ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή Εργασία

«Ηλεκτρονικό Έγκλημα»

Της φοιτήτριας: Χριστοδούλου Έλενα

Αριθμός Μητρώου: 05/2948

Επιβλέπων Καθηγήτρια: Κα. Βασιλάκη Αθηνά

ΠΡΟΛΟΓΟΣ

Η ανάπτυξη της τεχνολογίας και ως επακόλουθο η ανάπτυξη της πληροφορικής και του Διαδικτύου έχουν καταστήσει τους υπολογιστές αναπόσπαστο μέρος της καθημερινότητας μας. Αυτή η εξέλιξη έφερε μαζί με τα θετικά και αρκετά αρνητικά στοιχεία. Ένα από αυτά τα αρνητικά είναι η εμφάνιση μιας νέας μορφής εγκλήματος το λεγόμενο Ηλεκτρονικό Έγκλημα.

Με την χρήση των υπολογιστών και με ή χωρίς τη χρήση του Διαδικτύου διαπράττονται καθημερινά αμέτρητα εγκλήματα. Ακόμη και ο ίδιος ο υπολογιστής μπορεί να είναι το θύμα της επίθεσης. Απάτες, απειλές, υποκλοπές και κάθε είδους παρανομίες συμβαίνουν και το θύμα δεν το αντιλαμβάνεται καν.

Το Ηλεκτρονικό Έγκλημα πήρε τεράστιες διαστάσεις και ο κάθε οργανισμός και μεμονωμένος χρήστης πρέπει να ενημερωθεί για τους κινδύνους και τους τρόπους που θα προστατευθεί ο ίδιος και το πληροφοριακό του σύστημα από κάθε είδους κακόβουλη απειλή.

ΠΕΡΙΛΗΨΗ

Οι όροι «Ηλεκτρονικό Έγκλημα» και «Κυβερνοέγκλημα» έχουν μπει για τα καλά στη ζωή μας. Το Ηλεκτρονικό Έγκλημα ορίζεται ως μια εγκληματική πράξη στην οποία ο Ηλεκτρονικός Υπολογιστής χρησιμοποιείτε ως το κύριο μέσο τέλεσης της.

Η Πτυχιακή αυτή εργασία παρουσιάζει αρχικά τα χαρακτηριστικά γνωρίσματα της νέας αυτής μορφής εγκλήματος και τις σχετικές παραβάσεις. Στη συνέχεια γίνεται αναφορά στις απειλές που πέρα από τους ηλεκτρονικούς εγκληματίες πολλές φορές απειλή για ένα σύστημα είναι ο ίδιος ο χρήστης λόγω κακής χρήσης αλλά και ο ίδιος ο κατασκευαστής λόγω ύπαρξης ευπαθειών στο πληροφοριακό σύστημα. Τα εργαλεία τέλεσης του εγκλήματος είναι πλέον πολλά και εξελιγμένα ώστε και ο πιο απλός χρήστης να μπορεί να διαπράξει μια κακόβουλη πράξη.

Εν συνεχεία θα δούμε ότι οι μορφές του Ηλεκτρονικού Εγκλήματος είναι πάρα πολλές. Το άνοιγμα ενός κακόβουλου e-mail μπορεί να καταστρέψει στη στιγμή το σύστημα μας, η απλή χρήση του τηλεφώνου μας μπορεί να οδηγήσει στην υποκλοπή προσωπικών μας δεδομένων αλλά και τόσες άλλες απειλές όπως θα δούμε έχουν γίνει μέρος της καθημερινότητας κάθε χρήστη Η/Υ.

Έτσι πρέπει με κάθε τρόπο να προστατεύσουμε το σύστημα μας ώστε να προστατεύσουμε και το ίδιο το άτομο μας. Υπάρχουν πολλοί τρόποι να αποτρέψουμε αυτές τις επιθέσεις από την εγκατάσταση ενός απλού προγράμματος antivirus στον υπολογιστή μας μέχρι και εξειδικευμένα πρωτόκολλα όπως θα παρουσιάσουμε.

Πέρα από αυτά όμως θα γίνει εκτενείς αναφορά στη νομοθεσία που διέπει το Ηλεκτρονικό Έγκλημα σε παγκόσμιο επίπεδο και τα νομοθετικά ζητήματα. Τέλος θα γίνει αναφορά στην διερεύνηση του Ηλεκτρονικού Εγκλήματος, στο δύσκολο αυτό έργο της Αστυνομίας που με κάθε τρόπο πρέπει να το καταπολεμήσει.

ABSTRACT

The terms “Electronic Crime” and “Cyber crime” have come on well in our life. The Electronic Crime is defined as a criminal act in which the computer is used as the primary means of execution.

This paper presents original features of this new type of crime and related offences. Then it refers to threats beyond the electronic criminal often a threat to a system is the same user due to misuse and the manufacturer’s own vulnerabilities that exist in the information system. The tools of the crime are now many sophisticated that even the simplest user to commit a malicious act.

Then we see that the forms of computer crime are too many. Opening a malicious e-mail can ruin at the moment our system, simply use our phone can lead to steal our personal data as well as many other threats as we see have become part of everyday life of each computer user.

That means we should protect our system and our self. There are many ways to prevent these attacks by installing a simply program antivirus on our computer and specialized protocols as they are presents below.

However these will be extensive reference to the law governing cyber crime globally and legislative issues. Finally we mention the investigation of cyber crime, the arduous task of police in any way that we must fight.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

ΕΙΣΑΓΩΓΗ

Στη συγκεκριμένη Πτυχιακή εργασία γίνεται μια λεπτομερής μελέτη στο Ηλεκτρονικό Έγκλημα. Στόχος είναι ο αναγνώστης να αποκτήσει μια πλήρης εικόνα του θέματος, να προβληματιστεί αλλά και με τη σειρά του να είναι ικανός να προστατέψει το προσωπικό του σύστημα ή το σύστημα του οργανισμού του, το άτομο του σαν χρήστη αλλά και τον οποιοδήποτε χρήστη Η/Υ.

Στην εργασία υπάρχουν 6 κεφάλαια:

Στο πρώτο κεφάλαιο «Ορίζοντας το Ηλεκτρονικό Έγκλημα», δίνεται ο ορισμός του Ηλεκτρονικού εγκλήματος, των κατηγοριών του και γίνεται ένας διαχωρισμός του από το παραδοσιακό έγκλημα.

Στο δεύτερο κεφάλαιο «Ηλεκτρονικοί Εγκληματίες», παρουσιάζονται οι διάφορες στις αιτίες πρόκλησης του εγκλήματος, οι αιτίες τους και οι κίνδυνοι που φέρουν καθώς και τα μέσα τέλεσης της πράξης. Επίσης γίνεται μια παρουσίαση και στον ίδιο τον ηλεκτρονικό εγκληματία

Στο τρίτο κεφάλαιο «Μορφές Ηλεκτρονικού Εγκλήματος» γίνεται διεξοδική αναφορά στις μορφές του Ηλεκτρονικού Εγκλήματος και γι’ αυτό είναι απαραίτητος ο διαχωρισμός τους σε δυο βασικές κατηγορίες. Στην πρώτη κατηγορία έχουμε τα εγκλήματα που εμφανιστήκαν μαζί με τους ηλεκτρονικούς υπολογιστές και το διαδίκτυο και χαρακτηρίζονται ως «γνήσια» και στη δεύτερη κατηγορία εντάσσονται τα εγκλήματα που παρόλο προϋπήρχαν των ηλεκτρονικών υπολογιστών και του διαδικτύου, αυτά τα δυο συντελούν σε μεγάλο βαθμό στην εκτέλεση τους.

Στο τέταρτο κεφάλαιο «Ασφάλεια στο Διαδίκτυο και Ηλεκτρονικό Έγκλημα», παρουσιάζεται η έννοια της ασφάλειας στου Η/Υ, τα μέτρα που μπορούμε να πάρουμε για πρόληψη από μια κακόβουλη επίθεση αλλά και τα μέσα που θα μας βοηθήσουν να εντοπίσουμε μιας επίθεσης. Τέλος δίνονται κάποιες συμβουλές χρήσιμες για τον κάθε χρήστη.

Στο πέμπτο κεφάλαιο «Νομοθεσία και Ηλεκτρονικό Έγκλημα», γίνεται διεξοδική αναφορά στην νομοθεσία που διέπει το Ηλεκτρονικό Έγκλημα σε παγκόσμιο και εν χόριο επίπεδο, καθώς και στα προβλήματα που αντιμετωπίζει η νομοθεσία λόγω της ραγδαίας ανάπτυξης της τεχνολογίας αλλά και της παγκοσμιότητας που χαρακτηρίζει κάθε έγκλημα τέτοιου τύπου.

Στο έκτο κεφάλαιο «Η διερεύνηση του Ηλεκτρονικού Εγκλήματος», βλέπουμε πως πρέπει να αντιμετωπίσει ο εξερευνητής τη σκηνή του εγκλήματος, τα τεκμήρια που θα συλλέξει από το χώρο του εγκλήματος και γενικά το κάθε στοιχείο. Θα γίνει αναφορά στα λογισμικά που χρησιμοποιούνται για τη μελέτη των στοιχείων. Όπως θα δούμε είναι ένα έργο δύσκολο όπου το κάθε τι κρίνετε στην λεπτομέρεια ώστε η έρευνα να είναι αξιόπιστη και αποδεκτή από το δικαστήριο.

ΚΕΦΑΛΑΙΟ 1
ΟΡΙΖΟΝΤΑΣ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Το έγκλημα ως αναπόσπαστο κομμάτι κάθε κοινωνίας, έχει τη μορφή ενός ζωντανού οργανισμού. Συνεχώς μεταβάλλονται οι μορφές του, τα μέσα διάπραξης του και η νομοθεσία που το διέπει. Αναζητώντας τις ρίζες του ηλεκτρονικού εγκλήματος, διαπιστώνουμε ότι ταυτόχρονα με την εμφάνιση των υπολογιστών, έγιναν και οι πρώτες προσπάθειες από τους επίδοξους «ηλεκτρονικούς εγκληματίες» να βρούνε τρόπους να εκμεταλλευτούν τις νέες αυτές τεχνολογίες προς όφελος για τους ίδιους ή για τρίτους. Η νέα τεχνολογία, που αναπτυσσόταν με γοργούς ρυθμούς, έδινε νέες ευκαιρίες για εύκολη διάπραξη πλήθους εγκλημάτων. Στο κεφάλαιο αυτό θα αναφερθούμε στο ηλεκτρονικό έγκλημα αλλά και το κυβερνοέγκλημα και τις συνέπειες που φέρουν.

1.1 ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ ΚΑΙ ΤΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ ΓΝΩΡΙΣΜΑΤΑ

Σύμφωνα με τους Forester και Morrison (1994) το ηλεκτρονικό έγκλημα ορίζετε ως «μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσης της».
Στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται για να το περιγράψουν είναι: ηλεκτρονικό έγκλημα, δικτυακό έγκλημα, και έγκλημα του κυβερνοχώρου.

Βασικό συστατικό στοιχείο του ηλεκτρονικού εγκλήματος, αποτελεί η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως ηλεκτρονικός υπολογιστής, κινητό τηλέφωνο, notebook κ.λπ. Κυρίαρχο ρόλο διαδραματίζει ο Η/Υ, ο οποίος μπορεί (πηγή: Shinder 2002:5):

- Να αποτελεί τον στόχο κάποιας επίθεσης. Στην περίπτωση αυτή μπορούμε να πούμε ότι ο υπολογιστής είναι το «θύμα» της επίθεσης.
- Να αποτελεί το μέσο διάπραξης κάποιας επίθεσης, δηλαδή το εργαλείο που χρησιμοποιεί ο επιτιθέμενος για να πραγματοποιήσει τον εγκληματικό σκοπό του.

- Να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος, π.χ. να αποθηκεύονται σε αυτό στοιχεία ή πληροφορίες που αφορούν άτομα τα οποία συμμετέχουν σε παράνομες δραστηριότητες.

Παράλληλα, ο ορισμός του ηλεκτρονικού εγκλήματος εξαρτάται σε μεγάλο βαθμό από την οπτική γωνία από την οποία εξετάζετε. Η μορφής αυτής της εγκληματικότητας είναι τόσο πολύπλοκη σε σημείο που δυσχεραίνει ακόμη και το νομοθέτη, ο οποίος αποφεύγει να το ορίσει και είτε αφήνει την αρμοδιότητα αυτή στα δικαστήρια και τη παραγόμενη νομολογία, είτε δανείζεται τους χρησιμοποιούμενους από την τεχνολογία όρους.
Καλό είναι να σημειωθεί ότι η εμπλοκή ενός ηλεκτρονικού υπολογιστή ή δικτύου δεν σημαίνει αναγκαστικά ότι έχουμε να κάνουμε με ηλεκτρονικό έγκλημα.

Βασικές Κατηγορίες Ηλεκτρονικού Εγκλήματος (πηγή: Αργυρόπουλος, 2001):

- Σε εγκλήματα που διαπράττονται τόσο σε συμβατικό περιβάλλον ή σε περιβάλλον ηλεκτρονικών υπολογιστών. Παράδειγμα αποτελεί η συκοφαντική δυσφήμηση που μπορεί να διαπραχθεί με τη δημοσίευση στο διαδίκτυο μιας σελίδας με προσβλητικό περιεχόμενο για ένα πρόσωπο. Σε αυτή την περίπτωση το Διαδίκτυο αποτελεί το μέσο για την τέλεση του εγκλήματος.
- Σε εγκλήματα που διαπράττονται χωρίς τη βοήθεια του διαδικτύου, όπως είναι η παράνομη αντιγραφή λογισμικού.
- Σε εγκλήματα που διαπράττονται αποκλειστικά με την χρήση του διαδικτύου, όπως είναι η διασπορά κακόβουλου λογισμικού (ιών).

Τα ψηφιακά εγκλήματα διαφέρουν από τα παραδοσιακά εγκλήματα στα εξής χαρακτηριστικά:

- Διαπράττονται συνήθως από μακρινή απόσταση.
- Ο εντοπισμός του ψηφιακού εγκληματία είναι τεχνολογικά περίπλοκος.
- Αποδίδουν μεγάλα κέρδη με μικρό κίνδυνο ανακάλυψης του δράστη τους.
- Ο αριθμός των θυμάτων τους σε σχέση με εκείνο των παραδοσιακών εγκλημάτων είναι κατά πολύ μεγαλύτερος.

- Οι οικονομικές απώλειες που επιφέρουν στα θύματα τους είναι πολύ μεγαλύτερες από αυτές των παραδοσιακών εγκλημάτων και
- Στο μεγαλύτερο μέρος τους δεν καταγράφονται από καμιά επίσημη αρχή, δηλαδή, ο «σκοτεινός αριθμός» τους είναι ιδιαίτερα σημαντικός.

1.2 ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

Σαν κυβερνοέγκλημα θα μπορούσαμε να ορίσουμε το έγκλημα για το όποιο ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από τον κυβερνοχώρο, ορισμό τον όποιο δίνει ο Donn Parker, βετεράνος ασφαλείας με τριανταετή πείρα στα ηλεκτρονικά εγκλήματα. Ο ίδιος διαχωρίζει το κυβερνοέγκλημα από το ηλεκτρονικό έγκλημα ορίζοντας το τελευταίο ως «το έγκλημα στο όποιο ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από την τεχνολογία των υπολογιστών». Ωστόσο οι ορισμοί αυτοί δεν αρκούν για να διαφωτίσουν όλες τις διαστάσεις του προβλήματος.

Το κυβερνοέγκλημα απασχόλησε σε μεγάλο βαθμό την Εξεταστική Επιτροπή της Μεγάλης Βρετανίας, ένα σώμα ανεξάρτητο, υπεύθυνο κυρίως για τον έλεγχο των δραστηριοτήτων των τοπικών κυβερνήσεων και των υπηρεσιών υγείας στην Αγγλία και την Ουαλία. Από τις αρχές της δεκαετίας το ’80 (όπου και ιδρύθηκε) η Επιτροπή διενήργησε έρευνες προκειμένου να εξακριβώσει την έκταση του εγκλήματος μέσω ηλεκτρονικού υπολογιστή στο δημόσιο και στον ιδιωτικό τομέα. Οι έρευνες αυτές έδειξαν ότι με το πέρασμα του χρόνου το διαπιστωμένο ποσοστό των διαφόρων κατηγοριών εγκλημάτων έχει αυξηθεί. Στις μελέτες του 1981 οι μόνες κατηγορίες εγκλημάτων ήταν η άπατη και η κλοπή, ενώ το 1998 το ποσοστό αυτό είχε υπερτετραπλασιαστεί αφού είχαν συμπεριληφθεί κι άλλες κατηγορίες εγκλημάτων, των όποιων η περιγραφή ακολουθεί στον επερχόμενο πίνακα, σύμφωνα με την Εξεταστική Επιτροπή της Μεγάλης Βρετάνιας.

Ο πίνακας που ακολουθεί βοηθάει στον διαχωρισμό ανάμεσα στα εγκλήματα κατά τα οποία ο υπολογιστής αποτελεί βοηθητικό μέσο και σε αυτά που αποτελεί τον βασικό στόχο.

Στα εγκλήματα με τη βοήθεια του υπολογιστή, ο υπολογιστής λειτουργεί ως βοηθητικό μέσο αλλά το έγκλημα μπορεί να διαπραχθεί και χωρίς αυτόν, ενώ στα εγκλήματα που είναι επικεντρωμένα στους υπολογιστές, συμπεριλαμβάνονται και οι περιπτώσεις στις οποίες η εγκληματική πράξη αποτελεί το άμεσο αποτέλεσμα της τεχνολογίας των υπολογιστών χωρίς να υπάρχει παράλληλη εμφάνιση της και σε άλλους τομείς. Εδώ συμπεριλαμβάνονται τα προβλήματα των ιών και του hacking.

Σε αυτό το σημείο αξίζει να σημειωθεί ότι σε καμία περίπτωση δεν θα πρέπει να δοθεί η εντύπωση πως η πρώτη κατηγορία, στην οποία ο υπολογιστής αποτελεί βοήθημα, είναι λιγότερο σοβαρή. Ωστόσο θα μπορούσαμε να πούμε πως τα εγκλήματα που επικεντρώνονται στους υπολογιστές, είναι εκείνα που διαπράττονται από κυβερνοεγκληματίες με άμεση επίθεση στις τεχνολογίες που η κοινωνία της πληροφορίας έχει συστήσει.

Η χρήση παράνομου υλικού αποτελεί κι αυτή έμμεσα έγκλημα, αφού απαιτείται η παρουσία ηλεκτρονικού υπολογιστή. Η φύση της παρανομίας αυτής σχετίζεται με ζητήματα πνευματικής ιδιοκτησίας. Ωστόσο, αν καλούμασταν να την κατατάξουμε σε μία από τις παραπάνω κατηγορίες, θα την κατατάσσαμε στα εγκλήματα που τελούνται με τη βοήθεια του υπολογιστή.

ΠΙΝΑΚΑΣ 1

Κατηγορίες Ηλεκτρονικών Εγκλημάτων και Προσβολών κατά την Εξεταστική Επιτροπή της Μεγάλης Βρετανίας.

Έγκλημα / Προσβολή	**Περιγραφή**
Απάτη	(Για προσωπική ωφέλεια) Αλλοίωση των εισαγωγών με μη νόμιμο τρόπο: Καταστροφή / συμπίεση / ακαταλληλότητα εκροών Αλλοίωση των δεδομένων του Η/Υ Αλλοίωση ή κακή χρήση των προγραμμάτων.

Έγκλημα / Προσβολή	**Περιγραφή**
Χρήση λογισμικού χωρίς άδεια	Χρήση παράνομων αντίγραφων λογισμικού.
Κλοπή	Των δεδομένων Του λογισμικού.
Ιδιωτική εργασία	Μη εγκεκριμένη χρήση των δυνατοτήτων των συστημάτων Η/Υ του οργανισμού για αποκομιδή κέρδους ή για ίδιον όφελος.
Κακή χρήση προσωπικών δεδομένων	Ανεπίσημη «ανάγνωση» των αρχείων ενός συστήματος Η/Υ του οργανισμού της σχετικής νομοθεσίας
Χόκινγκ Σαμποτάζ	Ελεύθερη πρόσβαση σε ένα σύστημα υπολογιστή συνήθως με τη χρήση των δυνατοτήτων της επικοινωνίας. Η διαμεσολάβηση με την πρόκληση ζημιάς στον τρέχοντα κύκλο ή στον εξοπλισμό
Εισαγωγή	Εισαγωγή υλικού πορνογραφικού περιεχομένου μέσω internet.
Ιοί	Διάχυση ενός προγράμματος με σκοπό τη ματαίωση της τρέχουσας εφαρμογής.

Παράλληλα σύμφωνα με τη διεθνής σύμβαση για το κυβερνοέγκλημα του 2001 (Convention on Cyber Crime 2001) οι κύριες ψηφιακές παραβάσεις (εγκλήματα) είναι οι ακόλουθες:

- Παράνομη πρόσβαση,
- Παράνομη υποκλοπή,
- Παρεμβολή σε δεδομένα,
- Παρεμβολή σε συστήματα,
- Κακή χρήση συσκευών,
- Κλοπή που σχετίζετε με υπολογιστή,
- Απάτη που σχετίζετε με υπολογιστή,
- Παιδική πορνογραφία και
- Κλοπή πνευματικών δικαιωμάτων ηλεκτρονικών πληροφοριών.

Βλέπουμε ότι με την ανάπτυξη των ηλεκτρονικών υπολογιστών άρχισε να δημιουργείται μια νέα μορφή εγκλήματος το λεγόμενο ηλεκτρονικό έγκλημα, το οποίο χρησιμοποιεί τον Η/Υ είτε σαν θύμα, είτε σαν εργαλείο επίθεσης, είτε σαν βοηθητικό μέσο στο έγκλημα. Οι παραβάσεις των εγκλημάτων αυτών είναι πολλές και ο κατάλογος μεγαλώνει ακόμη περισσότερο όταν εμπλέκεται και το διαδίκτυο σ' αυτά. Έτσι η εξιχνίαση γίνεται ακόμη πιο δύσκολη και παράλληλα αυξάνονται οι συνέπειες τους. Καλό θα ήταν να μελετήσουμε τις μορφές του ηλεκτρονικού εγκλήματος αλλά και τους ίδιους τους ηλεκτρονικούς εγκληματίες, τις αιτίες-λάθη που προκαλούν αυτά τα εγκλήματα και τα μέσα τέλεσης τους ώστε να γνωρίζουμε πλήρως τους κινδύνους για να μπορούμε να προστατευτούμε.

ΚΕΦΑΛΑΙΟ 2
ΗΛΕΚΤΡΟΝΙΚΟΙ ΕΓΚΛΗΜΑΤΙΕΣ

Αφού ορίσαμε αρχικά το ηλεκτρονικό έγκλημα καλό θα ήταν να επικεντρωθούμε στις αιτίες πρόκλησης των εγκλημάτων αυτών, αλλά και στον ίδιο τον ηλεκτρονικό εγκληματία που όπως θα δούμε θεωρεί τον εαυτό του υγειές κομμάτι της κοινωνίας. Στο τέλος του κεφαλαίο θα αναφερθούμε και στα μέσα τέλεσης των εγκλημάτων αυτών.

2.1 ΒΑΣΙΚΕΣ ΜΟΡΦΕΣ ΑΠΕΙΛΩΝ

Ο όρος απειλή, όταν αναφέρετε σε ένα υπολογιστικό σύστημα, προσδιορίζει μια κατάσταση όπου υπάρχει η περίπτωση να προκληθεί απώλεια ή ζημιά. Οι απειλές μπορεί να προέρχονται από ανθρώπινες επιθέσεις, από φυσικές καταστροφές, από ακούσια ανθρώπινα λάθη ή από εξωτερικές ατέλειες του εξοπλισμού και του λογισμικού (πηγή: Πάγκαλος, 2002).

(i) Εξωτερικές απειλές (outside threats): είναι ίσως η πιο συνηθισμένη μορφή επιθέσεων. Οι επιθέσεις του τύπου αυτού, προέρχονται από τους hacker και cracker που ανήκουν στο εξωτερικό περιβάλλον ενός συστήματος. Οι πιο συχνές μορφές που συναντάμε είναι η μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο, οι επιθέσεις άρνησης εξυπηρέτησης και η διασπορά κακόβουλου λογισμικού.

(ii) Εσωτερικές απειλές (inside treats): προέρχονται από το εσωτερικό ενός οργανισμού και συνήθως από το ίδιο το εργαζόμενο σε αυτόν προσωπικό. Οι επιθέσεις της μορφής αυτής πραγματοποιούνται από πρώην υπαλλήλους που γνωρίζουν πολύ καλά τις πολιτικές ασφαλείας του οργανισμού. Εκτός όμως των επιθέσεων από άτομα, στις εσωτερικές απειλές εντάσσονται και προβλήματα που οφείλονται στο σχεδιασμό των συστημάτων, στις ευπάθειες λογισμικού και εξοπλισμού, στις πολιτικές ασφαλείας ακόμη και στους ίδιους τους χρήστες, που ενδεχομένως, να υποπέσουν σε λάθη, ικανά να θέσουν σε κίνδυνο την ασφάλεια του συστήματος.

(iii) Κοινωνική Μηχανή: αποτελεί μια από τις σοβαρότερες μορφές επιθέσεων. Ο επιτιθέμενος εκμεταλλεύεται τον ανθρώπινο παράγοντα

(π.χ. αφέλεια, ευπιστία κ.λπ.) ώστε να αποκτήσει πρόσβαση σε πληροφορίες που θα τον βοηθήσουν να εξαπολύσει μια επίθεση.

2.2 ΕΞΩΤΕΡΙΚΕΣ ΑΠΕΙΛΕΣ

2.2.1 HACKERS

Στη σύγχρονη τεχνολογία των ηλεκτρονικών υπολογιστών, ο όρος hacker έχει για τα καλά εισβάλει στη ζωή μας. Αντίστοιχο συνώνυμο δεν υπάρχει στην Ελληνική Γλώσσα. Στη δεκαετία του ’60 και ’70, ο όρος χρησιμοποιούταν για τους τελειομανείς των υπολογιστών αλλά και για τον καθένα που επιτελούσε οποιαδήποτε δραστηριότητα που σχετιζόταν με πολύπλοκα συστήματα.

Οι hackers αποτελούν άτομα με εξαιρετική γνώση της τεχνολογίας των υπολογιστών, που καταφέρνουν να διεισδύσουν σε υπολογιστικά συστήματα αποκτώντας πρόσβαση σε γνώση και πληροφορίες. Σκοπός τους, σύμφωνα με τις ιδεολογικές αρχές που τους διέπουν, δεν είναι ούτε η πρόκληση ζημιάς ούτε η αποκόμιση οικονομικού οφέλους. Παρόλα αυτά, οι περισσότεροι αντιμετωπίζουν τον όρο hacker με αρνητική διάθεση, θεωρώντας ότι αποτελεί συνώνυμο του εγκληματία του διαδικτύου.

Όταν σε οποιαδήποτε ενέργεια, που σχετίζεται με τους ηλεκτρονικούς υπολογιστές και τα δίκτυα, υπάρχει το στοιχείο της εγκληματικής πρόθεσης ο επιτιθέμενος χαρακτηρίζετε ως cracker. Οι cracker είναι hackers που χρησιμοποιούν την γνώση τους για τους ηλεκτρονικούς υπολογιστές για να αποκομίσουν όφελος για τους ίδιους ή για τρίτους

Εκτός από τους όρους hacker και cracker, υπάρχουν και άλλοι όροι για να περιγράψουν τους εγκληματίες του Διαδικτύου όπως, hacktivists, vandals και cyberterrorists. Σε όλες τις περιπτώσεις αναφερόμαστε στους hackers, που λόγω του συγκεκριμένου τρόπου υλοποίησης των εγκληματικών τους προθέσεων έχουν λάβει και τα ανάλογα προσωνύμια.

Ο όρος hactivist αναφέρετε σε μια «ηλεκτρονική απείθεια κατά των αρχών» που πραγματοποιείται στον κυβερνοχώρο, όπως π.χ. επιθέσεις άρνησης εξυπηρέτησης μέσω της μαζικής επίσκεψης σε ένα δικτυακό τόπο σε συγκεκριμένη χρονική στιγμή ή μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, παράνομη εισβολή σε κυβερνητικά site, διασπορά κακόβουλου λογισμικού κ.α. (πηγή: Denning, 2001).

Ο όρος vandals, αναφέρετε στους hackers που εισβάλουν σε δικτυακούς τόπους με μοναδικό σκοπό την τροποποίηση τους κατά τρόπο προπαγανδιστικό, προσβλητικό ή ακόμη και χιουμοριστικό, ανάλογα με το σκοπό που θέλουν να επιτύχουν. Οι επιθέσεις αυτές πλήττουν το κύρος και την αξιοπιστία του οργανισμού εναντίον του οποίου στρέφεται η επίθεση.

Ο όρος cyberterrotist αναφέρεται σ' αυτούς που χρησιμοποιούν το διαδίκτυο για την πραγματοποίηση τρομοκρατικών επιθέσεων.

2.2.2 ΤΟ ΠΡΟΦΙΛ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΙΑ

Τα κίνητρα των επιθέσεων διαφέρουν ανάλογα με την περίπτωση και την προσωπικότητα του επιτιθέμενου. Μπορούμε να διακρίνουμε τις ακόλουθες κατηγορίες (πηγή: Anderson 2001, Μάγκος 2004):

- Ερασιτέχνες: Πρόκειται για ανθρώπους χωρίς ιδιαίτερες δεξιότητες στους υπολογιστές, που προσπαθούν να εντοπίσουν μια ευπάθεια σε ένα υπολογιστικό σύστημα και στη συνέχεια να την εκμεταλλευτούν. Τα κίνητρα τους είναι η περιέργεια και η απόκτηση γνώσης, χωρίς όμως να αποκλείεται και το γεγονός ότι αποσκοπούν σε οποιοδήποτε είδους όφελος. Χρησιμοποιούν πάντα έτοιμα εργαλεία, γιατί οι περισσότεροι δεν κατέχουν τις απαραίτητες γνώσεις για να τα κατασκευάσουν.
- Hackers: Οι hackers είναι άριστοι γνώστες προγραμματισμού, δικτύων Η/Υ και Internet. Τα εργαλεία που χρησιμοποιούν τα αναπτύσσουν οι ίδιοι. Σκοπός των επιθέσεων τους είναι η ικανοποίηση της περιέργειας τους και η επιβεβαίωση της ικανότητας τους για εισβολή σε ένα σύστημα.
- Crackers: Οι crackers προέρχονται από τους hackers. Έχουν ως σκοπό την πρόκληση ζημιάς ή την αποκόμιση οφέλους από τα συστήματα στα οποία

επιτίθενται. Οι δημιουργοί των ιών και γενικότερα κακόβουλου λογισμικού μπορούν να θεωρηθούν ως crackers.

- Επαγγελματίες εισβολείς (career criminals): Οι εγκληματίες της κατηγορίας αυτής, έχουν το επίπεδο γνώσεως των hackers. Οι επιθέσεις τους σχετίζονται με τα σοβαρότερα εγκλήματα του κυβερνοχώρου, όπως η βιομηχανική κατασκοπία. Κερδίζουν μέρος ή το σύνολο του εισοδήματος τους από επιθέσεις.

2.2.3 Η ΗΘΙΚΗ ΤΩΝ HACKERS (hacker ethics)

Μέσα από τη συνεχή ενασχόληση με τους υπολογιστές, οι hackers δημιούργησαν ένα σύνολο κανόνων, το οποίο χαρακτηρίζει την κουλτούρα τους και έχει επικρατήσει διεθνώς ως η «η ηθική των hackers». Οι κανόνες ηθικής επιδιώκουν να αντικρούσουν τη λανθασμένη, κατά την άποψη τους, γνώμη ότι οι hackers είναι εγκληματίες, αυτοί που κατεξοχήν τελούν ηλεκτρονικά εγκλήματα.

Ο Steven Levy (2001), κατέγραψε τους βασικότερους κανόνες που διέπουν την ηθική των hackers:

- Η πρόσβαση στους υπολογιστές, καθώς και σ' οποιοδήποτε μέσο, ενδεχομένως, θα μπορούσε να σε διδάξει και να σε πληροφορήσει για τον τρόπο που λειτουργεί καθετί στον κόσμο – θα πρέπει να είναι ολοκληρωτική και χωρίς κανένα περιορισμό. Πάντα να υπακούς στην προσταγή: «Πάρε τον έλεγχο στα χέρια σου!».
- Κάθε είδους πληροφορία θα πρέπει να είναι ελεύθερη.
- Μην εμπιστεύεσαι εξουσία και αυθεντία. Να υποστηρίζεις τον αντισυγκεντρωτισμό.
- Οι hackers θα πρέπει να κρίνονται από την ίδια τη δράση τους, όχι από λανθασμένα κριτήρια, όπως πτυχία, ηλικία, φυλή ή κοινωνική θέση.
- Μπορείς να δημιουργήσεις τέχνη και ομορφιά σε ένα υπολογιστή.
- Οι υπολογιστές μπορούν να αλλάξουν τη ζωή σου προς το καλύτερο.

Οι hackers θεωρούν τους εαυτούς τους υγιές κομμάτι του Διαδικτύου και κατηγορούν τους crackers για τη διάπραξη των εγκλημάτων. Αν σκεφτούμε ότι οι hackers είναι αυτοί που εφευρίσκουν τις τεχνικές διείσδυσης σε υπολογιστικά

συστήματα, είναι αυτοί που δημιουργούν κακόβουλο λογισμικό, επίσης εντοπίζουν τις ευπάθειες των συστημάτων και τις κάνουν ευρέως γνωστές τότε θα έπρεπε να τους θεωρούμε εξίσου κακόβουλους με τους crackers αφού είναι αυτοί που δημιουργούν τις προϋποθέσεις, τις τεχνικές και τα μέσα τέλεσης του ηλεκτρονικού εγκλήματος.

2.3 ΕΣΩΤΕΡΙΚΕΣ ΑΠΕΙΛΕΣ

2.3.1 ΥΠΑΛΛΗΛΟΙ

Οι εσωτερικές απειλές, συχνά είναι ο μεγαλύτερος κίνδυνος που έχει να αντιμετωπίσει ένας οργανισμός. Αυτό αποδεικνύεται με διάφορες έρευνες εγκληματικότητας στο διαδίκτυο αφού έχουν καταδείξει ότι το 75% των επιθέσεων πραγματοποιείται από υπαλλήλους εταιρειών και μάλιστα από αυτούς που κατέχουν διευθυντικές θέσεις.

Τα κίνητρα των επιθέσεων ίσως είναι οικονομικό ή άλλο όφελος, για να βλάψουν κάποιο συνεργάτη ή για να εκδικηθούν κάποιο πρόσωπο ή την ίδια την εταιρεία. Η γνώση των πολιτικών ασφαλείας της εταιρείας, των κωδικών πρόσβασης στα συστήματα καθώς και άλλων λεπτομερειών για την ασφάλεια των συστημάτων καθιστούν μια εσωτερική επίθεση ιδιαιτέρως εύκολη και τον εντοπισμό της εξίσου δύσκολη.

2.3.2 ΛΑΘΗ ΣΤΟ ΣΧΕΔΙΑΣΜΟ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ – ΕΥΠΑΘΕΙΕΣ

Οι hackers ή crackers, εκμεταλλεύονται μια αδυναμία του στόχου, ένα σημείο που μπορεί να δώσει πρόσβαση σ’ ένα σύστημα. Επομένως απειλή δεν είναι μόνο ο επιτιθέμενος αλλά και η ελλιπής ασφάλεια του συστήματος που χρησιμοποιούμε.

Ένα σύστημα, όσο καλά και αν έχει δοκιμαστεί, πάντα θα έχει κάποια αδύνατα σημεία: τις ευπάθειες (vulnerabilities). Οι ευπάθειες των συστημάτων μπορούν να οριστούν ως «Αδυναμία ή ελάττωμα στο υλικό (hardware), στο λογισμικό (software) ή στην αρχιτεκτονική ενός συστήματος, καθώς και στις διαδικασίες ασφάλειας που ακολουθούνται και μπορεί κάποιος να εκμεταλλευτεί προκειμένου

να παραβιάσει τη διαθεσιμότητα, ακεραιότητα ή εμπιστευτικότητα του συγκεκριμένου συστήματος». Τις πιο σημαντικές ευπάθειες τις συναντάμε στο λογισμικό, από τη μια γιατί ο σχεδιασμός του είναι πιο δύσκολος από το υλικό και από την άλλη γιατί γενικά ο σχεδιασμός ασφαλούς λογισμικού είναι μια πολύ δύσκολη διαδικασία σε σχέση με τη δημιουργία ασφαλούς υλικού.

Η US-CERT σε μια έκθεση της σχετικά με τις ευπάθειες των λειτουργικών συστημάτων, αναφέρει ότι το 2005 εντοπίστηκαν συνολικά 5198 ευπάθειες από τις οποίες οι 812 αναφέρονται στα λειτουργικά συστήματα Windows, οι 2328 σε Linux-Unix και οι 2058 σε διάφορα λειτουργικά συστήματα.

Οι αδυναμίες στο λογισμικό εφαρμογών, προέρχονται από το λανθασμένο αρχικό σχεδιασμό τους και από την ελλιπή συντήρηση και διαχείριση, για την οποία ευθύνεται ο διαχειριστής του συστήματος.

Όσο αφορά τα δίκτυα και τα υπολογιστικά συστήματα, λάθη σχεδιασμού μπορούν να εντοπιστούν στη λειτουργία firewalls, στα συστήματα ελέγχου και καταγραφής συμβάντων και στο λογισμικό προστασίας από ιούς (antivirus).

2.3.3 ΧΡΗΣΤΕΣ ΣΥΣΤΗΜΑΤΩΝ

Πολλές φορές οι σημαντικότεροι κίνδυνοι για την ασφάλεια των συστημάτων προέρχονται από τους ίδιους τους χρήστες. Τα λάθη των χρηστών μπορεί να οδηγήσουν σε καταστροφικές συνέπειες για το σύστημα είτε άμεσα είτε έμμεσα. Άμεσα, στην περίπτωση όπου ένας χρήστης μπορεί π.χ. να ανοίξει ένα συνημμένο αρχείο από ένα άγνωστο e-mail, το οποίο να περιέχει κακόβουλο λογισμικό που μπορεί να προκαλέσει ζημιές στο σύστημα. Έμμεσα, στην περίπτωση π.χ. της κακής φύλαξης των κωδικών πρόσβασης, με αποτέλεσμα να διαρρεύσουν σε άτομα που δεν έχουν δικαίωμα πρόσβασης.

2.3.4 ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΗ

Η Κοινωνική Μηχανή (Social Engineering) είναι η πιο σοβαρή μορφή επιθέσεων και όσοι γνωρίζουν καλά την τεχνική αυτή δύσκολα αποτυγχάνουν στις επιθέσεις

τους. Οι επιθέσεις αυτές βασίζονται σε κάτι πού απλό: την επιρροή και πειθώ τους προς τα υποψήφια θύματα, με αποτέλεσμα, την απόσπαση ευαίσθητων πληροφοριών. Εκμεταλλεύονται την έμφυτη επιθυμία του ανθρώπου να είναι εξυπηρετικός, την τάση του να εμπιστεύεται άλλους ανθρώπους και το φόβο προς τους ανώτερους του (πηγή: Mitnic, 2002).

Σύμφωνα με την Κοινωνική Μηχανή, το αδύνατο σημείο ενός συστήματος ασφαλείας είναι ο ανθρώπινος παράγοντας. Ο κοινωνικός μηχανικός θα προσπαθήσει πρώτα να εκμεταλλευτεί την αδυναμία αυτή, πριν να σπαταλήσει χρόνο και προσπάθεια σε άλλες μεθόδους.

