Τμήμα Τηλεπικοινωνιακών Συστημάτων και Δικτύων
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Μεσολογγίου

ΠΤΥΧΙΑΚΗ ΑΣΚΗΣΗ

ΘΕΜΑ: Ασφάλεια προσωπικών δεδομένων στις τηλεπικοινωνίες και τα δίκτυα. Νομική προσέγγιση.

Επιβλέπων Καθηγητής:
Δρ. Νίκος Κρεμμύδας
Δικηγόρος Παρ' Αρείω Πάγω

Επιμέλεια εργασίας:
Κουκή Δήμητρα
Α.Μ: 0243

ΝΑΥΠΑΚΤΟΣ 2013

«Δηλώνω υπεύθυνα ότι το κείμενο που σας παραθέτω είναι από προσωπική μελέτη, έρευνα και εργασία. Οι πηγές που χρησιμοποιήθηκαν αναγράφονται στην βιβλιογραφία καθότι γνωρίζω ότι η λογοκλοπή θεωρείται παράπτωμα και μπορεί να επιφέρει νομικές κυρώσεις καθώς επίσης η οποιαδήποτε αναπαραγωγή του χωρίς την έγγραφη άδεια του υπευθύνου-επιμελήτριας τιμωρείται από το νόμο»

Ευχαριστίες

Ευχαριστώ θερμά,

τον επόπτη της πτυχιακή μου εργασίας ***Δρ. Νίκο Κρεμμύδα***
για την νομική βοήθεια και υποστήριξη κατά την διάρκεια εκπόνησης της πτυχιακής άσκησης.
Επίσης ευχαριστώ την οικογένεια μου και τους φίλους/συμφοιτητές-τριες που απέκτησα σ
την σχολή για την υπομονή και υποστήριξη που μου πρόσφεραν όλα αυτά τα χρόνια.

.

Περιεχόμενα

Κεφάλαιο 4: Ηλεκτρονικό Έγκλημα

Κεφάλαιο 5^{ο}: Προσωπικά δεδομένα

Πίνακας Γραφημάτων

Κεφάλαιο 1ο

1.1 Περίληψη

Η ραγδαία ανάπτυξη στις τηλεπικοινωνίες και τα δίκτυα έχουν εισβάλλει στην καθημερινότητα μας. Οι νέες τεχνολογίες μας προσφέρουν πληθώρα πλεονεκτημάτων με αποτέλεσμα η καθημερινότητα να γίνεται πιο ποιοτική και λιγότερο πολύπλοκη.

Οι τηλεπικοινωνίες και τα δίκτυα σε συνδυασμό με την χρήση του internet μας προσφέρει με ένα "click" πολλές από τις καθημερινές μας ανάγκες όπως αναζήτηση πληροφοριών, ηλεκτρονικού ταχυδρομείου για πιο άμεση επικοινωνία, ηλεκτρονικές συναλλαγές και άλλες ποικίλες εφαρμογές που κάνουν την καθημερινότητα μας σαφώς πιο εύκολη.

Οι νέες τεχνολογίες εκτός από την πληθώρα των πλεονεκτημάτων που προσφέρει δημιούργησε και νέες μορφές εγκλήματος δηλαδή το "Ηλεκτρονικό Έγκλημα".

Αυτές οι μορφές μπορεί να είναι υποκλοπή δεδομένων, παρακολούθηση χρηστών και πολλές άλλες μορφές που αναπτύσσονται ανάλογα με την καθημερινότητα και την χρήση των τηλεπικοινωνιών και δικτύων.

Επομένως οι τηλεπικοινωνίες και τα δίκτυα θα πρέπει να παρέχουν όσο δυνατόν μεγαλύτερη ασφάλεια στους χρήστες και οι χρήστες θα πρέπει να γνωρίζουν τους κινδύνους που μπορεί να προκληθούν από λάθος χειρισμό αυτών των τεχνολογιών.

Στην παρούσα πτυχιακή εργασία θα αναλύσουμε στις τηλεπικοινωνίες και τα δίκτυα τρόπους ασφαλείας για αποφυγή από τέτοιου είδους επιθέσεις αλλά και πώς η νομοθεσία μας προστατεύει στις Τηλεπικοινωνίες και τα δίκτυα.

1.2 Εισαγωγή

Στη σημερινή εποχή της πληροφορίας και των τεχνολογικών εξελίξεων παρατηρείται η ολοένα αυξανόμενη διείσδυση των ευρυζωνικών τεχνολογιών στην κοινωνία και διαφαίνεται η τάση για σύγκλιση των τηλεπικοινωνιών και δικτύων παροχής υπηρεσιών καθώς και για πρόσβαση «οποτεδήποτε», «από οπουδήποτε», και «με οτιδήποτε».

Έτσι σε αυτό το συνεχώς μεταβαλλόμενο περιβάλλον, η έννοια της Ασφάλειας Τηλεπικοινωνιών & Δικτύων αποκτά μια καινούρια διάσταση. Παραδοσιακές ηλεκτρονικές απειλές όπως: Κακόβουλο λογισμικό, μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και συστήματα, ενοχλητικά ηλεκτρονικά μηνύματα, επιθέσεις κλοπής ηλεκτρονικής ταυτότητας κ.λπ., αναμένεται να βρουν νέα και εξίσου γόνιμα εδάφη για την εξάπλωσή τους ειδικά στις τηελικοινωνίες και τα δίκτυα. Επιπλέον, η κακόβουλη χρήση των τεχνολογιών δικτύωσης μπορεί να διευκολύνει την τέλεση συμβατικών εγκλημάτων ή να ενισχύσει επιπλέον το καταστρεπτικό τους έργο.

Οι έννοιες «ηλεκτρονικό έγκλημα» ή «κυβερνο-έγκλημα» καθώς και οι τεχνολογίες που χρησιμοποιούνται για τη διάπραξη, ανίχνευση και αντιμετώπιση κακόβουλων επιθέσεων σε συστήματα και εφαρμογές, αποτελούν αναπόσπαστο κομμάτι του γνωστικού αντικειμένου της Ασφάλειας Πληροφοριακών Συστημάτων όπου οι εισβολείς μέσω αυτών υποβάλλονται στην παραβίαση των προσωπικών δεδομένων αλλωτε χωρίς αποτέλεσμα και αλλωτε με επιτυχή τρόπο απόστασης προσωπικών μας στοιχείων.

Στην παρούσα πτυχιακή εργασία θα παρουσιάσουμε την ορολογία των τηλεπικοινωνιών και δικτύων θα αναλύσουμε τις απειλές και τους κινδύνους που μπορεί να παρουσιαστούν με την χρήση αυτών των τεχνολογιών, ποιες είναι οι μορφές ηλεκτρονικού εγκλήματος και με ποιους τρόπους μπορεί ο ίδιος ο χρήστης να προστατευθεί από τυχόν εισβολείς, ποιο είναι το προφίλ των εισβολέων και γιατί επιδιώκουν την υποκλοπή των δεδομένων μας, στατιστικά στοιχεία με γραφήματα για τους χρήστες που υπέστησαν παραβίαση προσωπικών δεδομένων με βάση τα επίσημα στοιχεία της ελληνικής αστυνομίας καθώς επίσης και πως η πολιτεία μπορεί να προστατεύσει τον κάθε χρήστη όταν εκτεθούν τα προσωπικά του δεδομένα με βάση την νομοθεσία που ορίζει το κράτος αλλα και πως ο χρήστης προστατεύεται όταν τα προσωπικά του δεδομένα παραβιάζονται εκτός Ελλάδος.

Import

In the current season of information and technological developments is observed the continuously increasing infiltration of broadband technologies in the society and emerges the tendency for convergence of telecommunications and networks of benefit of services as well as for access "whenever", "from anywhere", and "with anything". Thus in this continuously altered environment, the significance of Safety of Telecommunications and Networks acquires a new dimension.
Traditional electronic threats as:
Malicious software, not permitted access in computers and systems, annoying electronic messages, attacks of theft of electronic identity etc. , they are expected to find new and equally fertile grounds for the spread specifically in the tielikoinonies and networks.
Moreover, the malicious use of technologies ofnetworking can facilitate the performance convention al crimes or it strengthens more over
their calamitous work. The significances"electronic crime" or "kyberno-crime" as well as
the technologies that areused for the perpetration, detection and confrontationof malicious attacks i n systems and applications, being the subject
of integral piececognitive of Safety Informative Systems where the intruders viathese are submitted in the violation personal data allote without result and allotewith successful way of dista nce of or personalelements.
In the present final work we will present the terminology of telecommunications and networks we will analyze the threats and the dangers that can present themselves with use of these technologies, who are also the forms of electronic crime with who ways can himself the user be protected from by any chance intruders, who is the profile intruders and because seek the wiretapping of our data, statistical elements with recordings for the users that suffered violation of personal data with base the official elements of Greek police as well as that the state can protect each user when are exposed his personal data with base the legislation that fixes the state but also that the user is protected when his personal data are forced except Greece.

1.3 Σκοπός και στόχος της πτυχιακής εργασίας

1.3.1 Σκοπός της πτυχιακής εργασίας

Σκοπός της υπάρχουσας πτυχιακής εργασίας είναι να αναδείξουμε τους κινδύνους που μπορούν να παρουσιαστούν στην καθημερινότητα μας χρησιμοποιώντας τις τηλεπικοινωνίες και τα δίκτυα είτε αυτές αφορούν τους κινδύνους που μπορούν να αφορούν τα μηχανήματα είτε τους κινδύνους που αφορούν τα φυσικά πρόσωπα, δηλαδή τους χρήστες ως προς την ασφάλεια για την διαφύλαξη των προσωπικών τους δεδομένων αλλά και σε περίπτωση που αυτό δεν είναι εφικτό με ποιους τρόπους είτε τεχνικούς είτε νομικούς τρόπους μπορεί να διαφυλάξει κάποιος χρήστης την ακεραιότητα των δεδομένων του.

1.3.2 Στόχος της πτυχιακής εργασίας

Στόχος της παρούσας πτυχιακής εργασίας είναι να παρουσιάσουμε τους κινδύνους και τους τρόπους αντιμετώπισης των τηλεπικοινωνιών και των δικτύων ως προς την ασφάλεια.
Να παρουσιάσουμε πως μπορεί να γίνει σωστή ενημέρωση ως προς τους τρόπους που μπορούν οι χρήστες να προφυλαχτούν καθώς επίσης και να ενημερωθούν με ποιόν τρόπο η πολιτεία τους προστατεύει με την νομική προσέγγιση από τους κακόβουλους χρήστες που παραβιάζουν τα δεδομένα των χρηστών.

Κεφάλαιο 2ο

2.1 Ιστορική Αναδρομή για την ασφάλεια των τηλεπικοινωνιών και δικτύων

1955-1965: η ασφάλεια των υπολογιστών περιοριζόταν μόνο στο να περιορίζεται ένας δυσαρεστημένος υπάλληλος για να μην προκαλέσει καταστροφές και στο να μην έχουν οι ανταγωνιστές πρόσβαση στον υπολογιστή της επιχείρησης.

965-1975: άρχισαν οι κεντρικοί υπολογιστές να γίνονται πιο ισχυροί και ο αριθμός των χρηστών που συνδεόταν σε αυτούς έφτασαν τις χιλιάδες, το θέμα της υπευθυνότητα έγινε πιο σημαντικό. Η εισβολή εκείνη την εποχή ήταν σε επίπεδο φημών, περί κακόβουλων προγραμματιστών, που έκαναν παράνομες ενέργειες - όπως να γράφουν κώδικα που έπαιρνε τα δεκαδικά ψηφία τραπεζικών συναλλαγών και τα κατέθετε στο δικό τους λογαριασμό ή να γράφουν συστήματα "πίσω πόρτας" στον κώδικά τους για να μπορούν να μπαίνουν σε συστήματα.

Η έλλειψη πραγματικής ασφάλειας εμφανίστηκε στην περίοδο 1975-1985, όταν οι εταιρείες άρχισαν να παρέχουν απομακρυσμένη προσπέλαση σε χρήστες τερματικών, μέσω μόντεμ που εργαζόταν χρησιμοποιώντας το δημόσιο τηλεφωνικό δίκτυο. Το 1969 η *Defense Advanced Research Projects Agency (DARPA)* ξεκίνησε ένα έργο για να μελετήσει τα δίκτυα δρομολόγησης πακέτων, όπου μεμονωμένα μικρά μηνύματα μπορούσαν να μεταδίδονται ανάμεσα σε δύο τερματικά συστήματα και να δρομολογούνται από ενδιάμεσα συστήματα με ένα χαλαρά ιεραρχικό τρόπο, επιτρέποντας έτσι σε οποιονδήποτε βρισκόταν στο δίκτυο να επικοινωνεί με τους άλλους. Αυτές οι ερευνητικές προσπάθειες άρχισαν να αποδίδουν καρπούς στα τέλη της δεκαετίας του '70. Η IBM ανέπτυξε τον αλγόριθμο *Data Encryption Standard (DES)* για την κυβέρνηση των Η.Π.Α το 1975. Σχεδόν ταυτόχρονα, οι *Whitfield Diffie* και *Martin Hellman* ανέπτυξαν την έννοια της κωδικοποίησης δημόσιου κλειδιού (Public Key Encryption, PKE), η οποία επέλυσε το πρόβλημα της ασφαλούς ανταλλαγής κλειδιού. Το 1977, οι *Rivest*, *Shamir* και *Adelman* υλοποίησαν την PKE στον ιδιοτελή αλγόριθμο κρυπτογράφησης RSA, που ήταν τα θεμέλια της σημερινής ασφάλειας δικτύων. Ωστόσο ενδιαφέρον για την ασφάλεια τροφοδοτήθηκε από το έγκλημα του *Kevin Mitnick* όπου διέπραξε το μεγαλύτερο έγκλημα σε Ιστορίας των Ηνωμένων Πολιτειών το 1979. Οι απώλειες ήταν ογδόντα εκατομμυρίων δολάρια στις ΗΠΑ και την πνευματική ιδιοκτησία του πηγαίου κώδικα από μια ποικιλία των εταιρειών. Από τότε, ασφάλεια των πληροφοριών ήρθε στο προσκήνιο. Σε τεχνικό επίπεδο στο προσκήνιο ήρθε και η προστασία των χρηστών από κακόβουλους χρήστες και στο νομοθετικό πλαίσιο. Οι διάφορες μορφές του ηλεκτρονικού εγκλήματος ρυθμίζονται και τιμωρούνται ξεχωριστά και από άλλα ειδικότερα νομοθετήματα στην Ελλάδα και στην Ευρωπαϊκή Ένωση. Η συγκέντρωση και επεξεργασία ηλεκτρονικών και μη δεδομένων αντιμετωπίστηκε από νωρίς και συνεχίζει να αντιμετωπίζεται ως ένας από τους μεγαλύτερους κινδύνους επέμβασης στην ιδιωτική ζωή.

Η υπάρχουσα νομοθεσία όπως θα παρουσιάσουμε και αναλυτικά στην συνέχεια παρέχει επαρκή προστασία στους πολίτες αλλά με την πάροδο του χρόνου και την περαιτέρω ανάπτυξη της τεχνολογίας χρειάζονται

ειδικότερες διατάξεις που θα αντικαταστήσουν τις γενικές και από τις οποίες θα προκύπτει με σαφήνεια ποιος, πότε ακριβώς, σε ποια δεδομένα και με ποιο σκοπό θα έχει δικαίωμα πρόσβασης και επεξεργασίας.
Στην προσπάθεια του Ελληνικού κράτους για εξασφάλιση υψηλού βαθμού εμπιστευτικότητας των πολιτών στις νέες τεχνολογίες επικοινωνιών είτε μέσω υπολογιστών είτε μέσω άλλων τηλεπικοινωνιακών μέσων, έχουν ιδρυθεί δύο αρχές προστασίας που σχετίζονται με τα προσωπικά δεδομένα, η Αρχή Προστασίας Προσωπικών Δεδομένων και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών τις οποίες θα αναλύσουμε στην συνέχεια.

2.2 Ορισμός τηλεπικοινωνιών και δικτύων

Δίκτυο στον τομέα των επικοινωνιών είναι ένα σύστημα που συνδέει κυρίως τερματικές συσκευές κάθε είδους, είτε αυτές είναι απλές (<κουτά> τερματικά) είτε πρόκειται για κανονικούς υπολογιστές, ενώ διαθέτει δομή τέτοια ώστε να επιτυγχάνεται η όποια μεταξύ τους επικοινωνία. Ένα δίκτυο αποτελείται επίσης από κόμβους, συσκευές τηλεπικοινωνιών και μέσα σύνδεσης διέλευσης πληροφοριών. Κύριος σκοπός του είναι να αποκτήσουν οι χρήστες του κοινή χρήση στους υπάρχοντες πόρους, δηλαδή πρόσβαση σε συσκευές υλικού, λογισμικό και δεδομένα.

2.3 Η Ασφάλεια έχει το Κόστος της

Οι διαχειριστές συχνά δεν υλοποιούν χαρακτηριστικά ασφαλείας μέσα σε λειτουργικά συστήματα, επειδή αν το κάνουν αυτό δημιουργούν προβλήματα στους χρήστες. Από την άλλη πλευρά οι χρήστες συχνά παρακάμπτουν την ασφάλεια αφού επιλέγουν εύχρηστους κωδικούς πρόσβασης χωρίς να τους αλλάζουν στη συνέχεια και χωρίς να διστάζουν να τους αποκαλύπτουν σε συνεργάτες και άλλους χρήστες. Οι προμηθευτές παραδίδουν το λογισμικό τους, έτσι ώστε να μπορεί να εγκατασταθεί με τα περισσότερα χαρακτηριστικά του και με ανενεργά τα χαρακτηριστικά ασφαλείας του. Με αυτόν τον τρόπο οι άπειροι χρήστες δεν χρειάζεται να κατανοούν και να διαμορφώνουν το λογισμικό σωστά πριν να το χρησιμοποιήσουν με αποτέλεσμα τις περισσότερες φορές οι εγκαταστάσεις των υπολογιστών να μην είναι σωστά ασφαλισμένες.

2.4 Τι είναι Εισβολή

Εισβολή είναι η προσπάθεια προσπέλασης ενός συστήματος υπολογιστή, χωρίς εξουσιοδότηση. Αρχικά ο όρος εισβολέας αναφερόταν απλώς σε ένα πεπειραμένο χρήστη υπολογιστών. Όταν η εισβολή σε συστήματα υπολογιστών έγινε δημοφιλής, τα μέσα χρησιμοποιούσαν τον όρο εισβολέας για να αναφέρονται μόνο σε εγκληματίες των υπολογιστών και έτσι ο όρος έλαβε αρνητική έννοια.Αρχικά πρέπει να τονίσουμε ιδιαίτερα ότι η εισβολή είναι παράνομη. Από τεχνικής σκοπιάς, ο νόμος απαιτεί ο δράστης να κάνει κάτι, και όχι απλώς να προσπελάσει και να διαβάσει τα δεδομένα, αλλά όμως, αν απλώς προσπελάσει ένα σύστημα ο ιδιοκτήτης

του συστήματος δεν είναι σε θέση να γνωρίζει την ενέργεια αυτή. Ο νόμος δηλώνει σαφώς ότι ο δράστης πρέπει να κάνει σκόπιμα το αδίκημα και έτσι απαιτεί να έχει δημοσιευθεί κάποιο είδος ειδοποίησης ότι μη εξουσιοδοτημένη προσπέλαση είναι παράνομη ή να καθοριστεί κάποιο εμπόδιο προσπέλασης, ώστε να θεωρηθεί αυτή η ενέργεια αδίκημα.

2.4.1 Τύποι Εισβολέων

Απαιτείται πολύς χρόνος για κάποιον που δεν γνωρίζει τόσο για να μάθει όσο και για να καταφέρει να πραγματοποιήσει μια εισβολή σε ένα ξένο σύστημα υπολογιστή. Εξαιτίας αυτού του γεγονότος υπάρχουν δύο τύποι σοβαρών εισβολέων, οι υποαπασχολούμενοι και αυτοί που πληρώνονται προκειμένου να πραγματοποιούν εισβολές. Οι εισβολείς ανήκουν στις παρακάτω κατηγορίες, με σειρά αυξανόμενης απειλής:

- Ειδικοί Ασφαλείας
- Έφηβοι Εισβολείς
- Υποαπασχολούμενοι Ενήλικες
- Εισβολείς από Ιδεολογία
- Εγκληματίες Εισβολείς
- Εταιρικοί Κατάσκοποι
- Δυσαρεστημένοι Υπάλληλοι

Ειδικοί Ασφαλείας: είναι σε θέση να κάνουν εισβολές αλλά δεν το κάνουν για ηθικούς ή για οικονομικούς λόγους. Γνωρίζουν ότι μπορούν να κερδίσουν περισσότερα χρήματα αν αποτρέπουν τις εισβολές παρά να τις προκαλούν, οπότε ξοδεύουν το χρόνο τους παρακολουθώντας τις κοινότητες των εισβολέων και τις τρέχουσες τεχνικές προκειμένου να γίνουν περισσότερο αποτελεσματικοί στη μάχη κατά των εισβολέων. Είναι πολλές οι εταιρίες που δραστηριοποιούνται στον κυβερνοχώρο που προσλαμβάνουν ηθικούς εισβολείς για να ελέγχουν τα συστήματα ασφαλείας τους και των μεγάλων πελατών τους. Αυτοί οι ειδικοί συχνά είναι οι πρώτοι που βρίσκουν νέες μεθόδους εισβολής και συχνά γράφουν λογισμικό για να ελέγχουν ή για να προκαλούν μια κατάσταση.

Έφηβοι Εισβολείς: είναι συνήθως σπουδαστές που κάνουν εισβολές, ενώ βρίσκονται σε κάποια βαθμίδα της. Αυτοί οι εισβολείς μπορούν να χρησιμοποιούν το δικό τους υπολογιστή ή να χρησιμοποιούν τους ισχυρούς πόρους της σχολής τους για να κάνουν τις εισβολές τους.Οι έφηβοι εισβολείς κάνουν βόλτες στον κυβερνοχώρο ψάχνοντας για στόχους και ενδιαφέρονται κυρίως για να εντυπωσιάσουν τους φίλους τους και να μην συλληφθούν. Συνήθως δεν βλάπτουν τους στόχους τους ενώ τις περισσότερες φορές η δράση τους δεν γίνεται καν αντιληπτή, εκτός και αν το σύστημα στο οποίο εισβάλουν ανιχνεύσει ασυνήθιστη δραστηριότητα και ειδοποιήσει τον ιδιοκτήτη ή αν ένα firewall καταγράψει την επίθεση ή εκτός και αν κάνουν κάποιο λάθος.Καμία σοβαρή προσπάθεια ασφάλειας δεν θα τους βγάλει από το παιχνίδι.

Υποαπασχολούμενοι Ενήλικες: είναι είτε πρώην έφηβοι εισβολείς, οι οποίοι είτε εκδιώχθηκαν από τη σχολή τους, είτε δεν κατάφεραν να βρουν μια εργασία πλήρους απασχόλησης. Συνήθως εργασίες που πληρώνουν μόνο για τις βασικές τους ανάγκες ενώ η πρώτη τους αγάπη είναι η εισβολή. Οι ενήλικες εισβολείς δεν είναι εγκληματίες από πρόθεση αφού δεν έχουν σκοπό να κάνουν κακό σε κανέναν. Ωστόσο συχνά δημιουργούν τα σπασίματα που εφαρμόζονται από άλλους εισβολείς για να ξεκλειδώσουν εμπορικό λογισμικό. Αυτή η ομάδα των εισβολέων γράφει τους περισσότερους ιούς λογισμικού και αποτελεί την περιβόητη συμμορία των εισβολέων. Κάνουν τις εισβολές τους για αποκτήσουν φήμη στην κοινότητα των εισβολέων, θέλουν να εντυπωσιάσουν τους όμοιούς τους, να πάρουν πληροφορίες και να κάνουν γνωστή την αντίδρασή τους στην κυβέρνηση και τις επιχειρήσεις. Η ομάδα αυτή αποτελεί το ένα δέκατο της κοινότητας των εισβολέων, αλλά είναι η πηγή του λογισμικού που γράφεται ειδικά για εισβολείς. Δεν αποτελούν κίνδυνο για το δίκτυο μιας εταιρίας αν αυτή κατέχει κάποιο είδος πνευματική ιδιοκτησίας που θέλει να προστατέψει, μιας και η πνευματική ιδιοκτησία δεν προστατεύεται αρκετά από το νόμο και η εισβολή δεν αποτελεί αδίκημα σε πολλές χώρες του κόσμου.

Εισβολείς από Ιδεολογία: είναι αυτοί που κάνουν εισβολές για να προωθήσουν κάποιο πολιτικό σκοπό. Από το 2000, η εισβολή από ιδεολογία έχει ξεφύγει από την εμφάνιση μερικών μόνο επεισοδίων και έχει φτάσει σε επίπεδο πλήρους πολέμου πληροφοριών. Σε μια προσπάθεια να διαδηλώσουν τις ιδέες τους, αυτοί οι εισβολείς συνήθως καταστρέφουν ιστοσελίδες ή κάνουν επιθέσεις άρνησης παροχής υπηρεσίας εναντίον των ιδεολογικών τους αντιπάλων. Συνήθως προσπαθούν να επιτύχουν ευρεία κάλυψη των κατορθωμάτων τους από τα μέσα και επειδή προέρχονται κυρίως από άλλες χώρες και έχουν την έμμεση υποστήριξη των κυβερνήσεών τους, δεν μπορούν να απαγγελθούν κατηγορίες εναντίον τους. Αυτό το είδος εισβολής εμφανίζεται κατά κύματα, όταν συμβαίνουν μεγάλα γεγονότα στον πολιτικό στίβο, και πολλές φορές εξαιτίας του ότι αυτού του είδους οι επιθέσεις καταναλώνουν πολύ μεγάλο εύρος ζώνης, προκαλούν χαοτικές καταιγίδες.

Εγκληματίες Εισβολείς: κάνουν εισβολές είτε για εκδίκηση είτε για να διαπράξουν κλοπές, είτε απλώς για να ικανοποιηθούν και να προκαλέσουν καταστροφές. Αυτή η κατηγορία εισβολέων δεν αποτελούν ένα ειδικό επίπεδο ηθικού προβλήματος. Αυτοί οι εισβολείς είναι παρόμοιοι με κάθε άλλο εγκληματία αφού προσπαθούν να κάνουν ζημιά αδιαφορώντας για το ποιος είναι το θύμα. Οι εγκληματίες εισβολείς είναι πολλοί σπάνιοι επειδή η ευφυΐα που απαιτείται για να κάνουν εισβολές συνήθως τους δίνει την ευκαιρία να βρουν κάποιο περισσότερο αποδεκτό κοινωνικά τρόπο ζωής.

Εταιρικοί Κατάσκοποι*:* Οι πραγματικοί εταιρικοί κατάσκοποι είναι πολύ σπάνιοι επειδή είναι πολύ ακριβό και πολύ επικίνδυνο να χρησιμοποιηθούν παράνομες τεχνικές εισβολής εναντίον ανταγωνιστικών εταιριών. Αυτές οι τεχνικές χρησιμοποιούνται εναντίον εταιριών υψηλής τεχνολογίας από ξένες κυβερνήσεις. Πολλές εταιρίες υψηλής τεχνολογίας είναι νέες και άπειρες στο θέμα ασφάλειας και έτσι μπορούν εύκολα να επιλεγούν από τους πεπειραμένους πράκτορες ξένων κυβερνήσεων. Αυτές οι υπηρεσίες έχουν ήδη τα χρήματα για να κάνουν κατασκοπία και επιτίθενται σε μερικές επιχειρήσεις μεσαίου μεγέθους για να υποκλέψουν τεχνολογία, η οποία θα δώσει στις εθνικές τους εταιρίες ένα ανταγωνιστικό πλεονέκτημα.

Δυσαρεστημένοι Υπάλληλοι: είναι οι πιο επικίνδυνοι και οι πιθανότεροι να δημιουργήσουν προβλήματα από όλους τους εισβολείς. Ένας υπάλληλος που θεωρεί ότι δεν του έχει φερθεί καλά η εταιρία έχει και τον τρόπο και τα κίνητρα να προκαλέσει σοβαρές καταστροφές στο δίκτυο της εταιρίας. Εξαιτίας των παραπάνω είναι αποδοτικό να γίνεται γνωστό σε όλους τους υπαλλήλους της εταιρίας ότι το τμήμα Πληροφορικής καταγράφει όλες τις δραστηριότητες των χρηστών για λόγους ασφαλείας. Αυτό αποτρέπει μέρος των προβλημάτων αφού οι υπάλληλοι γνωρίζουν ότι θα είναι γνωστές όλες οι ενέργειες που κάνουν στα συστήματα του δικτύου υπολογιστών της εταιρίας.

2.5 Κακόβουλα Προγράμματα

Κακόβουλα προγράμματα (malicious codes) χαρακτηρίζονται τα προγράμματα εκείνα που εκτελούν καταστροφικές ενέργειες σε υπολογιστικά συστήματα. Πρόκειται για προγράμματα που μπορούν να προκαλέσουν ανεπιθύμητα αποτελέσματα, όπως εμφάνιση μηνυμάτων, διαγραφή αρχείων, ακόμη και φορμάρισμα δίσκων. Τα κακόβουλα προγράμματα μπορεί να παραμένουν σε αδράνεια στη μνήμη του υπολογιστή για μεγάλο χρονικό διάστημα. Τα αποτελέσματά τους γίνονται αντιληπτά όταν ενεργοποιούνται μετά από κάποιο συμβάν ή σε μια συγκεκριμένη ημερομηνία. Αυτό όμως που κάνει τα κακόβουλα προγράμματα ιδιαίτερα επικίνδυνα είναι η δυνατότητά τους να αντιγράφονται και να εξαπλώνονται από υπολογιστή σε υπολογιστή.

Οι **βασικοί τύποι κακόβουλων προγραμμάτων** περιγράφονται στη συνέχεια και είναι:

- Ιοί Υπολογιστών (Computer Viruses)
- Δούρειοι Ίπποι (Trojan Horses)
- Σκουλήκια (Worms)

Άλλοι τύποι κακόβουλων προγραμμάτων που βρέθηκαν στην βιβλιογραφία είναι:

- **Λογικές Βόμβες (Logic Bombs):** κακόβουλα προγράμματα που «εκρήγνυνται» όταν ικανοποιηθεί μια λογική συνθήκη.
- **Χρονικές Βόμβες (Time Bombs):** κακόβουλα προγράμματα που ενεργοποιούνται όταν έρθει η κατάλληλη χρονική στιγμή ή μέρα.
- **Πίσω πόρτες (Trapdoors/Backdoors):** κρυμμένες λειτουργίες προγραμμάτων με τις οποίες παρέχεται η προσπέλαση σε ευαίσθητα δεδομένα.
- **Κουνέλια (Rabbits):** προγράμματα που αυτο-αντιγράφονται απεριόριστα με σκοπό την υπερβολική κατανάλωση υπολογιστικών πόρων.

2.6 Ιοί

Ιοί Υπολογιστών (Computer Viruses) ονομάζονται τα μέρη κώδικα που είναι προσαρτημένα σε ένα κανονικό (ωφέλιμο) πρόγραμμα και αντιγράφονται από μόνα τους (self-replicating). Μπορεί να μην κάνουν τίποτε, να μην προκαλούν ζημιές (π.χ. να παίζουν κάποιο τόνο μουσικής) ή να είναι καταστροφικά (π.χ. να μεταβάλλουν και να σβήνουν αρχεία). Υπάρχουν διάφοροι τύποι ιών:

- ***Ιοί Εκκίνησης*** **(Bootstrap Viruses):** κώδικας που εισάγεται στην διαδικασία εκκίνησης ενός υπολογιστή.
- ***Παρασιτικοί Ιοί*** **(Parasitic Viruses):** μέρη κώδικα που προσαρτώνται σε εκτελέσιμα προγράμματα (αρχεία .COM ή .EXE).
- ***Συνοδευτικοί Ιοί*** **(Companion Viruses):** εναλλακτικά εκτελέσιμα προγράμματα που εισάγονται στην διαδρομή αναζήτησης κανονικών προγραμμάτων.
- ***Ιοί Μακροεντολών*** **(Macro Viruses):** τμήματα κώδικα που εισάγονται σε αρχεία δεδομένων τα οποία επεξεργάζεται μια εφαρμογή που υποστηρίζει μακροεντολές.

Όσον αφορά τον τρόπο ενεργοποίησής τους, οι ιοί αντιγράφονται από μόνοι τους με δυο βασικούς τρόπους. Όταν εκτελείται ένα μολυσμένο πρόγραμμα:

- είτε μολύνει άμεσα άλλα μέρη του υπολογιστή (transient), π.χ. άλλες τοποθεσίες στο δίσκο ή άλλα προγράμματα
- είτε εγκαθίσταται μόνιμα στη μνήμη (memory resident) από μόνο του και κατόπιν μολύνει άλλα προγράμματα που εκτελούνται ή μέσα αποθήκευσης που εισάγονται για χρήση (π.χ. δισκέτες).

2.6.1 Ιοί Εκκίνησης

Στην διαδικασία εκκίνησης υπάρχουν πολλά πιθανά σημεία για επιθέσεις. Οι ιοί εκκίνησης (bootstrap viruses) παραμένουν στους τομείς εκκίνησης, ώστε η εκτέλεσή τους να προηγείται της εκτέλεσης του DOS. Με αυτόν τον τρόπο μπορούν να χρησιμοποιήσουν τις λειτουργίες του BIOS. Μπορούν έτσι να μολύνουν άμεσα τους τομείς εκκίνησης των άλλων δίσκων της μηχανής και αφού εγκατασταθούν μόνιμα στη μνήμη (memory resident) να μολύνουν τους τομείς εκκίνησης των δίσκων όποτε τους δίνεται η δυνατότητα να το κάνουν. Οι ιοί εκκίνησης εισχωρούν σε συστήματα μέσω μολυσμένων μέσων αποθήκευσης, όπως οι δισκέτες. Η μόλυνση θα συμβεί όταν ο ιδιοκτήτης του συστήματος ξεκινήσει την λειτουργία του συστήματος από μια μολυσμένη δισκέτα. Συχνά συμβαίνει αυτό ενώ ο ιδιοκτήτης του υπολογιστή δεν προτίθεται να ξεκινήσει τη λειτουργία του από μια δισκέτα, για παράδειγμα όταν η δισκέτα βρίσκεται κατά λάθος μέσα στον οδηγό καθώς το σύστημα σταματάει τη λειτουργία του. Αυτό συμβαίνει ιδίως μετά από μια διακοπή ρεύματος οπότε ακολουθεί μια αυτόματη επανεκκίνηση του συστήματος.

2.6.2 Παρασιτικοί Ιοί

Οι παρασιτικοί ιοί (parasitic viruses) προσκολλώνται μόνοι τους σε ένα εκτελέσιμο πρόγραμμα (.EXE ή .COM) και στη συνέχεια μολύνουν τα υπόλοιπα προγράμματα. Σε μια τυπική περίπτωση, προσαρτάται ο ιοικός κώδικας σε ένα κανονικό πρόγραμμα και κατόπιν εισάγεται στην αρχή του προγράμματος μια εντολή μεταφοράς του ελέγχου στο σημείο του ιοικού κώδικα. Στο τέλος του ιοικού κώδικα ο έλεγχος μεταφέρεται και πάλι στο κανονικό πρόγραμμα. Οι παρασιτικοί ιοί αντιγράφονται κατά τη διάρκεια της εκτέλεσης των μολυσμένων προγραμμάτων. Υπάρχουν όμως και πολύπλοκοι ιοί οι οποίοι αυτοδιασπώνται σε μικρότερα κομμάτια που παραμένουν κρυμμένα στην ενδιάμεση περιοχή των μολυσμένων προγραμμάτων.
Όταν εκτελείται ένα μολυσμένο πρόγραμμα, εκτελείται ο ιός και μετά το κανονικό πρόγραμμα οπότε τα αποτελέσματα της εκτέλεσης του ιού δεν γίνονται άμεσα αντιληπτά. Στα λειτουργικά συστήματα χωρίς μέτρα διασφάλισης της ακεραιότητας, οι ιοί μπορούν να κάνουν οτιδήποτε. Σε λειτουργικά συστήματα που παρέχουν τέτοια μέτρα, οι μολύνσεις μπορούν να περιορισθούν σε αρχεία που ανήκουν στον χρήστη που εκτελεί το μολυσμένο πρόγραμμα.

2.6.3 Συμπληρωματικοί Ιοί

Σε λειτουργικά συστήματα όπου παρέχεται η δυνατότητα εισαγωγής εντολών γραμμής, όπως για παράδειγμα το DOS, συχνά οι χρήστες εκτελούν τα προγράμματα δίνοντας μόνο το όνομα των σχετικών αρχείων χωρίς να προσδιορίζουν τις επεκτάσεις τους, οπότε το σύστημα ψάχνει να βρει αρχεία με το ίδιο όνομα και επέκταση.COM ή .EXE ή .BAT. Το σύστημα πρώτα ψάχνει στον τρέχοντα κατάλογο και μετά στους καταλόγους που αναφέρονται στη μεταβλητή συστήματος path.Οι Συμπληρωματικοί Ιοί (companion viruses) εκμεταλλεύονται αυτήν την συμπεριφορά του χρήστη και του λειτουργικού συστήματος. Έτσι, για ένα υπάρχον πρόγραμμα με επέκταση .EXE δημιουργούν ένα αρχείο .COM με το ίδιο όνομα το οποίο περιέχει τον ιοικό κώδικα. Τελικά, το αρχείο .COM είναι αυτό που εκτελείται κάθε φορά που ο χρήστης δίνει μόνο το όνομα του αρχείου με σκοπό να εκτελεστεί το κανονικό πρόγραμμα.
Ο ίδιος τύπος επίθεσης μπορεί να συμβεί και σε άλλα λειτουργικά συστήματα, όπως για παράδειγμα το Unix,εγκαθιστώντας ένα μολυσμένο αρχείο το οποίο έχει το ίδιο όνομα με ένα κανονικό σε έναν κατάλογο που ψάχνεται πριν από αυτόν που περιέχει το κανονικό πρόγραμμα.

2.6.4 Ιοί Μακροεντολών

Ο τελευταίος τύπος ιών που εξετάζουμε είναι οι Ιοί των Μακροεντολών (Macro viruses). Οι ιοί αυτού του είδους παραμένουν μέσα σε αρχεία δεδομένων που δημιουργούνται από τη σχετική εφαρμογή. Επομένως, μπορεί κανείς να τους βρει συχνά σε αρχεία επεξεργασίας κειμένου και σε αυτή τη περίπτωση είναι γραμμένοι στην γλώσσα μακροεντολών του συγκεκριμένου επεξεργαστή κειμένου.

Οι ιοί μακροεντολών είναι πολύ επικίνδυνοι καθώς ξεπερνούν τα μέτρα ελέγχου διανομής και χρήσης των εκτελέσιμων προγραμμάτων που έχουν σχεδιασθεί ώστε να αντιπαλέψουν τους παρασιτικούς ιούς. Επιπλέον, μπορεί να μην εξαρτώνται από επιμέρους πλατφόρμες. Αλλά το πιο ανησυχητικό είναι ότι τα αρχεία κειμένου ανταλλάσσονται ευρέως μεταξύ των χρηστών για νόμιμους σκοπούς, κάτι που δεν ισχύει για ανταλλαγές εκτελέσιμων αρχείων. Για αυτό οι ιοί μακροεντολών αποτελούν έναν πολύ σοβαρότερο κίνδυνο από τους άλλους τύπους ιών.Η δυνατότητα δημιουργίας ιών μακροεντολών ήταν γνωστή από τη δεκαετία του 1980. Εντούτοις, πραγματικές περιπτώσεις τέτοιων ιών δεν έγιναν αντιληπτές μέχρι τη δεκαετία του 1990. Το πρώτο γνωστό παράδειγμα ιού μακροεντολών είναι γνωστό ως *Concept virus*, ο οποίος ήταν για το Microsoft Word, αλλά μετά ακολούθησαν ιοί και για άλλες εφαρμογές, όπως για παράδειγμα το Excel. Ο ιός Concept μολύνει το αρχείο NORMAL.DOT file,που είναι το πρότυπο (template) που χρησιμοποιείται όταν το Microsoft Word δημιουργεί ένα νέο έγγραφο. Αφού φορτωθεί στη μνήμη του υπολογιστή, ο ιός μολύνει όλα τα έγγραφα που δημιουργούνται στη συνέχεια με την μακροεντολή *Concept*. Αν κατά τη διάρκεια μιας συνόδου του Word γίνει η έκδοση (edit) ενός μολυσμένου αρχείου, το αποτέλεσμα είναι ότι ο ιός φορτώνεται για τη συγκεκριμένη σύνοδο (session) του Word και όταν αυτή τερματίζεται μολύνεται το αρχείο NORMAL.DOT. Ενώ είναι δυνατόν να απομακρυνθεί ο ιός από το αρχείο NORMAL.DOT (απλά σβήνοντας το αρχείο αυτό),είναι πολύ δύσκολο να καθαριστούν τα μολυσμένα αρχεία, καθώς η μόλυνση μπορεί να επαναληφθεί πολύ εύκολα.

Από την έκδοση (version) Word 97 και μετά, παρέχεται η δυνατότητα απενεργοποίησης των μακροεντολών με την οποία εμποδίζονται οι μολύνσεις με την εμφάνιση ενός προειδοποιητικού μηνύματος όποτε φορτώνεται ένα έγγραφο που περιέχει μακροεντολές.

2.6.5 Υπογραφές των Ιών

Το ευτύχημα είναι ότι οι ιοί που εισχωρούν σε ένα σύστημα δεν μπορούν να παραμείνουν ολότελα αόρατοι αφού ο ιοικός κώδικας πρέπει να αποθηκευτεί κάπου. Αυτό σημαίνει ότι ο ιοί μπορούν να ανιχνεύονται με αναζήτηση των χαρακτηριστικών ακολουθιών πληροφοριών που ονομάζονται υπογραφές (signatures). Παρόλα αυτά οι ιοί μπορούν να κρύβονται είτε τεμαχίζοντας τον κώδικά τους είτε αποθηκευόμενοι σε κρυπτογραφημένη μορφή, όπως οι πολυμορφικοί ιοί (polymorphic viruses), χρησιμοποιώντας ένα μεταβλητό κρυπτογραφικό κλειδί το οποίο επίσης αποθηκεύεται μαζί με τον κρυπτογραφημένο ιοικό κώδικα. Το μέρος όμως του ιοικού κώδικα που είναι υπεύθυνο για την διαδικασία αποκρυπτογράφησης πρέπει να παραμένει χωρίς κρυπτογράφηση, αφήνοντας έτσι μια, έστω μικρή, υπογραφή που είναι ικανή για τον εντοπισμό των πολυμορφικών ιών.

2.7 Σκουλήκια

Τα σκουλήκια (worms) είναι προγράμματα που εξαπλώνονται μέσω των δικτυωμένων υπολογιστών, αντιγράφοντας τα ίδια ανεξέλεγκτα. Τα σκουλήκια μοιάζουν πολύ με τους ιούς στο ότι αντιγράφονται από μόνα τους και επιτίθενται σε συστήματα με σκοπό να επιφέρουν βλάβες. Πρόκειται για αυτόνομα προγράμματα τα οποία μολύνουν υπολογιστικά συστήματα μόνο μέσω δικτυακών συνδέσεων. Για τη δημιουργία τους απαιτούνται ιδιαίτερες γνώσεις πρωτοκόλλων επικοινωνιών, ευπαθειών δικτυακών συστημάτων και ειδικών θεμάτων πάνω σε λειτουργικά συστήματα.

Μόλις ένα σκουλήκι μολύνει ένα σύστημα, αναζητεί δραστήρια για πιθανές συνδέσεις με άλλους υπολογιστές, οπότε αν βρει, αμέσως αντιγράφεται σε αυτούς. Όμως, πέρα από την συμπεριφορά αναπαραγωγής τους από σύστημα σε σύστημα, τα σκουλήκια συχνά εκτελούν και κακόβουλες πράξεις, που δεν περιορίζονται μόνο στην καταστροφή αρχείων. Μέσω των δικτυακών συνδέσεων μπορούν να υποκλέψουν και να μεταφέρουν προς τους συγγραφείς τους πληροφορίες που αφορούν συνθηματικά χρηστών και άλλες ευαίσθητες αλλά και πολύτιμες πληροφορίες. Επιπλέον, μπορούν να επιφέρουν πλήρη αποδιοργάνωση των λειτουργιών ενός συστήματος ώστε να προκαλείται επίθεση άρνησης εξυπηρέτησης (denial of service). Αυτό συνήθως προκαλείται από παράλληλες και ανοργάνωτες επιθέσεις περισσότερων του ενός σκουληκιών στο ίδιο σύστημα. Ακριβώς επειδή η μόλυνση από σκουλήκια επιτυγχάνεται μέσω δικτυακών συνδέσεων, είναι δύσκολος ο εντοπισμός των σημείων προσβολής. Για την αποφυγή της μόλυνσης από σκουλήκια επιβάλλεται ο εντοπισμός και η αντιμετώπιση όλων των ευπαθών σημείων του υπολογιστικού συστήματος από τους διαχειριστές του. Αυτό σημαίνει ότι ιδιαίτερα πρέπει να προσεχθούν τα αδύνατα σημεία όπως εύκολα συνθηματικά ή ανεξέλεγκτες δικτυακές υπηρεσίες που μπορούν να εκμεταλλευθούν τα σκουλήκια για να εισβάλλουν στο σύστημα από το δίκτυο και να το μολύνουν.

Ένας καλός τρόπος προφύλαξης από τα σκουλήκια είναι η γνώση των μεθόδων που χρησιμοποιούν για τον εντοπισμό και την αξιοποίηση των ευπαθών σημείων του συστήματος. Όπως γίνεται γενικότερα για την πρόληψη εισβολών (intrusion prevention), η χρήση διατάξεων firewalls και ελέγχου προσπέλασης μπορούν να μειώσουν σημαντικά τους κινδύνους επίτευξης των στόχων των σκουληκιών.

2.8 Δούρειοι Ίπποι

Οι Δούρειοι Ίπποι (Trojan Horses) είναι προγράμματα με κρυφές λειτουργίες που δεν περιλαμβάνονται στην τεκμηρίωση που τα συνοδεύει. Τα προγράμματα αυτά ονομάσθηκαν έτσι γιατί λειτουργούν όπως το μυθικό άλογο του Τρωικού Πολέμου. Δηλαδή, ενώ επικαλούνται ότι επιτελούν κάποια εργασία, στην πραγματικότητα εκτελούν και/ή μια διαφορετική λειτουργία. Αυτή η λανθάνουσα δραστηριότητα είναι που συνήθως εκτελεί καλυμμένες ενέργειες, όπως η κλοπή των συνθηματικών των χρηστών.

