολοκλήρωση του οδηγού ελέγχου εμφανίζεται το παράθυρο εισόδου (Login) στο Nessus Server.

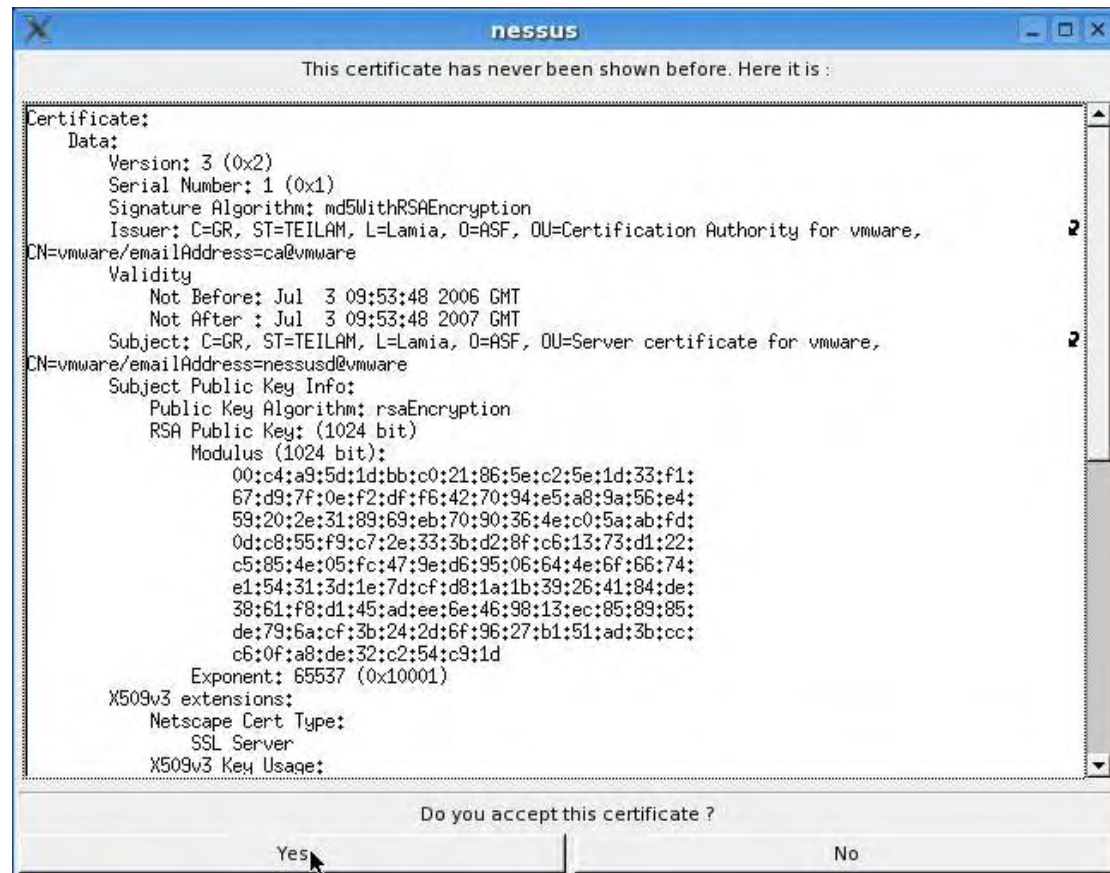




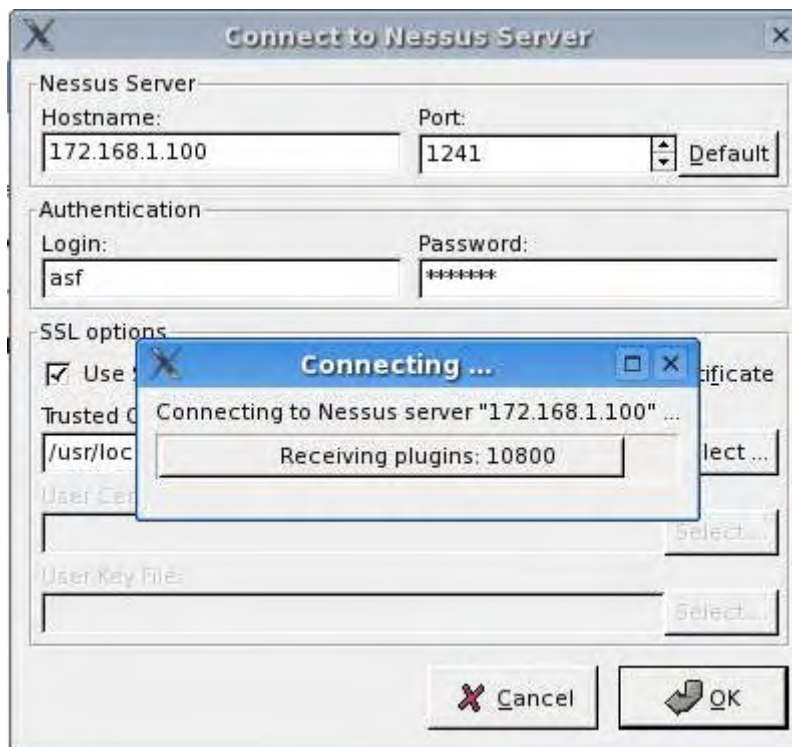
Στο πεδίο Hostname εισάγουμε την IP διεύθυνση του υπολογιστή στον οποίο εκτελείται ο Nessus Server.