2.4 ΤΑ ΜΕΣΑ ΤΕΛΕΣΗΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Υπάρχουν εργαλεία τα οποία οι ηλεκτρονικοί εγκληματίες χρησιμοποιούν για να εκμεταλλευτούν τις αδυναμίες των συστημάτων. Τα εργαλεία αυτά έχουν δημιουργηθεί για να χρησιμοποιούνται από τους διαχειριστές δικτύων, για να ελέγχουν την ευπάθεια των συστημάτων. Οι hackers, όμως, τα χρησιμοποιούν για τον αντίθετο ακριβώς σκοπό, δηλαδή, για να εκμεταλλευτούν τις αδυναμίες των συστημάτων.

Πολλά από τα εργαλεία διανέμονται ελεύθερα στο Διαδίκτυο με αποτέλεσμα ακόμη και αρχάριοι χρήστες να μπορούν να τα εντοπίσουν και να τα χρησιμοποιήσουν εναντίον κάποιου συστήματος.

- Port Scanners

  Έχουν τη δυνατότητα να ελέγχουν πολλές IP διευθύνσεις και να δίνουν στο χρήστη πληροφορίες για τις διαθέσιμες θύρες (ports).
- Vulnerability Scanners

  Ελέγχουν το λογισμικό εφαρμογών ενός Η/Υ, προσπαθώντας να εντοπίσουν κάποια ευπάθεια.
- Rootkits

  Ο όρος χρησιμοποιείται για να περιγράψει ένα σύνολο από σενάρια (scripts) και εκτελέσιμα πακέτα, τα οποία επιτρέπουν στους εισβολείς, να κρύψουν οποιαδήποτε πληροφορία προδίδει ότι απέκτησαν πρόσβαση σε

ένα σύστημα ή δίκτυο. Τα εργαλεία αυτά, επιτελούν μια σειρά από διαδικασίες στο σύστημα στο οποίο επιτέθηκαν, όπως:

● Τροποποίηση των εργαλείων του συστήματος.

● Δημιουργία κρυφών σημείων πρόσβασης στο σύστημα (backdoors).

● Χρησιμοποίηση του συστήματος ως το αρχικό σημείο εξαπόλυσης επιθέσεων σε άλλα συστήματα.

- Sniffers

  Χρησιμοποιούνται για να αναγνωρίσουν τις πληροφορίες που αφορούν την κίνηση σε ένα τοπικό δίκτυο υπολογιστή. Φιλτράρουν τα δεδομένα που συλλέγουν και έτσι έχουν τη δυνατότητα να ανακτούν ευαίσθητες πληροφορίες όπως ονόματα χρηστών, κωδικούς πρόσβασης και δεδομένα συναλλαγών, που διακινούνται σε ένα δίκτυο μέσω του πρωτοκόλλου επικοινωνίας TCP/IP.

- Anonymous re-mailers

  Ένα ανώνυμος re-mailer είναι ένα πρόγραμμα το οποίο εκτελείται σε κάθε υπολογιστή στο Διαδίκτυο και επιτρέπει στον οποιοδήποτε να στείλει μηνύματα σε ομάδες συζητήσεων ή σε μεμονωμένα άτομα, χωρίς να γίνει γνωστή η ταυτότητα του.

  Όταν ένα μήνυμα στέλνεται σε μια τέτοια διεύθυνση, το πρόγραμμα διαγράφει το όνομα και τη διεύθυνση του αποστολέα και το προωθεί στον προορισμό του.

- Password Crackers

  Είναι εργαλεία λογισμικού, τα οποία χρησιμοποιούνται για να ανακτήσουν τους κωδικούς πρόσβασης ενός συστήματος. Για το σκοπό αυτό οι crackers κάνουν χρήση ενός αρχείου με πιθανούς κωδικούς.

- Spoofers

  Είναι προγράμματα που αλλάζουν τη διεύθυνση IP του Η/Υ του επιτιθέμενου ώστε να μην ανιχνεύονται οι επιθέσεις του, ή με σκοπό την ενοχοποίηση κάποιου άλλου χρήστη. Συχνά ανυποψίαστοι χρήστες του Διαδικτύου κατηγορούνται για ηλεκτρονικά εγκλήματα επειδή κάποιος κακόβουλος χρησιμοποίησε την IP διεύθυνση τους.

Όπως είδαμε σ’ αυτό το κεφάλαιο υπάρχουν διάφορες μορφές απειλών, εσωτερικές, εξωτερικές και κοινωνική μηχανή αλλά υπάρχουν και πολλά κίνητρα που οδηγούν σ’ αυτά τα εγκλήματα όπως η εκδίκηση από πρώην υπαλλήλους εταιρειών ή η επιθυμία των hackers να επιβεβαιώσουν την ικανότητα τους να εισβάλουν σ’ ένα σύστημα κ.α. Φυσικά πολλά από αυτά συμβαίνουν όπως είδαμε λόγων της ύπαρξης ευπαθειών στα συστήματα αλλά και λόγων της κακής χρήσης τους. Τέλος αναφερθήκαμε και στα εργαλεία τέλεσης αυτών των εγκλημάτων που είτε υπάρχουν ελεύθερα στο διαδίκτυο είτε κατασκευάζονται από τους ίδιους τους εγκληματίες χρησιμοποιούνται ενάντια του συστήματος. Αφού ασχοληθήκαμε μ’ αυτά ως εδώ το επόμενο βήμα είναι να ασχοληθούμε με τις μορφές του ηλεκτρονικού εγκλήματος και αυτό είναι το κύριο θέμα του επόμενου κεφαλαίου.

ΚΕΦΑΛΑΙΟ 3
ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Μέχρι αυτό το σημείο έχει γίνει προσπάθεια ορισμού του Ηλεκτρονικού Εγκλήματος. Έχει γίνει λόγος για τους ηλεκτρονικούς εγκληματίες και για τις απειλές του ηλεκτρονικού εγκλήματος. Στο κεφάλαιο αυτό θα γίνει διεξοδική αναφορά στις μορφές του Ηλεκτρονικού Εγκλήματος και γι' αυτό είναι απαραίτητος ο διαχωρισμός τους σε δυο βασικές κατηγορίες. Στην πρώτη κατηγορία έχουμε τα εγκλήματα που εμφανιστήκαν μαζί με τους ηλεκτρονικούς υπολογιστές και το διαδίκτυο και χαρακτηρίζονται ως «γνήσια» και στη δεύτερη κατηγορία εντάσσονται τα εγκλήματα που παρόλο προϋπήρχαν των ηλεκτρονικών υπολογιστών και του διαδικτύου, αυτά τα δυο συντελούν σε μεγάλο βαθμό στην εκτέλεση τους.

3.1 ΓΝΗΣΙΑ ΗΛΕΚΤΡΟΝΙΚΑ ΕΓΚΛΗΜΑΤΑ

3.1.1 ΚΑΚΟΒΟΥΛΕΣ ΕΙΣΒΟΛΕΣ ΣΕ ΔΙΚΤΥΑ – HACKING

Η εισβολή σ' ένα δίκτυο υπολογιστών, το λεγόμενο hacking, αποτελεί βασικό στοιχείο πολλών διαδικτυακών εγκλημάτων και είναι πλέον το έγκλημα του 21ου αιώνα. Οι hackers επιδιώκουν να αποκτήσουν πρόσβαση σε ξένο υπολογιστή ή σύστημα υπολογιστών για να αποκτήσουν γνώσεις για την ασφάλεια του, να εντοπίσουν ευπάθειες και έτσι μπορούν να διαπράξουν μια επίθεση ή να προσφέρουν πληροφορίες σε κάποιο ο οποίος θέλει να διαπράξει μια επίθεση. Ανάλογα με τα δικαιώματα που αποκτά ο εισβολέας στο σύστημα μπορούμε να διακρίνουμε δύο βασικές κατηγορίες: α) την πλήρη διείσδυση με δικαιώματα διαχειριστή συστήματος και β) τη διείσδυση με δικαιώματα απλού χρήστη συστήματος.

Βασικές Τεχνικές των hackers

- Η εκμετάλλευση των cookies: Τα cookies είναι πολύ μικρά αρχεία κειμένου, τα οποία τοποθετούνται στον Η/Υ από διάφορες τοποθεσίες του διαδικτύου τις οποίες επισκέπτεται ένας χρήστης. Ο hacker εκμεταλλευόμενος κάποιες ευπάθειες του φυλλομετρητή ή του Λειτουργικού Συστήματος μπορεί να

ανακτήσει πληροφορίες που εμπεριέχονται σ' ένα αρχείο cookies όπως είναι το όνομα χρήστη και ο κωδικός πρόσβασης.

- Ανίχνευση δικτυακών υπηρεσιών συστημάτων: Σκοπός είναι ο εντοπισμός πληροφοριών για το σύστημα στόχο. Για να επιτευχθεί αυτό χρησιμοποιείται η τεχνική της σάρωσης θυρών (port scanning). Πρόκειται για μια διαδικασία αποστολής ερωτημάτων σε διακομιστές ώστε να ληφθούν πληροφορίες οι οποίες δίνουν τη δυνατότητα στον εισβολέα να παραβιάσει την ασφάλεια του συστήματος, εκμεταλλευόμενος γνωστές αδυναμίες του λειτουργικού συστήματος ή άλλων υπηρεσιών. Η ανίχνευση μπορεί επίσης να αποσκοπεί στην εύρεση και αξιοποίηση λογαριασμών χρηστών που δεν προστατεύονται με κωδικό πρόσβασης.
- Ανίχνευση δικτυακών πακέτων: Η ανίχνευση δικτυακών πακέτων πραγματοποιείται με τις εφαρμογές λογισμικού packet sniffers που έχουν τη δυνατότητα να εντοπίζουν όλα τα πακέτα τα οποία κυκλοφορούν στο Διαδίκτυο. Αν τα πακέτα δεν είναι κρυπτογραφημένα είναι δυνατή η απόσπαση πληροφοριών, όπως κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών κ.α. Επίσης λαμβάνονται πληροφορίες που αφορούν την τοπολογία ενός δικτύου, τις υπηρεσίες που προσφέρονται και τον αριθμό των υπολογιστών που είναι στο δίκτυο.
- Πλαστές διευθύνσεις IP: Οι εισβολείς παρεμβαίνουν στις επικεφαλίδες των πακέτων που διακινούνται σε ένα δίκτυο και τις τροποποιούν ώστε το μήνυμα να φαίνεται ότι προήλθε από αξιόπιστη πηγή. Έτσι αποκτούν πρόσβαση σε δικτυακές υπηρεσίες που προορίζονται για έμπιστους χρήστες του δικτύου.
- Επιθέσεις σε επίπεδο εφαρμογών: Στις επιθέσεις αυτές γίνεται εκμετάλλευση γνωστών αδυναμιών των δικτυακών εφαρμογών και των γλωσσών προγραμματισμού που χρησιμοποιούνται για τη δημιουργία δικτυακών τόπων με δυναμικό περιεχόμενο.

3.1.2 ΕΠΙΘΕΣΕΙΣ ΑΡΝΗΣΗΣ ΕΞΥΠΗΡΕΤΗΣΗΣ

Οι επιθέσεις άρνησης εξυπηρέτησης αποσκοπεί στην εξάντληση των πόρων ενός υπολογιστή, ώστε να μην μπορεί να εξυπηρετήσει άλλους υπολογιστές. Αυτό ισοδυναμεί με τη διακοπή λειτουργίας μιας κρίσιμης υπηρεσίας ή συνόλου

υπηρεσιών που προσφέρονται από έναν ή περισσότερους διακομιστές, με απρόβλεπτες συνέπειες για την εταιρεία ή τον οργανισμό.
Οι επιθέσεις αυτές στοχεύουν:

- Στην παρεμπόδιση της μετάδοσης των δεδομένων στο δίκτυο.
- Στην παρεμπόδιση σύνδεσης μεταξύ δύο σημείων, κάτι που ενδεχομένως σημαίνει αδυναμία πρόσβασης σε συγκεκριμένες υπηρεσίες.
- Στην αλλοίωση της ποιότητας μιας υπηρεσίας, που προσφέρεται σ' ένα χρήστη.

Πολλές τεχνικές χρησιμοποιούνται για επιθέσεις άρνησης εξυπηρέτησης, όπως SYN Flood, Attacks, UDP Flood Attacks, ICMP Flood Attacks, Teardrop Attacks, ping of death, port flooding, OOB Attacks, Fragmentation, Smurf Attacks, Fraggle Attacks και Papasmurf Attacks.

Οι επιθέσεις άρνησης εξυπηρέτησης ολοκληρώνονται σε τέσσερα βήματα:
Α) Ο εισβολέας εγκαθιστά προγράμματα απομακρυσμένης διαχείρισης σε αριθμό Η/Υ που διαθέτουν ευρυζωνικές συνδέσεις στο Διαδίκτυο. Με αυτά τα προγράμματα πραγματοποιούνται απόπειρες σύνδεσης προς το θύμα.
Β) Όταν ο εισβολέας είναι έτοιμος να αρχίσει την επίθεση του, δίνει εντολή στο πρόγραμμα, να ξεκινήσει να στέλνει «ping» σε μια συγκεκριμένη διεύθυνση. Ο υπολογιστής που περιέχει το απομακρυσμένο πρόγραμμα διαχείρισης, λειτουργεί ως «zombie».
Γ) Ο υπολογιστής του θύματος (έστω Α) απαντάει σε κάθε ping, αλλά, επειδή ο υπολογιστής zombie (έστω Β) έχει δώσει λάθος διεύθυνση για τα pings, ο Α δεν μπορεί να επιτύχει σύνδεση με το Β. Ωστόσο, ο Α περιμένει απάντηση στα ping που έχει στείλει, ενώ, ο Β και όσοι άλλοι υπολογιστές λειτουργούν ως zombies, συνεχίζουν να στέλνουν νέα ping, με αποτέλεσμα, οι πόροι του Α να εξαντλούνται από την πληθώρα των αιτημάτων και να μην μπορούν να προσφέρουν άλλες υπηρεσίες.
Δ) Συνήθως, μετά από κάποιο χρονικό διάστημα, ο επιτιθέμενος δίνει εντολή στα προγράμματα απομακρυσμένου ελέγχου, να σταματήσουν να στέλνουν ping, προκειμένου, να μην είναι δυνατό να εντοπιστεί από πού προέρχεται η επίθεση.

Υπόθεση Mafiaboy

Το έτος 2000 πραγματοποιήθηκαν πολλές επιθέσεις άρνησης εξυπηρέτησης σε δικτυακούς τόπους σημαντικών εταιρειών, που δραστηριοποιούνται στο χώρο του Διαδικτύου. Ανάμεσα στα θύματα ήταν Yahoo, Amazon.com, buy.com, cnn.com, eBay.com κ.α. Για τις επιθέσεις αυτές χρησιμοποιήθηκαν οι υπολογιστές των Πανεπιστημίων του Stanford και της Καλιφόρνιας, οι οποίοι έστελναν συνεχώς «ping». Κατά τη διερεύνηση της υπόθεσης, αποκαλύφθηκε ότι ο δράστης της επίθεσης, ήταν ένας 15χρονος μαθητής από το Montreal του Καναδά, ο οποίος εμφανιζόταν στο Διαδίκτυο με το ψευδώνυμο Mafiaboy.

Ο Mafiaboy απασχόλησε τις διωκτικές αρχές έως τα τέλη του 2001. Εντυπωσιακές ήταν οι ποινές που του επιβλήθηκαν, καθότι ήταν ανήλικος αντιμετωπιζόταν επιεικώς από το ισχύον νομικό πλαίσιο. Για παράδειγμα, μετά την αποκάλυψη της δράσης του, η αστυνομία του Καναδά, τον άφησε ελεύθερο με τους ακόλουθους περιοριστικούς όρους:

● Μπορούσε να χρησιμοποιεί Η/Υ μόνο υπό την επίβλεψη του καθηγητή του.

● Του απαγορεύτηκε να συνδέετε στο Διαδίκτυο.

● Του απαγορεύεται να εισέρχεται σε εταιρείες και καταστήματα που δραστηριοποιούνται στο χώρο της πληροφορικής.

● Του απαγορεύτηκε η επικοινωνία με τρεις από τους στενούς του φίλους.

Πηγή: http://www.rbs2.com/ccrime.htm#anchor111666

3.1.3 ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

Η διασπορά κακόβουλου κώδικα (malicious code) είναι από τα πιο διαδεδομένα εγκλήματα στο χώρο του Διαδικτύου. Ο κακόβουλος κώδικας είναι κώδικας Η/Υ, που δημιουργείται με σκοπό να προκαλέσει ζημιά σε Η/Υ ή να εισχωρήσει σε σ' ένα Η/Υ, για την υποκλοπή, αλλοίωση ή διαγραφή δεδομένων και προγραμμάτων.

Βασικές κατηγορίες κακόβουλου κώδικα (πηγή: Sinrod 2000):

- Ιοί (viruses):

Είναι ένα πρόγραμμα το οποίο επισυνάπτει τον εαυτό του σε αρχεία τα οποία υπάρχουν στον υπολογιστή, μια διαδικασία που είναι γνωστή ως μόλυνση.

Βασικά Χαρακτηριστικά ενός ιού:

I) Αποτελείται από μια σειρά από εντολές που εκτελούν συγκεκριμένες κακόβουλες ενέργειες σε ένα υπολογιστή.

II) Προσπαθεί να εγκατασταθεί σε κατάλληλη θέση στο σύστημα αρχείων του Η/Υ – θύματος που θα του εξασφαλίζει ότι οι οδηγίες του θα

εκτελούνται κατά προτεραιότητα ώστε ο χρήστης να μην μπορεί να αντιληφθεί την εκτέλεση του.

III) Η εκτέλεση του έχει δύο βασικές λειτουργίες την αναπαραγωγή του και την πρόκληση ζημιάς.

IV) Προσπαθεί να μολύνει προγράμματα, τα οποία πιθανόν να σταλούν ή να μεταφερθούν σε άλλο υπολογιστικό σύστημα.

Ο ιός Vienna

Υπήρξε ένας παρασιτικός ιός, οποίος όμως δεν παρέμενε στην κύρια μνήμη του συστήματος. Μόλυνε αρχεία με κατάληξη com. Όταν εκτελούνταν ένα πρόγραμμα μολυσμένο με το Vienna, ο ιός επέλεγε τυχαία και μόλυνε μόνο ένα πρόγραμμα .com στον τρέχοντα κατάλογο (που δεν είχε ήδη μολυνθεί). Ο ιός αυτός ήταν πολύ δύσκολο να ανιχνευθεί, αφού δεν μόλυνε όλα τα προγράμματα και δεν παρέμενε στη μνήμη του συστήματος.

Πηγή: McAfee Inc.AVERT library

Κυριότερες μορφές ιών:

- File – infectors ή parasitic viruses: Μολύνουν ένα εκτελέσιμο πρόγραμμα στο οποίο προσθέτουν τον κακόβουλο κώδικα. Επίσης γίνεται κάποια τροποποίηση του αρχείου - ξενιστή ώστε να είναι σίγουρο ότι θα εκτελεστεί πρώτο. Μολύνει αρχεία με επεκτάσεις .com, .exe, .sys, .olv.
- Boot Sector Virus: Μολύνει εκτελέσιμο κώδικα συστήματος, που εντοπίζει σε συσκευές βοηθητικής μνήμης, στον τομέα εκκίνησης ή στο MBR του δίσκου. Μολύνει κάθε δίσκο ή δισκέτα που θα χρησιμοποιηθεί τοπικά στο Η/Υ.
- Multi – partite viruses: Ενεργούν συνδυάζοντας χαρακτηριστικά των δύο παραπάνω κατηγοριών με αποτέλεσμα ένας Η/Υ να είναι δυνατόν να μολυνθεί είτε όταν εκκινήσει από μολυσμένο δίσκο είτε όταν εκτελεστεί ένα μολυσμένο πρόγραμμα.
- Companion Viruses: Εκμεταλλεύεται μια ευπάθεια του λειτουργικού συστήματος DOS. Αν υπάρχουν δύο προγράμματα με το ίδιο όνομα σε ένα κατάλογο, το DOS εκτελεί πρώτα το αρχείο .com και μετά το .exe. Ο ιός δεν μολύνει το αρχείο .exe αλλά δημιουργεί ένα αντίγραφο του με την κατάληξη .com. Όταν ο χρήστης επιχειρήσει να εκτελέσει το αρχείο .exe εκτελείται

πρώτα το .com που έχει αποθηκευτεί στον ίδιο κατάλογο που περιέχει το κακόβουλο κώδικα.

- Ιοί Link και Flash Bios: Λειτουργούν τροποποιώντας το αρχείο FAT με αποτέλεσμα να αλλάζει ο σύνδεσμος που «δείχνει» προς ένα πρόγραμμα του Η/Υ ώστε να «δείχνει» στο σημείο που βρίσκεται ο ιός και να εκτελεστεί αυτός.
- Macro viruses: Βρίσκονται κρυμμένοι σε κάποιο αρχείο προγράμματος αυτοματισμού γραφείου (π.χ. Microsoft Word, Excel κ.λπ.), το οποίο όταν το εκτελέσει ο χρήστης να ενεργοποιεί μια μακροεντολή, η οποία μπορεί να εκτελέσει μια σειρά από ανεπιθύμητες ενέργειες.

Mellisa Macro Virus

Αποτελεί την κλασικότερη μορφή μακρο-ιού. Εμφανίστηκε τον Μάρτιο του 1999. Έφτανε στον παραλήπτη μέσο e-mail, σε ένα συνημμένο αρχείο τύπου Word, το οποίο όταν ανοιγόταν περιείχε μια λίστα από κωδικούς για δικτυακούς τόπους, που προσφέρουν πορνογραφικό υλικό. Παράλληλα, χωρίς να το γνωρίζει ο χρήστης, ενεργοποιούνταν μια μακροεντολή, η οποία διάβαζε τις 50 πρώτες διευθύνσεις του βιβλίου outlook και έστελνε τον εαυτό της, σ' αυτές. Ο ιός διαδόθηκε τόσο γρήγορα, που μέσα σε 48 ώρες ανάγκασε τη Microsoft και την Intel, να κλείσουν τους διακομιστές τους. Μάλιστα, μια εταιρεία 500 υπαλλήλων ανέφερε μέσα σε 45 λεπτά ότι έλαβε πάνω από 32000 e-mail (πηγή: Sinrod, 2000).

- Σκουλήκια (worms):

Τα σκουλήκια είναι παρόμοια με τους ιούς με βασική διαφορά ότι πολλαπλασιάζοντας χωρίς να απαιτείται κάποια ενέργεια από το χρήστη. Στην αρχική του μορφή, ένα σκουλήκι τροποποιεί ή διαγράφει αρχεία ενός υπολογιστή. Στη συνέχεια δημιουργεί πολλαπλά αντίγραφα του εαυτού του και τα στέλνει στους Η/Υ των υποψήφιων θυμάτων.

ILOVEYOU WORM

Είναι το πιο διάσημο σκουλήκι όλων των εποχών. Το σκουλήκι έφτανε στον Η/Υ του θύματος με e-mail με θέμα ILOVEYOU και ένα συνημμένο αρχείο LOVE-LETTER-FOR-YOU.TXT.VPS. Το e-mail από μόνο του ήταν αθώο, όταν όμως ο χρήστης άνοιγε το συνημμένο αρχείο, εκτελούνταν ένα πρόγραμμα Visual Basic το οποίο: α) διέγραφε αρχεία από τον υπολογιστή, β) όριζε ως αρχική σελίδα στον Internet Explorer, μια σελίδα σ' ένα διακομιστή στις Φιλιππίνες και αυτόματα γινόταν λήψη ενός δούρειου ίππου, ο οποίος υπέκλεπτε τους κωδικούς πρόσβασης του χρήστη και τους απόστελλε στους δημιουργούς του, γ) πολλαπλασιαζόταν και έστελνε τον εαυτό του σ' όλες τις διευθύνσεις που υπήρχαν στο βιβλίο διευθύνσεων.

Επηρέασε περισσότερους από τους μισούς Η/Υ εταιρειών στην Αμερική και πάνω από 100000 διακομιστές στην Ευρώπη. Εκτιμάτε, ότι προκάλεσε τη μεγαλύτερη οικονομική καταστροφή στην

ιστορία των ηλεκτρονικών υπολογιστών, καθώς οι συνολικές ζημιές ξεπέρασαν τα 9.000.000.000$ (πηγή: Standler, 2002 , http://www.pchell.com/virus/loveletter.shtml).

- Δούρειοι Ίπποι: Είναι φαινομενικά «αθώα» προγράμματα, τα οποία, έχουν μια ή περισσότερες κρυμμένες λειτουργίες οι οποίες δεν είναι εύκολο να εντοπιστούν από τους χρήστες. Τα προγράμματα αυτά φορτώνονται στο σκληρό δίσκο του υπολογιστή και εκτελούνται κανονικά μαζί με τα υπόλοιπα προγράμματα. Επιτυγχάνετε η απόκτηση απομακρυσμένου ελέγχου του υπολογιστή του θύματος και η απόκτηση κωδικών πρόσβασης, αριθμών πιστωτικών καρτών ή η δημιουργία μιας επίθεσης άρνησης εξυπηρέτησης.
- Ad – ware, Spyware και diallers: Τα Ad – ware χρησιμοποιούνται για την διαφημιστική προώθηση συγκεκριμένων δικτυακών τόπων και προϊόντων που προσφέρονται μέσω του Διαδικτύου. Ενδέχεται να αποτελούν νόμιμο λογισμικό εφόσον η λειτουργία τους ορίζεται ρητά στους όρους χρήσης που αποδέχεται ο χρήστης κατά την εγκατάσταση του. Τα Spyware είναι κατεξοχήν κακόβουλο λογισμικό που υποκλέπτει πληροφορίες που αφορούν το χρήστη. Τα Ad – Ware και Spyware συνεργάζονται για τη δημιουργία προφίλ χρηστών για την αποστολή διαφημίσεων αλλά μπορούν να προκαλέσουν και ανεπιθύμητα αποτελέσματα όπως είναι η καταστροφή αρχείων, αποσυντονισμοί συστήματος και η επιβράδυνση της περιήγησης στο Διαδίκτυο και την γενικά τη λειτουργία του υπολογιστή. Οι diallers είναι μικρά προγράμματα τα οποία έχουν τη δυνατότητα να αποσυνδέσουν την υπάρχουσα κλήση της τηλεφωνικής γραμμής με τον τοπικό πάροχο υπηρεσιών Internet και καλούν αυτόματα έναν υψηλής χρέωσης αριθμό για πρόσβαση σε συγκεκριμένες υπηρεσίες χωρίς την συνειδητή συγκατάθεση του χρήστη. Προέρχονται από επισκέψεις σε συγκεκριμένες ιστοσελίδες που περιέχουν πειρατικό λογισμικό, πορνογραφικό ή άλλο αμφιλεγόμενο περιεχόμενο.
- Λογικές και ωρολογιακές βόμβες: Είναι ένα πρόγραμμα το οποίο ενεργοποιείται όταν συμβεί ένα συγκεκριμένο γεγονός. Το ενεργοποιημένο πρόγραμμα μπορεί να σταματήσει τη λειτουργία του υπολογιστή, να απελευθερώσει έναν ιό, να διαγράψει αρχεία ή να προβεί σε άλλες ζημιογόνες ενέργειες.

Οι ιοί Jerusalem και Michelangelo

Ο ιός Jerusalem αποτελεί κλασική περίπτωση λογικής βόμβας. Εμφανίστηκε το 1987 και είχε την δυνατότητα να σβήνει όλα τα προγράμματα που εκτελούσε ο χρήστης εφόσον η ημερομηνία του συστήματος ήταν Παρασκευή και 13.

Ο ιός Michelangelo ήταν προγραμματισμένος να απενεργοποιεί τους μολυσμένους Η/Υ στις 6 Μαρτίου 1992.

3.1.4 ΤΕΧΝΙΚΕΣ ΑΠΟΚΡΥΨΗΣ ΙΩΝ

Οι περισσότεροι ιοί λίγο χρόνο μετά τη δημιουργία τους εντοπίζονται από τις εταιρίες αντιβιοτικού λογισμικού (antivirus software), οι οποίες ενημερώνουν τις βάσεις τους με το κατάλληλο λογισμικό, για την αντιμετώπιση τους.

Οι αόρατοι ιοί, έχουν τη δυνατότητα, να παραμένουν ενεργοί στη μνήμη, να μολύνουν προγράμματα που εκτελούνται, μετά από μια μόνιμη εντολή του χρήστη και παράλληλα παρακάμπτουν το πρόγραμμα antivirus, όταν εκτελεί έλεγχο ακεραιότητας.

Οι πολυμορφικοί ιοί δημιουργούν αντίγραφα του εαυτού τους, τα οποία διαφέρουν μεταξύ τους, ωστόσο έχουν, τα ίδια καταστροφικά αποτελέσματα. Τα καινούργια αντίγραφα εμπεριέχουν μια μορφή «θορύβου» (π.χ. άσκοπες εντολές ή τροποποίηση της σειράς τους) με αποτέλεσμα τα προγράμματα antivirus να μην μπορούν να τους εντοπίσουν.

3.1.5 ΑΝΕΠΙΘΥΜΗΤΗ ΑΛΛΗΛΟΓΡΑΦΙΑ (SPAMMING)

Είναι η χρήση οποιουδήποτε ηλεκτρονικού μέσου για την αποστολή ανεπιθύμητων μηνυμάτων σε πολύ μεγάλες ποσότητες. Αν και ο όρος αναφέρεται, περισσότερο, στην αποστολή μεγάλων ποσοτήτων μηνυμάτων, με διαφημιστικό περιεχόμενο, χρησιμοποιείται επίσης και για την αποστολή οποιουδήποτε μηνύματος το οποίο μπορεί να χαρακτηριστεί ενοχλητικό από αυτό που το λαμβάνει.

Η συλλογή των ηλεκτρονικών διευθύνσεων από τους spammers γίνεται από τους καταλόγους εταιριών που διατηρούν ηλεκτρονικά καταστήματα ή χρησιμοποιούν

λογισμικό τύπου harvester, το οποίο σαρώνει όλο το internet και συλλέγει χιλιάδες διευθύνσεις από καταλόγους, δωμάτια συζητήσεων κ.λπ. Μπορούν να υποκλέψουν διευθύνσεις από καταλόγους μεγάλων εταιριών παροχής internet ή μπορεί να χρησιμοποιηθεί ειδικό λογισμικό το οποίο παράγει τεράστιες λίστες τυχαίων διευθύνσεων.

3.1.6 ΕΠΙΘΕΣΕΙΣ ΣΕ ΔΙΚΤΥΑΚΟΥΣ ΤΟΠΟΥΣ

Οι επιθέσεις αυτές πραγματοποιούνται από τους βάνδαλους (vandals). Σε μια επίθεση σ' ένα δικτυακό τόπο το αποτέλεσμα είναι αναστρέψιμο. Ο βάνδαλος θα διαγράψει ορισμένες σελίδες ή γραφικά και θα ανεβάσει τις δικές του σελίδες, το περιεχόμενο των οποίων μπορεί να είναι χιουμοριστικό έως προπαγανδιστικό. Όταν εντοπιστεί η επίθεση οι προβληματικές σελίδες διορθώνονται από εφεδρικά αρχεία. Το πρόβλημα είναι ο χρόνος που θα απαιτηθεί για την επιδιόρθωση γιατί ίσως χρειαστεί ο δικτυακός τόπος να μείνει εκτός δικτύου για μεγάλο χρονικό διάστημα. Το πλήγμα της εταιρίας μετά από μια τέτοια επίθεση στο δικτυακό της τόπο που αποτελεί την εικόνα της επιχείρησης προς τους πελάτες, τους εξωτερικούς συνεργάτες και τους υποψήφιους πελάτες είναι τεράστιο.

3.1.7 ΕΠΙΘΕΣΕΙΣ ΟΝΟΜΑΤΩΝ ΧΩΡΟΥ

Η πειρατεία ονομάτων χώρου γνώρισε μεγάλη άνθηση κατά τα πρώτα χρόνια του διαδικτύου. Διάφοροι επιτήδειοι εκμεταλλευόμενοι το γεγονός, πως μεγάλες εταιρίες δεν είχαν κατοχυρώσει, ακόμη, ονόματα χώρων για τους δικτυακούς τους τόπους, προέβαιναν σε κατοχύρωση ονομάτων διάσημων εταιριών, με αποτέλεσμα να αποκτούν τα δικαιώματα της νέας διεύθυνσης. Στη συνέχεια, μπορούσαν είτε να παραχωρήσουν την διεύθυνση στην εταιρία που κατείχε το συγκεκριμένο όνομα, έναντι, βέβαια σημαντικού ποσού, είτε να προβούν στην ανάρτηση, στη συγκεκριμένη διεύθυνση περιεχομένου προσβλητικού.

3.1.8 PHISING

Με το Phising επιχειρείται η απόσπαση προσωπικών πληροφοριών του θύματος, όπως ο αριθμός της πιστωτικής του κάρτας, κωδικοί πρόσβασης κ.λπ. προκειμένου να χρησιμοποιηθούν σε άλλες παράνομες δραστηριότητες.

Η ονομασία Phishing αναφέρεται χρησιμοποιούμενη για πρώτη φορά το 1996 από hackers που έκλεβαν ή παράνομα ιδιοποιούνταν τους λογαριασμούς νομίμων χρηστών της εταιρίας America Online (AOL) με παράνομη χρήση κωδικών πρόσβασης που ανήκαν σε ανυποψίαστους χρήστες—συνδρομητές της AOL. Η πρώτη αναφορά στο Διαδίκτυο για το Phishing έγινε σε newsgroup hackers γνωστό ως alt.2600 τον Ιανουάριο του 1996, και η πρώτη αναφορά των μέσων ενημέρωσης στο Phishing χρονολογείται τον Μάρτιο του 1997.

Τρόπος Δράσης: Τα υποψήφιο θύμα δέχεται ένα e-mail π.χ. από την υπηρεσία Ηλεκτρονικής Τραπεζικής (home banking) της τράπεζας που χρησιμοποιεί, που τον πληροφορεί ότι είναι σε εξέλιξη κάποιες εργασίες συντήρησης του συστήματος και τον προτρέπει να επισκεφτεί την υπηρεσία Ηλεκτρονικής Τραπεζικής επιλέγοντας τον σύνδεσμο, που έχει επισυναφθεί στο μήνυμα και να επιβεβαιώσει τους κωδικούς πρόσβασης της υπηρεσίας. Το ανυποψίαστο θύμα θα επιλέξει το σύνδεσμο, που θα τον οδηγήσει σε μια τοποθεσία – αντίγραφο της πραγματικής. Όταν πληκτρολογήσει τα προσωπικά του στοιχεία, αυτά θα υποκλαπούν από τον επιτιθέμενο.
Για να εξαπατηθεί ο χρήστης, προτιμώνται διευθύνσεις που μοιάζουν πάρα πολύ με τις πραγματικές π.χ. η διεύθυνση homebank.nbg.gr μπορεί να χρησιμοποιηθεί ως homebang.nbg.gr.

Απόπειρες Phising στις Ελληνικές Τράπεζες:

1. Win Bank – Τράπεζα Πειραιώς

Αγαπητε πελατη

Μπορειτε εχουν βραβευθει με κουπονι για 100 eur.

Δωροεπιταγη code: 11245325932

για να συλλεξουμε παρακαλω συνδεθειτε και να εισαγετε το κωδικο κουπονιου παραπανω.

Παρακαλω επιτρεψτε 3-5 μερες για μεταποιηση.

Copyright © winbank 2008

2. Citibank Ελλάδος

citibank

Κλεισιματος των λογαριασμων και περιοριζοντας την προσ
Ο λογαριασμος σας εχει Limited. Εμεις που αναθεωρηθηκε
καρτα για 2 λογαριασμους. Οπως μπορειτε να διαβασετε κ
Ειστε τωρα καλειται να παρασχει πληροφοριες σχετικα με
αποκαταστησει το λογαριασμο σας.

Καντε κλικ εδω για να επαναφερετε το λογαριασμο σας

Αυτο ειναι ενα μηνυμα που δημιουργουνται

citibank
Citibank.gr

3. EFG Eurobank Ergasias

4. Εθνική Τράπεζα της Ελλάδος

3.1.9 ΠΕΙΡΑΤΕΙΑ ΛΟΓΙΣΜΙΚΟΥ

Ο όρος πειρατεία λογισμικού, αναφέρεται στην αναπαραγωγή και/ή διάθεση προγραμμάτων ηλεκτρονικού υπολογιστή, τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων, χωρίς τη γραπτή συναίνεση του δημιουργού τους.

Αν και οι εταιρείες παραγωγής λογισμικού εφαρμόζουν στα προϊόντα τους διάφορα τεχνολογικά μέτρα, για να αποτρέψουν την αντιγραφή ή τη χρήση τους από πολλούς υπολογιστές, οι hackers (crackers) πάντα βρίσκουν τεχνικές για να παρακάμψουν τα μέτρα αυτά. Χρησιμοποιώντας την τεχνική «cracking» έχουν τη δυνατότητα να απενεργοποιούν τους κωδικούς, τα κλειδιά ή ότι άλλο χρησιμοποιείται για την προστασία των προγραμμάτων. Ακόμα και αν δεν έχουν εξειδικευμένες γνώσεις για να «σπάσουν» (crack) ένα πρόγραμμα, μπορούν να χρησιμοποιήσουν έτοιμο λογισμικό «crack», που διατίθεται ελεύθερα στο Διαδίκτυο και έχει τη δυνατότητα να απενεργοποιεί τα μέτρα προστασίας των εταιρειών παραγωγής λογισμικού.

Σύμφωνα με μια έρευνα της εταιρείας λογισμικού Business Software Alliance, τα ποσοστά πειρατείας λογισμικού παρουσιάζουν τάσεις σταθεροποίησης. Παράλληλα παρατηρείται μια αύξηση των οικονομικών απωλειών των εταιρειών λογισμικού, δυσανάλογη με τα ποσοστά πειρατείας.

Ακολουθεί ο πίνακας στατιστικών στοιχείων για την πειρατεία λογισμικού

ΠΙΝΑΚΑΣ 2

Στατιστικά Στοιχεία για την Πειρατεία Λογισμικού

Περιοχή	Ποσοστό Πειρατείας			Απώλειες από την Πειρατεία σε εκατ. Δολάρια		
	2005	2004	2003	2005	2004	2003
Μέση Ανατολή και Αφρική	57%	58%	56%	1,615	1,248	1,026
Βόρεια Αμερική	22%	22%	23%	7,686	7,549	7,243
Δυτική Ευρώπη	35%	34%	36%	11,825	11,856	9,604
Ασία	54%	53%	53%	8,050	7,897	7,555
Κεντρική και Ανατολική Ευρώπη	69%	71%	71%	3,095	2,615	2,111
Λατινική Αμερική	68%	66%	63%	2,026	1,546	1,263
Ευρωπαϊκή Ένωση	36%	35%	37%	12,048	12,151	9,786
Παγκόσμιο Ποσοστό	35%	35%	36%	34,297	32,711	28,803

Πηγή: http://www.bsa.org/globalstudy/upload/2005%20Piracy%20Study%20%20Official%20Version.pdf

3.2 ΕΓΚΛΗΜΑΤΑ ΠΟΥ ΤΕΛΟΥΝΤΑΙ ΜΕ ΤΗ ΧΡΗΣΗ Η/Υ

3.2.1 ΑΠΑΤΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Η εμφάνιση και ανάπτυξη του Διαδικτύου μεγιστοποίησε τις δυνατότητες για διάπραξη νέων μορφών απάτης. Η τάση αυτή, αυξήθηκε ακόμη περισσότερο, με την εξάπλωση του ηλεκτρονικού εμπορίου, που είχε ως επακόλουθο την ανάπτυξη οικονομικών συναλλαγών με τη χρήση του Διαδικτύου.