Υπάρχουν Δούρειοι Ίπποι που η εργασία που υποτίθεται ότι προσφέρουν δεν υπάρχει καν. Έτσι, όταν εκτελούνται απλά προχωρούν στην απροκάλυπτη καταστροφή αρχείων και πόρων του συστήματος. Από την

άλλη, υπάρχουν Δούρειοι Ίπποι που λειτουργούν με συγκαλυμμένο τρόπο, έτσι ώστε να επιτελούν την εργασία που επικαλούνται χωρίς να προκαλούν υποψίες. Ως Δούρειοι Ίπποι μπορούν να θεωρηθούν και όσα από τα γνωστά προγράμματα του εμπορίου διαθέτουν λειτουργίες οι οποίες δεν αναφέρονται πουθενά στα εγχειρίδια χρήσης τους, αλλά συνήθως αποκαλύπτονται τυχαία. Είναι προφανές ότι οι Δούρειοι Ίπποι αποτελούν την πλέον επικίνδυνη κατηγορία κακόβουλων προγραμμάτων, καθώς φανερά επικαλούνται μια δεδομένη λειτουργικότητα ενώ στην πραγματικότητα λειτουργούν λίγο ή πολύ διαφορετικά και μάλιστα χωρίς αυτό να φαίνεται. Έτσι, δεν χρειάζεται να αντιγράφουν τους εαυτούς τους ούτε να αναπαράγονται όπως οι ιοί και τα σκουλήκια. Είναι οι ίδιοι οι χρήστες που βοηθούν τους Δούρειους Ίππους να μολύνουν τα διάφορα υπολογιστικά συστήματα.

Κύριες πηγές Δούρειων Ίππων είναι οι διάφοροι εξυπηρετητές πληροφόρησης (bulletin board servers) και διανομής αρχείων (FTP servers). Σε αυτούς τους τόπους κανείς μπορεί να βρει πληθώρα ελεύθερων (freeware,shareware,demos) και πολλές φορές πειρατικών αντιγράφων προγραμμάτων τα οποία διατίθενται για 'κατέβασμα'(download) με μικρή ή καθόλου εγγύηση. Φυσικά με κίνητρο την δωρεάν απόκτηση «χρήσιμου» λογισμικού, οι χρήστες αναλαμβάνουν το ρίσκο να γίνουν οι ίδιοι βοηθοί των συγγραφέων των Δούρειων Ίππων, εγκαθιστώντας τους στους υπολογιστές τους. Οι πιο χρήσιμοι Δούρειοι ίπποι ονομάζονται πίσω πόρτες. Αυτά τα προγράμματα παρέχουν ένα μηχανισμό με βάση τον οποίο ο εισβολέας μπορεί να ελέγξει απευθείας τον υπολογιστή. Παραδείγματα περιλαμβάνουν κακόβουλα σχεδιασμένα προγράμματα όπως τα NetBus, Back Orifice και BO2K, καθώς και καλοκάγαθα προγράμματα, τα οποία μπορεί να εκμεταλλευθεί κάποιος για να πάρει τον έλεγχο ενός συστήματος, όπως τα netcat, VNC και pcAnywhere. Τα ιδανικά προγράμματα πίσω πόρτας είναι μικρά και γρήγορα εγκαθιστάμενα προγράμματα, τα οποία εκτελούνται διαρκώς. Οι Δούρειοι ίπποι συνήθως μεταφέρονται μέσω ιών που παράγονται από e-mail ή στέλνονται ως συνημμένα σε e-mail.

Η καλύτερη μέθοδος πρόληψης κατά των Δούρειων Ίππων είναι η ενημέρωση των χρηστών. Σε κάθε περίπτωση όμως είναι δύσκολη αλλά όχι αδύνατη η ανίχνευση των Δούρειων Ίππων πριν να εισχωρήσουν σε ένα υπολογιστικό σύστημα. Για αυτό επιβάλλεται η καθιέρωση και η συνεπής εφαρμογή από τους διάφορους οργανισμούς συγκεκριμένων πολιτικών εγκατάστασης επίσημα αγορασμένου λογισμικού, καθώς και εκπαίδευσης των χρηστών, έτσι ώστε να αποκτήσουν τα απαραίτητα για να συμμερίζονται τους κινδύνους που αναλαμβάνουν όταν δοκιμάζουν προγράμματα άγνωστης προέλευσης.

2.9 Τρόποι Εργασίας των Εισβολέων

Τέσσερις είναι οι τρόποι με τους οποίους ένας εισβολέας μπορεί να προσπελάσει το δίκτυο υπολογιστών μιας επιχείρησης :

- Συνδεόμενος μέσω του Internet,
- Χρησιμοποιώντας έναν υπολογιστή του ίδιου του δικτύου,
- Καλώντας μέσω ενός διακομιστή απομακρυσμένης προσπέλασης (Remote Access Service, RAS) και

- Συνδεόμενος μέσω ενός ανασφαλούς ασύρματου δικτύου.

Αυτός ο αριθμός τρόπων εισόδου ορίζει και τα όρια του προβλήματος της εισβολής.

Απευθείας Εισβολή: Οι εισβολείς σε πολλές περιπτώσεις εργάζονται στις επιχειρήσεις, διαχειρίζονται κάποιο τοπικό τερματικό ή βρίσκονται μπροστά σε ένα πελάτη δικτύου και με αυτό τον τρόπο διαμορφώνουν την κατάσταση για περαιτέρω απομακρυσμένη διείσδυση μέσα σε συστήματα.Η επίλυση του προβλήματος της απευθείας εισβολής είναι εύκολη αφού αρκεί να εφαρμοστεί firewalls, που παρακολουθούν κάθε σύνδεση που βγαίνει από το κτήριο, ανάμεσα στις συνδέσεις WAN και στο εσωτερικό δίκτυο της επιχείρησης ή πίσω από ασύρματες συνδέσεις.

Μέσω Τηλεφωνικής Κλήσης: Η εισβολή μέσω τηλεφωνικής κλήσης, μέσω μόντεμ, ήταν παλιότερα ο μόνος τρόπος εισβολής, αλλά γρήγορα πήρε τη δεύτερη θέση, μετά από την εισβολή μέσω του Internet. Αν και το πρόβλημα της εισβολής μέσω τηλεφωνικής κλήσης σημαίνει συνήθως εκμετάλλευση ενός μόντεμ που είναι συνδεδεμένο σε ένα διακομιστή υπηρεσίας απομακρυσμένης προσπέλασης (RAS), περιλαμβάνει επίσης το πρόβλημα κλήσης προς διακριτούς υπολογιστές. Κάθε μόντεμ που έχει διαμορφωθεί, ώστε να απαντά για να επιτρέπει απομακρυσμένη προσπέλαση ή απομακρυσμένο έλεγχο από τον υπάλληλο που χρησιμοποιεί τον υπολογιστή, αποτελεί ένα πρόβλημα ασφάλειας. **Μία λύση του προβλήματος της εισβολής μέσω τηλεφωνικής κλήσης** είναι η τοποθέτηση των διακομιστών RAS έξω από τα firewalls μέσα στη δημόσια ζώνη ασφάλειας και η υποχρεωτική πιστοποίηση των νόμιμων χρηστών στο firewall προκειμένου να εισέλθουν στους πόρους του δικτύου της επιχείρησης.

Internet: Η εισβολή μέσω του Internet είναι η περισσότερο διαθέσιμη, ευκολότερα εκμεταλλεύσιμη και πλέον προβληματική περιοχή εισβολής σε ένα δίκτυο.

Ξέρετε ήδη ότι το πρόβλημα της εισβολής μέσω του Internet επιλύεται αν χρησιμοποιείτε firewalls, οπότε δεν υπάρχει λόγος να συζητήσουμε περαιτέρω αυτό το θέμα εδώ.

2.10 Τεχνικές Εισβολής

Οι επιθέσεις εισβολής προχωρούν σε μια σειρά φάσεων, χρησιμοποιώντας διάφορα εργαλεία και τεχνικές. Μια σύνοδος εισβολής αποτελείται από τις παρακάτω φάσεις:

- Επιλογή στόχου
- Συλλογή πληροφοριών
- Επίθεση

Ο εισβολέας προσπαθεί να μάθει στοιχεία για το δίκτυο – στόχο, μέσω κάθε διαδοχικής επίθεσης, οπότε αυτές οι φάσεις παρέχουν στοιχεία στον εισβολέα, ώστε αυτός να μπορεί να συλλέξει πληροφορίες από επιθέσεις που απέτυχαν.

2.10.1 Επιλογή Στόχου Η επιλογή στόχου είναι η φάση στην οποία ο εισβολέας προσδιορίζει ένα συγκεκριμένο υπολογιστή για να του επιτεθεί. Για να περάσει από αυτήν την φάση, πρέπει να είναι διαθέσιμος κάποιος τρόπος επίθεσης, οπότε το μηχάνημα πρέπει είτε να έχει διαφημίσει την παρουσία του ή να έχει βρεθεί μέσω αναζήτησης.

2.10.2 Αναζήτηση DNS Οι εισβολείς που ψάχνουν για ένα συγκεκριμένο στόχο χρησιμοποιούν την ίδια μέθοδο που χρησιμοποιούν τα προγράμματα περιήγησης στο Web για να βρουν ένα ξενιστή (host), ψάχνουν δηλαδή το όνομα τομέα χρησιμοποιώντας ένα σύ*στημα Ονομάτων Τομέων* (DNS). Η μη καταχώρηση δημοσίων ονομάτων τομέων για τους ξενιστές μιας επιχείρησης, εκτός των διακομιστών ταχυδρομείου και Web, μπορεί να αποτελέσει μια λύση του προβλήματος. Για το εσωτερικό της δίκτυο η επιχείρηση θα πρέπει να χρησιμοποιεί εσωτερικούς διακομιστές DNS, που δεν είναι διαθέσιμοι στο Internet.

2.10.3 Σάρωση Διευθύνσεων Δικτύου Οι εισβολείς που ψάχνουν για ευκαιριακούς στόχους χρησιμοποιούν μια μέθοδο που καλείται *σάρωση* διευθύνσεων δικτύου για να τους βρουν. Ο εισβολέας θα καθορίσει διευθύνσεις αρχής και τέλους για σάρωση, και μετά το πρόγραμμά του θα στείλει ένα μήνυμα ηχούς ICMP σε καθεμία από αυτές τις διευθύνσεις δικτύου. Αν ένας υπολογιστής από μια από αυτές τις διευθύνσεις απαντήσει, τότε ο εισβολέας έχει βρει έναν ακόμη στόχο. Σαρώσεις διευθύνσεων γίνονται συνεχώς στο Internet. Ένας υπολογιστής συνδεδεμένος στο δημόσιο Internet υπολογίζεται πως η διεύθυνσή του σαρώνεται τουλάχιστον μια φορά κάθε ώρα.

2.10.4 Σάρωση θύρας. Αφού ο εισβολέας επιλέξει έναν υπολογιστή στόχου, θα προσπαθήσει να καθορίσει ποιο λειτουργικό σύστημα εκτελεί και ποιες υπηρεσίες παρέχει στους πελάτες του δικτύου. Σε ένα δίκτυο TCP/IP (όπως το Internet), οι υπηρεσίες παρέχονται σε αριθμημένες συνδέσεις, που καλούνται *θύρες*. Οι θύρες στις οποίες αποκρίνεται ένας υπολογιστής καθορίζουν συνήθως το λειτουργικό σύστημα και τις παρεχόμενες υπηρεσίες του υπολογιστή στόχου. Υπάρχουν αρκετά εργαλεία στο Internet, τα οποία μπορεί να χρησιμοποιήσει ένας εισβολέας για να καθορίσει ποιες θύρες αποκρίνονται σε αιτήσεις συνδέσεων δικτύου. Αυτά τα εργαλεία δοκιμάζουν κάθε θύρα με τη σειρά και αναφέρουν στον εισβολέα ποιες θύρες αρνούνται τις συνδέσεις και ποιες όχι. Ο εισβολέας μπορεί κατόπιν να επικεντρώσει την προσοχή του στις θύρες που αποκρίνονται σε υπηρεσίες, οι οποίες συχνά μένουν ανασφάλιστες ή έχουν προβλήματα ασφάλειας.Η σάρωση θυρών μπορεί να αποκαλύψει ποιο λειτουργικό σύστημα χρησιμοποιεί ο υπολογιστής, επειδή κάθε λειτουργικό σύστημα έχει ένα διαφορετικό σύνολο προεπιλεγμένων υπηρεσιών. Αυτές οι πληροφορίες είναι που «λένε» στον εισβολέα ποια εργαλεία να χρησιμοποιήσει για να εισβάλει σε ένα δίκτυο.

2.10.5 Σάρωση Υπηρεσίας: Η σάρωση υπηρεσίας αποτελεί μία ακόμα μορφή επίθεσης εισβολής. Υπεύθυνα για αυτήν είναι τα γνωστά ως σκουλήκια του Internet. Πρόκειται για αυτοματοποιημένες επιθέσεις εισβολής, που λειτουργούν υλοποιώντας μια επίθεση και μετά ψάχνοντας για υπολογιστές που είναι ευπρόσβλητοι σε

αυτή. Αυτή η αναζήτηση γίνεται με τη μορφή μιας σάρωσης θύρας προς τη συγκεκριμένη θύρα που εξετάζει η επίθεση. Επειδή το σκουλήκι κάνει σάρωση σε μια θύρα, δεν θα εμφανιστεί ούτε ως σάρωση διεύθυνσης (επειδή δεν είναι μια ICMP), ούτε ως σάρωση θύρας (επειδή χτυπά μόνο μια θύρα). Στην πραγματικότητα, δεν υπάρχει τρόπος να καταλάβει κανείς αν μια σάρωση υπηρεσίας είναι μια νόμιμη προσπάθεια σύνδεσης ή μια κακόβουλη σάρωση υπηρεσίας. Τις περισσότερες φορές μια σάρωση υπηρεσίας ακολουθείται είτε από μια ανίχνευση αρχιτεκτονικής, αν το σκουλήκι είναι ευφυές ή απλώς από μια προσπάθεια επίθεσης στην συγκεκριμένη υπηρεσία, όπως είναι μια υπερχείλιση καταχωρητή.

2.11 Συλλογή Πληροφοριών: Η συλλογή πληροφοριών είναι η φάση κατά την οποία ο εισβολέας καθορίζει τα χαρακτηριστικά του στόχου, πριν να του επιτεθεί. Αυτή μπορεί να γίνει είτε μέσω δημόσια διαθέσιμων πληροφοριών, που εκδίδονται για το στόχο ή ερευνώντας το στόχο, χρησιμοποιώντας μη επιθετικές μεθόδους, για να πάρει πληροφορίες από αυτόν.

2.11.1 Συλλογή Δεδομένων SNMP

Το πρωτόκολλο Simple Network Management Protocol (SNMP) είναι ένα βασικό εργαλείο για διαχείριση μεγάλων δικτύων TCP/IP. Το SNMP επιτρέπει στο διαχειριστή να υποβάλει ερωτήματα απομακρυσμένα για την κατάσταση συσκευών δικτύου και να ελέγξει τις λειτουργίες τους. Δυστυχώς, οι εισβολείς μπορούν επίσης να χρησιμοποιήσουν το SNMP για να συλλέξουν δεδομένα για ένα δίκτυο ή να επέμβουν στη λειτουργία του.

Το πρωτόκολλο SNMP έχει σχεδιαστεί έτσι, ώστε να παρέχει αυτόματα τις λεπτομέρειες διαμόρφωσης συσκευών δικτύου. Έτσι, «τρύπιες» συσκευές στην δημόσια πλευρά ενός εταιρικού δικτύου μπορούν να δώσουν πάρα πολλές πληροφορίες για το εσωτερικό του.

2.11.2 Ανίχνευση Αρχιτεκτονικής

Οι εισβολείς είναι σε θέση να προσδιορί*σουν* το λειτουργικό σύστημα που εκτελείται στον υπολογιστή στόχου, με βάση την ακριβή φύση του μηνύματος σφάλματος, επειδή κάθε τύπος λειτουργικού συστήματος αποκρίνεται κάπως διαφορετικά. Οι εισβολείς εξετάζουν τις αποκρίσεις σε λανθασμένες μεταδόσεις πακέτων από έναν ξενιστή στόχου, χρησιμοποιώντας ένα αυτοματοποιημένο εργαλείο, το οποίο περιέχει μια βάση δεδομένων με γνωστούς τύπους αποκρίσεων. Επειδή δεν υπάρχει πρότυπος ορισμός αποκρίσεων, κάθε λειτουργικό σύστημα απαντά με ένα μοναδικό τρόπο. Συγκρίνοντας τις μοναδικές αποκρίσεις με μια βάση δεδομένων γνωστών αποκρίσεων, οι εισβολείς μπορούν να καθορίσουν ποιο λειτουργικό σύστημα εκτελεί ο ξενιστής στόχου.

2.11.3 Αναζητήσεις Υπηρεσιών Καταλόγου

Το **πρωτόκολλο Lightweight Directory Access Protocol (LDAP)** είναι μια ακόμη υπηρεσία από την οποία μπορούν να εξαχθούν πληροφορίες. Παρέχοντας πληροφορίες LDAP στο κοινό, οι εισβολείς αποκτούν πάρα πολλές πληροφορίες, που μπορούν να περιλαμβάνουν πολύτιμες ενδείξεις για τη φύση του δικτύου και για τους χρήστες του. Οι εισβολείς χρησιμοποιούν το LDAP, καθώς και παλιότερες υπηρεσίες καταλόγου, όπως τις Finger και Whois, προκειμένου να συλλέξουν πληροφορίες για τα συστήματα μέσα στο δίκτυό σας και για τους χρήστες τους.

2.11.4 Μύρισμα

Το μύρισμα είναι μια επίθεση συλλογής πληροφοριών, αλλά δεν μπορεί να γίνει χωρίς να έχει κάποιος φυσική πρόσβαση στο δίκτυο ή να έχει ήδη παραβιάσει έναν υπολογιστή μέσα σε ένα δίκτυο. Δεν είναι δυνατό να υποκλέψει κανείς απομακρυσμένα μια σύνδεση, εκτός και αν κάνει μια επίθεση ενδιαμέσου εναντίον του υπολογιστή. Γι" αυτόν το λόγο, τέτοιες επιθέσεις είναι πολύ σπάνιες.

2.12 Επιθέσεις

Οι εισβολείς χρησιμοποιούν διάφορα είδη επιθέσεων εναντίον διαφόρων συστημάτων. Οι περισσότερες από τις επιθέσεις είναι εξειδικευμένες ώστε να εκμεταλλεύονται μια συγκεκριμένη υπηρεσία δικτύου. Παρακάτω αναφέρονται ορισμένα βασικά στοιχεία για τους συνηθέστερους και περισσότερο εφαρμόσιμους τύπους επιθέσεων, με αύξουσα σειρά δυσκολίας διάπραξής τους.

2.12.1 Άρνηση Παροχής Υπηρεσίας

Οι δικτυωμένοι υπολογιστές υλοποιούν ένα συγκεκριμένο πρωτόκολλο για μετάδοση δεδομένων και αναμένουν αυτό το πρωτόκολλο να μεταδώσει πληροφορίες που έχουν κάποια σημασία. Όταν το πρωτόκολλο υλοποιείται λανθασμένα και δεν γίνεται αρκετός έλεγχος σφαλμάτων για ανίχνευση του σφάλματος, είναι πιθανό να συμβεί μια επίθεση άρνησης παροχής υπηρεσίας. Σε ορισμένες περιπτώσεις, ο υπολογιστής που υφίσταται την επίθεση θα καταρρεύσει ή θα κρεμάσει. Σε άλλες περιπτώσεις, η υπηρεσία που υφίσταται την επίθεση θα αποτύχει χωρίς να προκαλέσει κατάρρευση του υπολογιστή.Η πιο δυσοίωνη ίσως επίθεση επιπέδου δικτύου είναι αυτή που ονομάστηκε σφύριγμα του θανάτου (Ping of Death). Ένα ειδικά κατασκευασμένο πακέτο ICMP, που παραβιάζει τους κανόνες κατασκευής πακέτων ICMP μπορεί να κάνει τον παραλήπτη υπολογιστή να καταρρεύσει, αν το λογισμικό του υπολογιστή δεν ελέγξει για την ύπαρξη μη έγκυρων πακέτων ICMP. Τα περισσότερα λειτουργικά συστήματα κάνουν αυτό τον έλεγχο, οπότε αυτή η συγκεκριμένη επίθεση δεν είναι πλέον δυνατό να χρησιμοποιηθεί. Υπάρχουν όμως πολλές άλλες επιθέσεις

άρνησης παροχής υπηρεσίας και συνεχώς ανακαλύπτονται καινούργιες.Όσο πιο περίπλοκη είναι μια υπηρεσία, τόσο πιθανότερο είναι να υποστεί μια επίθεση άρνησης παροχής υπηρεσίας. Οι επιθέσεις άρνησης παροχής υπηρεσίας είναι οι ευκολότερες και οι λιγότερο χρήσιμες μορφές επιθέσεων, και ως τέτοιες, οι εισβολείς αποφεύγουν τη χρήση τους.

2.12.2 Πλημμύρες

Οι *πλημμύρες* είναι απλές επιθέσεις άρνησης παροχής υπηρεσιών, που εργάζονται χρησιμοποιώντας σπάνιους πόρους, όπως είναι το εύρος ζώνης δικτύου ή την υπολογιστική ισχύ ενός υπολογιστή.

2.12.3 Πλαστογραφημένο E-mail

Οι εισβολείς μπορούν να δημιουργήσουν e-mail που φαίνεται να προέρχεται από οποιονδήποτε θέλουν. Σε μια παραλλαγή αυτής της επίθεσης, μπορούν να αλλάξουν και την απάντηση στον αποστολέα, κάνοντας την πλαστογράφηση μη ανιχνεύσιμη. Χρησιμοποιώντας μια τεχνική τόσο απλή, όσο η διαμόρφωση ενός πελάτη e-mail με λανθασμένες πληροφορίες, οι εισβολείς μπορούν να πλαστογραφήσουν μια διεύθυνση e-mail, ως τη διεύθυνση ενός εσωτερικού πελάτη. Ισχυριζόμενοι ότι είναι κάποιος τον οποίο ο πελάτης γνωρίζει και εμπιστεύεται, αυτό το e-mail είναι μια μορφή ψυχολογικής επίθεσης, που παρακινεί τον αναγνώστη να επιστρέψει χρήσιμες πληροφορίες, που περιλαμβάνουν έναν εγκαταστάσιμο Δούρειο Ίππο ή μια σύνδεση προς μια κακόβουλη ιστοθέση. Αυτός είναι ο ευκολότερος τρόπος για να προσπελάσετε ένα συγκεκριμένο δίκτυο στόχου. Το Internet e-mail δεν επαληθεύει την ταυτότητα του αποστολέα και πολλές εκδόσεις προγραμμάτων e-mail δεν καταγράφουν αρκετές πληροφορίες ώστενα παρακολουθούν σωστά την πηγή ενός μηνύματος e-mail. Υπογράφοντας απλώς ένα λογαριασμό e-mail με μια λανθασμένη ταυτότητα, ένας εισβολέας μπορεί να κρύψει την ταυτότητά του, ακόμη και αν το e-mail μπορεί να ανιχνευθεί μέχρι την πηγή του. Η μόνη εφικτή άμυνα από ένα πλαστογραφημένο e-mail μιας και δεν είναι εφικτό να χρησιμοποιεί όλος ο κόσμος κρυπτογράφηση δημόσιου κλειδιού για όλα τα e-mail του είναι η ενημέρωση του χρήστη. Οι περισσότεροι δημοφιλείς πελάτες e-mail επιτρέπουν την εγκατάσταση προσωπικών κλειδιών κρυπτογράφησης για πιστοποίηση, με τα οποία οι χρήστες υπογράφουν τα e-mail τους προς εσωτερικούς χρήστες.

2.12.4 Αυτοματοποιημένη Εύρεση Κωδικών Πρόσβασης: Αφού ένας εισβολέας αναγνωρίσει έναν ξενιστή και βρει ένα λογαριασμό χρήστη που μπορεί να χρησιμοποιήσει ή υπηρεσίες όπως τις Telnet και Network File System (NFS), μια εύρεση κωδικού πρόσβασης θα του δώσει τον έλεγχο ενός υπολογιστή. Οι περισσότερες υπηρεσίες προστατεύονται με ένα συνδυασμό ονόματος λογαριασμού και κωδικού πρόσβασης, σαν τελευταία γραμμή της άμυνάς τους. Όταν ένας εισβολέας ανακαλύψει μια υπηρεσία την οποία μπορεί να παραβιάσει σε ένα υπολογιστή στόχου, πρέπει να δώσει ένα έγκυρο όνομα-χρήστη και κωδικό πρόσβασης για να συνδεθεί με αυτήν.Η αυτοματοποιημένη εύρεση κωδικού πρόσβασης χρησιμοποιεί λίστες συνηθισμένων κωδικών

πρόσβασης, ονόματα και λέξεις από το λεξικό για να προσπαθήσει να μαντέψει σημαντικά ονόματα λογαριασμών, όπως είναι ο κωδικός πρόσβασης του χρήστη root σε συστήματα Unix ή του χρήστη administrator σε συστήματα NT. Το λογισμικό συνήθως παίρνει μια λίστα ονομάτων λογαριασμών και μια λίστα πιθανών κωδικών πρόσβασης και απλώς δοκιμάζει κάθε όνομα λογαριασμού με κάθε κωδικό πρόσβασης.Οι εισβολείς χρησιμοποιούν νέες λίστες «συνηθισμένων κωδικών πρόσβασης» για να κάνουν αυτές τις επιθέσεις ταχύτερες. Αυτές οι λίστες παράγονται από την στατιστική ανάλυση πληροφοριών λογαριασμών που έχουν κλαπεί από παραβιασμένους διακομιστές. Συνδυάζοντας λίστες κλεμμένων κωδικών πρόσβασης και αναλύοντας τα δεδομένα τους με βάση τη συχνότητα εμφάνισης των κωδικών πρόσβασης, οι εισβολείς έχουν δημιουργήσει λίστες κωδικών πρόσβασης, ταξινομημένες με βάση το πόσο συχνά χρησιμοποιούνται. Οι εισβολείς χρησιμοποιούν αυτές τις λίστες για να προσπελάσουν διακομιστές, σε επίπεδο διαχειριστή, σε λίγα μόλις δευτερόλεπτα.

2.12.5 Phising: Ο όρος *phising* αναφέρεται στη διαδικασία «ψαρέματος» για λογαριασμούς και κωδικούς πρόσβασης, διαμορφώνοντας μια ψεύτικη διασύνδεση χρήστη, όπως μια ιστοθέση που φαίνεται ότι είναι πραγματική και στέλνοντας ένα μήνυμα e-mail που προσκαλεί χρήστες να συνδεθούν σε αυτή.

Για παράδειγμα, μπορεί να δεχθεί ένας χρήστης ένα μήνυμα e-mail, που δηλώνει ότι ο λογαριασμός του στην eBay πρέπει να ενημερωθεί για κάποιο λόγο. Κάνει κλικ στην ενσωματωμένη σύνδεση μέσα στο μήνυμα, και αυτό που φαίνεται μοιάζει με τη σελίδα εισδοχής στην eBay. Εισάγει το όνομα λογαριασμού και τον κωδικό πρόσβασής του και παίρνει ένα μήνυμα σφάλματος, που λέει ότι έχει πληκτρολογήσει τον κωδικό πρόσβασης λανθασμένα Όταν κάνει πάλι κλικ στη σύνδεση, εισέρχεται κανονικά και ενημερώνει τις πληροφορίες, όπως του ζητείται. Αυτό που συμβαίνει στην πραγματικότητα είναι ότι ένας εισβολέας του έστειλε ένα e-mail που περιείχε μια σύνδεση προς μια ιστοσελίδα, την οποία είχε δημιουργήσει αυτός, έτσι ώστε να μοιάζει σε εμφάνιση με την ιστοθέση της eBay. Όταν πληκτρολογήθηκε ο λογαριασμός χρήστη και ο κωδικός πρόσβασης, αυτά τα στοιχεία καταγράφτηκαν και μετά ανακατευθύνθηκε ο χρήστης στην κανονική ιστοσελίδα, οπότε τη δεύτερη φορά που εισήγαγε τον κωδικό πρόσβασης, αυτός δούλεψε σωστά.

2.12.6 Δούρειοι Ίπποι: Οι Δούρειοι ίπποι, είναι προγράμματα, τα οποία εγκαθίστανται κρυφά σε ένα σύστημα στόχου απευθείας από έναν εισβολέα, από έναν ιό ή σκουλήκι υπολογιστή ή από έναν ανυποψίαστο χρήστη. Αφού εγκατασταθεί, ο Δούρειος Ίππος επιστρέφει πληροφορίες στον εισβολέα ή παρέχει άμεση πρόσβαση στον υπολογιστή.

2.13 Κίνδυνοι Ασφαλείας στο Διαδίκτυο

Το διαδίκτυο σχεδιάστηκε από επιστημονικές και ακαδημαϊκές κοινότητες προκειμένου να επιτευχθεί η ανταλλαγή πληροφοριών μεταξύ έμπιστων οντοτήτων. Το θέμα της ασφάλειας των ευαίσθητων πληροφοριών δεν απασχόλησε αρχικά τους σχεδιαστές του. Ο λόγος είναι ότι κανένας δεν μπορούσε να προβλέψει τότε ότι θα επεκταθεί και θα συνδέσει την πλειοψηφία των δημοσίων και ιδιωτικών δικτύων που υπάρχουν στον κόσμο σήμερα.

Το διαδίκτυο ως μέσο ψηφιακής επικοινωνίας κρύβει έναν αριθμό από σοβαρούς κινδύνους, όπως:

- **Έλλειψη εμπιστευτικότητας,** αφού τα δεδομένα που διακινούνται είναι χωρισμένα σε πακέτα και μπορούν εύκολα να κλαπούν και να αποκαλυφθεί το περιεχόμενό τους.

- **Έλλειψη μηχανισμών για την ταυτοποίηση των χρηστών των συστημάτων.** Όλα τα συστήματα που είναι συνδεδεμένα στο διαδίκτυο αναγνωρίζονται από την IP διεύθυνση τους. Το πρωτόκολλο IP δεν παρέχει κάποιο μηχανισμό για την αυθεντικοποίηση των χρηστών του συστήματος.

- **Έλλειψη αξιόπιστων μέσων για σύνδεση των IP** διευθύνσεων με συγκεκριμένους υπολογιστές.

- **Εκτεθειμένοι κωδικοί πρόσβασης.** Τα περισσότερα συστήματα χρησιμοποιούν κωδικούς για την ταυτοποίηση των χρηστών, οι οποίοι τις περισσότερες φορές μεταφέρονται στο δίκτυο χωρίς να κρυπτογραφηθούν.

Η υπηρεσία του παγκόσμιου ιστού (WWW) εισάγει ακόμα περισσότερους κινδύνους. Ένας παρουσιαστής ιστοσελίδων (browser) αποτελεί το ιδανικό μέσο για την αυτόματη εκτέλεση προγραμμάτων χωρίς τη γνώση του χρήστη,

Εγγενή Προβλήματα Ασφάλειας: Το διαδίκτυο δεν πρέπει να αντιμετωπίζεται από άποψη ασφάλειας ως ένα κοινό δίκτυο. Ο κυριότερος λόγος είναι ότι οι μηχανισμοί στους οποίους στηρίζει τη λειτουργικότητα του σχεδιάστηκαν με γνώμονα τη βελτιστοποίησή του στις δυνατότητες διασύνδεσης ετερογενών δικτύων και κοινής εκμετάλλευσης των πληροφοριών/πόρων τους κι όχι στην παρεχόμενη ασφάλεια. Σαν αποτέλεσμα, η ασφάλεια σε κάποιο βαθμό μπορεί να επιτευχθεί μόνο ως ένα πρόσθετο χαρακτηριστικό στην υπάρχουσα υποδομή παρά σαν ένα μέρος του πρωταρχικού δικτυακού σχηματισμού.

Πιο αναλυτικά, στα εγγενή προβλήματα ασφάλειας του διαδικτύου περιλαμβάνονται και τα ακόλουθα:

- **Η ετερογένεια των δικτύων που διασυνδέει,** η οποία με δεδομένο και το τεράστιο μέγεθος του, έχει το προφανές αποτέλεσμα οι σωστές διαδικασίες διασφάλισης ενός συστήματος σε περιβάλλον διαδικτύου, να απαιτούν μια πληθώρα περίπλοκων ρυθμίσεων και διαμορφώσεων.

- **Λόγω της εύκολης και χωρίς περιορισμούς πρόσβασης που προσφέρει σε εκατομμύρια χρήστες,** είναι πιο ευάλωτο από κάθε άλλο δίκτυο και αποτελεί στόχο περισσότερων επιθέσεων για επίδοξους εισβολείς.

- **Δεν υπάρχει συνολική πολιτική ελέγχου προσπέλασης.** Επιπλέον, πολλοί κόμβοι δεν είναι σε θέση για διάφορους λόγους (άγνοια, κόστος, αδιαφορία, κλπ.) να αποκτήσουν τη κατάλληλη διαμόρφωση, έτσι ώστε να μην κινδυνεύουν από την ευρέως ανοικτή σύνδεσή τους στο διαδίκτυο.

- **Η φύση του πρωτοκόλλου TCP/IP και των περισσότερων υπηρεσιών που υποστηρίζει, προσθέτουν νέες ευπάθειες και σημεία επιθέσεων.** Το γεγονός ότι επιτρέπονται τα πακέτα των δεδομένων να περνούν από μια σειρά απρόβλεπτων ενδιάμεσων υπολογιστών και επιμέρους δικτύων μέχρι να φτάσουν στο τελικό προορισμό τους, δίνει τη δυνατότητα σε ένα τρίτο μέρος να παρέμβει με διάφορους τρόπους στην επικοινωνία δυο νόμιμων μερών.

2.13.1 Απειλές Ασφάλειας

Στις τυπικές απειλές ασφάλειας σε ένα περιβάλλον διαδικτύου, συμπεριλαμβάνονται :

- ***Βλάβες συστατικών μερών (component failure):*** Σχεδιαστικά λάθη ή ελαττωματικά μέρη υλικού/λογισμικού, είναι ικανά να προκαλέσουν δυσλειτουργία σε κάποιο συστατικό του συστήματος και να οδηγήσουν έτσι σε άρνηση εξυπηρέτησης ή άλλες καταστάσεις επικίνδυνες για την ασφάλεια.
- ***Παρουσίαση πληροφοριών (information browsing):*** Η αποκάλυψη ευαίσθητων πληροφοριών σε μη-εξουσιοδοτημένους χρήστες, είτε είναι εισβολείς είτε είναι νόμιμοι χρήστες που επιχειρούν παράνομους τρόπους προσπέλασης, οδηγεί στην απώλεια εμπιστευτικότητας και μπορεί να προκληθεί από την εκμετάλλευση διάφορων μηχανισμών.
- ***Μη-εξουσιοδοτημένη διαγραφή, μεταβολή ή εισαγωγή πληροφοριών***: Η εκούσια ή και ακούσια πρόκληση ζημιών στα πληροφοριακά αγαθά (information assets) οδηγεί στην απώλεια της ακεραιότητας των λειτουργιών/δεδομένων των οργανισμών και των χρηστών.
- ***Κατάχρηση (misuse):*** Η χρήση των πληροφοριακών αγαθών αλλά και των υπόλοιπων πόρων για σκοπούς διαφορετικού από αυτούς που έχουν προκαθορισθεί, προκαλεί άρνηση εξυπηρέτησης, αύξηση κόστους λειτουργίας των συστημάτων και δυσφήμιση των οργανισμών που τα χρησιμοποιούν.
- ***Διείσδυση (penetration):*** Οι εισβολείς από μη-εξουσιοδοτημένα πρόσωπα ή συστήματα μπορούν να προκαλέσουν άρνηση εξυπηρέτησης ή να απαιτήσουν σοβαρότατα χρηματικά ποσά για την αντιμετώπιση των συνεπειών από τις παρενοχλήσεις του συστήματος.
- ***Διαστρέβλωση:*** Οι προσπάθειες ενός χρήστη που παρανομεί, να μεταμφιεστεί σαν ένας χρήστης με εξουσιοδοτήσεις τέτοιες ώστε να μπορεί να κλέψει πληροφορίες ή να εκμεταλλευτεί υπηρεσίες ή να εκκινήσει συναλλαγές που προκαλούν οικονομικές απώλειες ή δυσχέρειες σε ένα οργανισμό.

Οι πιθανότητες να εκδηλωθούν επιθέσεις και να πραγματοποιηθούν απειλές όπως οι προαναφερθείσες, αυξάνονται όταν προσφέρεται στο διαδίκτυο μια ευδιάκριτη εικόνα της οργάνωσης της δικτυακής υποδομής ενός συστήματος. Πάρα πολλές επιθέσεις στο Internet είναι ευκαιριακής φύσης (opportunistic), με την έννοια ότι δεν έχουν συγκεκριμένο στόχο παραβίασης. Απλά εκδηλώνονται σε ένα συγκεκριμένο σύστημα γιατί εκείνη τη στιγμή το σύστημα αυτό «φαντάζει» ως ιδανικός στόχος (τελικός ή ενδιάμεσος) για τους επίδοξους εισβολείς.

2.13.2: Συνέπειες ασφαλείας

- απλή ενόχληση ή καθυστέρηση του δικτύου
- Μερική ή ολική καταστροφή των δεδομένων μας
- Καταγραφή κωδικών και αποστολή σε συγκεκριμένο παραλήπτη.
- υποκλοπή δεδομένων

Κεφάλαιο 3ο

Βασικές Έννοιες

Στον όρο **«Ασφάλεια»** μπορούν να αποδοθούν πολλές ερμηνείες, κάθε μία από τις οποίες μπορεί να αποδώσει με ακρίβεια διαφορετικές καταστάσεις. Σύμφωνα με τον ορισμό του λεξικού της Οξφόρδης, «ασφάλεια είναι η ελευθερία από τον κίνδυνο ή το φόβο». Διάφοροι άλλοι ορισμοί μπορούν να χρησιμοποιηθούν για να προσδιορίσουν την ασφάλεια όπως:

• Υπηρεσία της Αστυνομίας.
• Ηλεκτρική διάταξη που αποτρέπει πιθανά ατυχήματα.
• Μηχανισμός στην πόρτα αυτοκινήτου.

Από μία πρακτική άποψη, η ασφάλεια μπορεί να έγκειται στην επαρκή προστασία ανθρώπων και αγαθών, για την οποία μπορεί να λαμβάνονται διάφορα μέτρα προστασίας από πιθανούς κινδύνους
Η ασφάλεια μίας ηλεκτρονικής βάσης δεδομένων έγκειται στην προστασία των δεδομένων από καταστροφή, διαγραφή, αλλοίωση ή αποκάλυψη σε μη εξουσιοδοτημένους χρήστες.
Η Ασφάλεια Τεχνολογίας Πληροφορίας και Επικοινωνιών – ασφάλεια ΤΠΕ(Information and Communication Technology Security – ICT Security) περιλαμβάνει την ασφάλεια:
1. Των υπολογιστικών συστημάτων και εφαρμογών, δηλαδή την προστασία από μη εξουσιοδοτημένες ενέργειες όπως αλλαγή δικαιωμάτων πρόσβασης, κακόβουλη εκτέλεση εντολών, τροποποίηση της διάρθρωσης του συστήματος, κακόβουλη ή λανθασμένη χρήση, διακοπή λειτουργίας, καθώς και τη φυσική προστασία των υπολογιστικών συστημάτων.
2. Των δικτύων και των υποδομών, δηλαδή την προστασία από μη εξουσιοδοτημένη λογική πρόσβαση σε ένα δίκτυο, παράκαμψη ή τροποποίηση των κανόνων δρομολόγησης στο δίκτυο, παρακολούθηση του μέσου επικοινωνίας, διακοπή της επικοινωνίας, φυσική προστασία των υποδομών επικοινωνίας κτλ.
3. Των πληροφοριών, δηλαδή την προστασία των δεδομένων ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα τους.

Ο ρόλος του Η/Υ κατά την εκτέλεση των μη εξουσιοδοτημένων πράξεων συνήθως είναι διττός:

1. Αποτελεί βασικό εργαλείο (αλλά όχι πάντα αποκλειστικό) για την τέλεση τους,
2. Ο ίδιος ο Η/Υ (και συγκεκριμένα τα δεδομένα ή/και οι πληροφορίες που
περιέχονται ή δημιουργούνται σε αυτόν) αποτελεί στόχο των πράξεων αυτών. Οι μη εξουσιοδοτημένες πράξεις, ανάλογα με τις συνέπειες τους μμπορούν να αποτελούν ή όχι ένα Ηλεκτρονικό Εγκλημα

3.2 Ασφάλεια – γιατί τη χρειαζόμαστε

Τα τελευταία χρόνια, και κυρίως λόγω της άνθησης και εξάπλωσης των τεχνολογιών και υπηρεσιών Web, οι πληροφοριακοί κίνδυνοι κατά της ασφάλειας Η/Υ και δικτύων είναι πολυάριθμοι. Μια (όχι πλήρης) λίστα από παραδείγματα:

• **Κακόβουλο Λογισμικό,** π.χ. Ιοί (Viruses), Σκουλήκια (Worms), Δούρειοι Ίπποι (Trojan Horses), Spyware, Adware, με σκοπό τη μη εξουσιοδοτημένη πρόσβαση στους πόρους ενός Η/Υ.

• **Μη εξουσιοδοτημένη εισβολή σε υπολογιστικά-πληροφοριακά συστήματα (Hacking).** Χρήση κακόβουλου λογισμικού ή/και τεχνικών Κοινωνικής Μηχανικής (Social Engineering) με σκοπό την εκμετάλλευση των αδυναμιών και την πρόσβαση στους πόρους του συστήματος

• **Επιθέσεις Άρνησης Εξυπηρέτησης (Denial Of Service).** Διακοπή ή υποβάθμιση των παρεχομένων υπηρεσιών ενός συστήματος.

• **Επιθέσεις Πλαστοπροσωπίας (Spoofing / Masquerading).** Χρήση «πλαστής» ταυτότητας με σκοπό τη μη ανίχνευση του επιτιθέμενου, ή/και την παράκαμψη των τεχνικών ελέγχου πρόσβασης του συστήματος.

• **Υποκλοπές Επικοινωνιών.** Αλλοίωση δεδομένων. Επιθέσεις στην εμπιστευτικότητα (confidentiality) και ακεραιότητα (integrity) των δεδομένων- πληροφοριών που είναι αποθηκευμένες ή ανταλλάσσονται μεταξύ δύο ηλεκτρονικών διατάξεων.

• **Μη ζητηθείσα επικοινωνία (spam).** Μηνύματα ηλεκτρονική αλληλογραφίας που αποστέλλονται χωρίς τη συγκατάθεση του παραλήπτη, ενώ συχνά η ταυτότητα του αποστολέα είναι πλαστογραφημένη ή απλά αδύνατον να εντοπιστεί.

• **Παραβίαση δικαιωμάτων πνευματικής ιδιοκτησίας.** Αντιγραφή, αναπαραγωγή, παραποίηση ή/και αναδιανομή δεδομένων-πληροφοριών που προστατεύονται από τους νόμους περί πνευματικής ιδιοκτησίας, χωρίς τη συγκατάθεση του δημιουργού τους.

3.3 Απειλές, Αδυναμίες και Συνέπειες

Απαραίτητη προϋπόθεση για το σχεδιασμό-διαχείριση της ασφάλειας ενός συστήματος είναι η καταγραφή των απειλών και των αδυναμιών του συστήματος. Έπειτα αναζητούνται και εφαρμόζονται τα κατάλληλα μέτρα προστασίας. Στην ενότητα αυτή παρατίθενται και επεξηγούνται οι όροι που σχετίζονται με την παραπάνω διαδικασία.

- Πληροφοριακός Πόρος ή Αγαθό (Asset). Κάθε αντικείμενο ή πόρος που ανήκει ή υποστηρίζει ένα πληροφοριακό σύστημα και το οποίο αξίζει να προστατευθεί.

Υπάρχουν **διάφορες κατηγορίες αγαθών**, όπως:

- **Φυσικά Αγαθά (Physical Assets):** Κτήρια, Υπολογιστές, δικτυακή Υποδομή, Έπιπλα, κτλ
- **Αγαθά Δεδομένων (Data Assets):** Αρχεία (ηλεκτρονικά, έντυπα)
- **Αγαθά Λογισμικού (Software Assets):** Λογισμικό Εφαρμογών, Λειτουργικά Συστήματα, κτλ.

Συνέπεια ή Αξία Αγαθού (Impact or Value). Η **απώλεια** που θα προκληθεί από την προσβολή ενός αγαθού. Αυτή μπορεί να μμετρηθεί ως:

• **Άμεση Οικονομική Συνέπεια**, δηλαδή το κόστος που απαιτείται για την επαναγορά του αγαθού ή για την συλλογή, επαναδημιουργία ή συντήρηση.

• **Έμμεση συνέπεια,** δηλαδή το μη μετρήσιμο κόστος που θα μπορούσε να προκληθεί από την προσβολή του αγαθού.

Παραδείγματα έμμεσης συνέπειας είναι:

- **Συνέπειες δυσφήμησης και Απώλειας Καλής Πίστης:** Είναι η απώλεια που θα προκαλέσει σε έναν οργανισμό μία επιτυχημένη επίθεση ασφάλειας, λόγω της δυσφήμησης και της απώλειας καλής πίστης που θα προκαλέσει. Για παράδειγμα, μία επιτυχημένη επίθεση στο δίκτυο μίας τράπεζας θα αποτρέψει πολλούς πελάτες από τη χρήση υπηρεσιών ηλεκτρονικής τραπεζικής και άρα θα έχει συνέπειες στα έσοδα αυτής της υπηρεσίας.

- **Νομικές Συνέπειες:** Είναι η απώλεια που θα προκαλέσει σε έναν οργανισμό μία επιτυχημένη επίθεση ασφάλειας λόγω αδυναμίας συμμόρφωσης με νομικές υποχρεώσεις. Για παράδειγμα, σε περίπτωση που κάποιο νοσηλευτικό ίδρυμα δεν λαμβάνει τα αναγκαία μέτρα για την προστασία των δεδομένων ασθενών και εξαιτίας ελλιπών μέτρων διαρρεύσουν δεδομένα υγείας ενός ασθενούς, τότε ενδέχεται να υπάρξουν πρόστιμα λόγω παραβίασης της νομοθεσίας περί προστασίας προσωπικών δεδομένων.