Εισάγουμε στο πεδίο Login το όνομα χρήστη με το οποίο θα συνδεθούμε (asf) και στο πεδίο Password τον κωδικό πρόσβασης (diploma) και πατάμε OK.

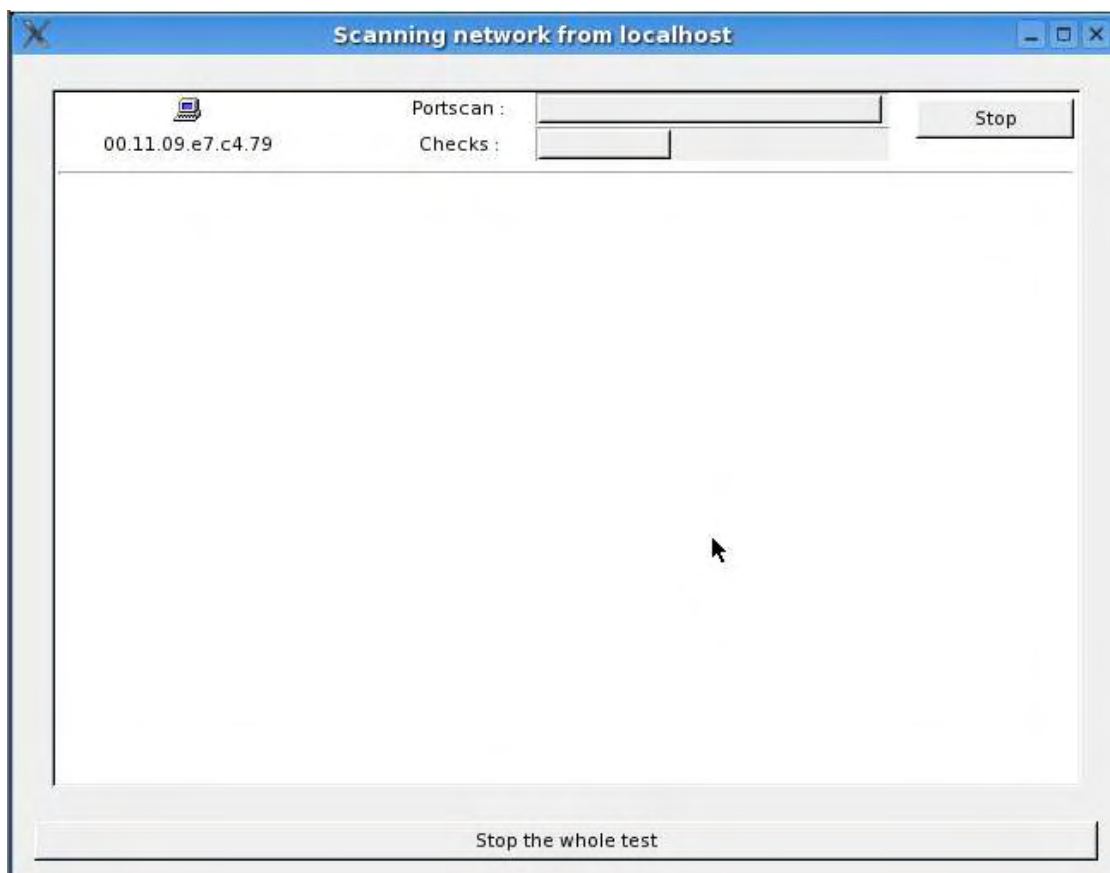
Εμφανίζεται το παράθυρο με το περιεχόμενο του πιστοποιητικού από τον Nessus Server το οποίο και αποδεχόμαστε πατώντας Yes.