3.2.1.1 ΑΠΑΤΗ ΜΕ E-MAIL

Η χρήση του ηλεκτρονικού ταχυδρομείου αποτελεί τη συχνότερη μορφή επιθέσεων προς τους χρήστες του Διαδικτύου. Ήδη μιλήσαμε για το phising. Οι

επαγγελματίες του είδους, συνεχώς, βρίσκουν νέους τρόπους για να εξαπατήσουν ανυποψίαστους χρήστες, χρησιμοποιώντας μηνύματα ηλεκτρονικού ταχυδρομείου. Χαρακτηριστικές περιπτώσεις απάτης με e-mail αποτελούν:

1) Οι νιγηριανές επιστολές: Ο αποστολέας-εγκληματίας στέλνει e-mail λέγοντας ότι είναι υπήκοος Αφρικανικής χώρας και ζητάει από το θύμα τη μεταφορά χρηματικού ποσού από τη χώρα του στο εξωτερικό, προβάλλοντας διάφορες δικαιολογίες (πόλεμος, θάνατος γονέων, φυσικές καταστροφές κ.λπ.) και ζητά από το θύμα το άνοιγμα τραπεζικού λογαριασμού με συνδικαιούχο τον ίδιο, τη γνωστοποίηση των στοιχείων του και την κατάθεση χρηματικού ποσού για τα έξοδα κίνησης. Ως αντάλλαγμα προσφέρει μεγάλο μερίδιο του μεταφερόμενου ποσού όταν ολοκληρωθεί η συναλλαγή. Ο σκοπός είναι να αποσπάσει το χρηματικό ποσό που κατάθεσε το θύμα για τα έξοδα κίνησης και ύστερα να καταργήσει το λογαριασμό.
2) Το Ισπανικό Λόττο: Αφρικανοί υπήκοοι, κάτοικοι Ισπανίας, αποστέλλουν e-mail σε ανυποψίαστους χρήστες, ζητώντας τους προσωπικά στοιχεία και αριθμούς τραπεζικών λογαριασμών, ώστε να μεταβιβάσουν τα κέρδη από την υποτιθέμενη νίκη τους στο ισπανικό Λόττο. Στη συνέχεια εφόσον πείσουν το θύμα ζητούν να καταβάλουν χρήματα για διαδικαστικά έξοδα. Έτσι καταφέρνουν να αποσπάσουν χρηματικά ποσά.

3.2.1.2 ΑΠΑΤΗ ΜΕ ΠΙΣΤΩΤΙΚΕΣ ΚΑΡΤΕΣ

Με τη χρήση των σύγχρονων τεχνολογιών δεν απαιτείται, πλέον, ιδιαίτερη δεξιότητα για να αποκτήσει κάποιος τον αριθμό μιας πιστωτικής κάρτας και να πραγματοποιήσει αγορές μέσω του Διαδικτύου. Με την τεχνολογία «websniffer», παρακολουθείται η μετάδοση δεδομένων και ανακτώνται αυτόματα δεκαεξαψήφιοι αριθμοί πιστωτικών καρτών. Επιπλέον, είναι δυνατή η αγορά μέσω του Διαδικτύου, αριθμών πιστωτικών καρτών που έχουν υποκλαπεί. Τέλος, υπάρχουν εφαρμογές λογισμικού, που δημιουργούν αυτόματα αριθμούς πιστωτικών καρτών, χρησιμοποιώντας διάφορούς λογάριθμους.

3.2.2 ΚΛΟΠΗ ΤΑΥΤΟΤΗΤΑΣ

Στη ψηφιακή εποχή που διανύουμε τεράστιες ποσότητες δεδομένων είναι αποθηκεμένες σε ηλεκτρονικές βάσεις δεδομένων για διάφορους σκοπούς.

Το έγκλημα της κλοπής ταυτότητας, ολοκληρώνεται σε δύο στάδια (πηγή: Newman, 2004):
Στο πρώτο ο επιτιθέμενος προσπαθεί να αποκτήσει τα στοιχεία της ταυτότητας ενός ατόμου με διάφορους τρόπους, συμβατικούς και ψηφιακούς όπως: αφαιρώντας πορτοφόλια, υποκλέπτοντας την αλληλογραφία, αποσπώντας τα ενημερωτικά σημειώματα των πιστωτικών καρτών, εισβάλλοντας στις βάσεις δεδομένων εταιρειών και οργανισμών όπου φυλάσσονται προσωπικά δεδομένα, χρησιμοποιώντας ειδικό λογισμικό το οποίο έχει τη δυνατότητα να αποσπά προσωπικά δεδομένα και άλλες πληροφορίες παρακολουθώντας την κίνηση των πακέτων στο Διαδίκτυο.
Στο δεύτερο βήμα χρησιμοποιούνται τα κλεμμένα στοιχεία, ανοίγοντας λογαριασμούς πιστωτικών καρτών με τα στοιχεία του θύματος τους οποίους χρησιμοποιεί για την αγορά προϊόντων μέσω του Διαδικτύου, ανοίγοντας τραπεζικούς λογαριασμούς τους οποίους χρεώνει με ακάλυπτες επιταγές, δημιουργώντας πλαστές πιστωτικές κάρτες όπως άδειες οδήγησης, διαβατήρια, ταυτότητες, υποβάλλονται ψευδή φορολογικές δηλώσεις για να εισπράξει την επιστροφή φόρου.

3.2.3 ΞΕΠΛΥΜΑ ΧΡΗΜΑΤΟΣ

Επιχειρείται η εξαφάνιση χρήματος που έχει προέλθει από παράνομες δραστηριότητες. Ο εγκληματίας επιχειρεί τη μετατροπή των χρημάτων σε μια μορφή λιγότερο ύποπτη, στη συνέχεια το χρήμα διαχωρίζεται από την παράνομη πηγή του χρησιμοποιώντας πολλαπλές οικονομικές συναλλαγές για να το αποκρύψουν και τέλος το παράνομο χρήμα μετατρέπεται, ώστε, να έχει τη μορφή εισοδήματος, που προήλθε από νόμιμες επαγγελματικές δραστηριότητες.

3.2.4 ΔΙΑΚΙΝΗΣΗ ΠΟΡΝΟΓΡΑΦΙΚΟΥ ΥΛΙΚΟΥ

Τα αδικήματα, που συνδέονται με τη μορφή αυτή του υλικού, σχετίζονται με την δημιουργία του υλικού όσο και με τη μη νόμιμη διακίνηση του. Η παράνομη διακίνηση υλικού παιδικής πορνογραφίας έχει λάβει τεράστιες διαστάσεις, προκαλώντας ιδιαίτερη ανησυχία στις διωκτικές αρχές.

Το πορνογραφικό υλικό που διακινείται μέσω του Διαδικτύου, μπορεί να είναι σε μορφή φωτογραφιών, βίντεο ή και οποιοδήποτε άλλης μορφής πολυμέσων. Ο καθένας μπορεί εύκολα να το «κατεβάσει» στον υπολογιστή του, χωρίς να χρειαστεί να αποκαλύψει την ταυτότητα του. Τέτοιου είδους υλικό, βρίσκεται σε διάφορους δικτυακούς τόπους. Μάλιστα, σε συγκεκριμένους δικτυακούς τόπους, γίνεται ανταλλαγή υλικού, δηλαδή, αντί να πληρώσει κάποιος τίμημα για το υλικό που προμηθεύεται, προσφέρει νέο υλικό, ως αντάλλαγμα.

3.2.5 ΔΙΚΤΥΑΚΗ ΤΡΟΜΟΚΡΑΤΙΑ

Το FBI ορίζει την κυβερνοτρομοκρατία ως την «προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίων πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι άμαχων στόχων από υποεθνικές ομάδες και μυστικούς πράκτορες».

Η χρήση του Διαδικτύου αποτελεί βασικό εργαλείο των τρομοκρατών, γιατί τους προσφέρει μια σειρά από πλεονεκτήματα: είναι φθηνότερο από τις παραδοσιακές τρομοκρατικές μεθόδους, οι ενέργειες τους είναι δύσκολο να εντοπιστούν, μπορούν να αποκρύψουν την τοποθεσία τους, δεν υπάρχουν φυσικά εμπόδια ή σημεία ελέγχου τα οποία πρέπει να διέλθουν, μπορούν να εξαπολύσουν την επίθεση τους από οποιοδήποτε σημείο του κόσμου και μπορούν να επιτεθούν, ταυτόχρονα, σε πολλούς στόχους.

3.2.6 ΕΠΙΘΕΣΕΙΣ ΠΑΡΕΝΟΧΛΗΣΗΣ

Με τον όρο παρενόχληση περιγράφεται μια εγκληματική συμπεριφορά όπου ο επιτιθέμενος με τη χρήση ηλεκτρονικών μέσων επικοινωνίας όπως το διαδίκτυο και τα κινητά τηλέφωνα, εκφοβίζει, απειλεί, εκβιάζει και γενικότερα παρενοχλεί τα θύματα του, για διάφορους λόγους, όπως εκδίκηση, επίλυση προσωπικών διαφορών κ.λπ.

Η παρενόχληση, που διαπράττεται μέσω του Διαδικτύου, μπορούμε να την διακρίνουμε σε δύο κατηγορίες (πηγή: Maxwell, 2001):

- Την άμεση παρενόχληση, είναι όταν ο επιτιθέμενος στέλνει απευθείας στο θύμα μηνύματα με προσβλητικό ή απειλητικό περιεχόμενο, άσχετα με το γεγονός, εάν οι απειλές πραγματοποιηθούν.
- Την έμμεση παρενόχληση, είναι όταν το μήνυμα δεν στέλνεται αμέσως στο θύμα, αλλά, σε τυχαίους χρήστες του Διαδικτύου και περιλαμβάνει προσβλητικό ή απειλητικό για το θύμα περιεχόμενο.

3.3 ΑΛΛΕΣ ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Αν και ο όρος ηλεκτρονικό έγκλημα αρχικά παραπέμπει σε εγκλήματα που τελούνται με τη χρήση των Η/Υ και του Διαδικτύου, η ενσωμάτωση και άλλων προηγμένων λειτουργιών ηλεκτρονικής επεξεργασίας δεδομένων και σε άλλες συσκευές όπως τα κινητά τηλέφωνα, τα palmtops κ.α. έχουν δημιουργήσει και νέες δυνατότητες διάπραξης εγκλημάτων.

3.3.1 ΚΙΝΗΤΗ ΤΗΛΕΦΩΝΙΑ

Μέσα από τα κινητά τηλέφωνα άρχισαν να παρέχονται διαδικτυακές υπηρεσίες με τη χρήση νέων πρωτοκόλλων επικοινωνίας (π.χ. WAP) μετατρέποντας τα σε κινητούς ηλεκτρονικούς υπολογιστές. Μαζί με τις νέες δυνατότητες, όμως, τα κινητά τηλέφωνα κληρονόμησαν και τις αδυναμίες των υπολογιστών. Έτσι ένα κινητό τηλέφωνο μπορεί να μολυνθεί από ιούς, σκουλήκια (worms), diallers και άλλα κακόβουλα προγράμματα.

Σημαντικά προβλήματα ασφαλείας έχουν τα κινητά τηλέφωνα που χρησιμοποιούν το Bluetooth Interface. Ο τηλεφωνικός κατάλογος του κινητού, όπως και η εσωτερική μνήμη (κλήσεις που έγιναν από/προς το κινητό, φωτογραφίες κ.λπ.) μπορούν να ανακτηθούν από μακριά εφόσον το κινητό έχει το Bluetooth σε λειτουργία εμφάνισης της συσκευής. Επίσης το κινητό μπορεί να ελεγχθεί από απόσταση και να πραγματοποιήσει κλήσεις με στόχο την υπερχρέωση ή την υποκλοπή των ομιλιών, να ενεργοποιήσει εκτροπές κ.α. Τέλος, το Bluetooth μπορεί να χρησιμοποιηθεί, εφόσον στηθούν κατάλληλες υποδομές κεραιών, για τον εντοπισμό ατόμων που φέρουν τη συσκευή του κινητού μαζί τους.

3.3.2 ΤΗΛΕΦΩΝΙΚΑ ΔΙΚΤΥΑ

Οι νέες τεχνολογίες, που αρχίζουν ήδη να υιοθετούνται στο τομέα των τηλεπικοινωνιών και η επέκταση της χρήσης του πρωτοκόλλου IP (Internet Protocol) που αναμένεται να κυριαρχήσει τα επόμενα χρόνια στις τηλεπικοινωνίες, δημιουργούν νέες δυνατότητες διάπραξης εγκλημάτων. Μέσω του πρωτοκόλλου IP μεταφέρεται φωνή (VoIP), video-τηλεόραση (TVoIP), εικόνες, κείμενα και μουσική.

3.3.3 ΠΑΙΧΝΙΔΟΜΗΧΑΝΕΣ

Οι σύγχρονες παιχνιδομηχανές με την ενσωμάτωση σ’ αυτές της τεχνολογίας WiFi (ασύρματη πρόσβαση) και εξελιγμένων δυνατοτήτων επεξεργασίας δεδομένων, σε συνδυασμό με τη χρήση ειδικών προγραμμάτων, επιτρέπουν να χρησιμοποιηθούν για hacking ή απομακρυσμένη διαχείριση υπολογιστή.

3.3.4 ΜΗΧΑΝΗΜΑΤΑ ΑΥΤΟΜΑΤΗΣ ΑΝΑΛΗΨΗΣ ΜΕΤΡΗΤΩΝ

Οι χρήστες των μηχανημάτων αυτόματης ανάληψης μετρητών (ATM) έχουν γίνει, πολλές φορές, στόχος επίθεσης με τη χρήση διάφορων τεχνικών. Έχουν καταγραφεί περιπτώσεις τοποθέτησης μηχανισμών που μπλοκάρουν τις πιστωτικές κάρτες, τοποθετήσεις μικροκαμερών, που καταγράφουν τους αριθμούς πιστωτικών καρτών και τα PIN όταν αυτά πληκτρολογούνε, ακόμη και η

τοποθέτηση πρόσθετων πληκτρολογίων πανομοιότυπων με των πραγματικών για την απόσπαση κωδικών.

Ο κατάλογος των μορφών ηλεκτρονικών εγκλημάτων όπως είδαμε σ' αυτό το κεφάλαιο είναι πραγματικά μεγάλος αν αναλογιστούμε ότι το ηλεκτρονικό έγκλημα είναι το πιο σύγχρονο έγκλημα. Γι' αυτό πλέον το κύριο μέλημα των οργανισμών αλλά και του κάθε χρήστη του διαδικτύου είναι η ασφάλεια ώστε να προστατεύσει το σύστημα του. Αυτό θα μελετήσουμε στο επόμενο κεφάλαιο.

ΚΕΦΑΛΑΙΟ 4
ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Οι Ηλεκτρονικοί Υπολογιστές και παράλληλα το Διαδίκτυο έχουν γίνει πλέον αναπόσπαστο κομμάτι των εξελιγμένων κοινωνιών. Αποτελεί εξαιρετικό βοήθημα του ανθρώπου στον τομέα της επιστήμης, της εκπαίδευσης, του εμπορίου, της ψυχαγωγίας. Ωστόσο το ερώτημα που τίθεται είναι κατά πόσο ασφαλές μπορεί να είναι; Πόσο ασφαλή είναι τα δεδομένα που καταθέτουμε σ' αυτά; Αρχικά θα πρέπει να δοθεί ο ορισμός της έννοιας «ασφάλεια».

4.1 Η ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Στον τομέα των πληροφοριακών συστημάτων, η ασφάλεια σχετίζεται με την ικανότητα ενός οργανισμού να προστατεύει τις πληροφορίες του, από τυχόν αλλοιώσεις και καταστροφές, καθώς και μη εξουσιοδοτημένη χρήση των πόρων του (πηγή: Πάγκαλος, 2005).

Η ασφάλεια των πληροφοριακών συστημάτων σχετίζεται με:

- την πρόληψη μη εξουσιοδοτημένων ενεργειών έναντι ενός συστήματος
- την ανίχνευση κάθε είδους επίθεσης
- την αντίδραση, δηλαδή, την λήψη μέτρων για την αποκατάσταση της ζημιάς, που προκλήθηκε από τον επιτιθέμενο

Η πρόληψη, η ανίχνευση και η αντίδραση περιλαμβάνουν στο γενικότερο σχεδιασμό της ασφάλειας ενός οργανισμού, που έχει επικρατήσει να ονομάζεται πολιτική ασφάλειας. Η πολιτική ασφάλειας καθορίζει τις διαδικασίες, που πρέπει να ακολουθούνται, για να μειωθούν οι κίνδυνοι επιθέσεων και τα αποτελέσματα αυτών.

4.1.1 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Η ασφάλεια ενός πληροφοριακού συστήματος, προσδιορίζεται με τρεις βασικές έννοιες, οι οποίες είναι κοινά αποδεκτές:

- εμπιστευτικότητα (Confidentiality)
- ακεραιότητα (Integrity)
- διαθεσιμότητα (Availability)

Η εμπιστευτικότητα σχετίζεται με την προστασία των δεδομένων, ώστε μη εξουσιοδοτημένα άτομα να μην έχουν πρόσβαση σ' αυτά. Η έννοια της εμπιστευτικότητας δεν προστατεύει μόνο τα ίδια τα δεδομένα αλλά και το γεγονός ότι υπάρχουν. Για παράδειγμα, η ύπαρξη ενός φακέλου ενός εγκληματία, τυγχάνει της ίδιας προστασίας και με τα περιεχόμενα του φακέλου (πηγή: Πάγκαλος, 2002:18).

Η ακεραιότητα αναφέρεται στην πρόληψη μη εξουσιοδοτημένης προσθήκης, διαγραφής και μη εξουσιοδοτημένη δημιουργίας δεδομένων των πληροφοριών.

Η διαθεσιμότητα περιλαμβάνει την δυνατότητα άμεσης προσπέλασης, χωρίς καθυστερήσεις, των πληροφοριών και υπηρεσιών ενός πληροφοριακού συστήματος.

4.2 ΜΕΤΡΑ ΠΡΟΛΗΨΗΣ

4.2.1 ΔΙΑΔΙΚΑΣΙΕΣ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ

Με τον όρο αυθεντικοποίηση εννοείται η διαδικασία κατά την οποία διαπιστώνεται ότι η ταυτότητα ενός χρήστη είναι αυθεντική. Για τον προσδιορισμό της ταυτότητας ενός ατόμου, υπάρχουν τρεις βασικές προσεγγίσεις:

i) Κάτι του ο χρήστης γνωρίζει π.χ. ένας κωδικός πρόσβασης, ένα PIN κ.λπ.
ii) Κάτι που ο χρήστης έχει στην κατοχή του π.χ. μια έξυπνη κάρτα.
iii) Κάτι που ο χρήστης έχει ως προσωπικό φυσικό χαρακτηριστικό π.χ. το δακτυλικό αποτύπωμα.

4.2.1.1 ΚΩΔΙΚΟΙ ΠΡΟΣΒΑΣΗΣ

Τα συστήματα που χρησιμοποιούν κωδικούς, απαιτούν την εισαγωγή από το χρήστη ενός ονόματος χρήστη (user ID) και ενός κωδικού πρόσβασης (password) για να επιτρέψουν την είσοδο. Μετά την εισαγωγή των στοιχείων, το σύστημα κάνει έλεγχο των κωδικών με τη βάση δεδομένων από κωδικούς, που έχει από πριν αποθηκευτεί και εφόσον διαπιστωθεί ταύτιση επιτρέπεται η είσοδος του χρήστη.

Οι βασικότεροι κίνδυνοι εναντίον της ασφάλειας εντός συστήματος, που βασίζεται στη χρήση κωδικών πρόσβασης είναι:

i) Η επιλογή των κωδικών πρόσβασης: Η ορθή επιλογή του κωδικού πρόσβασης είναι πολύ σημαντική. Αφήνοντας τους χρήστες να επιλέξουν μόνοι τους, τους κωδικούς που επιθυμούν, προτιμούν κωδικούς που μπορούν εύκολα να τους θυμούνται (π.χ. ονόματα, ημερομηνίες γέννησης κ.λπ.), με αποτέλεσμα κάποιος κακόβουλος να μπορεί να τους μαντέψει. Όταν η επιλογή των κωδικών πραγματοποιείται από τους διαχειριστές ενός συστήματος, τότε επιτυγχάνεται μεγαλύτερη ασφάλεια, υπάρχει όμως το ενδεχόμενο ο χρήστης, εάν ο κωδικός που του χορηγηθεί είναι δύσκολο να απομνημονευθεί, να τον γράψει σε ένα κομμάτι χαρτί, διευκολύνοντας τη διαρροή του εφόσον το χαρτί χαθεί ή κλαπεί.

ii) Διαμοιρασμός των κωδικών πρόσβασης: Πολλές φορές, ένας υπάλληλος μπορεί να δώσει τον κωδικό του σε ένα άλλο υπάλληλο, προκειμένου αυτός να έχει πρόσβαση στα αρχεία του, στη συνέχεια, να δοθεί για τον ίδιο λόγω σε κάποιο τρίτο κ.ο.κ. Τέτοιου είδους διαμοιρασμός των κωδικών πρόσβασης εγκυμονεί κινδύνους προερχόμενους, κυρίως από τους κοινωνικούς μηχανικούς.

iii) Παρακολούθηση πακέτων: Η παρακολούθηση των πακέτων που διακινούνται στο δίκτυο, μπορεί να έχει ως αποτέλεσμα την ανάκτηση κωδικών πρόσβασης.

iv) Πρόσβαση στο αρχείο αποθήκευσης των κωδικών: Οι κωδικοί πρόσβασης αποθηκεύονται σε ένα αρχείο του διακομιστή, ώστε, να είναι δυνατή η διαδικασία ταυτοποίησης. Αν το αρχείο αυτό δεν φυλάσσεται

καλά, ο επιτιθέμενος μπορεί να το ανακτήσει και να έχει, πλέον, στην κατοχή του όλους τους κωδικούς ενός οργανισμού.

4.2.1.2 ΒΙΟΜΕΤΡΙΚΕΣ ΤΕΧΝΙΚΕΣ

Βιομετρία (biometry) είναι η επιστήμη που χρησιμοποιεί ψηφιακή τεχνολογία, για να αναγνωρίσει την ταυτότητα ατόμων, βάση κάποιων ιδιαίτερων και μοναδικών χαρακτηριστικών τους.

Οι σημαντικότερες βιομετρικές τεχνικές είναι:

i) Σάρωση δακτυλικού αποτυπώματος: Η ταυτοποίηση δύο ατόμων με τη χρήση δακτυλικών αποτυπωμάτων, αποτελεί μια από τις πλέον κλασικές και αξιόπιστες μεθόδους ταυτοποίησης. Έχει αποδειχτεί, ότι η πιθανότητα δυο άτομα να έχουν το ίδιο δακτυλικό αποτύπωμα είναι μια στο δισεκατομμύριο. Η λήψη των αποτυπωμάτων γίνεται με οπτικούς αναγνώστες, υπέρυθρες ακτίνες και τεχνολογίες σιλικόνης.

Εικόνα 4.1: Σάρωση δακτυλικού αποτυπώματος με υπέρηχο

ii) Αναγνώριση προσώπου: Αποτελεί μια από τις πλέον ταχύτατα αναπτυσσόμενες βιομετρικές τεχνικές. Στην αναγνώριση προσώπου δίνεται έμφαση σε σημεία του προσώπου, που είναι λιγότερο ευάλωτα στην αλλαγή, όπως τα πάνω περιγράμματα του ματιού, οι περιοχές που περιβάλλουν τα ζυγωματικά και η όψη του στόματος καθώς και σε

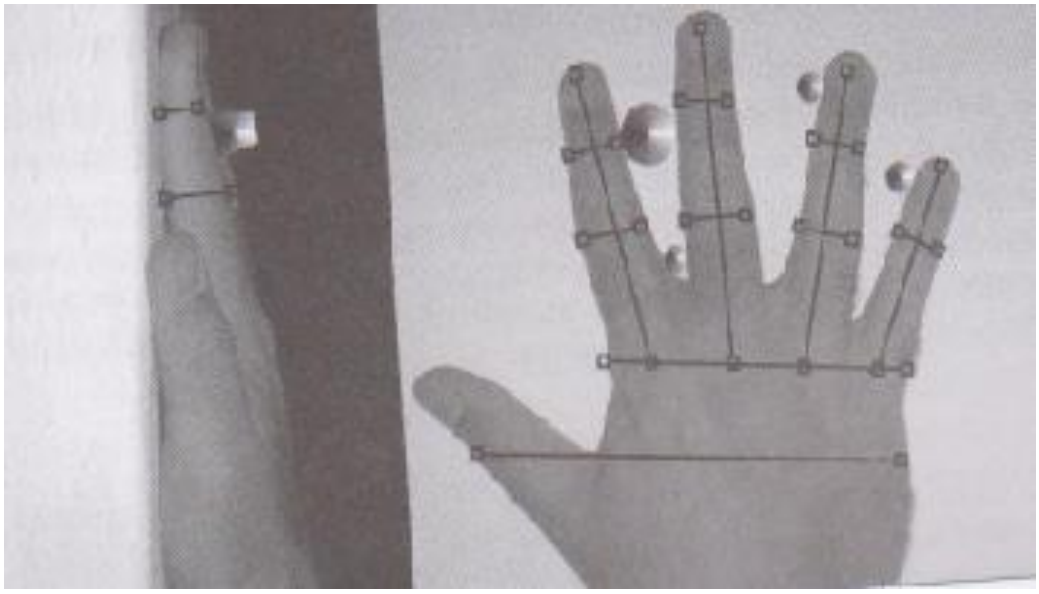
γεωμετρικά χαρακτηριστικά όπως η απόσταση από τα μάτια έως τη μύτη, το κενό ανάμεσα στα φρύδια κ.α. Όλα τα βασικά συστήματα είναι σχεδιασμένα, ώστε, να είναι αρκετά ισχυρά, για να διεξάγουν αναζητήσεις ένα-προς-πολλά, δηλαδή, να μπορούν να βρίσκουν ένα πρόσωπο, μέσα σε μια βάση δεδομένων χιλιάδων ή ακόμα και εκατοντάδων χιλιάδων προσώπων. Όμως, πολλά συστήματα αντιμετωπίζουν δυσκολίες στο να πετύχουν μεγάλα επίπεδα απόδοσης.

Εικόνα 4.2: Εξαγωγή γεωμετρικών χαρακτηριστικών προσώπου

iii) Σάρωση φωνής: Τα συστήματα σάρωσης φωνής λειτουργούν αναγνωρίζοντας το μοναδικό ηχητικό σήμα, που παράγει ο χρήστης, λέγοντας μια συγκεκριμένη φράση κλειδί (pass-phrase). Το βασικό προτέρημα αυτής της τεχνολογίας είναι η δυνατότητα για εξ-αποστάσεως ταυτοποίησης.

iv) Σάρωση ίριδας ματιού και αμφιβληστροειδή χιτώνα: Η ανθρώπινη ίριδα έχει σχεδόν 250 χαρακτηριστικά και καθένα από αυτά είναι μοναδικό σε κάθε άνθρωπο. Ο αριθμός των χαρακτηριστικών είναι δέκα φορές πάνω από τον αριθμό των γνωρισμάτων, που διαθέτουν τα δακτυλικά αποτυπώματα. Η αναγνώριση της ίριδας είναι ακόμα πιο αξιόπιστη και από την εξέταση DNA.

v) Σάρωση χεριού: Είναι γνωστή και ως γεωμετρία χεριού. Είναι μια αυτοματοποιημένη μέτρηση πολλών μεγεθών του χεριού και των δακτύλων. Η τεχνολογία αυτή χρησιμοποιεί το ύψος των δακτύλων, την απόσταση μεταξύ των κλειδώσεων και το σχήμα των αρθρώσεων, για να πιστοποιήσει την ταυτότητα του χρήστη. Παρόλο, που δεν είναι η πιο ακριβής τεχνολογία, η σάρωση χεριού έχει αποδειχθεί, ως η ιδανική λύση για χαμηλού επιπέδου ασφάλεια.



Εικόνα 4.3: Γεωμετρία Χεριού

vi) Σάρωση υπογραφής: Είναι γνωστή και ως Δυναμική Εξακρίβωση Υπογραφής. Επειδή, το κάθε άτομο έχει τον προσωπικό του γραφικό χαρακτήρα, το σύστημα παίρνει τα χαρακτηριστικά του τρόπου γραφής και αναλύει τη δυναμική του χτυπήματος, την ταχύτητα και την πίεση. Ενώ με εξάσκηση κάποιος ίσως μπορέσει να αντιγράψει την οπτική εικόνα της υπογραφής κάποιου άλλου, είναι πολύ δύσκολο, έως αδύνατο, να αντιγράψει τον τρόπο με τον οποίο το άτομο αυτό υπογράφει. Ακόμη και η υπογραφή να είναι τέλεια σχεδιασμένη, η ταχύτητα, η δύναμη και η πίεση θα διαφέρουν. Η σάρωση υπογραφής δεν έχει ακόμη ευρεία χρήση, αναμένεται όμως πολύ σύντομα να βοηθήσει στην πιστοποίηση επίσημων εγγράφων.

vii) Σάρωση πατήματος πλήκτρου: Είναι γνωστή και ως ρυθμός δακτυλογράφησης. Εξετάζει τον τρόπο με τον οποίο ένα άτομο

δακτυλογραφεί ή πιέζει τα πλήκτρα σε ένα πληκτρολόγιο. Τα χαρακτηριστικά που αναλύονται είναι η ταχύτητα, η δύναμη, η συχνότητα λάθους, ο συνολικός χρόνος δακτυλογράφησης ενός συγκεκριμένου συνθηματικού και ο χρόνος που μεσολαβεί από το πάτημα ενός συγκεκριμένου πλήκτρου έως το πάτημα ενός άλλου.

4.2.2 ΧΡΗΣΗ ΛΟΓΙΣΜΙΚΟΥ ΑΣΦΑΛΕΙΑΣ

4.2.2.1 ΛΟΓΙΣΜΙΚΟ ANTIVIRUS

Από πολλές έρευνες έχει διαπιστωθεί ότι η διασπορά ιών είναι η πιο διαδεδομένη μορφή επιθέσεων στο Διαδίκτυο. Καθημερινά δημιουργούνται χιλιάδες νέοι ιοί που απειλούν τα υπολογιστικά συστήματα. Η πιο σημαντική μέθοδος αντιμετώπισης ιών είναι η χρήση αντιβιοτικών προγραμμάτων (antivirus software).

Το λογισμικό αντιμετώπισης ιών, είναι από τα πιο πολύπλοκα εργαλεία λογισμικού. Ένα τέτοιο λογισμικό, επιτελεί τρεις βασικές λειτουργίες:

1) Ανίχνευση ιών: Η διαδικασία αυτή, μπορεί να γίνει είτε κατόπιν ενέργειας του χρήστη, που επιλέγει μέσω του λογισμικού τον έλεγχο του σκληρού δίσκου για ιούς, είτε πραγματοποιείται αυτόματα, καθώς, το λογισμικό φορτώνεται στην μνήμη RAM του συστήματος και ελέγχει όλες τις εφαρμογές που εκτελούνται.
2) Προσδιορισμός της ταυτότητας των ιών: Εάν το σύστημα μας έχει προσβληθεί από κάποιο ιό, το λογισμικό θα μας ενημερώσει για την ταυτότητα του. Αυτό μας επιτρέπει να εκτιμήσουμε το μέγεθος της ζημιάς που έχει προκληθεί ώστε να εκτελέσουμε τις απαραίτητες ενέργειες για την αποκατάσταση της ομαλής λειτουργίας του συστήματος.
3) Καθαρισμός ιών: Αφού έχουν εντοπιστεί οι ιοί που μόλυναν το σύστημα, θα πρέπει να αφαιρεθούν. Τα περισσότερα λογισμικά, όταν εντοπίσουν έναν ιόν, προτείνουν στον χρήστη είτε να επιδιορθώσει το αρχείο που έχει μολυνθεί, είτε να θέσει το αρχείο σε καραντίνα ώστε να μην μπορεί να χρησιμοποιηθεί, είτε να το διαγράψει.

Ένα λογισμικό μπορεί να εντοπίσει μόνο τους ιούς οι οποίοι του είναι γνωστοί. Γι' αυτό όλες οι εταιρείες που προσφέρουν λογισμικό ανίχνευσης ιών, δίνουν τη δυνατότητα στους χρήστες να κάνουν on-line ενημέρωση της βάσης δεδομένων του προγράμματος με τους νέους ιούς, ώστε να είναι δυνατός ο εντοπισμός και η απομάκρυνση τους. Το στοιχείο που κάνει μοναδικό τον κάθε ιό ονομάζεται αποτύπωμα ή υπογραφή (signature) του ιού. Στη βάση δεδομένων ενός προγράμματος antivirus, τηρείται λίστα με όλες τις υπογραφές που είναι γνωστές. Κατά τον έλεγχο ενός συστήματος, όταν βρεθεί κάποιο ταίριασμα της υπογραφής του αρχείου με την υπογραφή που έχει αποθηκευτεί στη βάση δεδομένων του antivirus, ενημερώνεται άμεσα ο χρήστης ότι έχει μολυνθεί από κάποιο ιό.

Αν και η ενημέρωση της βάσης δεδομένων του antivirus γίνεται λίγες μόνο ώρες αφού εντοπιστεί ο νέος ιός, αυτό το μικρό χρονικό διάστημα είναι το μεγαλύτερο μειονέκτημα των εφαρμογών antivirus γιατί μέχρι τότε ο ιός θα έχει προλάβει να προξενήσει ζημιά σε αρκετές χιλιάδες υπολογιστές. Για το λόγω αυτό, οι εταιρείες λογισμικού αναζητούν νέες τεχνολογίες και μεθόδους για την αντιμετώπιση των προβλημάτων αυτών. Νέες τεχνολογίες είναι:

1. Ευρετική (heuristic) ανάλυση: Κατά τη χρήση της ευρετικής ανάλυσης το πρόγραμμα δεν αναζητά τις υπογραφές των ιών, αλλά, ελέγχει τα εκτελέσιμα αρχεία και προσπαθεί να προσδιορίσει εάν στον κώδικα τους περιέχεται εντολή ή εντολές, οι οποίες πιθανώς να αποτελούν ιούς.
2. Έλεγχος ακεραιότητας (Integrity Check): Είναι μια τεχνική που χρησιμοποιείται για την ανίχνευση μόνο των ιών, χωρίς να δίνει τη δυνατότητα προσδιορισμού της ταυτότητας τους. Αρχικά για κάθε αρχείο του συστήματος υπολογίζεται το άθροισμα ελέγχου (checksum). Το άθροισμα αυτό είναι ένας αριθμός που προσδιορίζει μοναδικά ένα αρχείο, ενώ, κάθε τροποποίηση του, έστω και ενός bit, του αρχείου προκαλεί μεταβολή του αθροίσματος. Τα αθροίσματα αυτά αποθηκεύονται σε μια βάση δεδομένων. Ακολούθως ξανά υπολογίζονται τα αθροίσματα και συγκρίνονται με τα περιεχόμενα της βάσης δεδομένων. Εφόσον διαπιστωθεί διαφορά, πιθανολογείται ότι αυτή οφείλεται στην επίδραση του ιού.

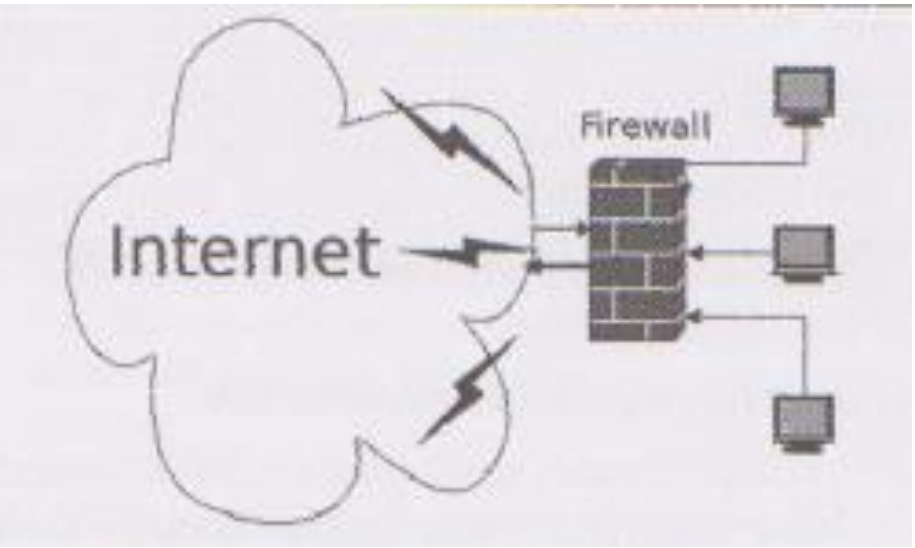
Σήμερα, στην παγκόσμια αγορά κυκλοφορούν πολλά πακέτα λογισμικού ανίχνευσης ιών. Τα κριτήρια, με τα οποία θα επιλέξουμε το λογισμικό, εξαρτάται

άμεσα από τις ανάγκες που θέλουμε να καλύψουμε. Οι βασικότερες προϋποθέσεις είναι:

- Εύχρηστο Interface και χαμηλή κατανάλωση πόρων
- Προστασία σε πραγματικό χρόνο
- Αυτόματη ενημέρωση
- Προστασία Ηλεκτρονική Αλληλογραφίας
- Προγραμματισμένος Έλεγχος
- Δισκέτα Εκκίνησης
- Καταγραφή Συμβάντων (event logging)

4.2.2.2 FIREWALLS

Ο όρος firewall προσδιορίζει μια συσκευή ή εργαλείο λογισμικού (ή και συνδυασμό των δύο), που παρακολουθεί και φιλτράρει τα πακέτα που επιχειρούν είτε να εισέλθουν, είτε να εξέλθουν από ένα εσωτερικό προστατευμένο δίκτυο ή υπολογιστή. Είναι εργαλεία που ξεχωρίζουν ένα εσωτερικό «ασφαλές» θα λέγαμε δίκτυο (π.χ. το intranet μιας επιχείρησης), από ένα εξωτερικό μη ασφαλές δίκτυο, όπως το internet.



Εικόνα 4.4: Τυπική διάταξη firewall

Τα περισσότερα firewalls επιτελούν δυο βασικές λειτουργίες ασφαλείας:

i) Φιλτράρισμα πακέτων (packet filtering), το οποίο βασίζεται στο να επιτρέπει ή να απαγορεύει την κίνηση των πακέτων που διακινούνται στο δίκτυο, με βάση την υιοθετούμενη πολιτική ασφαλείας.

ii) Πύλες εφαρμογών (Application proxy gateways), που προσφέρουν υπηρεσίες στους εσωτερικούς χρήστες και ταυτόχρονα προστατεύουν τους hosts από εξωτερικές απειλές.

Η επιλογή της λειτουργίας, που θα χρησιμοποιηθεί σε ένα firewall, σχετίζεται άμεσα με την πολιτική ασφαλείας ενός οργανισμού. Οι βασικότερες πολιτικές ασφαλείας που εφαρμόζονται είναι:

α) Πολιτική προκαθορισμένης άδειας χρήσης (Allow-everything-not-specifically-denied) όπου η κυκλοφορία πακέτων και η εκτέλεση εφαρμογών επιτρέπεται ελεύθερα, εκτός των περιπτώσεων που υπάρχει ρητή απαγόρευση.

β) Πολιτική προκαθορισμένης απαγόρευσης χρήσης (Deny-everything-not-specifically-allowed), στην οποία το firewall ρυθμίζεται, έτσι ώστε, να μην επιτρέπει καμιά κυκλοφορία πακέτων και καμιά εκτέλεση εφαρμογής, εφόσον, δεν έχουν εκ των προτέρων καθοριστεί. Στην περίπτωση αυτή, έχουμε μεγαλύτερη ασφάλεια από την πρώτη, όμως η έντονη «παρουσία» του firewall ενδέχεται να δυσανασχετήσει τους χρήστες.