- **Συνέπειες Διακοπής ή Παρεμπόδισης Λειτουργίας:** Είναι το κόστος που προκαλείται λόγω της προσωρινής διακοπής ή παρεμπόδισης λειτουργίας. Για παράδειγμα, εάν το δίκτυο ενός τηλεπικοινωνιακού παρόχου υποστεί μία επιτυχημένη επίθεση άρνησης εξυπηρέτησης (Denial-of-Service attack) και δεν λειτουργεί κανονικά για ορισμένο χρονικό διάστημα, τότε θα υπάρξουν απώλειες από τη μη χρήση της υπηρεσίας για το χρονικό αυτό διάστημα
(χαμένες κλήσεις sms, κτλ).

- **Κοινωνικές Συνέπειες:** Αυτές αφορούν τις απώλειες που θα προκληθούν στο κοινωνικό σύνολο από μία επιτυχημένη επίθεση στις ΤΠΕ ενός οργανισμού. Για παράδειγμα, σε περίπτωση που το σύστημα συλλογής κλήσεων άμεσης δράσης της Αστυνομίας υποστεί επίθεση και δεν λειτουργεί, θα υπάρξουν συνέπειες στο κοινωνικό σύνολο από την αδυναμία κλήσεως της Αρχής για αυτό το χρονικό διάστημα.

Σημειώνεται ότι σε πολλές περιπτώσεις μία επιτυχημένη επίθεση ασφάλειας μπορεί να έχει περισσότερες από μία άμεσες ή έμμεσες συνέπειες σε ένα αγαθό. Σε αυτή την περίπτωση η συνέπεια θα εκτιμηθεί με βάση την μεγαλύτερη συνέπεια της συγκεκριμένης επίθεσης.

- Απειλή (Threat): Οποιοδήποτε γεγονός το οποίο προκαλεί αρνητικές συνέπειες (impact) σε κάποιο αγαθό. Μία απειλή μπορεί να προκληθεί από τυχαία ή εσκεμμένα γεγονότα. Παραδείγματα απειλών είναι:

• **Περιβαλλοντικές απειλές:** Φωτιά, σεισμός, καταιγίδα, προβλήματα ηλεκτρισμού κτλ

• **Σκόπιμες ανθρώπινες απειλές:** πλαστοπροσωπία, εύρεση κωδικού, εκμετάλλευση αδυναμιών δικτύου, λογισμικού, λειτουργικού συστήματος, κακή χρήση των πόρων, μη εξουσιοδοτημένη πρόσβαση, κλοπή, απάτη, βανδαλισμός, εμπρησμός κτλ

• **Μη σκόπιμες ανθρώπινες απειλές:** Λανθασμένη χρήση συστήματος, προγραμματιστικά λάθη, μη σκόπιμη αποκάλυψη δεδομένων, μη σκόπιμη καταστροφή εξοπλισμού κτλ.

Οι απειλές στην ασφάλεια του συστήματος διακρίνονται σε Εξωτερικές (δηλαδή απειλές που προέρχονται από το εξωτερικό περιβάλλον – π.χ. εκτός του Οργανισμού/Επιχείρησης) και σε **Εσωτερικές** (δηλαδή απειλές που προέρχονται από το εσωτερικό περιβάλλον – π.χ. εντός του Οργανισμού/Επιχείρησης).

1. Εξωτερικές απειλές. Γεγονότα, καταστάσεις ή οντότητες που δρουν ή εκτυλίσσονται στο εξωτερικό περιβάλλον απειλούν την ασφάλεια του συστήματος.

• **Εξωτερικοί Εισβολείς (outsiders):** Hackers / Crackers / Vandals / Hacktivists,

Πραγματοποίηση Επιθέσεων όπως:

ο **Footprinting** – Εύρεση στοιχείων για την επιχείρηση π.χ. μπλοκ IP διευθύνσεων, e-mail διευθύνσεις, τοπολογία δικτύου, ονόματα υπολογιστών, διάρθρωση της επιχείρησης κ.λ.π

ο **Scanning & enumerating** - Εύρεση υπηρεσιών, προγραμμάτων εφαρμογών
και πρωτοκόλλων που υλοποιούν/εκτελεί ο υπολογιστής-στόχος,

ο **Hacking** - Παράκαμψη του μηχανισμού ασφάλειας με σκοπό τη μη
εξουσιοδοτημένη πρόσβαση σε κάποιο αγαθό του συστήματος).

• **Κακόβουλο λογισμικό:** Ιοί (Viruses), Σκουλήκια (Worms), Δούρειοι Ίπποι (Trojan Horses)κ.λ.π.

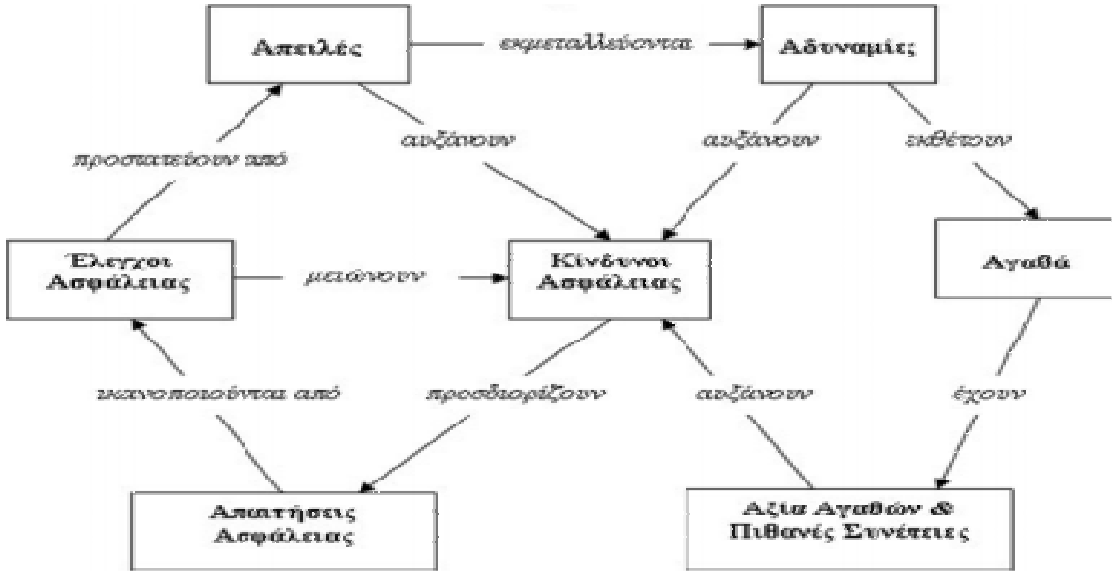
• **Κοινωνικοί Μηχανικοί (Social Engineers):** Εξωτερικοί χρήστες που εκμεταλλεύονται τον ανθρώπινο παράγοντα για να παρακάμψουν έναν μηχανισμό ασφάλειας και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στο σύστημα.

2. Εσωτερικές Απειλές. Δηλαδή, «νόμιμοι» χρήστες του συστήματος οι οποίοιπροσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε πόρους του συστήματος.

- Χρήστες της Επιχείρησης/Οργανισμού που παρακάμπτουν τις διαδικασίες ελέγχου για την πρόσβαση σε διαβαθμισμένα δεδομένα/πληροφορίες.

- Χρήστες που αποκτούν πρόσβαση σε λογαριαστείς χρηστών με περισσότερα δικαιώματα σε σχέση με τα δικαιώματα που ήδη έχουν.

Αδυναμία (Vulnerability). Οποιοδήποτε χαρακτηριστικό κάνει ευάλωτο ένα αγαθό σε κάποια απειλή. Για παράδειγμα, εάν η πρόσβαση σε ένα απόρρητο αρχείο δεν προστατεύεται επαρκώς, το αρχείο έχει μεγάλη αδυναμία στην απειλή της κλοπής. Όσο μεγαλύτερη είναι η αδυναμία ενός αγαθού σε μία απειλή, τόσο μεγαλύτερες θα είναι οι συνέπειες στο αγαθό σε περίπτωση που εκδηλωθεί η απειλή αυτή. Οι αδυναμίες μπορεί είτε να είναι «εγγενείς» (π.χ. «κακή» διαχείριση της μνήμης από μια εφαρμογή ή το Λ.Σ.), ή να δημιουργούνται από κακή χρήση-διαχείριση του συστήματος (π.χ. λάθος ορισμός των «δικαιωμάτων» - permissions σε ένα αρχείο).



Γραφήμα 1: Σύνδεση όρων ανάλυσης και διαχείρισης κινδύνου

Επιθέσεις (attacks)

Μια εξωτερική (ή εσωτερική) απειλή εκμεταλλεύεται μια ή περισσότερες αδυναμίες και εξαπολύει μια επίθεση που έχει ως συνέπεια την παραβίαση της εμπιστευτικότητας, της αυθεντικότητας, της ακεραιότητας ή της διαθεσιμότητας τουσυστήματος.

Τυχαίες και Εσκεμμένες Επιθέσεις. Οι επιθέσεις που πραγματοποιούνται μπορεί ναείναι:

- **Τυχαί**ες , π.χ. λάθη, αμέλεια, φωτιά, διακοπή ρεύματος..
- **Εσκεμμένες** , π.χ. hackers, crackers, vandals,..

Ένα σύστημα αποτελείται από διατάξεις υλικού (Υλικό), εφαρμογές λογισμικού(Λογισμικό), Δεδομένα, Γραμμές Επικοινωνίας, καθώς και ανθρώπους που τα διαχειρίζονται-χρησιμοποιούν. Σε χαμηλό επίπεδο, εκτός από τις προηγούμενες γενικές κατατάξεις, οι επιθέσεις στην Ασφάλεια Η/Υ μμπορούν επίσης να κατηγοριοποιηθούν ανάλογα με το είδος της συνέπειας που επιφέρουν, καθώς και ανάλογα με τον τύπο του αγαθού που επηρεάζουν. Έτσι, **οι επιθέσειςδιακρίνονται σε:**

• Επιθέσεις Υποκλοπής (Interception)

- **Μία μη εξουσιοδοτημένη οντότητα αποκτά πρόσβαση σε ένα αγαθό.**

Οι επιθέσεις Υποκλοπής μπορεί να έχουν ως στόχο το Υλικό (π.χ. εξαγωγή κλειδιών- κωδικών από κάρτες), τα Δεδομένα(π.χ. επιθέσεις sniffing, μη εξουσιοδοτημένη ανάγνωση ή αντιγραφή εγγράφων/φακέλων, αρχείων κωδικών (password files), υποκλοπή αριθμών πιστωτικών καρτών, κωδικών PIN, κωδικών password κατά τη μεταφορά τους στο δίκτυο), το Λογισμικό(π.χ. μη εξουσιοδοτημένη πρόσβαση στον κώδικα των προγραμμάτων, μη εξουσιοδοτημένη αντιγραφή προγραμμάτων) ή τις Γραμμές Επικοινωνίας του

συστήματος (π.χ. επιθέσεις ανάλυσης κίνησης -traffic analysis). Ουσιαστικά αποτελούν επιθέσεις κατά της Εμπιστευτικότητας (Confidentiality) του Συστήματος.

• Επιθέσεις Διακοπής (Interruption)

- **Ένα αγαθό χάνεται, γίνεται μη διαθέσιμο, ή τίθεται εν αχρηστία.** Για παράδειγμα, διαγραφή αρχείων, δεδομένων και πληροφοριών, κ.λ.π Οι επιθέσεις Διακοπής μπορεί να έχουν ως στόχο το Υλικό (ζημιά, βλάβες, διακοπή ρεύματος,επιθέσεις άρνησης εξυπηρέτησης σε ηλεκτρονικές διατάξεις), το Λογισμικό (διαγραφή ή αναστολή της εκτέλεσης προγράμματος), τα Δεδομένα (π.χ. διαγραφή ή απώλεια δεδομένων, επιθέσεις στο Σύστημα Αρχείων) ή τις Γραμμές Επικοινωνίας(π.χ. βλάβη/επίθεση στους δρομολογητές ή στο μέσο μετάδοσης με σκοπό τη διακοπή της επικοινωνίας). Ουσιαστικά αποτελούν επιθέσεις κατά της Διαθεσιμότητας (Availability) του Συστήματος.

• Επιθέσεις Αλλοίωσης (Modification)

- **Μία οντότητα αποκτά μη εξουσιοδοτημένη πρόσβαση με σκοπό τηναλλοίωση-τροποποίηση των περιεχομένων ενός αγαθού.**

Οι επιθέσεις Αλλοίωσης μπορεί να έχουν ως στόχο το Υλικό (π.χ. φθορά ή επιθέσεις σε ηλεκτρονικές διατάξεις με σκοπό την παράκαμψη μηχανισμών ασφάλειας), το Λογισμικό (π.χ. αλλοίωση του κώδικα του προγράμματος), ή τα Δεδομένα του Συστήματος (αλλοίωση των περιεχομένων ενός αρχείου, των εγγραφών σε μια ΒΔκλπ. Ουσιαστικά αποτελούν επιθέσεις κατά της Ακεραιότητας (Integrity) του Συστήματος.

• Επιθέσεις Εισαγωγής (Fabrication)

- **Ένα (μη αυθεντικό) αντικείμενο ή υποκείμενο εισέρχεται στο σύστημα.** Οι επιθέσεις Πλαστοπροσωπίας (Spoofing), παραπλανητικής αλληλογραφίας (Phishing), Ενδιάμεσης Οντότητας (Man in the Middle), καθώς και οι επιθέσεις Επανάληψης (replay attacks) αποτελούν υποπεριπτώσεις αυτής της κατηγορίας επιθέσεων.

Οι επιθέσεις Εισαγωγής μπορεί να έχουν ως στόχο το Υλικό (π.χ. αντικατάσταση ηλεκτρονικής διάταξης), το Λογισμικό (π.χ. αντικατάσταση του νομίμου προγράμματος με κάποιο άλλο, συνήθως κακόβουλο πρόγραμμα), τα Δεδομένα ή τους Ανθρώπους του συστήματος (π.χ. επιθέσεις πλαστοπροσωπίας). Αποτελούν επιθέσεις κατά της Ακεραιότητας (Integrity) και της Αυθεντικότητας του Συστήματος.

Σημείωση: Οι επιθέσεις Κοινωνικής Μηχανικής έχουν ως αρχικό στόχο τους ανθρώπους-μέλη του συστήματος, με απώτερο όμως σκοπό την πραγματοποίηση μιας εκ των ως άνω επιθέσεων.

Οι επιθέσεις κατά του Συστήματος μπορούν επίσης να κατηγοριοποιηθούν σε:

Παθητικές και Ενεργητικές:

• **Παθητικές (Passive):** Επιθέσεις υποκλοπής κατά τις οποίες ο «εχθρός» αποκτά μη εξουσιοδοτημένη πρόσβαση σε κάποιο αγαθό του συστήματος. Αναφέρονται ως παθητικές επειδή ο «εχθρός» υποκλέπτει (και μόνον) το αγαθό χωρίς να τροποποιεί, να διαγράφει ή να εισάγει δεδομένα που διακινούνται στο σύστημα.
Ενεργητικές (Active): Ο εχθρός έχει τη δυνατότητα να εξαπολύσει επιθέσεις Διακοπής, Αλλοίωσης, ή Εισαγωγής. Οι ενεργητικές επιθέσεις θεωρούνται οιπλέον δύσκολες ως προς την αντιμετώπιση τους.

Απαιτήσεις Ασφάλειας

Μια διαδεδομένη κατηγοριοποίηση περιλαμβάνει τα εξής:

• **Ιδιωτικότητα (Privacy).** Η ιδιωτικότητα θεωρείται ένας αρκετά γενικός όρος. Στη βιβλιογραφία συναντάμε δύο επιπλέον έννοιες που σχετίζονται με την ιδιωτικότητα:
- **Ανωνυμία (Anonymity):** Απόκρυψη της ταυτότητας μιας οντότητας(υποκείμενο, πρόγραμμα, ηλεκτρονική διάταξη) που συμμετέχει σε μια συναλλαγή.
- **Εμπιστευτικότητα / Μυστικότητα (Confidentiality, Secrecy).** Το περιεχόμενο των αποθηκευμένων ή μεταφερόμενων δεδομένων προστατεύεται από μη εξουσιοδοτημένη ανάγνωση-αντιγραφή (επιθέσεις υποκλοπής).
• **Αυθεντικότητα (Authenticity, Authentication).** Στη βιβλιογραφία, ο όρος συχνά σχετίζεται με τις ακόλουθες έννοιες:
- **Ταυτοποίηση (Identification) ή Αυθεντικοποίηση Οντότητας (Entity Authentication):** Με την ταυτοποίηση δίνεται απάντηση στο ερώτημα «Ποιος είναι αυτός που θέλει να αποκτήσει πρόσβαση;»
- Αυθεντικοποίηση Προέλευσης Μηνύματος (Data Origin Authentication):
Δίνεται απάντηση στο ερώτημα: «Ποιος έστειλε αυτό το μήνυμα;»
- **Εξουσιοδότηση (Authorization) ή Έλεγχος Προσπέλασης:** Τα μοντέλα εξουσιοδότησης δίνουν απάντηση στο ερώτημα «Τι μπορεί να κάνει αυτός που απέκτησε πρόσβαση;»
- **Μη αποποίηση Ευθύνης (Non-Repudiation):** Δίνεται (αρνητική) απάντηση στο ερώτημα: «Μπορεί ο χρήστης Α να αρνηθεί ότι πραγματοποίησε τη συναλλαγή;» Η απαίτηση της «μη αποποίησης Ευθύνης» βρίσκει σημαντική εφαρμογή σε εφαρμογές Ηλεκτρονικού Εμπορίου.
• **Ακεραιότητα (Integrity).** Προστασία των αγαθών του συστήματος από μη εξουσιοδοτημένη τροποποίηση-αλλοίωση. Σημείωση: Εάν ένα μήνυμα, κατά την μεταφορά του, τροποποιηθεί π.χ.

εσκεμμένα από κάποιον τρίτο, τότε το μήνυμα, εκτός από την ακεραιότητα, χάνει επίσης την αυθεντικότητα του.

• Δ**ιαθεσιμότητα (Availability).** Εξασφάλιση της συνεχούς και αδιάλειπτης πρόσβασης στα [δεδομένα / πληροφορίες / προγράμματα / υπηρεσίες / υλικό] του συστήματος.

3.4 Κρίσιμα Ερωτήματα κατά το Σχεδιασμό της Ασφάλειας

Α. Η προστασία θα επικεντρωθεί στα δεδομένα, στις διαδικασίες, ή στους χρήστες;

Δεδομένα: Τεχνικές ελέγχου πρόσβασης (access control) με τη χρήση εξειδικευμένων προγραμμάτων και εξοπλισμού ασφαλείας.

Διαδικασίες: Η ασφάλεια επικεντρώνεται κυρίως στις διαδικασίες που ακολουθούνται (Organizational Security) και λιγότερο σε εξεζητημένα τεχνολογικά μέσα. Για παράδειγμα, όταν οι χρήστες ταυτοποιούνται, η πολιτική ασφάλειας μπορεί να καθορίζει ότι κατά την ταυτοποίηση του χρήστη θα παρίσταται και ένα τρίτο εξουσιοδοτημένο πρόσωπο (π.χ. προσωπικό ασφάλειας) ώστε, σε περίπτωση που το ηλεκτρονικό σύστημα απορρίψει λανθασμένα (False Reject) την είσοδο στο σύστημα, να ελέγχεται η ταυτότητα του ατόμου με φυσικά μέσα. Συχνά οι διαδικασίες ασφάλειας περιγράφονται στα πλαίσια μιας Πολιτικής Ασφάλειας (Security Policy) και συμπληρώνονται ή/και υποβοηθούνται από τεχνολογικά μέσα.

Χρήστες: Δίνεται έμφαση στον ανθρώπινο παράγοντα, με σκοπό τη γνώση για την αντιμετώπιση επιθέσεων κοινωνικής μηχανικής (π.χ. ενημέρωση των χρηστών του συστήματος για την προστασία τους από τεχνικές παραπλάνησης - phishing).

Σημείωση: Ένα ολοκληρωμένο σύστημα ασφάλειας επικεντρώνεται εξίσου και στα τρεις κατηγορίες.

Β. Σε ποιο επίπεδο θα εφαρμόσουμε μηχανισμούς ασφάλειας;

Σε γενικές γραμμές, όσο πιο χαμηλό είναι το επίπεδο στο οποίο ενσωματώνονται κάποιος μηχανισμός ασφάλειας, τόσο πιο δύσκολη είναι η παράκαμψη του. Για παράδειγμα, ξεκινώντας από τα χαμηλά επίπεδα, η κατηγοριοποίηση έχει ως εξής:

• **Υλικό**. Παράδειγμα αποτελούν οι «έξυπνες» κάρτες (tamper-resistant smartcards) οποιαδήποτε προσπάθεια μη εξουσιοδοτημένης ανάγνωσης των περιεχομένων της κάρτας έχει ως αποτέλεσμα την αυτόματη διαγραφή των δεδομένων της κάρτας. Τονίζεται πως η παράκαμψη ενός μηχανισμού ασφάλειας που εφαρμόζεται σε αυτό το επίπεδο, ενδεχομένως απαιτεί επαρκείς γνώσεις τεχνολογιών υλικού και αρχιτεκτονικής Η/Υ, καθώς επίσης και εξοπλισμό (συνήθως) υψηλού κόστους.

• **Λειτουργικό Σύστημα (Λ.Σ.).** Οι μηχανισμοί ασφάλειας εφαρμόζονται στο επίπεδο του Λ.Σ. Παράδειγμα αποτελεί ο καθορισμός δικαιωμάτων πρόσβασης (permissions) στα σύγχρονα Λ.Σ. (τύπου Unix και Windows), τα αρχείακαταγραφής (log files) στο Λ.Σ., η δημιουργία Τομέων (Domains) στο Λ.Σ. Windows 2000 κλπ.

• **Λογισμικό Εφαρμογών.** Οι μηχανισμοί ασφάλειας εφαρμόζονται σε επίπεδο εφαρμογών χρήστη. Παραδείγματα αποτελούν οι εφαρμογές ασφαλούς ηλεκτρονικής αλληλογραφίας (π.χ. PGP), οι τεχνολογίες ασφαλών συναλλαγών μέσω του Διαδικτύου (π.χ. SSH), καθώς και εφαρμογές τύπου antivirus, προσωπικά firewalls, anti-spyware, Ανιχνευτές Ευπαθειών (Vulnerability Scanners), Συστήματα Ελέγχου Εισβολών (IDS), εφαρμογές Καταγραφής και Ελέγχου (Logging and Audit systems), προστασία από παράνομη αντιγραφή (π.χ. συστήματα DRM) κ.λ.π

• **Δεδομένα.** Στο επίπεδο αυτό εφαρμόζονται τεχνολογίες προστασίας ή κρυπτογράφησης των δεδομένων, ανεξαρτήτως της εφαρμογής που τα δημιουργεί ή διαχειρίζεται.

Θα δοθεί έμφαση στην πρόληψη (prevention), ανίχνευση (detection), ή ανάνηψη (recovery) από παραβίαση ασφάλειας;

Οι πλέον σημαντικές **πρακτικές στην ασφάλεια Η/Υ** επικεντρώνονται σε τρεις κατευθύνσεις:

• **Πρόληψη.** Στόχος είναι η αποτροπή μιας επίθεσης κατά των αγαθών του συστήματος, πριν αυτή συμβεί. Για παράδειγμα, η χρήση μίας πόρτας ασφαλείας στοχεύει στο να αποτρέψει τη μη εξουσιοδοτημένη είσοδο σε ένα χώρο. Αντίστοιχα, η χρήση ενός συστήματος firewall σε ένα δίκτυο αποσκοπεί στο να αποτρέψει τη μη εξουσιοδοτημένη είσοδο (έξοδο) πακέτων σε (από) ένα δίκτυο.
Τεχνολογίες όπως Έλεγχος Πρόσβασης σε επίπεδο Λ.Σ., ταυτοποίηση χρηστών,κρυπτογράφηση, ασφάλεια εφαρμογών, συστήματα antivirus, ανιχνευτές ευπαθειών (vulnerability scanners) χρησιμοποιούνται κατά κόρον για νααποτρέψουν κάθε πιθανή εισβολή.

• **Ανίχνευση**. Ανεξαρτήτως του είδους και της ποσότητας των μέτρων πρόληψης που θα υιοθετηθούν, κανένα σύστημα δε μπορεί να είναι 100% ασφαλές. Στο σχεδιασμό ασφάλειας θα πρέπει λοιπόν να ενσωματωθούν πρακτικές οι οποίες έχουν ως στόχο να ανιχνεύσουν μια εισβολή, όταν και εφόσον αυτή συμβεί. Τα συστήματα συναγερμού (alarm systems) αποτελούν το πλέον χαρακτηριστικό παράδειγμα στη φυσική ασφάλεια συστημάτων. Σε επίπεδο εφαρμογών, ενδιαφέρον παρουσιάζουν τα Συστήματα Ανίχνευσης Εισβολής (Intrusion Detection Systems) και τα προγράμματα καταγραφής συμβάντων (logging & audit systems). Με τη χρήση των συστημάτων IDS, είναι επίσης δυνατόν να περιοριστεί (ή ακόμα και να εξαλειφθεί) ένα περιστατικό εισβολής εν τη γενέσει του, εφόσον το IDS συνεργάζεται, σε πραγματικό χρόνο, με προγράμματα αποτροπής (π.χ. firewalls).

• **Ανάνηψη-Επαναφορά.** Τα μέτρα ανάνηψης είναι μέτρα προστασίας που στοχεύουν στο να μειώσουν τον απαιτούμενο χρόνο για την ανάκαμψη μετά από την εκδήλωση επίθεσης. Για παράδειγμα, η ασφαλιστική κάλυψη στοχεύει στο να αποκατασταθούν οι ζημιές από μία ενδεχόμενη κλοπή ή φυσική καταστροφή. Αντίστοιχα η λήψη αντιγράφων ασφάλειας (backup) σε ένα υπολογιστικό σύστημα στοχεύει να ελαχιστοποιήσει τις απώλειες και να επισπεύσει το χρόνο ανάκαμψης ενός συστήματος από μία πιθανή διακοπή λειτουργίας. Η βιωσιμότητα (survivability) ή αλλιώς Συνέχιση Λειτουργίας (Continuity) ενός συστήματος εξασφαλίζεται με τεχνικές όπως: αυτόματη λήψη (ή/και επαναφορά) Αντιγράφων Ασφαλείας

(backup), εργαλεία αφαίρεσης κακόβουλου λογισμικού, συστήματα Πλεονασμού (redundancy) και Ανοχής Λαθών (fault-tolerant systems) όπως συστοιχίες RAID, τεχνικές hot swapping, συστήματα UPS, εφεδρικές γραμμές επικοινωνίας, τεχνικές load balancing κ.α.

3.5 Πολιτικές Ασφάλειας

Ως **«Πολιτική Ασφάλειας»** ορίζεται το έγγραφο εκείνο το οποίο με επίσημο και δομημένο τρόπο καθορίζει τις γενικές αρχές που πρέπει να ισχύουν για την ασφάλεια των:

• πληροφοριών,

• πληροφοριακών συστημάτων

• δικτύων και υποδομών

ενός οργανισμού για την επαρκή προστασία τους από τους υφιστάμενους πληροφοριακούς κινδύνους. κινδύνους που αντιμετωπίζει ένας οργανισμός, ούτε και το επίπεδο αυτών των κινδύνων. Η διαδικασία του καθορισμού και της μέτρησης των πληροφοριακών κινδύνων γίνεται στο προηγούμενο στάδιο της Ανάλυσης Πληροφοριακού Κινδύνου. Η της Πολιτικής Ασφάλειας θα μπορούσε να θεωρηθεί ως μέρος της Διαχείρισης Πληροφοριακού Κινδύνου, εφόσον αφορά το στρατηγικό σχεδιασμό για τη μετέπειτα λήψη των κατάλληλων μέτρων ασφάλειας τα οποία και θα μειώνουν τους υφιστάμενους πληροφοριακούς κινδύνους. Άρα, η Πολιτική Ασφάλειας βοηθά στην αποτελεσματική διαχείριση του υφιστάμενου κινδύνου. Για να ανταποκρίνεται στις πραγματικές ανάγκες ασφάλειας ενός οργανισμού, η Πολιτική Ασφάλειας πρέπει να χρησιμοποιεί τα αποτελέσματα της ανάλυσης κινδύνου (risk analysis), ώστε να εστιάζει στα πραγματικά προβλήματα ασφάλειας που αντιμετωπίζει ο οργανισμός και στον απαιτούμενο βαθμό.

Πηγές για την Ανάπτυξη μιας Πολιτικής Ασφάλειας

Η ανάπτυξη της Πολιτικής πρέπει να βασίζεται σε διάφορες πηγές, οι οποίες αφενός μεν θα εστιάζουν στα συγκεκριμένα προβλήματα ασφάλειας του οργανισμού, αφετέρου δε θα δίδουν γενικές κατευθύνσεις με βάση τις διεθνώς αποδεκτές βέλτιστες πρακτικές. Οι πηγές αυτές περιλαμβάνουν:

Αποτελέσματα Ανάλυσης Επικινδυνότητα

• Αξιολογείται η αξία των αγαθών, οι αδυναμίες του συστήματος, οι (εσωτερικές και εξωτερικές) απειλές και υπολογίζεται το επίπεδο κινδύνου για κάθε συνδυασμό (Αγαθό, Αδυναμία, Απειλή) Æ Επίπεδο Κινδύνου

• Είναι απαραίτητα ώστε η Πολιτική που θα αναπτυχθεί να αντιμετωπίζει τους υφιστάμενους κινδύνους και να μην είναι γενικόλογη και αόριστη

• Η πολιτική θα θέτει το πλαίσιο για τη λήψη των κατάλληλων τεχνικών και οργανωτικών μέτρων για την αντιμετώπιση των κινδύνων

3.6 Νομοθεσία στις τηλεπικοινωνίες και τα δικτυα

• Μπορεί να περιλαμβάνει Εθνική Νομοθεσία, Κοινοτική Νομοθεσία/Οδηγίες, Κανονισμούς Ρυθμιστικών Αρχών (Αρχή Προστασίας Δεδομένων, Προσωπικού Χαρακτήρα, Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών κτλ)

• Θα πρέπει να λαμβάνεται υπόψη κατά την ανάπτυξη μίας πολιτικής ώστε να ικανοποιούνται οι απαιτήσεις συμβατότητας ενός οργανισμού με το νομικό και ρυθμιστικό πλαίσιο της χώρας

Παραδείγματα:

- Προστασία από την επεξεργασία προσωπικών δεδομένων
- Διασφάλιση απορρήτου επικοινωνιών
- Προστασία Πνευματικών Δικαιωμάτων
- Παρεμπόδιση ποινικών εγκλημάτων.

3.8 Αναγκαιότητα και Σκοπιμότητα της Ασφάλειας

Είναι γεγονός ότι η λήψη των απαραίτητων μέτρων ασφάλειας δημιουργεί πολλές φορές κάποια πρόσθετη επιβάρυνση στην απόδοση και το κόστος λειτουργίας του δικτύου υπολογιστών μιας επιχείρησης. Θα πρέπει ακόμη να αποδεχτούμε το κόστος της ασφάλειας και ως κόστος χρόνου και ως κόστος χρήματος. Συνεπώς, μπορεί να θεωρηθεί ότι η ασφάλεια βρίσκεται σε σχέση αντιστρόφως ανάλογη με την αποδοτικότητα του δικτύου υπολογιστών μιας επιχείρησης. Αυτό όμως δεν είναι σωστό γιατί η ασφάλεια είναι κόστος αναγκαίο για την ομαλή και εύρυθμη λειτουργία του.Το συγκεκριμένο κόστος για την ασφάλεια των δικτύων μιας επιχείρησης εξαρτάται και προκύπτει από την εκάστοτε ακολουθούμενη πολιτική ασφάλειας. Απαιτείται συνεπώς μια πολιτική ασφαλείας η οποία θα πρέπει να εξισορροπεί το κόστος εισαγωγής ασφάλειας από την μία πλευρά και το κόστος ζημιών από πιθανολογούμενο κίνδυνο από την άλλη. Επίσης, θα πρέπει να δημιουργούνται τέτοιες συνθήκες ασφάλειας ώστε να μη παρεμποδίζεται η ευελιξία και η ανάπτυξη της επιχείρησης. Η αναγκαία πολιτική ασφάλειας καθορίζεται από μία δυναμική εκτίμηση του κόστους των μέτρων ασφάλειας σε σχέση με τις συνέπειες που θα έχει για τον οργανισμό οποιαδήποτε πρόκληση δυσλειτουργίας. Ο βασικός αυτός κανόνας ισχύει για όλους τους τομείς και όλα τα επίπεδα ασφάλειας. Έτσι, σε κάθε περίπτωση όπου απαιτείται η λήψη κάποιου μέτρου ασφάλειας, πρέπει να εξετάζεται η πιθανότητα να συμβεί κάποιο πρόβλημα ασφάλειας, σε σχέση με τις συνέπειες που αυτό θα δημιουργήσει. Εάν η τιμή των δύο αυτών παραμέτρων είναι υψηλή, τότε πρέπει απαραίτητα να ληφθούν μέτρα, ανεξάρτητα από το κόστος πρόληψης. Τέλος, πρέπει να σημειωθεί ότι η ασφάλεια χαρακτηρίζεται από την φύση της ως δυναμική παράμετρος και όχι στατική, καθώς η τεχνολογία, ο ανταγωνισμός, η πολυπλοκότητα των πληροφοριακών συστημάτων και η ολοένα βελτιούμενη επιτηδειότητα των 'επιτιθέμενων', απαιτούν τη λήψη νέων και συνεχώς αυστηρότερων μέτρων ασφάλειας.

3.9 Τεχνικές και Επίπεδα Ασφαλείας

Υπάρχουν διάφορες τεχνικές που μπορούν να εφαρμοστούν ώστε να επιτευχθεί η ασφάλεια των πληροφοριών και των δεδομένων που διακινούνται σε ένα δίκτυο ή είναι αποθηκεμένες σε ένα σύστημα και μεταδίδονται στο διαδίκτυο. Οι χειρισμοί ασφάλειας τους οποίους πρέπει να λαμβάνει υπόψη της μια επιχείρηση προκειμένου να εξασφαλίσει αυξημένη ασφάλεια στο εταιρικό της δίκτυο κινούνται στις παρακάτω κατευθύνσεις οι οποίες διαγράφονται και αναλυτικότερα στο διάγραμμα που ακολουθεί:

- Προστασία της Εμπιστευτικότητας των Δεδομένων – Data Confidentiality
- Προστασία της Ακεραιότητας των Δεδομένων – Data Integrity
- Έλεγχος γνησιότητας της Ταυτότητας και Αυθεντικοποίηση – Identification & Authentication
- Έλεγχος Προσπέλασης – Access Control
- Επίβλεψη – Auditing

Προστασία της Εμπιστευτικότητας των Δεδομένων – Data Confidentiality

Προστασία της εμπιστευτικότητας των δεδομένων, δηλαδή προστασία ενάντια σε μη-εξουσιοδοτημένες αποκαλύψεις πληροφοριών. Η τεχνολογία της κρυπτογράφησης (encryption/cryptography) είναι σχεδόν συνώνυμη αυτής της λειτουργίας.Μια ειδική κατηγορία αποτελεί η εμπιστευτικότητα ροής δεδομένων (traffic flow confidentiality) καθώς πολλές φορές όχι το περιεχόμενο, αλλά απλά η ύπαρξη κάποιων μηνυμάτων αποτελεί ευαίσθητη πληροφορία και άρα χρειάζεται προστασία. Αυτός ο κίνδυνος διαρροής πληροφοριών γίνεται σοβαρότερος στις περιπτώσεις που κάποιος εισβολέας έχει καταφέρει να δημιουργήσει ένα κρυφό κανάλι στο δίκτυο, από όπου καταγράφοντας την εμφάνιση σποραδικών bits μπορεί να εξάγει συμπεράσματα σχετικά με την επικοινωνία που παρακολουθεί. Οι απόπειρες υποκλοπής εδώ, εκδηλώνονται με επιθέσεις τύπου ανάλυσης κίνησης (traffic analysis) και μπορούν να εξουδετερωθούν με δυο κυρίως μεθόδους ελέγχου κίνησης δικτύου (traffic controls):

Παρεμβολές στην κίνηση (traffic pad) όπου ο διαχειριστής ασφάλειας εισάγει «θόρυβο» στο δίκτυο, δηλαδή πλαστά μηνύματα, με σκοπό να διαταραχθεί η κανονική ροή των πληροφοριών και να συγκαλύψει τις πραγματικές ποσότητες της κυκλοφορίας των δεδομένων.

Έλεγχος δρομολόγησης (routing control) όπου ο διαχειριστής προσπαθεί να επέμβει ενεργά στη διαδρομή που ακολουθούν τα μηνύματα. Έτσι περιοδικά, καθυστερεί πακέτα δεδομένων, αλλάζει τους ενδιάμεσους κόμβους που επισκέπτονται ή ακόμη και σβήνει ορισμένα από αυτά.

3.10 Κρυπτογράφηση/Κρυπτογραφία – Encryption/Cryptography

Σχεδόν όλοι οι σύγχρονοι μηχανισμοί ασφάλειας βασίζονται στο γεγονός ότι ορισμένα μυστικά, κρατούνται ιδιωτικά σε ορισμένα άτομα. Τα συστήματα ασφάλειας χρησιμοποιούν κρυπτογράφηση για να κρατούν μυστικά και χρησιμοποιούν επαλήθευση για να αποδεικνύουν την ταυτότητα συγκεκριμένων ατόμων. Υπάρχουν δύο βασικοί μηχανισμοί ασφάλειας, που αποτελούν τη βάση επί της οποίας βασίζονται όλοι οι μηχανισμοί ασφάλειας.

Ο **όρος κρυπτογραφία** προέρχεται από τις λέξεις "κρυπτός" και "γράφος'. Κυριολεκτικά σημαίνει τη μελέτη της μυστικογραφίας. Γενικότερα, αφορά τον επιστημονικό κλάδο που ασχολείται με τη μελέτη, χρήση και ανάπτυξη τεχνικών κρυπτογράφησης και αποκρυπτογράφησης για την απόκρυψη των περιεχομένων των μηνυμάτων (ή των αποθηκευμένων δεδομένων) και την διευκόλυνση της ανίχνευσης κακόβουλων μετατροπών στα μηνύματα.

Κρυπτογράφηση (encryption) είναι η διεργασία μετασχηματισμού ενός μηνύματος σε μια ακατανόητη μορφή με τη χρήση ενός κρυπτογραφικού αλγορίθμου, έτσι ώστε αυτό να μην είναι αναγνώσιμο από τρίτα μέρη εκτός του νόμιμου παραλήπτη.

Αποκρυπτογράφηση (decryption) είναι η διεργασία ανάκτησης του αρχικού μηνύματος από μια ακατανόητη έκδοσή του που είχε παραχθεί μετά από μια κρυπτογράφηση. Η αποκρυπτογράφηση εκτελείται από κάποιο εξουσιοδοτημένο μέρος, σε αντίθεση με την κρυπτανάλυση, που ορίζεται στη συνέχεια.

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης και ενός κλειδιού κρυπτογράφησης. Κρυπτογραφικός αλγόριθμος (cipher) είναι η μέθοδος, συνήθως μια μαθηματική συνάρτηση μετασχηματισμού δεδομένων, σε μια μορφή που να μην επιτρέπει σε μη εξουσιοδοτημένα μέρη την αποκάλυψη του περιεχομένου τους. Αλλά, η δυνατότητα διατήρησης της μυστικότητας των πληροφοριών βασίζεται περισσότερο σε έναν αριθμό που ονομάζεται κλειδί (key) και χρησιμοποιείται μαζί με τον αλγόριθμο κρυπτογράφησης / αποκρυπτογράφησης, παρά στον αλγόριθμο μόνο του. Επομένως, η ανθεκτικότητα μιας κρυπτογράφησης εξαρτάται περισσότερο από το μέγεθος των κλειδιών που χρησιμοποιούνται παρά από τους αλγόριθμους. Το μέγεθος των κλειδιών μετριέται σε bits. Γενικά, κλειδιά μεγάλου μεγέθους παρέχουν ανθεκτικότερη κρυπτογράφηση. Για παράδειγμα, η κρυπτογράφηση 128-bit RC4 είναι3078 φορές ανθεκτικότερη από την 40-bit RC4.

Διαφορετικοί αλγόριθμοι απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης. Για παράδειγμα, ένας αλγόριθμος συμμετρικής κρυπτογράφησης με κλειδί μεγέθους 128 bits παρέχει ανθεκτικότερη κρυπτογράφηση από τον αλγόριθμο κρυπτογράφησης δημοσίου κλειδιού RSA με ίδιο μέγεθος κλειδιού. Για αυτό πρέπει να χρησιμοποιείται κλειδί μεγέθους τουλάχιστον 512 bits προκειμένου η κρυπτογράφηση RSA να θεωρείται ανθεκτική, ενώ οι συμμετρικοί αλγόριθμοι πετυχαίνουν περίπου το ίδιο επίπεδο ανθεκτικότητας με κλειδί μεγέθους 64 bits. Όμως ακόμη και αυτά τα επίπεδα ανθεκτικότητας έχουν αποδειχθεί ευπαθή σε επιθέσεις σήμερα.

Διάφοροι τρόποι κρυπτογράφησης άρχισαν να αναπτύσσονται από παλιά και συνεχώς εξελίσσονται και αλλάζουν όσο οι ηλεκτρονικοί υπολογιστές γίνονται ισχυρότεροι και ταχύτεροι. Η προσπάθεια να "σπάσει" μια συγκεκριμένη κρυπτογραφική τεχνική ονομάζεται κρυπτανάλυση (cryptanalysis). Κρυπτανάλυση είναι η διεργασία αποκρυπτογράφησης ενός μηνύματος από ένα μη εξουσιοδοτημένο μέρος, το οποίο ονομάζεται κρυπταναλυτής (cryptanalyst).
Το αντικείμενο της κρυπτολογίας (cryptology) καλύπτει και την κρυπτογραφία και την κρυπτανάλυση.

3.10.1 Κρυπτογράφηση

Ο κύριος σκοπός της κρυπτογράφησης είναι να κρατά μυστικά. Έχει και άλλες χρήσεις, αλλά η κρυπτογράφηση χρησιμοποιήθηκε αρχικά για να προστατεύει μηνύματα, έτσι ώστε μόνο το άτομο που γνώριζε το τέχνασμα αποκωδικοποίησης ενός μηνύματος να μπορεί να το διαβάσει. Σήμερα, η κρυπτογράφηση επιτρέπει σε υπολογιστές να κρατούν μυστικά, μετασχηματίζοντας δεδομένα σε μια ακατάληπτη μορφή, χρησιμοποιώντας μια μαθηματική συνάρτηση.
Όπως συμβαίνει και στην απλή αριθμητική, οι συναρτήσεις κρυπτογράφησης συνδυάζουν το μήνυμα και το κλειδί κρυπτογράφησης για να παράγουν ένα κρυπτογραφημένο αποτέλεσμα. Αν δεν γνωρίζει ο παραλήπτης το μυστικό κλειδί, το αποτέλεσμα δεν σημαίνει τίποτε.

3.10.2 Ακεραιότητα Δεδομένων – Data Integrity

Όταν μιλάμε για ακεραιότητα δεδομένων εννοούμε την δυνατότητα εντοπισμού παραποίησης και ανάκτησης δεδομένων. Για την προστασία της εγκυρότητας των δεδομένων εκτός της κρυπτογράφησης, χρησιμοποιούνται μηχανισμοί δημιουργίας συνοψίσεων μηνυμάτων (message digests) και ψηφιακών υπογραφών (digital signatures).

3.10.3 Ψηφιακές Υπογραφές – Digital Signatures

Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφοροποίηση από την κρυπτογράφηση, έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

3.10.4 Έλεγχος Προσπέλασης και Εξουσιοδότηση – Access Control and Authorization

Ο έλεγχος προσπέλασης θα μπορούσαμε να πούμε ότι έχει δύο πλευρές:
Η πρώτη είναι ότι είναι επιθυμητό να μην επιτρέπεται η προσπέλαση δεδομένων από αυτούς που δεν έχουν το δικαίωμα να το κάνουνκαι η δεύτερη, εξίσου σημαντική, είναι η ανάγκη να είναι εγγυημένη η δυνατότητα προσπέλασης όλων των σχετικών δεδομένων από τους χρήστες που εφαρμόζουν κατάλληλα τα δικαιώματα προσπέλασης που τους ανήκουν.