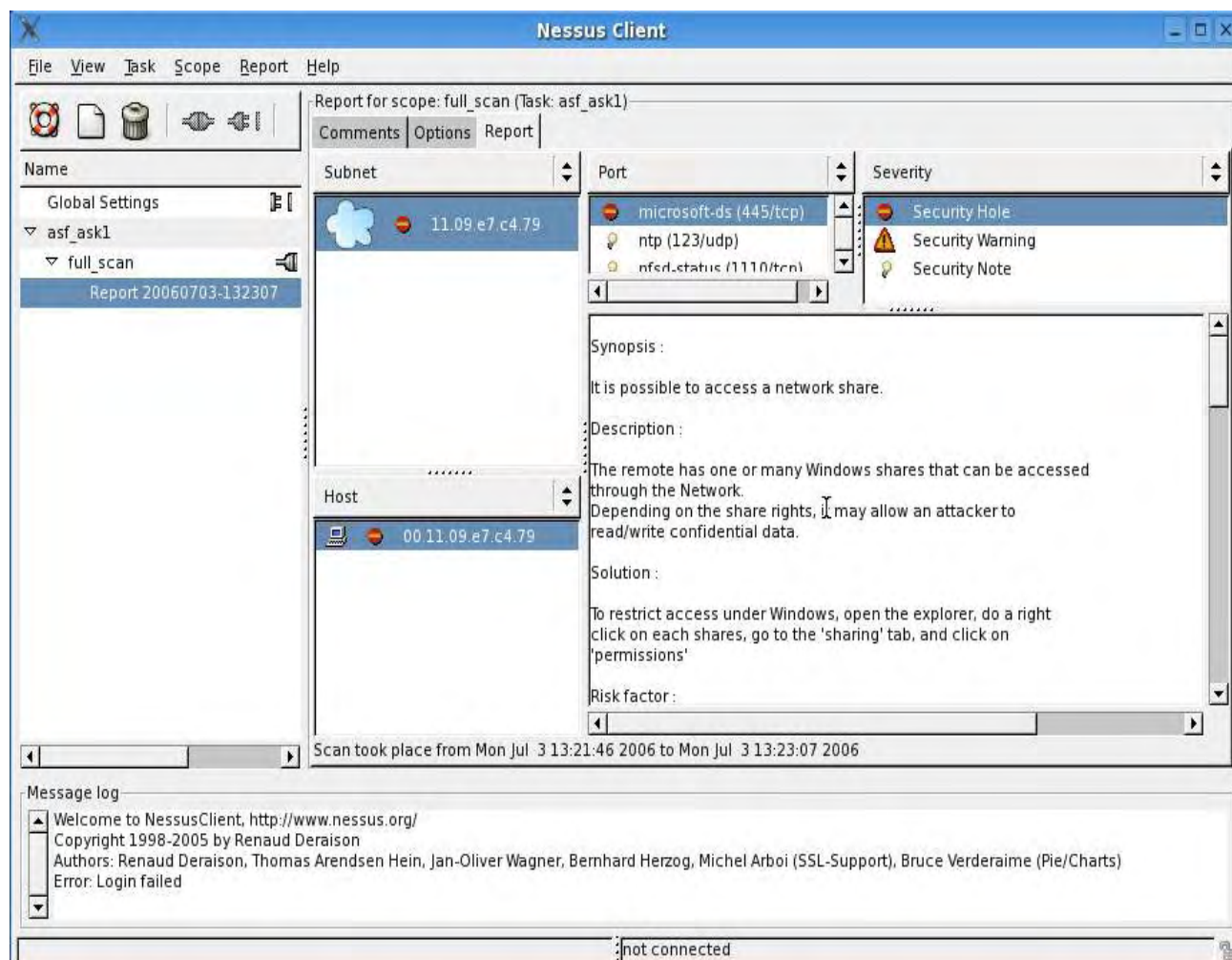
Εμφανίζεται το παράθυρο εισόδου και η ένδειξη προόδου της διαδικασίας φόρτωσης των βιβλιοθηκών του Nessus Server.



Μόλις ολοκληρωθεί η διαδικασία εισόδου εμφανίζεται το παράθυρο με την πρόοδο της διαδικασίας ελέγχου.

## Επισκόπηση αποτελεσμάτων

Μετά την ολοκλήρωση του ελέγχου εμφανίζεται το παράθυρο με τα αποτελέσματα της σάρωσης.



Από το αριστερό παράθυρο επιλέγουμε Report.

Στο πλαίσιο Subnet επιλέγουμε την MAC διεύθυνση που αντιστοιχεί στον υπολογιστή που κάναμε την σάρωση.

Στο πλαίσιο Port εμφανίζεται η λίστα με όλες τις ανοιχτές θύρες που εντοπίστηκαν και την υπηρεσία που αφορά την κάθε θύρα.

Επιλέγοντας κάποια θύρα, ακριβώς στο διπλανό πλαίσιο (Severity) εμφανίζονται χαρακτηρισμοί ασφαλείας για την θύρα και επιλέγοντας κάποιον χαρακτηρισμό βλέπουμε σημειώσεις και οδηγίες ασφαλείας σε περίπτωση που έχει ανιχνευτεί κάποια ευπάθεια στην συγκεκριμένη θύρα.

## **7. Η ΟΔΗΓΙΑ 2016/1148 ΤΗΣ Ε.Ε ΓΙΑ ΜΕΤΡΑ ΓΙΑ ΥΨΗΛΟ ΚΟΙΝΟ ΕΠΙΠΕΔΟ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΔΙΚΤΥΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ ΣΕ ΟΛΟΚΛΗΡΗ ΤΗΝ ΕΝΩΣΗ.**

### **7.1 Εισαγωγή**

Το Συμβούλιο της Ευρώπης θεωρεί ότι τα κράτη μέλη έχουν πολύ διαφορετικά επίπεδα ετοιμότητας, που έχουν οδηγήσει στον κατακερματισμό προσεγγίσεων στην Ένωση. Αυτό οδηγεί σε άνισο επίπεδο προστασίας καταναλωτών και επιχειρήσεων και υπονομεύει το συνολικό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών εντός της Ένωσης. Η απουσία κοινών απαιτήσεων για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών καθιστά εξάλλου αδύνατο να συσταθεί ένας καθολικός και αποτελεσματικός μηχανισμός συνεργασίας σε επίπεδο Ένωσης. Τα πανεπιστήμια και τα ερευνητικά κέντρα διαδραματίζουν καθοριστικό ρόλο στην προαγωγή της έρευνας, της ανάπτυξης και της καινοτομίας στους συγκεκριμένους τομείς. Προκειμένου λοιπόν να καλυφθούν όλα τα σχετικά συμβάντα και οι σχετικοί κίνδυνοι εξέδωσε την οδηγία 2016/1148 η οποία θα πρέπει να εφαρμόζεται τόσο στους φορείς εκμετάλλευσης βασικών υπηρεσιών όσο και στους παρόχους ψηφιακών υπηρεσιών.