Με τη ραγδαία ανάπτυξη του ηλεκτρονικού εγκλήματος, η χρήση του firewall είναι περισσότερο αναγκαία από ποτέ. Η τεχνολογία, στο συγκεκριμένο τομέα, αναπτύσσεται με γοργούς ρυθμούς και έχουν δημιουργηθεί firewalls, τα οποία επιτελούν πολλές εργασίες ταυτόχρονα. Μπορούμε να διαχωρίσουμε τα firewalls με κριτήριο την τεχνική που χρησιμοποιούν:

1) Πύλες φιλτραρίσματος πακέτων: Όλα τα πακέτα διακινούνται στο δίκτυο και διέρχονται από το firewall φιλτράρονται με βάση κάποιους προκαθορισμένους κανόνες που τίθενται από το διαχειριστή. Έτσι το πακέτο είτε επιτρέπεται να διέλθει είτε απορρίπτεται. Οι παράμετροι, που προσδιορίζουν τα κριτήρια επιλογής των πακέτων που θα διέλθουν ή θα εξέλθουν είναι: i) Η διεύθυνση IP του αποστολέα και του παραλήπτη, με δυνατότητα ομαδοποίησης των διευθύνσεων με τη χρήση μάσκας. ii) Η θυρίδα (port) προέλευσης και προορισμού. iii) Το χρησιμοποιούμενο

πρωτόκολλο επικοινωνίας. Μειονέκτημα αυτής της τεχνικής είναι ότι το περιεχόμενο των IP-πακέτων δεν λαμβάνονται υπόψη καθώς εξετάζονται μόνο οι IP-επικεφαλίδες από τις οποίες λαμβάνονται οι πληροφορίες δρομολόγησης, που στη συνέχεια αξιολογούνται και αναλόγως επιτρέπεται ή απαγορεύεται η διέλευση των πακέτων.

2) Πύλες εφαρμογών: Λειτουργούν στο υψηλότερο στρώμα επικοινωνίας, γνωστό ως επίπεδο εφαρμογών. Υπάρχει μια υπηρεσία διαμεσολάβησης, που πραγματώνεται με τη χρήση ενός πακέτου λογισμικού proxy server. Η υπηρεσία proxy έχει τη δυνατότητα να ενεργεί, για τους εξωτερικούς χρήστες ως πελάτης και για τους εσωτερικούς χρήστες ως διακομιστής. Το λογισμικό αυτό παρεμβάλλεται μεταξύ των πρωτοκόλλων επικοινωνίας και έχει ως βασικό σκοπό τον έλεγχο των επικοινωνιών. Για παράδειγμα, ένας εξωτερικός χρήστης για να αποκτήσει πρόσβαση σε μια υπηρεσία του προστατευμένου δικτύου, θα πρέπει πρώτα να συνδεθεί με την proxy εφαρμογή, η οποία θα προβεί στην αναγνώριση και πιστοποίηση του και έπειτα, θα του επιτρέψει την πρόσβαση στην υπηρεσία που ζήτησε. Η αντίστοιχη διαδικασία πραγματοποιείται, όταν ένας εσωτερικός χρήστης αιτείται τη χρήση μιας εξωτερικής υπηρεσίας.
3) Υβριδικές πύλες: Η τεχνολογία των υβριδικών firewalls, η Stateful Inspection συμπληρώνει το IP φιλτράρισμα από μια υπηρεσία ελέγχου του εσωτερικού των πακέτων, λαμβάνοντας υπόψη προηγούμενες επικοινωνίες. Οι πληροφορίες αυτές καταχωρούνται σε μια βάση δεδομένων που συνεχώς ανανεώνεται και η σύγκριση των δεδομένων της με τα πακέτα, που επιχειρούν να διέλθουν το firewall, επιτρέπει ή απαγορεύει την επικοινωνία.

4.2.3 ΚΡΥΠΤΟΓΡΑΦΙΑ

Η κρυπτογραφία (cryptography) αποτελεί μέρος της κρυπτολογίας (cryptology), της επιστήμης που ασχολείται με τη μελέτη της ασφαλής επικοινωνίας. Ο έτερος κλάδος της κρυπτολογίας είναι η κρυπτανάλυση, που ασχολείται με την ανάλυση και το σπάσιμο των αλγορίθμων κρυπτογράφησης. Η κρυπτογραφία σύμφωνα με τον ορισμό που δίνεται στη Βικιπαίδεια, είναι η επιστήμη που ασχολείται με τους

μαθηματικούς μετασχηματισμούς για την εξασφάλιση της ασφάλειας της πληροφορίας.

Οι βασικότεροι στόχοι της κρυπτογραφίας στην γενικότερη ασφάλεια ενός συστήματος είναι η εμπιστευτικότητα, η αυθεντικοποίηση, η ακεραιότητα, και η μη αποποίηση παραλαβής - αποστολής.

Με την κρυπτογράφηση επιχειρείται η μετατροπή της πληροφορίας από μια κατανοητή μορφή σε ένα γρίφο, ο οποίος παραμένει ακατανόητος. Με αντίθετη διαδικασία, δηλαδή την αποκρυπτογράφηση, ο γρίφος αυτός επανέρχεται στην αρχική του μορφή και η πληροφορία μπορεί να αναγνωστεί.

Τα βασικά στοιχεία, που αποτελούν ένα σύγχρονο σύστημα κρυπτογράφησης, είναι:

1) Το αρχικό μήνυμα.
2) Το κρυπτογραφικό σύστημα, το οποίο αποτελείται από ένα αλγόριθμο κρυπτογράφησης και ένα αλγόριθμο αποκρυπτογράφησης.
3) Το κρυπτογραφημένο κείμενο, το οποίο αποτελεί το αποτέλεσμα του αλγόριθμου κρυπτογράφησης στο αρχικό μήνυμα, πριν αυτό σταλεί στον παραλήπτη.
4) Ένα κλειδί, το οποίο είναι μια συμβολοσειρά, η οποία χρησιμοποιείται από τους αλγόριθμους στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης.

Από τεχνικής απόψεως, η κρυπτογραφία διακρίνεται σε δύο βασικές κατηγορίες:
Α) Την συμμετρική κρυπτογράφηση, στην οποία χρησιμοποιείται το ίδιο κλειδί, τόσο για την κρυπτογράφηση όσο και την αποκρυπτογράφηση των δεδομένων. Βασική προϋπόθεση είναι, το κλειδί να έχει δοθεί στους χρήστες, που επιθυμούν να επικοινωνήσουν, μέσω ενός ασφαλούς καναλιού επικοινωνίας. Η διαδικασία επικοινωνίας έχει ως εξής: Το αρχικό μήνυμα κρυπτογραφείται με το μυστικό κλειδί του αποστολέα και αποστέλλεται στον παραλήπτη μέσω του καναλιού επικοινωνίας. Ο παραλήπτης παραλαμβάνει το κρυπτογραφημένο μήνυμα και το αποκρυπτογραφεί με το ίδιο μυστικό κλειδί.

Β) Την ασύμμετρη κρυπτογράφηση, στην οποία χρησιμοποιείται ένα κλειδί για την κρυπτογράφηση των δεδομένων και ένα διαφορετικό κλειδί για την αποκρυπτογράφηση. Κύριο χαρακτηριστικό των κλειδιών αυτών είναι ότι αν και συσχετίζονται μεταξύ τους, η γνώση του ενός δεν μπορεί να οδηγήσει στην αποκάλυψη του άλλου. Το κλειδί που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων ονομάζεται δημόσιο (public key) και είναι γνωστό σε όλους, ενώ το κλειδί με το οποίο γίνεται αποκρυπτογράφηση ονομάζεται ιδιωτικό (private key) και το κατέχει μόνο αυτός που θα κάνει την αποκρυπτογράφηση.

Η προστασία που προσφέρεται με την ασύμμετρη κρυπτογράφηση, είναι πολύ πιο ισχυρή από την ασύμμετρη και επίσης δεν απαιτείται ασφαλής δίαυλος επικοινωνίας για την ανταλλαγή των κλειδιών. Όταν ένας χρήστης θέλει να λάβει ένα κρυπτογραφημένο μήνυμα, δίνει στον αποστολέα το δημόσιο κλειδί του με το οποίο γίνεται η κρυπτογράφηση του μηνύματος, η αποκρυπτογράφηση γίνεται μόνο με το ιδιωτικό κλειδί που μόνο αυτός κατέχει. Το πρόβλημα της μεθόδου αυτής είναι ότι απαιτούνται πολύ μεγαλύτερα κλειδιά απ’ ότι στην συμμετρική κρυπτογράφηση.

Γ) Την υβριδική κρυπτογράφηση, η οποία φέρει στοιχεία και από τις δύο πιο πάνω μεθόδους. Το υβριδικό σύστημα έχει επικρατήσει γιατί μ’ αυτό ξεπέρνιουνται τα προβλήματα που συναντούμε στις προηγούμενες τεχνικές, δηλαδή, συμμετρική κρυπτογράφηση η απαίτηση εύρεσης ασφαλούς καναλιού επικοινωνίας για την ανταλλαγή των μυστικών κλειδιών και στην ασύμμετρη κρυπτογράφηση η απαίτηση μεγαλύτερων κλειδιών που καθιστούν τη διαδικασία κρυπτογράφησης-αποκρυπτογράφησης χρονοβόρα. Στο υβριδικό σύστημα χρησιμοποιείται αρχικά η ασύμμετρη κρυπτογραφία για να γίνει η ανταλλαγή του μυστικού κλειδιού. Όταν ολοκληρωθεί η ανταλλαγή του μυστικού κλειδιού, το οποίο οι χρήστες παραλαμβάνουν μέσω του ασφαλούς καναλιού επικοινωνίας, η επικοινωνία πραγματοποιείται με συμμετρική κρυπτογράφηση των δεδομένων.

4.2.3.1 ΔΙΑΧΕΙΡΙΣΗ ΔΗΜΟΣΙΩΝ ΚΛΕΙΔΙΩΝ – ΠΙΣΤΟΠΟΙΗΤΙΚΑ

Το πρόβλημα που προκύπτει από τη χρήση δημόσιων κλειδιών κατά τη διαδικασία της κρυπτογράφησης, είναι το πώς θα εξακριβωθεί ότι το δημόσιο κλειδί που

λαμβάνει ένας χρήστης, είναι πράγματι αυθεντικό. Η εξακρίβωση αυτή είναι πολύ σημαντική, διότι κατά την επαλήθευση μιας ψηφιακής υπογραφής ο χρήστης πρέπει να είναι βέβαιος, ότι το δημόσιο κλειδί που χρησιμοποιείται για την επαλήθευση της υπογραφής είναι πραγματικά το δημόσιο κλειδί του υποτιθέμενα υπογράφοντος. Χωρίς πρόσθετα μέτρα θα πρέπει κάθε χρήστης να εξακριβώνει εξωσυστημικά την αυθεντικότητα κάθε δημόσιου κλειδιού πριν επιλέξει να το εμπιστευτεί. Η πολυπλοκότητα του ζητήματος μπορεί να μειωθεί με την αρχή πιστοποίησης η οποία υπογράφει με το δικό της ιδιωτικό κλειδί τα δημόσια κλειδιά και τα αντίστοιχα ονόματα, προσθέτοντας κάποια επιπλέον στοιχεία π.χ. περίοδο εγκυρότητας. Το κομμάτι των δεδομένων που έχει υπογραφεί από την αρχή πιστοποίησης ονομάζεται πιστοποιητικό. Το πιστοποιητικό μπορεί να επαληθευτεί, χρησιμοποιώντας το δημόσιο κλειδί της αρχής πιστοποίησης.

4.2.3.2 ΕΠΙΘΕΣΕΙΣ ΣΕ ΣΥΣΤΗΜΑΤΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Η χρήση της κρυπτογράφησης οδήγησε στην ανάπτυξη μιας σχετικά παράλληλης αλλά αντίθετης επιστήμης της κρυπτανάλυσης, που ασχολείται με την αποκρυπτογράφηση του κρυπτογραφημένου κειμένου. Οι μέθοδοι και οι τεχνικές της κρυπτανάλυσης αποτελούν τα βασικά εργαλεία των επιτιθέμενων έναντι των συστημάτων κρυπτογράφησης. Πολύ σημαντικό είναι το τι υλικό έχει στα χέρια του ο κρυπταναλυτής. Αν για παράδειγμα κατέχει μόνο το κρυπτογραφημένο κείμενο, είναι πολύ δύσκολο έως αδύνατο να βρει το μη κρυπτογραφημένο. Αν όμως έχει στα χέρια του το κρυπτογραφημένο αλλά και το αντίστοιχο αρχικό, είναι πιο εύκολο να βρει το κλειδί για τις κρυπτογραφήσεις και αποκρυπτογραφήσεις.

Η κυρίαρχη ιδέα ενός συστήματος κρυπτογράφησης είναι ο φόρτος εργασίας (workload) (πηγή: Shannon, 1948), που απαιτείται από έναν κρυπταναλυτή για να βρει το κλειδί. Όσο περισσότερος κόπος και χρόνος απαιτείται για να βρεθεί ένα κλειδί σε ένα κρυπτογραφικό σύστημα τόσο ασφαλέστερο αυτό θεωρείται.

Οι αλγόριθμοι κρυπτογράφησης μπορούν πολύ δύσκολα να σπάσουν. Αν υπάρχει, όμως, αρκετός χρόνος και υπομονή, ένα πρόγραμμα που θα δοκιμάσει όλα τα πιθανά κλειδιά κάποια στιγμή θα βρει το σωστό. Το κρίσιμο ζήτημα είναι ο χρόνος που θα απαιτηθεί για να ολοκληρωθεί αυτή η διαδικασία έστω και αν

χρησιμοποιηθούν υπερυπολογιστές για την διεκπεραίωση της. Ο χρόνος αυτός, όπως επίσης και το μήκος του κλειδιού, αποτελούν τα στοιχεία που αποτρέπουν τους επιτιθέμενους, συνεπώς καθορίζουν το βαθμό αξιοπιστίας του συστήματος κρυπτογράφησης.

4.2.4 ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ

Με τον όρο φυσική ασφάλεια, αναφερόμαστε σε όλα εκείνα τα μέτρα, που είναι απαραίτητο να ληφθούν, ώστε να προστατευθεί η φυσική υπόσταση των συσκευών που απαρτίζουν έναν υπολογιστή ή ένα δίκτυο υπολογιστών. Όσο και αν προστατεύσουμε ένα διακομιστή με εργαλεία λογισμικού, θα έχουμε αποτύχει παντελώς, αν κάποιος εισβολέας καταφέρει να φτάσει στην φυσική τοποθεσία όπου αυτός φυλάσσεται και να αφαιρέσει το σκληρό δίσκο, που περιέχει όλα τα ευαίσθητα και σημαντικά δεδομένα του οργανισμού.

Στη φυσική ασφάλεια εντάσσεται η προστασία από φυσικές καταστροφές. Πλημμύρες, σεισμοί και φωτιές μπορεί να προκαλέσουν ανεπανόρθωτες ζημιές. Η σωστή συντήρηση των κτιρίων, ο συχνός έλεγχος των υδραυλικών και ηλεκτρολογικών εγκαταστάσεων και η ύπαρξη συστήματος πυρόσβεσης, τουλάχιστον στους χώρους όπου έχουν τοποθετηθεί ηλεκτρονικοί υπολογιστές, μπορούν να αποσβήσουν τους κινδύνους αυτούς.

Επίσης σημασία πρέπει να δίνεται και στον βοηθητικό εξοπλισμό. Για παράδειγμα, τα καλώδια κινδυνεύουν από απευθείας παρέμβαση, η οποία μπορεί να στοχεύει είτε στην καταστροφή του δικτύου είτε στην παρεμβολή συσκευών για την υποκλοπή δεδομένων. Ακόμη, οι αφαιρούμενες αποθηκευτικές μονάδες καθώς και τα δεδομένα που τυπώνονται, μπορεί να περιέχουν σημαντικές πληροφορίες για την ασφάλεια του συστήματος, γι’ αυτό και αυτά πρέπει να προστατεύονται.

Τέλος, οι μέθοδοι και τα συστήματα αυθεντικοποίησης μπορούν να χρησιμοποιηθούν για τη φυσική ασφάλεια του εξοπλισμού. Βιομετρικές τεχνολογίες μπορούν να εμποδίσουν την μη εξουσιοδοτημένη πρόσβαση ατόμων στους χώρους όπου φυλάσσονται οι διακομιστές ενός δικτύου ή άλλα ευπαθή μέρη του εξοπλισμού.

4.3 ΑΝΙΧΝΕΥΣΗ ΕΠΙΘΕΣΕΩΝ

Τα μέτρα πρόληψης που αναφέραμε έχουν ως σκοπό την αποτροπή μιας επίθεσης σε ένα σύστημα. Αν όμως κάποιος καταφέρει να παραβιάσει τα μέτρα πρόληψης τότε το σύστημα θα πρέπει να έχει τη δυνατότητα να εντοπίσει την επίθεση, ώστε, να επιχειρήσει είτε να την αποτρέψει είτε να προβεί στην αποκατάσταση του συστήματος.

4.3.1 ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΠΙΘΕΣΕΩΝ (ΣΑΕ)

Για την ανίχνευση μιας επίθεσης, χρησιμοποιούνται τα Συστήματα Ανίχνευσης Επιθέσεων (Intrusion Detection System – IDS). Τα συστήματα ανίχνευσης επιθέσεων τοποθετούνται από το διαχειριστή ενός δικτύου, για να εντοπίσουν μια προσπάθεια μη εξουσιοδοτημένης πρόσβασης σε αυτό.

Υπάρχουν τρία βασικά μοντέλα συστημάτων ανίχνευσης επιθέσεων:

1) Ανίχνευση Ανωμαλιών: Τα συστήματα αυτά αυτοεκπαιδεύονται, δηλαδή, καταγράφουν ροές και διαδικασίες δεδομένων προσπαθώντας να κάνουν ένα είδος τυποποίησης. Οι τυποποιημένες αυτές διαδικασίες, χρησιμοποιούνται για να εντοπιστούν ανωμαλίες που πιθανώς θα αποτελούν εισβολή σύμφωνα με τα όσα έχουν καταγραφεί. Τα συστήματα αυτά χρησιμοποιούν ευρετικές μεθόδους και υπάρχει η πιθανότητα αν δεν έχουν ρυθμιστεί κατάλληλα να δίνουν λάθος συναγερμούς ή να μην εντοπίζουν μια επίθεση.
2) Ανίχνευση Υπογραφών: Τα συστήματα αυτά στηρίζονται στο γεγονός, ότι για κάθε επίθεση υπάρχει μια μοναδική μέθοδος ή υπογραφή η οποία και μπορεί να εντοπιστεί. Για την ταυτοποίηση των υπογραφών υπάρχει μια βάση δεδομένων στην οποία αποθηκεύονται οι υπογραφές των επιθέσεων, ώστε να υπάρχει δυνατότητα σύγκριση. Όπως βλέπουμε η λειτουργία των συστημάτων αυτών μοιάζει με τα λογισμικά ανίχνευσης ιών. Αν η βάση των υπογραφών δεν είναι ενημερωμένη δεν μπορεί να εντοπιστεί μια νέα μορφή επίθεσης.
3) Υβριδικό Μοντέλο: Λόγω των μειονεκτημάτων, που παρουσιάζουν τα πιο πάνω συστήματα αρχίζουν να αναπτύσσονται υβριδικά μοντέλα, τα οποία

δανείζονται χαρακτηριστικά από ήδη υπάρχοντα. Η τεχνολογία των υβριδικών μοντέλων είναι ακόμη σε πρώιμο στάδιο.

Περαιτέρω τα συστήματα ανίχνευσης επιθέσεων, ανάλογα με το μέσο το οποίο παρακολουθούν, μπορούμε να τα διακρίνουμε:

● ΣΑΕ που συλλέγουν πληροφορίες από το δίκτυο: παρακολουθούν την κίνηση στο δίκτυο, με σκοπό να εντοπίσουν επιθέσεις. Παρακολουθούν παθητικά την κίνηση στο δίκτυο και δεν επεμβαίνουν για να την διακόψουν ή αλλοιώσουν, γι' αυτό είναι πολύ δύσκολο να εντοπιστούν από τον επιτιθέμενο.

● ΣΑΕ που συλλέγουν πληροφορίες από υπολογιστές: επικεντρώνονται στην παρακολούθηση ενός και μόνο υπολογιστή, στον οποίο τοποθετείται κατάλληλο λογισμικό που παρακολουθεί συγκεκριμένα αρχεία καταγραφής (log files). Όταν διαπιστωθεί οποιαδήποτε μεταβολή, θεωρείται, ότι έχει γίνει κάποια κακόβουλη δραστηριότητα.

● ΣΑΕ που συλλέγουν πληροφορίες από εφαρμογές: αποτελούν υποκατηγορία των ΣΑΕ που συλλέγουν πληροφορίες από υπολογιστές. Χρησιμοποιούν τα αρχεία καταγραφής των εφαρμογών για να εντοπίσουν πιθανές επιθέσεις, που επιχειρούνται στο επίπεδο της εφαρμογής. Είναι κατάλληλα όταν θέλουμε να προστατέψουμε μια πολύ σημαντική εφαρμογή, όπως π.χ. μια βάση δεδομένων με σημαντικές πληροφορίες.

4.3.1.1 Η ΑΝΤΙΔΡΑΣΗ ΤΩΝ ΣΑΕ ΣΕ ΜΙΑ ΕΠΙΘΕΣΗ

Ένα σύστημα ανίχνευσης επιθέσεων εκτός από την παρακολούθηση ενός δικτύου ή υπολογιστή, όταν αντιληφθεί μια επίθεση, εκτελεί μια σειρά από εντολές, ανάλογα με τις ρυθμίσεις που έχει επιλέξει ο διαχειριστής. Τις αντιδράσεις των ΣΑΕ μπορούμε να τις διακρίνουμε σε δύο κατηγορίες:

a. Ενεργητικές αντιδράσει: όταν το σύστημα εντοπίσει μια επίθεση, εκτελεί μια σειρά από ενέργειες για την παρεμπόδιση της. Κάθε επίθεση και ο πιθανός κίνδυνος αξιολογείται. Εάν το ΣΑΕ δεν είναι σίγουρο για το πόσο επικίνδυνη είναι η επίθεση, μπορεί να μην αντιδράσει, αλλά να περιμένει για να συγκεντρώσει περισσότερες πληροφορίες και να επαναξιολογήσει την κατάσταση. Όταν αποφανθεί ότι η επίθεση είναι σοβαρή, έχει τη

δυνατότητα να αντιδράσει, π.χ. ενεργοποιώντας το firewall, με το οποίο «συνεργάζεται» για να αποτρέψει την είσοδο του επιτιθέμενου στο δίκτυο.

b. Παθητικές αντιδράσεις: Το ΣΑΕ δεν προβαίνει σε καμιά ενέργεια. Ειδοποιεί το διαχειριστή ή υπεύθυνο ασφαλείας του συστήματος ότι υπάρχει πρόβλημα. Και στην περίπτωση αυτή αξιολογείται η σοβαρότητα της επίθεσης και τα μέσα και οι τρόποι ειδοποίησης του διαχειριστή εξαρτώνται άμεσα από τον παράγοντα αυτό.

4.3.1.2 ΕΙΔΙΚΕΣ ΚΑΤΗΓΟΡΙΕΣ ΣΑΕ

Α) Συστήματα ελέγχου ακεραιότητας: Παρακολουθούν κρίσιμα αρχεία, όπως τα αρχεία συστήματος ώστε να εντοπίσουν τυχόν μεταβολές. Μπορούν επίσης να παρακολουθούν τους λογαριασμούς των χρηστών και να εντοπίζουν, εάν, κάποιος απλός χρήστης έχει αποκτήσει δικαιώματα διαχειριστή.

Β) Συστήματα παρακολούθησης αρχείων καταγραφής: Αρχικά δημιουργούν ένα φάκελο από αρχεία καταγραφής, τα οποία προέρχονται από τις υπηρεσίες του δικτύου. Στη συνέχεια, παρακολουθούν τα αρχεία, καταγράφουν τις συνηθισμένες λειτουργίες του συστήματος και βασιζόμενα σε αυτές προσπαθούν να εντοπίσουν πιθανές επιθέσεις.

Γ) Honey pots: Είναι εικονικά συστήματα τα οποία προσπαθούν να ξεγελάσουν τον επιτιθέμενο δίνοντας του την εντύπωση ότι είναι πολύ εύκολο να εισβάλει στο σύστημα. Όταν πραγματοποιηθεί η εισβολή θα έχει καταγράψει όλες τις μεθόδους και τεχνικές που χρησιμοποίησε ο επιτιθέμενος.

4.3.2 ΕΛΕΓΧΟΣ ΣΥΣΤΗΜΑΤΩΝ

Ο έλεγχος των αρχείων καταγραφής του συστήματος μπορεί να βοηθήσει στον εντοπισμό μιας επίθεσης. Σε κάθε λειτουργικό σύστημα υπάρχουν εργαλεία ελέγχου. Στις επαγγελματικές εκδόσεις των πρόσφατων λειτουργικών συστημάτων της Microsoft υπάρχουν τα ακόλουθα τρία βασικά αρχεία καταγραφής:

► Application log, τα οποία περιέχουν μηνύματα, πληροφορίες κατάστασης και άλλα γεγονότα που αναφέρονται από μη ζωτικές υπηρεσίες των Windows.

► System log, στα οποία καταγράφονται σφάλματα αρχείων, προειδοποιήσεις και γεγονότα τα οποία δημιουργούνται από το ίδιο το λειτουργικό σύστημα και σχετίζονται με υπηρεσίες του συστήματος.
► Security log , στο οποίο καταγράφονται αρχεία που σχετίζονται με την πολιτική ελέγχου που έχει καθοριστεί από το διαχειριστή του λειτουργικού συστήματος.

4.4 ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΑΤΑΣΤΡΟΦΩΝ

Στην περίπτωση που αποτύχουμε είτε να αποτρέψουμε είτε να αντιμετωπίσουμε μια επίθεση, ο επιτιθέμενος θα προκαλέσει κάποιου είδους ζημιά, όπως απώλεια δεδομένων και πληροφοριών, καταστροφή του συστήματος κ.λπ. Για τους λόγους αυτούς, είναι απαραίτητο κάθε οργανισμός αλλά και μεμονωμένος χρήστης που αποθηκεύει σημαντικά δεδομένα σε ένα υπολογιστικό σύστημα να έχει την προνοητικότητα να εξασφαλίζει ότι σε περίπτωση που δεχτεί μια επίθεση ή υποστεί τις συνέπειες μιας φυσικής καταστροφής, θα έχει εφεδρικά αρχεία των αρχείων και δεδομένων που χάθηκαν.

Για τη λήψη των εφεδρικών αντιγράφων (back-up files) χρησιμοποιούνται διάφορες τεχνικές:

1) Συστήματα ανάνηψης από καταστροφές: αποτελούν αναπόσπαστο κομμάτι της πολιτικής ασφάλειας κάθε μεγάλου οργανισμού. Αποτελείται από αρκετά υποσυστήματα τα οποία στοχεύουν στην εξασφάλιση της ακεραιότητας των δεδομένων του οργανισμού από διάφορους κινδύνους. Οι λειτουργίες ενός συστήματος εξαρτώνται από τις ανάγκες του οργανισμού. Τα κρίσιμα σημεία του σχεδιασμού του συστήματος είναι: α) Το είδος των δεδομένων που θα αποθηκευτούν. Εξαρτώνται από τις ανάγκες που θέλουμε να καλύψουμε αλλά και το κεφάλαιο που θα διαθέσουμε για την εργασία αυτή. β) Κάθε πότε θα γίνεται η αποθήκευση των δεδομένων. Εξαρτάται από το πόσο συχνά τα δεδομένα αλλάζουν, η ποσότητα των δεδομένων για τα οποία απαιτείται η λήψη εφεδρικών αντιγράφων, το χρονικό διάστημα στο οποίο μπορεί να λειτουργήσει ο οργανισμός χωρίς δεδομένα και το μέσο στο οποίο θα γίνει η αποθήκευση των εφεδρικών αντιγράφων. γ) Που θα αποθηκευτούν τα δεδομένα και η δυνατότητα τους να διατηρηθούν άλιωτα. Η αποθήκευση των δεδομένων

μπορεί να γίνει σε διάφορα μέσα, όπως μαγνητικές ταινίες, τοπικούς ή απομακρυσμένους δίσκους. Μπορεί επίσης να εγκατασταθούν εφεδρικοί υπολογιστές για την αποθήκευση των δεδομένων από τους βασικούς υπολογιστές.

2) Λήψη εφεδρικών αντιγράφων. Αν ένας οργανισμός δεν μπορεί να προμηθευτεί ένα πλήρες σύστημα ανάνηψης καταστροφών μπορεί να κρατήσει εφεδρικά αντίγραφα με τη χρήση διαφόρων εφαρμογών που κυκλοφορούν στο εμπόριο. Κάθε εφαρμογή φέρει τα δικά της χαρακτηριστικά και μπορεί να χρησιμοποιηθεί για την κάλυψη διαφόρων αναγκών. Παράλληλα, είναι δυνατή η συνέχιση των εργασιών καθ' όλη τη διάρκεια της αντιγραφής. Σε περίπτωση καταστροφής του πρωτότυπου δίσκου, γίνεται πλήρης αποκατάσταση και ο νέος δίσκος περιέχει ακριβώς τα δεδομένα που ήταν υποθηκευμένα στον παλαιό. Τη διαδικασία λήψης αντιγράφων μπορούμε να τη διακρίνουμε σε τρεις βασικές κατηγορίες: α) την πλήρη λήψη αντιγράφων, κατά την οποία λαμβάνονται εφεδρικά αντίγραφα από όλα τα αρχεία του συστήματος, β) την λήψη τροποποιημένων αντιγράφων, κατά την οποία λαμβάνονται μόνο τα αρχεία που έχουν τροποποιηθεί από την προηγούμενη χρονικά λήψη αντιγράφων και γ) λήψη διαφοροποιημένων αντιγράφων, κατά την οποία γίνεται λήψη εφεδρικών αντιγράφων των αρχείων, που έχουν διαφοροποιηθεί από την τελευταία πλήρη λήψη αντιγράφων ασφαλείας.

4.5 ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟΥ

Το ηλεκτρονικό ταχυδρομείο είναι το πιο διαδεδομένο μέσο επικοινωνίας στο Διαδίκτυο. Τα ζητήματα, ασφαλείας που σχετίζονται με το ηλεκτρονικό ταχυδρομείο ανάγονται στις έννοιες της εμπιστευτικότητας, της ακεραιότητας του μηνύματος και της αυθεντικότητας του αποστολέα. Παράλληλα το ηλεκτρονικό ταχυδρομείο γίνεται στόχος και άλλων επιθέσεων όπως άρνηση εξυπηρέτησης, η μετάδοση κακόβουλου λογισμικού, η μαζική αποστολή ανεπιθύμητων μηνυμάτων, το λεγόμενο spamming.

Για την αντιμετώπιση του προβλήματος των ιών, απαιτείται η χρήση μιας εφαρμογή antivirus, η οποία ελέγχει όλα τα εισερχόμενα και εξερχόμενα μηνύματα.

Επίσης οι χρήστες δεν πρέπει να ανοίγουν επικίνδυνα συνημμένα αρχεία (κυρίως αυτά με καταλήξεις .com, .exe, .dll, .bat) εάν δεν έχουν ελεγχθεί από το antivirus και δεν έχει εξακριβωθεί η ταυτότητα του αποστολέα.

Όσον αφορά την ενοχλητική αλληλογραφία πρέπει να μη δίνεται ποτέ σε άγνωστους δικτυακούς τόπους η ηλεκτρονική διεύθυνση και να μην απαντώνται μηνύματα τέτοιου τύπου. Στο εμπόριο κυκλοφορούν εργαλεία λογισμικού για την αντιμετώπιση του spamming σε περίπτωση ύπαρξης σοβαρού προβλήματος.

Τέλος, θα πρέπει να σημειωθεί, ότι η επικοινωνία μέσω e-mail παρέχει ελάχιστη ασφάλεια, γι' αυτό δεν πρέπει με αυτή να διακινούνται ευαίσθητα δεδομένα, όπως αριθμοί πιστωτικών καρτών και λογαριασμών. Ειδικότερα, στους λογαριασμούς web-mail το πρόβλημα ασφαλείας είναι ακόμα πιο εντονότερο, γι' αυτό προτείνεται να γίνεται σε τακτά χρονικά διαστήματα αλλαγή του κωδικού πρόσβασης. Ένας αποτελεσματικός τρόπος ασφαλούς επικοινωνίας, μέσω ηλεκτρονικής αλληλογραφίας, είναι η χρήση κρυπτογράφησης με το πρωτόκολλο SSL.

4.6 ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

Το Διαδίκτυο και ιδιαίτερα ο παγκόσμιος ιστός, έχει μεταφέρει μεγάλο μέρος των καθημερινών αγορών μας στα ηλεκτρονικά καταστήματα. Ως αποτέλεσμα, αναπτύχθηκαν μια σειρά από εργαλεία, για την πληρωμή αγαθών και υπηρεσιών μέσω του Διαδικτύου. Οι ηλεκτρονικές πληρωμές στο Διαδίκτυο πραγματοποιούνται με τη χρήση πιστωτικών ή χρεωστικών καρτών, ηλεκτρονικού χρήματος και επιταγών, αυτό μεταφοράς κεφαλαίων κ.α.

Αυτή νέα μορφή συναλλαγών γίνεται συχνά στόχος κακόβουλων επιθέσεων, και έτσι υπάρχει η ανάγκη για όσο το δυνατό ασφαλέστερα συστήματα συναλλαγών. Κύριο μέλημα, είναι η προστασία των δεδομένων των συναλλαγών (π.χ. αριθμούς πιστωτικών καρτών), που διακινούνται στο Διαδίκτυο. Για το λόγω αυτό δημιουργήθηκαν μια σειρά από πρωτόκολλα επικοινωνίας, τα οποία στοχεύουν στην προστασία των δεδομένων αυτών.

4.6.1 ΠΡΩΤΟΚΟΛΛΟ SSL

Το πρωτόκολλο SSL σχεδιάστηκε με σκοπό την ασφαλή μεταφορά των δεδομένων στο Διαδίκτυο και γενικότερα μεταξύ δύο συσκευών που είναι συνδεδεμένες στο Διαδίκτυο. Εκμεταλλεύεται τα πλεονεκτήματα της συμμετρικής και ασύμμετρης κρυπτογράφησης. Από άποψη ασφάλειας το SSL εξασφαλίζει τρεις βασικούς παραμέτρους των μεταδιδόμενων μηνυμάτων: την κρυπτογράφηση των δεδομένων, την αυθεντικοποίηση των μερών επικοινωνίας και την ακεραιότητα των μεταδιδόμενων μηνυμάτων.

Το βασικότερο μειονέκτημα του πρωτοκόλλου SSL είναι ότι δημιουργείται μεγάλος όγκος πρόσθετων δεδομένων, τα οποία και περιορίζουν την ταχύτητα μετάδοσης τους μέσω του Διαδικτύου. Για το λόγω αυτό χρησιμοποιείται μόνο σε συγκεκριμένες σελίδες ενός δικτυακού τόπου οι οποίες σχετίζονται με τα στοιχεία των συναλλαγών που χρήζουν πρόσθετης ασφάλειας.

4.6.2 ΠΡΩΤΟΚΟΛΛΟ SET

Οι μεγαλύτερες εταιρείες πιστωτικών καρτών όπως η MasterCard και Visa, έχουν αναπτύξει ένα άλλο πρωτόκολλο, το SET (Secure Electronic Transaction Standard – Πρωτόκολλο Ασφαλών Ηλεκτρονικών Συναλλαγών). Το SET επιχειρεί να εξασφαλίσει, ότι κανείς δεν θα μπορέσει να χρησιμοποιήσει ένα κλεμμένο αριθμό πιστωτικής κάρτας, αλλά και ότι ο πωλών δε θα δει ποτέ τον αριθμό αυτό και θα αρκεστεί σε μια επιβεβαίωση, ότι η κάρτα είναι εντάξει. Αμέσως οι πληροφορίες στέλνονται στην εταιρεία της κάρτας, η οποία τις αποκρυπτογραφεί και κάνει τη χρέωση.

4.7 ΑΣΦΑΛΕΙΑ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ

Οι βάσεις δεδομένων σήμερα, αποτελούν το κύριο συστατικό, σχεδόν του συνόλου των πληροφοριακών συστημάτων. Υπολογίζεται ότι το 90% των υπολογιστικών συστημάτων, που λειτουργούν παγκοσμίως, χρησιμοποιούν κάποιο σύστημα βάσεων δεδομένων. Οι απαιτήσεις ασφαλείας μιας βάσης δεδομένων δεν απέχουν και πολύ από την ασφάλεια οποιουδήποτε πληροφοριακού συστήματος. Μια βάση

δεδομένων έχει ιδιαίτερη δομή και μηχανισμούς διαχείρισης, που απαιτούν τη χρήση εξειδικευμένων και πολύπλοκων εργαλείων για να επιτευχθεί ικανοποιητικό επίπεδο ασφάλειας και τα δεδομένα που αποθηκεύονται στις βάσεις δεδομένων είναι ιδιαίτερα σημαντικά, συνήθως και ευαίσθητα, οπότε η προστασία τους αποτελεί πρωτεύον στόχο κάθε οργανισμού.

4.7.1 ΓΕΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΟΣ ΒΑΣΗΣ ΔΕΔΟΜΕΝΩΝ

Α) Φυσική ακεραιότητα της βάσης δεδομένων: αναφέρεται στη φυσική ασφάλεια της βάσης και ιδιαίτερα στην προστασία των υπολογιστικών συστημάτων, στα οποία έχει εγκατασταθεί.
Β) Λογική ακεραιότητα της βάσης δεδομένων: αναφέρεται στην εξασφάλιση της λογικής δομής της βάσης. Το πρόβλημα αυτό μπορεί να ξεπεραστεί αν εξ' αρχής γίνει σωστός σχεδιασμός. Κλασικό πρόβλημα ασφάλειας λογικής ακεραιότητας μιας βάσης έχουμε όταν η μεταβολή της τιμής ενός πεδίου επηρεάζει και τις τιμές άλλων πεδίων, χωρίς αυτό να έχει προβλεφθεί.
Γ) Ακεραιότητα των πεδίων της βάσης δεδομένων: οι τιμές των πεδίων της βάσης πρέπει να είναι σωστές.
Δ) Έλεγχος προσπέλασης: σε κάθε βάση δεδομένων υπάρχουν διάφοροι χρήστες, στον καθένα από τους οποίους εκχωρούνται συγκεκριμένα δικαιώματα χρήσης και προσπέλασης της βάσης. Ο έλεγχος προσπέλασης εγγυάται, ότι όλοι οι χρήστες της βάσης θα προσπελάσουν μόνο τα δεδομένα, για τα οποία έχουν λάβει σχετική εξουσιοδότηση.
Ε) Αυθεντικοποίηση των χρηστών: κάθε βάση δεδομένων, πριν δεχθεί ένα χρήστη, θα πρέπει να πιστοποιήσει την ταυτότητα του. Χρησιμοποιούνται κωδικοί πρόσβασης, ενώ σε εξελιγμένα συστήματα είναι δυνατή η ενσωμάτωση βιομετρικών μεθόδων.
ΣΤ) Διαθεσιμότητα: τα δεδομένα της βάσης θα πρέπει να είναι ανά πάσα στιγμή άμεσα προσπελάσιμα. Η παράμετρος αυτή είναι ιδιαίτερα σημαντική στις βάσεις δεδομένων, γιατί ενδέχεται να περιέχουν ευαίσθητα δεδομένα και απόρρητες πληροφορίες.