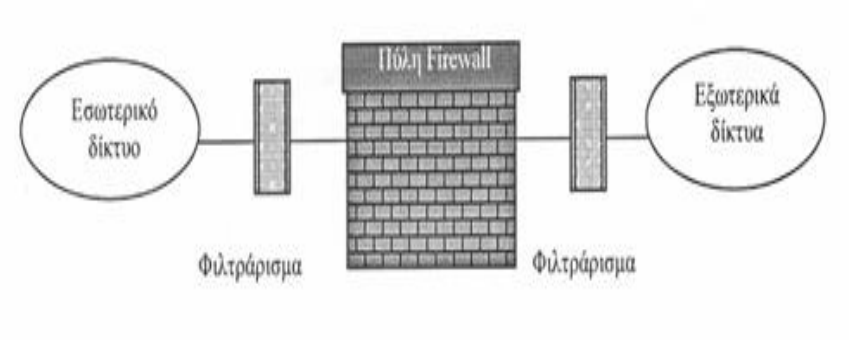
Υπάρχει μεγάλη ποικιλία όσων αφορά τον τρόπο και την τεχνική που μπορεί κανείς να εξασφαλίσει άρτιο έλεγχο στην προσπέλαση των δεδομένων που διακινούνται μέσω ενός δικτύου. Οι πιο σημαντικές μέθοδοι είναι:

- Λίστες Ελέγχου Προσπέλασης – Access Control Lists ACLs
- Ταυτότητες Ασφαλείας – Security Labels
- Firewalls
- Ψηφιακές Υπογραφές – Digital Signatures

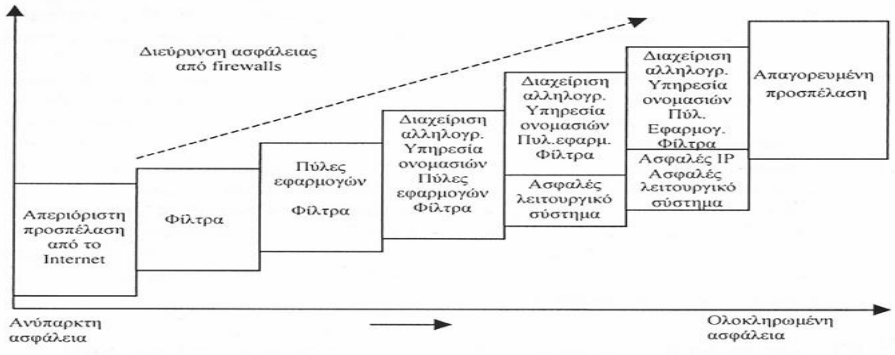
3.10.5 Firewalls

Γενικά η λέξη firewall αποδίδεται σε πυρίμαχους τοίχους που εμποδίζουν την εξάπλωση της φωτιάς από δωμάτιο σε δωμάτιο ή μεταξύ διαμερισμάτων. Στην περίπτωση των δικτύων υπολογιστών, τα firewalls αποτελούν την αναγκαία λύση προστασίας τους, καθώς αυτά συνδέονται ολοένα και περισσότερο σε μεγαλύτερα δίκτυα τα οποία επίσης είναι συνδεμένα στο διαδίκτυο.Από τη στιγμή που ένα δίκτυο αποκτήσει σύνδεση στο Internet, ανοίγει ένα κανάλι αμφίδρομης επικοινωνίας: οι χρήστες του δικτύου, insiders, αποκτούν επαφή με τον έξω κόσμο, αλλά ταυτόχρονα και οι outsiders, δηλαδή οι εξωτερικοί χρήστες ως προς αυτό το δίκτυο, αποκτούν πλέον δυνατότητα πρόσβασης σε αυτό. Ο τρομακτικός ρυθμός αύξησης του διαδικτύου, προκαλεί ανάλογη αύξηση των πιθανών κινδύνων στα ιδιωτικά δίκτυα που συνδέονται μαζί του. Για τη προστασία τους από διάφορες εισβολές απαιτείται ένας κατάλληλος φράκτης. Ο φράκτης αυτός που καλείται firewall, πρέπει να είναι ικανός να επεξεργάζεται όλη τη κυκλοφορία μηνυμάτων ανάμεσα σε ένα συγκεκριμένο τοπικό ή ιδιωτικό δίκτυο και στο Internet. Στην πραγματικότητα ένα σύστημα firewall ανορθώνει ένα εξωτερικό τοίχο ασφάλειας, οριοθετώντας μια περίμετρο προστασίας. Έτσι προκαλεί ένα σαφή διαχωρισμό ανάμεσα στο προστατευμένο-εσωτερικό δίκτυο ενός οργανισμού το οποίο θεωρείται ασφαλές και έμπιστο και στο εξωτερικό διαδίκτυο το οποίο θεωρείται μη ασφαλές και μη έμπιστο. Ο πρωταρχικός σκοπός των firewalls δηλαδή είναι να προστατεύσουν τα δίκτυα από εξωτερικούς εισβολείς, περιορίζοντας τους τα δικαιώματα προσπέλασης σε αυτό, χωρίς να περιορίζουν την προσπέλαση στον εξωτερικό περιβάλλον.Ένα σύστημα firewall ορίζεται ως το λογισμικό και ο εξοπλισμός που τοποθετούμενος ανάμεσα στο διαδίκτυο και στο υπό προστασία δίκτυο, επιτρέπει την προσπέλαση των εξωτερικών χρηστών στο προστατευμένο δίκτυο,

μόνο εφόσον διαθέτουν συγκεκριμένα χαρακτηριστικά. Έτσι ένα τυπικό σύστημα firewall μπορεί να επιτρέπει επιλεκτικά τη πρόσβαση στους εξωτερικούς χρήστες, βασιζόμενο σε ονόματα χρηστών και συνθηματικά ή σε IP διευθύνσεις ή ακόμη και σε ονόματα επικρατειών (domain names). Ο κύριος σκοπός του δηλαδή είναι να κρατήσει τις επικίνδυνες δραστηριότητες μακριά από το προστατευμένο περιβάλλον.Ένα firewall μπορεί να θεωρηθεί σαν ένα ζευγάρι μηχανισμών που ο ένας μπλοκάρει τη κυκλοφορία των δεδομένων και ο άλλος επιτρέπει τη ροή τους. Το ποια δεδομένα επιτρέπονται και ποια απορρίπτονται είναι ζήτημα της πολιτικής ελέγχου που υποστηρίζει και εξαρτάται από την συγκεκριμένη διαμόρφωσή του. Ένα σύστημα firewall δεν είναι απλά και μόνο ένας δρομολογητής, ένας διανομέας ή διακομιστής, ένας οικοδεσπότης ή ένα σύνολο εξοπλισμού και λογισμικού που παρέχει ασφάλεια στα δίκτυα. Οι αληθινές δυνατότητές του γίνονται εμφανείς αν τον θεωρήσουμε ως ένα ισχυρό μέσο υλοποίησης μιας πολιτικής ασφάλειας που καθορίζει τις παρεχόμενες υπηρεσίες και τις επιτρεπτές προσπελάσεις ανάμεσα σε έμπιστες και μη έμπιστες επικράτειες. Η υλοποίηση της πολιτικής ελέγχου προσπέλασης δικτύων γίνεται με την υποχρεωτική κατεύθυνση όλων των επικοινωνιών μέσω του firewall, ώστε να αποτελούν αντικείμενο για παραπέρα εξέταση και καταγραφή από αυτό.Μια τυπική διάταξη firewalls παρουσιάζεται στην ακόλουθη εικόνα:



Γράφημα 2 : τυπική διάταξη firewalls



Γράφημα 3 : Ασφάλεια σε firewall

Κεφάλαιο 4ο

4.1 Ηλεκτρονικό Έγκλημα

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής καθώς και το Διαδίκτυο έχουν επιφέρει πρωτόγνωρες αλλαγές στην παραγωγική διαδικασία, στις εργασιακές σχέσεις, στις συναλλαγές και σε κάθε έκφανση της καθημερινότητας και της ανθρώπινης επαφής. Μαζί όμως με τις αλλαγές αυτές που διευκολύνουν, προάγουν και βοηθούν στην καλυτέρευση της ποιότητας ζωής και στην τάχιστη εξυπηρέτηση των αναγκών που δημιουργεί η σύγχρονη κοινωνίας, οι νέες τεχνολογίες και το Ίντερνετ διευκόλυναν και δημιούργησαν ιδανικές συνθήκες για την καλλιέργεια και ανάπτυξη νέων μορφών εγκληματικότητας που συνοψίζονται στον όρο Ηλεκτρονικό έγκλημα. Ο **όρος Ηλεκτρονικό έγκλημα** 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. Οι μορφές του Ηλεκτρονικού εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του διαδικτύου πολλαπλασιάζονται. Για την αντιμετώπιση του κινδύνου αυτού ήταν απαραίτητη η συνεννόηση μεταξύ των κρατών και η εκπόνηση μιας αναλυτικής και αποτελεσματική στρατηγικής. Ο σκοπός αυτός επετέθη με το Συνέδριο για το Ηλεκτρονικό έγκλημα (Convention on Cybercrime), του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στην συνθήκη που υπογράφει στην Βουδαπέστη στις 23.11.2001.

Στη συνθήκη της Βουδαπέστη, που υπέγραψε μεταξύ πολλών άλλων χωρών και η Ελλάδα υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα ηλεκτρονικά εγκλήματα:

1. Για τα αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων ηλεκτρονικών υπολογιστών. Τέτοια αδικήματα είναι η παράνομη πρόσβαση, η παράνομη υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών.

2. Για τα αδικήματα που σχετίζονται με τους υπολογιστές όπως η απάτη με ηλεκτρονικό υπολογιστή και η πλαστογραφία.

3. Για τα αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας.

4. Για τα αδικήματα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας.

Επίσης η συνθήκη περιέχει ρυθμίσεις για την συνεργεία, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων καθώς και την ευθύνη των επιχειρήσεων. Ακόμα τονίζει την αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγει το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά. Η

συνθήκη αυτή αποτελεί το πιο άρτιο κείμενο σχετικά με το ηλεκτρονικό κείμενο στην Ευρωπαϊκή ένωση. Υπάρχουν φυσικά και άλλα γενικά νομοθετήματα που βοηθούν στην καταπολέμηση του Ηλεκτρονικού εγκλήματος.

Στην Ευρωπαϊκή Ένωση ισχύουν:

1. Η Σύσταση του Συμβουλίου με αριθμό 9193/01, με την οποία καλούνται τα κράτη μέλη να συμμετάσχουν στο δίκτυο πληροφόρησης της Ομάδας των Οκτώ, το οποίο λειτουργεί 24 ώρες το εικοσιτετράωρο, για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας.

2. Το Ψήφισμα του Συμβουλίου με αριθμό 2003/ C 48/01, για την ασφάλεια των δικτύων και των πληροφοριών.

3. Η Σύσταση του Συμβουλίου με αριθμό 95/144/ΕΚ, όπου αναφέρονται οι προτροπές του Συμβουλίου σχετικά με την ασφάλεια των συστημάτων πληροφορικής.

4. Η Κοινή θέση της 27ης Μαΐου 1999 (1999/364/ΔΕΥ), όπου τα κράτη μέλη υποστηρίζουν την κατάρτιση του σχεδίου σύμβασης του Συμβουλίου της Ευρώπης σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και ότι φροντίζουν ώστε να περιληφθούν στη σύμβαση διατάξεις που θα διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων που άπτονται των ηλεκτρονικών συστημάτων και δεδομένων.

5. Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 43/02 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων.

6. Το έγγραφο με αριθμό 2000/C 124/01 σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την πρόληψη και τον έλεγχο του οργανωμένου εγκλήματος. Στο έγγραφο αυτό αναλύονται διεξοδικά τα μέτρα που πρέπει να ληφθούν για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος όπου εντάσσονται και πολλές μορφές του ηλεκτρονικού εγκλήματος.

7. Το Σχέδιο Δράσης με αριθμό 97/C 251/01 για την καταπολέμηση του οργανωμένου εγκλήματος.

Στην Ελλάδα ισχύει ο νόμος 2928 του 2001 για την προστασία του πολίτη από αξιόποινες πράξεις εγκληματικών οργανώσεων.

4.2 Μορφές Ηλεκτρονικού Εγκλήματος

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:

4.2.1 Κυβερνοσφετερισμός – Προστασία των Domain Names

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

4.2.2 Παράνομη Διείσδυση σε Δεδομένα

Hacking αποτελεί η μη εξουσιοδοτημένη πρόσβαση σε ξένο υπολογιστή ή συστήματα υπολογιστών η οποία καταρχήν δε γίνεται με το σκοπό της υποκλοπής, της καταστροφής ή της κατασκοπείας αλλά για την ικανοποίηση από την επιτυχία παράκαμψης των συστημάτων ασφαλείας των ηλεκτρονικών υπολογιστών.

4.2.3 Cracking

Είναι η αλλαγή των κωδίκων πρόσβασης και η άρση της προστασίας των προγραμμάτων, η οποία καθιστά δυνατή την παράνομη αντιγραφή τους.Η χωρίς δικαίωμα διείσδυση – πρόσβαση σε συστήματα επεξεργασίας δεδομένων έστω και όταν γίνεται χωρίς πρόθεση βλάβης τιμωρείται με το άρθρο 370Γ του Ποινικού κώδικα.
Στην Ευρωπαϊκή Ένωση δεν έχουν ακόμα ψηφιστεί ειδικά νομοθετήματα για την αντιμετώπιση του hacking αλλά έχουν ήδη αρχίσει οι προπαρασκευαστικές εργασίες για την δημιουργία τους. Τέτοια είναι:
1.Η Ανακοίνωση της Επιτροπής με αριθμό COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά για τη μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών, μνεία στις ζημιές που μπορούν να προκληθούν και παράθεση πιθανών λύσεων.
2. Πρόταση Κανονισμού με αριθμό 2003.0063 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών στόχος του οποίου θα είναι να διευκολύνει την εφαρμογή των κοινοτικών μέτρων σχετικά με την ασφάλεια δικτύων και πληροφοριών και να συμβάλλει στη διασφάλιση της διαλειτουργικότητας των λειτουργιών ασφαλείας στα δίκτυα και τα συστήματα πληροφοριών.
3. Πρόταση Απόφασης Πλαισίου του Συμβουλίου με αριθμό COM/2002/0173-CNS 2002/0086 για τις επιθέσεις κατά των συστημάτων πληροφοριών όπου στοιχειοθετείται το αδίκημα της επίθεσης μέσω παράνομης πρόσβασης σε συστήματα πληροφοριών και γίνεται αναλυτική αναφορά στο τι αποτελεί παράνομη παρεμβολή σε συστήματα πληροφοριών.

4.2.4 Προστασία των δεδομένων από ιούς

Μια επικίνδυνη μορφή εγκληματικότητας που εμφανίζεται στο διαδίκτυο είναι η αλλοίωση ή διαγραφή των δεδομένων με ιούς. Οι ιοί των υπολογιστών, όπως είδαμε και σε προηγούμενο κεφάλαιο, είναι ειδικά προγράμματα που έχουν την ικανότητα να ανατυπώνονται από μόνα τους. Διακρίνονται σε δύο μορφές: στους ιούς των προγραμμάτων και στους ιούς των συστημάτων. Η παρεμβολή ιών στο πρόγραμμα ενός υπολογιστή γεννά την αστική ευθύνη του προμηθευτή και κάθε υπαιτίου και τη συμβατική ευθύνη του προμηθευτή του προγράμματος εφόσον υπάρχει πώληση προγράμματος. Σε αυτές τις περιπτώσεις εφαρμόζονται τα άρθρα 577 και 578 του ΑΚ. Επίσης γεννά και αδικοπρακτική ευθύνη του δράστη κατά τα άρθρα 914, 919 ΑΚ. Ο υπαίτιος όμως υπέχει και ποινική ευθύνη σύμφωνα με το άρθρο 381 ΠΚ.
Στην Ευρωπαϊκή Ένωση υπάρχει η Ανακοίνωση της Επιτροπής με αριθμό COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά και λεπτομερής επεξήγηση της έννοιας του ιού, του τρόπου που λειτουργεί και των τρόπων αντιμετώπισης του. Το νομοθέτημα αυτό δεν έχει ακόμα ψηφιστεί ώστε να ισχύει.

4.2.5 Προστασία Δεδομένων Προσωπικού Χαρακτήρα

Η ανάπτυξη των νέων τεχνολογιών και οι νέες μορφές διαφήμισης και ηλεκτρονικών συναλλαγών οδήγησαν στην αυξημένη ζήτηση προσωπικών πληροφοριών από τον ιδιωτικό και δημόσιο τομέα. Οι προσωπικές αυτές πληροφορίες που αναφέρονται σε κάθε είδους δραστηριότητα προσωπική είτε επαγγελματική του ατόμου ονομάζονται προσωπικά δεδομέναΠροσωπικά δεδομένα είναι, σύμφωνα με τον *Νόμο 2472/1997* και την *Οδηγία 95/46/ΕΚ* κάθε πληροφορία που αναφέρεται στο πρόσωπό του κάθε ατόμου, π.χ. το όνομα και το επάγγελμά του ατόμου, η οικογενειακή του κατάσταση, η ηλικία του, ο τόπος κατοικίας, η φυλετική του προέλευση, τα πολιτικά του φρονήματα, η θρησκεία που πιστεύει, οι φιλοσοφικές του απόψεις, η συνδικαλιστική του δράση, η υγεία του, η ερωτική του ζωή και οι τυχόν ποινικές του διώξεις και καταδίκες.Για την επεξεργασία και συλλογή προσωπικών δεδομένων είναι απαραίτητη άδεια από την Αρχή Προστασίας Προσωπικών Δεδομένων. Οι οδηγίες για την χορήγηση άδειας επεξεργασίας αναλύονται στην *Κανονιστική Πράξη 1/1999 ΑΠΠΔ* σχετικά με την ενημέρωση υποκειμένου των δεδομένων *κατ" άρθρο 11 Ν. 2472/1997* και στην *Απόφαση 408.1998 ΑΠΠΔ* σχετικά με την ενημέρωση υποκειμένων επεξεργασίας δεδομένων προσωπικού χαρακτήρα δια του τύπου.Η συγκέντρωση και επεξεργασία δεδομένων προσωπικού χαρακτήρα αποτελεί έναν από τους μεγαλύτερους κινδύνους επέμβασης στην προσωπική σφαίρα και στην ιδιωτική ζωή του ατόμου. Κάθε δραστηριότητα του σύγχρονου ανθρώπου γίνεται καθημερινά αντικείμενο επεξεργασίας και ανάλυσης γεγονός που χρήζει αντιμετώπισης και νομική κατοχύρωσης.Η συγκέντρωση και επεξεργασία ηλεκτρονικών δεδομένων αντιμετωπίστηκε από πολύ νωρίς ως ένας από τους μεγαλύτερους κινδύνους επέμβασης στην ιδιωτική και προσωπική σφαίρα. Τόσο στην Ελλάδα όσο και στην Ευρωπαϊκή Ένωση υπάρχει νομοθεσία που ρυθμίζει τα σχετικά με την επεξεργασίας δεδομένων όπως η Οδηγία 2002/58

σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και η Οδηγία 95/46 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού.

4.2.6 Απάτη μέσω του Διαδικτύου

Από τη σκοπιά του ποινικού δικαίου κατά τη χρήση του Διαδικτύου είναι δυνατό να τελεστούν απάτες μέσω υπολογιστή όπου ο υπολογιστής είναι απλώς το μέσω τέλεσης της κοινής απάτης (ΠΚ 386) αλλά και απάτες με υπολογιστή όπου το οικονομικό όφελος ή η 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.

4.2.7 Spamming

Το μεγαλύτερο πρόβλημα που αφορά στις διαδικτυακές διαφημίσεις είναι το λεγόμενο spamming, δηλαδή η αποστολή πολυάριθμων e-mails με διαφημιστικό περιεχόμενο σε χιλιάδες καταναλωτές-χρήστες του διαδικτύου. Η τακτική αυτή απαγορεύεται από την Οδηγία 2002.58 όπου στο άρθρο 13 αναφέρεται ότι «η χρησιμοποίηση αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση (συσκευές αυτόματων κλήσεων), τυλεομοιοτυπικών 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» καθώς και από άλλα νομοθετήματα.Στην Ελλάδα υπάρχουν πολλά νομοθετήματα για την προστασία των καταναλωτών αλλά αναφέρονται στα μηνύματα μέσω τηλεφώνου και φαξ κυρίως και μόνο αναλογικά στο ηλεκτρονικό ταχυδρομείο.

4.3 Προστασία της Πνευματικής Ιδιοκτησίας

Η μετάβαση από τη βιομηχανική κοινωνία στη λεγόμενη κοινωνία των πληροφοριών, της ψηφιακής τεχνολογίας και επικοινωνίας προκαλεί βαθιές επικοινωνιακές , πολιτισμικές και οικονομικές αλλαγές. Η αξία και η οικονομική σημασία των άυλων αγαθών και των πληροφοριών έχει πολλαπλασιασθεί σε μια κοινωνία της οποίας η οικονομία και η επικοινωνία έχει διεθνοποιηθεί. Η πνευματική ιδιοκτησία παρέχει την κινητήρια δύναμη στην κοινωνία της διασκέδασης και της παγκόσμιας επικοινωνίας.

Πνευματική ιδιοκτησία ονομάζεται το δικαίωμα που η έννομη τάξη απονέμει στον δημιουργό ενός πνευματικού έργου πάνω στον έργο αυτό. Πνευματικός δημιουργός είναι εκείνος που δημιουργεί νέες μορφές και ιδέες έστω και αν ενσωματώνει τα δημιουργήματά του σε ύλη που προϋπήρχε.

Η πνευματική ιδιοκτησία παρουσιάζει τρεις ιδιομορφίες.

Η πρώτη είναι ότι το αντικείμενό της είναι άυλο δηλαδή είναι το πνευματικό δημιούργημα και όχι το υλικό αντικείμενο πάνω στο οποίο το δημιούργημα έχει ενσωματωθεί. Ο άυλος χαρακτήρας του αντικειμένου της πνευματικής ιδιοκτησίας επιτρέπει τη σύγχρονη παρουσία του έργου σε άπειρους τόπους.**Η δεύτερη ιδιομορφία είναι** ότι η πνευματική ιδιοκτησία δεν προστατεύει μόνο περιουσιακά το δημιουργού σε σχέση με το έργο του αλλά και συμφέροντα που ανάγονται στη σφαίρα της προσωπικότητας του δημιουργού, δηλαδή στην ιδιαίτερη ηθική σχέση του κάθε δημιουργού με το δημιούργημά του. Έτσι η πνευματική ιδιοκτησία έχει ένα μικτό χαρακτήρα προσωπικό και περιουσιακό που προκαλεί περίεργες διχοτομήσεις του δικαιώματος, ιδίως σε ότι αφορά τη δυνατότητα μεταβίβασής του.**Η τρίτη ιδιομορφία της** πνευματικής ιδιοκτησίας προκαλείται από το γεγονός ότι κάθε πνευματικό δημιούργημα είναι μοναδικό και ανεπανάληπτο. Ο πνευματικός δημιουργός έχει μια θέση μονοπωλιακή αναφορικά με το κάθε δημιούργημά του.

4.3.1 Το δίκαιο της Πνευματικής ιδιοκτησίας σε σχέση με την κοινωνία των πληροφοριών και το Internet

Την κύρια πηγή του δικαίου της πνευματικής ιδιοκτησίας στην Ελλάδα αποτελεί ο Νόμος 2121/1993 με τίτλο «Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα» όπως τροποποιήθηκε από τον Νόμο 3057/2002. Με την έναρξη της ισχύος αυτού του νόμου όλοι σχεδόν οι προγενέστεροι νόμοι που αφορούσαν την πνευματική ιδιοκτησία καταργήθηκαν. Στον νόμο αυτόν περιέχονται μεταξύ άλλων και διατάξεις σχετικές με τα προγράμματα ηλεκτρονικών υπολογιστών και τις βάσεις δεδομένων και φωτογραφιών. Ανάλογες διατάξεις περιλαμβάνονται και στη συνθήκη του Παγκόσμιου Οργανισμού Διανοητικής Ιδιοκτησίας για την πνευματική ιδιοκτησία που κυρώθηκε με τον Νόμο 3184/2003. Επίσης ισχύει και η Συνθήκη του Παγκόσμιου Οργανισμού Διανοητικής Ιδιοκτησίας για τις εκτελέσεις και τα φωνογραφήματα, που κυρώθηκε με τον Νόμο 3183/2003. Σημαντική αρωγή στην προστασία των πνευματικών δικαιωμάτων προσφέρουν η Επιτροπή Ανταγωνισμού, που με σχετικές αποφάσεις της (π.χ. 245/ΙΙΙ.2003 σχετικά με την καταγγελία μουσικοσυνθετών κατά της «ΑΕΠΙ») βοηθά στην διασφάλιση των δικαιωμάτων πνευματικής ιδιοκτησίας, αλλά και οργανισμοί που ως σκοπό λειτουργίας τους έχουν τη διαχείριση πνευματικών δικαιωμάτων (ΥΑ 2170/2003).Η Ελληνική Νομολογία ενισχύει και αυτή με τη σειρά της την μάχη κατά της παραβίασης δικαιωμάτων πνευματικής ιδιοκτησίας, αν και κυρίως εστιάζεται σε θέματα συλλογικής διαχείρισης πνευματικών δικαιωμάτων (π.χ. 687/2003 Απόφαση Μονομελούς Πρωτοδικείου Τρικάλων) και ραδιοτηλεοπτικής φύσεως διενέξεων (π.χ. 1404/2002 Απόφαση του Συμβουλίου της Επικρατείας).Στην Ευρώπη ισχύει η Οδηγία 93/98 περί εναρμονίσεως της διάρκειας προστασίας του δικαιώματος πνευματικής ιδιοκτησίας και ορισμένων συγγενών δικαιωμάτων καθώς και η Οδηγία 2001/29 για την εναρμόνιση ορισμένων πτυχών του δικαιώματος του δημιουργού και συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας. Σχετικά με την πνευματική ιδιοκτησία στην κοινωνία των πληροφοριών υπάρχουν πληθώρα αποφάσεων νομολογίας που αναφέρονται τόσο σε προϊόντα λογισμικού δηλαδή προγράμματα ηλεκτρονικών υπολογιστών όσο και σε παράνομη αναπαραγωγή και ανταλλαγή δεδομένων και αρχείων μέσω του Internet

που καταπατούν δικαιώματα πνευματικής ιδιοκτησίας των δημιουργών τους.Η εμφάνιση των βάσεων δεδομένων σε συνδυασμό με τη διάδοση του Διαδικτύου έχει κάνει την αντιγραφή και την ηλεκτρονική διάδοση των πνευματικών δημιουργημάτων αποτελεσματική και εξαιρετικά απλή. Με τον τρόπο αυτό όμως καταστρατηγούνται τα δικαιώματα της πνευματικής ιδιοκτησίας των δημιουργών πάνω στα δημιουργήματά τους.Τα δικαιώματα πνευματικής ιδιοκτησίας λοιπόν καθώς και η κατοχύρωση και προστασία τους αποτελούν απαραίτητη προϋπόθεση ανάπτυξης του πολιτισμού γενικότερα αλλά και κάθε επιχείρησης μεμονωμένα.

4.4 Δικαιοδοσία στο Διαδίκτυο

Το πρόβλημα της δικαιοδοσίας στα εγκλήματα που τελούνται στο Διαδίκτυο δεν είναι απλό καθώς το Διαδίκτυο λόγω της παγκοσμιότητάς του επιτρέπει στον οποιοδήποτε να εισάγει και να καταστήσει προσβάσιμη από όλα τα σημεία του πλανήτη οποιαδήποτε πληροφορία θελήσει.Για την ανεύρεση της αρμοδιότητας του δικαστηρίου πρέπει να καθοριστεί ο τόπος τέλεσης του αδικήματος. Για τον καθορισμό του τόπου τελέσεως του αδικήματος υποστηρίζονται τέσσερις θεωρίες.

Α) Η θεωρία του τόπου ενέργειας, σύμφωνα με την οποία ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου ετελέσθη η ενέργεια που έτεινε στο άδικο αποτέλεσμα και αν η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, ο τόπος όπου ολοκληρώθηκε.

Β) Η θεωρία του τόπου του αποτελέσματος, όπου ως τόπος τελέσεως του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.

Γ) Η μικτή θεωρία, όπου ως τόπος τελέσεως του αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.

Δ) Η θεωρία του βαρύνοντος τόπου, σύμφωνα με την οποία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Βέβαια υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας δεδομένου ότι είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας. Η κρατούσα θεωρία στην Ελλάδα και στην Ευρώπη είναι η θεωρία του βαρύνοντος τόπου.Μέσω της δυναμικής εισβολής του ηλεκτρονικού υπολογιστή και της λειτουργίας του Διαδικτύου αναπτύσσονται αναρίθμητες δυνατότητες χρήσης και κατάχρησης που αφορούν την ηλεκτρονική επεξεργασία δεδομένων. Η ηλεκτρονική εγκληματικότητα συνεχώς εμπλουτίζεται με νέες εκφάνσεις και καθίσταται σαφές ότι μεμονωμένες προσπάθειες εκ μέρους του νομοθέτη ή των ιδιωτών δεν αρκούν για να δώσουν λύσεις. Για την καταπολέμηση της ηλεκτρονικής εγκληματικότητας απαιτείται συνεργασία μεταξύ όλων των κρατών όπως αναφέρεται σε πολλά νομοθετικά κείμενα.

4.5 Δίκτυα Υπολογιστών και Νομοθεσία

Η ασφάλεια των πληροφοριακών συστημάτων και ειδικότερα των δικτύων υπολογιστών μιας επιχείρησης είναι μία υποχρέωση που δεν αφορά μόνο την προστασία της επιχείρησης, αλλά και την προστασία των προσώπων, στοιχεία των οποίων έχουν καταχωριστεί στα συστήματα αυτά.Ήδη ο νόμος 2472/97 (άρθρο 10) έχει επιβάλει υποχρεώσεις προστασίας της εμπιστευτικότητας – μυστικότητας των πληροφοριών και λήψης μέτρων ασφαλείας. Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει όλα 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. Τα μέτρα ασφαλείας που λαμβάνονται θα πρέπει να είναι ανάλογα προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Στις υποχρεώσεις μιας επιχείρησης περιλαμβάνεται η επιλογή συνεργατών που διαθέτουν όχι μόνο τεχνικές γνώσεις αλλά και προσωπική ακεραιότητα που διασφαλίζει την τήρηση του απορρήτου της επεξεργασίας.Η Αρχή Προστασίας Προσωπικών Δεδομένων, όπως θα δούμε και στην συνέχεια, αποδίδει ιδιαίτερη σημασία στην εκπόνηση σχεδίου Ασφαλείας (security plan) και έκτακτης ανάγκης από τον υπεύθυνο επεξεργασίας, αλλά και στη συνεχή αναθεώρηση των σχεδίων αυτών ώστε να ανταποκρίνεται στις τεχνολογικές εξελίξεις. Συχνά μάλιστα οι άδειες επεξεργασίας ευαίσθητων δεδομένων συνοδεύονται από την επιβολή όρων ασφαλείας των δεδομένων και την υποχρέωση επεξεργασίας τέτοιων σχεδίων. Χωρίς να υπεισέρχεται σε λεπτομέρειες, η Αρχή Προστασίας Προσωπικών Δεδομένων έχει συντάξει ένα κείμενο οδηγιών, όπου αναφέρεται το βασικό περιεχόμενο των σχεδίων ασφαλείας και εκτάκτου ανάγκης, ώστε αυτά να κρίνονται επαρκή από την άποψη της προστασίας της εμπιστευτικότητας.

4.6 Αρχές Προστασίας Δεδομένων στα Δίκτυα Υπολογιστών

Η συγκέντρωση και επεξεργασία ηλεκτρονικών και μη δεδομένων αντιμετωπίστηκε από νωρίς και συνεχίζει να αντιμετωπίζεται ως ένας από τους μεγαλύτερους κινδύνους επέμβασης στην ιδιωτική ζωή. Η υπάρχουσα νομοθεσία παρέχει επαρκή προστασία στους πολίτες αλλά με την πάροδο του χρόνου και την περαιτέρω ανάπτυξη της τεχνολογίας χρειάζονται ειδικότερες διατάξεις που θα αντικαταστήσουν τις γενικές και από τις οποίες θα προκύπτει με σαφήνεια ποιος, πότε ακριβώς, σε ποια δεδομένα και με ποιο σκοπό θα έχει δικαίωμα πρόσβασης και επεξεργασίας. Στην προσπάθεια του Ελληνικού κράτους για εξασφάλιση υψηλού βαθμού εμπιστευτικότητας των πολιτών στις νέες τεχνολογίες επικοινωνιών είτε μέσω υπολογιστών είτε μέσω άλλων τηλεπικοινωνιακών μέσων, έχουν ιδρυθεί δύο αρχές προστασίας που σχετίζονται με τα προσωπικά δεδομένα, η Αρχή Προστασίας Προσωπικών Δεδομένων και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών.

4.6.1 Αρχή Προστασίας Προσωπικών Δεδομένων

Για την αμεσότερη και ταχύτερη προστασία των πολιτών από την επεξεργασία προσωπικών δεδομένων θεωρήθηκε αναγκαία η ίδρυση μιας Αρχής που θα εποπτεύει και θα ασχολείται αποκλειστικά με αυτό το αντικείμενο. Η αρχή αυτή, που ιδρύθηκε το 1997 και ονομάστηκε Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΠΔ) έχει ποικίλες αρμοδιότητες μεταξύ των οποίων είναι να εκδίδει οδηγίες και αποφάσεις και να γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα. Οι σημαντικότερες Οδηγίες της ΑΠΠΔ είναι :

- Η *Οδηγία 1122.2000* για τα κλειστά κυκλώματα τηλεόρασης και
- Η *Οδηγία 115/2001* για την επεξεργασία δεδομένων των εργαζομένων όπου επειδή αποτελεί και την ουσία της συγκεκριμένης εργασίας παρατίθεται στο Παράρτημα Α.

Οι σπουδαιότερες αποφάσεις της ΑΠΠΔ, που έχουν φυσικά συνάφεια με το αντικείμενο της συγκεκριμένης εργασίας, είναι οι εξής:

- Η *Απόφαση 50/2000* σχετικά με τους όρους για την νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης και της διαπίστωσης πιστοληπτικής ικανότητας.
- Η *Απόφαση 120/2001* για την επεξεργασία Προσωπικών Δεδομένων σχετικά την παροχή υπηρεσιών καρτοκινητής τηλεφωνίας
- Η *Απόφαση 1469.2000* για τη συλλογή προσωπικών δεδομένων από εταιρείες τηλεπικοινωνιακών δραστηριοτήτων.
- Η *Απόφαση 147/2001* για την χρήση ευαίσθητων δεδομένων ενώπιον δικαστηρίου
- Η *Απόφαση 8/2003* σχετικά με την πρόσβαση τρίτου σε δεδομένα εταιρείας κινητής τηλεφωνίας για άσκηση δικαιώματος υπεράσπισης ενώπιον δικαστηρίου.

Οι πιο άξιες προσοχής, τέλος, γνωμοδοτήσεις της ΑΠΠΔ είναι:

- Η *Γνωμοδότηση 71/2002* σχετικά με την επεξεργασία προσωπικών δεδομένων στην αυτόματη αναγνώριση της ταυτότητας του συνδρομητή καλούσας γραμμής σε ψηφιακά δίκτυα ενοποιημένων υπηρεσιών (ISDN),
- Η *Γνωμοδότηση 78/2002* για τις προϋποθέσεις διασταύρωσης προσωπικών δεδομένων στο χώρο της σταθερής τηλεφωνίας,
- Η *Γνωμοδότηση 86/2001* σχετικά με την είσοδο και παραμονή αλλοδαπών στην ελληνική επικράτεια,
- Η *Γνωμοδότηση 15/2001* σχετικά με την ανάλυση γενετικού υλικού για σκοπούς εξιχνίασης εγκλημάτων και ποινικής δίωξης.

4.6.2 Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) προβλέπεται από το Ν.3115/2003. Είναι ανεξάρτητη αρχή με διοικητική αυτοτέλεια και έχει ως σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης και επικοινωνίας με οποιονδήποτε άλλο τρόπο. Στο πλαίσιο αυτό, η Α.Δ.Α.Ε. είναι η αρμόδια αρχή για τον έλεγχο της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου. Η δράση της διέπεται πάντοτε από τις αρχές της διαφάνειας, της αντικειμενικότητας και της αμεροληψίας.Η Α.Δ.Α.Ε. αποτελείται από 7 μέλη και ισάριθμα αναπληρωματικά, τα οποία απολαμβάνουν κατά την άσκηση των καθηκόντων τους πλήρη προσωπική και λειτουργική ανεξαρτησία. Ωστόσο, έχουν καθήκον εχεμύθειας, το οποίο υφίσταται και μετά την αποχώρησή τους. Τα πρόσωπα που θα γίνουν μέλη της Α.Δ.Α.Ε. επιλέγονται από τη Βουλή και πρέπει να τυγχάνουν ευρείας κοινωνικής αποδοχής και να διακρίνονται για την επιστημονική τους κατάρτιση και την επαγγελματική τους ικανότητα στο νομικό τομέα ή στον τεχνικό τομέα των επικοινωνιών.

4.6.2.1 Αρμοδιότητες της Α.Δ.Α.Ε

Η Α.Δ.Α.Ε. στο πλαίσιο εκπλήρωσης του σκοπού της, μπορεί:

- Να διενεργεί αυτεπαγγέλτως ή έπειτα από καταγγελία τακτικούς ή έκτακτους ελέγχους σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών, άλλων δημόσιων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημόσιου τομέα και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία.
- Να καλεί σε ακρόαση τις διοικήσεις, τους νόμιμους εκπροσώπους και τους υπαλλήλους των ως άνω δημοσίων υπηρεσιών ή ιδιωτικών εταιριών.
- Να συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών και με ευρωπαϊκούς ή διεθνείς οργανισμούς.
- Να γνωμοδοτεί και να απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών, καθώς και για τη διαδικασία άρσης αυτού.

Τα μέλη και το προσωπικό της Α.Δ.Α.Ε., για να διαπιστώσουν παράβαση της νομοθεσίας για την προστασία του απορρήτου, μπορούν να ελέγχουν τα βιβλία και στοιχεία των ελεγχόμενων υπηρεσιών, οργανισμών και επιχειρήσεων, καθώς και πάσης φύσεως αρχεία, βιβλία, στοιχεία και λοιπά έγγραφα των προσώπων που ελέγχουν. Επιπλέον, έχουν δικαίωμα να ενεργούν έρευνες στα γραφεία και τις λοιπές εγκαταστάσεις των ελεγχομένων και να διενεργούν ένορκες και μη καταθέσεις, με την επιφύλαξη του επαγγελματικού απορρήτου των εξεταζόμενων προσώπων.Σε περίπτωση που κατά τον έλεγχο διαπιστωθεί παραβίαση του απορρήτου, τα μέλη της Α.Δ.Α.Ε. μπορούν να κατασχέσουν τα μέσα με τα οποία πραγματοποιείται η παραβίαση αυτή, ενώ παράλληλα καταστρέφουν τις πληροφορίες, τα δεδομένα ή τα στοιχεία που αποκτήθηκαν με παράνομη

παραβίαση του απορρήτου των επικοινωνιών. Για τα μέσα που κατάσχονται, ορίζεται μεσεγγυούχος ωσότου αποφανθούν τα αρμόδια δικαστήρια.

4.6.2.2 Πώς λαμβάνονται οι αποφάσεις της Α.Δ.Α.Ε.

Η Α.Δ.Α.Ε. αποφασίζει με απόλυτη πλειοψηφία των παρόντων μελών της με φανερή ψηφοφορία. Για να είναι όμως νόμιμη η συνεδρίαση, θα πρέπει να μετέχουν τουλάχιστον 3 μέλη. Οι αποφάσεις της πρέπει να είναι αιτιολογημένες, καταχωρούνται σε ειδικό βιβλίο και μπορούν να δημοσιεύονται, εφόσον δεν αφορούν στην εθνική άμυνα ή τη δημόσια ασφάλεια.Σε κάθε περίπτωση, η Α.Δ.Α.Ε. οφείλει να μην αποκαλύπτει πληροφορίες και δεδομένα για φυσικά ή νομικά πρόσωπα, τα οποία ενδέχεται να προσβάλλουν την προσωπικότητά τους ή να επηρεάσουν δυσμενώς την επαγγελματική ή την κοινωνική τους θέση, εκτός εάν προκύπτει τέτοια υποχρέωση από το νόμο.Ο πολίτης δικαιούται να υποβάλει καταγγελία προς την Α.Δ.Α.Ε., οπότε, εφόσον κριθεί αναγκαίο, η Αρχή μπορεί να τον καλέσει για να παράσχει έγγραφες ή προφορικές διευκρινίσεις. Εφόσον ο πολίτης είναι ο άμεσα ενδιαφερόμενος, έχει δικαίωμα πρόσβασης από το νόμο στους φακέλους των υποθέσεων που τον αφορούν και στα πρακτικά των αντίστοιχων συνεδριάσεων, εκτός αν οι υποθέσεις αυτές αφορούν στην εθνική άμυνα ή τη δημόσια ασφάλεια.Οι αποφάσεις της Α.Δ.Α.Ε. μπορούν να προσβληθούν δικαστικά και συγκεκριμένα κατά των εκτελεστών αποφάσεων της Α.Δ.Α.Ε. μπορεί να ασκηθεί αίτηση ακύρωσης ενώπιον του Συμβουλίου της Επικρατείας καθώς και οι προβλεπόμενες από το Σύνταγμα και τη νομοθεσία διοικητικές προσφυγές. Κατά των αποφάσεων αυτών μπορεί να ασκεί ένδικα βοηθήματα και ο υπουργός Δικαιοσύνης.

4.7 Παραβάσεις της Νομοθεσίας περί Ασφάλειας Δικτύων και Ποινές

Η τήρηση των επιταγών και απαγορεύσεων που σχετίζονται με την επεξεργασία αλλά και την ασφάλεια των προσωπικών δεδομένων επιβάλλεται από την οικεία νομοθεσία. Τυχόν παράβαση των υποχρεώσεων αυτών για προστασία και ασφάλεια των δεδομένων ενδέχεται να έχει ως αποτέλεσμα την επιβολή διοικητικών κυρώσεων από την Αρχή Προστασίας Προσωπικών Δεδομένων (όπως 11 πρόστιμα, αναστολή επεξεργασίας, καταστροφή αρχείων κλπ.) ή/και τη γέννηση αξιώσεων και υποχρεώσεων αποζημίωσης ή χρηματικής ικανοποίησης των προσώπων που θίγονται από τις παραβάσεις των νομοθετικών διατάξεων και των υποχρεώσεων ασφαλείας.Όποιος παραβιάζει με οποιονδήποτε τρόπο το απόρρητο των επικοινωνιών ή τους όρους και τη διαδικασία άρσης αυτού, τιμωρείται με ποινή φυλάκισης τουλάχιστον ενός έτους και χρηματική ποινή από 15.000 έως 60.000 ευρώ. Σε περίπτωση που ο παραβάτης ανήκει στο προσωπικό υπηρεσίας, οργανισμού, νομικού προσώπου ή επιχείρησης που ασχολείται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση ή την επικοινωνία, η επιβαλλόμενη ποινή φυλάκισης είναι τουλάχιστον 2 ετών και η χρηματική ποινή τουλάχιστον 30.000 ευρώ.Συγκεκριμένες παραβάσεις συνιστούν μάλιστα ποινικά αδικήματα και επισύρουν και ποινικές κυρώσεις. Ωστόσο, η μεγαλύτερη κύρωση είναι η

δυσπιστία των συναλλασσομένων. Πολλές πρόσφατες μελέτες έχουν αποδείξει ότι πολλοί άνθρωποι απέχουν από ηλεκτρονικές συναλλαγές από φόβο για τη μεταχείριση και την τύχη των προσωπικών τους δεδομένων. Η επένδυση σε τεχνολογίες ενίσχυσης της ιδιωτικότητας (Privacy Enhancing Technologies), η ύπαρξη, τήρηση και διαφήμιση πολιτικών για την προστασία της ιδιωτικότητας δεν είναι απλά συμμόρφωση προς το νόμο. Είναι ανταγωνιστικό πλεονέκτημα. Είναι προϋπόθεση για να αποκτηθεί η εμπιστοσύνη των καταναλωτών.Εκτός από την Ελληνική δικαιοσύνη και την Αρχή Προστασίας Προσωπικών Δεδομένων που επιβάλει κυρώσεις σε περιπτώσεις άρσης του απορρήτου στην επικοινωνία μέσω τηλεπικοινωνιακών δικτύων ή δικτύων υπολογιστών, και η Αρχή Διατήρησης της Ακεραιότητας των Επικοινωνιών μπορεί να επιβάλει στον παραβάτη διοικητικές κυρώσεις. Η απόφασή της πρέπει να είναι πλήρως αιτιολογημένη και πάντοτε ύστερα από προηγούμενη κλήτευση και ακρόαση του φερόμενου ως υπαιτίου, ο οποίος μπορεί να παραστεί μετά ή διά πληρεξουσίου δικηγόρου, εκτός αν ο Πρόεδρος της Α.Δ.Α.Ε. διατάξει την αυτοπρόσωπη παρουσία του. Οι **διοικητικές κυρώσεις** που μπορεί να επιβάλει η Αρχή είναι :

- Σύσταση για συμμόρφωση σε συγκεκριμένη διάταξη της νομοθεσίας με προειδοποίηση επιβολής κυρώσεων σε περίπτωση υποτροπής του παραβάτη, και
- Πρόστιμο από 15.000 έως 1.500.000 ευρώ.

4.8 Νομολογία για την Επεξεργασία Προσωπικών Δεδομένων

Παράλληλα με τα παραπάνω νομοθετικά κείμενα και την δραστηριότητα της Α.Π.Π.Δ. και της Α.Δ.Α.Ε. οι πολίτες που γίνονται υποκείμενα επεξεργασίας προσωπικών δεδομένων προστατεύονται όπως αναφέραμε και από τα δικαστήρια. Πληθώρα δικαστικών αποφάσεων, ελληνικών και ξένων, αναφέρονται και ρυθμίζουν κάθε είδους διαφορά που ανακύπτει σχετικά με την επεξεργασία προσωπικών δεδομένων. Μερικές από τις ελληνικές αποφάσεις είναι οι εξής:

- Η *1129.2001* του Μον.Πρωτ.Τρ. για την προστασία προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα.
- Η *1988.2002* του Μον.Πρωτ.Αθ. για την πώληση προϊόντων εξ αποστάσεως και την παράνομη αποστολή διαφημιστικών εντύπων
- Η *2950.2002* του Μον.Πρωτ.Θεσ. για την δωσιδικία νομικού προσώπου σε υπόθεση επεξεργασία δεδομένων προσωπικού χαρακτήρα
- Η *2279.2001* του ΣτΕ για την σύσταση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- Η *2286.2001* του ΣτΕ για την άσκηση αίτησης ακυρώσεως κατά πράξεως της Αρχής Προστασίας Προσωπικών Δεδομένων από Πολιτικό κόμμα.
- Η *984.2001* του Συμβουλίου Εφετών για την παράνομη γνώση, αλλοίωση και ανακοίνωση ευαίσθητων προσωπικών δεδομένων
- Η *3545/2002* του ΣτΕ για την συμμετοχή σε συνεδρίαση της Αρχής Προστασίας Προσωπικών Δεδομένων αναπληρωματικού μέλους της, στο οποίο έχουν ανατεθεί καθήκοντα εισηγητή.

Κάποιες από τις ξένες δικαστικές αποφάσεις σχετικά με τα προσωπικά δεδομένα είναι οι ακόλουθες:

- Απόφαση Αμερικανικού Δικαστηρίου για παραβίαση Ιδιωτικής Ζωής μέσω του Διαδικτύου όπου αναφέρεται ότι η παροχή συμβουλευτικών υπηρεσιών και οι κάθε είδους γραπτές αναφορές μέσω ηλεκτρονικού ταχυδρομείου (e-mail) στο κοινό δεν παρέχει το δικαίωμα ελέγχου των προσωπικών δεδομένων του παρόχου και αποκάλυψης της ηλεκτρονικής του αλληλογραφίας.
- Απόφαση Αμερικανικού Δικαστηρίου για παραβίαση Ιδιωτικής Ζωής που ρυθμίζει υπόθεση όπου ηλεκτρονικές βιβλιοθήκες χρησιμοποιήθηκαν για την παροχή πληροφοριών μέσω Internet
- Απόφαση Αμερικανικού Δικαστηρίου για παραβίαση ιδιωτικής ζωής εργαζομένου που ρυθμίζει υπόθεση όπου εργαζόμενος, ο οποίος απολύθηκε από την εταιρία που εργαζόταν διατυπώνει την επιφύλαξη του κατά πόσο η δημιουργία εσωτερικού δικτύου επικοινωνίας με τους υπόλοιπους εργαζομένους από αυτόν συνιστά παραβίαση της ιδιωτικής του σφαίρας μετά την απόλυσή του.