### **7.2 Αντικείμενο και πεδίο εφαρμογής**

Η Οδηγία θεσπίζει μέτρα για την επίτευξη υψηλού κοινού επιπέδου ασφάλειας συστημάτων δικτύου και πληροφοριών εντός της Ένωσης, με σκοπό την καλύτερη λειτουργία της εσωτερικής αγοράς. Για τον σκοπό αυτό, η οδηγία:

- προβλέπει τις υποχρεώσεις να θεσπιστεί εθνική στρατηγική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών από όλα τα κράτη μέλη·
- δημιουργεί ομάδα συνεργασίας με σκοπό την υποστήριξη και τη διευκόλυνση της στρατηγικής συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ των κρατών μελών, καθώς και την ανάπτυξη της εμπιστοσύνης και της αξιοπιστίας μεταξύ τους·

- δημιουργεί δίκτυο ομάδων απόκρισης συμβάντων που αφορούν την ασφάλεια των υπολογιστών («δίκτυο CSIRT»), προκειμένου να συμβάλει στην ανάπτυξη της της αξιοπιστίας και εμπιστοσύνης μεταξύ των κρατών μελών και να προωθήσει την ταχεία και αποτελεσματική επιχειρησιακή συνεργασία·
- θεσπίζει απαιτήσεις ασφάλειας και κοινοποίησης για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και για τους παρόχους ψηφιακών υπηρεσιών·
- προβλέπει τις υποχρεώσεις των κρατών μελών να ορίζουν εθνικές αρμόδιες αρχές, ενιαία κέντρα επαφής και CSIRT με καθήκοντα σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών.

Ωστόσο η οδηγία δεν θίγει μέτρα για τη διαφύλαξη των ουσιωδών κρατικών λειτουργιών τους και ιδίως για τη διαφύλαξη της εθνικής ασφάλειας, συμπεριλαμβανομένων των μέτρων για την προστασία πληροφοριών των οποίων τη διάδοση τα κράτη μέλη θεωρούν αντίθετη προς τα ουσιώδη συμφέροντα ασφαλείας τους, καθώς και για τη διατήρηση του νόμου και της τάξης και ιδίως για τη διευκόλυνση της διερεύνησης, ανίχνευσης και δίωξης ποινικών αδικημάτων.

### **7.3 Εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών**

Κάθε κράτος μέλος οφείλει με την εφαρμογή της οδηγίας να θεσπίζει εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών στην οποία καθορίζονται οι στρατηγικοί στόχοι και κατάλληλα μέτρα πολιτικής και κανονιστικής ρύθμισης με σκοπό την επίτευξη και τη διατήρηση υψηλού επιπέδου ασφάλειας συστημάτων δικτύου και πληροφοριών. Η εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών θα καλύπτει ιδίως τα ακόλουθα θέματα:

- τους στόχους και τις προτεραιότητες της εθνικής στρατηγικής για την ασφάλεια συστημάτων δικτύου και πληροφοριών·
- το πλαίσιο διακυβέρνησης για την επίτευξη των στόχων και των προτεραιοτήτων της εθνικής στρατηγικής για την ασφάλεια συστημάτων δικτύων και πληροφοριών, συμπεριλαμβανομένων του ρόλου και των αρμοδιοτήτων των κυβερνητικών οργάνων και των λοιπών αρμόδιων φορέων·

- τον προσδιορισμό των μέτρων ετοιμότητας, παρέμβασης και αποκατάστασης, συμπεριλαμβανομένης της συνεργασίας ανάμεσα στο δημόσιο και ιδιωτικό τομέα·
- αναφορά των προγραμμάτων εκπαίδευσης, ευαισθητοποίησης και κατάρτισης σε σχέση με την εθνική στρατηγική ασφάλειας δικτύων και συστημάτων πληροφοριών·
- αναφορά των σχεδίων έρευνας και ανάπτυξης σχετικά με την εθνική στρατηγική ασφάλειας συστημάτων δικτύου και πληροφοριών·
- σχέδιο εκτίμησης κινδύνου για τον προσδιορισμό κινδύνων·
- κατάλογο των διαφόρων φορέων που εμπλέκονται στην υλοποίηση της εθνικής στρατηγικής ασφάλειας συστημάτων δικτύου και πληροφοριών.