4.7.2 ΣΧΕΔΙΑΣΜΟΣ ΑΣΦΑΛΩΝ ΣΥΣΤΗΜΑΤΩΝ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ

Οι σημαντικότερες φάσεις, από πλευράς ασφάλειας, κατά το σχεδιασμό ενός συστήματος βάσεων δεδομένων είναι οι ακόλουθες:

Α) Προκαταρκτική ανάλυση: προσδιορίζονται οι στόχοι σχετικά με την ασφάλεια της βάσης δεδομένων και εξετάζονται οι πιθανοί κίνδυνοι.

Β) Ανάλυση απαιτήσεων ασφαλείας: προσδιορίζονται οι χρήστες της βάσης και τα δικαιώματα, που καταχωρούνται στον καθένα από αυτούς. Οι κυριότεροι παράγοντες, στη φάση αυτή, είναι το επίπεδο εξουσιοδότησης του χρήστη και ο βαθμός ευαισθησίας των δεδομένων.

Γ) Σχεδιασμός λογικού μοντέλου: καθορίζεται επακριβώς η πολιτική ασφάλειας της βάσης με τη χρήση ενός λογικού μοντέλου. Το μοντέλο αυτό περιλαμβάνει τα υποκείμενα της βάσης (π.χ. χρήστες), τα αντικείμενα (π.χ. τρόπους ενημέρωσης των δεδομένων) και τους επιτρεπόμενους τρόπους προσπέλασης της βάσης (π.χ. απαγόρευση προσπέλασης από το Διαδίκτυο).

Δ) Λογικός σχεδιασμός: είναι η ενσωμάτωση του λογικού μοντέλου στο γενικότερο μοντέλο δεδομένων, που υποστηρίζει το σύστημα βάσης δεδομένων. Κατά τον τρόπο αυτό, ο γενικότερος σχεδιασμός της βάσης δεδομένων στηρίζεται στο λογικό μοντέλο ασφαλείας.

Ε) Φυσικός σχεδιασμός: ο σχεδιαστής ασφαλείας καθορίζει τις τελευταίες λεπτομέρειες και ειδικότερα τους παραμέτρους του συστήματος, που σχεδιάζονται με την απόδοση, την αντίδραση σε περίπτωση υπερφόρτωσης, την ευελιξία και την προσαρμοστικότητα.

4.8 ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

Για την αντιμετώπιση του συνόλου των κινδύνων ασφαλείας, κάθε οργανισμός εφαρμόζει μια πολιτική ασφαλείας η οποία υλοποιεί τους στόχους ασφαλείας, που έχει θέσει η διοίκηση του οργανισμού. Η πολιτική ασφαλείας είναι το γραπτό κείμενο το οποίο καθορίζει τους κανόνες που θα πρέπει να ακολουθούνται για την ασφάλεια του πληροφοριακού συστήματος του οργανισμού από υφιστάμενους πληροφοριακούς κινδύνους.

Η σύνταξη του κειμένου αυτού πραγματοποιείται σε δύο βήματα:

1. Στο πρώτο βήμα και πριν τη σύνταξη του κειμένου της πολιτικής ασφαλείας, προσδιορίζονται οι κίνδυνοι ασφαλείας που διατρέχει ο οργανισμός.
   Ειδικότερα καθορίζεται:
   - Το είδος των κινδύνων ασφαλείας, έναντι των οποίων είναι ευάλωτος ο οργανισμός.
   - Η πιθανότητα να προκύψει ο κίνδυνος.
   - Το κόστος, που θα έχει ο οργανισμός σε περίπτωση, που αυτός πραγματοποιηθεί.
2. Στο δεύτερο βήμα γίνεται η σύνταξη του κειμένου της πολιτικής ασφάλειας. Το άτομο που θα αναλάβει αυτή τη διαδικασία εκτός από εμπειρία θα πρέπει να ακολουθήσει κάποιους βασικούς κανόνες. Κατ' αρχής το κείμενο θα πρέπει να χωρίζεται σε δύο βασικά έγγραφα: το πρώτο περιγράφει τις γενικές πολιτικές, οι οποίες σπάνια αλλάζουν, ενώ το δεύτερο περιγράφει συγκεκριμένες διαδικασίες οι οποίες αλλάζουν πιο συχνά. Πολύ σημαντικό είναι η γλώσσα γραφής να είναι απλή χωρίς ειδικευμένους τεχνικούς όρους.

4.8.1 ΒΑΣΙΚΗ ΔΟΜΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Α) Γενική πολιτική ασφάλειας: περιλαμβάνονται οι γενικές αρχές για την ασφάλεια του οργανισμού και καθορίζονται οι στρατηγικοί στόχοι, αλλά και οι πόροι για την επίτευξη τους.
Β) Ειδικούς σκοπούς και επιμέρους πολιτικές: γίνεται διαχωρισμός της γενικής πολιτικής ασφαλείας του οργανισμού σε επιμέρους πολιτικές π.χ. ασφάλεια δικτύων, χρηστών, ηλεκτρονικής αλληλογραφίας, φυσικής ασφάλειας κ.λπ.
Γ) Διαδικασίες ασφάλειας: περιγράφεται ο τρόπος υλοποίησης της πολιτικής ασφαλείας που έχει θέσει ο οργανισμός. Το κείμενο αναλύει, με λεπτομέρεια, τι πρέπει να γίνει σε συγκεκριμένες περιπτώσεις. Παράλληλα, καθορίζονται οι ρόλοι, τα δικαιώματα και οι υποχρεώσεις του κάθε χρήστη, όσον αφορά στα θέματα ασφαλείας.
Δ) Οδηγίες ασφαλείας και τεχνικά εγχειρίδια: παρέχεται ακόμη πιο λεπτομερής περιγραφή, ειδικότερες οδηγίες και κατευθύνσεις για πάσης φύσεως θέματα, κυρίως τεχνικής φύσεως, π.χ. εγχειρίδιο ρυθμίσεων του firewall, του web server κ.λπ.

4.9 ΣΥΜΒΟΥΛΕΣ ΠΡΟΣ ΤΟΥΣ ΧΡΗΣΤΕΣ

Συμβουλές για τους γονείς

► Ενημερώστε τα παιδιά σας

- για τους κινδύνους όταν συνομιλούν μα αγνώστους στο διαδίκτυο
- να μην δίνουν προσωπικές τους πληροφορίες
- να αρνούνται να συναντηθούν προσωπικά με άτομα που έχουν γνωρίσει στο Διαδίκτυο

► Έλεγχος

- Τοποθετήστε τον Η/Υ σας σε χώρους, όπου έχετε τη δυνατότητα να επιβλέπεται
- Κάντε την πλοήγηση στο Διαδίκτυο μια οικογενειακή δραστηριότητα
- Χρησιμοποιείστε ειδικά φίλτρα προστασίας
- Ελέγξτε το οπτικοακουστικό υλικό, που αγοράζουν τα παιδιά σας ή ανταλλάσσουν με τους φίκους τους.

Συμβουλές για ασφαλείς οικονομικές συναλλαγές

► Μην πραγματοποιείται οικονομικές συναλλαγές από υπολογιστές στους οποίους έχουν πολλά άτομα πρόσβαση

► Προστατέψτε τους κωδικούς πρόσβασης που χρησιμοποιείται για τις δικτυακές συναλλαγές

► Κάντε αγορές μόνο από γνωστές εταιρείες

► Διατηρείστε την ασφάλεια του υπολογιστή σας

► Να ενημερώνεστε για τους λογαριασμούς σας και να φροντίζεται για την ασφάλεια των προσωπικών σας στοιχείων και εγγράφων

Συμβουλές για τους χρήστες ΑΤΜ

► Πριν ξεκινήσετε τη συναλλαγή ελέγξτε προσεκτικά το χώρο γύρω σας για τυχόν ύποπτες κινήσεις

► Μην επιτρέπεται σε άγνωστα άτομα να σας πλησιάσουν κατά τη διάρκεια της συναλλαγής

► Βεβαιωθείτε ότι δεν υπάρχει κάποιο πρόσθετο εξάρτημα στο ΑΤΜ

► Αν παρουσιαστεί οποιαδήποτε βλάβη, π.χ. εμπλοκή κάρτας επικοινωνήστε μόνο με τα τηλέφωνα της τράπεζας

● Μην εμπιστεύεστε αγνώστους που προθυμοποιούνται να σας βοηθήσουν

► Όταν πληκτρολογείτε τον κωδικό PIN «προστατέψτε» το πληκτρολόγιο

Προστασία από το SPAM

► Να μην απαντάτε ποτέ σ' ένα spam e-mail

► Αναζητήστε και εγκαταστήστε ειδικά προγράμματα και φίλτρα που μπλοκάρουν τα spam e-mail

► Να μην παρασύρεστε ποτέ από δελεαστικούς τίτλους

► Να μην δίνεται εύκολα τη διεύθυνση του ηλεκτρονικού σας ταχυδρομείου (e-mail)

● Να έχετε μια πρόχειρη διεύθυνση για τα SPAM

Το Computer Ethics Institute στις ΗΠΑ σχεδίασε μια σειρά από απλές εντολές προς το χρήστη, τις «Δέκα Εντολές του Χρήστη»: «Δεν πρέπει να…

1. Χρησιμοποιείς τον υπολογιστή για να κάνει κακό σε άλλους ανθρώπους.
2. Παρεμβαίνεις στην με υπολογιστή εργασία των άλλων.
3. «Κάνεις βόλτες» στα αρχεία των άλλων.
4. Χρησιμοποιείς τον υπολογιστή για να κλέβεις.
5. Χρησιμοποιείς τον υπολογιστή για να γίνεις ψευδομάρτυρας (αλλοίωση στοιχείων).
6. Αντιγράφεις ή να χρησιμοποιείς λογισμικό για το οποίο δεν έχεις πληρώσει.
7. Χρησιμοποιείς χωρίς εξουσιοδότηση ή αποζημίωση τους πόρους των άλλων.
8. Ιδιοποιείσαι παράνομα το πνευματικό έργο των άλλων.
9. Σκέψου τις κοινωνικές συνέπειες των προγραμμάτων που δημιουργείς ή του συστήματος που σχεδιάζεις.
10. Θα πρέπει να χρησιμοποιείς τον υπολογιστή με τρόπο που να διασφαλίζεται το ενδιαφέρον και ο σεβασμός για τους συνανθρώπους σου.

Αν παρά τα προληπτικά μέτρα γνώσης και ευαισθητοποίησης, καταναλωτής, γονέας ή ένωση καταναλωτών τυχόν διαπιστώσουν ότι δεν τηρείται από κάποιον πάροχο υπηρεσιών οποιαδήποτε από τις αρχές ασφαλείας ως προς το περιεχόμενο, τη διαφήμιση, τη χρέωση, την πρόσβαση στην υπηρεσία, την προστασία προσωπικών δεδομένων κ.ο.κ., μπορούν να πράξουν τα εξής:

● Να επικοινωνήσουν με τον πάροχο υπηρεσιών διαδικτύου καταγγέλλοντας το περιστατικό και ζητώντας τις διευθύνσεις αποστολής των μηνυμάτων.
● Να αναστείλουν την πρόσβαση στον υπολογιστή και να ειδοποιήσουν αμέσως την αστυνομία και τις αρμόδιες διωκτικές αρχές.
● Να ειδοποιήσουν την Ομάδα Ψηφιακής Ασφάλειας με το ακρωνύμιο D.A.R.T (Digital Awareness & Response to Threats) στην ηλεκτρονική διεύθυνση http://www.dart.gov.gr. Πρόκειται για μια κοινή προσπάθεια των συναρμόδιων φορέων, όπως η Αρχή Διασφάλισης Απορρήτου Επικοινωνίας (ΑΔΑΕ), η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) και το Σώμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας, με στόχο την αντιμετώπιση κινδύνων από χρήση τεχνολογίας ηλεκτρονικών επικοινωνιών.
● Να καταθέσουν αναφορά-καταγγελία στον Συνήγορο του Καταναλωτή, ο οποίος είτε θα την εξετάσει ο ίδιος, αν εμπίπτει στην αρμοδιότητα του, καλώντας σε ακρόαση τα εμπλεκόμενα μέρη, όταν αυτό είναι εφικτό, είτε θα τη διαβιβάσει στα αρμόδια διωκτικά όργανα και ανεξάρτητες διοικητικές αρχές.

Ο τρόπος υποβολής καταγγελίας στον Συνήγορο του Καταναλωτή είναι ο ακόλουθος: α) Τηλεφωνικά στους αριθμούς: 210 6460814, 210 6460284, 210 6460276, β) Μέσω συμπλήρωσης και υποβολής, με αυτοπρόσωπη παρουσία, με συστημένη επιστολή, τηλεομοιοτυπία ή μήνυμα ηλεκτρονικού ταχυδρομείου, της έντυπης φόρμας υποβολής παραπόνων που διατίθεται από τον διαδικτυακό τόπο του Συνηγόρου του Καταναλωτή http://www.synigoroskatanaloti.gr.

Στο κεφάλαιο αυτό μελετήθηκε διεξοδικά το θέμα της ασφάλειας. Υπάρχουν πολλοί τεχνικές όπως διαδικασίες αυθεντικοποίησης, κωδικοί πρόσβασης, βιομετρικές τεχνικές, λογισμικά ασφαλείας, firewalls και κρυπτογραφία που μπορεί και πρέπει να εφαρμόζει κάθε οργανισμός και κάθε μεμονωμένος χρήστης ώστε να εξασφαλίσει την ασφάλεια του συστήματος και των δεδομένων του από διάφορες απειλές. Επίσης υπάρχουν πολιτικές ασφαλείας που εφαρμόζει κάθε εταιρεία για την ασφάλεια του. Παρόλα αυτά πολλές φορές παρά τα μέτρα προστασίας που λήφθηκαν μπορεί κάποιος εγκληματίας να καταφέρει να επέμβει στο σύστημα και να διαπράξει τις κακόβουλες ενέργειες του. Το άτομο αυτό διώκεται από το νόμο. Στο επόμενο κεφάλαιο θα μελετήσουμε τη νομοθεσία που διέπει το ηλεκτρονικό έγκλημα.

ΚΕΦΑΛΑΙΟ 5
ΝΟΜΟΘΕΣΙΑ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Στο κεφάλαιο αυτό στόχος είναι η παρουσίαση των προβλημάτων σχετικά με τη νομοθεσία και την δίωξη του ηλεκτρονικού εγκλήματος και θα γίνει μια νομική προσέγγιση του Διαδικτύου. Επίσης θα δούμε της Νομοθεσίας γύρο από το ηλεκτρονικό έγκλημα τόσο στην Ελλάδα τόσο και σε παγκόσμιο επίπεδο.

5.1 ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΝΟΜΟΘΕΣΙΑΣ

Η προσέγγιση των νομικών θεμάτων που αφορούν το ηλεκτρονικό έγκλημα είναι δύσκολη γιατί προϋποθέτει όχι μόνο νομικές αλλά και τεχνικές γνώσεις. Το ηλεκτρονικό έγκλημα φέρει κάποια ιδιαίτερα χαρακτηριστικά, που το διαφοροποιούν από το συμβατικό έγκλημα. Το πρόβλημα της νομοθεσίας επικεντρώνεται στην διαμόρφωση της κατάλληλης ορολογίας αλλά και την ειδικών νομοθετικών ρυθμίσεων, με βάση των χαρακτηριστικών του, για την εφαρμογή του Ποινικού και Δικονομικού Δικαίου, καθώς και σε θέματα που αφορούν τη διεθνή συνεργασία, όπως η διεθνής δικαιοδοσία. Όλα αυτά πολλές φορές καθιστούν αδύνατη τη δίωξη του.

Έως σήμερα, οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα προέρχονται κυρίως από την τεχνολογία. Ο τεχνικός λόγω έλλειψης νομικών γνώσεων, προσδιορίζει τους όρους με βάση τις επιστημονικές γνώσεις και τα τεχνολογικά χαρακτηριστικά κάθε αντικειμένου. Για τον νομικό, κάθε έννοια έχει το περιεχόμενο εκείνο που με ακρίβεια καθορίζει ο νόμος. Στην περίπτωση που δεν υπάρχει νόμος ερευνάται η σχετική νομολογία και αν δεν υπάρχει νομολογία, η ανάλυση γίνεται με τους γενικούς κανόνες του ισχύοντος δικαίου για να βρεθεί κάποια θεωρητική λύση του ζητήματος. Στην πράξη ο νομοθέτης αποφεύγει να δημιουργήσει ειδική ορολογία για το ηλεκτρονικό έγκλημα και δανείζεται τη χρησιμοποιούμενη από την τεχνολογία η οποία μπορεί να είναι ασαφής, γενική, αόριστη ή ελλιπής και έτσι να εμποδίζει την ορθή απονομή δικαιοσύνης.

Για την αντιμετώπιση του ηλεκτρονικού εγκλήματος δεν αρκεί μόνο ειδική νομοθεσία, αλλά απαιτείται συνεχής ενημέρωση της, λαμβάνοντας υπόψη τις τεχνολογικές εξελίξεις. Επιπλέον, σε ένα άρτιο σύστημα απονομής δικαιοσύνης, όλοι όσοι εμπλέκονται στη δίωξη του ηλεκτρονικού εγκλήματος όπως αστυνομικοί, εισαγγελέας, δικαστές και δικηγόροι πρέπει να κατέχουν τόσο νομικές όσο και τεχνικές γνώσεις για τη νέα μορφή εγκληματικής δραστηριότητας.

Τέλος τα σημαντικότερα νομοθετικά προβλήματα για το ηλεκτρονικό έγκλημα οφείλονται στον παγκόσμιο χαρακτήρα του. Ο τόπος διάπραξης των συμβατικών εγκλημάτων, προσδιορίζεται από ένα συγκεκριμένο γεωγραφικό χώρο. Στα ηλεκτρονικά εγκλήματα, ο τόπος διάπραξης πολλές φορές είναι αδύνατο να προσδιοριστεί, οι συνέπειες της εγκληματικής συμπεριφοράς μπορεί να είναι ορατές σε περισσότερες από μια χώρες στις οποίες ισχύει διαφορετικό νομικό πλαίσιο. Η δικαιοδοσία, η συνεργασία μεταξύ των κρατών σε διεθνείς έρευνες ηλεκτρονικών εγκλημάτων και η διαδικασία έκδοσης όσων έχουν διαπράξει ηλεκτρονικά εγκλήματα με εθνικό χαρακτήρα, είναι μερικά μόνο από τα ζητήματα που επιτείνουν τους νομικούς προβληματισμούς.

5.2 ΝΟΜΟΘΕΤΙΚΟΙ ΠΡΟΒΛΗΜΑΤΙΣΜΟΙ

5.2.1 ΝΟΜΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Βασικό ζήτημα για την αντιμετώπιση του ηλεκτρονικού εγκλήματος, αποτελεί η νομική ρύθμιση του Διαδικτύου. Έως σήμερα δεν υπάρχουν συγκεκριμένες διατάξεις που να ρυθμίζουν συνολικά τις υπηρεσίες που προσφέρει το Διαδίκτυο. Οποιαδήποτε προσπάθεια ρύθμισης συναντά φραγμούς λόγω δύο αντιμαχόμενων παρατάξεων από την μια αυτών που είναι υπέρ και αυτών που είναι κατά της ρύθμισης του Διαδικτύου.

Τα επιχειρήματα υπέρ της ρύθμισης του Διαδικτύου είναι τα ακόλουθα:

- Το Διαδίκτυο είναι ανοιχτό σε όλους και απαιτείται η ρύθμιση του για τον έλεγχο του παράνομου περιεχομένου του.
- Δεν αποτελεί διαφορετικό μέσο επικοινωνίας, σε σχέση με το ραδιόφωνο και την τηλεόραση, τα οποία υπόκεινται ήδη σε νομοθετικές ρυθμίσεις.

● Υπάρχει πολύ επιβλαβές υλικό σε αυτό, όπως και αυξανόμενη εγκληματική δραστηριότητα, που γεννά την υποχρέωση στην πολιτεία για τον έλεγχο και την αντιμετώπιση της.
● Οι περισσότεροι χρήστες, απαιτούν κάποια μορφή ρύθμισης για την προστασία των δεδομένων τους και των περιουσιακών δικαιωμάτων τους, έναντι επιθέσεων κακόβουλων χρηστών.

Τα επιχειρήματα εναντίον οποιασδήποτε ρύθμισης του Διαδικτύου είναι τα ακόλουθα:
● Η ελευθερία του λόγου που προσφέρεται μέσω του Διαδικτύου είναι απόλυτο δικαίωμα κάθε πολίτη, προστατευμένο από συνταγματικές διατάξεις.
● Το Διαδίκτυο είναι διαφορετικό από τα άλλα μέσα επικοινωνίας, διαθέτει ιδιαίτερα χαρακτηριστικά όπως η ελευθερία, η ειλικρίνεια και ο πειραματισμός.
● Το Διαδίκτυο δεν μπορεί να ρυθμιστεί, διότι είναι τεράστιο και παγκόσμιο και οποιαδήποτε προσπάθεια, θα έρχεται πάντα αντιμέτωπη με το ζήτημα της λογοκρισίας.
● Οι γονείς είναι υπεύθυνοι για να προστατεύσουν τα παιδιά από το παράνομο περιεχόμενο του Διαδικτύου και όχι τα κράτη με νομοθετικές ρυθμίσεις.

5.2.2 Ο ΠΑΓΚΟΣΜΙΟΣ ΧΑΡΑΚΤΗΡΑΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Το κύριο χαρακτηριστικό γνώρισμα του ηλεκτρονικού εγκλήματος είναι ο παγκόσμιος χαρακτήρας του και το γεγονός ότι έχει υπερβεί τα στενά γεωγραφικά όρια των κρατών. Σε νομοθετικό επίπεδο, η παγκοσμιότητα του δημιουργεί μια σειρά από ερωτήματα. Τι γίνεται όταν ένα έγκλημα διαπράττεται σε δύο ή περισσότερες χώρες ταυτόχρονα, στις οποίες ισχύει διαφορετικό νομικό πλαίσιο ή όταν σε μια από τις χώρες αυτές δεν υπάρχει καθόλου νομοθετικό πλαίσιο για τη συγκεκριμένη συμπεριφορά; Σε περίπτωση διεθνών ερευνών για ένα ηλεκτρονικό έγκλημα, πως θα γίνουν οι απαραίτητες ενέργειες σε μια χώρα που δεν διαθέτει νομοθεσία;

Οι νομοθετικές παρεμβάσεις συγκεκριμένων κρατών για την αντιμετώπιση των προβλημάτων αυτών δεν επαρκούν. Απαιτείται πρωταρχικά εναρμόνιση της διεθνούς νομοθεσίας σχετικά με το ηλεκτρονικό έγκλημα, μέσω συμβάσεων ή

άλλων επίσημων εγγράφων. Η διαδικασία αυτή, είναι ιδιαίτερα πολύπλοκη. Ενδεικτικά, αναφέρεται ότι σε κάποιες χώρες δεν έχει καν φθάσει η τεχνολογία των υπολογιστών και του Διαδικτύου, ενώ το ηλεκτρονικό έγκλημα, όπως και πολλές άλλες μορφές εγκλήματος, αντιμετωπίζεται με διαφορετικό τρόπο σε κάθε χώρα, ανάλογα με το συγκεκριμένο κοινωνικοπολιτιστικό καθεστώς, τα ήθη, τα έθιμα και τις παραδόσεις κάθε λαού.

5.2.3 ΤΟ ΖΗΤΗΜΑ ΤΗΣ ΔΙΚΑΙΟΔΟΣΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Ο όρος δικαιοδοσία αναφέρεται στην αρμοδιότητα ενός δικαστηρίου να δικάσει μια συγκεκριμένη υπόθεση, καθώς και στην αρμοδιότητα των διωκτικών αρχών να διερευνήσουν μια εγκληματική συμπεριφορά. Τα κριτήρια με τα οποία καθορίζεται η δικαιοδοσία ποικίλουν. Συνήθως, η δικαιοδοσία προσδιορίζεται από γεωγραφικά κριτήρια, σύμφωνα με τα οποία ένα κράτος έχει απόλυτη δικαιοδοσία για εγκλήματα που διαπράττονται εντός των γεωγραφικών του ορίων, ή εθνικά κριτήρια, όπου ένα κράτος έχει απόλυτη δικαιοδοσία για τα εγκλήματα που τελούνται από τους πολίτες του (πηγή: Shinder, 2002:626).

Στο χώρο του Διαδικτύου, το ζήτημα περιπλέκεται. Με τη χρήση του Η/Υ, ένα άτομο που βρίσκεται σε οποιοδήποτε σημείο του κόσμου, μπορεί να διαπράξει ένα έγκλημα στην Αμερική. Επομένως, στον κυβερνοχώρο η έννοια της γεωγραφικής κυριαρχίας δεν μπορεί να τύχει εφαρμογής. Οι διακινούμενες πληροφορίες μέσω του Παγκόσμιου Ιστού και άλλων υπηρεσιών του Διαδικτύου δεν στοχεύουν σε ένα συγκεκριμένο αποδέκτη, αλλά διανέμονται ταυτόχρονα σε ένα παγκόσμιο κοινό, επηρεάζοντας μεμονωμένα άτομα και οργανισμούς, που ανήκουν σε διαφορετικές δικαιοδοσίες και υπάγονται σε εντελώς διαφορετικό νομικό πλαίσιο (πηγή: Lakshminarayen, 2001).

Μπορούμε να θεωρήσουμε, ότι το ζήτημα της δικαιοδοσίας στο Διαδίκτυο, καθορίζεται από τρεις διαφορετικές νομικές πηγές:

1) Ισχύουν οι εθνικές νομοθεσίες, οι οποίες καθορίζουν κάποιους βασικούς κανόνες.
2) Υπάρχουν διεθνείς συμφωνίες οι οποίες προσπαθούν να ρυθμίσουν το θέμα της δικαιοδοσίας σε πολυεθνικό επίπεδο.

3) Υπάρχουν οι αποφάσεις των δικαστηρίων. Η νομολογία αυτή έχει ιδιαίτερη βαρύτητα, καθότι σε αυτή εφαρμόζεται η ισχύουσα νομοθεσία ενώ μέσα από τις δικαστικές αποφάσεις, εντοπίζονται προβλήματα, αλλά και παρουσιάζονται ερμηνείες του υφιστάμενου νομοθετικού πλαισίου, που ο νομοθέτης δεν είχε υπ' όψη του.

Το Κριτήριο των επιπτώσεων

Ο Jones διάσημος ηθοποιός που ζούσε και εργαζόταν στην Καλιφόρνια, υπέβαλε μήνυση στο δικαστήριο της Καλιφόρνια εναντίον των Calder εκδότη του περιοδικού National Enquirer και Smith συντάκτη, οι οποίοι δημοσίευσαν ένα άρθρο το οποίο δυσφημούσε το Jones. Τα παραπάνω πραγματοποιήθηκαν στην Πολιτεία της Φλόριντας. Το περιοδικό όμως είχε τη μεγαλύτερη κυκλοφορία στην Καλιφόρνια. Το δικαστήριο εξετάζοντας τη μήνυση, έκρινε ότι υφίσταται προσωπική δικαιοδοσία για τους Calder και Smith, οι οποίοι κλήθηκαν στο δικαστήριο της Καλιφόρνια, για να αποδείξουν την αλήθεια των ισχυρισμών τους. Ο δικαστής στήριξε την απόφαση του στο ότι οι επιπτώσεις της δημοσίευσης του άρθρου στην Καλιφόρνια ήταν σημαντικές και έβλαπταν την τιμή και την υπόληψη του Jones.

Το Κριτήριο της υπόθεσης Zippo

Η Zippo, διατηρούσε ένα δικτυακό τόπο στην Καλιφόρνια, μέσω του οποίου επιχειρούσε ηλεκτρονικές επικοινωνίες για διαφημιστικούς σκοπούς, με πάνω από 3000 κατοίκους της Πενσυλβλάνια. Το δικαστήριο, λαμβάνοντας υπόψη ότι μεταξύ του δικτυακού τόπου και των χρηστών του υπήρχε μεγάλος βαθμός διαδραστικότητας, αποφάσισε ότι έχει τη δικαιοδοσία να δικάσει την υπόθεση. Το κριτήριο, λοιπόν, για τη στήριξη της δικαιοδοσίας είναι το πόσο διαδραστικός τόπος ήταν διαδραστικός ή παθητικός.

Στην Ευρωπαϊκή Ένωση, η δικαιοδοσία δεν αφήνετε στην κρίση των δικαστηρίων, αλλά βασίζεται σε συγκεκριμένη νομοθεσία. Το βασικό νομοθετικό κείμενο για τον προσδιορισμό της δικαιοδοσίας είναι η Συνθήκη των Βρυξελλών (1968), η οποία θέτει τους ακόλουθους βασικούς κανόνες (πηγή: Clandstone, 2003):

1) Ένα άτομο που ζει μόνιμα σε κάποιο κράτος-μέλος της Ευρωπαϊκής Ένωσης, μπορεί να ενταχθεί σ' αυτό.

2) Σε υποθέσεις παραβίασης συμβατικής υποχρέωσης, ένα άτομο μπορεί να ενταχθεί στον τόπο, όπου έλαβε χώρα η υποχρέωση, που τίθεται από αμφισβήτηση.
3) Σε αστικά ζητήματα, ένα άτομο μπορεί να ενταχθεί στον τόπο, όπου έλαβε χώρα το ζημιογόνο αποτέλεσμα.
4) Ένας καταναλωτής, μπορεί να ενταχθεί μόνο στο τόπο που ζει μόνιμα, μπορεί να επιλέξει τη μεταφορά της υπόθεσης στον τόπο μόνιμης κατοικίας του αντιδίκου, εφόσον σε αυτόν υπέστη μεγαλύτερη ζημιά.
5) Σε συμβάσεις, που δεν εμπλέκεται μόνο ένας καταναλωτής, οι αντίδικοι μπορούν να συμφωνήσουν για τον τόπο εκδίκασης της υπόθεσης.

Υπόθεση Yahoo!

Δύο οργανισμοί στην Γαλλία υπέβαλαν αγωγή εναντίον της εταιρείας Yahoo!, επειδή μέσω του δικτυακού της τόπου διενεργούσε on-line δημοπρασίες, στις οποίες εμφανίζονταν και ήταν διαθέσιμο προς πώληση προπαγανδιστικό υλικό για τους Ναζί. Η πρόσβαση ήταν διαθέσιμη μόνο μέσω του Yahoo.com, στην αγγλική γλώσσα και όχι μέσω του Yahoo.fr. Η Yahoo!, ισχυρίστηκε ενώπιον του γαλλικού δικαστηρίου, ότι δεν είχε δικαιοδοσία να δικάσει την υπόθεση. Ο ισχυρισμός αυτός απορρίφθηκε από το γαλλικό δικαστήριο το οποίο υποχρέωσε την εταιρεία Yahoo! Να τοποθετήσει φίλτρα, προκειμένου οι Γάλλοι πολίτες να μην έχουν πρόσβαση στις συγκεκριμένες σελίδες, αλλιώς θα έπρεπε να πληρώσει πρόστιμο 13000 δολάρια για κάθε μέρα που περνά χωρίς να τοποθετηθούν τα φίλτρα.

Η εταιρεία Yahoo! Υποστήριξε(και δικαίως) ότι μια τέτοια απόφαση εφόσον εφαρμοστεί ευρέως θα προκαλούσε τεράστια προβλήματα σε εταιρείες που διαθέτουν κάθε υλικό στο Διαδίκτυο το οποίο μπορεί σε κάποια χώρα να θεωρείται νόμιμο και σε κάποια άλλη παράνομο. Οπότε, η Yahoo! απευθύνθηκε στο δικαστήριο της Καλιφόρνια, ζητώντας να αποφανθεί ότι η απόφαση του Γαλλικού δικαστηρίου δεν μπορεί να τύχει εφαρμογής στις Ηνωμένες Πολιτείες. Το δικαστήριο της Βόρειας Καλιφόρνια κατέληξε στο συμπέρασμα ότι η απαγόρευση που επιβλήθηκε από το Γαλλικό Δικαστήριο στη Yahoo!, παραβίαζε την ελευθερία του λόγου, σύμφωνα με τις συνταγματικές επιταγές και αποφάνθηκε, τελικά, ότι η απόφαση του δεν μπορεί να εφαρμοσθεί στις Η.Π.Α.

Η περίπτωση αυτή καταδεικνύει το μεγάλο νομικό χάσμα που υφίσταται μεταξύ των κρατών στο ζήτημα της δικαιοδοσίας.

5.3 ΠΑΓΚΟΣΜΙΑ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

5.3.1 ΗΝΩΜΕΝΕΣ ΠΟΛΙΤΕΙΕΣ ΤΗΣ ΑΜΕΡΙΚΗΣ

Το πρώτο νομοθέτημα σχετικά με το ηλεκτρονικό έγκλημα θεσπίστηκε στις Ηνωμένες Πολιτείες της Αμερικής το 1984. Ο νόμος περιοριζόταν, στην προστασία κρατικών υπολογιστικών συστημάτων από μη εξουσιοδοτημένη πρόσβαση, με σκοπό την απόκτηση απόρρητων πληροφοριών που θα μπορούσαν να βλάψουν τις ΗΠΑ. Η πρώτη αναθεώρηση έγινε το 1986 όπου χρησιμοποιήθηκε πιο σαφής ορολογία ενώ διαφαίνεται και η πρώτη προσπάθεια αντιμετώπισης περιπτώσεων άρνησης εξυπηρέτησης με τη φράση «εμποδίζει την εξουσιοδοτημένη χρήση ενός υπολογιστή». Και πάλι, όμως, η συγκεκριμένη τροποποίηση αναφέρεται μόνο σε κρατικά υπολογιστικά συστήματα. Η πιο σημαντική τροποποίηση έγινε το 1994, με τρεις αλλαγές. Το νομοθετικό πλαίσιο επεκτάθηκε και σε ηλεκτρονικούς υπολογιστές, που χρησιμοποιούνται στο διαπολιτειακό εμπόριο, αφαιρέθηκε ο όρος «μη εξουσιοδοτημένη πρόσβαση», που σημαίνει ότι οι υπάλληλοι εταιρειών και οι εξουσιοδοτημένοι χρήστες θα μπορούσαν να διωχτούν και πλέον συγκεκριμένες μορφές σκόπιμων και σκόπιμων ενεργειών θεωρούνται παράνομες, όπως η διασπορά κακόβουλου λογισμικού και οι επιθέσεις άρνησης εξυπηρέτησης. Τέλος το 1996 συμπληρώθηκε ο νόμος με τη National Information Infrastructure Protection Act (NIIPA) και αναφέρεται στους προστατευμένους υπολογιστές. Η πιο σημαντική διάταξη του νομοθετήματος αυτού προβλέπει ότι κάθε μεμονωμένος χρήστης που εισέρχεται σε ένα προστατευμένο υπολογιστή, είναι υπεύθυνος όχι μόνο για τις πράξεις του αλλά και για τις συνέπειες αυτών, εάν η πρόσβαση είναι εξουσιοδοτημένη, είναι ποινικά υπεύθυνος μόνο εάν έχει πρόθεση να προξενήσει ζημιά στο θύμα.

5.3.2 ΑΥΣΤΡΑΛΙΑ

Ο νόμος «Crime Act 1914» προβλέπει τέσσερις βασικές μορφές ηλεκτρονικού εγκλήματος: α) παράνομη πρόσβαση σε δεδομένα αποθηκεμένα σε κρατικό

ηλεκτρονικό υπολογιστή, β) καταστροφή δεδομένων αποθηκευμένων σε κρατικό ηλεκτρονικό υπολογιστή, γ) πρόσβαση σε δεδομένα αποθηκευμένα σε ηλεκτρονικό υπολογιστή χρησιμοποιώντας μέσα κρατικής διευκόλυνσης και δ) καταστροφή δεδομένων σε ηλεκτρονικό υπολογιστή χρησιμοποιώντας μέσα κρατικής διευκόλυνσης.

Σήμερα ισχύει ο νόμος The Cybercrime Act 2001 ο οποίος προήλθε από την τροποποίηση του νόμου Crime Act 2001 και του Ποινικού Κώδικα που ψηφίστηκε το 1995 και προβλέπει τρεις βασικές κατηγορίες ηλεκτρονικών εγκλημάτων: α) μη εξουσιοδοτημένη πρόσβαση, μετατροπή και φθορά δεδομένων, με σκοπό τη διάπραξη σοβαρού εγκλήματος. Στην περίπτωση αυτή, η ποινή είναι ισοδύναμη της αντίστοιχης που επιβάλλεται στο συμβατικό έγκλημα, β) μη εξουσιοδοτημένη τροποποίηση δεδομένων, που οδηγεί σε φθορά δεδομένων, γ) μη εξουσιοδοτημένη φθορά ηλεκτρονικών επικοινωνιών, για την οποία προβλέπεται ποινή έως δέκα ετών.

Παράλληλα, ο νόμος δημιούργησε τέσσερις νέες μορφές εγκλημάτων: α) μη εξουσιοδοτημένη πρόσβαση ή μετατροπή προστατευμένων δεδομένων, β) παράνομη καταστροφή δεδομένων αποθηκευμένων σε δίσκους Η/Υ, γ) κατοχή ή έλεγχος δεδομένων, με σκοπό την διάπραξη ηλεκτρονικών αδικημάτων, δ) παραγωγή, προμήθεια ή απόκτηση δεδομένων, με σκοπό τη διάπραξη ηλεκτρονικού εγκλήματος.

5.3.3 ΑΓΓΛΙΑ

Το πρώτο νομοθέτημα για το ηλεκτρονικό έγκλημα ψηφίστηκε το 1990. Είναι ο νόμος «Computer Misuse Act» ένα από τα πλέον σημαντικά νομοθετικά κείμενα για το ηλεκτρονικό έγκλημα. Διακρίνει τρεις βασικές κατηγορίες αδικημάτων, που σχετίζονται με ηλεκτρονικό υπολογιστή: α) μη εξουσιοδοτημένη πρόσβαση, σε πληροφορίες που είναι αποθηκευμένες σε ηλεκτρονικό υπολογιστή, β) μη εξουσιοδοτημένη πρόσβαση με σκοπό τη διάπραξη αδικημάτων, γ) μη εξουσιοδοτημένη τροποποίηση πληροφοριών, αποθηκευμένων σε υπολογιστικό σύστημα. Στο νομοθέτημα περιλαμβάνονται διατάξεις σχετικά με τη δικαιοδοσία και τον τρόπο απονομής της δικαιοσύνης, όσο αφορά στα ηλεκτρονικά εγκλήματα.

5.3.4 ΑΡΓΕΝΤΙΝΗ

Δεν υφίσταται συγκεκριμένο νομοθετικό πλαίσιο για το ηλεκτρονικό έγκλημα. Η ποινική αντιμετώπιση των εγκλημάτων της μορφής αυτής προέρχεται από τον Ποινικό Κώδικα, ο οποίος δεν περιλαμβάνει συγκεκριμένες διατάξεις για τη δίωξη αδικημάτων, που τελούνται με τη χρήση υπολογιστών και Διαδικτύου. Τα εγκλήματα αυτά είναι δυνατόν να διωχτούν μόνο με διασταλτικές ερμηνείες των ισχυουσών διατάξεων.

5.3.5 ΚΙΝΑ

Αντιμετωπίζει το ηλεκτρονικό έγκλημα με ειδική νομοθεσία που έχει θεσπίσει για το σκοπό αυτό. Καθιστά παράνομη οποιαδήποτε δραστηριότητα σχετίζεται με τη διασπορά ιών ή άλλου είδους «κακόβουλου» λογισμικού, σε ηλεκτρονικούς υπολογιστές. Επίσης, παράνομη είναι η πώληση συστημάτων προστασίας υπολογιστών χωρίς άδεια. Το ζήτημα της πορνογραφίας αντιμετωπίζεται με την υπάρχουσα νομοθεσία.