Κεφάλαιο 5ο

5.1 προσωπικά δεδομένα

Προσωπικά δεδομένα είναι κάθε πληροφορία που σε χαρακτηρίζει, όπως για παράδειγμα το όνομά, η διεύθυνσή, το τηλέφωνό, τα ενδιαφέροντά σου, οι φωτογραφίες σου κ.α.
Μερικές φορές τα προσωπικά δεδομένα αφορούν ιδιαίτερα ευαίσθητα στοιχεία της ιδιωτικής σου ζωής, όπως στο θρήσκευμά σου, στις πολιτικές σου πεποιθήσεις, στην κατάσταση της υγείας σου ή στην ερωτική σου ζωή.

5.2 Πότε επιτρέπεται κάποιος να χρησιμοποιεί τα προσωπικά μου δεδομένα;

Στην Ελλάδα, όπως και στις υπόλοιπες χώρες της Ευρωπαϊκής Ένωσης, υπάρχει ειδική νομοθεσία που προστατεύει τα άτομα από την ανεξέλεγκτη χρήση των προσωπικών τους δεδομένων. Η Αρχή Προστασίας Δεδομένων είναι ο αρμόδιος φορέας για την εφαρμογή αυτής της νομοθεσίας (νόμοι 2472/1997 και 3471/2006).
Ως βασικός κανόνας ισχύει ότι για να χρησιμοποιήσει κάποιος τα προσωπικά σου δεδομένα για έναν συγκεκριμένο σκοπό πρέπει να έχει εξασφαλίσει την συγκατάθεσή σου και, σε αρκετές περιπτώσεις, τη συναίνεση των γονιών σου. Με αυτό εννοούμε ότι, αφού προηγουμένως έχεις ενημερωθεί ακριβώς για το ποιος είναι αυτός που θέλει να χρησιμοποιήσει τα δεδομένα σου, για ποιον λόγο θέλει να τα χρησιμοποιήσει, ποια στοιχεία σου θέλει να πάρει και με ποιους θα τα μοιραστεί, τότε έχεις δεχθεί και έχεις πει με σαφή τρόπο ότι συμφωνείς.
Η συγκατάθεση είναι ο γενικός κανόνας, αλλά υπάρχουν και εξαιρέσεις. Για παράδειγμα κάποιοι οργανισμοί, όπως π.χ. ο δήμος ή το σχολείο σου, μπορούν να επεξεργάζονται συγκεκριμένα προσωπικά δεδομένα χωρίς τη συγκατάθεσή σου. Αυτό συμβαίνει γιατί τα δεδομένα σου είναι απαραίτητα για να εκτελέσουν το έργο τους και αυτό συνήθως ορίζεται σε κάποιο νόμο.

5.3 Ορισμοί πληροφορία, διασύνδεση αρχείων, αρχείο

Πληροφορία είναι έννομο αγαθό με αυτοτελή υπόσταση και ιδιαίτερη αξία, διακριτή σε σχέση με την έγχαρτη αξία του τυχόν εντύπου στο οποίο είναι καταγεγγραμένη.

Διασύνδεση αρχείων είναι μια μορφή επεξεργασίας προσωπικών δεδομένων κατά την οποία γίνεται συσχέτιση των δεδομένων ενός αρχείου με δεδομένα αρχείου ή αρχείων που τηρούνται από άλλον ή άλλους υπεύθυνους επεξεργασίας.

Π.χ. η διασύνδεση αρχείων κινητής τηλεφωνίας με υπηρεσίες ΕΥΠ σε εξαιρετικές περιπτώσεις και μόνο μετά από γραπτή εισαγγελική παραγγελία για εντοπισμό ή παρακολούθηση υπόπτου.
Αρχείο είναι το σύνολο δεδομένων προσωπικού χαρακτήρα που αποτελούν ή μπορεί να αποτελέσουν.
Αντικείμενο επεξεργασίας και τα οποία τηρούνται από τη Δημόσια ή από ΝΠΔΔ ή ΝΠΙΔ ή από ένωση προσώπων ή από φυσικό πρόσωπο ονομάζεται αρχείο ΔΠΧ.

5.4 Βασικές εννοιες δεδομένα, Επεξεργασία ΔΠΧ

Τα **δεδομένα** διακρίνονται :

Α) σε **απλά ΔΠΧ**
Τα **απλά ΔΠΧ** είναι κάθε πληροφορία που αφορά ένα φυσικό πρόσωπο π.χ. φύλλο, ηλικία, κατοικία.
Β) σε **ευαίσθητα ΔΠΧ**
Τα **ευαίσθητα ΔΠΧ** είναι τα δεδομένα που αφορούν την φυλετική ή εθνική προέλευση (ιθαγένεια) πολιτικά φρονήματα, θρησκευτικές πεποιθήσεις, υγεία, κοινωνική πρόνοια, ερωτική ζωή, ποινικές διώξεις ή καταδίκες.
Επεξεργασία ΔΠΧ νοείται κάθε εργασία η σειρά εργασιών που πραγματοποιείται από το Δημόσιο ή από ΑΠΔΔ ή ΝΠΙΔ ή ένωση προσώπων ή φυσικό πρόσωπο και εφαρμόζεται σε ΔΠΧ όπως συλλογή-καταχώρηση-οργάνωση-διατήρηση-αποθήκευση-τροποποίηση-εξαγωγή-χρήσηδιαβίβαση-διάδοση,διάθεση,συσχέτηση-συνδιασμό-διασύνδεση,δέσμευση-κλείδωμα-διαγραφή-καταστροφή.
Δεν είναι Επ ΔΠΧ η επεξεργασία που πραγματοποιείται από φυσικό πρόσωπο για την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών (τήρηση αρχείου αλληλογραφίας) ή οικιακών (οικιακοί λογαριασμοί). Επεξεργασία ΔΠΧ είτε διεξαγόμενη με ηλεκτρονικές μεθόδους είτε ΜΗ αυτοματοποιημένη (χειρόγραφη).

Υπεύθυνος ΕΔΠΧ είναι οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο επεξεργασίας των ΔΠΧ, όπως Φ.Π, ή Ν.Π, δημόσια αρχή, υπηρεσία ή άλλος οργανισμός. Όταν ο σκοπός και ο τρόπος ΕΔΠΧ καθορίζονται με διατάξεις νόμου και ΥΕΔΠΧ και η επιλογή καθορίζεται από το εθνικό ή κοινοτικό δίκαιο.

5.5 Απόρρητο και Ασφάλεια

Η ΕπΔΠΧ είναι απόρρητη. Διεξάγεται αποκλειστικά και μόνο από τα πρόσωπα που αποτελούν υπό τον έλεγχο του Υπ ΕπΔΠΧ και μόνο με εντολή του. Ο ΥπΕπΔΠΧ επιλέγει πρόσωπο με αντίστοιχα επαγγελματικά προσόντα, με επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων για τήρηση του απορρήτου.Ο ΥπΕπΔΠΧ λαμβάνει τα κατάλληλα μέτρα για την ασφάλεια των δεδομένων και την προστασία από:
Καταστροφή, απώλεια, αλλοίωση, απαγορευμένη διάδοση και αθέμιτη επεξεργασία.
Η αρχή Πρ.ΔΠΧ παρέχει οδηγίες, μέτρα προστασίας.

5.6 Δικαίωμα ενημέρωσης

Το δικαίωμα αυτό προστατεύεται αυτοτελώς. Ο Υπ. Επ. ΔΠΧ κατά το στάδιο συλλογής δεδομένων π.χ οφείλει να ενημερώνει το Υπ.Επ.ΔΠΧ για:

Την ταυτότητα του

Σκοπό επεξεργασίας

Αποδέκτες

Ύπαρξη δικαιώματος πρόσβασης και του δικαιώματος αντίρρησης για τα δεδομένα που αφορούν το υποκείμενο.

Τέλος με απόφαση της Αρχής μπορεί να αρθεί η υποχρέωση ενημέρωσης εφόσον η επεξεργασία των δεδομένων γίνεται για λόγους ασφαλείας ή για την διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

5.7 Δικαιώματα πρόσβασης

Καθένας έχει το δικαίωμα να γνωρίζει εάν τα δεδομένα π.χ.χ που τον αφορούν αποτελούν αντικείμενο επεξεργασίας. Συγκεκριμένα, το Υπ. ΔΠΧ δικαιούνται να λαμβάνει τις ακόλουθες πληροφορίες:

Δεδομένα π.χ. που το αφορούν

Προέλευση τους

Σκοπός επεξεργασίας

Αποδέκτες

Εξέλιξη επεξεργασίας

Εάν ο Υπ. Επ.ΠΔ δεν απαντήσει εγγράφως εντός15 ημερών, το Υποκ.Δεδ. προσφεύγει στην Αρχή. Το δικαίωμα στην πληροφόρηση αποκλείεται μόμο για τους λόγους εθνικής ασφάλειας ή διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

5.8 Τι είναι η αρχή;

Είναι ελεγκτικό όργανο για τον έλεγχο της προστασίας του ατόμου από αθέμιτη Επ.Π.Δ η αρχή είναι ανεξάρτητη διοικητική αρχή με δικό της προϋπολογισμό, Γραμματεία. Οι πράξεις της καταρχήν δεν υποκινούνται σε κανενός είδους έλεγχο νομιμότητας ή σκοπιμότητας από την εκτελεστική εξουσία. Η Αρχή είναι 5μελής. Ο νόμος καθορίζει ενδεικτικά τις αρμοδιότητας της ΑΠΠΔ μεταξύ των οποίων συμπεριλαμβάνονται:

Η διεξαγωγή διοικητικών εξετάσεων, διεξαγωγή ελέγχων, η επιβολή κυρώσεων, η έκδοση κανονιστικών πράξεων, η ανακοίνωση στη Βουλή παραβάσεων των ισχυόντων νομικών ρυθμίσεων

Η υποβολή στον Πρόεδρο της Βουλής και στον πρωθυπουργό ετήσιας έκθεσης για την δράση της και την κατάσταση της προστασίας προσωπικών δεδομένων.

Κεφάλαιο 6ο

6.1 Νόμος 2472/1997: Θεσμικό πλαίσιο η προστασία προσωπικών δεδομένων στην Ελλάδα

ΚΕΦΑΛΑΙΟ Α'
ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1: Αντικείμενο

Αντικείμενο του παρόντος νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής.

Άρθρο 2: Ορισμοί

Για τους σκοπούς του παρόντος νόμου νοούνται ως:
α) «Δεδομένα προσωπικού χαρακτήρα», κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.
β) «Ευαίσθητα δεδομένα», τα δεδομένα που αφορούν τη φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε ένωση, σωματείο και συνδικαλιστική οργάνωση, την υγεία, την κοινωνική πρόνοια και τη ερωτική ζωή, καθώς και τα σχετικά με ποινικές διώξεις ή καταδίκες.
γ) «Υποκείμενο των δεδομένων», το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική.
δ) «Επεξεργασία δεδομένων προσωπικού χαρακτήρα» («επεξεργασία»), κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή.
ε) «Αρχείο δεδομένων προσωπικού χαρακτήρα» («αρχείο»), σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία αποτελούν ή μπορεί να αποτελέσουν αντικείμενο επεξεργασίας, και τα οποία τηρούνται είτε από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου, ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο.

στ) «Διασύνδεση», μορφή επεξεργασίας που συνίσταται στην δυνατότητα συσχέτισης των δεδομένων ενός αρχείου με δεδομένα αρχείου ή αρχείων που τηρούνται από άλλον ή άλλους υπεύθυνους επεξεργασίας ή που τηρούνται από τον ίδιο υπεύθυνο επεξεργασίας για άλλο σκοπό.

ζ) «Υπεύθυνος επεξεργασίας», οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός. Όταν ο σκοπός και ο τρόπος της επεξεργασίας καθορίζονται με διατάξεις νόμου ή κανονιστικές διατάξεις εθνικού ή κοινοτικού δικαίου, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια βάσει των οποίων γίνεται η επιλογή του καθορίζονται αντίστοιχα από το εθνικό ή το κοινοτικό δίκαιο.

η) «Εκτελών την επεξεργασία», οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπεύθυνου επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποισδήποτε άλλος οργανισμός.

θ) «Τρίτος», κάθε φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμός, εκτός από το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας και τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, εφόσον ενεργούν υπό την άμεση εποπτεία ή για λογαριασμό του υπεύθυνου επεξεργασίας.

ι) «Αποδέκτης», το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμός, στον οποίο ανακοινώνονται ή μεταδίδονται τα δεδομένα, ανεξαρτήτως αν πρόκειται για τρίτο ή όχι.

ια) «Συγκατάθεση» του υποκειμένου των δεδομένων, κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή, και εν πλήρη επιγνώσει, και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Η ενημέρωση αυτή περιλαμβάνει πληροφόρηση τουλάχιστον για τον σκοπό της επεξεργασίας, τα δεδομένα ή τις κατηγορίες δεδομένων που αφορά η επεξεργασία, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, 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.

ιβ) "Αρχή", η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που θεσπίζεται στο κεφάλαιο Δ΄ του παρόντος νόμου.

Άρθρο 3: Πεδίο εφαρμογής

1. Οι διατάξεις του παρόντος νόμου εφαρμόζονται στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία καθώς και στη μη αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο.

2. Οι διατάξεις του παρόντος νόμου δεν εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία πραγματοποιείται από φυσικό πρόσωπο για την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών ή οικιακών.

3. Ο παρών νόμος εφαρμόζεται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον αυτή εκτελείται:

α) Από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, εγκατεστημένο στην Ελληνική Επικράτεια ή σε τόπο όπου βάσει του δημοσίου διεθνούς δικαίου εφαρμόζεται το ελληνικό δίκαιο.

β) Από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην Ελληνική Επικράτεια ή σε τόπο όπου εφαρμόζεται το ελληνικό δίκαιο, όταν η επεξεργασία αφορά υποκείμενα εγκατεστημένα στην Ελληνική Επικράτεια. Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας οφείλει να υποδείξει με γραπτή δήλωσή του προς την Αρχή εκπρόσωπο εγκατεστημένο στην Ελληνική Επικράτεια, ο οποίος υποκαθίσταται στα δικαιώματα και υποχρεώσεις του υπεύθυνου, χωρίς ο τελευταίος αυτός να απαλλάσσεται από τυχόν ιδιαίτερη ευθύνη του. Το αυτό ισχύει και όταν ο υπεύθυνος επεξεργασίας καλύπτεται από ετεροδικία, ασυλία, ή άλλο λόγο που κωλύει την ποινική δίωξη.

γ) Από υπεύθυνο επεξεργασίας που δεν είναι εγκατεστημένος στην επικράτεια Κράτους- Μέλους της Ευρωπαϊκής 'Ενωσης αλλά τρίτης χώρας και για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προσφεύγει σε μέσα, αυτοματοποιημένα ή όχι, ευρισκόμενα στην Ελληνική Επικράτεια, εκτός εάν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη διέλευση από αυτήν. Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας οφείλει να υποδείξει με γραπτή δήλωσή του προς την Αρχή εκπρόσωπο εγκατεστημένο στην Ελληνική Επικράτεια, ο οποίος υποκαθίσταται στα δικαιώματα και υποχρεώσεις του υπεύθυνου, χωρίς ο τελευταίος αυτός να απαλλάσσεται από τυχόν ιδιαίτερη ευθύνη του. Το αυτό ισχύει και όταν ο υπεύθυνος επεξεργασίας καλύπτεται από ετεροδικία, ασυλία ή άλλο λόγο που κωλύει την ποινικήδίωξη.

ΚΕΦΑΛΑΙΟ Β'
ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Άρθρο 4: Χαρακτηριστικά δεδομένων προσωπικού χαρακτήρα

1. Τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει:

α) Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς καινα υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών.

β) Να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει τωνσκοπών της επεξεργασίας.

γ) Να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση.

δ) 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 τους και της επεξεργασίας τους. Μετά την παρέλευση της περιόδου αυτής, η Αρχή μπορεί, με αιτιολογημένη απόφασή της, να επιτρέπει τη διατήρηση δεδομένων προσωπικού χαρακτήρα για ιστορικούς επιστημονικούς ή στατιστικούς σκοπούς, εφ΄ όσον κρίνει ότι δεν θίγονται σε κάθε συγκεκριμένη περίπτωση τα δικαιώματα των υποκειμένων τους ή και τρίτων. Η τήρηση των διατάξεων της παραγράφου αυτής βαρύνει τον υπεύθυνο επεξεργασίας.

2. Δεδομένα προσωπικού χαρακτήρα που έχουν συλλεγεί ή υφίστανται επεξεργασία κατά παράβαση της προηγούμενης παραγράφου καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας. Η Αρχή, εάν εξακριβώσει αυτεπαγγέλτως ή μετά από σχετική καταγγελία παράβαση των διατάξεων της προηγούμενης παραγράφου, επιβάλλει την διακοπή της συλλογής ή της επεξεργασίας και την καταστροφή των δεδομένωνπροσωπικού χαρακτήρα που έχουν ήδη συλλεγεί ή τύχει επεξεργασίας.

Άρθρο 5: Προϋποθέσεις επεξεργασίας

1. Επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον όταν το υποκείμενο των δεδομένωνέχει δώσει τη συγκατάθεσή του.

2. Κατ' εξαίρεση επιτρέπεται η επεξεργασία και χωρίς τη συγκατάθεση, όταν:

α) 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.

β) Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο.

γ) Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.

δ) Η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημόσιου 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.

ε) Η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα και υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών.

3. Η Αρχή μπορεί να εκδίδει ειδικούς κανόνες επεξεργασίας για τις πλέον συνήθεις κατηγορίες επεξεργασιών και αρχείων, οι οποίες προφανώς δεν θίγουν τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα. Οι κατηγορίες αυτές προσδιορίζονται με κανονισμούς που καταρτίζει η Αρχή και κυρώνονται με προεδρικά διατάγματα, τα οποία εκδίδονται με πρόταση του Υπουργού Δικαιοσύνης.

Άρθρο 6: Γνωστοποίηση αρχείων

1. Ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει εγγράφως στην Αρχή, τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας.

2. Με τη γνωστοποίηση της προηγούμενης παραγράφου ο υπεύθυνος επεξεργασίας πρέπει απαραιτήτως να δηλώνει:

α) Το ονοματεπώνυμο ή την επωνυμία ή τον τίτλο του και τη διεύθυνσή του. Εάν ο υπεύθυνος επεξεργασίας δεν είναι εγκατεστημένος στην ελληνική επικράτεια ή σε τόπο όπου εφαρμόζεται το ελληνικό δίκαιο, θα πρέπει επιπροσθέτως να δηλώνεται το ονοματεπώνυμο ή η επωνυμία ή ο τίτλος και η διεύθυνση του εκπροσώπου του στην Ελλάδα.¨

β) Τη διεύθυνση όπου είναι εγκατεστημένο το αρχείο ή ο κύριος εξοπλισμός που υποστηρίζει την επεξεργασία.

γ) Την περιγραφή του σκοπού της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που περιέχονται ή πρόκειται να περιληφθούν στο αρχείο.

δ) Το είδος των δεδομένων προσωπικού χαρακτήρα που υφίστανται ή πρόκειται να υποστούν επεξεργασία ή περιέχονται ή πρόκειται να περιληφθούν στο αρχείο.

ε) Το χρονικό διάστημα για το οποίο προτίθεται να εκτελεί την επεξεργασία ή να διατηρήσει το αρχείο.

στ) Τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους ανακοινώνει ή ενδέχεται να ανακοινώνει τα δεδομένα προσωπικού χαρακτήρα.

ζ) Τις ενδεχόμενες διαβιβάσεις και το σκοπό της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες.

η) Τα βασικά χαρακτηριστικά του συστήματος και των μέτρων ασφαλείας του αρχείου ή της επεξεργασίας.

3. Τα στοιχεία της προηγούμενης παραγράφου καταχωρίζονται στο Μητρώο Αρχείων και Επεξεργασιών που τηρεί η Αρχή.

4. Κάθε μεταβολή των στοιχείων που αναφέρονται στην παράγραφο 2 πρέπει να γνωστοποιείται εγγράφως και χωρίς καθυστέρηση από τον υπεύθυνο στην Αρχή.

Άρθρο 7: Επεξεργασία ευαίσθητων δεδομένων

1. Απαγορεύεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων.

2. Κατ΄ εξαίρεση επιτρέπεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων, καθώς και η ίδρυση και λειτουργία σχετικού αρχείου, ύστερα από άδεια της Αρχής, όταν συντρέχουν μία ή περισσότερες από τις ακόλουθες προϋποθέσεις:

α) Το υποκείμενο έδωσε τη γραπτή συγκατάθεσή του εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που αντίκειται στο νόμο ή τα χρηστά ήθη ή νόμος ορίζει ότι η συγκατάθεση δεν αίρει την απαγόρευση.

β) Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν τούτο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.

γ) Η επεξεργασία αφορά δεδομένα που δημοσιοποιεί το ίδιο το υποκείμενο ή είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου ή πειθαρχικού οργάνου.

δ) Η επεξεργασία αφορά θέματα υγείας και εκτελείται από πρόσωπο που ασχολείται κατ' επά γγελμα με την παροχή υπηρεσιών υγείας και υπόκειται σε καθήκον εχεμύθειας ή σε συναφείς κώδικες δεοντολογίας, υπό τον όρο ότι η επεξεργασία είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή τη διαχείριση υπηρεσιών υγείας.

ε) Η επεξεργασία εκτελείται από Δημόσια Αρχή και είναι αναγκαία είε

αα) για λόγους εθνικής ασφάλειας, είτε

ββ) για την εξυπηρέτηση των αναγκών της εγκληματολογικής ή σωφρονιστικής πολιτικής που αφορά τη διακρίβωση εγκλημάτων, ποινικές καταδίκες ή μέτρα ασφάλειας είτε **γγ)** για λόγους προστασίας της δημόσιας υγείας ή για την άσκηση δημόσιου ελέγχου κοινωνικών παροχών.

στ)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.

ζ) Η επεξεργασία αφορά δεδομένα δημοσίων προσώπων, εφόσον αυτά συνδέονται με την άσκηση δημοσίου λειτουργήματος ή τη διαχείρηση συμφερόντων τρίτων, και πραγματοποιείται αποκλειστικά για την άσκηση του δημοσιογραφικού επαγγέλματος. Η άδεια της αρχής χορηγείται μόνο εφόσον η επεξεργασία είναι απολύτως αναγκαία για την εξασφάλιση του δικαιώματος πληροφόρησης επί θεμάτων δημοσίου

ενδιαφέροντος καθώς και στο πλαίσιο καλλιτεχνικής έκφρασης και εφόσον δεν παραβιάζεται καθ' οιονδήποτε τρόπο το δικαίωμα προστασίας της ιδιωτικής και οικογενειακής ζωής.

3. Η Αρχή χορηγεί άδεια συλλογής και επεξεργασίας ευαίσθητων δεδομένων, καθώς και άδεια ιδρύσεως και λειτουργίας σχετικού αρχείου, ύστερα από αίτηση του υπεύθυνου επεξεργασίας. Εφ' όσον η Αρχή διαπιστώσει ότι πραγματοποιείται επεξεργασία ευαίσθητων δεδομένων, η γνωστοποίηση αρχείου, σύμφωνα με το άρθρο 6 του παρόντος νόμου, επέχει θέση αιτήσεως για τη χορήγηση άδειας. Η Αρχή μπορεί να επιβάλλει όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία του δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων. Πριν χορηγήσει την άδεια, η Αρχή καλεί σε ακρόαση τον υπεύθυνο επεξεργασίας ή τον εκπρόσωπο του και τον εκτελούντα την επεξεργασία.

4. Η άδεια εκδίδεται για ορισμένο χρόνο, ανάλογα με τον σκοπό της επεξεργασίας. Μπορεί να ανανεωθεί ύστερα από αίτηση του υπεύθυνου επεξεργασίας.

5. Η άδεια περιέχει απαραιτήτως:

α) Το ονοματεπώνυμο ή την επωνυμία ή τον τίτλο καθώς και τη διεύθυνση του υπεύθυνου επεξεργασίας και του τυχόν εκπροσώπου του.

β) Τη διεύθυνση όπου είναι εγκατεστημένο το αρχείο.

γ) Το είδος των δεδομένων προσωπικού χαρακτήρα που επιτρέπεται να περιληφθούν στο αρχείο.

δ) Το χρονικό διάστημα για το οποίο χορηγείται η άδεια.

ε) Τους τυχόν όρους και προϋποθέσεις που έχει επιβάλει η Αρχή για την ίδρυση και λειτουργία του αρχείου.

στ) Την υποχρέωση γνωστοποίησής του ή των αποδεκτών ευθύς ως εξατομικευθούν.

6. Αντίγραφο της άδειας καταχωρίζεται στο Μητρώο Αδειών που διατηρεί η Αρχή.

7. Κάθε μεταβολή των στοιχείων που αναφέρονται στην παράγραφο 5 γνωστοποιείται χωρίς καθυστέρηση στην Αρχή. Κάθε άλλη μεταβολή, πλην της διεύθυνσης του υπευθύνου ή του εκπροσώπου του, συνεπάγεται την έκδοση νέας άδειας, εφόσον συντρέχουν οι νόμιμες προυποθέσεις.

Άρθρο 7α Απαλλαγή υποχρέωσης γνωστοποίησης και λήψης άδειας

1. Ο υπεύθυνος επεξεργασίας απαλλάσσεται από την υποχρέωση γνωστοποίησης του άρθρου 6 και από την υποχρέωση λήψης άδειας του άρθρου 7 του παρόντος νόμου στις ακόλουθες περιπτώσεις:

α. Όταν η επεξεργασία πραγματοποιείται αποκλειστικά για σκοπούς που συνδέονται άμεσα σε σχέση εργασίας ή έργου ή με παροχή υπηρεσιών στο δημόσιο τομέα και είναι αναγκαία για την εκπλήρωση υποχρέωσης που επιβάλλει ο νόμος ή για την εκτέλεση των υποχρεώσεων από τις παραπάνω σχέσεις και το υποκείμενο έχει προηγουμένως ενημερωθεί.

β. Όταν η επεξεργασία αφορά πελάτες ή προμηθευτές, εφόσον τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους. Για την εφαρμογή της παρούσας διάταξης τα δικαστήρια και οι δημόσιες αρχές δεν λογίζονται ως τρίτοι εφόσον τη διαβίβαση ή κοινοποίηση επιβάλλει νόμος ή δικαστική απόφαση. Δεν απαλλάσσονται από την υποχρέωση γνωστοποίησης οι ασφαλιστικές εταιρείες για όλους τους κλάδους

ασφάλισης, οι φαρμακευτικές εταιρείες, οι εταιρείες εμπορίας πληροφοριών και τα χρηματοπιστωτικά νομικά πρόσωπα, όπως οι τράπεζες και οι εταιρείες έκδοσης πιστωτικών καρτών.

γ. Όταν η επεξεργασία γίνεται από σωματεία, εταιρείες, ενώσεις προσώπων και πολιτικά κόμματα και αφορά δεδομένα τω μελών ή εταίρων τους, εφόσον αυτοί έχουν δώσει τη συγκατάθεσή τους και τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους. Δεν λογίζονται ως τρίτοι τα μέλη ή οι εταίροι, εφόσον η διαβίβαση γίνεται προς αυτούς για τους σκοπούς των ως άνω νομικών προσώπων ή ενώσεων, ούτε τα δικαστήρια και οι δημόσιες αρχές, εφόσον τη διαβίβαση επιβάλλει νόμος ή δικαστική απόφαση.

δ. Όταν η επεξεργασία γίνεται από ιατρούς ή άλλα πρόσωπα που παρέχουν υπηρεσίες υγείας και αφορά ιατρικά δεδομένα, εφόσον ο υπεύθυνος επεξεργασίας δεσμεύεται από το ιατρικό απόρρητο ή άλλο απόρρητο που προβλέπει νόμος ή κώδικας δεοντολογίας και τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους. Για την εφαρμογή της παρούσας διάταξης τα δικαστήρια και οι δημόσιες αρχέςδεν λογίζονται ως τρίτοι, εφόσον τη διαβίβαση ή κοινοποίηση επιβάλλει νόμος ή δικαστική απόφαση. Δ Δεν εμπίπτουν στην απαλλαγή της παρούσας διάταξης τα νομικά πρόσωπα ή οι οργανισμοί που παρέχουν υπηρεσίες υγείας, όπως κλινικές, νοσοκομεία, κέντρα υγείας, κέντρα αποθεραπείας και αποτοξίνωσης, ασφαλιστικά ταμεία και ασφαλιστικές εταιρείες, καθώς και οι υπεύθυνοι επεξεργασίας δεδομένων προσωπικού χαρακτήρα όταν η επεξεργασία διεξάγεται στο πλαίσιο προγραμμάτων τηλεϊατρικής ή παροχής
ιατρικών υπηρεσιών μέσω δικτύου.

ε. Όταν η επεξεργασία γίνεται από δικηγόρους, συμβολαιογράφους, άμισθους υποθηκοφύλακες και δικαστικούς επιμελητές και αφορά την παροχή νομικών υπηρεσιών προς πελάτες τους, εφόσον ο υπεύθυνος επεξεργασίας δεσμεύεται από υποχρέωση απορρήτου που προβλέπει νόμος και τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους, εκτός από τις περιπτώσεις που αυτό είναι αναγκαίο και συνδέεται άμεσα με την εκπλήρωση εντολής του πελάτη.

2. Σε όλες τις προαναφερθείσες περιπτώσεις της παραγράφου 1 του παρόντος άρθρου, ο υπεύθυνος επεξεργασίας υπόκειται σε όλες τις υποχρεώσεις που προβλέπει ο παρών νόμος και υποχρεούται να συμμορφώνεται με ειδικούς κανόνες επεξεργασίας που η Αρχή εκδίδει σύμφωνα με την παράγραφο 3 του άρθρου 5 του παρόντος νόμου.

3. Οι προθεσμίες για την υποβολή γνωστοποίησης αρχείου με μη ευαίσθητα προσωπικά δεδομένα, την υποβολή αίτησης για λήψη άδειας για αρχείο με ευαίσθητα δεδομένα και για την ενημέρωση των υποκειμένων παρατείνονται έως την 21 η Ιανουαρίου 2001.

Άρθρο 8: Διασύνδεση αρχείων

1. Διασύνδεση αρχείων επιτρέπεται μόνον υπό τους όρους του παρόντος άρθρου.

2. Κάθε διασύνδεση γνωστοποιείται στην Αρχή με δήλωση την οποία υποβάλλουν από κοινού οι υπεύθυνοι επεξεργασίας ή ο υπεύθυνος επεξεργασίας που διασυνδέει δύο ή περισσότερα αρχεία που εξυπηρετούν διαφορετικούς σκοπούς.

3. Εάν ένα τουλάχιστον από τα αρχεία που πρόκειται να διασυνδεθούν περιέχει ευαίσθητα δεδομένα, ή εάν η διασύνδεση έχει ως συνέπεια την αποκάλυψη ευαίσθητων δεδομένων, ή εάν για την πραγματοποίηση της διασύνδεσης, πρόκειται να γίνει χρήση ενιαίου κωδικού αριθμού, η διασύνδεση επιτρέπεται μόνον με προηγούμενη άδεια της Αρχής (άδεια διασύνδεσης).

4. Η άδεια διασύνδεσης της προηγούμενης παραγράφου χορηγείται ύστερα από ακρόαση των υπεύθυνων επεξεργασίας των αρχείων και περιέχει απαραιτήτως:

α)Τον σκοπό για τον οποίο η διασύνδεση θεωρείται αναγκαία.

β)Το είδος των δεδομένων προσωπικού χαρακτήρα που αφορά η διασύνδεση.

γ)Το χρονικό διάστημα για το οποίο επιτρέπεται η διασύνδεση.

δ) Τους τυχόν όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία των δικαιωμάτων και ελευθεριών και ιδίως του δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων.

5. Η άδεια διασύνδεσης μπορεί να ανανεωθεί ύστερα από αίτηση των υπεύθυνων επεξεργασίας.

6. Οι δηλώσεις της παρ. 2 του παρόντος άρθρου καθώς και αντίγραφα των αδειών διασύνδεσης καταχωρίζονται στο Μητρώο Διασυνδέσεων που τηρεί η Αρχή.

Άρθρο 9: Διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα

1. Η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε χώρες της Ευρωπαικής Ένωσης είναι ελεύθερη. Η διαβίβαση προς χώρα που δεν ανήκει στην Ευρωπαϊκή Ένωση δεδομένων προσωπικού χαρακτήρα τα οποίαέχουν υποστεί ή πρόκειται να υποστούν επεξεργασία μετά τη διαβίβασή τους, επιτρέπεται ύστερα από άδεια της Αρχής. Η Αρχή παρέχει την άδεια μόνον εάν κρίνει ότι η εν λόγω χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Προς τούτο, λαμβάνει υπ' όψη ιδίως τη φύση των δεδομένων, τους σκοπούς και τη διάρκεια της επεξεργασίας, τους σχετικούς γενικούς και ειδικούς κανόνες δικαίου, τους κώδικες δεοντολογίας, τα μέτρα ασφαλείας για την προστασία δεδομένων προσωπικού χαρακτήρα, καθώς και το επίπεδο προστασίας των χωρών προέλευσης, διέλευσης και τελικού προορισμού των δεδομένων.

2. Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς χώρα που δεν ανήκει στην Ευρωπαϊκή Ένωση και η οποία δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, επιτρέπεται κατ' εξαίρεση, με άδεια της Αρχής, εφ' όσον συντρέχει μία ή περισσότερες από τις κατωτέρω προυποθέσεις:

α) Το υποκείμενο των δεδομένων έδωσε τη συγκατάθεσή του για τη διαβίβαση, εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που να αντίκειται στο νόμο ή τα χρηστά ήθη.

β) Η διαβίβαση είναι απαραίτητη

i) για τη διασφάλιση ζωτικού συμφέροντος του υποκειμένου των δεδομένων, εφ΄όσον αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του, ή

ii) για τη συνομολόγηση και εκτέλεση σύμβασης μεταξύ αυτού και του υπεύθυνου επεξεργασίας ή μεταξύ του υπεύθυνου επεξεργασίας και τρίτου προς το συμφέρον του υποκειμένου των δεδομένων, εφ' όσον το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του, ή

iii) για την εκτέλεση προσυμβατικών μέτρων που έχουν ληφθεί κατ΄αίτηση του υποκειμένου των δεδομένων.

γ) Η διαβίβαση είναι απαραίτητη για την αντιμετώπιση εξαιρετικής ανάγκης και τη διαφύλαξη υπέρτερου δημόσιου συμφέροντος, ιδίως για την εκτέλεση συμβάσεων συνεργασίας με δημόσιες αρχές της άλλης χώρας, εφόσον ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις για την προστασία της ιδιωτικής ζωής και των θεμελιωδών ελευθεριών και την άσκηση των σχετικών δικαιωμάτων.

δ) Η διαβίβαση είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον τουδικαστηρίου.

ε) Η μετάδοση πραγματοποιείται από δημόσιο μητρώο, το οποίο κατά το νόμο προορίζεται για την παροχή πληροφοριών στο κοινό και είναι προσιτό στο κοινό ή σε κάθε πρόσωπο που αποδεικνύει έννομο συμφέρον, εφόσον στη συγκεκριμένη περίπτωση πληρούνται οι νόμιμες προυποθέσεις για την πρόσβαση στο μητρώο.

3. Στις περιπτώσεις των προηγούμενων παραγράφων η Αρχή ενημερώνει την Ευρωπαϊκή Επιτροπή και τις αντίστοιχες Αρχές των άλλων κρατών μελών, όταν θεωρεί ότι μία χώρα δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας.

Άρθρο 10: Απόρρητο και ασφάλεια της επεξεργασίας

1. 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 μόνον κατ' εντολήν του.

2. Για τη διεξαγωγή της επεξεργασίας ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου.

3. Ο υπεύθυνος επεξεργασίας οφείλει 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. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Η Αρχή παρέχει εκάστοτε οδηγίες για τον βαθμό ασφαλείας των δεδομένων καθώς και για τα μέτρα προστασίας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία δεδομένων, εν' όψει και των τεχνολογικών εξελίξεων.

4. Αν η επεξεργασία διεξάγεται για λογαριασμό του υπεύθυνου από πρόσωπο μη εξαρτώμενο από αυτόν, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως. Η ανάθεση προβλέπει υποχρεωτικά ότι ο ενεργών την επεξεργασία την διεξάγει μόνο κατ' εντολήν του υπεύθυνου και ότι οι λοιπές υποχρεώσεις του παρόντος άρθρου βαρύνουν αναλόγως και αυτόν.

ΚΕΦΑΛΑΙΟ Γ΄

ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Άρθρο 11: Δικαίωμα ενημέρωσης

1. Ο υπεύθυνος επεξεργασίας οφείλει, κατά το στάδιο της συλλογής δεδομένων προσωπικού χαρακτήρα, να ενημερώνει με τρόπο πρόσφορο και σαφή το υποκείμενο για τα εξής τουλάχιστον στοιχεία:

α) την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του.

β) τον σκοπό της επεξεργασίας.

γ) του αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων.

δ) την ύπαρξη του δικαιώματος πρόσβασης

2. Εάν για τη συλλογή των δεδομένων προσωπικού χαρακτήρα ο υπεύθυνος επεξεργασίας ζητεί την συνδρομή του υποκείμενου, οφείλει να το ενημερώνει ειδικώς και εγγράφως για τα στοιχεία της παρ. 1 του παρόντος άρθρου καθώς και για τα δικαιώματά του, σύμφωνα με τα άρθρα 11 έως και 13 του παρόντος νόμου. Με την αυτή ενημέρωση ο υπεύθυνος επεξεργασίας γνωστοποιεί στο υποκείμενο εάν υποχρεούται ή όχι να παράσχει τη συνδρομή του, με βάση ποιες διατάξεις, καθώς και για τις τυχόν συνέπειες της αρνήσεώς του.

3. Εάν τα δεδομένα ανακοινώνονται σε τρίτους, το υποκείμενο ενημερώνεται για την ανακοίνωση πριν από αυτούς.

4. Με απόφαση της Αρχής, μπορεί να αρθεί εν όλω ή εν μέρει η υποχρέωση ενημέρωσης, σύμφωνα με τις παρ. 1 και 3 του παρόντος άρθρου, εφ' όσον η επεξεργασία δεδομένων προσωπικού χαρακτήρα γίνεται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Σε επείγουσες περιπτώσεις η άρση της υποχρέωσης μπορεί να γίνει με προσωρινή, άμεσα εκτελεστή από φαση του Προέδρου, ο οποίος πρέπει να συγκαλέσει το συντομότερο την Αρχή για την έκδοση οριστικής απόφασης επί του θέματος.

5. Με την επιφύλαξη των δικαιωμάτων εκ των άρθρων 12 και 13, η υποχρέωση ενημέρωσης δεν υφίσταται όταν η συλλογή γίνεται αποκλειστικά για δημοσιογραφικούς σκοπούς και αφορά δημόσια πρόσωπα.

Άρθρο 12: Δικαίωμα πρόσβασης

1. Καθένας έχει δικαίωμα να γνωρίζει εάν δεδομένα προσωπικού χαρακτήρα που τον αφορούν αποτελούν ή αποτέλεσαν αντικείμενο επεξεργασίας. Προς τούτο, ο υπεύθυνος επεξεργασίας, έχει υποχρέωση να του απαντήσει εγγράφως.

2. Το υποκείμενο των δεδομένων έχει δικαίωμα να ζητεί και να λαμβάνει από τον υπεύθυνο επεξεργασίας, χωρίς καθυστέρηση και κατά τρόπο εύληπτο και σαφή, τις ακόλουθες πληροφορίες:

α) Όλα τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, καθώς και την προέλευσή τους.

β) Τους σκοπούς της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών.

γ) Την εξέλιξη της επεξεργασίας για το χρονικό διάστημα από την προηγούμενη ενημέρωση ή πληροφόρησή του.

δ) Τη λογική της αυτοματοποιημένης επεξεργασίας. Το δικαίωμα πρόσβασης μπορεί να ασκείται από το υποκείμενο των δεδομένων και με τη συνδρομή ειδικού.

3. Το δικαίωμα της προηγούμενης παραγράφου και τα δικαίωματα του άρθρου 13 ασκούνται με την υποβολή της σχετικής αίτησης στον υπεύθυνο της επεξεργασίας και ταυτόχρονη καταβολή χρηματικού ποσού, το ύψος του οποίου, ο τρόπος καταβολής του και κάθε άλλο συναφές ζήτημα ρυθμίζονται με απόφαση της Αρχής. Το ποσό αυτό επιστρέφεται στον αιτούντα εάν το αίτημα διόρθωσης ή διαγραφής των δεδομένων κριθεί βάσιμο είτε από τον υπεύθυνο της επεξεργασίας είτε από την Αρχή, σε περίπτωση προσφυγής του σ' αυτήν. Ο υπεύθυνος έχει υποχρέωση στην περίπτωση αυτή να χορηγήσει στον αιτούντα, χωρίς καθυστέρηση δωρεάν και σε γλώσσα κατανοητή, αντίγραφο του διορθωμένου μέρους της
επεξεργασίας που τον αφορά.

4. Εάν ο υπεύθυνος επεξεργασίας δεν απαντήσει εντός δεκαπέντε (15) ημερών ή εάν η απάντησή του δεν είναι ικανοποιητική, το υποκείμενο των δεδομένων έχει δικαίωμα να προσφύγει στην Αρχή. Στην περίπτωση κατά την οποία ο υπεύθυνος επεξεργασίας αρνηθεί να ικανοποιήσει το αίτημα του ενδιαφερόμενου, κοινοποιεί την απάντησή του στην Αρχή και ενημερώνει τον ενδιαφερόμενο ότι μπορεί να προσφύγει σε αυτήν.

5. Με απόφαση της Αρχής, ύστερα από αίτηση του υπεύθυνου επεξεργασίας, η υποχρέωση πληροφόρησης, σύμφωνα με τις παρ. 1 και 2 του παρόντος άρθρου, μπορεί να αρθεί, εν όλω ή εν μέρει, εφ' όσον η επεξεργασία δεδομένων προσωπικού χαρακτήρα γίνεται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Στην περίπτωση αυτή ο Πρόεδρος της Αρχής ή ο αναπληρωτής του προβαίνει σε όλες τις αναγκαίες ενέργειες και έχει ελεύθερη πρόσβαση στο αρχείο.

6. Δεδομένα που αφορούν την υγεία γνωστοποιούνται στο υποκείμενο μέσω ιατρού.

Άρθρο 13: Δικαίωμα αντίρρησης

1. Το υποκείμενο των δεδομένων έχει δικαίωμα να προβάλλει οποτεδήποτε αντιρρήσεις για την επεξεργασία δεδομένων που το αφορούν. Οι αντιρρήσεις απευθύνονται εγγράφως στον υπεύθυνο επεξεργασίας και πρέπει να περιέχουν αίτημα για συγκεκριμένη ενέργεια, όπως διόρθωση, προσωρινή μη χρησιμοποίηση, δέσμευση, μη διαβίβαση ή διαγραφή. Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να απαντήσει εγγράφως επί των αντιρρήσεων μέσα σε αποκλειστική προθεσμία δεκαπέντε (15) ημερών. Στην απάντησή του οφείλει να ενημερώσει το υποκείμενο για τις ενέργειες στις οποίες προέβη ή, ενδεχομένως, για τους λόγους που δεν ικανοποίησε το αίτημα. Η απάντηση σε περίπτωση απόρριψης των αντιρρήσεων πρέπει να
κοινοποιείται και στην Αρχή.

2. Εάν ο υπεύθυνος επεξεργασίας δεν απαντήσει εμπροθέσμως ή η απάντησή του δεν είναι ικανοποιητική, το υποκείμενο των δεδομένων έχει δικαίωμα να προσφύγει στην Αρχή και να ζητήσει την εξέταση των αντιρρήσεών του. Εάν η Αρχή πιθανολογήσει ότι οι αντιρρήσεις είναι εύλογες και ότι συντρέχει κίνδυνος σοβαρής βλάβης του υποκειμένου από την συνέχιση της επεξεργασίας, μπορεί να επιβάλλει την άμεση αναστολή της επεξεργασίας έως ότου εκδώσει οριστική απόφαση επί των αντιρρήσεων.

3. Καθένας έχει δικαίωμα να δηλώσει στην Αρχή ότι δεδομένα που τον αφορούν δεν επιθυμεί να αποτελέσουν αντικείμενο επεξεργασίας από οποιονδήποτε, για λόγους προώθησης πωλήσεως αγαθών ή παροχής υπηρεσιών εξ αποστάσεως. Η Αρχή τηρεί μητρώο με τα στοιχεία ταυτότητας των ανωτέρω. Οι υπεύθυνοι επεξεργασίας των σχετικών αρχείων έχουν την υποχρέωση να συμβουλεύονται πριν από κάθε επεξεργασία το εν λόγω μητρώο και να διαγράφουν από το αρχείο τους τα πρόσωπα της παραγράφου αυτής.

Άρθρο 14: Δικαίωμα προσωρινής δικαστικής προστασίας

1. Καθένας έχει δικαίωμα να ζητήσει από το αρμόδιο κάθε φορά δικαστήριο την άμεση αναστολή ή μη εφαρμογή πράξης ή απόφασης που τον θίγει, την οποία έχει λάβει διοικητική αρχή, νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο αποκλειστικά με αυτοματοποιημένη επεξεργασία στοιχείων, εφόσον η επεξεργασία αυτή αποβλέπει στην αξιολόγηση της προσωπικότητάς του και ιδίως της αποδοτικότητάς του στην εργασία, της οικονομικής φερεγγυότητάς του, της αξιοπιστίας του και της εν γένει συμπεριφοράς του.
2. Το δικαίωμα του παρόντος άρθρου μπορεί να ικανοποιηθεί και όταν δεν συντρέχουν οι λοιπές ουσιαστικές προϋποθέσεις της προσωρινής δικαστικής προστασίας, όπως προβλέπονται κάθε φορά.