#### 7.4 Εθνικές αρμόδιες αρχές

- Η οδηγία προβλέπει ότι τα κράτη μέλη οφείλουν να ορίσουν ή μία ή περισσότερες εθνικές αρμόδιες αρχές για την ασφάλεια των συστημάτων δικτύου και πληροφοριών («η αρμόδια αρχή»). Οι αρμόδιες αρχές παρακολουθούν την εφαρμογή της παρούσας οδηγίας σε εθνικό επίπεδο.
- Κάθε κράτος μέλος ορίζει ένα εθνικό ενιαίο κέντρο επαφής για την ασφάλεια των συστημάτων δικτύου και πληροφοριών («ενιαίο κέντρο επαφής»). Τα κράτη μέλη μπορούν να αναθέτουν τον ρόλο αυτόν σε υφιστάμενη αρχή. Σε περίπτωση που κράτος μέλος ορίσει μόνο μία αρμόδια αρχή, η εν λόγω αρμόδια αρχή αποτελεί και το ενιαίο κέντρο επαφής. Το ενιαίο κέντρο επαφής ασκεί καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών των κρατών μελών καθώς και με τις αρμόδιες αρχές άλλων κρατών μελών και την ομάδα συνεργασίας που αναφέρεται και το δίκτυο CSIRT.
- Κάθε κράτος μέλος ορίζει «Ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών» CSIRT, οι οποίες είναι υπεύθυνες για τον χειρισμό κινδύνων και συμβάντων βάσει επακριβώς καθορισμένης διαδικασίας.

Εφόσον αυτά είναι διαφορετικά, η αρμόδια αρχή, το ενιαίο κέντρο επαφής και οι CSIRT του ίδιου κράτους μέλους συνεργάζονται ως προς την τήρηση των υποχρεώσεων που προβλέπονται στην οδηγία.

## **7.5 Ομάδες συνεργασίας**

Συγκροτείται ομάδα συνεργασίας με σκοπό την υποστήριξη και τη διευκόλυνση της στρατηγικής συνεργασίας και την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών, και την ανάπτυξη της αξιοπιστίας και της εμπιστοσύνης, καθώς και την επίτευξη ενός κοινού υψηλού επιπέδου ασφάλειας συστημάτων δικτύου και πληροφοριών στην Ένωση. Η ομάδα συνεργασίας απαρτίζεται από αντιπροσώπους των κρατών μελών, την Επιτροπή και τον ENISA.

Η ομάδα συνεργασίας έχει τα εξής καθήκοντα:

- παρέχει στρατηγική καθοδήγηση για τις δραστηριότητες του δικτύου CSIRT
- ανταλλάσσει βέλτιστες πρακτικές για την ανταλλαγή πληροφοριών που αφορούν την κοινοποίηση συμβάντων
- ανταλλάσσει βέλτιστες πρακτικές μεταξύ των κρατών μελών και, σε συνεργασία με τον ENISA, επικουρεί τα κράτη μέλη στην ανάπτυξη ικανοτήτων στον τομέα της ασφάλειας συστημάτων δικτύου και πληροφοριών
- συζητεί τις δυνατότητες και την ετοιμότητα των κρατών μελών και, σε εθελούσια βάση, αξιολογεί τις εθνικές στρατηγικές ασφάλειας συστημάτων δικτύου και πληροφοριών και την αποτελεσματικότητα των CSIRT, και προσδιορίζει βέλτιστες πρακτικές,
- ανταλλάσσει πληροφορίες και βέλτιστες πρακτικές όσον αφορά την ευαισθητοποίηση και την κατάρτιση.
- ανταλλάσσει πληροφορίες και βέλτιστες πρακτικές για την έρευνα και την ανάπτυξη σχετικά με την ασφάλεια συστημάτων δικτύου και πληροφοριών.

- Κατά περίπτωση, ανταλλάσσει εμπειρίες για θέματα ασφάλειας συστημάτων δικτύου και πληροφοριών με τα αρμόδια θεσμικά και λοιπά όργανα της Ένωσης και με τους αρμόδιους οργανισμούς της.
- Συζητεί τα πρότυπα και τις προδιαγραφές με αντιπροσώπους των αρμόδιων ευρωπαϊκών οργανισμών τυποποίησης.
- Συλλέγει πληροφορίες για βέλτιστες πρακτικές σχετικά με κινδύνους και συμβάντα.
- Εξετάζει σε ετήσια βάση τις συνοπτικές εκθέσεις
- Συζητεί τις εργασίες που πραγματοποιούνται σε επίπεδο ασκήσεων σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών, εκπαιδευτικών προγραμμάτων και κατάρτισης, συμπεριλαμβανομένων των εργασιών που έγιναν από τον ENISA.
- Με τη συνδρομή του ENISA, ανταλλάσσει βέλτιστες πρακτικές σχετικά με τον προσδιορισμό των φορέων εκμετάλλευσης βασικών υπηρεσιών από τα κράτη μέλη, συμπεριλαμβανομένων μεταξύ άλλων όσον αφορά διασυννοριακές εξαρτήσεις σε σχέση με κινδύνους και συμβάντα.
- Συζητεί τις λεπτομέρειες για την υποβολή κοινοποιήσεων συμβάντων.

## **7.6 Ασφάλεια συστημάτων δικτύου και πληροφοριών των φορέων εκμετάλλευσης βασικών υπηρεσιών**

- Τα κράτη μέλη εξασφαλίζουν ότι οι φορείς εκμετάλλευσης βασικών υπηρεσιών λαμβάνουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν στις δραστηριότητές τους. Λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες, τα μέτρα αυτά διασφαλίζουν επίπεδο ασφάλειας των συστημάτων δικτύου και πληροφοριών ανάλογο προς τον εκάστοτε κίνδυνο.
- Τα κράτη μέλη εξασφαλίζουν ότι οι φορείς εκμετάλλευσης βασικών υπηρεσιών λαμβάνουν κατάλληλα μέτρα για την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων που επηρεάζουν την ασφάλεια

των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούνται για την παροχή αυτών των βασικών υπηρεσιών, με σκοπό τη διασφάλιση της συνέχειάς τους.