Εξαιρετικό ενδιαφέρον παρουσιάζουν ορισμένες διατάξεις της νομοθεσίας στην Κίνα, τις οποίες δεν συναντάμε σε άλλες χώρες. Για παράδειγμα, θεωρείται παράνομη η δημιουργία, αναπαραγωγή, ανάκτηση και διάδοση πληροφοριών, που μπορούν να βλάψουν την εθνική ενότητα. Επίσης απαγορεύεται η παραποίηση της αλήθειας και η διάδοση φημών που μπορούν να βλάψουν τη συνοχή της κοινωνίας, η διάδοση προλήψεων, υλικού σχετικά με τη βία κ.α., δημιουργώντας σαφή ερωτήματα για τα όρια της ελευθερίας του λόγου στο Διαδίκτυο.

5.3.6 ΔΙΕΘΝΕΙΣ ΠΡΟΣΠΑΘΕΙΕΣ

Σε διεθνές επίπεδο πρώτη η Interpol προσέγγισε το ζήτημα του ηλεκτρονικού εγκλήματος, στο Τρίτο Διεθνές Συμπόσιο για την Απάτη, στο Παρίσι, το 1979. Έγιναν και άλλες προσπάθειες τα επόμενα χρόνια με πιο σημαντικές αυτές που αναπτύχθηκαν από τον OECD, τα Ηνωμένα Έθνη και την «Ομάδα των Οκτώ» (Group of Eight).

i) Organization for Economic Cooperation and Development (OECD): Ο Οργανισμός για την Οικονομική συνεργασία και Ανάπτυξη (Ο.Ο.Σ.Α.) διόρισε στο Παρίσι το 1983, μια επιτροπή για το ζήτημα του ηλεκτρονικού εγκλήματος και την ανάγκη για την τροποποίηση των ποινικών διατάξεων στα κράτη-μέλη του οργανισμού. Η επιτροπή αφού εξέτασε τις ισχύουσες νομοθετικές διατάξεις των κρατών-μελών, κατέληξε σε ένα κείμενο για το ηλεκτρονικό έγκλημα, που λειτουργούσε ως κοινός παρονομαστής μεταξύ των διαφορετικών νομικών προσεγγίσεων, που εξετάστηκαν στα κράτη-μέλη. Οι διατάξεις του κειμένου αυτού απαγόρευαν την εισαγωγή, τροποποίηση, διαγραφή και απόκρυψη δεδομένων, με σκοπό την παράνομη μεταφορά κεφαλαίων, τη διάπραξη πλαστογραφίας και την παρεμπόδιση λειτουργίας ενός υπολογιστή ή δικτύου. Επίσης, απαγόρευε την πρόσβαση σε συστήματα Η/Υ χωρίς άδεια, ενώ προστάτευε και την παράνομη αντιγραφή και διάθεση πακέτων λογισμικού.

ii) Οργανισμός Ηνωμένων Εθνών: Τα Ηνωμένα Έθνη παρουσίασαν ένα ψήφισμα, σχετικά με τη νομοθεσία για το ηλεκτρονικό έγκλημα στο 8ο Συνέδριο για την Πρόληψη του Εγκλήματος και την Μεταχείριση των Παραβατών. Το Εγχειρίδιο για την Πρόληψη και τον Έλεγχο του Ηλεκτρονικού Εγκλήματος εκδόθηκε το 1994. Το Εγχειρίδιο αυτό αντιμετωπίζει συνολικά το ζήτημα του ηλεκτρονικού εγκλήματος, παρουσιάζοντας την έκταση του φαινόμενου, τις μορφές του και την υπάρχουσα νομοθεσία σε διάφορες χώρες και καταλήγει σε προτάσεις για την καλύτερη αντιμετώπιση του. Το συγκεκριμένο κείμενο, πρέπει να αναθεωρηθεί, λόγω των τεχνολογικών εξελίξεων που έγιναν από την έκδοση του μέχρι σήμερα. Αποτελεί, όμως, την πρώτη συστηματική διεθνής προσπάθεια νομοθετικής προσέγγισης του ηλεκτρονικού εγκλήματος, γι' αυτό θεωρείται η βάση πάνω στην οποία μπορούν να στηριχτούν μελλοντικές προσπάθειες.

iii) Ομάδα των Οκτώ – Group of Eight (G8): Οι οκτώ ισχυρότερες χώρες του κόσμου, δημιούργησαν το 1997 μια Υποομάδα για το Έγκλημα Υψηλής Τεχνολογίας (Hi-tech crime Subgroup). Η Υποομάδα αυτή σε μια συνάντηση που πραγματοποιήθηκε τον ίδιο χρόνο στην Ουάσιγκτον, με την συμμετοχή των υπουργών Εσωτερικών και Δικαιοσύνης των

οκτώ χωρών, κατέληξε σε «Δέκα Αρχές» και «Δέκα Τομείς Δράσης» για την αντιμετώπιση του ηλεκτρονικού εγκλήματος. Οι αρχές αυτές είχαν ως σκοπό τη διασφάλιση της ενιαίας αντιμετώπισης του εγκληματικού φαινόμενου, σε όλες τις χώρες του κόσμου. Εκτός από αυτά η Υποομάδα ίδρυσε ένα δίκτυο επικοινωνίας, το οποίο λειτουργούσε όλο το εικοσιτετράωρο, επτά μέρες την εβδομάδα, με αποστολή τη συνεργασία μεταξύ των χωρών σε επίπεδο ερευνών για εγκλήματα υψηλής τεχνολογίας. Στο δίκτυο επικοινωνίας συμμετέχουν σήμερα πάνω από σαράντα χώρες.

5.4 Η ΣΥΜΒΑΣΗ ΓΙΑ ΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Οι εργασίες για τη δημιουργία μιας Σύμβασης για τον Κυβερνοχώρο (Convention on Cybercrime) ξεκίνησαν το 1997, όταν δημιουργήθηκε μια επιτροπή ειδικών στον τομέα του ηλεκτρονικού εγκλήματος, με σκοπό να εξετάσει τα νομοθετικά προβλήματα που προκύπτουν από την εγκληματική δραστηριότητα στον κυβερνοχώρο. Τελικά το κείμενο της «Σύμβασης για τον Κυβερνοχώρο» υπογράφηκε στις 23 Νοεμβρίου 2001, στη Βουδαπέστη.

Η Σύμβαση έχει ως στόχο την εναρμόνιση των εθνικών νομοθεσιών, σχετικά με το ηλεκτρονικό έγκλημα και την παροχή νομοθετικού πλαισίου στον τομέα του δικονομικού δικαίου για τη διερεύνηση και δίωξη εγκλημάτων που σχετίζονται με τον κυβερνοχώρο. Επίσης, θέτει τις βάσεις για άμεση και αποτελεσματική διεθνή συνεργασία για τα ηλεκτρονικά εγκλήματα.

Το κείμενο της Σύμβασης χωρίζεται σε τέσσερα κεφάλαια:
Στο πρώτο κεφάλαιο είναι οι όροι που χρησιμοποιούνται στη Σύμβαση. Οι όροι είναι τέσσερις: υπολογιστικό σύστημα, ηλεκτρονικά δεδομένα, παροχέας υπηρεσιών και μεταδιδόμενα δεδομένα.

Το δεύτερο κεφάλαιο της Σύμβασης ορίζει τα νομοθετικά μέτρα, που πρέπει να ληφθούν σε εθνικό επίπεδο. Χωρίζεται σε τρία μέρη: Στο πρώτο μέρος καθορίζονται τέσσερις βασικές μορφές του ηλεκτρονικού εγκλήματος:

Α) Αδικήματα ενάντια στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων.

1) Παράνομη πρόσβαση: Σύμφωνα με το άρθρο 2 της Σύμβασης, ποινικοποιείται η από πρόθεση πρόσβαση σε ολόκληρο ή μέρος συστήματος ηλεκτρονικών υπολογιστών, χωρίς δικαίωμα. Το αδίκημα διαπράττεται με την παραβίαση των μέτρων ασφαλείας με σκοπό την απόκτηση ηλεκτρονικών δεδομένων.

2) Αθέμιτη παγίδευση-Υποκλοπή: Σύμφωνα με το άρθρο 3 της Σύμβασης, καθίσταται παράνομη η από πρόθεση, παγίδευση – υποκλοπή, που γίνεται με τεχνικά μέσα, από μη δημόσια εκπομπή δεδομένων ηλεκτρονικών υπολογιστών, από, προς ή μέσα σε ένα σύστημα υπολογιστών, συμπεριλαμβανομένου ηλεκτρομαγνητικών εκπομπών από ένα σύστημα υπολογιστών, που «μεταφέρει» τέτοια στοιχεία.

Η διάταξη αυτή μπορεί να εφαρμοστεί σε κάθε μορφή υποκλοπής ηλεκτρονικών δεδομένων, είτε αυτά διακινούνται μέσω του Κυβερνοχώρου με μεταφορά αρχείων (file transfer), είτε με ηλεκτρονικό ταχυδρομείο, ή τηλεομοιοτυπία (fax).

3) Επέμβαση σε δεδομένα: Ως επέμβαση σε δεδομένα, νοείται η από πρόθεση καταστροφή, διαγραφή, χειροτέρευση, μεταβολή, ή απόκρυψη δεδομένων χωρίς δικαίωμα.

4) Επέμβαση σε σύστημα: Ως επέμβαση σε σύστημα θεωρείται η από πρόθεση σοβαρή παρεμπόδιση, χωρίς δικαίωμα, της λειτουργίας ενός συστήματος υπολογιστή που γίνεται με πρόσθεση, μεταφορά, καταστροφή, διαγραφή, χειροτέρευση, μεταβολή ή απόκρυψη δεδομένων υπολογιστών.

5) Κακή χρήση συσκευών: Σύμφωνα με το άρθρο 6 της Σύμβασης, απαγορεύεται η από πρόθεση και χωρίς δικαίωμα παραγωγή, πώληση, προετοιμασία για χρήση, εισαγωγή, διανομή ή με οποιοδήποτε άλλο τρόπο διάθεση μιας συσκευής, συμπεριλαμβανομένου προγράμματος υπολογιστή, που έχει σχεδιαστεί ή προσαρμοστεί με σκοπό, τη διάπραξη οποιουδήποτε από τα αδικήματα που περιγράφονται στα άρθρα 2-5 της Σύμβασης.

Β) Αδικήματα σχετικά με τους ηλεκτρονικούς υπολογιστές

1) Πλαστογραφία σχετιζόμενη με ηλεκτρονικούς υπολογιστές: Αυτό το αδίκημα διαπράττει όποιος από πρόθεση και χωρίς δικαίωμα προβαίνει στην εισαγωγή, μεταβολή, διαγραφή ή απόκρυψη δεδομένων ηλεκτρονικών υπολογιστών, με

σκοπό τα δεδομένα αυτά να θεωρούνται ή να χρησιμοποιούνται για νόμιμους σκοπούς, σαν να ήταν αυθεντικά.
2) Απάτη σχετιζόμενη με ηλεκτρονικούς υπολογιστές: Αυτό το αδίκημα διαπράττει όποιος με πρόθεση χωρίς δικαίωμα, προκαλεί απώλεια περιουσίας σε κάποιον άλλον με οποιαδήποτε εισαγωγή, τροποποίηση, διαγραφή ή απόκρυψη δεδομένων ηλεκτρονικού υπολογιστή ή άλλη δόλια επέμβαση στην λειτουργία ενός συστήματος ηλεκτρονικού υπολογιστή, με σκοπό να επιφέρει οικονομικό όφελος στον εαυτό του ή σε άλλον.

Γ) Αδικήματα σχετικά με το περιεχόμενο
Το άρθρο 9 της Σύμβαση, ασχολείται αποκλειστικά με το αδίκημα της διακίνησης πορνογραφικού υλικού μέσω του Διαδικτύου. Θεωρείται παράνομη η από πρόθεση:

- Παραγωγή υλικού παιδικής πορνογραφίας, με σκοπό την διακίνηση του με τη χρήση ηλεκτρονικού υπολογιστή.
- Προσφορά ή διακίνηση υλικού παιδικής πορνογραφίας, με τη χρήση ηλεκτρονικού υπολογιστή.
- Απόκτηση υλικού παιδικής πορνογραφίας με τη χρήση ηλεκτρονικού υπολογιστή για ίδια χρήση ή για χρήση άλλου ατόμου.
- Κατοχή υλικού παιδικής πορνογραφίας, αποθηκευμένο σε ηλεκτρονικό υπολογιστή ή οποιαδήποτε άλλη μονάδα αποθήκευσης δεδομένων.

Ο όρος «παιδική πορνογραφία» περιλαμβάνει υλικό, στο οποίο απεικονίζεται ανήλικος ή άτομο που εμφανίζεται ως ανήλικος και συμμετέχει σε σεξουαλικές επαφές καθώς επίσης και φωτογραφικό υλικό που απεικονίζει παρόμοιο περιεχόμενο. Ως ανήλικος θεωρείται αυτός που δεν έχει συμπληρώσει το 18^{ο} έτος της ηλικίας του.

Δ) Αδικήματα σχετικά με την πνευματική ιδιοκτησία και συναφή δικαιώματα
Το άρθρο 10 προστατεύει την πνευματική ιδιοκτησία και τα συναφή δικαιώματα.
Το άρθρο 13 αναφέρεται στις ποινές που θα πρέπει να επιβάλλονται στους παραβάτες των παραπάνω διατάξεων.

Στο δεύτερο μέρος καθορίζονται οι δικονομικές διατάξεις σχετικά με τη δίωξη του ηλεκτρονικού εγκλήματος. Οι πιο σημαντικές διατάξεις αναφέρονται:

1) Στην υποχρέωση όσων υπογράφουν να θέσουν σε ισχύ τη σύμβαση, να προστατεύσουν τα ανθρώπινα δικαιώματα και ελευθερίες, συμπεριλαμβανομένων και των υποχρεώσεων τους που απορρέουν από i) τη Σύμβαση του Συμβουλίου της Ευρώπης για την Προστασία των Ανθρωπίνων Δικαιωμάτων και Θεμελιωδών ελευθεριών (1950), ii) το διεθνές σύμφωνο των Ηνωμένων Εθνών για τα Αστικά και Πολιτικά Δικαιώματα (1966) και iii) οποιαδήποτε άλλη διεθνής Σύμβαση για τα ανθρώπινα δικαιώματα (Άρθρο 15).
2) Στην υποχρέωση ενός ατόμου, κατόπιν παραγγελίας των αρμοδίων διωκτικών αρχών, να διατηρεί δεδομένα, που είναι αποθηκευμένα στον ηλεκτρονικό υπολογιστή του για όσο χρονικό διάστημα (δεν μπορεί να υπερβεί τις 90 μέρες) προκειμένου να βοηθηθούν οι έρευνες.
3) Στην δυνατότητα των διωκτικών αρχών να έχουν πρόσβαση και δυνατότητα αναζήτησης δεδομένων, που είναι αποθηκευμένα σε ένα σύστημα Η/Υ ή σε φορητά μέσα, όπως, επίσης, να υποχρεώσουν ένα άτομο που κατέχει ειδικές γνώσεις για τη διατήρηση των δεδομένων σε ένα Η/Υ, να παράσχει στις διωκτικές αρχές όλες τις απαραίτητες πληροφορίες (Άρθρο 19).

Στο τρίτο μέρος αναφέρεται στο ζήτημα της δικαιοδοσίας (άρθρο 22) η οποία ορίζεται από το γεωγραφικό χώρο κάθε χώρας και επεκτείνεται στα πλοία που φέρουν τη σημαία της και τα αεροσκάφη, τα οποία υπόκεινται στους νόμους της. Η προσωπική δικαιοδοσία εφαρμόζεται όταν το διαπραττόμενο έγκλημα τιμωρείται με τους νόμους της χώρας στην οποία διαπράχθηκε σε τόπο που δεν εφαρμόζεται καμιά δικαιοδοσία. Η εφαρμογή των ανώτερων κανόνων, αφήνετε στην ελεύθερη κρίση κάθε χώρας, η οποία πρέπει να εφαρμόσει και την εθνική της νομοθεσία. Σε περίπτωση που μπορεί να τύχουν εφαρμογής παραπάνω από μια δικαιοδοσία, η καταλληλότερη καθορίζεται κατόπιν συνεννόησης των εμπλεκόμενων μερών.

Το τρίτο κεφάλαιο, προσεγγίζει το ζήτημα της διεθνούς συνεργασίας. Στο άρθρο 24 θίγεται το ζήτημα της έκδοσης, για το οποίο προβλέπεται η επιβολή της μικρότερης ποινής, που επιβάλλεται για ένα αδίκημα σε δύο χώρες, εφόσον απαιτηθεί η έκδοση του κατηγορουμένου από την μια στην άλλη. Τα άρθρο 25, αναφέρεται στην υποχρέωση για αμοιβαία συνεργασία κατά το μεγαλύτερο δυνατό, για τη διευκόλυνση των ερευνών για ηλεκτρονικά εγκλήματα. Το άρθρο 29

υποχρεώνει μια χώρα να διατηρήσει δεδομένα, αποθηκευμένα σε Η/Υ ή άλλα μέσα, εφόσον της ζητηθεί από άλλη χώρα για τα οποία αναμένεται να υποβληθεί αίτημα για πρόσβαση και έρευνα. Στο τελευταίο άρθρο της ενότητας αυτής, άρθρο 35, προβλέπεται η δημιουργία ενός κέντρου επικοινωνίας σχετικά με την έρευνα του ηλεκτρονικού εγκλήματος, το οποίο θα λειτουργεί 24 ώρες το 24ωρο, επτά μέρες την εβδομάδα, με κύριες αρμοδιότητες την παροχή τεχνικών συμβουλών, τη διατήρηση δεδομένων, που προβλέπονται από τη σύμβαση, τη συλλογή δεδομένων, την παροχή νομικών πληροφοριών και τον εντοπισμό υπόπτων.

Στο τέταρτο και τελευταίο μέρος, περιλαμβάνονται οι τελικές διατάξεις, σχετικά με το χρόνο στον οποίο θα τεθεί σε ισχύ η σύμβαση, η γεωγραφική εφαρμογή της, η ακολουθούμενη διαδικασία που θα απαιτηθεί για πιθανή τροποποίηση της στο μέλλον και άλλες διατάξεις.

Το κυρίως κείμενο της Σύμβασης για τον Κυβερνοχώρο, συνοδεύεται και από μια Επεξηγηματική Αναφορά, στην οποία αναλύονται όλα τα άρθρα της Σύμβασης, υπάρχουν συμπληρωματικές πληροφορίες και αιτιολόγηση των επιλογών των συντακτών της Σύμβασης.

Τέλος, η Σύμβαση συμπληρώθηκε το 2002 από ένα Πρόσθετο Πρωτόκολλο, σχετικά με την Ποινικοποίηση Πράξεων Ρατσισμού και Ξενοφοβίας που διαπράττονται μέσω ηλεκτρονικού υπολογιστή. Το Πρόσθετο Πρωτόκολλο, προτρέπει όσους το υπογράψουν και το θέσουν σε ισχύ, να υιοθετήσουν τέτοια νομοθετικά μέτρα ώστε να ποινικοποιηθεί:

1) η διάδοση ρατσιστικού και ξενοφοβικού υλικού, με τη χρήση ηλεκτρονικών υπολογιστών,
2) η διάδοση ρατσιστικών και ξενοφοβικών απειλών ή υβριστικών συνθημάτων, μέσω τέτοιων συστημάτων και
3) η χρησιμοποίηση τέτοιων συστημάτων, για τη διάδοση υλικού, το οποίο αρνείται, ελαχιστοποιεί, εγκρίνει ή δικαιολογεί πράξεις γενοκτονίας ή εγκλημάτων ενάντια στην ανθρωπότητα, όπως αυτά ορίζονται από τη διεθνή νομοθεσία.

5.5 Η ΙΣΧΥΟΥΣΑ ΝΟΜΟΘΕΣΙΑ ΣΤΗΝ ΕΛΛΑΔΑ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Στην Ελληνική νομοθεσία, δεν υπάρχουν ειδικές διατάξεις για τα ηλεκτρονικά εγκλήματα. Ο όρος «ηλεκτρονικό έγκλημα», δεν αναφέρεται πουθενά στο ελληνικό δίκαιο. Οι περισσότερες υποθέσεις που έχουν προκύψει μέχρι σήμερα, έχουν διωχτεί με τις διατάξεις του Ν. 1805/1988, ο οποίος πρόσθεσε τα άρθρα 370Β, 370Γ και 386^{A} στον Ποινικό Κώδικα, τα οποία αναφέρονται στα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές. Επίσης το άρθρο 370^{A} αναφέρεται στην παραβίαση του απορρήτου των τηλεφωνημάτων και το άρθρο 348^{A} στην πορνογραφία ανηλίκων.

Τα άρθρα αυτά του Ποινικού Κώδικα δεν επαρκούν για να καλύψουν τις ανάγκες δίωξης των σύγχρονων ηλεκτρονικών εγκλημάτων, κυρίως γιατί δεν έχουν προβλέψει την ύπαρξη του Διαδικτύου. Αδικήματα όπως η διασπορά κακόβουλου λογισμικού και οι επιθέσεις άρνησης εξυπηρέτησης, δεν μπορούν να τιμωρηθούν με βάση το ισχύον νομοθετικό πλαίσιο.

Το κενό στη νομοθεσία για τα ηλεκτρονικά εγκλήματα αντιμετωπίζεται με την υπάρχουσα νομοθεσία για τα συμβατικά εγκλήματα, η οποία προσαρμόζεται στον εικονικό κόσμο του Διαδικτύου, θεωρώντας το ως ένα ακόμη μέσο για τη διάπραξη εγκλημάτων.

Ειδικότερα διατάξεις για τα θέματα, που σχετίζονται με το ηλεκτρονικό έγκλημα, περιλαμβάνονται μόνο στο Π.Δ. 131/2003, το οποίο θεσπίσθηκε σε εφαρμογή κοινοτικής οδηγίας για το ηλεκτρονικό εμπόριο και αναφέρεται στην ανεπιθύμητη αλληλογραφία (spam-mail) και στην ευθύνη των παρόχων υπηρεσιών Διαδικτύου για πράξεις των χρηστών (συνδρομητών) τους. Επίσης ο Ν. 2867/2000 για την «Οργάνωση και Λειτουργία του τομέα των Τηλεπικοινωνιών», οι Ν. 2774/99 και 2472/97 «περί προσωπικών δεδομένων» και ο Ν. 2225/94 για την «προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας» προσεγγίζουν κάποιες πτυχές του ηλεκτρονικού εγκλήματος.

Αν και η χώρα μας έχει υπογράψει την Ευρωπαϊκή Σύμβαση για το Έγκλημα στον Κυβερνοχώρο, δεν την έχει θέσει ακόμη σε ισχύ. Η θέση, σε ισχύ της Σύμβασης θα καλύψει ένα πολύ μεγάλο κενό της Ελληνικής νομοθεσίας, όχι μόνο, στον τομέα του Ποινικού αλλά και του Δικονομικού Δικαίου.

5.6 ΑΛΛΑ ΘΕΜΑΤΑ ΠΟΥ ΕΧΟΥΝ ΣΧΕΣΗ ΜΕ ΤΗ ΝΟΜΟΘΕΣΙΑ

5.6.1 Η ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

Η ψηφιακή μορφή των πληροφοριών έχει μετατρέψει την αναπαραγωγή της σε εύκολη και γρήγορη διαδικασία και η ενσωμάτωση της σε πρότυπα όπως mp3, mpeg κ.λπ. έχουν μειώσει πολύ τον όγκο της και έτσι είναι πολύ εύκολη η μετάδοση της μέσω δικτύων. Το δίκαιο της πνευματικής ιδιοκτησίας έχει ως αντικείμενο προστασίας τα έργα του λόγου της τέχνης και της επιστήμης. Τα δύο βασικά στοιχεία της έννοιας του έργου είναι να έχει μορφή και να είναι πρωτότυπο. Τα κυρίαρχα ζητήματα προστασίας της πνευματικής ιδιοκτησίας που έχουν προκύψει από την ανάπτυξη του Διαδικτύου, είναι η προστασία των πνευματικών δικαιωμάτων σε έργα που δημοσιεύονται στο Διαδίκτυο και η προστασία των βάσεων δεδομένων και των προγραμμάτων Η/Υ.

5.6.1.1 ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ ΕΡΓΩΝ ΔΗΜΟΣΙΕΥΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Σύμφωνα με τον Καράκωστα (2003: 104) δυο είναι τα βασικότερα τεχνικά ζητήματα που έχουν σχέση με το Διαδίκτυο και το δίκαιο της πνευματικής ιδιοκτησίας: α) η χρήση των συνδέσμων και β) το mp3 και άλλα σχετικά πρότυπα. Στην πρώτη περίπτωση, η χρήση συνδέσμων που παραπέμπουν απευθείας σε σελίδες που περιλαμβάνουν προστατευμένα έργα συνιστούν παραβίαση των πνευματικών δικαιωμάτων. Στην δεύτερη περίπτωση, η ευρεία διάδοση μουσικών κομματιών σε μορφή mp3 ή και βιντεοταινιών με τη μορφή mpeg, χωρίς την έγκριση του δημιουργού, αποτελούν σήμερα την πλέον διαδεδομένη προσβολή δικαιωμάτων πνευματικής ιδιοκτησίας των δημιουργών.

5.6.1.2 ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ ΣΕ ΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ

Στο Ελληνικό δίκαιο οι βάσεις δεδομένων προστατεύονται από τον Ν. 2819/2000, ο οποίος εκδόθηκε με βάση την Ευρωπαϊκή Οδηγία 96/9 ΕΚ και τροποποίησε το Ν. 2121/1993 περί πνευματικής ιδιοκτησία. Η οδηγία κατ' αρχής ορίζει ότι μια βάση δεδομένων είναι «μια συλλογή έργων, δεδομένων ή ανεξάρτητων μεταξύ τους στοιχείων διευθετημένων κατά τρόπο συστηματικό ή μεθοδικό που είναι ατομικός προσιτή με ηλεκτρονικά μέσα ή κατ' άλλον τρόπο».

Η οδηγία προστατεύει τις βάσεις δεδομένων κατά δύο τρόπους: είτε ως πνευματικά δημιουργήματα, λόγω της διευθέτησης του περιεχομένου τους, είτε ως προϊόν πνευματικής ουσιαστικής (ποιοτικά και ποσοτικά) επένδυσης του κατασκευαστή, ο οποίος έχει το δικαίωμα ειδικής φύσης σε αυτές για 15 έτη από την κατασκευή της βάσης, δικαίωμα το οποίο απαγορεύει την εξαγωγή ή επαναχρησιμοποίηση σημαντικού μέρους της βάσης δεδομένων.

Οι διατάξεις αυτές, καθιερώνουν την απόλυτη προστασία των βάσεων δεδομένων, οι οποίες αν δεν θεωρηθούν πνευματικά δημιουργήματα, τότε οι κατασκευαστές τους μπορούν να προσφύγουν στο δικαίωμα ειδικής φύσεως. Εκτός αυτών, δεν αποκλείεται και η προστασία μεμονωμένων στοιχείων μιας βάσης εφόσον αποτελούν αυτοτελή πνευματικά δημιουργήματα, ενώ και το λογισμικό που καθιστά εφικτή τη λειτουργία της βάσης, προστατεύεται ως πρόγραμμα ηλεκτρονικού υπολογιστή.

5.6.1.3 ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ ΣΕ ΠΡΟΓΡΑΜΜΑΤΑ Η/Υ

Ένα πρόγραμμα ηλεκτρονικού υπολογιστή είναι μια σειρά από εντολές ή οδηγίες, οι οποίες χρησιμοποιούνται από τον Η/Υ, για να επιτευχθεί ένα συγκεκριμένο αποτέλεσμα.
Τα προγράμματα Η/Υ είναι γραμμένα σε τρία επίπεδα γλώσσας:
► Στη γλώσσα προγραμματισμού, η οποία αποτελείται από σύνθετα σύμβολα, τα οποία ακολουθούν συγκεκριμένους κανόνες.
► Στον κώδικα πηγής (source code), η κατοχή του οποίου αποτελεί πλήρη απόδειξη των πνευματικών δικαιωμάτων.

► Στον κώδικα μηχανής (object code), ο οποίος χρησιμοποιεί μόνο 2 σύμβολα, το 0 και το 1.

Η Ευρωπαϊκή Ένωση, παρακολουθώντας τις εξελίξεις στις Η.Π.Α. θέλησε να αντιμετωπίσει το ζήτημα της πνευματικής ιδιοκτησίας σε προγράμματα Η/Υ και εξέδωσε την Οδηγία 91/250 ΕΟΚ, με την οποία αναγνωρίζονται τα πνευματικά δικαιώματα σε προγράμματα Η/Υ. Προστατεύεται όχι μόνο το πρόγραμμα, αλλά και το προπαρασκευαστικό υλικό, από το οποίο μπορεί σε μεταγενέστερο στάδιο να προκύψει το πρόγραμμα. Όσον αφορά στο ζήτημα της πρωτοτυπίας, η Οδηγία ορίζει, ότι το πρόγραμμα πρέπει να είναι προσωπικό πνευματικό δημιούργημα του δημιουργού του.

Στο άρθρο 4 της Οδηγίας, περιλαμβάνονται οι εξουσίες του δικαιούχου, όπως το αποκλειστικό του δικαίωμα να χορηγεί άδειες, για την αναπαραγωγή του προγράμματος, τη μετάφραση, προσαρμογή ή οποιαδήποτε άλλη μετατροπή, τη διανομή του στο κοινό και την εκμίσθωση του πρωτότυπου προγράμματος.

Η Οδηγία αυτή, υιοθετήθηκε χωρίς καμιά σχεδόν μεταβολή από την ελληνική νομοθεσία και προστέθηκε στο Ν. 2121/1993 για την προστασία των πνευματικών δικαιωμάτων. Στον ελληνικό νόμο, περιλαμβάνονται και οι κυρώσεις σε περίπτωση προσβολής πνευματικής ιδιοκτησίας σε προγράμματα Η/Υ, οι οποίες είναι και ποινικές και αστικές, με βάση την αρχή του ελληνικού δικαίου, ότι όποια αποζημίωση επιδικαστεί, θα πρέπει να είναι αντίστοιχη της ζημιάς που προκλήθηκε.

5.6.2 ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ - ΠΡΟΣΤΑΣΙΑ ΑΠΟΡΡΗΤΟΥ

Η προστασία του απαραβίαστου της προσωπικής ζωής, των προσωπικών δεδομένων και του απορρήτου της αλληλογραφίας είναι αξίες που έχουν κατοχυρωθεί συνταγματικά αλλά και μέσω διεθνών συμβάσεων, στα περισσότερα κράτη του κόσμου. Στο χώρο του Διαδικτύου, η συλλογή προσωπικών δεδομένων από επιχειρήσεις και οργανισμούς και η περαιτέρω επεξεργασία τους για εμπορικούς και διαφημιστικούς λόγους, συνιστούν την πιο διαδεδομένη μορφή καταπάτησης της ιδιωτικής σφαίρας του ατόμου.

Σε μια απλή περιήγηση στο Διαδίκτυο, ο χρήστης αφήνει, χωρίς καν να το αντιληφθεί, πλήθος προσωπικών πληροφοριών που αφορούν την ταυτότητα του, τις προτιμήσεις του, και την προσωπικότητα του, τον αριθμό της πιστωτικής κάρτας κ.α. Τα cookies και πολλά άλλα προγράμματα, «φροντίζουν» να συλλέξουν τις πληροφορίες αυτές και να τις στείλουν στους ιδιοκτήτες των δικτυακών τόπων, για περαιτέρω επεξεργασία.

ΔΙΕΘΝΕΙΣ ΣΥΜΒΑΣΕΙΣ

Η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του ΟΗΕ στις 10-12-1948, αποτέλεσε το πρώτο διεθνές κείμενο για την προστασία της ιδιωτικής σφαίρας του ατόμου. Στο άρθρο 12, διακηρύσσεται ότι «κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του…».

Η Σύμβαση της Ρώμης για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών στις 4-11-1950 (ΕΣΔΑ), ορίζει ότι «κάθε πρόσωπο έχει δικαίωμα για σεβασμό της ιδιωτικής και οικογενειακής ζωής του και κατοικίας του και της αλληλογραφίας του».

Οι Συμβάσεις αυτές εφαρμόζονται ανάλογα και στο Διαδίκτυο, που αποτελεί ένα εικονικό χώρο, στον οποίο διακινούνται πληροφορίες με προσωπικό περιεχόμενο.

ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ

Η Ελληνική νομοθεσία για την προστασία του απορρήτου και της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, αποτελεί ένα συνδυασμό διεθνών συνθηκών, συνταγματικών διατάξεων του κοινού ποινικού δικαίου και νόμων που έχουν εκδοθεί βάση κοινοτικών οδηγιών.

Στο Σύνταγμα της Ελλάδος, περιλαμβάνονται μια σειρά από διατάξεις, για την προστασία της ιδιωτικής σφαίρας του ατόμου. Η θεμελιώδης διάταξη του άρθρου 2 παρ. 1, αναφέρει ότι «ο σεβασμός και η προστασία της αξίας του ανθρώπου αποτελεί πρωταρχική υποχρέωση της πολιτείας». Σημαντικές διατάξεις περιλαμβάνονται στα άρθρα 9 και 19. Στο άρθρο 9 αναφέρεται ότι «η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη» διάταξη που απαγορεύει τη

δημοσιοποίηση της ζωής του ατόμου. Το άρθρο 19 προστατεύει το απόρρητο των επιστολών και την ελευθερία ανταπόκρισης και επικοινωνίας. Βασικό στοιχείο της επικοινωνίας αποτελεί η μυστικότητα του περιεχομένου της.

Στον Ποινικό Κώδικα, η προστασία του απορρήτου προβλέπεται από τα άρθρα 370, 370Α, 370Β και 370Γ. Τα άρθρα 370 και 370^{A} αναφέρονται στην προστασία των επιστολών και την παραβίαση του απορρήτου των τηλεφωνημάτων και της προσωπικής συνομιλίας αντίστοιχα. Η ανάλογη εφαρμογή των διατάξεων αυτών στο χώρο του Διαδικτύου, έχει προκαλέσει έντονο προβληματισμό στους νομικούς κύκλους, ιδιαίτερα όσο αφόρα το άρθρο 370^{A}, το οποίο κατά πολλούς θεωρείται ότι μπορεί να εφαρμοστεί για το Διαδίκτυο αν και η σύνδεση γίνεται μέσω μισθωμένης τηλεφωνικής γραμμής (πηγή: Καρακώστας, 2001). Το άρθρο 370Β, παρέχει προστασία μόνο για κρατικά, επιστημονικά και επαγγελματικά απόρρητα, αποκλείοντας τα ιδιωτικά απόρρητα. Η πιο ουσιαστική διάταξη, όσο αφορά το χώρο του Διαδικτύου, περιλαμβάνεται στο άρθρο 370Γ, που τιμωρεί τη χωρίς άδεια πρόσβαση σε δεδομένα και αποθηκευμένα σε Η/Υ. Δεν περιλαμβάνει μόνο δεδομένα τα οποία χαρακτηρίζονται από τη φύση τους απόρρητα, αλλά προστατεύει το δικαίωμα του νόμιμου κατόχου των δεδομένων να αποκλείει σε άλλους την πρόσβαση σε όλα τα δεδομένα που είναι αποθηκευμένα στον υπολογιστή.

Το νομοθετικό πλαίσιο για την προστασία του απορρήτου και την ασφάλεια των επικοινωνιών στο Διαδίκτυο συμπληρώνεται με μια σειρά από νόμους που ρυθμίζουν τα θέματα αυτά:

Ν. 2225/1994 και Ν. 3115/2003 «για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις»
Ο Νόμος 2225/1994 αναφέρεται στην ίδρυση της «Εθνικής Επιτροπής Προστασίας του Απορρήτου των Επικοινωνιών», η οποία με τις διατάξεις του Ν. 3115/2003 μετονομάστηκε σε «Αρχή Διασφάλισης Απορρήτου Επικοινωνιών», με σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιοδήποτε τρόπο και την τήρηση των όρων και διαδικασιών άρσης του απορρήτου.

Τα άρθρα 3 και 4, προβλέπουν ότι η άρση του απορρήτου είναι δυνατή μόνο όταν πρόκειται για θέματα εθνικής ασφάλειας ή για διακρίβωση ορισμένων κακουργημάτων.

Υπουργική Απόφαση 68141 της 4-7-1995

Η συγκεκριμένη απόφαση, αποτελεί τον «Κώδικα Δεοντολογίας Άσκησης Τηλεπικοινωνιακών Δραστηριοτήτων». Σύμφωνα με τις διατάξεις του Κώδικα, ο πάροχος τηλεπικοινωνιακών υπηρεσιών απαγορεύεται να παρακολουθεί, καταγράφει, ακροάζει, αποκαλύπτει και αναμεταδίδει το περιεχόμενο οποιασδήποτε επικοινωνίας, να δημοσιεύσει προσωπικές πληροφορίες των χρηστών του και γενικά όλες οι ενέργειες του να μην οδηγούν σε προσβολή των ατομικών δικαιωμάτων του πολίτη.

Ν. 2472/1997 για την προστασία των προσωπικών δεδομένων

Ο Νόμος αυτός καθορίζει τις προϋποθέσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Στα άρθρα 15-20, προβλέπεται η σύσταση, συγκρότησης και τρόπος λειτουργίας της «Αρχής προστασίας δεδομένων προσωπικού χαρακτήρα» μιας ανεξάρτητης αρχής για τη διασφάλιση της προστασίας των δεδομένων προσωπικού χαρακτήρα. Ο νόμος θεσπίστηκε, βάσει της 95/46/ΕΚ οδηγίας, οι βασικές αρχές της οποίας αναφέρονται στην προστασία της ιδιωτικής σφαίρας του ατόμου από:

► τη δημιουργία αρχείων με δεδομένα προσωπικού χαρακτήρα, τα οποία θα αποκτώνται με οποιοδήποτε τρόπο μέσω του Διαδικτύου.

► τη μεταφορά αρχείων με δεδομένα προσωπικού χαρακτήρα μέσω του Διαδικτύου.

► τη συγκέντρωση και διασύνδεση τέτοιων αρχείων, τα οποία προέρχονται από διαφορετικούς ηλεκτρονικούς υπολογιστές συνδεδεμένους στο Διαδίκτυο.

Ν. 2774/1999 «για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα»

Ο Νόμος 2774/1997 ρυθμίζει τα θέματα προστασίας δεδομένων προσωπικού χαρακτήρα. Ο Ν. 2774/99 επεκτείνει την προστασία αυτή σε όλες τις πτυχές του τηλεπικοινωνιακού τομέα. Αποτελεί την προσαρμογή της Ελληνικής Νομοθεσίας

στην Οδηγία 97/66/ΕΚ. Σκοπός της Οδηγίας και του νόμου, είναι να προστατευτούν τα προσωπικά δεδομένα σε τομείς, όπως η συμβατική και κινητή τηλεφωνία, το Διαδίκτυο και γενικά όλες οι υπηρεσίες που περιλαμβάνονται στα ψηφιακά δίκτυα (π.χ. ISDN).
Όσον αφορά το χώρο του Διαδικτύου, η προστασία επεκτείνεται και στο ηλεκτρονικό ταχυδρομείο, οι διατάξεις περί αγοράς και διαφήμισης απαγορεύουν τη χρήση των cookies, ενώ προβλέπεται η προστασία από την ενοχλητική αλληλογραφία. Οι παραβάτες των διατάξεων του νόμου φέρουν αστικές και ποινικές ευθύνες.