ΚΕΦΑΛΑΙΟ Δ΄

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Άρθρο 15: Σύσταση - αποστολή - νομική φύση

1. Συνιστάται Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Αρχή), με αποστολή την εποπτεία της εφαρμογής του παρόντος νόμου και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά.
2. Η Αρχή αποτελεί ανεξάρτητη δημόσια αρχή, έχει δικό της προϋπολογισμό και εξυπηρετείται από δική της γραμματεία. Η Αρχή δεν υπόκειται σε οποιονδήποτε διοικητικό έλεγχο. Κατά την άσκηση των καθηκόντων τους τα μέλη της Αρχής απολαύουν προσωπικής και λειτουργικής ανεξαρτησίας. Η Αρχή υπάγεται στον Υπουργό Δικαιοσύνης και εδρεύει στην Αθήνα.
3. Τον προϋπολογισμό της Αρχής εισηγείται ο Υπουργός Δικαιοσύνης, ύστερα από πρόταση της Αρχής. Ποσοστό των κάθε είδους εσόδων του Δημοσίου από την εφαρμογή του παρόντος νόμου, συμπεριλαμβανομένων των παραβόλων και προστίμων που επιβάλλει η Αρχή, διατίθεται για τις ανάγκες της Αρχής. Το ποσοστό αυτό καθορίζεται κάθε φορά με κοινή απόφαση των Υπουργών Οικονομικών και Δικαιοσύνης.

Άρθρο 16: Συγκρότηση της Αρχής

1. Η Αρχή συγκροτείται από έναν δικαστικό λειτουργό βαθμού Συμβούλου της Επικρατείας ή αντίστοιχου και άνω, ως Πρόεδρο, και έξι μέλη ως εξής:

α) Έναν καθηγητή ή αναπληρωτή καθηγητή ΑΕΙ σε γνωστικό αντικείμενο του δικαίου.

β) Έναν καθηγητή ή αναπληρωτή καθηγητή ΑΕΙ σε γνωστικό αντικείμενο της πληροφορικής.

γ) Έναν καθηγητή ή αναπληρωτή καθηγητή Α.Ε.Ι.

δ, ε, στ) Τρία πρόσωπα κύρους και εμπειρίας στον τομέα της προστασίας δεδομένων προσωπικού χαρακτήρα.

Ο δικαστικός λειτουργός - Πρόεδρος και οι καθηγητές - μέλη μπορεί να είναι εν ενεργεία ή μη.

2. Ο Πρόεδρος της Αρχής είναι πλήρους και αποκλειστικής απασχόλησης και διορίζεται με προεδρικό διάταγμα, που εκδίδεται με πρόταση του Υπουργικού Συμβουλίου, ύστερα από εισήγηση του Υπουργού Δικαιοσύνης. Εάν για τη θέση του Προέδρου επιλεγεί εν ενεργεία δικαστικός λειτουργός, απαιτείται απόφαση του οικείου Ανώτατου Δικαστικού Συμβουλίου. Με την ίδια διαδικασία επιλέγεται και διορίζεται ο αναπληρωτής του Προέδρου.

3. Τα μέλη της Αρχής διορίζονται με την εξής διαδικασία: ο Υπουργό Δικαιοσύνης υποβάλλει στον Πρόεδρο της Βουλής πρόταση για το διορισμό των έξι τακτικών μελών της Αρχής και των ισάριθμων αναπληρωτών τους. Η πρόταση περιλαμβάνει διπλάσιο αριθμό υποψηφίων. Ο Πρόεδρος της Βουλής διαβιβάζει την πρόταση στην Επιτροπή Θεσμών και Διαφάνειας, η οποία διατυπώνει γνώμη. Τα τακτικά μέλη της Αρχής και οι αντίστοιχοι αναπληρωτές τους επιλέγονται από τη Διάσκεψη των Προέδρων. Οι επιλεγέντες διορίζονται με προεδρικό διάταγμα, που εκδίδεται με πρόταση του Υπουργού Δικαιοσύνης και δημοσιεύεται στην Εφημερίδα της Κυβερνήσεως.

4. Ο Πρόεδρος και τα μέλη της Αρχής διορίζονται με θητεία. Η θητεία τους είναι τετραετής και μπορεί να ανανεωθεί μία μόνο φορά. Κανείς δεν μπορεί να υπηρετήσει συνολικά περισσότερο από οκτώ (8) χρόνια. Η σύνθεση των έξι μελών της Αρχής ανανεώνεται κατά το ήμισυ ανά διετία. Μετά την πρώτη συγκρότηση της Αρχής, γίνεται κλήρωση μεταξύ των έξι τακτικών μελών της, ώστε τρία να έχουν τετραετή θητεία και τρία διετή.

5. Ο Πρόεδρος και τα μέλη της Αρχής διορίζονται με ισάριθμους αναπληρωτές, οι οποίοι πρέπει να διαθέτουν τις αυτές ιδιότητες και προσόντα. Οι αναπληρωτές του Προέδρου και των μελών μετέχουν στις συνεδριάσεις της Αρχής μόνο σε περίπτωση προσωρινής απουσίας ή κωλύματος του αντίστοιχου τακτικού. Με απόφασή του ο Πρόεδρος της Αρχής αναθέτει ειδικά καθήκοντα στους αναπληρωτές. Η θητεία του κάθε αναπληρωτή είναι ίση με τη θητεία του αντίστοιχου τακτικού.

Άρθρο 17 Κωλύματα-ασυμβίβαστα μελών της Αρχής

1. Δεν μπορεί να διορισθεί μέλος της Αρχής :

α) Υπουργός, υφυπουργός, γενικός γραμματέας υπουργείου ή αυτοτελούς γενικής γραμματείας και βουλευτής.

β) Διοικητής, διευθυντής, διαχειριστής, μέλος του διοικητικού συμβουλίου ή ασκών διευθυντικά καθήκοντα εν γένει σε επιχείρηση η οποία παράγει, μεταποιεί, διαθέτει ή εμπορεύεται υλικά χρησιμοποιούμενα στην πληροφορική ή τις τηλεπικοινωνίες ή παρέχει υπηρεσίες σχετικές με την πληροφορική, τις τηλεπικοινωνίες ή την επεξεργασία δεδομένων προσωπικού χαρακτήρα καθώς και οι συνδεόμενοι με σύμβαση έργου με τέτοια επιχείρηση.

2. Εκπίπτει αυτοδικαίως από την ιδιότητα του μέλους της Αρχής όποιος, μετά το διορισμό του :

α) Αποκτά μία από τις ιδιότητες που συνιστούν κώλυμα διορισμού, σύμφωνα με την προηγούμενη παράγραφο.

β) Προβαίνει σε πράξεις ή αναλαμβάνει οποιαδήποτε εργασία ή έργο ή αποκτά άλλη ιδιότητα που, κατά την κρίση της Αρχής, δεν συμβιβάζονται με τα καθήκοντά του ως μέλους της Αρχής.

3. Στην διαπίστωση των ασυμβίβαστων της προηγούμενης παραγράφου προβαίνει η Αρχή, χωρίς συμμετοχή του μέλους της, στο πρόσωπο του οποίου ενδέχεται να συντρέχει το ασυμβίβαστο. Η Αρχή αποφασίζει ύστερα από ακρόαση του εν λόγω μέλους. Την διαδικασία κινεί είτε ο Πρόεδρος της Αρχής είτε ο Υπουργός Δικαιοσύνης.

4. Απώλεια της ιδιότητας βάσει της οποίας μέλος της Αρχής διορίσθηκε, σύμφωνα με την παρ.1 του άρθρου 16 του παρόντος νόμου, συνεπάγεται την αυτοδίκαιη έκπτωσή του αν οφείλεται σε αμετάκλητη πειθαρχική ή ποινική καταδίκη.

Άρθρο 18 Υποχρεώσεις και δικαιώματα μελών της Αρχής

1. Κατά την άσκηση των καθηκόντων τους τα μέλη της Αρχής υπακούουν στη συνείδησή τους και το νόμο. Υπόκεινται στο καθήκον εχεμύθειας. Ως μάρτυρες ή πραγματογνώμονες μπορούν να καταθέτουν στοιχεία που αφορούν αποκλειστικά και μόνο την τήρηση των διατάξεων του παρόντος νόμου από υπεύθυνους επεξεργασίας. Το καθήκον εχεμύθειας υφίσταται και μετά την με οποιονδήποτε τρόπο αποχώρηση των μελών της Αρχής.

2. Με απόφαση των Υπουργών Οικονομικών και Δικαιοσύνης καθορίζονται οι μηνιαίες αποδοχές του Προέδρου και των μελών της Αρχής καθώς και η αποζημίωση τους για κάθε συνεδρίαση, κατά παρέκκλιση από κάθε άλλη διάταξη. Στους αναπληρωτές καταβάλλεται το ένα τρίτο (1/3) των μηνιαίων αποδοχών των μελών της Αρχής και αποζημίωση για κάθε συνεδρίαση στην οποία μετέχουν. Οι διατάξεις για τις δαπάνες κινήσεως των μετακινουμένων προσώπων με εντολή του Δημοσίου για εκτέλεση υπηρεσίας που ισχύουν κάθε φορά έχουν εφαρμογή και για την μετακίνηση των μελών και των υπαλλήλων της Γραμματείας της Αρχής. Ο Πρόεδρος της Αρχής εκδίδει τις σχετικές εντολές μετακίνησης.

3. Για κάθε παράβαση των υποχρεώσεών τους που απορρέουν από τον παρόντα νόμο, τα μέλη της Αρχής υπέχουν πειθαρχική ευθύνη. Την πειθαρχική αγωγή ασκεί ενώπιον του πειθαρχικού συμβουλίου ο Υπουργός Δικαιοσύνης για τον Πρόεδρο και τα μέλη της Αρχής και ο Πρόεδρος της Αρχής για τα μέλη της. Το πειθαρχικό συμβούλιο συντίθεται από έναν Αντιπρόεδρο του Συμβουλίου της Επικρατείας, ως πρόεδρο, έναν Αρεοπαγίτη, ένα Σύμβουλο του Ελεγκτικού Συνεδρίου και δύο Καθηγητές Α.Ε.Ι. σε γνωστικό αντικείμενο του δικαίου. Χρέη γραμματέα του συμβουλίου εκτελεί υπάλληλος της Αρχής. Ο πρόεδρος, τα μέλη και ο γραμματέας του συμβουλίου ορίζονται με ισάριθμους αναπληρωτές. Για τα μέλη του συμβουλίου που είναι δικαστικοί λειτουργοί απαιτείται απόφαση του οικείου ανώτατου δικαστικού συμβουλίου. Το συμβούλιο συγκροτείται με απόφαση του Υπουργού Δικαιοσύνης με τριετή θητεία. Το συμβούλιο συνεδριάζει με την παρουσία τεσσάρων τουλάχιστον μελών, μεταξύ των οποίων οπωσδήποτε ο πρόεδρος ή ο αναπληρωτής του, και αποφασίζει με απόλυτη πλειοψηφία των παρόντων. Σε περίπτωση ισοψηφίας υπερισχύει η ψήφος του προέδρου. Αν υπάρχουν περισσότερες από δύο γνώμες, οι ακολουθούντες την ασθενέστερη οφείλουν να προσχωρήσουν σε μία από τις επικρατέστερες. Το πειθαρχικό συμβούλιο αποφασίζει σε πρώτο και τελευταίο βαθμό την απαλλαγή ή την παύση του εγκαλουμένου. Η αμοιβή του προέδρου, των μελών και του γραμματέα του συμβουλίου καθορίζεται με κοινή απόφαση των Υπουργών Οικονομικών και Δικαιοσύνης κατά παρέκκλιση κάθε άλλης διατάξεως.

4. Μέλος της Αρχής που, κατά παράβαση του παρόντος νόμου, γνωστοποιεί με οποιονδήποτε τρόπο δεδομένα προσωπικού χαρακτήρα που είναι προσιτά σε αυτό λόγω της υπηρεσίας του ή αφήνει άλλον να λάβει γνώση αυτών, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή τουλάχιστον δύο εκατομμυρίων (2.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών. Αν όμως τέλεσε την πράξη με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο αθέμιτο όφελος ή να βλάψει άλλον, επιβάλλεται κάθειρξη . Αν η πράξη του πρώτου εδαφίου τελέστηκε από αμέλεια επιβάλλεται φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή.

Άρθρο 19 Αρμοδιότητες, λειτουργία και αποφάσεις της Αρχής

1. Η Αρχή έχει τις εξής ιδίως αρμοδιότητες :

α) Εκδίδει οδηγίες προς τον σκοπό ενιαίας εφαρμογής των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

β) Καλεί και επικουρεί τα επαγγελματικά σωματεία και τις λοιπές ενώσεις φυσικών ή νομικών προσώπων που διατηρούν αρχεία δεδομένων προσωπικού χαρακτήρα στην κατάρτιση κωδίκων δεοντολογίας για την αποτελεσματικότερη προστασία της ιδιωτικής ζωής και των εν γένει δικαιωμάτων και θεμελιωδών ελευθεριών των φυσικών προσώπων στον τομέα της δραστηριότητάς τους.

γ) Απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους επεξεργασίας ή τους τυχόν εκπροσώπους τους και δίδει κατά την κρίση της δημοσιότητα σε αυτές.

δ)Χορηγεί τις άδειες που προβλέπουν οι διατάξεις του παρόντος νόμου και καθορίζει το ύψος των σχετικών παραβόλων.

ε) Καταγγέλλει τις παραβάσεις των διατάξεων του παρόντος νόμου στις αρμόδιες διοικητικές και δικαστικές αρχές.

στ) Επιβάλλει τις κατά το άρθρο 21 του παρόντος νόμου διοικητικές κυρώσεις.

ζ) Αναθέτει σε μέλος ή μέλη της τη διενέργεια διοικητικών εξετάσεων.

η) Ενεργεί αυτεπαγγέλτως ή κατόπιν καταγγελίας διοικητικούς ελέγχους σε κάθε αρχείο. Έχει προς τούτο δικαίωμα προσβάσεως στα δεδομένα προσωπικού χαρακτήρα και συλλογής κάθε πληροφορίας για τους σκοπούς του ελέγχου, χωρίς να μπορεί να της αντιταχθεί κανενός είδους απόρρητο. Κατ' εξαίρεση, η Αρχή δεν έχει πρόσβαση στα στοιχεία ταυτότητας συνεργατών που περιέχονται σε αρχεία που τηρούνται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Τον έλεγχο διενεργεί μέλος ή μέλη της Αρχής ή υπάλληλος της Γραμματείας, ειδικά προς τούτο εντεταλμένος από τον Πρόεδρο της Αρχής. Κατά τον έλεγχο αρχείων που τηρούνται για λόγους εθνικής ασφαλείας παρίσταται αυτοπροσώπως ο Πρόεδρος της Αρχής.

θ) Γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα.

ι) Εκδίδει κανονιστικές πράξεις για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων, στα οποία αναφέρεται ο παρών νόμος.

ια) Ανακοινώνει στη Βουλή παραβάσεις των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

ιβ) Συντάσσει κάθε χρόνο έκθεση για την εκτέλεση της αποστολής της κατά το προηγούμενο ημερολογιακό έτος. Στην έκθεση επισημαίνονται και οι τυχόν ενδεικνυόμενες νομοθετικές μεταβολές στον τομέα της προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η έκθεση υποβάλλεται από τον Πρόεδρο της Αρχής στον Πρόεδρο της Βουλής και τον Πρωθυπουργό και δημοσιεύεται στην Εφημερίδα της Κυβερνήσεως με ευθύνη της Αρχής, η οποία μπορεί να δώσει και άλλου είδους δημοσιότητα στην έκθεση.

ιγ) Εξετάζει παράπονα σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων των αιτούντων όταν αυτά θίγονται από την επεξεργασία δεδομένων που τους αφορούν και αιτήσεις με τις οποίες ζητείται ο έλεγχος και η εξακρίβωση της νομιμότητας των επεξεργασιών αυτών και ενημερώνει τους αιτούντες για τις σχετικές ενέργειές της.

ιδ) Συνεργάζεται με αντίστοιχες αρχές άλλων κρατών μελών της Ευρωπαικής Ένωσης και τουΣυμβουλίου της Ευρώπης σε ζητήματα σχετικά με την άσκηση των αρμοδιοτήτων της.

2. Η Αρχή συνεδριάζει τακτικώς ύστερα από πρόσκληση του Προέδρου. Συνεδριάζει εκτάκτως ύστερα από πρόσκληση του Προέδρου ή αίτηση δύο τουλάχιστον μελών της. Οι αποφάσεις της Αρχής λαμβάνονται με πλειοψηφία τουλάχιστον τεσσάρων μελών της. Σε περίπτωση ισοψηφίας υπερισχύει η ψήφος του Προέδρου ή του αναπληρωτή του.

3. Η Αρχή μπορεί να συνεδριάζει και σε τμήματα συντιθεμένα από τρία τουλάχιστον τακτικά ή αναπληρωματικά μέλη και προεδρευόμενα από τον Πρόεδρο της Αρχής ή τον αναπληρωτή του. Ο κανονισμός λειτουργίας της ρυθμίζει περαιτέρω τη σύνθεση, τους όρους λειτουργίας των τμημάτων και την κατανομή των αρμοδιοτήτων μεταξύ ολομέλειας και τμημάτων. Αποφάσεις των τμημάτων μπορούν να τροποιούνται ή ανακαλούνται από την ολομέλεια. Η Αρχή καταρτίζει τον κανονισμό λειτουργίας της, με τον οποίο ρυθμίζονται ιδίως η κατανομή αρμοδιοτήτων μεταξύ των μελών της, η προηγούμενη ακρόαση των ενδιαφερομένων, θέματα πειθαρχικής διαδικασίας και ο τρόπος διεξαγωγής των κατά την περίπτωση η' της παρ. 1 του παρόντος άρθρου ελέγχων.

4. Η Αρχή τηρεί τα ακόλουθα μητρώα :

α) Μητρώο Αρχείων και Επεξεργασιών, στο οποίο περιλαμβάνονται τα αρχεία και οι επεξεργασίες που γνωστοποιούνται στην Αρχή.

β) Μητρώο Αδειών, στο οποίο περιλαμβάνονται οι άδειες που εκδίδει η Αρχή για την ίδρυση και λειτουργία αρχείων που περιέχουν ευαίσθητα δεδομένα.

γ) Μητρώο Διασυνδέσεων, στο οποίο περιλαμβάνονται οι δηλώσεις και οι άδειες που εκδίδει η Αρχή για τη διασύνδεση αρχείων.

δ) Μητρώο προσώπων που δεν επιθυμούν να περιλαμβάνονται σε αρχεία, τα οποία έχουν ως σκοπό την προώθηση προμήθειας αγαθών ή την παροχή υπηρεσιών εξ αποστάσεως.

ε) Μητρώο Αδειών Διαβίβασης, στο οποίο καταχωρίζονται οι άδειες διαβίβασης δεδομένων προσωπικού χαρακτήρα.

στ) Μητρώο Απόρρητων Αρχείων, στο οποίο καταχωρίζονται, με απόφαση της Αρχής ύστερα από αίτηση του εκάστοτε υπεύθυνου επεξεργασίας, αρχεία που τηρούν τα Υπουργεία Εθνικής Άμυνας και Δημόσιας Τάξης καθώς και η Εθνική Υπηρεσία Πληροφοριών, για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Στο Μητρώο Απόρρητων Αρχείων καταχωρίζονται και οι διασυνδέσεις με ένα τουλάχιστον αρχείο της περίπτωσης αυτής.

5. Καθένας έχει πρόσβαση στα υπό στοιχεία α, β, γ, δ και ε μητρώα της προηγούμενης παραγράφου. Ύστερα από αίτηση του ενδιαφερόμενου και με απόφαση της Αρχής είναι δυνατό να επιτραπεί εν όλω ή εν μέρει, η πρόσβαση και στο Μητρώο Απόρρητων Αρχείων. Ύστερα από αίτηση του υπεύθυνου επεξεργασίας ή του εκπροσώπου του και με απόφαση της Αρχής είναι δυνατόν να απαγορευθεί, εν όλω ή εν μέρει, η πρόσβαση στο Μητρώο Αδειών Διαβίβασης, εφ' όσον από αυτήν θα προέκυπτε κίνδυνος για την ιδιωτική ζωή τρίτου, την εθνική ασφάλεια, τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων και την εκπλήρωση των υποχρεώσεων της χώρας που απορρέουν από διεθνείς συμβάσεις.

6. Ο Πρόεδρος εκπροσωπεί την Αρχή ενώπιον κάθε άλλης αρχής, καθώς και σε επιτροπές και ομάδες, συνεδριάσεις και συνόδους οργάνων της Ευρωπαϊκής Ένωσης καθώς και άλλων διεθνών οργανισμών και οργάνων που προβλέπονται από διεθνείς συμβάσεις ή στις οποίες μετέχουν εκπρόσωποι αντίστοιχων αρχών άλλων χωρών. Ο Πρόεδρος μπορεί να αναθέτει την εκπροσώπηση της Αρχής σε μέλος της, αναπληρωτή ή και υπάλληλο του κλάδου ελεγκτών της Γραμματείας.

7. Στον Πρόεδρο της Αρχής ανήκει η ευθύνη της λειτουργίας της καθώς και της λειτουργίας της Γραμματείας. Ο Πρόεδρος μπορεί να εξουσιοδοτεί μέλος της Αρχής ή τον προϊστάμενο της Γραμματείας ή προϊστάμενο υπηρεσίας της Γραμματείας να υπογράφει με «εντολή Προέδρου» έγγραφα, εντάλματα πληρωμής ή άλλες πράξεις. Ο Πρόεδρος είναι ο διοικητικός προϊστάμενος του προσωπικού της Γραμματείας, ασκεί την επ' αυτού πειθαρχική εξουσία και μπορεί να επιβάλλει πειθαρχική ποινή το πολύ προστίμου ίσου προς το ήμισυ των μηνιαίων αποδοχών του εγκαλουμένου.

7α. Όταν η προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων επιβάλλει την άμεση λήψη απόφασης, ο Πρόεδρος μπορεί ύστερα από αίτηση του ενδιαφερόμενου, να εκδίδει προσωρινή διαταγή για άμεση, ολική ή μερική, αναστολή της επεξεργασίας ή της λειτουργίας του αρχείου. Η διαταγή ισχύει μέχρι την έκδοση της οριστικής απόφασης από την Αρχή. Την παραπάνω αρμοδιότητα έχει και η Αρχή, όταν επιλαμβάνεται επί του θέματος.

8. Οι κανονιστικές αποφάσεις της Αρχής δημοσιεύονται στην Εφημερίδα της Κυβερνήσεως. Οι λοιπές αποφάσεις της Αρχής ισχύουν από την έκδοση ή την κοινοποίησή τους.

9. Ένδικα βοηθήματα κατά των αποφάσεων της Αρχής μπορεί να ασκεί και το Δημόσιο. Το ένδικο βοήθημα ασκεί ο κατά περίπτωση αρμόδιος υπουργός. Σε κάθε δίκη που αφορά απόφαση της Αρχής διάδικος είναι η ίδια εκπροσωπούμενη από τον πρόεδρο. Η παράσταση στο δικαστήριο γίνεται είτε από μέλος του Νομικού Συμβουλίου του Κράτους είτε από μέλος της Αρχής, τακτικό ή αναπληρωματικό, ή ελεγκτή που είναι δικηγόρος και ενεργεί με εντολή του Προέδρου χωρίς αμοιβή.

10. Κάθε δημόσια αρχή παρέχει τη συνδρομή της στην Αρχή.

Άρθρο 20: Γραμματεία της Αρχής

1. Η Αρχή εξυπηρετείται από Γραμματεία. Η Γραμματεία λειτουργεί σε επίπεδο Διευθύνσεως. Η υπηρεσιακή κατάσταση των υπαλλήλων της διέπεται από τις διατάξεις που ισχύουν εκάστοτε για τους δημόσιους διοικητικούς υπαλλήλους.

2. Η οργάνωση της Γραμματείας, η διαίρεση της σε τμήματα και γραφεία και οι επί μέρους αρμοδιότητες τούτων, ο αριθμός των θέσεων του προσωπικού κατά κλάδους και ειδικότητες και κάθε άλλη αναγκαία λεπτομέρεια καθορίζονται με προεδρικό διάταγμα που εκδίδεται με πρόταση των Υπουργών Εσωτερικών Δημόσιας Διοίκησης & Αποκέντρωσης, Οικονομικών και Δικαιοσύνης, ύστερα από εισήγηση της Αρχής, η οποία διατυπώνεται μέσα σε δύο (2) μήνες από τη συγκρότησή της. Με το αυτό διάταγμα προβλέπεται συγκρότηση, ως υπηρεσιακής μονάδας της Γραμματείας, τμήματος Ελεγκτών, η πρόσληψη και η υπηρεσιακή κατάσταση των υπαλλήλων του οποίου ρυθμίζεται κατά παρέκκλιση από τις εκάστοτε ισχύουσες διατάξεις. Ο προϊστάμενος της Γραμματείας προέρχεται υποχρεωτικά από τον κλάδο ελεγκτών. Ο αριθμός των θέσεων του πάσης φύσεως προσωπικού της Γραμματείας δεν μπορεί να υπερβαίνει τις τριάντα (30).

3. Η πλήρωση των θέσεων της Γραμματείας γίνεται σύμφωνα με τις εκάστοτε ισχύουσες διατάξεις για την πρόσληψη δημόσιων υπαλλήλων. Ειδικά για τους υπαλλήλους του κλάδου ελεγκτών της Γραμματείας η πρόσληψή τους γίνεται από την Αρχή, με επιλογή ή διαγωνισμό, ύστερα από προκήρυξή της.

4. Τα θέματα υπηρεσιακής κατάστασης του προσωπικού της Γραμματείας κρίνονται από υπηρεσιακό συμβούλιο, που συγκροτείται με απόφαση του Προέδρου της Αρχής και αποτελείται από δύο (2) μέλη της, έναν (1) υπάλληλο που ορίζεται από αυτήν και δύο (2) αιρετούς εκπροσώπους των υπαλλήλων. Κατά τα λοιπά εφαρμόζονται οι εκάστοτε ισχύουσες διατάξεις για τα υπηρεσιακά συμβούλια του προσωπικού των δημόσιων υπηρεσιών και των νομικών προσώπων δημοσίου δικαίου.

5. Οι τακτικοί υπάλληλοι της Γραμματείας της Αρχής υπάγονται ως προς την επικουρική ασφάλισή τους στο Ταμείο Αρωγής Προσωπικού Υπηρεσιών Αρμοδιότητος Υπουργείου Δικαιοσύνης. Όσοι προέρχονται από άλλες υπηρεσίες μπορούν να διατηρήσουν τα ταμεία ασφαλίσεως της προηγούμενης υπηρεσίας τους. Οι υπάλληλοι της Γραμματείας ασφαλίζονται υποχρεωτικώς στο Ταμείο Νομικών, υπό τους αυτούς όρους με τους οποίους ασφαλίζονται και οι λοιποί έμμισθοι ασφαλισμένοι του. Οι διατάξεις της παραγράφου αυτής έχουν εφαρμογή και επί των υπαλλήλων που μετατάσσονται στη Γραμματεία της Αρχής από νομικά πρόσωπα ιδιωτικού δικαίου.

6. Κατά την πρώτη εφαρμογή του παρόντος, η πλήρωση των θέσεων προϊσταμένων υπηρεσιακών μονάδων της Γραμματείας, εκτός του Τμήματος Ελεγκτών, γίνεται ύστερα από προκήρυξη της Αρχής, είτε με μετάταξη υπαλλήλων βαθμού Α' ή αντίστοιχου του Δημοσίου ή νομικών προσώπων δημοσίου δικαίου, είτε με διορισμό. Διορισμός γίνεται μόνο στις θέσεις που δεν θα πληρωθούν με μετάταξη. Η επιλογή των μετατασσομένων ή διοριζομένων γίνεται από την Αρχή. Ο διορισμός των επιλεγομένων από την Αρχή γίνεται με απόφαση του Υπουργού Δικαιοσύνης και η μετάταξη με απόφαση του ίδιου και του οικείου Υπουργού. Για την μετάταξη δεν απαιτείται γνώμη του οικείου υπηρεσιακού συμβουλίου της υπηρεσίας από
την οποία μετατάσσεται ο υπάλληλος. Τον προϊστάμενο της Γραμματείας επιλέγει η Αρχή από τους υπαλλήλους του κλάδου ελεγκτών, κατά παρέκκλιση από κάθε άλλη διάταξη.

7. Κατά την πρώτη εφαρμογή του παρόντος οι λοιπές θέσεις της Γραμματείας πληρούνται με τις προϋποθέσεις και την διαδικασία της προηγούμενης παραγράφου. Προτιμούνται υποψήφιοι που έχουν αποδεδειγμένη εμπειρία σε θέματα πληροφορικής. Για τους υπαλλήλους του κλάδου ελεγκτών ισχύουν οι διατάξεις της παρ. 3 του παρόντος άρθρου.

8. Ο χρόνος της προηγούμενης υπηρεσίας των μετατασσομένων από νομικά πρόσωπα δημοσίου δικάιου ή νομικά πρόσωπα ιδιωτικού δικαίου λογίζεται ως χρόνος πραγματικής δημόσιας υπηρεσίας για κάθε συνέπεια.

9. Οι διατάξεις της παρ. 4 του άρθρου 18 εφαρμόζονται και επί των υπαλλήλων της Γραμματείας.

ΚΕΦΑΛΑΙΟ Ε'

ΚΥΡΩΣΕΙΣ

Άρθρο 21: Διοικητικές κυρώσεις

1. Η Αρχή επιβάλλει στους υπεύθυνους επεξεργασίας ή στους τυχόν εκπροσώπους τους τις ακόλουθες διοικητικές κυρώσεις, για παράβαση των υποχρεώσεών τους που απορρέουν από τον παρόντα νόμο και από κάθε άλλη ρύθμιση που αφορά την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα :

α) Προειδοποίηση, με αποκλειστική προθεσμία για άρση της παράβασης.

β) Χρηματικό πρόστιμο.

γ) Προσωρινή ανάκληση άδειας.

δ) Οριστική ανάκληση άδειας.

ε) Καταστροφή αρχείου ή διακοπή επεξεργασίας και καταστροφή των σχετικών δεδομένων.

2. Οι υπό στοιχεία β, γ, δ και ε διοικητικές κυρώσεις της προηγούμενης παραγράφου επιβάλλονται πάντοτε ύστερα από ακρόαση του υπεύθυνου επεξεργασίας ή του εκπροσώπου του. Είναι ανάλογες προς τη βαρύτητα της παράβασης που καταλογίζεται. Οι υπό στοιχεία γ, δ και ε διοικητικές κυρώσεις επιβάλλονται σε περιπτώσεις ιδιαίτερα σοβαρής ή καθ' υποτροπήν παράβασης. Πρόστιμο μπορεί να επιβληθεί σωρευτικά και με τις υπό στοιχεία γ, δ και ε κυρώσεις. Εάν επιβληθεί η κύρωση της καταστροφής αρχείου, για την καταστροφή ευθύνεται ο υπεύθυνος επεξεργασίας αρχείου, στον οποίο μπορεί να επιβληθεί και πρόστιμο για μη συμμόρφωση.

3. Τα ποσά των προστίμων της παρ. 1 μπορεί να αναπροσαρμόζονται με απόφαση του Υπουργού Δικαιοσύνης, ύστερα από πρόταση της Αρχής.

4. Οι πράξεις της Αρχής με τις οποίες επιβάλλονται πρόστιμα συνιστούν εκτελεστό τίτλο και επιδίδονται στον υπεύθυνο επεξεργασίας ή τον τυχόν εκπρόσωπό του. Η είσπραξη των προστίμων γίνεται κατά τις διατάξεις του Κώδικα Εισπράξεως Δημοσίων Εσόδων (ΚΕΔΕ).

Άρθρο 22: Ποινικές κυρώσεις

1. Όποιος παραλείπει να γνωστοποιήσει στην Αρχή, κατά το άρθρο 6 του παρόντος νόμου τη σύσταση και λειτουργία αρχείου ή οποιαδήποτε μεταβολή στους όρους και τις προϋποθέσεις χορηγήσεως της άδειας που προβλέπεται από την παρ. 3 του άρθρου 7 του παρόντος νόμου, τιμωρείται με φυλάκιση έως τριών (3) ετών και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

2. Όποιος κατά παράβαση του άρθρου 7 του παρόντος νόμου διατηρεί αρχείο χωρίς άδεια ή κατά παράβαση των όρων και προϋποθέσεων της άδειας της Αρχής, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

3. Όποιος κατά παράβαση του άρθρου 8 του παρόντος νόμου προβαίνει σε διασύνδεση αρχείων χωρίς να την γνωστοποιήσει στην Αρχή, τιμωρείται με φυλάκιση έως τριών (3) ετών και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

Όποιος προβαίνει σε διασύνδεση αρχείων χωρίς την άδεια της Αρχής, όπου αυτή απαιτείται ή κατά παράβαση των όρων της άδειας που του έχει χορηγηθεί, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

4. Όποιος χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση των δεδομένων αυτών ή τα αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει, ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων, ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή και αν πρόκειται για ευαίσθητα δεδομένα με φυλάκιση τουλάχιστον ενός (1) τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών, αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.

5. Υπεύθυνος επεξεργασίας που δεν συμμορφώνεται με τις αποφάσεις της Αρχής που εκδίδονται για την ικανοποίηση του δικαιώματος πρόσβασης, σύμφωνα με την παρ. 4 του άρθρου 12, για την ικανοποίηση του δικαιώματος αντίρρησης, σύμφωνα με την παρ. 2 του άρθρου 13, καθώς και με πράξεις επιβολής των διοικητικών κυρώσεων των περιπτώσεων γ', δ' και ε' της παρ. 1 του άρθρου 21 τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και με χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών. Με τις ποινές του προηγούμενου εδαφίου τιμωρείται ο υπεύθυνος επεξεργασίας που διαβιβάζει δεδομένα προσωπικού χαρακτήρα κατά παράβαση του άρθρου 9 καθώς και εκείνος που δεν συμμορφώνεται προς την δικαστική απόφαση του άρθρου 14 του παρόντος νόμου.

6.Αν ο υπαίτιος των πράξεων των παρ. 1 έως 5 του παρόντος άρθρου είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, ή να βλάψει τρίτον, επιβάλλεται κάθειρξη έως δέκα (10) ετών και χρηματική ποινή τουλάχιστον δύο εκατομμυρίων (2.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών.

7. Αν από τις πράξεις των παρ. 1 έως και 5 του παρόντος άρθρου προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή τουλάχιστον πέντε εκατομμυρίων (5.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών.

8. Αν οι πράξεις των παρ. 1 έως 5 του παρόντος άρθρου τελέσθηκαν από αμέλεια, επιβάλλεται φυλάκιση έως τριών (3) ετών και χρηματική ποινή.

9. Για την εφαρμογή των διατάξεων του παρόντος άρθρου, αν υπεύθυνος επεξεργασίας δεν είναι φυσικό πρόσωπο, ευθύνεται ο εκπρόσωπος του νομικού προσώπου ή ο επικεφαλής της δημόσιας αρχής ή υπηρεσίας ή οργανισμού αν ασκεί και ουσιαστικά τη διοίκηση ή διεύθυνση αυτών.

10. Για τα εγκλήματα του παρόντος άρθρου ο Πρόεδρος και τα μέλη της Αρχής καθώς και οι προς τούτο ειδικά εντεταλμένοι υπάλληλοι του τμήματος ελεγκτών της Γραμματείας, είναι ειδικοί ανακριτικοί υπάλληλοι και έχουν όλα τα δικαιώματα που προβλέπει σχετικά ο Κώδικας Ποινικής Δικονομίας. Μπορούν να

διενεργούν προανάκριση και χωρίς εισαγγελική παραγγελία, όταν πρόκειται για αυτόφωρο κακούργημα ή πλημμέλημα ή υπάρχει κίνδυνος από την αναβολή.

11. Για τα εγκλήματα της παρ. 5 του παρόντος άρθρου καθώς επίσης και σε κάθε άλλη περίπτωση όπου προηγήθηκε διοικητικός έλεγχος από την Αρχή, ο Πρόεδρος αυτής ανακοινώνει γραπτώς στον αρμόδιο εισαγγελέα οτιδήποτε αποτέλεσε αντικείμενο έρευνας από την Αρχή και διαβιβάζει σε αυτόν όλα τα στοιχεία και τις αποδείξεις.

12. Η προανάκριση για τα εγκλήματα του παρόντος άρθρου περατώνεται μέσα σε δύο (2) το πολύ μήνες από την άσκηση της ποινικής δίωξης και εφόσον υπάρχουν αποχρώσες ενδείξεις για την παραπομπή του κατηγορουμένου σε δίκη, η δικάσιμος ορίζεται σε ημέρα που δεν απέχει περισσότερο από τρεις (3) μήνες από το πέρας της προανάκρισης ή αν η παραπομπή έγινε με βούλευμα δύο (2) μήνες από τότε που αυτό έγινε αμετάκλητο. Σε περίπτωση εισαγωγής της υπόθεσης με απευθείας κλήση του κατηγορουμένου στο ακροατήριο δεν επιτρέπεται η προσφυγή κατά του κλητηρίου θεσπίσματος.

13. Δεν επιτρέπεται αναβολή της δίκης για τα εγκλήματα του παρόντος άρθρου παρά μόνον μία φορά για εξαιρετικά σοβαρό λόγο. Στην περίπτωση αυτή ορίζεται ρητή δικάσιμος, που δεν απέχει περισσότερο από δύο (2) μήνες και η υπόθεση εκδικάζεται κατ' εξαίρεση πρώτη.

14. Τα κακουργήματα που προβλέπονται από τον παρόντα νόμο υπάγονται στην αρμοδιότητα του δικαστηρίου των εφετών.

Άρθρο 23: Αστική ευθύνη

1. Φυσικό πρόσωπο ή νομικό πρόσωπο ιδιωτικού δικαίου, που κατά παράβαση του παρόντος νόμου, προκαλεί περιουσιακή βλάβη, υποχρεούται σε πλήρη αποζημίωση. Αν προκάλεσε ηθική βλάβη, υποχρεούται σε χρηματική ικανοποίηση. Η ευθύνη υπάρχει και όταν ο υπόχρεος όφειλε να γνωρίζει την πιθανότητα να επέλθει βλάβη σε άλλον.

2. Η κατά το άρθρο 932 ΑΚ χρηματική ικανοποίηση λόγω ηθικής βλάβης για παράβαση του παρόντος νόμου ορίζεται κατ' ελάχιστο στο ποσό των δύο εκατομμυρίων (2.000.000) δραχμών, εκτός αν ζητήθηκε από τον ενάγοντα μικρότερο ποσό ή η παράβαση οφείλεται σε αμέλεια. Η χρηματική αυτή ικανοποίηση επιδικάζεται ανεξαρτήτως από την αιτούμενη αποζημίωση για περιουσιακή βλάβη.

3. Οι απαιτήσεις του παρόντος άρθρου εκδικάζονται κατά τα άρθρα 664 - 676 του Κώδικα Πολιτικής Δικονομίας, ανεξάρτητα από την τυχόν έκδοση ή μη απόφασης της Αρχής ή την τυχόν άσκηση ποινικής δίωξης, καθώς και από την αναστολή ή αναβολή της για οποιοδήποτε λόγο. Η απόφαση του δικαστηρίου εκδίδεται μέσα σε δύο (2) μήνες από την πρώτη συζήτηση στο ακροατήριο.

ΚΕΦΑΛΑΙΟ ΣΤ'
ΤΕΛΙΚΕΣ - ΜΕΤΑΒΑΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 24: Υποχρεώσεις υπεύθυνου επεξεργασίας

1. Οι υπεύθυνοι επεξεργασίας αρχείων τα οποία λειτουργούν κατά την έναρξη ισχύος του παρόντος νόμου, υποχρεούνται να υποβάλλουν την κατά το άρθρο 6 γνωστοποίηση λειτουργίας στην Αρχή μέσα σε έξι (6) μήνες από την έναρξη λειτουργίας της Αρχής.

2. Την ίδια υποχρέωση έχουν και οι υπεύθυνοι επεξεργασίας αρχείων με ευαίσθητα δεδομένα, τα οποία λειτουργούν κατά την έναρξη ισχύος του παρόντος νόμου, προκειμένου να εκδοθεί η κατά την παρ. 3 του άρθρου 7 άδεια.

3. Για αρχεία που λειτουργούν και επεξεργασίες που εκτελούνται κατά την έναρξη ισχύος του παρόντος νόμου οι υπεύθυνοι επεξεργασίας οφείλουν να προβούν στην κατά την παρ. 1 του άρθρου 11 ενημέρωση των υποκειμένων μέσα σε έξι (6) μήνες από την έναρξη λειτουργίας της Αρχής. Η ενημέρωση, εφόσον αφορά μεγάλο αριθμό υποκειμένων μπορεί να γίνει και δια του τύπου. Στην περίπτωση αυτή τις λεπτομέρειες καθορίζει η Αρχή. Οι διατάξεις της παρ. 4 του άρθρου 11 έχουν εφαρμογή και εν προκειμένω.

4. Για τα εξ ολοκλήρου μη αυτοματοποιημένα αρχεία οι προθεσμίες των προηγουμένων παραγράφων είναι ενός (1) χρόνου.

5. Οι διατάξεις των άρθρων 11, 12, 13, και 19 παρ. 1 του παρόντος νόμου δεν εφαρμόζονται στο ποινικό μητρώο και στα υπηρεσιακά αρχεία που τηρούνται από τις αρμόδιες δικαστικές αρχές για την εξυπηρέτηση των αναγκών της λειτουργίας της ποινικής δικαιοσύνης και στο πλαίσιο της λειτουργίας της.

Άρθρο 25: Έναρξη λειτουργίας της Αρχής

1. Μέσα σε εξήντα (60) μέρες από την έναρξη ισχύος του παρόντος νόμου, διορίζεται ο Πρόεδρος της Αρχής και ο αναπληρωτής του. Μέσα στην ίδια προθεσμία ο Υπουργός Δικαιοσύνης υποβάλει στον Πρόεδρο της Βουλής πρόταση για τον διορισμό των τεσσάρων τακτικών μελών της Αρχής και των ισάριθμων αναπληρωτών τους.

2. Ο χρόνος της έναρξης λειτουργίας της Αρχής ορίζεται με απόφαση του Υπουργού Δικαιοσύνης που εκδίδεται το αργότερο μέσα σε τέσσερις (4) μήνες μετά τη συγκρότηση της Αρχής. Από τον διορισμό των μελών της και έως την κατά τις παρ. 6 και 7 του άρθρου 20 του παρόντος νόμου πλήρωση των θέσεων της Γραμματείας της, η Αρχή εξυπηρετείται από προσωπικό το οποίο αποσπάται προσωρινά σε αυτήν, με απόφασή της, κατά παρέκκλιση από κάθε άλλη διάταξη.

3. Έως ότου η Αρχή λειτουργήσει σύμφωνα με την προηγούμενη παράγραφο, η εκκαθάριση των δαπανών της γίνεται από τη Διεύθυνση Οικονομικού της Κεντρικής Υπηρεσίας του Υπουργείου Δικαιοσύνης, σε βάρος του προϋπολογισμού του Υπουργείου Δικαιοσύνης.

4. Η κατά την παρ. 2 του παρόντος άρθρου απόφαση του Υπουργού Δικαιοσύνης για τον χρόνο έναρξης λειτουργίας της Αρχής δημοσιεύεται στην Εφημερίδα της Κυβερνήσεως και σε τέσσερις (4) τουλάχιστον

ημερήσιες πολιτικές εφημερίδες ευρείας κυκλοφορίας που εκδίδονται στην Αθήνα και την Θεσσαλονίκη και σε δύο (2) τουλάχιστον ημερήσιες οικονομικές εφημερίδες.

6.2 ΝΟΜΟΣ 3471/2006 : Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ

Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Ενσωμάτωση της Οδηγίας
2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης ουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, ΕΕ L 201/37 της 31ης Ιουλίου 2002).

Άρθρο 1: Σκοπός

Σκοπός των διατάξεων των άρθρων 1 έως 17 του παρόντος νόμου είναι η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών.

Άρθρο 2: Ορισμοί

Πέραν των ορισμών που περιλαμβάνονται στο άρθρο 2 του ν. 2472/1997 (ΦΕΚ 50 Α'), όπως ισχύει, λαμβανομένων δε υπόψη των ορισμών του ν. 3431/2006 (ΦΕΚ 13 Α') νοούνται, για τους σκοπούς του νόμου αυτού, ως:

1. «συνδρομητής»: κάθε φυσικό ή νομικό πρόσωπο που έχει συνάψει σύμβαση με φορέα παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών για την παροχή των υπηρεσιών αυτών.

2. «χρήστης»: κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας.

3. «δεδομένα κίνησης»: τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσης της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων,

πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της επικοινωνίας καθώς και το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία.

4. «δεδομένα θέσης»: τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών ή από μια υπηρεσία ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μια διαθέσιμης στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών.»

5. «επικοινωνία»: κάθε πληροφορία που ανταλλάσσεται ή διαβιβάζεται μεταξύ ενός πεπερασμένου αριθμού μερών, μέσω μίας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Δεν περιλαμβάνονται πληροφορίες που διαβιβάζονται ως τμήμα ραδιοτηλεοπτικών υπηρεσιών στο κοινό μέσω δικτύου ηλεκτρονικών επικοινωνιών, εκτός από τις περιπτώσεις κατά τις οποίες οι πληροφορίες μμπορούν να αφορούν αναγνωρίσιμο συνδρομητή ή χρήστη που τις λαμβάνει.

6. «Υπηρεσία προστιθέμενης αξίας»: κάθε υπηρεσία η οποία επιβάλλει την επεξεργασία δεδομένων κίνησης ή δεδομένων θέσης πέραν εκείνων που απαιτούνται για τη μετάδοση μίας επικοινωνίας και τη χρέωση της.

7. «Ηλεκτρονικό ταχυδρομείο»: 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.

8. «Υπηρεσίες ηλεκτρονικών επικοινωνιών»: οι υπηρεσίες που παρέχονται συνήθως έναντι αμοιβής και των οποίων η παροχή συνίσταται, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοτηλεοπτικές μεταδόσεις. Στις υπηρεσίες ηλεκτρονικών επικοινωνιών δεν περιλαμβάνονται υπηρεσίες παροχής ή ελέγχου περιεχομένου που μεταδίδεται μέσω δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και υπηρεσίες της Κοινωνίας της Πληροφορίας, όπως αυτές ορίζονται στην παράγραφο 2 του άρθρου 2 του π.δ. 39/2001 (ΦΕΚ 28 Α'), και που δεν αφορούν, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών. «Στον ορισμό αυτόν, περιλαμβάνονται τα σύντομα μηνύματα κειμένου, μηνύματα πολυμέσων και άλλες παρεμφερείς εφαρμογές.»

9. «Δημόσιο δίκτυο επικοινωνιών»: το δίκτυο ηλεκτρονικών επικοινωνιών, το οποίο χρησιμοποιείται, εξ ολοκλήρου ή κυρίως, για την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών.