- Τα κράτη μέλη εξασφαλίζουν ότι οι φορείς εκμετάλλευσης βασικών υπηρεσιών κοινοποιούν χωρίς αδικαιολόγητη καθυστέρηση στην αρμόδια αρχή ή στην CSIRT συμβάντα με σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών που παρέχουν. Οι κοινοποιήσεις περιλαμβάνουν πληροφορίες που επιτρέπουν στην αρμόδια αρχή ή την CSIRT να προσδιορίσει τυχόν διασυννοριακό αντίτυπο του συμβάντος. Η κοινοποίηση δεν συνεπάγεται αυξημένη ευθύνη για τον κοινοποιούντα.
- Για να προσδιοριστεί η σοβαρότητα του αντίκτυπου ενός συμβάντος, λαμβάνονται υπόψη ειδικότερα οι ακόλουθες παράμετροι:
  - α) ο αριθμός των χρηστών που επηρεάζονται από τη διατάραξη της βασικής υπηρεσίας·
  - β) η διάρκεια του συμβάντος·
  - γ) το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν·
- Βάσει των πληροφοριών που παρέχονται στην κοινοποίηση από τον φορέα εκμετάλλευσης βασικών υπηρεσιών, η αρμόδια αρχή ή η CSIRT ενημερώνει το ή τα άλλα επηρεαζόμενα κράτη μέλη αν το συμβάν έχει σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών στο εν λόγω κράτος μέλος. Στο πλαίσιο της ενημέρωσης αυτής, η αρμόδια αρχή ή η CSIRT, διαφυλάσσει σύμφωνα με το ενωσιακό δίκαιο ή με την εθνική νομοθεσία που είναι σύμφωνη προς το ενωσιακό δίκαιο, την ασφάλεια και τα εμπορικά συμφέροντα του φορέα εκμετάλλευσης βασικών υπηρεσιών, καθώς και το απόρρητο των πληροφοριών που έχουν παρασχεθεί στην κοινοποίησή του.
- Όταν οι περιστάσεις το επιτρέπουν, η αρμόδια αρχή ή η CSIRT παρέχει στον κοινοποιούντα φορέα εκμετάλλευσης βασικών υπηρεσιών πληροφορίες όσον αφορά τις ενέργειες σε συνέχεια της κοινοποίησής του, όπως πληροφορίες που θα μπορούσαν να υποστηρίξουν τον αποτελεσματικό χειρισμό του συμβάντος.



- Κατόπιν αιτήματος της αρμόδιας αρχής ή της CSIRT, το ενιαίο κέντρο επαφής διαβιβάζει τις κοινοποιήσεις στα ενιαία κέντρα επαφής άλλων επηρεαζόμενων κρατών μελών.
- Κατόπιν διαβούλευσης με τον κοινοποιούντα φορέα εκμετάλλευσης βασικών υπηρεσιών, η αρμόδια αρχή ή η CSIRT μπορεί να ενημερώνει το κοινό σχετικά με μεμονωμένα συμβάντα, σε περίπτωση που η ενημέρωση του κοινού είναι απαραίτητη για την πρόληψη συμβάντος ή την αντιμετώπιση συμβάντος που βρίσκεται σε εξέλιξη.
- Οι αρμόδιες αρχές, ενεργώντας από κοινού εντός της ομάδας συνεργασίας, μπορούν να καταρτίζουν και να εκδίδουν κατευθυντήριες γραμμές σχετικά με τις περιστάσεις υπό τις οποίες οι φορείς εκμετάλλευσης βασικών υπηρεσιών είναι υποχρεωμένοι να κοινοποιούν συμβάντα, συμπεριλαμβανομένων μεταξύ άλλων των παραμέτρων που προσδιορίζουν τη σοβαρότητα του αντίκτυπου ενός συμβάντος.

## **7.7 Ασφάλεια συστημάτων δικτύου και πληροφοριών των παρόχων ψηφιακών υπηρεσιών**

Τα κράτη μέλη εξασφαλίζουν ότι οι πάροχοι ψηφιακών υπηρεσιών προσδιορίζουν και λαμβάνουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν στο πλαίσιο της παροχής υπηρεσιών εντός της Ένωσης. Λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες, τα μέτρα αυτά εξασφαλίζουν ένα επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών ανάλογο προς τον εκάστοτε κίνδυνο, και συνεκτιμούν τα ακόλουθα στοιχεία:

- την ασφάλεια των συστημάτων και των εγκαταστάσεων,
- τη διαχείριση συμβάντων,
- τη διαχείριση της επιχειρησιακής συνέχειας,
- την παρακολούθηση, τις επιθεωρήσεις και τις δοκιμές,
- τη συμμόρφωση με διεθνή πρότυπα.

Τα κράτη μέλη εξασφαλίζουν ότι οι πάροχοι ψηφιακών υπηρεσιών κοινοποιούν στην αρμόδια αρχή ή την CSIRT χωρίς αδικαιολόγητη καθυστέρηση κάθε συμβάν που έχει σημαντικό αντίκτυπο στην παροχή της υπηρεσίας που προσφέρουν εντός της Ένωσης.