Ν. 3431/2006 «Περί ηλεκτρονικών επικοινωνιών»
Ο Νόμος αυτός ενσωματώνει στο εθνικό δίκαιο μια σειρά από οδηγίες της Ευρωπαϊκής Ένωσης, σχετικά με τον έλεγχο των ηλεκτρονικών επικοινωνιών οποιασδήποτε μορφής. Βασικοί στόχοι του νόμου, είναι η απελευθέρωση της αγοράς των τηλεπικοινωνιών και η υιοθέτηση κανόνων για τον έλεγχο των επιχειρήσεων – οργανισμών, που προσφέρουν τηλεπικοινωνιακές υπηρεσίες. Επίσης, δίνεται ιδιαίτερη βαρύτητα, στην προστασία του χρήστη έναντι κάθε παράνομης δραστηριότητας, καθώς υποχρεώνει τους παρόχους να λάβουν κάθε απαραίτητο μέτρο, ώστε να εξασφαλιστεί υψηλό επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής.
Με το Νόμο αυτό ενδυναμώνεται η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) η οποία, αποτελεί ανεξάρτητη αρχή και έχει διοικητική και οικονομική αυτοτέλεια. Οι αρμοδιότητες της επεκτείνονται σε όλο το φάσμα των ηλεκτρονικών επικοινωνιών. Όσον αφορά τον κυβερνοχώρο, η Ε.Ε.Τ.Τ. είναι αρμόδια για την καταχώρηση ονομάτων χώρου με καταλήξεις gr και eu, καθώς και για τη ρύθμιση όλων των θεμάτων που σχετίζονται με τις ηλεκτρονικές υπογραφές.

5.6.3 ΝΟΜΟΘΕΣΙΑ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Μια από τις πιο σημαντικές συνέπειες της ανάπτυξης του Διαδικτύου είναι η ενσωμάτωση σε αυτό εμπορικών δραστηριοτήτων. Οι προσφερόμενες μέσω του Διαδικτύου υπηρεσίες αναπτύχθηκαν σε τέτοιο βαθμό που σήμερα είναι δυνατή η on-line παραγγελία, πληρωμή και παράδοση αγαθών και υπηρεσιών. Οι διαδικτυακές συναλλαγές πραγματοποιούνται σε ένα εικονικό κόσμο, χωρίς τη

φυσική παρουσία των συναλλασσόμενων και αυτό δημιουργεί δυσπιστία για την εγκυρότητα μιας συναλλαγής. Επιπλέον θα πρέπει να ρυθμιστεί η διαφήμιση, οι ηλεκτρονικές υπογραφές, τα ηλεκτρονικά έγγραφα και οι ηλεκτρονικές πληρωμές.

Για όλα αυτά η Ευρωπαϊκή Κοινότητα έχει εκδώσει μια σειρά από Οδηγίες, οι περισσότερες από τις οποίες ενσωματώθηκαν στο Ελληνικό Δίκαιο. Η πιο σημαντική και πρόσφατη Οδηγία 2000/31/ΕΚ, ρυθμίζει τα θέματα του ηλεκτρονικού εμπορίου. Σκοπός της Οδηγίας είναι η εξασφάλιση της ελεύθερης κυκλοφορίας των υπηρεσιών και της κοινωνίας της πληροφορίας μεταξύ των κρατών-μελών, περιοριζόμενη από τις θεμελιώδεις ανάγκες για την προστασία των ανηλίκων, της ανθρώπινης αξιοπρέπειας, την προστασία του καταναλωτή και της δημόσιας υγείας.

ΕΛΛΗΝΙΚΟ ΔΙΚΑΙΟ

Το ζήτημα του ηλεκτρονικού εμπορίου στο Ελληνικό Δίκαιο, ρυθμίζεται με το Π.Δ. 131/2003 στο οποίο ενσωματώθηκε η Οδηγία 2000/31/ΕΚ. Οι πιο σημαντικές διατάξεις περιλαμβάνονται:

► Στο άρθρο 6, το οποίο ρυθμίζει το ζήτημα της μη ζητηθείσας εμπορικής επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου (spam mail), βάσει του οποίου, οι πάροχοι των υπηρεσιών αυτών, υποχρεούνται να τηρούν και να συμβουλεύονται ταχτικά μητρώα επιλογών, όπου μπορούν να εγγράφονται τα φυσικά πρόσωπα που επιλέγουν να μη λαμβάνουν τέτοιες εμπορικές επικοινωνίες.

► Στα άρθρα 8-10, που αναφέρονται στις ηλεκτρονικές συμβάσεις και τους τρόπους ηλεκτρονικής παραγγελίας. Γενικά, επιτρέπεται η κατάρτιση ηλεκτρονικών συμβάσεων, εξαιρουμένων περιπτώσεων που αφορούν θεμελίωση ή μεταβίβαση εμπράγματων δικαιωμάτων επί ακινήτων, που εμπίπτουν στο οικογενειακό ή κληρονομικό δίκαιο και όσες, εκ του νόμου, απαιτείται προσφυγή σε δημόσιες αρχές, δικαστήρια ή επαγγέλματα που ασκούν δημόσια εξουσία. Η ηλεκτρονική παραγγελία θεωρείται έγκυρη, όταν ο παροχέας ενημερώσει πλήρως τον πελάτη για τις λεπτομέρειες της σύμβασης και μετά την παραγγελία, αποσταλεί και ηλεκτρονικό μήνυμα επιβεβαίωσης.

► Στο άρθρο 20, το οποίο εξαιρεί την εφαρμογή του Διατάγματος από ορισμένες δραστηριότητες όπως π.χ. το φορολογικό τομέα και θέματα που ήδη ρυθμίζονται με το νόμο περί προστασίας των προσωπικών δεδομένων.

Για τα ηλεκτρονικά έγγραφα εφαρμόζεται η διάταξη του άρθρου 13 εδ. γ' Π.Κ., η οποία εξομοιώνει τα ηλεκτρονικά με τα συμβατικά έγγραφα. Η διάταξη αυτή, όμως, δεν είναι πλήρης, καθότι τα έγγραφα στο Διαδίκτυο παρουσιάζουν ιδιαιτερότητες, όπως π.χ. ο μεγάλος βαθμός μεταβλητότητας και η έλλειψη ιδιόχειρης υπογραφής. Τα ζητήματα αυτά, επιχειρείται να επιλυθούν με την καθιέρωση των ψηφιακών υπογραφών. Ήδη έχει ψηφιστεί και τεθεί σε ισχύ το Π.Δ 150/2001, το οποίο προσάρμοσε την Οδηγία 99/93/ΕΚ, σχετικά με τις ψηφιακές υπογραφές στο Ελληνικό Δίκαιο. Σύμφωνα με τις διατάξεις του Π.Δ, η ηλεκτρονική ή ψηφιακή υπογραφή πρέπει να πληροί τους εξής όρους:
Α) να συνδέεται μονοσήμαντα με τον υπογράφοντα,
Β) να είναι ικανή να καθορίσει, ειδικά και αποκλειστικά, την ταυτότητα του υπογράφοντος,
Γ) να δημιουργείται με μέσα, τα οποία ο υπογράφων μπορεί να διατηρεί υπό τον αποκλειστικό του έλεγχο,
Δ) να συνδέεται με τα δεδομένα, στα οποία αναφέρεται, κατά τρόπο, ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων.

Επιπλέον, το άρθρο 3 εξομοιώνει την ψηφιακή υπογραφή με τη διαχείριση. Δυστυχώς, η πολύ σημαντική αυτή διάταξη δεν εφαρμόζεται ευρέως και συναλλαγές μέσω του Διαδικτύου με τη χρήση ψηφιακών υπογραφών, αντιμετωπίζονται, ακόμη και σήμερα, με δυσπιστία.

Τέλος, όσο αφορά το ζήτημα των ηλεκτρονικών πληρωμών, αυτές πραγματοποιούνται στο χώρο του Διαδικτύου με τρεις κύριους τρόπους: α) την ηλεκτρονική μεταφορά κεφαλαίου, β) τη χρήση πιστωτικών καρτών και γ) την ύπαρξη ηλεκτρονικού χρήματος. Σε νομοθετικό επίπεδο οι συναλλαγές με τη χρήση πιστωτικών καρτών προστατεύονται από τις κοινοτικές Οδηγίες 87/102/ΕΟΚ και 90/88/ΕΟΚ για την καταναλωτική πίστη, ενώ οι Οδηγία 97/7/ΕΚ για τις συμβάσεις από απόσταση, επιτρέπει την εκ των υστέρων ανατροπή της

συμβάσεως, δίνοντας προθεσμία υπαναχώρησης στον καταναλωτή, επιρρίπτοντας το βάρος τέτοιων κινδύνων στον προμηθευτή προϊόντων ή υπηρεσιών.

Σ' αυτό το κεφάλαιο έγινε διεξοδική ανάλυση της νομοθεσίας για το ηλεκτρονικό έγκλημα. Πλέον με την εξάπλωση του Διαδικτύου είδαμε τα προβλήματα που διέπουν τη νομοθεσία αυτή και πως προσεγγίζει νομοθετικά κάθε χώρα το ηλεκτρονικό έγκλημα. Θα μπορούσαμε να πούμε ότι γίνεται μεγάλη προσπάθεια για έλεγχο του προβλήματος αλλά η συνεχής εξέλιξη της τεχνολογίας δημιουργεί μεγάλο πρόβλημα καθώς δημιουργούνται συνεχώς νέα εγκλήματα και οι νόμοι πρέπει συνεχώς να ρυθμίζονται. Επίσης, όπως θα δούμε και στο επόμενο κεφάλαιο πέρα από την νομοθεσία για την διαλεύκανση ενός τέτοιου εγκλήματος σημαντική είναι και η διερεύνηση του που είναι μια δύσκολη διαδικασία.

ΚΕΦΑΛΑΙΟ 6
Η ΔΙΕΡΕΥΝΗΣΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Η Ηλεκτρονική Εγκληματολογία (Computer Forensic Science), είναι «η επιστήμη που ασχολείται με την αναγνώριση, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό» (πηγή: Mc Kemmish, 1999). Όλο και πιο συχνά οι αποδείξεις μιας αξιόποινης πράξης είναι κρυμμένες σε ένα υπολογιστή. Είναι αρκετά δύσκολο, όχι μόνο να εντοπίσουμε τις αποδείξεις, αλλά και να τις συγκεντρώσουμε με τέτοιο τρόπο ώστε να είναι αποδεκτές στο δικαστήριο. Οι διωκτικές αρχές πρέπει να αποδείξουν, ότι τα στοιχεία που συλλέχθηκαν από τη σκηνή διάπραξης του εγκλήματος, διατηρήθηκαν αναλλοίωτα και τεκμηριώνουν την ενοχή του κατηγορουμένου. Παράλληλα, θα πρέπει να βεβαιώσουν ότι δεν έγινε κάποια παράλειψη που κατάστρεψε αποδείξεις σχετικά με την αθωότητα του κατηγορουμένου.

6.1 ΨΗΦΙΑΚΕΣ ΑΠΟΔΕΙΞΕΙΣ ΚΑΙ ΔΕΔΟΜΕΝΑ

Οι ψηφιακές αποδείξεις αποτελούν το πιο σπουδαίο αποδεικτικό μέσο, κατά την εξέταση μιας υπόθεσης ηλεκτρονικού εγκλήματος και γενικά κατά την εξέταση οποιουδήποτε στοιχείου έχει ψηφιακή μορφή. Ο SWGDE (Scientific Working Group on Digital Evidence), μια κοινοπραξία διεθνών οργανισμών, που δραστηριοποιείται στον τομέα των ψηφιακών αποδείξεων, τον Οκτώβριο του 1999 διαχώρισε τις αποδείξεις που έχουν ψηφιακή μορφή σε:

► Ψηφιακές αποδείξεις: Πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και μπορούν να αποθηκευτούν ή να μεταδοθούν σε ψηφιακή μορφή.

► Αντικείμενα δεδομένων: Αντικείμενα ή πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και σχετίζονται με φυσικά αντικείμενα.

► Φυσικά αντικείμενα: Τα φυσικά μέσα όπου αποθηκεύονται ή μέσω των οποίων μεταδίδονται πληροφορίες και αντικείμενα δεδομένων.

► Γνήσιες ψηφιακές αποδείξεις: Φυσικά αντικείμενα και αντικείμενα δεδομένων τη στιγμή που συλλέγονται από τη σκηνή του εγκλήματος.

► Διπλότυπες ψηφιακές αποδείξεις: Ένα ακριβές ψηφιακό αντίγραφο όλων των αντικειμένων δεδομένων που περιέχονται σε ένα γνήσιο ψηφιακό αντικείμενο.
► Αντίγραφο: Μια ακριβής αναπαραγωγή των πληροφοριών που περιέχονται σε ένα γνήσιο φυσικό αντικείμενο, ανεξάρτητα από το αντικείμενο αυτό.

Οι ψηφιακές αποδείξεις μπορεί να είναι αποθηκευμένες σε οποιαδήποτε συσκευή, όπως ηλεκτρονικό υπολογιστή, palmtop, κινητό τηλέφωνο κ.α., καθώς και σε οποιοδήποτε μέσο αποθήκευσης, όπως δισκέτες, CDs, DVDs, κάρτες μνήμης κ.α.

6.2 Η ΕΡΕΥΝΑ ΤΗΣ ΣΚΗΝΗΣ ΔΙΑΠΡΑΞΗΣ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ

6.2.1 Ο ΡΟΛΟΣ ΤΩΝ «ΠΡΩΤΩΝ ΑΝΤΑΠΟΚΡΙΤΩΝ» ΠΟΥ ΦΤΑΝΟΥΝ ΣΤΗ ΣΚΗΝΗ ΔΙΑΠΡΑΞΗΣ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ

Βασικός σκοπός, γι' αυτόν που θα φτάσει πρώτος στη σκηνή διάπραξης του εγκλήματος, είναι να εξασφαλίσει ότι δεν θα προκληθεί ζημιά στα στοιχεία και τις πληροφορίες, που περιλαμβάνονται στη σκηνή. Ο πρώτος αστυνομικός που θα φτάσει στη σκηνή του εγκλήματος πρέπει:
► Να αναγνωρίσει τη σκηνή του εγκλήματος και να δημιουργήσει γύρω από αυτή μια περίμετρο ασφαλείας. Η περίμετρος, μπορεί να περιορίζεται σε ένα μόνο δωμάτιο, ή μπορεί να επεκτείνεται και σε άλλους χώρους, εάν κριθεί ότι μπορεί να έχουν σχέση με το διαπραττόμενο έγκλημα.
► Να προστατεύσει όλο τον εξοπλισμό, από τον οποίο μπορεί να υπάρχουν πληροφορίες για την υπόθεση, όπως Η/Υ (σταθεροί και φορητοί), συσκευές αποθήκευσης κ.λπ.
► Να προστατεύσει και να καταγράψει τα μεταβλητά δεδομένα. Αυτά μπορεί να είναι, π.χ. οι ενδείξεις στην οθόνη ενός Η/Υ. Στην περίπτωση αυτή, καλό είναι να γίνει βιντεοσκόπηση ή φωτογράφηση ή αν αυτό είναι αδύνατο να κρατηθούν λεπτομερείς σημειώσεις για το τι ακριβώς παρουσιάζεται στην οθόνη, ώστε να είναι δυνατή η αξιοποίηση των πληροφοριών αυτών.

6.2.2 Ο ΡΟΛΟΣ ΤΩΝ ΕΞΕΡΕΥΝΗΤΩΝ

Οι εξερευνητές κατέχουν ειδικότερες και εξειδικευμένες γνώσεις για τη μεθοδολογία εξέτασης της σκηνής του εγκλήματος και τη συγκέντρωση του απαραίτητου, για περαιτέρω εξέταση, υλικού. Στην περίπτωση διαπράξεως ενός εγκλήματος, με το οποίο σχετίζεται με οποιοδήποτε τρόπο ένας Η/Υ ή παρόμοια συσκευή, ο εξερευνητής πρέπει να ακολουθήσει συγκεκριμένες διαδικασίες, ώστε να μην χαθούν ψηφιακά δεδομένα.

Βασικός κανόνας για τον εξερευνητή, όταν φτάσει στην σκηνή του εγκλήματος, είναι να εντοπίσει τις διάφορες συσκευές που περικλείονται στο χώρο. Ο εντοπισμός δεν περιορίζεται μόνο στους ηλεκτρονικούς υπολογιστές αλλά περιλαμβάνει: λογισμικό, αποθηκευτικά μέσα πάσης φύσεως, γραπτές σημειώσεις, εγχειρίδια χρήσεως συσκευών, περιφερειακές συσκευές κ.α.

Ακολούθως, ο εξερευνητής θα ξεκινήσει τη διαδικασία συλλογής των δεδομένων, που πιθανώς σχετίζονται με την υπόθεση. Αρχικά γίνεται η συλλογή των μεταβλητών δεδομένων, είναι αυτά που βρίσκονται αποθηκευμένα στην μνήμη RAM και στην cache ενός συστήματος και χάνονται όταν διακοπεί η τροφοδοσία του συστήματος με ρεύμα.

Η επόμενη εργασία είναι η συλλογή των διαρκών δεδομένων, αυτών δηλαδή που βρίσκονται αποθηκευμένα σε σκληρούς δίσκους, Συνήθως τα δεδομένα αυτά αντιγράφονται στη σκηνή του εγκλήματος με τη χρήση ενός λογισμικού imaging ή άλλου παρόμοιου εργαλείου. Τα αντίγραφα των σκληρών δίσκων ή άλλων συσκευών αποθήκευσης αποστέλλονται για αναλυτική εξέταση στο εργαστήριο, έχοντας ως εφεδρικά τα αρχικά αποθηκευτικά μέσα.

Εν συνεχεία γίνεται η αποσύνδεση και συσκευασία των συσκευών. Για τον τερματισμό ενός Η/Υ οι απόψεις διίστανται. Κάποιοι προτείνουν να γίνεται κανονικά με τη διαδικασία που προβλέπεται για το υπό εξέταση λειτουργικό σύστημα, ενώ άλλοι υποστηρίζουν ότι ο τερματισμός πρέπει να γίνεται τραβώντας το καλώδιο από την πρίζα, προκειμένου να αποφευχθεί το ενδεχόμενο διαγραφής δεδομένων κατά τον τερματισμό του υπολογιστή. Η

επιλογή της κατάλληλης μεθόδου γίνεται από τον εξερευνητή πώς θα εκτιμήσει την κατάσταση και από την εμπειρία του.

Η αποσύνδεση των καλωδίων του υπολογιστή πρέπει, επίσης, να γίνεται με επιμέλεια. Όλα τα καλώδια και οι συνδέσεις τους θα πρέπει να καταγραφούν με ιδιαίτερη προσοχή. Καλό θα ήταν να φωτογραφηθούν ή να βιντεοσκοπηθούν οι συνδέσεις, ώστε να μην γίνει κάποιο λάθος κατά την επανασύνδεση των μηχανημάτων.

Τέλος, η μεταφορά των υλικών θα πρέπει να πραγματοποιηθεί, αφού προηγουμένως έχουν συσκευαστεί κατάλληλα για να αποφευχθούν φθορές κατά τη μεταφορά. Τα ψηφιακά δεδομένα είναι ευαίσθητα σε μαγνητικά πεδία, υψηλές θερμοκρασίες και υγρασία. Όλα αυτά θα πρέπει να ληφθούν σοβαρά υπόψη κατά την μεταφορά και την αποθήκευση τους.

6.3 ΜΕΘΟΔΟΙ ΕΞΕΤΑΣΗΣ ΤΩΝ ΨΗΦΙΑΚΩΝ ΤΕΚΜΗΡΙΩΝ

6.3.1 ΑΝΑΚΤΗΣΗ ΔΙΑΓΕΓΡΑΜΜΕΝΩΝ ΔΕΔΟΜΕΝΩΝ

Στα λειτουργικά συστήματα της Microsoft, η διαγραφή ενός αρχείου σημαίνει τη μεταφορά του στον Κάδο Ανακύκλωσης. Από εκεί είναι δυνατή η επαναφορά του αρχείου στην αρχική του θέση ή η οριστική διαγραφή του. Πολλοί χρήστες ηλεκτρονικών υπολογιστών πιστεύουν ότι διαγράφοντας ένα αρχείο από τον Κάδο Ανακύκλωσης, χάνεται οριστικά. Ωστόσο, η διαγραφή δεν επηρεάζει το αποθηκευμένο αρχείο, που παραμένει αποθηκευμένο μέχρι ένα καινούργιο αρχείο να εγγραφεί στον ίδιο αποθηκευτικό χώρο. Όταν διαγράφεται ένα αρχείο δεν διαγράφονται τα ψηφιακά δεδομένα που το αποτελούν. Αν ο σκληρός δίσκος έχει μεγάλη χωρητικότητα, ίσως περάσει πολύ μεγάλο χρονικό διάστημα ώσπου να σβήσουν τα παλιά. Το διαγραμμένο αρχείο εξακολουθεί να υπάρχει στον σκληρό δίσκο, δεν μπορεί όμως να το εντοπίσει το λειτουργικό σύστημα. Η ανάκτηση των αρχείων αυτών, είναι δυνατή με τη χρήση μιας σειράς από εργαλεία λογισμικού.

6.3.2 ΑΝΑΚΤΗΣΗ ΚΡΥΠΤΟΓΡΑΦΗΜΕΝΩΝ ΔΕΔΟΜΕΝΩΝ

Η κρυπτογράφηση, εκτός από εργαλείο ασφάλειας των πληροφοριακών συστημάτων, αποτελεί ταυτόχρονα και βασικό εργαλείο των ηλεκτρονικών εγκληματιών. Δεδομένα, που εμπεριέχονται σε μηνύματα ηλεκτρονικού ταχυδρομείου, έγγραφα, συμπιεσμένους φακέλους, αρχεία PDF, λογιστικά φύλλα κ.λπ. ενδέχεται να έχουν κρυπτογραφηθεί, εφόσον περιέχουν σημαντικές πληροφορίες σχετικά με εγκληματική δραστηριότητα. Η ανάκτηση των δεδομένων αυτών, γίνεται με τη χρήση ειδικών πακέτων λογισμικού, που χρησιμοποιούν κυρίως τη μέθοδο της εξαντλητικής αναζήτησης. Τα προγράμματα αυτά δοκιμάζουν όλους τους πιθανούς συνδυασμούς γραμμάτων, αριθμών και συμβόλων για να βρουν τον αλγόριθμο κρυπτογράφησης.

6.3.3 ΑΝΑΚΤΗΣΗ ΚΡΥΦΩΝ ΔΕΔΟΜΕΝΩΝ

ΜΑΓΝΗΤΙΚΟΙ ΔΙΣΚΟΙ

Οι σκληροί δίσκοι είναι χωρισμένοι σε τομείς μεγέθους συνήθως 512 bytes. Λόγω της κατασκευής των δίσκων ίσως να παραμένει κάποιο κενό ανάμεσα στους τομείς στο οποίο μπορούν να αποθηκευτούν δεδομένα. Ορισμένες εφαρμογές ανάκτησης αρχείων έχουν τη δυνατότητα να εντοπίζουν και να ανακτούν τα δεδομένα που είναι αποθηκευμένα σε αυτό το κενό. Οι τομείς του σκληρού δίσκου ομαδοποιούνται σε συστοιχίες. Το μέγεθος κάθε συστοιχίας διαφέρει. Ένα αρχείο που αποθηκεύεται, δεν έχει ποτέ το ίδιο μέγεθος με τη συστοιχία στην οποία τοποθετείται. Ο κενός χώρος που απομένει, ονομάζεται slack area και σε αυτόν μπορεί να αποθηκευτούν διάφορα δεδομένα, η ανάκτηση των οποίων είναι δυνατή μόνο με την έρευνα του σκληρού δίσκου με εξειδικευμένα εργαλεία λογισμικού. Τέλος, οι μηχανικές κεφαλές, που γράφουν στα μαγνητικά μέσα, δεν είναι πάντα απόλυτα στοιχισμένες και ευθυγραμμισμένες. Ενδέχεται, λοιπόν ακόμη και όταν γράφονται δεδομένα σε ένα σκληρό δίσκο πάνω σε παλιά, να παραμένουν κάποια δείγματα των παλιών αρχείων, τα οποία με κατάλληλα εργαλεία να μπορούν να ανακτηθούν και να επανασυσταθούν.

ΣΤΕΝΟΓΡΑΦΙΚΑ ΔΕΔΟΜΕΝΑ

Η στενογραφία είναι μια τεχνική, με την οποία είναι δυνατόν να κρυφτούν δεδομένα μέσα σε άλλα δεδομένα. Η διαδικασία εντοπισμού των δεδομένων που έχουν στεγανογραφηθεί, ονομάζεται στεγανάλυση.

Στο ψηφιακό περιβάλλον τα αρχεία αυτά είναι της μορφής jpg, gif, bmp, wav, voc, gz και txt. Η συχνότερη χρησιμοποιούμενη μέθοδος είναι η απόκρυψη ενός μηνύματος μέσα σε μια φωτογραφία. Αυτό επιτυγχάνεται με την αλλαγή στο ελάχιστο ενός εικονοστοιχείου (pixel), τέτοιας που δεν είναι δυνατόν να εντοπιστείς στο ανθρώπινο μάτι. Αν λοιπόν σε μια φωτογραφία πραγματοποιηθούν μια σειρά από τέτοιες μεταβολές είναι δυνατός ο σχηματισμός ενός ολόκληρου μηνύματος με τα μεταβαλλόμενα εικονοστοιχεία. Ο εντοπισμός τέτοιων δεδομένων από τις διωκτικές αρχές μπορεί να πραγματοποιηθεί με τη χρήση κατάλληλου λογισμικού. Το δυσκολότερο σημείο δεν είναι η εξαγωγή των κρυμμένων δεδομένων αλλά η ανακατασκευή του μηνύματος.

6.3.4 ΑΝΑΚΤΗΣΗ «ΞΕΧΑΣΜΕΝΩΝ» ΔΕΔΟΜΕΝΩΝ

ΜΝΗΜΗ CACHE ΚΑΙ ΙΣΤΟΡΙΚΟ

Κατά την περιήγηση στο Διαδίκτυο, οι φυλλομετρητές αποθηκεύουν στην μνήμη cache διάφορα αρχεία, τα οποία λαμβάνουν από τις ιστοσελίδες που επισκέπτεται ο χρήστης, προκειμένου την επόμενη φορά που θα την επισκεφτεί, να μπορούν να την εμφανίσουν πιο γρήγορα, χωρίς να χρειάζεται η πρόσβαση σε όλο το περιεχόμενο, μέσω των αργών διαδικτυακών ταχυτήτων. Τα αρχεία αυτά αποθηκεύονται στο φάκελο Temporary Internet Files και ενδέχεται να εμπεριέχουν σημαντικές πληροφορίες για την υπό εξέταση υπόθεση. Πληροφορίες επίσης μπορούν να ανακτηθούν και από το ιστορικό του φυλλομετρητή. Στο ιστορικό αποθηκεύονται οι διευθύνσεις όλων των σελίδων που επισκέφτηκε πρόσφατα ο χρήστης. Οι πληροφορίες αυτές μπορεί να είναι ιδιαίτερα χρήσιμες, κατά την εξέταση αδικημάτων όπως π.χ. πορνογραφία.

ΠΡΟΣΩΡΙΝΑ ΑΡΧΕΙΑ

Πολλές εφαρμογές, κατά την δημιουργία ενός αρχείου από το χρήστη αποθηκεύουν, κατά τακτά χρονικά διαστήματα, προσωρινά αντίγραφα στο δίσκο, για να ανακτηθούν σε περίπτωση που το πρόγραμμα τερματιστεί με σφάλμα. Τα αρχεία αυτά διαγράφονται, όταν ο χρήστης τερματίσει το πρόγραμμα με την κατάλληλη διαδικασία. Στην ουσία, όμως, τα αρχεία αυτά δεν διαγράφονται οριστικά από το σκληρό δίσκο, μέχρι κάποιο άλλο αρχείο εγγραφεί στο σημείο που ήταν αποθηκευμένα. Ο εξερευνητής μπορεί να ανακτήσει από τα αρχεία αυτά σημαντικές πληροφορίες.

ΑΡΧΕΙΑ ΣΕΛΙΔΟΠΟΙΗΣΗΣ

Τα σύγχρονα λειτουργικά συστήματα χρησιμοποιούν την εικονική μνήμη για να «ξεγελάσουν» το σύστημα, το οποίο «νομίζει» ότι έχει μεγαλύτερη μνήμη RAM. Η εικονική μνήμη, χρησιμοποιεί ένα μέρος του σκληρού δίσκου, στον οποίο αποθηκεύονται δεδομένα, που προορίζονται για την πραγματική - φυσική μνήμη. Τα δεδομένα αυτά, όπως μηνύματα ηλεκτρονικού ταχυδρομείου, αρχεία κειμένου, ιστοσελίδες κ.α. αποθηκεύονται στα αρχεία σελιδοποίησης. Τα αρχεία αυτά, δημιουργούνται αυτόματα από το λειτουργικό σύστημα. Πολλοί χρήστες Η/Υ δεν γνωρίζουν την ύπαρξη των αρχείων ή ποια δεδομένα αποθηκεύονται σε αυτά. Τα δεδομένα που θα ανακτηθούν από τα page files, ενδέχεται να έχουν σημαντική αποδεικτική αξία.

ΚΑΔΟΣ ΑΝΑΚΥΚΛΩΣΗΣ

Οι περισσότεροι χρήστες Η/Υ δεν γνωρίζουν ότι διαγράφοντας ένα αρχείο μετακινείται στον Κάδο Ανακύκλωσης, ιδιαίτερα δε και στις περιπτώσεις που το εικονίδιο του Κάδου Ανακύκλωσης δεν εμφανίζεται στην επιφάνεια εργασίας. Πολλοί ξεχνούν τα δεδομένα αυτά στον Κάδο Ανακύκλωσης, δίνοντας εύκολα αποδεικτικά στοιχεία στους εξερευνητές.

ΑΝΑΚΤΗΣΗ ΔΕΔΟΜΕΝΩΝ ΑΠΟ ΕΦΕΔΡΙΚΑ ΑΡΧΕΙΑ

Ένας χρήστης, εφόσον θέλει να εξαφανίσει δεδομένα που είναι αποθηκευμένα σε ένα Η/Υ, μπορεί να τα διαγράψει με τη χρήση κατάλληλου λογισμικού ώστε να μην παραμείνουν υπολείμματα αυτών στο σκληρό δίσκο. Στις περιπτώσεις αυτές, ο εξερευνητής θα πρέπει να αναζητήσει τυχόν εφεδρικά αρχεία, που

ίσως έχει αποθηκεύσει ο χρήστης σε φορητά μέσα ή σε άλλους σκληρούς δίσκους και έχει ξεχάσει να διαγράψει.

6.4 Ο ΕΝΤΟΠΙΣΜΟΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

6.4.1 ΑΡΧΕΙΑ ΚΑΤΑΓΡΑΦΗΣ (log files)

Στα αρχεία καταγραφής αποθηκεύονται πληροφορίες που αφορούν τη λειτουργία του συστήματος. Ο εντοπισμός όλων αυτών των πληροφοριών μπορεί να γίνει μέσω της κονσόλας διαχείρισης των Windows. Η χρησιμότητα των αρχείων καταγραφής των Windows μεγιστοποιείται, όταν έχουν ενεργοποιηθεί συγκεκριμένες πολιτικές ομάδων. Τα security logs είναι κενά, εάν δεν έχει οριστεί συγκεκριμένη πολιτική ασφάλειας για μια ομάδα χρηστών. Η ευθύνη ορισμού πολιτικών ασφαλείας ανήκει στο διαχειριστή και υπεύθυνο ασφαλείας ενός συστήματος. Από τα αρχεία καταγραφής, ο ερευνητής του ηλεκτρονικού εγκλήματος μπορεί να διαπιστώσει εάν χρησιμοποιήθηκε συγκεκριμένη εφαρμογή από ένα χρήστη, εάν κάποιος μη εξουσιοδοτημένος χρήστης απέκτησε πρόσβαση στο σύστημα, εάν χρησιμοποιήθηκε κάποια περιφερειακή συσκευή και πλήθος άλλων σημαντικών πληροφοριών.
Επίσης το firewall, ως βασικό εργαλείο, που ελέγχει την κίνηση από και προς ένα προστατευμένο δίκτυο ή υπολογιστή, αποθηκεύει σημαντικές πληροφορίες στα αρχεία καταγραφής του. Οι πληροφορίες των αρχείων αυτών, αποτελούν σημαντικό προανακριτικό αλλά και αποδεικτικό υλικό, σε περιπτώσεις μη εξουσιοδοτημένης πρόσβασης σε δίκτυα.

6.4.2 ΣΥΝΑΓΕΡΜΟΙ, ΠΡΟΕΙΔΟΠΟΙΗΣΕΙΣ, ΑΝΑΦΟΡΕΣ

Τα firewalls μπορούν να προσφέρουν πληροφορίες:
Συναγερμοί: Τα firewalls έχουν τη δυνατότητα να αποστέλλουν μηνύματα υψηλής προτεραιότητας σε συγκεκριμένους παραλήπτες, σε περίπτωση που διαπιστωθεί κάποια ύποπτη δραστηριότητα. Ένα τέτοιο μήνυμα μπορεί να αποσταλεί με e-mail στο διαχειριστή του συστήματος ή ακόμη να γίνει τηλεφωνική κλήση και παράλληλα η ύποπτη δραστηριότητα να αποθηκευτεί στα αρχεία καταγραφής.

Προειδοποιήσεις: Αποτελούν μια πιο ήπια μορφή συναγερμού. Η ενημέρωση του διαχειριστή, μπορεί να γίνει με τους τρόπους που αναφέρθηκαν πιο πάνω. Η βασική διαφορά είναι ότι τα μηνύματα δεν έχουν το χαρακτήρα του άμεσου κινδύνου, όπως στην προηγούμενη περίπτωση, αλλά προειδοποιούν για το ενδεχόμενο εκδήλωσης επίθεσης.
Αναφορές: Οι αναφορές μπορούν να δώσουν επιπρόσθετα δεδομένα, όπως τη συχνότητα αποτυχημένων προσπαθειών απόκτησης μη εξουσιοδοτημένης πρόσβασης, την συχνότητα σφαλμάτων κ.α.

Οι πληροφορίες, που μπορεί να συλλέξει ο ερευνητής από τα firewalls, όπως το χρονικό σημείο το οποίο συνέβη μια δραστηριότητα, η IP διεύθυνση από την οποία προήλθε μια επίθεση, το πρωτόκολλο που χρησιμοποιήθηκε από τον επιτιθέμενο, το είδος του μηνύματος που στάλθηκε, η θύρα που χρησιμοποιήθηκε κ.α. μπορούν να βοηθήσουν στον εντοπισμό του επιτιθέμενου.

6.4.3 ΕΝΤΟΠΙΣΜΟΣ ΟΝΟΜΑΤΩΝ ΧΩΡΟΥ ΚΑΙ ΔΙΕΥΘΥΝΣΗΣ IP

Ο εντοπισμός της διεύθυνσης IP, αποτελεί βασική ενέργεια των διωκτικών αρχών για την εξιχνίαση πολλών υποθέσεων μη εξουσιοδοτημένης πρόσβασης σε δίκτυο. Στις επιθέσεις αυτές οι εισβολείς χρησιμοποιούν πλαστές διευθύνσεις IP, ώστε να παραπλανήσουν τις διωκτικές αρχές. Κάθε διεύθυνση στο Διαδίκτυο έχει ένα αντίστοιχο αριθμό IP. Το σύστημα, που έχει αναλάβει τη διατήρηση των αντιστοιχιών μεταξύ μιας ηλεκτρονικής διεύθυνσης και του αντίστοιχου IP, είναι το DNS. Κατά την εκδήλωση μιας επίθεσης, ο επιτιθέμενος πλαστογραφεί την διεύθυνση του για να φαίνεται ότι είναι νόμιμος χρήστης, δεν πλαστογραφεί όμως τον αντίστοιχο αριθμό IP. Συνήθως τα firewalls έχουν τη δυνατότητα να ελέγχουν αν μια διεύθυνση είναι αληθινή ή όχι και ανάλογα να επιτρέπουν ή να απαγορεύουν την πρόσβαση ενός χρήστη. Εφόσον το firewall δεν έχει ρυθμιστεί κατάλληλα ο ερευνητής θα ελέγξει τις διευθύνσεις όλων όσων απόκτησαν πρόσβαση προκειμένου να εξακριβώσει από ποιόν προήλθε η κακόβουλη επίθεση. Η εργασία αυτή μπορεί να γίνει με διάφορα εργαλεία λογισμικού, τα οποία ελέγχουν αν οι ηλεκτρονικές διευθύνσεις αναλογούν σε σωστούς αριθμούς IP.

6.4.4 ΜΗΝΥΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

Τα μηνύματα ηλεκτρονικού ταχυδρομείου πολλές φορές χρησιμοποιούνται για την διάπραξη πολλών αδικημάτων, όπως η μετάδοση ιών και άλλου κακόβουλου κώδικα, επιθέσεις άρνησης εξυπηρέτησης, απάτες, απειλές κ.α. Η εύρεση του αποστολέα των μηνυμάτων ηλεκτρονικού ταχυδρομείου, αποτελεί βασική εργασία στην αναζήτηση των ηλεκτρονικών ιχνών του επιτιθέμενου. Τα μηνύματα ηλεκτρονικού ταχυδρομείου, κατά την μετάβαση τους από τον αποστολέα στον παραλήπτη, διέρχονται από πολλούς ενδιάμεσους υπολογιστές. Κάθε ένας από τους υπολογιστές αυτούς προσθέτει τις δικές του πληροφορίες στην επικεφαλίδα του μηνύματος. Οι πληροφορίες στην επικεφαλίδα του μηνύματος καταγράφονται σε διάφορα πεδία που αφορούν τις επικεφαλίδες του αποστολέα και του παραλήπτη, τις επικεφαλίδες ημερομηνίας και διάφορες άλλες. Κατά την αναζήτηση του αποστολέα κακόβουλων μηνυμάτων, οι σημαντικότερες πληροφορίες περιλαμβάνονται στις επικεφαλίδες του αποστολέα. Από αυτές μπορούμε να συλλέξουμε τη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα, τη διεύθυνση ηλεκτρονικού ταχυδρομείου στην οποία μπορούν να αποστέλλονται πιθανές απαντήσεις, το μονοπάτι προς τον αποστολέα και τους διακομιστές από τους οποίους πέρασε το μήνυμα για να φτάσει στον τελικό παραλήπτη.

6.4.5 HONEYPOTS AND HONEYNETS

Αποτελούν τα πλέον σύγχρονα εργαλεία των διωκτικών αρχών, για την αντιμετώπιση του ηλεκτρονικού εγκλήματος. Τα honeypots είναι μια συλλογή από συστήματα τα οποία «προσποιούνται» ότι είναι αληθινοί στόχοι, προκειμένου να ξεγελάσουν τον επιτιθέμενο και να τον ωθήσουν στην παραβίαση τους. Ένα honeynet είναι μια συλλογή από συστήματα honeypots, τα οποία συνεργάζονται μεταξύ τους. Βασικός σκοπός των honeypots είναι η παρακολούθηση των ενεργειών του επιτιθέμενου και η καταγραφή τους προκειμένου να αναλυθεί η μεθοδολογία της επίθεσης του. Σε αντίθεση με τα firewalls τα honeypots λειτουργούν παθητικά, δηλαδή αναμένουν την επίθεση του χρήστη και δεν ενεργούν για την παρεμπόδιση της, απλά καταγράφουν τις ενέργειες του.

6.5 ΜΟΝΤΕΛΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑΣ

Η Ηλεκτρονική Εγκληματολογία (Computer Forensic Science) βρίσκεται στα πρώιμα στάδια της ανάπτυξης της σε σχέση με άλλους τομείς της Εγκληματολογικής Επιστήμης. Γι' αυτό έως τώρα δεν υπάρχει κοινά αποδεκτή μεθοδολογία που να καθορίζει τα στάδια της έρευνας σε μια υπόθεση ηλεκτρονικού εγκλήματος. Η ύπαρξη ενός ολοκληρωμένου μοντέλου ερευνών είναι πάρα πολύ σημαντική, γιατί θα βοηθούσε το έργο των ερευνών, έτσι ώστε να υπάρχει ένας βασικός σκελετός ενεργειών και μεθόδων έρευνας, ανεξάρτητα του περιβάλλοντος στο οποίο διεξάγεται. Επιπλέον, θα βοηθούσε στην ανάπτυξη κατάλληλων εργαλείων για την υποβοήθηση του έργου των ερευνητών (πηγή: Ciardhuain, 2004), στην υιοθέτηση κοινής ορολογίας, ενώ θα αποτελούσε βασικό μέσο εκπαίδευσης και επιμόρφωσης του προσωπικού, που ασχολείται με την έρευνα του ηλεκτρονικού εγκλήματος.

Οι πρώτες προσπάθειες δημιουργίας ενός μοντέλου διαδικτυακών ερευνών, επικεντρώθηκαν στην παροχή ενός αναλυτικού πλαισίου οδηγιών για τον τρόπο έρευνας της σκηνής διάπραξης του εγκλήματος. Ο Lee κ.α. (2001), πρότειναν ένα μοντέλο έρευνας της σκηνής διάπραξης του εγκλήματος,:

1) Αναγνώριση: Εντοπίζονται τα αντικείμενα που πιθανώς έχουν αποδεικτική αξία. Ο ερευνητής θα πρέπει να γνωρίζει τι πρέπει να αναζητήσει και που μπορεί να το βρει. Η αναγνώριση οδηγεί στην τεκμηρίωση, συλλογή και διατήρηση των αποδεικτικών στοιχείων.
2) Ταυτοποίηση: Γίνεται η ταξινόμηση των αποδεικτικών στοιχείων (π.χ. φυσικές, βιολογικές, χημικές αποδείξεις κ.λπ.) και η μεταξύ τους σύγκριση με γνωστά πρότυπα.
3) Εξατομίκευση: Εξετάζεται, εάν τα αποδεικτικά στοιχεία φέρουν συγκεκριμένα μοναδικά χαρακτηριστικά, που μπορούν να συνδεθούν με κάποιο άτομο. Βασική αρχή αποτελεί η αξιολόγηση όλων των αντικειμένων.
4) Συμπέρασμα: Περιλαμβάνει τη συγκέντρωση όλων των αποδεικτικών στοιχείων και σχετικών πληροφοριών και την σύσταση και παρουσίαση λεπτομερής αναφοράς, για τα ευρήματα από τη σκηνή του εγκλήματος.

Το παραπάνω μοντέλο επικεντρώνεται στην έρευνα της σκηνής διάπραξης του εγκλήματος, για την εύρεση αποδεικτικών στοιχείων, που έχουν φυσική υπόσταση. Δεν γίνεται όμως αναφορά στις ψηφιακές αποδείξεις και αυτό μειώνει την αξία του μοντέλου, αν και τα στάδια που περιγράφει μπορούν να χρησιμοποιηθούν και σε ένα μοντέλο έρευνας σε ψηφιακό περιβάλλον.

Ο DFRW (Digital Forensic Research Workshop), είναι ένας από τους πλέον σημαντικούς οργανισμούς που ασχολούνται με την ανάπτυξη μοντέλων για την έρευνα του ηλεκτρονικού εγκλήματος. Η κοινοπραξία αποτελείται περισσότερο από μέλη της ακαδημαϊκής κοινότητας. ΤΟ 2001 πρότεινε ένα μοντέλο ερευνών αποτελούμενο από επτά βήματα:

1) Αναγνώριση
2) Διατήρηση
3) Συλλογή
4) Εξέταση
5) Ανάλυση
6) Παρουσίαση
7) Απόφαση

Το μοντέλο αυτό είχε σκοπό να αποτελέσει τη βάση για την ανάπτυξη στο μέλλον ενός πιο πλήρους μοντέλου.

Ένα από τα πιο πλήρης μοντέλα δικτυακών ερευνών, προτάθηκε το 2004, από τον Ciardjuain. Στο μοντέλο αυτό συμπεριλαμβάνονται όλες οι πτυχές της έρευνας του ηλεκτρονικού εγκλήματος και δεν περιορίζεται μόνο στη σκηνή διάπραξης του εγκλήματος.

1) Επίγνωση: Αναφέρεται στην ενημέρωση ενός αρμόδιου φορέα, ότι έχει προκύψει η ανάγκη για την διεξαγωγή μιας έρευνας.
2) Εξουσιοδότηση: Αποκτάται η εξουσιοδότηση για την διεξαγωγή της έρευνας. Για παράδειγμα, η αστυνομία θα πρέπει να αποκτήσει εξουσιοδότηση για την διεξαγωγή της έρευνας, μέσω ενός εντάλματος του αρμόδιου εισαγγελέα.
3) Σχεδιασμός: Κατά το σχεδιασμό της έρευνας μπορεί να προκύψουν διάφορα προβλήματα, όπως η ανάγκη για περαιτέρω εξουσιοδότηση, γι' αυτό πρέπει να διεξάγεται με ιδιαίτερη προσοχή και επιμέλεια.

4) Ενημέρωση: Αναφέρεται στην ενημέρωση ενός οργανισμού ή προσώπου ότι πρόκειται να διεξαχθεί η έρευνα. Το βήμα αυτό μπορεί να παραληφθεί σε περίπτωση που η έρευνα απαιτεί το στοιχείο του αιφνιδιασμού.
5) Αναζήτηση και αναγνώριση αποδεικτικών στοιχείων: Περιλαμβάνει τον εντοπισμό και αναγνώριση των αποδεικτικών στοιχείων.
6) Συλλογή αποδεικτικών στοιχείων: Ο ερευνητής καλείται να συλλέξει όλα τα αποδεικτικά στοιχεία που θα συναντήσει στη σκηνή του εγκλήματος.
7) Μεταφορά των αποδεικτικών στοιχείων: Αποτελεί σημαντικό βήμα, καθώς η λανθασμένη συσκευασία και μεταφορά τους μπορεί να οδηγήσει σε καταστροφή ή απώλεια σημαντικών πληροφοριών.
8) Αποθήκευση αποδείξεων: Γίνεται όταν δεν είναι δυνατή η άμεση εξέταση των αποδείξεων. Και εδώ πρέπει να διατηρηθούν αναλλοίωτα τα αποδεικτικά στοιχεία.
9) Εξέταση Αποδείξεων: Απαιτείται η εξέταση ποικίλων τεχνικών για την ανάκτηση σημαντικών δεδομένων. Μπορεί να χρησιμοποιηθούν εργαλεία λογισμικού για την ανάκτηση δεδομένων από κατεστραμμένους δίσκους, για τον εντοπισμό ηλεκτρονικών ιχνών και την τελική επεξεργασία μεγάλων ποσοτήτων δεδομένων.
10) Υπόθεση: Η υπόθεση αποτελεί το συμπέρασμα της εξέτασης των ψηφιακών αποδείξεων. Στις αστυνομικές έρευνες, η υπόθεση αποτελεί την μορφή της έκθεση πραγματογνωμοσύνης, στην οποία καταγράφονται όλα τα γεγονότα και αποδεικτικά στοιχεία που εξετάστηκαν κατά τη διάρκεια της έρευνας. Το κείμενο βοηθά τον ερευνητή να κατανοήσει καλύτερα τα αποτελέσματα της έρευνας του.
11) Παρουσίαση της υπόθεσης: Η παρουσίαση της υπόθεσης σε μια αστυνομική έρευνα, γίνεται συνήθως ενώπιον του αρμόδιου δικαστηρίου.
12) Απόδειξη-υποστήριξη της υπόθεσης: Στις περισσότερες περιπτώσεις η υπόθεση θα αμφισβητηθεί στο ακροατήριο από τα μέρη τα οποία θίγονται από αυτή. Οπότε, ο ερευνητής καλείται να υποστηρίξει προφορικά, όλα όσα έχει αναφέρει στην έκθεση του, στηρίζοντας τα σε επιστημονικά στοιχεία.
13) Διανομή των πληροφοριών: Στοχεύει στη χρησιμοποίηση της τεχνογνωσίας που αποκτήθηκε από μια έρευνα, σε παρόμοιες περιπτώσεις, που ενδεχομένως προκύψουν στο μέλλον.

6.6 ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ

Η διερεύνηση μιας υπόθεσης ηλεκτρονικού εγκλήματος εκτός από τεχνικής απόψεως πρέπει να είναι και σύννομη, συμβαδίζοντας με τους ισχύοντες νόμους και κανονισμούς σε κάθε χώρα. Η Ηλεκτρονική Εγκληματολογία, ως μια σχετικά νέα επιστήμη, έχει προβληματίσει τους νομικούς κύκλους για το κατά πόσο αξιόπιστη είναι και σε πιο βαθμό οι ψηφιακές αποδείξεις μπορούν να τύχουν εφαρμογής σε μια δίκη. Οι νομικοί προβληματίζονται σχετικά με την έρευνα και κατάσχεση ψηφιακών αποδείξεων, το κατά πόσο οι γνώσεις ενός ερευνητή είναι επαρκείς για τη διεκπεραίωση μιας έρευνας σε ένα Η/Υ και τέλος αν η ανάλυση και διατήρηση των αποδείξεων έγινε σύμφωνα με τις προβλεπόμενες διαδικασίες.

Η έρευνα και κατάσχεση πληροφοριών είναι η πρώτη διαδικασία που αμφισβητείται σε μια δίκη. Σύμφωνα με το Ελληνικό Δίκαιο, μια έρευνα μπορεί να διενεργηθεί όταν διεξάγεται ανάκριση για κακούργημα ή πλημμέλημα και μόνο με το μέσο αυτό μπορεί να κατορθωθεί ή να διευκολυνθεί η βεβαίωση του εγκλήματος, η ανακάλυψη και σύλληψη των δραστών ή η βεβαίωση και αποκατάσταση της ζημιάς που προκλήθηκε. Επιπλέον, κατά τη διεξαγωγή μιας έρευνας θα πρέπει να τηρούνται και οι βασικές αρχές της αναγκαίας αναλογίας, της αναγκαιότητας και της απαγορεύσεως του υπέρμετρου (πηγή: Κάρας 1996:474). Επειδή δεν υπάρχει συγκεκριμένο νομοθετικό πλαίσιο για τις διαδικτυακές έρευνες, τα πιο πάνω εφαρμόζονται κατ' αναλογία και σε περιπτώσεις ηλεκτρονικών εγκλημάτων. Επομένως, μια έρευνα στην οποία δεν έχουν τηρηθεί οι προβλεπόμενες προϋποθέσεις, θα επηρεάσει την αποδεικτικότητα των στοιχείων που συλλέχτηκαν.

Κατά την διεξαγωγή μιας έρευνα αυτό που διακυβεύεται είναι η ιδιωτικότητα του ατόμου. Το Αμερικανικό Σύνταγμα απαιτεί την ύπαρξη εντάλματος για τη διεξαγωγή μιας έρευνας, το οποίο εκδίδεται αν υπάρχει πιθανή αιτία, ότι διαπράχθηκε ένα έγκλημα. Το ένταλμα θα πρέπει να καθορίζει επακριβώς το μέρος και τα αντικείμενα που θα ερευνηθούν. Για παράδειγμα, εάν η πιθανή αιτία υποδεικνύει ότι τα αποδεικτικά στοιχεία είναι αποθηκευμένα σε ένα CD, η αστυνομία δεν έχει το δικαίωμα να ερευνήσει κάθε υπολογιστή που υπάρχει

στο χώρο για την εύρεση συμπληρωματικών στοιχείων. Αν το πράξει, έστω και αν βρει επιπρόσθετα αποδεικτικά στοιχεία, αυτά δεν θα έχουν αποδεικτική αξία στο δικαστήριο, γιατί παραβιάστηκε το ένταλμα (πηγή: Wegman, 2004).

Ένα άλλο νομικό ζήτημα, που σχετίζεται με υποθέσεις που εμπλέκονται αποδεικτικά στοιχειά σε ψηφιακή μορφή, είναι το κατά πόσο τα προσόντα ενός επιστημονικού ερευνητή επαρκούν για τη διεκπεραίωση μιας ηλεκτρονικής έρευνας. Υπάρχει προβληματισμός για τα εργαλεία λογισμικού που χρησιμοποίησε αφού ο ερευνητής απλά γνωρίζει τη χρήση του εργαλείου και δεν γνωρίζει τον πηγαίο κώδικα άρα δεν μπορεί να ξέρει τι εργασίες επιτελεί το λογισμικό. Πώς μπορεί λοιπόν να βεβαιώσει ότι τα ψηφιακά δεδομένα που συλλέχθηκαν αποδεικνύουν την ενοχή ή την αθωότητα του κατηγορουμένου; Έως σήμερα δεν υπάρχει απόφαση δικαστηρίου που να απέρριπτε την επιστημονική άποψη του ερευνητή δεν αποκλείεται όμως αυτό να συμβεί στο μέλλον αφού τα εργαλεία λογισμικού εξελίσσονται και γίνονται πιο πολύπλοκα.

Το τελευταίο ζήτημα αφορά την ανάλυση και διατήρηση των αποδεικτικών στοιχείων. Είναι κοινή πρακτική των διωκτικών αρχών η αντιγραφή του μέσου αποθήκευσης, που θα εξεταστεί δημιουργώντας ένα ακριβές αντίγραφο του πρωτοτύπου. Τα δικαστήρια έχουν αποδεχθεί ότι αφού τα αντίγραφα είναι ακριβές τότε θεωρούνται γνήσια. Ωστόσο πρέπει να λαμβάνονται τα απαραίτητα μέτρα για την άρτια διατήρηση τους. Για παράδειγμα, στην υπόθεση Ohio v. Cook, ο κατηγορούμενος παρουσίασε μια σειρά από ισχυρισμούς έναντι της μη ορθής διατήρησης των ψηφιακών αποδείξεων, που οδήγησαν στην αλλοίωση τους, όπως η μη τοποθέτηση του σκληρού δίσκου που αφαιρέθηκε σε αντιστατική θήκη. Το δικαστήριο λαμβάνοντας υπόψη τα παραπάνω, καθώς και μια σειρά από άλλες παραλήψεις των διωκτικών αρχών κατά τη διατήρηση των ψηφιακών στοιχείων, έκρινε τον κατηγορούμενο αθώο λόγω αμφιβολιών.

6.7 ΑΣΤΥΝΟΜΙΑ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η αντιμετώπιση του ηλεκτρονικού εγκλήματος, από τις υπηρεσίες επιβολής του νόμου και ιδιαίτερα την αστυνομία είναι το πρώτο σημαντικό ζήτημα. Ο παραδοσιακός τρόπος προσέγγισης του εγκλήματος, δηλαδή να γίνει περιγραφή του δράστη με κατάθεση από το θύμα, συλλογή πληροφοριών από πληροφοριοδότες, να διεξαχθεί έρευνα, κατάσχεση κ.λπ. δεν ισχύουν στον κυβερνοχώρο. Για την έρευνα του ηλεκτρονικού εγκλήματος απαιτούνται εξειδικευμένες αστυνομικές υπηρεσίες με εκπαιδευμένο προσωπικό και σύγχρονα τεχνικά μέσα.

Οι πρώτες υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος, ιδρύθηκε στις Ηνωμένες Πολιτείες της Αμερικής, αφού από εκεί ξεκίνησε το hacking, στα μέσα της δεκαετίας του ’70 και επίσης αναπτύχθηκε η τεχνολογία των ηλεκτρονικών υπολογιστών και το Διαδίκτυο. Σήμερα, στις Η.Π.Α. λειτουργούν υπηρεσίες αντιμετώπισης και δίωξης του ηλεκτρονικού εγκλήματος σε κάθε πολιτεία, οι οποίες έχουν τοπικές αρμοδιότητες. Οι απειλές, όμως, που προβάλλουν από το οργανωμένο έγκλημα μέσω του κυβερνοχώρου, οδήγησαν στη σύσταση της US-CERT (United States Computer Emergency Readness Team) μιας εθνικής υπηρεσίας που έχει κύρια ευθύνη την ασφάλεια των Η.Π.Α. από επιθέσεις που μπορεί να προκύψουν από τον κυβερνοχώρο. Η US-CERT αποτελεί το υπηρεσιακό κομμάτι της NCSD (National Cyber Security Division), η οποία με τη σειρά της υπάγεται στο Υπουργείο Εσωτερικών. Οι κύριες αρμοδιότητες της US-CERT είναι:

► Η ανάλυση των πιθανών διαδικτυακών απειλών και ευπαθειών και η καταβολή προσπαθειών για τον περιορισμό τους.

► Η ενημέρωση των συναρμόδιων υπηρεσιών για πιθανές δικτυακές απειλές.

► Ο συντονισμός των ενεργειών αντιμετώπισης συμβάντων σχετικών με το Διαδίκτυο.

Σε επίπεδο εξέτασης ψηφιακών τεκμηρίων, το Ομοσπονδιακό Γραφείο Ερευνών (Federal Bureau Of Investigation – FBI) διαθέτει το πιο σύγχρονο εργαστήριο στον κόσμο. Το εξειδικευμένο προσωπικό της Computer Analysis and Response Team, είναι εξοπλισμένο με τα απαιτούμενα εργαλεία υλικού και λογισμικού, εξετάζει πάσης φύσεως ψηφιακά δεδομένα και υπολογιστικά

συστήματα, έχει τη δυνατότητα για ανάλυση και ανάκτηση αρχείων, σπάσιμο κωδικών, προσδιορισμό του χρόνου και της σειράς δημιουργίας των αρχείων κ.α.

Στην Αγγλία έχει ιδρυθεί Μονάδα Ηλεκτρονικού Εγκλήματος στην Μητροπολιτική Αστυνομία, για την αντιμετώπιση των απειλών με ηλεκτρονικούς υπολογιστές, που οριοθετούνται από το ισχύον νομικό πλαίσιο και ειδικότερα τη Computer Misuse Act 1990. Επίσης στον Καναδά έχει ιδρυθεί η Integrated Technological Crime Unit στην Royal Mounted Police.

Στην Αυστραλία έχει συσταθεί το Australian High Tech Crime Centre το οποίο υπάγεται στην Ομοσπονδιακή Αστυνομία. Σκοπός του είναι ο συντονισμός των εθνικών προσπαθειών για την πάταξη του ηλεκτρονικού εγκλήματος, καθώς αναγνωρίζει ότι η αντιμετώπιση του γίνεται ακόμη πιο δύσκολη από πλήθος εμποδίων νομικών και μη. Για το σκοπό αυτό συνεργάζονται και με άλλες υπηρεσίες στον κόσμο, με τις οποίες μπορεί από κοινού να ερευνήσουν υποθέσεις παράνομης δραστηριότητας στο Διαδίκτυο και να ανταλλάξουν τεχνογνωσία.

Στην Ελλάδα η αντιμετώπιση των υποθέσεων ηλεκτρονικού εγκλήματος από την Ελληνική Αστυνομία, ουσιαστικά, άρχισε με την ίδρυση του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος το 2004. Έως τότε οι υποθέσεις που σχετίζονταν με οποιοδήποτε τρόπο με ηλεκτρονικούς υπολογιστές αντιμετωπίζονταν από το Τμήμα Δίωξης Οικονομικού Εγκλήματος.

Το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής ιδρύθηκε με το Π.Δ. 100/2004, έχοντας αρμοδιότητες την δίωξη των εγκλημάτων, που διαπράττονται στο Διαδίκτυο ή με τη χρήση του εντός της περιοχή δικαιοδοσίας της Διεύθυνσης Ασφάλειας Αττικής, καθώς και την επί 24ώρου βάσεως παρακολούθηση του Διαδικτύου, προς διαπίστωση εγκληματικών πράξεων, που τελούνται στη χώρα και την διαβίβαση όλων των απαραίτητων σχετικών στοιχείων στις αρμόδιες υπηρεσίες.

Επίσης με το Π.Δ. 48/2006 ιδρύθηκε Τμήμα Δίωξης Ηλεκτρονικού εγκλήματος στην Υποδιεύθυνση Δίωξης Οικονομικού Εγκλήματος της Γενικής Αστυνομικής Διεύθυνσης Θεσσαλονίκης, με αρμοδιότητες την εντός της περιοχής δικαιοδοσίας της Διεύθυνσης Ασφαλείας Θεσσαλονίκης, δίωξη των εγκλημάτων που διαπράττονται στο Διαδίκτυο ή με τη χρήση αυτού.

Η ύπαρξη των εργαστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών βοηθά το έργο των πιο πάνω υπηρεσιών. Στο Εργαστήριο Γραφολογίας λειτουργεί Τομέας Εξέτασης Ψηφιακών Τεκμηρίων, ο οποίος:

► Εξετάζει, αναγνωρίζει και συγκρίνει ψηφιακά δεδομένα ή αρχεία τα οποία βρίσκονται σε αποθηκευτικούς χώρους Η/Υ ή σε περιφερειακά συστήματα.

► Εξετάζει την γνησιότητα λογισμικού.

► Εξετάζει κινητά τηλέφωνα ή άλλες ηλεκτρονικές συσκευές, οι οποίες περιέχουν ή αποθηκεύουν ψηφιακά δεδομένα.

► Εξετάζει και αναγνωρίζει δεδομένα σε μαγνητικές ταινίες πιστωτικών ή άλλων καρτών και εξετάζει άλλα σύγχρονα μέσα ψηφιακής αποθήκευσης δεδομένων σε ηλεκτρονικό κύκλωμα ή άλλη μορφή αποθηκευτικούς χώρους.

► Βοηθά τεχνικά σε διαδικασίες κατάσχεσης, μεταφοράς, αποθήκευσης και αποστολής των ψηφιακών τεκμηρίων, που σχετίζονται με εγκληματική δραστηριότητα.

► Τηρεί αρχείο των εργαστηριακών εξετάσεων που γίνονται καθώς και συλλογές ψηφιακών πειστηρίων, λογισμικών και συσκευών ψηφιακής αποθήκευσης, για βοήθεια των συγκριτικών εξετάσεων.

Η πρώτη υπόθεση που απασχόλησε το εργαστήριο ήταν το 1995. Στη συνέχεια οι υποθέσεις πολλαπλασιάστηκαν. Σήμερα το εργαστήριο διαθέτει εξειδικευμένο προσωπικό και τεχνικά μέσα για την διεκπεραίωση απαιτητικών εργασιών.

6.8 ΛΟΓΙΣΜΙΚΟ ΔΙΕΡΕΥΝΗΣΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Η διερεύνηση του ηλεκτρονικού εγκλήματος από τις αρμόδιες αρχές απαιτεί τη χρήση κατάλληλου λογισμικού. Οι πληροφορίες, που αποθηκεύονται σε ένα υπολογιστή ή διακινούνται μέσω ενός δικτύου, δεν είναι δυνατόν να

ανακτηθούν και να εξεταστούν με φυσικό τρόπο. Τα πακέτα λογισμικού που δημιουργούνται για την κάλυψη αναγκών των διωκτικών αρχών και των εργαστηρίων εξέτασης ψηφιακών τεκμηρίων έχουν εξελιχθεί σημαντικά τα τελευταία χρόνια επιτυγχάνοντας την ακρίβεια των δεδομένων που ανακτώνται, την ταχύτητα ανάκτησης τους και τη δυνατότητα επεξεργασίας μεγάλου όγκου δεδομένων για την εύρεση των αναγκαίων πληροφοριών.

EnCase Forensics

Το λογισμικό EnCase Forensics της εταιρείας Guidance Software, χρησιμοποιείται από τις πιο σημαντικές υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος, όπως το FBI και η Scotland Yard, καθώς και από κρατικές και στρατιωτικές υπηρεσίες και οργανισμούς. Το λογισμικό χρησιμοποιείται επίσης από εργαστήρια εξέτασης ψηφιακών τεκμηρίων, καθώς εκτός από τις δυνατότητες ανάκτησης και αρχείων που έχουν διαγραφεί ή αποκρυφτεί σε ένα ηλεκτρονικό υπολογιστή, έχει τη δυνατότητα να επεξεργάζεται, σε πολύ λίγο χρόνο, τεράστιες ποσότητες δεδομένων.

Βασικά χαρακτηριστικά:

► Υποστηρίζει όλα τα συστήματα αρχείων και όλα τα λειτουργικά συστήματα. Δίνεται ακόμη και η δυνατότητα αξιοποίησης του σε συστοιχίες δίσκων (RAIDS).

► Κατά τη διάρκεια της διαδικασίας δημιουργίας αντιγράφων των υπό εξέτασης δίσκων και άλλων αποθηκευτικών μέσων γίνεται, επανειλημμένως, έλεγχος για την ακρίβεια των δεδομένων. Στο τέλος γίνεται ένας ακόμη οριστικός έλεγχος με τον αλγόριθμο MD5, για να είναι βέβαιο ότι το αρχείο αποδείξεων είναι πιστό (bit to bit) αντίγραφο του αρχικού δίσκου.

► Τα αρχεία που εξετάζονται μπορούν να ταξινομηθούν με βάση τριάντα διαφορετικά κριτήρια. Επίσης, μπορούν να εφαρμοστούν φίλτρα και να γίνουν ερωτήματα για γρηγορότερη ανάκτηση των επιθυμητών δεδομένων.

► Μπορούν να ανακτηθούν διαγραμμένα αρχεία, swap και page files, να ερευνηθεί η slack area κ.α.

► Υποστηρίζει Unicode και έτσι μπορούν να αναγνωστούν αρχεία σε οποιαδήποτε γλώσσα.

► Το πρόγραμμα δημιουργεί αυτόματα ένα χάρτη με όλα τα αρχεία που συνδέονται μεταξύ τους, ώστε ο ερευνητής να μπορεί να ελέγξει τη διαδρομή, που ακολουθούν τα αρχεία σε ένα σύστημα.

► Αναγνωρίζει αυτόματα όλες τις συσκευές (hardware), που είναι συνδεδεμένες στο σύστημα δίνοντας πρόσθετες πληροφορίες, όπως το είδος, η εταιρεία κατασκευής, η έκδοση κ.α.

► Ανακτά αυτόματα τα εφεδρικά αρχεία, που δημιουργούνται από εφαρμογές όπως αυτές που περιλαμβάνονται στη σουίτα Microsoft Office.

► Περιέχει εξελιγμένες δυνατότητες αναζήτησης αρχείων.

► Έχει τη δυνατότητα να δημιουργεί αναλυτικές αναφορές για δικαστική χρήση, ανάλογα με τις επιθυμίες του χρήστη. Για παράδειγμα, μπορεί να δημιουργήσει μια αναφορά, που να περιλαμβάνει μια λίστα με τις διευθύνσεις που επισκέφτηκε ο χρήστης στο Διαδίκτυο, ταξινομημένες κατά ημέρα και ώρα, έχοντας επισημάνει με έντονη γραφή αυτές που σχετίζονται άμεσα με την εξεταζόμενη υπόθεση.

► Περιέχει εξειδικευμένα εργαλεία για την έρευνα μηνυμάτων ηλεκτρονικού ταχυδρομείου και την δραστηριότητα στο Διαδίκτυο.

► Με τη γλώσσα προγραμματισμού EnScript, που έχει ενσωματωθεί στο λογισμικό, ο ερευνητής μπορεί να δημιουργήσει δικά του σενάρια για να επιταχύνει κάποιες διαδικασίες ανάλογα με την έρευνα που επιτελεί.

Computer Incident Response Suite (CIRS)

Το CIRS αποτελεί το κορυφαίο πακέτο λογισμικού της εταιρείας New Technologies Int. Απευθύνεται σε οργανισμούς, κρατικούς και μη και σε υπηρεσίες επιβολής νόμου. Περιλαμβάνει εικοσιένα διαφορετικά προγράμματα, για την αντιμετώπιση κάθε ανάγκης κατά την έρευνα ενός ηλεκτρονικού υπολογιστή.

LiveWire Investigator

Ο LiveWire Investigator, της εταιρείας λογισμικού Wetstone, αποτελεί ένα σύγχρονο εργαλείο. Το κύριο χαρακτηριστικό του είναι ότι μπορεί να κάνει πλήρη ανάλυση του υπολογιστή-στόχου, χωρίς να απαιτηθεί να τερματιστεί η λειτουργία του. Η σύνδεση του με τον υπολογιστή-στόχο μπορεί να πραγματοποιηθεί απευθείας, είτε απομακρυσμένα με τη χρήση ασφαλούς

σύνδεσης τοπικού δικτύου, χωρίς να απαιτείται η εγκατάσταση ειδικού λογισμικού. Η εξέταση του υπολογιστή-στόχου πραγματοποιείται, ενώ αυτός συνεχίζει να λειτουργεί κανονικά. Η δυνατότητα αυτή επιτρέπει στο λογισμικό:

► Να καταγράφει τις μεταβολές, που πραγματοποιούνται από τις τρέχουσες διαδικασίες στα αρχεία καταγραφής και το μητρώο του συστήματος.

► Να συλλέγει πληροφορίες για τα προγράμματα που εκτελούνται, τις συνδέσεις δικτύου και τις μεταδόσεις δεδομένων.

► Να αποκτά πληροφορίες, που θα χάνονταν αν τερματιζόταν η λειτουργία του υπολογιστής-στόχου όπως π.χ. τις διεργασίες που εκτελούνται στο παρασκήνιο.

► Να ερευνά τυχόν, παραβατική δραστηριότητα τη στιγμή ακριβώς που εκδηλώνεται.

Wireless StrongHold Tent

Αποτελεί μια μοναδική πατέντα της εταιρείας Paraben Forensics. Είναι μια τέντα κατασκευασμένη από ειδικά υλικά (τρεις μεμβράνες από νικέλιο, χαλκό και άργυρο), οι οποίες δεν επιτρέπουν σε ασύρματα δίκτυα να έρθουν σε επαφή με κάποια ηλεκτρονική συσκευή. Χρησιμοποιείται π.χ. για τον αποκλεισμό πρόσβασης στο ασύρματο ενδοδίκτυο ενός φορητού υπολογιστή, ο οποίος εξετάζεται από τον εξερευνητή στο χώρο του οργανισμού για την εύρεση σημαντικών δεδομένων, που πιθανώς έχουν αποθηκευτεί σ' αυτό.

WinHex Editor Και X-Ways Trace

Ο WinHex Editor αποτελεί ένα ισχυρό εργαλείο λογισμικού, με το οποίο μπορούν να διεκπεραιωθούν πολλές εργασίες κατά την έρευνα ενός υπολογιστή για την εύρεση ψηφιακών αποδείξεων. Στην έκδοση forensics, που προορίζεται για τις υπηρεσίες επιβολής του νόμου, περιλαμβάνονται διάφορα χαρακτηριστικά, όπως αντιγραφή δίσκων, ανάκτηση αρχείων, αναζήτηση αρχείων, αυτόματη επεξεργασία των αρχείων καταγραφής, αυτόματη αναγνώριση εγγραφών του Office και PDF που έχουν κρυπτογραφηθεί κ.α.

Το X-Ways Trace είναι πολύ πιο απλό και ισχυρό εργαλείο για την άντληση πληροφοριών, σχετικά με τη δραστηριότητα ενός υπολογιστή στη Διαδίκτυο. Έχει τη δυνατότητα να εξάγει πληροφορίες από τα αρχεία index.dat, που δημιουργούνται από τον φυλλομετρητή Internet Explorer. Ένα αρχείο index.dat

αποτελεί μια βάση δεδομένων, στην αποθηκεύονται πληροφορίες για τις τοποθεσίες που επισκέφτηκε ο χρήστης κατά την πλοήγηση του στο Διαδίκτυο. Το κύριο χαρακτηριστικό των αρχείων αυτών είναι ότι οι πληροφορίες που περιέχουν δεν σβήνονται, όταν διαγραφεί το ιστορικό και τα προσωρινά αρχεία και γενικότερα η διαγραφή τους είναι εφικτή μόνο από έμπειρους χρήστες και μόνο με τη χρήση κατάλληλων εργαλείων λογισμικού. Επομένως, εάν εξετάσουμε τα αρχεία index.dat ενός συστήματος θα αντλήσουμε πολύ σημαντικές πληροφορίες για τις διευθύνσεις, που έχει επισκεφτεί ο χρήστης του υπολογιστή.

Στο κεφάλαιο αυτό είδαμε ότι το έργο του ερευνητή μιας υπόθεσης ηλεκτρονικού εγκλήματος δεν είναι καθόλου εύκολη. Αν και δεν υπάρχει ένα συγκεκριμένο μοντέλο έρευνας ώστε να τον καθοδηγεί, υπάρχουν πολλές λεπτομέρειες και στάδια έρευνας τα οποία μπορεί και πρέπει να εφαρμόσει για να είναι έννομη η έρευνα του και να μην αμφισβητηθεί από το δικαστήριο. Ο ίδιος ο υπολογιστής του εγκλήματος μπορεί να βοηθήσει στο έργο του εξερευνητή αφού υπάρχουν πολλά στοιχεία της υπόθεσης στα κρυφά και διαγραμμένα αρχεία, στον κάδο ανακύκλωσης, στα κρυπτογραφημένα δεδομένα κ.α. Επίσης πλέον υπάρχουν εξειδικευμένα λογισμικά διερεύνησης του ηλεκτρονικού εγκλήματος με τα οποία μπορεί να μελετήσει τα τεκμήρια, δηλαδή, τους δίσκους, τους υπολογιστές κ.α. που έχουν κατασχεθεί από τη σκηνή του εγκλήματος ώστε να βρει αποδείξεις. Το έργο της διαλεύκανσης ενός ηλεκτρονικού εγκλήματος δεν είναι καθόλου εύκολη υπόθεση αλλά η ανάπτυξη της τεχνολογίας και η αύξηση των εγκλημάτων αυτών στις μέρες μας απαιτούν να υπάρξει οργάνωση από τις αρχές ώστε να εξαλειφθεί όσο γίνεται το φαινόμενο πλέον αυτών των εγκλημάτων.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Με το τέλος της πτυχιακής εργασίας μπορούμε να πούμε πλέον ότι με την ανάπτυξη της τεχνολογίας αναπτύχθηκαν δραματικά και η νέα μορφή εγκλήματος, το Ηλεκτρονικό Έγκλημα.

Ακόμη και ο πιο απλός χρήστης Η/Υ πρέπει να είναι ενημερωμένος και προετοιμασμένος ώστε να μην πέσει θύμα οποιασδήποτε επίθεσης. Πολλές φορές τα λάθη του ίδιου του χρήστη τον οδηγούν σε καταστροφή του συστήματος του. Ποτέ δεν πρέπει να ανοίγουμε e-mail αγνώστου αποστολέα ακόμη και αν το θέμα είναι δελεαστικό. Δεν πρέπει να εμπιστευόμαστε κωδικούς πρόσβασης και αριθμούς λογαριασμών σε κανένα.

Πρέπει να λαμβάνουμε προληπτικά μέτρα για την προστασία μας. Από ένα απλό antivirus πρόγραμμα μέχρι και πιο εξειδικευμένα μέτρα τα οποία πρέπει να λαμβάνουν κυρίως οι εταιρείες οι οποίες σε καμία περίπτωση δεν θα ήθελαν να πέσουν θύμα επίθεση, όχι μόνο γιατί το οικονομικό κόστος θα είναι μεγάλο αλλά και γιατί μαζί θίγετε το κύρος και η εμπιστοσύνη που της έχουν οι πελάτες της. Βιομετρικές τεχνικές για να γίνεται ακριβές έλεγχος για το ποιος μπαίνει στην εταιρεία, χρήση firewalls για την ασφάλεια των δικτύων ακόμη και κρυπτογραφία για να μην μπορούν να διαβαστούν σημαντικά αρχεία και δεδομένα σε περίπτωση κλοπής. Παράλληλα πρέπει να λαμβάνονται προληπτικά μέτρα, δηλαδή, να υπάρχουν Συστήματα Ανίχνευση Επιθέσεων ώστε να μπορεί να εντοπιστεί κάθε κακόβουλη ενέργεια, να κρατείται back up αρχείων ώστε σε περίπτωση καταστροφής να μην χαθούν σημαντικά δεδομένα-αρχεία. Τέλος ο καθένας θα πρέπει να προστατεύει το πληροφοριακό του σύστημα και από φυσικές καταστροφές.

Επίσης το κάθε κράτος θα πρέπει να ενημερώσει τους πολίτες του για τη νέα αυτή μορφή εγκλήματος ώστε να είναι προετοιμασμένοι να αντιμετωπίσουν τέτοιου είδους επιθέσεις. Ακόμη θα πρέπει να υπάρξει οργάνωση και παράλληλα με την ανάπτυξη της τεχνολογίας να ενημερώνεται η νομοθεσία και να θεσπίζονται νέοι νόμοι. Βλέπουμε ότι στην Ελλάδα αν και υπογράφηκε η Σύμβαση για το Κυβερνοχώρο ακόμη δεν έχει εφαρμοστεί. Με το Ηλεκτρονικό

Έγκλημα ασχολούνται κυρίως αστυνομικοί που απλά τους ενδιαφέρει το θέμα. Πρέπει να υπάρξει εξειδικευμένο προσωπικό το οποίο να εκπαιδεύεται συνεχώς, παράλληλα με την εξέλιξη της τεχνολογίας. Μόνο αν η ίδια η πολιτεία ασχοληθεί συνειδητά με το Ηλεκτρονικό Έγκλημα μόνο τότε θα υπάρξει οργάνωση και τα κατάλληλα μέτρα για να βρεθούν λύσεις.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

1) Αγγέλη Ι.(2001), Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον Κυβερνοχώρο
2) Βλαχόπουλος Κ. (2007), Ηλεκτρονικό Έγκλημα, Εκδ. Νομική Βιβλιοθήκη
3) Κριθαράς Θ. (2009), Ποινικό Δίκαιο και Διαδίκτυο
4) Λάζος Γ. (2001), Πληροφορική & Έγκλημα, Εκδ. Νομική Βιβλιοθήκη
5) Μαλλέρου Α. Το Δίκαιο του Ηλεκτρονικού Χρήματος
6) Μαρκοπούλου Παγώνα (2008),Η Σύμβαση για το Κυβερνοέγκλημα
7) Νούσκαλη Γ., Απάτη με Ηλεκτρονικό Υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386^{A} ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και της Ευρωπαϊκής Ένωση, ΠοινΔικ 2003
8) Σούρης Α. (2004), Ασφάλεια της Πληροφορίας, Εκδ. Νέων Τεχνολογιών
9) Συνήγορος του Καταναλωτή (2008), Τι πρέπει να γνωρίζουν οι καταναλωτές για την προστασία τους από το ηλεκτρονικό έγκλημα
10) Τσουμάνης Χ. (2005), Ψηφιακή Εγκληματικότητα, Εκδ. Βας. Ν. Κατσαρού
11) http://www.diaplous.org/library/nomothesia.php
12) www.synigoroskatanaloti.gr
13) http://www.nouskalis.gr/Nouskalis.pdf
14) http://library.panteion.gr:8080/dspace/bitstream/123456789/678/1/papaeuthimiou.pdf
15) www.ictplus.gr/files/9_ICT.../E.../**SARAFIANOS_DIMITRIS.ppt**
16) http://www.cybercellmumbai.com/files/Types%20of%20cyber%20crime.pdf
17) http://www.intellectum.org/articles/issues/intellectum4/ITL04P043052_Kybernoegklima.pdf
18) http://library.panteion.gr:8080/dspace/bitstream/123456789/117/1/ergasia_papanikolaou.pdf
19) http://library.panteion.gr:8080/dspace/bitstream/123456789/679/1/alexandropoulos.pdf