10. «Διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών»: οι υπηρεσίες ηλεκτρονικών επικοινωνιών που παρέχονται στο κοινό.

11. «Παραβίαση δεδομένων προσωπικού χαρακτήρα»: η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη διάδοση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάσθηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατά οποιονδήποτε άλλο τρόπο σε επεξεργασία σε συνάρτηση με την παροχή

* Το στοιχείο 4 αντικαταστάθηκε ως άνω με το άρθρο 168, παρ. 1 στοιχ. α' του Ν. 4070/2012 (ΦΕΚ Α 82/2012).

** Το στοιχείο 6 διαγράφηκε και τα στοιχεία 7-11 αναριθμήθηκαν σε στοιχεία 6-10 ως άνω, σύμφωνα με το άρθρο 168, παρ. 1 στοιχ. β' του Ν. 4070/2012 (ΦΕΚ Α 82/2012).
*** Στο στοιχείο 8 προστέθηκε το εντός «» εδάφιο, σύμφωνα με το άρθρο 168, παρ. 1 στοιχ. γ' του Ν. 4070/2012 (ΦΕΚ Α 82/2012). διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.»

Άρθρο 3: Πεδίο εφαρμογής

«**1.** Οι διατάξεις των άρθρων 1 έως 17 του παρόντος νόμου έχουν εφαρμογή κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών, στο πλαίσιο της παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών περιλαμβανομένων αυτών που υποστηρίζουν συσκευές συλλογής δεδομένων και ταυτοποίησης. Για την επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται στο πλαίσιο μη διαθεσίμων στο κοινό δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, εφαρμόζεται ο ν. 2472/1997 (Α`50), όπως ισχύει.»
2. Ο ν. 2472/1997, όπως ισχύει, και οι εκτελεστικοί του άρθρου 19 του
Συντάγματος νόμοι, όπως ισχύουν, εφαρμόζονται για κάθε ζήτημα σχετικό με την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών, που δεν ρυθμίζεται ειδικότερα από τον παρόντα νόμο.
3. Οι διατάξεις των άρθρων 8 και 9 εφαρμόζονται στις γραμμές συνδρομητών που συνδέονται με ψηφιακά κέντρα και, όταν αυτό είναι τεχνικώς εφικτό, σε γραμμές συνδρομητών που συνδέονται με αναλογικά κέντρα, εφόσον τούτο δεν συνεπάγεται δυσανάλογη οικονομική επιβάρυνση. Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) διαπιστώνει τις περιπτώσεις όπου η σύνδεση με αναλογικά κέντρα είναι τεχνικώς αδύνατη ή απαιτεί δυσανάλογη επένδυση, και ενημερώνει σχετικώς την Ευρωπαϊκή Επιτροπή

Άρθρο 4: Απόρρητο

1. Οποιαδήποτε χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών που παρέχονται μέσω δημοσίου δικτύου επικοινωνιών και των διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης και θέσης, όπως ορίζονται στις διατάξεις του άρθρου 2 του παρόντος νόμου, προστατεύεται από το απόρρητο των επικοινωνιών. Η άρση του απορρήτου είναι επιτρεπτή μόνο υπό τις προϋποθέσεις και τις διαδικασίες που προβλέπονται από το άρθρο 19 του Συντάγματος.
2. Απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης, εκτός αν προβλέπεται άλλως από το νόμο.

3. Επιτρέπεται η καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης, όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων εμπορικής συναλλαγής ή άλλης επικοινωνίας επαγγελματικού χαρακτήρα, υπό την προϋπόθεση ότι και τα δύο μέρη, μετά από προηγούμενη ενημέρωση σχετικά με το σκοπό της καταγραφής, παρέχουν τη συγκατάθεση τους. Με πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, καθορίζεται ο τρόπος

ενημέρωσης των μερών και παροχής της συγκατάθεσης, καθώς και ο τρόπος και ο χρόνος διατήρησης των καταγεγραμμένων συνδιαλέξεων και των συναφών δεδομένων κίνησης.

4. Με την επιφύλαξη της τήρησης των υποχρεώσεων που απορρέουν από την προστασία του απορρήτου, σύμφωνα με τον παρόντα νόμο, επιτρέπεται η τεχνικής φύσεως αποθήκευση, η οποία είναι αναγκαία για τη διαβίβαση της επικοινωνίας.

«**5.** Η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται μόνο αν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεση του μετά από σαφή και εκτενή ενημέρωση κατά την παρ. 1 του άρθρου 11 του ν. 2472/1997, όπως ισχύει. Η συγκατάθεση του συνδρομητή ή χρήστη μπορεί να δίδεται μέσω κατάλληλων ρυθμίσεων στο φυλλομετρητή ιστού ή μέσω άλλης εφαρμογής. Τα παραπάνω δεν εμποδίζουν την οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή η οποία είναι αναγκαία για την παροχή υπηρεσίας της κοινωνίας της πληροφορίας, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής. Με πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) ορίζονται ειδικότερα οι τρόποι παροχής πληροφοριών και δήλωσης της συγκατάθεσης.»

4. Προστέθηκε στοιχείο με αρ. 11 ως άνω, σύμφωνα με το άρθρο 168, παρ. 1 στοιχ. δ' του Ν. 4070/2012 (ΦΕΚ Α 82/2012).

5. Η παρ. 1 αντικαταστάθηκε ως άνω με το άρθρο 169 του Ν. 4070/2012 (ΦΕΚ Α 82/2012).

Άρθρο 5 : Κανόνες επεξεργασίας

«**1.** Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, περιλαμβανομένων των δεδομένων κίνησης και θέσης, πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των σκοπών της.

2. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον εφόσον:

α) ο συνδρομητής ή ο χρήστης μετά από ενημέρωση για το είδος των δεδομένων, το σκοπό και την έκταση της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών έχει συγκατατεθεί, ή

β) η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία ο συνδρομητής ή ο χρήστης είναι συμβαλλόμενο μέρος, ή για τη λήψη μέτρων κατά το προσυμβατικό στάδιο, μετά από αίτηση του συνδρομητή.

3. Όπου ο παρών νόμος απαιτεί τη συγκατάθεση του συνδρομητή ή χρήστη, η σχετική δήλωση δίδεται εγγράφως ή με ηλεκτρονικά μέσα. Στην τελευταία περίπτωση, ο υπεύθυνος επεξεργασίας εξασφαλίζει ότι ο συνδρομητής ή χρήστης ενεργεί με πλήρη επίγνωση των συνεπειών που έχει η δήλωσή του η οποία καταγράφεται με ασφαλή τρόπο, είναι ανά πάσα στιγμή προσβάσιμη στον χρήστη ή συνδρομητή και μπορεί οποτεδήποτε να ανακληθεί.

4. Ο σχεδιασμός και η επιλογή των τεχνικών μέσων και των πληροφοριακών συστημάτων, καθώς και ο εξοπλισμός για την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, πρέπει να γίνονται με βασικό κριτήριο την επεξεργασία όσο το δυνατόν λιγότερων δεδομένων προσωπικού χαρακτήρα.

5. Ο φορέας παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει, στο βαθμό που αυτό είναι τεχνικώς εφικτό και με την επιφύλαξη του ν. 3783/2009 (Α` 136), όπως ισχύει, να καθιστά δυνατή τη χρήση και πληρωμή των υπηρεσιών αυτών ανωνύμως ή με ψευδώνυμο. Σε περίπτωση αμφισβήτησης της τεχνικής δυνατότητας της ανώνυμης και ψευδώνυμης χρήσης και πληρωμής των υπηρεσιών αυτών, γνωμοδοτεί η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.).»

* Η παρ. 5 του άρθρου 4 αντικαταστάθηκε ως άνω με το άρθρο 170 του Ν. 4070/2012 (ΦΕΚ Α 82/2012).

Άρθρο 6: Δεδομένα κίνησης και θέσης

«**1.** 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 επικοινωνιών, με τη λήξη της επικοινωνίας καταστρέφονται ή καθίστανται ανώνυμα, με την επιφύλαξη του ν. 3917/2011 (Α`22), καθώς και των παραγράφων 2 έως 6 του παρόντος άρθρου.

2. Για τη χρέωση των συνδρομητών και την πληρωμή των διασυνδέσεων, εφόσον είναι αναγκαίο, ο φορέας παροχής δημόσιου δικτύου ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, επιτρέπεται να επεξεργάζεται τα δεδομένα κίνησης. Ο φορέας παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών ενημερώνει τον συνδρομητή σχετικά με τον τύπο των δεδομένων κίνησης που υποβάλλονται σε επεξεργασία, καθώς και σχετικά με τη διάρκεια της επεξεργασίας. Η επεξεργασία αυτή για το σκοπό της χρέωσης και πληρωμής επιτρέπεται για χρονικό διάστημα που δεν μπορεί να υπερβαίνει τους δώδεκα (12) μήνες από την ημερομηνία της επικοινωνίας, εκτός και αν αμφισβητήθηκε ο λογαριασμός ή δεν εξοφλήθηκε. Στην περίπτωση αυτή η επεξεργασία επιτρέπεται μέχρι την αμετάκλητη επίλυση της διαφοράς. Η διαβίβαση των δεδομένων κίνησης σε άλλο φορέα παροχής δημοσίου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών επιτρέπεται για το σκοπό της χρέωσης των παρεχόμενων υπηρεσιών, υπό τον όρο ότι ο συνδρομητής ή ο χρήστης ενημερώνεται με τρόπο σαφή και πρόσφορο, εγγράφως ή με ηλεκτρονικά μέσα,

κατά την κατάρτιση της σύμβασης ή πριν τη διαβίβαση. Ομοίως, επιτρέπεται η διαβίβαση των αναγκαίων δεδομένων κίνησης και των δεδομένων προσωπικού χαρακτήρα που αφορούν στη σύμβαση με αποκλειστικό σκοπό την είσπραξη του λογαριασμού, υπό τον όρο ότι ο συνδρομητής ή ο χρήστης ενημερώνεται με τρόπο σαφή και πρόσφορο, εγγράφως ή με ηλεκτρονικά μέσα, κατά την κατάρτιση της σύμβασης ή πριν τη διαβίβαση.

3. Για την εμπορική προώθηση των υπηρεσιών ηλεκτρονικών επικοινωνιών ή για την παροχή υπηρεσιών προστιθέμενης αξίας, ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών δύναται να επεξεργάζεται τα δεδομένα κίνησης στην απαιτούμενη έκταση και για την απαιτούμενη διάρκεια, αντιστοίχως, μόνον εφόσον ο συνδρομητής ή χρήστης έχει προηγουμένως
συγκατατεθεί αφού ενημερωθεί σχετικά με τον τύπο των δεδομένων κίνησης που

*Το άρθρο 5 αντικαταστάθηκε ως άνω με το άρθρο 171, παρ. 1 του Ν. 4070/2012 (ΦΕΚ Α 82/2012). υποβάλλονται σε επεξεργασία, καθώς και σχετικά με τη διάρκεια της επεξεργασίας. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε. Αν ανακληθεί και εφόσον τα δεδομένα έχουν εντωμεταξύ ανακοινωθεί σε τρίτους, η ανάκληση ανακοινώνεται σε αυτούς με φροντίδα του φορέα. Ο φορέας παροχής δημοσίου
δικτύου ή και διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, απαγορεύεται να εξαρτά την παροχή των υπηρεσιών αυτών προς το συνδρομητή ή το χρήστη από τη συγκατάθεση του στην επεξεργασία των δεδομένων αυτών, για σκοπούς άλλους από εκείνους που εξυπηρετούν άμεσα την παροχή των υπηρεσιών στις οποίες αφορούν τα άρθρα του παρόντος νόμου.

4. Επιτρέπεται η επεξεργασία δεδομένων που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του συνδρομητή ή χρήστη δημόσιου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών για την παροχή υπηρεσίας προστιθέμενης αξίας, μόνον εφόσον αυτά καθίστανται ανώνυμα ή με τη ρητή συγκατάθεση του συνδρομητή ή χρήστη, στην απαιτούμενη έκταση και για την απαιτούμενη διάρκεια για την παροχή μίας υπηρεσίας προστιθέμενης αξίας. Ο φορέας παροχής υπηρεσιών ενημερώνει τον χρήστη ή τον συνδρομητή, πριν από τη χορήγηση της συγκατάθεσης του, σχετικά με τον τύπο των δεδομένων που υποβάλλονται σε επεξεργασία, τους σκοπούς και τη διάρκεια της εν λόγω επεξεργασίας, καθώς και σχετικά με το ενδεχόμενο μετάδοσης τους σε τρίτους για το σκοπό παροχής της υπηρεσίας προστιθέμενης αξίας. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε. Στον χρήστη ή συνδρομητή πρέπει να παρέχεται η δυνατότητα, σε κάθε σύνδεση με το δίκτυο ή μετάδοση μίας επικοινωνίας, να αρνείται προσωρινά την επεξεργασία των εν λόγω δεδομένων με απλά μέσα και ατελώς.

5. Κατ` εξαίρεση επιτρέπεται, χωρίς προηγούμενη συγκατάθεση του συνδρομητή ή του χρήστη, η επεξεργασία δεδομένων θέσης από τους φορείς παροχής δημοσίου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών, προκειμένου να παρέχουν στις αρμόδιες για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης αρχές, όπως στις διωκτικές αρχές, στις υπηρεσίες πρώτων βοηθειών και πυρόσβεσης, τις απαραίτητες πληροφορίες για τον εντοπισμό του καλούντος και μόνο για το συγκεκριμένο αυτό σκοπό. Με

πράξη της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) καθορίζονται οι διαδικασίες, ο τρόπος και κάθε άλλη τεχνική λεπτομέρεια για την εφαρμογή της παρούσας διάταξης.

*Οι παράγραφοι 1 και 2 του παρόντος άρθρου δεν εφαρμόζονται όταν η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) ενημερώνεται από τα ενδιαφερόμενα πρόσωπα για τα δεδομένα κίνησης, με σκοπό την επίλυση διαφορών που σχετίζονται ιδίως με τη διασύνδεση ή τη χρέωση, σύμφωνα με τις διατάξεις της κείμενης νομοθεσίας.»

**Το άρθρο 6 αντικαταστάθηκε ως άνω με το άρθρο 171, παρ. 2 του Ν. 4070/2012 (ΦΕΚ Α 82/2012). κατά περίπτωση προσφορότερο τρόπο, για την αποστολή αναλυτικών λογαριασμών στον συνδρομητή. Σε περίπτωση επικοινωνίας χωρίς χρέωση, η κληθείσα σύνδεση δεν περιλαμβάνεται στους αναλυτικούς λογαριασμούς.

Άρθρο 7: Αναλυτική χρέωση

1. Οι συνδρομητές έχουν το δικαίωμα να λαμβάνουν μη αναλυτικούς λογαριασμούς. Όταν μία σύνδεση χρησιμοποιείται από πολλούς χρήστες ή όταν ο συνδρομητής είναι υπόχρεος για την πληρωμή της σύνδεσης που χρησιμοποιεί ένας ή περισσότεροι χρήστες, απαιτείται βεβαίωση του συνδρομητή ότι οι χρήστες έχουν ενημερωθεί ή θα ενημερωθούν.

2. Αν το ζητήσει ο συνδρομητής, ο φορέας παροχής δημοσίου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών οφείλει να διαγράφει από τον αναλυτικό λογαριασμό τα τρία τελευταία ψηφία των κληθέντων αριθμών-συνδέσεων.

Άρθρο 8: Ένδειξη της ταυτότητας και περιορισμός αναγνώρισης καλούσας και συνδεδεμένης γραμμής

1. Όταν παρέχεται η ένδειξη της ταυτότητας καλούσας γραμμής, ο καλών χρήστης πρέπει να έχει τη δυνατότητα, με απλά μέσα και ατελώς, να εμποδίζει αυτή τη λειτουργία ανά κλήση. Ο καλών συνδρομητής πρέπει να έχει τη δυνατότητα αυτή ανά γραμμή.

2. Όταν παρέχεται ένδειξη της ταυτότητας καλούσας γραμμής, ο καλούμενος χρήστης πρέπει να έχει τη δυνατότητα, με απλά μέσα και ατελώς, να μην επιτρέπει την ένδειξη της ταυτότητας της καλούσας γραμμής για τις εισερχόμενες κλήσεις.

3. Όταν παρέχεται ένδειξη της ταυτότητας καλούσας γραμμής και η ένδειξη αυτή γίνεται πριν γίνει οριστικά η κλήση, ο καλούμενος χρήστης πρέπει να έχει τη δυνατότητα, με απλά μέσα, να μη δέχεται την εισερχόμενη κλήση όταν ο καλών χρήστης ή συνδρομητής δεν έχει επιτρέψει την ένδειξη της ταυτότητας της καλούσας γραμμής.

4. Όταν παρέχεται ένδειξη της ταυτότητας της συνδεδεμένης γραμμής, ο καλούμενος χρήστης πρέπει να έχει τη δυνατότητα να απαλείφει, με απλά μέσα και ατελώς, την ένδειξη της ταυτότητας της συνδεδεμένης γραμμής στον καλούντα χρήστη.

Οι διατάξεις της παραγράφου 1 ισχύουν και για κλήσεις προς χώρες που δεν ανήκουν στην Ευρωπαϊκή Ένωση. Οι διατάξεις των παραγράφων 2, 3 και ισχύουν και για τις εισερχόμενες κλήσεις που προέρχονται από τρίτες χώρες.

6. Οι δυνατότητες που προβλέπονται στις παραγράφους 1 έως 4 παρέχονται από τον φορέα παροχής των υπηρεσιών ηλεκτρονικών επικοινωνιών. Όταν παρέχεται ένδειξη της ταυτότητας καλούσας ή και συνδεδεμένης γραμμής, οι φορείς παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ενημερώνουν, με κάθε πρόσφορο τρόπο ή μέσο, το κοινό και

τους συνδρομητές σχετικά με την ύπαρξη υπηρεσιών αναγνώρισης καλούσας ή και συνδεδεμένης γραμμής στο δίκτυο, τις υπηρεσίες που προσφέρονται, επί τη βάσει της αναγνώρισης καλούσας ή και συνδεδεμένης γραμμής, και τις δυνατότητες που ορίζονται στις παραγράφους 1 έως 4.

7. Ο φορέας παροχής δημοσίου δικτύου επικοινωνιών ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών οφείλει να διαθέτει μέσα εξουδετέρωσης της δυνατότητας μη αναγραφής της καλούσας γραμμής:

α) για τον εντοπισμό κακόβουλων ή ενοχλητικών κλήσεων για περιορισμένο χρονικό διάστημα, μετά από αίτηση του συνδρομητή. Τα δεδομένα που περιέχουν την αναγνώριση της ταυτότητας του καλούντος συνδρομητή ή χρήστη αποθηκεύονται και είναι διαθέσιμα από τον φορέα παροχής δημοσίου δικτύου ή και διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών μόνο έναντι του συνδρομητή ή χρήστη που ζητεί τον εντοπισμό και κατόπιν

διαγράφονται, εφόσον δεν ορίζεται διαφορετικά στον παρόντα νόμο.

Με πράξη της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.), καθορίζονται οι ειδικότερες διαδικασίες, ο τρόπος και η διάρκεια εξουδετέρωσης των δυνατοτήτων και κάθε άλλη αναγκαία λεπτομέρεια, ώστε να διασφαλίζεται η διαφάνεια της διαδικασίας.

β) για κλήσεις άμεσης επέμβασης προς τις αρμόδιες δημόσιες υπηρεσίες που ασχολούνται με τέτοιες κλήσεις ή προς ιδιωτικούς φορείς άμεσης επέμβασης, αναγνωρισμένους από το κράτος, ώστε να δίδεται απάντηση στις κλήσεις αυτές, ανεξάρτητα από την ύπαρξη προσωρινής συγκατάθεσης του συνδρομητή ή χρήστη. Τα δεδομένα που περιέχουν την αναγνώριση της ταυτότητας του καλούντος συνδρομητή αποθηκεύονται και είναι διαθέσιμα

από τη δημόσια υπηρεσία ή τον ιδιωτικό φορέα άμεσης επέμβασης, μόνο για το σκοπό της άμεσης απάντησης και επέμβασης και μόνο για το χρονικό διάστημα που είναι αναγκαίο για την ολοκλήρωση του σκοπού, και στη συνέχεια διαγράφονται. Με πράξη της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.), καθορίζονται οι διαδικασίες, ο τρόπος και κάθε άλλη τεχνική λεπτομέρεια για την εφαρμογή της παρούσας διάταξης.

γ) για κλήσεις στις οποίες εφαρμόζεται η διαδικασία άρσης απορρήτου σύμφωνα με την κείμενη νομοθεσία.

Άρθρο 9: Αυτόματη προώθηση κλήσεων

Ο συνδρομητής έχει το δικαίωμα να εμποδίζει τις αυτόματα προωθούμενες κλήσεις από τρίτους στην τερματική συσκευή του. Ο φορέας παροχής δημοσίου δικτύου ή και διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών οφείλει να παρέχει ατελώς την αντίστοιχη τεχνική δυνατότητα.

Άρθρο 10: Κατάλογοι συνδρομητών

1. Οι συνδρομητές ενημερώνονται, με πρόσφορο και σαφή τρόπο και ατελώς, για τους σκοπούς των εντύπων ή ηλεκτρονικών καταλόγων συνδρομητών οι οποίοι διατίθενται στο κοινό ή μπορεί να αποκτηθούν μέσω υπηρεσιών πληροφοριών καταλόγων, στους οποίους μπορεί να περιλαμβάνονται προσωπικά δεδομένα τους. Οι συνδρομητές ενημερώνονται, επίσης, για κάθε περαιτέρω δυνατότητα χρήσης που βασίζεται σε λειτουργίες αναζήτησης ενσωματωμένες σε ηλεκτρονικές εκδόσεις των καταλόγων. Η ενημέρωση γίνεται πριν τα δεδομένα περιληφθούν στον κατάλογο.

2. Τα περιεχόμενα στους έντυπους ή ηλεκτρονικούς καταλόγους συνδρομητών δεδομένα προσωπικού χαρακτήρα, τα οποία βρίσκονται στη διάθεση του κοινού ή μμπορούν να ληφθούν μέσω των υπηρεσιών πληροφοριών καταλόγου, πρέπει να περιορίζονται στα απαραίτητα για την αναγνώριση της ταυτότητας συγκεκριμένου συνδρομητή (όνομα, επώνυμο, πατρώνυμο, διεύθυνση), εκτός εάν ο συνδρομητής έχει δώσει τη ρητή

συγκατάθεση του για τη δημοσίευση συμπληρωματικών δεδομένων προσωπικού χαρακτήρα.

3. Ο συνδρομητής δικαιούται να μη συμπεριλαμβάνεται σε έντυπο ή ηλεκτρονικό δημόσιο κατάλογο. Η καταχώριση σε κατάλογο γίνεται εφόσον ο συνδρομητής, μετά την ενημέρωση του κατά την παράγραφο 1 του παρόντος άρθρου, δεν εκφράσει αντίρρηση. Ο συνδρομητής μπορεί επίσης να ζητήσει να παραλείπεται η διεύθυνση του, εν μέρει, και να μην επιτρέπει να υπάρχει αναφορά που να αποκαλύπτει το φύλο του, εφόσον τούτο είναι γλωσσικά

εφικτό. Η μη εγγραφή, η επαλήθευση, η διόρθωση ή η απόσυρση των προσωπικών δεδομένων από το δημόσιο κατάλογο συνδρομητών γίνεται ατελώς.

4. Τα δεδομένα προσωπικού χαρακτήρα που περιλαμβάνονται σε δημόσιο κατάλογο επιτρέπεται να υπόκεινται σε επεξεργασία μόνο για τους σκοπούς για τους οποίους έχουν συλλεγεί. Όταν τα δεδομένα αυτά διαβιβάζονται σε τρίτους, ο συνδρομητής θα πρέπει να ενημερώνεται, πριν από τη διαβίβαση, για αυτή τη δυνατότητα και για τον παραλήπτη ή για τις κατηγορίες των πιθανών παραληπτών, να έχει δε την ευκαιρία να αντιταχθεί στη διαβίβαση.

Για τη χρησιμοποίηση των δεδομένων αυτών για άλλο σκοπό, είτε από τον φορέα είτε από τρίτο, απαιτείται εκ νέου η ρητή συγκατάθεση του συνδρομητή. Δεν επιτρέπεται στους φορείς παροχής υπηρεσιών δημοσίων καταλόγων να εξαρτούν την παροχή των υπηρεσιών δημοσίου καταλόγου από τη συγκατάθεση του συνδρομητή για τη διαβίβαση των δεδομένων για σκοπούς άλλους από αυτούς για τους οποίους έχουν συλλεγεί.

5. Τα δικαιώματα που παρέχονται σύμφωνα με τις παραγράφους 1, 2 και 3 ισχύουν για τους συνδρομητές που είναι φυσικά πρόσωπα. Όταν οι συνδρομητές είναι νομικά πρόσωπα, τα στοιχεία που δημοσιεύονται σε δημόσιους καταλόγους περιορίζονται στα απαραίτητα για την αναγνώριση της ταυτότητας του νομικού προσώπου (επωνυμία ή διακριτικός τίτλος, έδρα,
νομική μορφή, διεύθυνση), εκτός εάν ο νόμιμος εκπρόσωπος του νομικού προσώπου έχει δώσει τη ρητή συγκατάθεση του για τη δημοσίευση συμπληρωματικών στοιχείων.

Άρθρο 11: Μη ζητηθείσα επικοινωνία

1. "Η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, [με ή] χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής
συγκατατεθεί εκ των προτέρων ρητώς".
2. "Δεν επιτρέπεται η πραγματοποίηση μη ζητηθεισών επικοινωνιών με ανθρώπινη παρέμβαση (κλήσεων) για τους ανωτέρω σκοπούς, εφόσον ο συνδρομητής έχει δηλώσει προς τον φορέα παροχής της διαθέσιμης στο κοινό υπηρεσίας, ότι δεν επιθυμεί γενικώς να δέχεται τέτοιες κλήσεις."

*Ο φορέας υποχρεούται να καταχωρίζει δωρεάν τις δηλώσεις αυτές σε ειδικό κατάλογο συνδρομητών, ο οποίος είναι στη διάθεση κάθε ενδιαφερομένου.
** Οι λέξεις "με ή" της παρ.1 διαγράφονται, από 1ης Σεπτεμβρίου 2011, με την παρ.1 άρθρου 16 Ν.3917/2011 (ΦΕΚ Α 22/21.2.2011).
*** Το πρώτο εδάφιο της παρ.2 αντικαθίσταται από 1ης Σεπτεμβρίου 2011,ως άνω, με την παρ.1 άρθρου 16 Ν.3917/2011 (ΦΕΚ Α 22/21.2.2011). *

«**3.** Τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου που αποκτήθηκαν νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής, μμπορούν να χρησιμοποιούνται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει
δώσει εκ των προτέρων τη συγκατάθεση του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιτάσσεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων και αυτό κατά τη συλλογή των στοιχείων επαφής, καθώς και σε κάθε μήνυμα, σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση.
4. Απαγορεύεται η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, που έχουν σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, καθώς και κάθε είδους διαφημιστικούς σκοπούς, όταν δεν

αναφέρεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, καθώς επίσης και μια έγκυρη
διεύθυνση στην οποία ο αποδέκτης του μηνύματος μπορεί να ζητεί τον τερματισμό της επικοινωνίας, ή κατά παράβαση του άρθρου 5 του π.δ.131/2003 (Α 116), ως ισχύει, ή όταν ενθαρρύνονται οι αποδέκτες να επισκεφθούν ιστοσελίδες που παραβιάζουν τις υποχρεώσεις που απορρέουν από το παρόν άρθρο.»

«**5.** Οι φορείς παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών έχουν την υποχρέωση να λαμβάνουν τα κατάλληλα μέτρα, που καθορίζονται με κοινή πράξη της Α.Π.Δ.Π.Χ. και της Α.Δ.Α.Ε., για την αποτροπή της μη ζητηθείσας επικοινωνίας. Από τον φορέα παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών που παραβίασε από αμέλεια την υποχρέωση αυτή καθώς και την υποχρέωση που προβλέπεται στο εδάφιο β` της παραγράφου 2, οι αποδέκτες μη ζητηθείσας επικοινωνίας, έχουν το δικαίωμα να αξιώσουν αποζημίωση για κάθε περιουσιακή ζημία ή χρηματική ικανοποίηση για ηθική βλάβη. Για τη χρηματική ικανοποίηση λόγω ηθικής βλάβης, εφαρμόζεται αναλογικώς η διάταξη της παραγράφου 2 του άρθρου 14 του παρόντος νόμου. Ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών δεν υποχρεούται σε αποζημίωση και στη λήψη μέτρων ώστε να μην επαναληφθεί η παραβίαση στο μέλλον εφόσον αποδείξει ότι δεν τον βαρύνει αμέλεια.

6. Εκτός της αποζημίωσης σύμφωνα με το άρθρο 14 του παρόντος νόμου, οι αποδέκτες μη ζητηθείσας επικοινωνίας, καθώς και οι φορείς παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών έχουν δικαίωμα, σύμφωνα με τη διαδικασία του άρθρου 14 παρ. 3 του παρόντος νόμου, να απαιτήσουν από όποιον παραβιάζει τις υποχρεώσεις που προβλέπονται στις παραγράφους 1 έως 4 του παρόντος άρθρου, να μην επαναλάβει την παραβίαση στο μέλλον, με απειλή χρηματικής ποινής.»

7. Οι ανωτέρω ρυθμίσεις ισχύουν και για τους συνδρομητές που είναι νομικά πρόσωπα.

«**8.** Η Α.Π.Δ.Π.Χ. ορίζεται ως αρμόδια αρχή για την εφαρμογή του

* Οι παρ. 3 και 4 αντικαταστάθηκαν ως άνω με το άρθρο 172, παρ. 1 του Ν. 4070/2012 (ΦΕΚ Α 82/2012).

**Οι παρ. 5 και 6 προστέθηκαν ως άνω με το άρθρο 172, παρ. 2 του Ν. 4070/2012 (ΦΕΚ Α 82/2012).

*** Η παρ. 5 αναριθμήθηκε σε παρ. 7 με το άρθρο 172, παρ. 3 του Ν. 4070/2012 (ΦΕΚ Α 82/2012). Κανονισμού 2006/2004/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ L 364. 9.12.2004) στον τομέα της μη ζητηθείσας επικοινωνίας. Κατά τα λοιπά εφαρμόζεται η κ.υ.α. Ζ1-827/2006 (Β`1086, 9.8.2006), όπως ισχύει.»

Άρθρο 12: «Ασφάλεια Επεξεργασίας»

1. Ο φορέας παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να λαμβάνει τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα, προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του, καθώς και η ασφάλεια του δημοσίου δικτύου ηλεκτρονικών επικοινωνιών. Τα μέτρα αυτά, εφόσον είναι αναγκαίο, λαμβάνονται από κοινού με τον φορέα

παροχής του δημοσίου δικτύου ηλεκτρονικών επικοινωνιών, πρέπει δε να εγγυώνται επίπεδο ασφαλείας ανάλογο προς τον υπάρχοντα κίνδυνο, λαμβανομένων υπόψη αφ' ενός των πλέον προσφάτων τεχνικών δυνατοτήτων αφ' ετέρου δε του κόστους εφαρμογής τους.

2. Αν υπάρχει ιδιαίτερος κίνδυνος παραβίασης της ασφάλειας του δημοσίου δικτύου ηλεκτρονικών επικοινωνιών, ο φορέας που παρέχει διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών οφείλει να ενημερώσει τους συνδρομητές. Εφόσον ο κίνδυνος αυτός είναι εκτός του πεδίου των μέτρων που οφείλει να λαμβάνει ο πάροχος της υπηρεσίας, ο φορέας έχει την υποχρέωση να ενημερώνει τους συνδρομητές και για όλες τις δυνατότητες αποτροπής του κινδύνου, καθώς και για το αναμενόμενο κόστος.

3. Με την επιφύλαξη του άρθρου 10 του ν. 2472/1997. όπως ισχύει, με τα μέτρα του παρόντος άρθρου κατ` ελάχιστον:

α) εξασφαλίζεται ότι πρόσβαση σε δεδομένα προσωπικού χαρακτήρα μπορεί να έχει μόνον εξουσιοδοτημένο προσωπικό για νομίμως εγκεκριμένους σκοπούς,

β) προστατεύονται τα αποθηκευμένα ή διαβιβασθέντα δεδομένα προσωπικού χαρακτήρα από τυχαία ή παράνομη καταστροφή, τυχαία απώλεια ή αλλοίωση και από μη εξουσιοδοτημένη ή παράνομη επεξεργασία, συμπεριλαμβανομένης της αποθήκευσης, πρόσβασης ή αποκάλυψης και

γ) διασφαλίζεται η εφαρμογή πολιτικής ασφάλειας σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Συναφείς ειδικές διατάξεις, καθώς και Κανονισμοί Ανεξαρτήτων Αρχών, εξακολουθούν να ισχύουν.

4. Οι αρμόδιες αρχές εκδίδουν συστάσεις σχετικά με βέλτιστες πρακτικές όσον αφορά το επίπεδο ασφαλείας το οποίο πρέπει να επιτυγχάνεται με τα μέτρα των προηγούμενων παραγράφων.

5. Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών γνωστοποιεί αμελλητί την παραβίαση στην Α.Π.Δ.Π.Χ. και στην Α.Δ.Α.Ε.. Η γνωστοποίηση προς τις αρμόδιες αρχές περιλαμβάνει κατ` ελάχιστον περιγραφή της φύσης της παραβίασης δεδομένων προσωπικού χαρακτήρα και των σημείων επαφής από τα οποία μμπορούν να αποκτηθούν περισσότερες πληροφορίες.

* Η παρ. 8 προστέθηκε ως άνω με το άρθρο 172, παρ. 4 του Ν. 4070/2012 (ΦΕΚ Α 82/2012).

** Ο τίτλος του άρθρου 12 αντικαταστάθηκε ως άνω με το άρθρο 173, παρ. 1 του Ν. 4070/2012 (ΦΕΚ Α 82/2012). μέτρα που προτάθηκαν ή λήφθηκαν από τον φορέα για την αντιμετώπιση της παραβίασης.

6. Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να έχει δυσμενείς επιπτώσεις στα δεδομένα προσωπικού χαρακτήρα ή την ιδιωτική ζωή του συνδρομητή ή άλλου ατόμου, ο φορέας ενημερώνει αμελλητί για την παραβίαση αυτή και τον θιγόμενο συνδρομητή ή το θιγόμενο άτομο. Η ενημέρωση του προηγούμενου εδαφίου περιλαμβάνει κατ' ελάχιστον περιγραφή της φύσης της παραβίασης δεδομένων προσωπικού χαρακτήρα και των σημείων επαφής από τα οποία μμπορούν να αποκτηθούν περισσότερες πληροφορίες, καθώς και συστάσεις που δύνανται να περιορίσουν ενδεχόμενα δυσμενή αποτελέσματα της παραβίασης δεδομένων προσωπικού χαρακτήρα.

7. Η ενημέρωση του θιγόμενου συνδρομητή ή του θιγόμενου ατόμου για την παραβίαση δεδομένων προσωπικού χαρακτήρα δεν είναι αναγκαία, εάν ο φορέας έχει αποδείξει κατά ικανοποιητικό τρόπο στις αρμόδιες αρχές, ότι έχει εφαρμόσει τα κατάλληλα τεχνολογικά μέτρα προστασίας και ότι τα μέτρα αυτά εφαρμόσθηκαν για τα δεδομένα που αφορούσε η παραβίαση της ασφάλειας. Αυτά τα τεχνολογικά μέτρα προστασίας πρέπει, κατ` ελάχιστον,
να περιλαμβάνουν ασφαλή κρυπτογράφηση των δεδομένων, ώστε να μην είναι δυνατή η μη εξουσιοδοτημένη πρόσβαση. Αν ο φορέας δεν έχει προβεί σε ενημέρωση σύμφωνα με την παράγραφο 6 του παρόντος άρθρου, οι αρμόδιες αρχές, αφού εξετάσουν τις πιθανές δυσμενείς επιπτώσεις της παραβίασης, δύνανται να του ζητήσουν να το πράξει.

8. Με κοινή πράξη τους, η Α.Π.Δ.Π.Χ. και η Α.Δ.Α.Ε. δύνανται να εκδίδουν οδηγίες σχετικά με τις περιστάσεις κατά τις οποίες απαιτείται από τον φορέα η γνωστοποίηση των παραβιάσεων δεδομένων προσωπικού χαρακτήρα, το μορφότυπο της εν λόγω γνωστοποίησης, καθώς και τον τρόπο με τον οποίο πρέπει να γίνεται η γνωστοποίηση αυτή.

9. Οι φορείς που παρέχουν διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών τηρούν αρχείο παραβιάσεων δεδομένων προσωπικού χαρακτήρα που περιλαμβάνει την περιγραφή των σχετικών περιστατικών, τα αποτελέσματα τους και τις διορθωτικές ενέργειες στις οποίες προέβησαν, με στοιχεία επαρκή ώστε να δύνανται οι αρμόδιες αρχές να διαπιστώνουν τη συμμόρφωση με τις διατάξεις του παρόντος άρθρου. Το εν λόγω αρχείο
περιλαμβάνει μόνον τις πληροφορίες που απαιτούνται προς το σκοπό αυτόν.

10. Για τη διαχείριση των παραβιάσεων δεδομένων προσωπικού χαρακτήρα, σύμφωνα με τις διατάξεις του παρόντος άρθρου, οι αρμόδιες αρχές ενημερώνονται αμοιβαία για τα μέτρα που προτίθενται να λάβουν.»

11. Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα των συνδρομητών και χρηστών, καθώς και των συναφών δεδομένων κίνησης, θέσης και χρέωσης, πρέπει να ανατίθεται σε πρόσωπα τα οποία ενεργούν υπό τον έλεγχο των φορέων παροχής των δημοσίων δικτύων ηλεκτρονικών επικοινωνιών ή και των διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών και τα οποία ασχολούνται με τη διαχείριση των χρεώσεων ή της κίνησης, τις απαντήσεις σε ερωτήσεις πελατών, την ανίχνευση της απάτης, την εμπορική προώθηση των υπηρεσιών ηλεκτρονικών επικοινωνιών του φορέα ή με την παροχή υπηρεσίας προστιθέμενης αξίας, και περιορίζεται σε ενέργειες που είναι απολύτως αναγκαίες για την εξυπηρέτηση των σκοπών

* Οι παρ. 3 έως 10 προστέθηκαν ως άνω με το άρθρο 173, παρ. 2 του Ν. 4070/2012 (ΦΕΚ Α 82/2012). αυτών.

Άρθρο 13: Αρμοδιότητες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών

1. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει και ως προς την τήρηση των διατάξεων του παρόντος νόμου τις αρμοδιότητες που προβλέπονται από το ν. 2472/1997, όπως εκάστοτε ισχύει.

2. Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) έχει ως προς την τήρηση των διατάξεων του παρόντος νόμου, που αναφέρονται σε αυτήν, τις αρμοδιότητες που προβλέπονται από το ν. 3115/2003, όπως εκάστοτε ισχύει.

3. Στις περιπτώσεις στις οποίες προβλέπεται γνωμοδότηση της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.), αυτή γνωμοδοτεί μετά από αίτηση συνδρομητή ή αίτημα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ή και αυτεπαγγέλτως.

4. Σε περίπτωση παράβασης των διατάξεων των άρθρων 1 έως 17 του παρόντος νόμου, για την τήρηση των οποίων αρμόδια είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, αυτή επιβάλλει τις προβλεπόμενες από το άρθρο 21 του ν. 2472/1997 διοικητικές κυρώσεις. Σε περίπτωση παράβασης των διατάξεων του παρόντος νόμου, για την τήρηση

των οποίων αρμόδια είναι η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, αυτή επιβάλλει τις προβλεπόμενες από το άρθρο 11 του ν. 3115/2003 διοικητικές κυρώσεις. Οι πράξεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών με τις οποίες επιβάλλονται οι διοικητικές

κυρώσεις σε φορείς παροχής δημοσίου δικτύου ή/και διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών υπηρεσιών γνωστοποιούνται στην Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.).

5. Με κοινή πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών,ρυθμίζονται θέματα σχετικά με τις εργασίες που πραγματοποιούνται σε συστήματα των παροχών ηλεκτρονικών επικοινωνιών για το συσχετισμό των στοιχείων ταυτότητας των συνδρομητών τους με τα αντίστοιχα δεδομένα

επικοινωνίας τους.

1. Φυσικό ή νομικό πρόσωπο που, κατά παράβαση του νόμου αυτού, προκαλεί περιουσιακή βλάβη υποχρεούται σε πλήρη αποζημίωση. Αν προκάλεσε ηθική βλάβη, υποχρεούται σε χρηματική ικανοποίηση.

2. Η κατά το άρθρο 932 Α.Κ. χρηματική ικανοποίηση λόγω ηθικής βλάβης για παράβαση του παρόντος νόμου ορίζεται, κατ' ελάχιστο, στο ποσό των δέκα χιλιάδων ευρώ (10.000), εκτός αν ζητηθεί από τον ενάγοντα μικρότερο ποσό. Η χρηματική ικανοποίηση επιδικάζεται ανεξάρτητα από την αιτούμενη αποζημίωση για περιουσιακή βλάβη.

3. Οι απαιτήσεις του παρόντος άρθρου εκδικάζονται κατά τη διαδικασία των άρθρων 664 έως 676 Κ.Πολ.Δ,, ανεξάρτητα από την έκδοση ή μη απόφασης της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ή της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών για τη διαπίστωση παρανομίας ή την άσκηση ποινικής δίωξης.

*Η παρ. 3 αναριθμήθηκε σε παρ. 11 ως άνω με το άρθρο 173, παρ. 3 του Ν. 4070/2012 (ΦΕΚ Α 82/2012).

Άρθρο 15: Ποινικές κυρώσεις

1. Όποιος, κατά παράβαση του παρόντος νόμου, χρησιμοποιεί, συλλέγει, αποθηκεύει, λαμβάνει γνώση, αφαιρεί, αλλοιώνει, καταστρέφει, μεταδίδει, ανακοινώνει, δημοσιοποιεί δεδομένα προσωπικού χαρακτήρα συνδρομητών ή χρηστών, ή τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με φυλάκιση τουλάχιστον
ενός (1) έτους και χρηματική ποινή τουλάχιστον δέκα χιλιάδων ευρώ (10.000) μέχρι και εκατό χιλιάδων ευρώ (100.000), αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.
2. Υπεύθυνος επεξεργασίας και τυχόν εκπρόσωπός του που δεν συμμορφώνεται με τις πράξεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που επιβάλλουν τις διοικητικές κυρώσεις της προσωρινής ανάκλησης αδείας, της οριστικής ανάκλησης αδείας και της καταστροφής αρχείου ή διακοπής επεξεργασίας και καταστροφής των σχετικών δεδομένων, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και με χρηματική ποινή τουλάχιστον δώδεκα χιλιάδων ευρώ (12.000) μέχρι και εκατόν είκοσι χιλιάδων ευρώ (120.000).
3. Εφόσον ο δράστης των πράξεων των προηγούμενων παραγράφων είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να βλάψει τρίτο, επιβάλλεται κάθειρξη μέχρι δέκα (10) ετών και χρηματική ποινή τουλάχιστον δεκαπέντε χιλιάδων ευρώ (15.000) μέχρι και εκατόν πενήντα χιλιάδων ευρώ (150.000). Αν προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική
ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή πενήντα χιλιάδων ευρώ (50.000) μέχρι και τριακοσίων πενήντα χιλιάδων ευρώ (350.000).
4. Εφόσον οι πράξεις των παραγράφων 1 και 2 του παρόντος άρθρου τελεσθούν από αμέλεια, επιβάλλεται φυλάκιση μέχρι δεκαοκτώ (18) μηνών και χρηματική ποινή μέχρι και δέκα χιλιάδων ευρώ (10.000).

Άρθρο 16: Μεταβατικές διατάξεις

Οι ρυθμίσεις του άρθρου 10 δεν εφαρμόζονται σε εκδόσεις καταλόγων οι οποίοι έχουν ήδη διατεθεί στην αγορά, σε έντυπη ή εξωδικτυακή (off-line) ηλεκτρονική μορφή, πριν από την έναρξη ισχύος του παρόντος.
Όταν προσωπικά δεδομένα συνδρομητών σε διαθέσιμες στο κοινό υπηρεσίες σταθερής ή κινητής τηλεφωνίας έχουν περιληφθεί σε δημόσιο κατάλογο συνδρομητών, σύμφωνα με προϊσχύουσες διατάξεις, τα προσωπικά δεδομένα των συνδρομητών αυτών μμπορούν να εξακολουθούν να περιλαμβάνονται στην έντυπη ή ηλεκτρονική μορφή του εν λόγω δημοσίου καταλόγου, συμπεριλαμβανομένων των μορφών που διαθέτουν λειτουργίες αναζήτησης, εκτός εάν οι συνδρομητές δηλώσουν διαφορετικά, αφού ενημερωθούν πλήρως για τους σκοπούς και τις επιλογές, σύμφωνα με το άρθρο 10 του παρόντος νόμου.

Άρθρο 17: Καταργούμενες διατάξεις

Ο ν. 2774/1999 (ΦΕΚ 287 Α) καταργείται από την έναρξη ισχύος του παρόντος.

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ

Τροποποίηση του ν. 2472/1997 (ΦΕΚ 50 Α')

Άρθρο 18

1. Η παρ. β' του άρθρου 2 του ν. 2472/1997 αντικαθίσταται ως εξής:
«Ευαίσθητα δεδομένα», τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.
2. Η παρ. ε' του άρθρου 2 του ν. 2472/1997 αντικαθίσταται ως εξής:
«Αρχείο δεδομένων προσωπικού χαρακτήρα» («αρχείο»), κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία είναι προσιτά με γνώμονα συγκεκριμένα κριτήρια.

Άρθρο 19

1. Το στοιχείο β' της παρ. 3 του άρθρου 3 του ν. 2472/1997 καταργείται. Το στοιχείο γ' της παρ. 3 του άρθρου 3 του ν. 2472/1997 αναριθμείται ως στοιχείο β'
2. Το πρώτο εδάφιο στο νέο στοιχείο β' (πρώην γ') της παρ. 3 του άρθρου 3 του ν. 2472/1997 τροποποιείται ως εξής:
«Από υπεύθυνο επεξεργασίας που δεν είναι εγκατεστημένος 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, ευρισκόμενα στην Ελληνική Επικράτεια, εκτός εάν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη διέλευση από αυτήν.»