Οι κοινοποιήσεις περιλαμβάνουν πληροφορίες που επιτρέπουν στην αρμόδια αρχή ή την CSIRT να προσδιορίσουν τη σοβαρότητα τυχόν διασυνοριακού αντίκτυπου.

Για να προσδιοριστεί εάν ο αντίκτυπος ενός συμβάντος είναι σημαντικός, λαμβάνονται

υπόψη ειδικότερα οι ακόλουθες παράμετροι:

- ο αριθμός των χρηστών που επηρεάζονται από το συμβάν, ιδίως των χρηστών που εξαρτώνται από την υπηρεσία για την παροχή των δικών τους υπηρεσιών·
- η διάρκεια του συμβάντος·
- το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν·
- η έκταση της διατάραξης της λειτουργίας της υπηρεσίας·
- η έκταση του αντίκτυπου στις οικονομικές και κοινωνικές δραστηριότητες.

Κατά περίπτωση, και ιδίως εάν το συμβάν αφορά δύο ή περισσότερα κράτη μέλη, η αρμόδια αρχή ή η CSIRT ενημερώνουν τα άλλα κράτη μέλη που επηρεάζονται από το συμβάν. Κατά περίπτωση, οι αρχές ή οι CSIRT άλλων ενδιαφερομένων κρατών μελών μπορούν να ενημερώνουν το κοινό σχετικά με μεμονωμένα συμβάντα ή να απαιτούν από τον πάροχο ψηφιακών υπηρεσιών να το πράξει, όταν η ενημέρωση του κοινού είναι απαραίτητη για την πρόληψη συμβάντος ή την αντιμετώπιση συμβάντος που βρίσκεται σε εξέλιξη ή σε περίπτωση που η αποκάλυψη του συμβάντος είναι προς το δημόσιο συμφέρον.

## **7.8 Μεταφορά στο εθνικό δίκαιο**

Τα κράτη μέλη υποχρεούνται να θεσπίσουν και να δημοσιεύσουν έως τις 9 Μαΐου 2018 τις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις για να

συμμορφωθούν με τη νέα οδηγία, ενώ τα μέτρα αυτά θα τεθούν σε εφαρμογή από τις 10 Μαΐου 2018.

## 8. ΕΠΙΛΟΓΟΣ

Μείζον ζήτημα της εποχής μας αποτελεί η ασφάλεια των πληροφοριακών συστημάτων και των δικτύων τους. Για να αντιμετωπιστεί ο κίνδυνος αυτός έχουν κατά καιρούς καταρτιστεί διάφορες πολιτικές ασφαλείας. Αυτές ουσιαστικά προσπαθούν να προβλέψουν συμβάντα και καταστάσεις απειλητικές για την ασφάλεια και με τεχνικούς τρόπους να την αποτρέψουν. Έχει όμως εκ των πραγμάτων αποδειχθεί ότι από μόνη της καμία πολιτική ασφαλείας, με τους μηχανισμούς και τις τεχνικές που προβλέπει, δεν αρκεί για να αντιμετωπίσει τα διαρκώς ανανεώσιμα και γι' αυτό ουσιαστικά απρόβλεπτα συμβάντα ασφαλείας. Κι αυτό γιατί οι πιθανοί συνδυασμοί ενεργειών είναι άπειροι και ο δυσκολότερος όλων παράγοντας είναι η ανθρώπινη φύση που κρύβει εκπλήξεις άλλοτε ευχάριστες και άλλοτε δυσάρεστες.

Μέσα σε αυτό το πλαίσιο ο νομοθέτης καλείται να παρακολουθεί συνεχώς τις εξελίξεις στην τεχνολογία και πληροφορική. Η σκέψη του και οι νομικές του ενέργειες πρέπει να αποσκοπούν στην ανάπτυξη του αισθήματος ασφαλείας στους χρήστες του διαδικτύου. Σκοπός κατά συνέπεια του νομοθετικού του έργου πρέπει να είναι η βελτίωση της διαδικτυακής – πληροφορικής ζωής τους. Σε καμία περίπτωση δεν πρέπει το διαδίκτυο να καταστεί παράγοντας καταδυνάστευσης, καταπάτησης ελευθεριών και νέο μέσο επίτευξης εγκλημάτων.

Σε ενωσιακό επίπεδο τώρα , έχει επίσης παρατηρηθεί ότι η συχνότητα των συμβάντων ασφαλείας έχει αυξηθεί και συνεχώς αυξάνεται. Αυτό αποτελεί μείζονα απειλή για τη λειτουργία των συστημάτων δικτύου και των πληροφοριακών συστημάτων. Έχει επίσης παρατηρηθεί, ότι λόγω του διακρατικού τους χαρακτήρα ενδεχόμενη σημαντική διατάραξη των συστημάτων αυτών μπορεί να επηρεάσει την ένωση στο σύνολό της. Κατά συνέπεια , η νέα Οδηγία 2016/1148 όπως αναλύθηκε παραπάνω είναι ανάγκη να εφαρμόζεται τόσο στους φορείς εκμετάλλευσης βασικών υπηρεσιών όσο και στους παρόχους ψηφιακών υπηρεσιών.

Συμπερασματικά λοιπόν, οι νομοθετικές προσπάθειες είτε αυτές γίνονται στο πλαίσιο των εσωτερικού δικαίου με έκδοση και ψήφιση νόμων , είτε στο επίπεδο της Ευρωπαϊκής Ένωσης με έκδοση σχετικών Οδηγιών πρέπει να διαπνέονται από τα ακόλουθα :

- Σεβασμό της ιδιωτικής ζωής και των επικοινωνιών.
- Προστασία των δεδομένων προσωπικού χαρακτήρα.
- Επιχειρηματική ελευθερία.
- Προστασία του δικαιώματος ιδιοκτησίας
- Το δικαίωμα της πραγματικής προσφυγής ενώπιον δικαστηρίου.
- Το προηγούμενο δικαίωμα της ακρόασης.

## ΒΙΒΛΙΟΓΡΑΦΙΑ

- Ευγενία Αλεξανδροπούλου- Αιγυπτιάδου, «Προσωπικά δεδομένα», εκδόσεις Σάκκουλα Αθήνα-Κομοτηνή, 2007
- Ειρήνη Βασιλάκη, Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, εκδόσεις Αντ.Ν. Σάκκουλα, ΑθήναΚομοτηνή, 1993
- Αποστόλης Γέροντας, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, εκδ. Αντ. Ν Σάκκουλας, Αθήνα-Κομοτηνή, 2002
- Αποστόλης Γέροντας, Πληροφορική και δίκαιο, εκδόσεις Αντ.Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 1990
- Ιωάννης Δ. Ιγγλεζάκης, Εισαγωγή στο δίκαιο της Πληροφορικής, εκδόσεις Σάκκουλα Αθήνα- Θεσσαλονίκη, 2006
- Γρηγόρης Λάζος, Πληροφορική και έγκλημα, εκδόσεις Νομική Βιβλιοθήκη, Αθήνα 2001
- Τάσος Ν.Μαρίνου, Οι ηλεκτρονικοί υπολογιστές και το δίκαιο, εκδόσεις Αντ.Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 1991
- Λίλιαν Μήτρου, Το δίκαιο στην κοινωνία της πληροφορίας, εκδόσεις Σάκκουλα Αθήνα- Θεσσαλονίκη, 2002

- Γεώργιος Νούσκαλης, Ψηφιακή Τεχνολογία και Δίκαιο, εκδόσεις Αντ.Ν. Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2004
- Ευάγγελος Παπακωνσταντίνου, Νομικά θέματα πληροφορικής, εκδόσεις Σάκκουλα Αθήνα- Θεσσαλονίκη, 2006
- Θεόδωρος Σιδηρόπουλος, Το δίκαιο του Διαδικτύου, εκδόσεις Σάκκουλα Αθήνα- Θεσσαλονίκη, 2003
- Τατιάνα-Ελένη Συνοδινού, Η Νομική Προστασία των Βάσεων Δεδομένων, εκδόσεις Σάκκουλα Αθήνα- Θεσσαλονίκη, 2004
- Α.Φραγκούλη, Προστασία Δεδομένων στο Διαδίκτυο, εις συλλογικόν έργον Εφαρμογές Εμπορικού Δικαίου, Επιμέλεια Γ Τριανταφυλλάκη, Νομική Βιβλιοθήκη 2007
- Καρακώστας Ι., Δίκαιο & Internet, Νομικά ζητήματα του Διαδικτύου, εκδόσεις Π. Σάκκουλας, Αθήνα, 2003
- Κάτσικας Σωκ., Γκρίτζαλης Δημ., Γκρίτζαλης Στ., Ασφάλεια πληροφοριακών συστημάτων, Εκδόσεις Νέων Τεχνολογιών Αθήνα, 2004
- Κομνηνός Θεόδωρος, Σπυράκης Γ.Παύλος, Ασφάλεια Δικτύων και Υπολογιστικών Συστημάτων, Εκδόσεις Ελληνικά Γράμματα, 2002
- Μάττας Α., Ασφάλεια Πληροφοριακών Συστημάτων σε συνεργατικά περιβάλλοντα εφαρμογών με βάση το διαδίκτυο, Θεσσαλονίκη 2007.
- Κωνσταντίνος Αντωνής, Ασφάλεια Υπολογιστικών Συστημάτων, Λαμία 2003
- Χρήστος Α. Ηλιούδης, Κων/νος Ράντος, Θέματα ασφάλειας των εφαρμογών κινητών τηλεφώνων, Λαμία
- Κωνσταντίνος Αντωνής, Ασκήσεις Εργαστηρίου Ασφάλειας Υπολογιστικών Συστημάτων, Λαμία 2006
- Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα.

- Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6<sup>ης</sup> Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση.
- Νόμος 2472/97, Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, 10-4-97/ΦΕΚ 50/Τεύχος Α', 1997.
- Δικτυακός τόπος «Αρχής Προστασίας Προσωπικών Δεδομένων», [www.dpa.gr](http://www.dpa.gr)
- [www.lawandtech.eu](http://www.lawandtech.eu)
- [www.lawspot.gr](http://www.lawspot.gr)
- [www.infosec.aueb.gr](http://www.infosec.aueb.gr)
- [www.safeline.gr](http://www.safeline.gr)
- [www.e-crime.gr](http://www.e-crime.gr)