Άρθρο 20

1. Το τελευταίο εδάφιο του στοιχείου δ' της παρ.1 του άρθρου 4 του ν. 2472/1997 καταργείται.

2. Το πρώτο εδάφιο της παρ. 2 του άρθρου 4 του ν. 2472/1997 τροποποιείται ως εξής:

«Η τήρηση των διατάξεων της προηγούμενης παραγράφου βαρύνει τον υπεύθυνο επεξεργασίας. Δεδομένα προσωπικού χαρακτήρα που έχουν συλλεχθεί ή υφίστανται επεξεργασία κατά παράβαση της προηγούμενης παραγράφου, καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας.»

Άρθρο 21

Το δεύτερο εδάφιο του στοιχείου α' της παρ. 2 του άρθρου 6 του ν. 2472/1997 καταργείται.

Άρθρο 22

1. Το στοιχείο β' της παρ. 2 του άρθρου 7 του ν. 2472/1997 τροποποιείται ως εξής:

«**β.** Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή προβλεπομένου από το νόμο συμφέροντος τρίτου, εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεση του.»

2. Το τελευταίο εδάφιο της παρ. 3 του άρθρου 7 του ν. 2472/1997 καταργείται.

Άρθρο 23

1. Το πρώτο εδάφιο του στοιχείου δ' της παρ. 1 του άρθρου 7Α του ν. 2472/1997 τροποποιείται ως εξής:

«Όταν η επεξεργασία αφορά δεδομένα υγείας και γίνεται από ιατρούς ή άλλα πρόσωπα που παρέχουν υπηρεσίες υγείας, εφόσον ο υπεύθυνος επεξεργασίας δεσμεύεται από το ιατρικό απόρρητο ή άλλο απόρρητο που προβλέπει νόμος ή κώδικας δεοντολογίας, και τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους.»

2. Το στοιχείο ε' της παρ. 1 του άρθρου 7Α του ν. 2472/1997 τροποποιείται ως εξής:

«ε. Όταν η επεξεργασία γίνεται από δικηγόρους, συμβολαιογράφους, άμισθους υποθηκοφύλακες και δικαστικούς επιμελητές ή εταιρείες των προσώπων αυτών και αφορά στην παροχή νομικών υπηρεσιών προς πελάτες τους, εφόσον ο υπεύθυνος επεξεργασίας και τα μέλη των εταιρειών δεσμεύονται από υποχρέωση απορρήτου που προβλέπει νόμος, και τα
δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους, εκτός από τις περιπτώσεις που αυτό είναι αναγκαίο και συνδέεται άμεσα με την εκπλήρωση εντολής του πελάτη.»

Άρθρο 24

1. Η παρ. 1 του άρθρου 9 του ν. 2472/1997 αντικαθίσταται ως εξής:

«**1.** Η διαβίβαση δεδομένων προσωπικού χαρακτήρα είναι ελεύθερη:

α) προς χώρες - μέλη της Ευρωπαϊκής Ένωσης,

β) προς χώρα μη μέλος της

Ευρωπαϊκής Ένωσης, μετά από άδεια της Αρχής που παρέχεται εάν κρίνει ότι η εν λόγω χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Προς τούτο, λαμβάνει υπόψη ιδίως τη φύση των δεδομένων, τους σκοπούς και τη διάρκεια της επεξεργασίας, τους σχετικούς γενικούς και ειδικούς κανόνες δικαίου, τους κώδικες δεοντολογίας, τα μέτρα ασφαλείας για την προστασία δεδομένων προσωπικού χαρακτήρα, καθώς και το επίπεδο προστασίας των

χωρών προέλευσης, διέλευσης και τελικού προορισμού των δεδομένων. Δεν απαιτείται άδεια της Αρχής εφόσον η Ευρωπαϊκή Επιτροπή έχει αποφανθεί, με τη διαδικασία του άρθρου 31 παρ. 2 της Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995, ότι η χώρα αυτή εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, κατά την έννοια της παρ. 2 του άρθρου 25 της ανωτέρω Οδηγίας.»

2. Η περίπτωση ii του στοιχείου β της παρ. 2 του άρθρου 9 του ν. 2472/1997 αντικαθίσταται ως εξής:

«ii. για τη συνομολόγηση και εκτέλεση σύμβασης μεταξύ αυτού και του υπευθύνου επεξεργασίας ή μεταξύ του υπευθύνου επεξεργασίας και τρίτου προς το συμφέρον του υποκειμένου των δεδομένων,».

3. Μετά το στοιχείο ε' της παρ. 2 του άρθρου 9 του ν. 2472/1997, προστίθεται στοιχείο στ' ως εξής:

«στ. Ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις για την προστασία των προσωπικών δεδομένων των υποκειμένων και την άσκηση των σχετικών δικαιωμάτων τους, όταν οι εγγυήσεις προκύπτουν από συμβατικές ρήτρες, σύμφωνες με τις ρυθμίσεις του παρόντος νόμου. Δεν απαιτείται άδεια εάν η Ευρωπαϊκή Επιτροπή έκρινε, κατά το άρθρο 26 παρ. 4 της Οδηγίας 95/46/ΕΚ, ότι ορισμένες συμβατικές ρήτρες παρέχουν επαρκείς

εγγυήσεις για την προστασία των προσωπικών δεδομένων.»

4. Η παρ. 3 του άρθρου 9 του ν. 2472/1997 αντικαθίσταται ως εξής:

«Στις περιπτώσεις των προηγούμενων παραγράφων, η Αρχή ενημερώνει την Ευρωπαϊκή Επιτροπή και τις αντίστοιχες Αρχές των άλλων κρατών - μελών:

α) όταν θεωρεί ότι μία χώρα δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας και

β) για τις άδειες που χορηγεί κατ' εφαρμογήν της παραγράφου 2 στοιχείο στ'.»

Άρθρο 25

Το εδάφιο 3 της παρ. 3 του άρθρου 10 του ν. 2472/1997 αντικαθίσταται ως εξής:

«Με την επιφύλαξη άλλων διατάξεων, η Αρχή παρέχει οδηγίες ή εκδίδει κανονιστικές πράξεις σύμφωνα με το άρθρο 19 παρ. 11' για τη ρύθμιση θεμάτων σχετικά με το βαθμό ασφαλείας των δεδομένων και των

υπολογιστι-κών και επικοινωνιακών υποδομών, τα μέτρα ασφαλείας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία και επεξεργασία δεδομένων, καθώς και
για τη χρήση τεχνολογιών ενίσχυσης της ιδιωτικότητας.»

Άρθρο 26

Στην παρ. 2 του άρθρου 12 του ν. 2472/1997 προστίθενται περιπτώσεις που αριθμούνται ως:
« κατά περίπτωση, τη διόρθωση, τη διαγραφή ή τη δέσμευση (κλείδωμα) των δεδομένων των οποίων η επεξεργασία δεν είναι σύμφωνη προς τις διατάξεις του παρόντος νόμου, ιδίως λόγω του ελλιπούς ή ανακριβούς χαρακτήρα των δεδομένων, και την κοινοποίηση σε τρίτους, στους οποίους έχουν ανακοινωθεί τα δεδομένα, κάθε διόρθωσης, διαγραφής ή δέσμευσης (κλειδώματος) που διενεργείται σύμφωνα με την περίπτωση ε', εφόσον τούτο δεν είναι αδύνατον ή δεν προϋποθέτει δυσανάλογες προσπάθειες.»

Άρθρο 27

Η περίπτωση η' της παρ. 1 του άρθρου 19 ν. 2472/1997 αντικαθίσταται ως εξής:
«η. Ενεργεί αυτεπαγγέλτως ή κατόπιν καταγγελίας διοικητικούς ελέγχους στο πλαίσιο των οποίων ελέγχονται η τεχνολογική υποδομή και άλλα, αυτοματοποιημένα ή μη, μέσα που υποστηρίζουν την επεξεργασία των δεδομένων. Έχει προς τούτο δικαίωμα προσβάσεως στα δεδομένα προσωπικού χαρακτήρα και συλλογής κάθε πληροφορίας για τους σκοπούς του ελέγχου, χωρίς να μπορεί να της αντιταχθεί κανενός είδους απόρρητο. Κατ' εξαίρεση, η Αρχή δεν έχει πρόσβαση στα στοιχεία ταυτότητας συνεργατών που περιέχονται σε αρχεία που τηρούνται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Τον έλεγχο διενεργεί μέλος ή μέλη της Αρχής ή υπάλληλος του κλάδου των ελεγκτών.
της Γραμματείας, ειδικά προς τούτο εντεταλμένος από τον Πρόεδρο της Αρχής. Κατά τον έλεγχο αρχείων που τηρούνται για λόγους εθνικής ασφάλειας, παρίσταται αυτοπροσώπως ο Πρόεδρος της Αρχής.»

Άρθρο 28

Η περίπτωση ιγ' της παρ. 1 του άρθρου 19 του ν. 2472/1997 αντικαθίσταται ως εξής:
«ιγ. Εξετάζει τα παράπονα των υποκειμένων των δεδομένων σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων τους, όταν αυτά θίγονται από την επεξεργασία δεδομένων που τους αφορούν. Εξετάζει επίσης αιτήσεις του υπεύθυνου επεξεργασίας με τις οποίες ζητείται ο έλεγχος και η εξακρίβωση της νομιμότητας της επεξεργασίας. Η Αρχή μπορεί να θέτει στο αρχείο αιτήσεις ή παράπονα που κρίνονται προδήλως αόριστα, αβάσιμα ή υποβάλλονται καταχρηστικώς ή ανωνύμως. Η Αρχή ενημερώνει τα υποκείμενα των δεδομένων και τους αιτούντες για τις ενέργειες της.»

Άρθρο 29

Μετά την περίπτωση ιδ' της παρ. 1 του άρθρου 19 του ν. 2472/1997, προστίθεται περίπτωση ιέ' ως εξής:
«ιε. Ασκεί ανεξάρτητο έλεγχο στο εθνικό τμήμα του Συστήματος Πληροφοριών Σένγκεν, σύμφωνα με το άρθρο 114 παράγραφος 1 της Σύμβασης Εφαρμογής της Συμφωνίας Σένγκεν (ν. 2514/1997 ΦΕΚ 140 Α'), ασκεί τις αρμοδιότητες της εθνικής εποπτικής αρχής που προβλέπεται στο άρθρο 23 της Σύμβασης ΕΥΡΩΠΟΛ (ν. 2605/1998 ΦΕΚ 88 Α'), και τις
αρμοδιότητες της εθνικής εποπτικής αρχής που προβλέπεται στο άρθρο 17 της Σύμβασης για τη χρήση της πληροφορικής στον τελωνειακό τομέα (ν. 2706/1999 ΦΕΚ 77 Α'), καθώς και τις αρμοδιότητες εποπτείας που προκύπτουν από οποιαδήποτε άλλη διεθνή συμφωνία.»

Άρθρο 30

Η περίπτωση ε' της παρ. 1 του άρθρου 21 του ν. 2472/1997 αντικαθίσταται ως εξής:
«ε. Καταστροφή αρχείου ή διακοπή επεξεργασίας και καταστροφή, επιστροφή ή κλείδωμα (δέσμευση) των σχετικών δεδομένων».

6.3 'Αδεια διαβίβασης δεδομένων εκτός ΕΕ- BCR

Πληροφορίες για υπευθύνους επεξεργασίας

Κάθε όμιλος εταιριών πρέπει καταρχήν να αποφασίσει ποια θα είναι τα λεγόμενα "γεωγραφικά όρια" της προστασίας που θα παρέχουν τα BCR του, δηλαδή αν τα BCR θα καλύπτουν μόνο τα δεδομένα που διαβιβάζονται από χώρες της Ε.Ε. σε χώρες εκτός της Ε.Ε. ή αν θα καλύπτουν όλα τα δεδομένα που τυγχάνουν επεξεργασίας από τον όμιλο, δηλαδή ακόμα και εκείνα που δεν υπόκεινται σε καμιά επεξεργασία εντός της Ε.Ε. Συστήνεται, βέβαια, σε κάθε όμιλο εταιριών να υπάρχει ένα μοναδικό σύνολο κανόνων που θα παρέχουν προστασία σε όλα τα δεδομένα που επεξεργάζεται ο όμιλος. Με αυτόν τον τρόπο θα είναι πιο εύκολο τόσο για το προσωπικό να εφαρμόσει τους κανόνες, όσο και για τα υποκείμενα των δεδομένων να τους κατανοήσουν. Περαιτέρω, τα BCR θα πρέπει οπωσδήποτε να περιέχουν μια περιγραφή της διαβίβασης, ήτοι το είδος των δεδομένων (απλά/ευαίσθητα, δεδομένα εργαζομένων/πελατών/προμηθευτών κλπ.), τον σκοπό (ή τους σκοπούς) της διαβίβασης/επεξεργασίας, καθώς και τους "εισαγωγείς" και "εξαγωγείς" των δεδομένων εντός και εκτός Ε.Ε. (ουσιαστικά τις πηγές και τους αποδέκτες). Επιπρόσθετα, τα BCR πρέπει να περιλαμβάνουν:

- Τις θεμελιώδεις αρχές της επεξεργασίας (νομιμότητα σκοπού, αναλογικότητα).
- Τη νομιμοποιητική βάση επεξεργασίας απλών ή/και ευαίσθητων δεδομένων.
- Όρους για την άσκηση των δικαιωμάτων των υποκειμένων.
- Όρους για το απόρρητο και την ασφάλεια της επεξεργασίας.
- Επεξήγηση της σχέσης με τυχόν εκτελούντες την επεξεργασία που είναι μέλη το ίδιου ομίλου.
- Επεξήγηση των μέτρων που έχουν ληφθεί για τον περιορισμό των διαβιβάσεων σε εταιρίες που δεν ανήκουν στον ίδιο όμιλο.
- Μέτρα εξασφάλισης της εφαρμογής και αποτελεσματικότητάς τους, ήτοι ειδική εκπαίδευση του προσωπικού που θα ασχολείται με την επεξεργασία των δεδομένων,πρόγραμμα αυτοελέγχου και διευκόλυνση ελέγχου από την εκάστοτε αρμόδια εθνική αρχή προστασίας δεδομένων, καθορισμός ενός εξειδικευμένου προσώπου (ή ενός ειδικού εταιρικού τμήματος) επιφορτισμένου με την αρμοδιότητα παρακολούθησης της ορθής εφαρμογής των κανόνων (π.χ. "privacy officers"), δημιουργία εσωτερικού μηχανισμού για τον χειρισμό παραπόνων (μηχανισμός "οιονεί διαιτητικής επίλυσης" των σχετικών διαφορών) αμοιβαία συνεργασία μεταξύ μελών του ομίλου, αλλά και για συνεργασία με τις εθνικές αρχές προστασίας δεδομένων, επικαιροποίηση των κανόνων που θεσπίζονται με τα BCR, λαμβάνοντας υπόψη και τυχόν συστάσεις εθνικών αρχών προστασίας δεδομένων, δέσμευση για λήψη κατάλληλων μέτρων σε περίπτωση που κάποιο εθνικό δίκαιο εμποδίζει την πλήρη εφαρμογή των BCR. Μέτρα εξασφάλισης της δεσμευτικότητάς τους, ήτοι σαφής υποχρέωση τόσο των εταιριών του ομίλου όσο και των εργαζομένων να σέβονται τα BCR, κατοχύρωση στα BCR δικαιωμάτων του υποκειμένου (third-party beneficiary rights) –στο ελληνικό δίκαιο μέσω σύμβασης υπέρ τρίτου (ΑΚ 410 -

414). Το υποκείμενο δηλαδή έχει τη δυνατότητα να ζητήσει δικαστική προστασία στη χώρα της Ε.Ε που είναι εγκατεστημένος ο εξαγωγέας των δεδομένων ή στη χώρα της Ε.Ε. που είναι εγκατεστημένη η κεντρική διοίκηση του ομίλου ή η εταιρία-μέλος του ομίλου στην οποία έχει εκχωρηθεί η ευθύνη για την προστασία προσωπικών δεδομένων ("with delegated responsibilities"), καθώς και διοικητική προστασία ενώπιον των αρμόδιων εθνικών αρχών προστασίας δεδομένων (σημειώνεται δε ότι η σχετική δήλωση πρέπει να είναι εύκολα προσβάσιμη στο υποκείμενο, να αποδεικνύεται δηλαδή ότι το υποκείμενο μπορεί εύκολα να λάβει γνώση των ως άνω δικαιωμάτων του), δέσμευση ότι η κεντρική διοίκηση εντός της Ε.Ε. ή η εταιρία-μέλος του ομίλου στην οποία έχει εκχωρηθεί ή ευθύνη για την προστασία προσωπικών δεδομένων ("with delegated responsibilities")

(α) αναλαμβάνει την ευθύνη για πράξεις άλλων μελών του ομίλου εκτός Ε.Ε.,

(β) θα αποζημιώσει το υποκείμενο για κάθε ζημία που θα προκληθεί από μέλη του ομίλου εξαιτίας παράβασης των BCR, και

(γ) φέρει το βάρος απόδειξης ότι το μέλος του ομίλου εκτός Ε.Ε. δεν ευθύνεται για παράβαση που προκάλεσε τη ζημία που επικαλείται το υποκείμενο

Δήλωση για τη σχέση των BCR με την εθνική νομοθεσία (π.χ. ότι όταν η εθνική νομοθεσία απαιτεί υψηλότερο επίπεδο προστασίας, τότε κατισχύει των BCR, ότι σε κάθε περίπτωση τα δεδομένα πρέπει να τυγχάνουν επεξεργασίας σύμφωνα με το εφαρμοστέο δίκαιο όπως ορίζεται στο άρθρο 4 της Οδηγίας 95/46/ΕΚ και σύμφωνα με την αντίστοιχη εθνική νομοθεσία).

Διατάξεις για την ημερομηνία ισχύος των BCR και τη μεταβατική περίοδο προκειμένου να επιτευχθεί η δεσμευτικότητα των BCR, η οποία είναι απαραίτητη προϋπόθεση για να αποτελούν αυτά "επαρκείς εγγυήσεις" υπό την έννοια του άρθρου 26 παρ. 2 της Οδηγίας 95/46/ΕΚ, αλλά και για την προστασία του υποκειμένου, οι περισσότερες εταιρείες επιλέγουν μέχρι στιγμής τη μορφή της «εταιρικής συμφωνίας» (intra-group agreement - IGA). Η επιλογή αυτή είναι η ασφαλέστερη, καθώς η εναλλακτική μορφή της μονομερούς δήλωσης (unilateral declaration) δεν γίνεται προς το παρόν καθολικά αποδεκτή.

Ένας όμιλος εταιριών μπορεί να χρησιμοποιήσει τα BCR ως νομική βάση για τη διαβίβαση δεδομένων εκτός Ε.Ε. μόνο εφόσον κάθε κράτος-μέλος, από το οποίο θα γίνεται η διαβίβαση, εγκρίνει τα BCR. Η διαδικασία αυτή εξελίσσεται σε τρεις φάσεις, οι οποίες περιλαμβάνουν τα ακόλουθα βήματα:

ΦΑΣΗ 1η : ΕΠΙΛΟΓΗ ΤΗΣ "LEAD AUTHORITY"

1ο βήμα: Ο όμιλος πρέπει να συμπληρώσει μια αίτηση (Βλ. υπ' αριθμ. 133 Έγγραφο Εργασίας (Σύσταση 1/2007) της Ομάδας του Άρθρου 29 "Τυποποιημένη αίτηση σχετικά με την έγκριση Εταιρικών Δεσμευτικών Κανόνων για τη διαβίβαση προσωπικών δεδομένων", 10.01.2007.), στο πλαίσιο της οποίας προτείνει μια εθνική αρχή προστασίας δεδομένων ως "lead authority", ήτοι ως την εθνική αρχή στην οποία θα υποβληθεί το αρχικό κείμενο των BCR και η οποία θα συντονίσει τη διαδικασία έγκρισης. Ο όμιλος οφείλει να αιτιολογήσει

την επιλογή της "lead authority" με βάση συγκεκριμένα κριτήρια, όπως (ενδεικτικά): η έδρα (ο τόπος εγκατάστασης) της κεντρικής διοίκησης της εταιρίας στην Ε.Ε., η έδρα της εταιρίας-μέλους του ομίλου στην οποία έχει εκχωρηθεί η ευθύνη για την προστασία προσωπικών δεδομένων (απαιτείται όταν η κεντρική διοίκηση είναι εγκατεστημένη εκτός Ε.Ε./Ε.Ο.Χ.),η έδρα της εταιρίας-μέλους του ομίλου με την πιο κατάλληλη τοποθεσία (από άποψη διαχειριστικής λειτουργίας, διοικητικών αρμοδιοτήτων-εξουσιών κλπ.) για να αναλάβει την αίτηση και να επιβάλλει την εφαρμογή των BCR εντός του ομίλου,ο τόπος όπου λαμβάνονται οι περισσότερες αποφάσεις σχετικά με τους σκοπούς και τα μέσα της επεξεργασίας,το κράτος-μέλος της Ε.Ε. από το οποίο θα γίνονται οι περισσότερες διαβιβάσεις. Για παράδειγμα, η εταιρία Hewlett Packard που δεν έχει την κύρια έδρα της στην Ε.Ε., επέλεξε ως lead authority την Γαλλική Αρχή, καθώς στο Παρίσι βρίσκονται τα γραφεία του European Privacy Officer της εταιρίας (κριτήριο τρίτο).

2ο βήμα: Η εθνική αρχή που επιλέχθηκε από τον όμιλο ως lead authority στέλνει στις εθνικές αρχές των χωρών που δηλώνονται από τον όμιλο ως τόποι επεξεργασίας (χώρες από όπου θα γίνονται οι διαβιβάσεις) ένα ηλεκτρονικό μήνυμα. Με το μήνυμα αυτό ερωτά τις ως άνω εθνικές αρχές αν συμφωνούν ή όχι με την επιλογή της lead authority και τους στέλνει επίσης την αίτηση του ομίλου. Αν η επιλεγείσα από τον όμιλο εθνική αρχή (που στέλνει το μήνυμα αυτό) συμφωνεί να παραμείνει η ίδια lead authority, ζητά από τις υπόλοιπες αρχές να προβάλουν τυχόν αντιρρήσεις τους μέσα σε προθεσμία δυο (2) εβδομάδων.

3ο βήμα: Από τη στιγμή που μια εθνική αρχή αναλαμβάνει με την σύμφωνη γνώμη όλων των υπολοίπων το ρόλο της lead authority, ξεκινά να συνεργάζεται με τον όμιλο, ώστε να καταλήξουν σε ένα πρώτο σχέδιο BCR.

4ο βήμα: Το πρώτο σχέδιο αποστέλλεται με ηλεκτρονικό μήνυμα στις υπόλοιπες εθνικές αρχές. Όσες εθνικές αρχές έχουν υπογράψει τη λεγόμενη "declaration on mutual recognition" (δήλωση αμοιβαίας αναγνώρισης), έχουν προθεσμία ενός μηνός για να επιβεβαιώσουν ότι έλαβαν γνώση (χωρίς βέβαια να τους αποκλείεται η δυνατότητα να αποστείλουν και σχόλια, αν το κρίνουν απαραίτητο). Όσες αρχές δεν έχουν υπογράψει την ως άνω δήλωση (μεταξύ των οποίων και η Ελλάδα), έχουν προθεσμία ενός μηνός για να κάνουν σχόλια.

5ο βήμα: Ο όμιλος συντάσσει το τελικό κείμενο BCR λαμβάνοντας υπόψη όλα τα σχόλια που δέχθηκε. Στο πλαίσιο αυτό, μπορεί να χρειαστεί να επικοινωνήσει απευθείας με κάποιες από τις εθνικές αρχές που έκαναν σχόλια.

6ο βήμα: Το τελικό κείμενο αποστέλλεται στις εθνικές αρχές, οι οποίες επιβεβαιώνουν ότι έλαβαν γνώση. Η επιβεβαίωση αυτή λογίζεται ως συμφωνία των εθνικών αρχών ότι τα υπό έγκριση BCR προσφέρουν επαρκείς εγγυήσεις για την προστασία των δεδομένων που πρόκειται να διαβιβαστούν εκτός Ε.Ε. Ωστόσο, κάθε φορά που μια εταιρία του ομίλου υποβάλλει αίτημα για διαβίβαση στην αρμόδια κατά τόπον εθνική αρχή, η τελευταία δεν υποχρεούται να χορηγήσει άνευ ετέρου την απαιτούμενη έγκριση ή άδεια, αν η εν γένει διαβίβαση αντίκειται στο εθνικό δίκαιο (π.χ. αν διαπιστώσει ότι τα δεδομένα που διαβιβάζονται δεν είναι συναφή και πρόσφορα ενόψει του επιδιωκόμενου σκοπού). Με άλλα λόγια, κάθε εθνική αρχή διατηρεί την αρμοδιότητα να εξετάζει την νομιμότητα της επεξεργασίας εν γένει. Επιπρόσθετα, κάθε εταιρία του ομίλου πρέπει να συμμορφωθεί με πρόσθετες διοικητικές προϋποθέσεις που ισχύουν σε κάθε χώρα, όπως π.χ. υποβολή γνωστοποίησης.

7ο βήμα: Οι εταιρίες του ομίλου υποβάλλουν ενώπιον των εθνικών αρχών (η καθεμιά στη χώρα εγκατάστασής της) αίτημα για χορήγηση άδειας για διαβίβαση δεδομένων εκτός Ε.Ε. με βάση τα BCR του ομίλου.

8ο βήμα: Η κάθε εθνική αρχή, ανάλογα με το τι προβλέπεται από το εθνικό δίκαιο, είτε εκδίδει άδεια διαβίβασης με νομιμοποιητική βάση τα BCR σε συνδυασμό με τις λοιπές διατάξεις του εθνικού δικαίου, είτε εκδίδει άδεια μόνο για τα BCR, είτε και τα δυο μαζί (είτε απορρίπτει εν όλω ή εν μέρει την αίτηση αν η διαβίβαση αντίκειται στο εθνικό δίκαιο).

Πληροφορίες για υποκείμενα των δεδομένων

Για την προστασία του υποκειμένου, είναι απαραίτητο να κατοχυρώνονται στα BCR δικαιώματα αυτού (third-party beneficiary rights) –στο ελληνικό δίκαιο μέσω σύμβασης υπέρ τρίτου (ΑΚ 410 - 414). Τα δικαιώματα αυτά πρέπει να αναφέρονται το καθένα ξεχωριστά με λεπτομέρεια και σαφήνεια σε συγκεκριμένες παραγράφους των BCR, έτσι ώστε να είναι εύκολα προσβάσιμα και στο υποκείμενο. Το τελικό κείμενο των BCR πρέπει εν γένει να είναι εύκολα προσβάσιμο χωρίς καν να απαιτείται αίτηση, μέσω πχ της ανάρτησής του στο site της εταιρείας.Στα δικαιώματα αυτά του υποκειμένου περιέχεται και η δυνατότητα αυτού να υποβάλει προσφυγή για παραβίαση των προσωπικών του δεδομένων ενώπιον της αρμόδιας εθνικής Αρχής. Το υποκείμενο, δηλαδή, θα υποβάλει την προσφυγή στην εθνική Αρχή του κράτους στο οποίο κατοικεί, η οποία θα συνεργαστεί με την Αρχή του κράτους στο οποίο έλαβε χώρα η παραβίαση. Η δε ενδεχόμενη κύρωση θα επιβληθεί από την Αρχή του κράτους στο οποίο σημειώθηκε η παραβίαση.

Κεφάλαιο 7ο

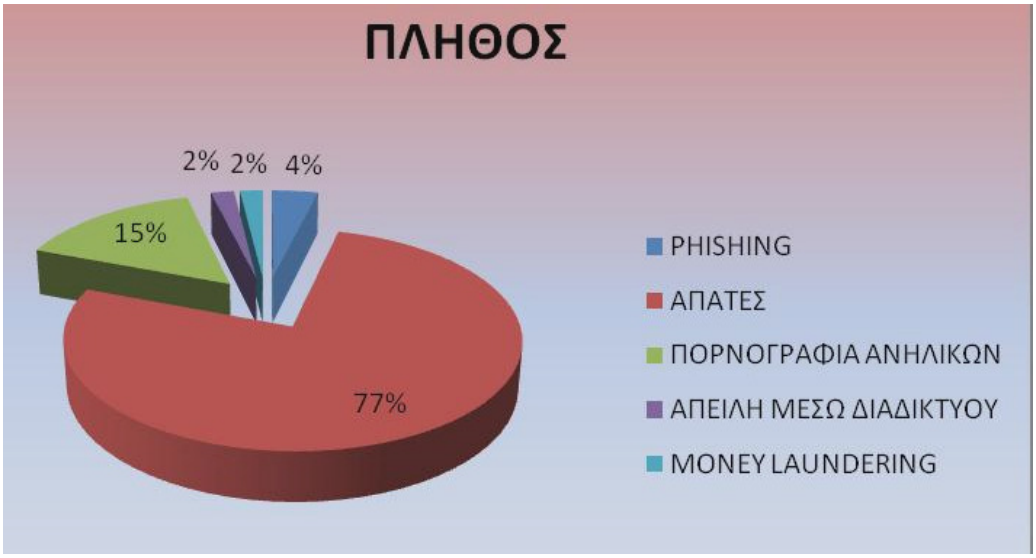
Στατιστικά στοιχεία

2011: Στον τομέα της ηλεκτρονικής μορφής εγκληματικών συμπεριφορών, η Δίωξη Ηλεκτρονικού Εγκλήματος, χειρίστηκε 832 δικογραφίες για πληθώρα διαδικτυακών ή ηλεκτρονικών εγκλημάτων. Έμφαση στη δράσης της δόθηκε σε εκείνες τις ηλεκτρονικές παράνομες και ταυτόχρονα αντικοινωνικές συμπεριφορές που στερούν από την Εθνική Οικονομία αρκετά έσοδα, προκαλούν οικονομικό ρήγμα στις δομές κοινωνικής ασφάλισης, καθώς και σε εκείνες που διαταράσσουν το κλίμα εμπιστοσύνης και υγιούς συναλλαγής μεταξύ των ηλεκτρονικών χρηστών.

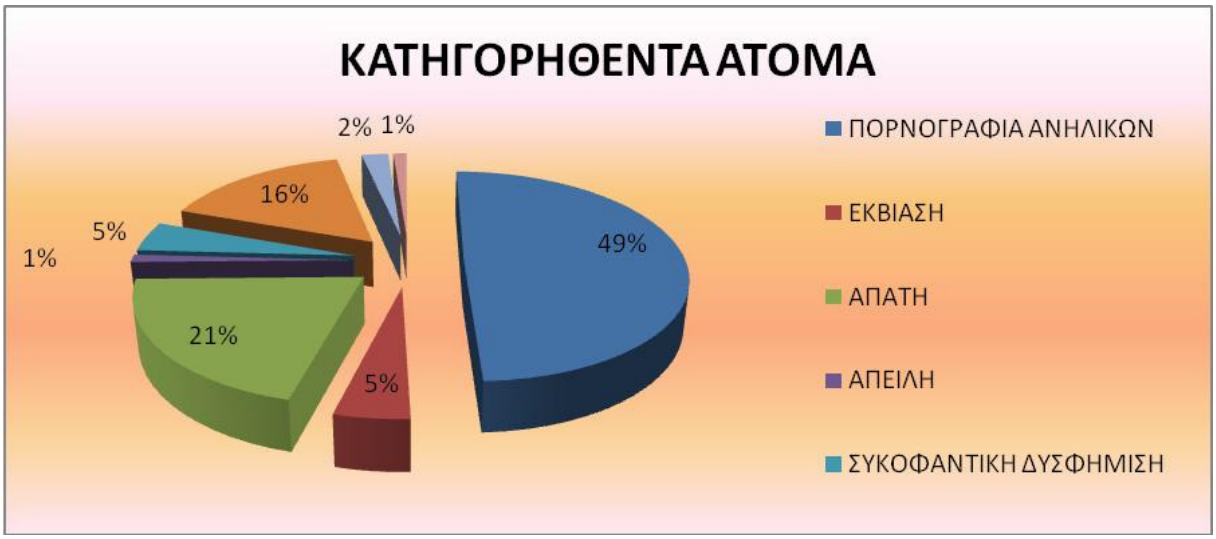
Σε άλλες 364 περιπτώσεις, ακολουθήθηκε αστυνομική έρευνα και σχηματίσθηκε δικογραφία, από κλιμάκια της Δίωξης Ηλεκτρονικού Εγκλήματος, ύστερα από καταγγελίες Φορέων Προστασίας Καταναλωτών, Οργανισμών, Χρηματοπιστωτικών Ιδρυμάτων, Εταιρειών Τηλεπικοινωνιών, καθώς και καταστημάτων ηλεκτρονικού εμπορίου .

Επιπλέον, στο πλαίσιο της διεθνούς αστυνομικής συνεργασίας (Interpol & Europol), παρασχέθηκε συνδρομή σε 71 περιπτώσεις διακρατικών αστυνομικών ερευνών, που είχαν ως αντικείμενο κακουργηματικού χαρακτήρα ηλεκτρονικά εγκλήματα, και αφορούσαν στο ηλεκτρονικό εμπόριο, στις διαδικτυακές απάτες, στις υφαρπαγές στοιχειών και κωδικών πρόσβασης σε ηλεκτρονικές βάσεις, πλατφόρμες και ιστοχώρους ηλεκτρονικών οικονομικών δραστηριοτήτων.

Από τις μέχρι σήμερα χειρισθείσες υποθέσεις αυτόφωρης διαδικασίας της Δίωξης Ηλεκτρονικού Εγκλήματος, που αφορούν το διάστημα από την επίσημη έναρξη της νέας Υπηρεσίας, έχουν αποδοθεί κατηγορίες για διάφορα αδικήματα σε συνολικά 87 άτομα.

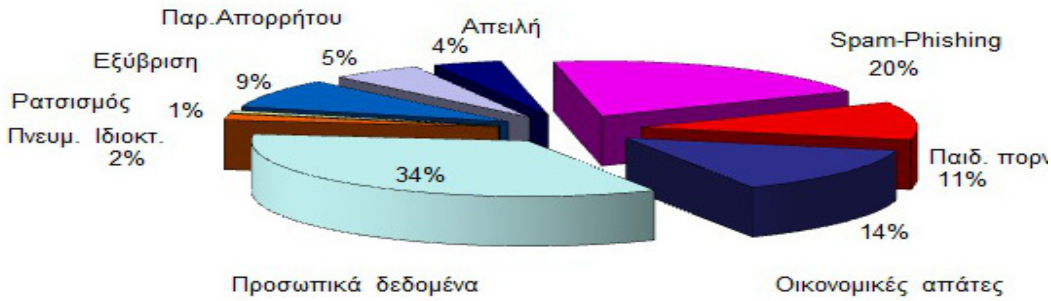


Γράφημα 4: Παράνομες δραστηριότητες για το έτος 2011



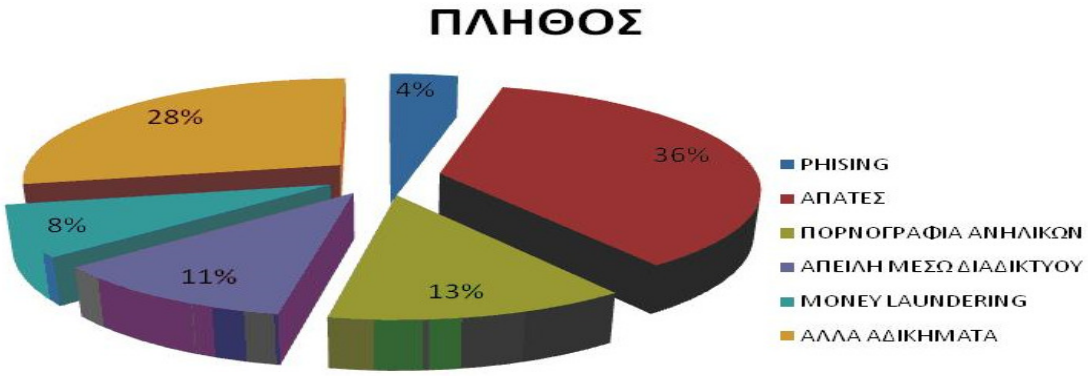
Γράφημα 5: Κατηγορηθέντα άτομα για παράνομες δραστηριότητες μέσω διαδικτύου για το έτος 2011

Το **2012** το μεγαλύτερο ποσοστό καταγγελιών ανήκει στην κατηγορία των Προσωπικών δεδομένων (34%). Είναι προφανές από το ποσοστό αυτό ότι πάνω από το ένα τρίτο των περιπτώσεων των αναφορών είχαν να κάνουν με την έλλειψη σεβασμού της διαδικτυακής ταυτότητας καθώς και της ιδιωτικής ζωής των χρηστών του Διαδικτύου. Το τελευταίο αποδεικνύεται και από τον αριθμό των καταγγελιών που αφορούσαν το Facebook (845 καταγγελίες), οι οποίες περιελάμβαναν περιπτώσεις δημιουργίας ψεύτικων προφίλ, διαδικτυακό εκφοβισμό (cyber bulling), κα. Το περιεχόμενο επιβεβαιώνεται ως παράνομο έχει ως χώρο προέλευσης την Ελλάδα , προωθούνται στη Μονάδα Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, καθώς επίσης και σε άλλες ανεξάρτητες ελληνικές αρχές, όπως είναι η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών και η Αρχή Προστασίας Προσωπικών Δεδομένων. Στις περιπτώσεις που το παράνομο περιεχόμενο εντοπίζεται σε άλλη χώρα του εξωτερικού, τότε οι καταγγελίες αυτές προωθούνται στις αντίστοιχες Ανοικτές Γραμμές του εξωτερικού



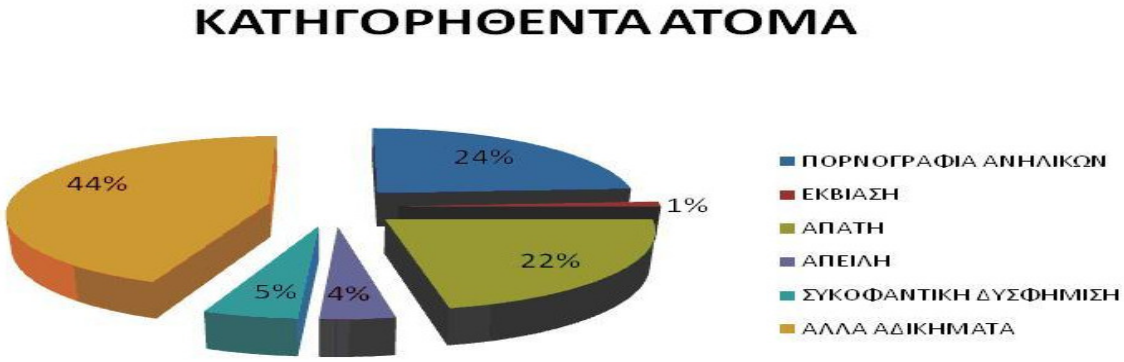
Γράφημα 6: Παράνομες δραστηριότητες στο διαδίκτυο το έτος 2012

Στον τομέα της ηλεκτρονικής-διαδικτυακής μορφής εγκληματικών συμπεριφορών, η Δίωξη Ηλεκτρονικού Εγκλήματος, χειρίστηκε **3.193** δικογραφίες για πληθώρα διαδικτυακών ή ηλεκτρονικών εγκλημάτων. Έμφαση στη δράση της δόθηκε σε εκείνες τις ηλεκτρονικές παράνομες και ταυτόχρονα αντικοινωνικές συμπεριφορές που στερούν από την Εθνική Οικονομία αρκετά έσοδα, προκαλούν οικονομικό ρήγμα στις δομές κοινωνικής ασφάλισης, καθώς και σε εκείνες που διαταράσσουν το κλίμα εμπιστοσύνης και υγιούς συναλλαγής μεταξύ των ηλεκτρονικών χρηστών.



Γράφημα 7: Παράνομες δραστηριότητες για το έτος 2012

Σε άλλες **115** περιπτώσεις, ακολουθήθηκε αστυνομική έρευνα και σχηματίσθηκε δικογραφία, από κλιμάκια της Δίωξης Ηλεκτρονικού Εγκλήματος, ύστερα από καταγγελίες Φορέων Προστασίας Καταναλωτών, Οργανισμών, Χρηματοπιστωτικών Ιδρυμάτων, Εταιρειών Τηλεπικοινωνιών, καθώς και καταστημάτων ηλεκτρονικού εμπορίου (e shops). Ηλεκτρονικού εγκλήματος διαχειρίστηκε **(746)** αιτήματα συνεργασίας. Τα αιτήματα αφορούν περιπτώσεις διακρατικών αστυνομικών ερευνών, που είχαν ως αντικείμενο κακουργηματικού χαρακτήρα ηλεκτρονικά εγκλήματα, και αφορούσαν στο ηλεκτρονικό εμπόριο, στις διαδικτυακές απάτες, στις υφαρπαγές στοιχείων και κωδικών πρόσβασης σε ηλεκτρονικές βάσεις, πλατφόρμες και ιστοχώρους ηλεκτρονικών οικονομικών δραστηριοτήτων. Συνολικά έχουν αποδοθεί κατηγορίες σε συνολικά **(458)** άτομα για διάφορα αδικήματα.



Γράφημα 8: Κατηγορηθέντα άτομα για παράνομες δραστηριότητες μέσω διαδικτύου για το έτος 2012

Συμπερασματικά…

Η ασφάλεια προσωπικών δεδομένων στις τηλεπικοινωνίες και τα δίκτυα είναι πολύ σημαντικό στις μέρες μας καθώς οι απειλές γίνονται ολοένα και πιο έντονες με αποτέλεσμα τα κρούσματα να αυξάνονται συνεχώς όπως και οι μορφές επιθέσεων στις τηλεπικοινωνίες και τα δίκτυα.

Σε αυτή την περίπτωση με βάση όσα προαναφερθησαν παρατηρούμε ότι πρεπει να είμαστε ποιο προσεκτικοί όταν ανταλλάσουμε πληροφορίες που αφορούν τα προσωπικά μας δεδομένα καθως επίσης θα πρεπει να έχουμε λάβει τα απαραίτητα μέτρα έτσι ώστε να είμαστε πιο <ασφαλείς> όταν χρησιμοποιούμε αυτές τις τεχνολογίες.

Ο κάθε χρήστης θα πρέπει να γνωρίζει ότι οι τηλεπικοινωνίες και τα δίκτυα παρόλη την απαραίτητη ασφάλεια πάντα υπάρχει και η πιθανότητα <επίθεσης> όπου παρόλα τα μέτρα μπορεί να γίνει υπέρβαση και να γίνει θύμα υποκλοπής.

Επιπροσθέτως όπως αναφέρθηκε στην πτυχιακή εργασία όταν ένας χρήστης γίνει θύμα παραβίασης των προσωπικών δεδομένων η πολιτεία μπορεί με τους υπάρχων νόμους να τον διασφαλίσει έτσι ώστε να επιλυθεί το πρόβλημα.

ΠΑΡΑΡΤΗΜΑ Α

Software: Advanced keylogger

Το Advanced Keylogger είναι ένα εργαλείο ασφάλειας που καταγράφει πολλές ενέργειες που λαμβάνονται στο PC σας. Τα πράγματα που δακτυλογραφούνται που στέλνονται, λαμβανόμενα και που επισκέπτονται, και screenshots ακόμη και καταγράφονται, έτσι μπορείτε να ελέγξετε τη χρήση PC.

Η προηγμένου Keylogger είναι εύκολη, αν και μπορεί να παρεμποδίσει μερικές εφαρμογές αντιιών, επειδή μπόρεσε να ανιχνευθεί ως spyware. Το πρόγραμμα είναι δύσκολο για τους χρήστες να δουν επειδή δεν δημιουργεί μια γραμματοθήκη προγράμματος ή δεν αφήνει ένα εικονίδιο στο δίσκο συστημάτων.

Τα προηγμένα αρχεία Keylogger πληκτρολογούν τα κτυπήματα, τους προσωπικούς κωδικούς, επισκέφτηκαν ιστοσελίδας, και το περιεχόμενο περιοχών αποκομμάτων. Μπορεί να τεθεί ως στόχος να πάρει screenshots περιοδικά. Τα αρχεία είναι εύκολο να διαβαστούν, και μπορούν ακόμη και να σταλθούν μήνυμα με το ηλεκτρονικό ταχυδρομείο σε σας έτσι μπορείτε να ελέγξετε το PC μακρινά.

Οι εφαρμογές όπως προηγμένο Keylogger προκύπτουν τα σοβαρά ζητήματα εμπιστοσύνης, και δεν μπορούν κατάλληλα να αντικαταστήσουν τη γονική επίβλεψη. Ως εκ τούτου, είναι πάντα καλύτερο να εποπτευθούν τα μικρά παιδιά προσωπικά όταν χρησιμοποιούν το Διαδίκτυο. Το advanced Keylogger είναι πολύ αποτελεσματικό στην κατασκόπευση στους χρήστες ενός PC. Δεδομένου ότι κρύβεται πολύ καλά, πρέπει να χρησιμοποιηθεί με σύνεση.

Χαρακτηριστικά του:

- Μπορεί να καταγράψει όλους τους απολογισμούς χρηστών
- Εύκολος να διαβάσει logs
- Εκθέσεις ηλεκτρονικού ταχυδρομείου

ΠΑΡΑΡΤΗΜΑ Β

Βιβλιογραφία

1. Ηλεκτρονικό Έγκλημα, Συγγραφέας Κ. Βλαχόπουλος, πρόλογος Ε. Μάγκος

2. Ασφάλεια στα δίκτυα υπολογιστών , Κίτσος

3. Αρχές δικαίου, Δρ. Νίκος Κρεμμύδας

Ιστοτόποι

1. greg61.gr : η γωνια του υπολογιστη και του διαδικτύου

2. http://el.wikipedia.org/wiki/Ασφάλεια_δικτύων_υπολογιστών

3. www.dpa.gr

4. www.safeline.gr

5.http://di.ionio.gr/~emagos/security/0/SHMEIWSEIS%20(OLD)%20 %20EISAGWGIKA%20THEMATA.pdf

6. ιστορια ασφάλειας των υπολογιστών

7. http://www.fa3.gr/nomothesia_2/nomoth_gen/prosopika-dedomena/n.2472.1997.pdf

8.http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=12774&Itemid=863&lang

9. http://advanced-keylogger.en.softonic.com/

10. www.royt.org

11.http://1.bp.blogspot.com/-kpkBDy5dpQM/T31_iuAEATI/AAAAAAAACVo/YJztvgBRg-E/s1600/%CE%93%CE%A1%CE%91%CE%A8%CE%99%CE%9C%CE%9F-250x190.jpg

12. http://www.neurocenter.gr/imagebank/writing_b.jpg